ICE-cold connection

ICE, TURN, STUN and more in between

Anton Kvyatkovsky
Sr. Software Engineer at DINS

What’s up?

Client

UDP

?

Server

Local configuration

Client: 192.168.0.1

UDP

?

Server: 192.168.0.2

Connecting
Allocating a socket

Client: 192.168.0.1

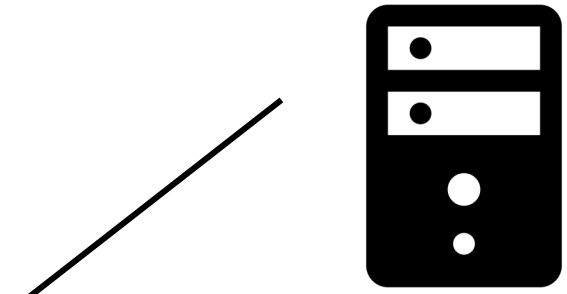
UDP

?

Server:
192.168.0.2:1234

Connecting

Some intermediate server



I AM: 192.168.0.2:1234

Client: 192.168.0.1

Server:
192.168.0.2:1234

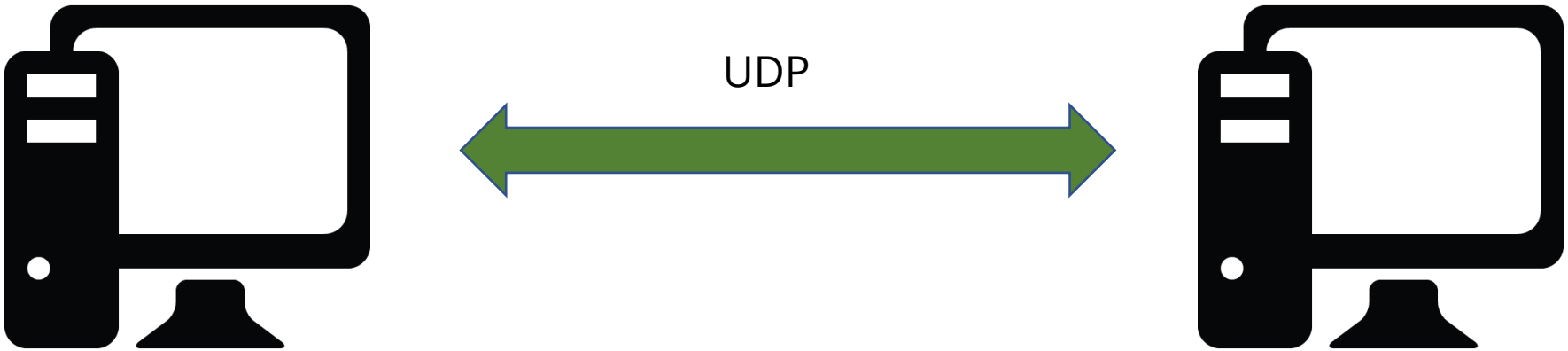
UDP

?

