What’s in a Network?

Hitesh Dharmdasani
Informant Networks

#whoami

- Security Research, Cyber Crime
- GIT > George Mason > UC Berkeley > FireEye > On Stage
- Founded Informant Networks in 2015
- Extensive research on Cyber crime and internet threats
- Currently Building Data-driven Network Security Products at Informant Networks
- I love the Internet. A LOT!
- http://hitesh.xyz

How this works?

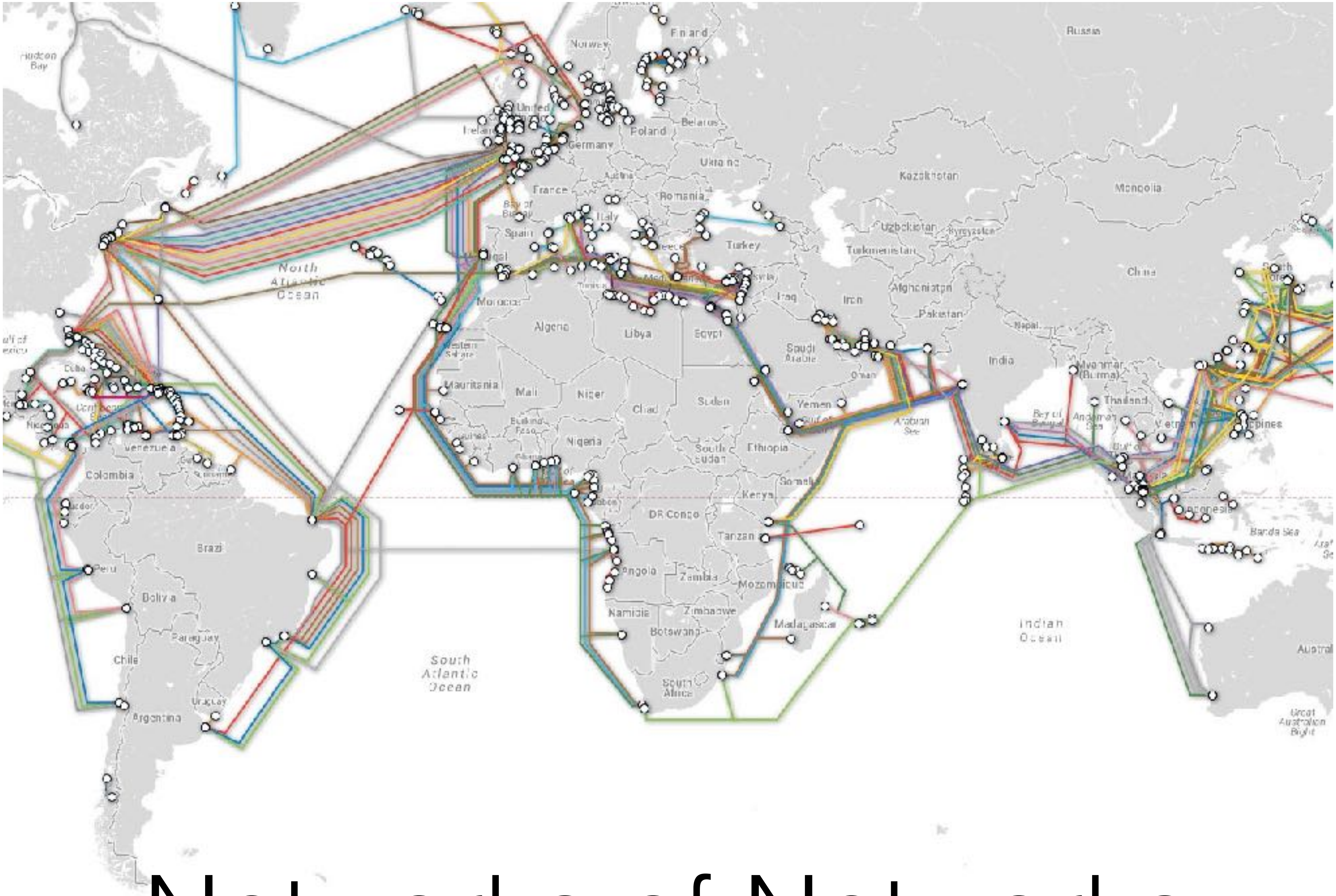
- Questions win points
- Highest points get a reward
- The best questions get a reward
- I want you to learn something valuable today

What are we talking about?

- How does the Internet work?
- What goes into a network
- Different aspects of a network
- A standard small medium business office network
- How to setup a network
- How to solve problems in a network
- 10 mins Q&A

“Internet”

What do you picture in your mind?



