



Security and privacy in network

Damien Saucez
Inria Sophia Antipolis

March 2014

Contact information

- Damien Saucez
 - Email: damien.saucez@inria.fr
 - Mobile: +32 497 19.34.83
 - Phone: +33 4 89.73.24.18

Table of Content

1. Reminders
2. Threats by the example
3. The basics of security
4. Securing communications
5. Overlay networking
6. Privacy

References

- O. Bonaventure. Computer Networking: Principles, Protocols and Practice. <http://inl.info.ucl.ac.be/CNP3>.
 - slides inspired from this book
- J. Kurose and K. Ross. Computer Networking: A Top-Down Approach, Addison-Wesley, 6th Edition.
- L. Peterson and B. Davie. Computer Networks: A Systems Approach. Morgan Kaufmann Publishers, 4th Edition.
- A. Tanenbaum, D. Wetherall, Computer Networks, Prentice Hall, 4th Edition
- A. Legout, Peer-to-Peer Applications From BitTorrent to Privacy, Inria
 - slides inspired from this course

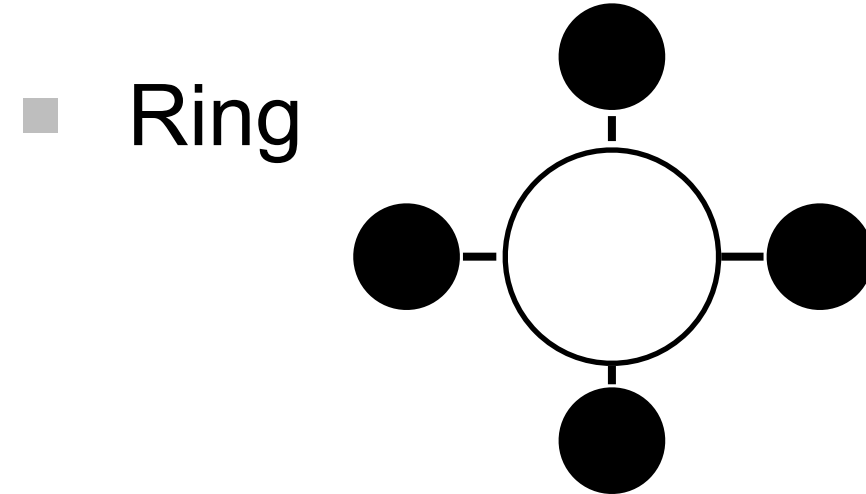
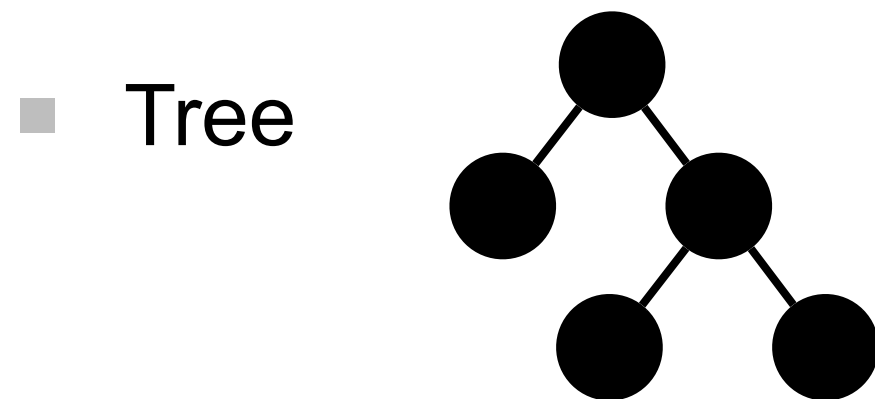
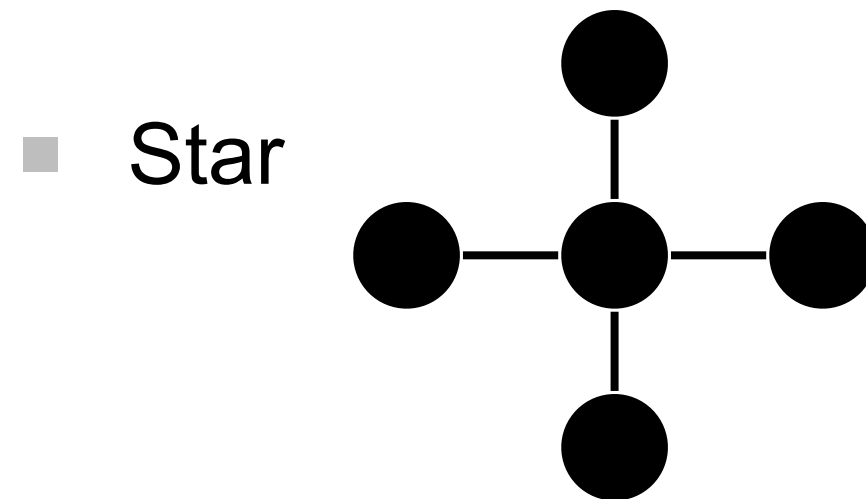
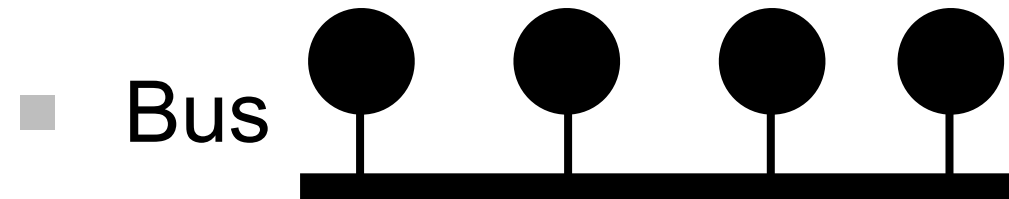
Reminders

Generalities

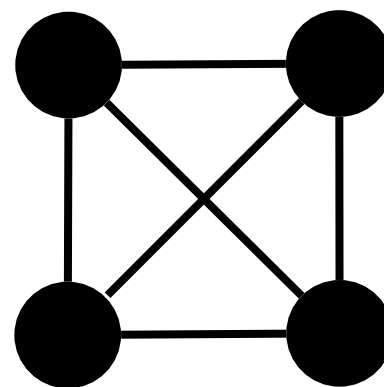
Network

- Network:
 - set of nodes (e.g., hosts, routers) exchanging information and interconnected with links
- Communication rules in a network are specified by a set of protocols (e.g., IEEE 802.3, IP, OSPF, BGP)
- Example of networks:
 - Telephone System
 - Mobile network
 - Television, radio
 - Internet, LAN

Network topologies

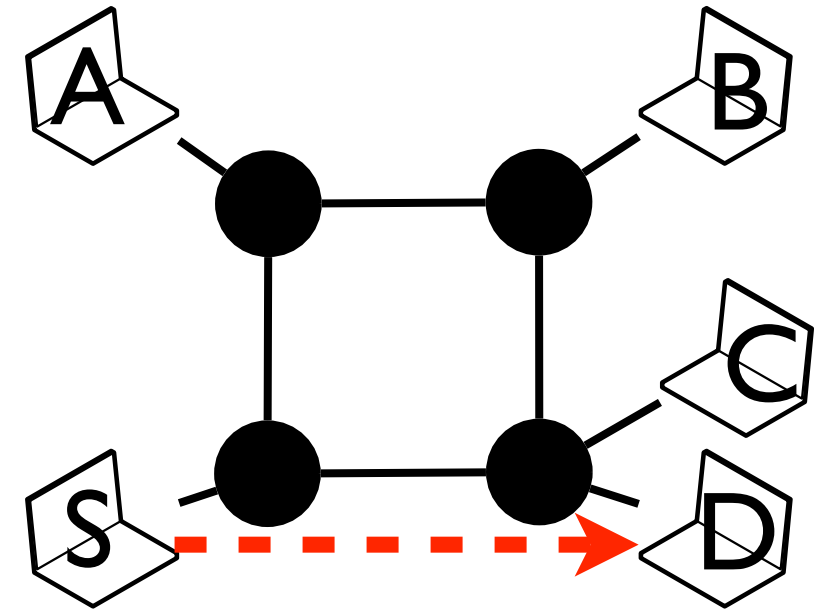


■ Full-Mesh



Transmission modes

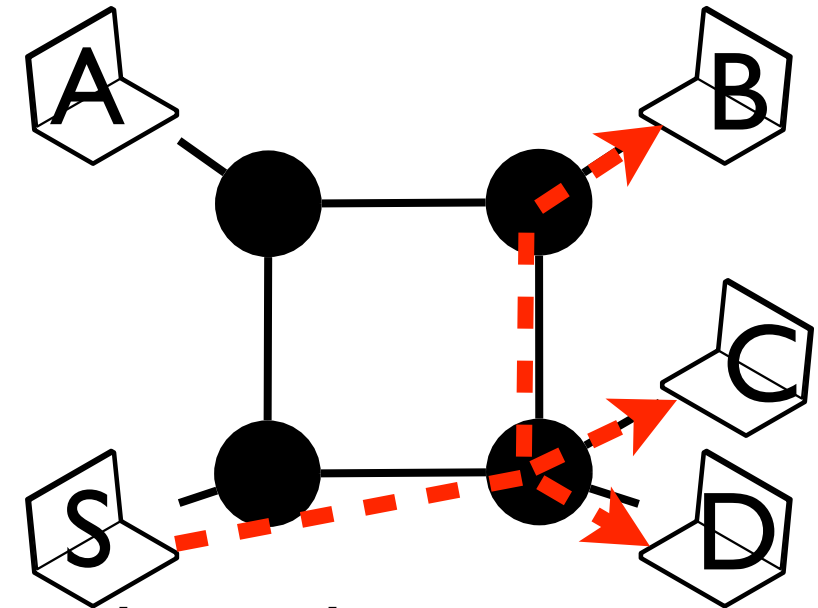
- Unicast (Point-to-Point)
 - one sender
 - one receiver
 - example: telephone
 - the variant where the receiver is taken in a set of possible receivers is called anycast
 - anycast helps scalability



Transmission modes

(cont.)

- Multicast (Point-to-Multipoint)
 - one sender
 - a group of receivers
 - every member of the group receives the same information
 - example: videoconference
 - when the information is sent to every node, the term broadcast is used (e.g., Terrestrial television)



Digital networking communications modes

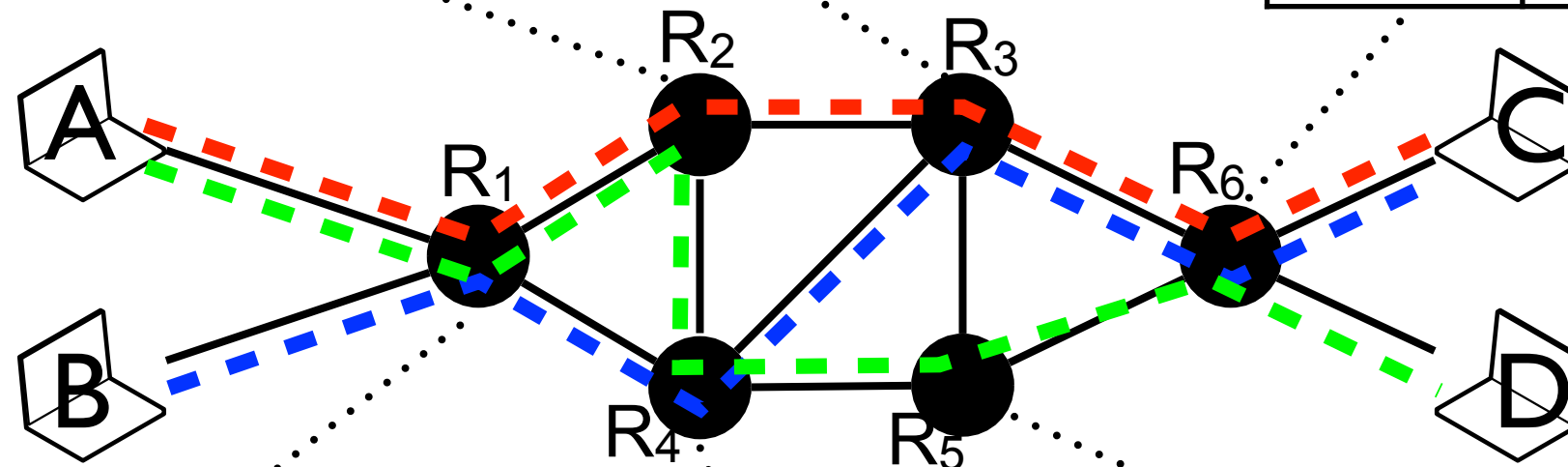
- Circuit switching
 - before transmitting information, a dedicated circuit is established from the source to the destination nodes
 - the information is transmitted through its dedicated circuit that guarantees the bandwidth during the whole communication
 - each intermediate node knows how to forward information received on circuits crossing itself
 - example: 19th century telephone system

Circuit switching example

Circuit	Send to
Red NW	E
Green NW	S

Circuit	Send to
Red W	SE
Blue SW	SE

Circuit	Send to
Red NW	NE
Green SW	SE
Blue NW	NE



Circuit	Send to
Red NW	NE
Green NW	NE
Blue SW	SE

Circuit	Send to
Green N	E
Blue NW	NE

Circuit	Send to
Green W	NE

Digital networking communications modes (cont.)

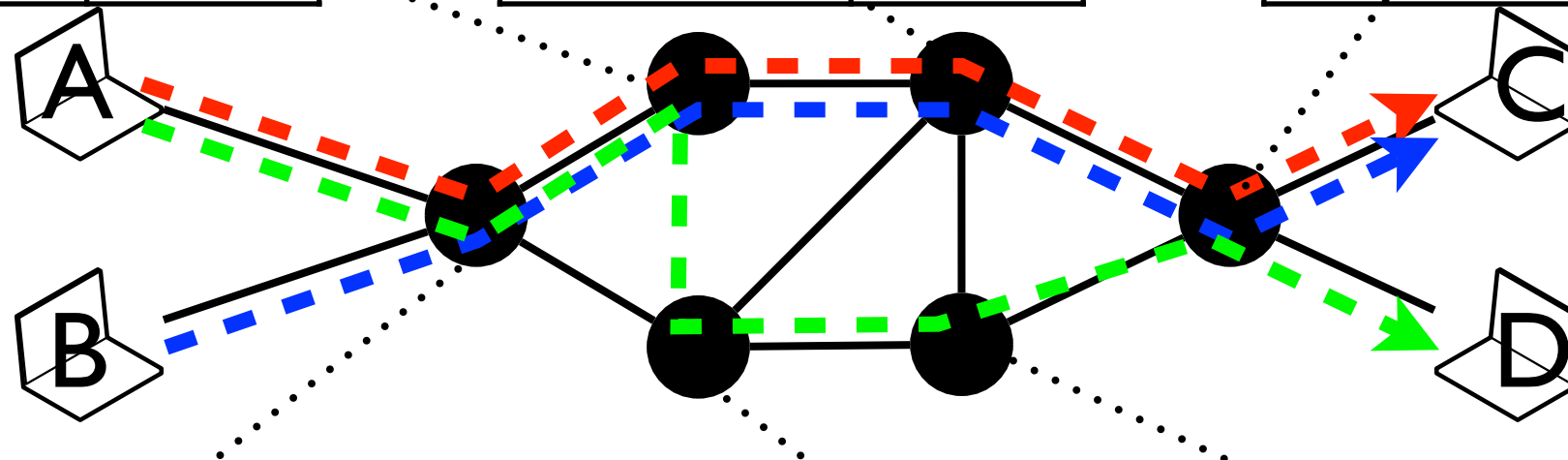
- Packet switching
 - data is divided in packets of information containing
 - a piece of data
 - the address of the source node
 - the address of the destination node
 - packets are transmitted on the network independently of each others
 - each intermediate node knows how to forward information to each destination
 - example: IP, Internet

Packet switching example

Destination	Send to
A	SW
B	SW
C	E
D	S

Destination	Send to
A	W
B	W
C	SE
D	SE

Destination	Send to
A	NW
B	SW
C	NE
D	SE



Destination	Send to
A	NW
B	SW
C	NE
D	NE

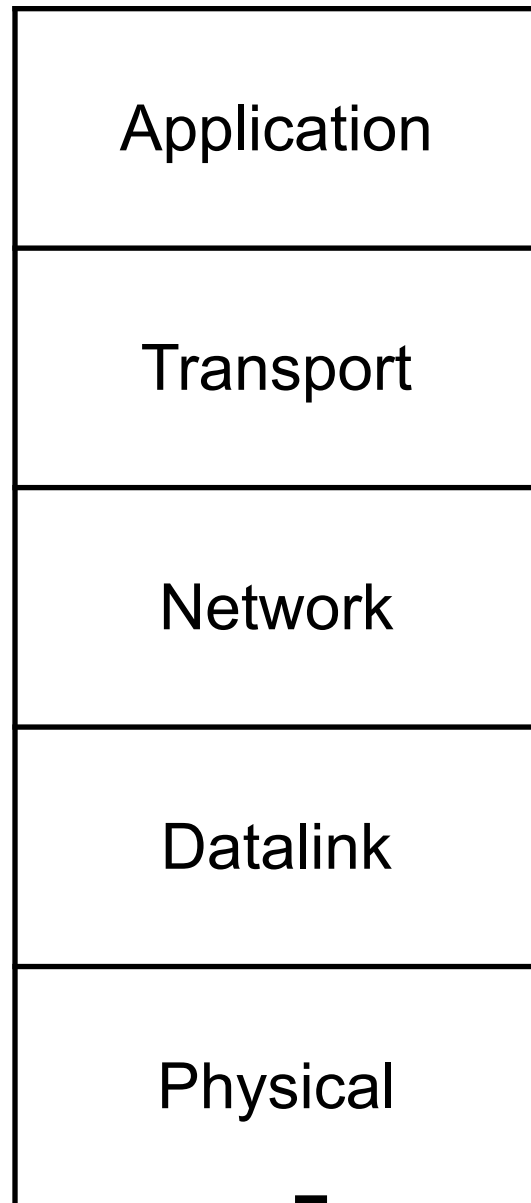
Destination	Send to
A	NW
B	NW
C	E
D	E

Destination	Send to
A	W
B	W
C	NE
D	NE

Layered model

- Network systems are complex
 - dividing the functionality helps reasoning on them
- Divide network functionalities into layers
 - Layer i provides services to layer $i+1$
 - Layer i relies on services provided by layer $i-1$

Layers



Exchange of useful information (**Service Data Unit**) between applications relying on the transport layer hiding the network complexity (e.g., HTTP)

Provide a service to (reliably) exchange data between hosts with **segments** (e.g., TCP, UDP)

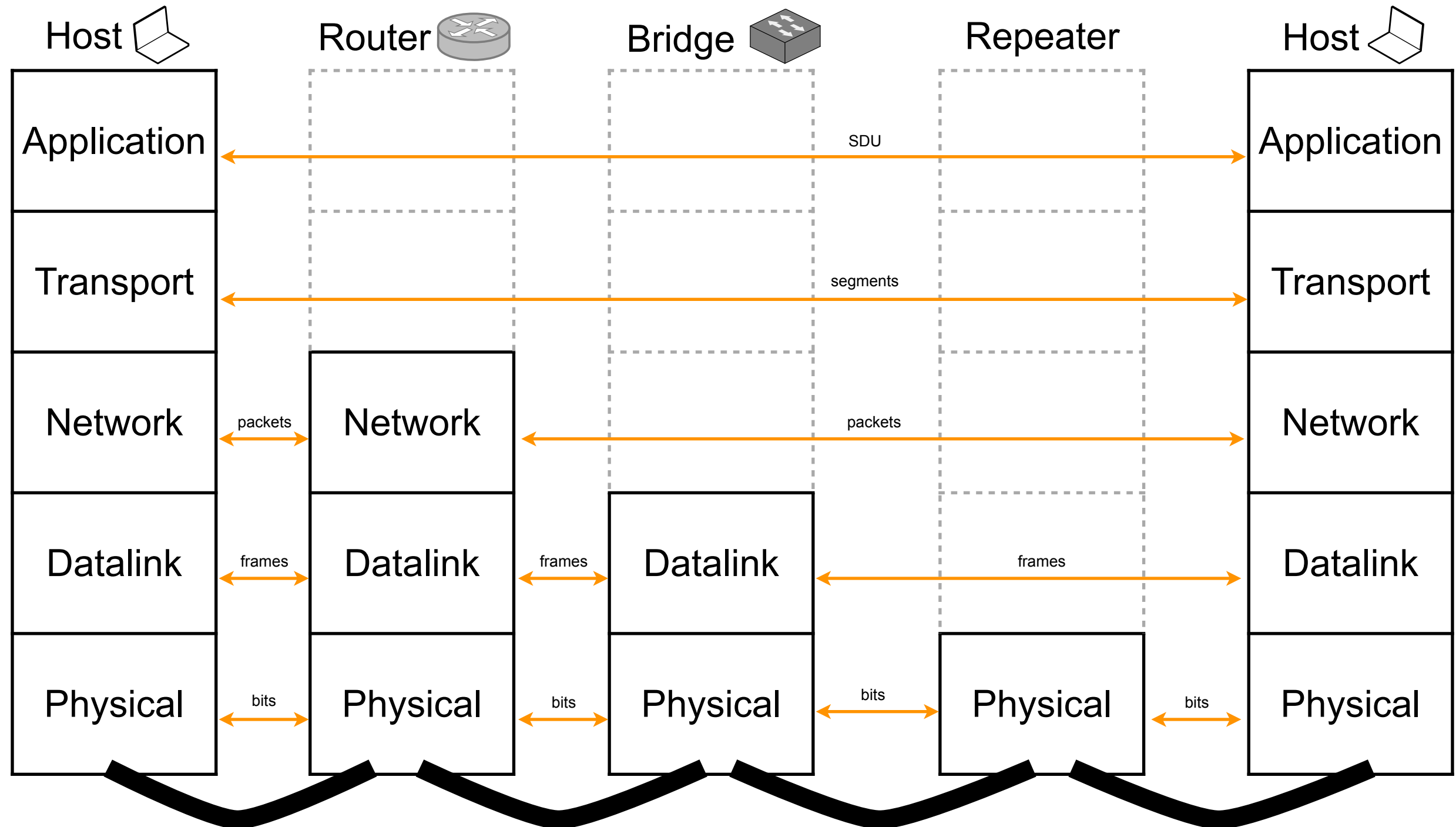
Provide a service to exchange **packets** of information between hosts that can be arbitrarily distant (e.g., IP)

Provide a service to exchange structured group of bits called **frames** (e.g., Ethernet)

Transmit **bits** between two physically connected devices (e.g., Manchester)

Physical transmission medium (e.g., UTP)

Layer of networking devices



Middleboxes

- The original TCP/IP architecture is only composed of hosts and routers
- Modern networks contain devices that
 - process (e.g., proxies)
 - analyze (e.g., firewall)
 - modify (e.g., NAT)
- Middleboxes can work at any layer or even be cross layer

Middleboxes are everywhere

- In enterprise networks [SHC+12]

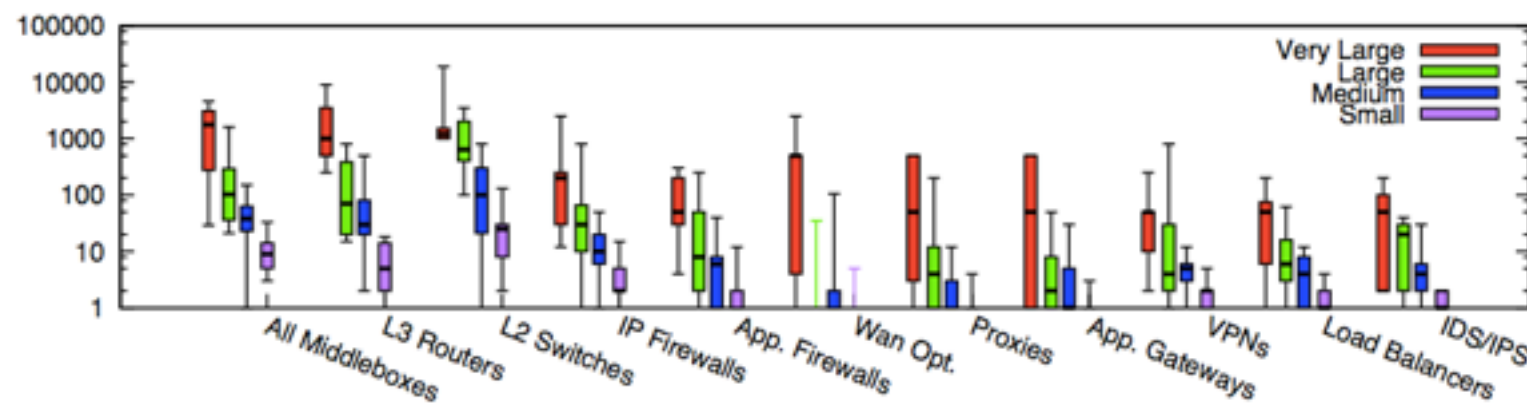


Figure 1: Box plot of middlebox deployments for small (fewer than 1k hosts), medium (1k-10k hosts), large (10k-100k hosts), and very large (more than 100k hosts) enterprise networks. Y-axis is in log scale.

- In ISP networks [HRN+11]
 - very likely that your packet will be touched by a middlebox before reaching its destination
- Middleboxes limit deployment of new protocols in the Internet
- Middleboxes can be used against user interests

Naming and addressing

Name and addresses in the Internet

- DNS Names identify hosts
- IP addresses uniquely identify host interfaces
 - `nslookup example.com`
Server: 138.96.0.10
Address: 138.96.0.10#53

Non-authoritative answer:
Name: example.com
Address: 192.0.43.10
- Ethernet address identifies network adapters in a collision domain
 - `arp -na`
? (138.96.192.3) at 0:50:56:88:0:0 on en1 ifscope [ethernet]
? (138.96.192.250) at 0:1e:4a:e0:9e:0 on en1 ifscope [ethernet]
? (138.96.193.164) at 0:23:df:aa:cc:4c on en1 ifscope [ethernet]
...
- Names and addresses are hierarchically organized

Hierarchical naming/ addressing

- Objectives: ensure uniqueness of names/addresses and provide naming/addressing scalability
- Flat: probe all the other naming/addressing authorities before choosing a name/address
 - doesn't scale
 - not robust to network partition
- Hierarchy: carve up set of possible names/address (i.e., the name/address space) into mutually exclusive portions

Addressing in Ethernet

- Objective: determine the origin and destination of a frame within a collision domain
- Every Ethernet network adapter is assigned a unique datalink layer address encoded on 48 bits
- Every frame is transmitted to all network adapters of the collision domain
 - but only the network adapter with the address corresponding to the destination address of the frame accepts it

Addressing in IP

- Objective: determine the origin and destination of a packet in the Internet
- Every host interface has its own IP address
 - routers have multiple interfaces, each with its own IP address
 - the IP address determines the topological position of the interface
- Current version of IP is version 4 (IPv4)
 - addresses are encoded on 32 bits, fixed length
- 4 billions addresses were a lot... in 1981, but today it becomes too short for 1 billion hosts [ISC]
- IP version 6 (IPv6) starts to be deployed
 - addresses are encoded on 128 bits, fixed length*

IP address structure

- Addresses are separated in two parts
 - network number: identifies the network the address belongs to
 - local address: identifies the interface of the host in the network
 - all bits = 0: network address
 - all bits = 1: broadcast address
- Addresses are aggregated according to the network number
 - routing and packet forwarding are based on the network number only, the local address is ignored

Classless InterDomain Routing (CIDR)

- No predetermined separation position between network number and local address with CIDR
 - number of bits allocated for the network number may vary from 0 to 32 bits
 - the address contains no information about the separation position
 - Routers determine the network number by using longest-prefix matching
- Notation $a.b.c.d/n$
 - $a.b.c.d$ is the address
 - n is the number of bits assigned to the network number

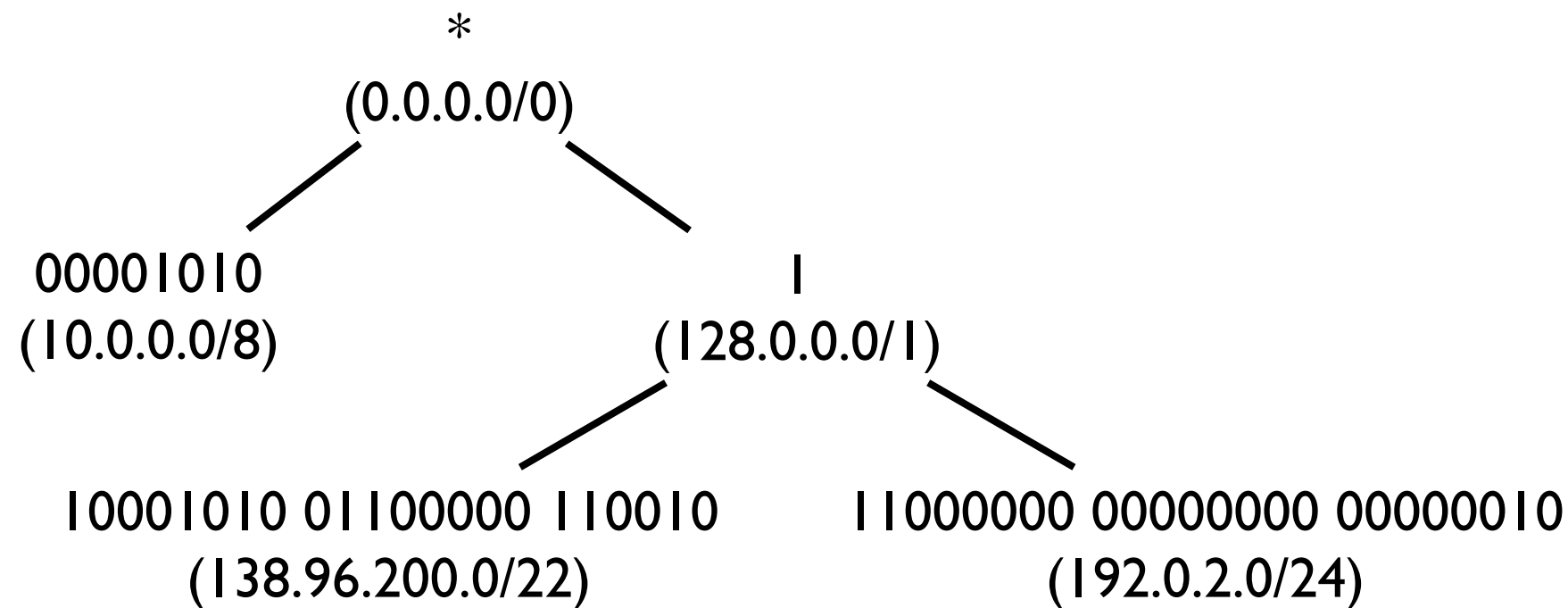
CIDR (cont.)

- An address matches a route if both share the same prefix
 - 0.0.0.0/0 is the default route matched by every addresses
- With CIDR, an address can match several routes
 - 192.0.2.1 matches 128.0.0.0/1, but also 192.0.2.0/24 or 0.0.0.0/0
- Longest prefix matching is used to determine the route that has the longest prefix in common with the address
- Typically implemented with a trie

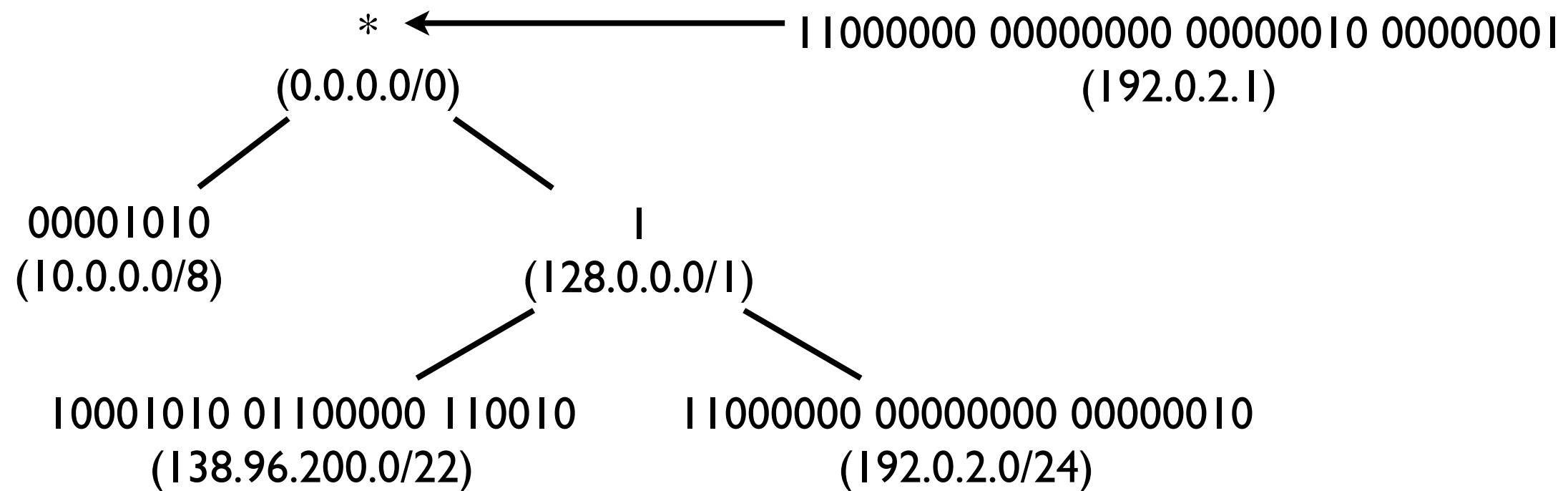
Longest prefix matching with a trie

- Routes are inserted in a trie, route prefixes being node keys
- The key of a node is a prefix of the key of all of its children, recursively;
 - siblings cannot be prefixes
- The binary tree is descended, starting from the root, following the children with the key that is a prefix of the address to match
- The descend ends when no children has a key prefixing the address to match
 - the route corresponding to the node where the descent stopped is the best matching route

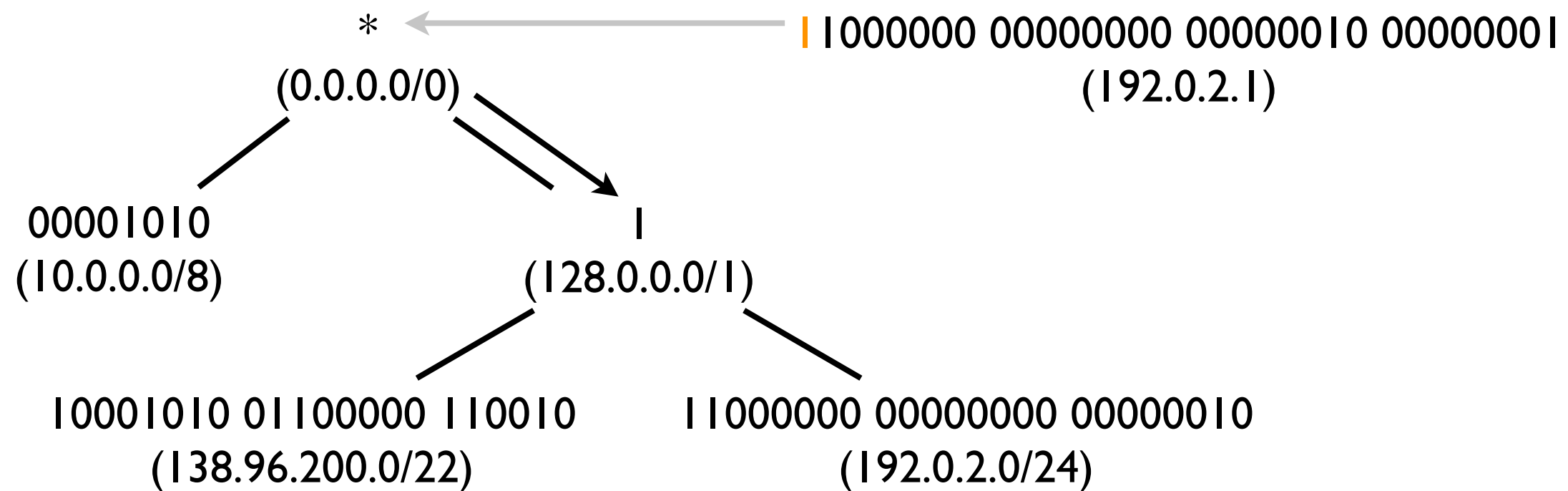
Longest prefix matching with a trie (examples)



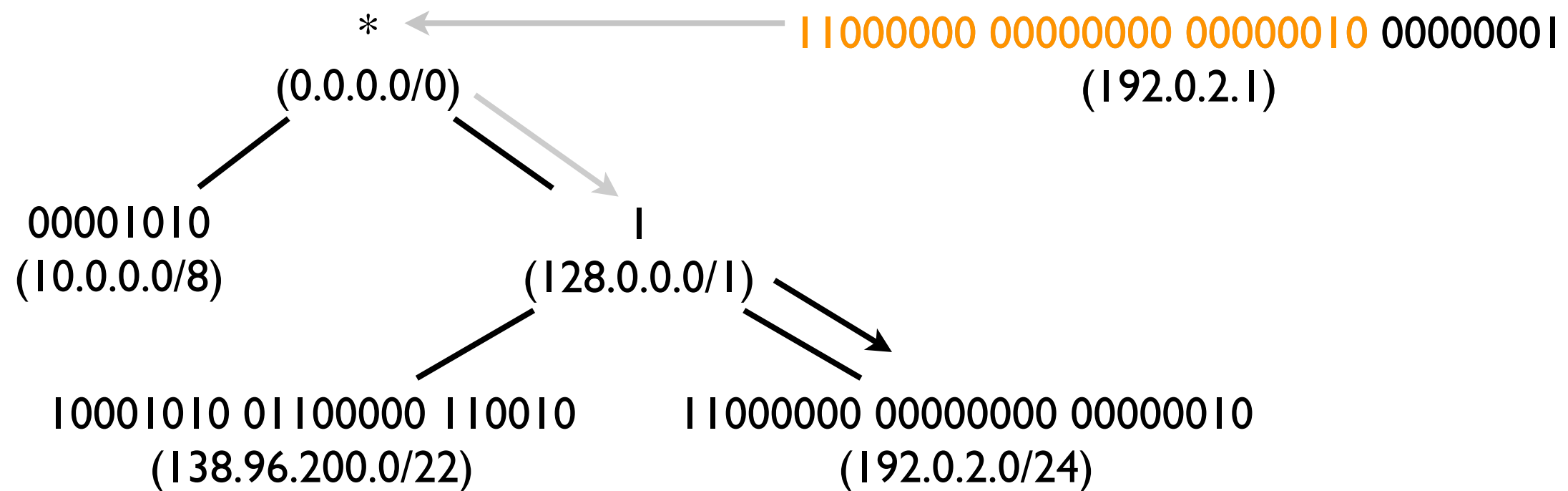
Longest prefix matching with a trie (examples)



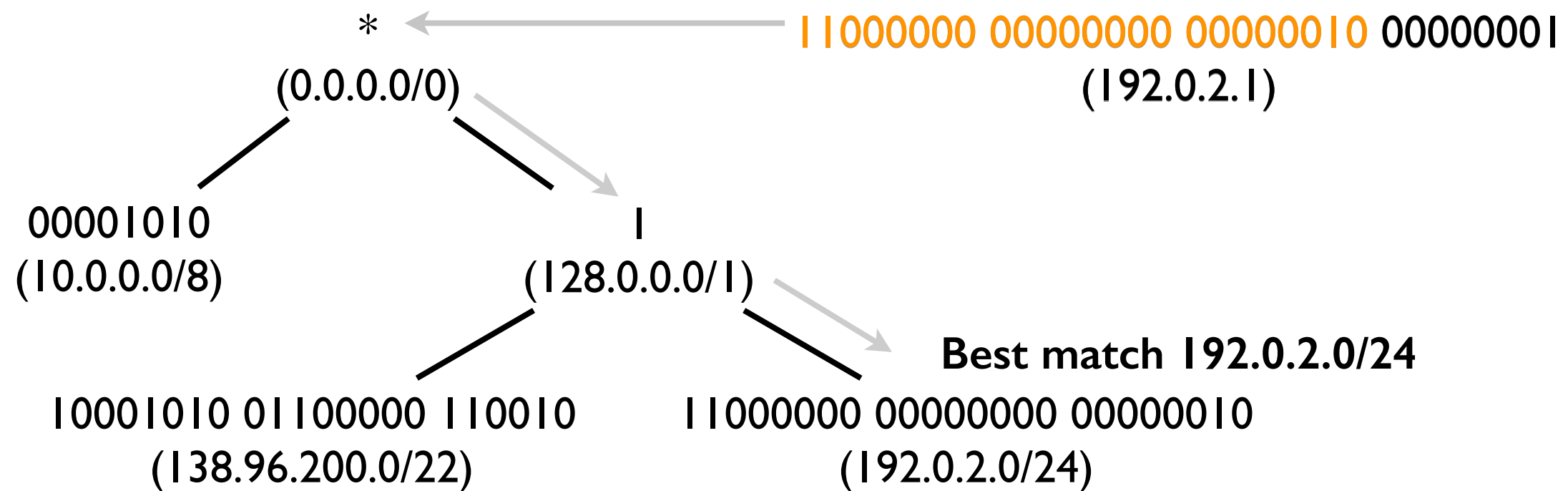
Longest prefix matching with a trie (examples)



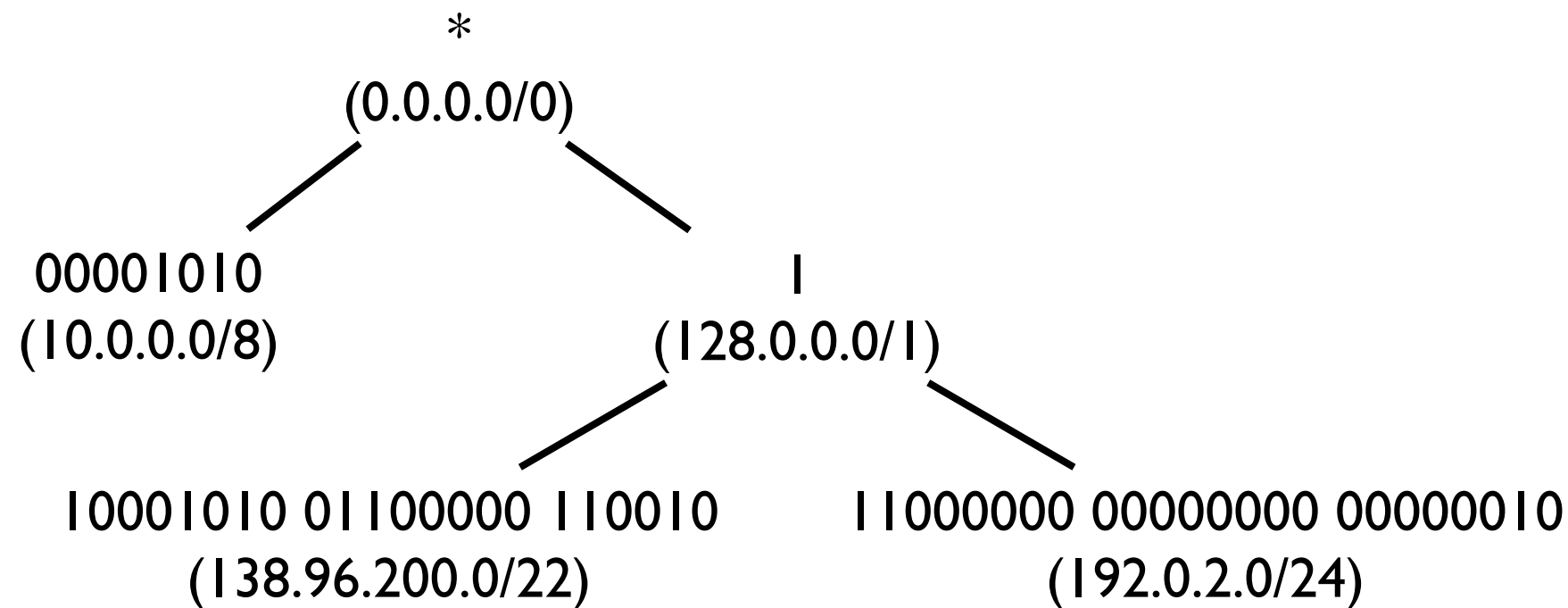
Longest prefix matching with a trie (examples)



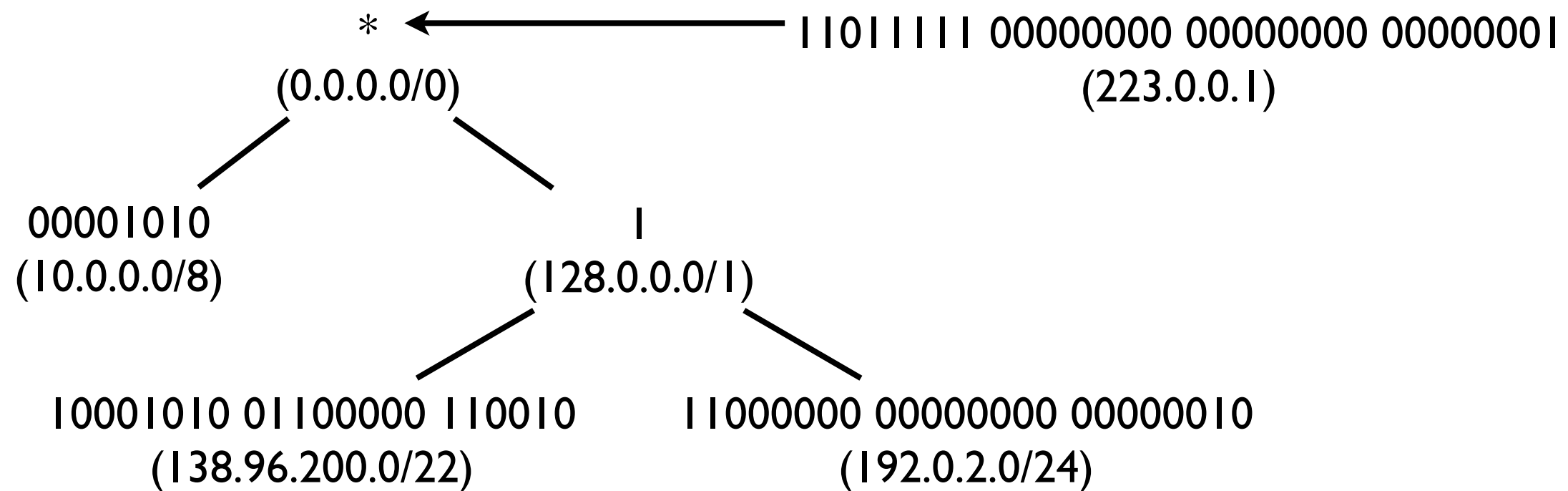
Longest prefix matching with a trie (examples)



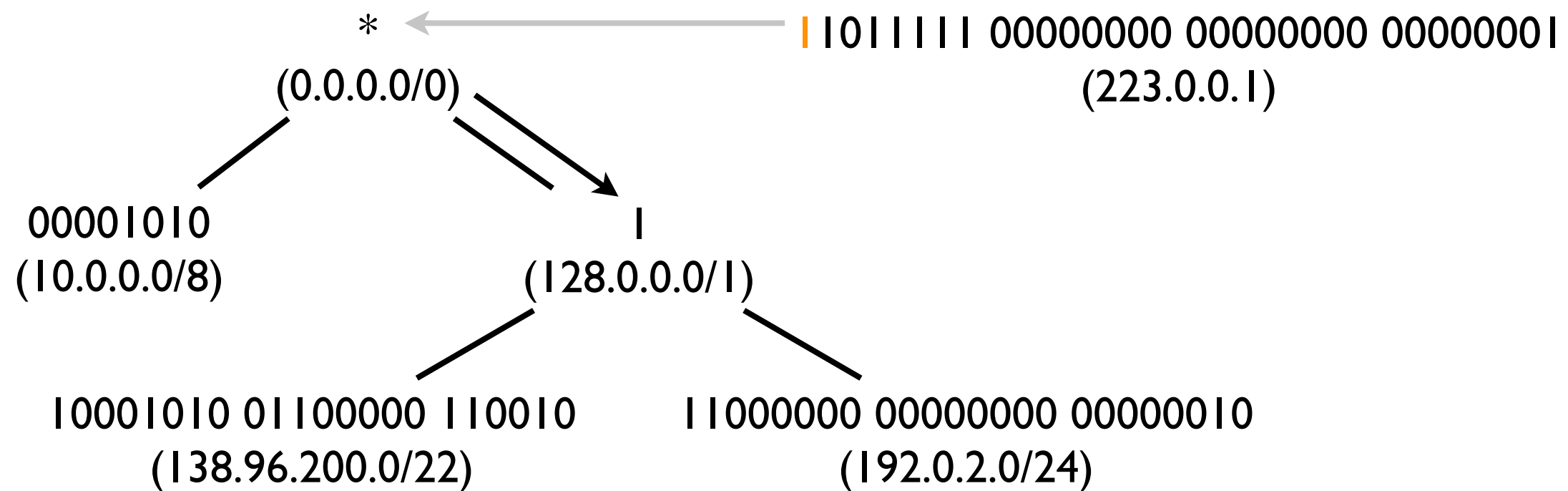
Longest prefix matching with a trie (examples)



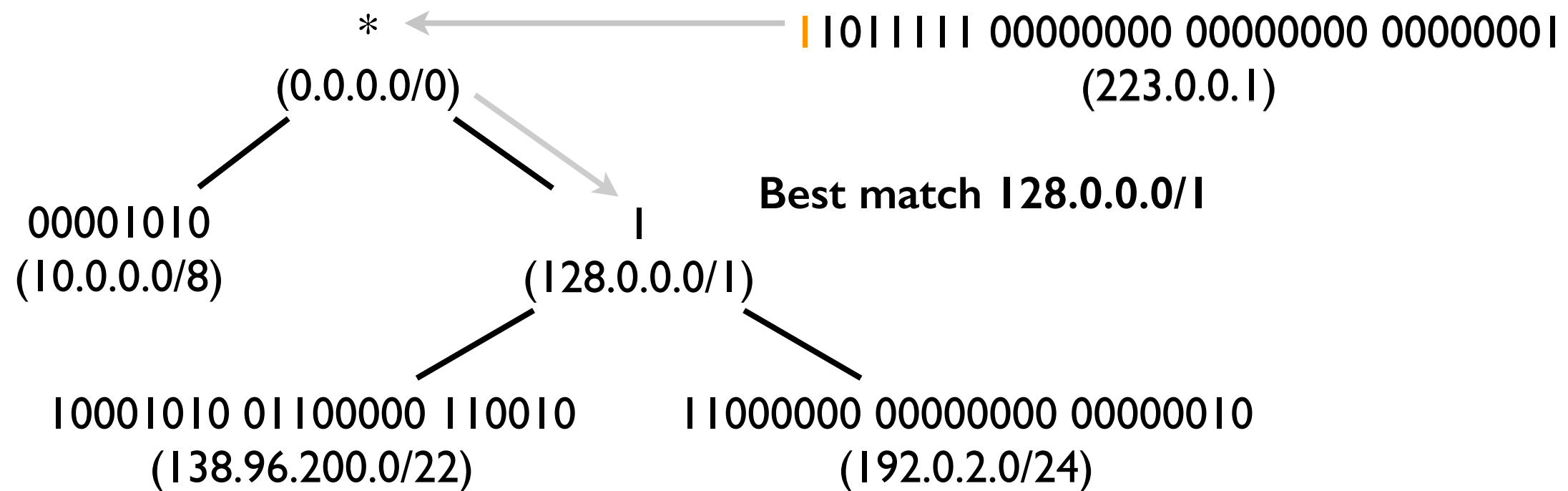
Longest prefix matching with a trie (examples)



Longest prefix matching with a trie (examples)



Longest prefix matching with a trie (examples)



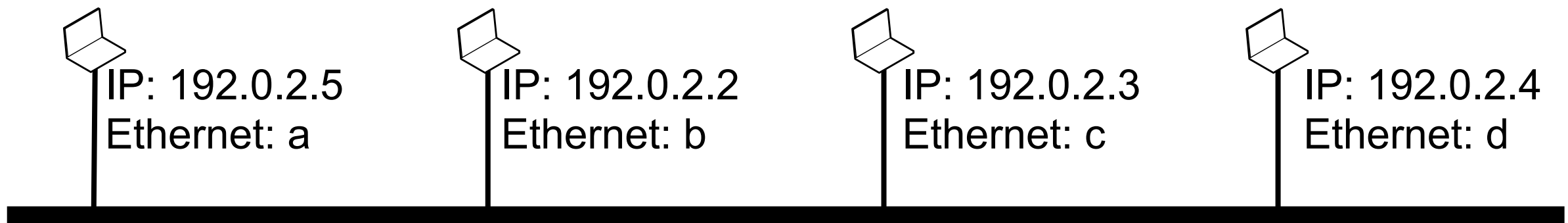
IP to Ethernet Address

- To put an IP packet over an Ethernet frame, its IP addresses must be resolved into Ethernet addresses
- Protocol used:
 - Address Resolution Protocol (ARP) in IPv4
 - Neighbor Discovery Protocol (NDP) in IPv6

ARP

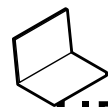
- ARP is used to get datalink layer address of a machine on the local subnet
- Broadcast an ARP request frame on the local subnet for the IP address to resolve
 - destination address: FF:FF:FF:FF:FF:FF (broadcast)
 - source address: Ethernet address of the network adapter that issued the ARP request
- The host (or a proxy) that owns the address replies with an ARP response frame
 - destination address: Ethernet address of the requester's network adapter
 - source address: Ethernet address of the address's owner's (or proxy) network adapter
- Every network device is required to listen for ARP requests and replies on its network adapters
- Optimizations
 - replies are stored in an ARP cache to avoid that every single packet results in ARP request/response
 - cached for a limited duration as host can change their IP address
 - ARP request message contains the IP address of the origin of the frame
 - destination (or any hosts in the local subnet) can learn the IP/Ethernet mapping for free

ARP example

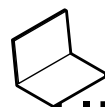


ARP example

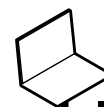
IP source: 192.0.2.2	IP destination: 192.0.2.3	
----------------------	---------------------------	--



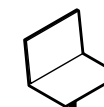
IP: 192.0.2.5
Ethernet: a



IP: 192.0.2.2
Ethernet: b

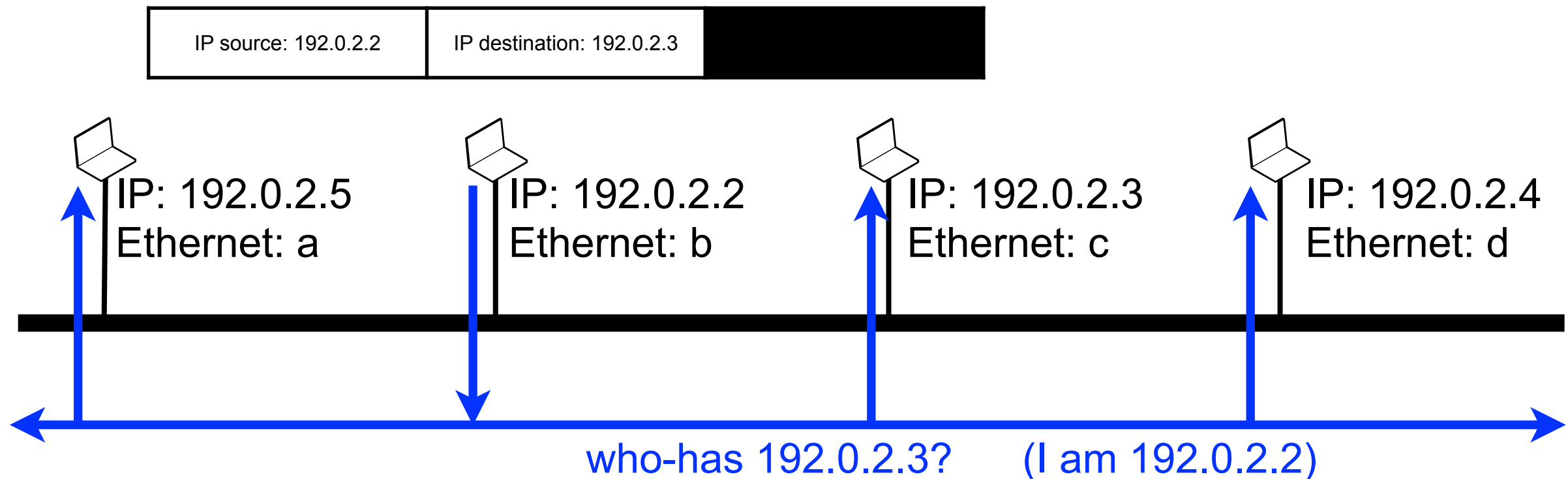


IP: 192.0.2.3
Ethernet: c

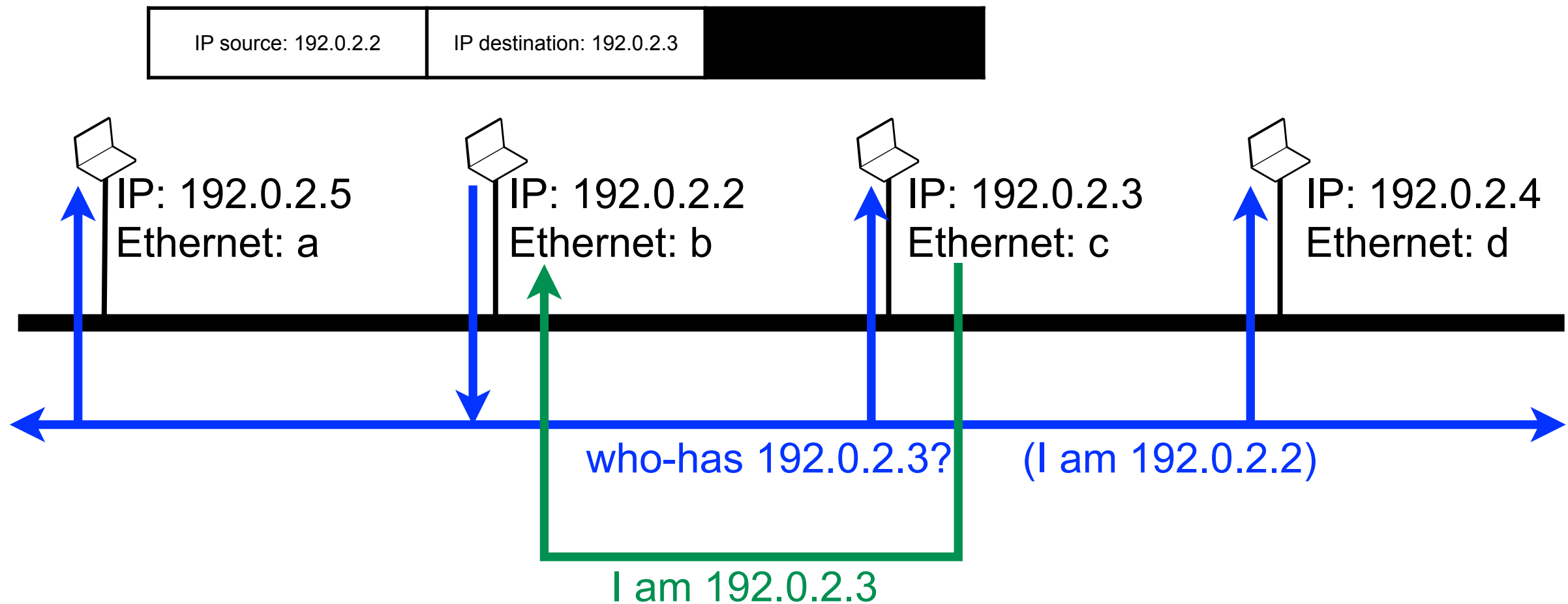


IP: 192.0.2.4
Ethernet: d

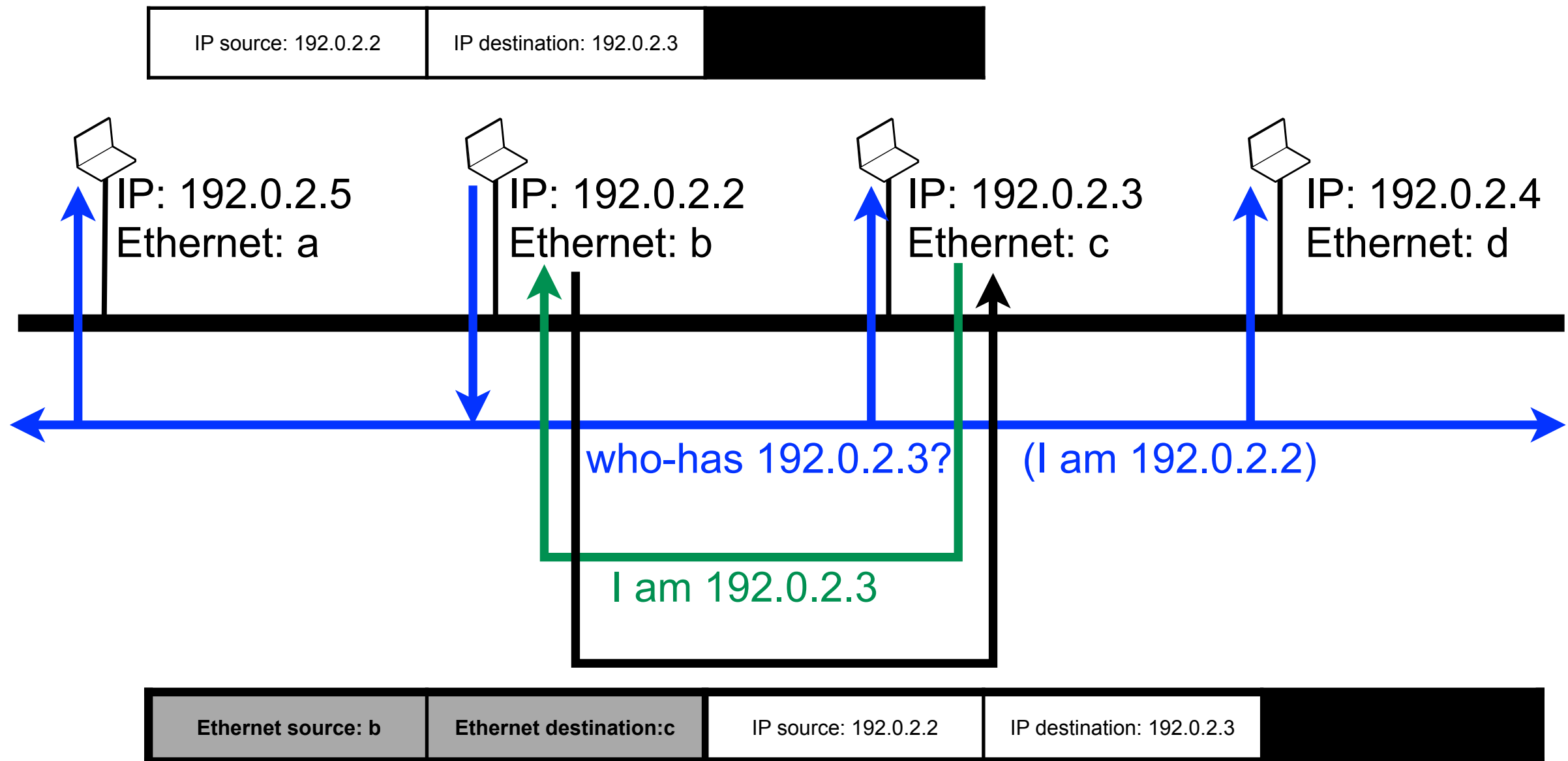
ARP example



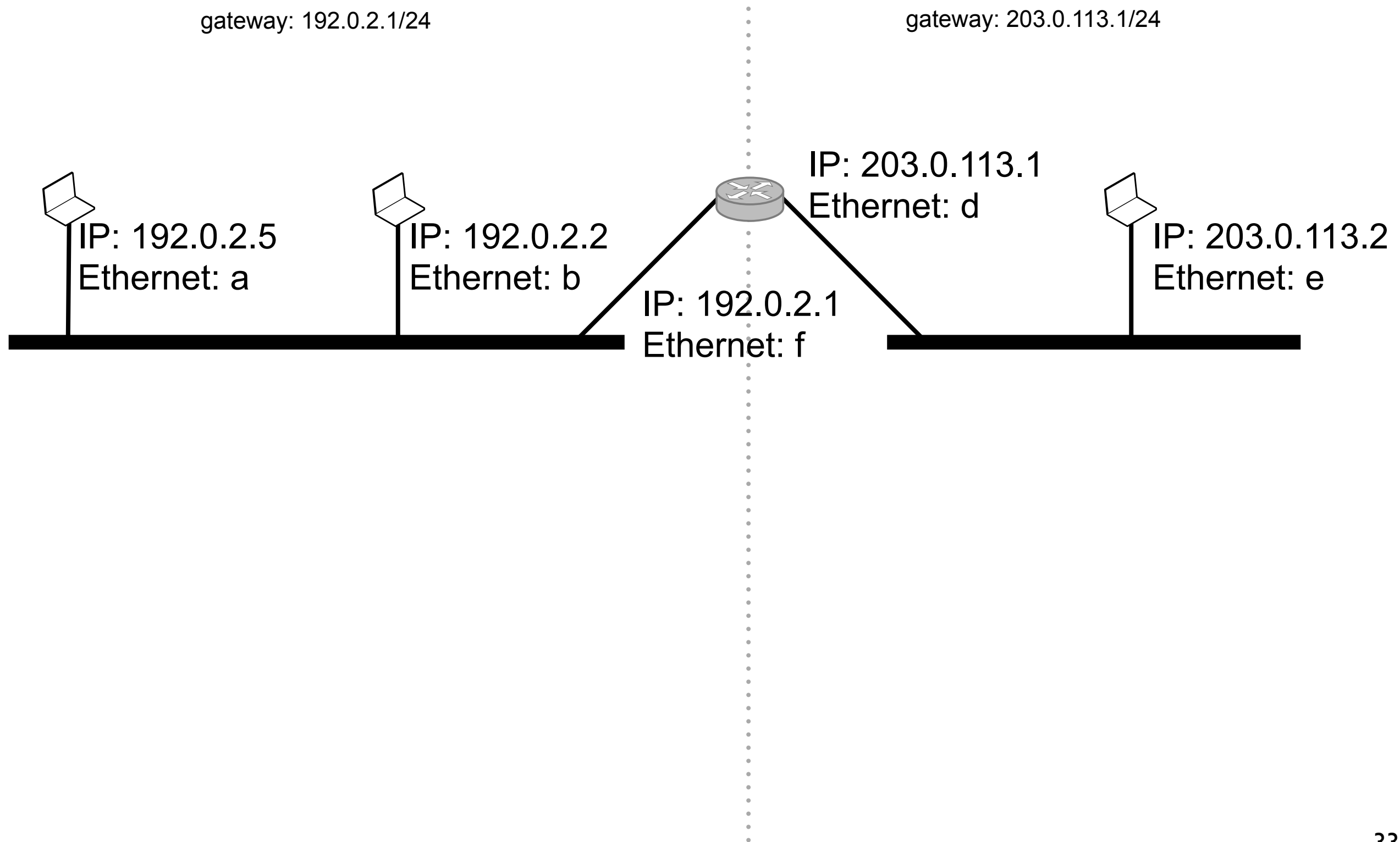
ARP example



ARP example



ARP example (router)



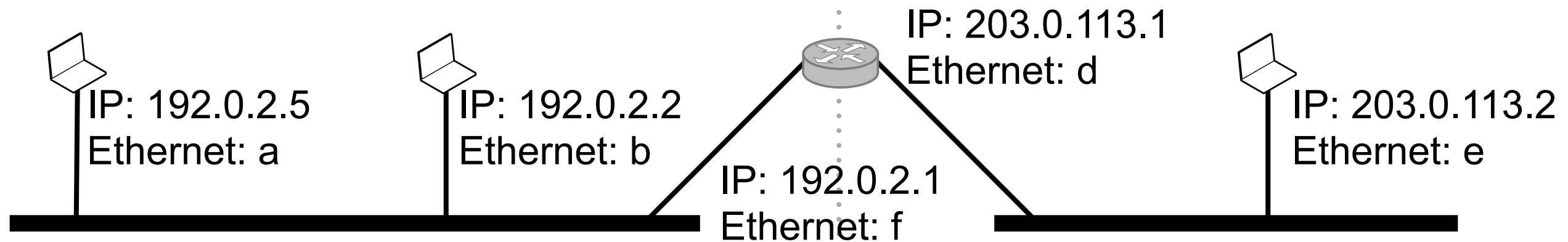
ARP example (router)

gateway: 192.0.2.1/24

gateway: 203.0.113.1/24

IP source: 192.0.2.2

IP destination: 203.0.113.2



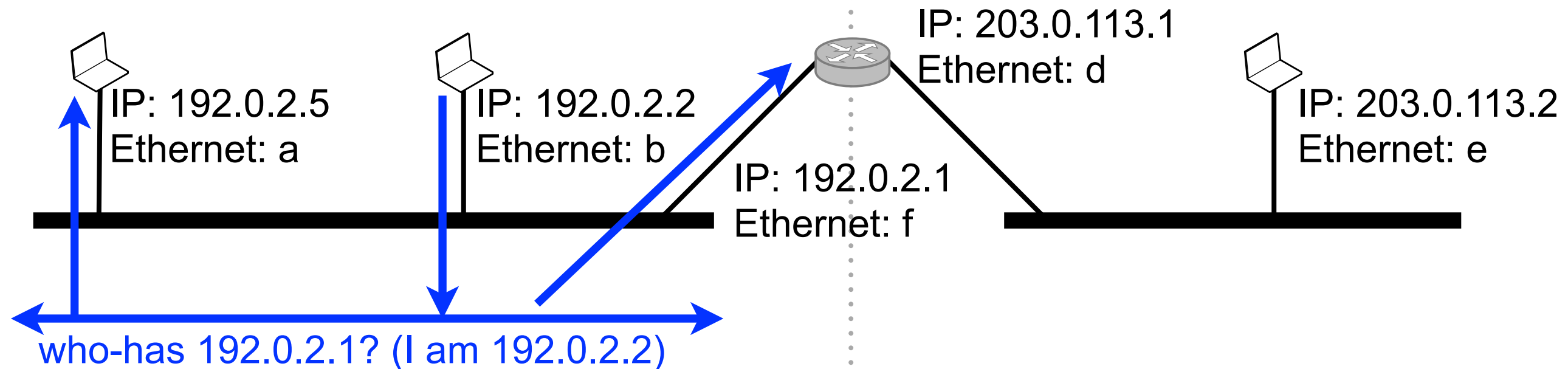
ARP example (router)

gateway: 192.0.2.1/24

gateway: 203.0.113.1/24

IP source: 192.0.2.2

IP destination: 203.0.113.2



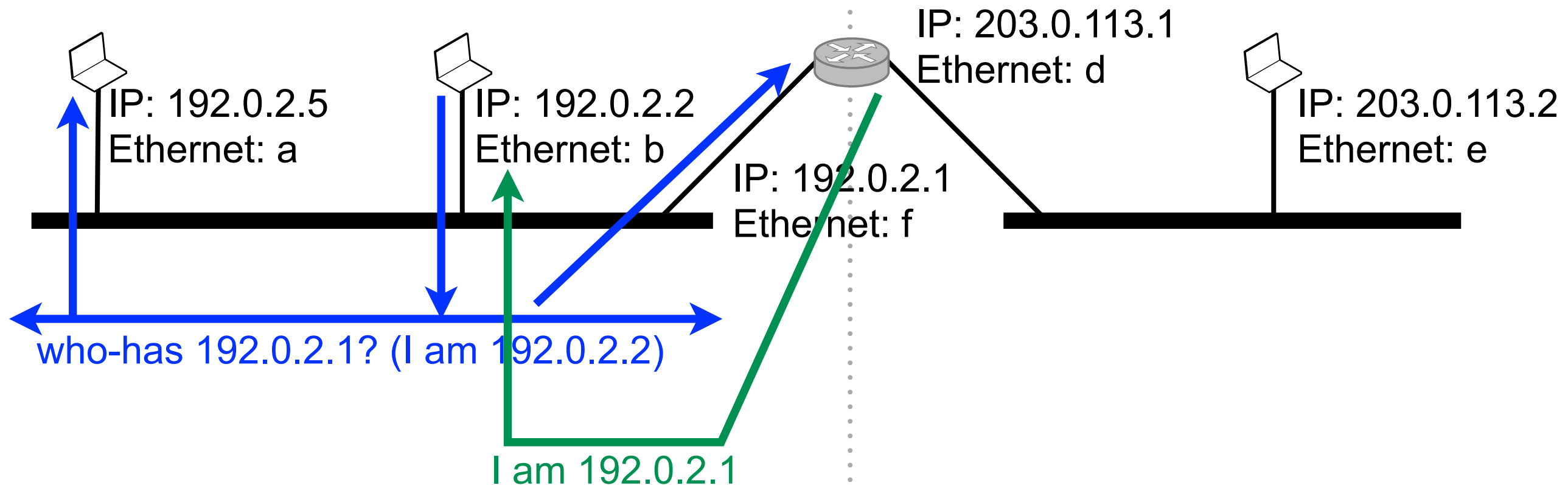
ARP example (router)

gateway: 192.0.2.1/24

gateway: 203.0.113.1/24

IP source: 192.0.2.2

IP destination: 203.0.113.2



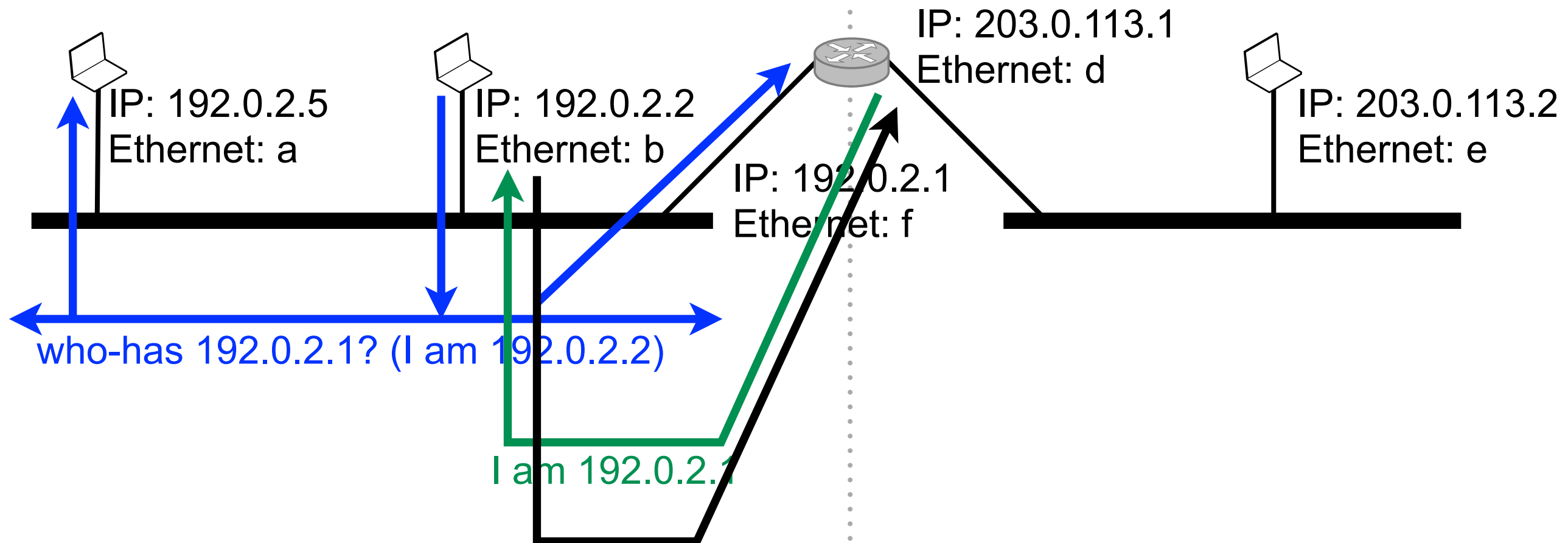
ARP example (router)

gateway: 192.0.2.1/24

gateway: 203.0.113.1/24

IP source: 192.0.2.2

IP destination: 203.0.113.2



Ethernet source: b

Ethernet destination: f

IP source: 192.0.2.2

IP destination: 203.0.113.2

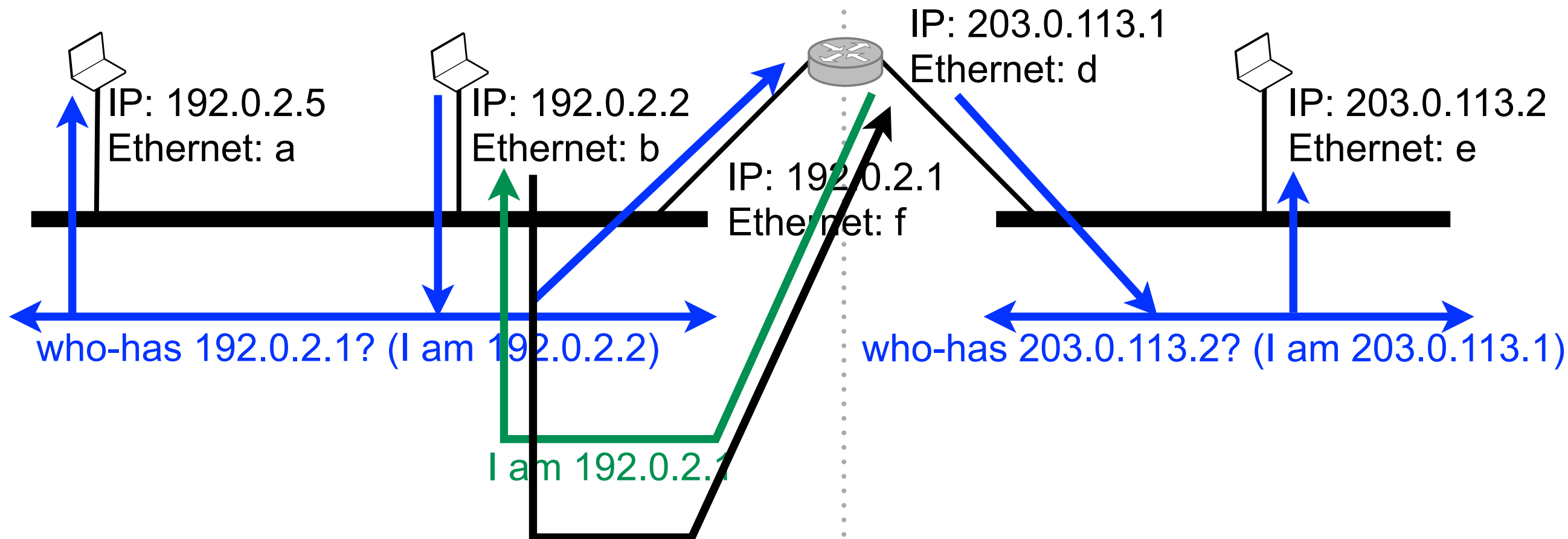
ARP example (router)

gateway: 192.0.2.1/24

gateway: 203.0.113.1/24

IP source: 192.0.2.2

IP destination: 203.0.113.2



Ethernet source: b

Ethernet destination: f

IP source: 192.0.2.2

IP destination: 203.0.113.2

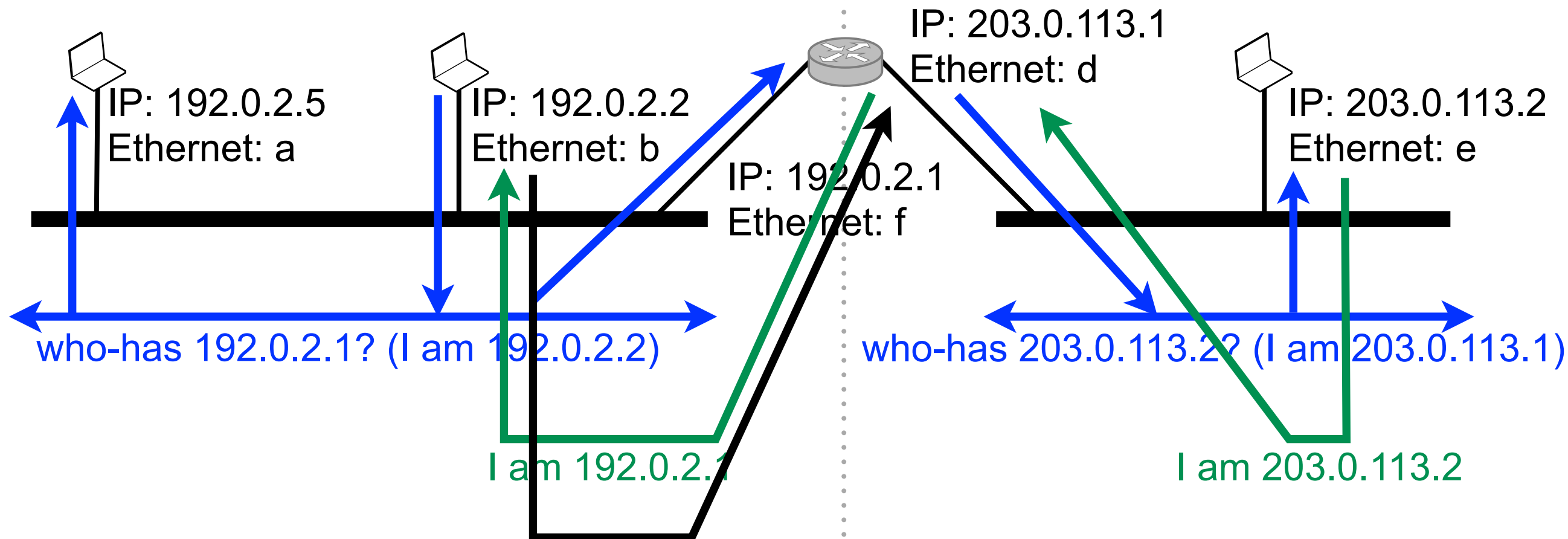
ARP example (router)

gateway: 192.0.2.1/24

gateway: 203.0.113.1/24

IP source: 192.0.2.2

IP destination: 203.0.113.2



Ethernet source: b

Ethernet destination: f

IP source: 192.0.2.2

IP destination: 203.0.113.2

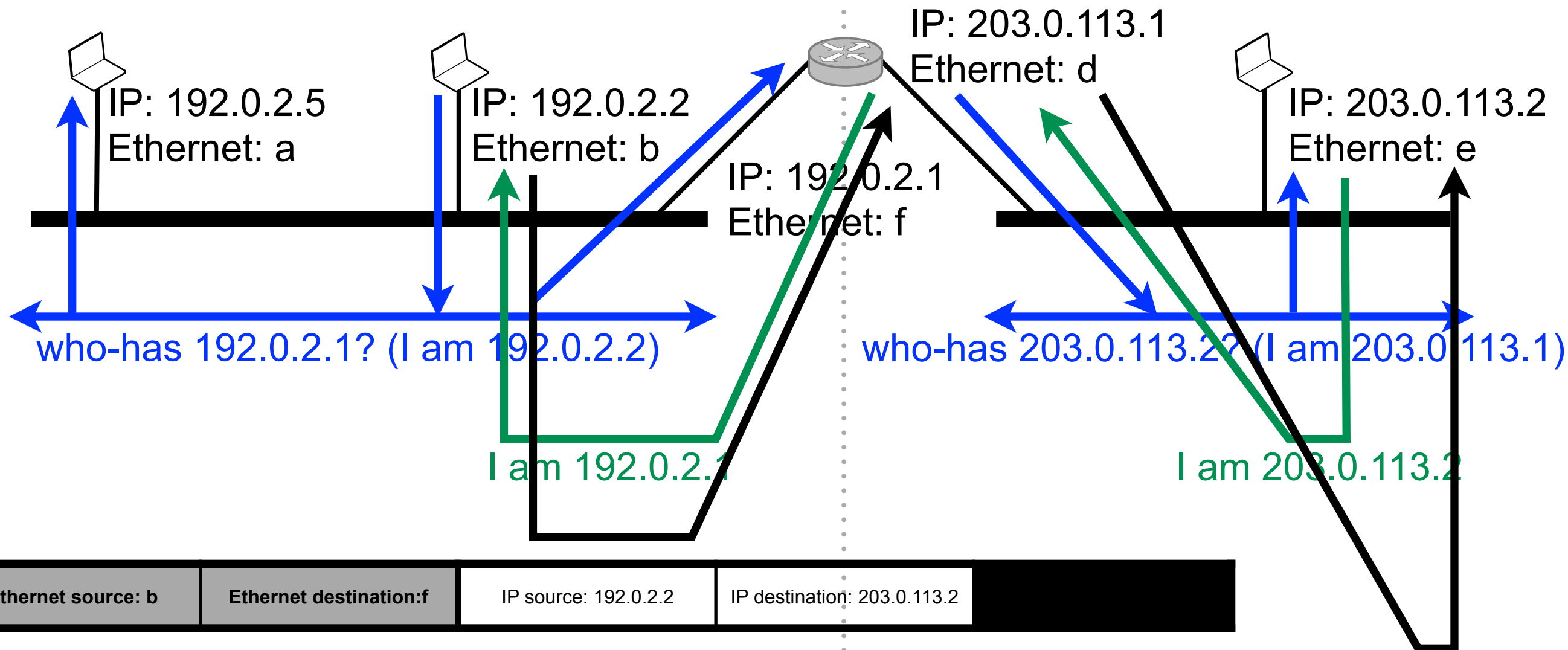
ARP example (router)

gateway: 192.0.2.1/24

gateway: 203.0.113.1/24

IP source: 192.0.2.2

IP destination: 203.0.113.2



Dynamic address configuration

- Allow a set of hosts to share a pool of IP address
- Two approaches
 - stateless auto-configuration
 - no infrastructure necessary
 - Dynamic Host Configuration Protocol (DHCP)
 - hosts query a DHCP server to obtain their configuration
- Advantages
 - less address wastage: a host can use the address of another hosts when it is not connected
 - improves flexibility and reduces the risk of configuration error as no manual operation is necessary

Stateless auto-configuration

- When a host connects to the network:
 1. The host chooses an address randomly in 169.254/16 (not globally routable)
 2. Sends an ARP request for the chosen address
 3. If an ARP reply is received (another host already uses the address)
 - restart from point 1
 4. Otherwise, the address is not used by another host and the host can use it safely
- Auto-configuration is used only for communications within the same network
 - In IPv6, hosts can auto-configure their globally routable addresses and discover network services (e.g., routers, DNS...)

