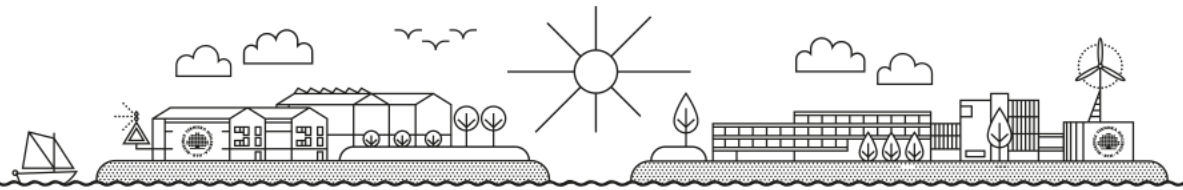
# SCANNING IPV6 NETWORKS

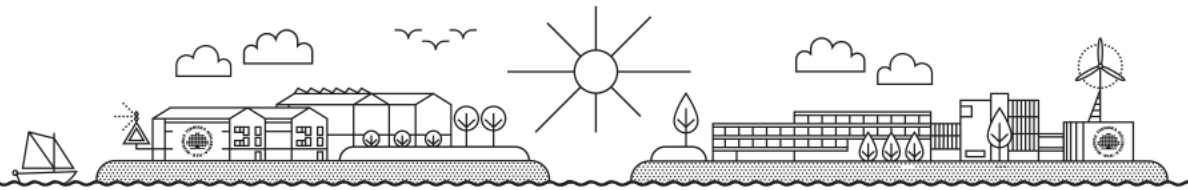
# ABOUT ME

- Erik Bergenholtz
- Ph.D. student in computer science at BTH since October 2017
  - Currently focusing on autonomous malware analysis
- Graduated from the M.Sc. in Engineering Computer Security programme at BTH in 2016
- erik.bergenholtz@bth.se (ebz@bth.se)



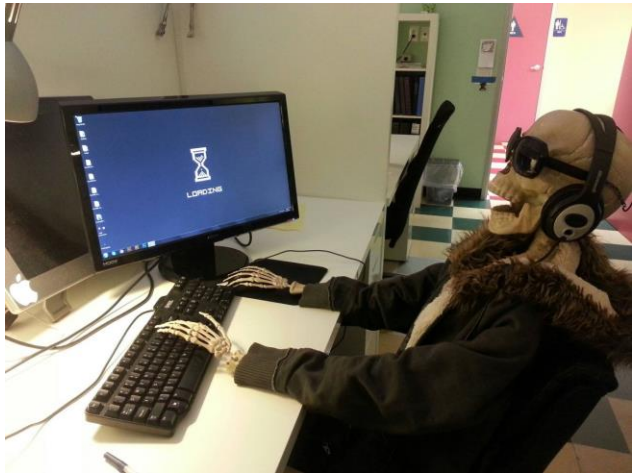
# ABOUT IPV6 RECONNAISSANCE

- Used in security testing, tries to answer questions like
  - **What hosts are on the network?**
  - What are their roles?
  - What operating systems and services are running?
- IPv4 scanning methods are infeasible
- IPv6 address space is $2^{96}$ times larger than IPv4
- `masscan` can scan all of IPv4 in 5 minutes
  - One IPv6 subnet would take 40000 years to scan



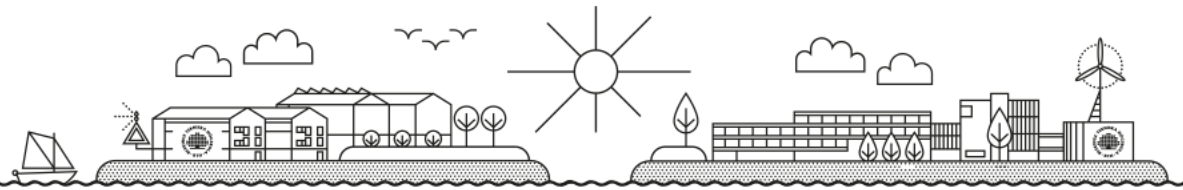
# ABOUT IPV6 RECONNAISSANCE

- Used in security testing, tries to answer questions like
  - **What hosts are on the network?**
  - What are their roles?
  - What operating systems and services are running?
- IPv4 scanning methods are infeasible
- IPv6 address space is $2^{96}$ times larger than IPv4
- `masscan` can scan all of IPv4 in 5 minutes
  - One IPv6 subnet would take 40000 years to scan



