

**A Firewall for your
Radical Network**

firewall

/'faɪəwɔːl/

noun

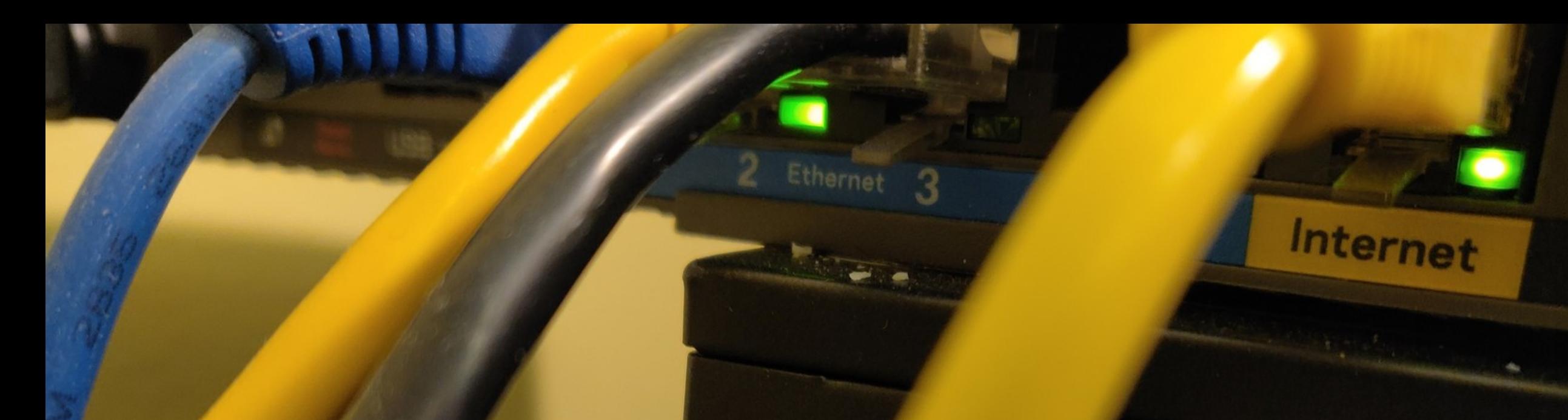
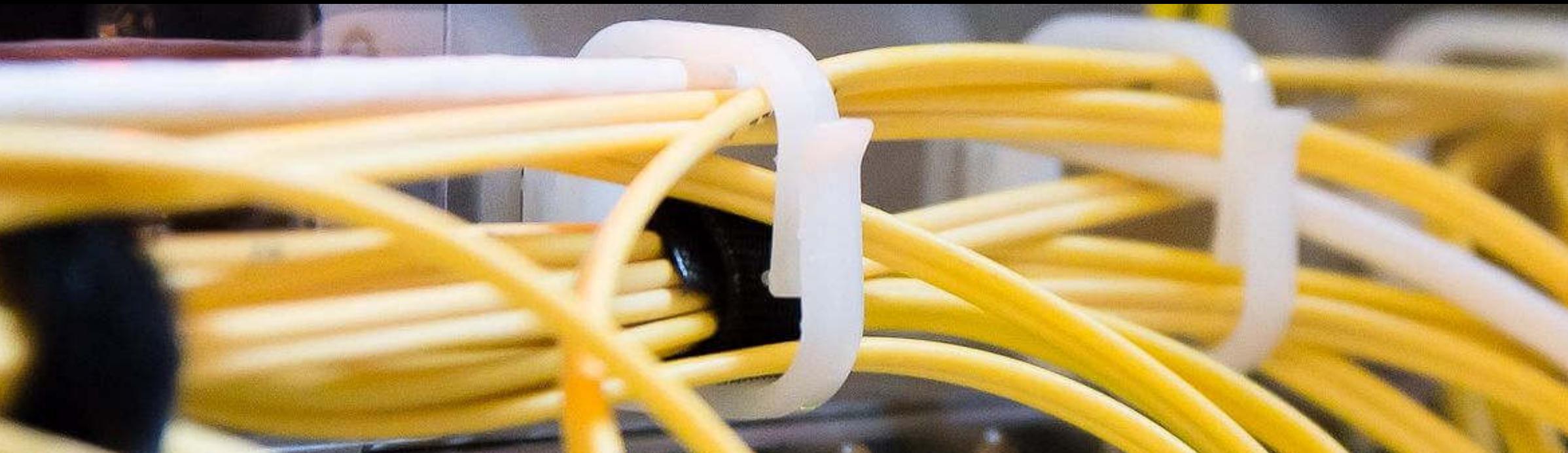
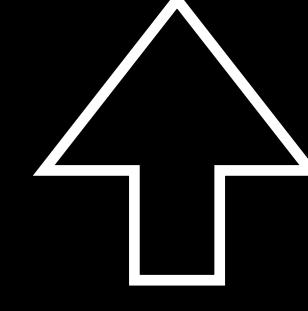
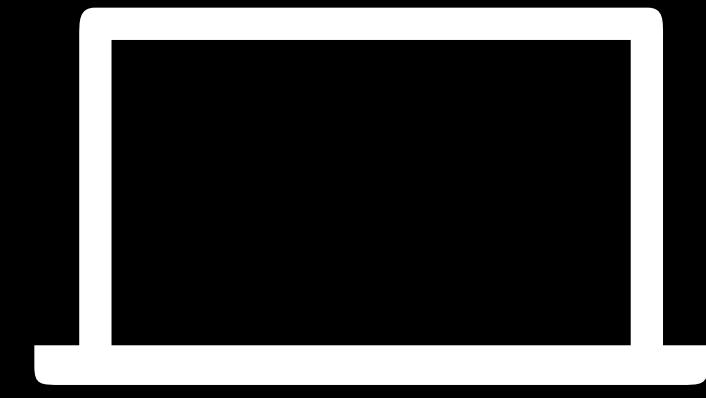
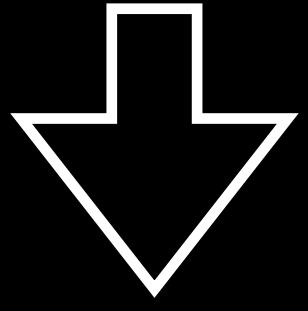
1. a wall or partition designed to inhibit or prevent the spread of fire.