Dynamic Host Configuration Protocol (DHCP)

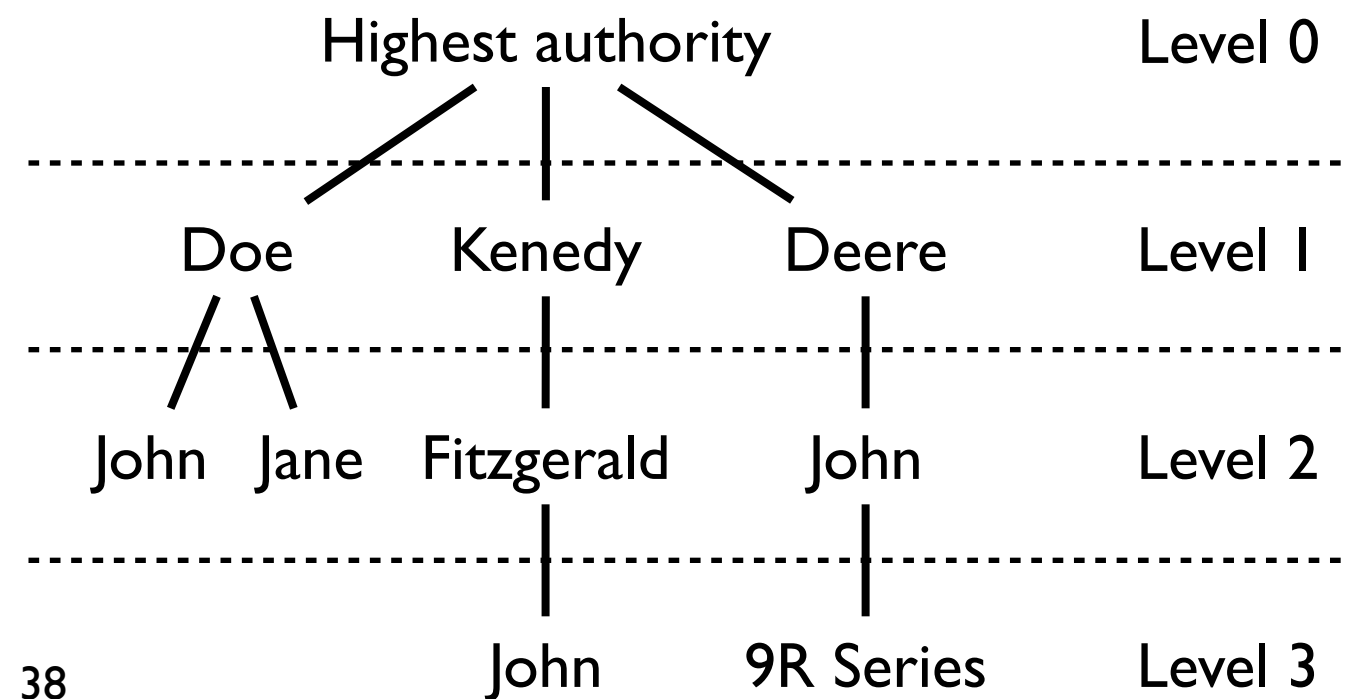
- When a host connects to the network, it broadcasts a DHCP discovery datagram
- Any DHCP server that receives such a message replies with a DHCP offer datagram that contains an offer of IP address
- The host picks one offer and broadcasts a DHCP request message to announce the offers it selected
- The selected DHCP server assigns the address to the host and sends it back a DHCP acknowledgment that confirms the lease of the address and give additional parameters such as the lease time, the IP address of the default gateway, or the IP address of the DNS servers
 - when the lease time is elapsed, the address is released and made available for other hosts
- The other DHCP servers withdraw their offers

Naming

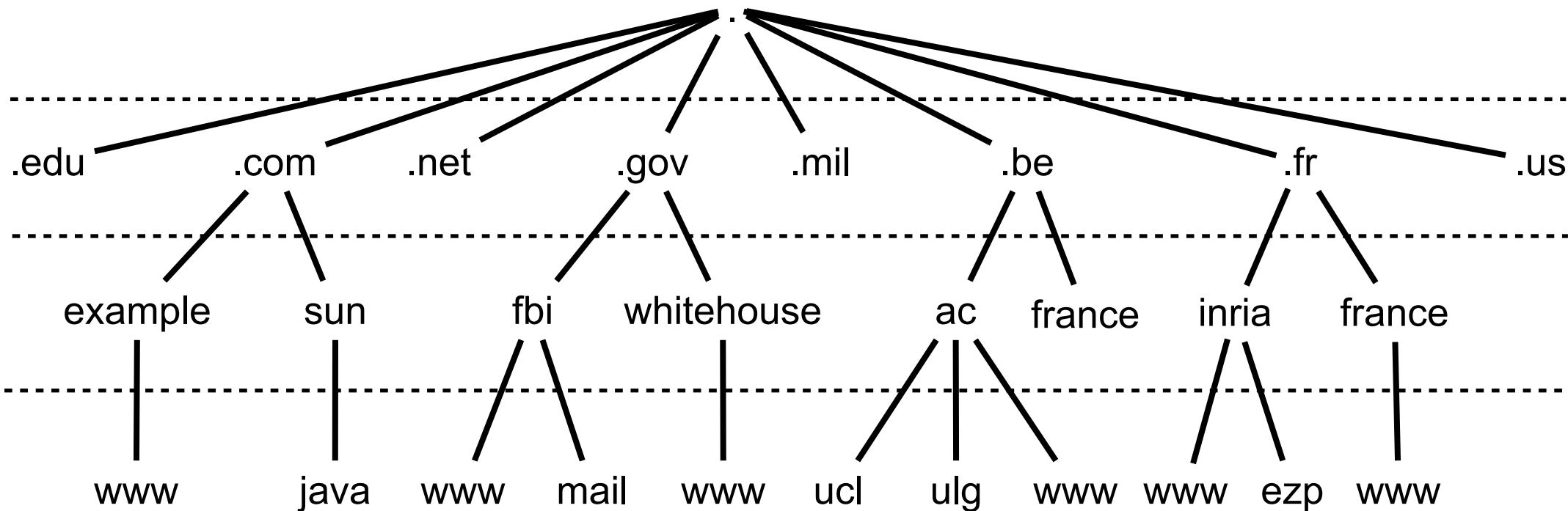
- Objective: provide a mean for human to easily identify (and remember) hosts
- Hosts receive textual names easy to remember but long and of variable size (e.g., goo.gl, www.example.org, 3.141592653589793238462643383279502884197169399375105820974944592.com...)
 - wastes space to carry them in packet headers
 - hard to parse
- Address are shorter and easy to process by hosts
- Indirection
 - multiple names may point to the same address
 - upon address change, only the resolution table has to be updated

Hierarchical naming

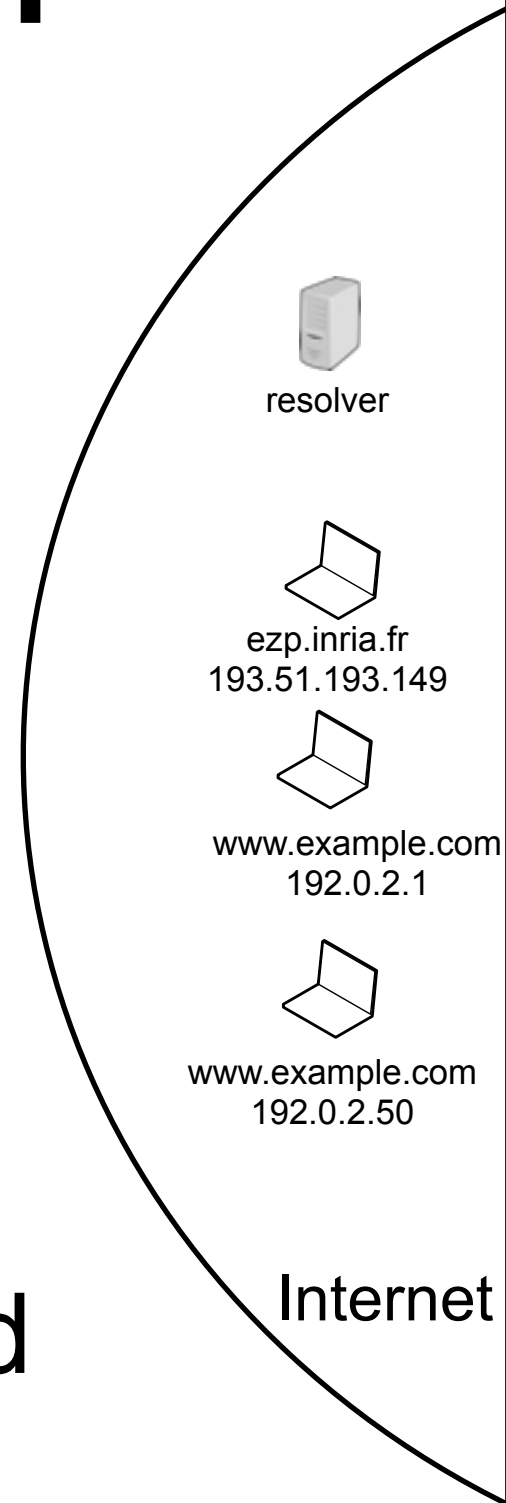
- Simplifies distributed naming/addressing
 - level i deals only with level $i+1$
- Global uniqueness is guaranteed
 - level i ensures uniqueness at level $i+1$
- Scales arbitrarily
 - level $i+1$ does not influence level $i-1$



Iterative resolution

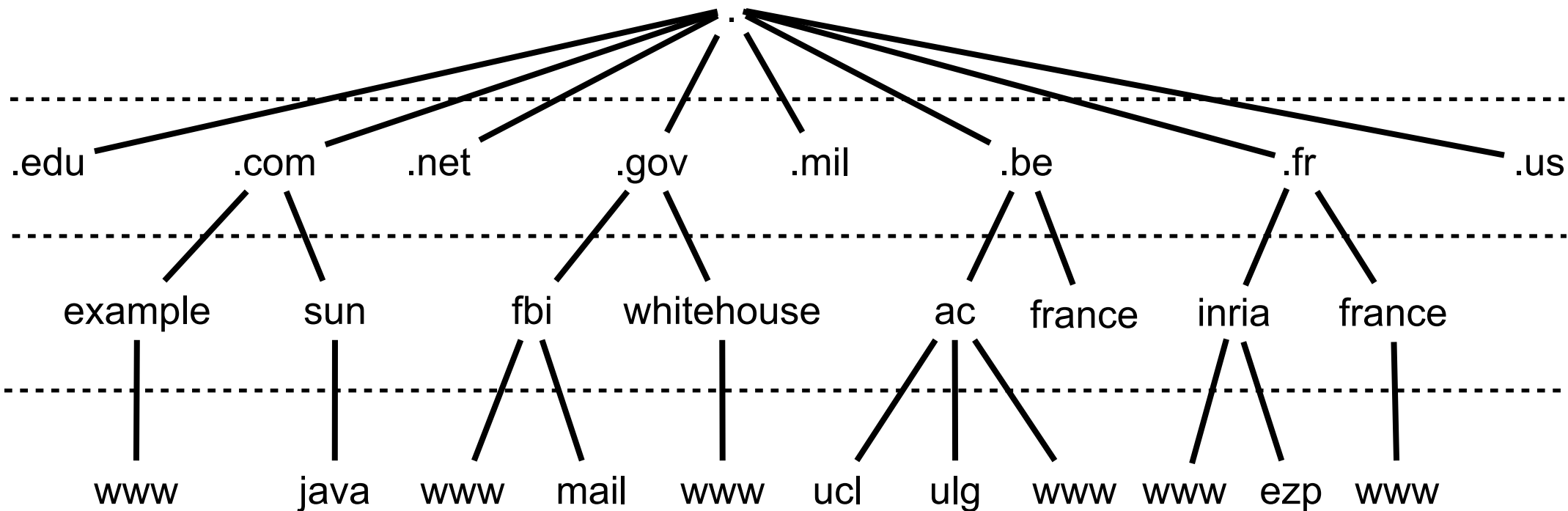


- The resolver learns the hierarchy
- responses can be cached to avoid querying twice the same server

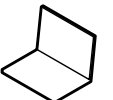


Iterative resolution

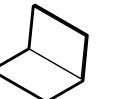
Query: ezp.inria.fr



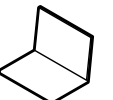
resolver



ezp.inria.fr
193.51.193.149



www.example.com
192.0.2.1

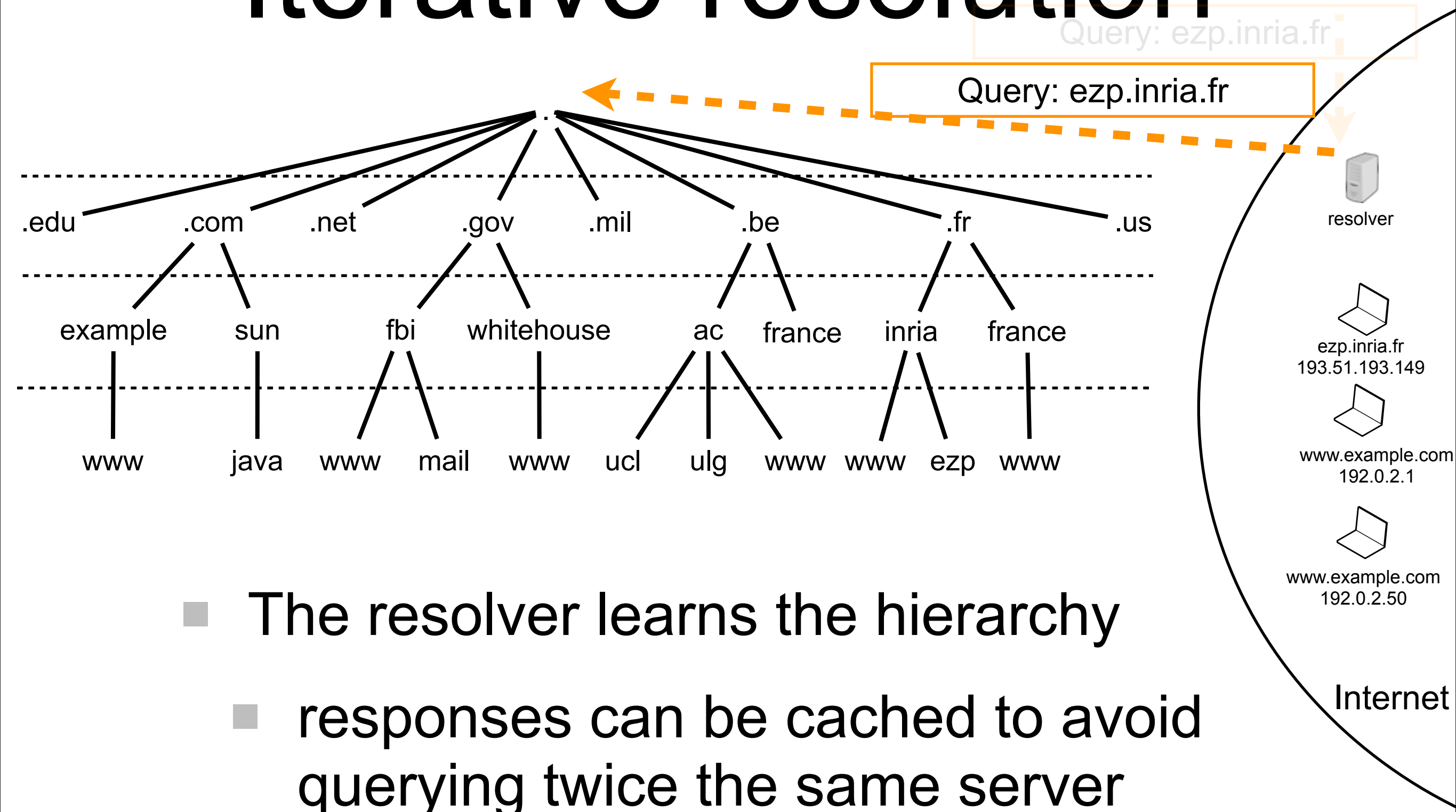


www.example.com
192.0.2.50

Internet

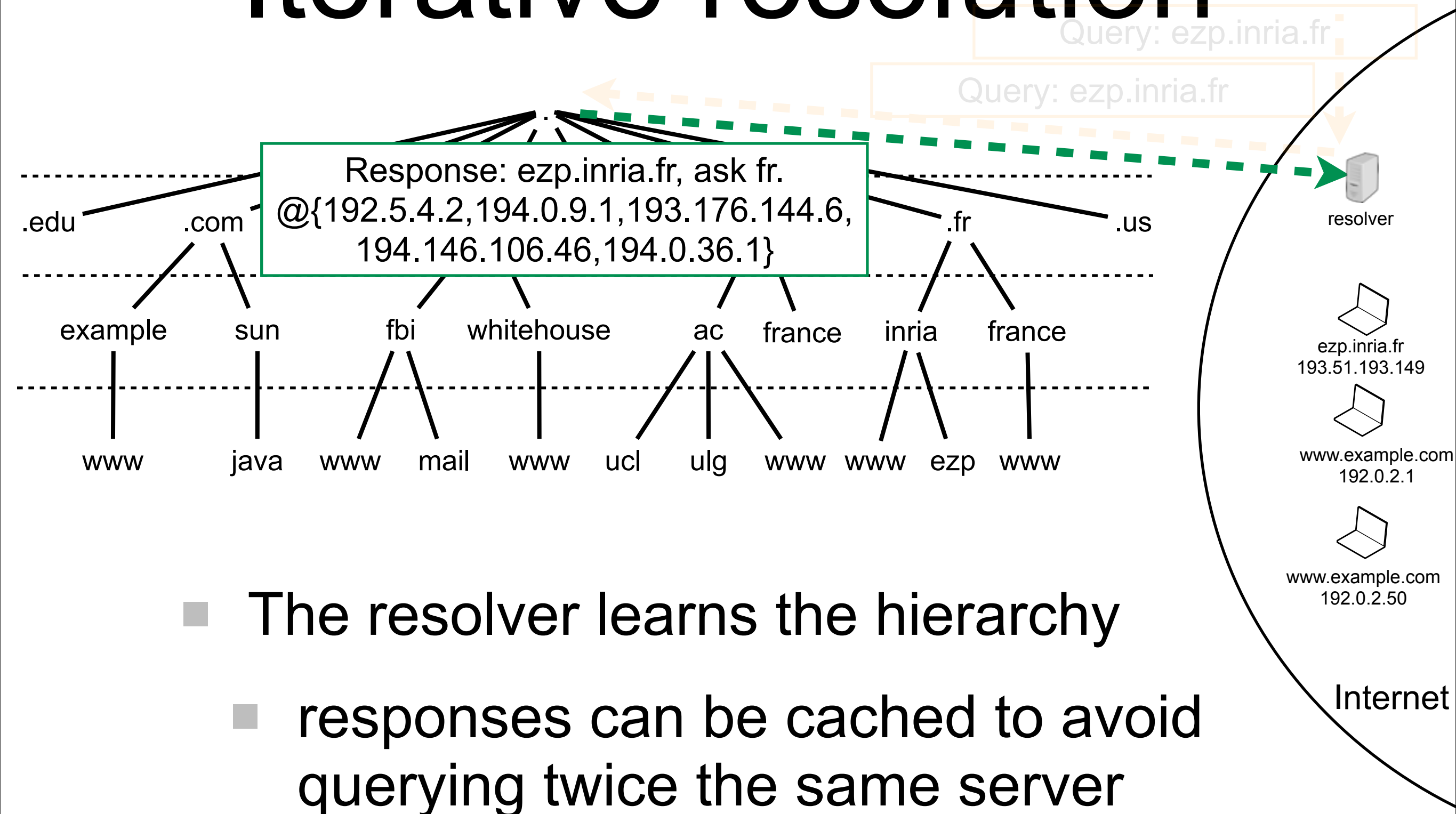
- The resolver learns the hierarchy
- responses can be cached to avoid querying twice the same server

Iterative resolution



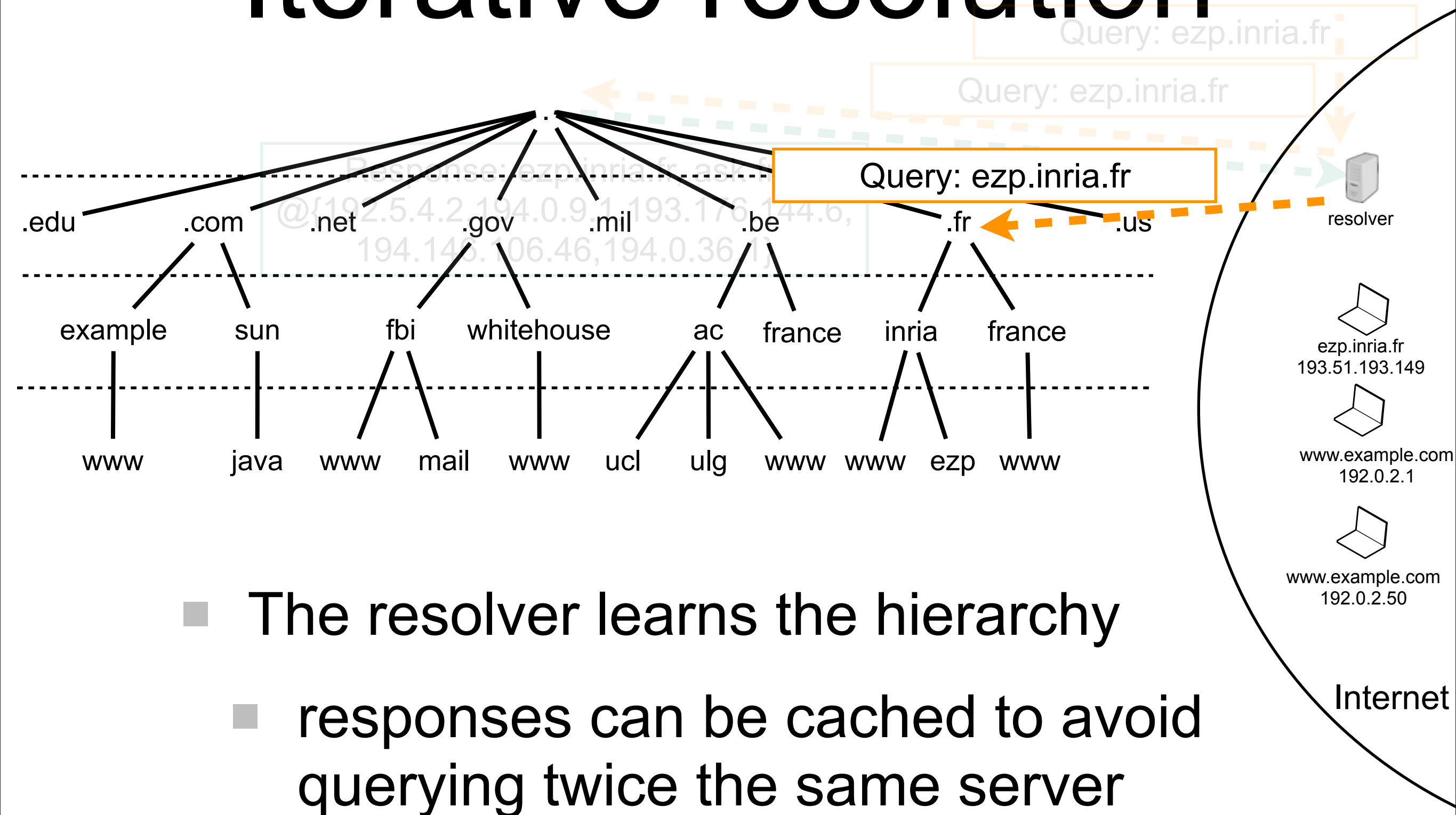
- The resolver learns the hierarchy
- responses can be cached to avoid querying twice the same server

Iterative resolution

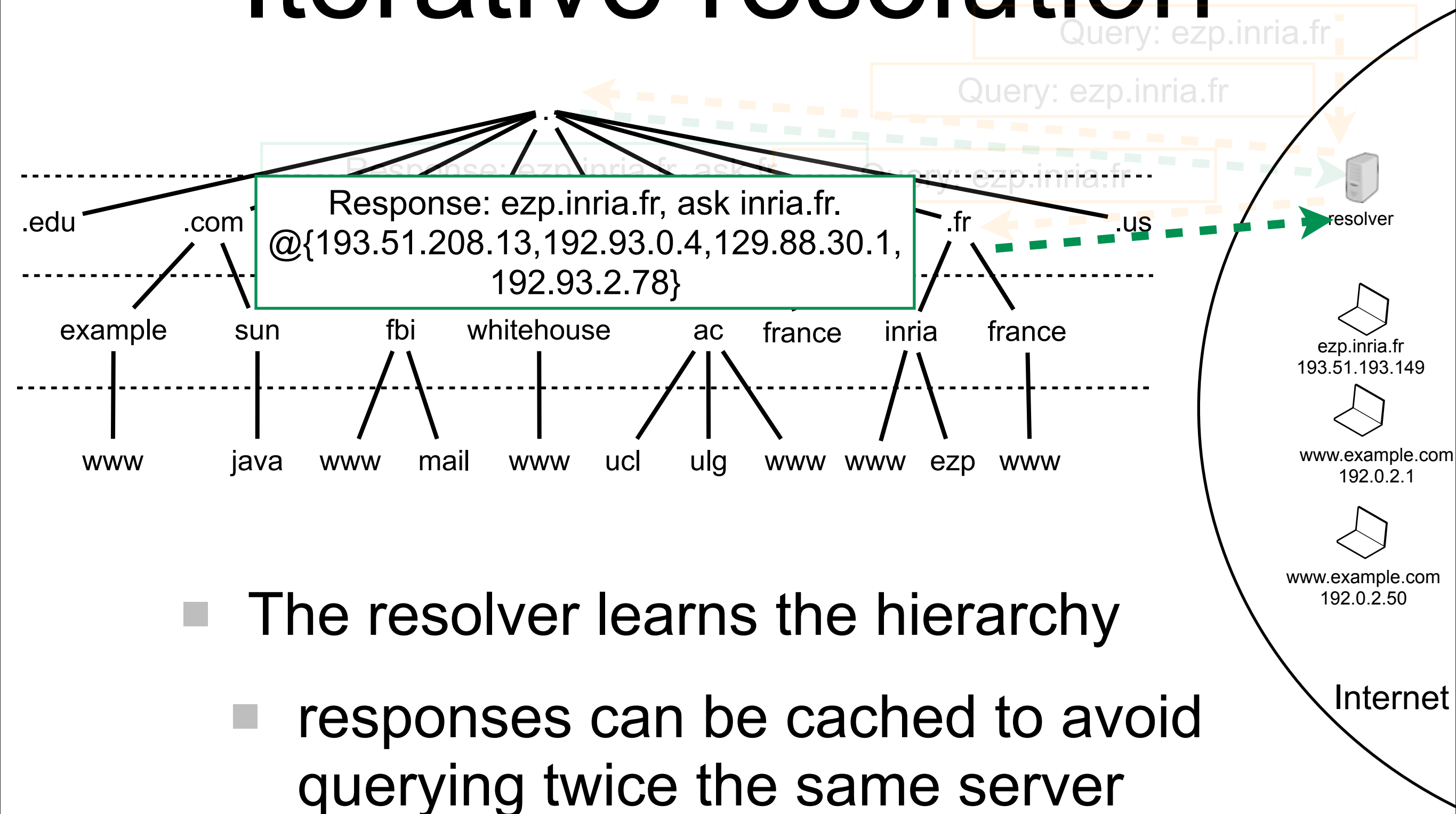


- The resolver learns the hierarchy
- responses can be cached to avoid querying twice the same server

Iterative resolution

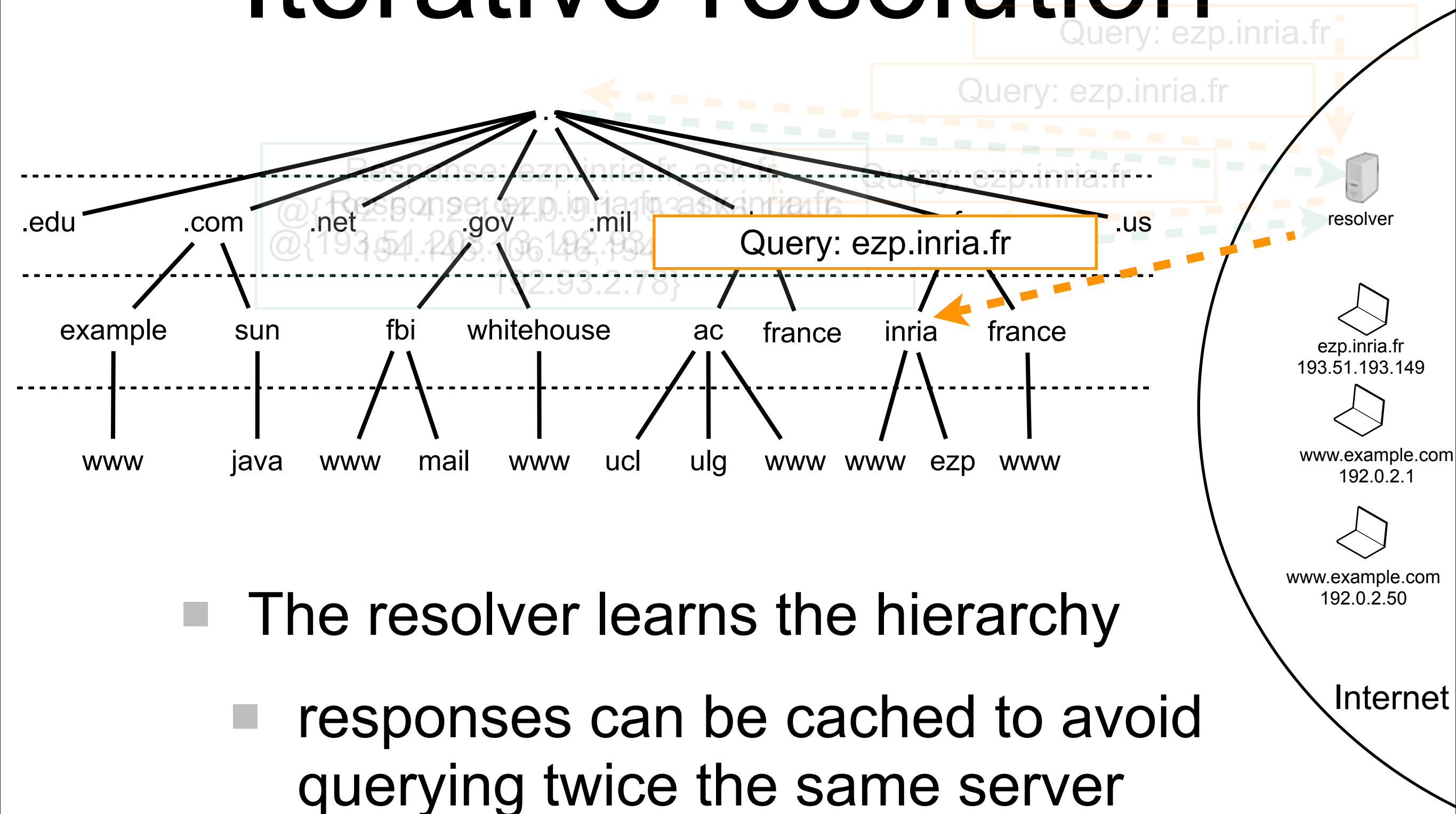


Iterative resolution

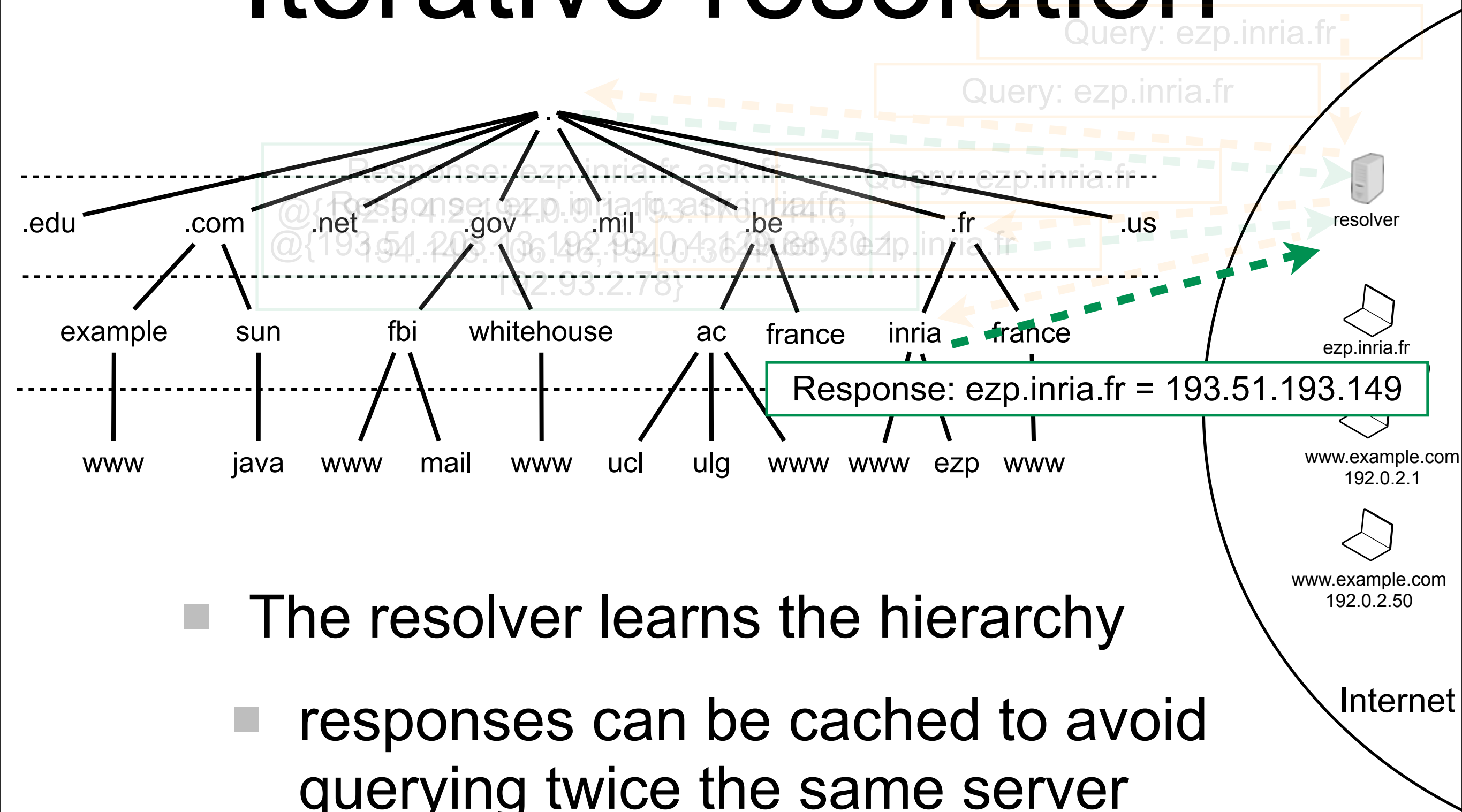


- The resolver learns the hierarchy
- responses can be cached to avoid querying twice the same server

Iterative resolution

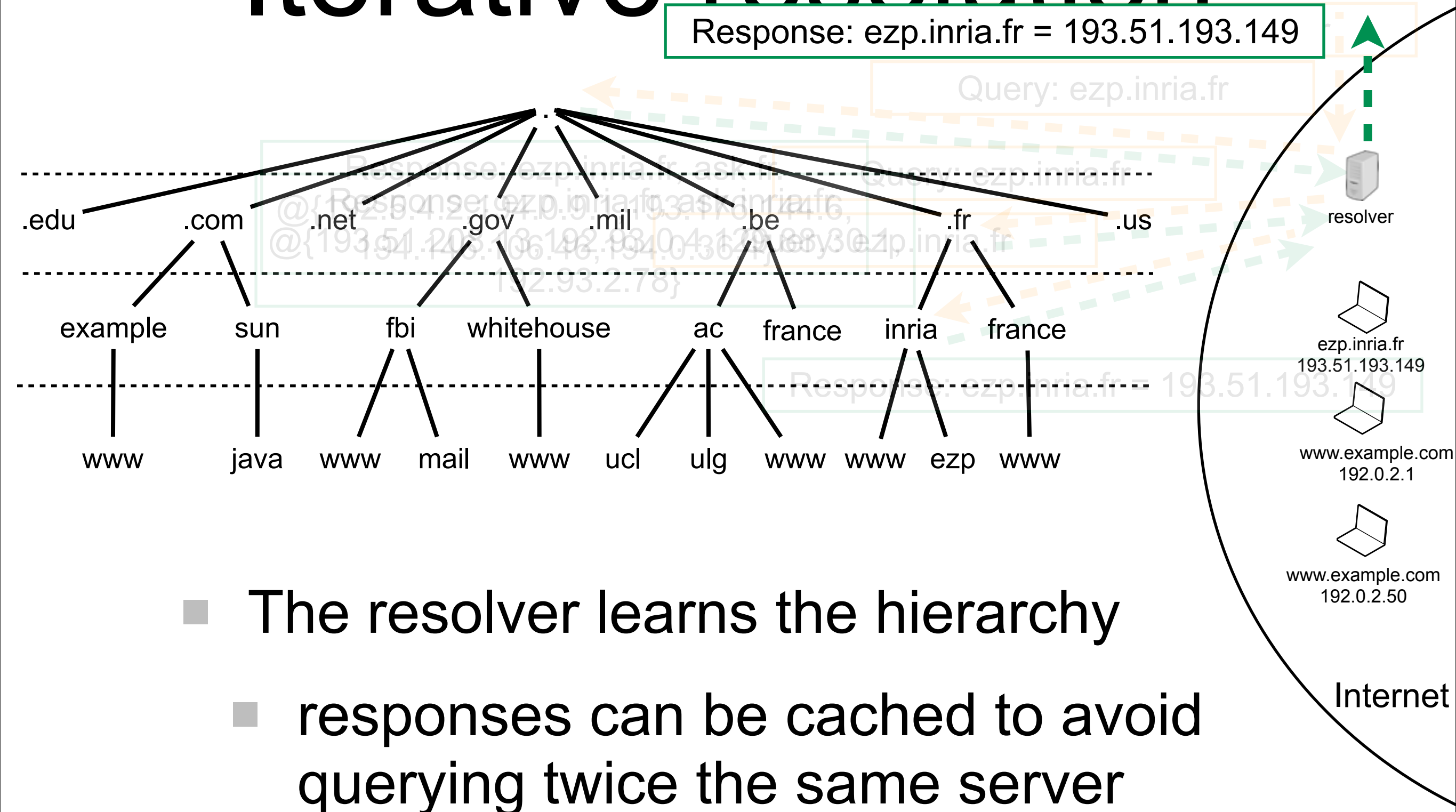


Iterative resolution

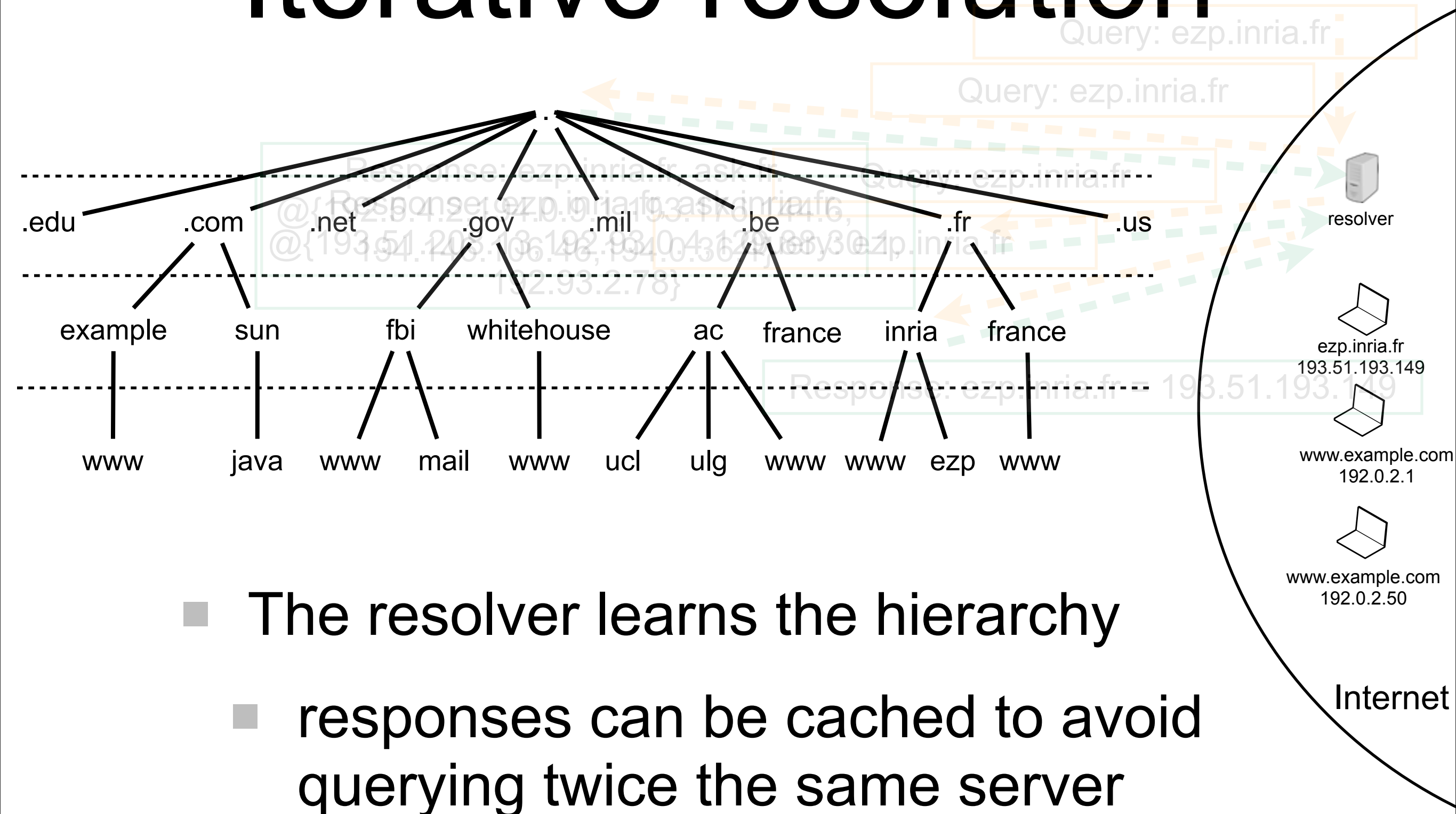


Iterative resolution

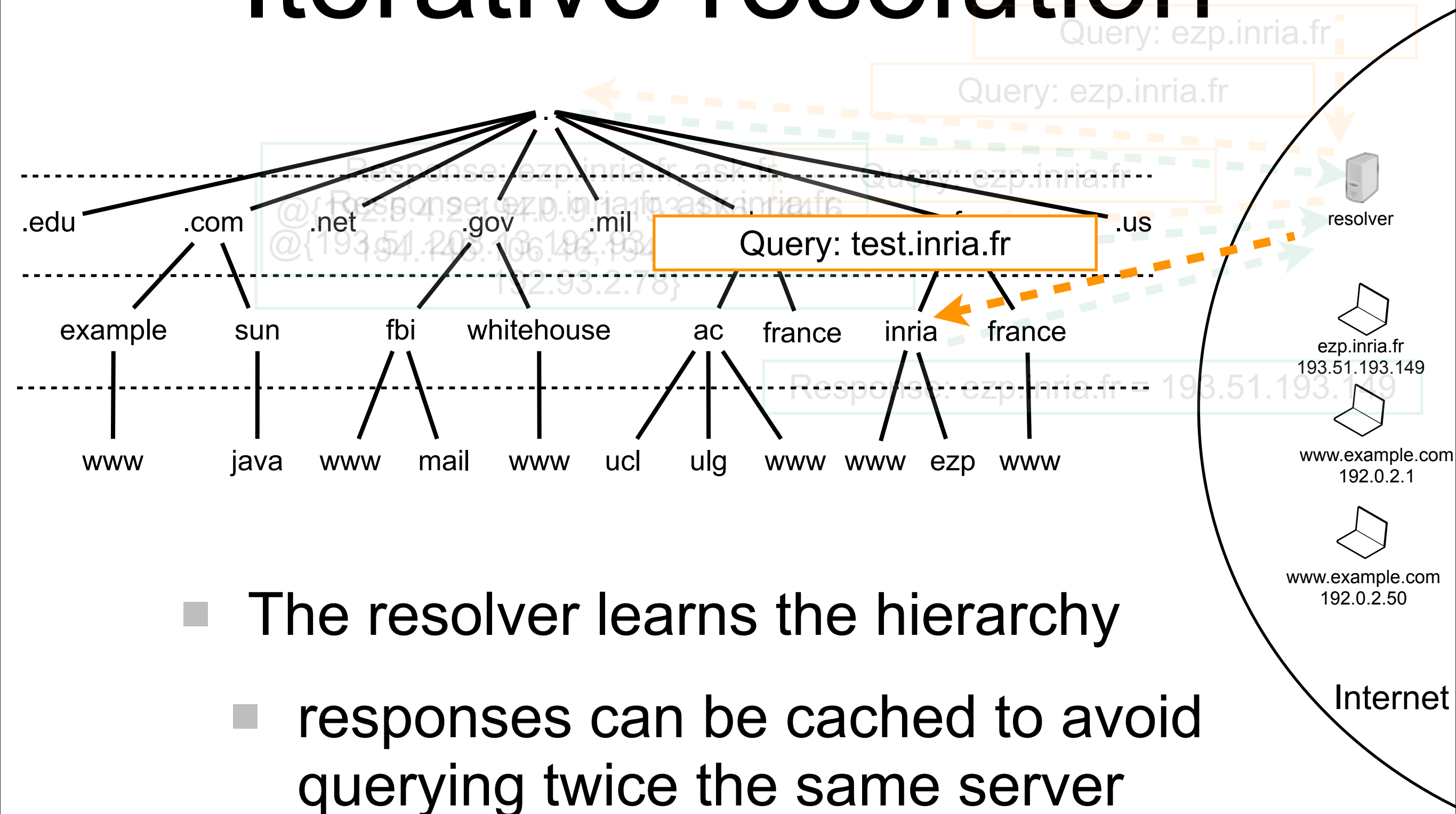
Response: ezp.inria.fr = 193.51.193.149



Iterative resolution



Iterative resolution



Transport

Transport of data between hosts

- Transport layer provides an end-to-end communication service
 - applications just deal with stream of bytes
- Most popular protocols:
 - UDP: connection-less, non reliable
 - TCP: connection-full, reliable