# PIECES OF THE PUZZLE

| | | |
|---|---|---|
| Multicast ICMP | Error Detection | Anycast ICMP |
| Traceroute | SNMP | Fake RA |
| Pattern Inference | Eavesdropping | Eavesdropping P2P |
| Eavesdropping SLAAC | Search Engines | Lists of known hosts |
| CAIDA | DNS Lookup | Reverse DNS |
| mDNS | DNS Zone Transfer | Routing Information |
| Routing protocols | Neighbor cache | Server logs |
| Client logs | Host configuration | Temporary Addresses |
| EUI-64 addresses | Low-byte addresses | IPv4 based addresses |
| Service port addresses | Wordy addresses | |



# PIECES OF THE PUZZLE

IPv6 mechanics

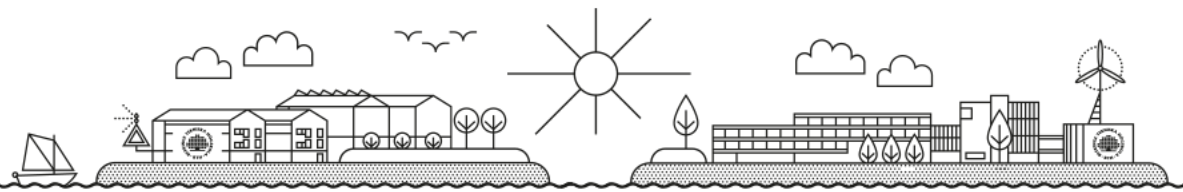
| | | |
|---|---|---|
| Multicast ICMP | Error Detection | Anycast ICMP |
| Traceroute | SNMP | Fake RA |
| Pattern Inference | Eavesdropping | Eavesdropping P2P |
| Eavesdropping SLAAC | Search Engines | Lists of known hosts |
| CAIDA | DNS Lookup | Reverse DNS |
| mDNS | DNS Zone Transfer | Routing Information |
| Routing protocols | Neighbor cache | Server logs |
| Client logs | Host configuration | Temporary Addresses |
| EUI-64 addresses | Low-byte addresses | IPv4 based addresses |
| Service port addresses | Wordy addresses | |

Listening to network

Infer addressing scheme from samples

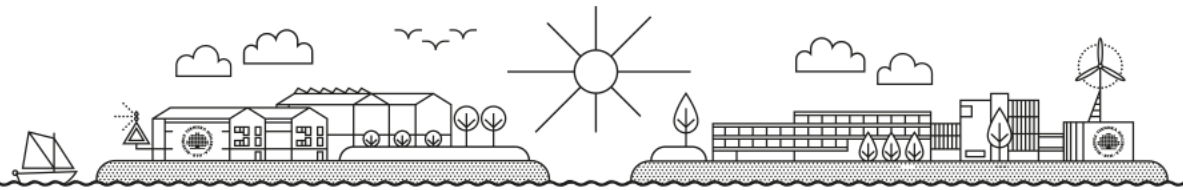
DNS

Assumed addressing schemes



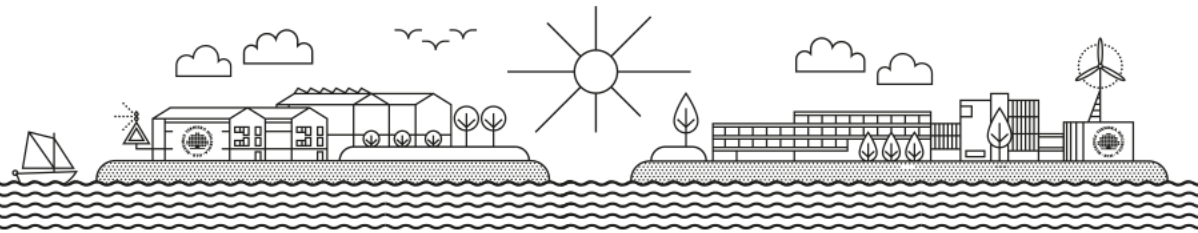
# PIECES OF THE PUZZLE

| Multicast ICMP | Error Detection | Anycast ICMP |
|---|---|---|
| Traceroute | SNMP | Fake RA |
| Pattern Inference | Eavesdropping | Eavesdropping P2P |
| Eavesdropping SLAAC | Search Engines | Lists of known hosts |
| CAIDA | DNS Lookup | Reverse DNS |
| mDNS | DNS Zone Transfer | Routing Information |
| Routing protocols | Neighbor cache | Server logs |
| Client logs | Host configuration | Temporary Addresses |
| EUI-64 addresses | Low-byte addresses | IPv4 based addresses |
| Service port addresses | Wordy addresses | |