Networks of Networks

Internet Service Providers

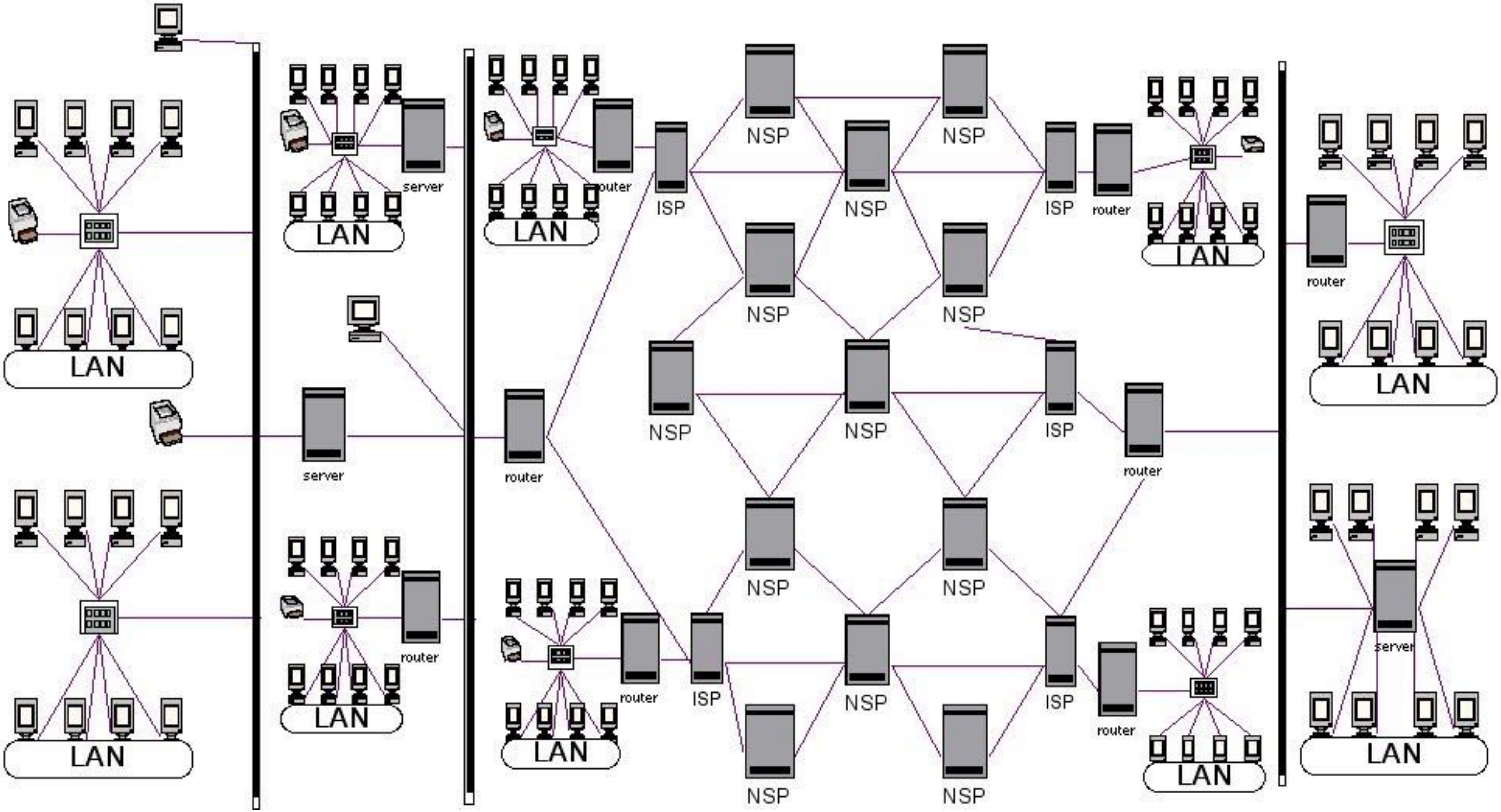
- Tier 1, Tier 2 and Tier 3
- Peering Agreements
- Large cables laid on the sea floor
- India has only one Tier 1 network. Tata Communications