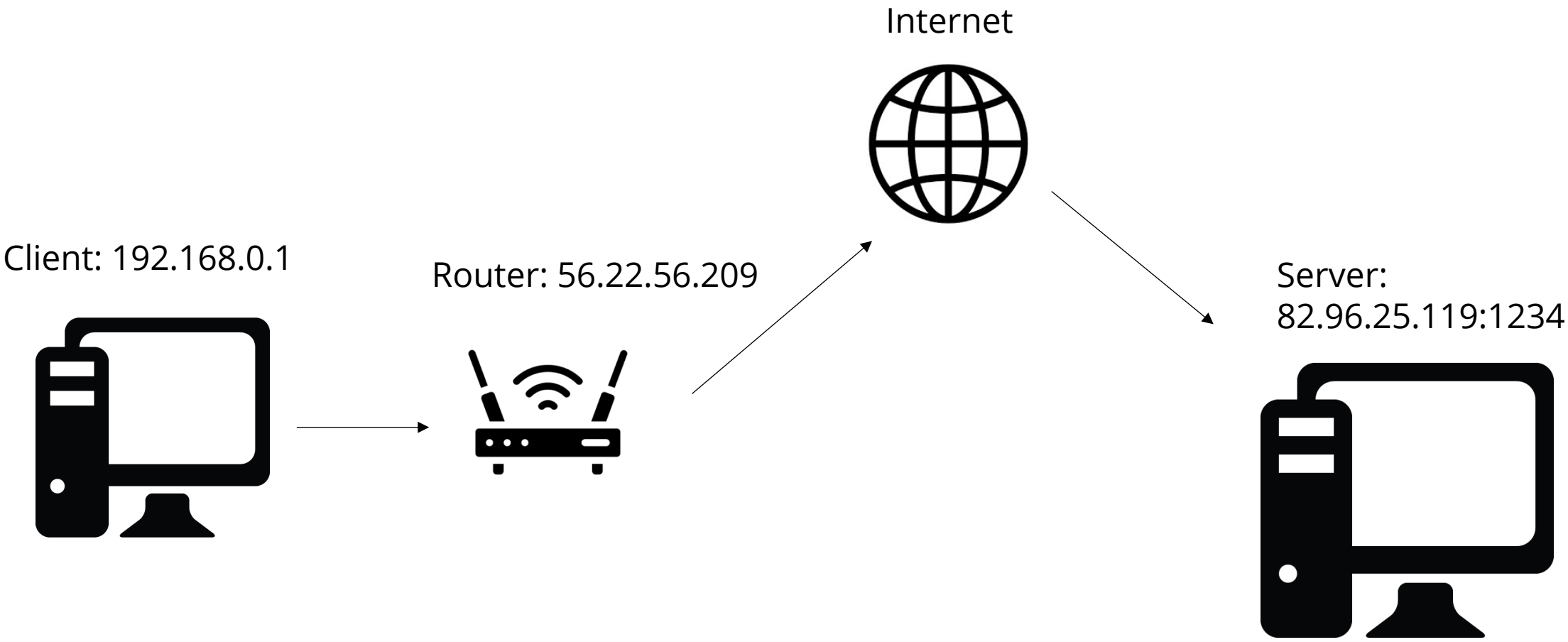
Connecting

Client: 192.168.0.1

Server:
192.168.0.2:1234



Real life configuration
NAT



NAT

NAT

Client: 192.168.0.1:1

Router: 56.22.56.209

Server: 82.96.25.119:2

UDP packet		
	Ip	port
Src	192.168.0.1	1
Dst	82.96.25.119	2

NAT Table

Client: 192.168.0.1:1

Local ip	Local port	External ip	External port
192.168.0.1	1	56.22.56.209	3

Server: 82.96.25.119:2

Router: 56.22.56.209

UDP packet		
	Ip	port
Src	192.168.0.1	1
Dst	82.96.25.119	2

NAT Table

Client: 192.168.0.1:1

Local ip	Local port	External ip	External port
192.168.0.1	1	56.22.56.209	3

Router: 56.22.56.209

Server: 82.96.25.119:2

UDP packet		
	Ip	port
Src	192.168.0.1	1
Dst	82.96.25.119	2

UDP packet		
	Ip	port
Src	56.22.56.209	3
Dst	82.96.25.119	2

NAT

Client: 192.168.0.1:1

Router: 56.22.56.209:3

Server: 82.96.25.119:2

UDP packet		
	Ip	port
Src	56.22.56.209	3
Dst	82.96.25.119	2

NAT Reply

Client: 192.168.0.1

Router: 56.22.56.209:3

Server: 82.96.25.119:2

UDP packet		
	Ip	port
Src	82.96.25.119	2
Dst	56.22.56.209	3

NAT Reply

Client: 192.168.0.1

Local ip	Local port	External ip	External port
192.168.0.1	1	56.22.56.209	3

Router: 56.22.56.209:3

Server: 82.96.25.119:2

UDP packet		
	Ip	port
Src	82.96.25.119	2
Dst	56.22.56.209	3

NAT Reply

Client: 192.168.0.1:1

Local ip	Local port	External ip	External port
192.168.0.1	1	56.22.56.209	3

Router: 56.22.56.209:3

Server: 82.96.25.119:2

UDP packet		
	Ip	port
Src	82.96.25.119	2
Dst	192.168.0.1	1

UDP packet		
	Ip	port
Src	82.96.25.119	2
Dst	56.22.56.209	3

NAT Reply

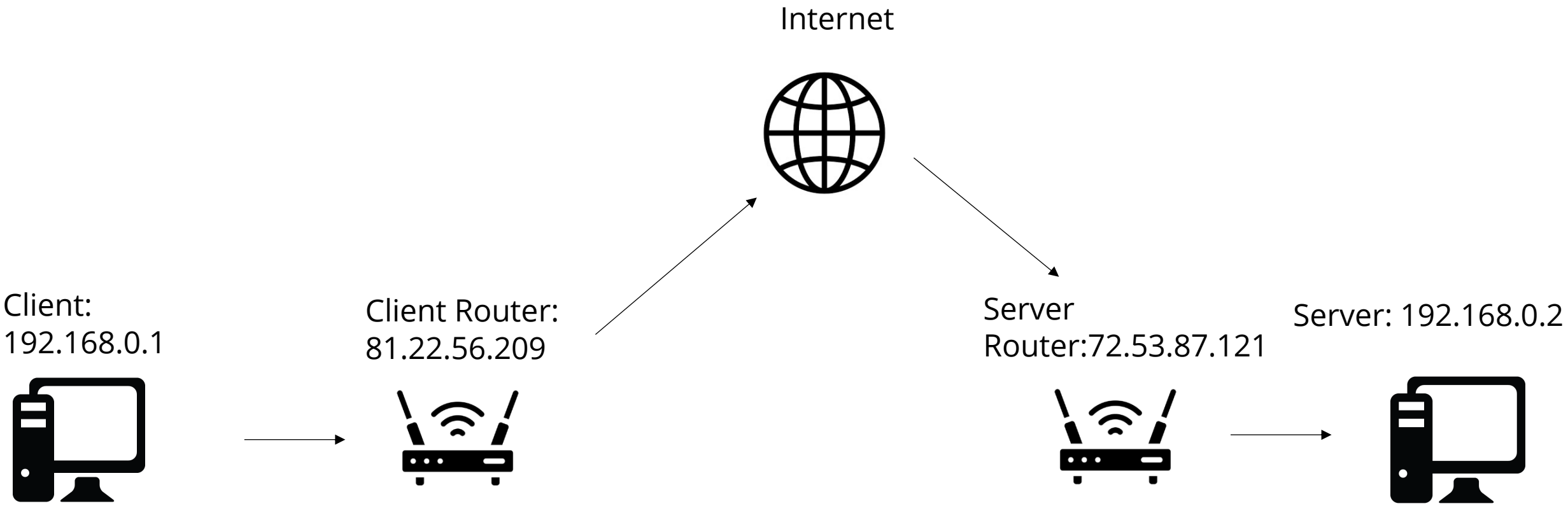
Client: 192.168.0.1:1

Router: 56.22.56.209:3

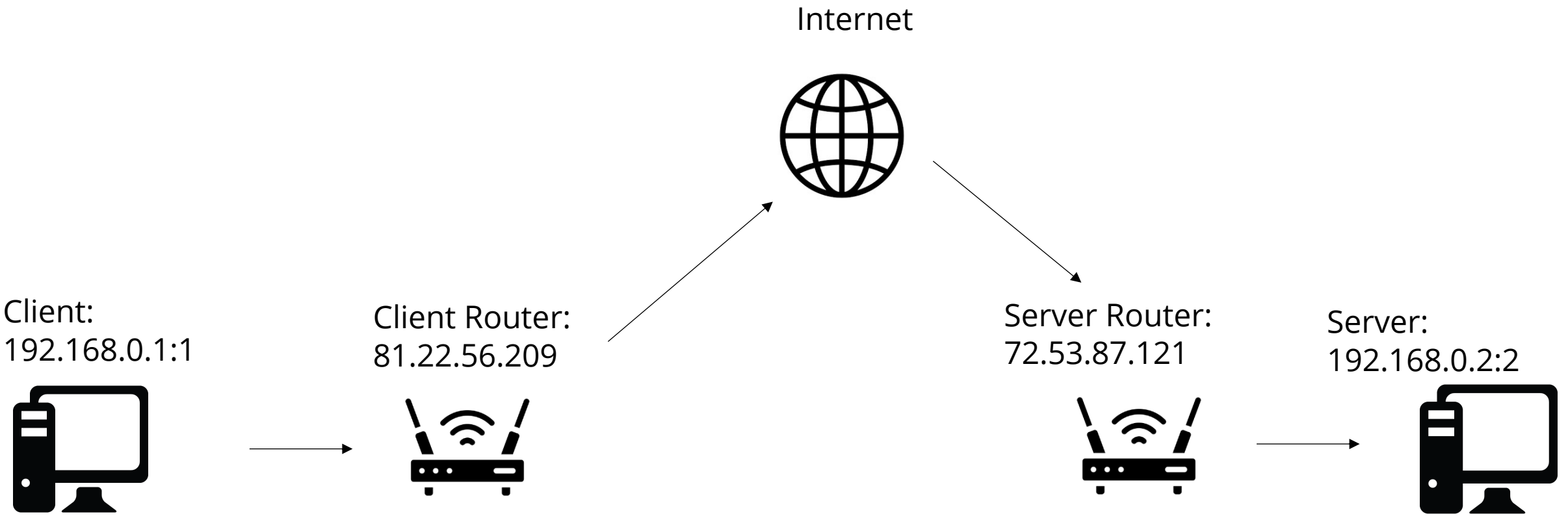
Server: 82.96.25.119:2

UDP packet		
	Ip	port
Src	82.96.25.119	2
Dst	192.168.0.1	1

Server NAT


Internet
Client:
192.168.0.1
Client Router:
81.22.56.209
Server
Router:72.53.87.121
Server: 192.168.0.2