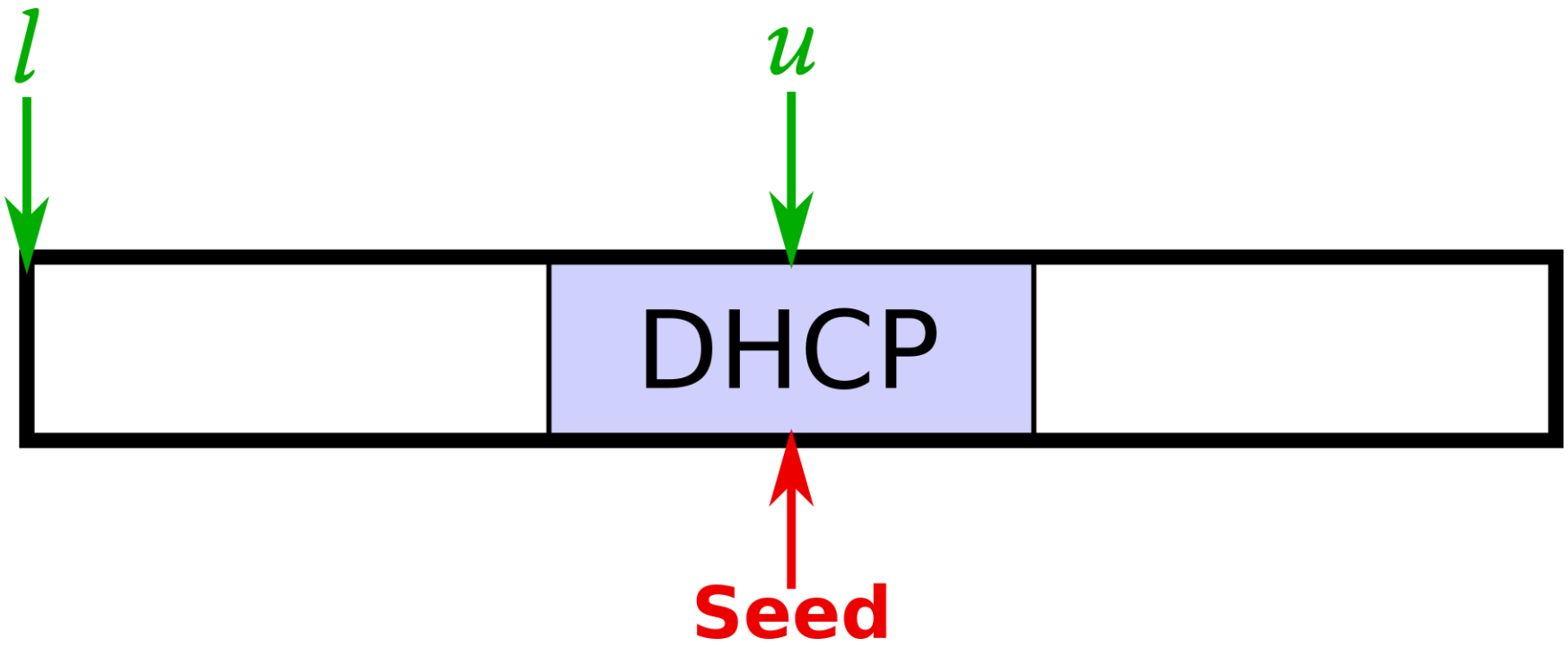


# DEHCP – SOLVING PART OF THE PUZZLE

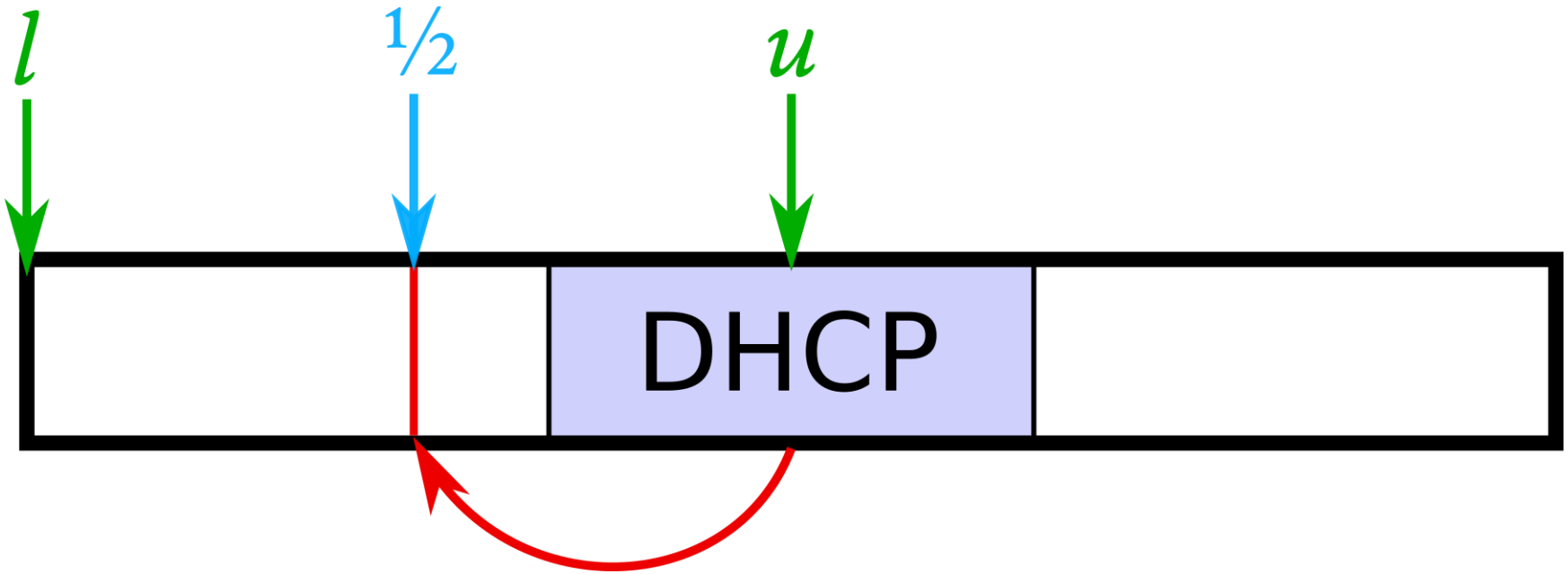
- Delimit DHCP
- Attempts decreasing the search space
- Exploits clustering of addresses assigned via DHCP
- Binary search for limits of used part of DHCP pool