TCP connection establishment

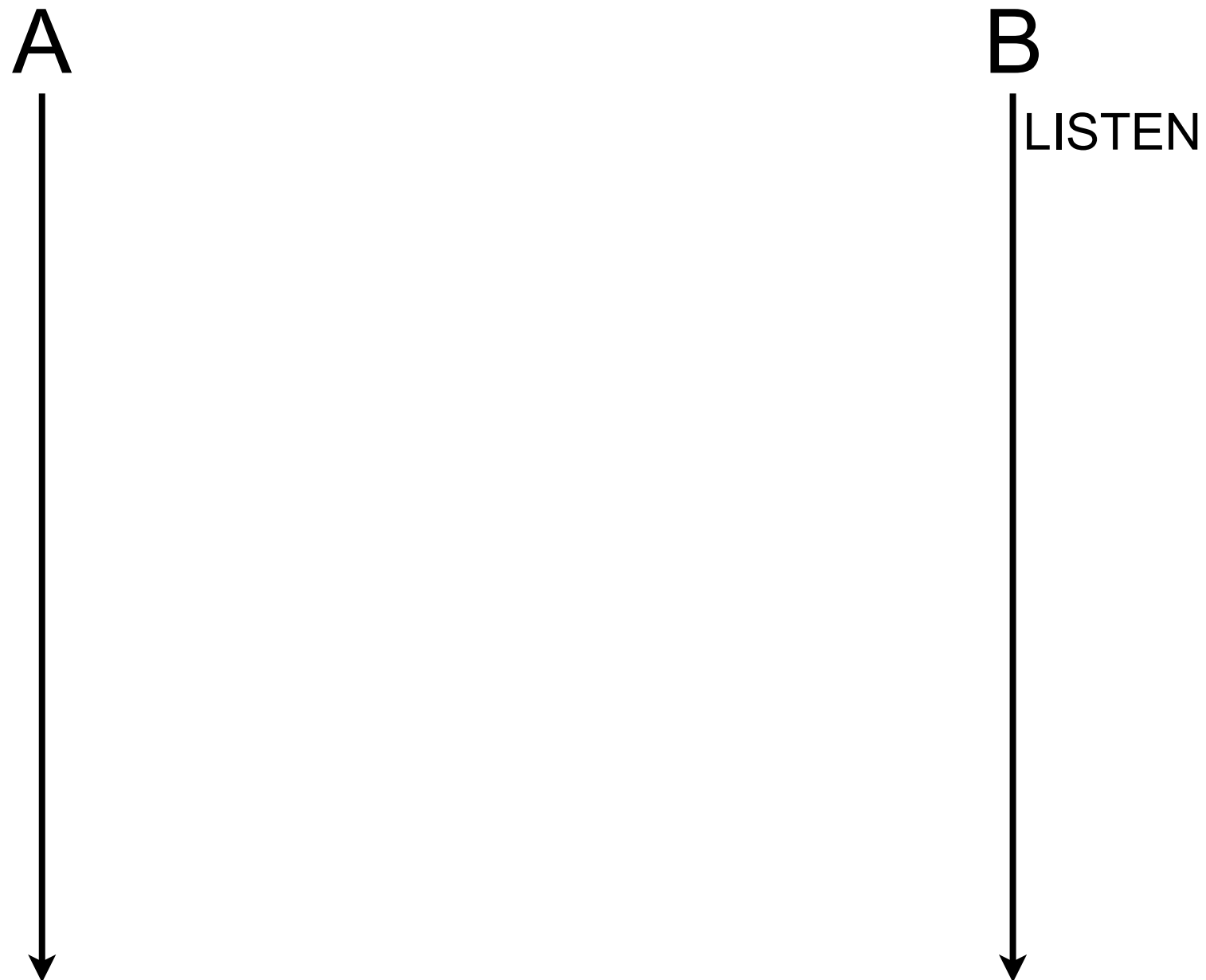
A



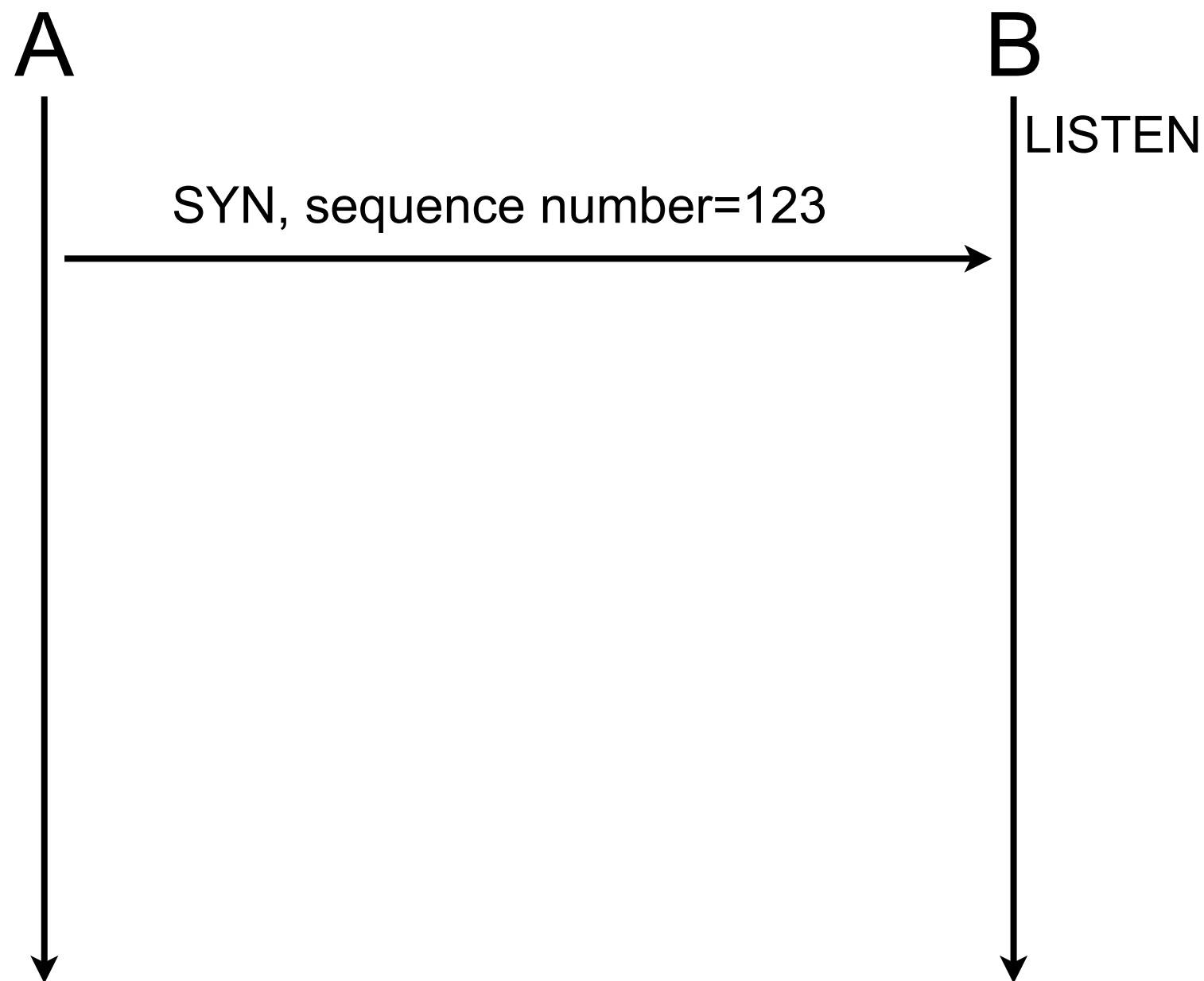
B



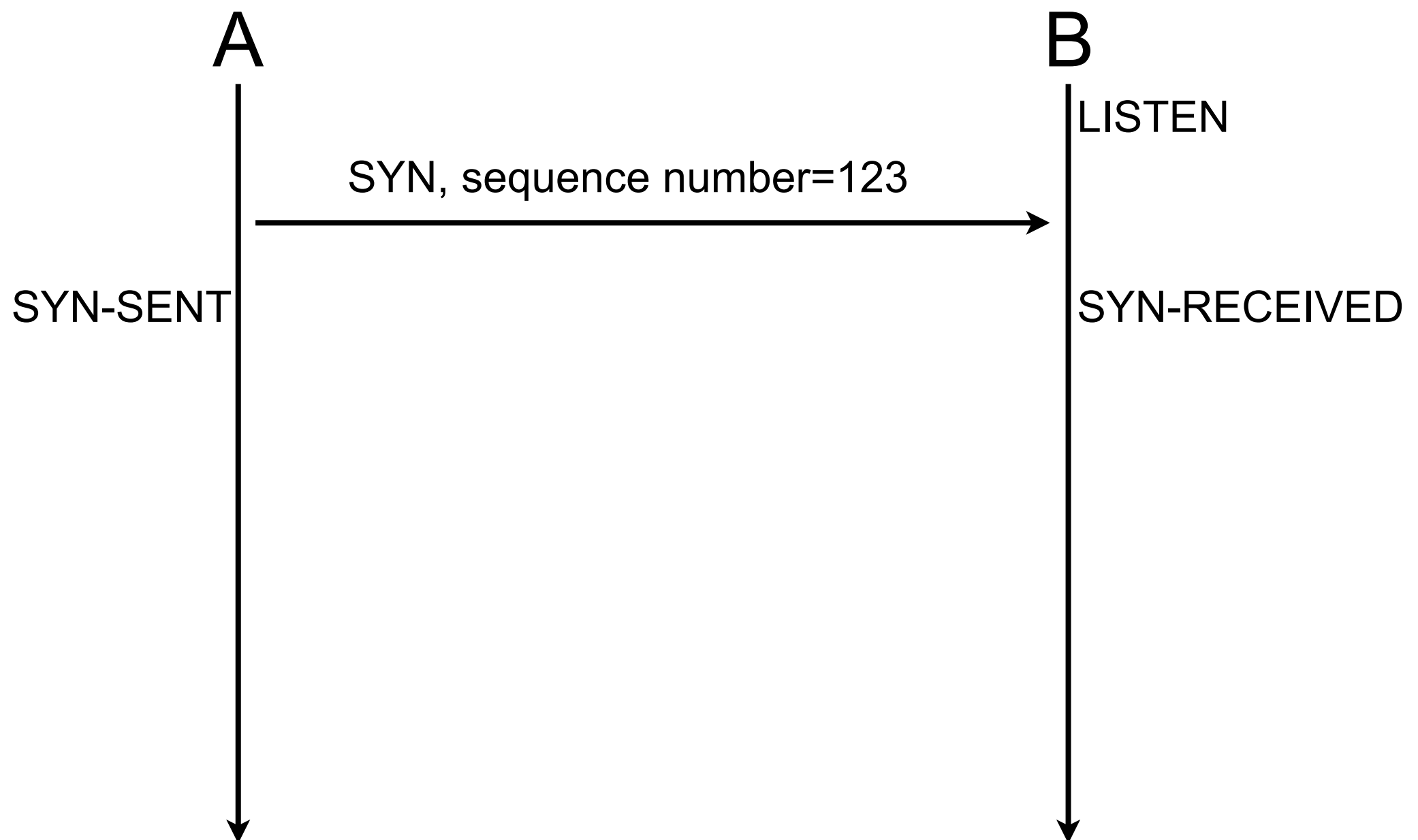
TCP connection establishment



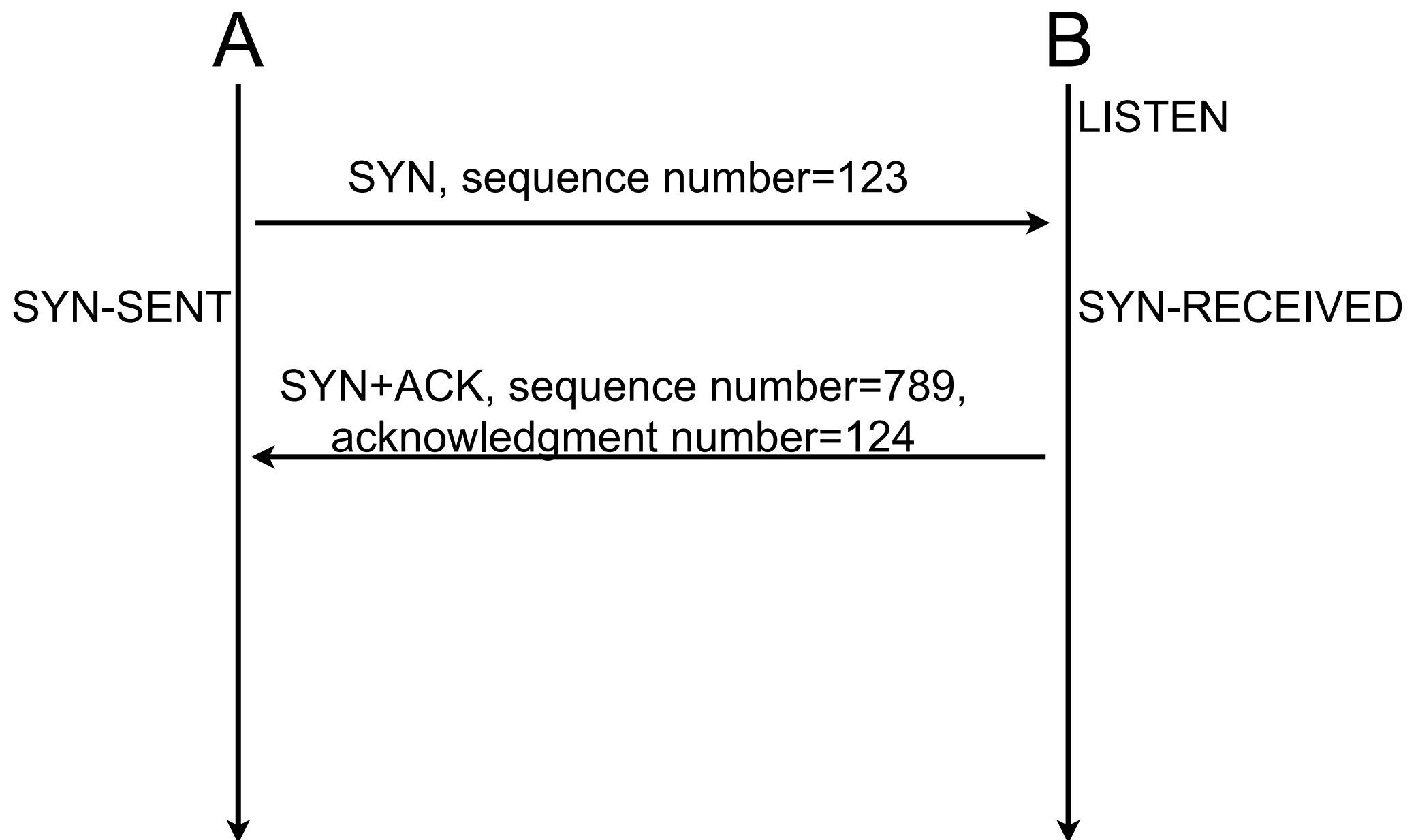
TCP connection establishment



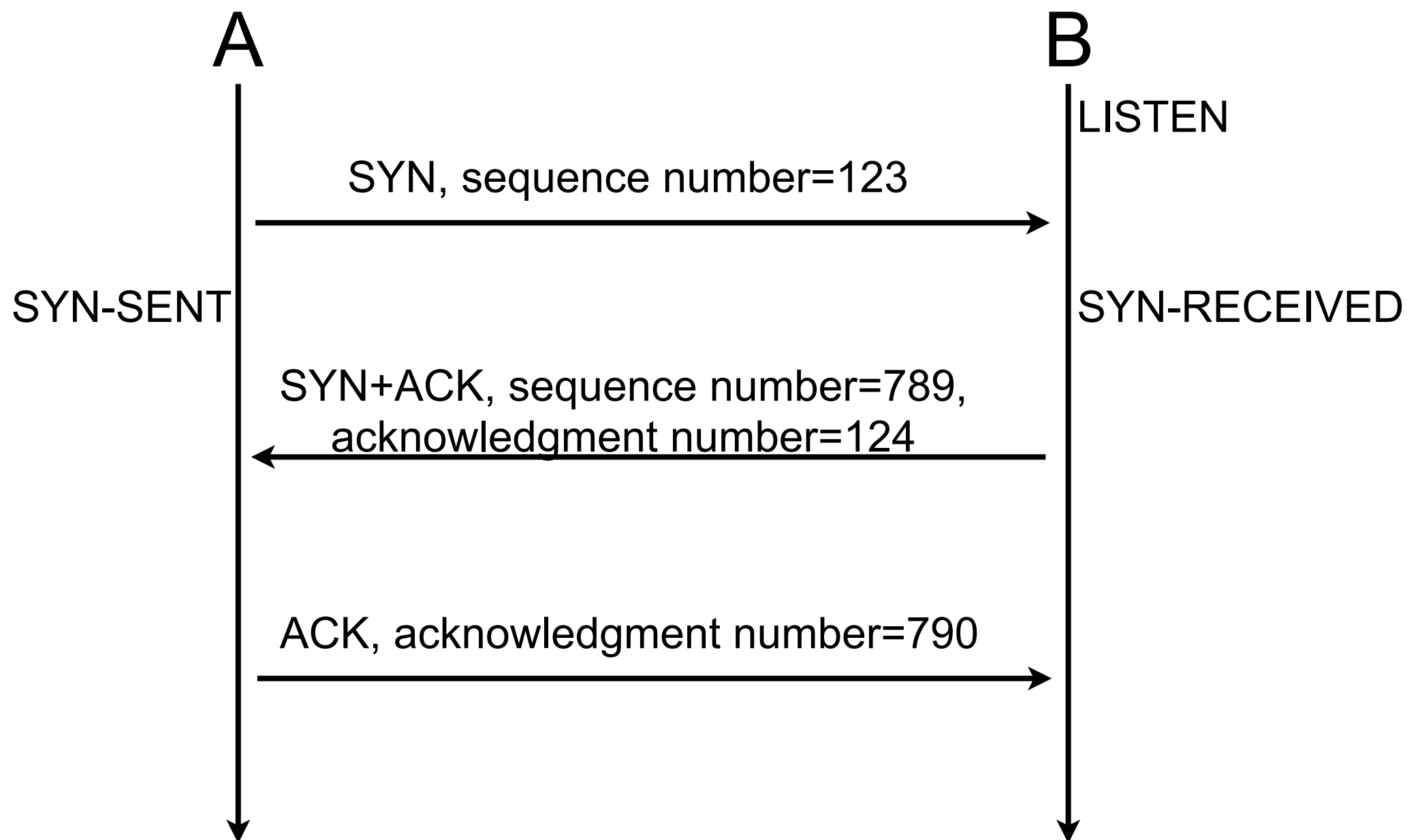
TCP connection establishment



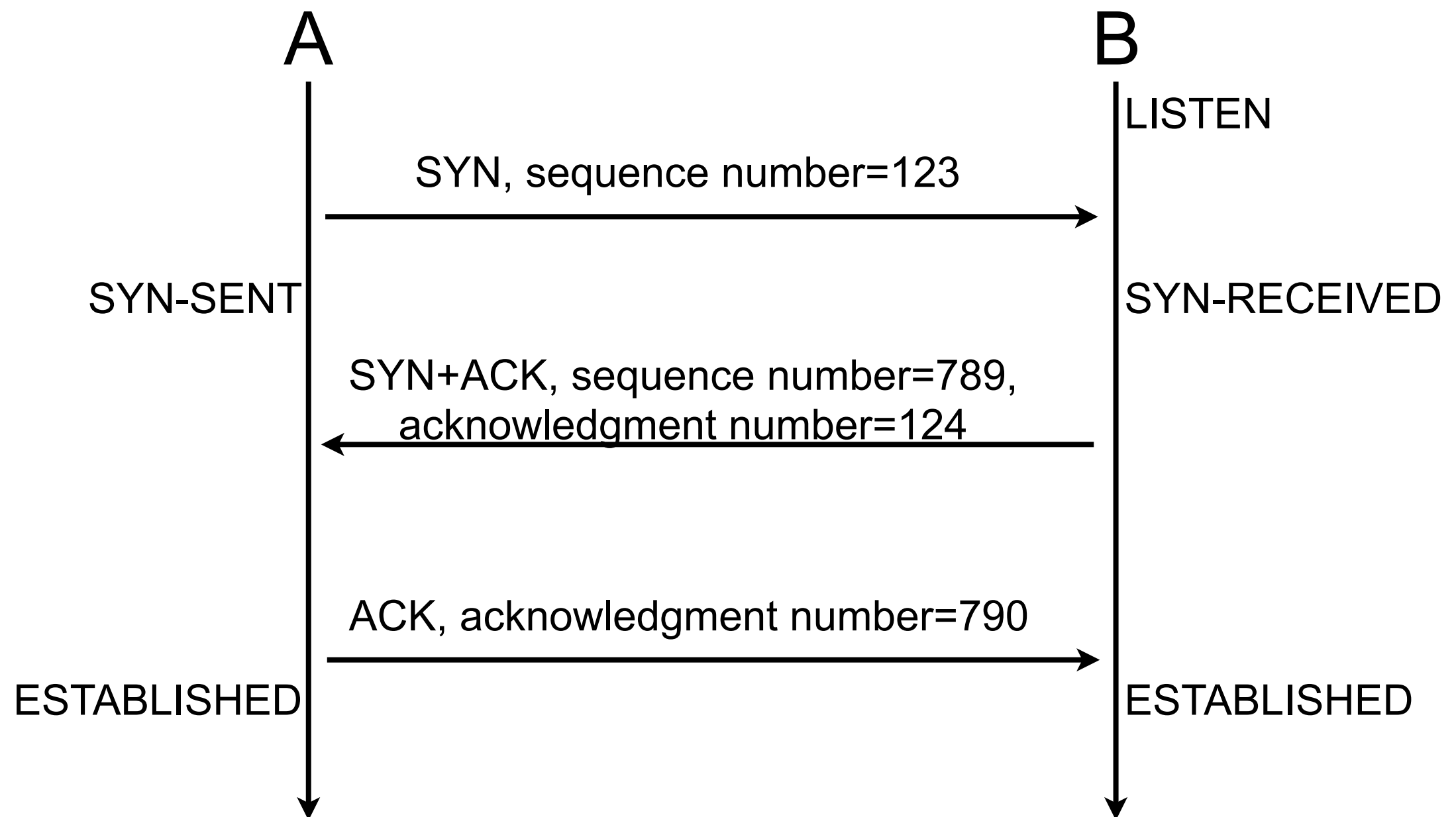
TCP connection establishment



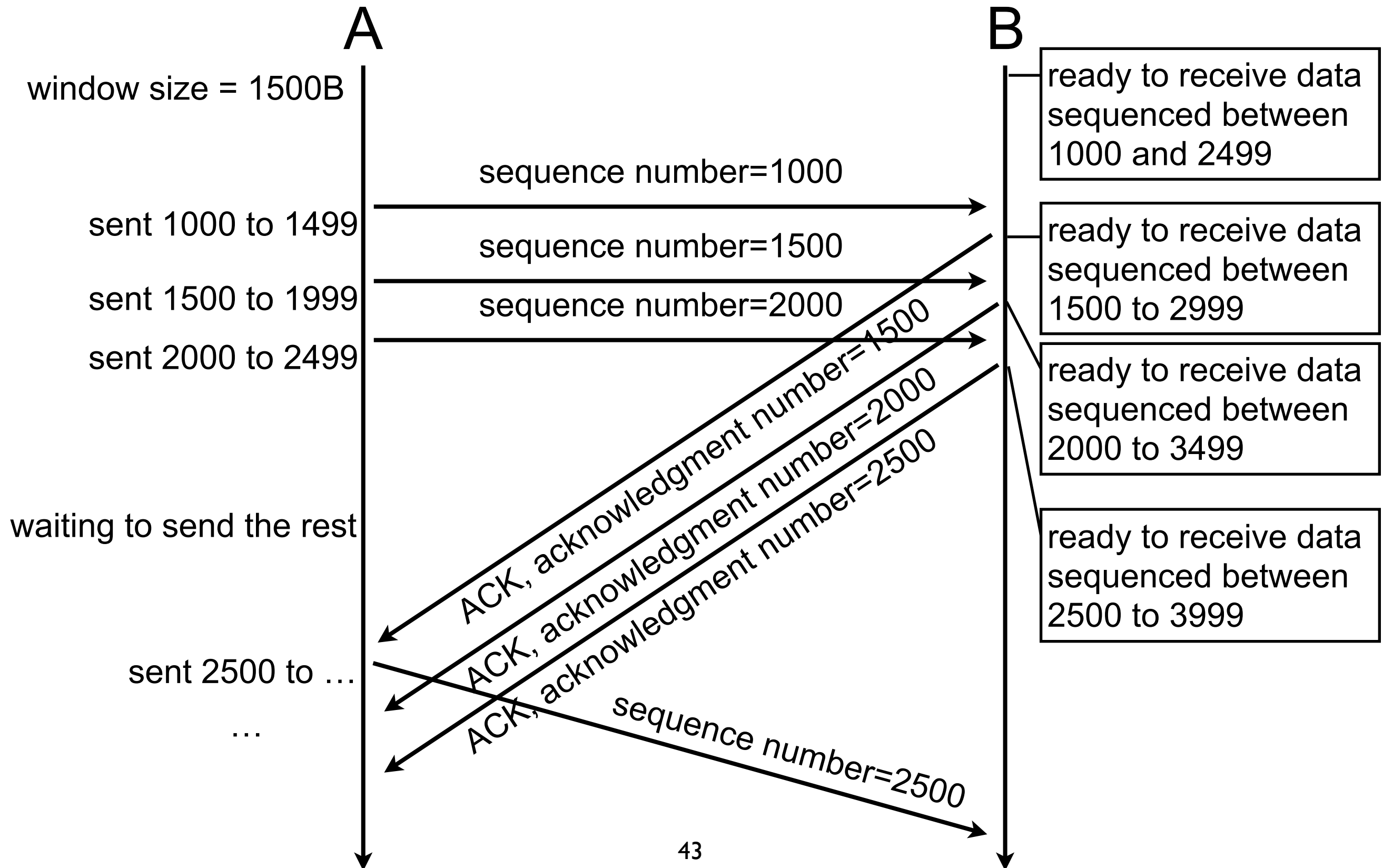
TCP connection establishment



TCP connection establishment



TCP data transfer



TCP connection termination

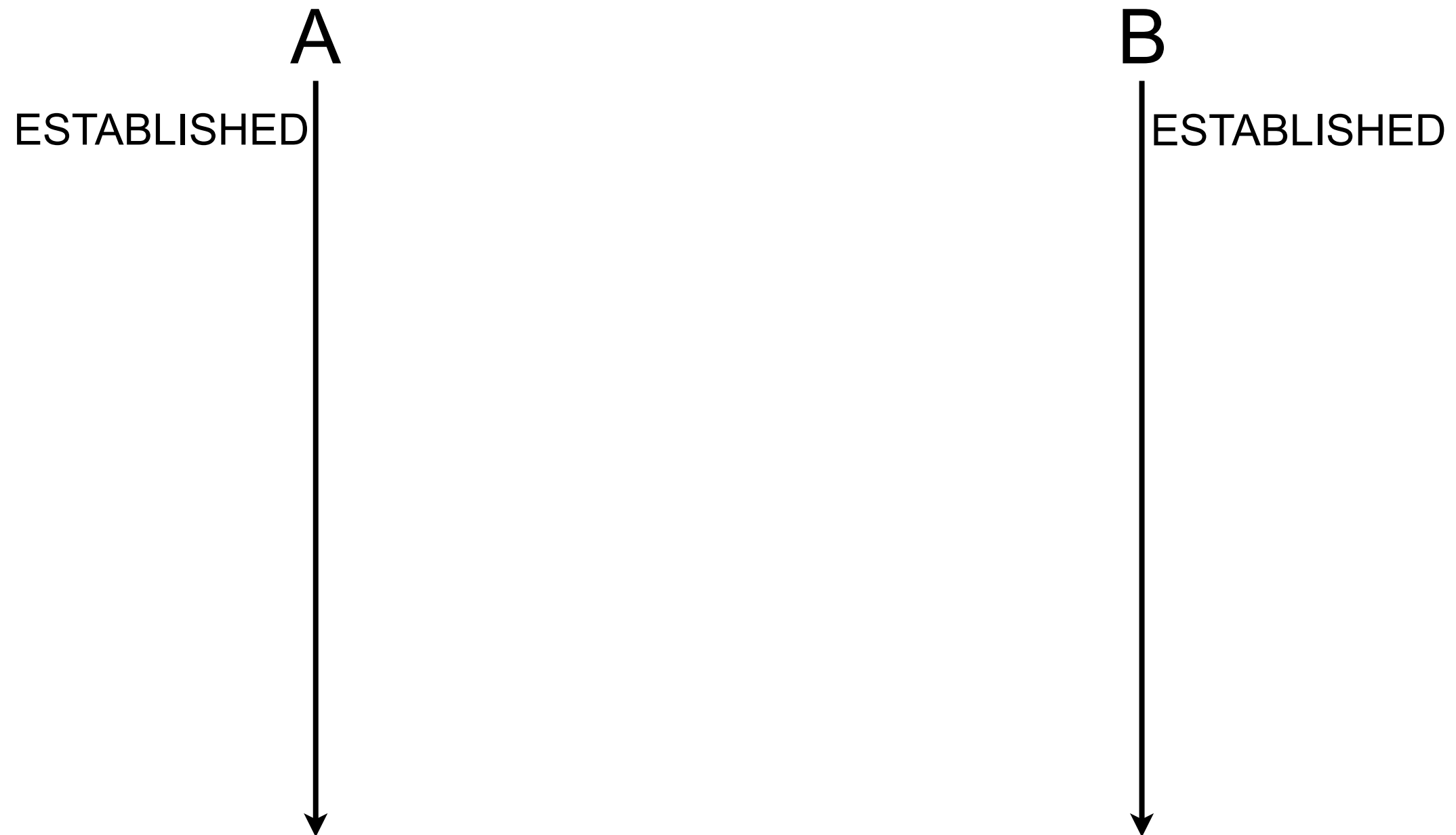
A



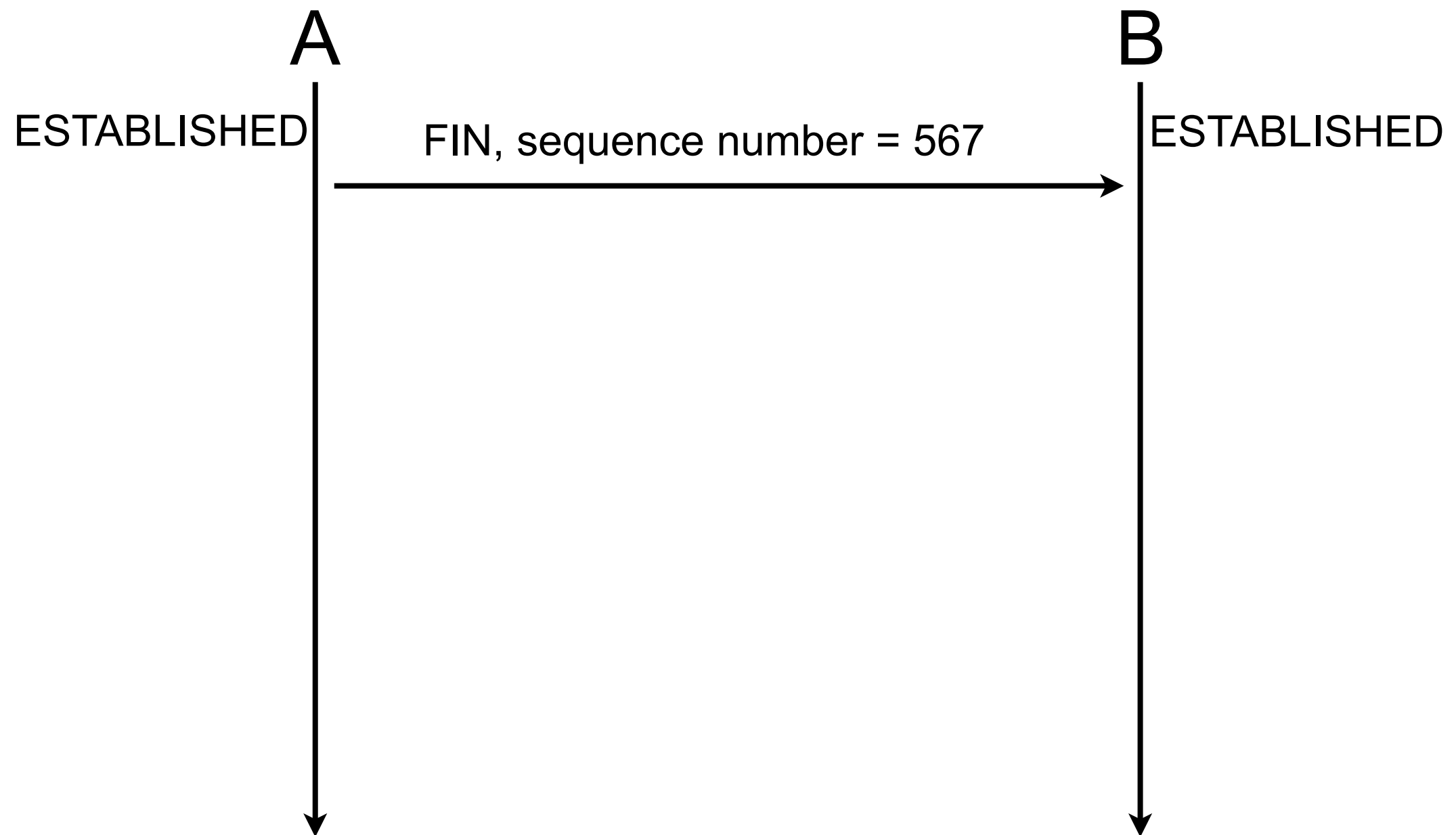
B



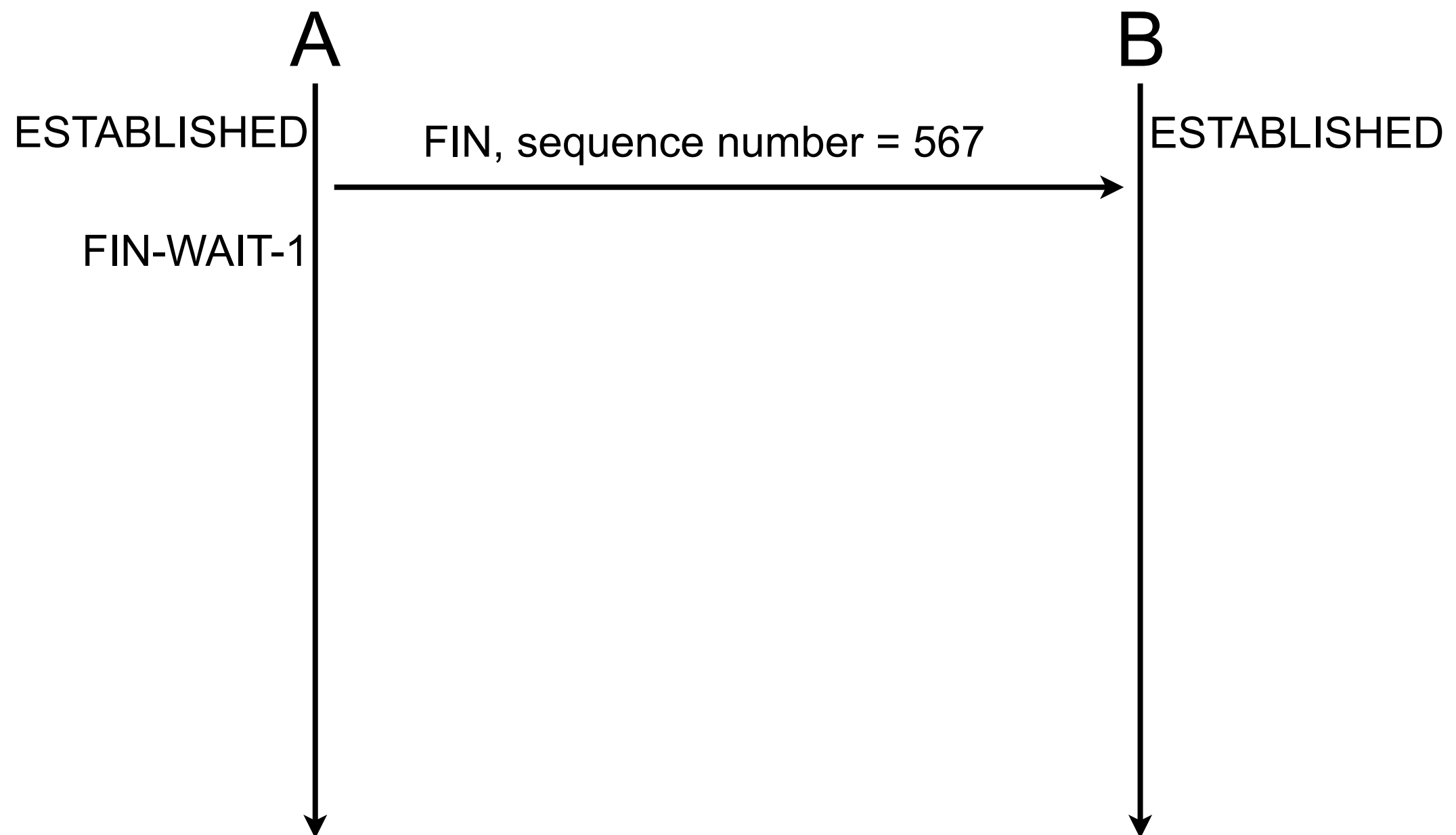
TCP connection termination



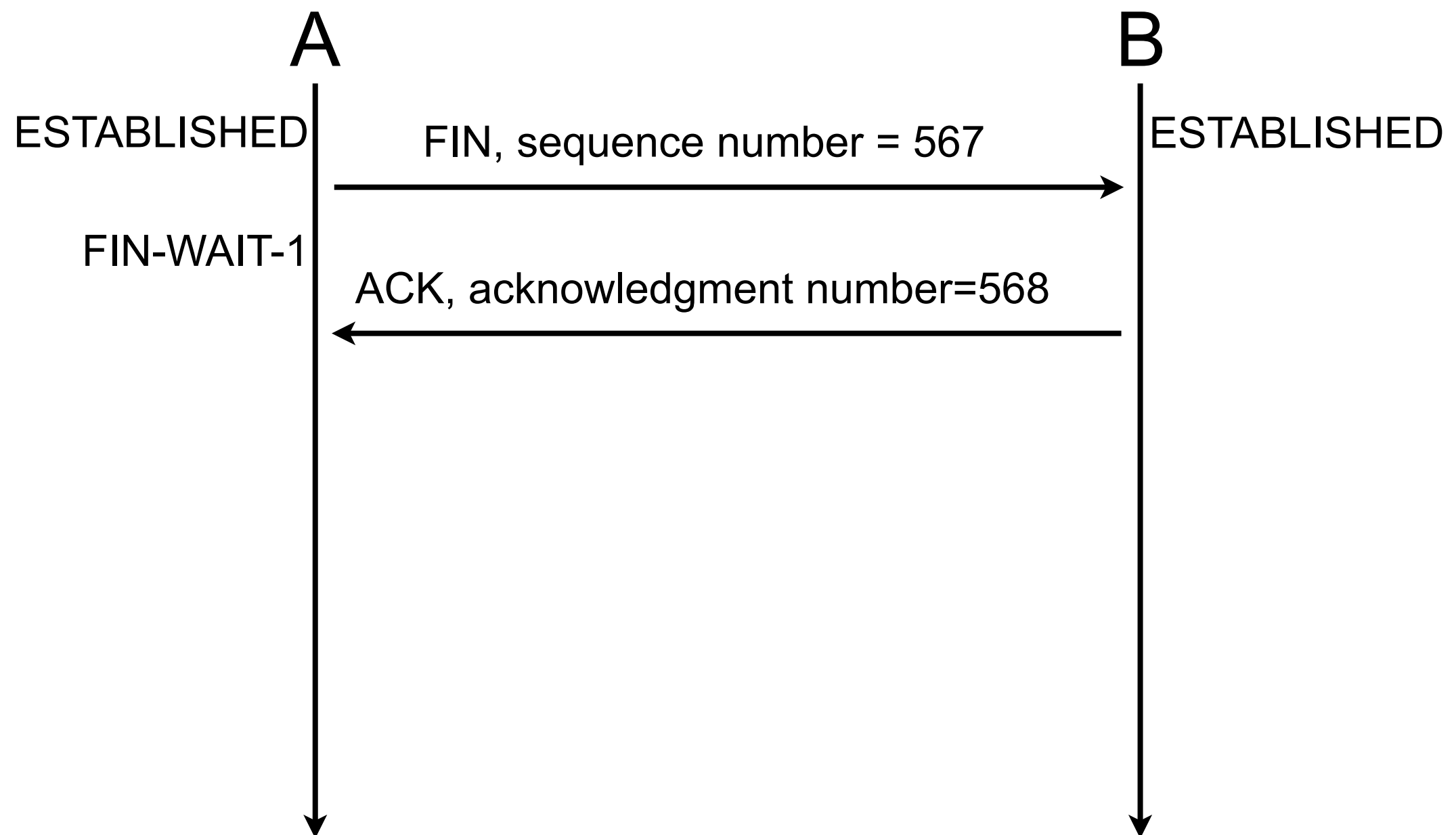
TCP connection termination



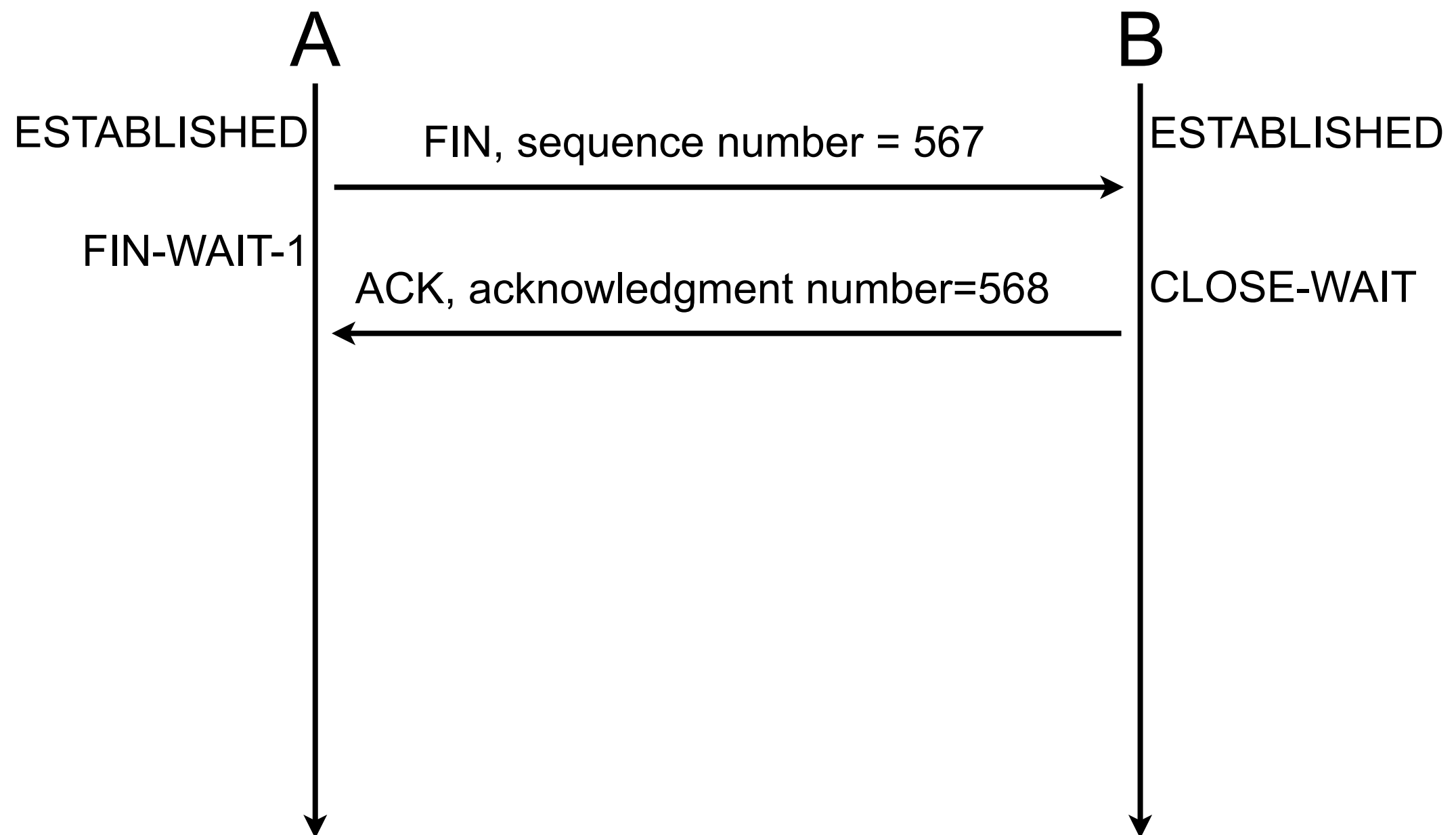
TCP connection termination



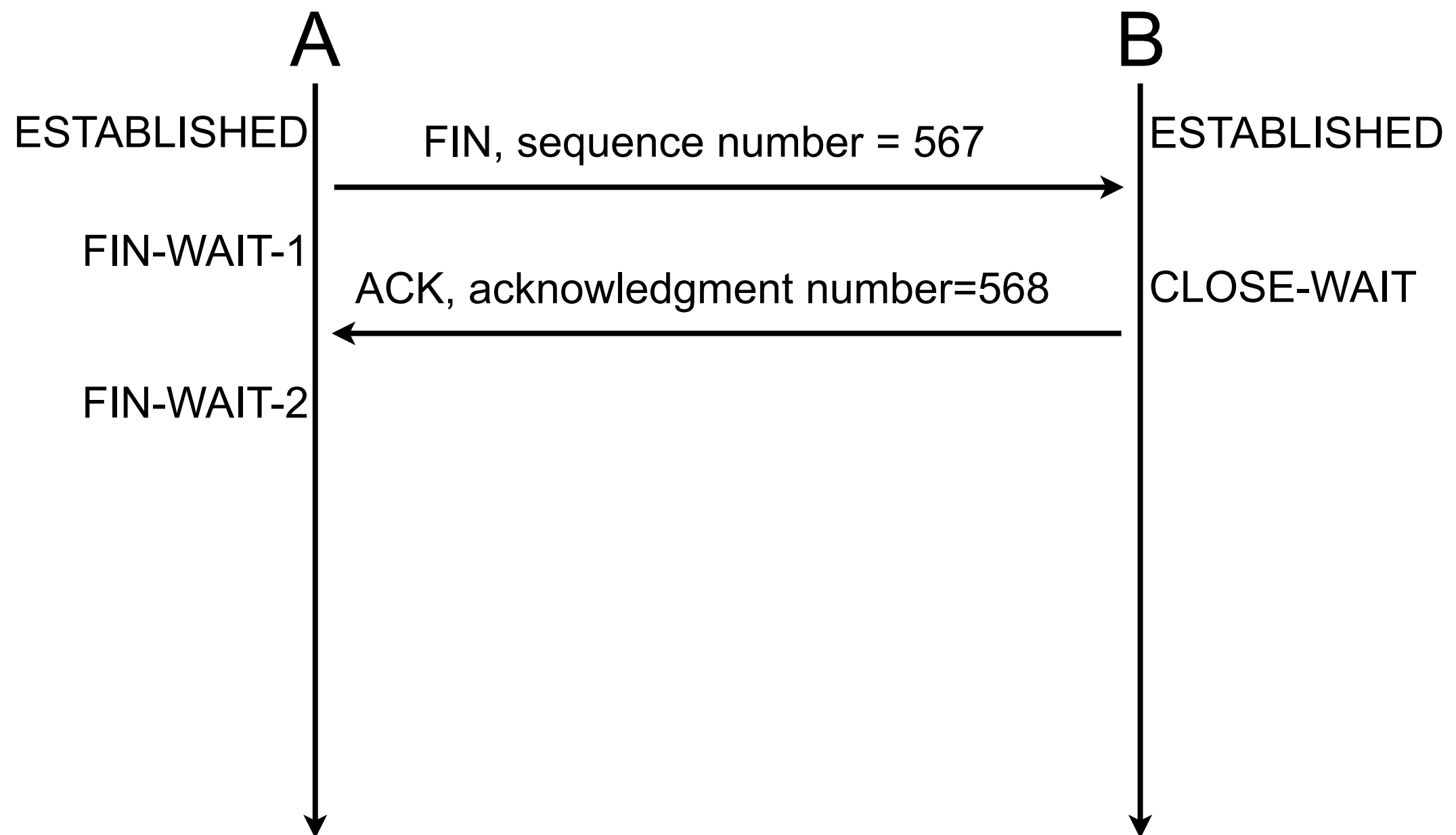
TCP connection termination



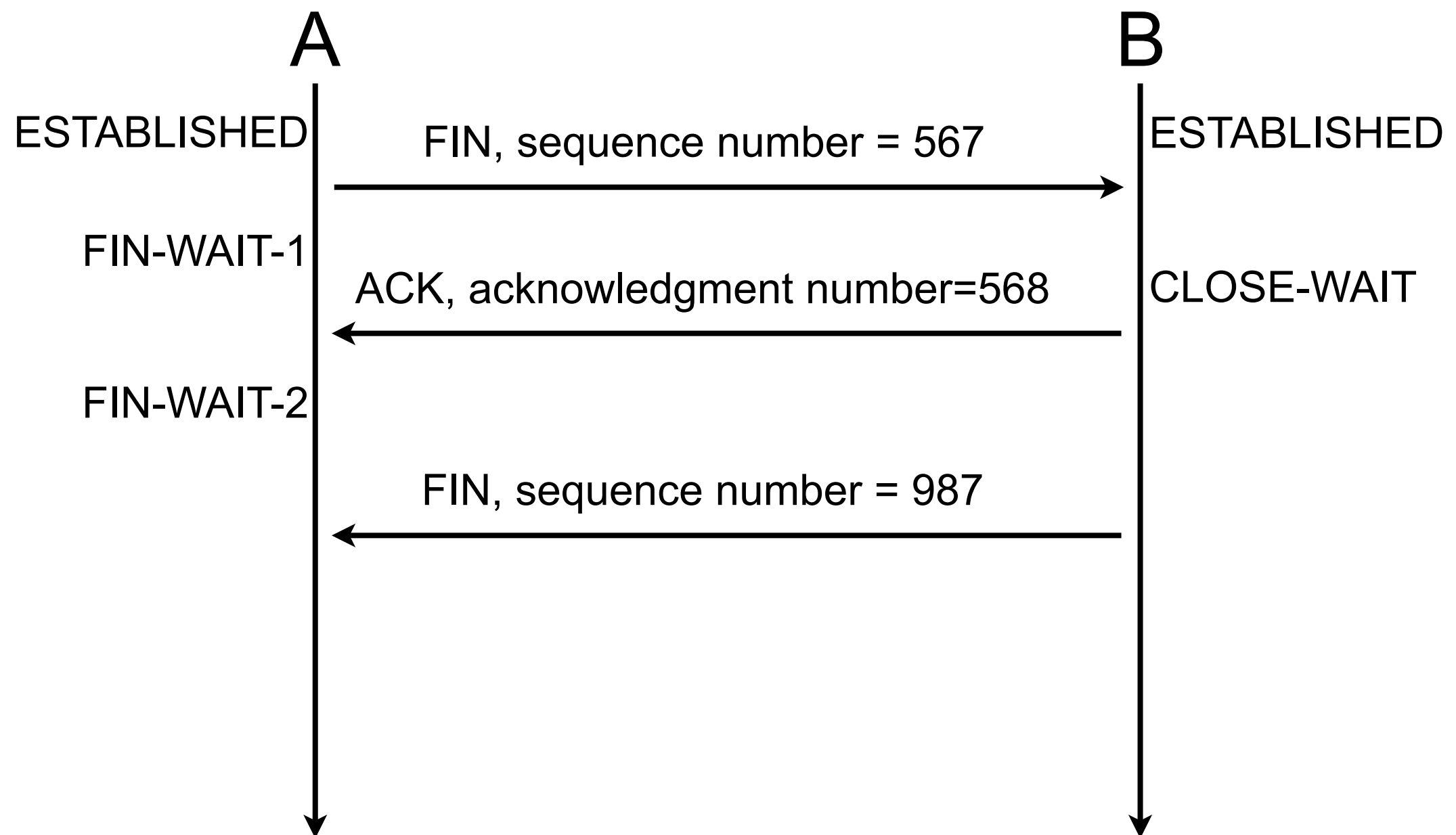
TCP connection termination



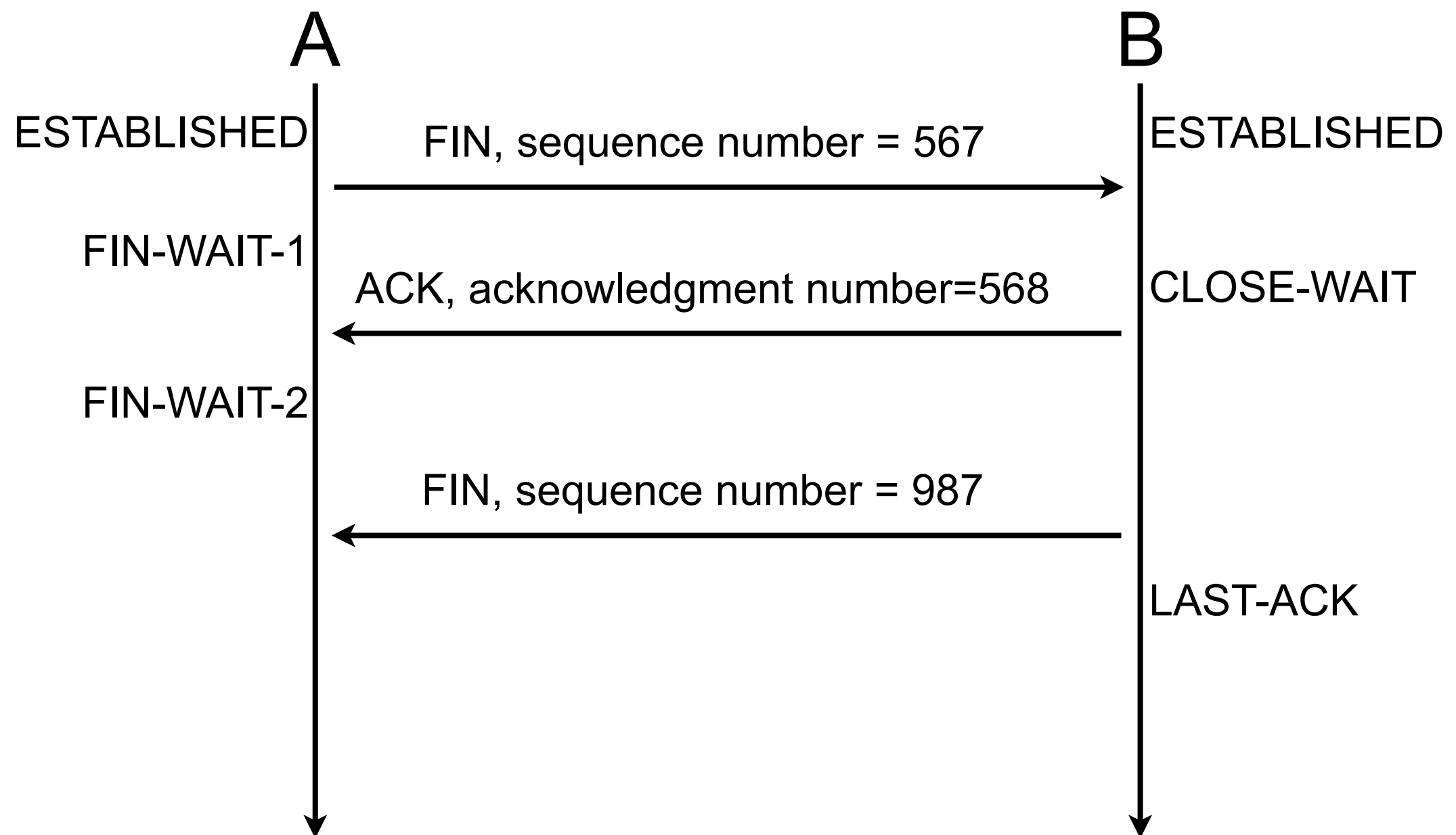
TCP connection termination



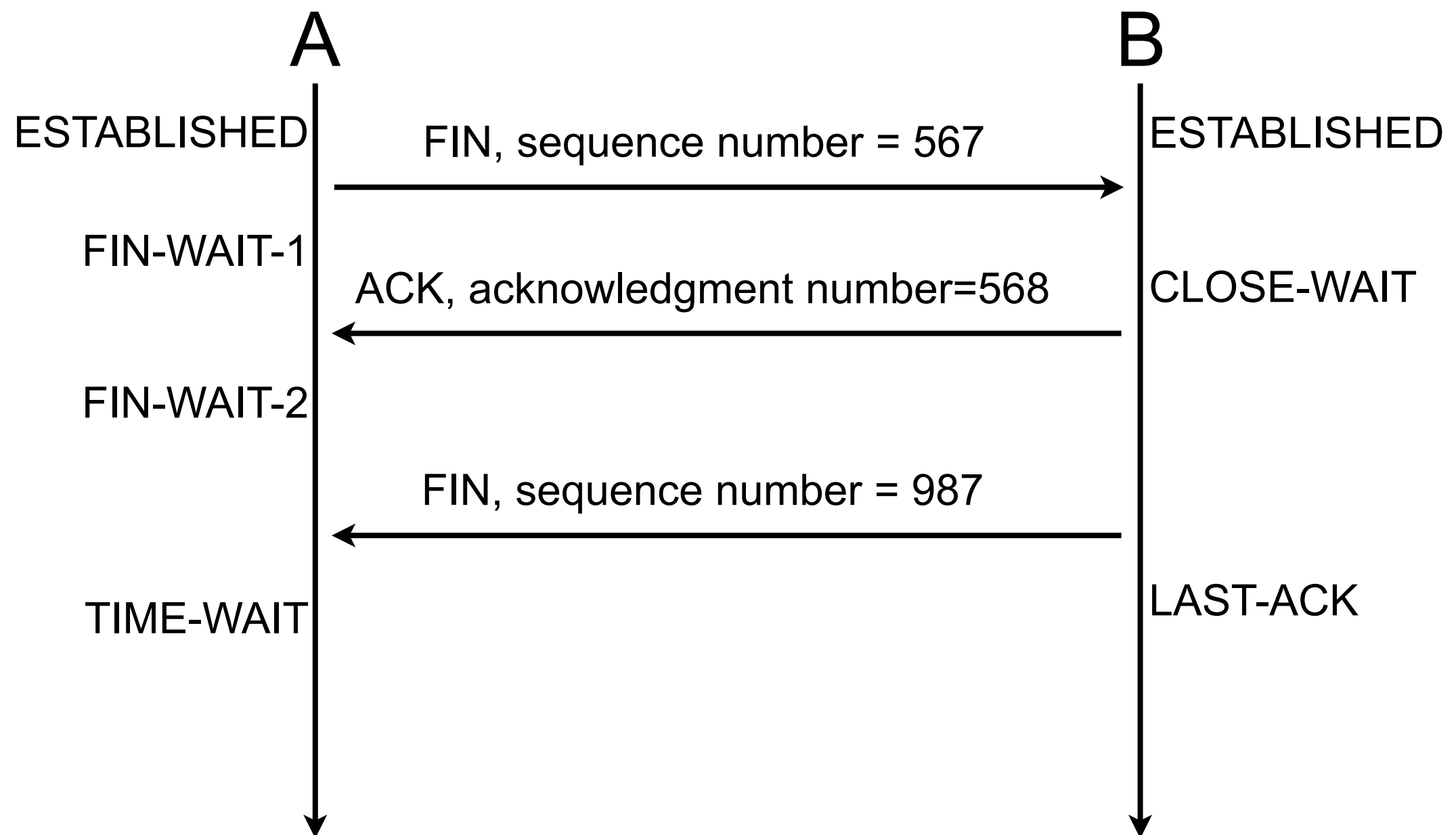
TCP connection termination



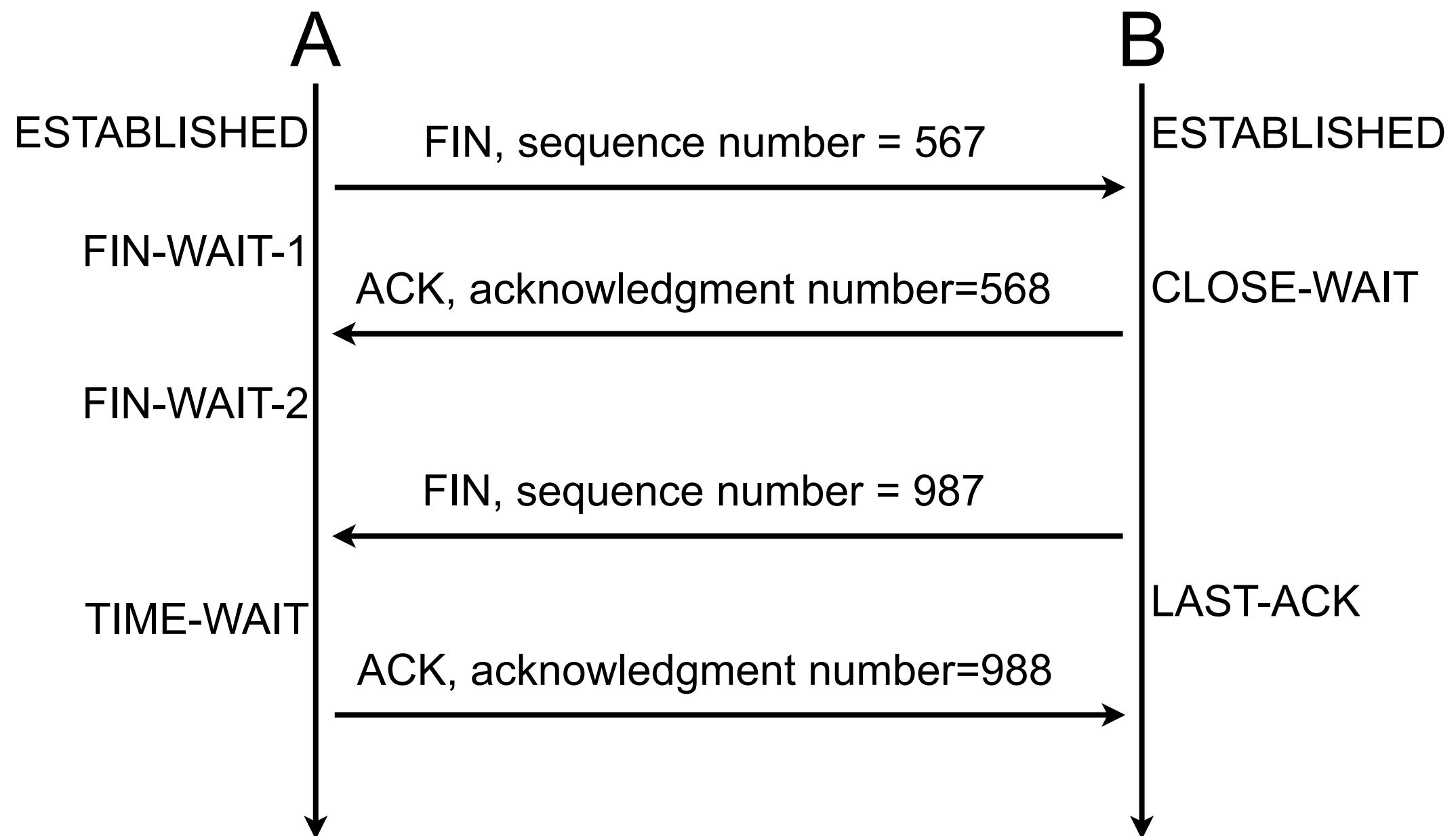
TCP connection termination



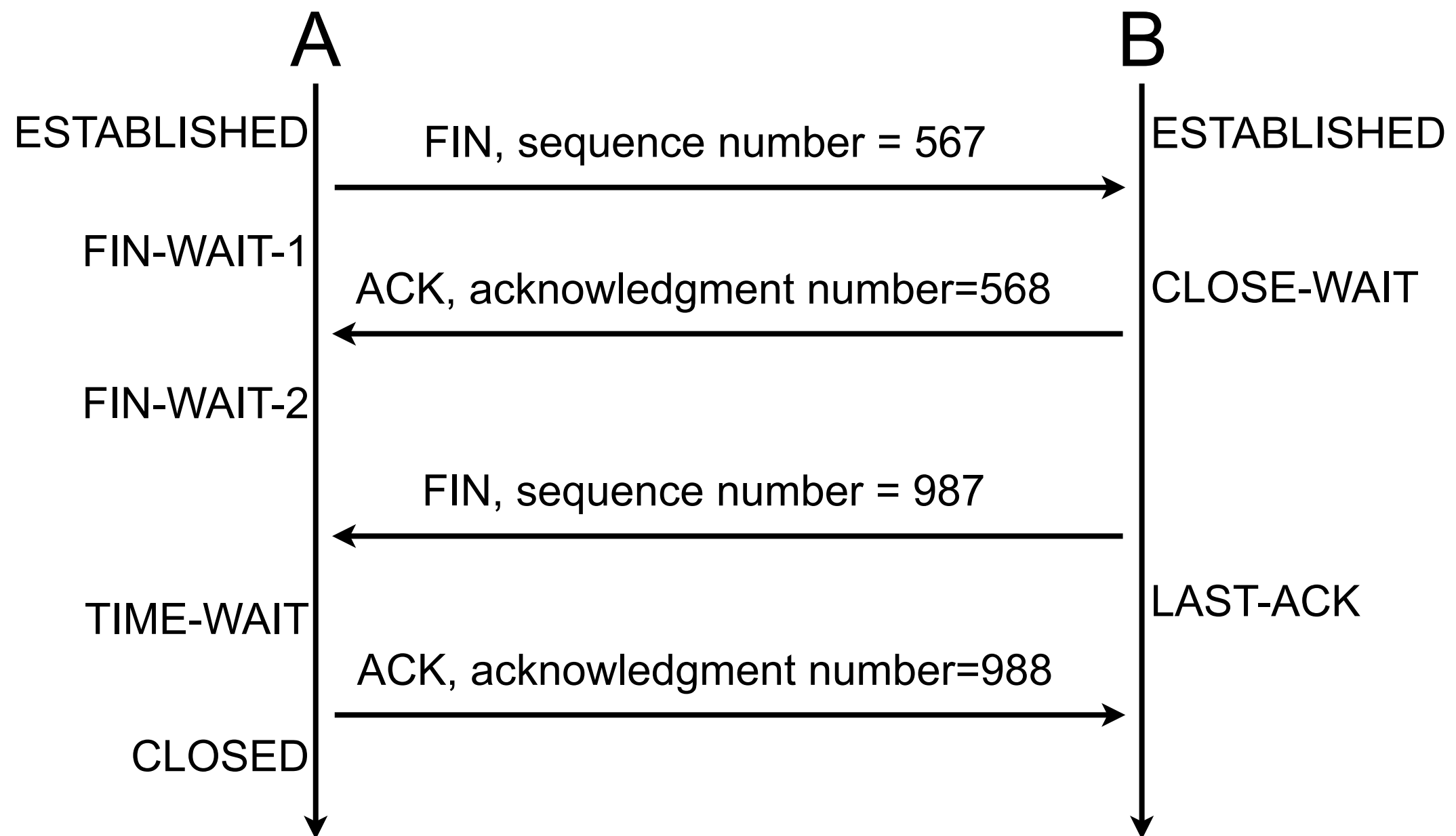
TCP connection termination



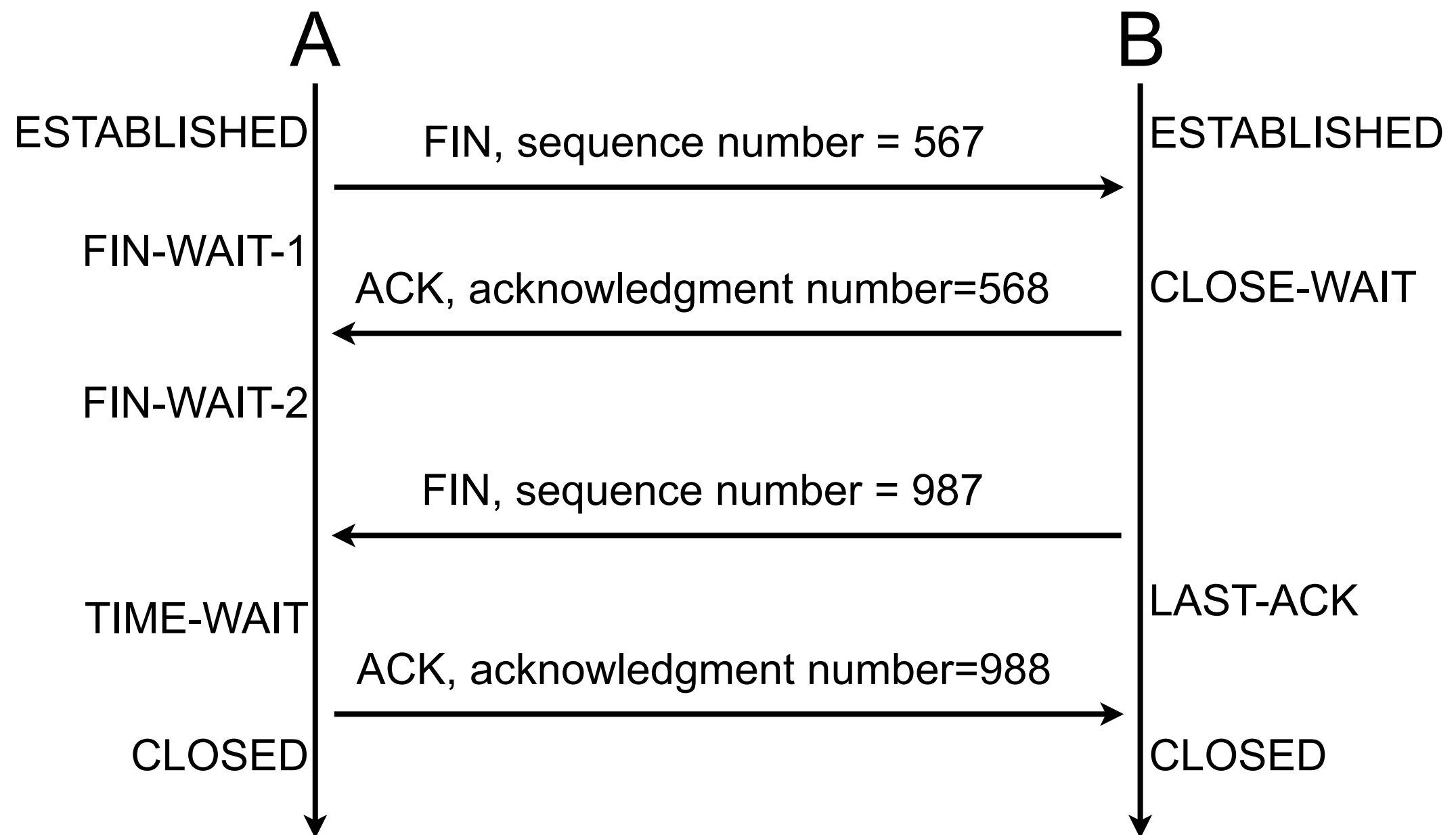
TCP connection termination



TCP connection termination

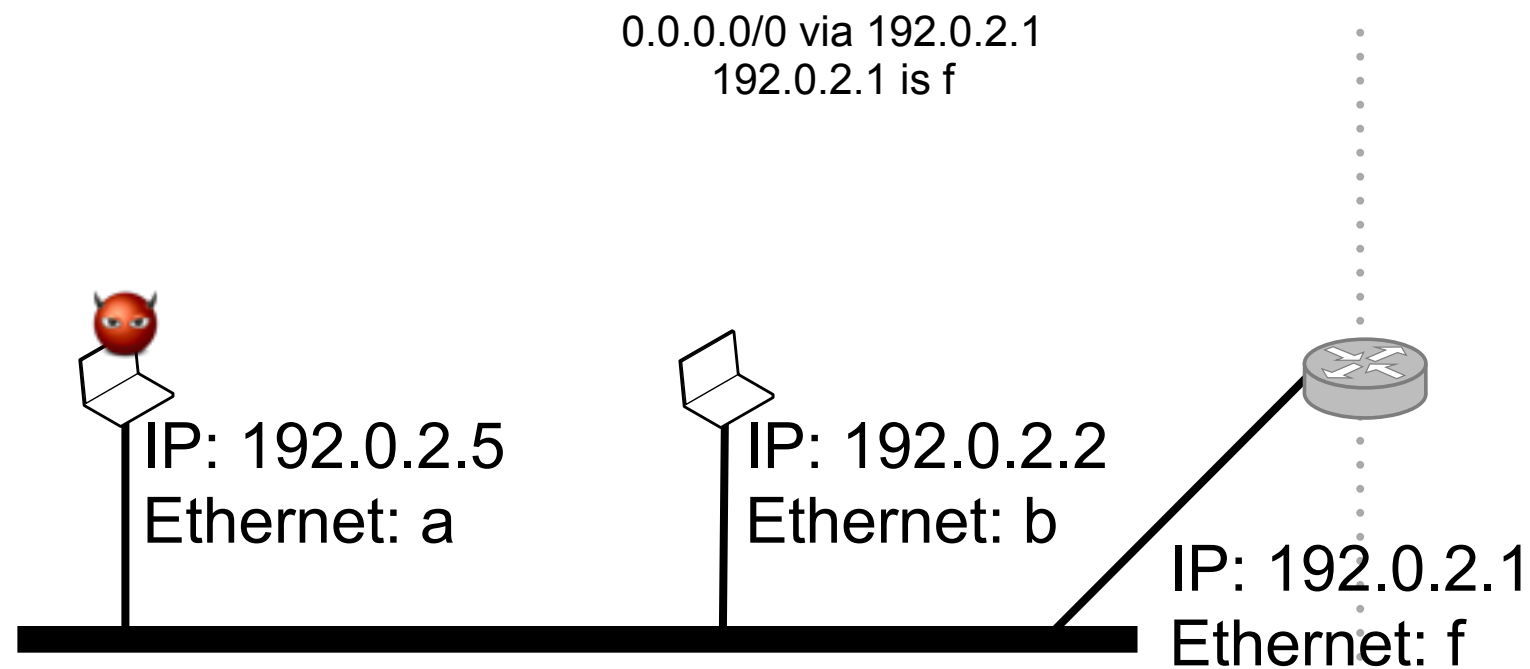


TCP connection termination

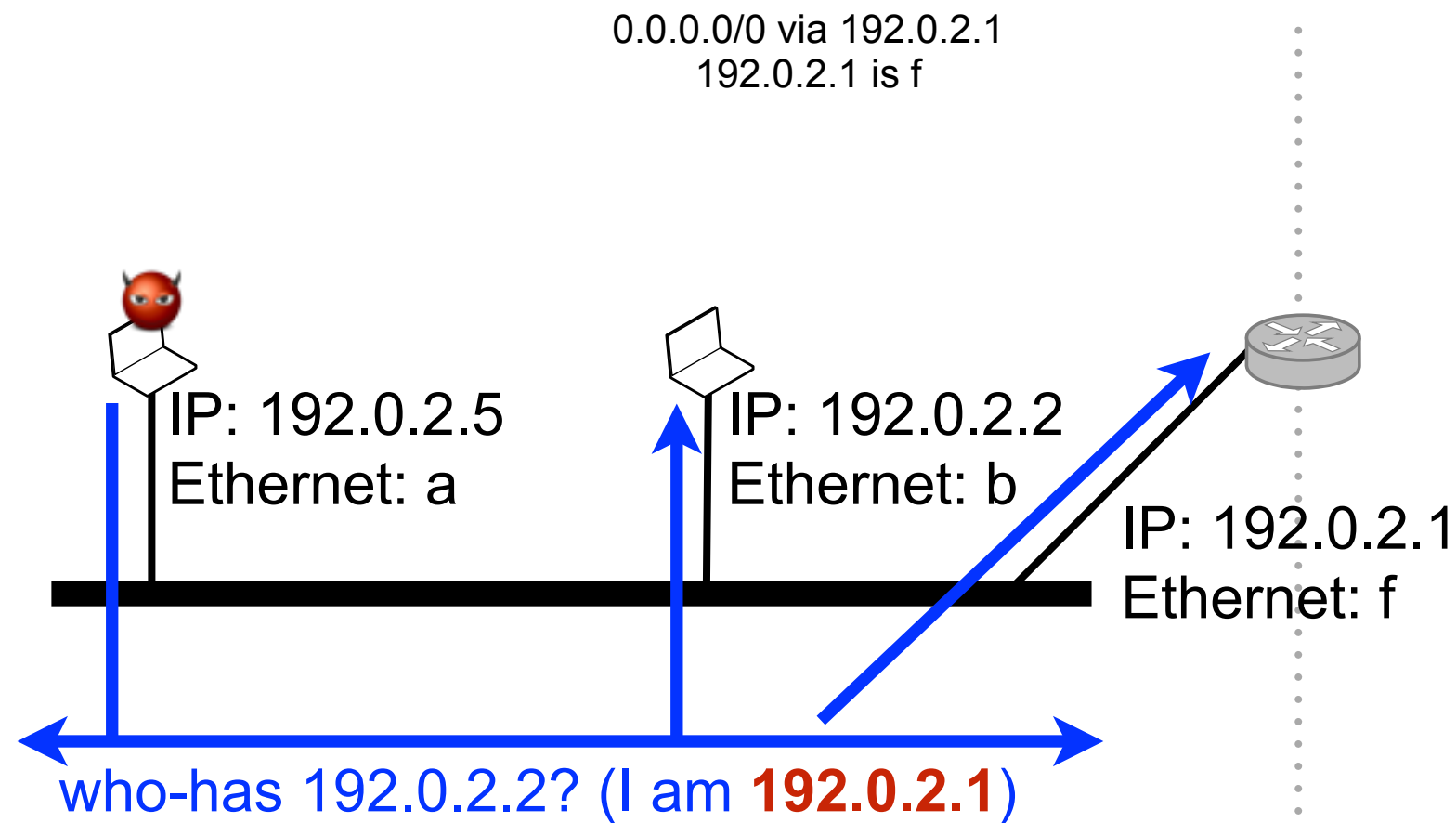


Threats by the example

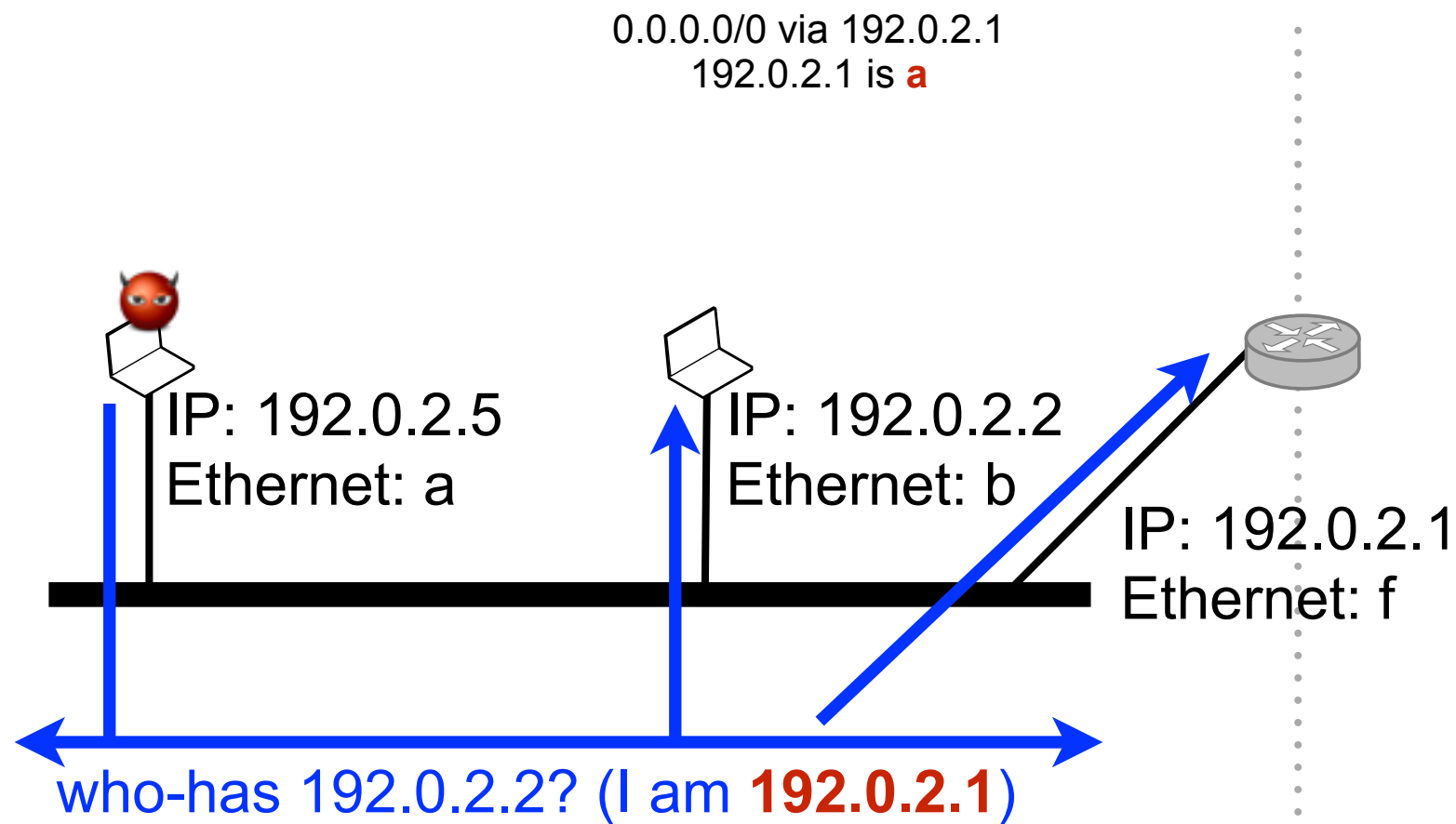
ARP poisoning



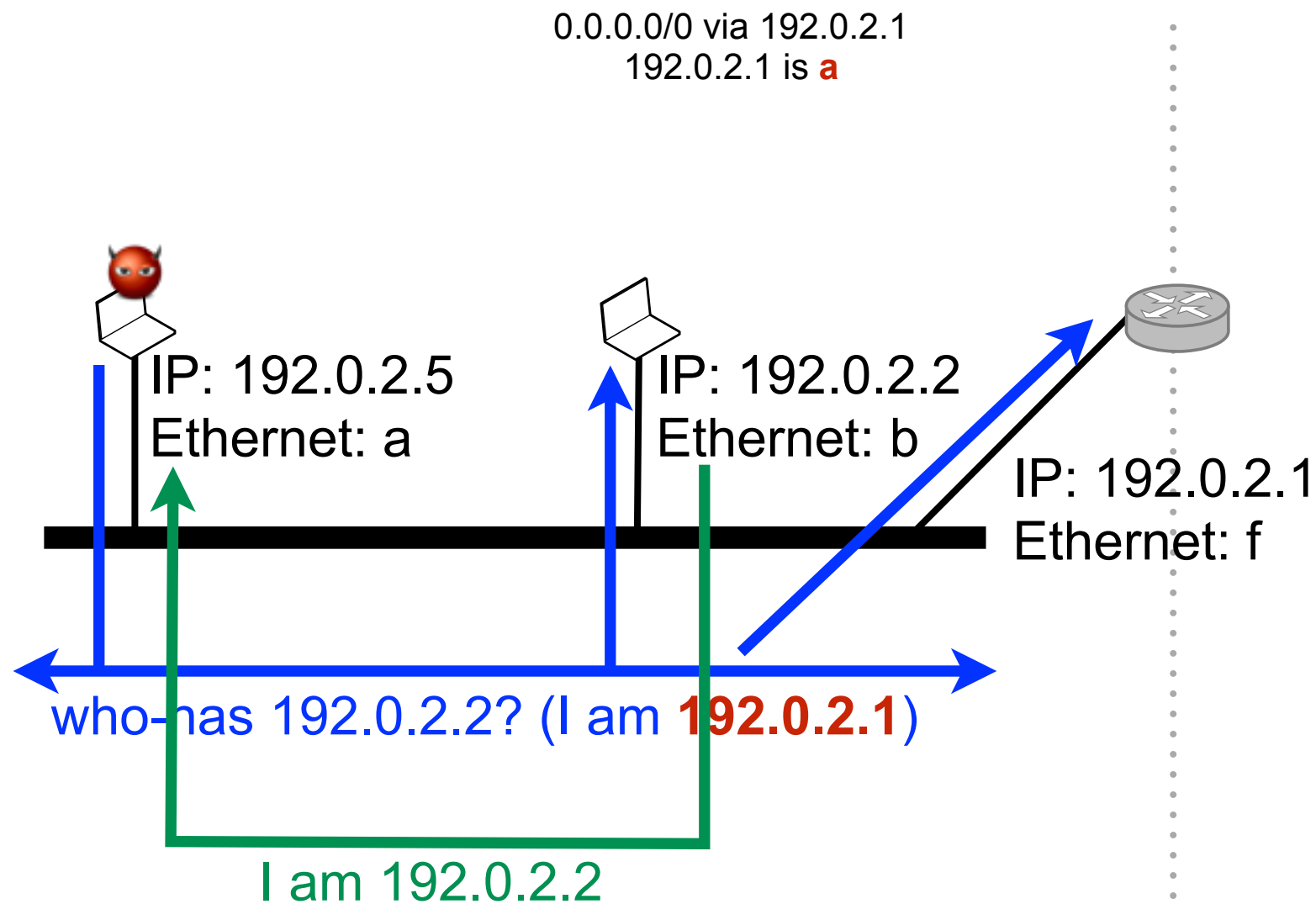
ARP poisoning



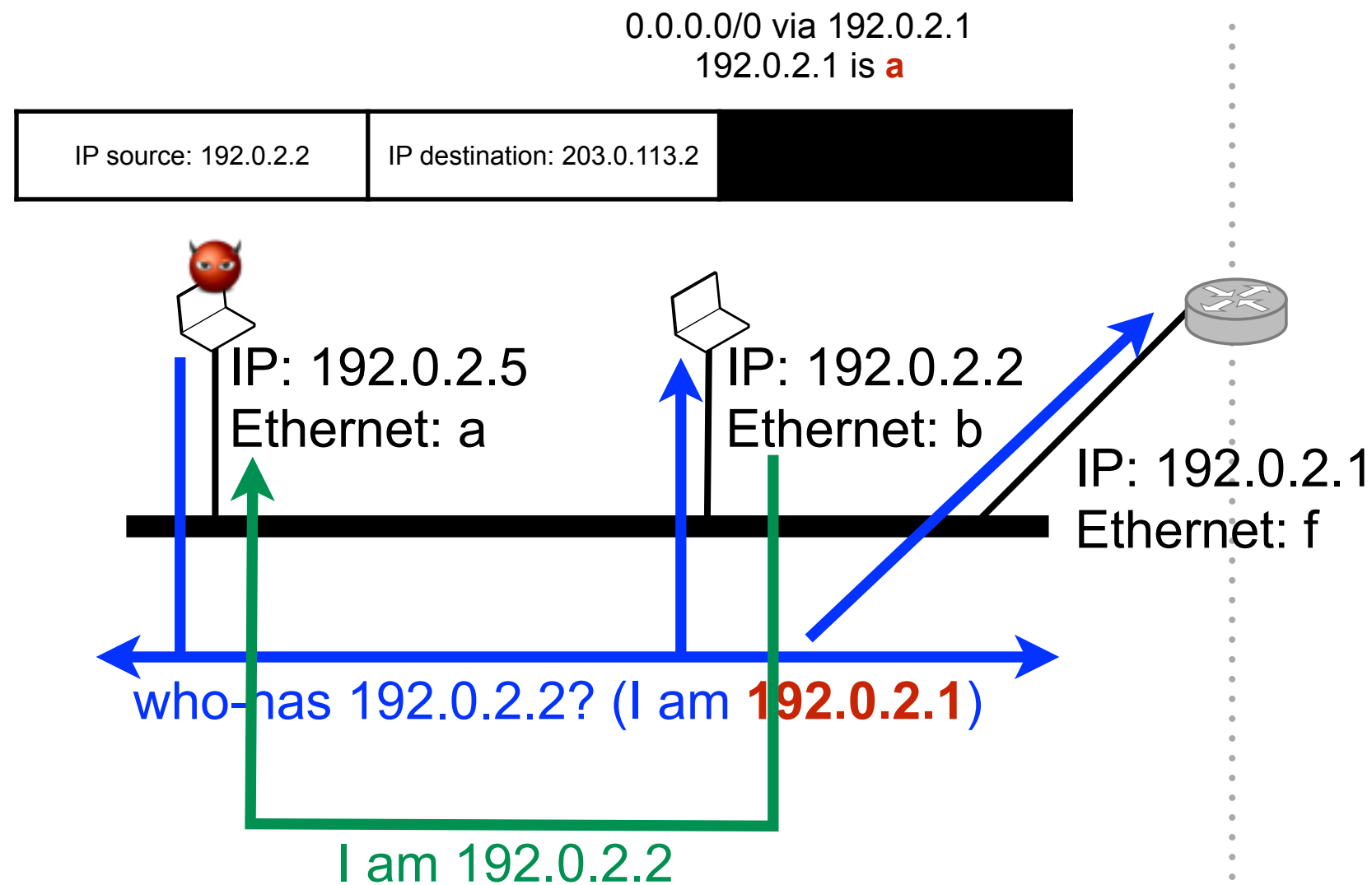
ARP poisoning



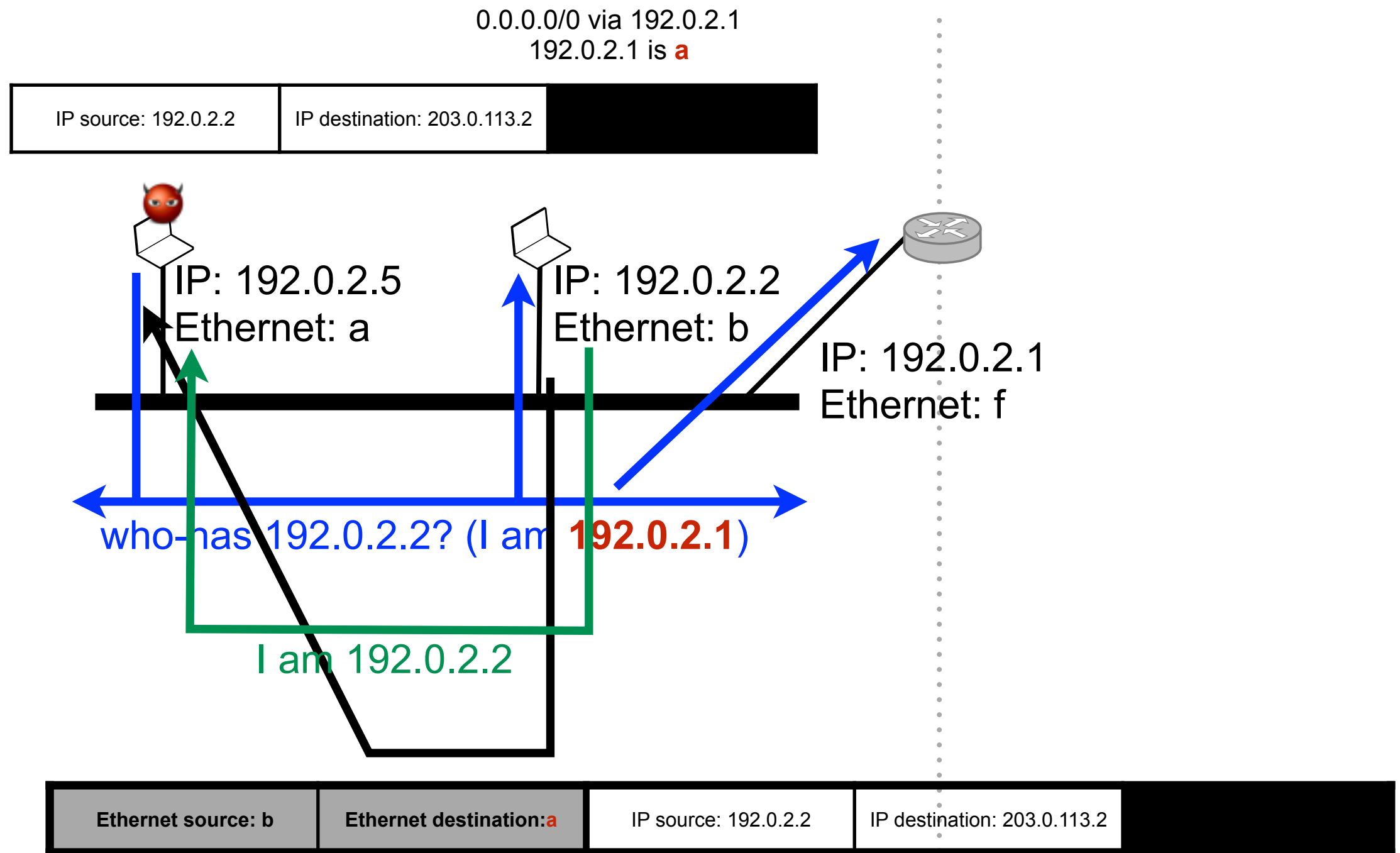
ARP poisoning



ARP poisoning



ARP poisoning

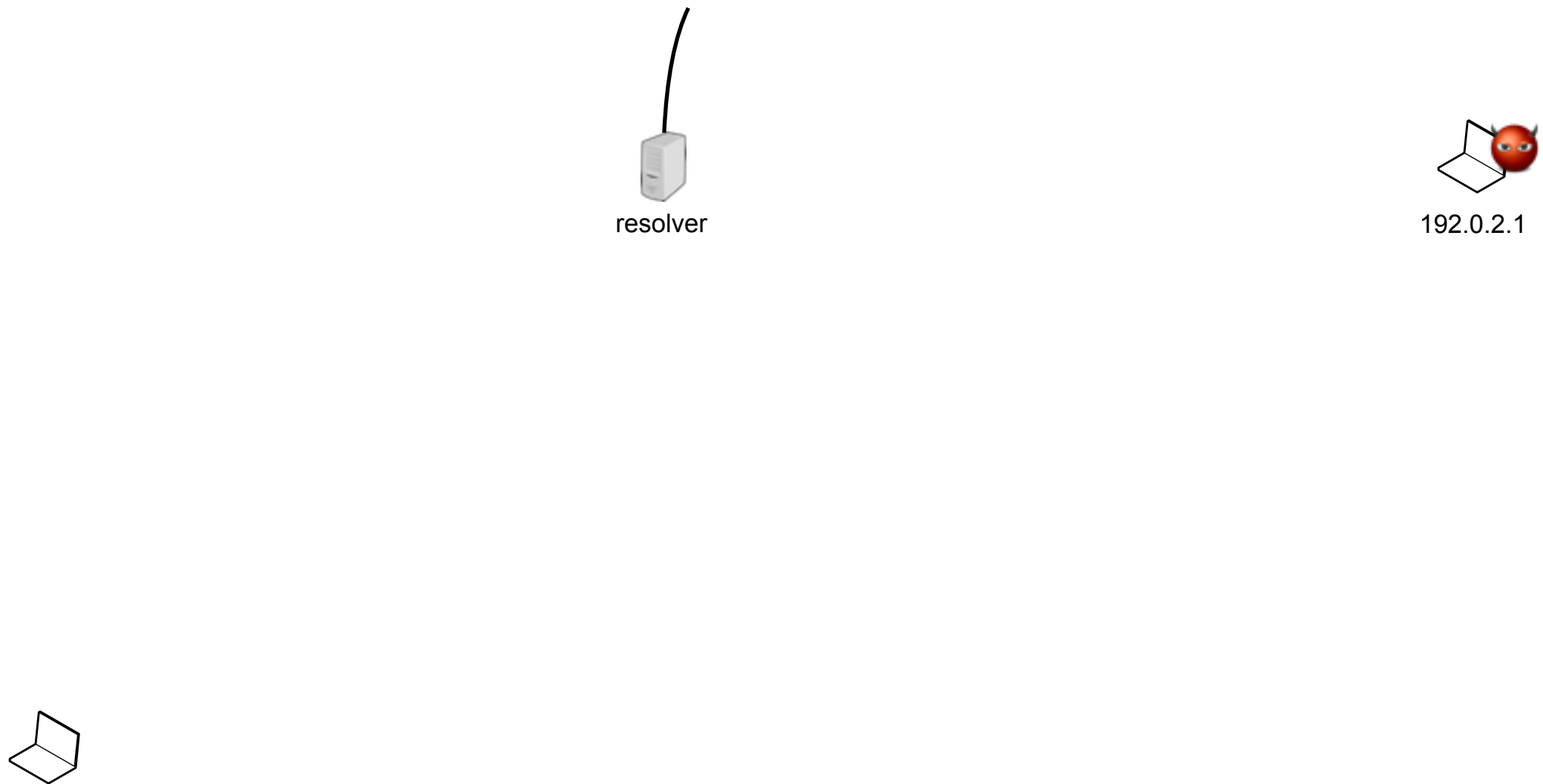


Why does it work?

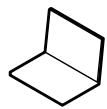
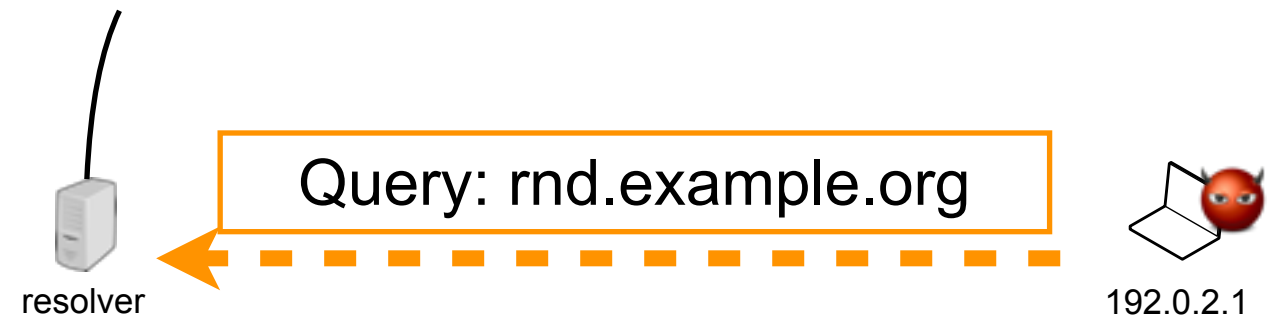
Why does it work?

- Conceptual vulnerability
 - using non-requested information as ground truth is dangerous
 - using non-authenticated information is dangerous

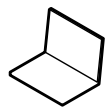
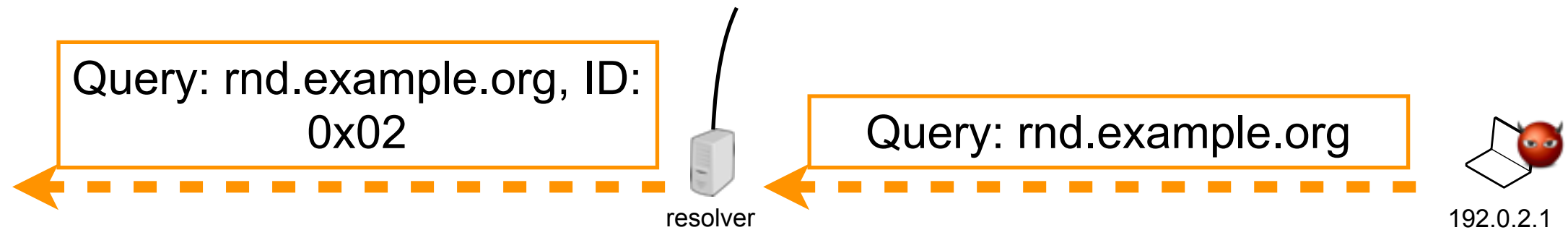
DNS cache poisoning



