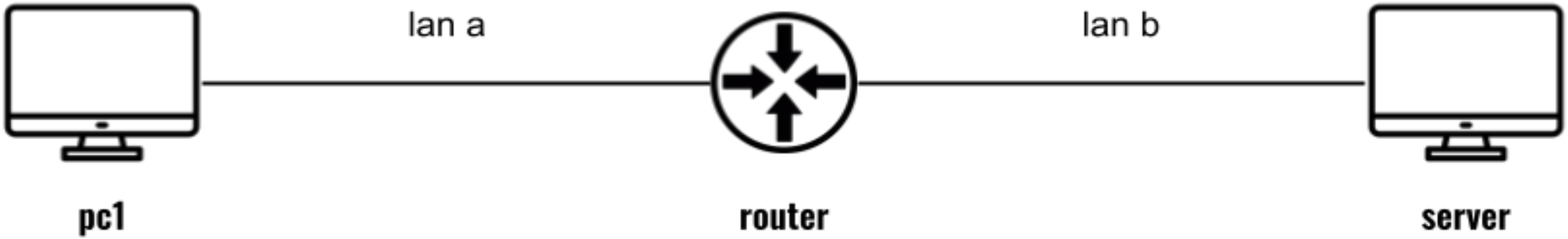
backward learning

AND MAC ADDRESS FLOODING ATTACK

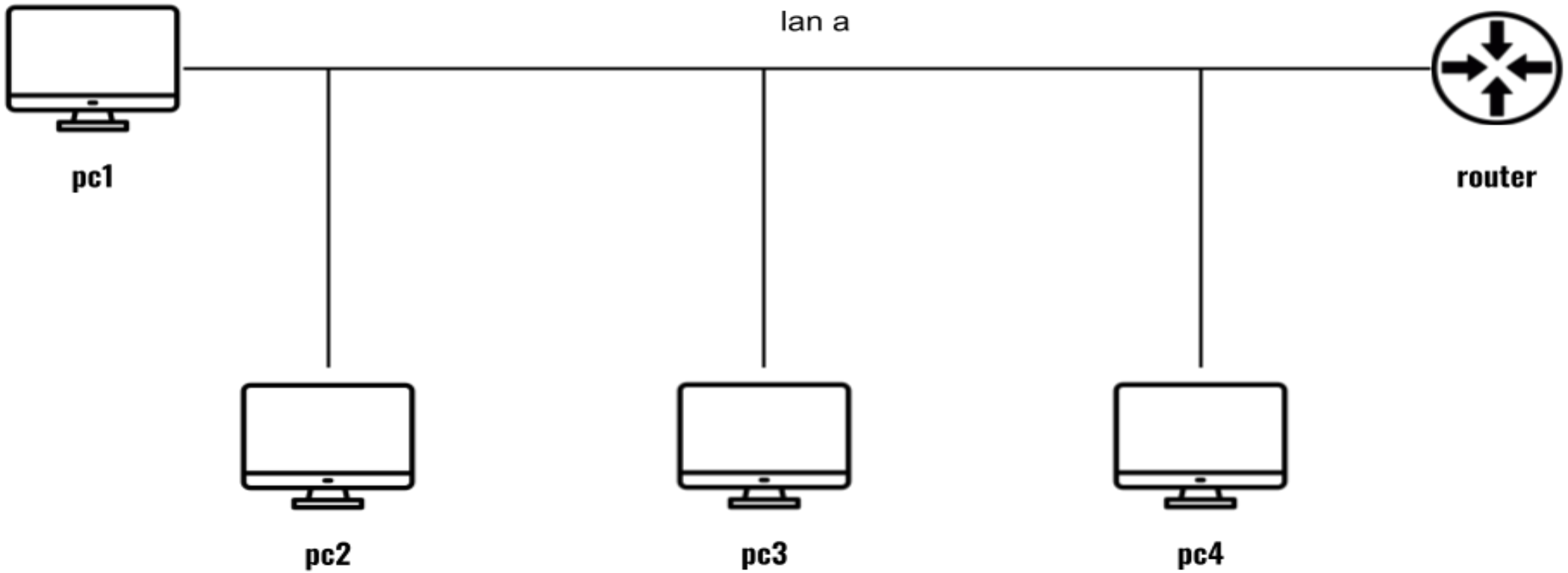
agenda

- local area network
- backward learning