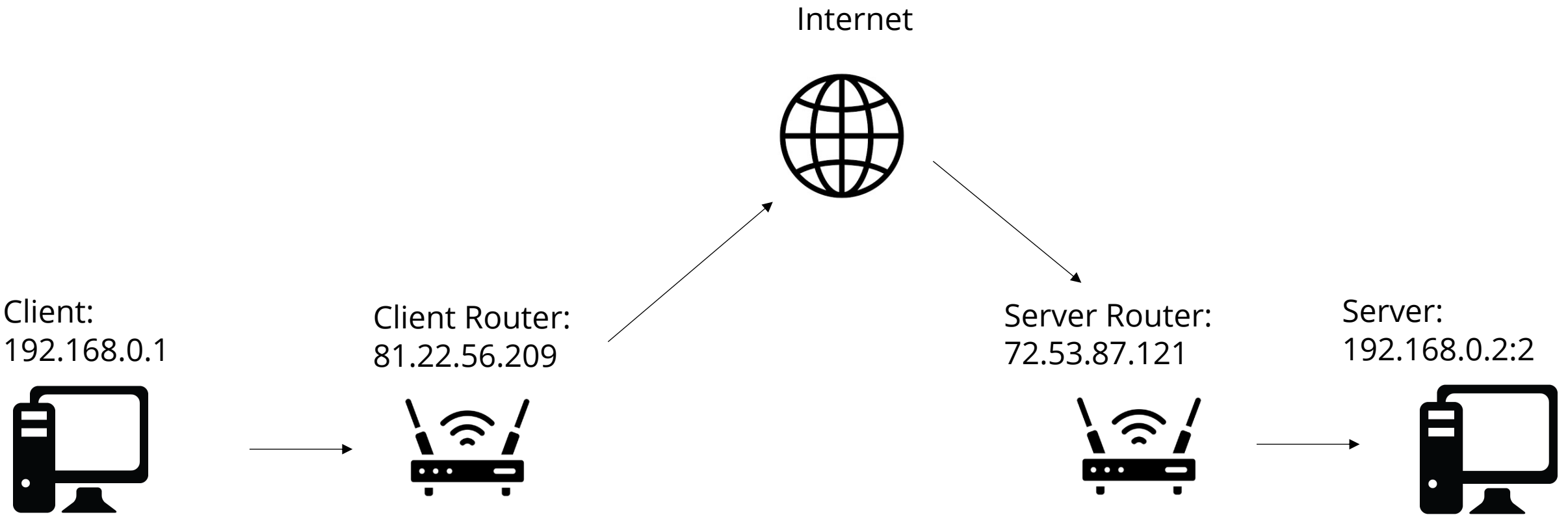
Server NAT



UDP packet		
	Ip	port
Src	192.168.0.1	1
Dst	192.168.0.2	2

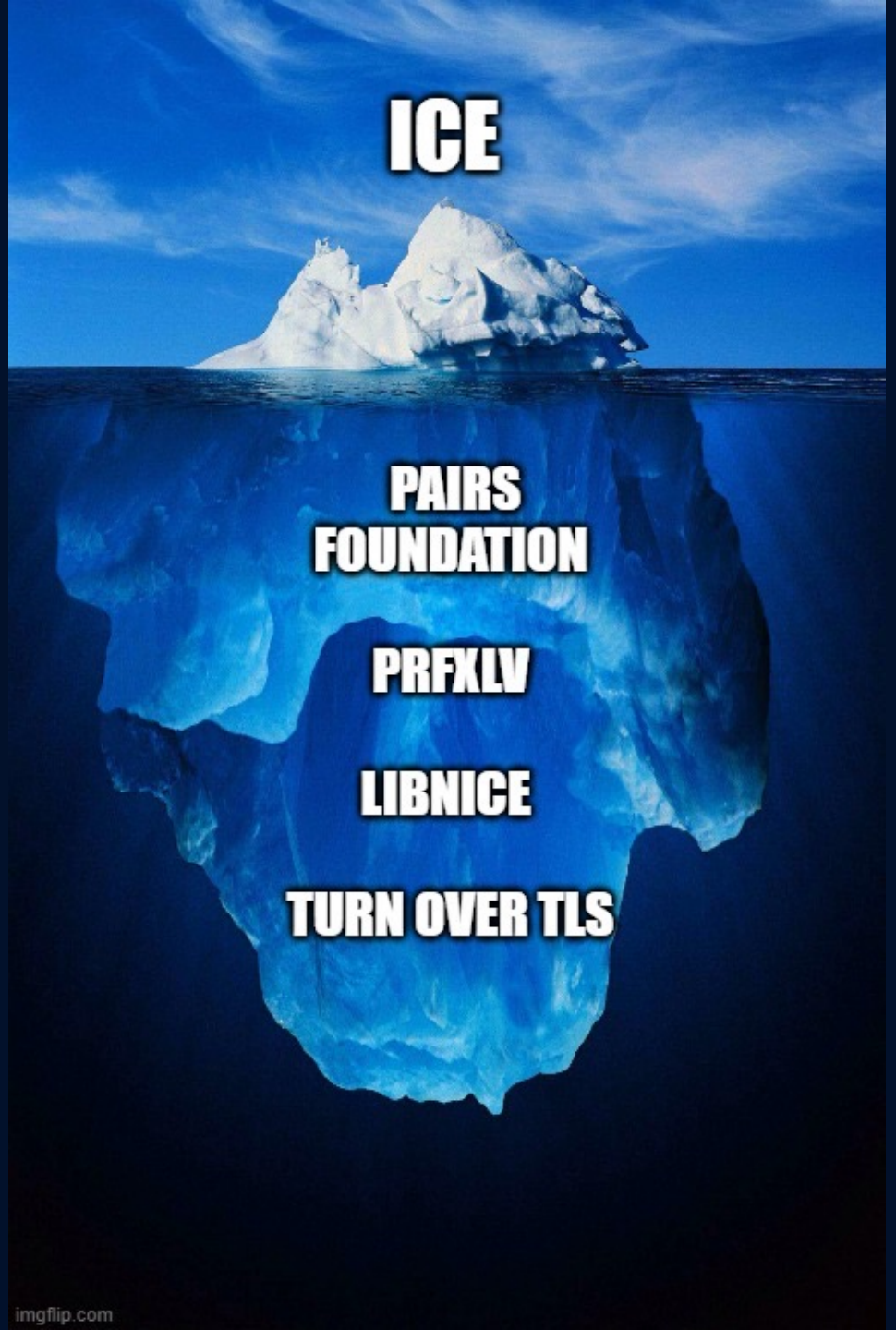
No route to host

Server NAT



UDP packet		
	Ip	port
Src	192.168.0.1	1
Dst	72.53.87.121	2

Port is unavailable


ICE
PAIRS
FOUNDATION
PRFXLV
LIBNICE
TURN OVER TLS
imgflip.com

Interactive Connectivity Establishment

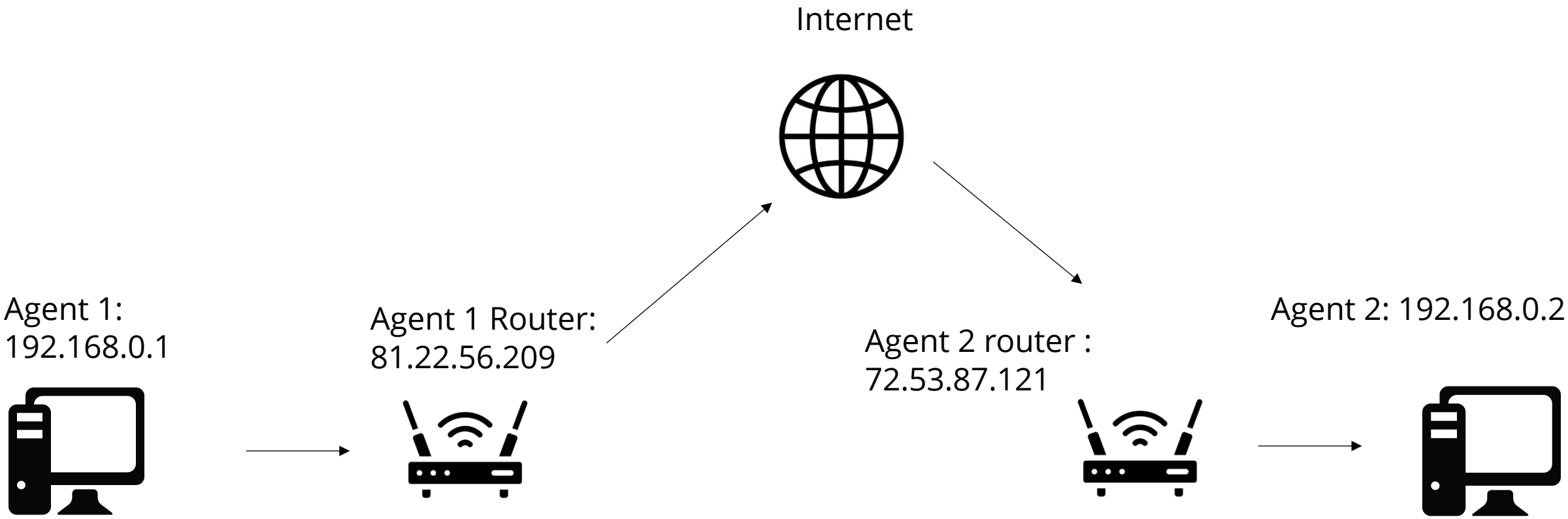
Protocol which describes NAT traversal using STUN and TURN

Described in RFC, latest - RFC 8445

Currently used by most of implementations - RFC 5245

“The problem is, the language about priority updates is _extremely_ muddy when we look at the specs from the aggressive nomination days.” - Byron Campen, Author of ICE Trickle proposal

ICE Procedures



Gather the ~~Elders~~ Candidates

Candidates Gathering

Agent

eth0:192.168.0.1

tun0:10.12.15.1

Candidates Gathering

Agent

eth0:192.168.0.1

tun0:10.12.15.1

Candidate 1: 192.168.0.1:1

Candidate 2: 10.12.15.1:2

Pairs making

Agent 1

Local candidates:

1: 192.168.0.1:1

2: 10.12.15.1:2

Agent 2

Local candidates:

1: 192.168.0.2:3

2: 10.11.17.8:4

Pairs making

Agent 1

Local candidates:
1: 192.168.0.1:1

2: 10.12.15.1:2

Remote candidates:

Agent 2

Local candidates:

1: 192.168.0.2:3

2: 10.11.17.8:4

Remote candidates:

Pairs making

Agent 1

Pairs

	Local candidates	Remote candidates
1	192.168.0.1:1	192.168.0.2:3
2	192.168.0.1:1	10.11.17.8:4
3	10.12.15.1:2	192.168.0.2:3
4	10.12.15.1:2	10.11.17.8:4