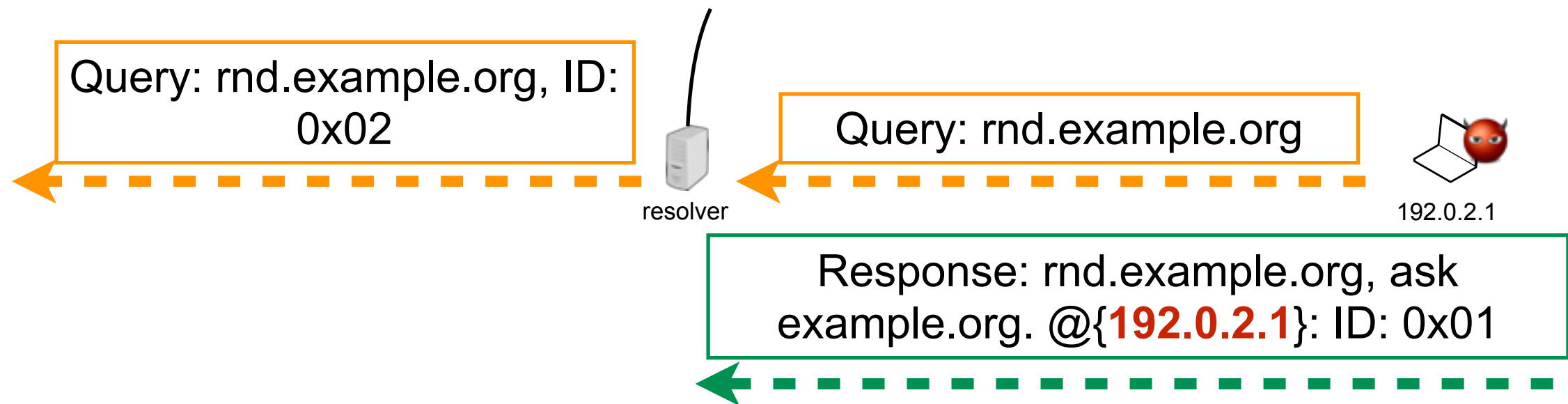
DNS cache poisoning



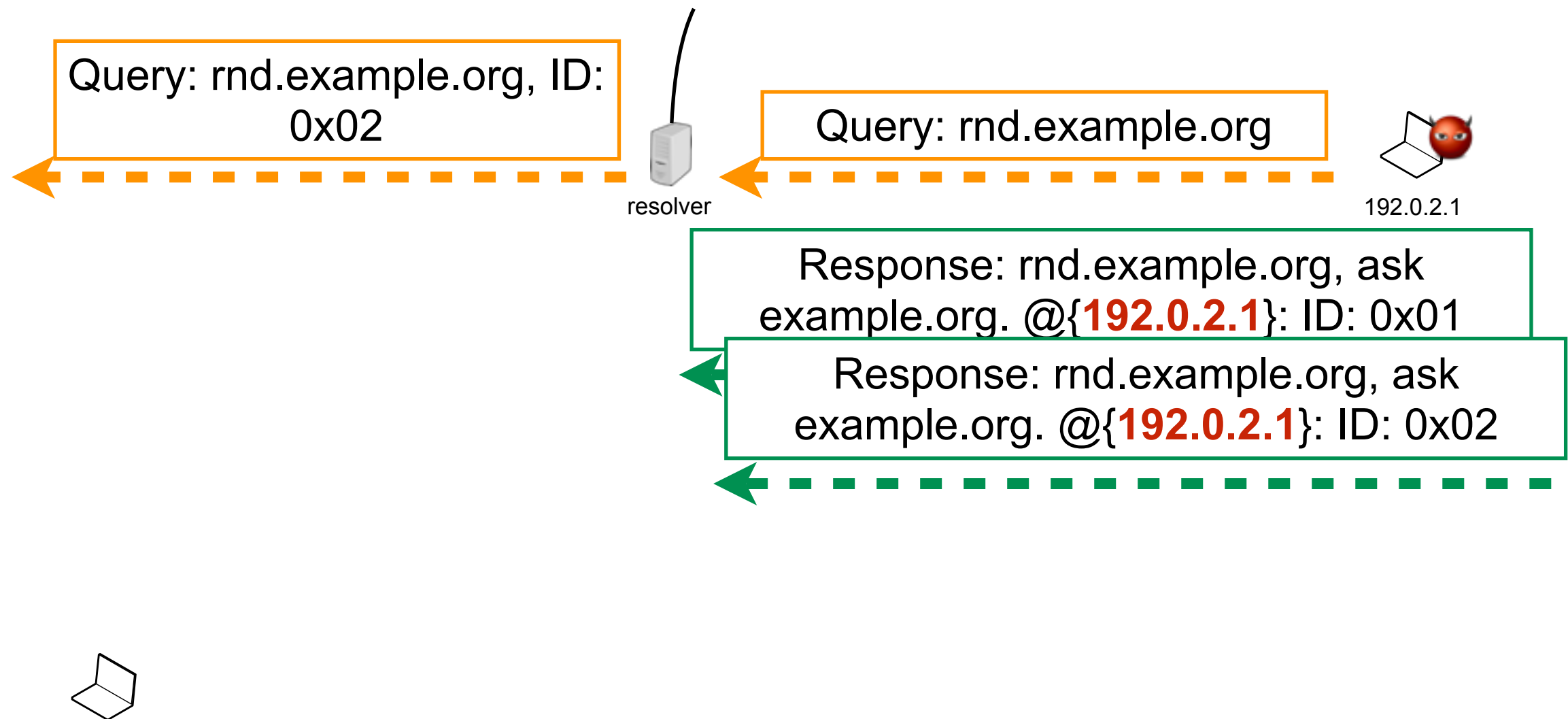
DNS cache poisoning



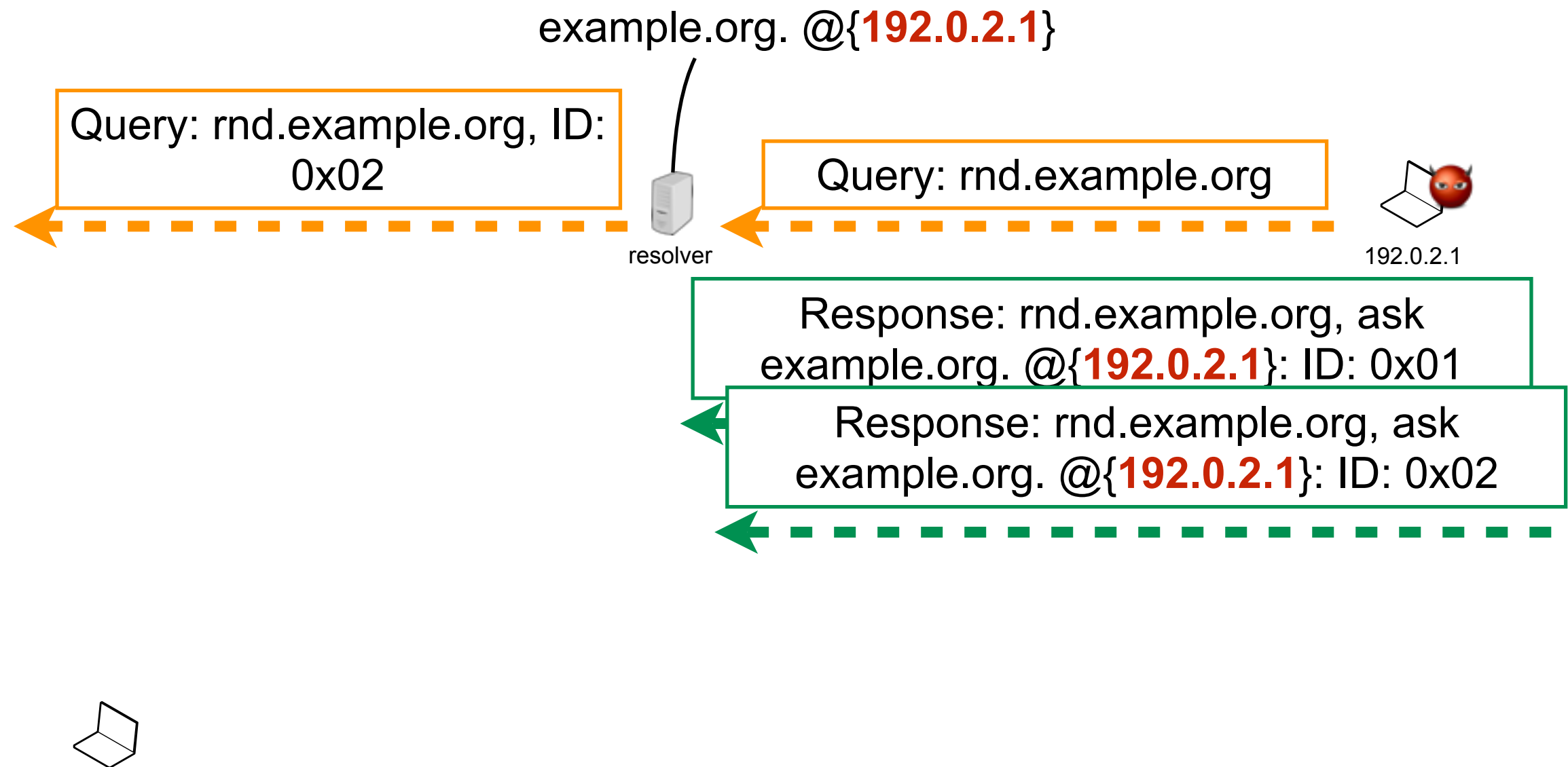
DNS cache poisoning



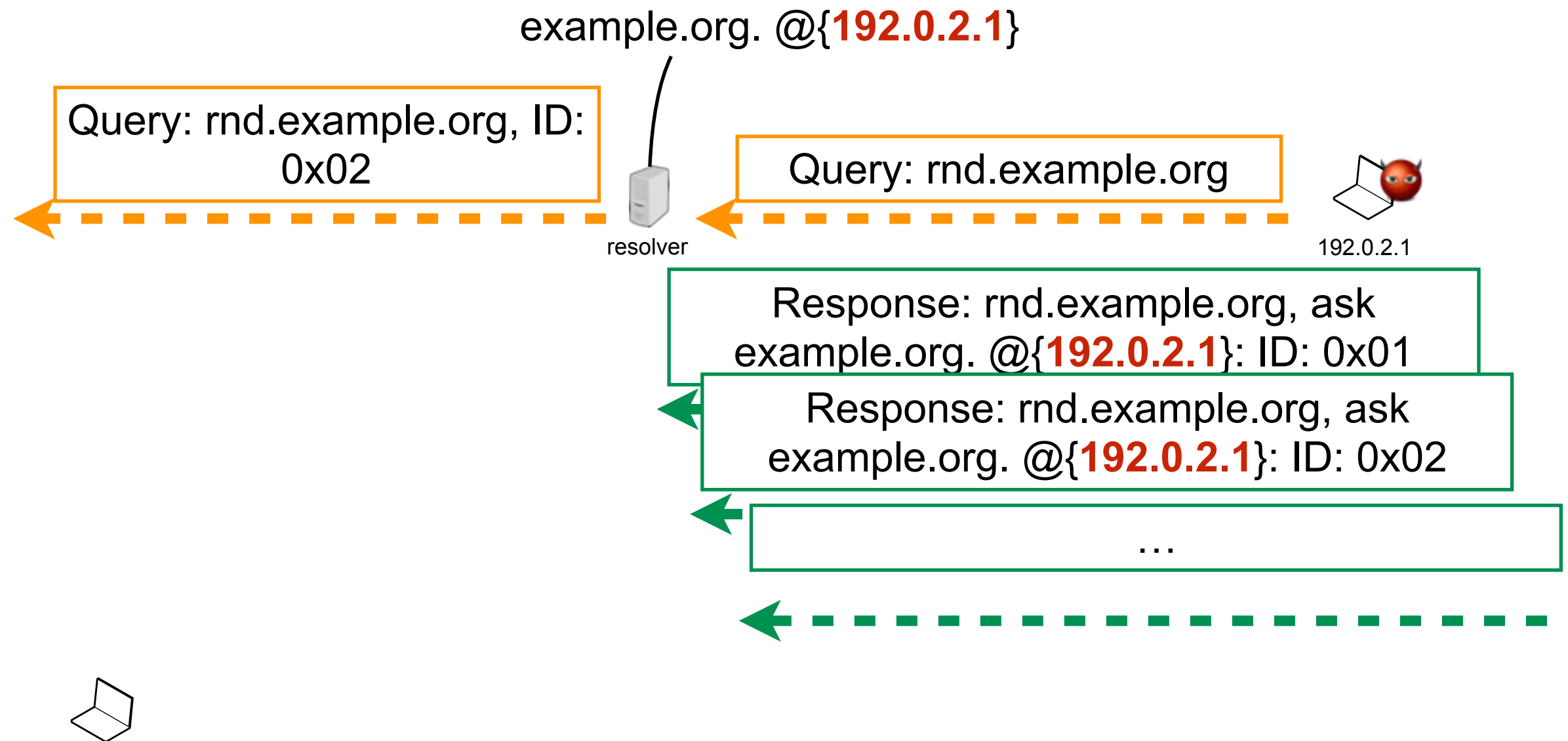
DNS cache poisoning



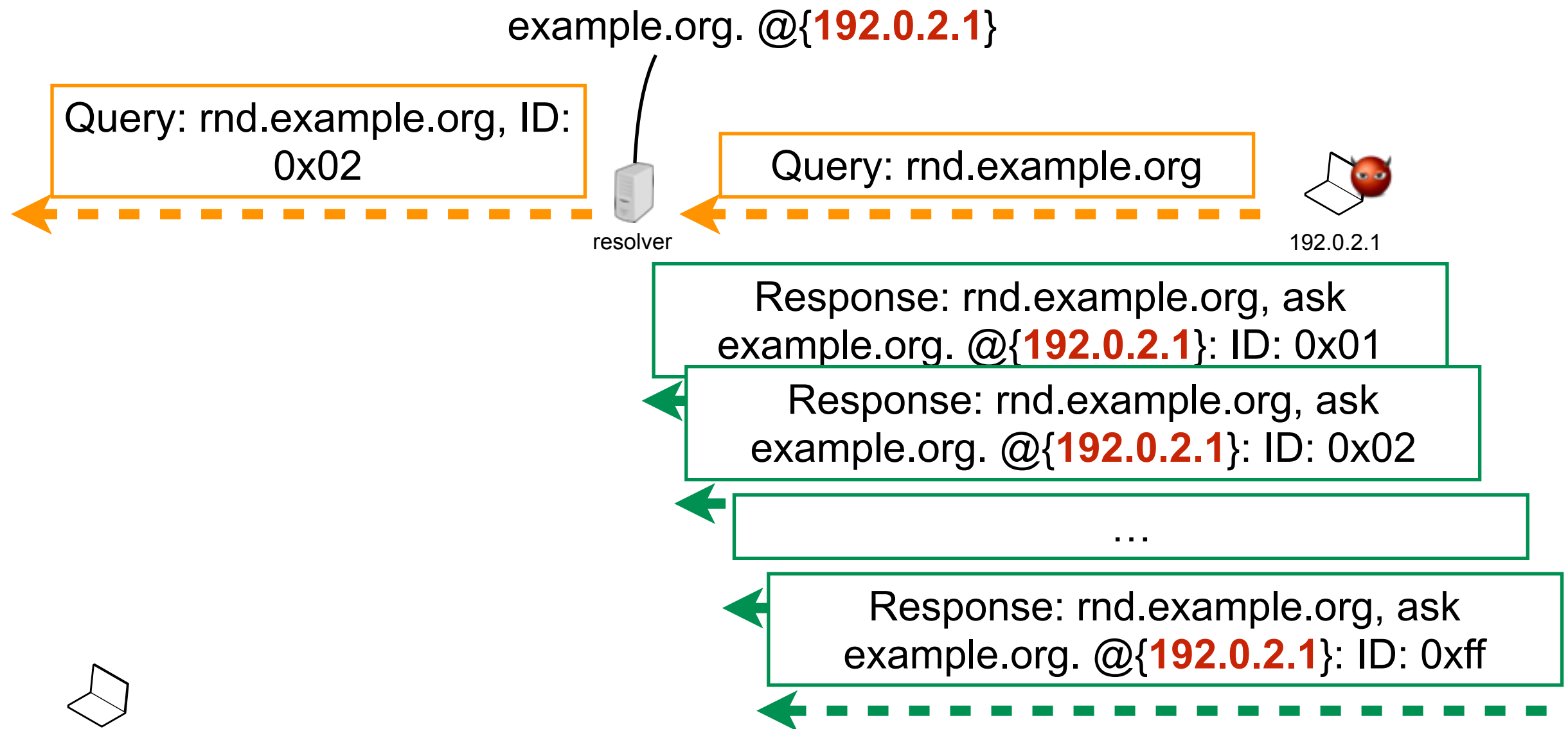
DNS cache poisoning



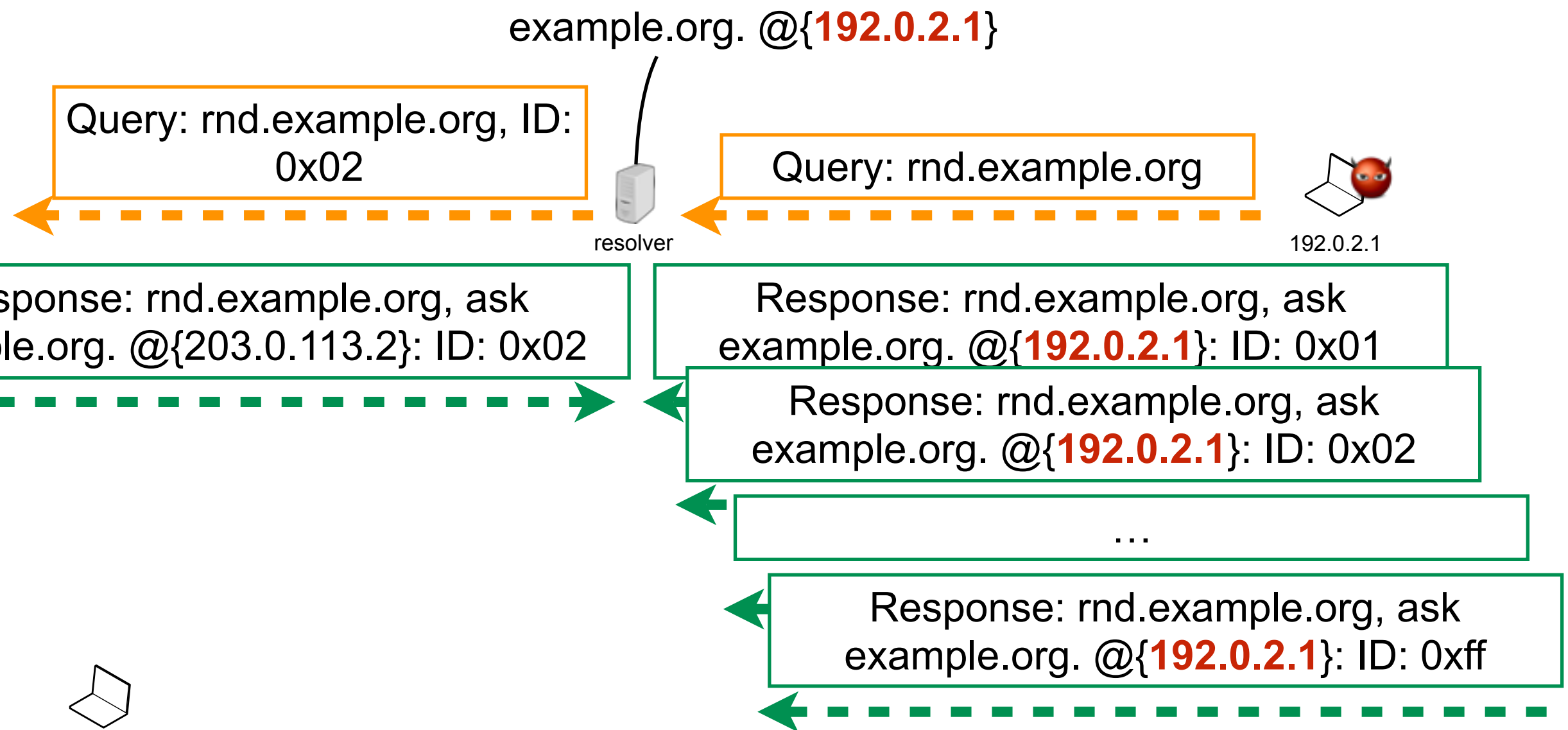
DNS cache poisoning



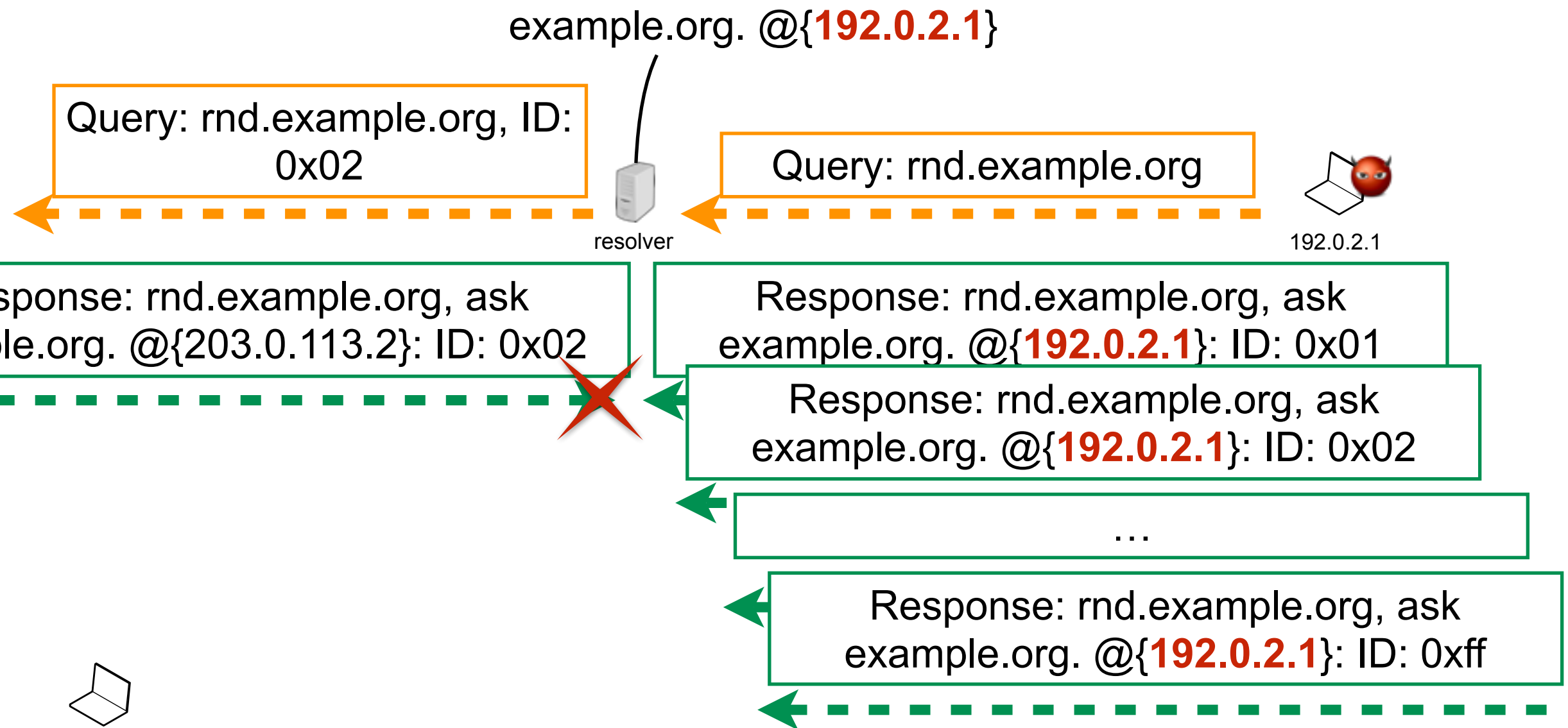
DNS cache poisoning



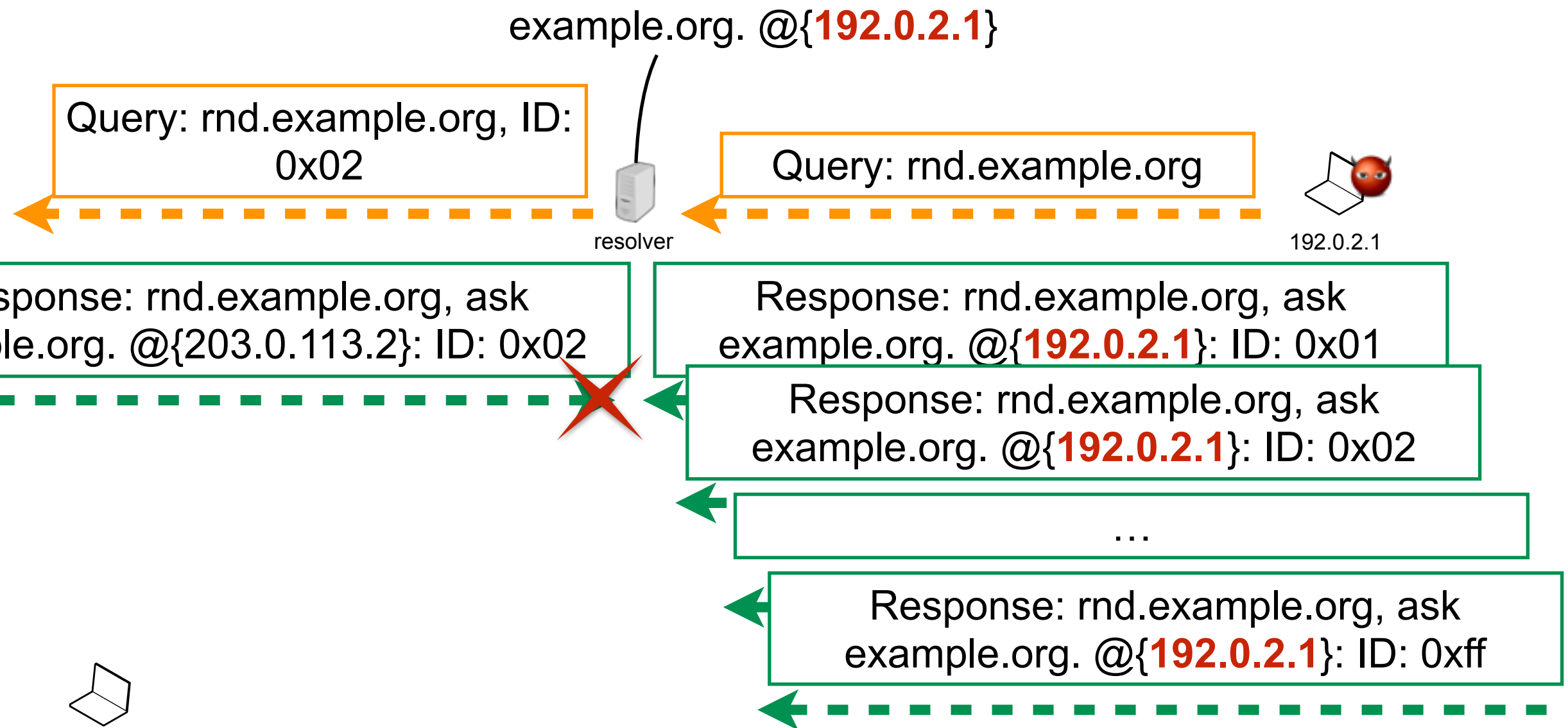
DNS cache poisoning



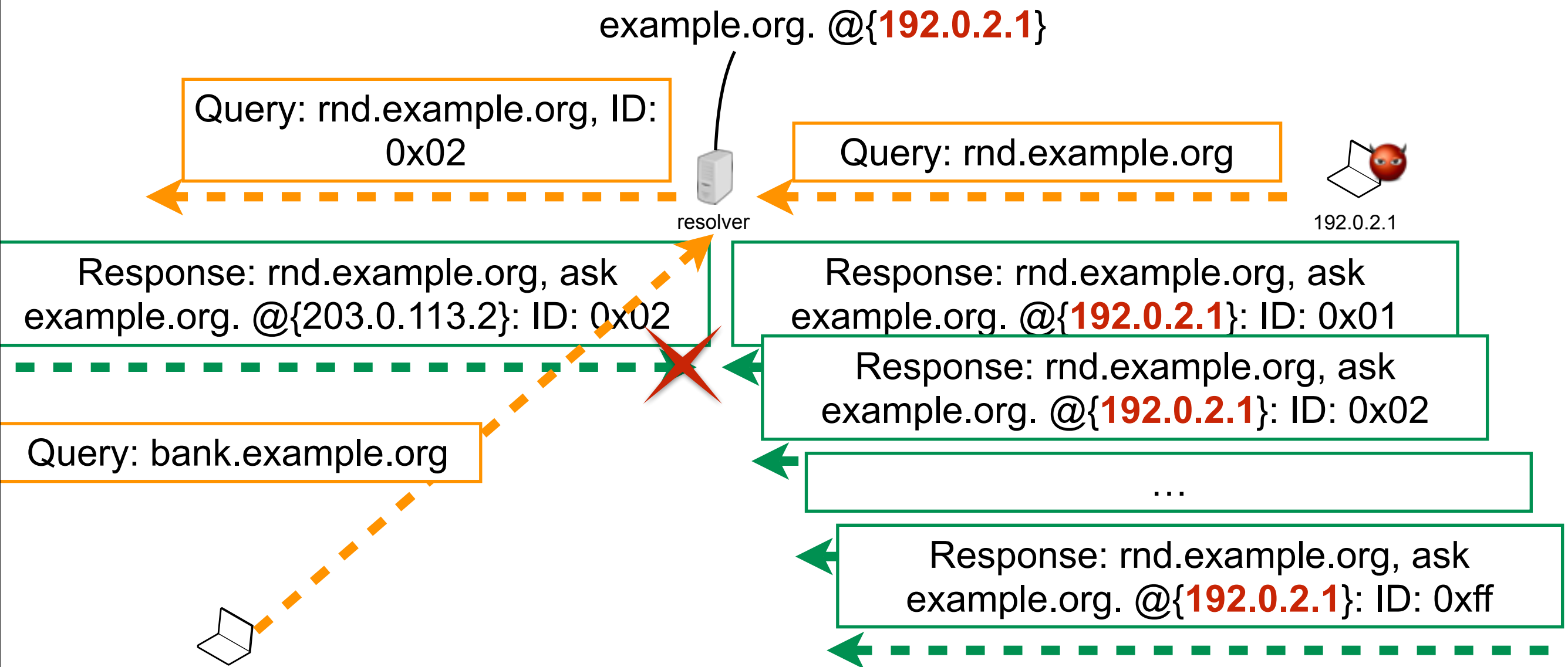
DNS cache poisoning



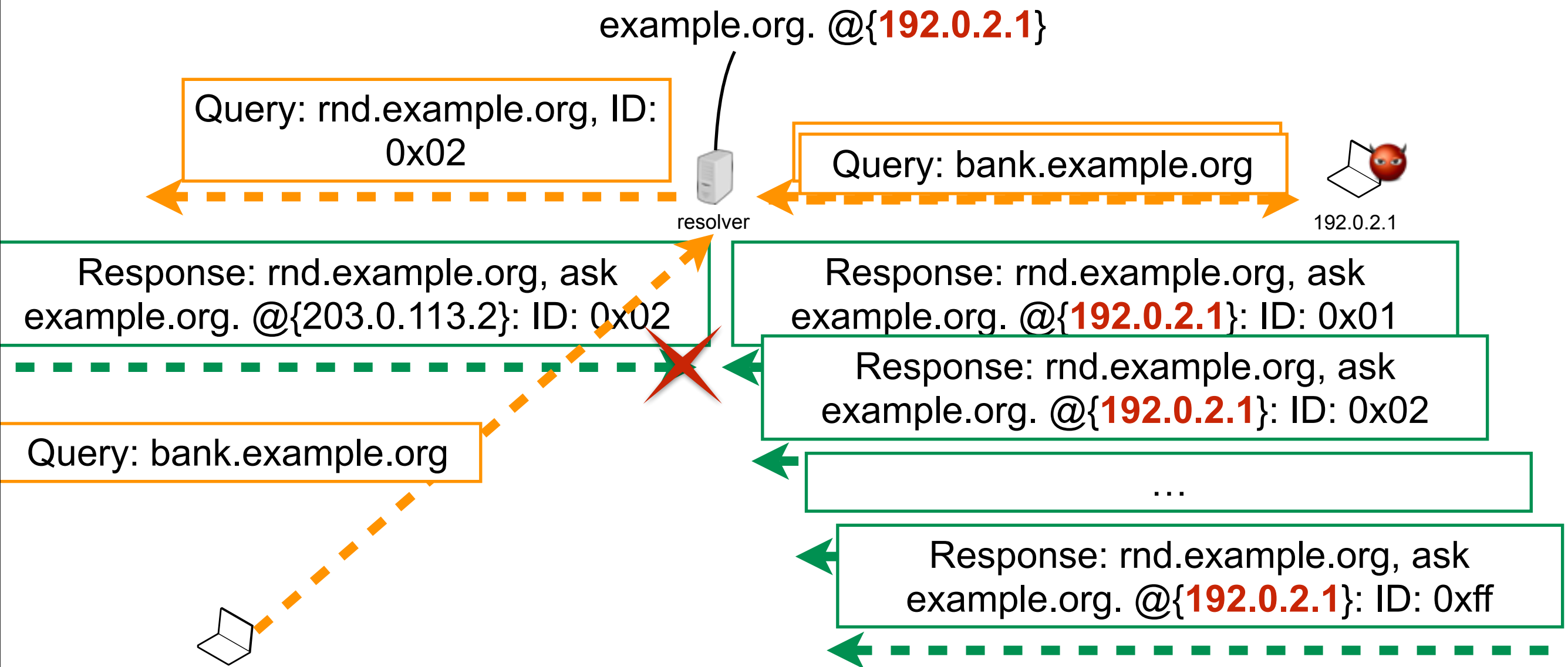
DNS cache poisoning



DNS cache poisoning



DNS cache poisoning

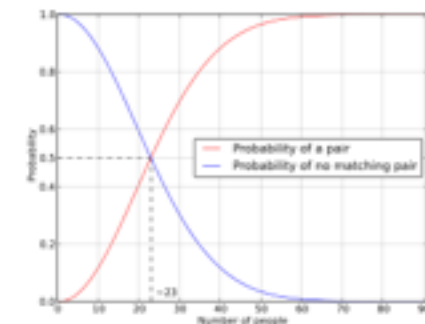


Why does it work?

Why does it work?

- Birthday paradox
 - probability that n elements uniformly picked from the finite set T is

$$p(n) = 1 - \frac{|T|!}{(|T| - n)!} \cdot \frac{1}{|T|^n}$$



- Relying solely on transaction ID is dangerous
 - particularly when IDs are small (16 bits in DNS)

YouTube Hijacking

- *BBC Breaking news: A router problem made YouTube inaccessible for many*
- *RIPE NIS: “On Sunday, 24 February 2008, Pakistan Telecom (AS17557) started an unauthorised announcement of the prefix 208.65.153.0/24. One of Pakistan Telecom's upstream providers, PCCW Global (AS3491) forwarded this announcement to the rest of the Internet, which resulted in the hijacking of YouTube traffic on a global scale”*

YouTube Hijacking (contd.)

YouTube Hijacking (contd.)

- **Before, during and after Sunday, 24 February 2008:** AS36561 (YouTube) announces 208.65.152.0/22.

YouTube Hijacking (contd.)

- **Before, during and after Sunday, 24 February 2008:** AS36561 (YouTube) announces **208.65.152.0/22**.
- **Sunday, 24 February 2008, 18:47 (UTC):** AS17557 (Pakistan Telecom) starts announcing **208.65.153.0/24**. AS3491 (PCCW Global) propagates the announcement. Routers around the world receive the announcement, and YouTube traffic is redirected to Pakistan.

YouTube Hijacking (contd.)

- **Before, during and after Sunday, 24 February 2008:** AS36561 (YouTube) announces **208.65.152.0/22**.
- **Sunday, 24 February 2008, 18:47 (UTC):** AS17557 (Pakistan Telecom) starts announcing **208.65.153.0/24**. AS3491 (PCCW Global) propagates the announcement. Routers around the world receive the announcement, and YouTube traffic is redirected to Pakistan.
- **Sunday, 24 February 2008, 20:07 (UTC):** AS36561 (YouTube) starts announcing **208.65.153.0/24**. [...] BGP decision process means that AS17557 (Pakistan Telecom) continues to attract some of YouTube's traffic.

YouTube Hijacking (contd.)

- **Before, during and after Sunday, 24 February 2008:** AS36561 (YouTube) announces **208.65.152.0/22**.
- **Sunday, 24 February 2008, 18:47 (UTC):** AS17557 (Pakistan Telecom) starts announcing **208.65.153.0/24**. AS3491 (PCCW Global) propagates the announcement. Routers around the world receive the announcement, and YouTube traffic is redirected to Pakistan.
- **Sunday, 24 February 2008, 20:07 (UTC):** AS36561 (YouTube) starts announcing **208.65.153.0/24**. [...] BGP decision process means that AS17557 (Pakistan Telecom) continues to attract some of YouTube's traffic.
- **Sunday, 24 February 2008, 20:18 (UTC):** AS36561 (YouTube) starts announcing **208.65.153.128/25** and **208.65.153.0/25**. Because of the longest prefix match rule, every router that receives these announcements will send the traffic to YouTube.

YouTube Hijacking (contd.)

- **Before, during and after Sunday, 24 February 2008:** AS36561 (YouTube) announces **208.65.152.0/22**.
- **Sunday, 24 February 2008, 18:47 (UTC):** AS17557 (Pakistan Telecom) starts announcing **208.65.153.0/24**. AS3491 (PCCW Global) propagates the announcement. Routers around the world receive the announcement, and YouTube traffic is redirected to Pakistan.
- **Sunday, 24 February 2008, 20:07 (UTC):** AS36561 (YouTube) starts announcing **208.65.153.0/24**. [...] BGP decision process means that AS17557 (Pakistan Telecom) continues to attract some of YouTube's traffic.
- **Sunday, 24 February 2008, 20:18 (UTC):** AS36561 (YouTube) starts announcing **208.65.153.128/25** and **208.65.153.0/25**. Because of the longest prefix match rule, every router that receives these announcements will send the traffic to YouTube.
- **Sunday, 24 February 2008, 20:51 (UTC):** All prefix announcements, including the hijacked /24 which was originated by AS17557 (Pakistan Telecom) via AS3491 (PCCW Global), are seen **prepended by another 17557**. The longer AS path means that more routers prefer the announcement originated by YouTube.

YouTube Hijacking (contd.)

- **Before, during and after Sunday, 24 February 2008:** AS36561 (YouTube) announces **208.65.152.0/22**.
- **Sunday, 24 February 2008, 18:47 (UTC):** AS17557 (Pakistan Telecom) starts announcing **208.65.153.0/24**. AS3491 (PCCW Global) propagates the announcement. Routers around the world receive the announcement, and YouTube traffic is redirected to Pakistan.
- **Sunday, 24 February 2008, 20:07 (UTC):** AS36561 (YouTube) starts announcing **208.65.153.0/24**. [...] BGP decision process means that AS17557 (Pakistan Telecom) continues to attract some of YouTube's traffic.
- **Sunday, 24 February 2008, 20:18 (UTC):** AS36561 (YouTube) starts announcing **208.65.153.128/25** and **208.65.153.0/25**. Because of the longest prefix match rule, every router that receives these announcements will send the traffic to YouTube.
- **Sunday, 24 February 2008, 20:51 (UTC):** All prefix announcements, including the hijacked /24 which was originated by AS17557 (Pakistan Telecom) via AS3491 (PCCW Global), are seen **prepended by another 17557**. The longer AS path means that more routers prefer the announcement originated by YouTube.
- **Sunday, 24 February 2008, 21:01 (UTC):** AS3491 (PCCW Global) **withdraws all prefixes originated by AS17557** (Pakistan Telecom), thus stopping the hijack of 208.65.153.0/24. Note that AS17557 was not completely disconnected by AS3491. Prefixes originated by other Pakistani ASs were still announced by AS17557 through AS3491.

Why does it work?

Why does it work?

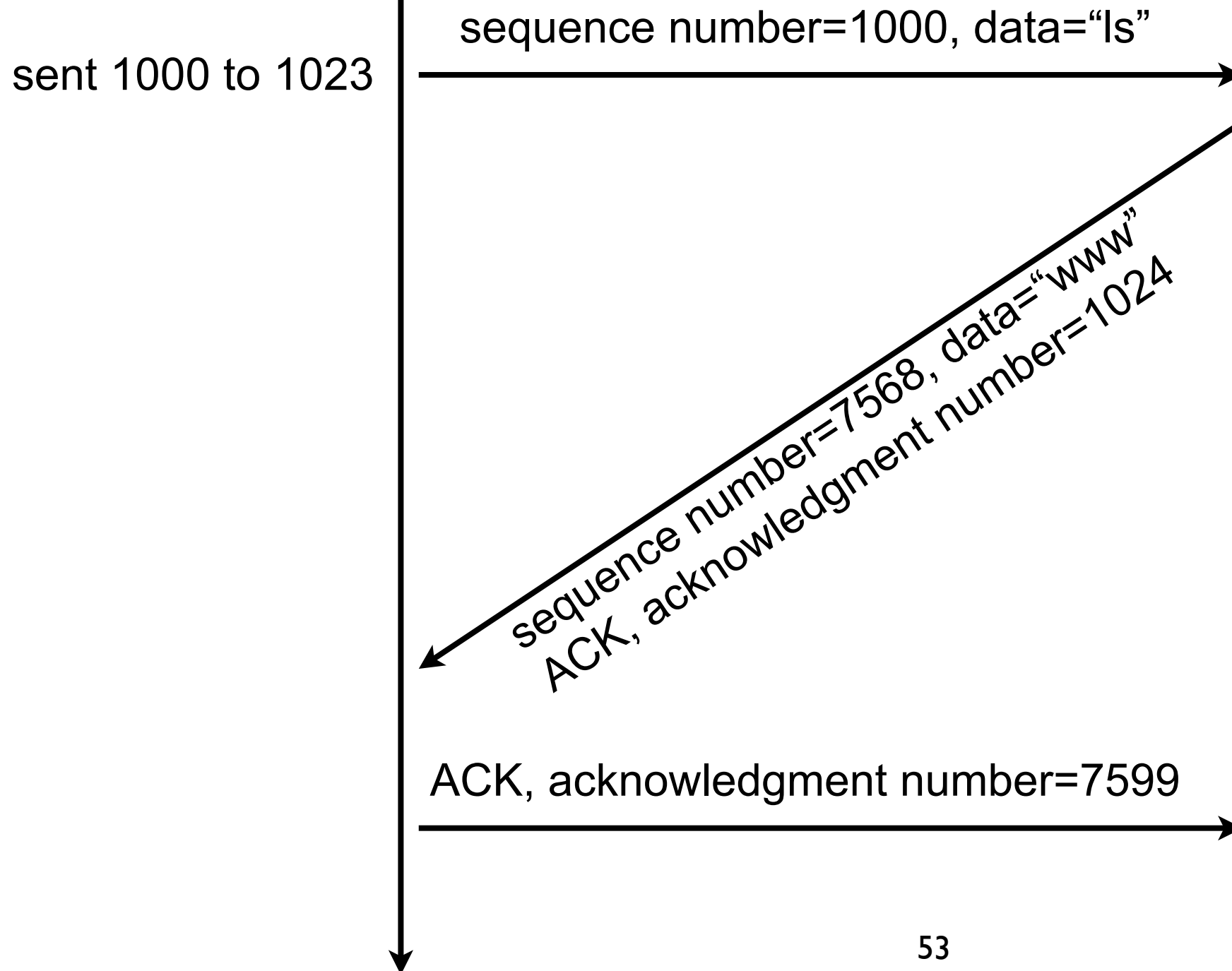
- Any AS can claim to be the originator of a prefix (i.e., she hijacks the prefix)
- To protect against that, only the import filters can be used
 - rely on databases that are not so accurate
- A not secure global routing system is a major threat against freedom

TCP session hijacking

window size = 1500B

Client

Telnet server

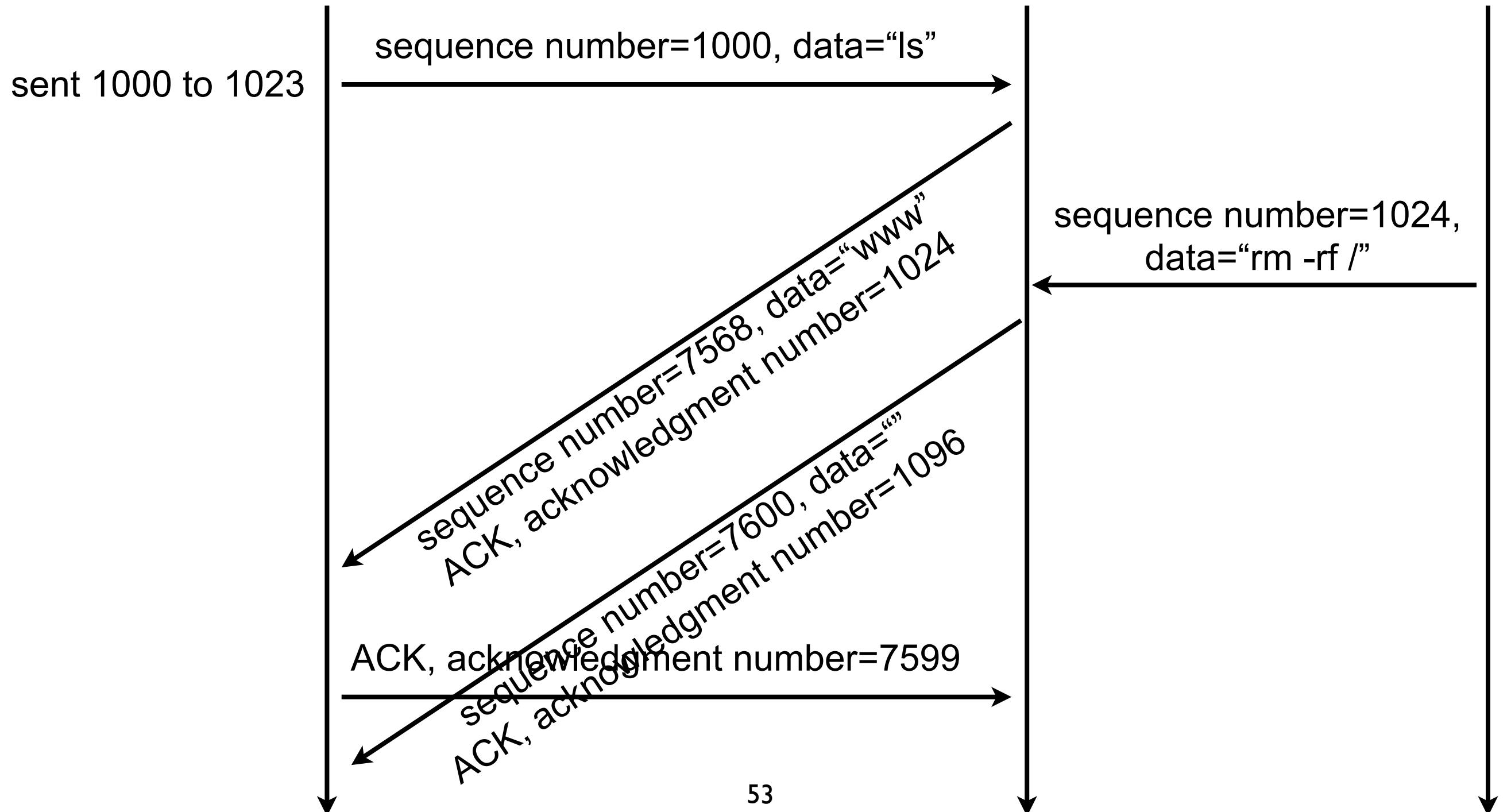


TCP session hijacking

window size = 1500B

Client

Telnet server



Why does it work?

Why does it work?

- If the attacker can
 - guess the initial sequence number
 - guess actions from the sender
- then easy to guess a sequence number that will be accepted by the receiver

The basics of security

Security threats

- Intrusion
 - an attacker gains remote access to some resources that are normally denied to her
 - e.g., steal processing power, botnets
- Eavesdropping
 - an attacker collects traffic of a target in order to gain access to restricted sensitive information
 - e.g., steal passwords by sniffing wireless traffic
- Denial of Service (DoS)
 - an attacker disrupts a specific targeted service
 - e.g., block the youtube website

The attackers

- Hackers
 - look for challenge, notoriety, and fun
 - e.g., hackers, script kiddies, students :-D
- Spies
 - look for political/business gains
 - e.g., intelligence, police, industrial spies
- Criminals
 - look for financial gains, religious/political visibility, or just to break something
 - e.g., criminals, terrorists, vandals

Definitions

- Key
 - input of cryptographic functions to determine its output
- Authentication
 - proof that the message is coming from the one claiming to be at the origin of the message
- Integrity
 - proof that the message has not been altered since its creation
- Non-repudiation of origin
 - an entity that generated a message cannot deny have generated the message
- Encryption
 - action of encoding of a message such that an eavesdropper can't read the message but legitimate destination can
- Decryption
 - action of decoding an encrypted message
- Signature
 - a mathematically constructed proof of authenticity of a message

Hall of fame

- Alice and Bob
 - are legitimate users, Alice and Bob exchange messages
- Chuck
 - is a malicious user that is not between Alice and Bob
- Eve
 - is a malicious user that can eavesdrop
- Trudy
 - is a malicious user that can perform (wo)man-in-the-middle attacks
- Trent
 - is a legitimate user that plays the role of a trusted arbitrator

Why is good security level so hard to obtain?

- The security level of a system equals the security level of the weakest part of the system
 - e.g., encrypting your HDD to avoid information leak if the laptop is stolen is useless if the password is written on a post-it attached on the laptop
- Digital system are complexes
 - interactions with many components, distribution, easily bugged...

Security is a tradeoff

- Compare cost and probability of an attack and cost of securing the system against this attack
 - e.g., is that necessary to make data unbreakable for 20 years if they are outdated after 1 hour?
- Explain the security systems and their reasons
 - if a user does not understand why he must follow a procedure, he will not follow it
 - e.g., how many of you already give their password to someone else?
- Never “over-secure” a system
 - if the system is too hard to use, people will find countermeasure
 - e.g., too hard to use corporate mails? Then use gmail to send corporate mails...

Security is a tradeoff (contd.)

- Protection system
 - lifetime = 10 years
 - cost = 10,000 EUR
- Attack
 - yearly probability = 10%
 - cost of restoring the system = 1,000 EUR
- Do I invest?

Procedures!

- Protection will never be perfect
- Prepare procedures
 - what to do BEFORE an attack?
 - what to do to limit the risk (e.g., passwords) of attack and to be ready if an attack happens (e.g., backup)
 - what to do DURING an attack?
 - the attack is on going, how to stop it
 - what to do AFTER an attack?
 - the attack succeeded, how to recover from it

Securing communications

Objective

- Construct a communication mechanism where Alice and Bob can exchange messages such that
 - only Alice and Bob can generate messages
 - nobody else than Alice or Bob can read messages
 - nobody can alter messages

Steps

- fill me
- fill me
- fill me

Hash function

- Validate that a message has not been altered on its way between Alice and Bob
- Hash functions map arbitrary large numbers of variable length to fixed-length numbers
 - $h = H(m)$, h is called hash or digest
 - e.g., MD5, SHA-1, SHA-256
- Good hash functions for cryptography must be such that
 - $H(m)$ is not complex to compute
 - but finding a m_2 such that $H(m_2) = H(m)$ is complex,
 - $H(m)$ is deterministic,
 - H output must be evenly distributed over the output set
- Example
 - SHA-1 maps messages its input space on a 160-bits output
 - $\text{SHA-1}(\text{Message to validate}) = 5e06ee754bda0d33cf65ec305ffc779404e66029$
 - $\text{SHA-1}(\text{Message to validate}) = b1c306f8cb792fa14d4d1fdc6f37d86c2fe6bb9$

Is that enough?

Alice



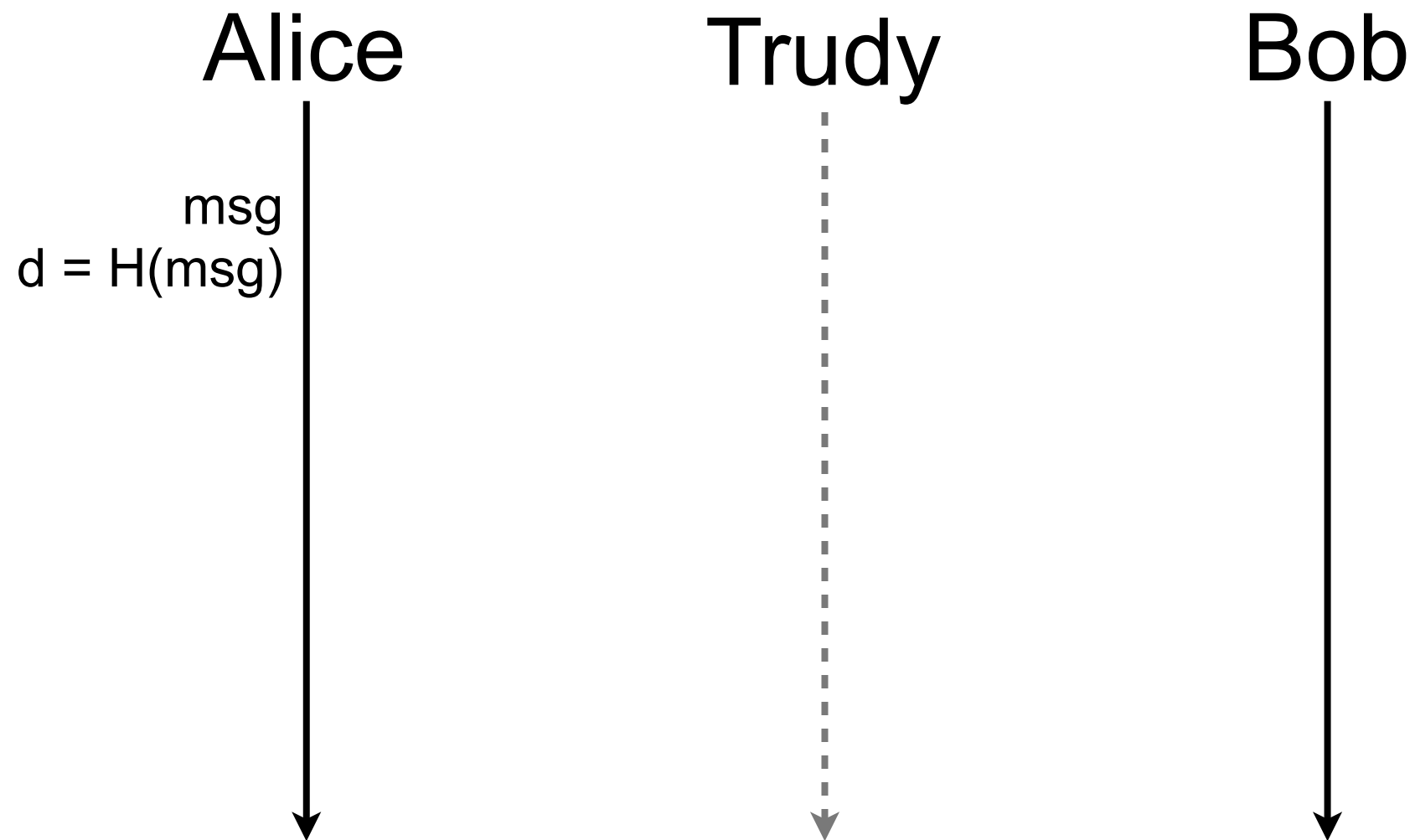
Trudy



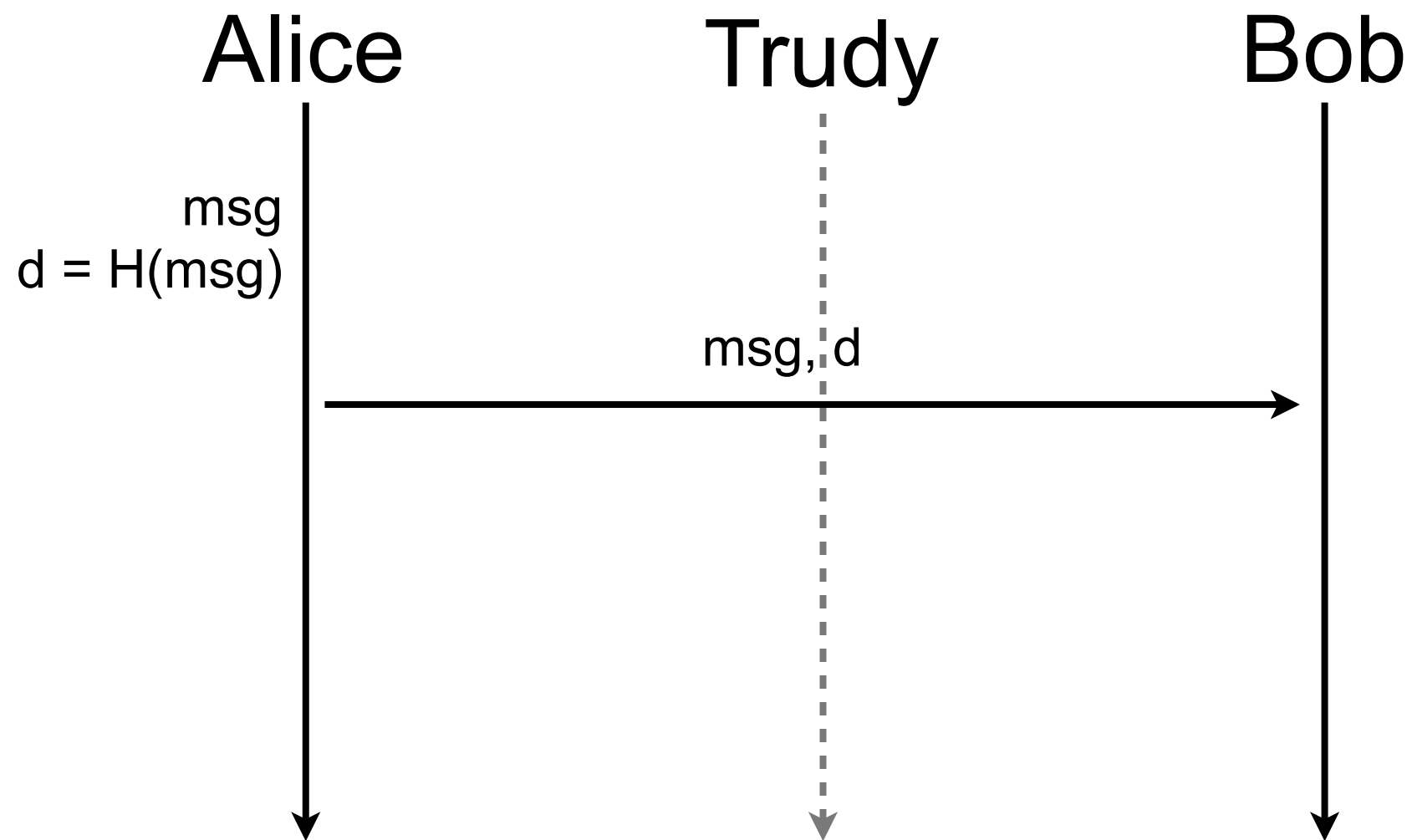
Bob



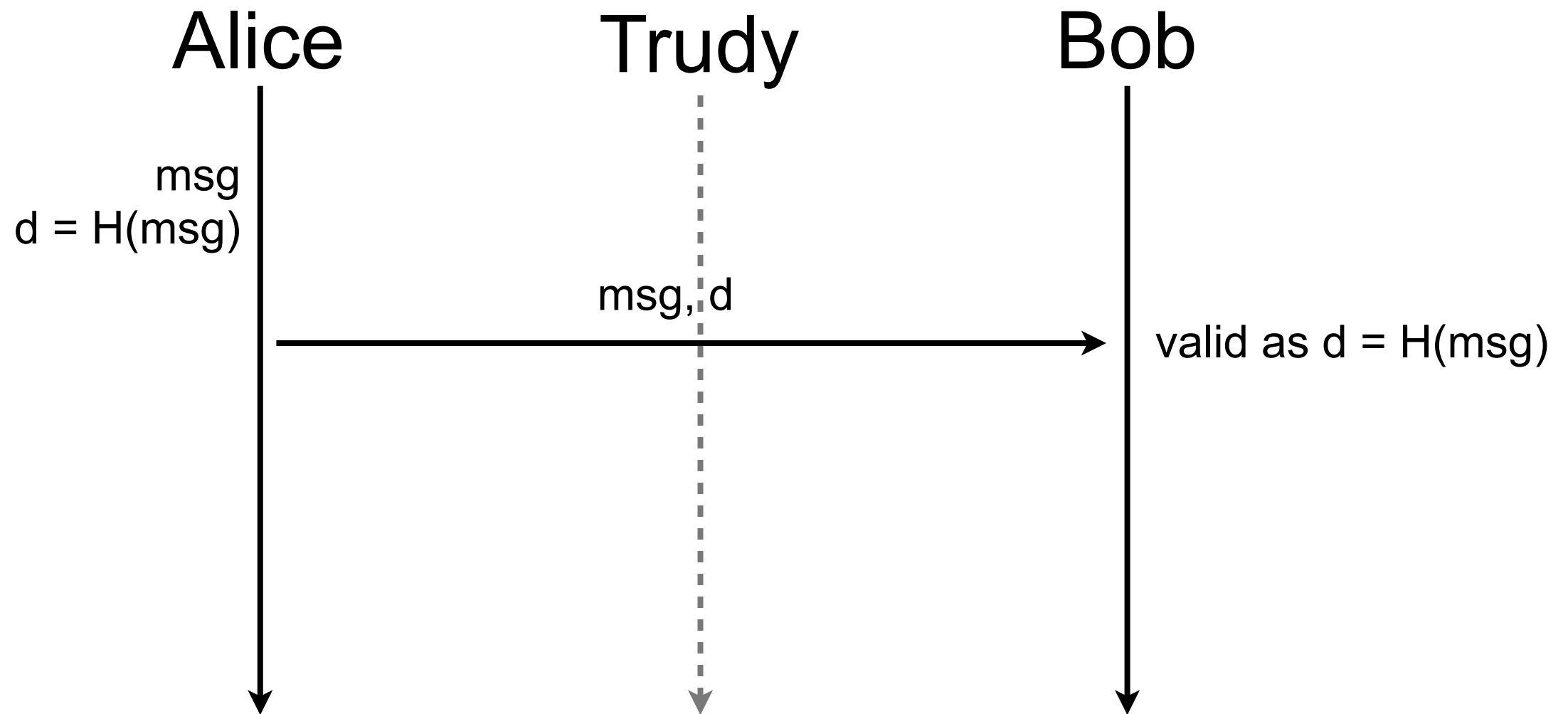
Is that enough?



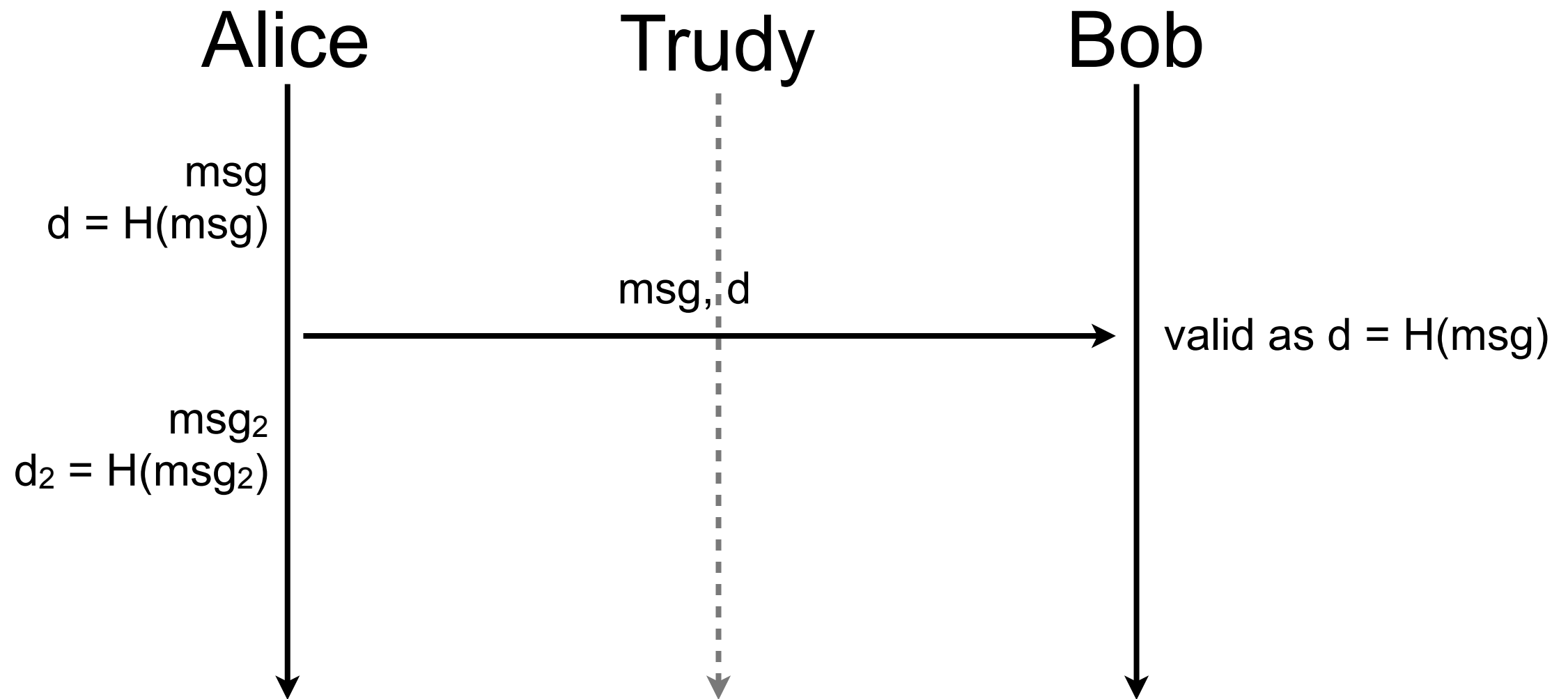
Is that enough?



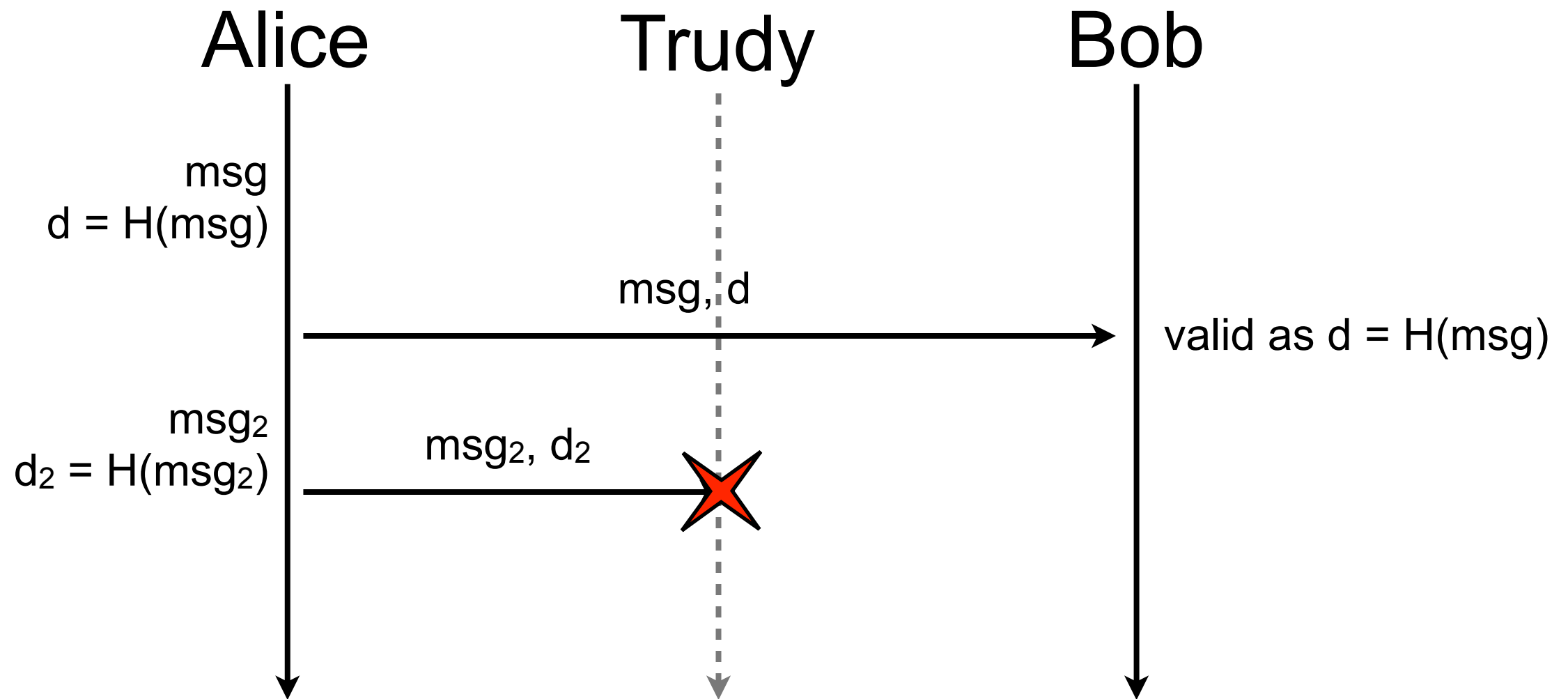
Is that enough?



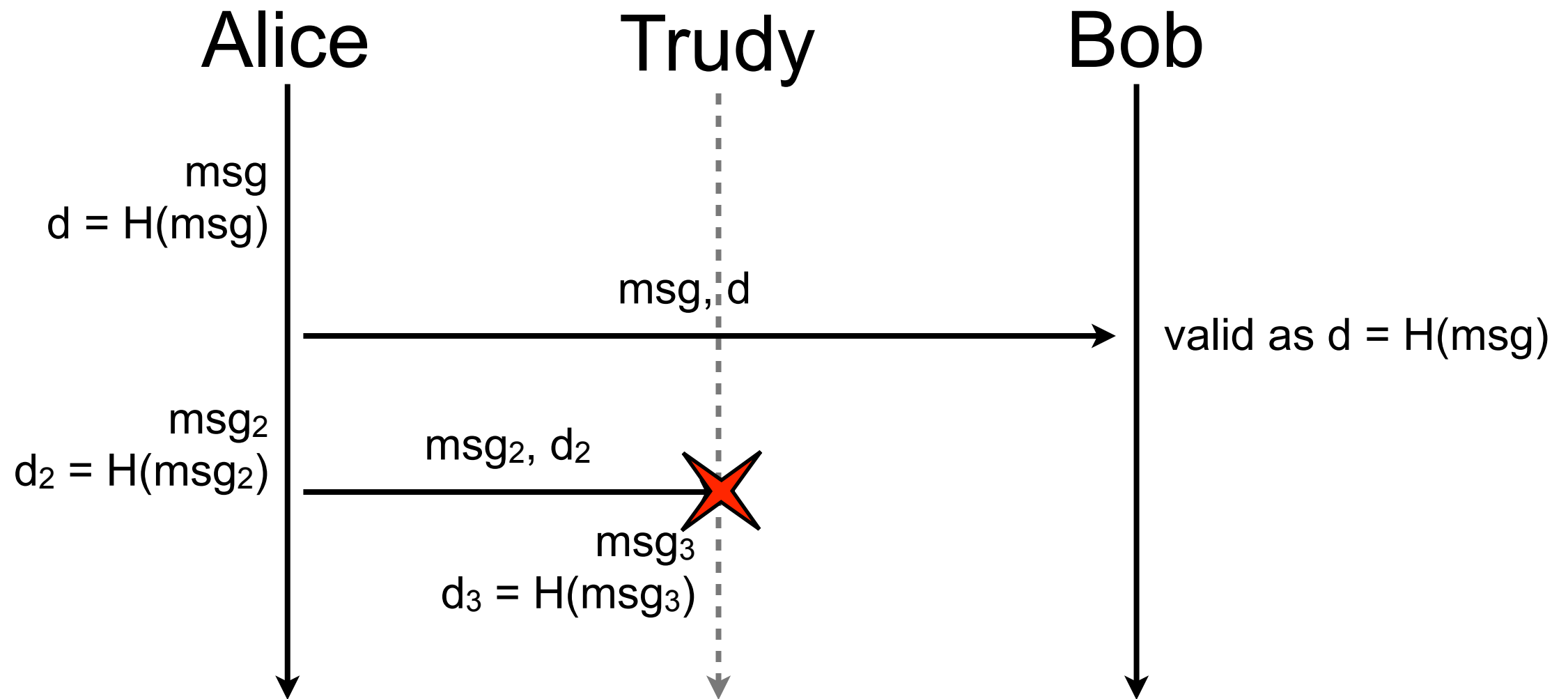
Is that enough?



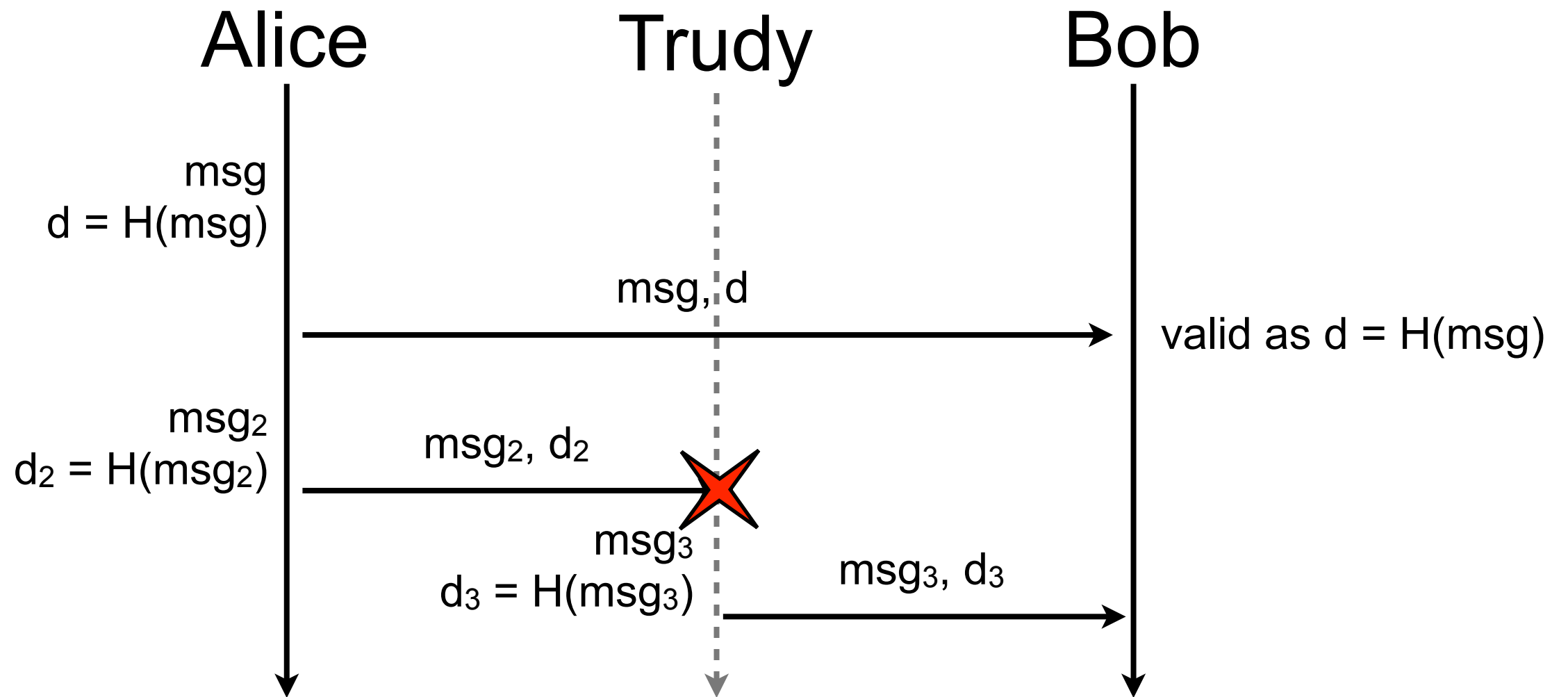
Is that enough?



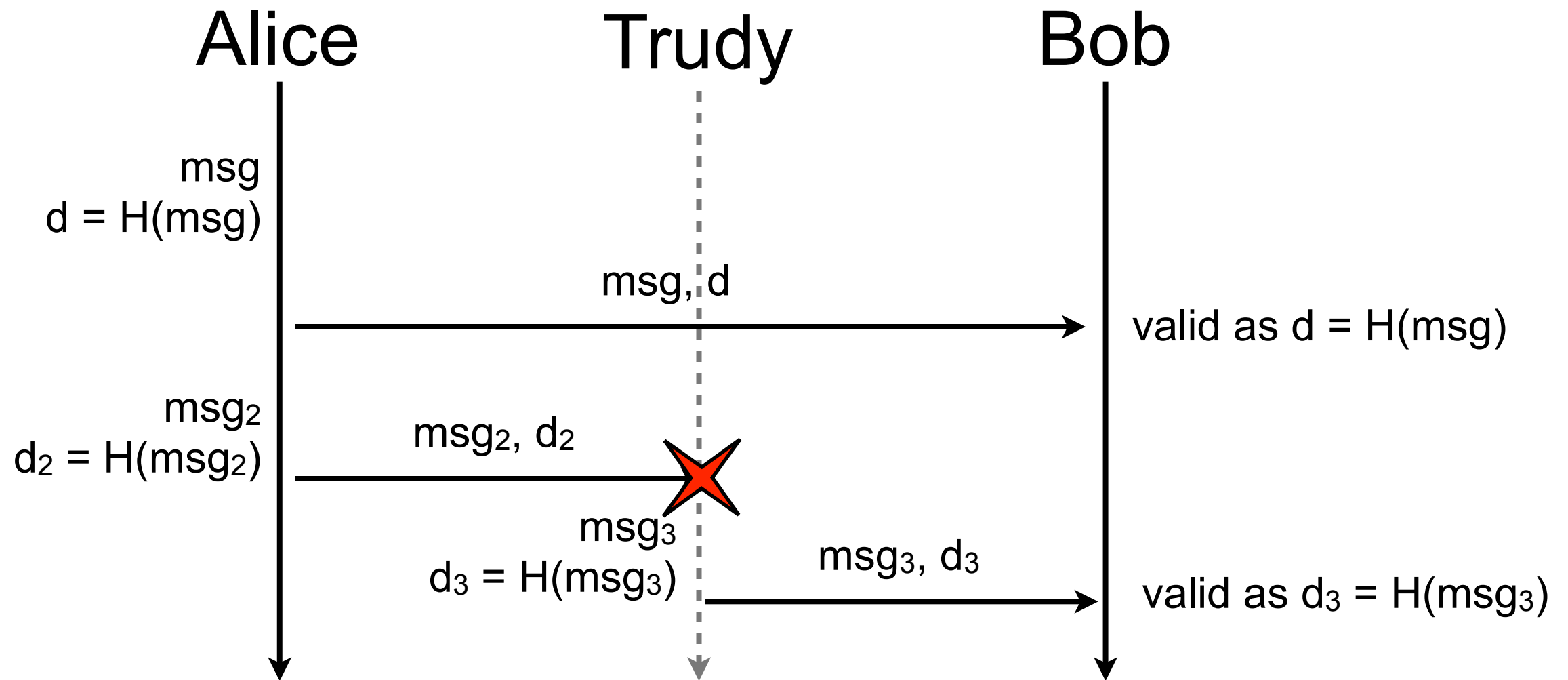
Is that enough?



Is that enough?



Is that enough?



Hash function with salt

- Hash functions are deterministic
- Add a salt such that the output of the hash function is a function of the message and the salt
- $h = H(m, K)$ where s is the salt or key of the hash function
- As long as Trudy does not know the salt, she can't forge a valid digest

Hash function with salt (contd.)

Alice

K



Trudy

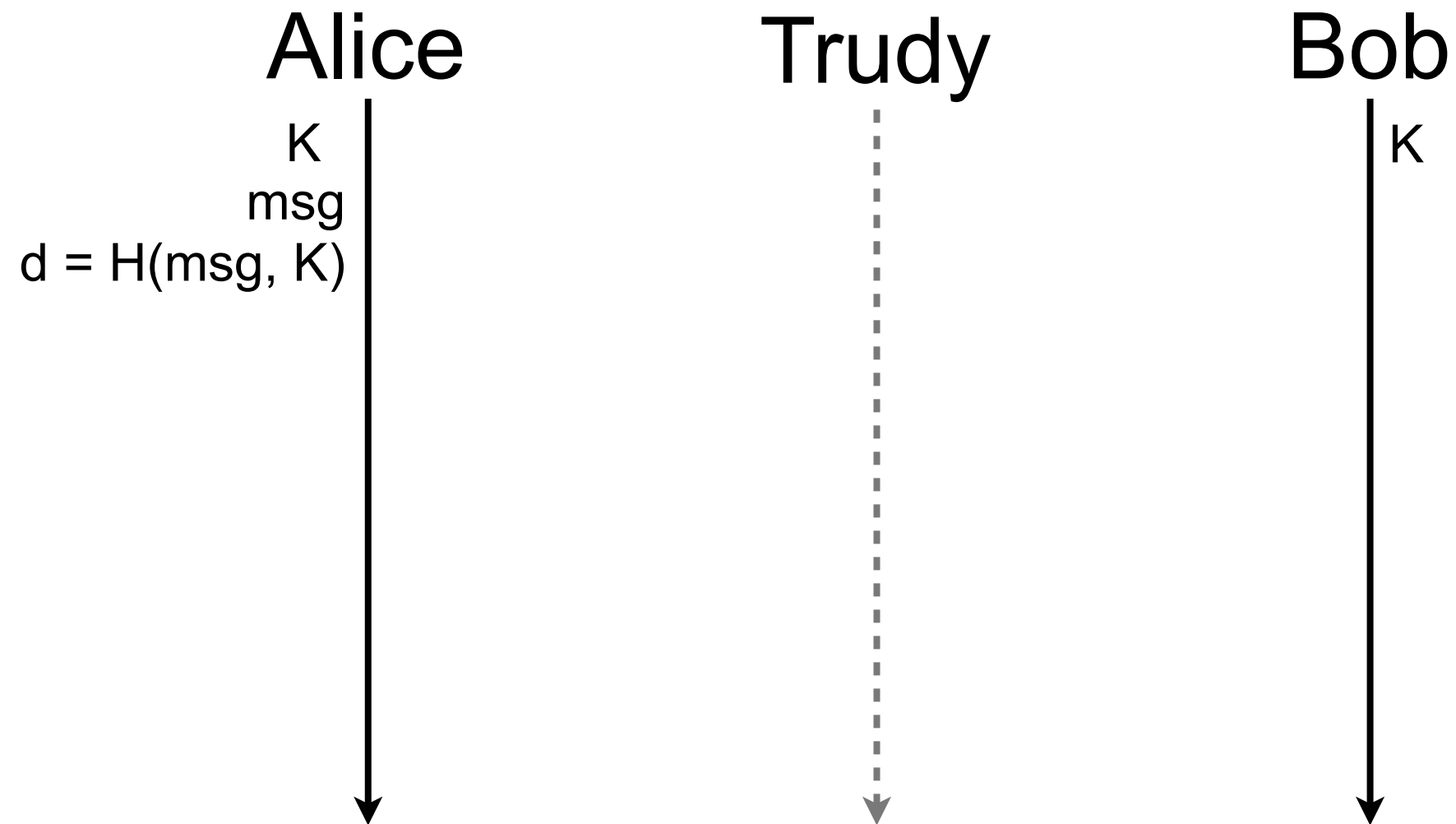


Bob

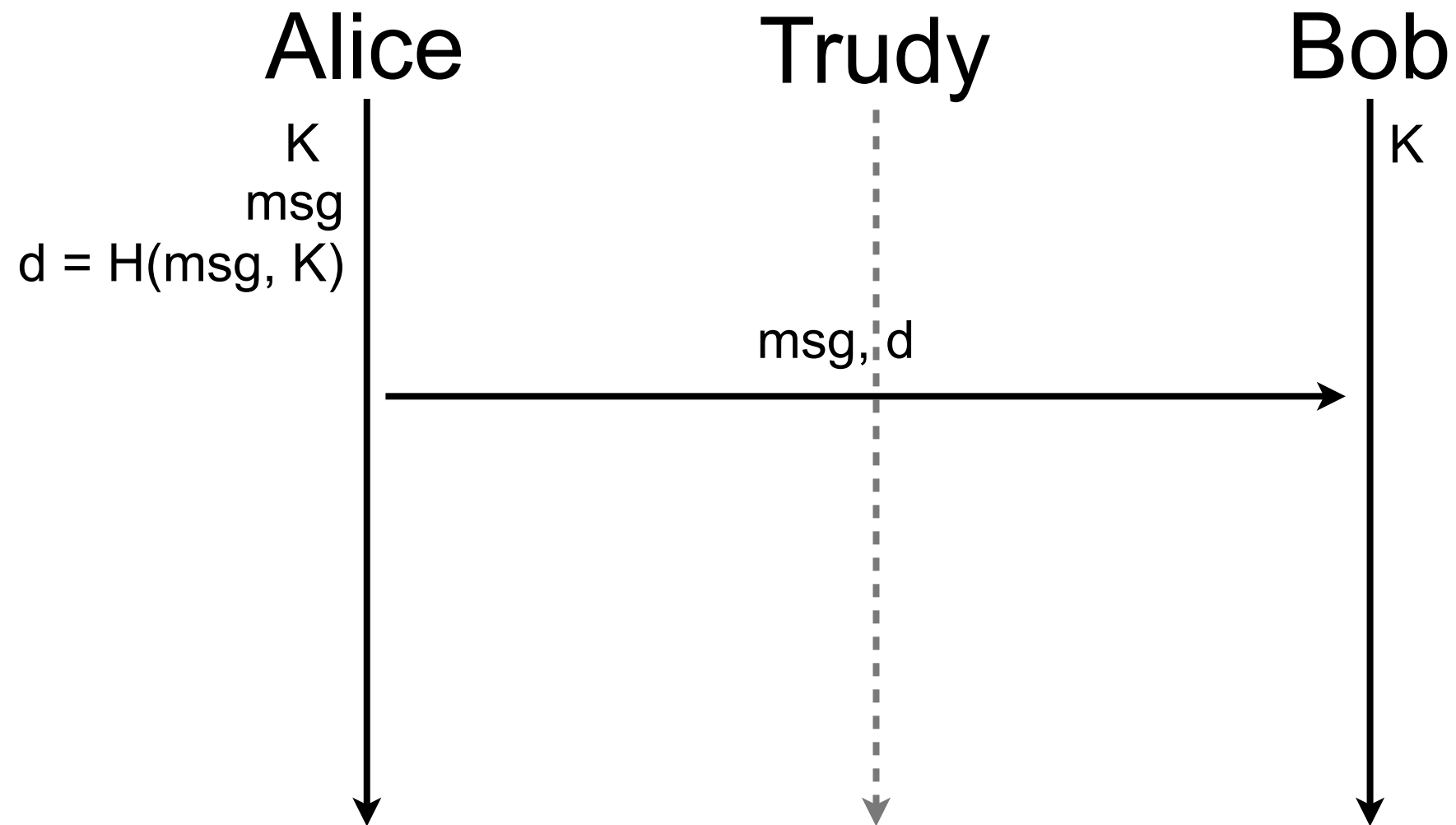
K



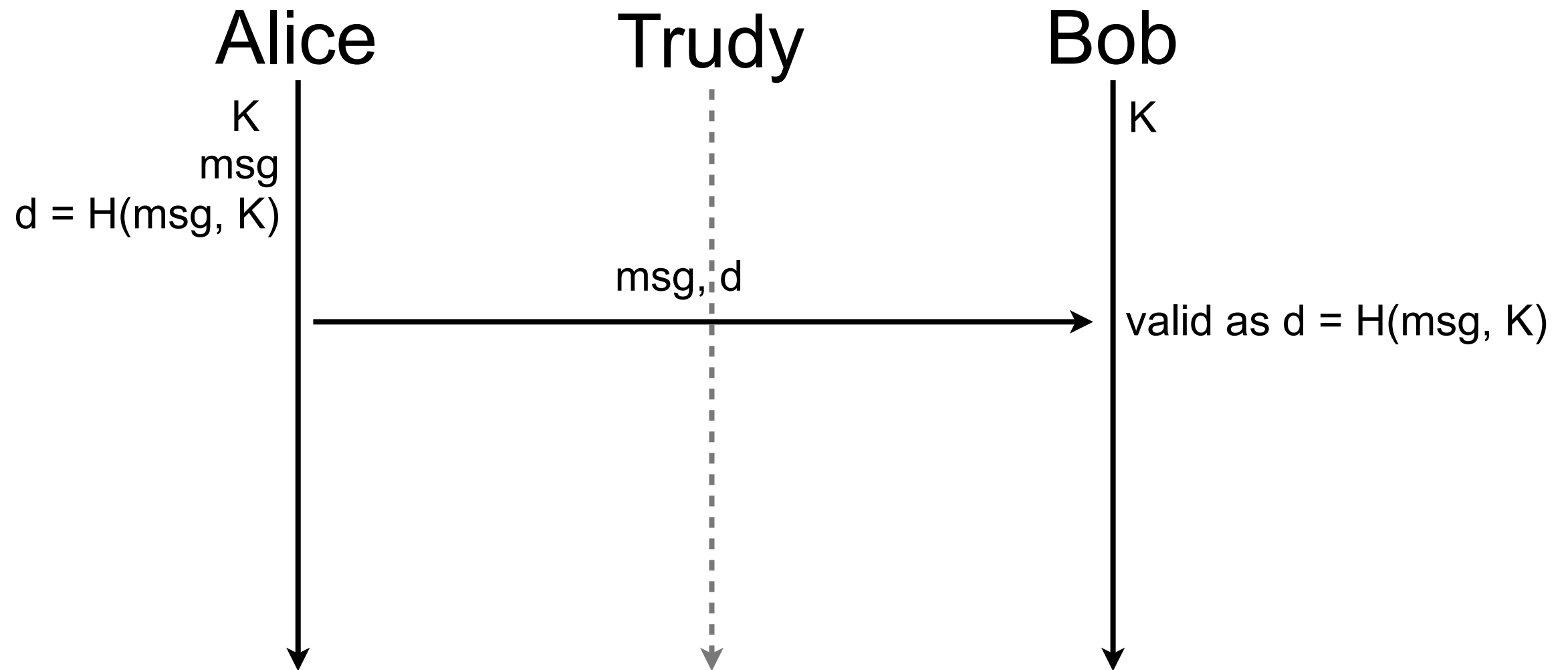
Hash function with salt (contd.)



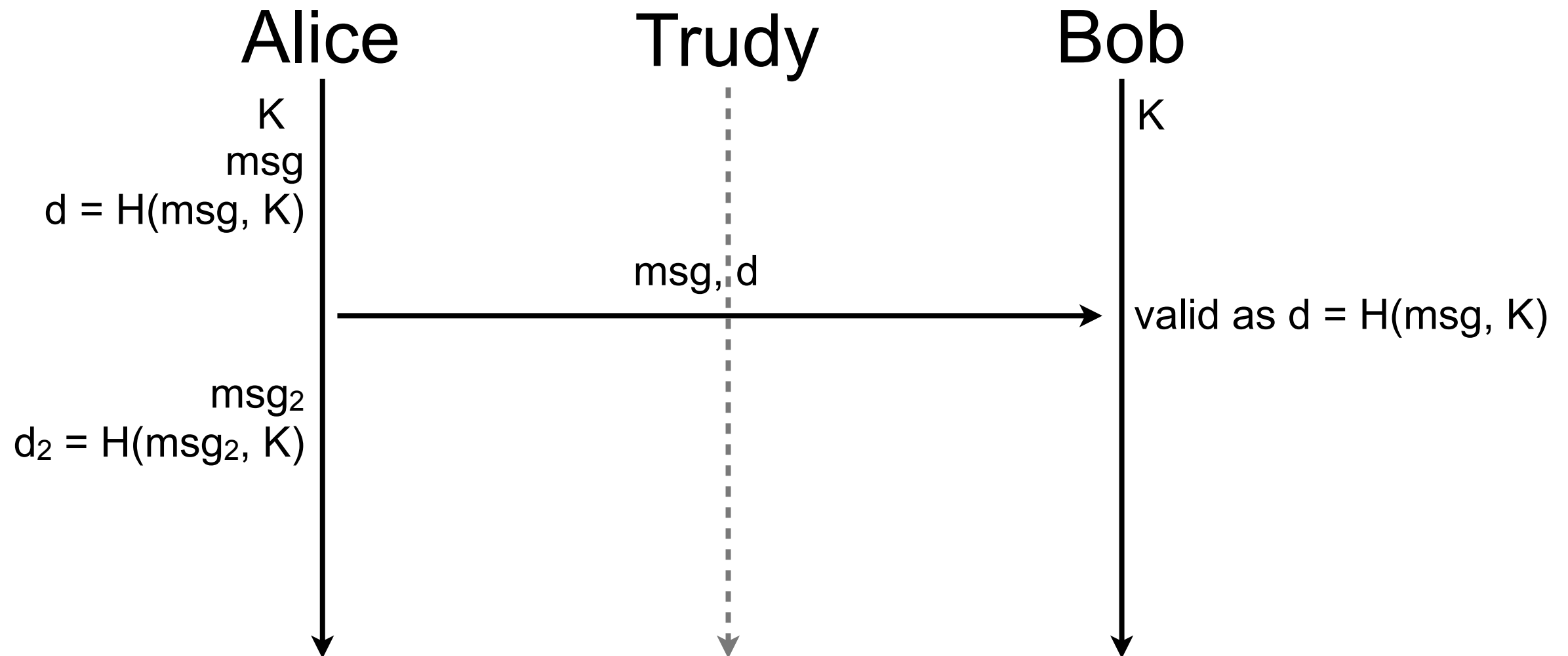
Hash function with salt (contd.)



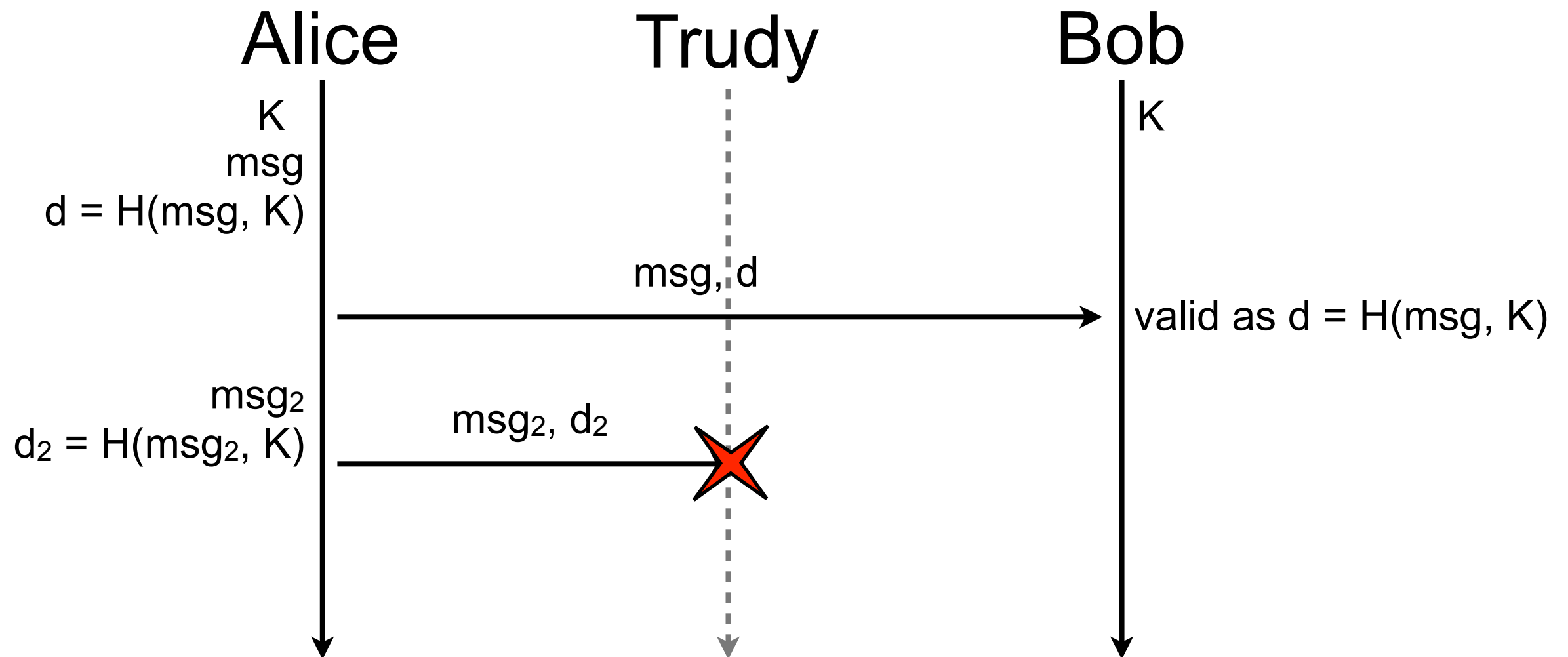
Hash function with salt (contd.)



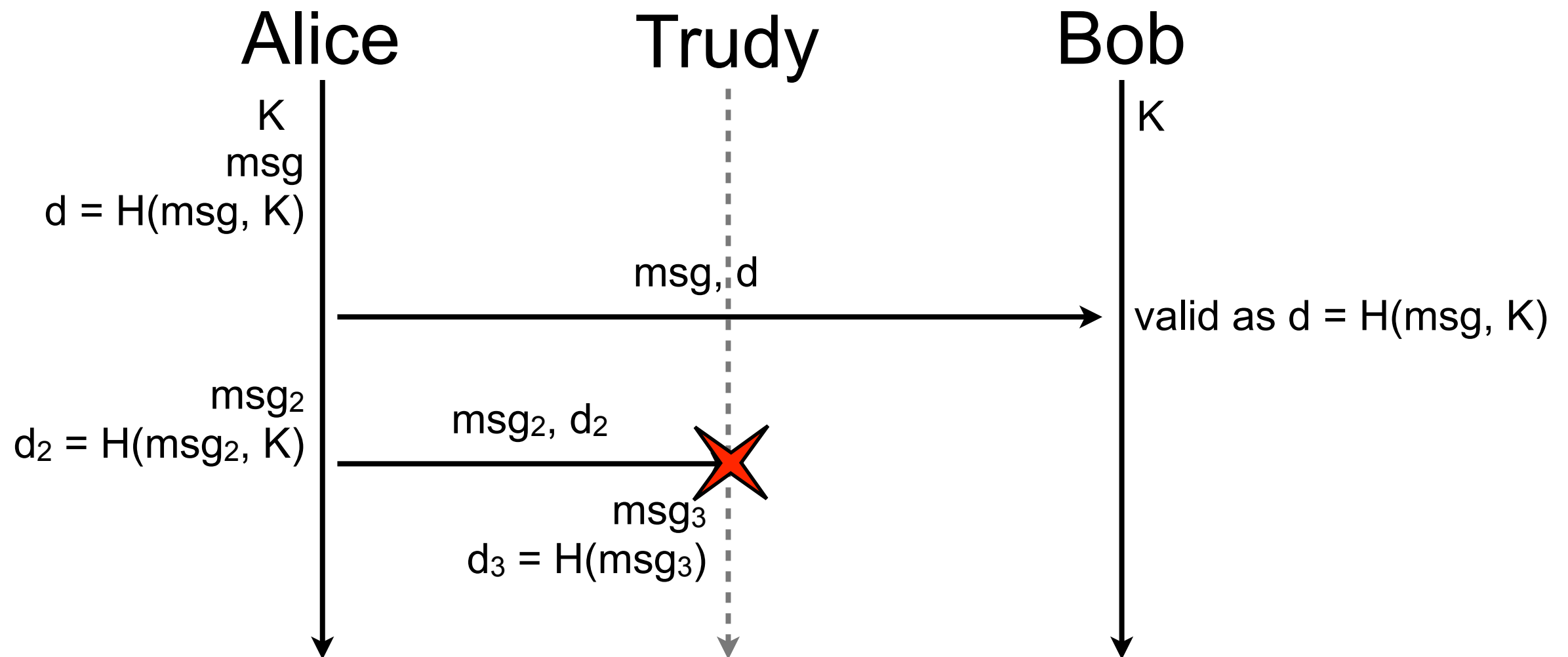
Hash function with salt (contd.)



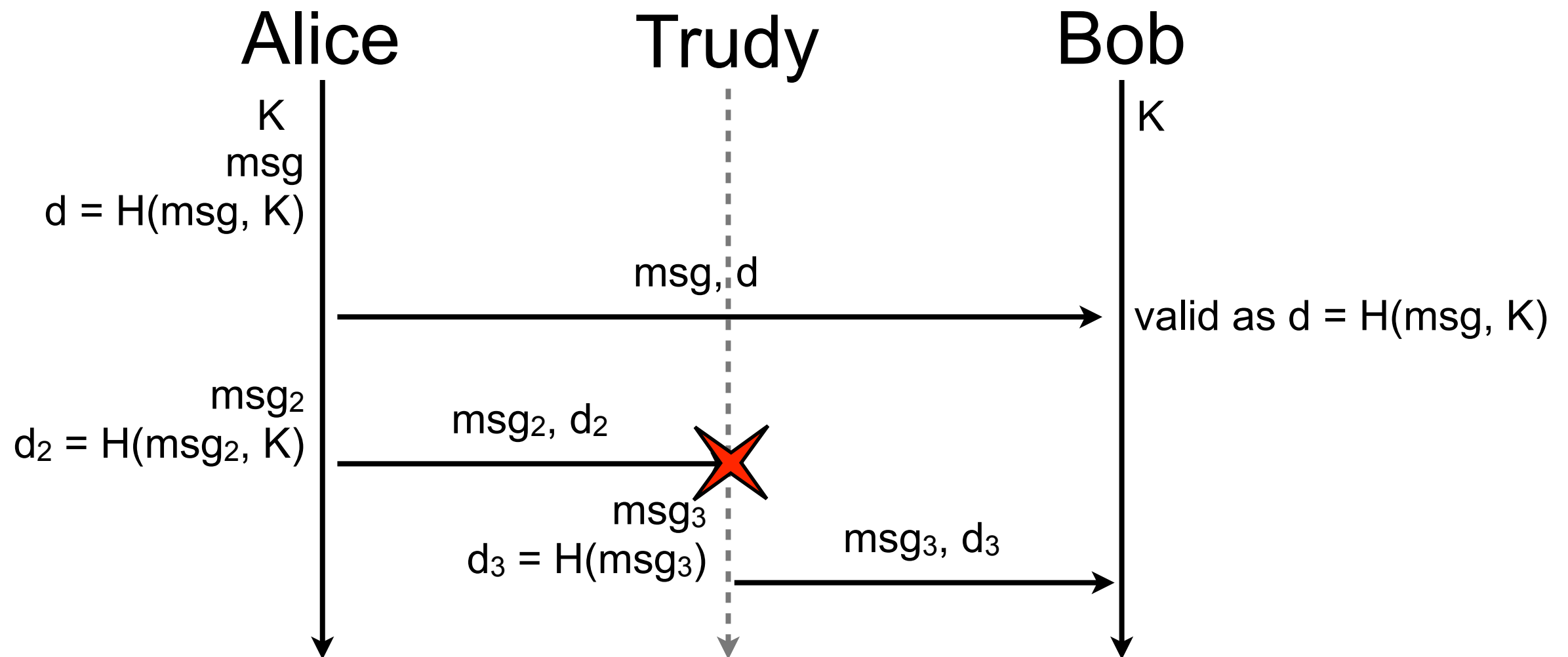
Hash function with salt (contd.)