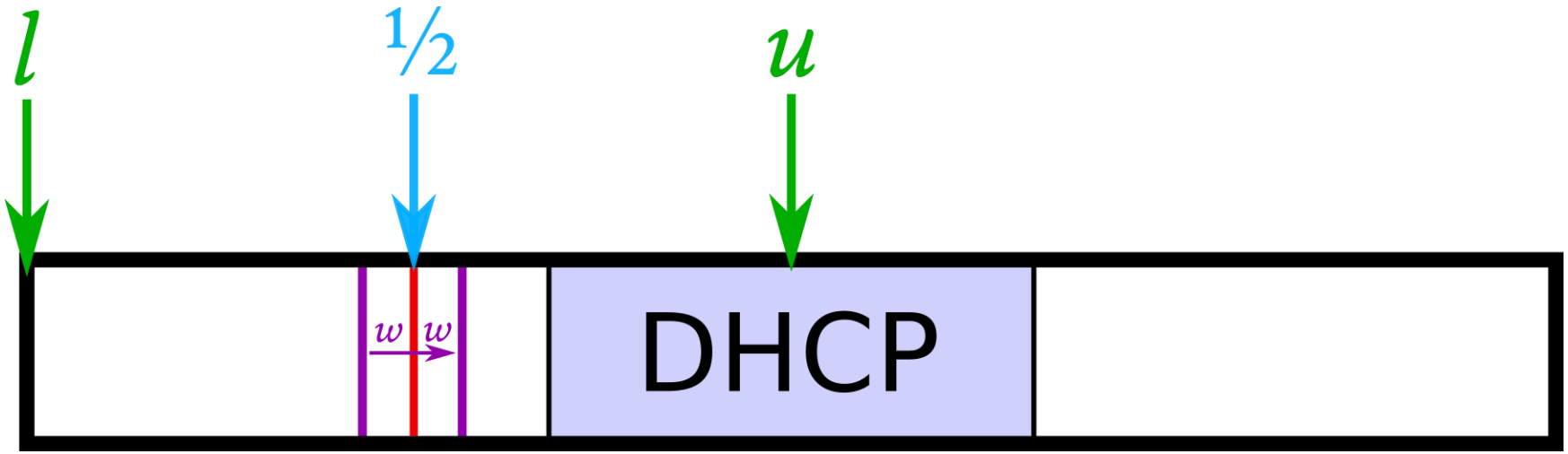
# DEHCP – SEED ADDRESS



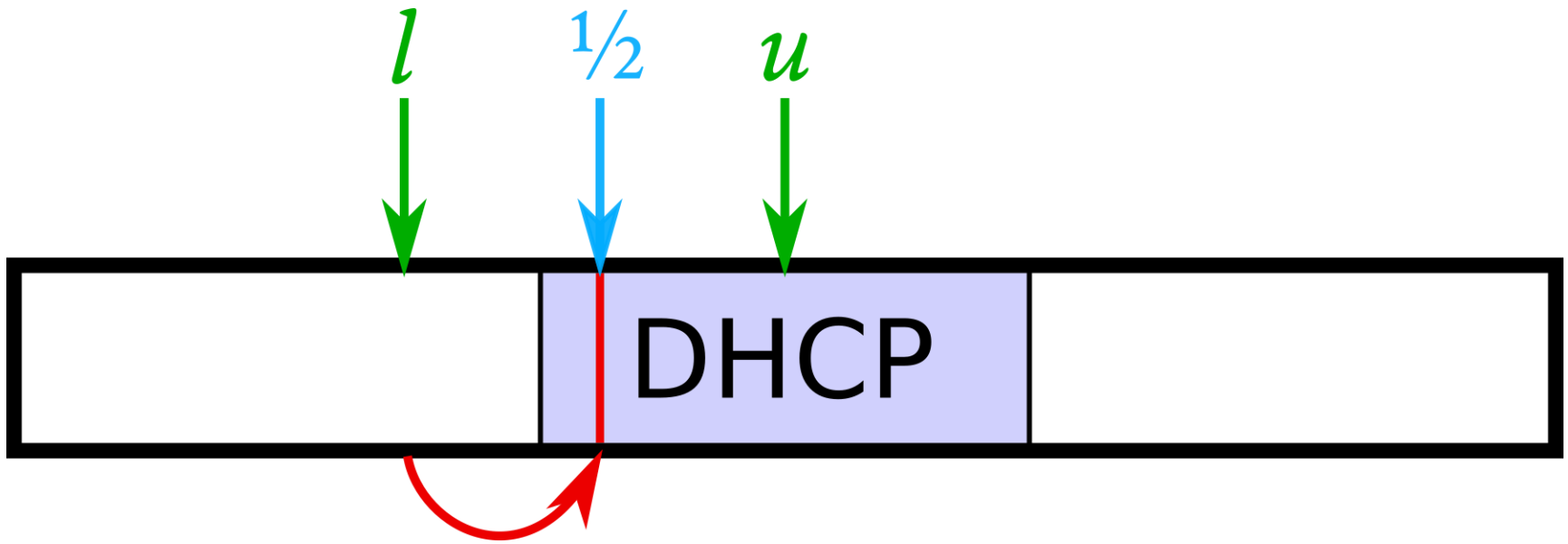
# DEHCP – FIRST STEP



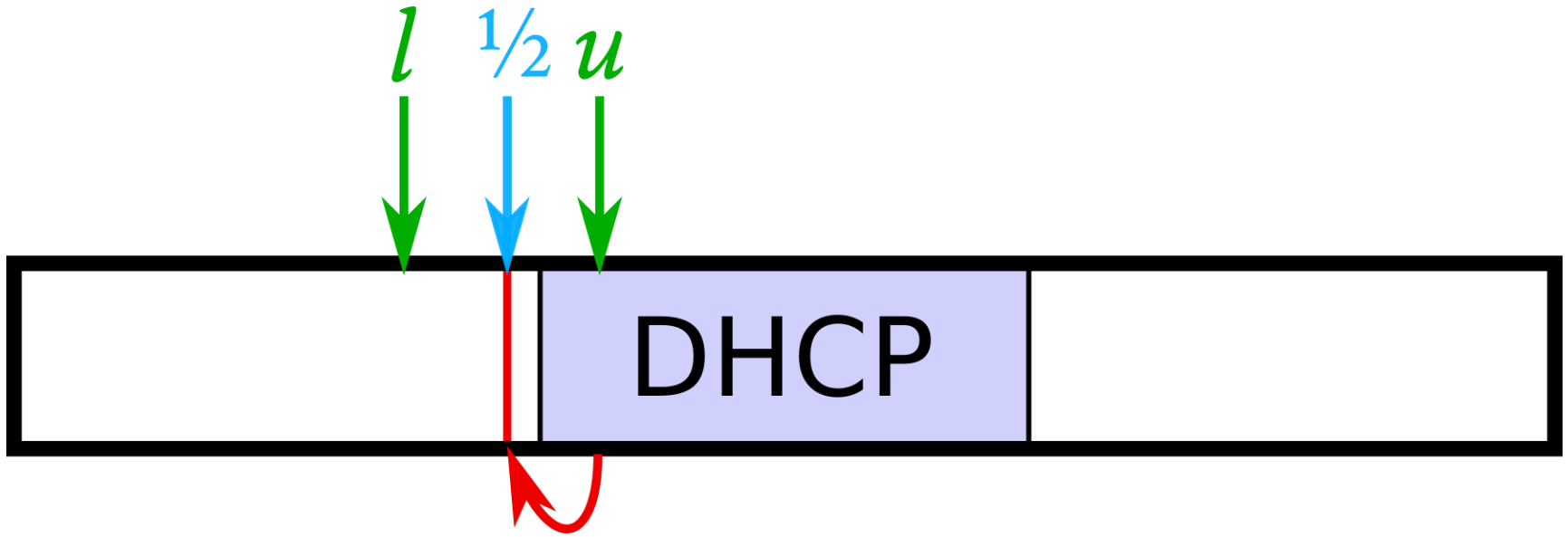
# DEHCP - PING WINDOW



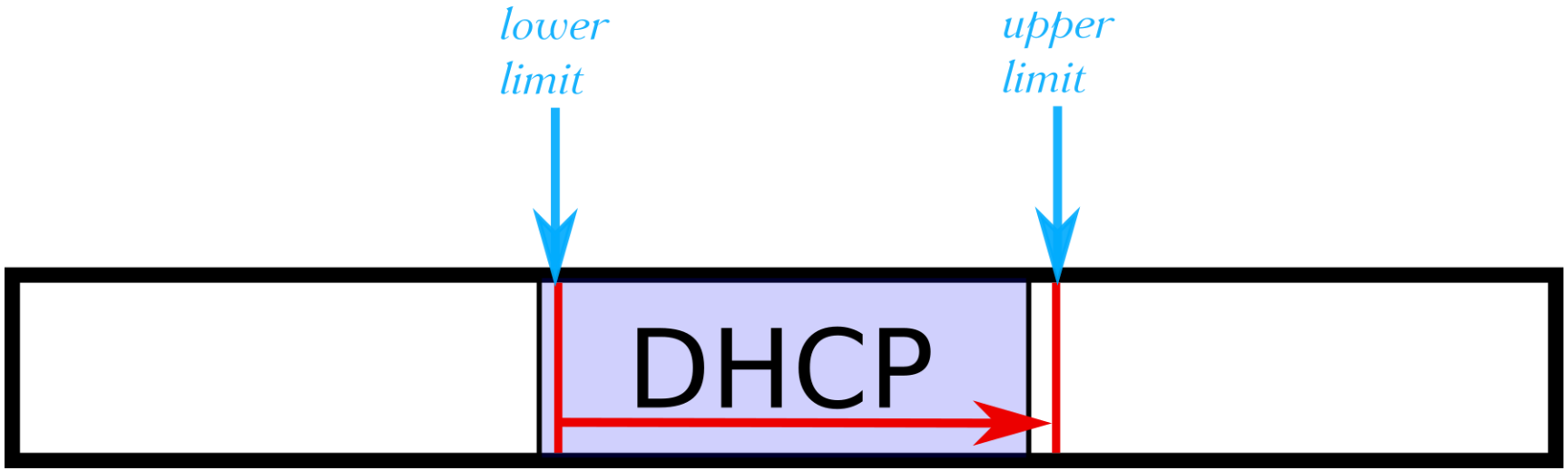
# DEHCP – MOVE BACK



# DEHCP – TRY FARTHER DOWN AGAIN

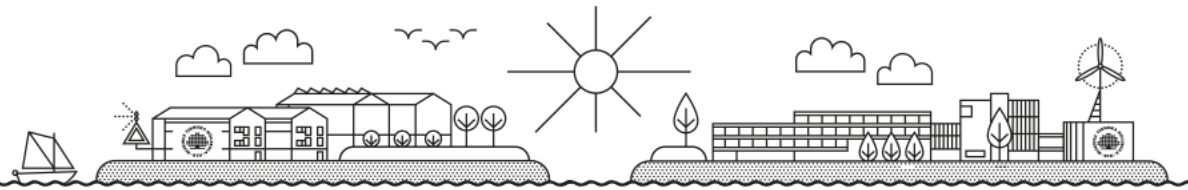


# DEHCP – SEQUENTIAL SCAN



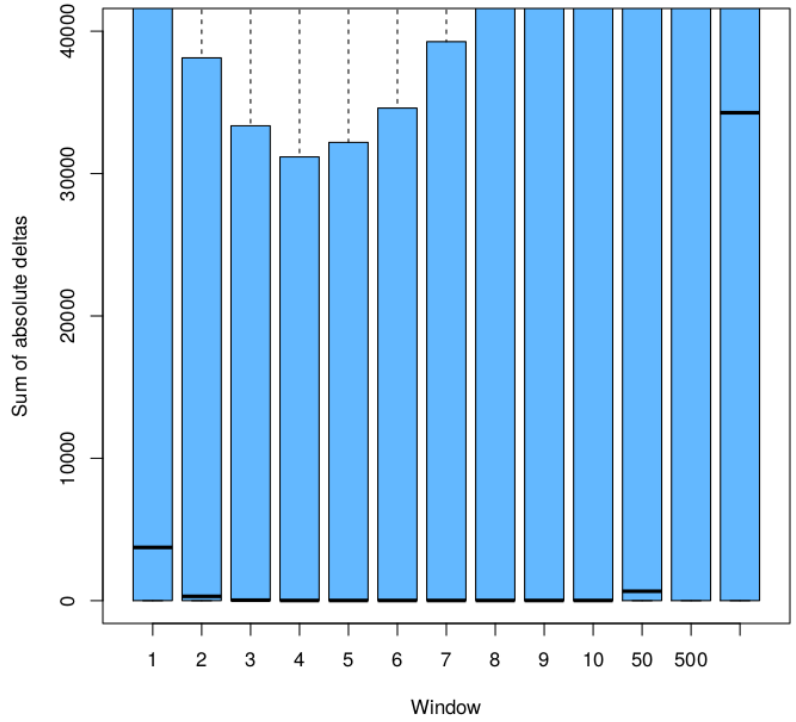