- mac address flooding attack

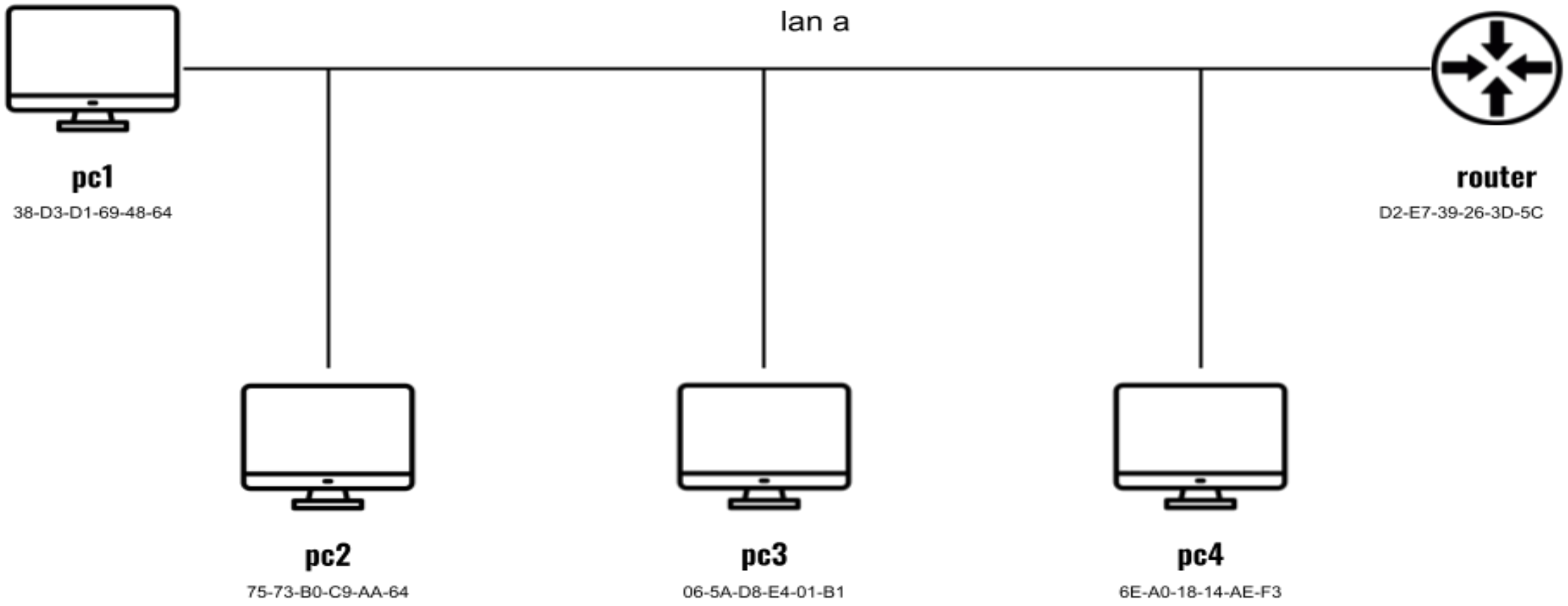
scenario



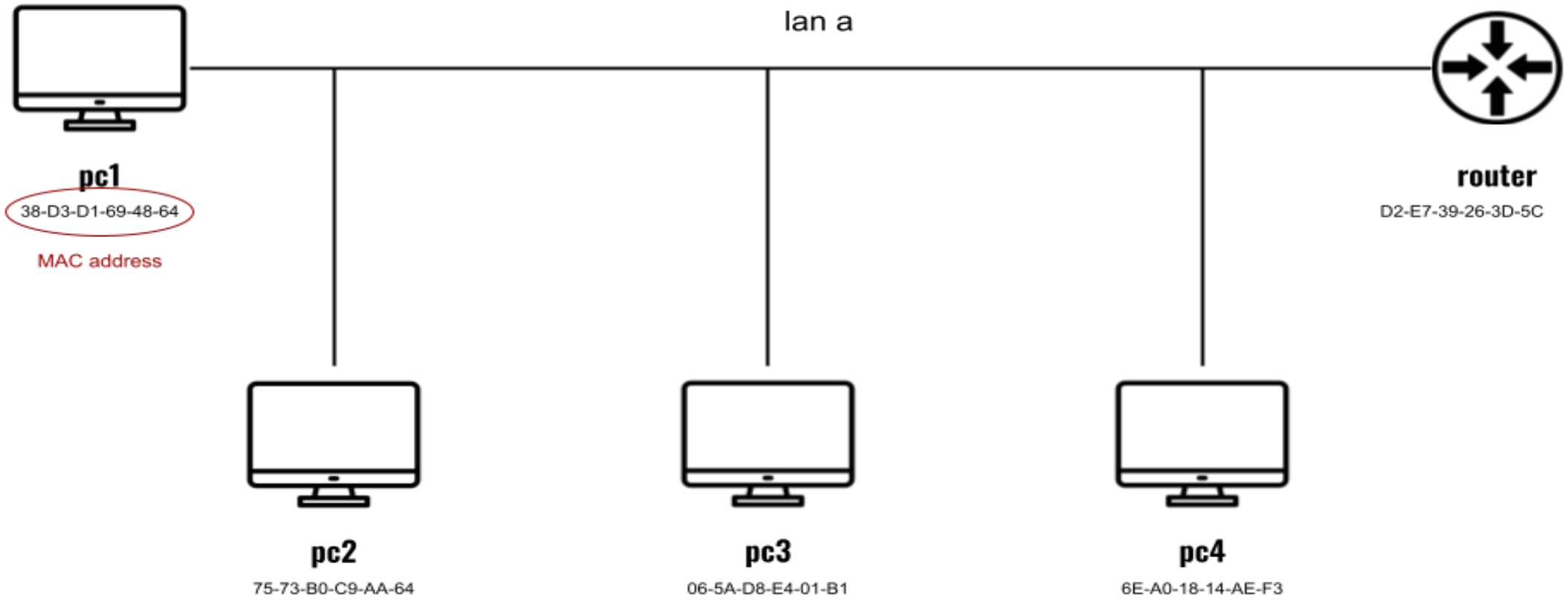
local area network



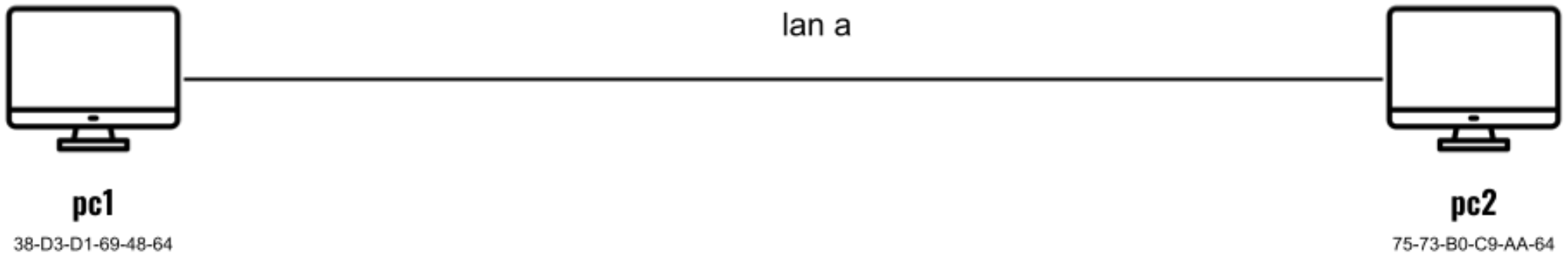
local area network