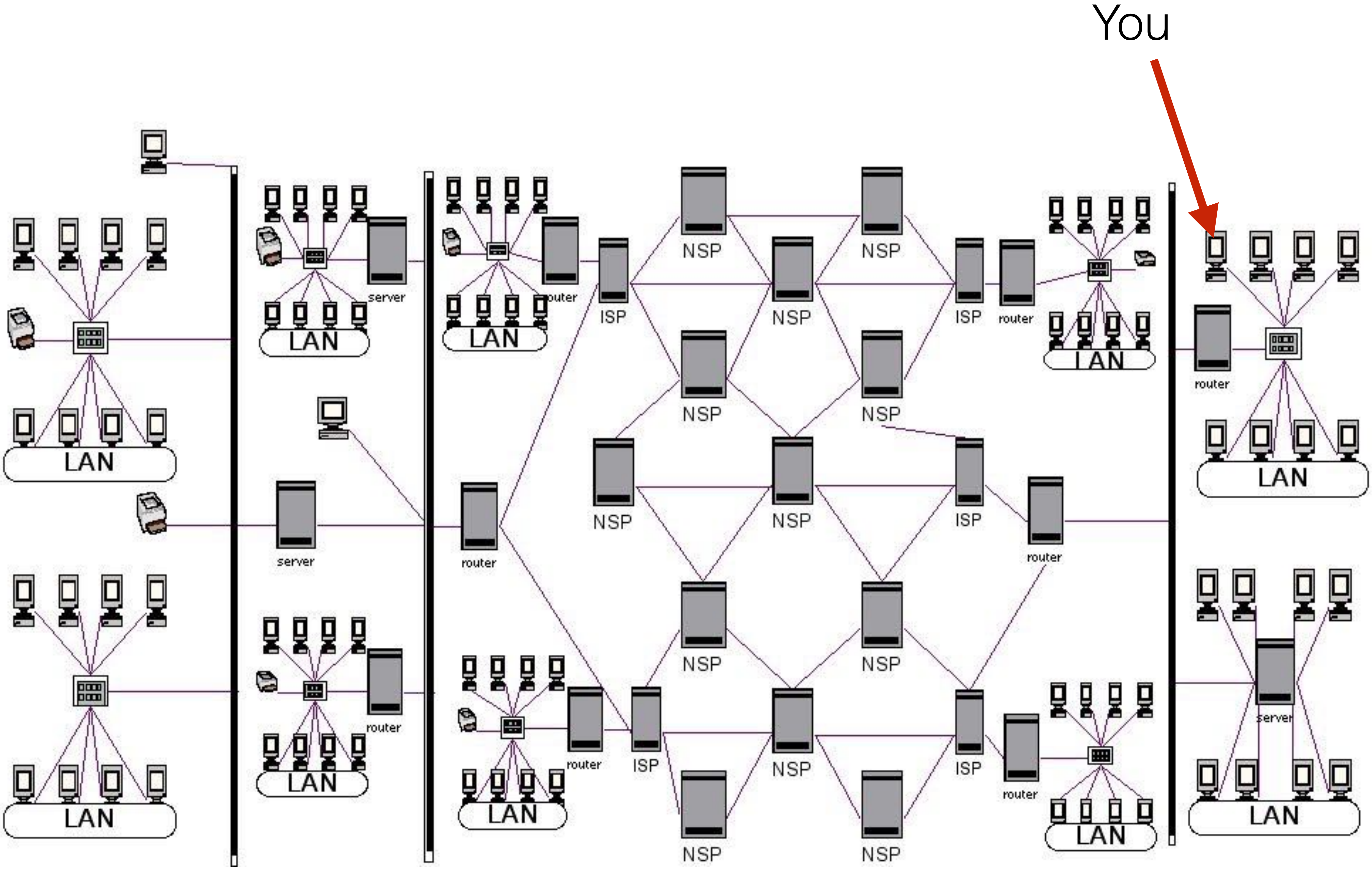
WAN

- Wide area network
- A network bigger than the one you are on
- WAN also connected smaller networks to each other

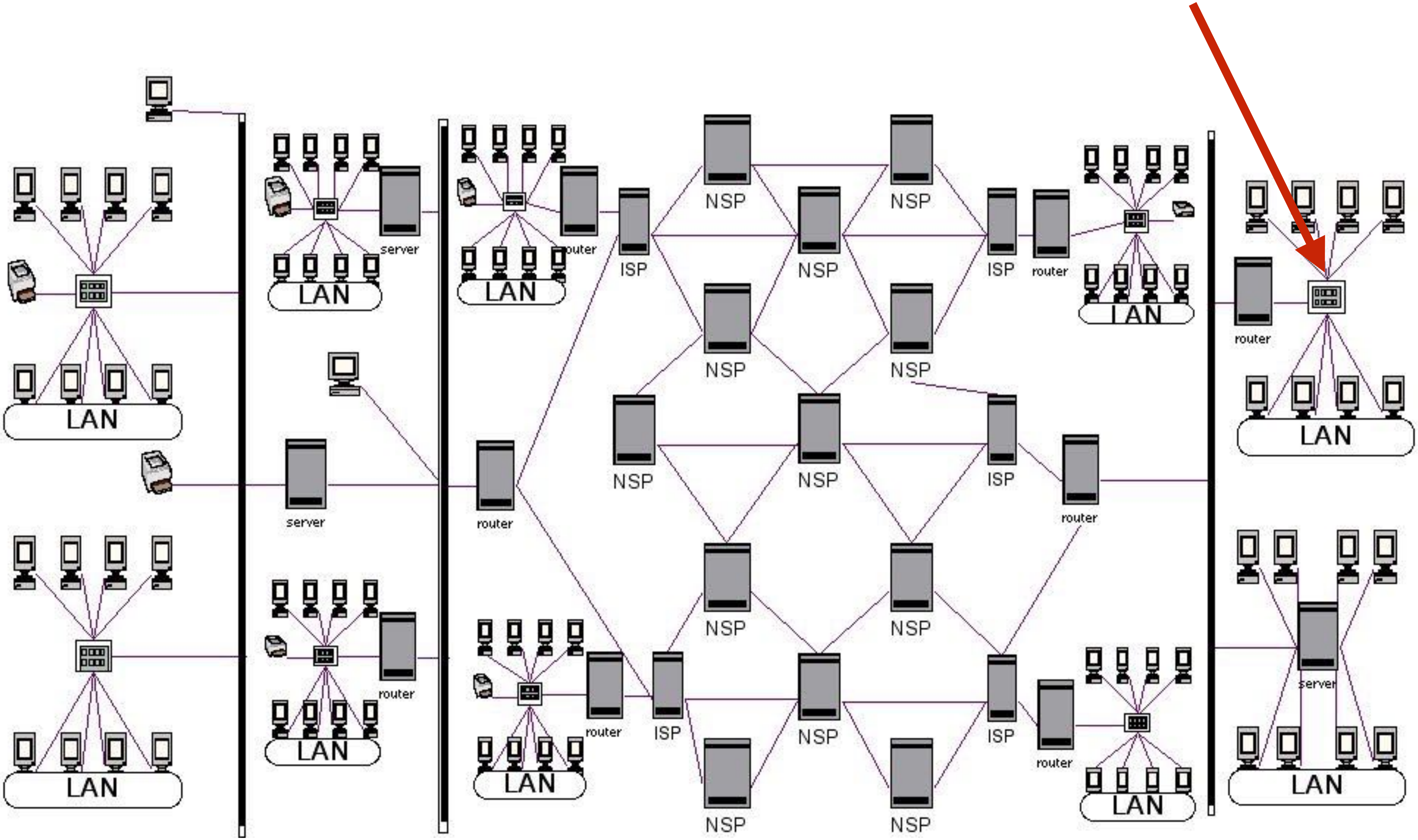
Internet

- The biggest WAN
- You connect to your ISP
- Your ISP connects to the regional hub
- the regional hub is connected to geographic hub
- geographic hub connected to main backbone
- backbone connected to Tier-1 ISP