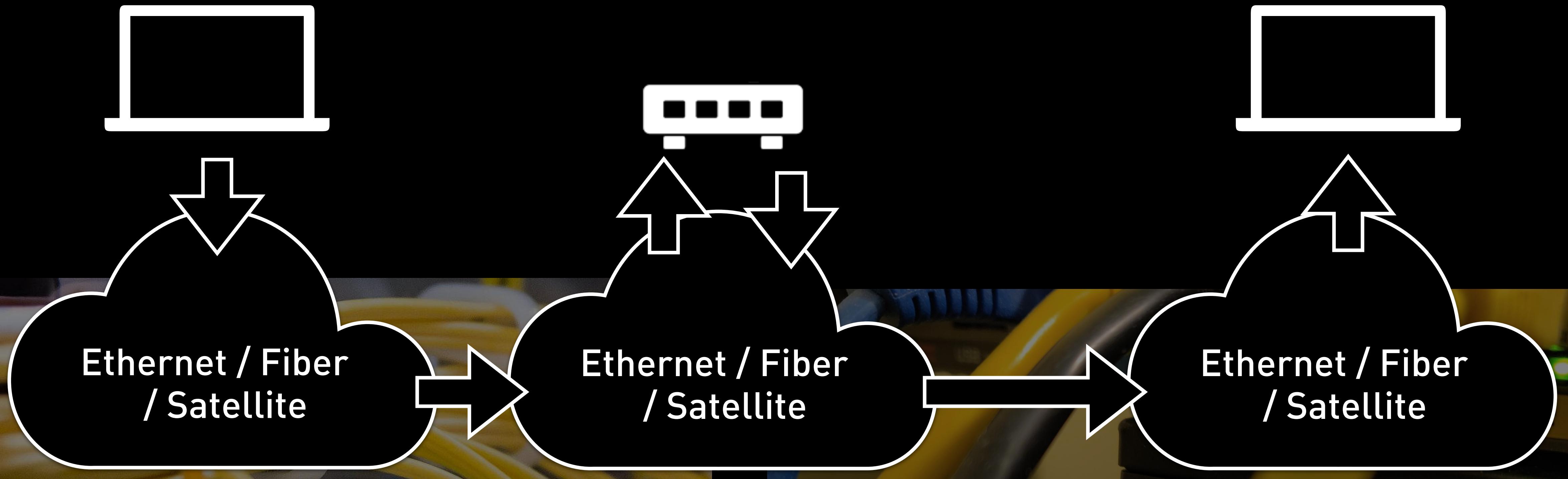
verb

2. COMPUTING: protect a network or system from unauthorized access with a firewall. "*a firewalled network*"



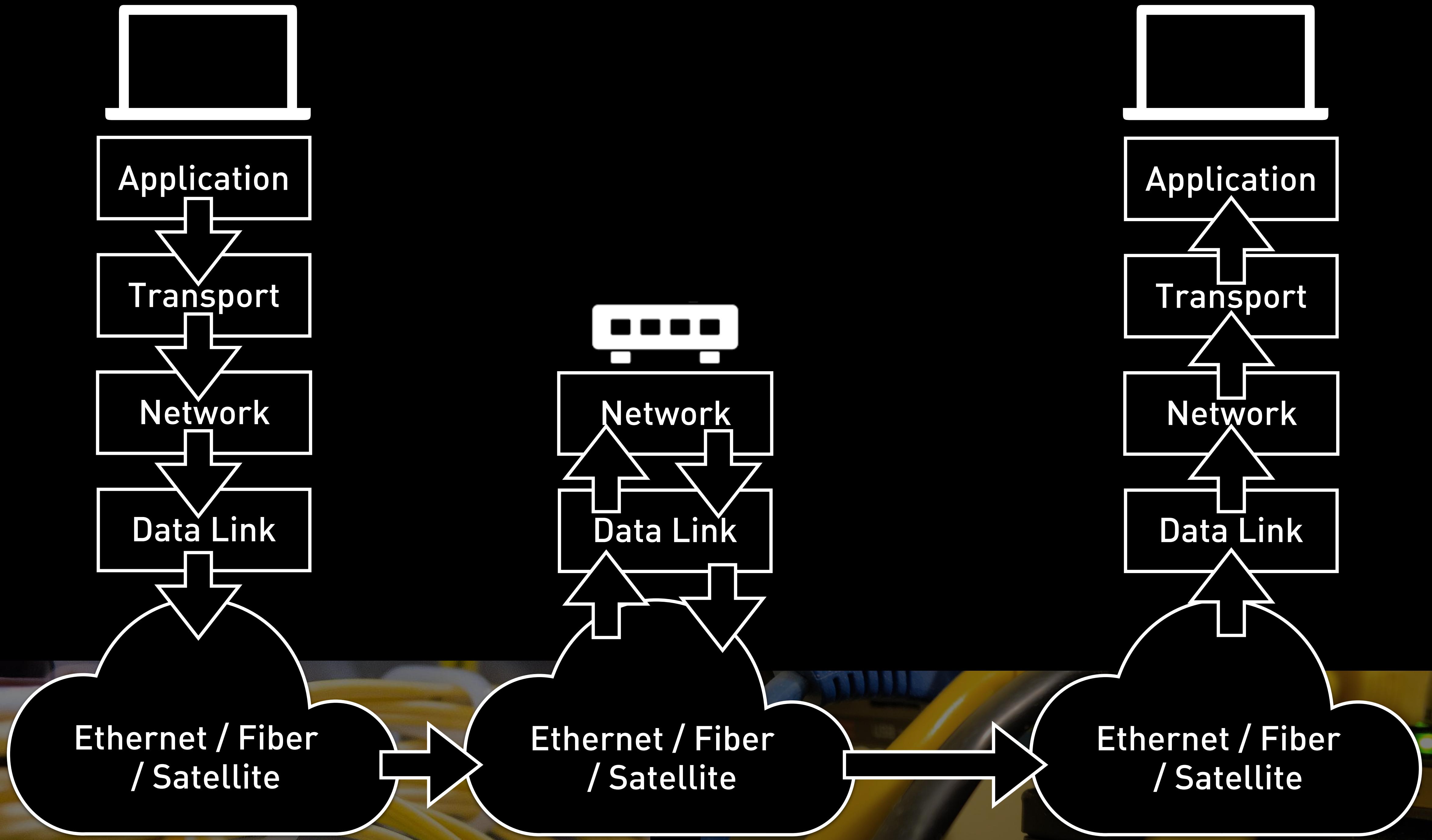
Networks

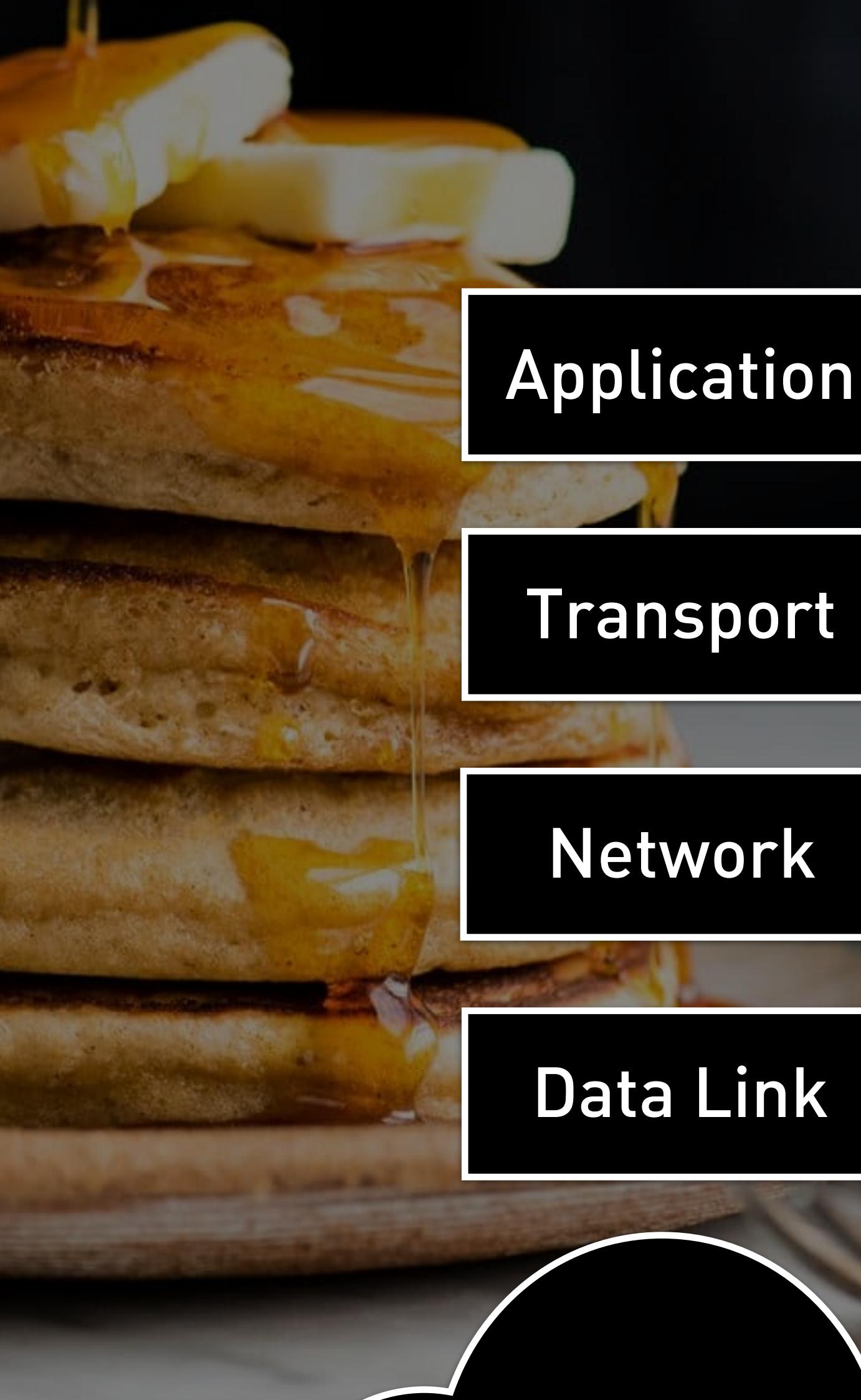






Network Layers





Application

Transport

Network

Data Link

Ethernet / Fiber
/ Satellite

HTTP

TCP

UDP

ICMP

IP

ARP

Ethernet Frame

MAC

Tunnels





**What's an
IP Address?**



+49

+49 179

+49 179 22700122



Dialing...

? . ? . ? . ?

192 . 168 . 0 . 9

0 . 0 . 0 . 0

to

255 . 255 . 255 . 255

Let's look up a
public IP address!

```
→ ~ host radicalnetworks.org | head -1  
radicalnetworks.org has address 90.187.37.21  
→ ~ |
```

LUNAR

digital VT100



Let's look up
our own
IP address!

LUNAR

digital VT100

```
→ ~ ifconfig en0 | grep inet
inet fe80::cf.bdf..655:8da3%en0 prefixle
inet 192.168.178.71 netmask 0xffffffff00 brd
inet6 2003:e9:ff0a:ed00:49d:567e:a096:5214
inet6 2003:e9:ff0a:ed00:49ab:4043:be30:33c
→ ~ |
```

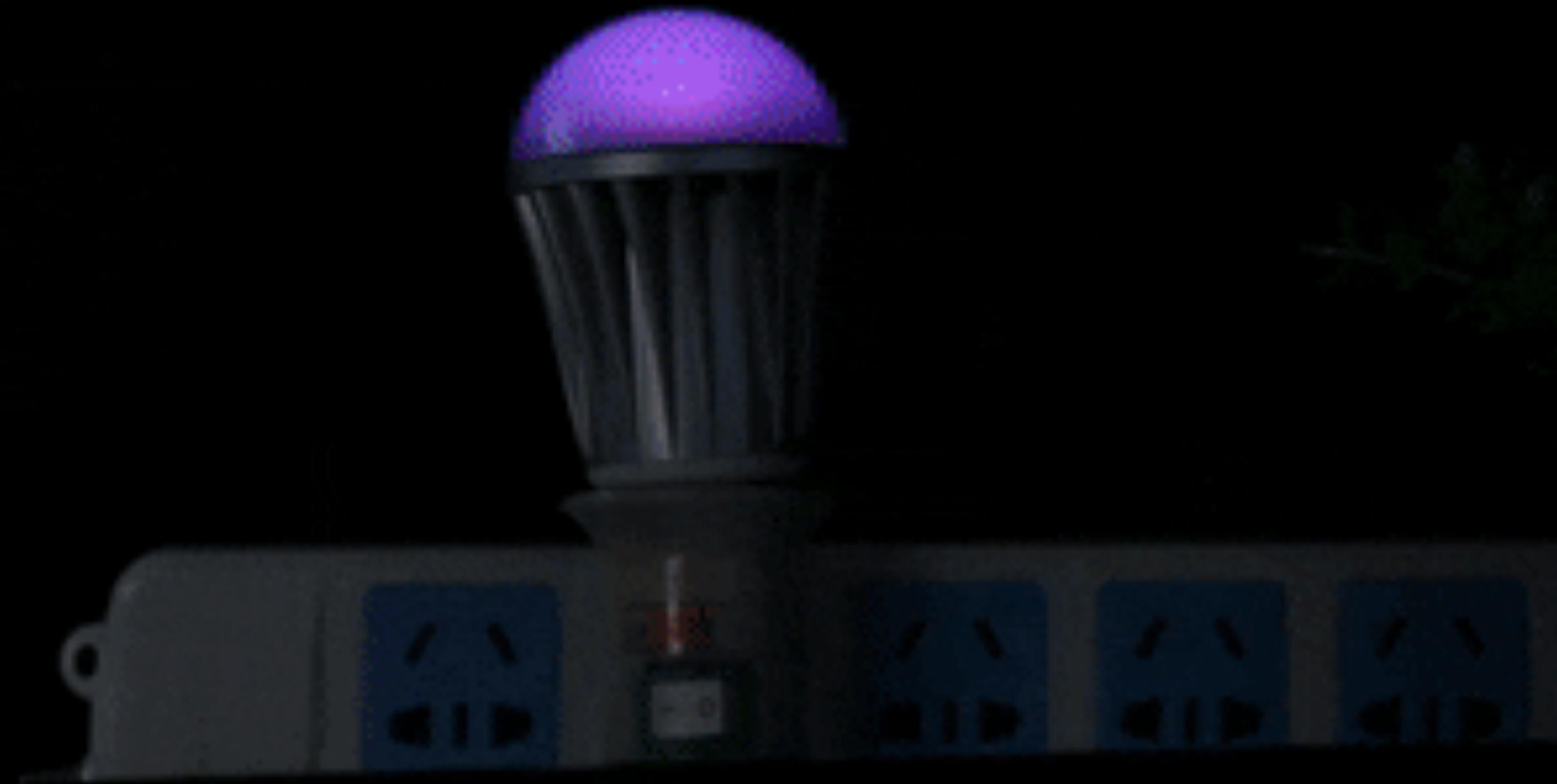
Let's send some
test packet!

```
→ ~ ping radicalnetworks.org
PING radicalnetworks.org (90.187.37.21): 56 data bytes
64 bytes from 90.187.37.21: icmp_seq=0 ttl=54 time=44.265 ms
64 bytes from 90.187.37.21: icmp_seq=1 ttl=54 time=41.654 ms
^C
--- radicalnetworks.org ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 41.654/42.960/44.265/1.305 ms
→ ~ █
```