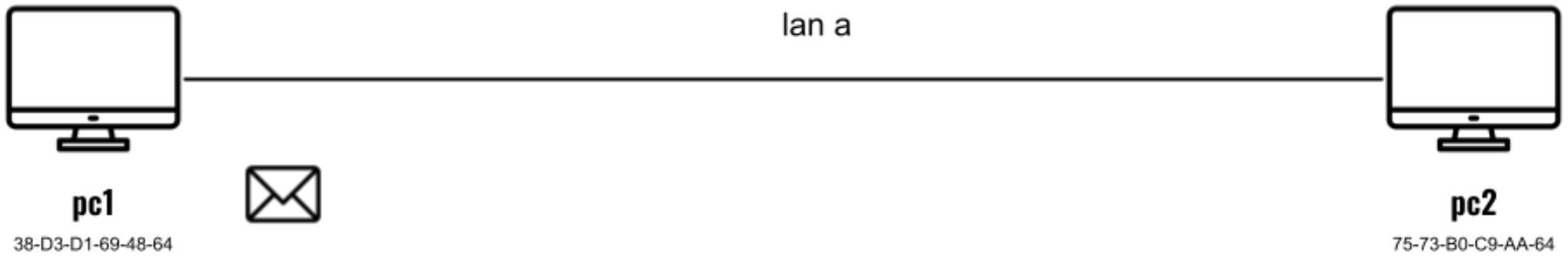
local area network



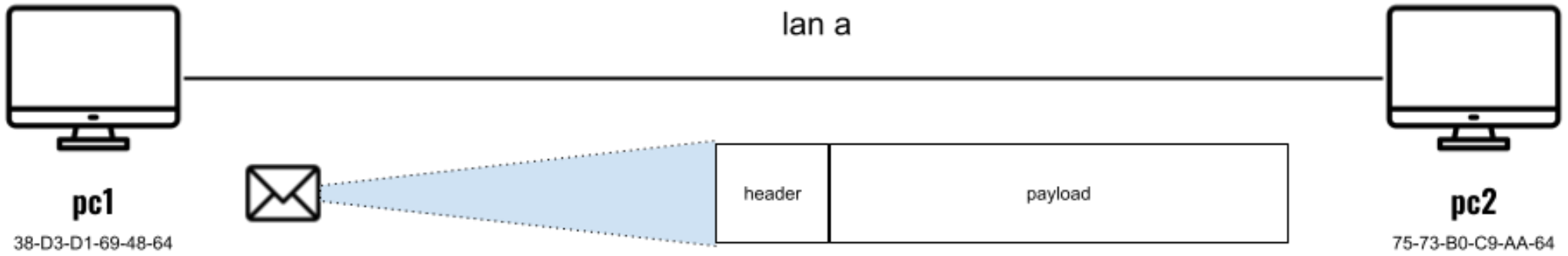
example



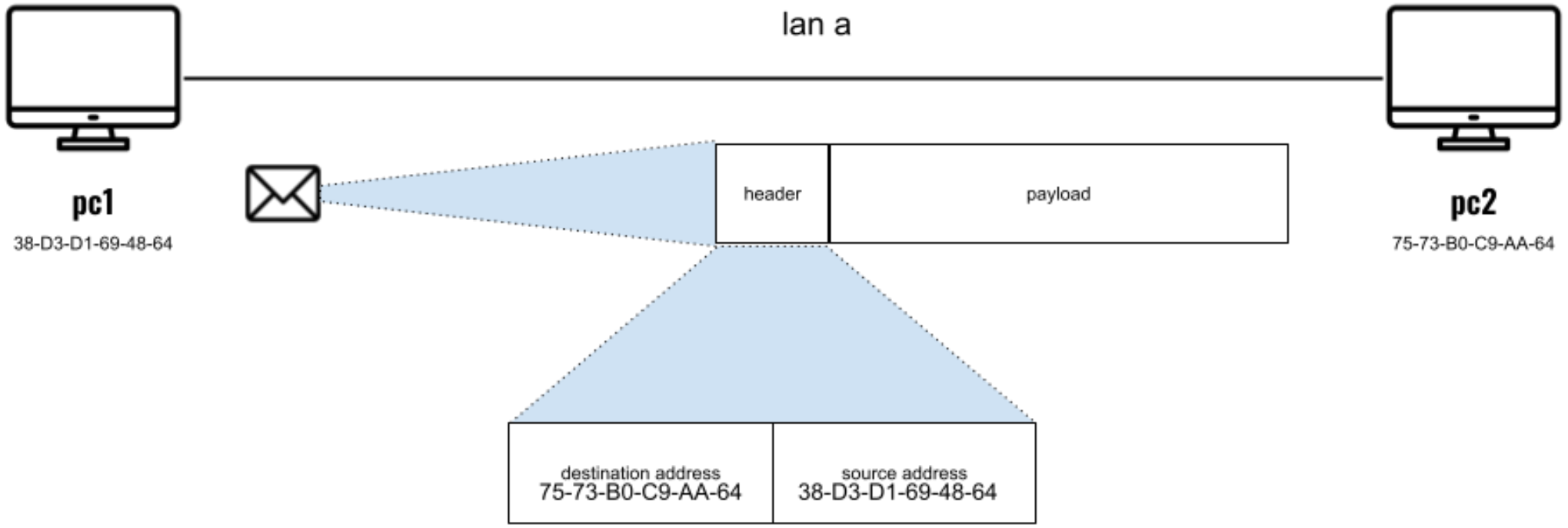
example



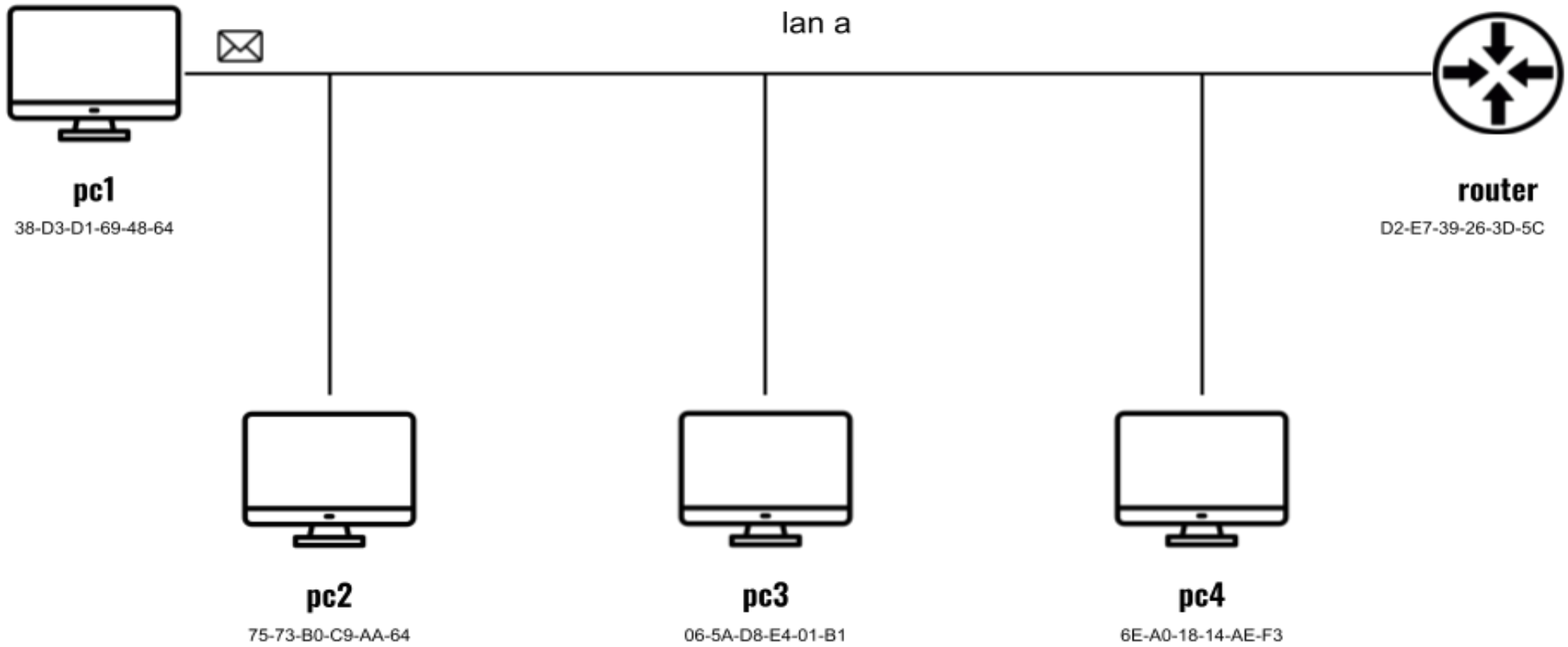