# EXPERIMENTS

- Three experiments were performed
- Simulation to find optimal window size
- Emulation in controlled environment
- Scanning the BTH IPv6 and IPv4 networks
- Emulation and scanning of live networks compared four methods
  - DeHCP with `ICMP` and `nmap` probes
  - Multicast ICMPv6
  - Multicast ICMPv6 with Hop-by-Hop header
  - Eavesdropping



# SIMULATION

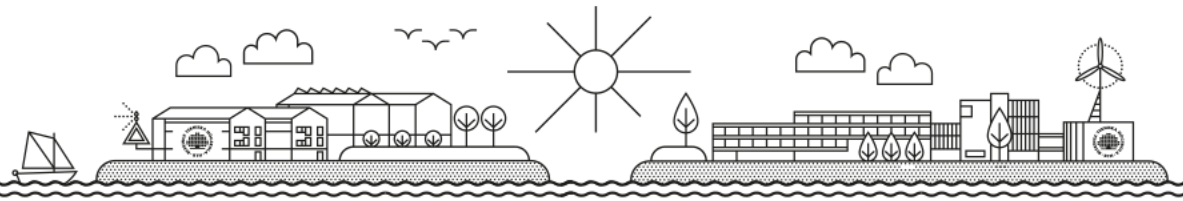
- 1M addresses in “network”
- 500k address DHCP pool in middle
- Density ranges from 0.001% up to 100%
- Window sizes 1-10, 50, 500, 5000



# EMULATION

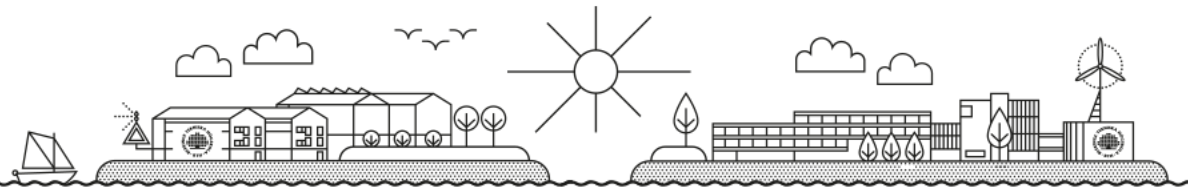
- 430 computers in total (13 physical, 13*32 VMs, 1 DHCP server)
- Brief port scan at least once per 90 minutes to generate traffic

| | Global probe source | | Link-local probe source | |
|---|---|---|---|---|
| | Link-local (F/T) | Global (F/T) | Link-local (F/T) | Global (F/T) |
| Eavesdropping | 430/430 | 430/430 | 430/430 | 430/430 |
| Multicast ICMP | 0/430 | 430/430 | 430/430 | 0/430 |
| Hop-by-Hop ICMP | 0/430 | 430/430 | 430/430 | 0/430 |
| DeHCPv6 (ICMP) | 0/430 | 429*/430 | 0/430 | 429*/430 |
| DeHCPv6 (nmap) | 0/430 | 429*/430 | 0/430 | 429*/430 |