Agent 2

Pairs

	Local candidates	Remote candidates
1	192.168.0.2:3	192.168.0.1:1
2	192.168.0.2:3	10.12.15.1:2
3	10.11.17.8:4	192.168.0.1:1
4	10.11.17.8:4	10.12.15.1:2

Connectivity checks

Pair:

Local candidate	Remote candidate
192.168.0.1:1	192.168.0.2:3

Connectivity checks

Pair:

Local candidate	Remote candidate
192.168.0.1:1	192.168.0.2:3

- Is it writable? – Send check and receive response
- Is it readable? – Receive check from the other side and send response

STUN

STUN

- Protocol build usually over UDP, but can be used with TCP too
- Most popular implementations uses spec rfc5389
- Defines different message types
- Is a tool, not a solution

Connectivity checks
STUN Binding Request

Pair:

Local candidate	Remote candidate
192.168.0.1:1	192.168.0.2:3

STUN BINDING REQUEST

STUN BINDING RESPONSE

Connectivity checks
STUN Binding Request

Pair:

Local candidate	Remote candidate	Writable
192.168.0.1:1	192.168.0.2:3	+

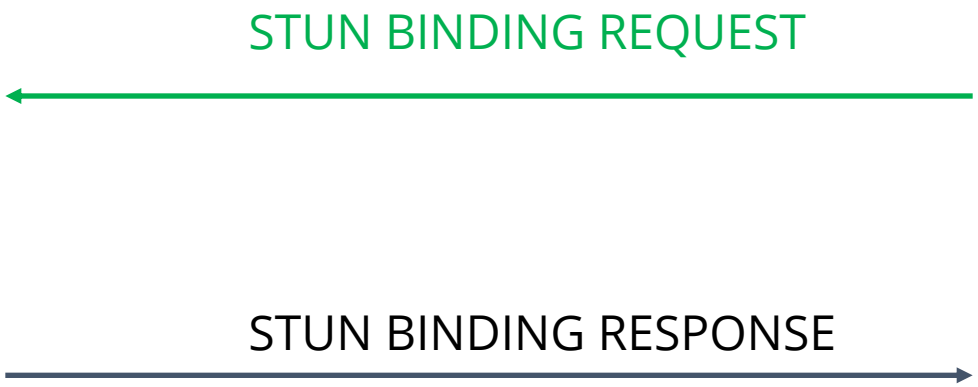
STUN BINDING REQUEST

STUN BINDING RESPONSE

Connectivity checks
STUN Binding Request

Pair:

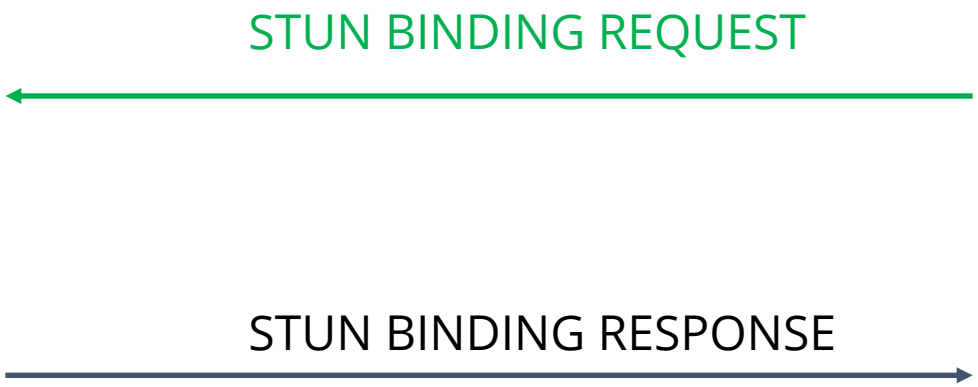
Local candidate	Remote candidate
192.168.0.1:1	192.168.0.2:3



Connectivity checks
STUN Binding Request

Pair:

Local candidate	Remote candidate	Readable
192.168.0.1:1	192.168.0.2:3	+



Connectivity checks
ICE Connected

Pair:

Local candidate	Remote candidate	Readable	Writable	Nominated
192.168.0.1:1	192.168.0.2:3	+	+	true

Connecting → Connected

Nominated pairs

Pairs

	Local candidates	Remote candidates	Writable	Readable	Nominated
1	192.168.0.1:1	192.168.0.2:3	+	+	+
2	192.168.0.1:1	10.11.17.8:4	?	?	-
3	10.12.15.1:2	192.168.0.2:3	+	?	-
4	10.12.15.1:2	10.11.17.8:4	+	+	+

Nominated pairs

Pairs

	Local candidates	Remote candidates	Writable	Readable	Nominated
1	192.168.0.1:1	192.168.0.2:3	+	+	+
2	192.168.0.1:1	10.11.17.8:4	?	?	-
3	10.12.15.1:2	192.168.0.2:3	+	?	-
4	10.12.15.1:2	10.11.17.8:4	+	+	+

Nominated pairs
Priority

Pairs

	Local candidates	Remote candidates	Writable	Readable	Nominated	Priority
1	192.168.0.1:1	192.168.0.2:3	+	+	+	8923479124793244
2	192.168.0.1:1	10.11.17.8:4	?	?	-	
3	10.12.15.1:2	192.168.0.2:3	+	?	-	
4	10.12.15.1:2	10.11.17.8:4	+	+	+	5468792347892347