example



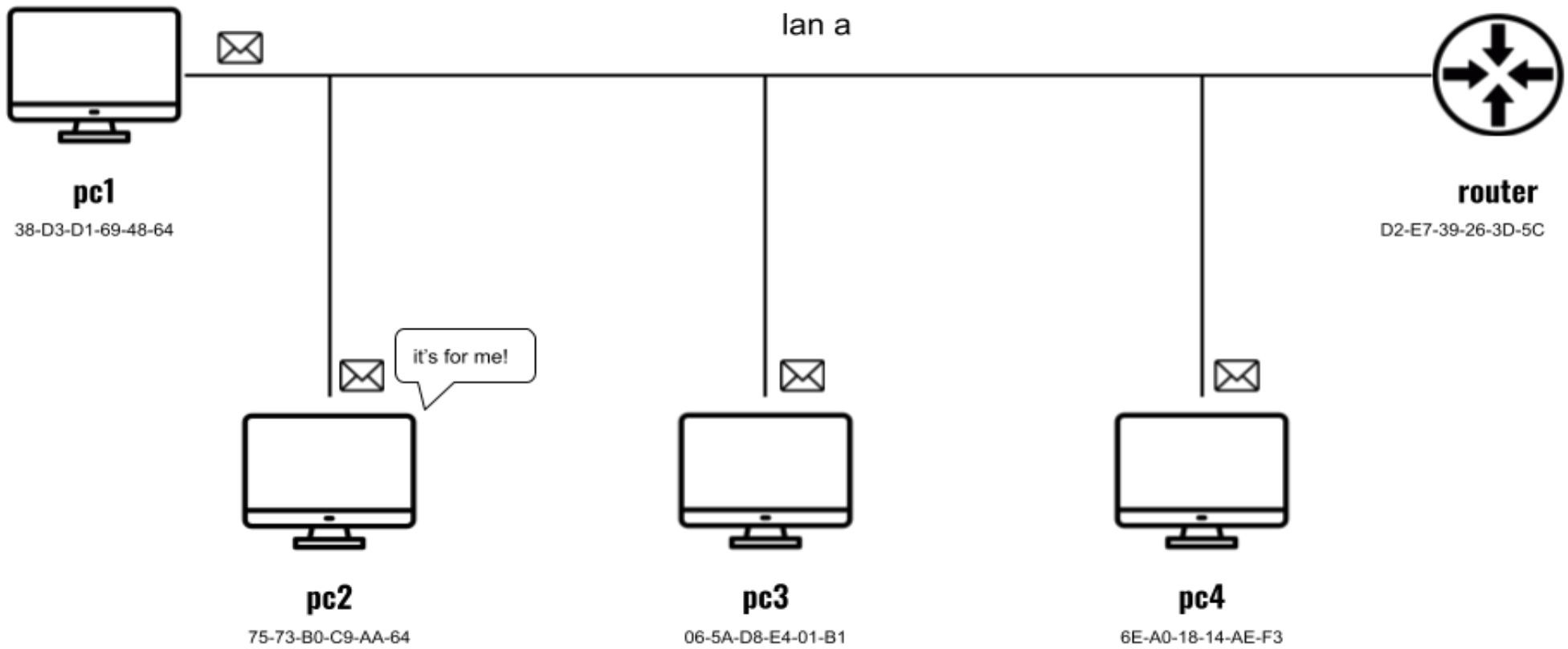
example


lan a
pc1
38-D3-D1-69-48-64
header
payload
pc2
75-73-B0-C9-AA-64
destination address
75-73-B0-C9-AA-64
source address