LUNAR

digital VT100





How NAT works









Public IP Address

90.187.37.21



x.x.x.x

Private IP Address

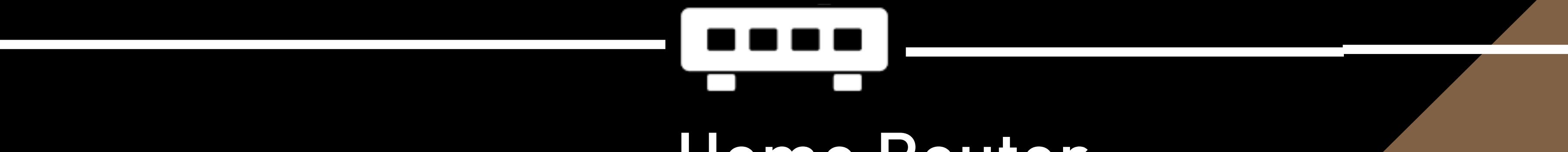
192.168.1.9



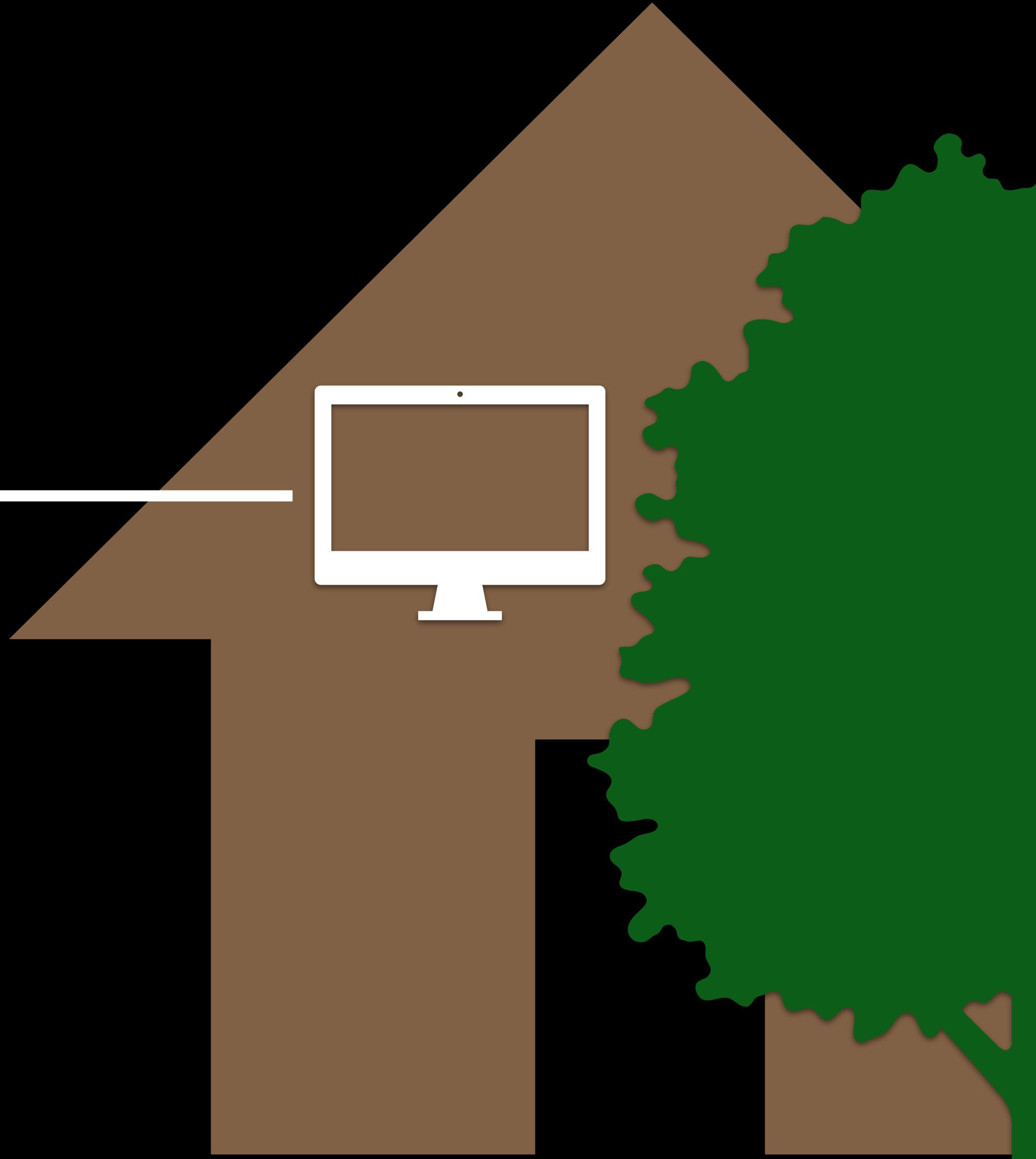
10.x.x.x

Publicly registered!!!