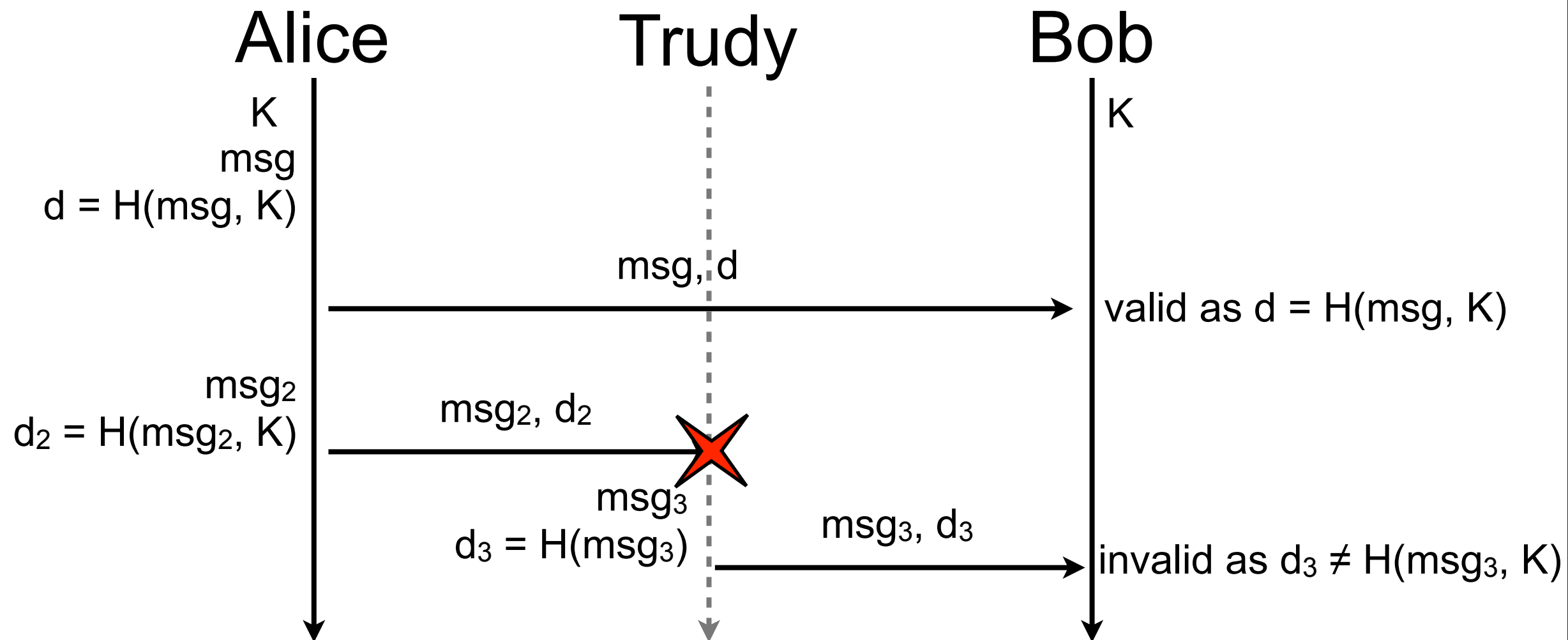
Hash function with salt (contd.)



Hash function with salt (contd.)



Hash function with salt (contd.)



Problem solved?

- fill me
- fill me
- fill me

Problem solved?

- fill me
- fill me
- fill me

How can Alice and Bob agree on K ?

Diffie-Hellman key exchange

- How can Alice and Bob agree on a secret number and be sure that Eve will not discover it?
- Principle
 - do not exchange the secret number but other numbers that are use to build up the secret

Diffie-Hellman key exchange (contd.)

- Working on finite group and positive integers

Alice



Eve



Bob



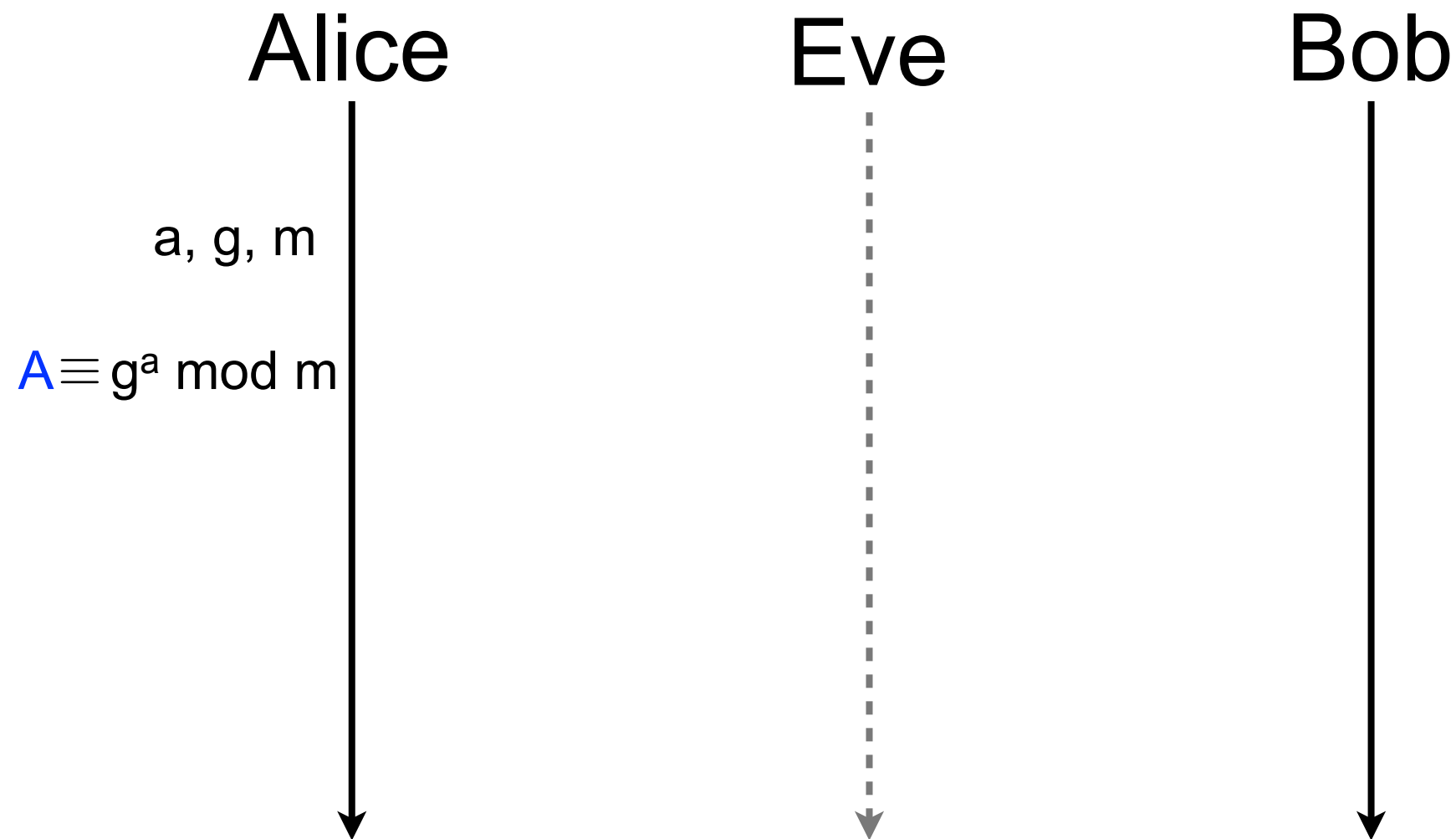
Diffie-Hellman key exchange (contd.)

- Working on finite group and positive integers



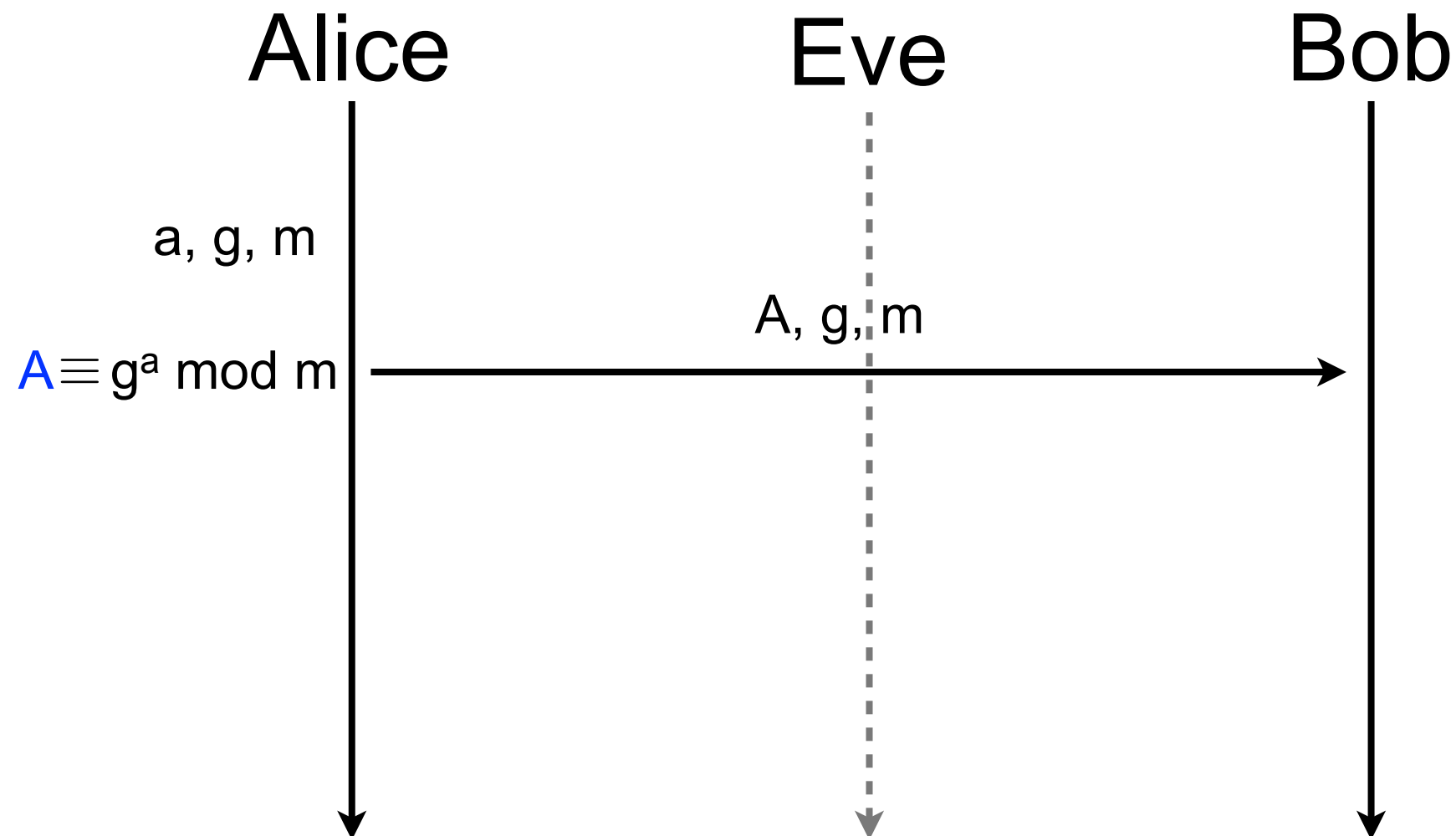
Diffie-Hellman key exchange (contd.)

- Working on finite group and positive integers



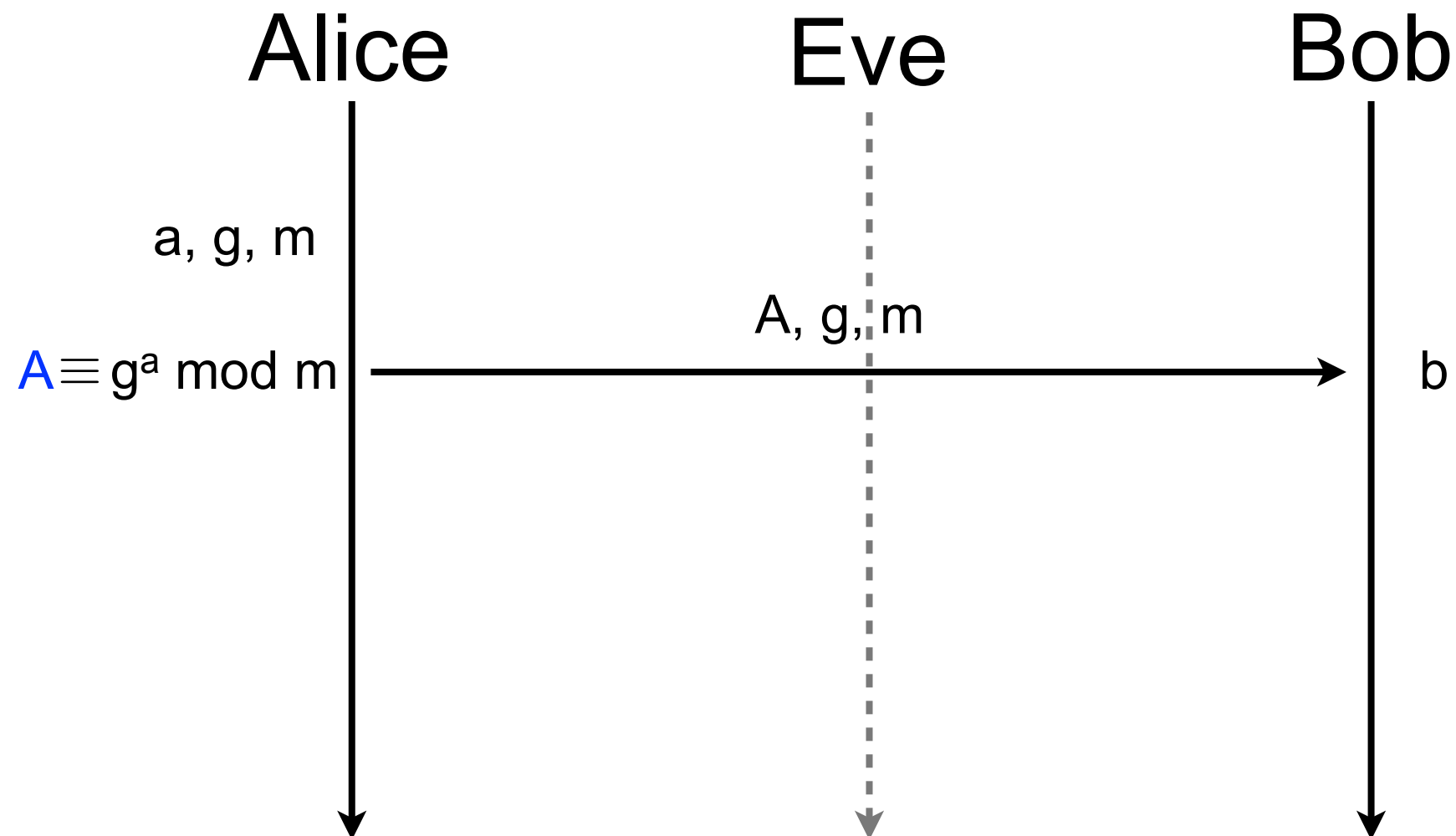
Diffie-Hellman key exchange (contd.)

- Working on finite group and positive integers



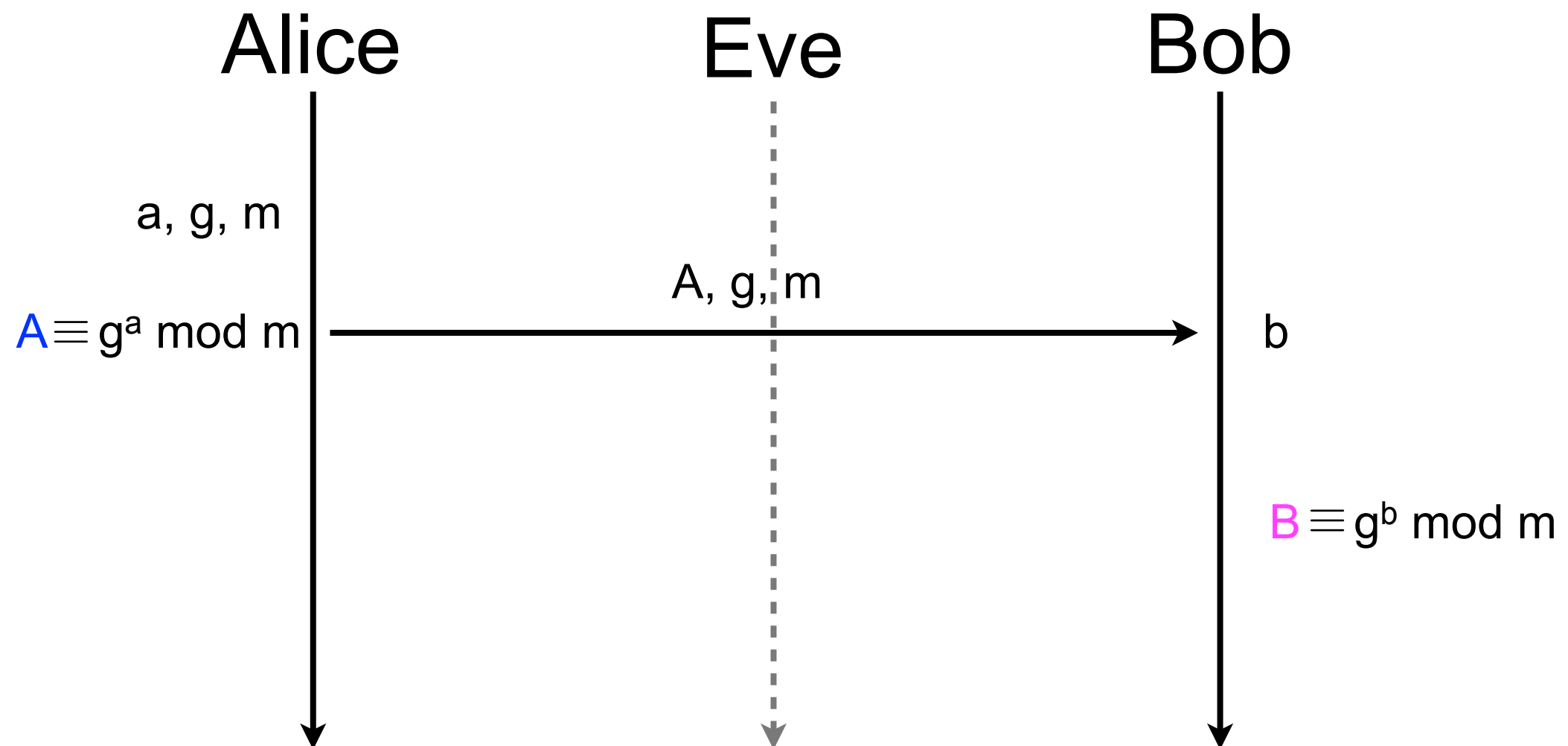
Diffie-Hellman key exchange (contd.)

- Working on finite group and positive integers



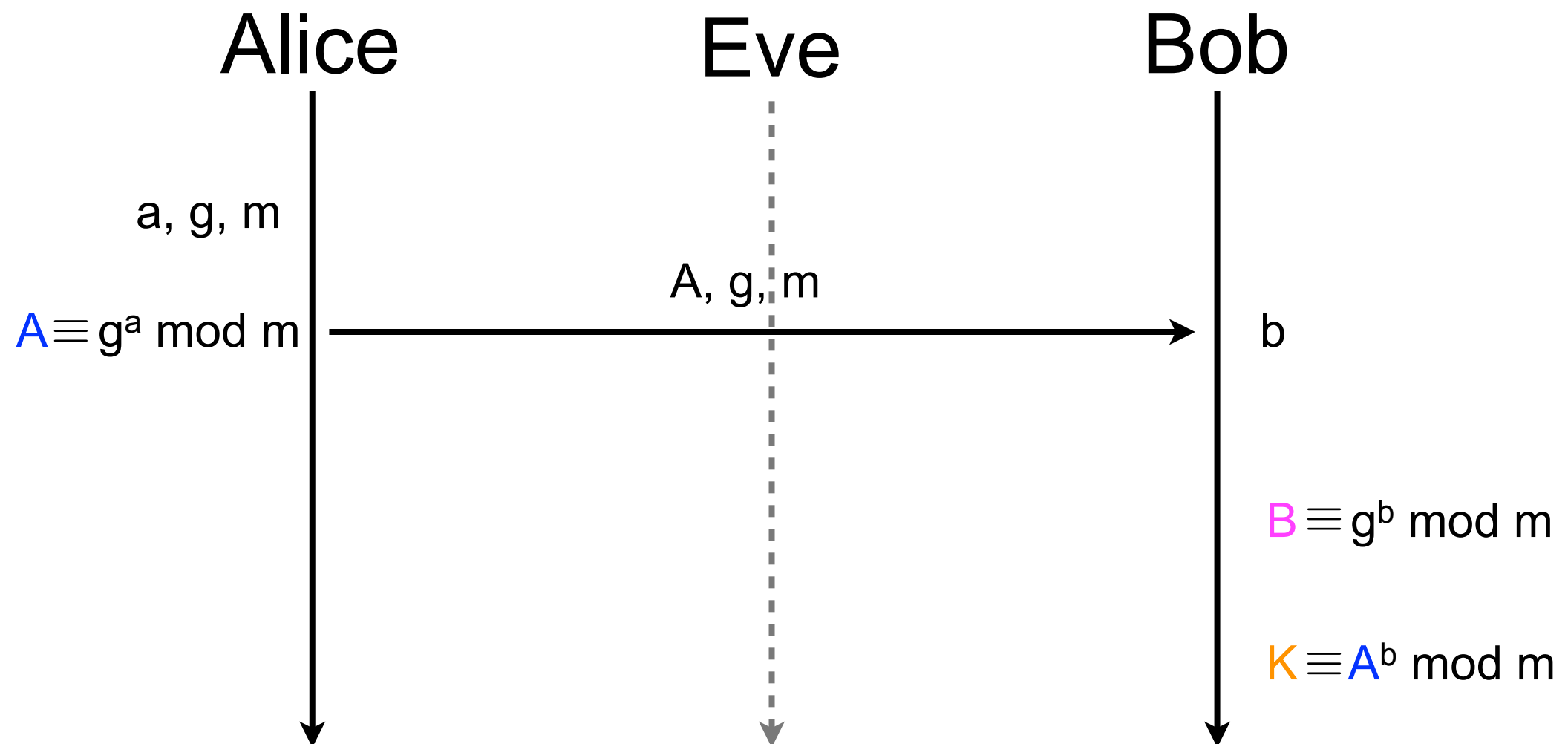
Diffie-Hellman key exchange (contd.)

- Working on finite group and positive integers



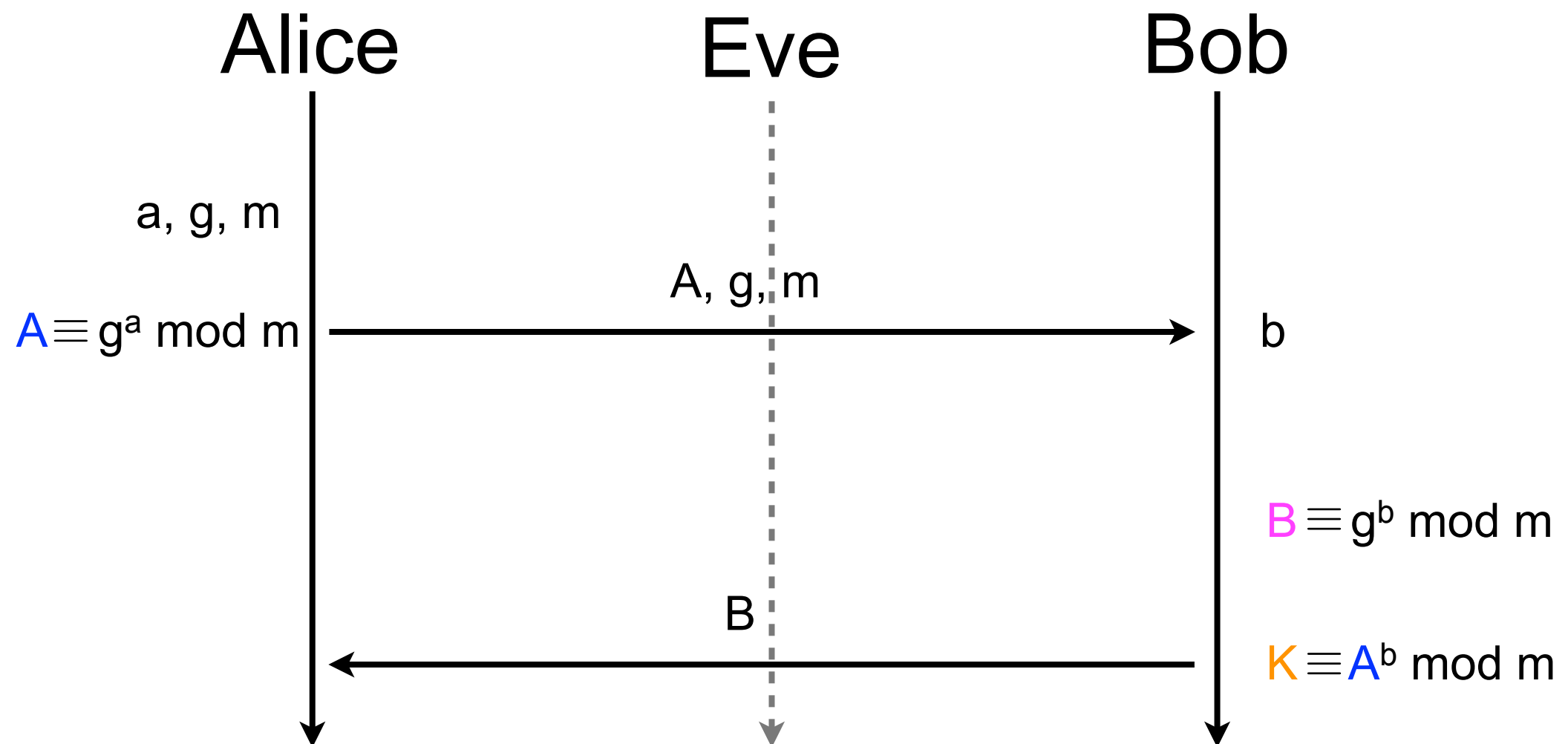
Diffie-Hellman key exchange (contd.)

- Working on finite group and positive integers



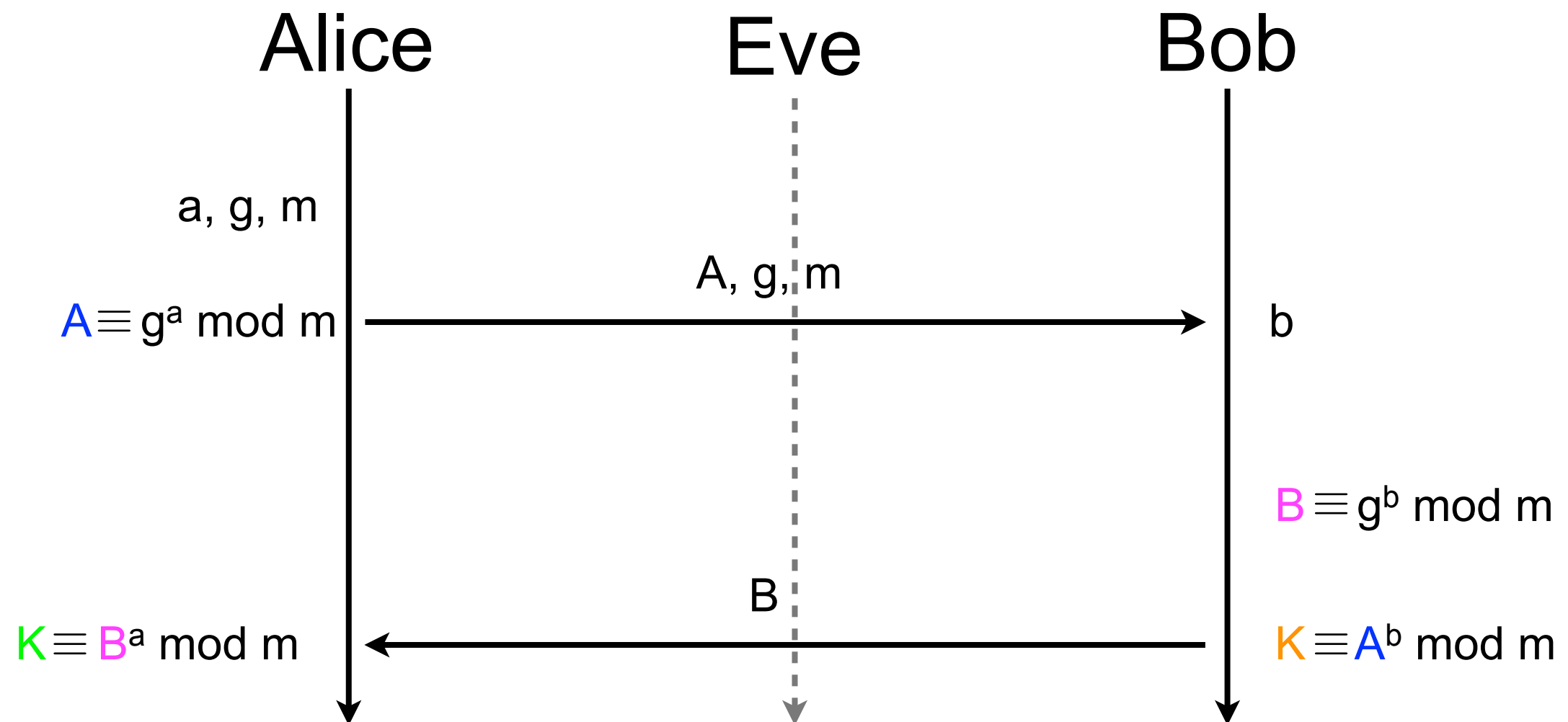
Diffie-Hellman key exchange (contd.)

- Working on finite group and positive integers



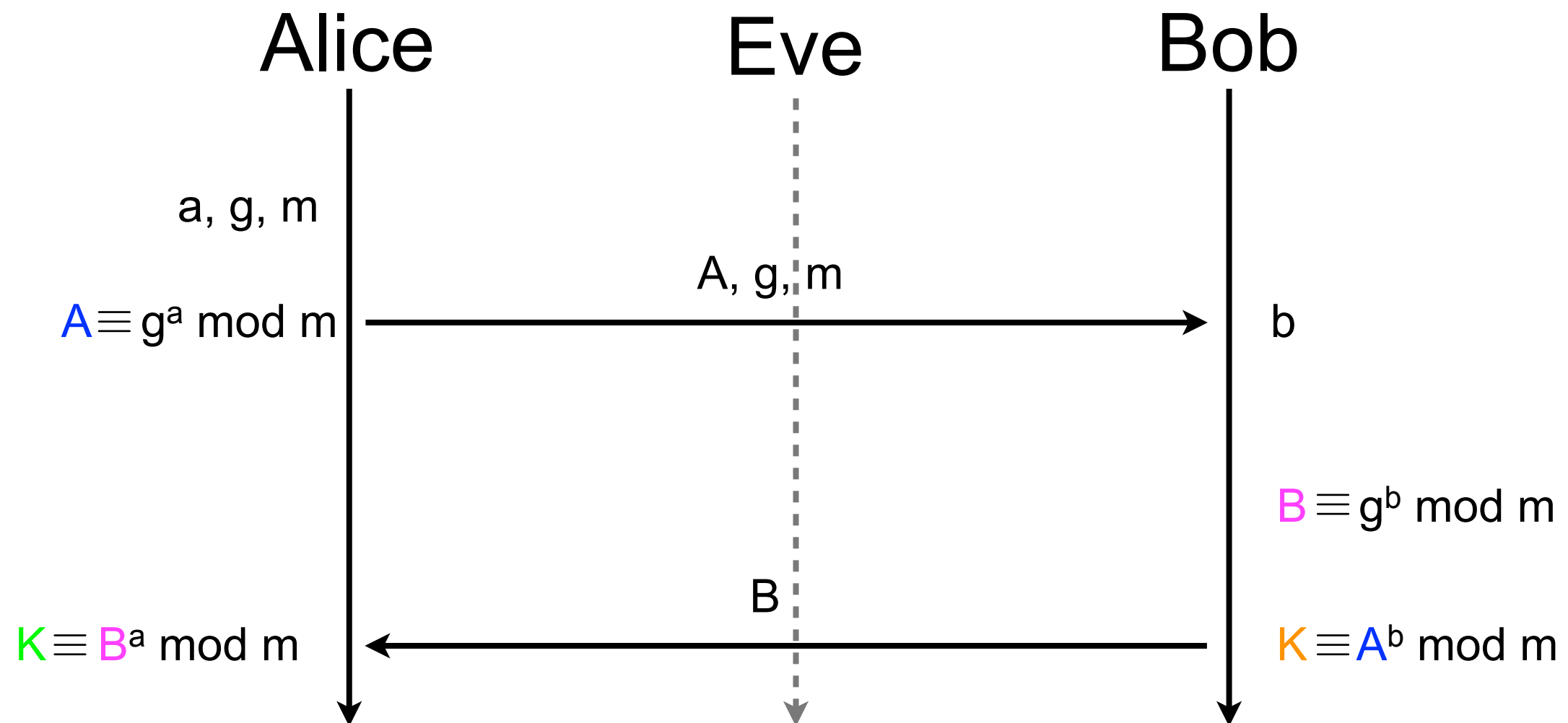
Diffie-Hellman key exchange (contd.)

- Working on finite group and positive integers



Diffie-Hellman key exchange (contd.)

- Working on finite group and positive integers



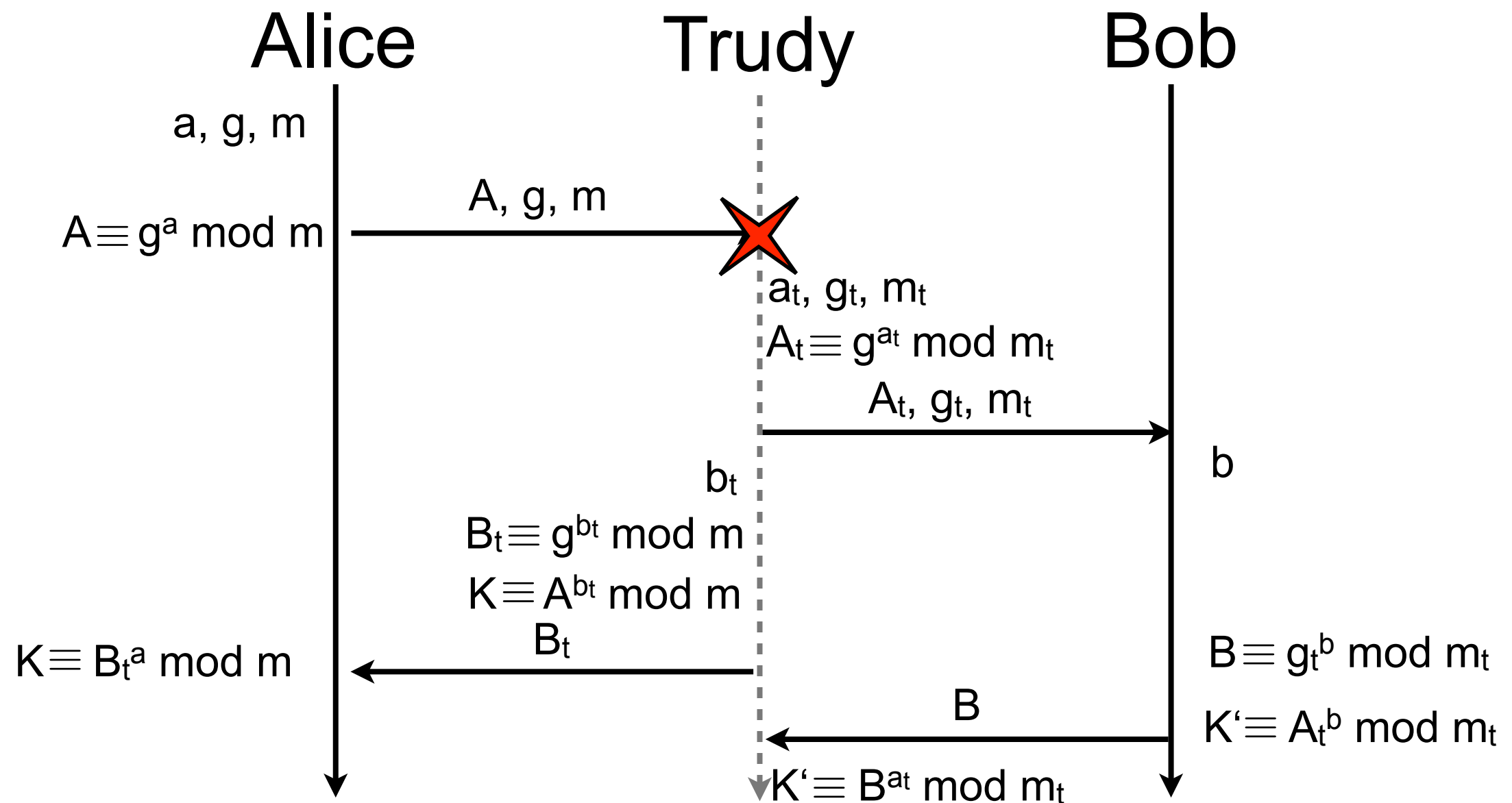
$$K \equiv A^b \pmod{m} \equiv (g^a \pmod{m})^b \pmod{m} \equiv g^{ba} \pmod{m} \equiv (g^b \pmod{m})^a \pmod{m} \equiv B^a \pmod{m} \equiv K$$

Diffie-Hellman key exchange (contd.)

- Why can't Eve guess K if she knows A , B , g , and m ?
 - discrete exponentiation is linear with the size of the argument
 - easy to compute $x \equiv y^z \pmod{p}$
 - but for some discrete groups, no efficient algorithm is known to compute discrete logarithm
 - hard to determine natural z that ensures $x \equiv y^z \pmod{p}$
- Eve knows A , B , g , and m but can't determine neither **a** nor **b** that are absolutely necessary to compute K
 - $$\begin{aligned}
 K &\equiv A^b \pmod{m} \equiv (g^a \pmod{m})^b \pmod{m} \equiv g^{ab} \pmod{m} \\
 &\equiv (g^b \pmod{m})^a \pmod{m} \equiv B^a \pmod{m}
 \end{aligned}$$

Diffie-Hellman key exchange (contd.)

- Trudy can break Diffie-Hellman



Diffie-Hellman key exchange (contd.)

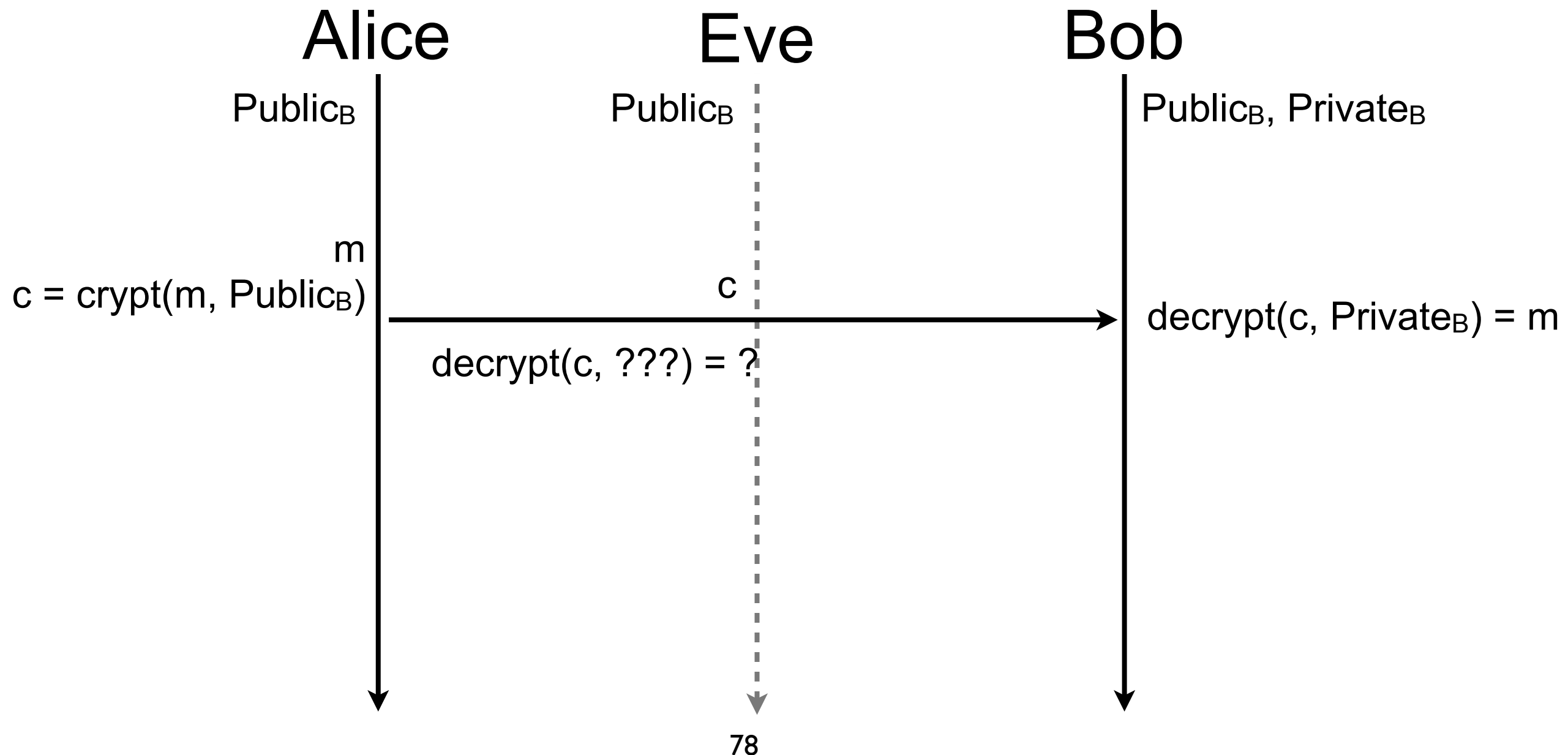
- How can we protect Diffie-Hellman from Trudy?
- Principle
 - Alice and Bob sign the messages exchanged in Diffie-Hellman (?!)

Asymmetric cryptography

- In asymmetric cryptography (aka public-key cryptography), two keys are used
 - public key
 - publicly available to anybody (even attackers)
 - used to encrypt a message
 - private key
 - known only by the legitimate owner of the public key
 - used to decrypt a message
- e.g., RSA, PGP, Diffie-Hellman
- Public-key cryptography is 10 to 100 times slower than symmetric-key cryptography
 - seldom (never?) used to encrypt communications

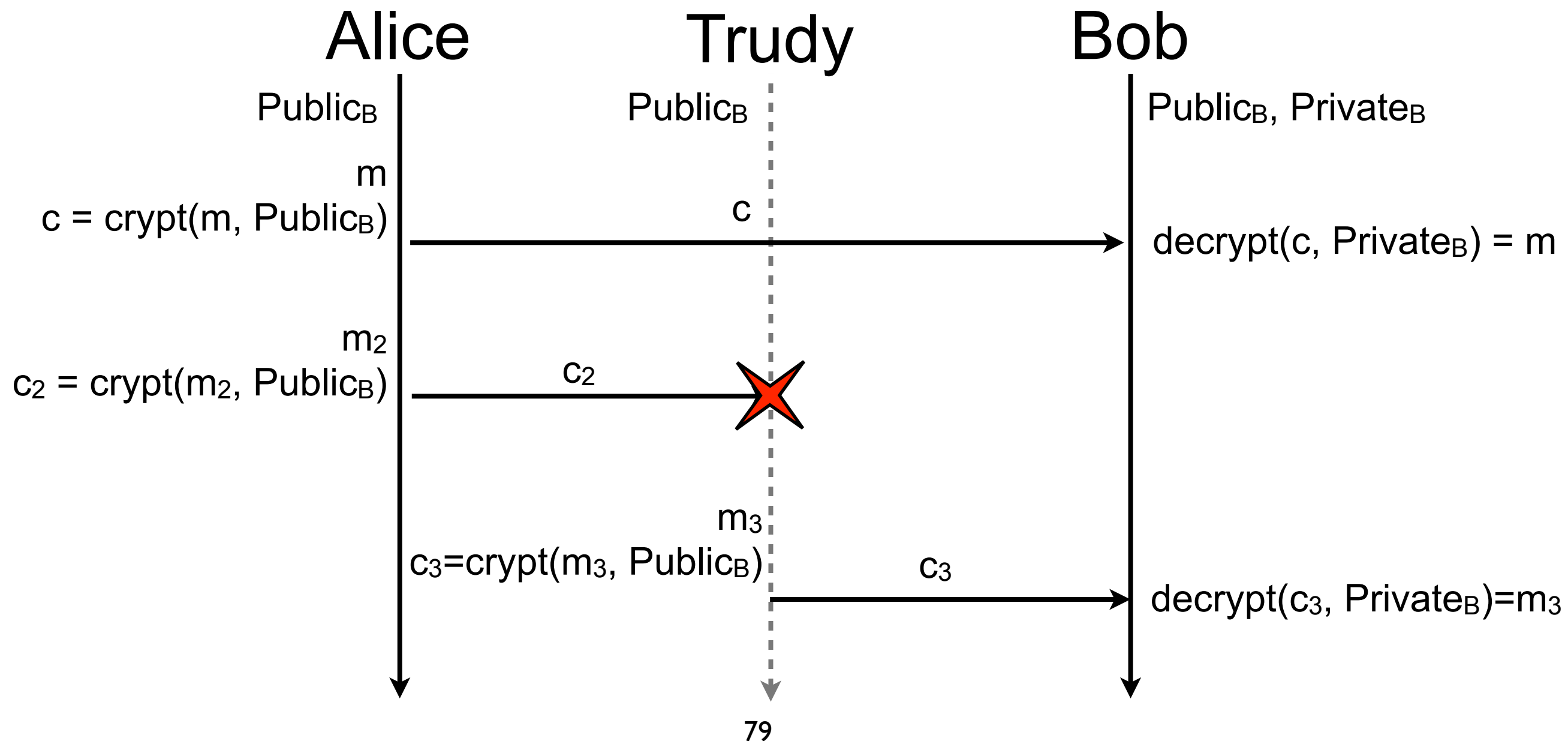
Asymmetric cryptography (contd.)

- Eve cannot determine the message



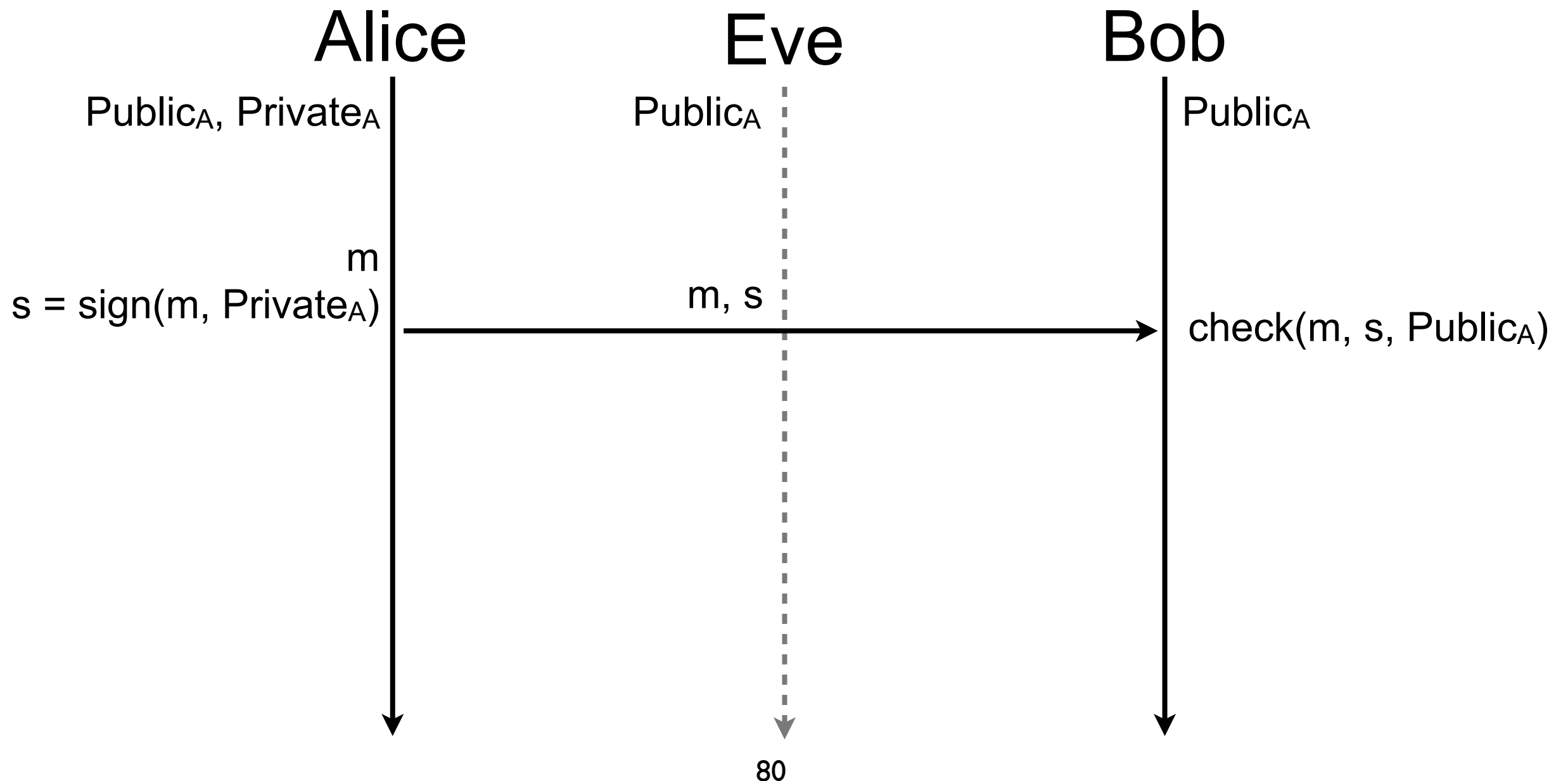
Asymmetric cryptography (contd.)

- Trudy can send a forged message



Asymmetric cryptography (contd.)

- Eve can read the message



How to build sign and check?

- $s = \text{sign}(H(m), k) = \text{crypt}(H(m), k)$
- $\text{check}(m, s, K) = (H(m) == \text{decrypt}(s, K))$
 - where k is the private key of the signer and K is the public key
- Asymmetric cryptography is slow and m can be large
 - encrypting m would be too costly
 - solution: consider the digest of m while signing

Public key infrastructure

- How to safely obtain Bob's public key?

Alice



Trudy



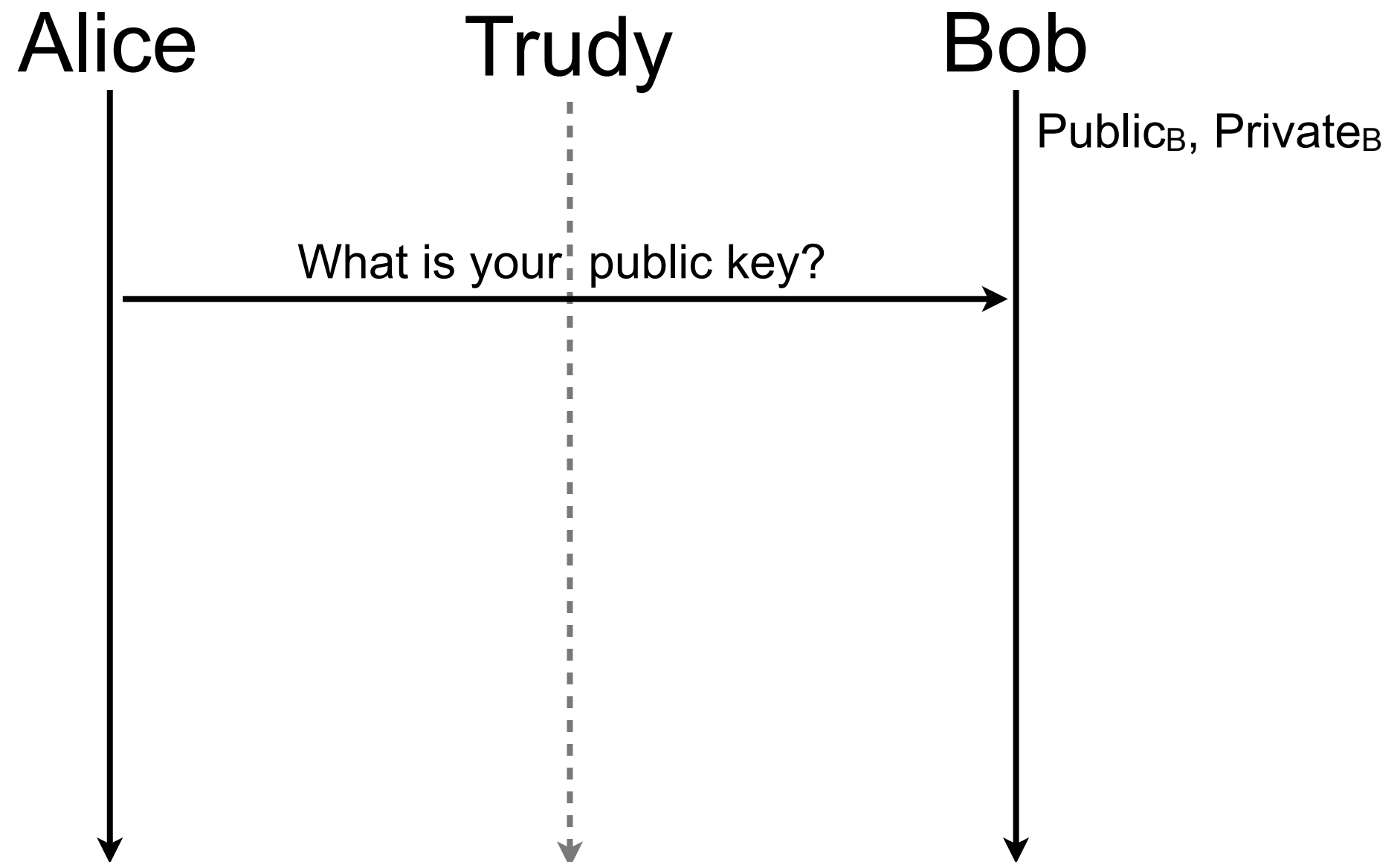
Bob

Public_B, Private_B



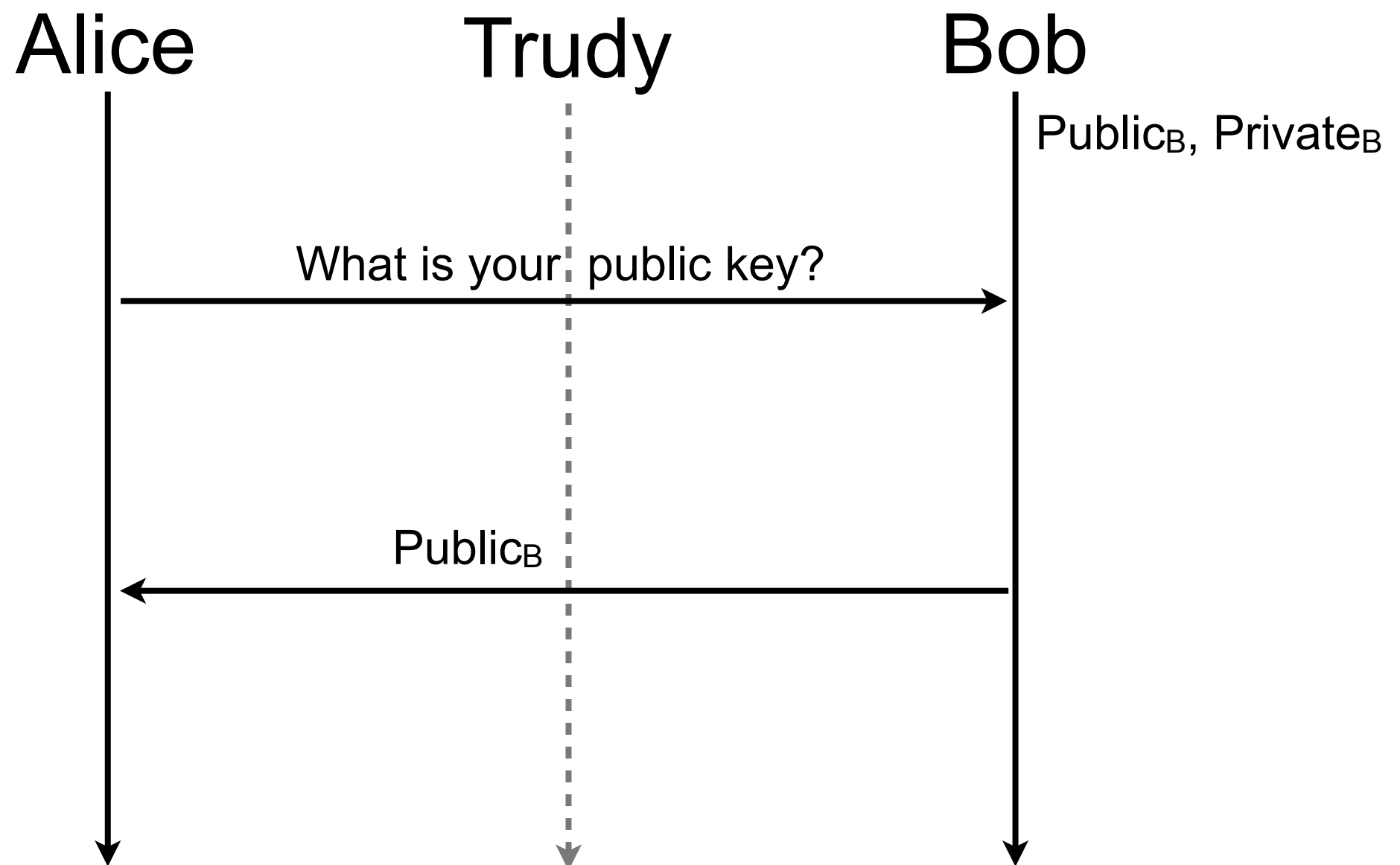
Public key infrastructure

- How to safely obtain Bob's public key?



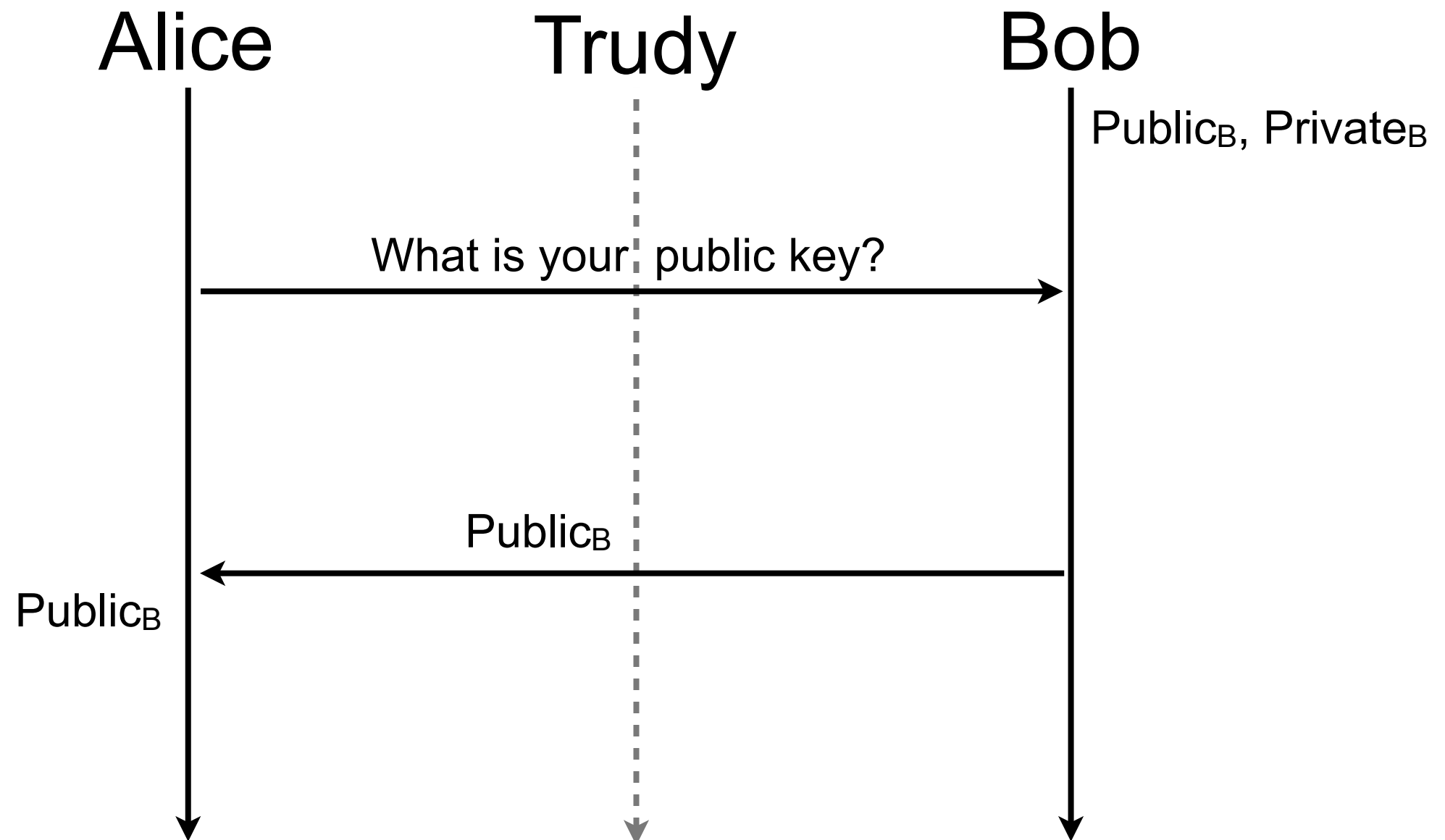
Public key infrastructure

- How to safely obtain Bob's public key?



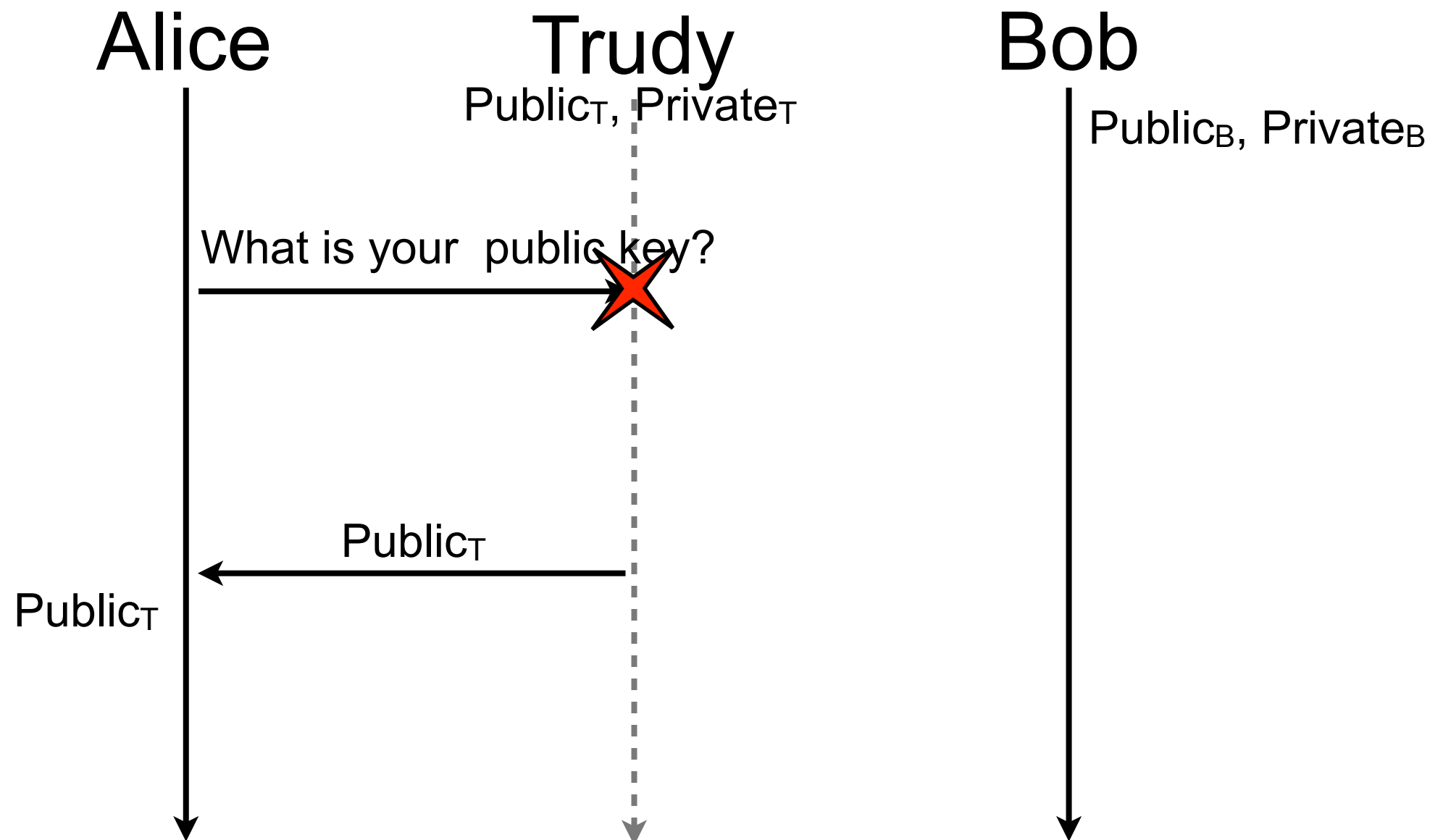
Public key infrastructure

- How to safely obtain Bob's public key?



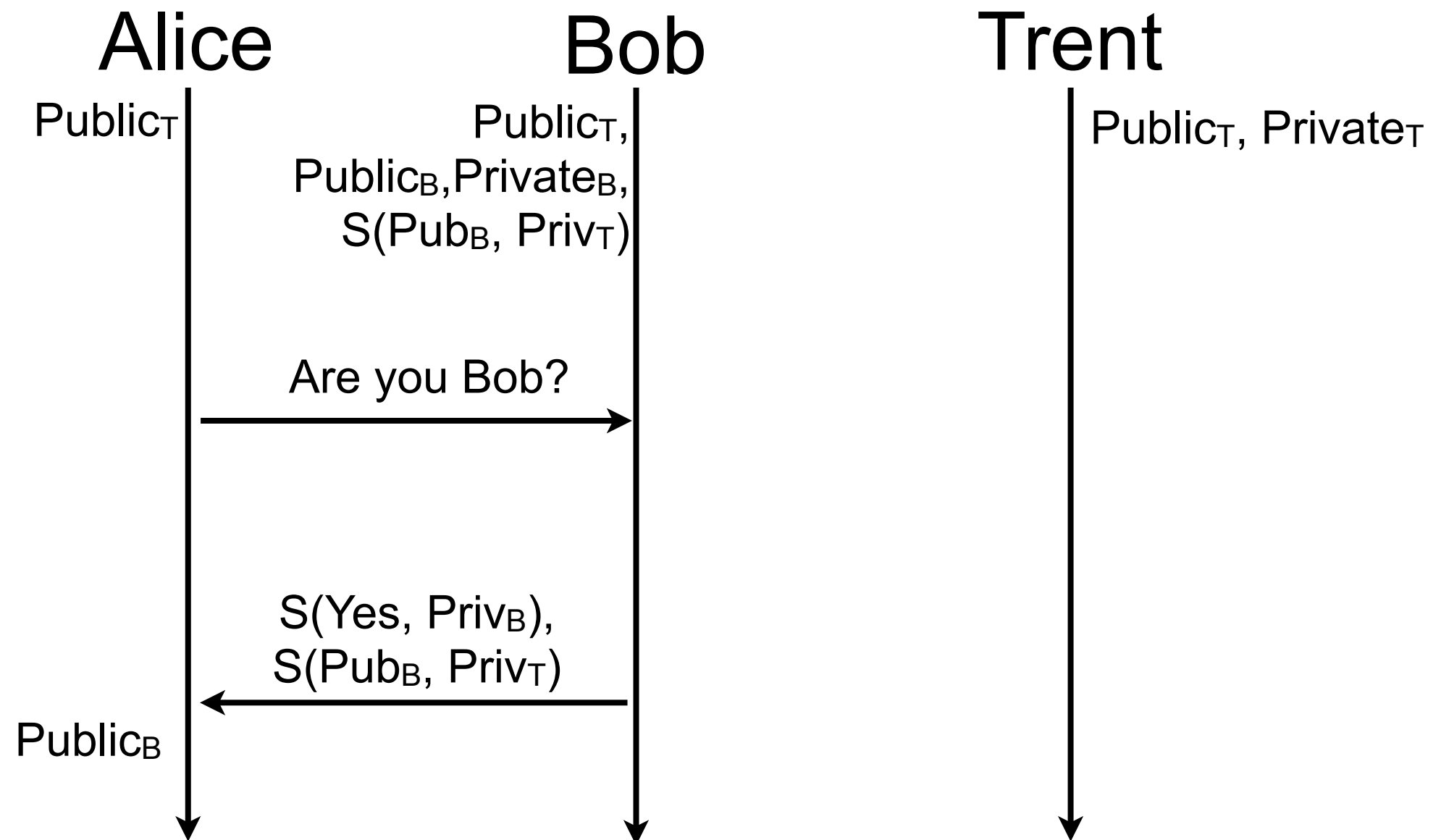
Public key infrastructure (contd.)

- Trudy can send a forged key



Public key infrastructure (contd.)

- Alice and Bob trust a third party (e.g., Trent) for authentication



Public key infrastructure (contd.)

- Practically, Bob sends a certificate (e.g., X.509), not only its public key and signature
- A certificate provides many information to be able to correctly identify and authenticate its subject (e.g., Bob)
 - the subject name and organization
 - the subject public key (and type)
 - the issuer name and organization
 - the certificate validity time (valid not before and not after)
 - the certificate signature and type, signature made by the issuer of the certificate
 - ...

Public key infrastructure (contd.)

- A certificate signed with the private key of the public key indicated into the certificate is said self-signed
 - prove nothing except that the issuer knows the private key of the subject
- Certificates can be chained, the subject is certified by its issuer, the issuer itself is certified by its own issuer, and so on until the root of the certification is reach
 - when a certificate is not self-signed, it indicates the chain of certificates used for its authentication
- The entity verifying the certificates backtracks the chain of certificate until is reaches the certificate of a certification authority (CA) he knows
- Trusted parties are installed separately (e.g., hardcoded, during OS updates)
 - assumption: the trusted party is not compromised

Public key infrastructure (contd.)

- Certificates are issued once and valid during a given time period, whatever the number of time it is used
- What if the subjects leaves its organization? The private key of the subject is stolen? The private key of the issuer is stolen?
- Keys are selected big enough to not be broken during validity time
- When a certified key is compromised, the certificate is revoked
 - the issuer maintains the list of revoked certificates
 - when a certificate is checked for validity, the verifying client should verify that the certificate is not in the revoked certificates list

Public key infrastructure (contd.)

- *“A public key infrastructure is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates” [1]*
- A certificate $Cert_1$ issued by a CA can be used to certify any certificate $Cert_2$
 - $Cert_2$ is authenticated if
 - check($Cert_2$, $Cert_2$.signature, $Cert_2$.issuer.public_key) &
check($Cert_1$, $Cert_1$.signature, $Cert_1$.issuer.public_key) &
 $Cert_2$ not in $Cert_2$.issuer.revoke_list &
 $Cert_1$ not in $Cert_1$.issuer.revoke_list
 - where $Cert_2$.issuer is identified with $Cert_1$ and $Cert_1$.issuer is identified by CA's certificate
 - assuming that the verifier knows CA's certificate

Public key infrastructure (contd.)

Public key infrastructure (contd.)