38-D3-D1-69-48-64

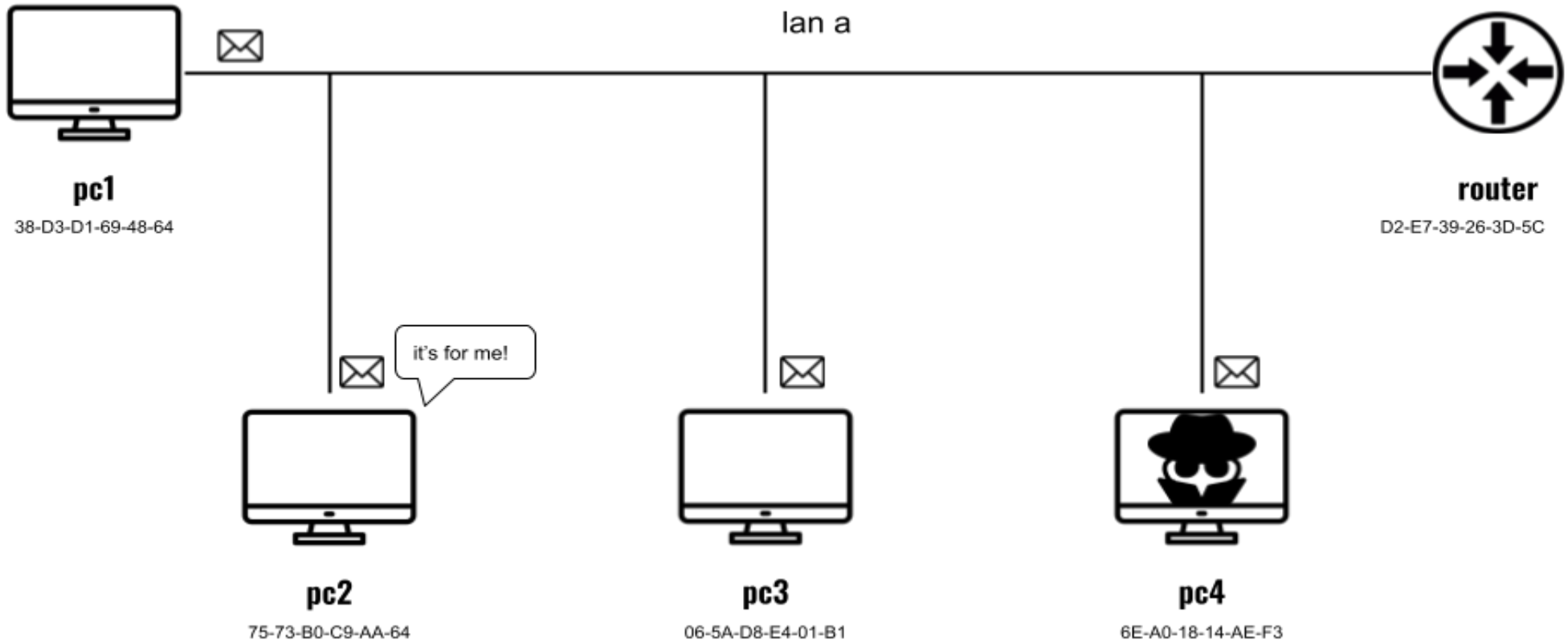
example


lan a
pc1
38-D3-D1-69-48-64
router
D2-E7-39-26-3D-5C
pc2
75-73-B0-C9-AA-64
pc3
06-5A-D8-E4-01-B1
pc4
6E-A0-18-14-AE-F3