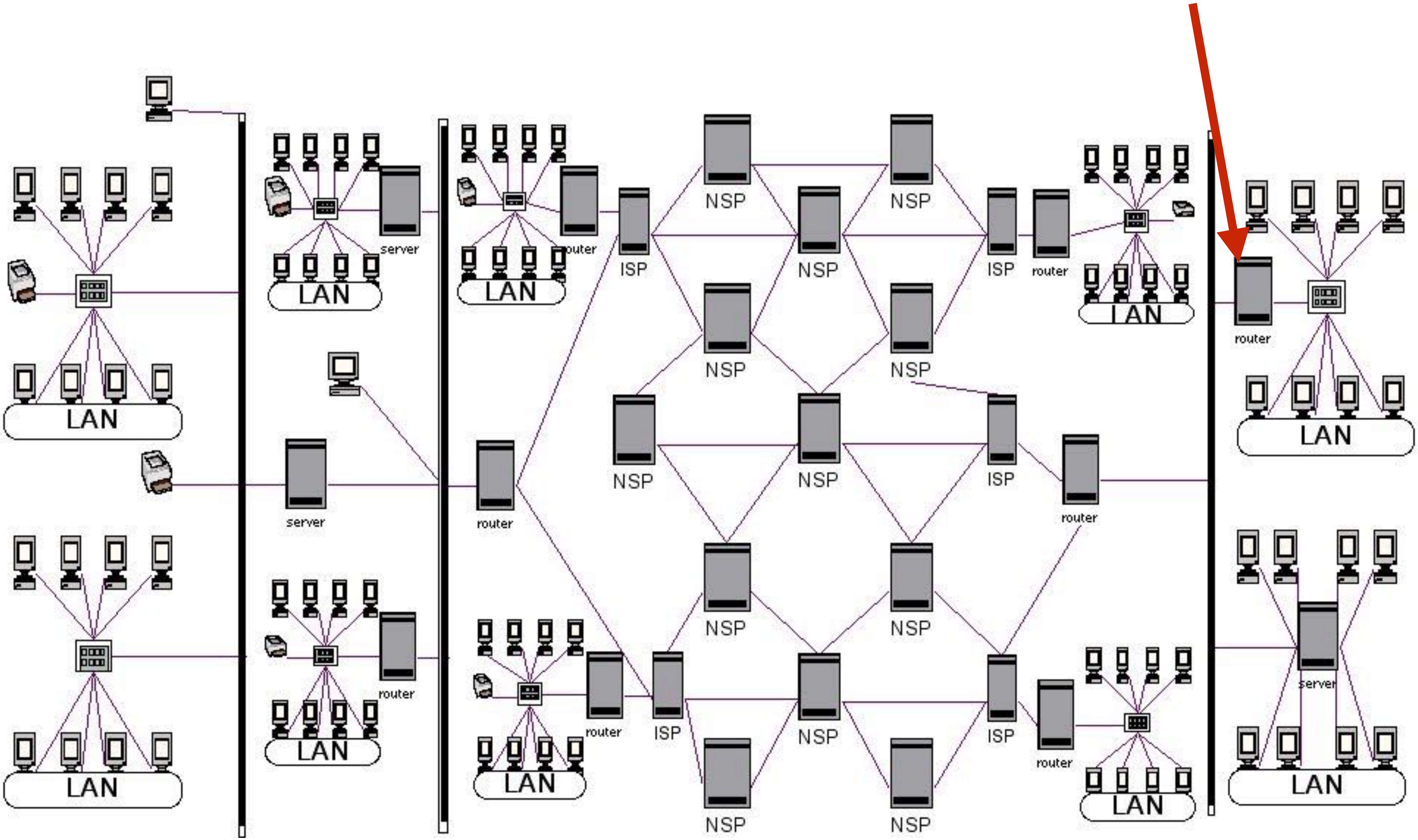

NSP
NSP
server
router
ISP
NSP
ISP
router
LAN
LAN
LAN
router
NSP
NSP
LAN
NSP
NSP
ISP
server
router
router
NSP
NSP
NSP
router
LAN
server
NSP
NSP
router
router
ISP
NSP
ISP
router
LAN
LAN
LAN
LAN
NSP
NSP


You
LAN
LAN
LAN
LAN
LAN
LAN
LAN
LAN
LAN
server
server
server
router
router
router
router
router
router
router
router
ISP
ISP
ISP
ISP
ISP
NSP
NSP
NSP
NSP
NSP
NSP
NSP
NSP
NSP
NSP
NSP
NSP
NSP
NSP
NSP