GeoTrust Global CA
Google Internet Authority G2
www.google.com

www.google.com
Issued by: Google Internet Authority G2
Expires: Thursday 29 May 2014 02 h 00 min 00 s Central European Summer Time
This certificate is valid

Trust
Details

Subject Name	
Country	US
State/Province	California
Locality	Mountain View
Organization	Google Inc
Common Name	www.google.com
Issuer Name	
Country	US
Organization	Google Inc
Common Name	Google Internet Authority G2
Serial Number	4879068403411162094
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Wednesday 29 January 2014 15 h 05 min 37 s Central European Summer Time
Not Valid After	Thursday 29 May 2014 02 h 00 min 00 s Central European Summer Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : A4 78 79 A6 79 86 3B B8 ...
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Derive
Signature	256 bytes : 3A 8F DA 0F 28 4E 64 FC ...
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	NO
Extension	Extended Key Usage (2.5.29.37)

GeoTrust Global CA
Google Internet Authority G2
www.google.com

Google Internet Authority G2
Intermediate certificate authority
Expires: Saturday 4 April 2015 17 h 15 min 55 s Central European Summer Time
This certificate is valid

Trust
Details

Subject Name	
Country	US
Organization	Google Inc
Common Name	Google Internet Authority G2
Issuer Name	
Country	US
Organization	GeoTrust Inc.
Common Name	GeoTrust Global CA
Serial Number	146025
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Friday 5 April 2013 17 h 15 min 55 s Central European Summer Time
Not Valid After	Saturday 4 April 2015 17 h 15 min 55 s Central European Summer Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : 9C 2A 04 77 5C D8 50 91 ...
Exponent	65537
Key Size	2048 bits
Key Usage	Verify
Signature	256 bytes : 36 D7 06 80 11 27 AD 2A ...
Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Key Cert Sign, CRL Sign
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES

GeoTrust Global CA
Google Internet Authority G2
www.google.com

GeoTrust Global CA
Root certificate authority
Expires: Saturday 21 May 2022 06 h 00 min 00 s Central European Summer Time
This certificate is valid

Trust
Details

Subject Name	
Country	US
Organization	GeoTrust Inc.
Common Name	GeoTrust Global CA
Issuer Name	
Country	US
Organization	GeoTrust Inc.
Common Name	GeoTrust Global CA
Serial Number	144470
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Tuesday 21 May 2002 06 h 00 min 00 s Central European Summer Time
Not Valid After	Saturday 21 May 2022 06 h 00 min 00 s Central European Summer Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : DA CC 18 63 30 FD F4 17 ...
Exponent	65537
Key Size	2048 bits
Key Usage	Any
Signature	256 bytes : 35 E3 29 6A E5 2F 5D 54 ...
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : A4 78 79 A6 79 86 3B 88 C3 11 C4 A8 35 E0 D3 F1 F3 31 6D 0F F5 66 50 8D 98 E0 57 50 62 00 FC 02 E4 62 7C 0F 9F AA FC 62 70 49 22 ED 37 75 4A B6 78 CE 57 67 02 36 C0 48 E7 C2 D1 E4 23 88 C7 E8 25 3A 2C AE 45 E0 42 0B F9 76 CD 3E F2 55 37 76 8A 15 5E 8A 9E 99 E2 4A 52 28 73 23 F8 7E ED C7 F5 D8 CE FF EC 46 CC 23 94 5A 0C 15 0F 4C 79 99 1D E0 ED 93 7F 17 51 8B 01 AD 2F 77 9C 80 AA E1 50 D4 03 1C 86 04 AB 06 49 2D A5 F7 04 6F 97 87 E1 74 30 E6 82 E4 39 71 10 CA 9F FA 6A 75 81 2A 02 AC 45 54 48 DA 9B 08 DC 51 64 81 B1 69 6A 4A 7D FB 7C 8F 6C FC C6 43 0B 37 CC C3 3E 80 85 E1 4C AD 13 4B D2 82 76 63 77 15 74 1C 62 0D 57 6A 8C 64 BE 00 6E 6A 21 4C FF 02 C8 C7 34 BD C9 12 C6 B9 E4 E4 AB 30 5B 98 08 F0 B3 60 33 00 54 B2 B3 8A A6 57 E4 6D B9 73 47 BF AA 1D 1B 48 AE 3F
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Derive
Signature	256 bytes : 3A 8F DA 0F 28 4E 64 FC 55 F9 B1 B2 D8 E2 9E F1 B2 79 6D 9D D1 C3 37 5A 32 CE 66 FC F9 C9 A4 7B A5 BF 78 51 EC 63 48 3E CD 47 94 05 6D F3 6F 41 0C 06 73 57 58 D4 C2 07 56 95 21 C4 46 7B C1 94 0C 30 27 03 34 97 31 00 5E 06 2B 0D 6F AF 64 9F 6B A7 B5 2E D1 6E 52 FC DF EF 07 EF CE D1 80 87 97 B9 C6 A1 AF 79 02 A1 CE B5 A1 37 A6 23 41 C4 23 8D CE 0E D5 48 B8 51 03 34 90 C4 D7 0A AC 1E 47 59 79 C9 CD 48 6F 48 67 24 A9 2B 6B 24 AF 7A C7 EE A5 24 6C FD 65 93 36 C5 BE C9 C5 53 2A 77 00 94 B8 89 BF 7E E3 13 EB EB 91 90 7D 48 BF F2 F8 28 49 5B CE CB 96 37 AD 3F D4 DC 2B 48 F6 D3 E8 0D 26 53 60 64 E5 E8 82 C3 C4 96 BC 74 41 98 99 32 87 82 3C 89 1E 66 CA CD EB 35 DC DF C1 37 5F 17 52 5B D3 9E 31 1A 89 F4 17 BC 98 FD CA 9A 9C 30 75 05 3E 39 2A C0 8D 47 4B 26 F5 89 1B 61
Extension	
Basic Constraints (2.5.29.19)	
Critical	YES
Certificate Authority	NO
Extension	
Extended Key Usage (2.5.29.37)	
Critical	NO
Purpose #1	Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose #2	Client Authentication (1.3.6.1.5.5.7.3.2)
Extension	
Subject Key Identifier (2.5.29.14)	
Critical	NO
Key ID	75 20 EA D1 F9 B9 B7 34 D5 E9 E4 35 8A AE E8 64 C6 73 2B A4
Extension	
Authority Key Identifier (2.5.29.35)	
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	
Subject Alternative Name (2.5.29.17)	
Critical	NO
DNS Name	www.google.com
Extension	
Certificate Policies (2.5.29.32)	
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	
CRL Distribution Points (2.5.29.31)	
Critical	NO
URI	http://aki.google.com/GIAG2.crl

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : 9C 2A 04 77 5C D8 50 91 3A 06 A3 82 E0 D8 50 48 BC 89 3F F1 19 70 1A 88 46 7E E0 8F C5 F1 89 CE 21 EE 5A FE 61 0D B7 32 44 89 A0 74 0B 53 4F 55 A4 CE 82 62 95 EE EB 59 5F C6 E1 05 80 12 C4 5E 94 3F BC 58 48 38 F4 53 F7 24 E6 FB 91 E9 15 C4 CF F4 53 0D F4 4A FC 9F 54 DE 7D BE A0 68 6F 87 C0 D0 50 1F 28 30 03 40 DA 08 73 51 6C 7F FF 3A 3C A7 37 06 8E BD 48 11 04 EB 7D 24 DE E6 F9 FC 31 71 FB 94 D5 60 F3 2E 4A AF 42 D2 CB EA C4 6A 1A B2 CC 53 DD 15 48 88 1F C8 19 61 1F CD 9D A8 3E 63 2B 84 35 69 65 84 C8 19 C5 46 22 F8 53 95 BE E3 80 4A 10 C6 2A EC BA 97 20 11 C7 39 99 10 04 A0 F0 61 7A 95 25 8C 4E 52 75 E2 B6 ED 08 CA 14 FC CE 22 6A B3 4E CF 46 03 97 97 03 7E C0 B1 DE 78 AF 45 33 CF BA 3E 71 B7 DE F4 25 25 C2 0D 35 89 9D 9D FB 0E 11 79 89 1E 37 C5 AF 8E 72 69
Exponent	65537
Key Size	2048 bits
Key Usage	Verify
Signature	256 bytes : 36 D7 06 80 11 27 AD 2A 14 9B 38 77 B3 23 A0 75 58 B8 B1 7E 83 42 BA 72 DA 1E D8 8E 36 06 97 E0 F0 95 3B 37 FD 1B 42 58 FE 22 C8 6B BD 38 5E D1 3B 25 6E 12 EB 5E 67 76 46 40 90 DA 14 C8 78 0D ED 95 66 DA 8E 86 6F 80 A1 BA 56 32 95 86 DC DC 6A CA 04 8C 5B 7F F6 BF CC 6F 85 03 58 C3 68 51 13 CD FD C8 F7 79 3D 99 35 F0 56 A3 BD E0 59 ED 4F 44 09 A3 9E 38 7A F6 46 D1 1D 12 9D 4F BE D0 40 FC 55 FE 06 5E 3C DA 1C 56 BD 96 51 7B 6F 57 2A DB A2 AA 96 DC 8C 74 C2 95 BE F0 6E 95 13 FF 17 F0 3C AC B2 10 8D CC 73 FB E8 8F 02 C6 F0 FB 33 B3 95 3B E3 C2 CB 68 58 73 DB A8 24 62 3B 06 35 9D 0D A9 33 BD 78 03 90 2E 4C 78 5D 50 3A 81 D4 EE A0 C8 70 38 DC B2 F9 67 FA 87 40 5D 61 C0 51 8F 6B 83 6B CD 05 3A CA E1 A7 05 78 FC CA DA 94 D0 2C 08 3D 7E 16 79 C8 A0 50 20 24 54 33 71
Extension	
Key Usage (2.5.29.15)	
Critical	YES
Usage	Key Cert Sign, CRL Sign
Extension	
Basic Constraints (2.5.29.19)	
Critical	YES
Certificate Authority	YES
Path Length Constraint	0
Extension	
Subject Key Identifier (2.5.29.14)	
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	
Authority Key Identifier (2.5.29.35)	
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	
Certificate Policies (2.5.29.32)	
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	
CRL Distribution Points (2.5.29.31)	
Critical	NO
URI	http://crl.geotrust.com/crls/gtglobal.crl
Extension	
Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)	
Critical	NO

Issuer Name	
Country	US
Organization	GeoTrust Inc.
Common Name	GeoTrust Global CA
Serial Number	
Version	3
Signature Algorithm	
Parameters	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Not Valid Before	Tuesday 21 May 2002 06 h 00 min 00 s Central European Summer Time
Not Valid After	Saturday 21 May 2022 06 h 00 min 00 s Central European Summer Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : DA CC 18 63 30 FD F4 17 23 1A 56 7E 58 DF 3C 6C 38 E4 71 B7 78 91 D4 BC A1 D8 4C F8 A8 43 B6 03 E9 4D 21 07 08 88 DA 58 2F 66 39 29 BD 05 78 88 9D 38 E8 05 B7 6A 7E 71 A4 E6 C4 60 A6 80 EF 80 E4 89 28 0F 9E 25 D6 ED 83 F3 AD A6 91 C7 98 C9 42 18 35 14 9D AD 98 46 92 2E 4F CA F1 87 43 C1 16 95 57 2D 50 EF 89 2D 80 7A 57 AD F2 EE 5F 68 D2 00 8D B9 14 F8 14 15 35 D9 C0 46 A3 7B 72 C8 91 BF C9 55 2B CD D0 97 3E 9C 26 64 CC DF CE 83 19 71 CA 4E E6 D4 D5 7B A9 19 CD 55 DE C8 EC D2 5E 38 53 E5 5C 4F 8C 2D FE 50 23 36 FC 66 E6 C8 8E A4 39 19 00 87 95 02 39 91 08 0E FE 38 2E D1 1D 05 9A F6 4D 3E 6F 0F 07 1D AF 2C 1E 8F 60 39 E2 FA 36 53 13 39 D4 5E 26 28 DB 3D A8 14 BD 32 EB 18 03 28 52 04 71 E5 A8 33 3D E1 38 B8 07 36 84 62 9C 79 EA 16 30 F4 5F C0 2B E8 71 6B E4 F9
Exponent	65537
Key Size	2048 bits
Key Usage	Any
Signature	256 bytes : 35 E3 29 6A E5 2F 5D 54 8E 29 50 94 9F 99 1A 14 E4 8F 78 2A 62 94 A2 27 67 9E D0 CF 1A 5E 47 E9 C1 B2 A4 CF DD 41 1A 05 4E 9B 4B EE 4A 6F 55 52 B3 24 A1 37 0A EB 64 76 2A 2E 2C F3 FD 38 75 90 BF FA 71 D8 C7 3D 37 D2 B5 05 95 62 B9 A6 DE 89 3D 36 7B 38 77 48 97 AC A6 20 8F 2E A6 C9 0C C2 B2 99 45 00 C7 CE 11 51 22 22 E0 A5 EA B6 15 48 09 64 EA 5E 4F 74 F7 05 3E C7 8A 52 0C DB 15 B4 BD 6D 98 E5 C6 B1 54 68 A9 E3 69 90 B6 9A A5 0F B8 B9 3F 20 7D AE 4A B5 B8 9C E4 1D B6 AB E6 94 A5 C1 C7 83 AD DB F5 27 87 0E 04 6C D5 FF DD A0 5D ED 87 52 B7 2B 15 02 AE 39 A6 6A 74 E9 DA C4 E7 BC 4D 34 1E A9 5C 4D 33 5F 92 09 2F 88 66 5D 77 97 C7 1D 76 13 A9 D5 E5 F1 16 09 11 35 D5 AC DB 24 71 70 2C 98 56 0B D9 17 B4 D1 E3 51 2B 5E 75 E8 D5 D0 DC 4F 34 ED C2 05 66 80 A1 CB E6 33
Extension	
Basic Constraints (2.5.29.19)	
Critical	YES
Certificate Authority	YES
Extension	
Subject Key Identifier (2.5.29.14)	
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	
Authority Key Identifier (2.5.29.35)	
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Public Key	256 bytes : A4 78 79 A6 79 86 3B 88 C3 11 C4 A8 35 E0 D3 F1 F3 31 6D 0F F5 66 50 8D 98 E0 57 50 62 00 FC 02 E4 62 7C 0F 9F AA FC 62 70 49 22 ED 37 75 4A B6 78 CE 57 67 02 36 C0 48 E7 C2 D1 E4 23 88 C7 E8 25 3A 2C AE 45 E0 42 0B F9 76 CD 3E F2 55 37 76 8A 15 5E 8A 9E 99 E2 4A 52 28 73 23 F8 7E ED C7 F5 D8 CE FF EC 46 CC 23 94 5A 0C 15 0F 4C 79 99 1D E0 ED 93 7F 17 51 8B 01 AD 2F 77 9C 80 AA E1 50 D4 03 1C B6 04 AB 06 49 2D A5 F7 04 6F 97 87 E1 74 30 E6 82 E4 39 71 10 CA 9F FA 6A 75 81 2A 02 AC 45 54 48 DA 9B 08 DC 51 64 81 B1 69 6A 4A 7D FB 7C 8F 6C FC C6 43 0B 37 CC C3 3E 80 85 E1 4C AD 13 4B D2 82 76 63 77 15 74 1C 62 0D 57 6A 8C 64 BE 00 6E 6A 21 4C FF 02 C8 C7 34 BD C9 12 C6 B9 E4 E4 AB 30 5B 98 08 F0 B3 60 33 00 54 B2 B3 8A A6 57 E4 6D B9 73 47 BF AA 1D 1B 48 AE 3F
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Derive
Signature	256 bytes : 3A 8F DA 0F 28 4E 64 FC 55 F9 B1 B2 D8 E2 9E F1 B2 79 6D 9D D1 C3 37 5A 32 CE 66 FC F9 C9 A4 7B A5 BF 78 51 EC 63 48 3E CD 47 94 05 6D F3 6F 41 0C 06 73 57 58 D4 C2 07 56 95 21 C4 46 7B C1 94 0C 30 27 03 34 97 31 00 5E 06 2B 0D 6F AF 64 9F 6B A7 B5 2E D1 6E 52 FC DF EF 07 EF CE D1 80 87 97 B9 C6 A1 AF 79 02 A1 CE B5 A1 37 A6 23 41 C4 23 8D CE 0E D5 48 B8 51 03 34 90 C4 D7 0A AC 1E 47 59 79 C9 CD 48 6F 48 67 24 A9 2B 6B 24 AF 7A C7 EE A5 24 6C FD 65 93 36 C5 BE C9 C5 53 2A 77 00 94 B8 89 BF 7E E3 13 EB EB 91 90 7D 48 BF F2 F8 28 49 5B CE CB 96 37 AD 3F D4 DC 2B 48 F6 D3 E8 0D 26 53 60 64 E5 E8 82 C3 C4 96 BC 74 41 98 99 32 87 82 3C 89 1E 66 CA CD EB 35 DC DF C1 37 5F 17 52 5B D3 9E 31 1A 89 F4 17 BC 98 FD CA 9A 9C 30 75 05 3E 39 2A C0 8D 47 4B 26 F5 89 1B 61
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	NO
Extension	Extended Key Usage (2.5.29.37)
Critical	NO
Purpose #1	Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose #2	Client Authentication (1.3.6.1.5.5.7.3.2)
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	75 20 EA D1 F9 B9 B7 34 D5 E9 E4 35 8A AE E8 64 C6 73 2B A4
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	Subject Alternative Name (2.5.29.17)
Critical	NO
DNS Name	www.google.com
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://aki.google.com/GIAG2.crl

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : 9C 2A 04 77 5C D8 50 91 3A 06 A3 82 E0 D8 50 48 BC 89 3F F1 19 70 1A 88 46 7E E0 8F C5 F1 89 CE 21 EE 5A FE 61 0D B7 32 44 89 A0 74 0B 53 4F 55 A4 CE 82 62 95 EE EB 59 5F C6 E1 05 80 12 C4 5E 94 3F BC 58 48 38 F4 53 F7 24 E6 FB 91 E9 15 C4 CF F4 53 0D F4 4A FC 9F 54 DE 7D BE A0 6B 6F 87 C0 D0 50 1F 28 30 03 40 DA 08 73 51 6C 7F FF 3A 3C A7 37 06 8E BD 4B 11 04 EB 7D 24 DE E6 F9 FC 31 71 FB 94 D5 60 F3 2E 4A AF 42 D2 CB EA C4 6A 1A B2 CC 53 DD 15 4B 8B 1F C8 19 61 1F CD 9D A8 3E 63 2B 84 35 69 65 84 C8 19 C5 46 22 F8 53 95 BE E3 80 4A 10 C6 2A EC BA 97 20 11 C7 39 99 10 04 A0 F0 61 7A 95 25 8C 4E 52 75 E2 B6 ED 08 CA 14 FC CE 22 6A B3 4E CF 46 03 97 97 03 7E C0 B1 DE 78 AF 45 33 CF BA 3E 71 B7 DE F4 25 25 C2 0D 35 89 9D 9D FB 0E 11 79 89 1E 37 C5 AF 8E 72 69
Exponent	65537
Key Size	2048 bits
Key Usage	Verify
Signature	256 bytes : 36 D7 06 80 11 27 AD 2A 14 9B 38 77 B3 23 A0 75 58 B8 B1 7E 83 42 BA 72 DA 1E D8 8E 36 06 97 E0 F0 95 3B 37 FD 1B 42 58 FE 22 C8 6B BD 38 5E D1 3B 25 6E 12 EB 5E 67 76 46 40 90 DA 14 C8 78 0D ED 95 66 DA 8E 86 6F 80 A1 BA 56 32 95 86 DC DC 6A CA 04 8C 5B 7F F6 BF CC 6F 85 03 58 C3 68 51 13 CD FD C8 F7 79 3D 99 35 F0 56 A3 BD E0 59 ED 4F 44 09 A3 9E 38 7A F6 46 D1 1D 12 9D 4F BE D0 40 FC 55 FE 06 5E 3C DA 1C 56 BD 96 51 7B 6F 57 2A DB A2 AA 96 DC 8C 74 C2 95 BE F0 6E 95 13 FF 17 F0 3C AC B2 10 8D CC 73 FB E8 8F 02 C6 F0 FB 33 B3 95 3B E3 C2 CB 68 58 73 DB A8 24 62 3B 06 35 9D 0D A9 33 BD 78 03 90 2E 4C 78 5D 50 3A 81 D4 EE A0 C8 70 38 DC B2 F9 67 FA 87 40 5D 61 C0 51 8F 6B 83 6B CD 05 3A CA E1 A7 05 78 FC CA DA 94 D0 2C 08 3D 7E 16 79 C8 A0 50 20 24 54 33 71
Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Key Cert Sign, CRL Sign
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Path Length Constraint	0
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://crl.geotrust.com/crls/gtglobal.crl
Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO

Issuer Name	
Country	US
Organization	GeoTrust Inc.
Common Name	GeoTrust Global CA
Serial Number	144470
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Tuesday 21 May 2002 06 h 00 min 00 s Central European Summer Time
Not Valid After	Saturday 21 May 2022 06 h 00 min 00 s Central European Summer Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : DA CC 18 63 30 FD F4 17 23 1A 56 7E 58 DF 3C 6C 38 E4 71 B7 78 91 D4 BC A1 D8 4C F8 A8 43 B6 03 E9 4D 21 07 08 88 DA 58 2F 66 39 29 BD 05 78 88 9D 38 E8 05 B7 6A 7E 71 A4 E6 C4 60 A6 80 EF 80 E4 89 28 0F 9E 25 D6 ED 83 F3 AD A6 91 C7 98 C9 42 18 35 14 9D AD 98 46 92 2E 4F CA F1 87 43 C1 16 95 57 2D 50 EF 89 2D 80 7A 57 AD F2 EE 5F 68 D2 00 8D B9 14 F8 14 15 35 D9 C0 46 A3 7B 72 C8 91 BF C9 55 2B CD D0 97 3E 9C 26 64 CC DF CE 83 19 71 CA 4E E6 D4 D5 7B A9 19 CD 55 DE C8 EC D2 5E 38 53 E5 5C 4F 8C 2D FE 50 23 36 FC 66 E6 C8 8E A4 39 19 00 B7 95 02 39 91 08 0E FE 38 2E D1 1D 05 9A F6 4D 3E 6F 0F 07 1D AF 2C 1E 8F 60 39 E2 FA 36 53 13 39 D4 5E 26 28 DB 3D A8 14 BD 32 EB 18 03 28 52 04 71 E5 A8 33 3D E1 38 B8 07 36 84 62 9C 79 EA 16 30 F4 5F C0 2B E8 71 6B E4 F9
Exponent	65537
Key Size	2048 bits
Key Usage	Any
Signature	256 bytes : 35 E3 29 6A E5 2F 5D 54 8E 29 50 94 9F 99 1A 14 E4 8F 78 2A 62 94 A2 27 67 9E D0 CF 1A 5E 47 E9 C1 B2 A4 CF DD 41 1A 05 4E 9B 4B EE 4A 6F 55 52 B3 24 A1 37 0A EB 64 76 2A 2E 2C F3 FD 38 75 90 BF FA 71 D8 C7 3D 37 D2 B5 05 95 62 B9 A6 DE 89 3D 36 7B 38 77 48 97 AC A6 20 8F 2E A6 C9 0C C2 B2 99 45 00 C7 CE 11 51 22 22 E0 A5 EA B6 15 48 09 64 EA 5E 4F 74 F7 05 3E C7 8A 52 0C DB 15 B4 BD 6D 98 E5 C6 B1 54 68 A9 E3 69 90 B6 9A A5 0F B8 B9 3F 20 7D AE 4A B5 B8 9C E4 1D B6 AB E6 94 A5 C1 C7 83 AD DB F5 27 87 0E 04 6C D5 FF DD A0 5D ED 87 52 B7 2B 15 02 AE 39 A6 6A 74 E9 DA C4 E7 BC 4D 34 1E A9 5C 4D 33 5F 92 09 2F 88 66 5D 77 97 C7 1D 76 13 A9 D5 E5 F1 16 09 11 35 D5 AC DB 24 71 70 2C 98 56 0B D9 17 B4 D1 E3 51 2B 5E 75 E8 D5 D0 DC 4F 34 ED C2 05 66 80 A1 CB E6 33
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Public Key	256 bytes : A4 78 79 A6 79 86 3B 88 C3 11 C4 A8 35 E0 D3 F1 F3 31 6D 0F F5 66 50 8D 98 E0 57 50 62 00 FC 02 E4 62 7C 0F 9F AA FC 62 70 49 22 ED 37 75 4A B6 78 CE 57 67 02 36 C0 48 E7 C2 D1 E4 23 88 C7 E8 25 3A 2C AE 45 E0 42 0B F9 76 CD 3E F2 55 37 76 8A 15 5E 8A 9E 99 E2 4A 52 28 73 23 F8 7E ED C7 F5 D8 CE FF EC 46 CC 23 94 5A 0C 15 0F 4C 79 99 1D E0 ED 93 7F 17 51 8B 01 AD 2F 77 9C 80 AA E1 50 D4 03 1C B6 04 AB 06 49 2D A5 F7 04 6F 97 87 E1 74 30 E6 82 E4 39 71 10 CA 9F FA 6A 75 81 2A 02 AC 45 54 48 DA 9B 08 DC 51 64 81 B1 69 6A 4A 7D FB 7C 8F 6C FC C6 43 0B 37 CC C3 3E 80 85 E1 4C AD 13 4B D2 82 76 63 77 15 74 1C 62 0D 57 6A 8C 64 BE 00 6E 6A 21 4C FF 02 C8 C7 34 BD C9 12 C6 B9 E4 E4 AB 30 5B 98 08 F0 B3 60 33 00 54 B2 B3 8A A6 57 E4 6D B9 73 47 BF AA 1D 1B 48 AE 3F
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Derive
Signature	256 bytes : 3A 8F DA 0F 28 4E 64 FC 55 F9 B1 B2 D8 E2 9E F1 B2 79 6D 9D D1 C3 37 5A 32 CE 66 FC F9 C9 A4 7B A5 BF 78 51 EC 63 48 3E CD 47 94 05 6D F3 6F 41 0C 06 73 57 58 D4 C2 07 56 95 21 C4 46 7B C1 94 0C 30 27 03 34 97 31 00 5E 06 2B 0D 6F AF 64 9F 6B A7 B5 2E D1 6E 52 FC DF EF 07 EF CE D1 80 B7 97 B9 C6 A1 AF 79 02 A1 CE B5 A1 37 A6 23 41 C4 23 8D CE 0E D5 48 B8 51 03 34 90 C4 D7 0A AC 1E 47 59 79 C9 CD 48 6F 48 67 24 A9 2B 6B 24 AF 7A C7 EE A5 24 6C FD 65 93 36 C5 BE C9 C5 53 2A 77 00 94 B8 89 BF 7E E3 13 EB EB 91 90 7D 48 BF F2 F8 28 49 5B CE CB 96 37 AD 3F D4 DC 2B 48 F6 D3 E8 0D 26 53 60 64 E5 E8 82 C3 C4 96 BC 74 41 98 99 32 87 82 3C 89 1E 66 CA CD EB 35 DC DF C1 37 5F 17 52 5B D3 9E 31 1A 89 F4 17 BC 98 FD CA 9A 9C 30 75 05 3E 39 2A C0 8D 47 4B 26 F5 89 1B 61
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	NO
Extension	Extended Key Usage (2.5.29.37)
Critical	NO
Purpose #1	Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose #2	Client Authentication (1.3.6.1.5.5.7.3.2)
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	75 20 EA D1 F9 B9 B7 34 D5 E9 E4 35 8A AE E8 64 C6 73 2B A4
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	Subject Alternative Name (2.5.29.17)
Critical	NO
DNS Name	www.google.com
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://aki.google.com/GIAG2.crl

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : 9C 2A 04 77 5C D8 50 91 3A 06 A3 82 E0 D8 50 48 BC 89 3F F1 19 70 1A 88 46 7E E0 8F C5 F1 89 CE 21 EE 5A FE 61 0D B7 32 44 89 A0 74 0B 53 4F 55 A4 CE 82 62 95 EE EB 59 5F C6 E1 05 80 12 C4 5E 94 3F BC 58 48 38 F4 53 F7 24 E6 FB 91 E9 15 C4 CF F4 53 0D F4 4A FC 9F 54 DE 7D BE A0 6B 6F 87 C0 D0 50 1F 28 30 03 40 DA 08 73 51 6C 7F FF 3A 3C A7 37 06 8E BD 4B 11 04 EB 7D 24 DE E6 F9 FC 31 71 FB 94 D5 60 F3 2E 4A AF 42 D2 CB EA C4 6A 1A B2 CC 53 DD 15 4B 8B 1F C8 19 61 1F CD 9D A8 3E 63 2B 84 35 69 65 84 C8 19 C5 46 22 F8 53 95 BE E3 80 4A 10 C6 2A EC BA 97 20 11 C7 39 99 10 04 A0 F0 61 7A 95 25 8C 4E 52 75 E2 B6 ED 08 CA 14 FC CE 22 6A B3 4E CF 46 03 97 97 03 7E C0 B1 DE 78 AF 45 33 CF BA 3E 71 B7 DE F4 25 25 C2 0D 35 89 9D 9D FB 0E 11 79 89 1E 37 C5 AF 8E 72 69
Exponent	65537
Key Size	2048 bits
Key Usage	Verify
Signature	256 bytes : 36 D7 06 80 11 27 AD 2A 14 9B 38 77 B3 23 A0 75 58 B8 B1 7E 83 42 BA 72 DA 1E D8 8E 36 06 97 E0 F0 95 3B 37 FD 1B 42 58 FE 22 C8 6B BD 38 5E D1 3B 25 6E 12 EB 5E 67 76 46 40 90 DA 14 C8 78 0D ED 95 66 DA 8E 86 6F 80 A1 BA 56 32 95 86 DC DC 6A CA 04 8C 5B 7F F6 BF CC 6F 85 03 58 C3 68 51 13 CD FD C8 F7 79 3D 99 35 F0 56 A3 BD E0 59 ED 4F 44 09 A3 9E 38 7A F6 46 D1 1D 12 9D 4F BE D0 40 FC 55 FE 06 5E 3C DA 1C 56 BD 96 51 7B 6F 57 2A DB A2 AA 96 DC 8C 74 C2 95 BE F0 6E 95 13 FF 17 F0 3C AC B2 10 8D CC 73 FB E8 8F 02 C6 F0 FB 33 B3 95 3B E3 C2 CB 68 58 73 DB A8 24 62 3B 06 35 9D 0D A9 33 BD 78 03 90 2E 4C 78 5D 50 3A 81 D4 EE A0 C8 70 38 DC B2 F9 67 FA 87 40 5D 61 C0 51 8F 6B 83 6B CD 05 3A CA E1 A7 05 78 FC CA DA 94 D0 2C 08 3D 7E 16 79 C8 A0 50 20 24 54 33 71
Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Key Cert Sign, CRL Sign
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Path Length Constraint	0
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://crl.geotrust.com/crls/gtglobal.crl
Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO

Issuer Name	
Country	US
Organization	GeoTrust Inc.
Common Name	GeoTrust Global CA
Serial Number	144470
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Tuesday 21 May 2002 06 h 00 min 00 s Central European Summer Time
Not Valid After	Saturday 21 May 2022 06 h 00 min 00 s Central European Summer Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : DA CC 18 63 30 FD F4 17 23 1A 56 7E 58 DF 3C 6C 38 E4 71 B7 78 91 D4 BC A1 D8 4C F8 A8 43 B6 03 E9 4D 21 07 08 88 DA 58 2F 66 39 29 BD 05 78 88 9D 38 E8 05 B7 6A 7E 71 A4 E6 C4 60 A6 80 EF 80 E4 89 28 0F 9E 25 D6 ED 83 F3 AD A6 91 C7 98 C9 42 18 35 14 9D AD 98 46 92 2E 4F CA F1 87 43 C1 16 95 57 2D 50 EF 89 2D 80 7A 57 AD F2 EE 5F 68 D2 00 8D B9 14 F8 14 15 35 D9 C0 46 A3 7B 72 C8 91 BF C9 55 2B CD D0 97 3E 9C 26 64 CC DF CE 83 19 71 CA 4E E6 D4 D5 7B A9 19 CD 55 DE C8 EC D2 5E 38 53 E5 5C 4F 8C 2D FE 50 23 36 FC 66 E6 C8 8E A4 39 19 00 B7 95 02 39 91 08 0E FE 38 2E D1 1D 05 9A F6 4D 3E 6F 0F 07 1D AF 2C 1E 8F 60 39 E2 FA 36 53 13 39 D4 5E 26 28 DB 3D A8 14 BD 32 EB 18 03 28 52 04 71 E5 A8 33 3D E1 38 B8 07 36 84 62 9C 79 EA 16 30 F4 5F C0 2B E8 71 6B E4 F9
Exponent	65537
Key Size	2048 bits
Key Usage	Any
Signature	256 bytes : 35 E3 29 6A E5 2F 5D 54 8E 29 50 94 9F 99 1A 14 E4 8F 78 2A 62 94 A2 27 67 9E D0 CF 1A 5E 47 E9 C1 B2 A4 CF DD 41 1A 05 4E 9B 4B EE 4A 6F 55 52 B3 24 A1 37 0A EB 64 76 2A 2E 2C F3 FD 38 75 90 BF FA 71 D8 C7 3D 37 D2 B5 05 95 62 B9 A6 DE 89 3D 36 7B 38 77 48 97 AC A6 20 8F 2E A6 C9 0C C2 B2 99 45 00 C7 CE 11 51 22 22 E0 A5 EA B6 15 48 09 64 EA 5E 4F 74 F7 05 3E C7 8A 52 0C DB 15 B4 BD 6D 98 E5 C6 B1 54 68 A9 E3 69 90 B6 9A A5 0F B8 B9 3F 20 7D AE 4A B5 B8 9C E4 1D B6 AB E6 94 A5 C1 C7 83 AD DB F5 27 87 0E 04 6C D5 FF DD A0 5D ED 87 52 B7 2B 15 02 AE 39 A6 6A 74 E9 DA C4 E7 BC 4D 34 1E A9 5C 4D 33 5F 92 09 2F 88 66 5D 77 97 C7 1D 76 13 A9 D5 E5 F1 16 09 11 35 D5 AC DB 24 71 70 2C 98 56 0B D9 17 B4 D1 E3 51 2B 5E 75 E8 D5 D0 DC 4F 34 ED C2 05 66 80 A1 CB E6 33
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Public Key	256 bytes : A4 78 79 A6 79 86 3B 88 C3 11 C4 A8 35 E0 D3 F1 F3 31 6D 0F F5 66 50 8D 98 E0 57 50 62 00 FC 02 E4 62 7C 0F 9F AA FC 62 70 49 22 ED 37 75 4A B6 78 CE 57 67 02 36 C0 48 E7 C2 D1 E4 23 88 C7 E8 25 3A 2C AE 45 E0 42 0B F9 76 CD 3E F2 55 37 76 8A 15 5E 8A 9E 99 E2 4A 52 28 73 23 F8 7E ED C7 F5 D8 CE FF EC 46 CC 23 94 5A 0C 15 0F 4C 79 99 1D E0 ED 93 7F 17 51 8B 01 AD 2F 77 9C 80 AA E1 50 D4 03 1C B6 04 AB 06 49 2D A5 F7 04 6F 97 87 E1 74 30 E6 82 E4 39 71 10 CA 9F FA 6A 75 81 2A 02 AC 45 54 48 DA 9B 08 DC 51 64 81 B1 69 6A 4A 7D FB 7C 8F 6C FC C6 43 0B 37 CC C3 3E 80 85 E1 4C AD 13 4B D2 82 76 63 77 15 74 1C 62 0D 57 6A 8C 64 BE 00 6E 6A 21 4C FF 02 C8 C7 34 BD C9 12 C6 B9 E4 E4 AB 30 5B 98 08 F0 B3 60 33 00 54 B2 B3 8A A6 57 E4 6D B9 73 47 BF AA 1D 1B 48 AE 3F
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Derive
Signature	256 bytes : 3A 8F DA 0F 28 4E 64 FC 55 F9 B1 B2 D8 E2 9E F1 B2 79 6D 9D D1 C3 37 5A 32 CE 66 FC F9 C9 A4 7B A5 BF 78 51 EC 63 48 3E CD 47 94 05 6D F3 6F 41 0C 06 73 57 58 D4 C2 07 56 95 21 C4 46 7B C1 94 0C 30 27 03 34 97 31 00 5E 06 2B 0D 6F AF 64 9F 6B A7 B5 2E D1 6E 52 FC DF EF 07 EF CE D1 80 B7 97 B9 C6 A1 AF 79 02 A1 CE B5 A1 37 A6 23 41 C4 23 8D CE 0E D5 48 B8 51 03 34 90 C4 D7 0A AC 1E 47 59 79 C9 CD 48 6F 48 67 24 A9 2B 6B 24 AF 7A C7 EE A5 24 6C FD 65 93 36 C5 BE C9 C5 53 2A 77 00 94 B8 89 BF 7E E3 13 EB EB 91 90 7D 48 BF F2 F8 28 49 5B CE CB 96 37 AD 3F D4 DC 2B 48 F6 D3 E8 0D 26 53 60 64 E5 E8 82 C3 C4 96 BC 74 41 98 99 32 87 82 3C 89 1E 66 CA CD EB 35 DC DF C1 37 5F 17 52 5B D3 9E 31 1A 89 F4 17 BC 98 FD CA 9A 9C 30 75 05 3E 39 2A C0 8D 47 4B 26 F5 89 1B 61
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	NO
Extension	Extended Key Usage (2.5.29.37)
Critical	NO
Purpose #1	Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose #2	Client Authentication (1.3.6.1.5.5.7.3.2)
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	75 20 EA D1 F9 B9 B7 34 D5 E9 E4 35 8A AE E8 64 C6 73 2B A4
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	Subject Alternative Name (2.5.29.17)
Critical	NO
DNS Name	www.google.com
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://aki.google.com/GIAG2.crl

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : 9C 2A 04 77 5C D8 50 91 3A 06 A3 82 E0 D8 50 48 BC 89 3F F1 19 70 1A 88 46 7E E0 8F C5 F1 89 CE 21 EE 5A FE 61 0D B7 32 44 89 A0 74 0B 53 4F 55 A4 CE 82 62 95 EE EB 59 5F C6 E1 05 80 12 C4 5E 94 3F BC 58 48 38 F4 53 F7 24 E6 FB 91 E9 15 C4 CF F4 53 0D F4 4A FC 9F 54 DE 7D BE A0 6B 6F 87 C0 D0 50 1F 28 30 03 40 DA 08 73 51 6C 7F FF 3A 3C A7 37 06 8E BD 4B 11 04 EB 7D 24 DE E6 F9 FC 31 71 FB 94 D5 60 F3 2E 4A AF 42 D2 CB EA C4 6A 1A B2 CC 53 DD 15 4B 8B 1F C8 19 61 1F CD 9D A8 3E 63 2B 84 35 69 65 84 C8 19 C5 46 22 F8 53 95 BE E3 80 4A 10 C6 2A EC BA 97 20 11 C7 39 99 10 04 A0 F0 61 7A 95 25 8C 4E 52 75 E2 B6 ED 08 CA 14 FC CE 22 6A B3 4E CF 46 03 97 97 03 7E C0 B1 DE 78 AF 45 33 CF BA 3E 71 B7 DE F4 25 25 C2 0D 35 89 9D 9D FB 0E 11 79 89 1E 37 C5 AF 8E 72 69
Exponent	65537
Key Size	2048 bits
Key Usage	Verify
Signature	256 bytes : 36 D7 06 80 11 27 AD 2A 14 9B 38 77 B3 23 A0 75 58 B8 B1 7E 83 42 BA 72 DA 1E D8 8E 36 06 97 E0 F0 95 3B 37 FD 1B 42 58 FE 22 C8 6B BD 38 5E D1 3B 25 6E 12 EB 5E 67 76 46 40 90 DA 14 C8 78 0D ED 95 66 DA 8E 86 6F 80 A1 BA 56 32 95 86 DC DC 6A CA 04 8C 5B 7F F6 BF CC 6F 85 03 58 C3 68 51 13 CD FD C8 F7 79 3D 99 35 F0 56 A3 BD E0 59 ED 4F 44 09 A3 9E 38 7A F6 46 D1 1D 12 9D 4F BE D0 40 FC 55 FE 06 5E 3C DA 1C 56 BD 96 51 7B 6F 57 2A DB A2 AA 96 DC 8C 74 C2 95 BE F0 6E 95 13 FF 17 F0 3C AC B2 10 8D CC 73 FB E8 8F 02 C6 F0 FB 33 B3 95 3B E3 C2 CB 68 58 73 DB A8 24 62 3B 06 35 9D 0D A9 33 BD 78 03 90 2E 4C 78 5D 50 3A 81 D4 EE A0 C8 70 38 DC B2 F9 67 FA 87 40 5D 61 C0 51 8F 6B 83 6B CD 05 3A CA E1 A7 05 78 FC CA DA 94 D0 2C 08 3D 7E 16 79 C8 A0 50 20 24 54 33 71
Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Key Cert Sign, CRL Sign
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Path Length Constraint	0
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://crl.geotrust.com/crls/gtglobal.crl
Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO

Issuer Name	
Country	US
Organization	GeoTrust Inc.
Common Name	GeoTrust Global CA
Serial Number	144470
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Tuesday 21 May 2002 06 h 00 min 00 s Central European Summer Time
Not Valid After	Saturday 21 May 2022 06 h 00 min 00 s Central European Summer Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : DA CC 18 63 30 FD F4 17 23 1A 56 7E 58 DF 3C 6C 38 E4 71 B7 78 91 D4 BC A1 D8 4C F8 A8 43 B6 03 E9 4D 21 07 08 88 DA 58 2F 66 39 29 BD 05 78 88 9D 38 E8 05 B7 6A 7E 71 A4 E6 C4 60 A6 80 EF 80 E4 89 28 0F 9E 25 D6 ED 83 F3 AD A6 91 C7 98 C9 42 18 35 14 9D AD 98 46 92 2E 4F CA F1 87 43 C1 16 95 57 2D 50 EF 89 2D 80 7A 57 AD F2 EE 5F 6B D2 00 8D B9 14 F8 14 15 35 D9 C0 46 A3 7B 72 C8 91 BF C9 55 2B CD D0 97 3E 9C 26 64 CC DF CE 83 19 71 CA 4E E6 D4 D5 7B A9 19 CD 55 DE C8 EC D2 5E 38 53 E5 5C 4F 8C 2D FE 50 23 36 FC 66 E6 C8 8E A4 39 19 00 B7 95 02 39 91 08 0E FE 38 2E D1 1D 05 9A F6 4D 3E 6F 0F 07 1D AF 2C 1E 8F 60 39 E2 FA 36 53 13 39 D4 5E 26 28 DB 3D A8 14 BD 32 EB 18 03 28 52 04 71 E5 A8 33 3D E1 38 B8 07 36 84 62 9C 79 EA 16 30 F4 5F C0 2B E8 71 6B E4 F9
Exponent	65537
Key Size	2048 bits
Key Usage	Any
Signature	256 bytes : 35 E3 29 6A E5 2F 5D 54 8E 29 50 94 9F 99 1A 14 E4 8F 78 2A 62 94 A2 27 67 9E D0 CF 1A 5E 47 E9 C1 B2 A4 CF DD 41 1A 05 4E 9B 4B EE 4A 6F 55 52 B3 24 A1 37 0A EB 64 76 2A 2E 2C F3 FD 38 75 90 BF FA 71 D8 C7 3D 37 D2 B5 05 95 62 B9 A6 DE 89 3D 36 7B 38 77 48 97 AC A6 20 8F 2E A6 C9 0C C2 B2 99 45 00 C7 CE 11 51 22 22 E0 A5 EA B6 15 48 09 64 EA 5E 4F 74 F7 05 3E C7 8A 52 0C DB 15 B4 BD 6D 98 E5 C6 B1 54 68 A9 E3 69 90 B6 9A A5 0F B8 B9 3F 20 7D AE 4A B5 B8 9C E4 1D B6 AB E6 94 A5 C1 C7 83 AD DB F5 27 87 0E 04 6C D5 FF DD A0 5D ED 87 52 B7 2B 15 02 AE 39 A6 6A 74 E9 DA C4 E7 BC 4D 34 1E A9 5C 4D 33 5F 92 09 2F 88 66 5D 77 97 C7 1D 76 13 A9 D5 E5 F1 16 09 11 35 D5 AC DB 24 71 70 2C 98 56 0B D9 17 B4 D1 E3 51 2B 5E 75 E8 D5 D0 DC 4F 34 ED C2 05 66 80 A1 CB E6 33
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Public Key	256 bytes : A4 78 79 A6 79 86 3B 88 C3 11 C4 A8 35 E0 D3 F1 F3 31 6D 0F F5 66 50 8D 98 E0 57 50 62 00 FC 02 E4 62 7C 0F 9F AA FC 62 70 49 22 ED 37 75 4A B6 78 CE 57 67 02 36 C0 48 E7 C2 D1 E4 23 88 C7 E8 25 3A 2C AE 45 E0 42 0B F9 76 CD 3E F2 55 37 76 8A 15 5E 8A 9E 99 E2 4A 52 28 73 23 F8 7E ED C7 F5 D8 CE FF EC 46 CC 23 94 5A 0C 15 0F 4C 79 99 1D E0 ED 93 7F 17 51 8B 01 AD 2F 77 9C 80 AA E1 50 D4 03 1C B6 04 AB 06 49 2D A5 F7 04 6F 97 87 E1 74 30 E6 82 E4 39 71 10 CA 9F FA 6A 75 81 2A 02 AC 45 54 48 DA 9B 08 DC 51 64 81 B1 69 6A 4A 7D FB 7C 8F 6C FC C6 43 0B 37 CC C3 3E 80 85 E1 4C AD 13 4B D2 82 76 63 77 15 74 1C 62 0D 57 6A 8C 64 BE 00 6E 6A 21 4C FF 02 C8 C7 34 BD C9 12 C6 B9 E4 E4 AB 30 5B 98 08 F0 B3 60 33 00 54 B2 B3 8A A6 57 E4 6D B9 73 47 BF AA 1D 1B 48 AE 3F
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Derive
Signature	256 bytes : 3A 8F DA 0F 28 4E 64 FC 55 F9 B1 B2 D8 E2 9E F1 B2 79 6D 9D D1 C3 37 5A 32 CE 66 FC F9 C9 A4 7B A5 BF 78 51 EC 63 48 3E CD 47 94 05 6D F3 6F 41 0C 06 73 57 58 D4 C2 07 56 95 21 C4 46 7B C1 94 0C 30 27 03 34 97 31 00 5E 06 2B 0D 6F AF 64 9F 6B A7 B5 2E D1 6E 52 FC DF EF 07 EF CE D1 80 B7 97 B9 C6 A1 AF 79 02 A1 CE B5 A1 37 A6 23 41 C4 23 8D CE 0E D5 48 B8 51 03 34 90 C4 D7 0A AC 1E 47 59 79 C9 CD 48 6F 48 67 24 A9 2B 6B 24 AF 7A C7 EE A5 24 6C FD 65 93 36 C5 BE C9 C5 53 2A 77 00 94 B8 89 BF 7E E3 13 EB EB 91 90 7D 48 BF F2 F8 28 49 5B CE CB 96 37 AD 3F D4 DC 2B 48 F6 D3 E8 0D 26 53 60 64 E5 E8 82 C3 C4 96 BC 74 41 98 99 32 87 82 3C 89 1E 66 CA CD EB 35 DC DF C1 37 5F 17 52 5B D3 9E 31 1A 89 F4 17 BC 98 FD CA 9A 9C 30 75 05 3E 39 2A C0 8D 47 4B 26 F5 89 1B 61
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	NO
Extension	Extended Key Usage (2.5.29.37)
Critical	NO
Purpose #1	Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose #2	Client Authentication (1.3.6.1.5.5.7.3.2)
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	75 20 EA D1 F9 B9 B7 34 D5 E9 E4 35 8A AE E8 64 C6 73 2B A4
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	Subject Alternative Name (2.5.29.17)
Critical	NO
DNS Name	www.google.com
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://aki.google.com/GIAG2.crl

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : 9C 2A 04 77 5C D8 50 91 3A 06 A3 82 E0 D8 50 48 BC 89 3F F1 19 70 1A 88 46 7E E0 8F C5 F1 89 CE 21 EE 5A FE 61 0D B7 32 44 89 A0 74 0B 53 4F 55 A4 CE 82 62 95 EE EB 59 5F C6 E1 05 80 12 C4 5E 94 3F BC 58 48 38 F4 53 F7 24 E6 FB 91 E9 15 C4 CF F4 53 0D F4 4A FC 9F 54 DE 7D BE A0 6B 6F 87 C0 D0 50 1F 28 30 03 40 DA 08 73 51 6C 7F FF 3A 3C A7 37 06 8E BD 4B 11 04 EB 7D 24 DE E6 F9 FC 31 71 FB 94 D5 60 F3 2E 4A AF 42 D2 CB EA C4 6A 1A B2 CC 53 DD 15 4B 8B 1F C8 19 61 1F CD 9D A8 3E 63 2B 84 35 69 65 84 C8 19 C5 46 22 F8 53 95 BE E3 80 4A 10 C6 2A EC BA 97 20 11 C7 39 99 10 04 A0 F0 61 7A 95 25 8C 4E 52 75 E2 B6 ED 08 CA 14 FC CE 22 6A B3 4E CF 46 03 97 97 03 7E C0 B1 DE 78 AF 45 33 CF BA 3E 71 B7 DE F4 25 25 C2 0D 35 89 9D 9D FB 0E 11 79 89 1E 37 C5 AF 8E 72 69
Exponent	65537
Key Size	2048 bits
Key Usage	Verify
Signature	256 bytes : 36 D7 06 80 11 27 AD 2A 14 9B 38 77 B3 23 A0 75 58 B8 B1 7E 83 42 BA 72 DA 1E D8 8E 36 06 97 E0 F0 95 3B 37 FD 1B 42 58 FE 22 C8 6B BD 38 5E D1 3B 25 6E 12 EB 5E 67 76 46 40 90 DA 14 C8 78 0D ED 95 66 DA 8E 86 6F 80 A1 BA 56 32 95 86 DC DC 6A CA 04 8C 5B 7F F6 BF CC 6F 85 03 58 C3 68 51 13 CD FD C8 F7 79 3D 99 35 F0 56 A3 BD E0 59 ED 4F 44 09 A3 9E 38 7A F6 46 D1 1D 12 9D 4F BE D0 40 FC 55 FE 06 5E 3C DA 1C 56 BD 96 51 7B 6F 57 2A DB A2 AA 96 DC 8C 74 C2 95 BE F0 6E 95 13 FF 17 F0 3C AC B2 10 8D CC 73 FB E8 8F 02 C6 F0 FB 33 B3 95 3B E3 C2 CB 68 58 73 DB A8 24 62 3B 06 35 9D 0D A9 33 BD 78 03 90 2E 4C 78 5D 50 3A 81 D4 EE A0 C8 70 38 DC B2 F9 67 FA 87 40 5D 61 C0 51 8F 6B 83 6B CD 05 3A CA E1 A7 05 78 FC CA DA 94 D0 2C 08 3D 7E 16 79 C8 A0 50 20 24 54 33 71
Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Key Cert Sign, CRL Sign
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Path Length Constraint	0
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://crl.geotrust.com/crls/gtglobal.crl
Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO

Issuer Name	
Country	US
Organization	GeoTrust Inc.
Common Name	GeoTrust Global CA
Serial Number	144470
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Tuesday 21 May 2002 06 h 00 min 00 s Central European Summer Time
Not Valid After	Saturday 21 May 2022 06 h 00 min 00 s Central European Summer Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : DA CC 18 63 30 FD F4 17 23 1A 56 7E 58 DF 3C 6C 38 E4 71 B7 78 91 D4 BC A1 D8 4C F8 A8 43 B6 03 E9 4D 21 07 08 88 DA 58 2F 66 39 29 BD 05 78 8B 9D 38 E8 05 B7 6A 7E 71 A4 E6 C4 60 A6 80 EF 80 E4 89 28 0F 9E 25 D6 ED 83 F3 AD A6 91 C7 98 C9 42 18 35 14 9D AD 98 46 92 2E 4F CA F1 87 43 C1 16 95 57 2D 50 EF 89 2D 80 7A 57 AD F2 EE 5F 6B D2 00 8D B9 14 F8 14 15 35 D9 C0 46 A3 7B 72 C8 91 BF C9 55 2B CD D0 97 3E 9C 26 64 CC DF CE 83 19 71 CA 4E E6 D4 D5 7B A9 19 CD 55 DE C8 EC D2 5E 38 53 E5 5C 4F 8C 2D FE 50 23 36 FC 66 E6 C8 8E A4 39 19 00 B7 95 02 39 91 0B 0E FE 38 2E D1 1D 05 9A F6 4D 3E 6F 0F 07 1D AF 2C 1E 8F 60 39 E2 FA 36 53 13 39 D4 5E 26 28 DB 3D A8 14 BD 32 EB 18 03 28 52 04 71 E5 A8 33 3D E1 38 B8 07 36 84 62 9C 79 EA 16 30 F4 5F C0 2B E8 71 6B E4 F9
Exponent	65537
Key Size	2048 bits
Key Usage	Any
Signature	256 bytes : 35 E3 29 6A E5 2F 5D 54 8E 29 50 94 9F 99 1A 14 E4 8F 78 2A 62 94 A2 27 67 9E D0 CF 1A 5E 47 E9 C1 B2 A4 CF DD 41 1A 05 4E 9B 4B EE 4A 6F 55 52 B3 24 A1 37 0A EB 64 76 2A 2E 2C F3 FD 38 75 90 BF FA 71 D8 C7 3D 37 D2 B5 05 95 62 B9 A6 DE 89 3D 36 7B 38 77 48 97 AC A6 20 8F 2E A6 C9 0C C2 B2 99 45 00 C7 CE 11 51 22 22 E0 A5 EA B6 15 48 09 64 EA 5E 4F 74 F7 05 3E C7 8A 52 0C DB 15 B4 BD 6D 98 E5 C6 B1 54 68 A9 E3 69 90 B6 9A A5 0F B8 B9 3F 20 7D AE 4A B5 B8 9C E4 1D B6 AB E6 94 A5 C1 C7 83 AD DB F5 27 87 0E 04 6C D5 FF DD A0 5D ED 87 52 B7 2B 15 02 AE 39 A6 6A 74 E9 DA C4 E7 BC 4D 34 1E A9 5C 4D 33 5F 92 09 2F 88 66 5D 77 97 C7 1D 76 13 A9 D5 E5 F1 16 09 11 35 D5 AC DB 24 71 70 2C 98 56 0B D9 17 B4 D1 E3 51 2B 5E 75 E8 D5 D0 DC 4F 34 ED C2 05 66 80 A1 CB E6 33
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Public Key	256 bytes : A4 78 79 A6 79 86 3B 88 C3 11 C4 A8 35 E0 D3 F1 F3 31 6D 0F F5 66 50 8D 98 E0 57 50 62 00 FC 02 E4 62 7C 0F 9F AA FC 62 70 49 22 ED 37 75 4A B6 78 CE 57 67 02 36 C0 4B E7 C2 D1 E4 23 88 C7 E8 25 3A 2C AE 45 E0 42 0B F9 76 CD 3E F2 55 37 76 8A 15 5E 8A 9E 99 E2 4A 52 28 73 23 F8 7E ED C7 F5 D8 CE FF EC 46 CC 23 94 5A 0C 15 0F 4C 79 99 1D E0 ED 93 7F 17 51 8B 01 AD 2F 77 9C 80 AA E1 50 D4 03 1C B6 04 AB 06 49 2D A5 F7 04 6F 97 87 E1 74 30 E6 82 E4 39 71 10 CA 9F FA 6A 75 81 2A 02 AC 45 54 48 DA 9B 08 DC 51 64 81 B1 69 6A 4A 7D FB 7C 8F 6C FC C6 43 0B 37 CC C3 3E 80 85 E1 4C AD 13 4B D2 82 76 63 77 15 74 1C 62 0D 57 6A 8C 64 BE 00 6E 6A 21 4C FF 02 C8 C7 34 BD C9 12 C6 B9 E4 E4 AB 30 5B 98 08 F0 B3 60 33 00 54 B2 B3 8A A6 57 E4 6D B9 73 47 BF AA 1D 1B 48 AE 3F
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Derive
Signature	256 bytes : 3A 8F DA 0F 28 4E 64 FC 55 F9 B1 B2 D8 E2 9E F1 B2 79 6D 9D D1 C3 37 5A 32 CE 66 FC F9 C9 A4 7B A5 BF 78 51 EC 63 48 3E CD 47 94 05 6D F3 6F 41 0C 06 73 57 58 D4 C2 07 56 95 21 C4 46 7B C1 94 0C 30 27 03 34 97 31 00 5E 06 2B 0D 6F AF 64 9F 6B A7 B5 2E D1 6E 52 FC DF EF 07 EF CE D1 80 B7 97 B9 C6 A1 AF 79 02 A1 CE B5 A1 37 A6 23 41 C4 23 8D CE 0E D5 48 B8 51 03 34 90 C4 D7 0A AC 1E 47 59 79 C9 CD 48 6F 48 67 24 A9 2B 6B 24 AF 7A C7 EE A5 24 6C FD 65 93 36 C5 BE C9 C5 53 2A 77 00 94 B8 89 BF 7E E3 13 EB EB 91 90 7D 48 BF F2 F8 28 49 5B CE CB 96 37 AD 3F D4 DC 2B 48 F6 D3 E8 0D 26 53 60 64 E5 E8 82 C3 C4 96 BC 74 41 98 99 32 87 82 3C 89 1E 66 CA CD EB 35 DC DF C1 37 5F 17 52 5B D3 9E 31 1A 89 F4 17 BC 98 FD CA 9A 9C 30 75 05 3E 39 2A C0 8D 47 4B 26 F5 89 1B 61
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	NO
Extension	Extended Key Usage (2.5.29.37)
Critical	NO
Purpose #1	Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose #2	Client Authentication (1.3.6.1.5.5.7.3.2)
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	75 20 EA D1 F9 B9 B7 34 D5 E9 E4 35 8A AE E8 64 C6 73 2B A4
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	Subject Alternative Name (2.5.29.17)
Critical	NO
DNS Name	www.google.com
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://aki.google.com/GIAG2.crl

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Public Key	256 bytes : 9C 2A 04 77 5C D8 50 91 3A 06 A3 82 E0 D8 50 48 BC 89 3F F1 19 70 1A 88 46 7E E0 8F C5 F1 89 CE 21 EE 5A FE 61 0D B7 32 44 89 A0 74 0B 53 4F 55 A4 CE 82 62 95 EE EB 59 5F C6 E1 05 80 12 C4 5E 94 3F BC 58 48 38 F4 53 F7 24 E6 FB 91 E9 15 C4 CF F4 53 0D F4 4A FC 9F 54 DE 7D BE A0 6B 6F 87 C0 D0 50 1F 28 30 03 40 DA 08 73 51 6C 7F FF 3A 3C A7 37 06 8E BD 4B 11 04 EB 7D 24 DE E6 F9 FC 31 71 FB 94 D5 60 F3 2E 4A AF 42 D2 CB EA C4 6A 1A B2 CC 53 DD 15 4B 8B 1F C8 19 61 1F CD 9D A8 3E 63 2B 84 35 69 65 84 C8 19 C5 46 22 F8 53 95 BE E3 80 4A 10 C6 2A EC BA 97 20 11 C7 39 99 10 04 A0 F0 61 7A 95 25 8C 4E 52 75 E2 B6 ED 08 CA 14 FC CE 22 6A B3 4E CF 46 03 97 97 03 7E C0 B1 DE 78 AF 45 33 CF BA 3E 71 B7 DE F4 25 25 C2 0D 35 89 9D 9D FB 0E 11 79 89 1E 37 C5 AF 8E 72 69
Exponent	65537
Key Size	2048 bits
Key Usage	Verify
Signature	256 bytes : 36 D7 06 80 11 27 AD 2A 14 9B 38 77 B3 23 A0 75 58 B8 B1 7E 83 42 BA 72 DA 1E D8 8E 36 06 97 E0 F0 95 3B 37 FD 1B 42 58 FE 22 C8 6B BD 38 5E D1 3B 25 6E 12 EB 5E 67 76 46 40 90 DA 14 C8 78 0D ED 95 66 DA 8E 86 6F 80 A1 BA 56 32 95 86 DC DC 6A CA 04 8C 5B 7F F6 BF CC 6F 85 03 58 C3 68 51 13 CD FD C8 F7 79 3D 99 35 F0 56 A3 BD E0 59 ED 4F 44 09 A3 9E 38 7A F6 46 D1 1D 12 9D 4F BE D0 40 FC 55 FE 06 5E 3C DA 1C 56 BD 96 51 7B 6F 57 2A DB A2 AA 96 DC 8C 74 C2 95 BE F0 6E 95 13 FF 17 F0 3C AC B2 10 8D CC 73 FB E8 8F 02 C6 F0 FB 33 B3 95 3B E3 C2 CB 68 58 73 DB A8 24 62 3B 06 35 9D 0D A9 33 BD 78 03 90 2E 4C 78 5D 50 3A 81 D4 EE A0 C8 70 38 DC B2 F9 67 FA 87 40 5D 61 C0 51 8F 6B 83 6B CD 05 3A CA E1 A7 05 78 FC CA DA 94 D0 2C 08 3D 7E 16 79 C8 A0 50 20 24 54 33 71
Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Key Cert Sign, CRL Sign
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Path Length Constraint	0
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://crl.geotrust.com/crls/gtglobal.crl
Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO

Issuer Name	
Country	US
Organization	GeoTrust Inc.
Common Name	GeoTrust Global CA
Serial Number	144470
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Tuesday 21 May 2002 06 h 00 min 00 s Central European Summer Time
Not Valid After	Saturday 21 May 2022 06 h 00 min 00 s Central European Summer Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : DA CC 18 63 30 FD F4 17 23 1A 56 7E 58 DF 3C 6C 38 E4 71 B7 78 91 D4 BC A1 D8 4C F8 A8 43 B6 03 E9 4D 21 07 08 88 DA 58 2F 66 39 29 BD 05 78 8B 9D 38 E8 05 B7 6A 7E 71 A4 E6 C4 60 A6 80 EF 80 E4 89 28 0F 9E 25 D6 ED 83 F3 AD A6 91 C7 98 C9 42 18 35 14 9D AD 98 46 92 2E 4F CA F1 87 43 C1 16 95 57 2D 50 EF 89 2D 80 7A 57 AD F2 EE 5F 6B D2 00 8D B9 14 F8 14 15 35 D9 C0 46 A3 7B 72 C8 91 BF C9 55 2B CD D0 97 3E 9C 26 64 CC DF CE 83 19 71 CA 4E E6 D4 D5 7B A9 19 CD 55 DE C8 EC D2 5E 38 53 E5 5C 4F 8C 2D FE 50 23 36 FC 66 E6 C8 8E A4 39 19 00 B7 95 02 39 91 0B 0E FE 38 2E D1 1D 05 9A F6 4D 3E 6F 0F 07 1D AF 2C 1E 8F 60 39 E2 FA 36 53 13 39 D4 5E 26 28 DB 3D A8 14 BD 32 EB 18 03 28 52 04 71 E5 A8 33 3D E1 38 B8 07 36 84 62 9C 79 EA 16 30 F4 5F C0 2B E8 71 6B E4 F9
Exponent	65537
Key Size	2048 bits
Key Usage	Any
Signature	256 bytes : 35 E3 29 6A E5 2F 5D 54 8E 29 50 94 9F 99 1A 14 E4 8F 78 2A 62 94 A2 27 67 9E D0 CF 1A 5E 47 E9 C1 B2 A4 CF DD 41 1A 05 4E 9B 4B EE 4A 6F 55 52 B3 24 A1 37 0A EB 64 76 2A 2E 2C F3 FD 38 75 90 BF FA 71 D8 C7 3D 37 D2 B5 05 95 62 B9 A6 DE 89 3D 36 7B 38 77 48 97 AC A6 20 8F 2E A6 C9 0C C2 B2 99 45 00 C7 CE 11 51 22 22 E0 A5 EA B6 15 48 09 64 EA 5E 4F 74 F7 05 3E C7 8A 52 0C DB 15 B4 BD 6D 98 E5 C6 B1 54 68 A9 E3 69 90 B6 9A A5 0F B8 B9 3F 20 7D AE 4A B5 B8 9C E4 1D B6 AB E6 94 A5 C1 C7 83 AD DB F5 27 87 0E 04 6C D5 FF DD A0 5D ED 87 52 B7 2B 15 02 AE 39 A6 6A 74 E9 DA C4 E7 BC 4D 34 1E A9 5C 4D 33 5F 92 09 2F 88 66 5D 77 97 C7 1D 76 13 A9 D5 E5 F1 16 09 11 35 D5 AC DB 24 71 70 2C 98 56 0B D9 17 B4 D1 E3 51 2B 5E 75 E8 D5 D0 DC 4F 34 ED C2 05 66 80 A1 CB E6 33
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Public Key	256 bytes : A4 78 79 A6 79 86 3B 88 C3 11 C4 A8 35 E0 D3 F1 F3 31 6D 0F F5 66 50 8D 98 E0 57 50 62 00 FC 02 E4 62 7C 0F 9F AA FC 62 70 49 22 ED 37 75 4A B6 78 CE 57 67 02 36 C0 4B E7 C2 D1 E4 23 88 C7 E8 25 3A 2C AE 45 E0 42 0B F9 76 CD 3E F2 55 37 76 8A 15 5E 8A 9E 99 E2 4A 52 28 73 23 F8 7E ED C7 F5 D8 CE FF EC 46 CC 23 94 5A 0C 15 0F 4C 79 99 1D E0 ED 93 7F 17 51 8B 01 AD 2F 77 9C 80 AA E1 50 D4 03 1C B6 04 AB 06 49 2D A5 F7 04 6F 97 87 E1 74 30 E6 82 E4 39 71 10 CA 9F FA 6A 75 81 2A 02 AC 45 54 48 DA 9B 08 DC 51 64 81 B1 69 6A 4A 7D FB 7C 8F 6C FC C6 43 0B 37 CC C3 3E 80 85 E1 4C AD 13 4B D2 82 76 63 77 15 74 1C 62 0D 57 6A 8C 64 BE 00 6E 6A 21 4C FF 02 C8 C7 34 BD C9 12 C6 B9 E4 E4 AB 30 5B 98 08 F0 B3 60 33 00 54 B2 B3 8A A6 57 E4 6D B9 73 47 BF AA 1D 1B 48 AE 3F
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Derive
Signature	256 bytes : 3A 8F DA 0F 28 4E 64 FC 55 F9 B1 B2 D8 E2 9E F1 B2 79 6D 9D D1 C3 37 5A 32 CE 66 FC F9 C9 A4 7B A5 BF 78 51 EC 63 48 3E CD 47 94 05 6D F3 6F 41 0C 06 73 57 58 D4 C2 07 56 95 21 C4 46 7B C1 94 0C 30 27 03 34 97 31 00 5E 06 2B 0D 6F AF 64 9F 6B A7 B5 2E D1 6E 52 FC DF EF 07 EF CE D1 80 B7 97 B9 C6 A1 AF 79 02 A1 CE B5 A1 37 A6 23 41 C4 23 8D CE 0E D5 48 B8 51 03 34 90 C4 D7 0A AC 1E 47 59 79 C9 CD 48 6F 48 67 24 A9 2B 6B 24 AF 7A C7 EE A5 24 6C FD 65 93 36 C5 BE C9 C5 53 2A 77 00 94 B8 89 BF 7E E3 13 EB EB 91 90 7D 48 BF F2 F8 28 49 5B CE CB 96 37 AD 3F D4 DC 2B 48 F6 D3 E8 0D 26 53 60 64 E5 E8 82 C3 C4 96 BC 74 41 98 99 32 87 82 3C 89 1E 66 CA CD EB 35 DC DF C1 37 5F 17 52 5B D3 9E 31 1A 89 F4 17 BC 98 FD CA 9A 9C 30 75 05 3E 39 2A C0 8D 47 4B 26 F5 89 1B 61
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	NO
Extension	Extended Key Usage (2.5.29.37)
Critical	NO
Purpose #1	Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose #2	Client Authentication (1.3.6.1.5.5.7.3.2)
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	75 20 EA D1 F9 B9 B7 34 D5 E9 E4 35 8A AE E8 64 C6 73 2B A4
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	Subject Alternative Name (2.5.29.17)
Critical	NO
DNS Name	www.google.com
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://aki.google.com/GIAG2.crl

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Public Key	256 bytes : 9C 2A 04 77 5C D8 50 91 3A 06 A3 82 E0 D8 50 48 BC 89 3F F1 19 70 1A 88 46 7E E0 8F C5 F1 89 CE 21 EE 5A FE 61 0D B7 32 44 89 A0 74 0B 53 4F 55 A4 CE 82 62 95 EE EB 59 5F C6 E1 05 80 12 C4 5E 94 3F BC 58 48 38 F4 53 F7 24 E6 FB 91 E9 15 C4 CF F4 53 0D F4 4A FC 9F 54 DE 7D BE A0 6B 6F 87 C0 D0 50 1F 28 30 03 40 DA 08 73 51 6C 7F FF 3A 3C A7 37 06 8E BD 4B 11 04 EB 7D 24 DE E6 F9 FC 31 71 FB 94 D5 60 F3 2E 4A AF 42 D2 CB EA C4 6A 1A B2 CC 53 DD 15 48 8B 1F C8 19 61 1F CD 9D A8 3E 63 2B 84 35 69 65 84 C8 19 C5 46 22 F8 53 95 BE E3 80 4A 10 C6 2A EC BA 97 20 11 C7 39 99 10 04 A0 F0 61 7A 95 25 8C 4E 52 75 E2 B6 ED 08 CA 14 FC CE 22 6A B3 4E CF 46 03 97 97 03 7E C0 B1 DE 78 AF 45 33 CF BA 3E 71 B7 DE F4 25 25 C2 0D 35 89 9D 9D FB 0E 11 79 89 1E 37 C5 AF 8E 72 69
Exponent	65537
Key Size	2048 bits
Key Usage	Verify
Signature	256 bytes : 36 D7 06 80 11 27 AD 2A 14 9B 38 77 B3 23 A0 75 58 8B 81 7E 83 42 BA 72 DA 1E D8 8E 36 06 97 E0 F0 95 3B 37 FD 1B 42 58 FE 22 C8 6B BD 38 5E D1 3B 25 6E 12 EB 5E 67 76 46 40 90 DA 14 C8 78 0D ED 95 66 DA 8E 86 6F 80 A1 BA 56 32 95 86 DC DC 6A CA 04 8C 5B 7F F6 BF CC 6F 85 03 58 C3 68 51 13 CD FD C8 F7 79 3D 99 35 F0 56 A3 BD E0 59 ED 4F 44 09 A3 9E 38 7A F6 46 D1 1D 12 9D 4F BE D0 40 FC 55 FE 06 5E 3C DA 1C 56 BD 96 51 7B 6F 57 2A DB A2 AA 96 DC 8C 74 C2 95 BE F0 6E 95 13 FF 17 F0 3C AC B2 10 8D CC 73 FB E8 8F 02 C6 F0 FB 33 B3 95 3B E3 C2 CB 68 58 73 DB A8 24 62 3B 06 35 9D 0D A9 33 BD 78 03 90 2E 4C 78 5D 50 3A 81 D4 EE A0 C8 70 38 DC B2 F9 67 FA 87 40 5D 61 C0 51 8F 6B 83 6B CD 05 3A CA E1 A7 05 78 FC CA DA 94 D0 2C 08 3D 7E 16 79 C8 A0 50 20 24 54 33 71
Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Key Cert Sign, CRL Sign
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Path Length Constraint	0
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://crl.geotrust.com/crls/gtglobal.crl
Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO

Issuer Name	US
Country	US
Organization	GeoTrust Inc.
Common Name	GeoTrust Global CA
Serial Number	144470
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Tuesday 21 May 2002 06 h 00 min 00 s Central European Summer Time
Not Valid After	Saturday 21 May 2022 06 h 00 min 00 s Central European Summer Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : DA CC 18 63 30 FD F4 17 23 1A 56 7E 58 DF 3C 6C 38 E4 71 B7 78 91 D4 BC A1 D8 4C F8 A8 43 B6 03 E9 4D 21 07 08 88 DA 58 2F 66 39 29 BD 05 78 8B 9D 38 E8 05 B7 6A 7E 71 A4 E6 C4 60 A6 80 EF 80 E4 89 28 0F 9E 25 D6 ED 83 F3 AD A6 91 C7 98 C9 42 18 35 14 9D AD 98 46 92 2E 4F CA F1 87 43 C1 16 95 57 2D 50 EF 89 2D 80 7A 57 AD F2 EE 5F 6B D2 00 8D B9 14 F8 14 15 35 D9 C0 46 A3 7B 72 C8 91 BF C9 55 2B CD D0 97 3E 9C 26 64 CC DF CE 83 19 71 CA 4E E6 D4 D5 7B A9 19 CD 55 DE C8 EC D2 5E 38 53 E5 5C 4F 8C 2D FE 50 23 36 FC 66 E6 C8 8E A4 39 19 00 B7 95 02 39 91 08 0E FE 38 2E D1 1D 05 9A F6 4D 3E 6F 0F 07 1D AF 2C 1E 8F 60 39 E2 FA 36 53 13 39 D4 5E 26 28 DB 3D A8 14 BD 32 EB 18 03 28 52 04 71 E5 A8 33 3D E1 38 B8 07 36 84 62 9C 79 EA 16 30 F4 5F C0 2B E8 71 6B E4 F9
Exponent	65537
Key Size	2048 bits
Key Usage	Any
Signature	256 bytes : 35 E3 29 6A E5 2F 5D 54 8E 29 50 94 9F 99 1A 14 E4 8F 78 2A 62 94 A2 27 67 9E D0 CF 1A 5E 47 E9 C1 B2 A4 CF DD 41 1A 05 4E 9B 4B EE 4A 6F 55 52 B3 24 A1 37 0A EB 64 76 2A 2E 2C F3 FD 38 75 90 BF FA 71 D8 C7 3D 37 D2 B5 05 95 62 B9 A6 DE 89 3D 36 7B 38 77 48 97 AC A6 20 8F 2E A6 C9 0C C2 B2 99 45 00 C7 CE 11 51 22 22 E0 A5 EA B6 15 48 09 64 EA 5E 4F 74 F7 05 3E C7 8A 52 0C DB 15 B4 BD 6D 98 E5 C6 B1 54 68 A9 E3 69 90 B6 9A A5 0F B8 B9 3F 20 7D AE 4A B5 B8 9C E4 1D B6 AB E6 94 A5 C1 C7 83 AD DB F5 27 87 0E 04 6C D5 FF DD A0 5D ED 87 52 B7 2B 15 02 AE 39 A6 6A 74 E9 DA C4 E7 BC 4D 34 1E A9 5C 4D 33 5F 92 09 2F 88 66 5D 77 97 C7 1D 76 13 A9 D5 E5 F1 16 09 11 35 D5 AC DB 24 71 70 2C 98 56 0B D9 17 B4 D1 E3 51 2B 5E 75 E8 D5 D0 DC 4F 34 ED C2 05 66 80 A1 CB E6 33
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Public Key	256 bytes : A4 78 79 A6 79 86 3B 88 C3 11 C4 A8 35 E0 D3 F1 F3 31 6D 0F F5 66 50 8D 98 E0 57 50 62 00 FC 02 E4 62 7C 0F 9F AA FC 62 70 49 22 ED 37 75 4A B6 78 CE 57 67 02 36 C0 4B E7 C2 D1 E4 23 88 C7 E8 25 3A 2C AE 45 E0 42 0B F9 76 CD 3E F2 55 37 76 8A 15 5E 8A 9E 99 E2 4A 52 28 73 23 F8 7E ED C7 F5 D8 CE FF EC 46 CC 23 94 5A 0C 15 0F 4C 79 99 1D E0 ED 93 7F 17 51 8B 01 AD 2F 77 9C 80 AA E1 50 D4 03 1C B6 04 AB 06 49 2D A5 F7 04 6F 97 87 E1 74 30 E6 82 E4 39 71 10 CA 9F FA 6A 75 81 2A 02 AC 45 54 48 DA 9B 08 DC 51 64 81 B1 69 6A 4A 7D FB 7C 8F 6C FC C6 43 0B 37 CC C3 3E 80 85 E1 4C AD 13 4B D2 82 76 63 77 15 74 1C 62 0D 57 6A 8C 64 BE 00 6E 6A 21 4C FF 02 C8 C7 34 BD C9 12 C6 B9 E4 E4 AB 30 5B 98 08 F0 B3 60 33 00 54 B2 B3 8A A6 57 E4 6D B9 73 47 BF AA 1D 1B 48 AE 3F
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Derive

Signature	256 bytes : 3A 8F DA 0F 28 4E 64 FC 55 F9 B1 B2 D8 E2 9E F1 B2 79 6D 9D D1 C3 37 5A 32 CE 66 FC F9 C9 A4 7B A5 BF 78 51 EC 63 48 3E CD 47 94 05 6D F3 6F 41 0C 06 73 57 58 D4 C2 07 56 95 21 C4 46 7B C1 94 0C 30 27 03 34 97 31 00 5E 06 2B 0D 6F AF 64 9F 6B A7 B5 2E D1 6E 52 FC DF EF 07 EF CE D1 80 B7 97 B9 C6 A1 AF 79 02 A1 CE B5 A1 37 A6 23 41 C4 23 8D CE 0E D5 48 B8 51 03 34 90 C4 D7 0A AC 1E 47 59 79 C9 CD 48 6F 48 67 24 A9 2B 6B 24 AF 7A C7 EE A5 24 6C FD 65 93 36 C5 BE C9 C5 53 2A 77 00 94 B8 89 BF 7E E3 13 EB EB 91 90 7D 48 BF F2 F8 28 49 5B CE CB 96 37 AD 3F D4 DC 2B 48 F6 D3 E8 0D 26 53 60 64 E5 E8 82 C3 C4 96 BC 74 41 98 99 32 87 82 3C 89 1E 66 CA CD EB 35 DC DF C1 37 5F 17 52 5B D3 9E 31 1A 89 F4 17 BC 98 FD CA 9A 9C 30 75 05 3E 39 2A C0 8D 47 4B 26 F5 89 1B 61
-----------	---

Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	NO
Extension	Extended Key Usage (2.5.29.37)
Critical	NO
Purpose #1	Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose #2	Client Authentication (1.3.6.1.5.5.7.3.2)
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	75 20 EA D1 F9 B9 B7 34 D5 E9 E4 35 8A AE E8 64 C6 73 2B A4
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	Subject Alternative Name (2.5.29.17)
Critical	NO
DNS Name	www.google.com
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://aki.google.com/GIAG2.crl

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Public Key	256 bytes : 9C 2A 04 77 5C D8 50 91 3A 06 A3 82 E0 D8 50 48 BC 89 3F F1 19 70 1A 88 46 7E E0 8F C5 F1 89 CE 21 EE 5A FE 61 0D B7 32 44 89 A0 74 0B 53 4F 55 A4 CE 82 62 95 EE EB 59 5F C6 E1 05 80 12 C4 5E 94 3F BC 58 48 38 F4 53 F7 24 E6 FB 91 E9 15 C4 CF F4 53 0D F4 4A FC 9F 54 DE 7D BE A0 6B 6F 87 C0 D0 50 1F 28 30 03 40 DA 08 73 51 6C 7F FF 3A 3C A7 37 06 8E BD 4B 11 04 EB 7D 24 DE E6 F9 FC 31 71 FB 94 D5 60 F3 2E 4A AF 42 D2 CB EA C4 6A 1A B2 CC 53 DD 15 4B 8B 1F C8 19 61 1F CD 9D A8 3E 63 2B 84 35 69 65 84 C8 19 C5 46 22 F8 53 95 BE E3 80 4A 10 C6 2A EC BA 97 20 11 C7 39 99 10 04 A0 F0 61 7A 95 25 8C 4E 52 75 E2 B6 ED 08 CA 14 FC CE 22 6A B3 4E CF 46 03 97 97 03 7E C0 B1 DE 78 AF 45 33 CF BA 3E 71 B7 DE F4 25 25 C2 0D 35 89 9D 9D FB 0E 11 79 89 1E 37 C5 AF 8E 72 69
Exponent	65537
Key Size	2048 bits
Key Usage	Verify

Signature	256 bytes : 36 D7 06 80 11 27 AD 2A 14 9B 38 77 B3 23 A0 75 58 B8 B1 7E 83 42 BA 72 DA 1E D8 8E 36 06 97 E0 F0 95 3B 37 FD 1B 42 58 FE 22 C8 6B BD 38 5E D1 3B 25 6E 12 EB 5E 67 76 46 40 90 DA 14 C8 78 0D ED 95 66 DA 8E 86 6F 80 A1 BA 56 32 95 86 DC DC 6A CA 04 8C 5B 7F F6 BF CC 6F 85 03 58 C3 68 51 13 CD FD C8 F7 79 3D 99 35 F0 56 A3 BD E0 59 ED 4F 44 09 A3 9E 38 7A F6 46 D1 1D 12 9D 4F BE D0 40 FC 55 FE 06 5E 3C DA 1C 56 BD 96 51 7B 6F 57 2A DB A2 AA 96 DC 8C 74 C2 95 BE F0 6E 95 13 FF 17 F0 3C AC B2 10 8D CC 73 FB E8 8F 02 C6 F0 FB 33 B3 95 3B E3 C2 CB 68 58 73 DB A8 24 62 3B 06 35 9D 0D A9 33 BD 78 03 90 2E 4C 78 5D 50 3A 81 D4 EE A0 C8 70 38 DC B2 F9 67 FA 87 40 5D 61 C0 51 8F 6B 83 6B CD 05 3A CA E1 A7 05 78 FC CA DA 94 D0 2C 08 3D 7E 16 79 C8 A0 50 20 24 54 33 71
-----------	---

Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Key Cert Sign, CRL Sign
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Path Length Constraint	0
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://crl.geotrust.com/crls/gtglobal.crl
Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO

Issuer Name	US
Country	US
Organization	GeoTrust Inc.
Common Name	GeoTrust Global CA
Serial Number	144470
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Tuesday 21 May 2002 06 h 00 min 00 s Central European Summer Time
Not Valid After	Saturday 21 May 2022 06 h 00 min 00 s Central European Summer Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : DA CC 18 63 30 FD F4 17 23 1A 56 7E 58 DF 3C 6C 38 E4 71 B7 78 91 D4 BC A1 D8 4C F8 A8 43 B6 03 E9 4D 21 07 08 88 DA 58 2F 66 39 29 BD 05 78 88 9D 38 E8 05 B7 6A 7E 71 A4 E6 C4 60 A6 80 EF 80 E4 89 28 0F 9E 25 D6 ED 83 F3 AD A6 91 C7 98 C9 42 18 35 14 9D AD 98 46 92 2E 4F CA F1 87 43 C1 16 95 57 2D 50 EF 89 2D 80 7A 57 AD F2 EE 5F 6B D2 00 8D B9 14 F8 14 15 35 D9 C0 46 A3 7B 72 C8 91 BF C9 55 2B CD D0 97 3E 9C 26 64 CC DF CE 83 19 71 CA 4E E6 D4 D5 7B A9 19 CD 55 DE C8 EC D2 5E 38 53 E5 5C 4F 8C 2D FE 50 23 36 FC 66 E6 C8 8E A4 39 19 00 B7 95 02 39 91 08 0E FE 38 2E D1 1D 05 9A F6 4D 3E 6F 0F 07 1D AF 2C 1E 8F 60 39 E2 FA 36 53 13 39 D4 5E 26 28 DB 3D A8 14 BD 32 EB 18 03 28 52 04 71 E5 A8 33 3D E1 38 B8 07 36 84 62 9C 79 EA 16 30 F4 5F C0 2B E8 71 6B E4 F9
Exponent	65537
Key Size	2048 bits
Key Usage	Any
Signature	256 bytes : 35 E3 29 6A E5 2F 5D 54 8E 29 50 94 9F 99 1A 14 E4 8F 78 2A 62 94 A2 27 67 9E D0 CF 1A 5E 47 E9 C1 B2 A4 CF DD 41 1A 05 4E 9B 4B EE 4A 6F 55 52 B3 24 A1 37 0A EB 64 76 2A 2E 2C F3 FD 38 75 90 BF FA 71 D8 C7 3D 37 D2 B5 05 95 62 B9 A6 DE 89 3D 36 7B 38 77 48 97 AC A6 20 8F 2E A6 C9 0C C2 B2 99 45 00 C7 CE 11 51 22 22 E0 A5 EA B6 15 48 09 64 EA 5E 4F 74 F7 05 3E C7 8A 52 0C DB 15 B4 BD 6D 98 E5 C6 B1 54 68 A9 E3 69 90 B6 9A A5 0F B8 B9 3F 20 7D AE 4A B5 B8 9C E4 1D B6 AB E6 94 A5 C1 C7 83 AD DB F5 27 87 0E 04 6C D5 FF DD A0 5D ED 87 52 B7 2B 15 02 AE 39 A6 6A 74 E9 DA C4 E7 BC 4D 34 1E A9 5C 4D 33 5F 92 09 2F 88 66 5D 77 97 C7 1D 76 13 A9 D5 E5 F1 16 09 11 35 D5 AC DB 24 71 70 2C 98 56 0B D9 17 B4 D1 E3 51 2B 5E 75 E8 D5 D0 DC 4F 34 ED C2 05 66 80 A1 CB E6 33
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Public Key	256 bytes : A4 78 79 A6 79 86 3B 88 C3 11 C4 A8 35 E0 D3 F1 F3 31 6D 0F F5 66 50 8D 98 E0 57 50 62 00 FC 02 E4 62 7C 0F 9F AA FC 62 70 49 22 ED 37 75 4A B6 78 CE 57 67 02 36 C0 4B E7 C2 D1 E4 23 88 C7 E8 25 3A 2C AE 45 E0 42 0B F9 76 CD 3E F2 55 37 76 8A 15 5E 8A 9E 99 E2 4A 52 28 73 23 F8 7E ED C7 F5 D8 CE FF EC 46 CC 23 94 5A 0C 15 0F 4C 79 99 1D E0 ED 93 7F 17 51 8B 01 AD 2F 77 9C 80 AA E1 50 D4 03 1C B6 04 AB 06 49 2D A5 F7 04 6F 97 87 E1 74 30 E6 82 E4 39 71 10 CA 9F FA 6A 75 81 2A 02 AC 45 54 48 DA 9B 08 DC 51 64 81 B1 69 6A 4A 7D FB 7C 8F 6C FC C6 43 0B 37 CC C3 3E 80 85 E1 4C AD 13 4B D2 82 76 63 77 15 74 1C 62 0D 57 6A 8C 64 BE 00 6E 6A 21 4C FF 02 C8 C7 34 BD C9 12 C6 B9 E4 E4 AB 30 5B 98 08 F0 B3 60 33 00 54 B2 B3 8A A6 57 E4 6D B9 73 47 BF AA 1D 1B 48 AE 3F
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Derive
Signature	256 bytes : 3A 8F DA 0F 28 4E 64 FC 55 F9 B1 B2 D8 E2 9E F1 B2 79 6D 9D D1 C3 37 5A 32 CE 66 FC F9 C9 A4 7B A5 BF 78 51 EC 63 48 3E CD 47 94 05 6D F3 6F 41 0C 06 73 57 58 D4 C2 07 56 95 21 C4 46 7B C1 94 0C 30 27 03 34 97 31 00 5E 06 2B 0D 6F AF 64 9F 6B A7 B5 2E D1 6E 52 FC DF EF 07 EF CE D1 B0 87 97 B9 C6 A1 AF 79 02 A1 CE B5 A1 37 A6 23 41 C4 23 8D CE 0E D5 48 B8 51 03 34 90 C4 D7 0A AC 1E 47 59 79 C9 CD 48 6F 48 67 24 A9 2B 6B 24 AF 7A C7 EE A5 24 6C FD 65 93 36 C5 BE C9 C5 53 2A 77 00 94 B8 89 BF 7E E3 13 EB EB 91 90 7D 48 BF F2 F8 28 49 5B CE CB 96 37 AD 3F D4 DC 2B 48 F6 D3 E8 0D 26 53 60 64 E5 E8 82 C3 C4 96 BC 74 41 98 99 32 87 82 3C 89 1E 66 CA CD EB 35 DC DF C1 37 5F 17 52 5B D3 9E 31 1A 89 F4 17 BC 98 FD CA 9A 9C 30 75 05 3E 39 2A C0 8D 47 4B 26 F5 89 1B 61
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	NO
Extension	Extended Key Usage (2.5.29.37)
Critical	NO
Purpose #1	Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose #2	Client Authentication (1.3.6.1.5.5.7.3.2)
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	75 20 EA D1 F9 B9 B7 34 D5 E9 E4 35 8A AE E8 64 C6 73 2B A4
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	Subject Alternative Name (2.5.29.17)
Critical	NO
DNS Name	www.google.com
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://aki.google.com/GIAG2.crl

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Public Key	256 bytes : 9C 2A 04 77 5C D8 50 91 3A 06 A3 82 E0 D8 50 48 BC 89 3F F1 19 70 1A 88 46 7E E0 8F C5 F1 89 CE 21 EE 5A FE 61 0D B7 32 44 89 A0 74 0B 53 4F 55 A4 CE 82 62 95 EE EB 59 5F C6 E1 05 80 12 C4 5E 94 3F BC 58 48 38 F4 53 F7 24 E6 FB 91 E9 15 C4 CF F4 53 0D F4 4A FC 9F 54 DE 7D BE A0 6B 6F 87 C0 D0 50 1F 28 30 03 40 DA 08 73 51 6C 7F FF 3A 3C A7 37 06 8E BD 4B 11 04 EB 7D 24 DE E6 F9 FC 31 71 FB 94 D5 60 F3 2E 4A AF 42 D2 CB EA C4 6A 1A B2 CC 53 DD 15 4B 8B 1F C8 19 61 1F CD 9D A8 3E 63 2B 84 35 69 65 84 C8 19 C5 46 22 F8 53 95 BE E3 80 4A 10 C6 2A EC BA 97 20 11 C7 39 99 10 04 A0 F0 61 7A 95 25 8C 4E 52 75 E2 B6 ED 08 CA 14 FC CE 22 6A B3 4E CF 46 03 97 97 03 7E C0 B1 DE 78 AF 45 33 CF BA 3E 71 B7 DE F4 25 25 C2 0D 35 89 9D 9D FB 0E 11 79 89 1E 37 C5 AF 8E 72 69
Exponent	65537
Key Size	2048 bits
Key Usage	Verify
Signature	256 bytes : 36 D7 06 80 11 27 AD 2A 14 9B 38 77 B3 23 A0 75 58 B8 B1 7E 83 42 BA 72 DA 1E D8 8E 36 06 97 E0 F0 95 3B 37 FD 1B 42 58 FE 22 C8 6B BD 38 5E D1 3B 25 6E 12 EB 5E 67 76 46 40 90 DA 14 C8 78 0D ED 95 66 DA 8E 86 6F 80 A1 BA 56 32 95 86 DC DC 6A CA 04 8C 5B 7F F6 BF CC 6F 85 03 58 C3 68 51 13 CD FD C8 F7 79 3D 99 35 F0 56 A3 BD E0 59 ED 4F 44 09 A3 9E 38 7A F6 46 D1 1D 12 9D 4F BE D0 40 FC 55 FE 06 5E 3C DA 1C 56 BD 96 51 7B 6F 57 2A DB A2 AA 96 DC 8C 74 C2 95 BE F0 6E 95 13 FF 17 F0 3C AC B2 10 8D CC 73 FB E8 8F 02 C6 F0 FB 33 B3 95 3B E3 C2 CB 68 58 73 DB A8 24 62 3B 06 35 9D 0D A9 33 BD 78 03 90 2E 4C 78 5D 50 3A 81 D4 EE A0 C8 70 38 DC B2 F9 67 FA 87 40 5D 61 C0 51 8F 6B 83 6B CD 05 3A CA E1 A7 05 78 FC CA DA 94 D0 2C 08 3D 7E 16 79 C8 A0 50 20 24 54 33 71
Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Key Cert Sign, CRL Sign
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Path Length Constraint	0
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://crl.geotrust.com/crls/gtglobal.crl
Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO

Issuer Name	US
Country	US
Organization	GeoTrust Inc.
Common Name	GeoTrust Global CA
Serial Number	144470
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Tuesday 21 May 2002 06 h 00 min 00 s Central European Summer Time
Not Valid After	Saturday 21 May 2022 06 h 00 min 00 s Central European Summer Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : DA CC 18 63 30 FD F4 17 23 1A 56 7E 58 DF 3C 6C 38 E4 71 B7 78 91 D4 BC A1 D8 4C F8 A8 43 B6 03 E9 4D 21 07 08 88 DA 58 2F 66 39 29 BD 05 78 8B 9D 38 E8 05 B7 6A 7E 71 A4 E6 C4 60 A6 80 EF 80 E4 89 28 0F 9E 25 D6 ED 83 F3 AD A6 91 C7 98 C9 42 18 35 14 9D AD 98 46 92 2E 4F CA F1 87 43 C1 16 95 57 2D 50 EF 89 2D 80 7A 57 AD F2 EE 5F 6B D2 00 8D B9 14 F8 14 15 35 D9 C0 46 A3 7B 72 C8 91 BF C9 55 2B CD D0 97 3E 9C 26 64 CC DF CE 83 19 71 CA 4E E6 D4 D5 7B A9 19 CD 55 DE C8 EC D2 5E 38 53 E5 5C 4F 8C 2D FE 50 23 36 FC 66 E6 C8 8E A4 39 19 00 B7 95 02 39 91 0B 0E FE 38 2E D1 1D 05 9A F6 4D 3E 6F 0F 07 1D AF 2C 1E 8F 60 39 E2 FA 36 53 13 39 D4 5E 26 28 DB 3D A8 14 BD 32 EB 18 03 28 52 04 71 E5 A8 33 3D E1 38 B8 07 36 84 62 9C 79 EA 16 30 F4 5F C0 2B E8 71 6B E4 F9
Exponent	65537
Key Size	2048 bits
Key Usage	Any
Signature	256 bytes : 35 E3 29 6A E5 2F 5D 54 8E 29 50 94 9F 99 1A 14 E4 8F 78 2A 62 94 A2 27 67 9E D0 CF 1A 5E 47 E9 C1 B2 A4 CF DD 41 1A 05 4E 9B 4B EE 4A 6F 55 52 B3 24 A1 37 0A EB 64 76 2A 2E 2C F3 FD 38 75 90 BF FA 71 D8 C7 3D 37 D2 B5 05 95 62 B9 A6 DE 89 3D 36 7B 38 77 48 97 AC A6 20 8F 2E A6 C9 0C C2 B2 99 45 00 C7 CE 11 51 22 22 E0 A5 EA B6 15 48 09 64 EA 5E 4F 74 F7 05 3E C7 8A 52 0C DB 15 B4 BD 6D 98 E5 C6 B1 54 68 A9 E3 69 90 B6 9A A5 0F B8 B9 3F 20 7D AE 4A B5 B8 9C E4 1D B6 AB E6 94 A5 C1 C7 83 AD DB F5 27 87 0E 04 6C D5 FF DD A0 5D ED 87 52 B7 2B 15 02 AE 39 A6 6A 74 E9 DA C4 E7 BC 4D 34 1E A9 5C 4D 33 5F 92 09 2F 88 66 5D 77 97 C7 1D 76 13 A9 D5 E5 F1 16 09 11 35 D5 AC DB 24 71 70 2C 98 56 0B D9 17 B4 D1 E3 51 2B 5E 75 E8 D5 D0 DC 4F 34 ED C2 05 66 80 A1 CB E6 33
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Public Key	256 bytes : A4 78 79 A6 79 86 3B 88 C3 11 C4 A8 35 E0 D3 F1 F3 31 6D 0F F5 66 50 8D 9B E0 57 50 62 00 FC 02 E4 62 7C 0F 9F AA FC 62 70 49 22 ED 37 75 4A B6 78 CE 57 67 02 36 C0 4B E7 C2 D1 E4 23 88 C7 E8 25 3A 2C AE 45 E0 42 0B F9 76 CD 3E F2 55 37 76 8A 15 5E 8A 9E 99 E2 4A 52 28 73 23 F8 7E ED C7 F5 D8 CE FF EC 46 CC 23 94 5A 0C 15 0F 4C 79 99 1D E0 ED 93 7F 17 51 8B 01 AD 2F 77 9C 80 AA E1 50 D4 03 1C B6 04 AB 06 49 2D A5 F7 04 6F 97 87 E1 74 30 E6 82 E4 39 71 10 CA 9F FA 6A 75 81 2A 02 AC 45 54 48 DA 9B 08 DC 51 64 81 B1 69 6A 4A 7D FB 7C 8F 6C FC C6 43 0B 37 CC C3 3E 80 85 E1 4C AD 13 4B D2 82 76 63 77 15 74 1C 62 0D 57 6A 8C 64 BE 00 6E 6A 21 4C FF 02 C8 C7 34 BD C9 12 C6 B9 E4 E4 AB 30 5B 98 08 F0 B3 60 33 00 54 B2 B3 8A A6 57 E4 6D B9 73 47 BF AA 1D 1B 48 AE 3F
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Derive