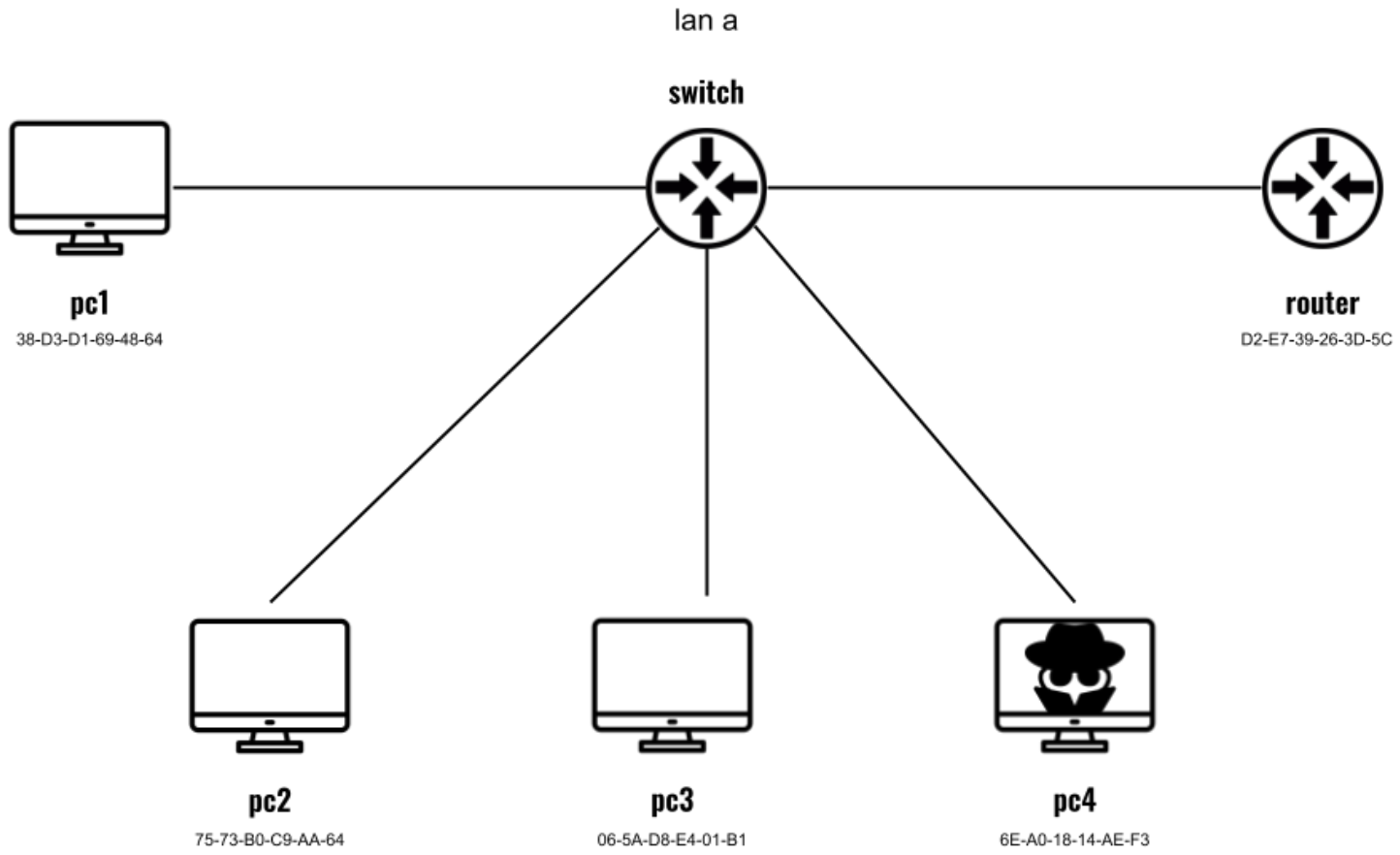
example


lan a
pc1
38-D3-D1-69-48-64
router
D2-E7-39-26-3D-5C
it's for me!
pc2
75-73-B0-C9-AA-64
pc3
06-5A-D8-E4-01-B1
pc4
6E-A0-18-14-AE-F3

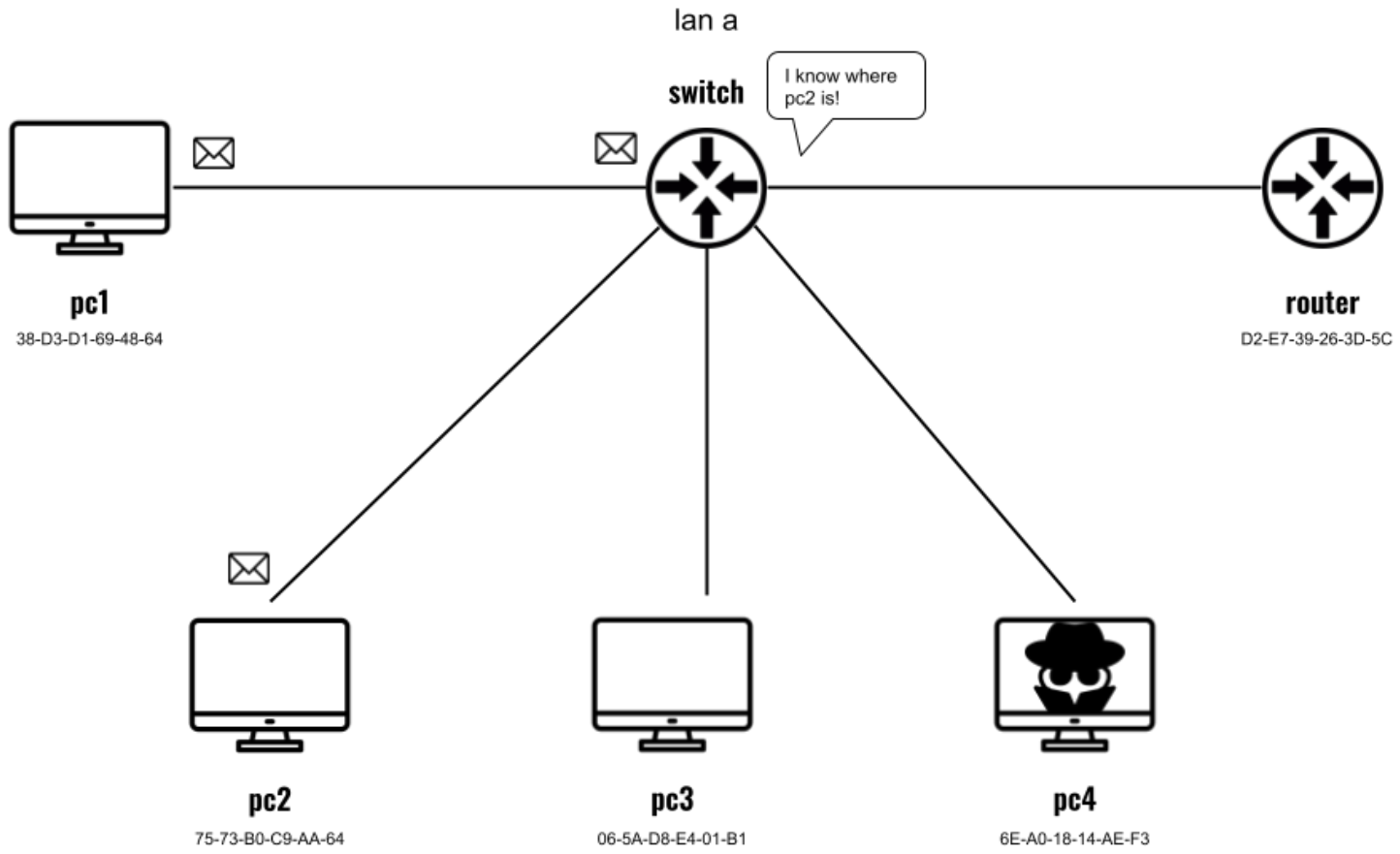
security issue!