192.168.x.x

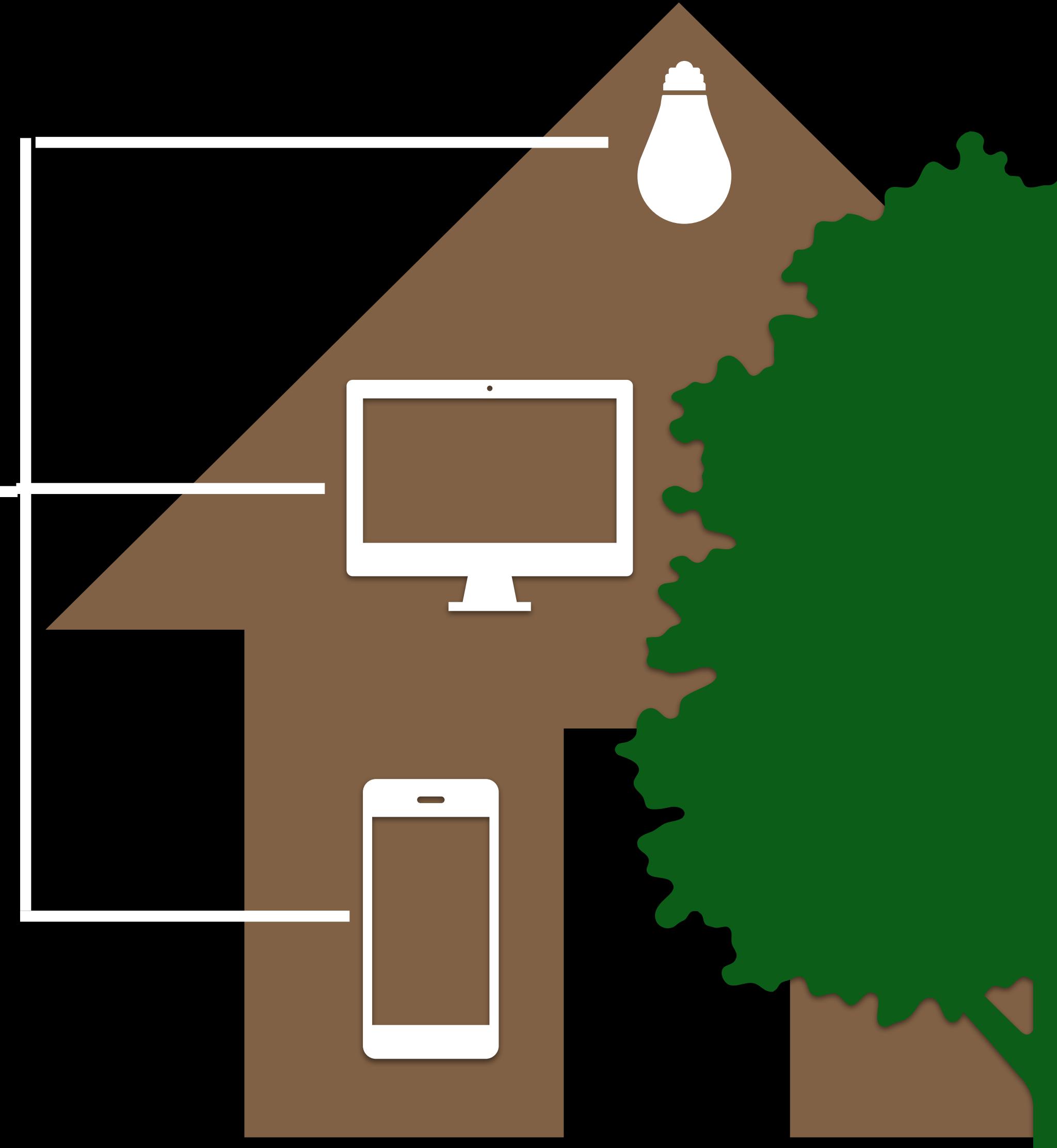


Home Router





Home Router



Internet
Provider



90.187.37.21

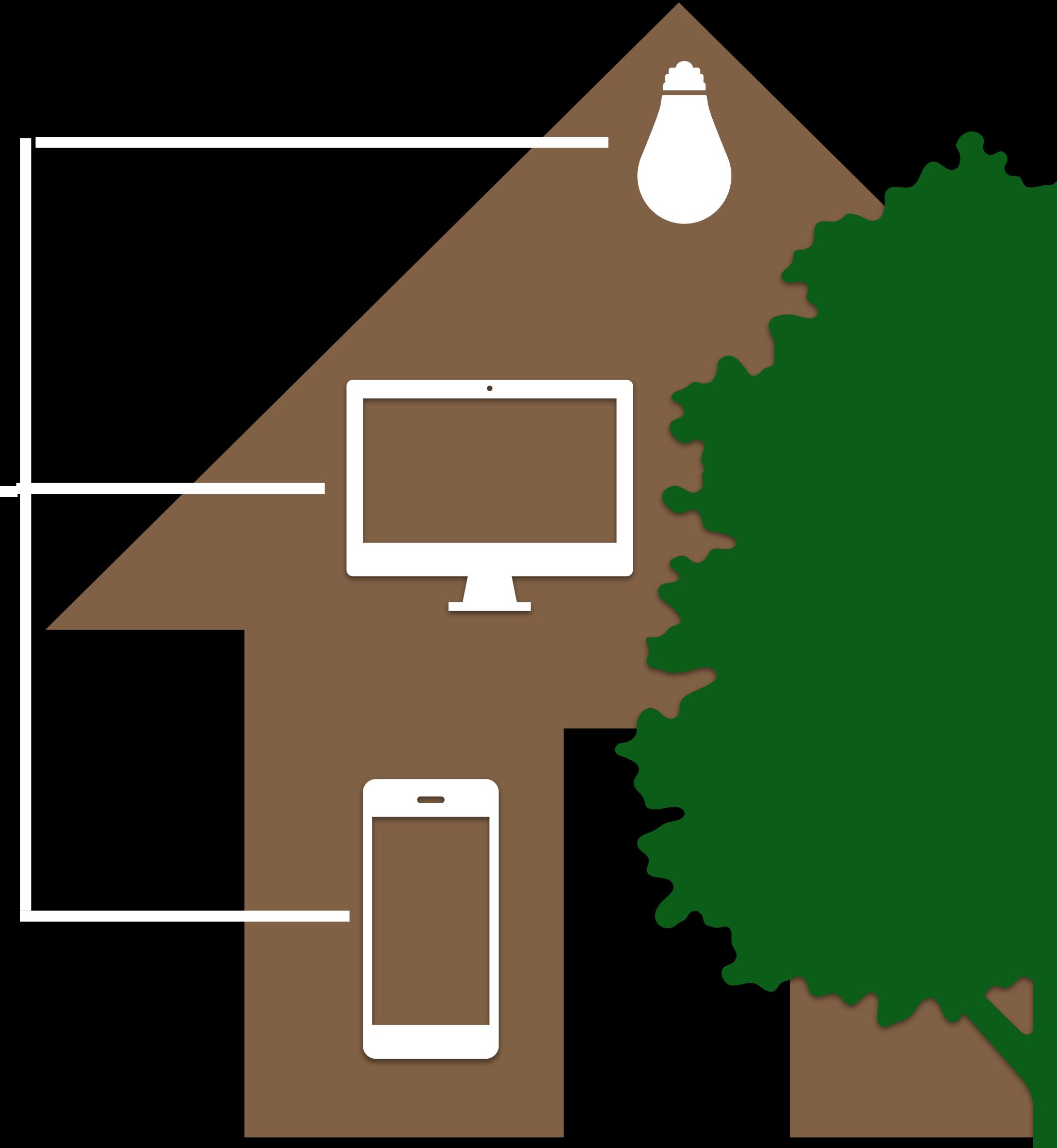
90.187.37.42

90.187.37.6

Internet
Provider



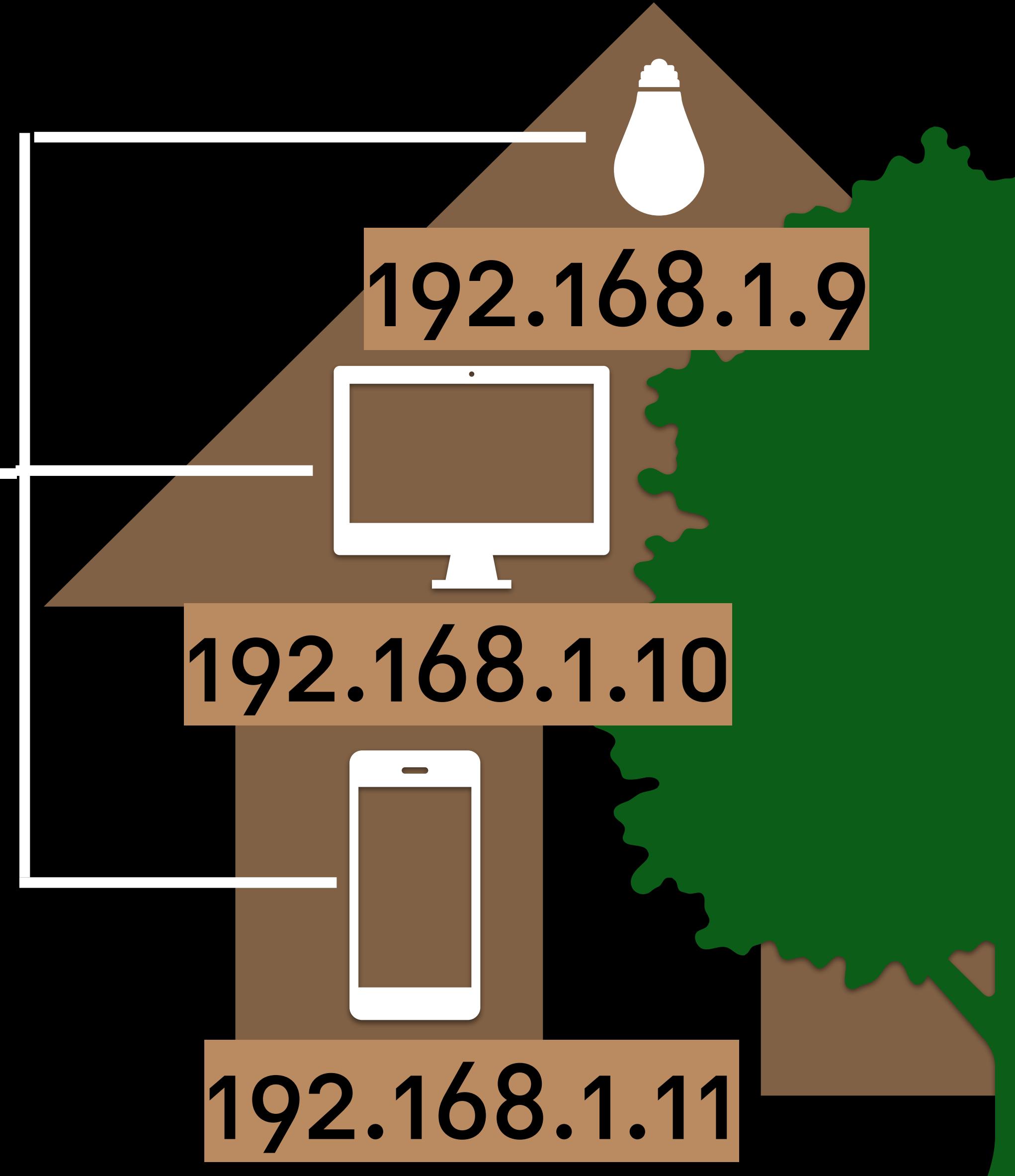
Home Router
90.187.37.21



Internet
Provider



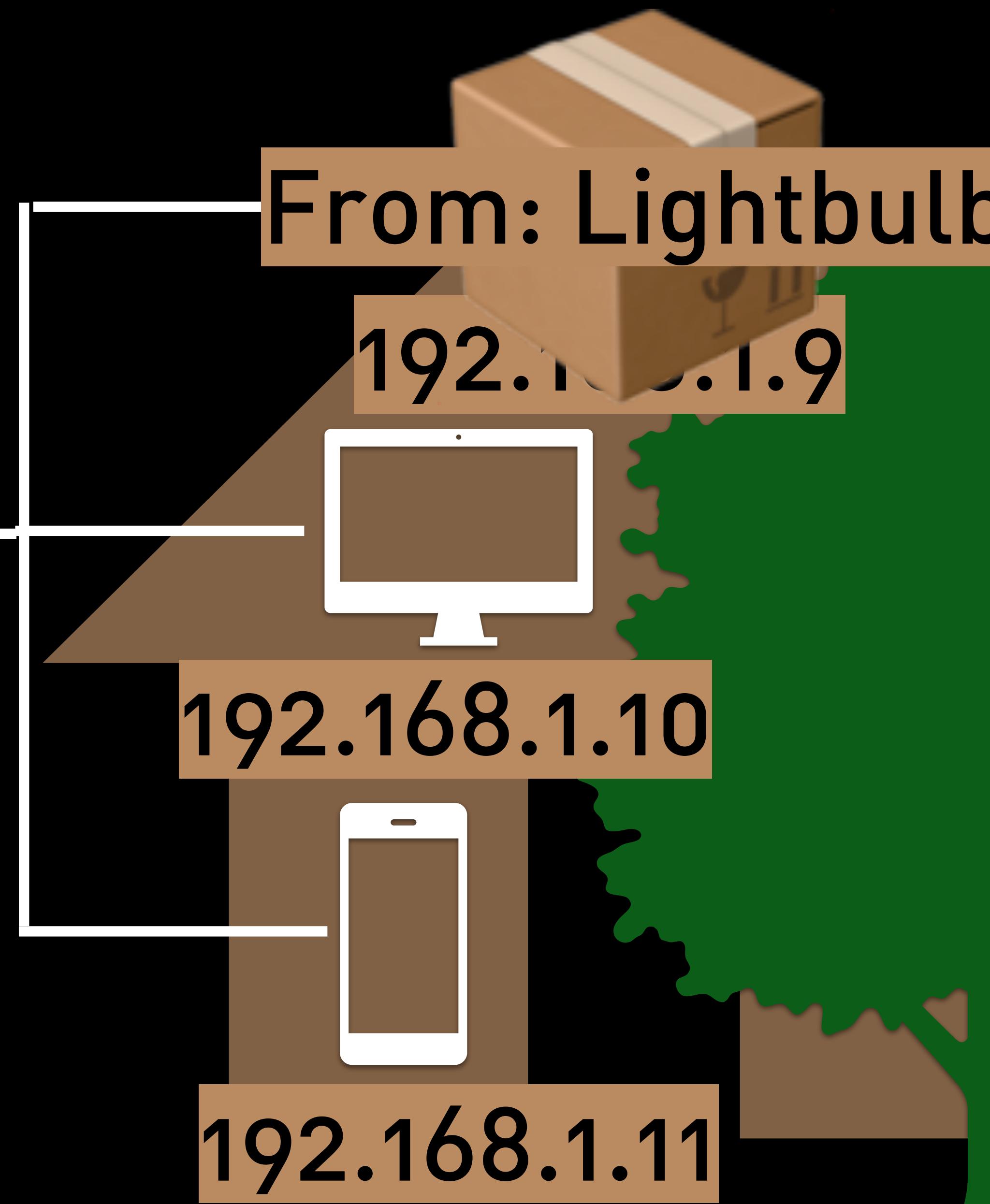
Home Router
90.187.37.21



Internet
Provider



Home Router
90.187.37.21



Internet
Provider

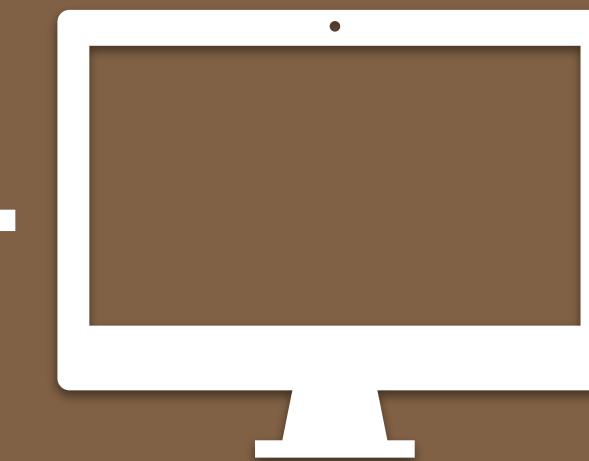


Home Router
90.187.37.21

From: Lightbulb



192.168.1.9



192.168.1.10



192.168.1.11

Internet
Provider

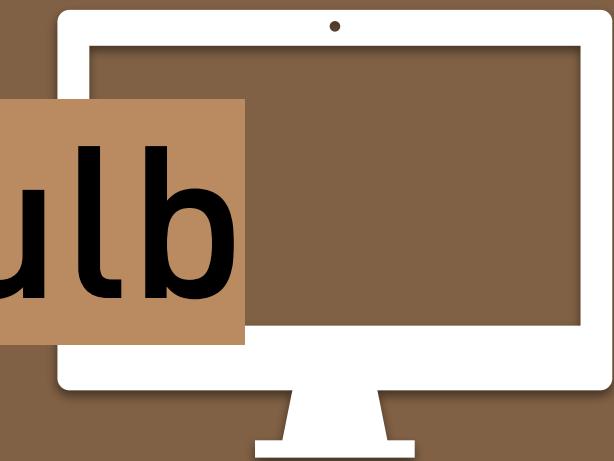


Home Router

90.187.37.21

From: Lightbulb

192.168.1.9



192.168.1.10



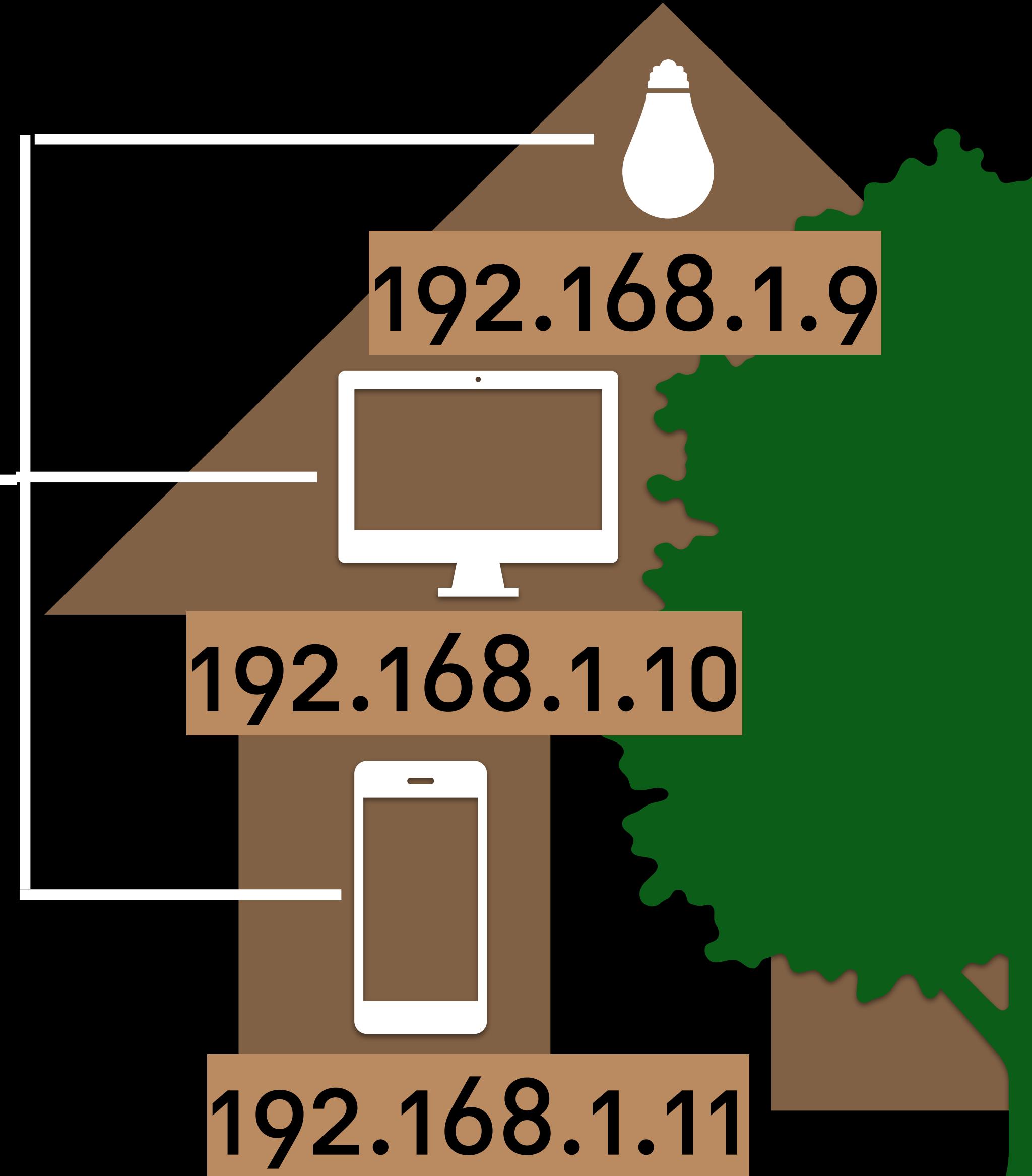
192.168.1.11

Internet
Provider

From: Lightbulb

Home Router

90.187.37.21

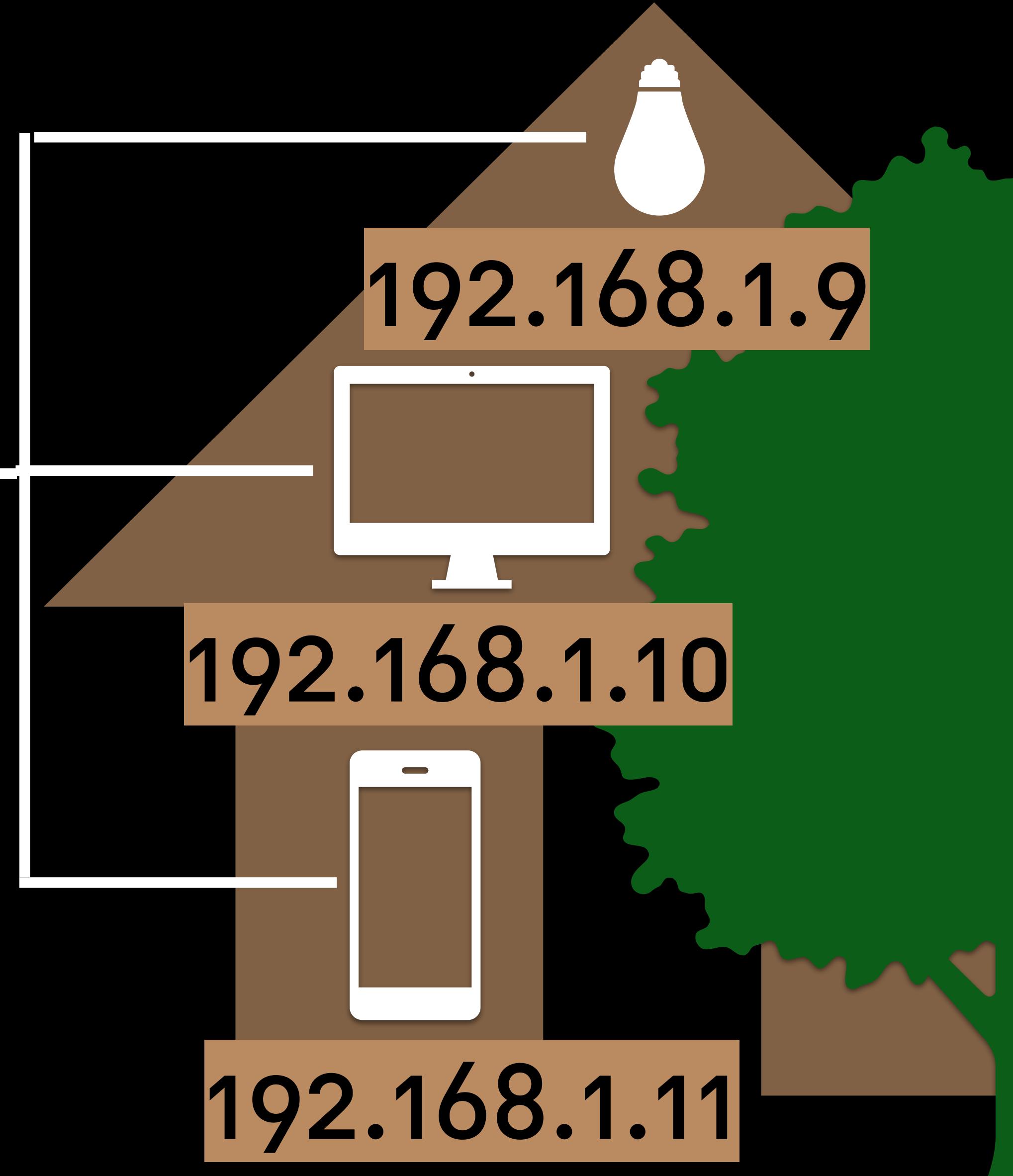


Internet
Provider

From: Router

To: Router

90.187.37.21



IN THE FUTURE™:



2003:cd:ebd1:f200:144b:4e7e:6c7:57bc

? : ? : ? : ? : ? : ? : ? : ? : ? : ?

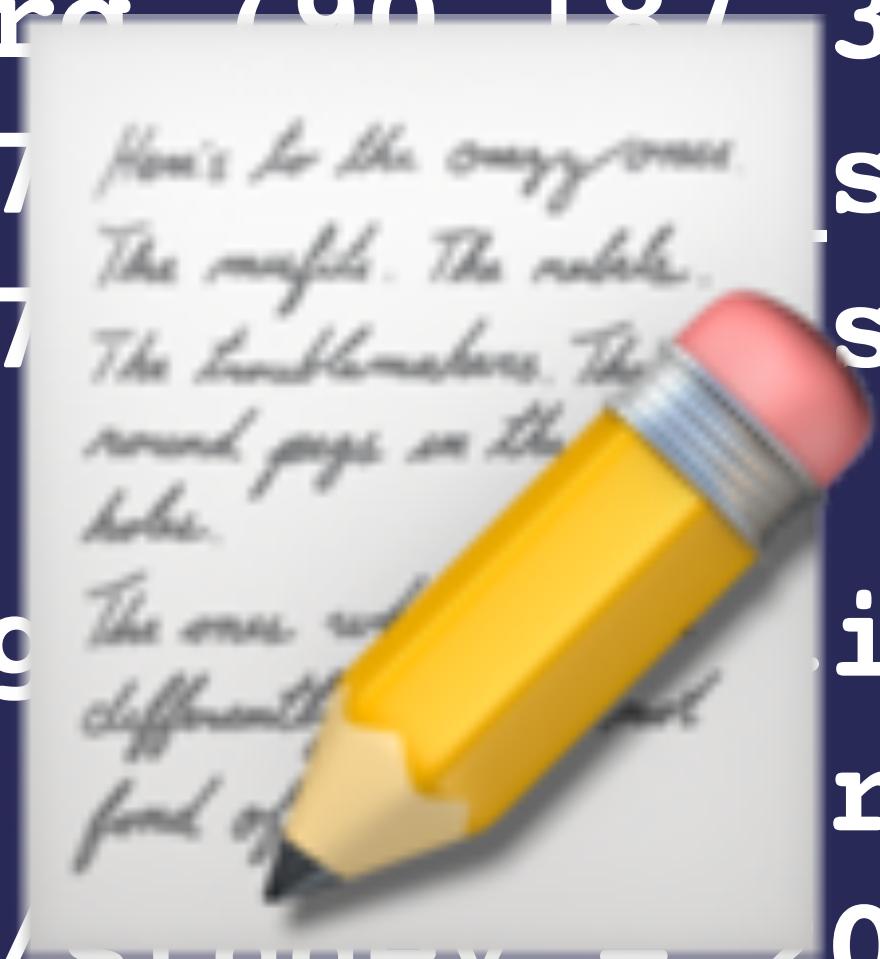
0 - ffffff

Network Protocols





```
→ ~ ping radicalnetw...  
PING radicalnetworks.org (90.187.37.21): 56 data bytes  
64 bytes from 90.187.37.21: icmp_seq=0 ttl=55 time=22.743 ms  
64 bytes from 90.187.37.21: icmp_seq=1 ttl=55 time=20.487 ms  
^C  
--- radicalnetworks.org ping statistics ---  
2 packets transmitted, 2 packets received, 0.0% packet loss  
round-trip min/avg/max/stddev = 20.487/21.615/22.743/1.128 ms
```



→ ~ ping radicalnetworks.org

```
PING radicalnetworks.org (90.187.37.21): 56 data bytes
64 bytes from 90.187.37.21: seq=0 ttl=55 time=22.743 ms
64 bytes from 90.187.37.21: seq=1 ttl=55 time=20.487 ms
^C
--- radicalnetworks.org statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 20.487/21.615/22.743/1.128 ms