Signature	256 bytes : 3A 8F DA 0F 28 4E 64 FC 55 F9 B1 B2 D8 E2 9E F1 B2 79 6D 9D D1 C3 37 5A 32 CE 66 FC F9 C9 A4 7B A5 BF 78 51 EC 63 48 3E CD 47 94 05 6D F3 6F 41 0C 06 73 57 58 D4 C2 07 56 95 21 C4 46 7B C1 94 0C 30 27 03 34 97 31 00 5E 06 2B 0D 6F AF 64 9F 6B A7 B5 2E D1 6E 52 FC DF EF 07 EF CE D1 80 B7 97 B9 C6 A1 AF 79 02 A1 CE B5 A1 37 A6 23 41 C4 23 8D CE 0E D5 48 B8 51 03 34 90 C4 D7 0A AC 1E 47 59 79 C9 CD 48 6F 48 67 24 A9 2B 6B 24 AF 7A C7 EE A5 24 6C FD 65 93 36 C5 BE C9 C5 53 2A 77 00 94 B8 89 BF 7E E3 13 EB EB 91 90 7D 48 BF F2 F8 28 49 5B CE CB 96 37 AD 3F D4 DC 2B 48 F6 D3 E8 0D 26 53 60 64 E5 E8 82 C3 C4 96 BC 74 41 98 99 32 87 82 3C 89 1E 66 CA CD EB 35 DC DF C1 37 5F 17 52 5B D3 9E 31 1A 89 F4 17 BC 98 FD CA 9A 9C 30 75 05 3E 39 2A C0 8D 47 4B 26 F5 89 1B 61
-----------	---

Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	NO
Extension	Extended Key Usage (2.5.29.37)
Critical	NO
Purpose #1	Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose #2	Client Authentication (1.3.6.1.5.5.7.3.2)
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	75 20 EA D1 F9 B9 B7 34 D5 E9 E4 35 8A AE E8 64 C6 73 2B A4

Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F

Extension	Subject Alternative Name (2.5.29.17)
Critical	NO
DNS Name	www.google.com
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://aki.google.com/GIAG2.crl

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Public Key	256 bytes : 9C 2A 04 77 5C D8 50 91 3A 06 A3 82 E0 D8 50 48 BC 89 3F F1 19 70 1A 88 46 7E E0 8F C5 F1 89 CE 21 EE 5A FE 61 0D B7 32 44 89 A0 74 0B 53 4F 55 A4 CE 82 62 95 EE EB 59 5F C6 E1 05 80 12 C4 5E 94 3F BC 58 48 38 F4 53 F7 24 E6 FB 91 E9 15 C4 CF F4 53 0D F4 4A FC 9F 54 DE 7D BE A0 6B 6F 87 C0 D0 50 1F 28 30 03 40 DA 08 73 51 6C 7F FF 3A 3C A7 37 06 8E BD 4B 11 04 EB 7D 24 DE E6 F9 FC 31 71 FB 94 D5 60 F3 2E 4A AF 42 D2 CB EA C4 6A 1A B2 CC 53 DD 15 4B 8B 1F C8 19 61 1F CD 9D A8 3E 63 2B 84 35 69 65 84 C8 19 C5 46 22 F8 53 95 BE E3 80 4A 10 C6 2A EC BA 97 20 11 C7 39 99 10 04 A0 F0 61 7A 95 25 8C 4E 52 75 E2 B6 ED 08 CA 14 FC CE 22 6A B3 4E CF 46 03 97 97 03 7E C0 B1 DE 78 AF 45 33 CF BA 3E 71 B7 DE F4 25 25 C2 0D 35 89 9D 9D FB 0E 11 79 89 1E 37 C5 AF 8E 72 69
Exponent	65537
Key Size	2048 bits
Key Usage	Verify

Signature	256 bytes : 36 D7 06 80 11 27 AD 2A 14 9B 38 77 B3 23 A0 75 58 B8 B1 7E 83 42 BA 72 DA 1E D8 8E 36 06 97 E0 F0 95 3B 37 FD 1B 42 58 FE 22 C8 6B BD 38 5E D1 3B 25 6E 12 EB 5E 67 76 46 40 90 DA 14 C8 78 0D ED 95 66 DA 8E 86 6F 80 A1 BA 56 32 95 86 DC DC 6A CA 04 8C 5B 7F F6 BF CC 6F 85 03 58 C3 68 51 13 CD FD C8 F7 79 3D 99 35 F0 56 A3 BD E0 59 ED 4F 44 09 A3 9E 38 7A F6 46 D1 1D 12 9D 4F BE D0 40 FC 55 FE 06 5E 3C DA 1C 56 BD 96 51 7B 6F 57 2A DB A2 AA 96 DC 8C 74 C2 95 BE F0 6E 95 13 FF 17 F0 3C AC B2 10 8D CC 73 FB E8 8F 02 C6 F0 FB 33 B3 95 3B E3 C2 CB 68 58 73 DB A8 24 62 3B 06 35 9D 0D A9 33 BD 78 03 90 2E 4C 78 5D 50 3A 81 D4 EE A0 C8 70 38 DC B2 F9 67 FA 87 40 5D 61 C0 51 8F 6B 83 6B CD 05 3A CA E1 A7 05 78 FC CA DA 94 D0 2C 08 3D 7E 16 79 C8 A0 50 20 24 54 33 71
-----------	---

Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Key Cert Sign, CRL Sign
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Path Length Constraint	0

Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F

Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E

Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://crl.geotrust.com/crls/gtglobal.crl
Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO

Issuer Name	US
Country	US
Organization	GeoTrust Inc.
Common Name	GeoTrust Global CA
Serial Number	144470
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Tuesday 21 May 2002 06 h 00 min 00 s Central European Summer Time
Not Valid After	Saturday 21 May 2022 06 h 00 min 00 s Central European Summer Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none

Public Key	256 bytes : DA CC 18 63 30 FD F4 17 23 1A 56 7E 58 DF 3C 6C 38 E4 71 B7 78 91 D4 BC A1 D8 4C F8 A8 43 B6 03 E9 4D 21 07 08 88 DA 58 2F 66 39 29 BD 05 78 8B 9D 38 E8 05 B7 6A 7E 71 A4 E6 C4 60 A6 80 EF 80 E4 89 28 0F 9E 25 D6 ED 83 F3 AD A6 91 C7 98 C9 42 18 35 14 9D AD 98 46 92 2E 4F CA F1 87 43 C1 16 95 57 2D 50 EF 89 2D 80 7A 57 AD F2 EE 5F 6B D2 00 8D B9 14 F8 14 15 35 D9 C0 46 A3 7B 72 C8 91 BF C9 55 2B CD D0 97 3E 9C 26 64 CC DF CE 83 19 71 CA 4E E6 D4 D5 7B A9 19 CD 55 DE C8 EC D2 5E 38 53 E5 5C 4F 8C 2D FE 50 23 36 FC 66 E6 C8 8E A4 39 19 00 B7 95 02 39 91 0B 0E FE 38 2E D1 1D 05 9A F6 4D 3E 6F 0F 07 1D AF 2C 1E 8F 60 39 E2 FA 36 53 13 39 D4 5E 26 28 DB 3D A8 14 BD 32 EB 18 03 28 52 04 71 E5 A8 33 3D E1 38 B8 07 36 84 62 9C 79 EA 16 30 F4 5F C0 2B E8 71 6B E4 F9
------------	---

Key Size	2048 bits
Key Usage	Any
Signature	256 bytes : 35 E3 29 6A E5 2F 5D 54 8E 29 50 94 9F 99 1A 14 E4 8F 78 2A 62 94 A2 27 67 9E D0 CF 1A 5E 47 E9 C1 B2 A4 CF DD 41 1A 05 4E 9B 4B EE 4A 6F 55 52 B3 24 A1 37 0A EB 64 76 2A 2E 2C F3 FD 38 75 90 BF FA 71 D8 C7 3D 37 D2 B5 05 95 62 B9 A6 DE 89 3D 36 7B 38 77 48 97 AC A6 20 8F 2E A6 C9 0C C2 B2 99 45 00 C7 CE 11 51 22 22 E0 A5 EA B6 15 48 09 64 EA 5E 4F 74 F7 05 3E C7 8A 52 0C DB 15 B4 BD 6D 9B E5 C6 B1 54 68 A9 E3 69 90 B6 9A A5 0F B8 B9 3F 20 7D AE 4A B5 B8 9C E4 1D B6 AB E6 94 A5 C1 C7 83 AD DB F5 27 87 0E 04 6C D5 FF DD A0 5D ED 87 52 B7 2B 15 02 AE 39 A6 6A 74 E9 DA C4 E7 BC 4D 34 1E A9 5C 4D 33 5F 92 09 2F 88 66 5D 77 97 C7 1D 76 13 A9 D5 E5 F1 16 09 11 35 D5 AC DB 24 71 70 2C 98 56 0B D9 17 B4 D1 E3 51 2B 5E 75 E8 D5 D0 DC 4F 34 ED C2 05 66 80 A1 CB E6 33

Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES

Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E

Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Public Key	256 bytes : A4 78 79 A6 79 86 3B 88 C3 11 C4 A8 35 E0 D3 F1 F3 31 6D 0F F5 66 50 8D 98 E0 57 50 62 00 FC 02 E4 62 7C 0F 9F AA FC 62 70 49 22 ED 37 75 4A B6 78 CE 57 67 02 36 C0 4B E7 C2 D1 E4 23 88 C7 E8 25 3A 2C AE 45 E0 42 0B F9 76 CD 3E F2 55 37 76 8A 15 5E 8A 9E 99 E2 4A 52 28 73 23 F8 7E ED C7 F5 D8 CE FF EC 46 CC 23 94 5A 0C 15 0F 4C 79 99 1D E0 ED 93 7F 17 51 8B 01 AD 2F 77 9C 80 AA E1 50 D4 03 1C B6 04 AB 06 49 2D A5 F7 04 6F 97 87 E1 74 30 E6 82 E4 39 71 10 CA 9F FA 6A 75 81 2A 02 AC 45 54 48 DA 9B 08 DC 51 64 81 B1 69 6A 4A 7D FB 7C 8F 6C FC C6 43 0B 37 CC C3 3E 80 85 E1 4C AD 13 4B D2 82 76 63 77 15 74 1C 62 0D 57 6A 8C 64 BE 00 6E 6A 21 4C FF 02 C8 C7 34 BD C9 12 C6 B9 E4 E4 AB 30 5B 98 08 F0 B3 60 33 00 54 B2 B3 8A A6 57 E4 6D B9 73 47 BF AA 1D 1B 48 AE 3F
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Derive
Signature	256 bytes : 3A 8F DA 0F 28 4E 64 FC 55 F9 B1 B2 D8 E2 9E F1 B2 79 6D 9D D1 C3 37 5A 32 CE 66 FC F9 C9 A4 7B A5 BF 78 51 EC 63 48 3E CD 47 94 05 6D F3 6F 41 0C 06 73 57 58 D4 C2 07 56 95 21 C4 46 7B C1 94 0C 30 27 03 34 97 31 00 5E 06 2B 0D 6F AF 64 9F 6B A7 B5 2E D1 6E 52 FC DF EF 07 EF CE D1 B0 87 97 B9 C6 A1 AF 79 02 A1 CE B5 A1 37 A6 23 41 C4 23 8D CE 0E D5 48 B8 51 03 34 90 C4 D7 0A AC 1E 47 59 79 C9 CD 48 6F 48 67 24 A9 2B 6B 24 AF 7A C7 EE A5 24 6C FD 65 93 36 C5 BE C9 C5 53 2A 77 00 94 B8 89 BF 7E E3 13 EB EB 91 90 7D 48 BF F2 F8 28 49 5B CE CB 96 37 AD 3F D4 DC 2B 48 F6 D3 E8 0D 26 53 60 64 E5 E8 82 C3 C4 96 BC 74 41 98 99 32 87 82 3C 89 1E 66 CA CD EB 35 DC DF C1 37 5F 17 52 5B D3 9E 31 1A 89 F4 17 BC 98 FD CA 9A 9C 30 75 05 3E 39 2A C0 8D 47 4B 26 F5 89 1B 61
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	NO
Extension	Extended Key Usage (2.5.29.37)
Critical	NO
Purpose #1	Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose #2	Client Authentication (1.3.6.1.5.5.7.3.2)
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	75 20 EA D1 F9 B9 B7 34 D5 E9 E4 35 8A AE E8 64 C6 73 2B A4
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	Subject Alternative Name (2.5.29.17)
Critical	NO
DNS Name	www.google.com
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://aki.google.com/GIAG2.crl

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Public Key	256 bytes : 9C 2A 04 77 5C D8 50 91 3A 06 A3 82 E0 D8 50 48 BC 89 3F F1 19 70 1A 88 46 7E E0 8F C5 F1 89 CE 21 EE 5A FE 61 0D B7 32 44 89 A0 74 0B 53 4F 55 A4 CE 82 62 95 EE EB 59 5F C6 E1 05 80 12 C4 5E 94 3F BC 58 48 38 F4 53 F7 24 E6 FB 91 E9 15 C4 CF F4 53 0D F4 4A FC 9F 54 DE 7D BE A0 6B 6F 87 C0 D0 50 1F 28 30 03 40 DA 08 73 51 6C 7F FF 3A 3C A7 37 06 8E BD 4B 11 04 EB 7D 24 DE E6 F9 FC 31 71 FB 94 D5 60 F3 2E 4A AF 42 D2 CB EA C4 6A 1A B2 CC 53 DD 15 4B 8B 1F C8 19 61 1F CD 9D A8 3E 63 2B 84 35 69 65 84 C8 19 C5 46 22 F8 53 95 BE E3 80 4A 10 C6 2A EC BA 97 20 11 C7 39 99 10 04 A0 F0 61 7A 95 25 8C 4E 52 75 E2 B6 ED 08 CA 14 FC CE 22 6A B3 4E CF 46 03 97 97 03 7E C0 B1 DE 78 AF 45 33 CF BA 3E 71 B7 DE F4 25 25 C2 0D 35 89 9D 9D FB 0E 11 79 89 1E 37 C5 AF 8E 72 69
Exponent	65537
Key Size	2048 bits
Key Usage	Verify
Signature	256 bytes : 36 D7 06 80 11 27 AD 2A 14 9B 38 77 B3 23 A0 75 58 B8 B1 7E 83 42 BA 72 DA 1E D8 8E 36 06 97 E0 F0 95 3B 37 FD 1B 42 58 FE 22 C8 6B BD 38 5E D1 3B 25 6E 12 EB 5E 67 76 46 40 90 DA 14 C8 78 0D ED 95 66 DA 8E 86 6F 80 A1 BA 56 32 95 86 DC DC 6A CA 04 8C 5B 7F F6 BF CC 6F 85 03 58 C3 68 51 13 CD FD C8 F7 79 3D 99 35 F0 56 A3 BD E0 59 ED 4F 44 09 A3 9E 38 7A F6 46 D1 1D 12 9D 4F BE D0 40 FC 55 FE 06 5E 3C DA 1C 56 BD 96 51 7B 6F 57 2A DB A2 AA 96 DC 8C 74 C2 95 BE F0 6E 95 13 FF 17 F0 3C AC B2 10 8D CC 73 FB E8 8F 02 C6 F0 FB 33 B3 95 3B E3 C2 CB 68 58 73 DB A8 24 62 3B 06 35 9D 0D A9 33 BD 78 03 90 2E 4C 78 5D 50 3A 81 D4 EE A0 C8 70 38 DC B2 F9 67 FA 87 40 5D 61 C0 51 8F 6B 83 6B CD 05 3A CA E1 A7 05 78 FC CA DA 94 D0 2C 08 3D 7E 16 79 C8 A0 50 20 24 54 33 71
Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Key Cert Sign, CRL Sign
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Path Length Constraint	0
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://crl.geotrust.com/crls/gtglobal.crl
Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO

Issuer Name	
Country	US
Organization	GeoTrust Inc.
Common Name	GeoTrust Global CA
Serial Number	144470
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Tuesday 21 May 2002 06 h 00 min 00 s Central European Summer Time
Not Valid After	Saturday 21 May 2022 06 h 00 min 00 s Central European Summer Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : DA CC 18 63 30 FD F4 17 23 1A 56 7E 5B DF 3C 6C 38 E4 71 B7 78 91 D4 BC A1 D8 4C F8 A8 43 B6 03 E9 4D 21 07 08 88 DA 58 2F 66 39 29 BD 05 78 88 9D 38 E8 05 B7 6A 7E 71 A4 E6 C4 60 A6 80 EF 80 E4 89 28 0F 9E 25 D6 ED 83 F3 AD A6 91 C7 98 C9 42 18 35 14 9D AD 98 46 92 2E 4F CA F1 87 43 C1 16 95 57 2D 50 EF 89 2D 80 7A 57 AD F2 EE 5F 6B D2 00 8D B9 14 F8 14 15 35 D9 C0 46 A3 7B 72 C8 91 BF C9 55 2B CD D0 97 3E 9C 26 64 CC DF CE 83 19 71 CA 4E E6 D4 D5 7B A9 19 CD 55 DE C8 EC D2 5E 38 53 E5 5C 4F 8C 2D FE 50 23 36 FC 66 E6 C8 8E A4 39 19 00 B7 95 02 39 91 08 0E FE 38 2E D1 1D 05 9A F6 4D 3E 6F 0F 07 1D AF 2C 1E 8F 60 39 E2 FA 36 53 13 39 D4 5E 26 2B DB 3D A8 14 BD 32 EB 18 03 28 52 04 71 E5 A8 33 3D E1 38 B8 07 36 84 62 9C 79 EA 16 30 F4 5F C0 2B E8 71 6B E4 F9
Key Size	2048 bits
Key Usage	Any
Signature	256 bytes : 35 E3 29 6A E5 2F 5D 54 8E 29 50 94 9F 99 1A 14 E4 8F 78 2A 62 94 A2 27 67 9E D0 CF 1A 5E 47 E9 C1 B2 A4 CF DD 41 1A 05 4E 9B 4B EE 4A 6F 55 52 B3 24 A1 37 0A EB 64 76 2A 2E 2C F3 FD 38 75 90 BF FA 71 D8 C7 3D 37 D2 B5 05 95 62 B9 A6 DE 89 3D 36 7B 38 77 48 97 AC A6 20 8F 2E A6 C9 0C C2 B2 99 45 00 C7 CE 11 51 22 22 E0 A5 EA B6 15 48 09 64 EA 5E 4F 74 F7 05 3E C7 8A 52 0C DB 15 B4 BD 6D 98 E5 C6 B1 54 68 A9 E3 69 90 B6 9A A5 0F B8 B9 3F 20 7D AE 4A B5 B8 9C E4 1D B6 AB E6 94 A5 C1 C7 83 AD DB F5 27 87 0E 04 6C D5 FF DD A0 5D ED 87 52 B7 2B 15 02 AE 39 A6 6A 74 E9 DA C4 E7 BC 4D 34 1E A9 5C 4D 33 5F 92 09 2F 88 66 5D 77 97 C7 1D 76 13 A9 D5 E5 F1 16 09 11 35 D5 AC DB 24 71 70 2C 98 56 0B D9 17 B4 D1 E3 51 2B 5E 75 E8 D5 D0 DC 4F 34 ED C2 05 66 80 A1 CB E6 33
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Public Key	256 bytes : A4 78 79 A6 79 86 3B 88 C3 11 C4 A8 35 E0 D3 F1 F3 31 6D 0F F5 66 50 8D 98 E0 57 50 62 00 FC 02 E4 62 7C 0F 9F AA FC 62 70 49 22 ED 37 75 4A B6 78 CE 57 67 02 36 C0 4B E7 C2 D1 E4 23 88 C7 E8 25 3A 2C AE 45 E0 42 0B F9 76 CD 3E F2 55 37 76 8A 15 5E 8A 9E 99 E2 4A 52 28 73 23 F8 7E ED C7 F5 D8 CE FF EC 46 CC 23 94 5A 0C 15 0F 4C 79 99 1D E0 ED 93 7F 17 51 8B 01 AD 2F 77 9C 80 AA E1 50 D4 03 1C B6 04 AB 06 49 2D A5 F7 04 6F 97 87 E1 74 30 E6 82 E4 39 71 10 CA 9F FA 6A 75 81 2A 02 AC 45 54 48 DA 9B 08 DC 51 64 81 B1 69 6A 4A 7D FB 7C 8F 6C FC C6 43 0B 37 CC C3 3E 80 85 E1 4C AD 13 4B D2 82 76 63 77 15 74 1C 62 0D 57 6A 8C 64 BE 00 6E 6A 21 4C FF 02 C8 C7 34 BD C9 12 C6 B9 E4 E4 AB 30 5B 98 08 F0 B3 60 33 00 54 B2 B3 8A A6 57 E4 6D B9 73 47 BF AA 1D 1B 48 AE 3F
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Derive
Signature	256 bytes : 3A 8F DA 0F 28 4E 64 FC 55 F9 B1 B2 D8 E2 9E F1 B2 79 6D 9D D1 C3 37 5A 32 CE 66 FC F9 C9 A4 7B A5 BF 78 51 EC 63 48 3E CD 47 94 05 6D F3 6F 41 0C 06 73 57 58 D4 C2 07 56 95 21 C4 46 7B C1 94 0C 30 27 03 34 97 31 00 5E 06 2B 0D 6F AF 64 9F 6B A7 B5 2E D1 6E 52 FC DF EF 07 EF CE D1 B0 87 97 B9 C6 A1 AF 79 02 A1 CE B5 A1 37 A6 23 41 C4 23 8D CE 0E D5 48 B8 51 03 34 90 C4 D7 0A AC 1E 47 59 79 C9 CD 48 6F 48 67 24 A9 2B 6B 24 AF 7A C7 EE A5 24 6C FD 65 93 36 C5 BE C9 C5 53 2A 77 00 94 B8 89 BF 7E E3 13 EB EB 91 90 7D 48 BF F2 F8 28 49 5B CE CB 96 37 AD 3F D4 DC 2B 48 F6 D3 E8 0D 26 53 60 64 E5 E8 82 C3 C4 96 BC 74 41 98 99 32 87 82 3C 89 1E 66 CA CD EB 35 DC DF C1 37 5F 17 52 5B D3 9E 31 1A 89 F4 17 BC 98 FD CA 9A 9C 30 75 05 3E 39 2A C0 8D 47 4B 26 F5 89 1B 61
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	NO
Extension	Extended Key Usage (2.5.29.37)
Critical	NO
Purpose #1	Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose #2	Client Authentication (1.3.6.1.5.5.7.3.2)
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	75 20 EA D1 F9 B9 B7 34 D5 E9 E4 35 8A AE E8 64 C6 73 2B A4
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	Subject Alternative Name (2.5.29.17)
Critical	NO
DNS Name	www.google.com
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://aki.google.com/GIAG2.crl

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Public Key	256 bytes : 9C 2A 04 77 5C D8 50 91 3A 06 A3 82 E0 D8 50 48 BC 89 3F F1 19 70 1A 88 46 7E E0 8F C5 F1 89 CE 21 EE 5A FE 61 0D B7 32 44 89 A0 74 0B 53 4F 55 A4 CE 82 62 95 EE EB 59 5F C6 E1 05 80 12 C4 5E 94 3F BC 58 48 38 F4 53 F7 24 E6 FB 91 E9 15 C4 CF F4 53 0D F4 4A FC 9F 54 DE 7D BE A0 6B 6F 87 C0 D0 50 1F 28 30 03 40 DA 08 73 51 6C 7F FF 3A 3C A7 37 06 8E BD 4B 11 04 EB 7D 24 DE E6 F9 FC 31 71 FB 94 D5 60 F3 2E 4A AF 42 D2 CB EA C4 6A 1A B2 CC 53 DD 15 4B 8B 1F C8 19 61 1F CD 9D A8 3E 63 2B 84 35 69 65 84 C8 19 C5 46 22 F8 53 95 BE E3 80 4A 10 C6 2A EC BA 97 20 11 C7 39 99 10 04 A0 F0 61 7A 95 25 8C 4E 52 75 E2 B6 ED 08 CA 14 FC CE 22 6A B3 4E CF 46 03 97 97 03 7E C0 B1 DE 78 AF 45 33 CF BA 3E 71 B7 DE F4 25 25 C2 0D 35 89 9D 9D FB 0E 11 79 89 1E 37 C5 AF 8E 72 69
Exponent	65537
Key Size	2048 bits
Key Usage	Verify
Signature	256 bytes : 36 D7 06 80 11 27 AD 2A 14 9B 38 77 B3 23 A0 75 58 B8 B1 7E 83 42 BA 72 DA 1E D8 8E 36 06 97 E0 F0 95 3B 37 FD 1B 42 58 FE 22 C8 6B BD 38 5E D1 3B 25 6E 12 EB 5E 67 76 46 40 90 DA 14 C8 78 0D ED 95 66 DA 8E 86 6F 80 A1 BA 56 32 95 86 DC DC 6A CA 04 8C 5B 7F F6 BF CC 6F 85 03 58 C3 68 51 13 CD FD C8 F7 79 3D 99 35 F0 56 A3 BD E0 59 ED 4F 44 09 A3 9E 38 7A F6 46 D1 1D 12 9D 4F BE D0 40 FC 55 FE 06 5E 3C DA 1C 56 BD 96 51 7B 6F 57 2A DB A2 AA 96 DC 8C 74 C2 95 BE F0 6E 95 13 FF 17 F0 3C AC B2 10 8D CC 73 FB E8 8F 02 C6 F0 FB 33 B3 95 3B E3 C2 CB 68 58 73 DB A8 24 62 3B 06 35 9D 0D A9 33 BD 78 03 90 2E 4C 78 5D 50 3A 81 D4 EE A0 C8 70 38 DC B2 F9 67 FA 87 40 5D 61 C0 51 8F 6B 83 6B CD 05 3A CA E1 A7 05 78 FC CA DA 94 D0 2C 08 3D 7E 16 79 C8 A0 50 20 24 54 33 71
Extension	Key Usage (2.5.29.15)
Critical	YES
Usage	Key Cert Sign, CRL Sign
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Path Length Constraint	0
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	4A DD 06 16 1B BC F6 68 B5 76 F5 81 B6 B8 62 1A BA 5A 81 2F
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://crl.geotrust.com/crls/gtglobal.crl
Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO

Issuer Name	
Country	US
Organization	GeoTrust Inc.
Common Name	GeoTrust Global CA
Serial Number	144470
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Tuesday 21 May 2002 06 h 00 min 00 s Central European Summer Time
Not Valid After	Saturday 21 May 2022 06 h 00 min 00 s Central European Summer Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : DA CC 18 63 30 FD F4 17 23 1A 56 7E 5B DF 3C 6C 38 E4 71 B7 78 91 D4 BC A1 D8 4C F8 A8 43 B6 03 E9 4D 21 07 08 88 DA 58 2F 66 39 29 BD 05 78 88 9D 38 E8 05 B7 6A 7E 71 A4 E6 C4 60 A6 80 EF 80 E4 89 28 0F 9E 25 D6 ED 83 F3 AD A6 91 C7 98 C9 42 18 35 14 9D AD 98 46 92 2E 4F CA F1 87 43 C1 16 95 57 2D 50 EF 89 2D 80 7A 57 AD F2 EE 5F 6B D2 00 8D B9 14 F8 14 15 35 D9 C0 46 A3 7B 72 C8 91 BF C9 55 2B CD D0 97 3E 9C 26 64 CC DF CE 83 19 71 CA 4E E6 D4 D5 7B A9 19 CD 55 DE C8 EC D2 5E 38 53 E5 5C 4F 8C 2D FE 50 23 36 FC 66 E6 C8 8E A4 39 19 00 B7 95 02 39 91 0B 0E FE 38 2E D1 1D 05 9A F6 4D 3E 6F 0F 07 1D AF 2C 1E 8F 60 39 E2 FA 36 53 13 39 D4 5E 26 2B DB 3D A8 14 BD 32 EB 18 03 28 52 04 71 E5 A8 33 3D E1 38 B8 07 36 84 62 9C 79 EA 16 30 F4 5F C0 2B E8 71 6B E4 F9
Key Size	2048 bits
Key Usage	Any
Signature	256 bytes : 35 E3 29 6A E5 2F 5D 54 8E 29 50 94 9F 99 1A 14 E4 8F 78 2A 62 94 A2 27 67 9E D0 CF 1A 5E 47 E9 C1 B2 A4 CF DD 41 1A 05 4E 9B 4B EE 4A 6F 55 52 B3 24 A1 37 0A EB 64 76 2A 2E 2C F3 FD 38 75 90 BF FA 71 D8 C7 3D 37 D2 B5 05 95 62 B9 A6 DE 89 3D 36 7B 38 77 48 97 AC A6 20 8F 2E A6 C9 0C C2 B2 99 45 00 C7 CE 11 51 22 22 E0 A5 EA B6 15 48 09 64 EA 5E 4F 74 F7 05 3E C7 8A 52 0C DB 15 B4 BD 6D 98 E5 C6 B1 54 68 A9 E3 69 90 B6 9A A5 0F B8 B9 3F 20 7D AE 4A B5 B8 9C E4 1D B6 AB E6 94 A5 C1 C7 83 AD DB F5 27 87 0E 04 6C D5 FF DD A0 5D ED 87 52 B7 2B 15 02 AE 39 A6 6A 74 E9 DA C4 E7 BC 4D 34 1E A9 5C 4D 33 5F 92 09 2F 88 66 5D 77 97 C7 1D 76 13 A9 D5 E5 F1 16 09 11 35 D5 AC DB 24 71 70 2C 98 56 0B D9 17 B4 D1 E3 51 2B 5E 75 E8 D5 D0 DC 4F 34 ED C2 05 66 80 A1 CB E6 33
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	YES
Extension	Subject Key Identifier (2.5.29.14)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E
Extension	Authority Key Identifier (2.5.29.35)
Critical	NO
Key ID	C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E

Public Key Info

Algorithm RSA Encryption (1.2.840.113549.1.1.1)

Public Key 256 bytes : A4 78 79 A6 79 86 3B 88 C3 11 C4 A8 35 E0 D3 F1
F3 31 6D 0F F5 66 50 8D 9B E0 57 50 62 00 FC 02 E4 62 7C 0F
9F AA FC 62 70 49 22 ED 37 75 4A B6 78 CE 57 67 02 36 C0 4B
E7 C2 D1 E4 23 88 C7 E8 25 3A 2C AE 45 E0 42 0B F9 76 CD 3E
F2 55 37 76 8A 15 5E 8A 9E 99 E2 4A 52 28 73 23 F8 7E ED C7
F5 D8 CE FF EC 46 CC 23 94 5A 0C 15 0F 4C 79 99 1D E0 ED 93
7F 17 51 8B 01 AD 2F 77 9C 80 AA E1 50 D4 03 1C B6 04 AB 06

Public Key Info

Algorithm RSA Encryption (1.2.840.113549.1.1.1)

Public Key 256 bytes : 9C 2A 04 77 5C D8 50 91 3A 06 A3 82 E0 D8 50
48 BC 89 3F F1 19 70 1A 88 46 7E E0 8F C5 F1 89 CE 21 EE
5A FE 61 0D 87 32 44 89 A0 74 0B 53 4F 55 A4 CE 82 62 95
EE EB 59 5F C6 E1 05 80 12 C4 5E 94 3F BC 58 48 38 F4 53
F7 24 E6 FB 91 E9 15 C4 CF F4 53 0D F4 4A FC 9F 54 DE 7D
BE A0 6B 6F 87 C0 D0 50 1F 28 30 03 40 DA 08 73 51 6C 7F

Issuer Name

Country US
Organization GeoTrust Inc.
Common Name GeoTrust Global CA
Serial Number 144470
Version 3
Signature Algorithm SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)

Keychain Access



Click to unlock the System Roots keychain.

Keychains

- login
- Local Items
- System
- System Roots

Category

- All Items
- Passwords
- Secure Notes
- My Certificates
- Keys
- Certificates



GeoTrust Global CA

Root certificate authority

Expires: Saturday 21 May 2022 06 h 00 min 00 s Central European Summer Time

✓ This certificate is valid

Name	Kind	Date Modified	Expires	Keychain
Equifax Secure eBusiness CA-2	certificate	--	23 Jun 2019 14:14:45	System Roots
Equifax Secure Global eBusiness CA-1	certificate	--	21 Jun 2020 06:00:00	System Roots
Federal Common Policy CA	certificate	--	01 Dec 2030 17:45:27	System Roots
GeoTrust Global CA	certificate	--	21 May 2022 06:00:00	System Roots
GeoTrust Primary Certification Authority	certificate	--	17 Jul 2036 01:59:59	System Roots
GeoTrust Primary Certification Authority - G2	certificate	--	19 Jan 2038 00:59:59	System Roots
GeoTrust Primary Certification Authority - G3	certificate	--	02 Dec 2037 00:59:59	System Roots
Global Chambersign Root	certificate	--	30 Sep 2037 18:14:18	System Roots
Global Chambersign Root - 2008	certificate	--	31 Jul 2038 14:31:40	System Roots
GlobalSign	certificate	--	18 Mar 2029 11:00:00	System Roots
GlobalSign	certificate	--	19 Jan 2038 04:14:07	System Roots
GlobalSign	certificate	--	19 Jan 2038 04:14:07	System Roots
GlobalSign	certificate	--	15 Dec 2021 09:00:00	System Roots
GlobalSign Root CA	certificate	--	28 Jan 2028 13:00:00	System Roots
Go Daddy Class 2 Certification Authority	certificate	--	29 Jun 2034 19:06:20	System Roots
Go Daddy Root Certificate Authority - G2	certificate	--	01 Jan 2038 00:59:59	System Roots
GTE CyberTrust Global Root	certificate	--	14 Aug 2018 01:59:00	System Roots
Hellenic Academic and Research Institutions RootCA 2011	certificate	--	01 Dec 2031 14:49:52	System Roots
Hongkong Post Root CA 1	certificate	--	15 May 2023 06:52:29	System Roots
http://www.valicert.com/	certificate	--	26 Jun 2019 00:23:48	System Roots
http://www.valicert.com/	certificate	--	26 Jun 2019 02:19:54	System Roots
http://www.valicert.com/	certificate	--	26 Jun 2019 02:22:33	System Roots

206 items

Critical NO

Policy ID #1 (1.3.6.1.4.1.11129.2.5.1)

Extension CRL Distribution Points (2.5.29.31)

Critical NO

URI <http://aki.google.com/GIAG2.crl>

Extension CRL Distribution Points (2.5.29.31)

Critical NO

URI <http://crl.geotrust.com/crls/gtglobal.crl>

Extension Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)

Critical NO

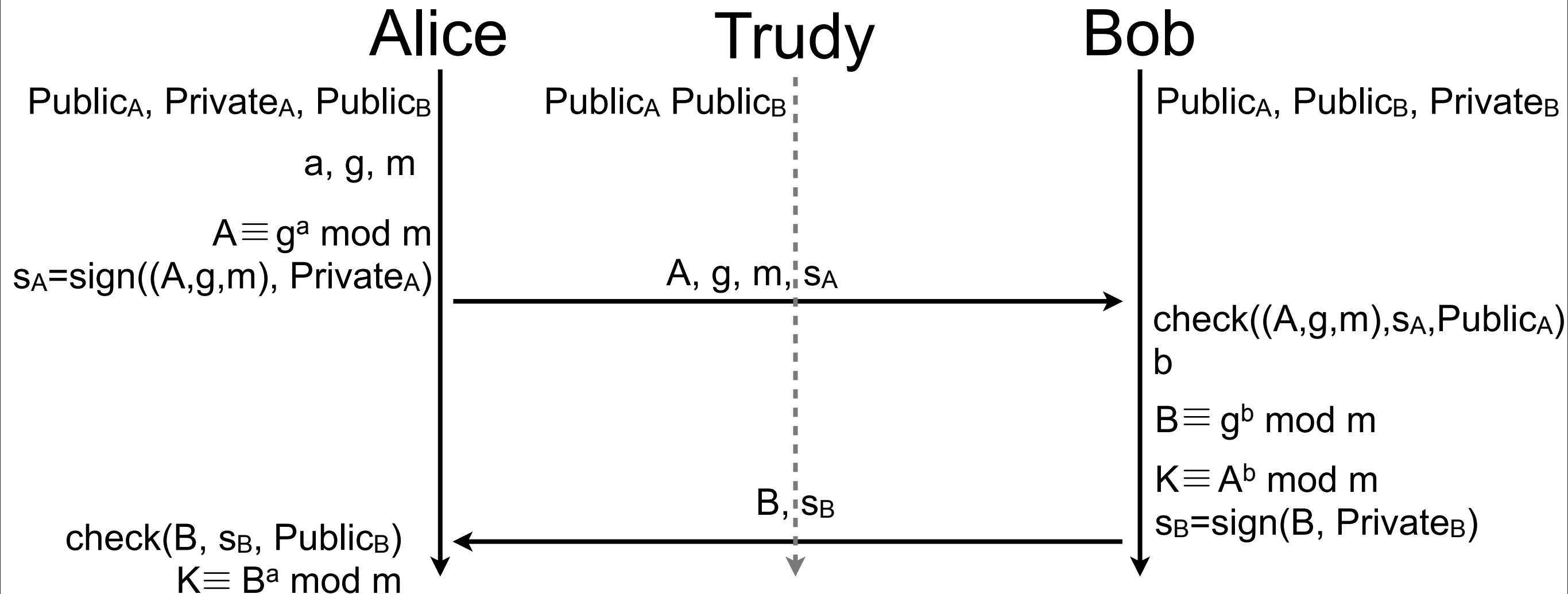
Extension Authority Key Identifier (2.5.29.35)

Critical NO

Key ID C0 7A 98 68 8D 89 FB AB 05 64 0C 11 7D AA 7D 65 B8 CA CC 4E

Diffie-Hellman key exchange (the return)

- Trudy cannot perform her attack anymore



Problem solved?

- fill me
- fill me
- fill me

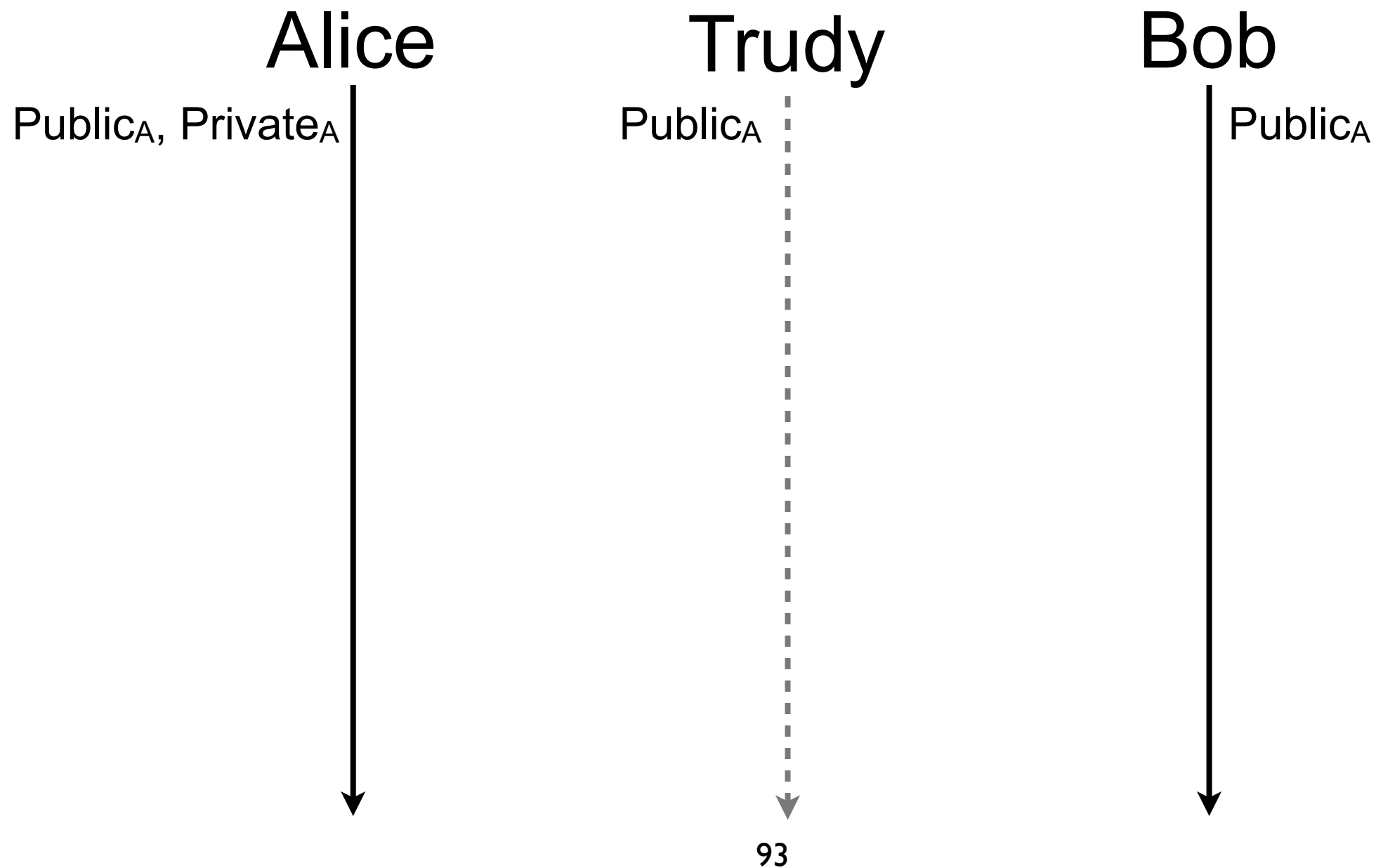
Problem solved?

- fill me
- fill me
- fill me

Replay attacks are still possible!

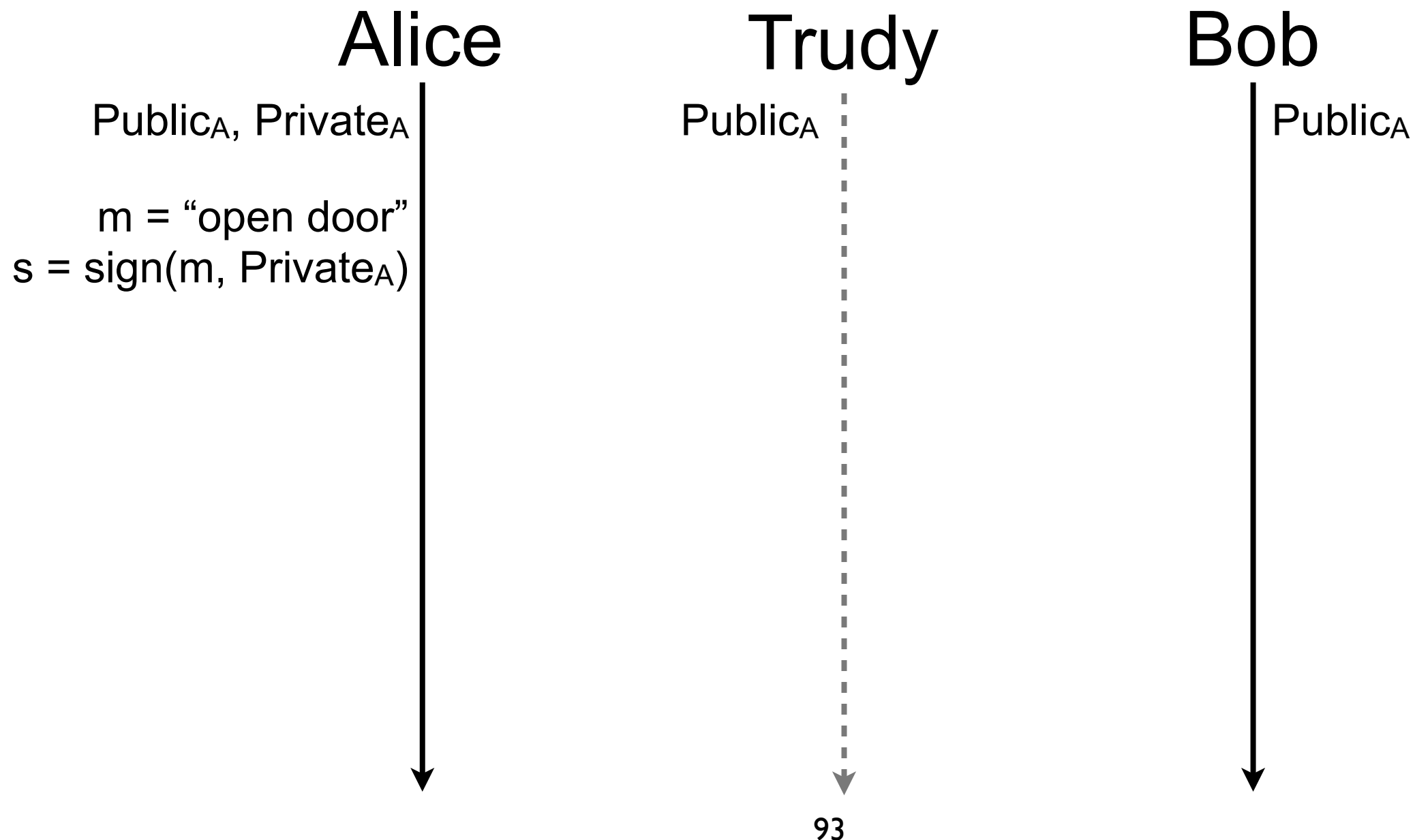
Nonce

- Trudy can replay a message



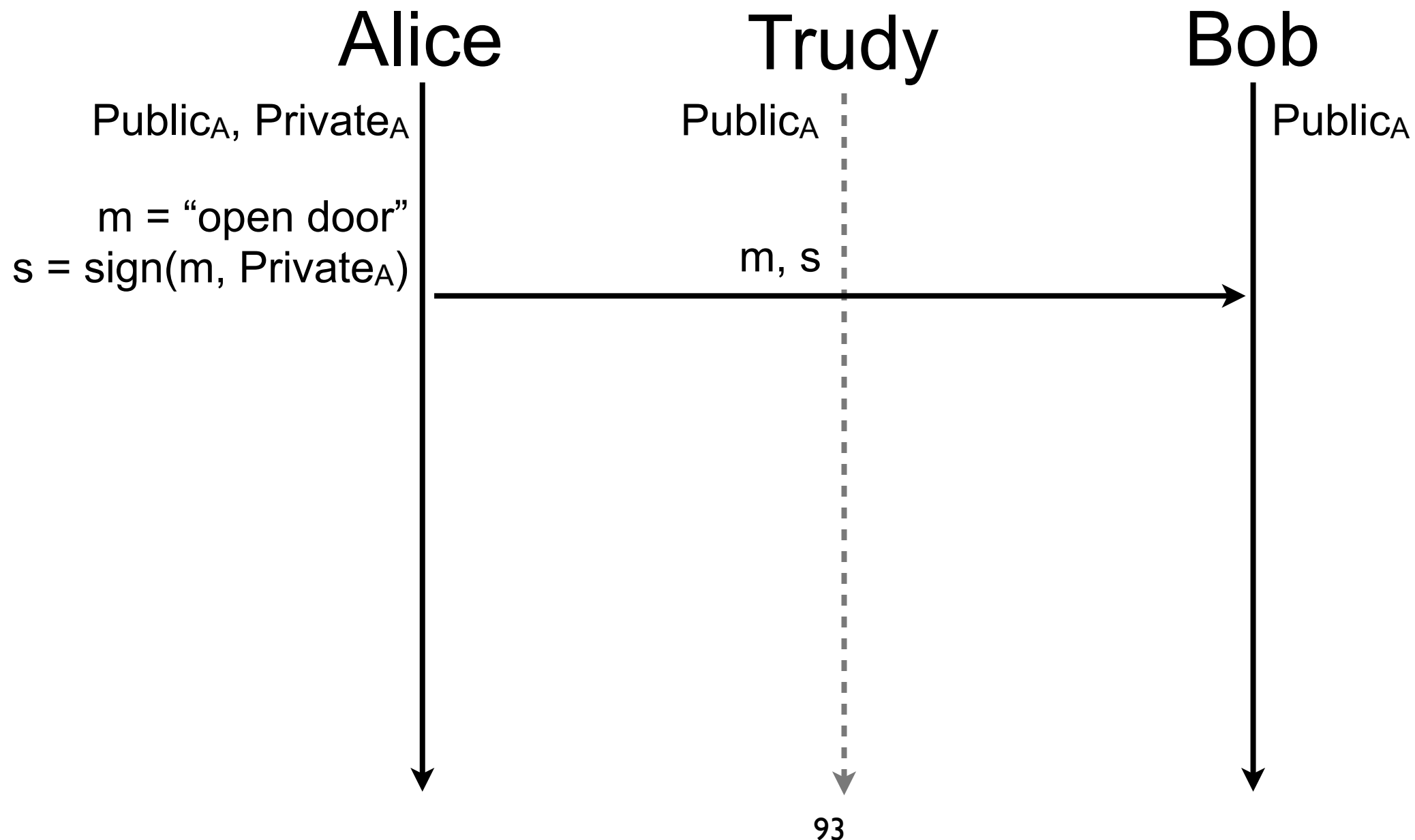
Nonce

- Trudy can replay a message



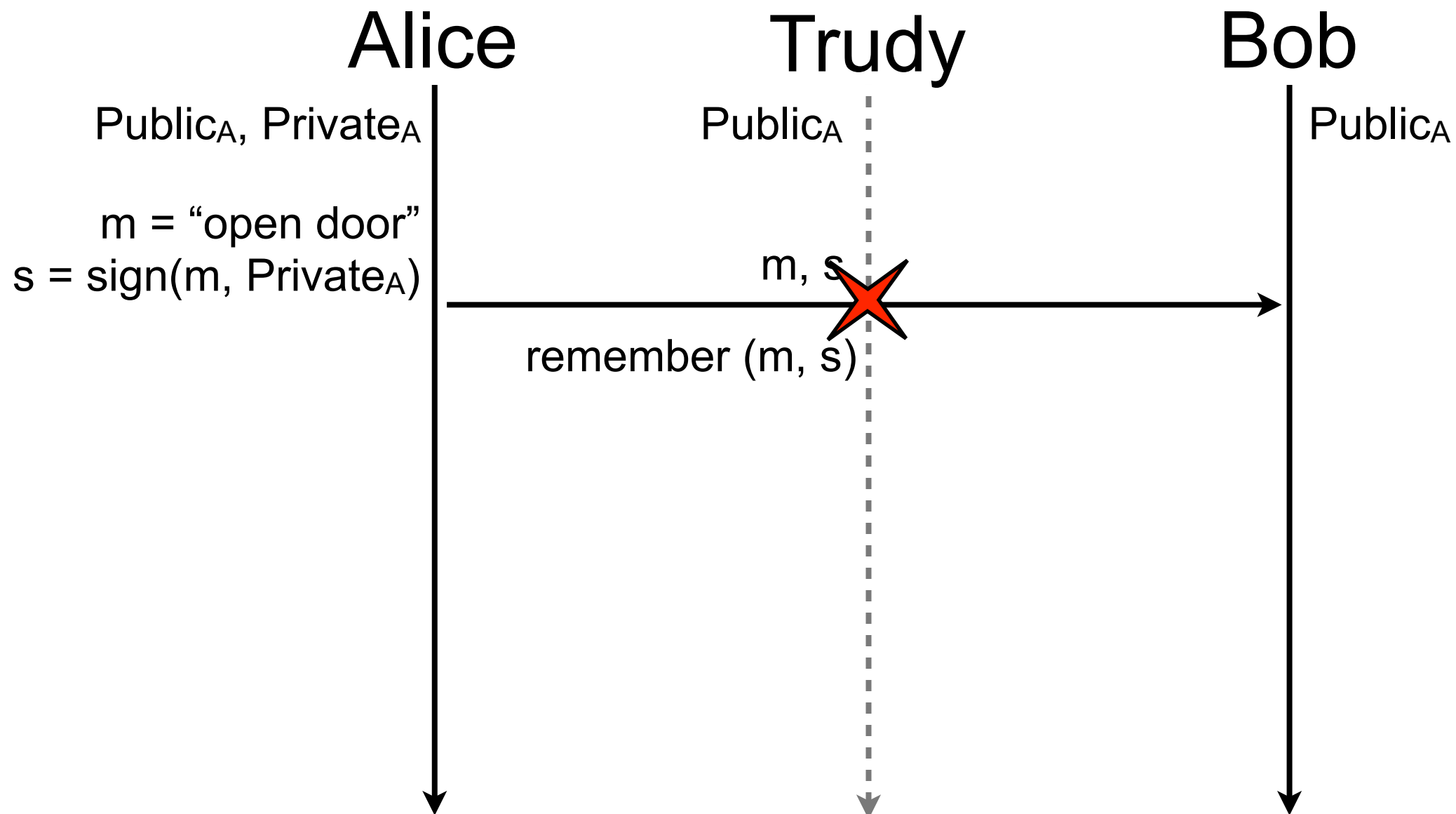
Nonce

- Trudy can replay a message



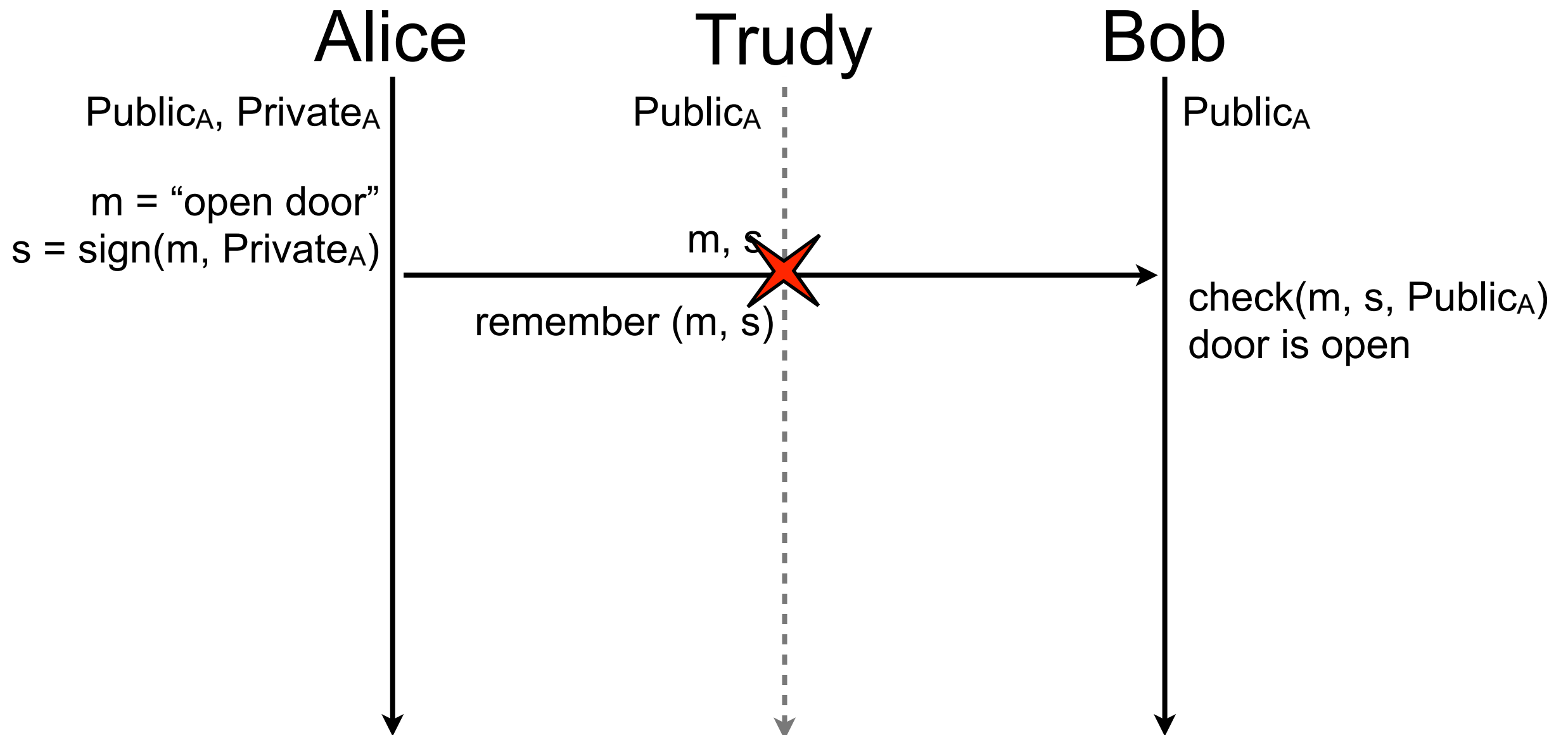
Nonce

- Trudy can replay a message



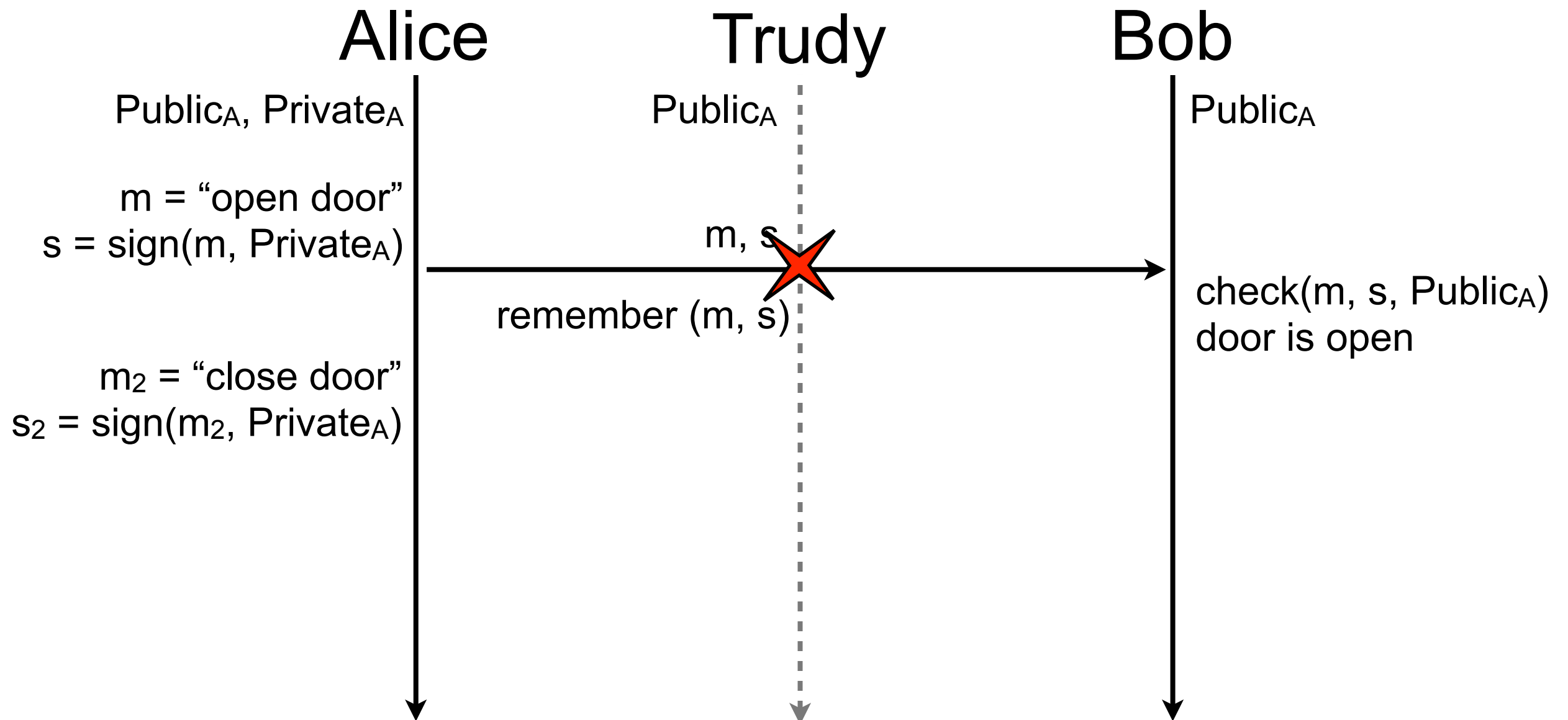
Nonce

- Trudy can replay a message



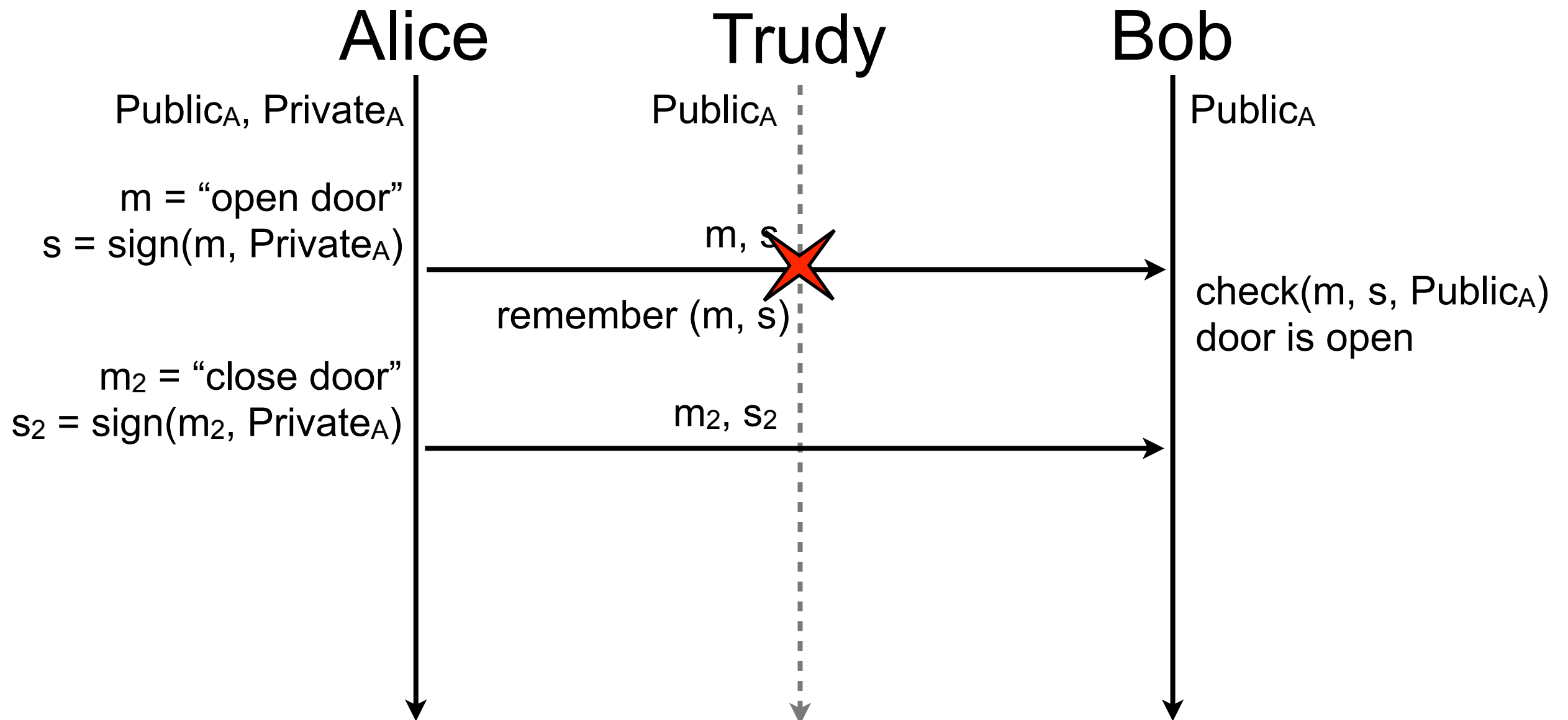
Nonce

- Trudy can replay a message



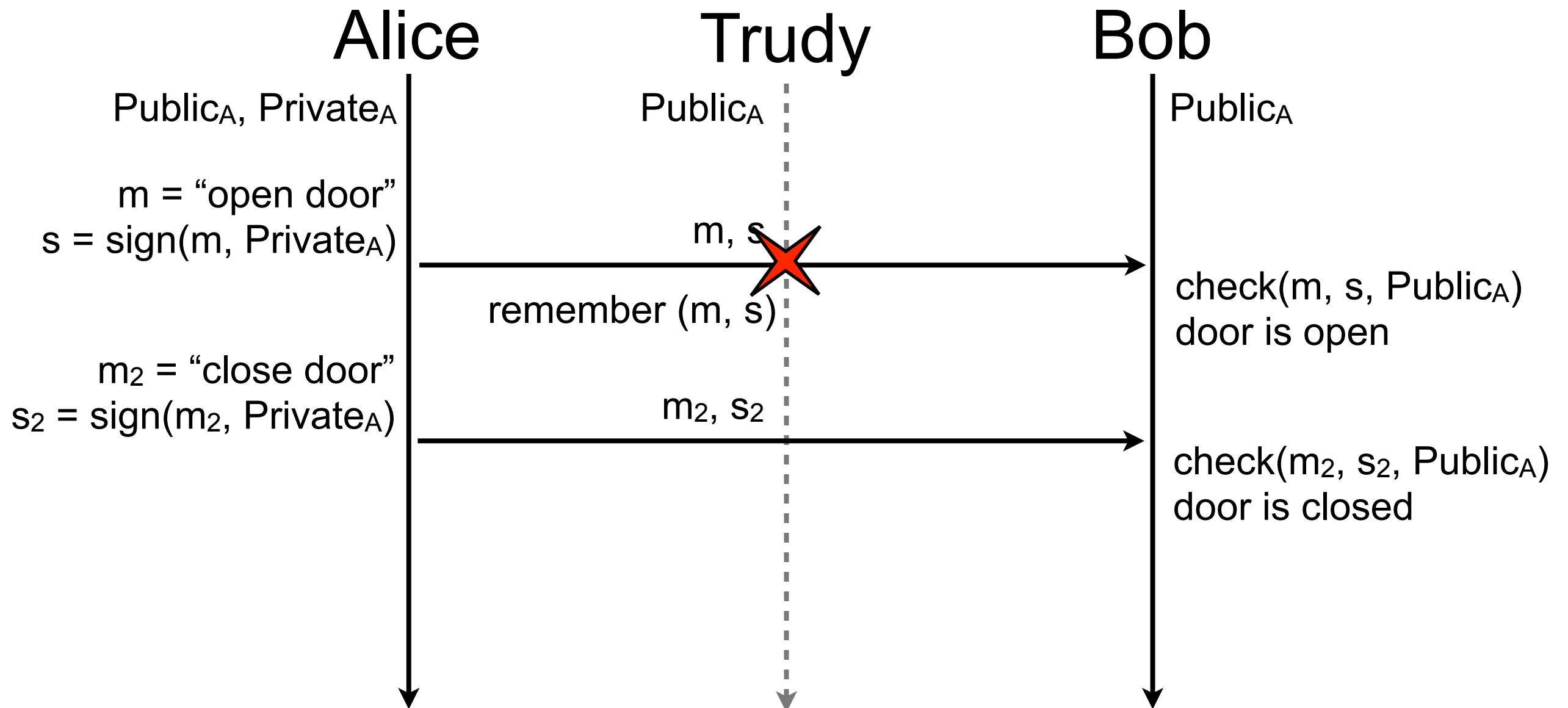
Nonce

- Trudy can replay a message



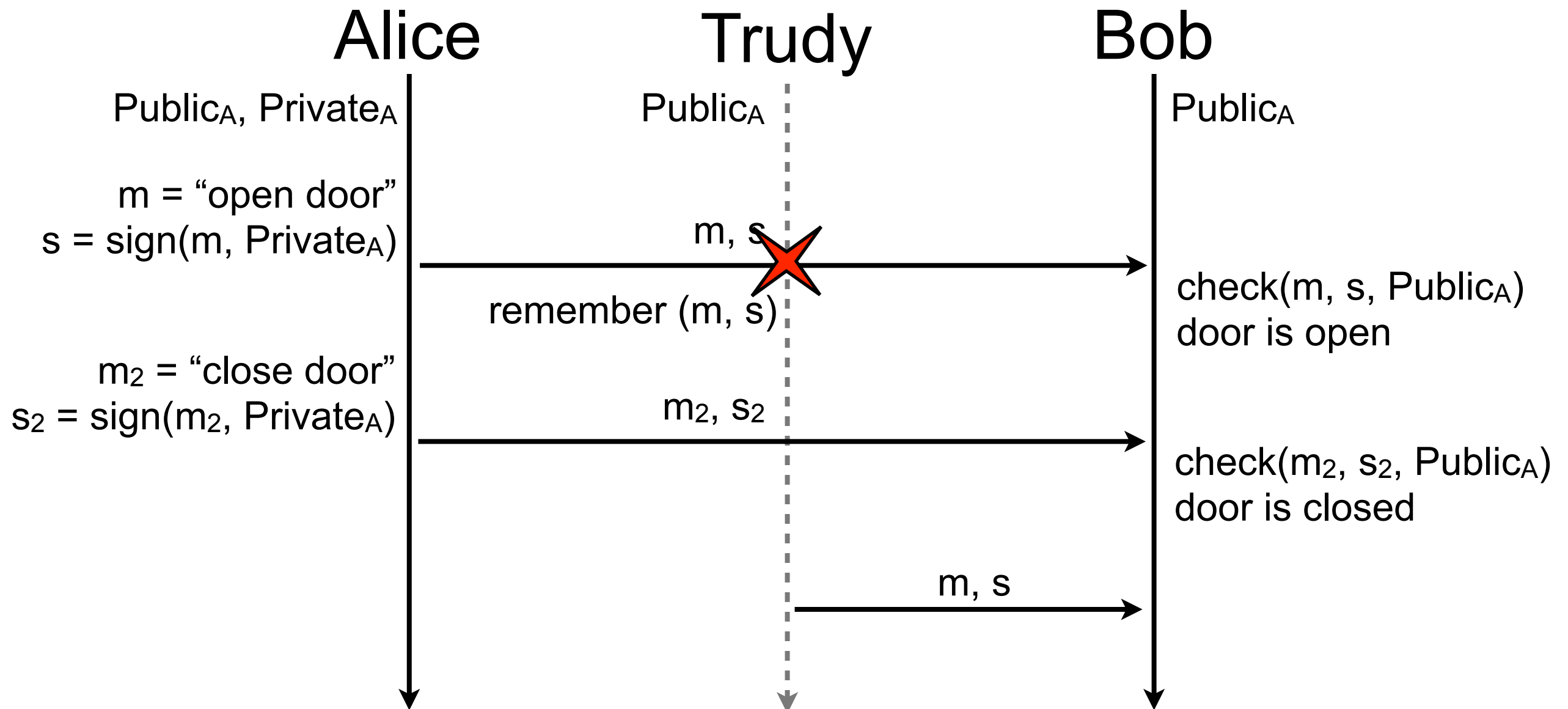
Nonce

- Trudy can replay a message



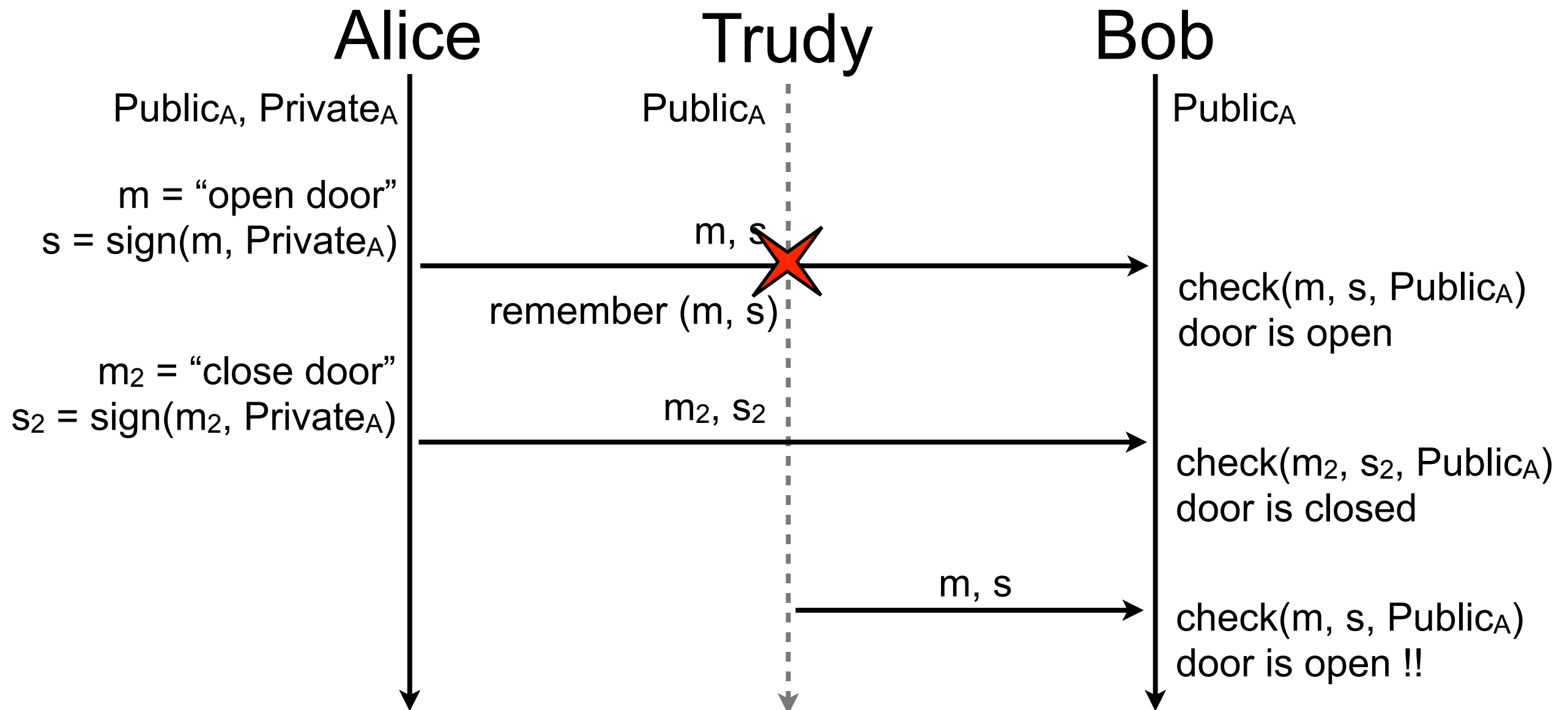
Nonce

- Trudy can replay a message



Nonce

- Trudy can replay a message

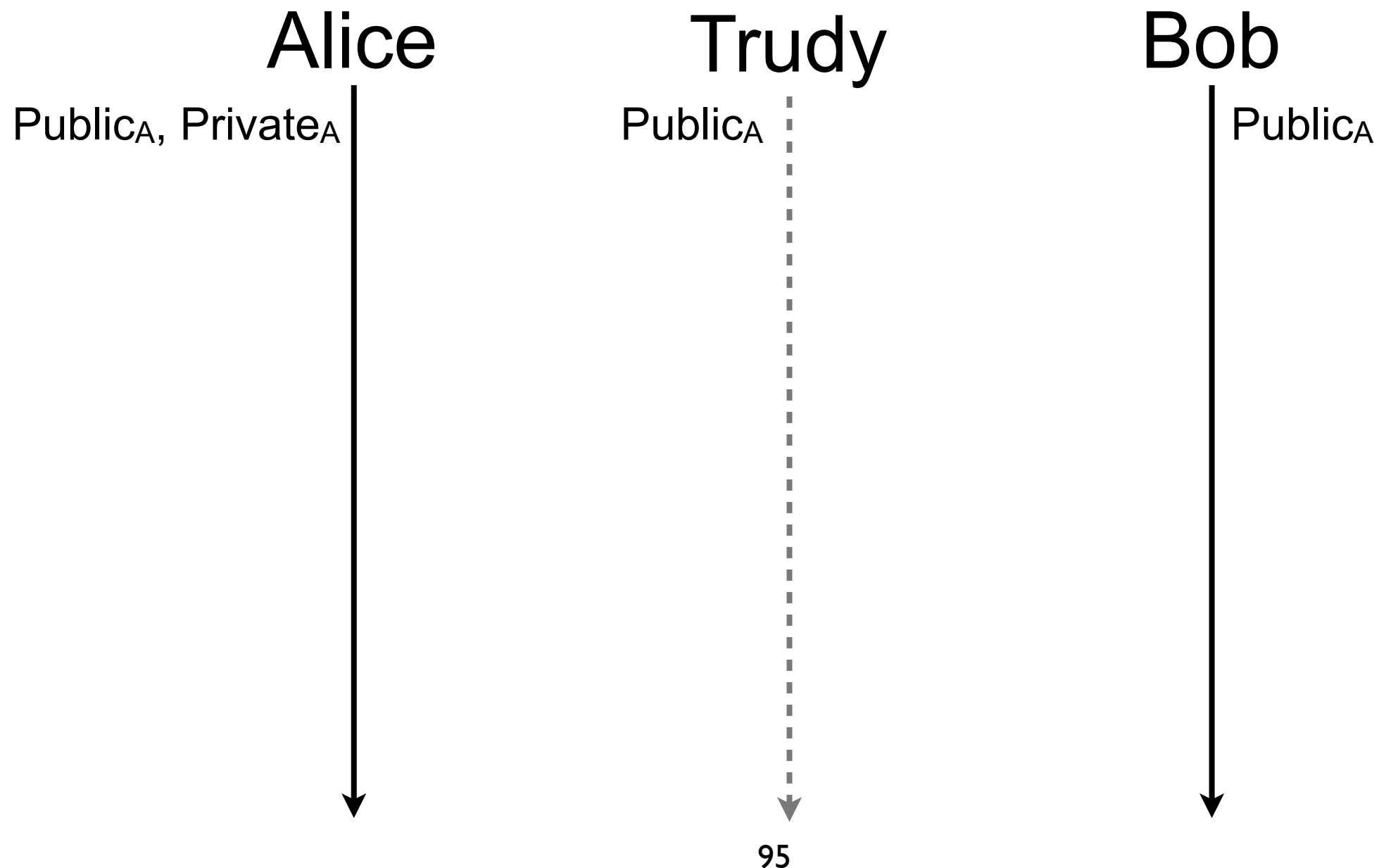


Nonce (contd.)

- A nonce is a number used only once
- Three general methods to create nonces
 - sequential number
 - increment after each use
 - keep it in non-volatile storage in case of reboot
 - timestamp
 - current time of the nonce generation
 - be sure clock is not going backward (e.g., winter time)
 - random number
 - low collision probability if the pseudo random number generator is good and random number is big enough (e.g., more than 128 bits)
- Nonce alone is rarely enough to have a good protection
 - not robust to eavesdropping or man-in-the-middle attack

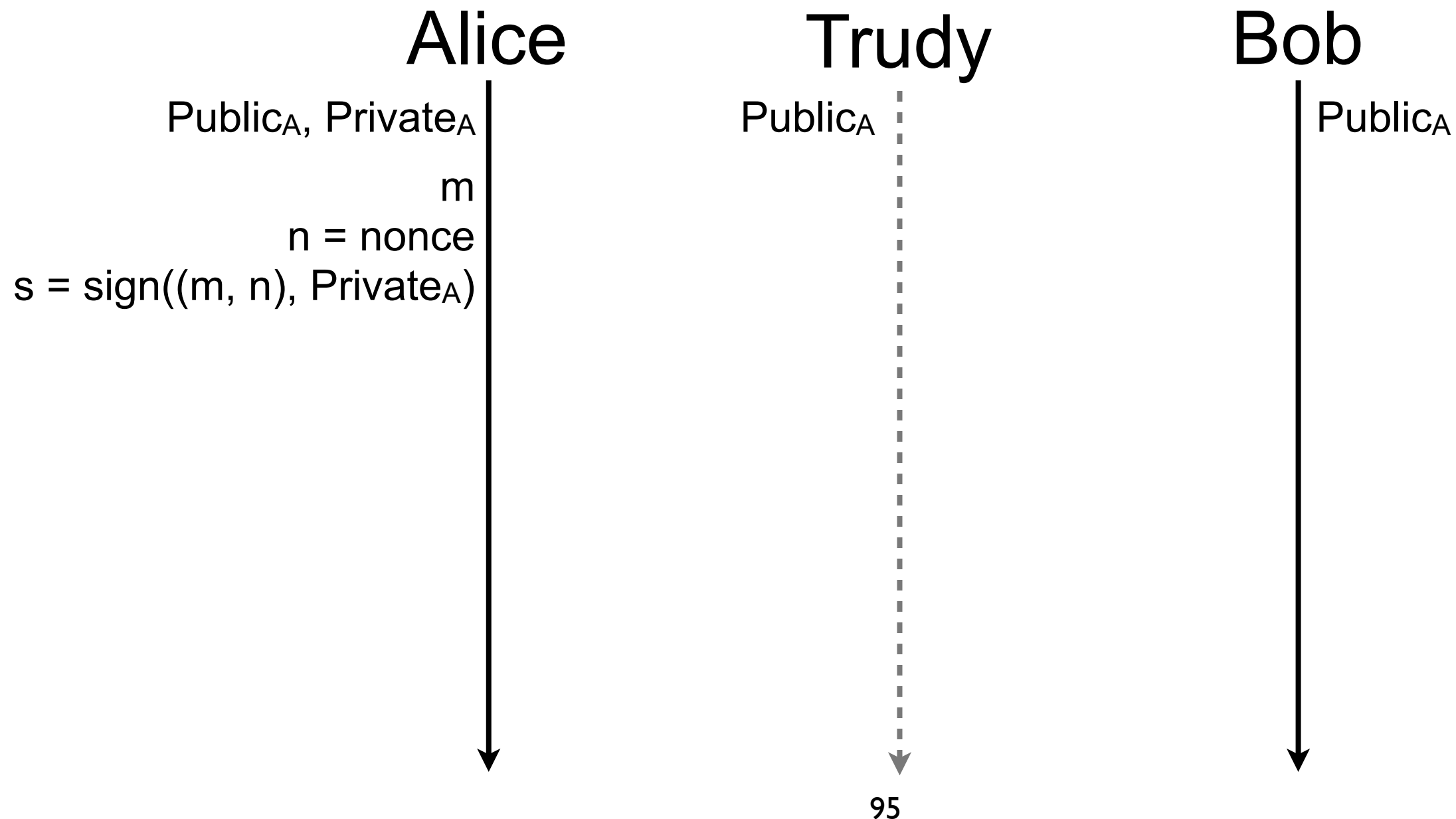
Nonce (contd.)