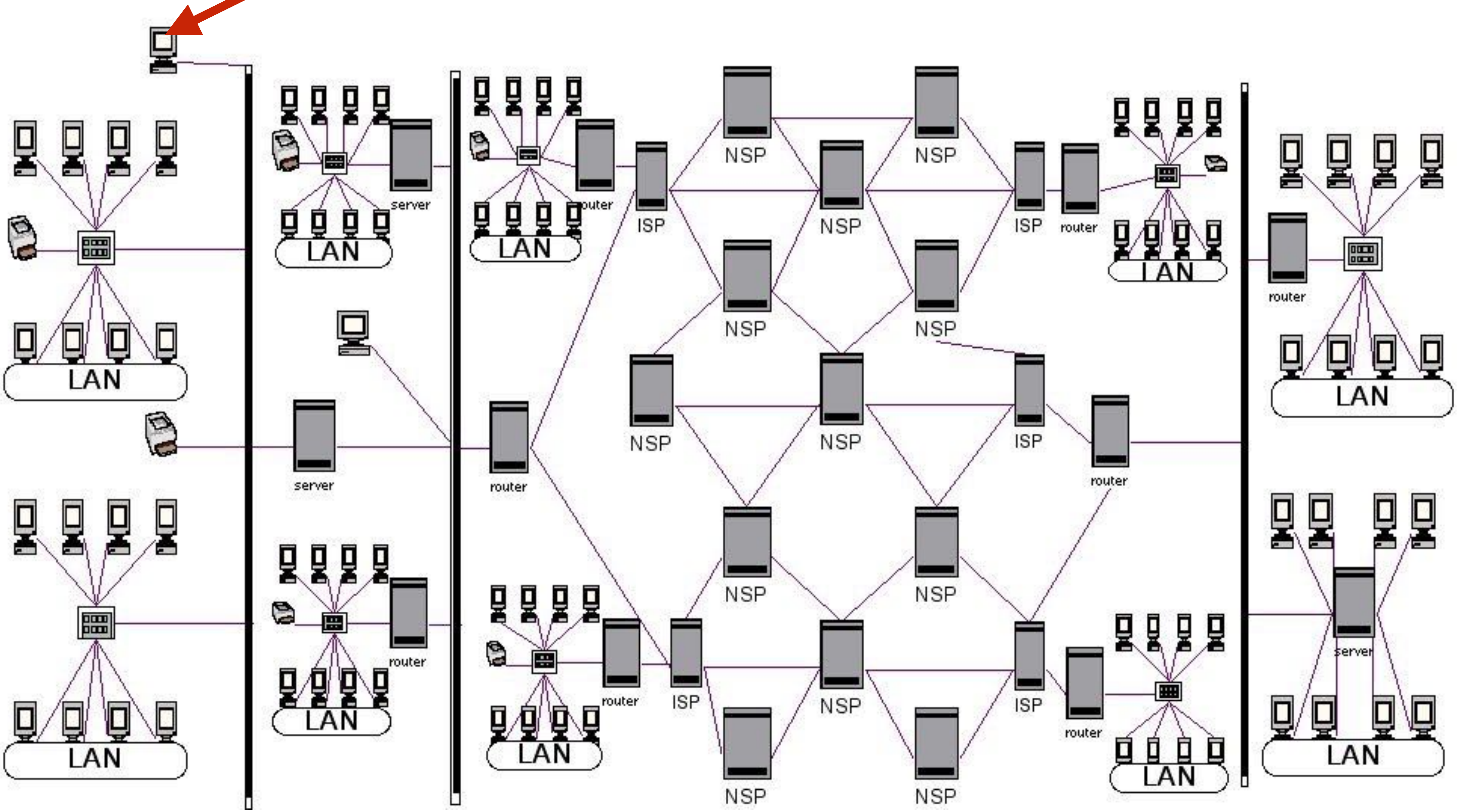
Your Home Router

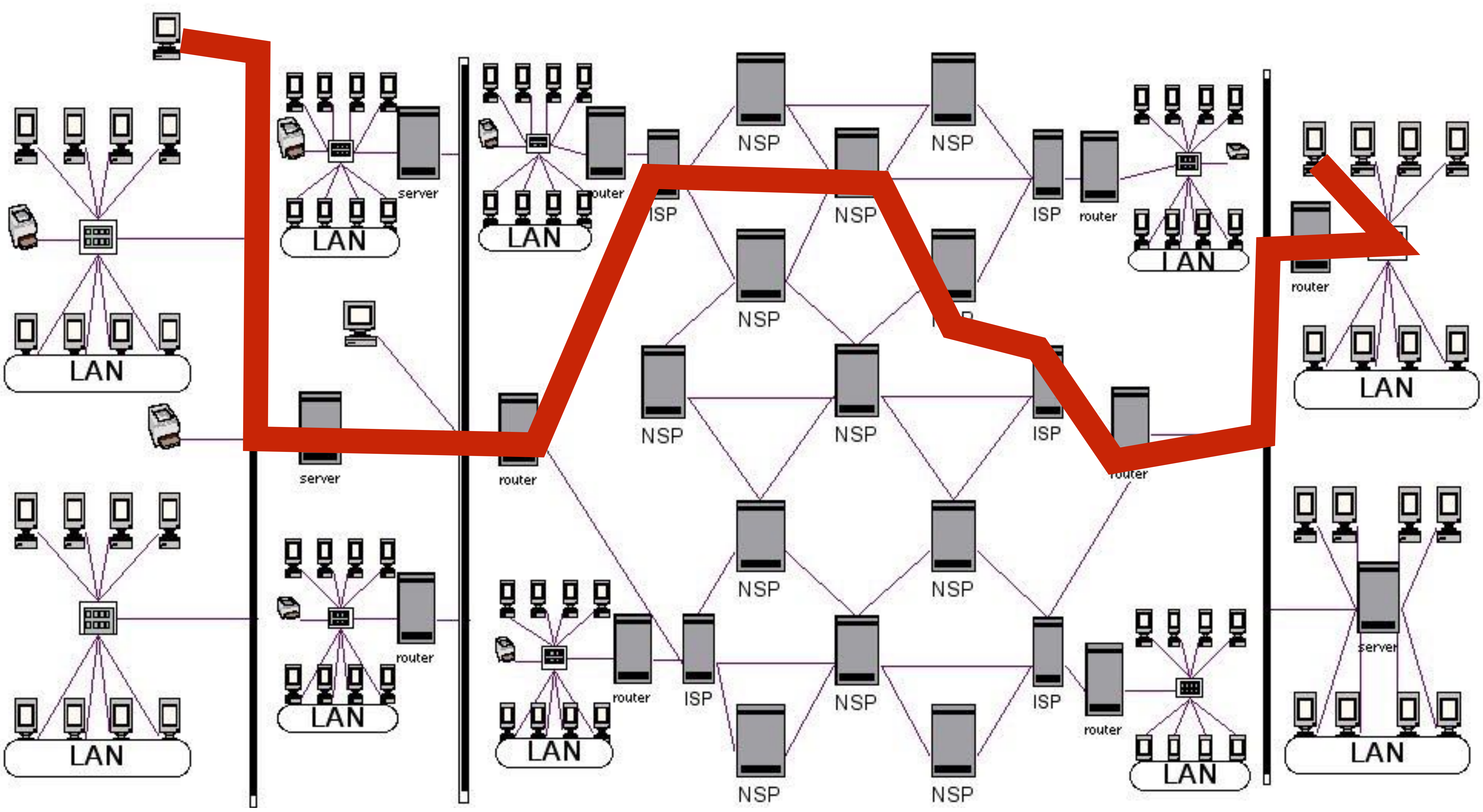


Your ISPs Router



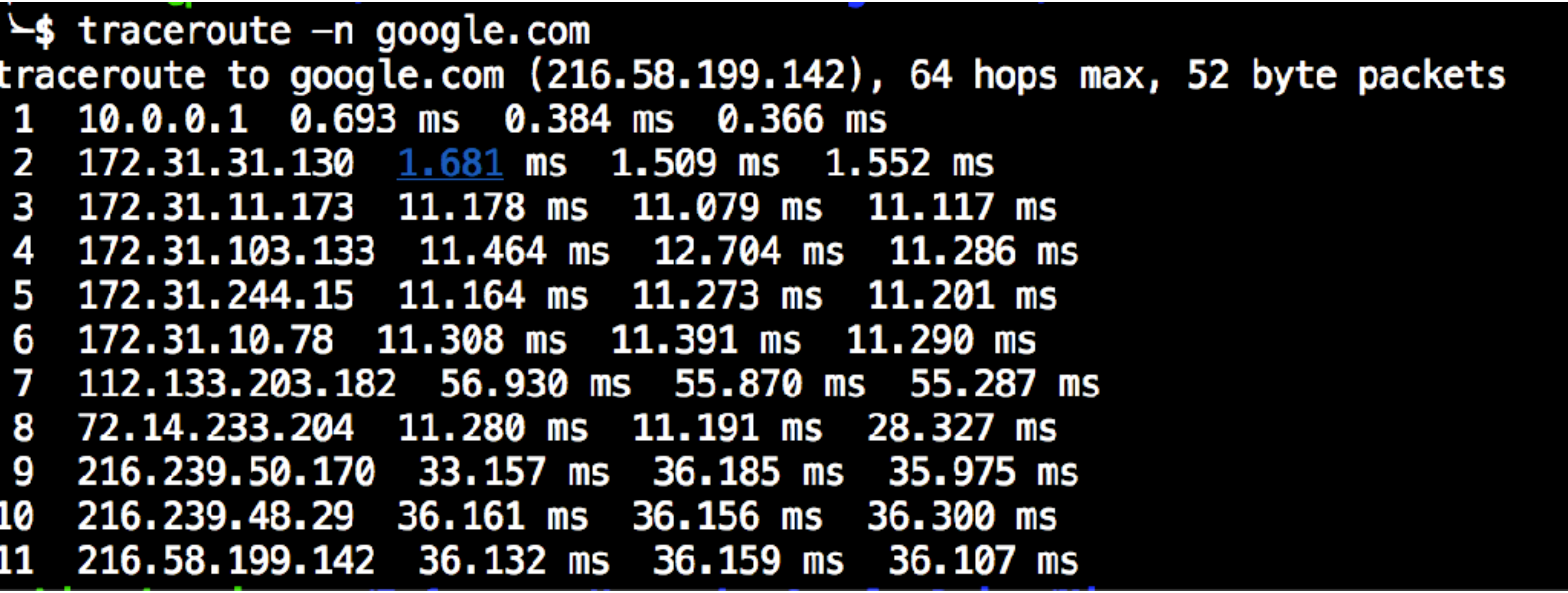
google.com


server
router
ISP
NSP
NSP
NSP
ISP
router
LAN
LAN
LAN
NSP
NSP
router
LAN
NSP
NSP
ISP
server
router
router
NSP
NSP
LAN
router
ISP
NSP
ISP
server
LAN
LAN
LAN
router
NSP
NSP
LAN
LAN