```



→ ~ sudo tcpdump -e -n -i en0 icmp -w ping.pcap



→ ~ wireshark ping.pcap

trace.pcap

Apply a display filter ... <⌘/>

No. Time Source Destination Protocol Length Info

→ 1 0.000000 192.168.1.9 90.187.37.21 ICMP 98 Echo (ping) request id=0xef45, seq=0/0...

← 2 0.023830 90.187.37.21 192.168.1.9 ICMP 98 Echo (ping) reply id=0xef45, seq=0/0...

▶ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▶ Ethernet II, Src: Apple_11:17:c6 (b8:e8:56:11:17:c6), Dst: ZyxelCom_95:13:2a (a0:e4:cb:95:13:2a)
▶ Internet Protocol Version 4, Src: 192.168.1.9, Dst: 90.187.37.21
▶ Internet Control Message Protocol

	0000	a0 e4 cb 95 13 2a b8 e8 56 11 17 c6 08 00 45 00*.. V.....E.
0010	00 54 e3 60 00 00 40 01 55 c7 c0 a8 01 09 5a bb	.T.`...@. U.....Z.	
0020	25 15 08 00 b6 0b ef 45 00 00 5d 9b 2f 5f 00 07	%.....E ..]./_...	
0030	da a9 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15	
0040	16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 !"#\$%	

trace Packets: 2 · Displayed: 2 (100.0%) · Load time: 0:0:0 · Profile: Default

More Tools

→ ~ sudo mtr radicalnetworks.org

My traceroute [v0.93]							
	2019-10-10T12:17:17+0200						
Host	Packets	Pings					
	Loss%	Snt	Last	Avg	Best	Wrst	StDev
1. 192.168.1.1	90.9%	12	4.2	4.2	4.2	4.2	0.0
2. 62.52.200.178	66.7%	12	12.0	12.4	11.1	15.2	1.9
3. ae15-0.0002.dbrx.02.ber.de.net.t	72.7%	12	10.9	10.8	10.4	11.0	0.4
4. ae1-0.0002.prrx.02.ber.de.net.te	54.5%	12	11.3	13.9	10.8	21.5	4.5
5. b-grad-rt-peer-1.bcix.de	81.8%	12	12.4	13.0	12.4	13.7	0.9
6. ip5886ed96.static.kabel-deutschl	90.9%	12	12.1	12.1	12.1	12.1	0.0
7. ip5886edb3.static.kabel-deutschl	75.0%	12	13.2	12.4	11.9	13.2	0.7
8. ip5886c230.static.kabel-deutschl	72.7%	12	12.5	12.4	11.9	12.7	0.4
9. 83-169-179-179-isp.superkabel.de	70.0%	11	14.5	41.4	14.0	95.7	47.0