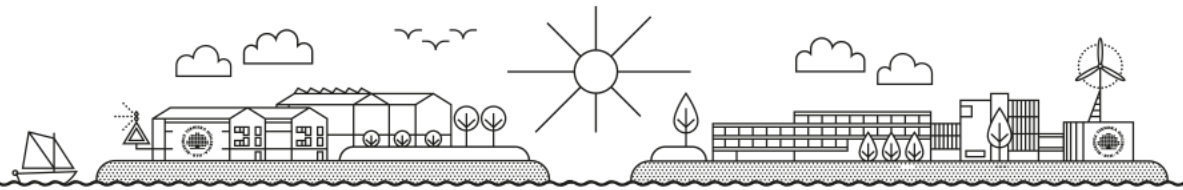
# LIVE SCAN SET UP

- Four networks scanned:
  - Wired IPv6 (/48)
  - Wireless IPv6 (/64)
  - Wired IPv4 (/19)
  - Wireless IPv4 (/22)
- Script set up to dump neighbor cache and ARP table
- Scans were performed across multiple VLANs
- DeHCP was restarted once per hour



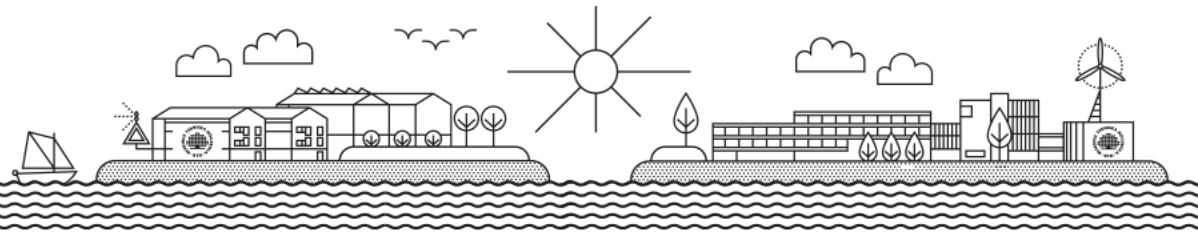
# RESULTS OF LIVE SCAN – IPV6

| | Wired | | WiFi | |
|---|---|---|---|---|
| | Link-local (F/T) | Global (F/T) | Link-local (F/T) | Global (F/T) |
| Eavesdropping | 29/1290 | 37/4483 | 247/249 | 235/486 |
| Multicast ICMP | 5/1290 | 40/4483 | 2/249 | 83/486 |
| Hop-by-Hop ICMP | 0/1290 | 1/4483 | 0/249 | 1/486 |
| DeHCPv6 (ICMP) | 0/1290 | 1/4483 | 0/249 | 1/486 |
| DeHCPv6 (nmap) | 0/1290 | 0/4483 | 0/249 | 1/486 |



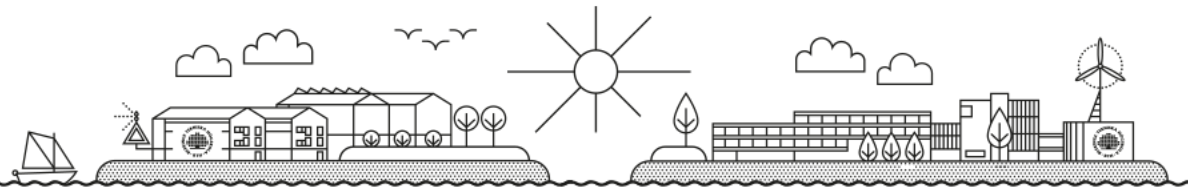
# RESULTS OF LIVE SCAN – IPV4

| | Wired | WiFi |
|---|---|---|
| DeHCPv4 (ICMP) | 122/1449 | 33/226 |
| DeHCPv4 (nmap) | 119/1449 | 51/226 |



# THOUGHTS ON DEHCP

- Simulation and emulation shows promise DeHCP
- Doesn't perform as well without DHCP as expected
- Doesn't solve the whole puzzle, but maybe a part of it
- https://git.cse.bth.se/erikphd/v6scan
  - Feedback and results are appreciated!




BLEKINGE TEKNISKA HÖGSKOLA
BTH