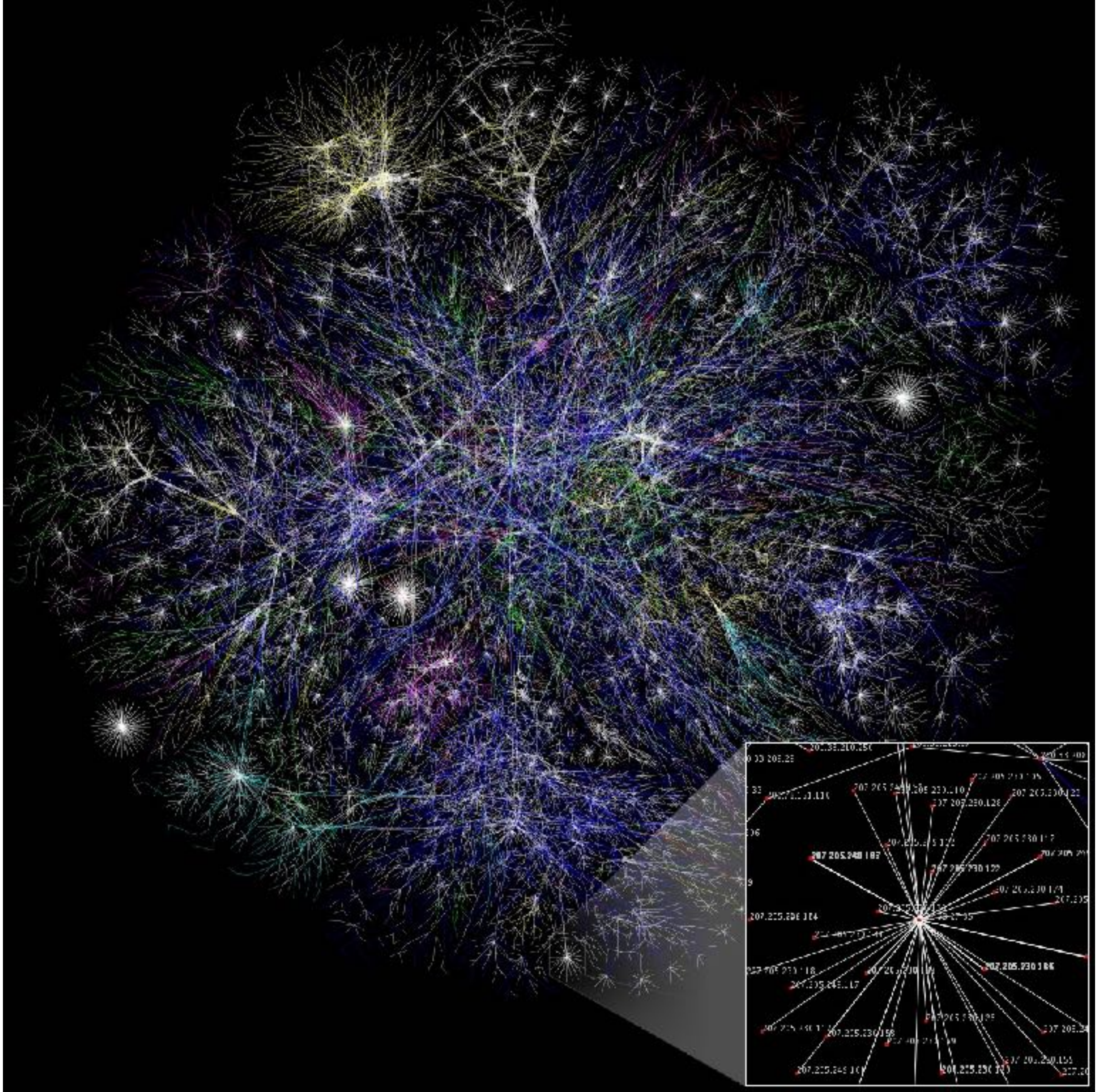


Go to google.com

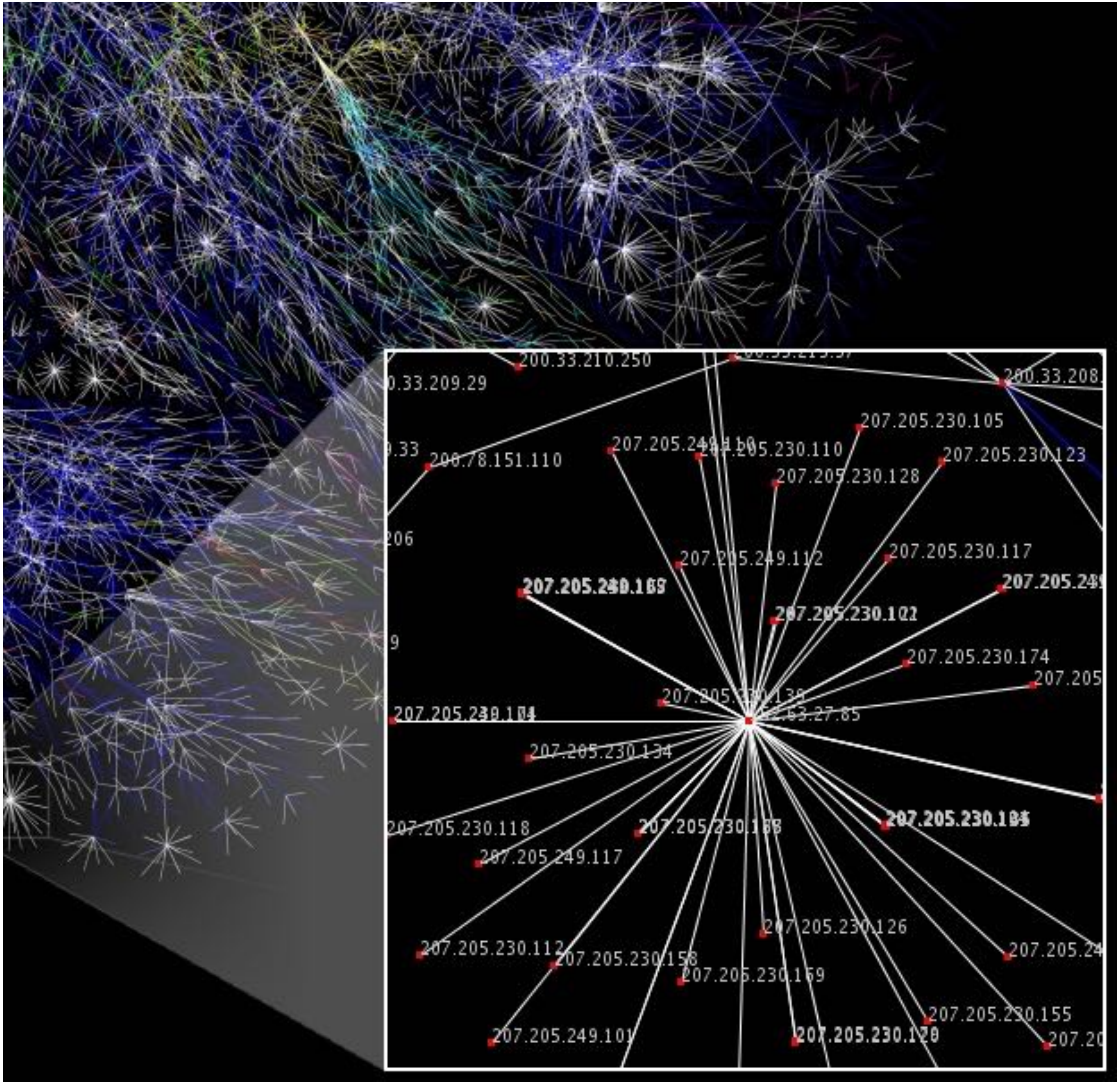
But Practically?



```
└$ traceroute -n google.com
traceroute to google.com (216.58.199.142), 64 hops max, 52 byte packets
 1  10.0.0.1  0.693 ms  0.384 ms  0.366 ms
 2  172.31.31.130  1.681 ms  1.509 ms  1.552 ms
 3  172.31.11.173  11.178 ms  11.079 ms  11.117 ms
 4  172.31.103.133  11.464 ms  12.704 ms  11.286 ms
 5  172.31.244.15  11.164 ms  11.273 ms  11.201 ms
 6  172.31.10.78  11.308 ms  11.391 ms  11.290 ms
 7  112.133.203.182  56.930 ms  55.870 ms  55.287 ms
 8  72.14.233.204  11.280 ms  11.191 ms  28.327 ms
 9  216.239.50.170  33.157 ms  36.185 ms  35.975 ms
10  216.239.48.29  36.161 ms  36.156 ms  36.300 ms
11  216.58.199.142  36.132 ms  36.159 ms  36.107 ms
```



207.205.248.187
207.205.230.128
207.205.230.122
207.205.230.117
207.205.230.129
207.205.230.174
207.205.236.184
207.205.230.166
207.205.248.117
207.205.230.158
207.205.230.155
207.205.248.10


200.33.210.250
0.33.209.29
200.33.208.
207.205.230.105
207.205.230.110
207.205.230.123
9.33
200.78.151.110
207.205.230.128
206
207.205.249.112
207.205.230.117
207.205.24
207.205.230.174
207.205
207.205.230.139
.63.27.85
207.205.230.134
207.205.230.118
207.205.249.117
207.205.230.126
207.205.230.112
207.205.230.158
207.205.230.169
207.205.24
207.205.230.155
207.205.249.101
207.20

But how does that work?

- PPPoE/ Leased Line/FTTH
- DHCP
- DNS
- TCP/UDP