10. rxe0.weise7.org	80.0%	11	21.3	20.6	19.8	21.3	1.1

**Secure
Protocols?**

```
→ ~ curl https://box.linse.me/secret.txt  
don't tell :)
```

https.pcap

Apply a display filter ... <%> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.9	178.63.212.185	TCP	78	60213 → 443 [SYN] Seq=0 Win=65535 L
2	0.026596	178.63.212.185	192.168.1.9	TCP	74	443 → 60213 [SYN, ACK] Seq=0 Ack=1
3	0.026724	192.168.1.9	178.63.212.185	TCP	66	60213 → 443 [ACK] Seq=1 Ack=1 Win=1
4	0.036381	192.168.1.9	178.63.212.185	TLSv1...	289	Client Hello
5	0.062504	178.63.212.185	192.168.1.9	TCP	66	443 → 60213 [ACK] Seq=1 Ack=224 Win
6	0.063241	178.63.212.185	192.168.1.9	TLSv1...	1506	Server Hello
7	0.063903	178.63.212.185	192.168.1.9	TLSv1...	1506	Certificate [TCP segment of a reass
8	0.063911	178.63.212.185	192.168.1.9	TLSv1...	221	Server Key Exchange, Server Hello D
9	0.064033	192.168.1.9	178.63.212.185	TCP	66	60213 → 443 [ACK] Seq=224 Ack=2881
10	0.064034	192.168.1.9	178.63.212.185	TCP	66	60213 → 443 [ACK] Seq=224 Ack=3036
11	0.068118	192.168.1.9	178.63.212.185	TLSv1...	192	Client Key Exchange, Change Cipher
12	0.095794	178.63.212.185	192.168.1.9	TLSv1...	117	Change Cipher Spec, Encrypted Hand

► Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
► Ethernet II, Src: Apple_11:17:c6 (b8:e8:56:11:17:c6), Dst: ZyxelCom_95:13:2a (a0:e4:cb:95:13:2a)
► Internet Protocol Version 4, Src: 192.168.1.9, Dst: 178.63.212.185
► Transmission Control Protocol, Src Port: 60213, Dst Port: 443, Seq: 0, Len: 0

0000	a0 e4 cb 95 13 2a b8 e8 56 11 17 c6 08 00 45 00*.. V.....E.
0010	00 40 00 00 40 00 40 06 f2 0d c0 a8 01 09 b2 3f	.@...@.?.
0020	d4 b9 eb 35 01 bb 87 23 a4 28 00 00 00 00 b0 02	...5....# .(.....
0030	ff ff b0 c4 00 00 02 04 05 b4 01 03 03 06 01 01
0040	08 0a 22 7a 02 d6 00 00 00 00 04 02 00 00	."z....