Local configuration

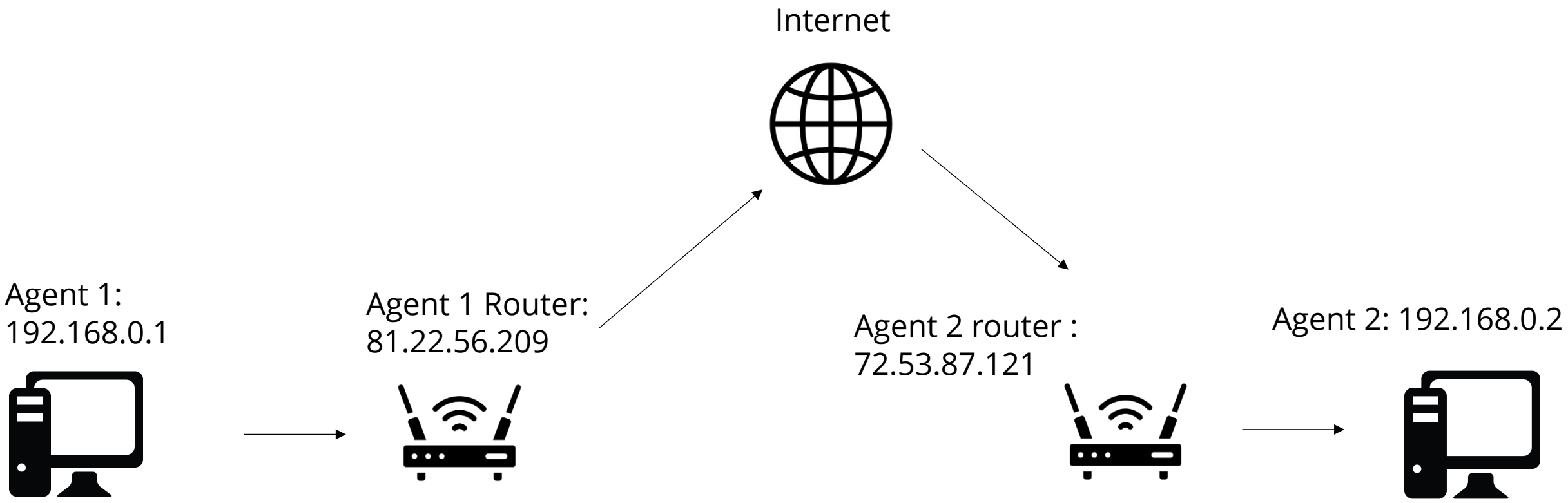
Agent1: 192.168.0.1:1

UDP

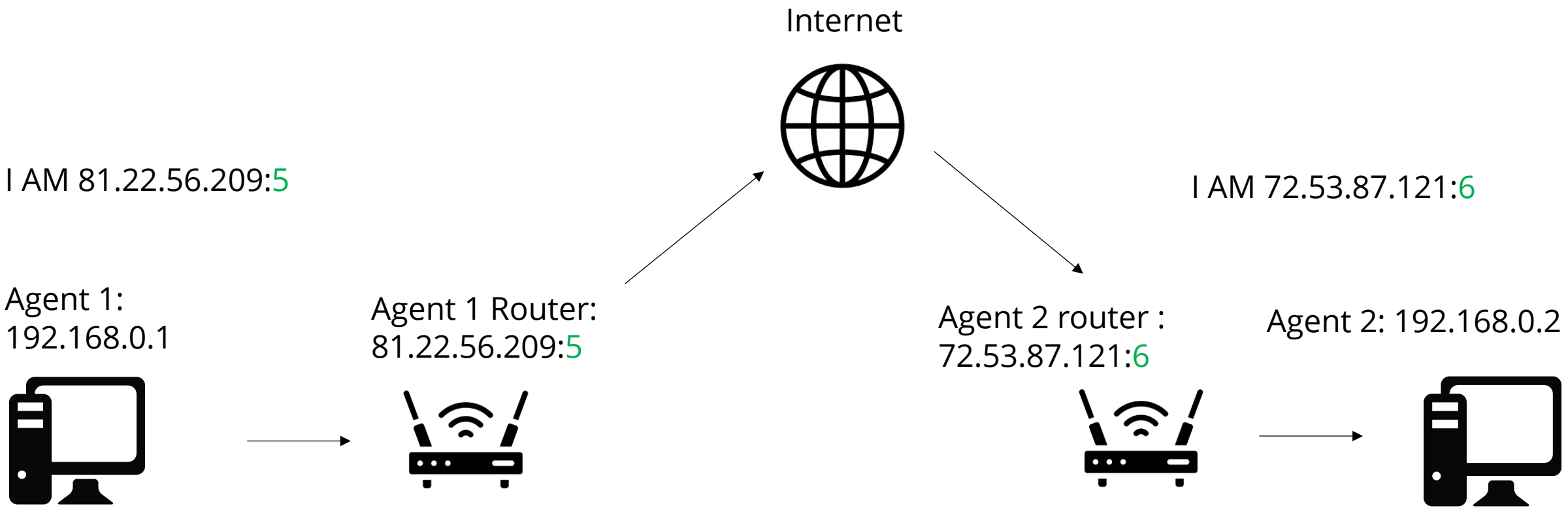
?

Agent2: 192.168.0.2:3

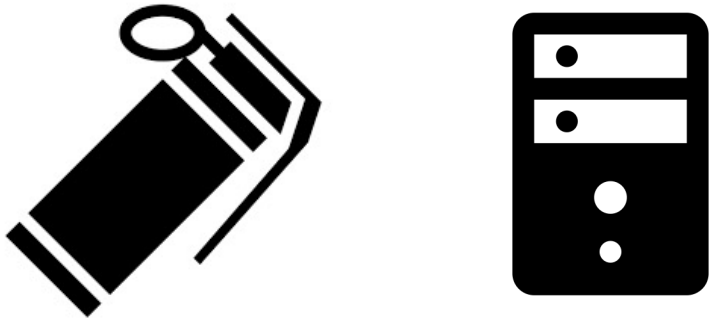
Common network configuration



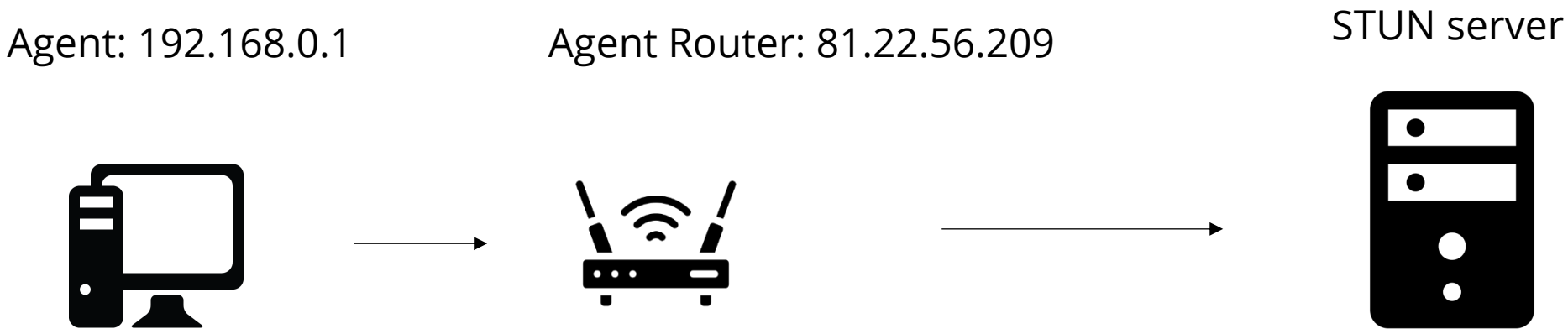
Common network configuration
Ports opening



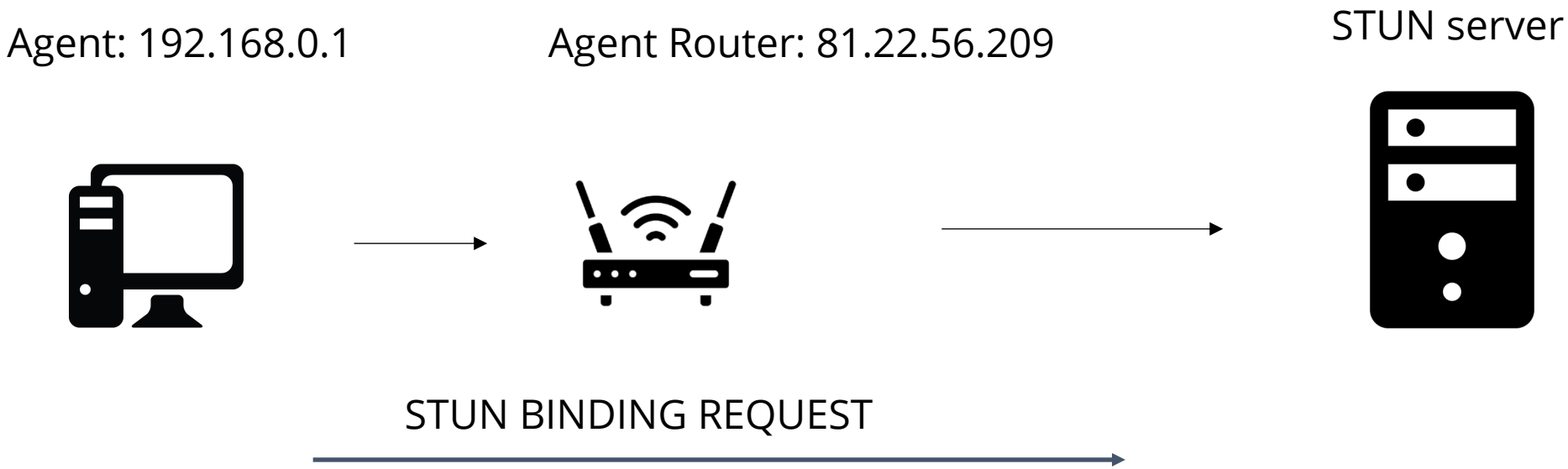
STUN
server



STUN server


Agent: 192.168.0.1
Agent Router: 81.22.56.209
STUN server
Who am I?
You are: 81.22.56.209:5

STUN server


Agent: 192.168.0.1
Agent Router: 81.22.56.209
STUN server
STUN BINDING REQUEST
STUN BINDING RESPONSE
XOR-MAPPED-ADDRESS: 81.22.56.209:5

STUN server
Gathering STUN candidate

Agent

Pairs

	Local candidates	Remote candidates
1	192.168.0.1:1	192.168.0.2:3
2	192.168.0.1:1	10.11.17.8:4
3	10.12.15.1:2	192.168.0.2:3
4	10.12.15.1:2	10.11.17.8:4

STUN server
Gathering STUN candidate

Agent

Pairs

	Local candidates	Remote candidates
1	192.168.0.1:1	192.168.0.2:3

STUN server
Gathering STUN candidate

Agent

Pairs

	Local candidates	Remote candidates
1	192.168.0.1:1	192.168.0.2:3
2	81.22.56.209:5	192.168.0.2:3

STUN server
Server reflexive candidate

Agent

Pairs

	Local candidates	Type	Remote candidates
1	192.168.0.1:1	Host	192.168.0.2:3
2	81.22.56.209:5	Server reflexive	192.168.0.2:3