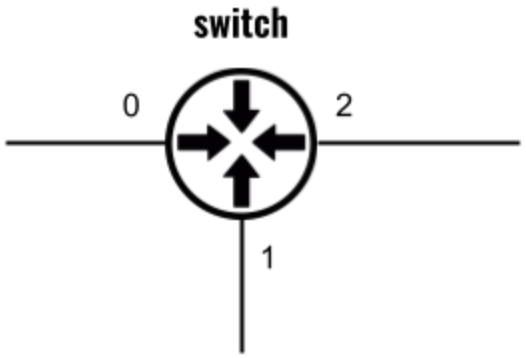
switch


lan a
switch
pc1
38-D3-D1-69-48-64
router
D2-E7-39-26-3D-5C
pc2
75-73-B0-C9-AA-64
pc3
06-5A-D8-E4-01-B1
pc4
6E-A0-18-14-AE-F3

switch


lan a
switch
I know where pc2 is!
pc1
38-D3-D1-69-48-64
router
D2-E7-39-26-3D-5C
pc2
75-73-B0-C9-AA-64
pc3
06-5A-D8-E4-01-B1
pc4
6E-A0-18-14-AE-F3

switch



destination	port
38-D3-D1-69-48-64	1
75-73-B0-C9-AA-64	2
06-5A-D8-E4-01-B1	2
6E-A0-18-14-AE-F3	0
…	…

switch configuration

- manually (administrative effort!)
- autonomously (backward learning)

backward learning

backward learning

`received a packet` ***`p`*** `from port` ***`i`***

backward learning

```
received a packet p from port i
      source_address = get_source(p)
```

backward learning

```
received a packet p from port i
      source_address = get_source(p)
      destination_address = get_destination(p)
```

backward learning

```
received a packet p from port i
      source_address = get_source(p)
      destination_address = get_destination(p)

      map[source_address] = i
```

backward learning

```
received a packet p from port i
      source_address = get_source(p)
      destination_address = get_destination(p)

      map[source_address] = i

      exit_port = map[destination_address]
```

backward learning

```
received a packet p from port i
      source_address = get_source(p)
      destination_address = get_destination(p)

      map[source_address] = i

      exit_port = map[destination_address]
      if exit_port == None:
         send_in_flooding(p)
```

backward learning

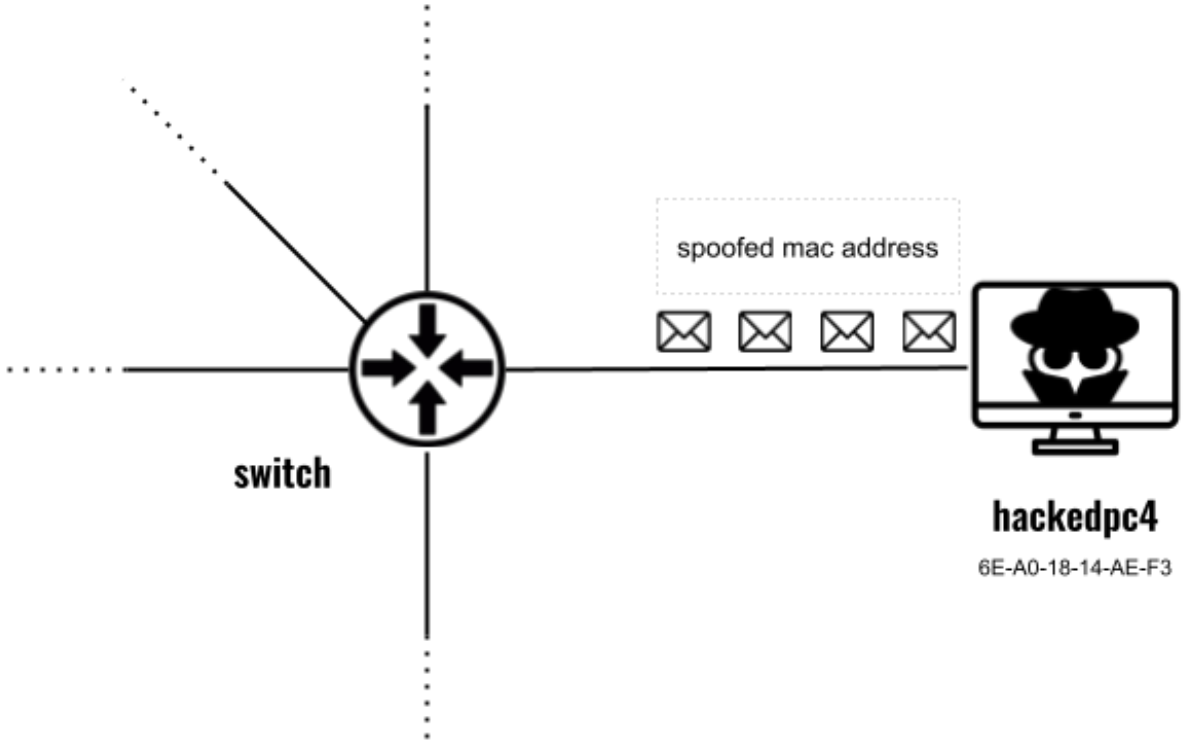
```
received a packet p from port i
      source_address = get_source(p)
      destination_address = get_destination(p)

      map[source_address] = i

      exit_port = map[destination_address]
      if exit_port == None:
         send_in_flooding(p)
      else:
         send(p, exit_port)
```