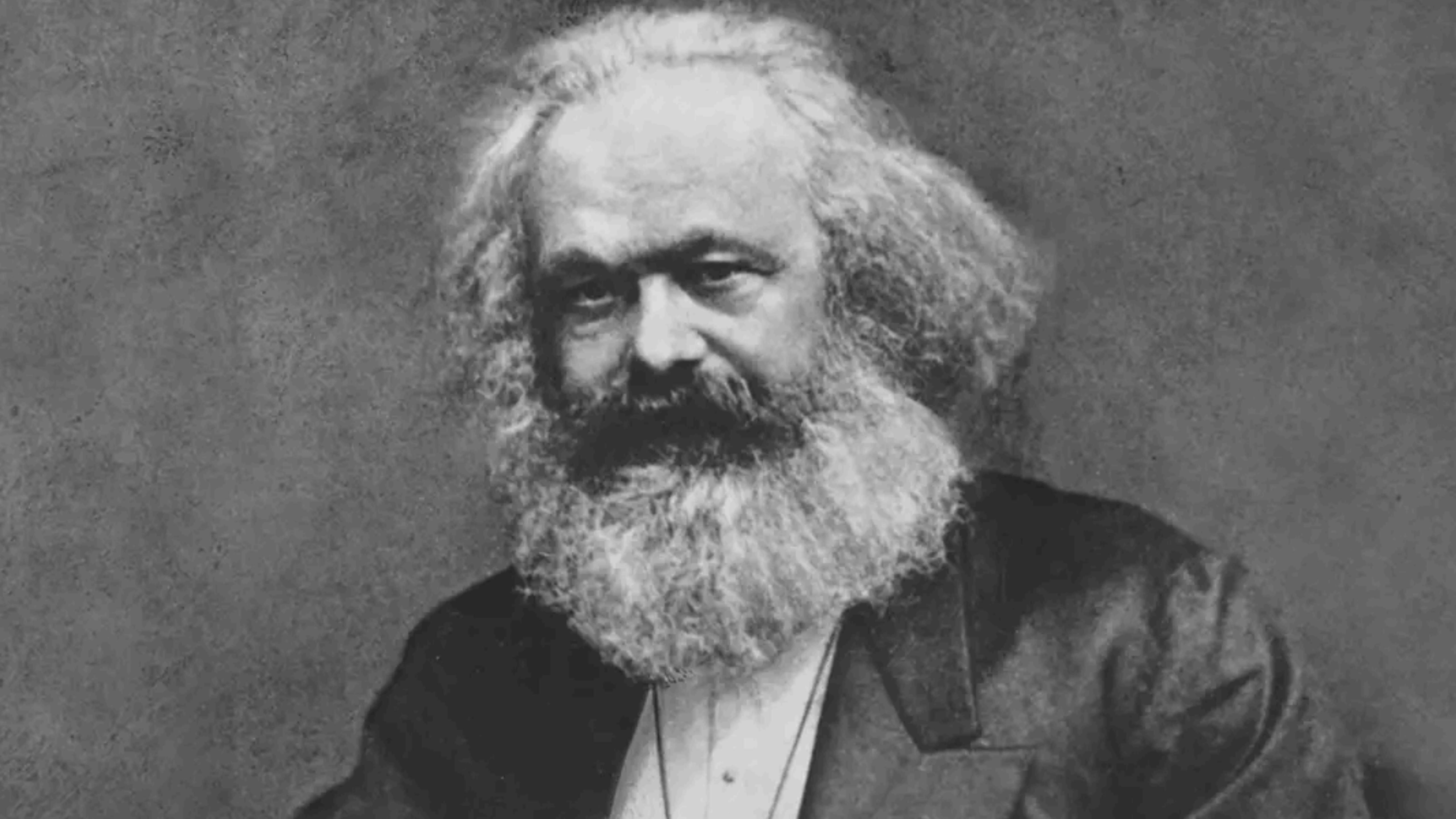
Transmission Control Protocol (tcp), 44 bytes

Packets: 21 · Displayed: 21 (100.0%) · Load time: 0:0.7 · Profile: Default

Wireshark · Follow TCP Stream (tcp.stream eq 0) · https

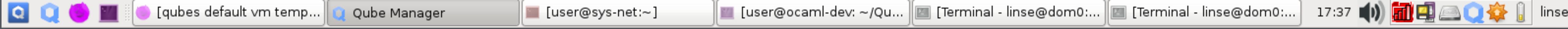
```
.....( .a.P.....,6Bo....E..d...K.E6...T.0.,..($...
...k.9.....=5...../.+'.#... ...g.3...E...<./...A.....
....Y.....box.linse.me.....
.....
.....h2.http/1.1....]...Y.w...4....*.{./.=tB..V.TE..e+.... B..kq..
$....<A.=...}.ZKZ ....?0.....
...
...
...v0..r0..Z.....A.Q#.%q..L...}..A0
.*.H..
....0J1.0..U....US1.0....U.
.
Let's Encrypt1#0!..U....Let's Encrypt Authority X30..
190731173125Z.
191029173125Z0.1.0...U....linse.me0.."0
.*.H..
....0...
.....*..U....4..#v.6"..K.7Hr...`HB..7.....!I.5..AF \.....l.[s...^T.).&X'.S11.$0.....9..Rl....}
&.....5..FP[.B.....i..S.q..jc3..~.A.....q...{.o^..G...C...N^...wB.#?.E..{a".
g.t.IG\7h...E_ai..c.Eqh.7U.U.v.[...T.....k.1...m..Zq...b:A.....gF..p:.G%.....0...0....U.....
0...U.%..0....+.....+....0...U.....0.0...U.....8...'.....-U&..c.x...0...U.#..0....Jjc.}....9..Ee.....
0o..+.....c0a0....+....0.."http://ocsp.int-x3.letsencrypt.org0/..+....0..#http://cert.int-
x3.letsencrypt.org/0>..U...705.
blog.linse.me..box.linse.me..git.linse.me..linse.me0L..U. .E0C0...g.....07..+.....0(0&..+.....http://
cps.letsencrypt.org0....
+....y.....u..iK.&..@ ....;..>..t....(.....lIM.....F0D. V]..r.....g.Y.yf.....v._|D2)..A.
n.....z.....n.*.o;;s.w0.s\>.....v.)<Q.T.9e..P.X...o.Xz)r.....EG.x...lIM.....G0E. i.+..X.
.kmf.....W..s.fM.....*....!....D.
"[.... JH..|!.T1 `f...g....0
.*.H..
.....t..8..&...zN7.zP..Fg._`B..,E.....+...A.(.....U..X....S9..$.
1.&...QwG|...B.|..)D..@..&..d....u.,X....Y..0.^.....<v...0....3.!..>.F..G.4v12.....0..[.A.Y.
7?..>K....gQd....L*B...UR..Pj..y.p$.?(..[;NT>..,9
e....6G.k ..%..ak.o..o..
..._|B..5].9.$....vl.X....0...0...z.....
```

QubesOS



QubesOS

QubesOS



[Dom0] Qube Manager

System Qube View About

Search:

	Name	State	Template	NetVM	Disk usage	Internal	IP
1	dom0	●	AdminVM	n/a	n/a		n/a
2	debian-9		TemplateVM	n/a	3147.78 MiB		
3	fedora-29	⬇️	TemplateVM	n/a	4222.36 MiB		
4	whonix-gw-14	⬇️	TemplateVM	n/a	2106.37 MiB		
5	whonix-ws-14		TemplateVM	n/a	2565.12 MiB		
6	fetchmotron		StandaloneVM	mirage-fw-test	0.0 MiB		10.137.0.19
7	mirage-fw-test		StandaloneVM	sys-net	0.0 MiB		10.137.0.7
8	mirage-test	⬇️	StandaloneVM	default (sys-firewall)	4056.06 MiB		10.137.0.13
9	ocaml-dev	● ⬇️	StandaloneVM	sys-firewall	6987.26 MiB		10.137.0.16
10	anon-whonix	●	whonix-ws-14	sys-whonix	0.0 MiB		10.137.0.10
11	sys-net	●	fedora-29	n/a	103.01 MiB		10.137.0.5
12	whonix-ws-14-dvm		whonix-ws-14	sys-whonix	0.0 MiB		10.137.0.9
13	sys-firewall		fedora-29	sys-net	98.92 MiB		10.137.0.6
14	personal		debian-9	mirage-fw-test	0.0 MiB		10.137.0.17
15	network-testing		debian-9	mirage-fw-test	0.0 MiB		10.137.0.14
16	work		debian-9	mirage-fw-test	0.0 MiB		10.137.0.15
17	default-mgmt-dvm		fedora-29	n/a	0.0 MiB	Yes	