PPPoE

- Point to point over Ethernet
- Connect you with the nearest router
- Give username and password
  - Decides if you are a subscriber
  - How much speed you should get?

What does a computer need to know?

- Who am I? - > An IP Address
- Who is my gateway
- What network am i on?
- Who should i contact for DNS ?

DHCP

- Dynamic Host Configuration Protocol
- When a device connects to the network. Give it the correct network configuration
- Give MAC, get back configuration

DNS

- Connected to Internet
- Domain name server
- Give domain, Get back IP Address(es)

TCP/UDP

- Protocols that do data transfer from Point A to Point B (i.e. From your IP to Other IP)

- TCP - Provides Guarantee that traffic will be received

- UDP - No Guarantee for receipt

TCP at a glance

- Sender numbers the packets 1. 2, 3, 4, 5…
- Receiver acknowledges last received number.
    - If 1, 2 and 3 are received, it sends back 3
- Hence, If sender sent 1,2,3,4,5 and got back 3, it sends 4 and 5 again
- This mechanism guarantees that all packets will be sent

UDP

- I dont care
- Here are 500 packets

Ping

- Send one ICMP Packet (HELLO)
- Get back packet if machine is on (ACK HELLO)
- Machine is alive!

When a network goes down

- Check if the machine has an IP from DHCP
- Check local network (Ping Local Gateway)
- Check router status (PPPoE Internet connection status)
- Ping by IP (8.8.8.8)
- Ping by Domain Name (google.com)