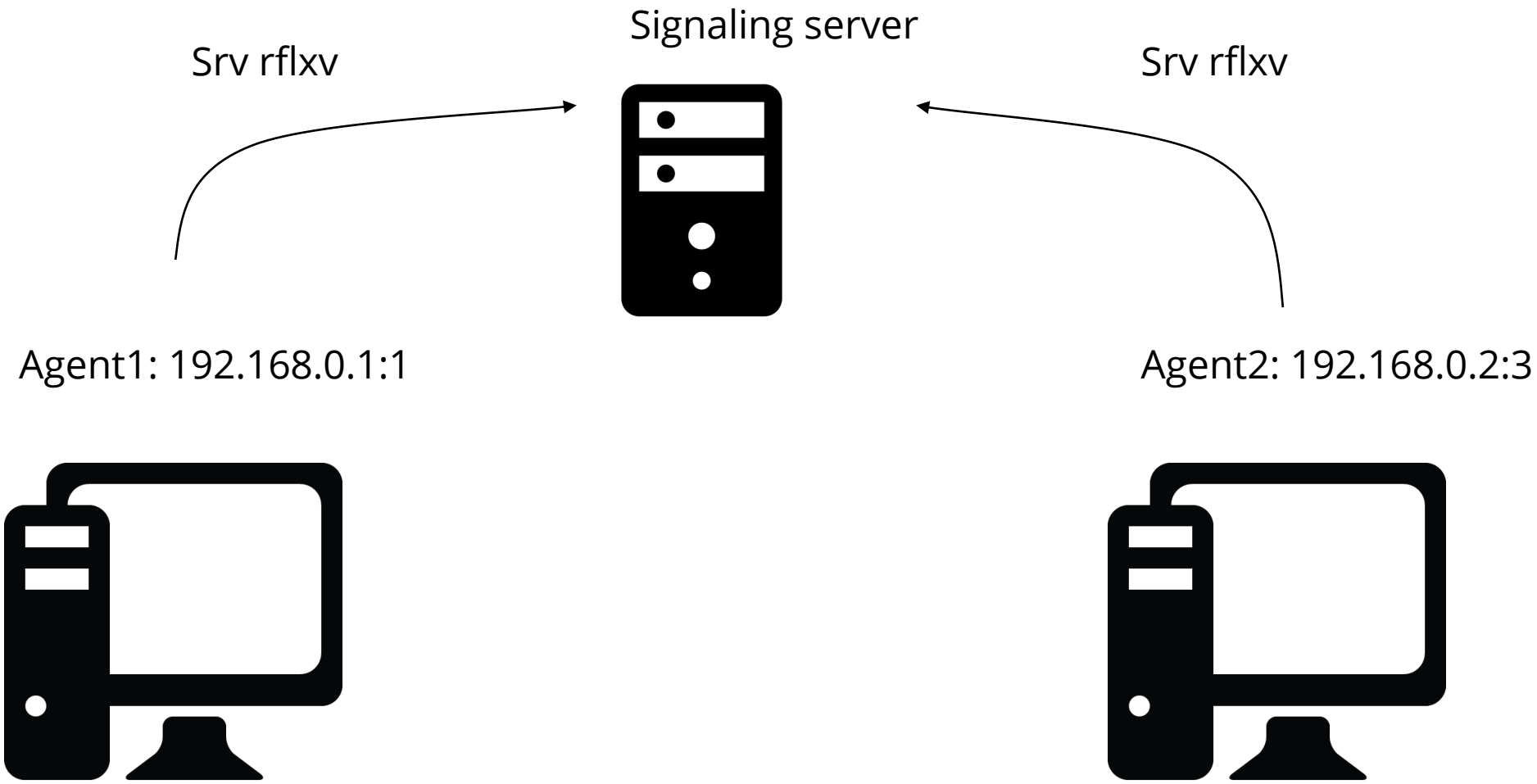
STUN server
Server reflexive candidate

Agent

Pairs

	Local candidates	Type	Remote candidates	Priority
1	192.168.0.1:1	Host	192.168.0.2:3	5437
2	81.22.56.209:5	Server reflexive	192.168.0.2:3	2342

Share the candidates



STUN server
Server reflexive remote candidate

Pairs

Agent

	Local candidates	Type	Remote candidates	Type	Priority
1	192.168.0.1:1	Host	192.168.0.2:3	Host	5437
2	192.168.0.1:1	Host	72.53.87.121:5	Server reflexive	2340
3	81.22.56.209:5	Server reflexive	192.168.0.2:3	Host	2342
4	81.22.56.209:5	Server reflexive	72.53.87.121:5	Server reflexive	1324

STUN server
Main pair

Agent

Pairs

	Local candidates	Type	Remote candidates	Type	Priority
1	192.168.0.1:1	Host	192.168.0.2:3	Host	5437
2	192.168.0.1:1	Host	72.53.87.121:5	Server reflexive	2340
3	81.22.56.209:5	Server reflexive	192.168.0.2:3	Host	2342
4	81.22.56.209:5	Server reflexive	72.53.87.121:5	Server reflexive	1324

Connectivity checks
STUN Binding Request

Pair:

Local candidate	Remote candidate
81.22.56.209:5	72.53.87.121:5

STUN BINDING REQUEST

STUN BINDING RESPONSE

Connectivity checks
STUN Binding Request

Pair:

Local candidate	Remote candidate
81.22.56.209:5	72.53.87.121:5

STUN BINDING REQUEST

STUN BINDING RESPONSE

Connectivity checks
Base address

Pair:

Local candidate	Remote candidate
192.168.0.1:1	72.53.87.121:5

STUN BINDING REQUEST

STUN BINDING RESPONSE

Connectivity checks
Pair with base address

Agent

Pairs

	Local candidates	Type	Remote candidates	Type	Priority
1	192.168.0.1:1	Host	192.168.0.2:3	Host	5437
2	192.168.0.1:1	Host	72.53.87.121:5	Server reflexive	2340
3	81.22.56.209:5	Server reflexive	192.168.0.2:3	Host	2342
4	81.22.56.209:5	Server reflexive	72.53.87.121:5	Server reflexive	1324

STUN server

Agent: 192.168.0.1

Agent Router: 81.22.56.209

STUN server (2nd Agent)

STUN BINDING REQUEST

STUN BINDING RESPONSE
XOR-MAPPED-ADDRESS: 81.22.56.209:5

Connectivity checks
Pair with base address

Agent

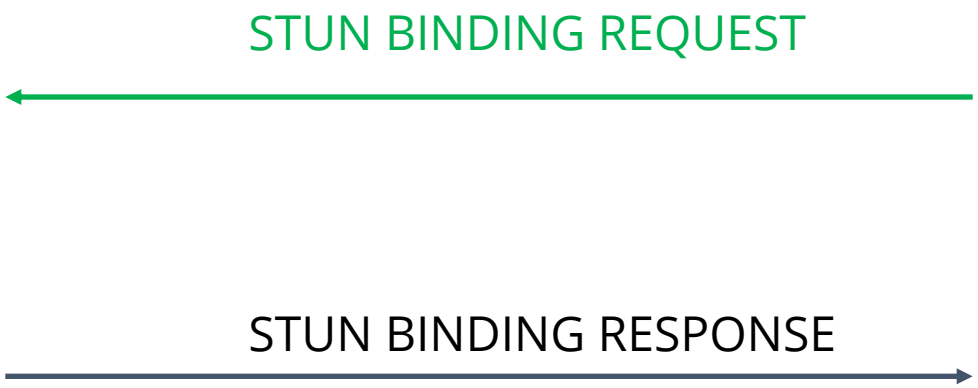
Pairs

	Local candidates	Type	Remote candidates	Type	Priority	Status
1	192.168.0.1:1	H	192.168.0.2:3	H	5437	
2	192.168.0.1:1	H	72.53.87.121:5	S	2340	Succeeded
3	81.22.56.209:5	S	192.168.0.2:3	H	2342	
4	81.22.56.209:5	S	72.53.87.121:5	S	1324	Writable

Connectivity checks
STUN Binding Response

Pair:

Local candidate	Remote candidate
81.22.56.209:5	72.53.87.121:5



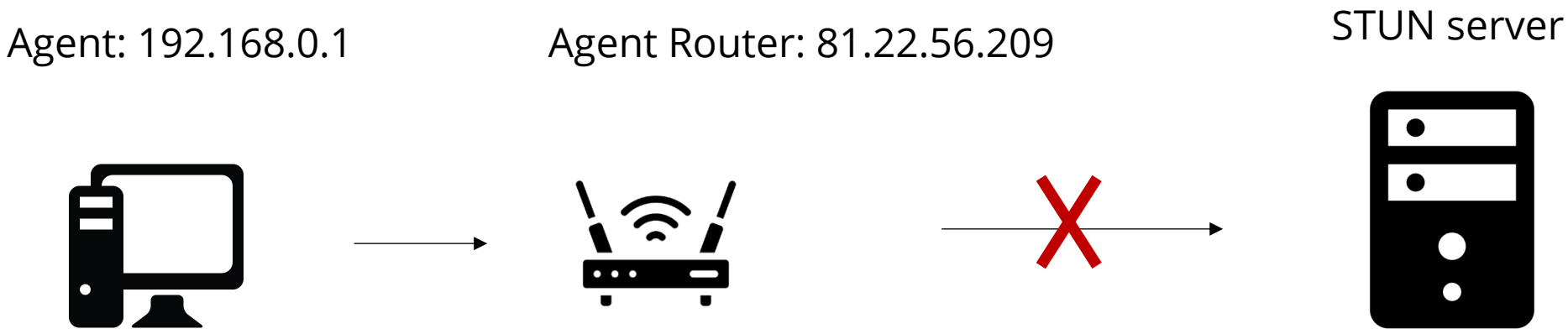
Connectivity checks
ICE Connected

Pair:

Local candidate	Remote candidate	Readable	Writable	Nominated
81.22.56.209:5	72.53.87.121:5	+	+	true

Connecting → Connected

STUN server
Failed discovery



STUN server
Failed discovery

Pairs

Agent

	Local candidates	Type	Remote candidates	Type	Priority
1	192.168.0.1:1	Host	192.168.0.2:3	Host	5437
2	192.168.0.1:1	Host	72.53.87.121:5	Server reflexive	2340
3	~~81.22.56.209:5~~	~~Server reflexive~~	~~192.168.0.2:3~~	~~Host~~	~~2342~~
4	~~81.22.56.209:5~~	~~Server reflexive~~	~~72.53.87.121:5~~	~~Server reflexive~~	~~1324~~

STUN server
Failed discovery

Agent

Pairs

	Local candidates	Type	Remote candidates	Type	Priority
1	192.168.0.1:1	Host	192.168.0.2:3	Host	5437
2	192.168.0.1:1	Host	72.53.87.121:5	Server reflexive	2340

Connectivity checks

Pair:

Local candidate	Remote candidate
192.168.0.1:1	72.53.87.121:5

STUN BINDING REQUEST

STUN BINDING RESPONSE

Connectivity checks

Pair:

Local candidate	Remote candidate
192.168.0.1:1	72.53.87.121:5

STUN BINDING REQUEST

STUN BINDING RESPONSE
XOR-MAPPED-ADDRESS: 81.22.56.209:5

STUN server
Gathering candidate

Agent

	Local candidates
1	192.168.0.1:1

XOR-MAPPED-ADDRESS: 81.22.56.209:5

STUN server
Gathering candidate

Agent

	Local candidates
1	192.168.0.1:1
3	81.22.56.209:5

XOR-MAPPED-ADDRESS: 81.22.56.209:5

STUN server
Peer reflexive candidate

Agent

	Local candidates	Type
1	192.168.0.1:1	Host
2	81.22.56.209:5	Peer reflexive

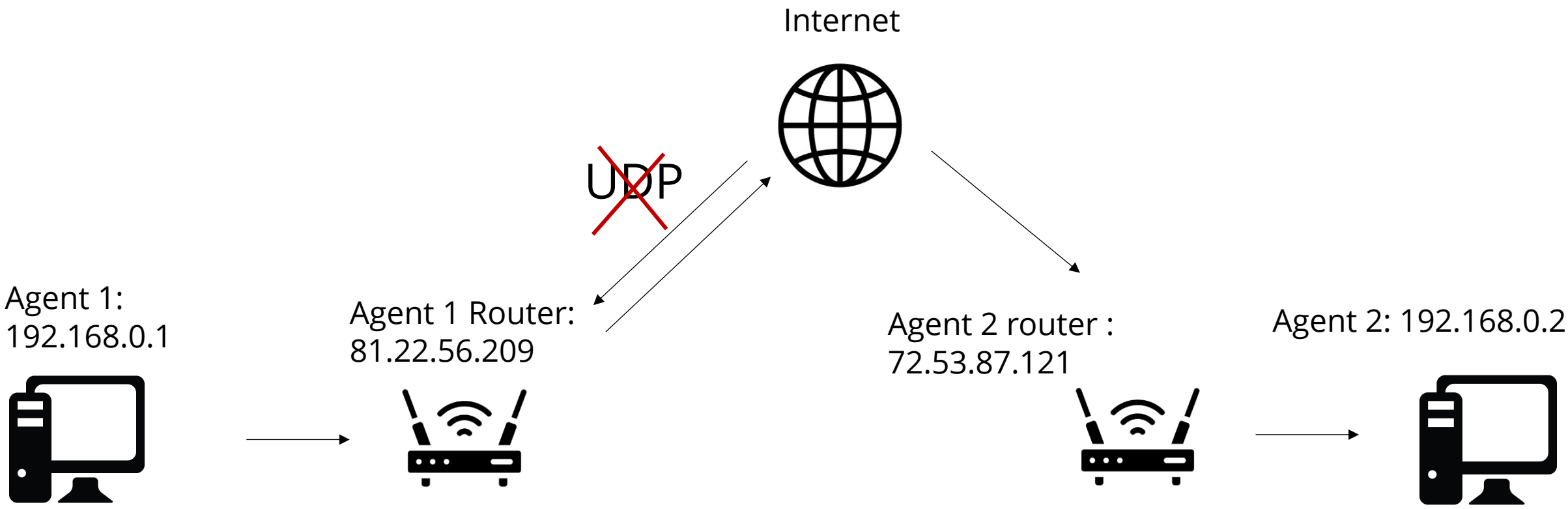
Connectivity checks
ICE Connected

Pair:

Local candidate	Remote candidate	Readable	Writable	Nominated
81.22.56.209:5	72.53.87.121:5	+	+	true

Connecting → Connected

Firewall rules

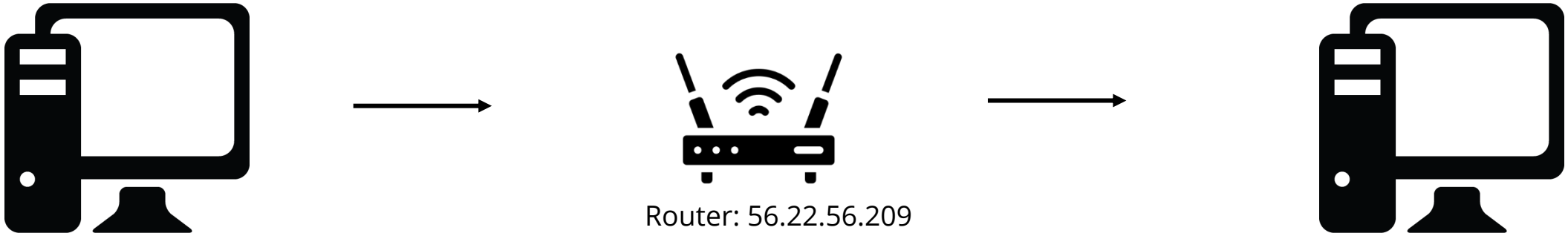


NAT Table
Symmetric NAT

Local ip	Local port	External ip	External port	Destination addr
192.168.0.1	1	56.22.56.209	3	82.96.25.119:2