[ocaml-dev] user@ocaml-dev: ~/cloned/qubes-mirage-firewall

File Edit View Terminal Help

)

```
(* Main unikernel entry point (called from auto-generated main.ml). *)
let start_random_clock () =
  let start_time = Clock.elapsed_ns clock in
  (* Start qrexec agent, GUI agent and QubesDB agent in parallel *)
  let qrexec = RExec.connect ~domid:0 () in
  GUI.connect ~domid:0 () |> watch_gui;
  let qubesDB = DB.connect ~domid:0 () in

  (* Wait for clients to connect *)
  qrexec >>= fun qrexec ->
  let agent_listener = RExec.listen qrexec in
  qubesDB >>= fun qubesDB ->
  let startup_time =
    let (-) = Int64.sub in
    let time_in_ns = Clock.elapsed_ns clock in
    Int64.to_float time_in_ns /. 1e9
  in
  Log.info (fun f -> f "QubesDB and qrexec connected")
  (* Watch for shutdown requests from QubesDB *)
  let shutdown_rq =
    OS.Lifecycle.await_shutdown_request () |> ignore
  (* Set up networking *)
  let get_time () = Clock.elapsed_ns clock in
  let max_entries = Key_gen.nat_table_size in
  My_nat.create ~get_time ~max_entries >>= fun my_nat -

  (* Read network configuration from QubesDB *)
  Dao.read_network_config qubesDB >>= fun config -
  let rng i = R.generate i in
  Uplink.connect ~clock config >>= fun uplink -
  let uplink' = Uplink.send_dns_client_query in
  let stack = (uplink', Lwt_mvar.create_exn) in
  let dns_client = My_dns_client.Dns_client.create ~stack in
  let net_listener = network ~clock config in
  (* Report memory usage to XenStore *)
  unikernel.ml
```

[ocaml-dev] Qubes OS - Wikipedia - Mozilla Firefox

W Qubes OS - Wikipedia Imgur: The magic of the Internet +

Not logged in Talk Contributions Create account Log in

Article Talk Read Edit View history Search Wikipedia

Qubes OS

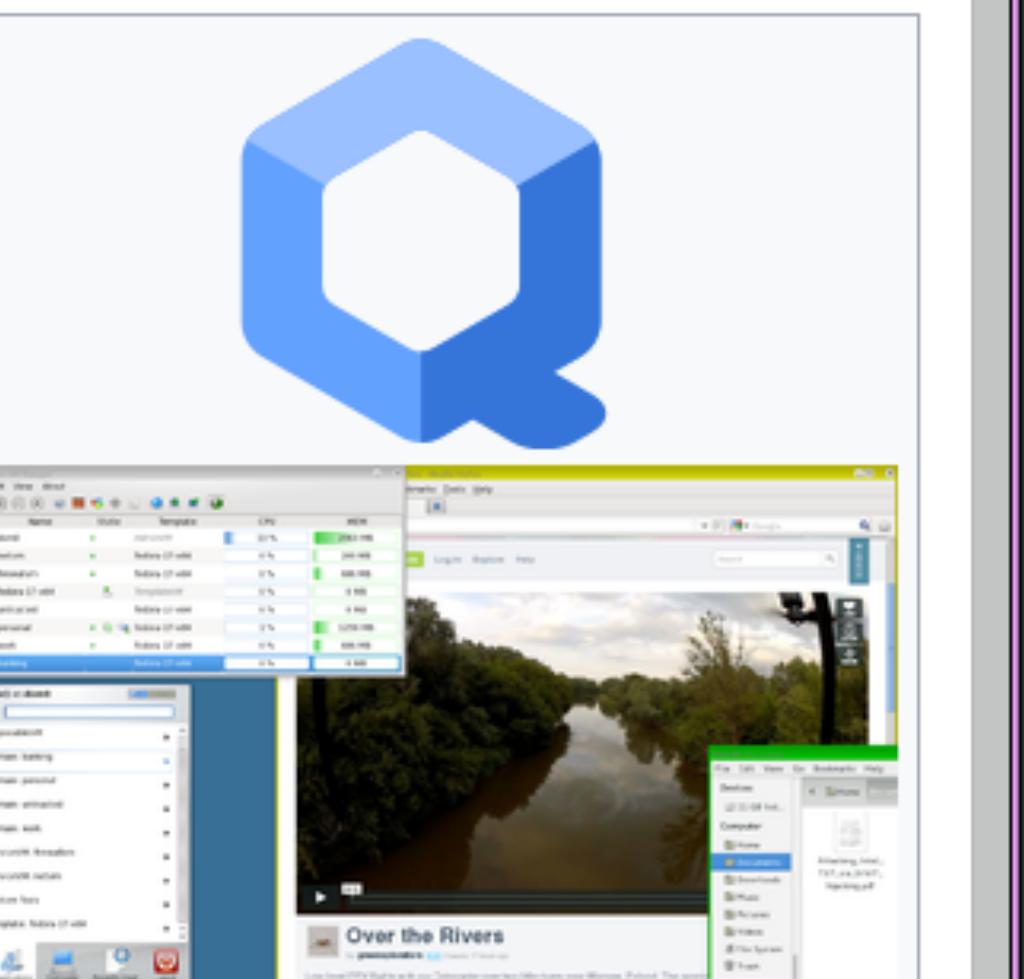
From Wikipedia, the free encyclopedia
(Redirected from Qubesos)

"Qubes" redirects here. For the arcade game, see *Q*bert's Qubes*.

Qubes OS is a security-focused desktop operating system that aims to provide security through isolation.^[6] Virtualization is performed by Xen, and user environments can be based on Fedora, Debian, Whonix, and Microsoft Windows, among other operating systems.^{[7][8]}

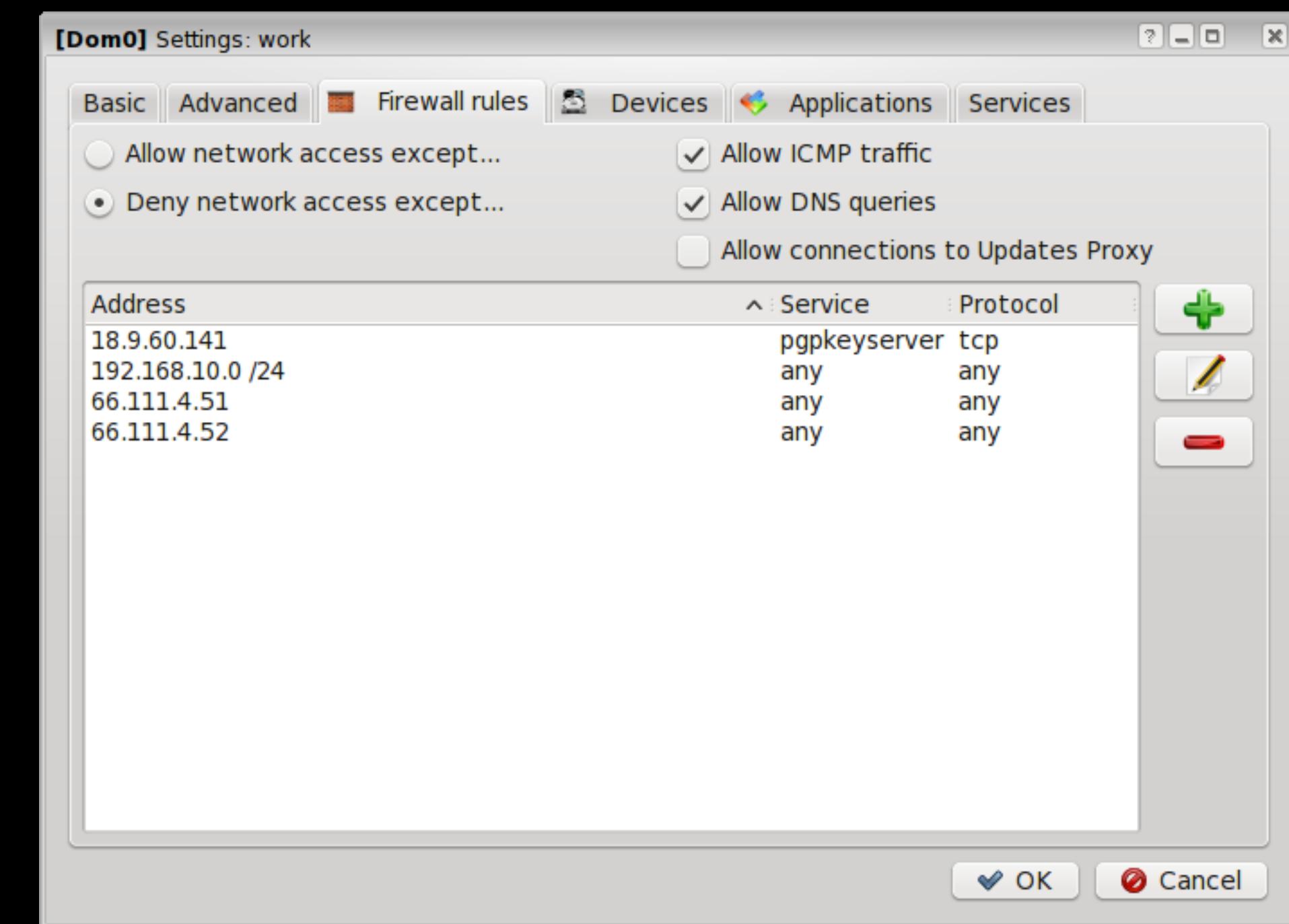
Contents [hide]

- 1 Security goals
- 2 System architecture overview
 - 2.1 Xen hypervisor and administrative domain (Dom0)
 - 2.2 Network domain
 - 2.3 Application Virtual Machines (AppVM)
- 3 Reception
- 4 See also
- 5 References



QubesOS ❤️ MirageOS

Configuring Your Firewall



Testing Your Firewall



Takeaways

- security in depth: not just patches
 - try a few tools and look at traffic
 - explore your network stack
-
- play with wireshark :D
 - don't block yourself :D

Thanks!!! ❤

Try it soon in QubesOS.

Thanks!!! ❤

Try it soon in QubesOS.



**Thanks to
Marek Marczykowski-Górecki
from Invisible Things Lab!!!**

Thanks!!! ❤

Try it soon in QubesOS.

We are **Stefanie Schirmer..**
linse.me
@linse

..and **Mindy Preston**
somerandomidiot.com
@yomimono



<https://jvns.ca/networking-zine.pdf>