mac address flooding attack

mac address flooding attack



mac address flooding attack

destination	port
38-D3-D1-69-48-64	1
75-73-B0-C9-AA-64	2
06-5A-D8-E4-01-B1	2
6E-A0-18-14-AE-F3	0
empty	empty
…	…
empty	empty

real | fake

mac address flooding attack

destination	port
38-D3-D1-69-48-64	1
75-73-B0-C9-AA-64	2
06-5A-D8-E4-01-B1	2
6E-A0-18-14-AE-F3	0
empty	empty
…	…
empty	empty

destination	port
38-D3-D1-69-48-64	1
75-73-B0-C9-AA-64	2
06-5A-D8-E4-01-B1	2
6E-A0-18-14-AE-F3	0
4D-6F-EC-BC-32-9C	0
AE-35-8D-A7-61-52	0
6A-3A-AB-1F-76-9B	0

real	fake

mac address flooding attack

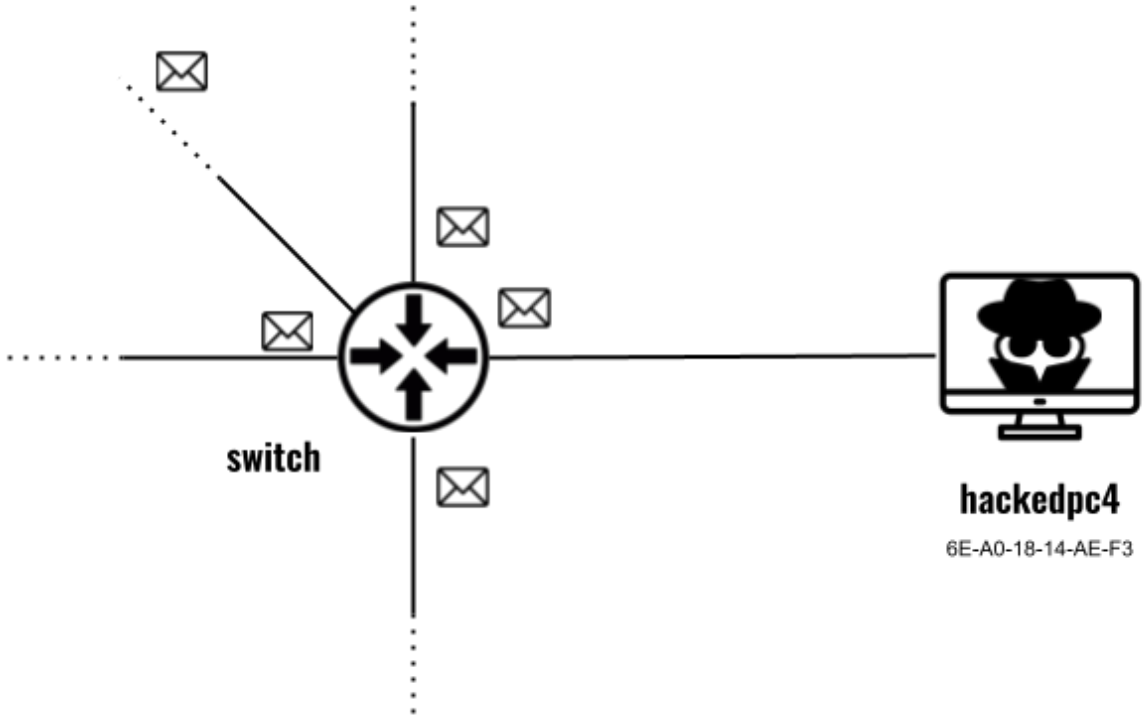
destination	port
38-D3-D1-69-48-64	1
75-73-B0-C9-AA-64	2
06-5A-D8-E4-01-B1	2
6E-A0-18-14-AE-F3	0
empty	empty
…	…
empty	empty

destination	port
38-D3-D1-69-48-64	1
75-73-B0-C9-AA-64	2
06-5A-D8-E4-01-B1	2
6E-A0-18-14-AE-F3	0
4D-6F-EC-BC-32-9C	0
AE-35-8D-A7-61-52	0
6A-3A-AB-1F-76-9B	0

destination	port
AC-EF-36-C7-89-DE	0
8A-C1-88-FE-20-B9	0
38-33-54-91-D1-BF	0
47-F7-4B-07-F8-C6	0
4D-6F-EC-BC-32-9C	0
AE-35-8D-A7-61-52	0
6A-3A-AB-1F-76-9B	0

real	fake

mac address flooding attack



some important mitigations

- port security feature
  - set a maximum number of mac address in the table
  - set a maximum number of mac address on each port
- trust mac address that match in arp table

questions?

thank you!

TACK ☺