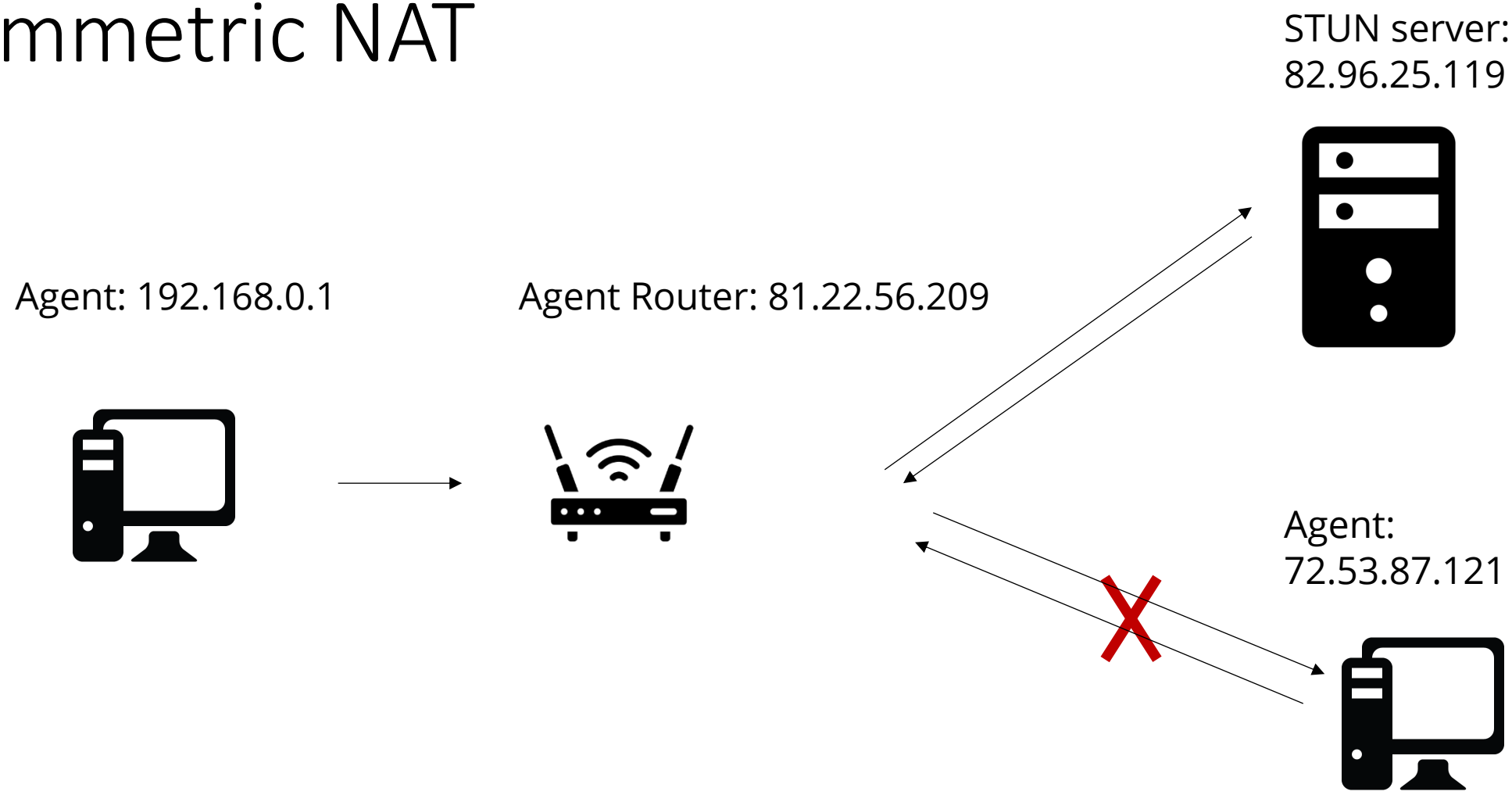
Client:
192.168.0.1

Server: 82.96.25.119:2

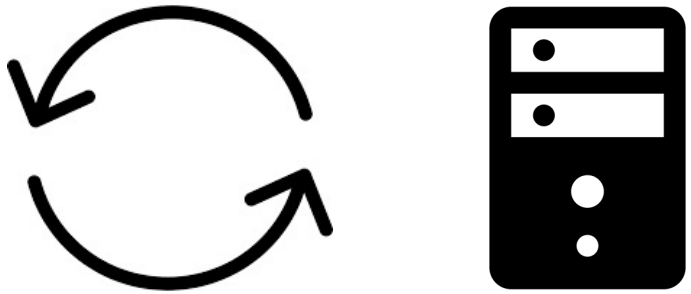


Router: 56.22.56.209

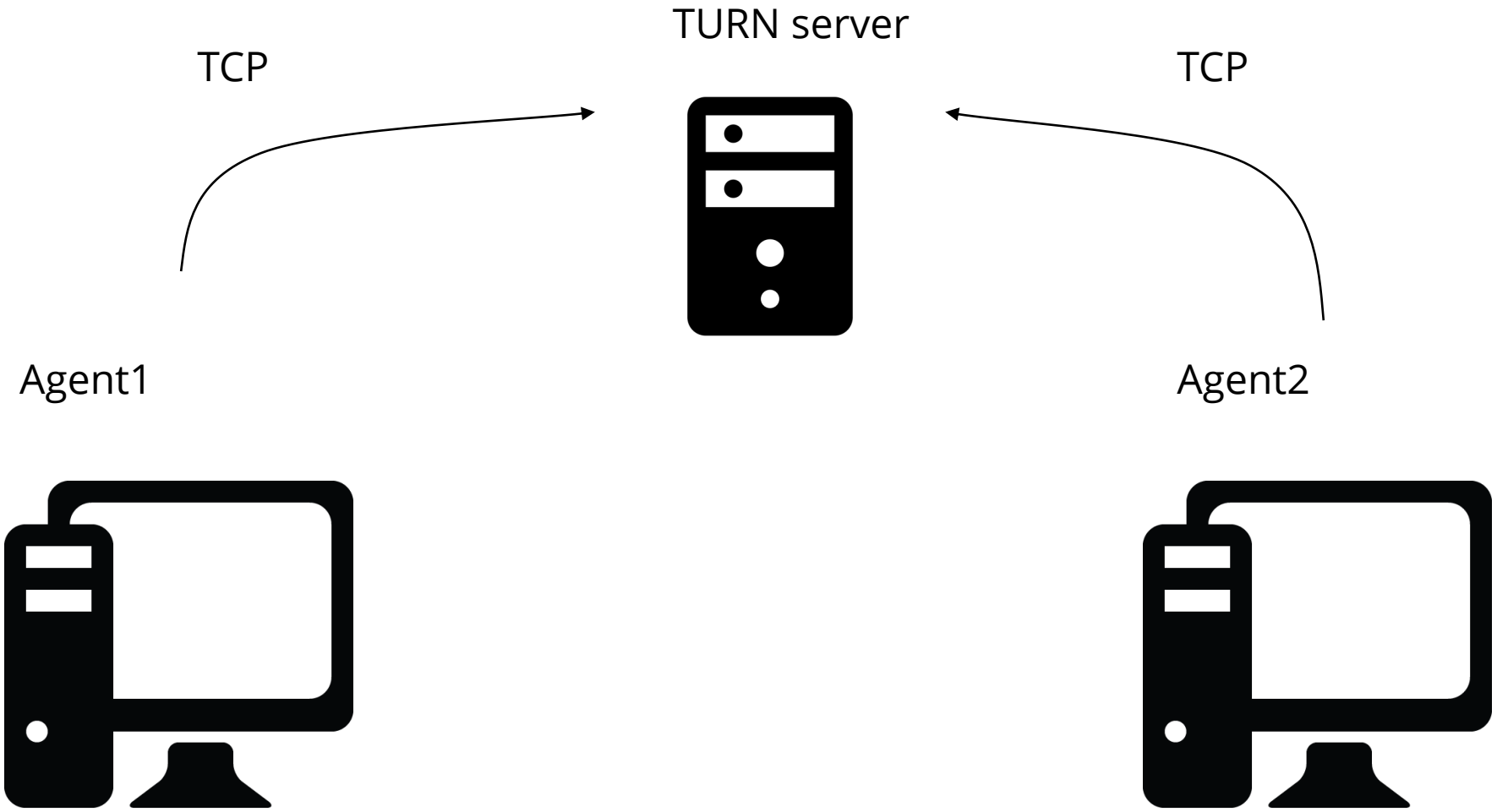
Symmetric NAT



TURN server



TURN Server



TURN server
Relayed candidates

Pairs

Agent

	Local candidates	Type	Remote candidates	Type	Priority
1	192.168.0.1:1	Host	192.168.0.2:3	Host	5437
2	192.168.0.1:1	Host	72.53.87.121:5	Relayed	220