- Each message is made unique thanks to the nonce



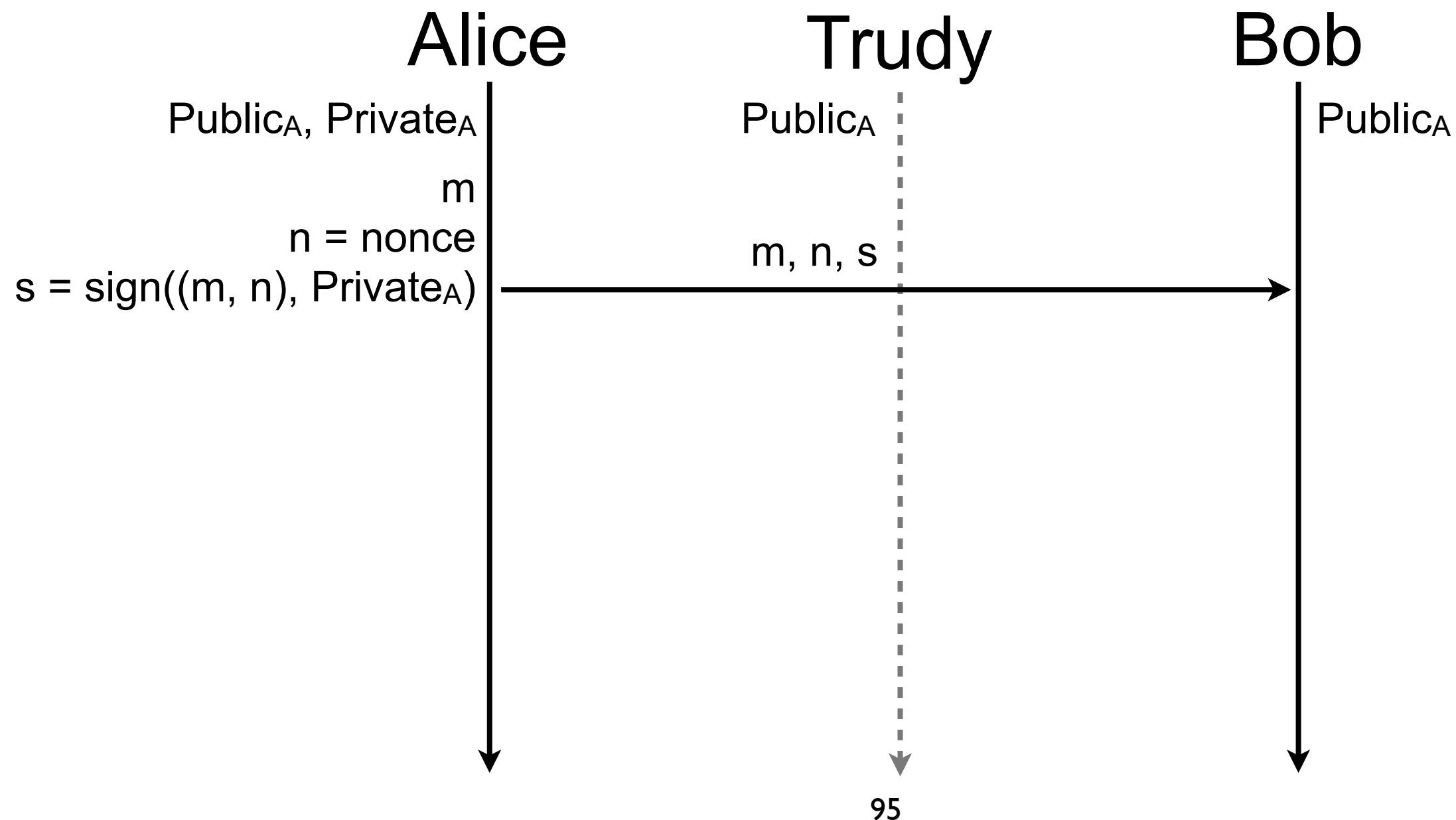
Nonce (contd.)

- Each message is made unique thanks to the nonce



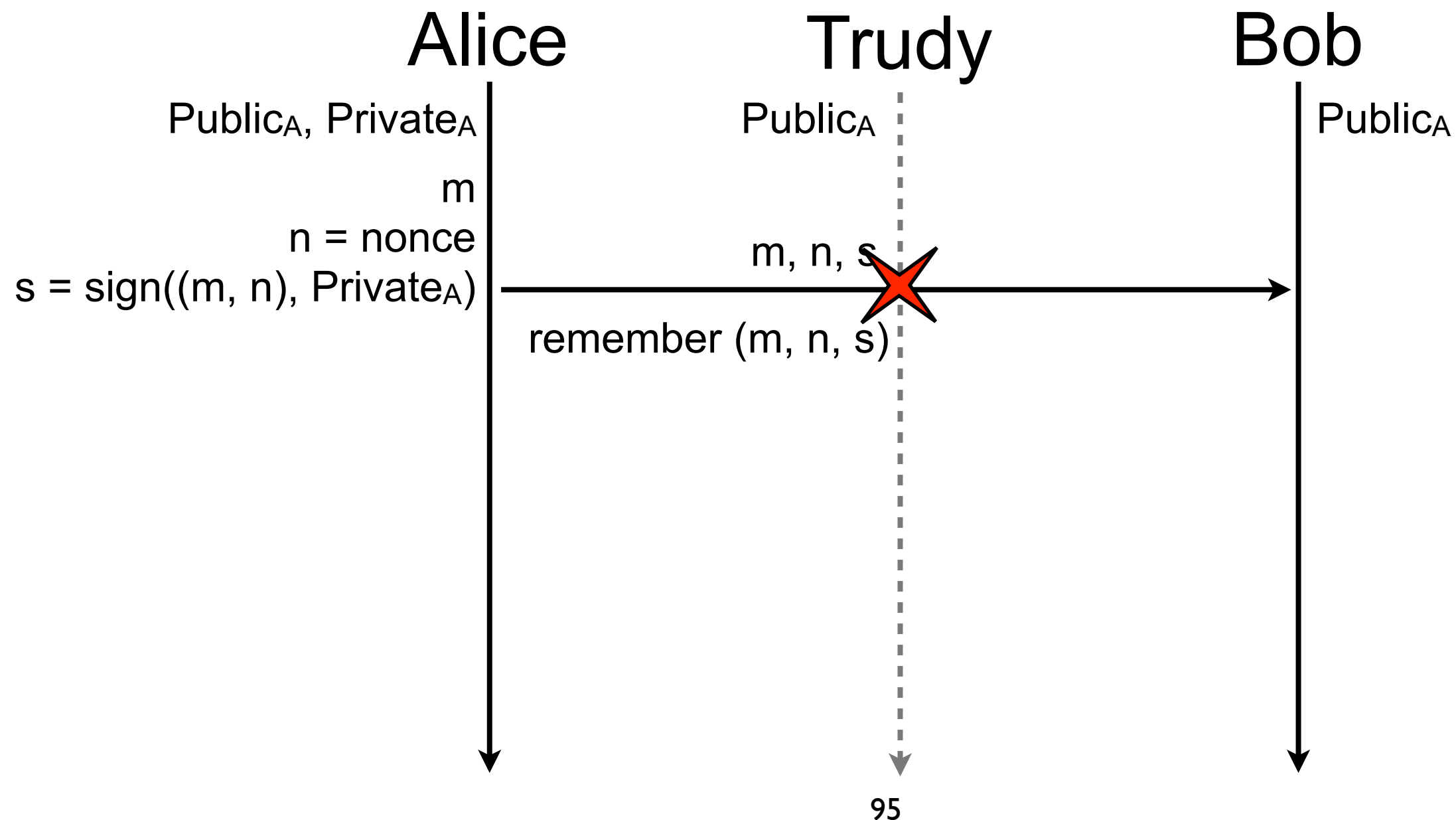
Nonce (contd.)

- Each message is made unique thanks to the nonce



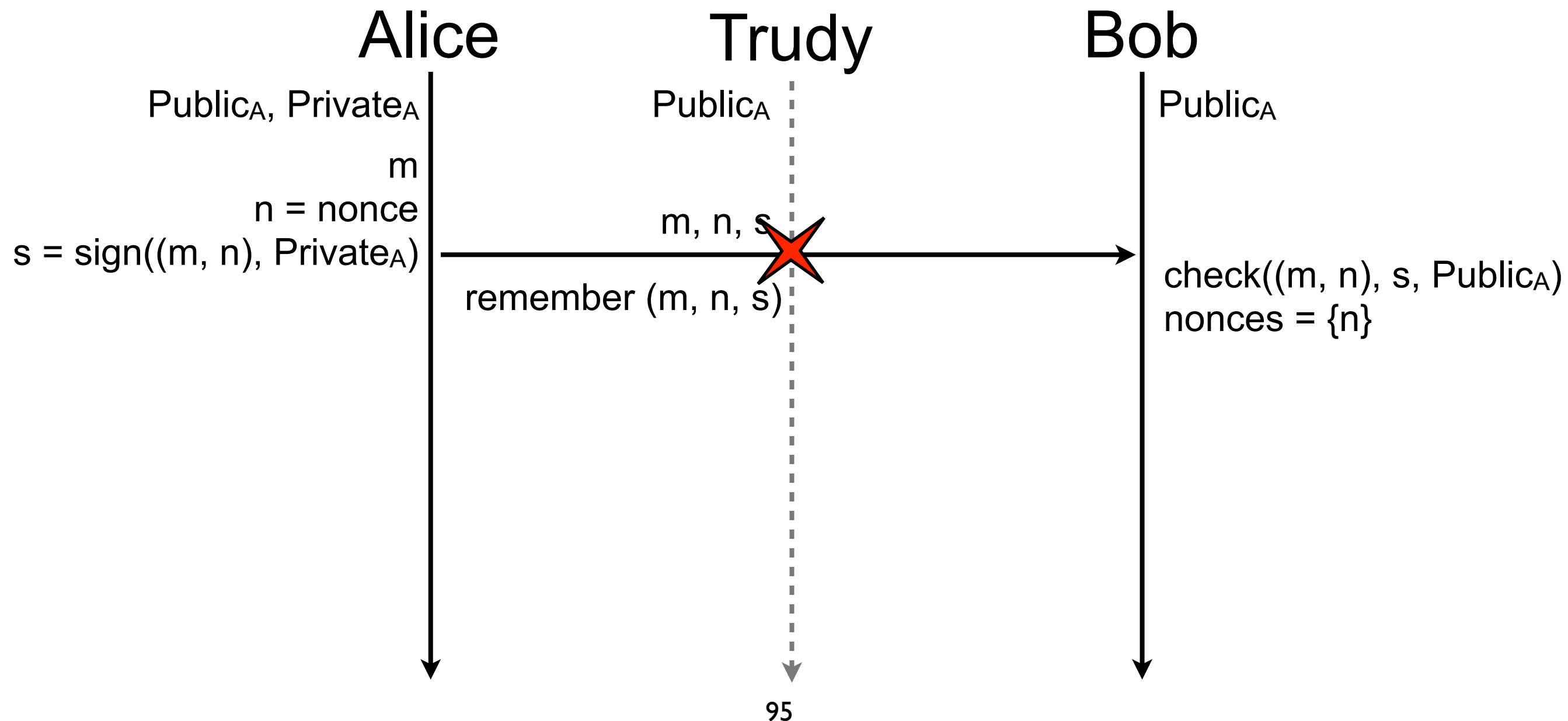
Nonce (contd.)

- Each message is made unique thanks to the nonce



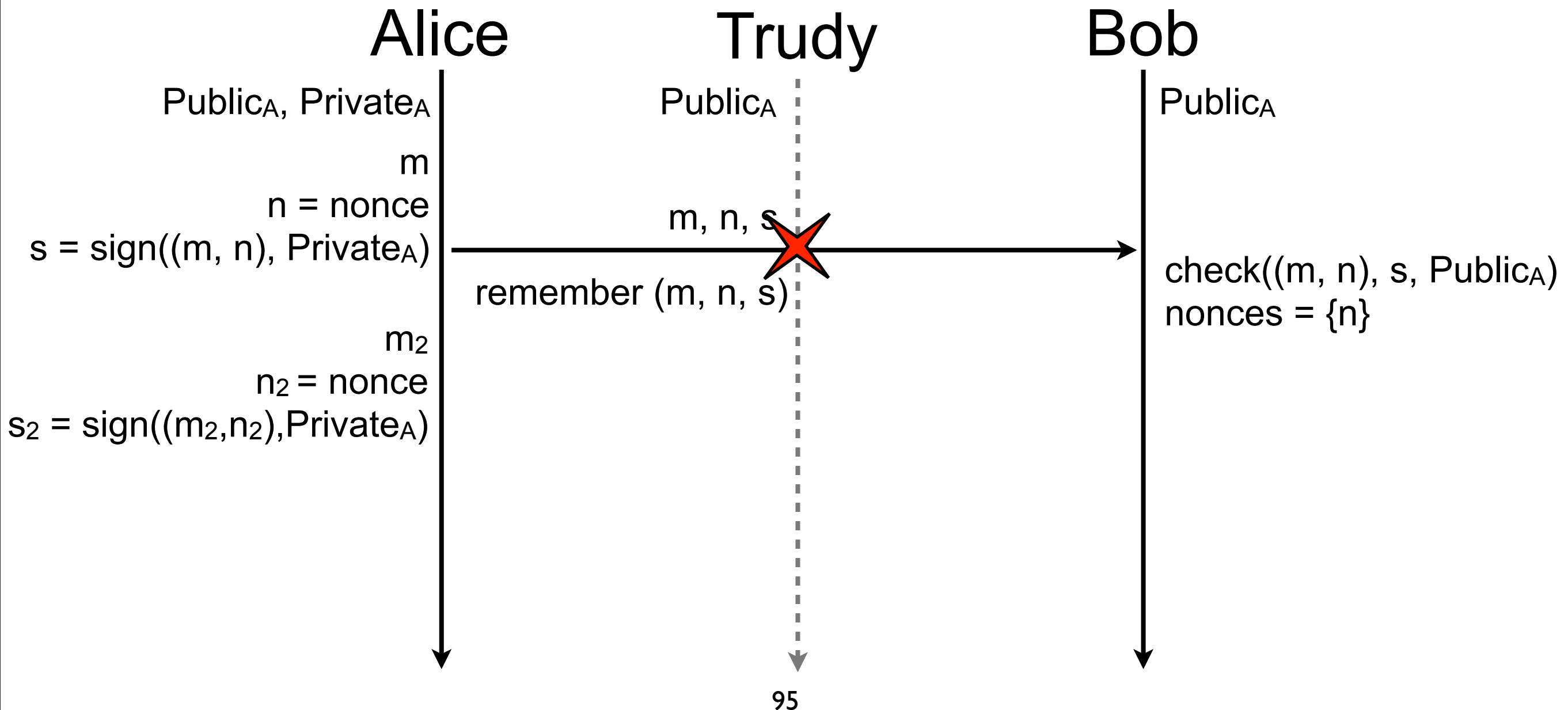
Nonce (contd.)

- Each message is made unique thanks to the nonce



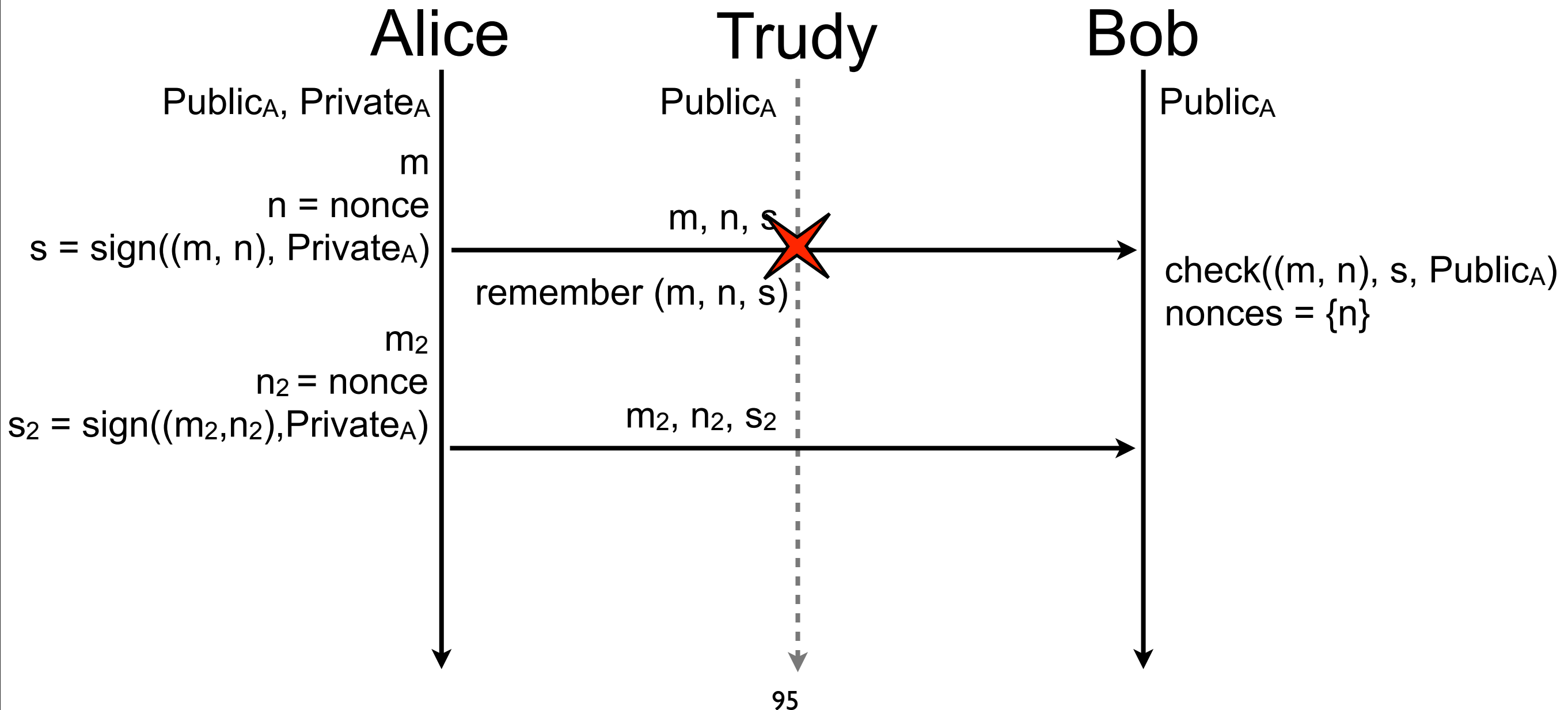
Nonce (contd.)

- Each message is made unique thanks to the nonce



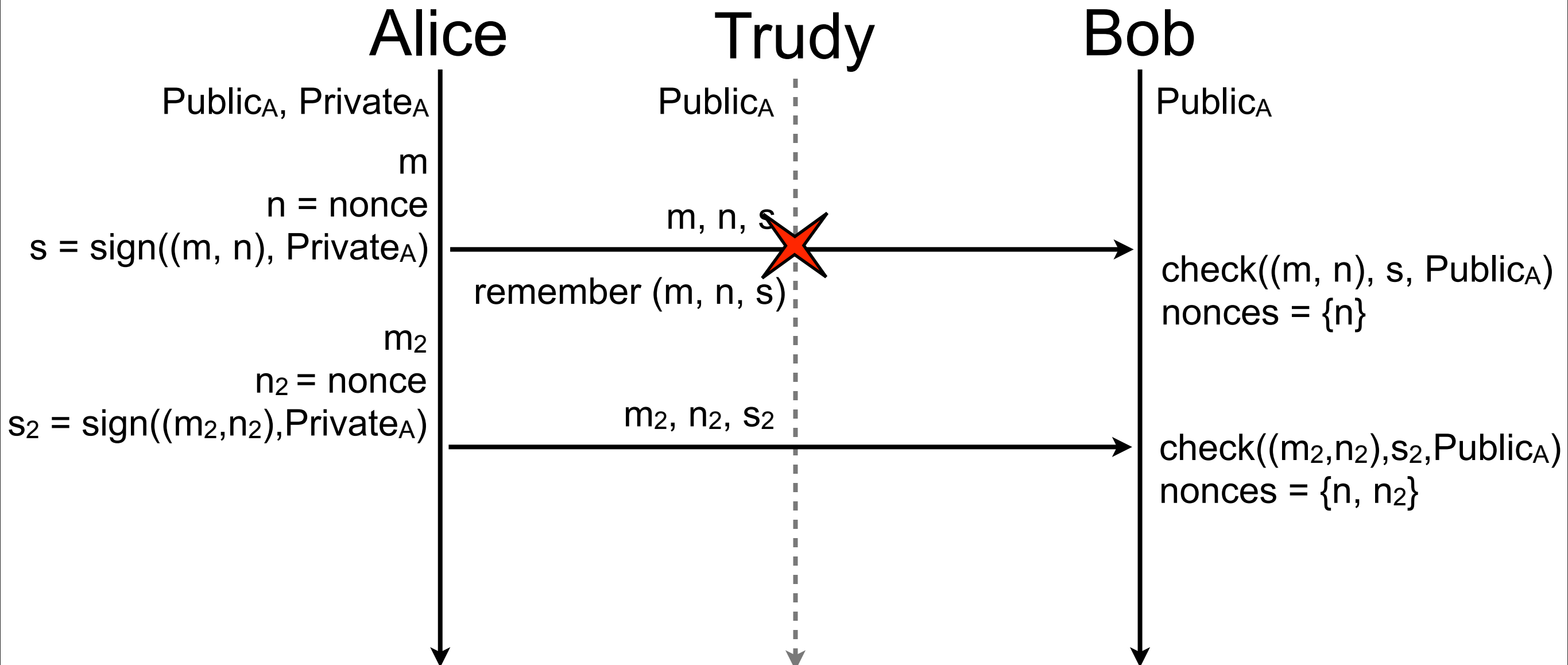
Nonce (contd.)

- Each message is made unique thanks to the nonce



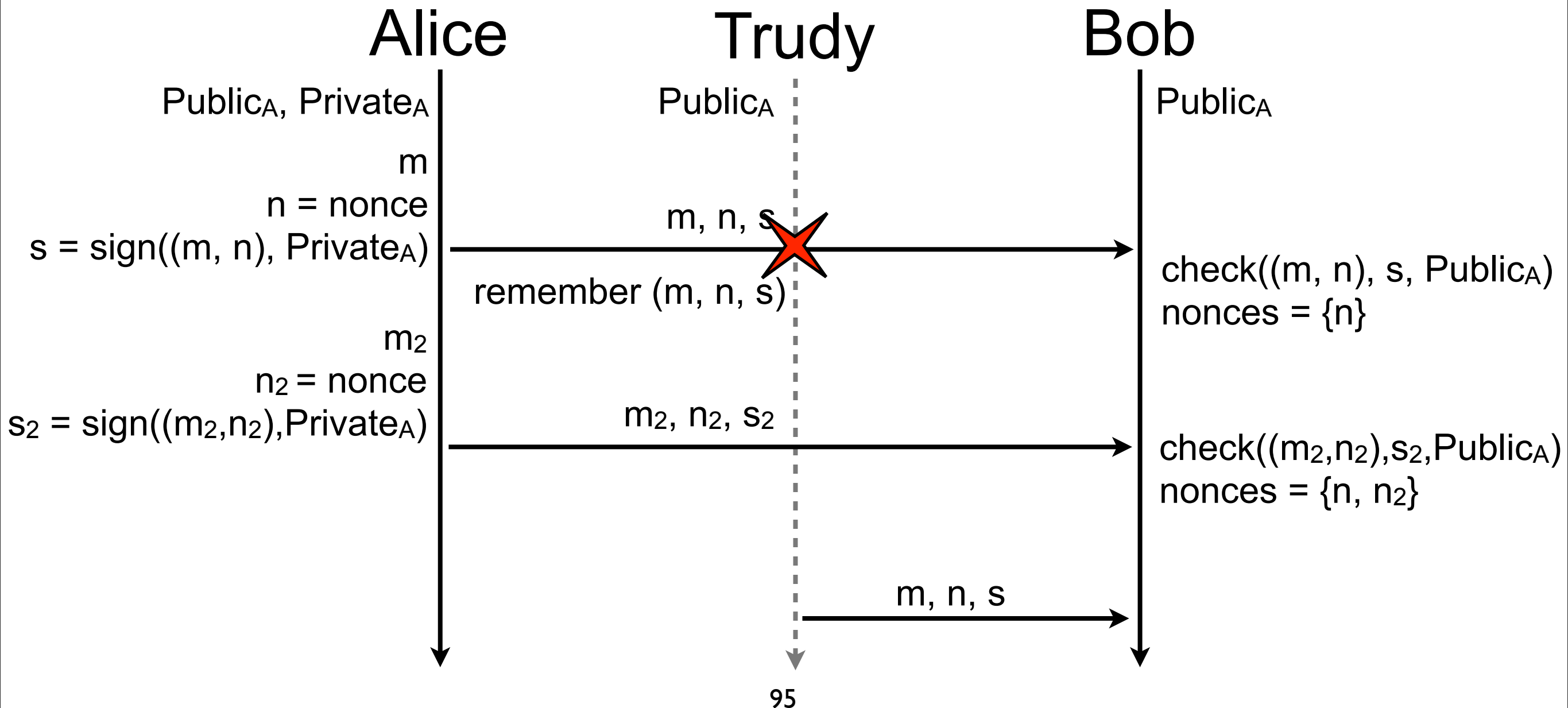
Nonce (contd.)

- Each message is made unique thanks to the nonce



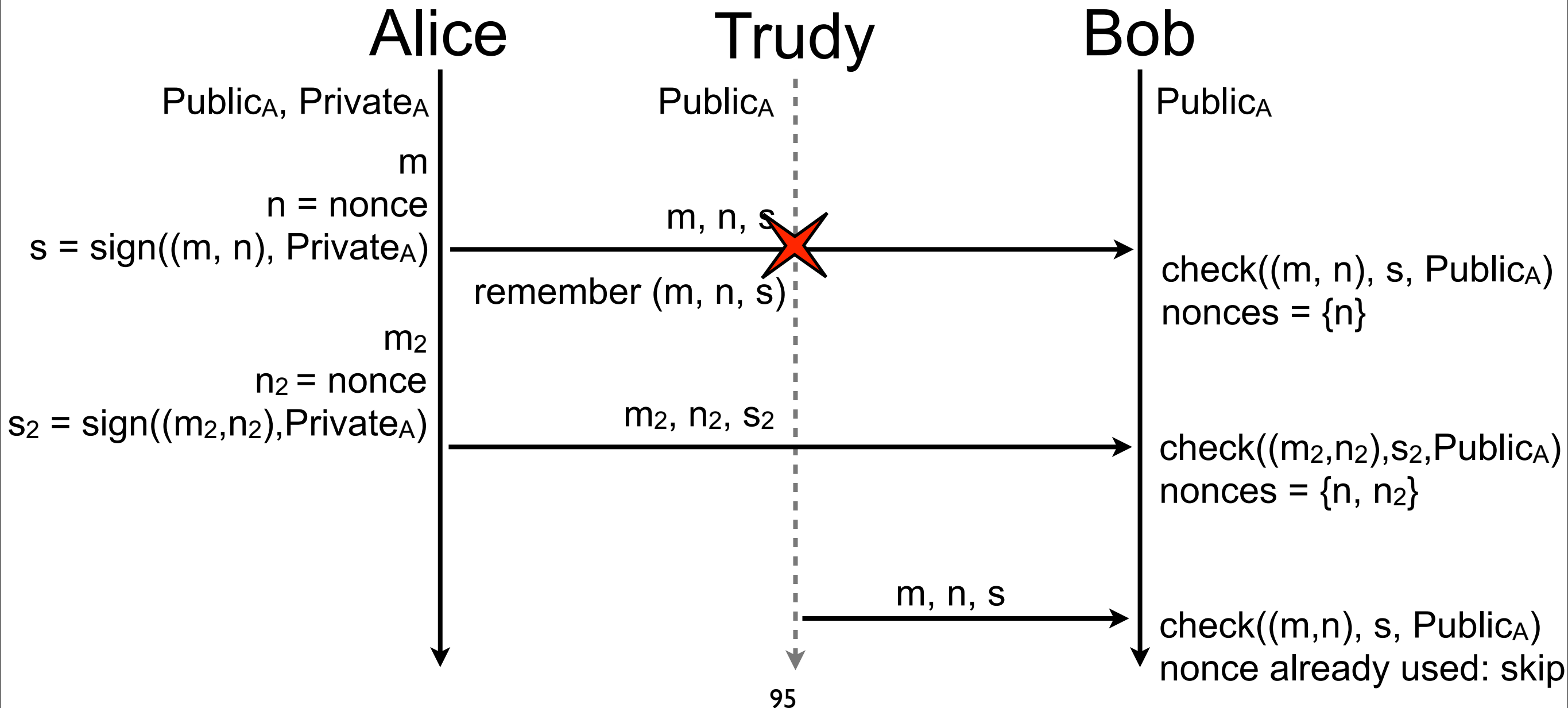
Nonce (contd.)

- Each message is made unique thanks to the nonce



Nonce (contd.)

- Each message is made unique thanks to the nonce



Nonce (contd.)

- TCP sequence number does not protect against segment injection attacks in TCP

Alice



Bob

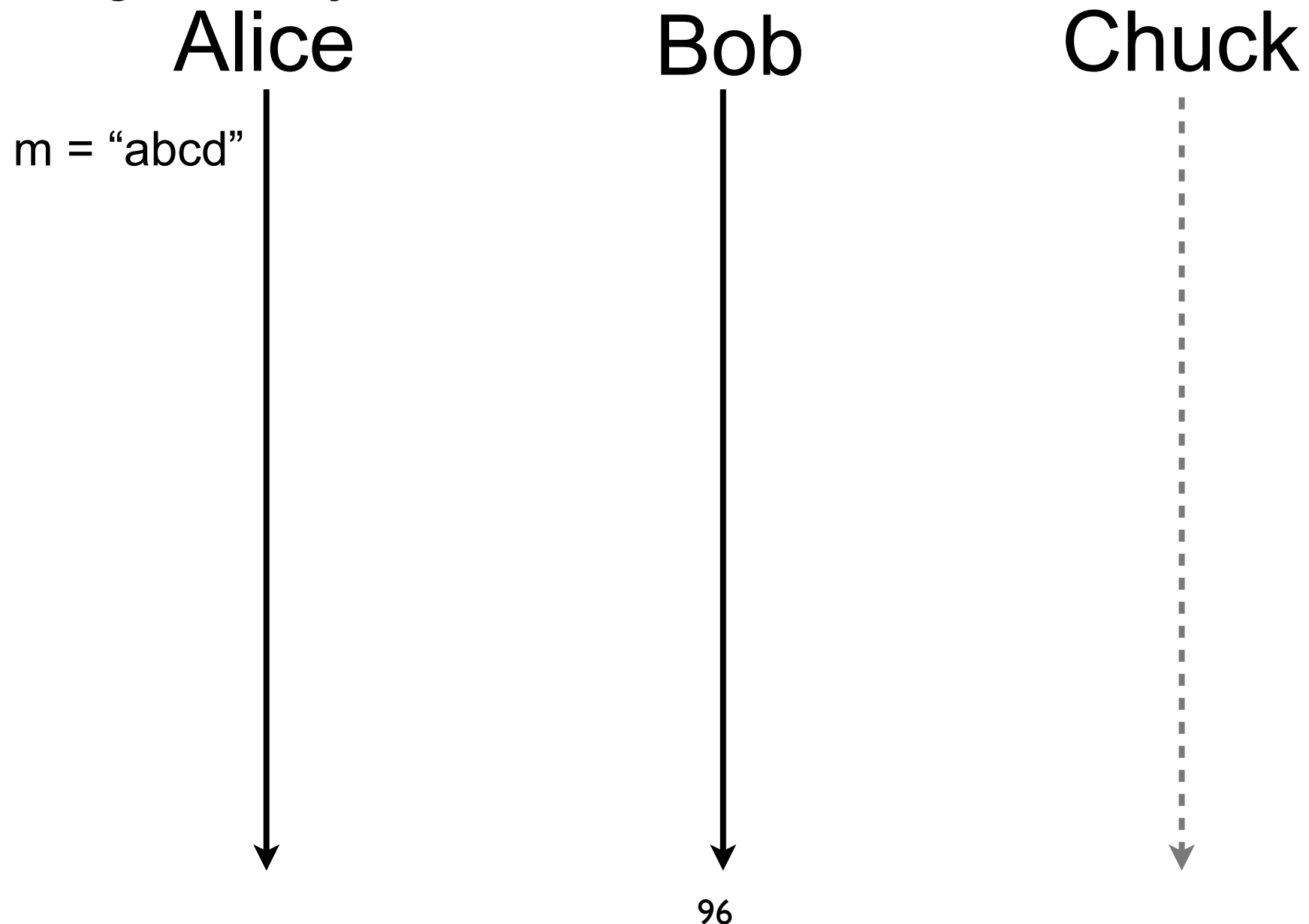


Chuck



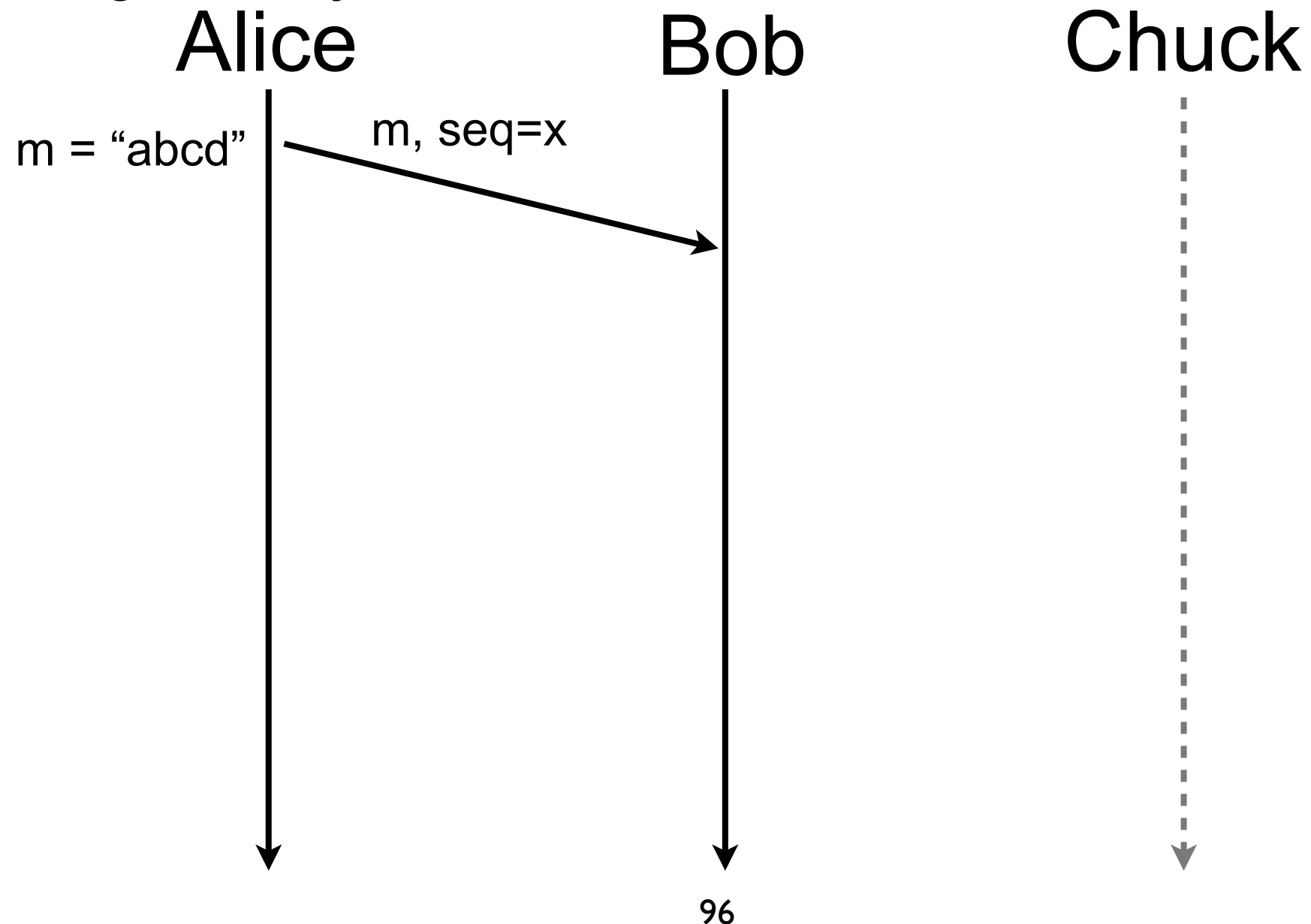
Nonce (contd.)

- TCP sequence number does not protect against segment injection attacks in TCP



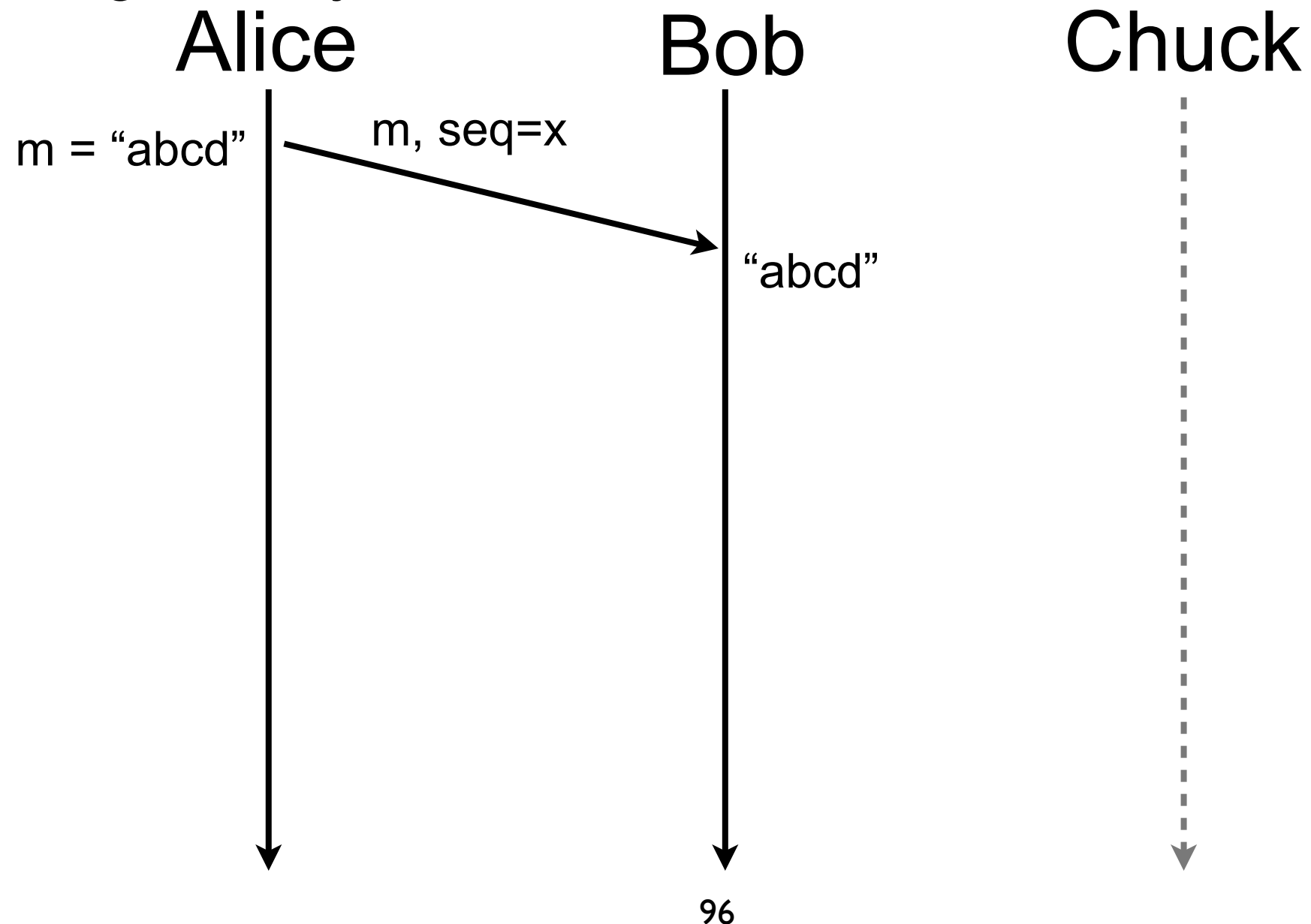
Nonce (contd.)

- TCP sequence number does not protect against segment injection attacks in TCP



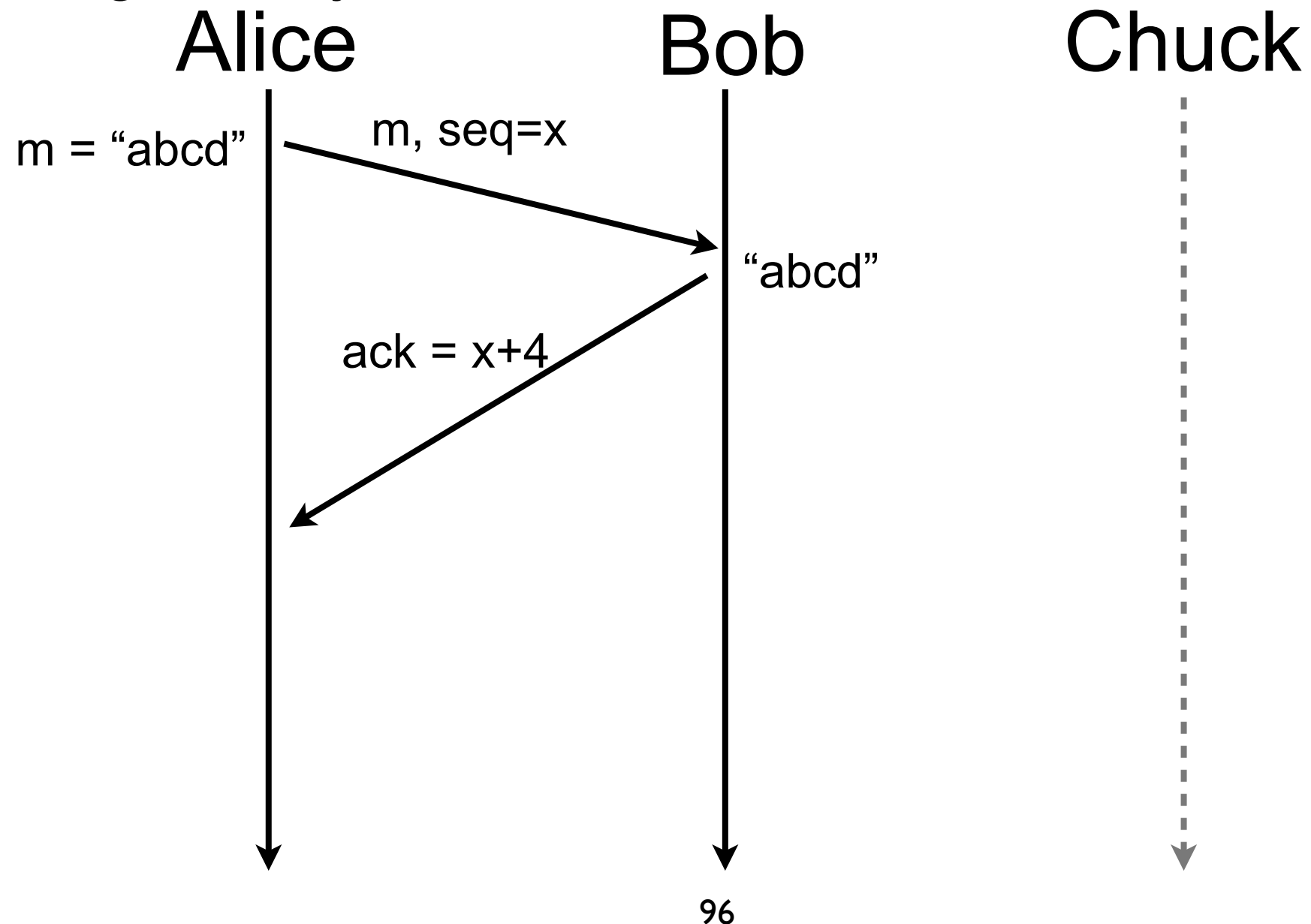
Nonce (contd.)

- TCP sequence number does not protect against segment injection attacks in TCP



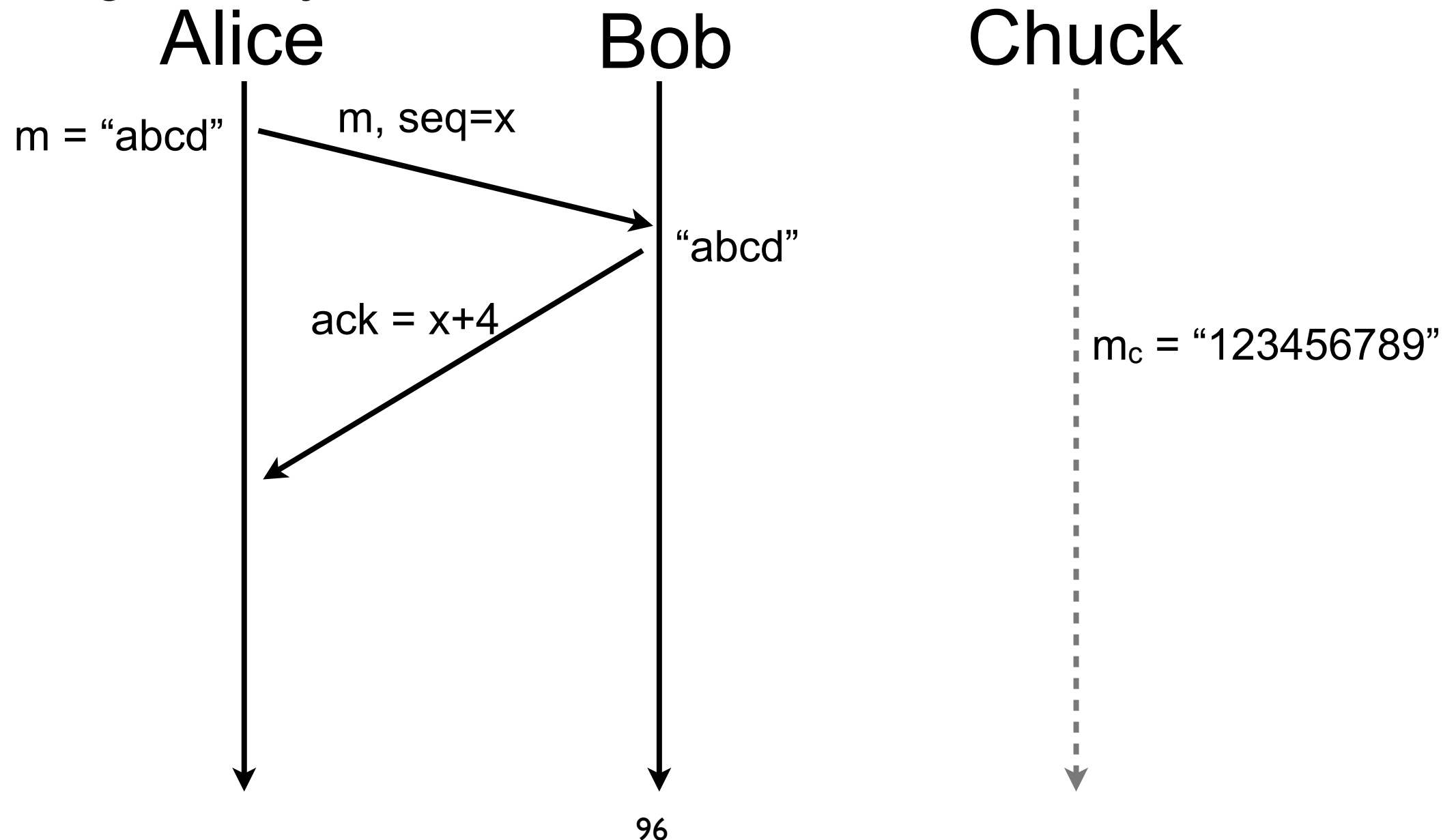
Nonce (contd.)

- TCP sequence number does not protect against segment injection attacks in TCP



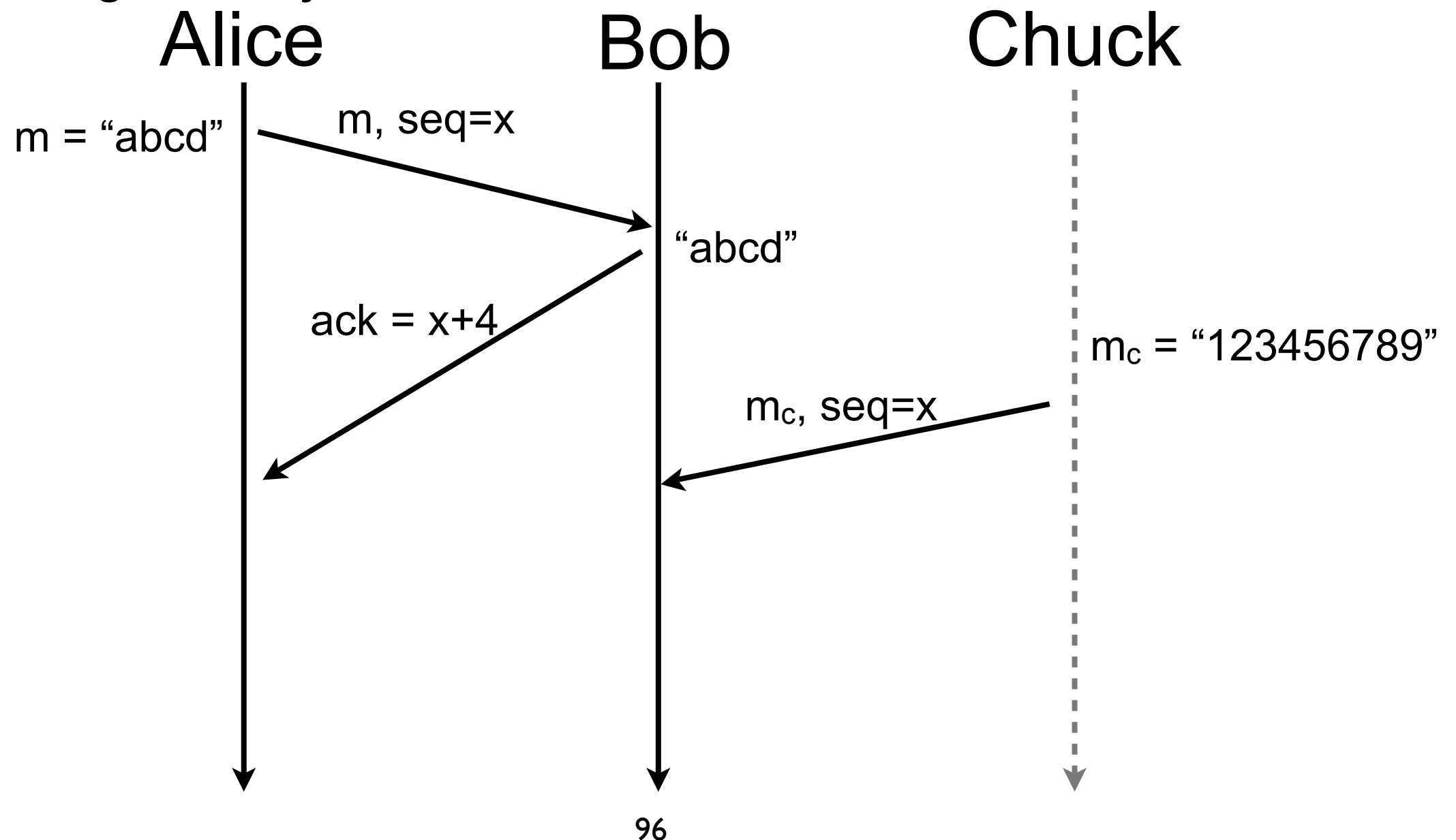
Nonce (contd.)

- TCP sequence number does not protect against segment injection attacks in TCP



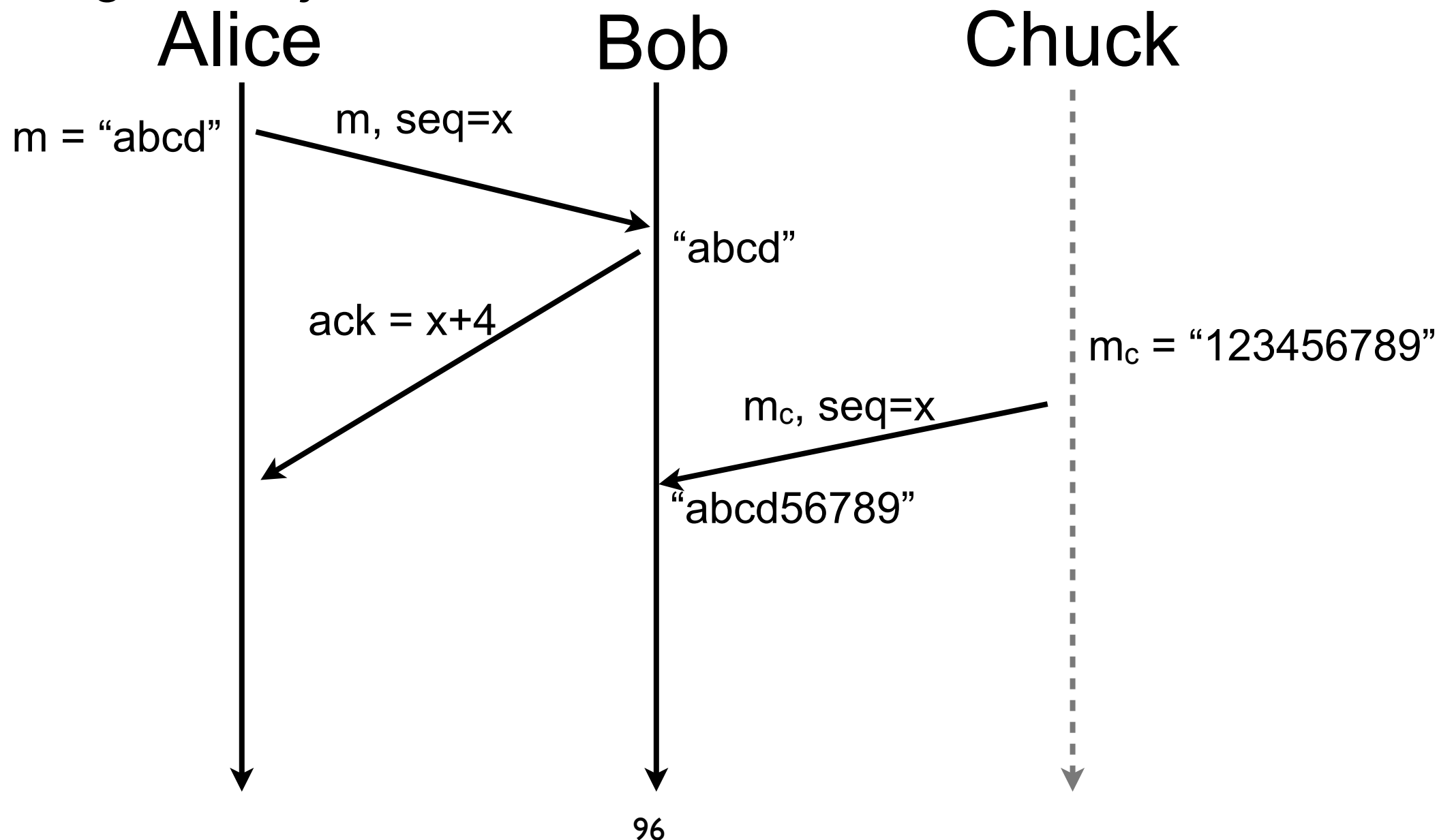
Nonce (contd.)

- TCP sequence number does not protect against segment injection attacks in TCP



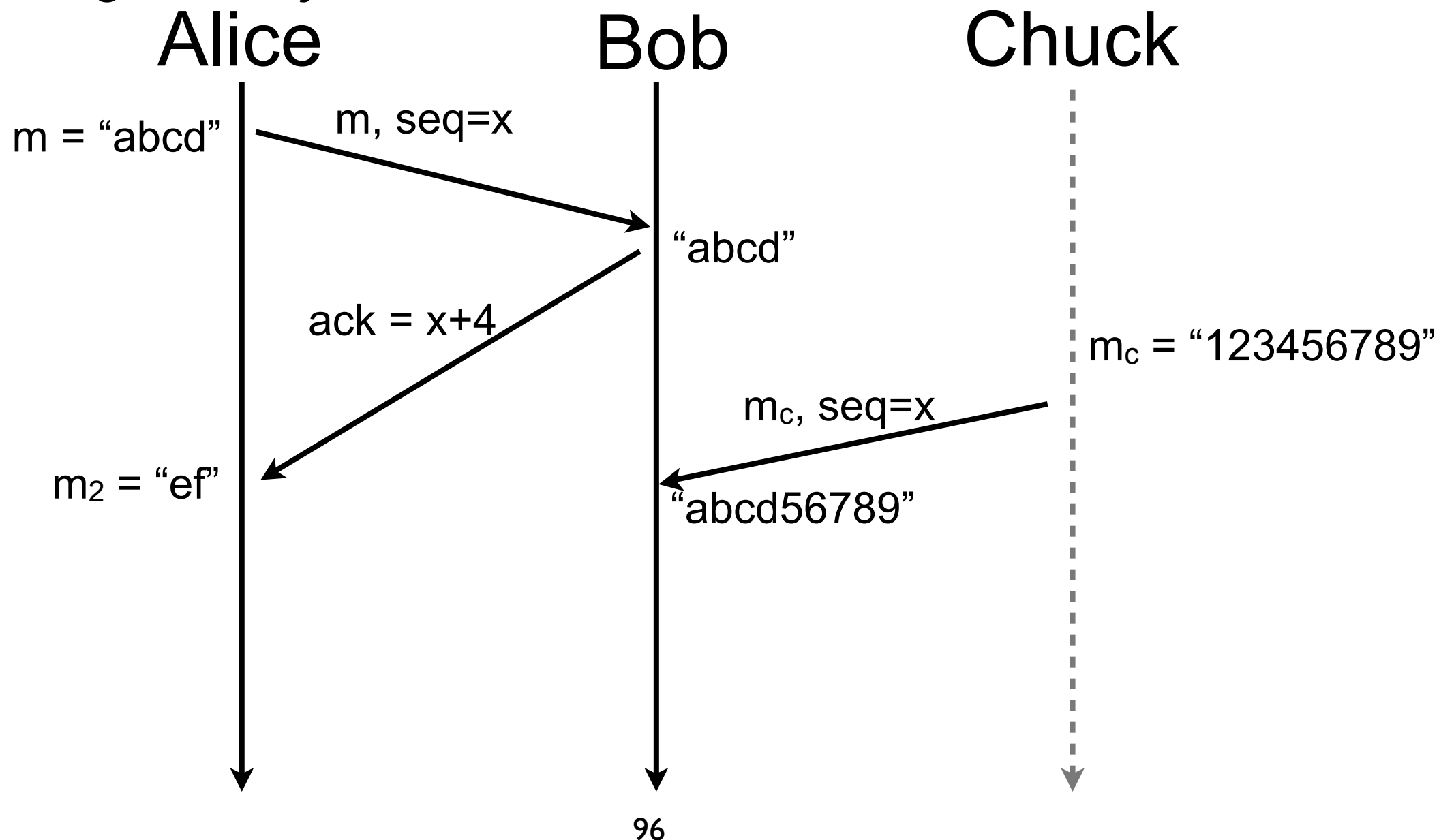
Nonce (contd.)

- TCP sequence number does not protect against segment injection attacks in TCP



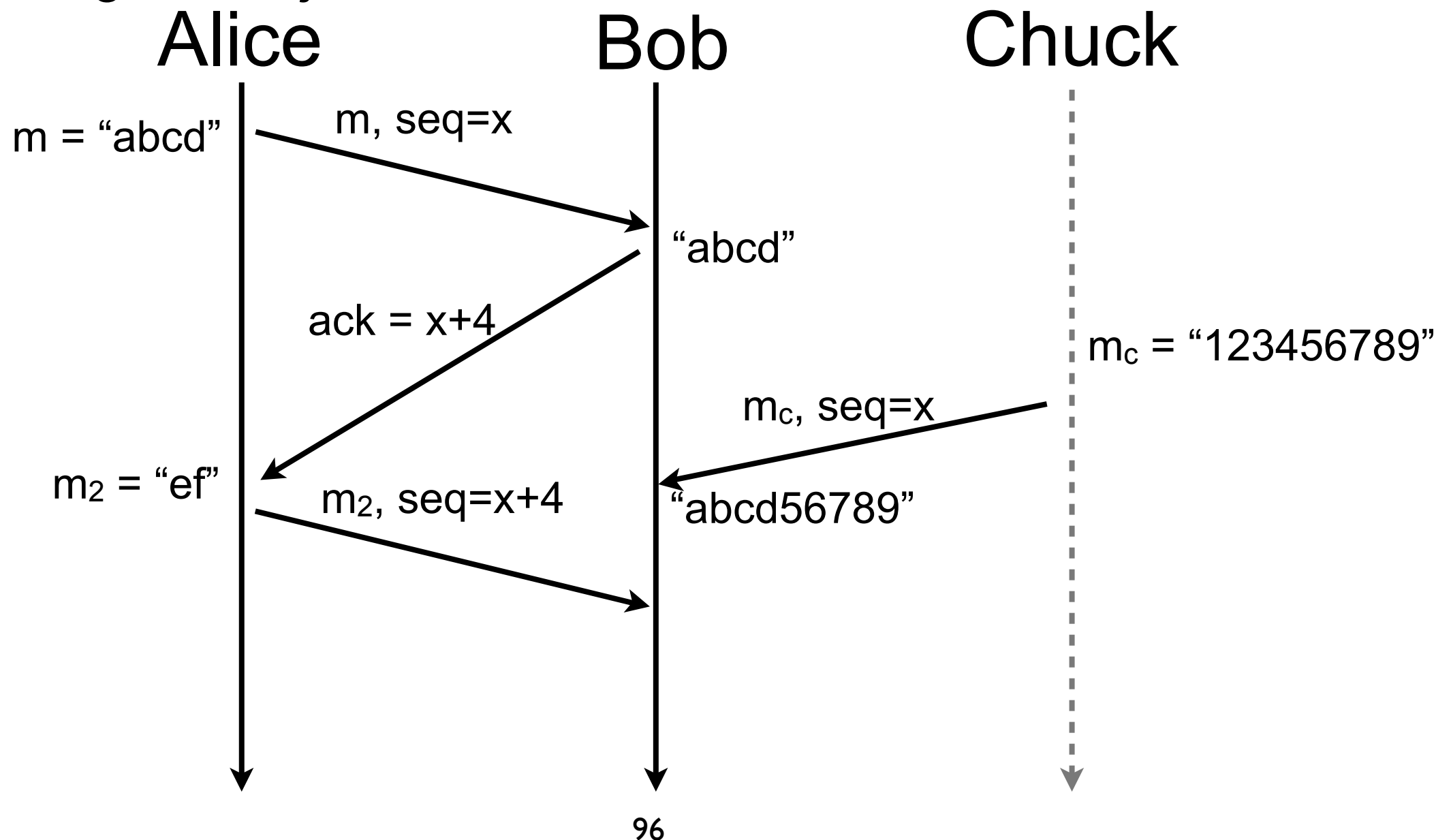
Nonce (contd.)

- TCP sequence number does not protect against segment injection attacks in TCP



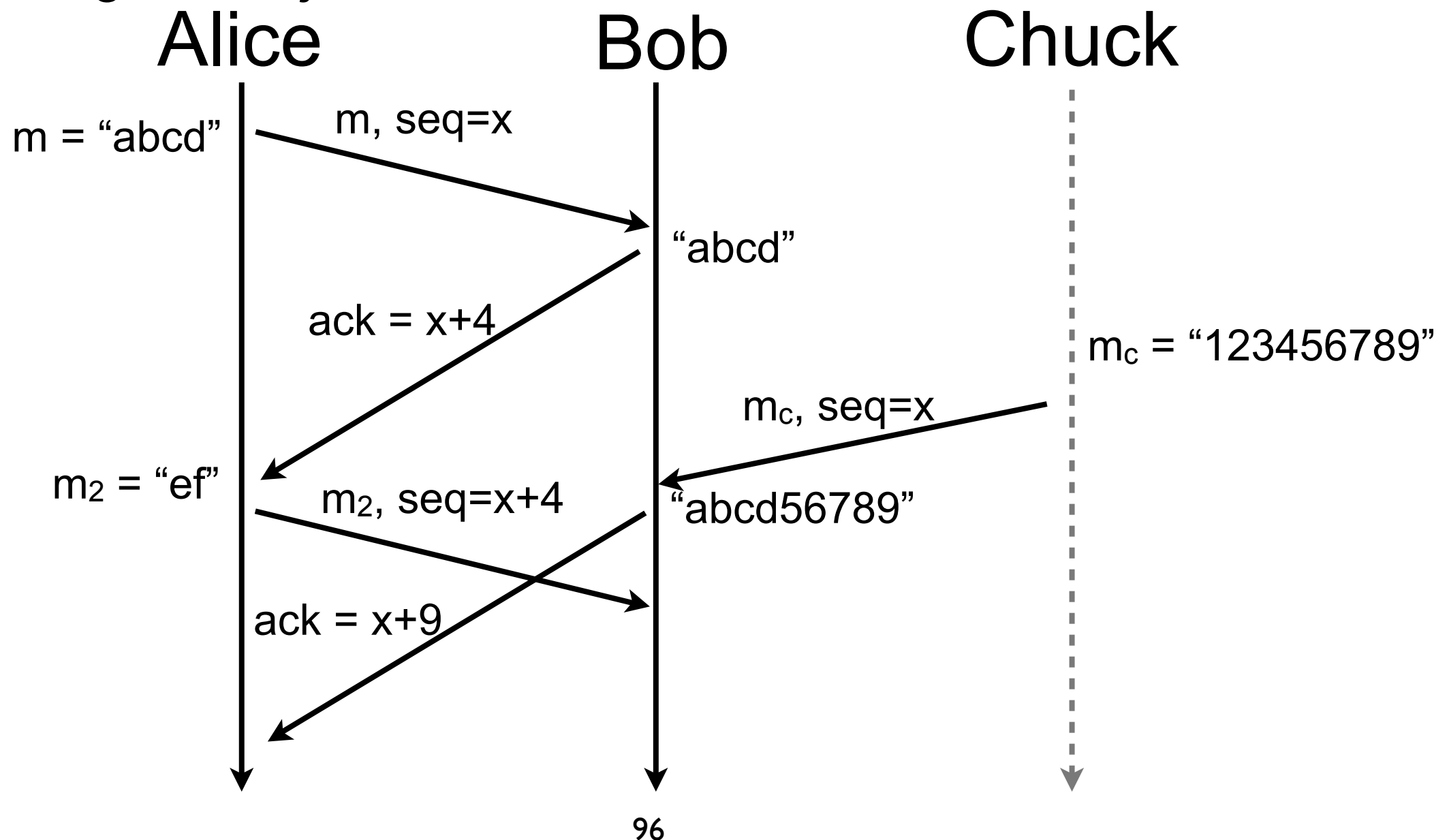
Nonce (contd.)

- TCP sequence number does not protect against segment injection attacks in TCP



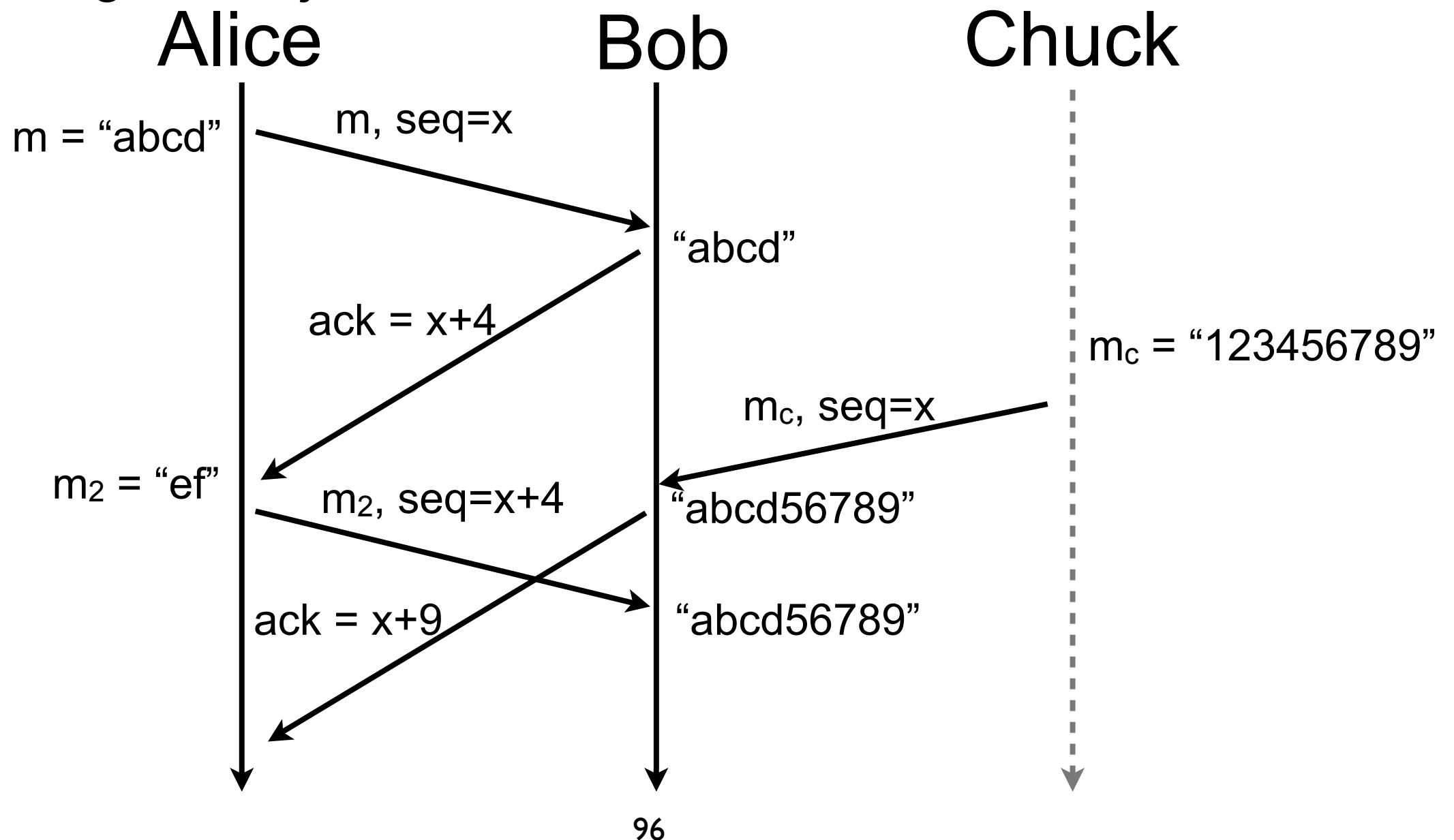
Nonce (contd.)

- TCP sequence number does not protect against segment injection attacks in TCP



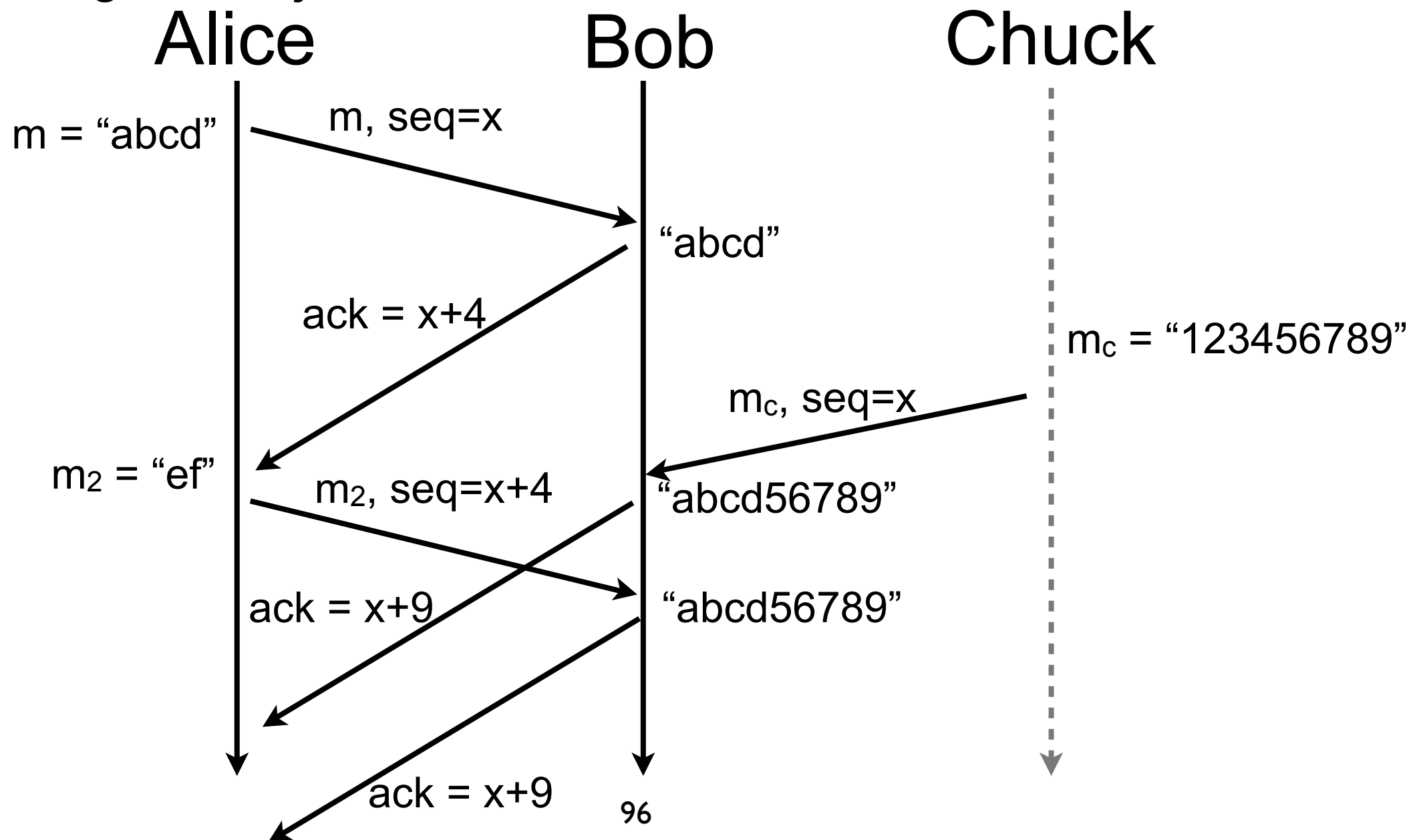
Nonce (contd.)

- TCP sequence number does not protect against segment injection attacks in TCP



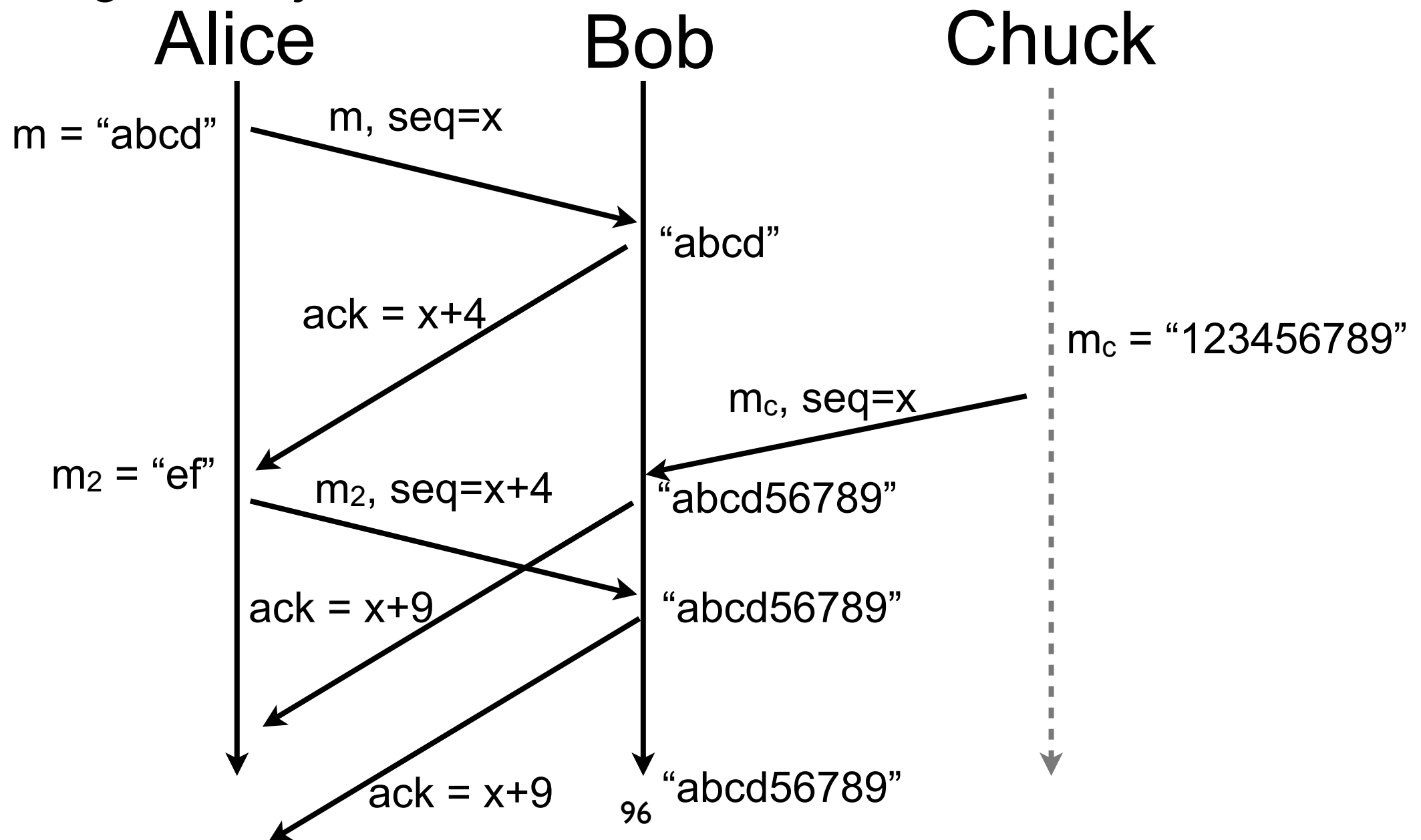
Nonce (contd.)

- TCP sequence number does not protect against segment injection attacks in TCP



Nonce (contd.)

- TCP sequence number does not protect against segment injection attacks in TCP



Nonce (contd.)

- TCP segment injection attack can be mitigated for short connections when there is not eavesdropping by
 - setting the initial sequence number with a good nonce, but sequence number is short (32 bits)
 - only allowing reception of segments that fit in the window
 - keeping small enough window (attackers can try a lot of sequence numbers on 1Gbps links!)
- In case of eavesdropping or long connections, segments should be authenticated
 - TCP MD5 option [RFC2385] tags every segment with its MD5 hash (without options and checksum) and a secret shared between Alice and Bob

Problem solved?

- fill me
- fill me
- fill me

Problem solved?

- fill me
- fill me
- fill me

DoS attacks are still possible!

Denial of Services

- Resources are always limited
 - e.g., processor, memory, link capacity
- The easiest way of leading a DoS is to overwhelm CPUs, memory, or links of the target
- A more complicated way is to manage an intrusion and neutralize the target
 - imagine you gain administrative access to border router of your network!

Danger of state

- Establishment and maintenance of session requires state
 - often maintained in “tables” with predefined capacity
- An attacker can saturate state tables by initiating multiple sessions
- Principle
 - require attacker to maintain state before maintaining state yourself
 - in general it is too costly for an attacker to maintain state

Danger of state (contd.)

- TCP relied on a state machine started upon reception of a SYN packet

Alice



Bob



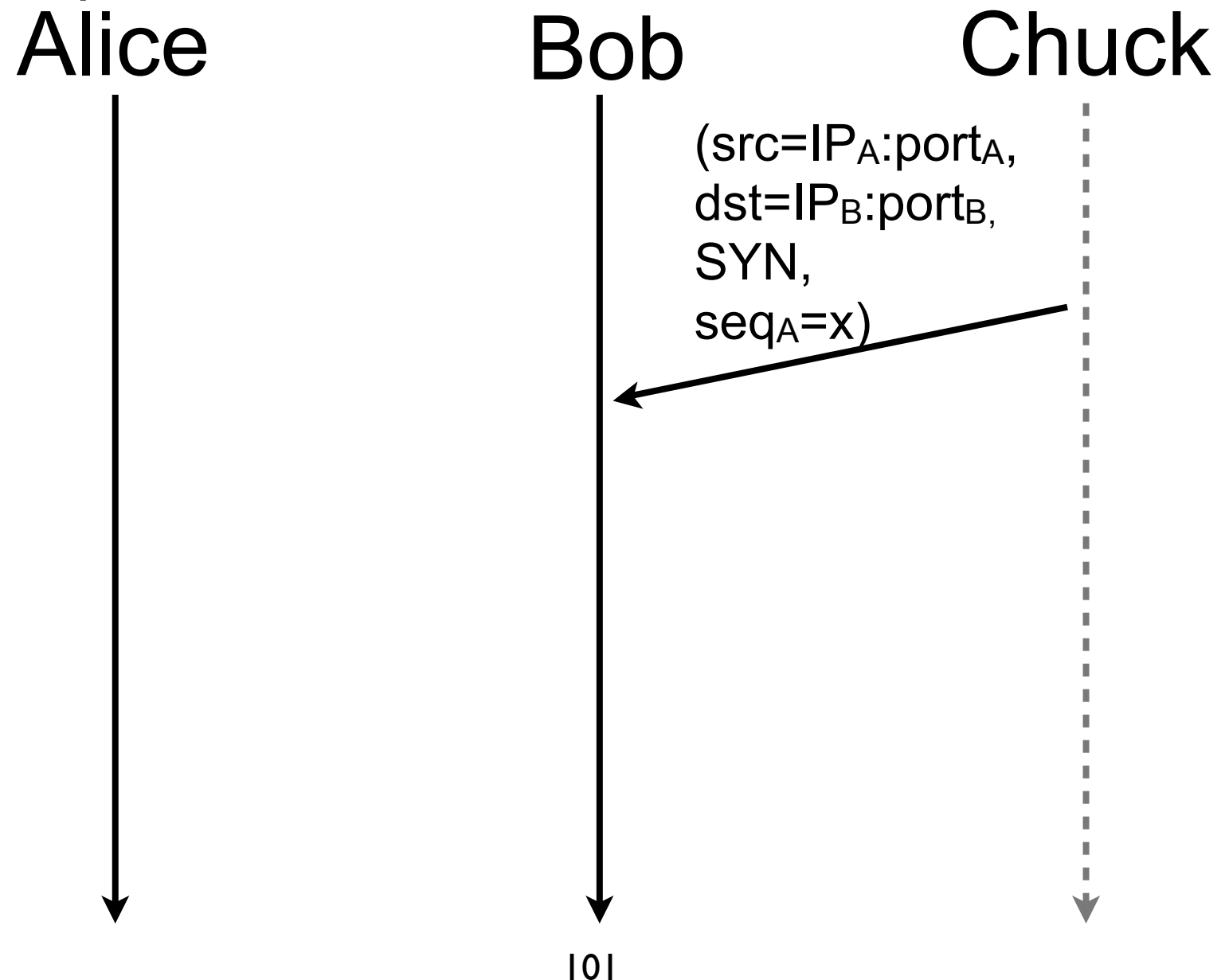
101

Chuck



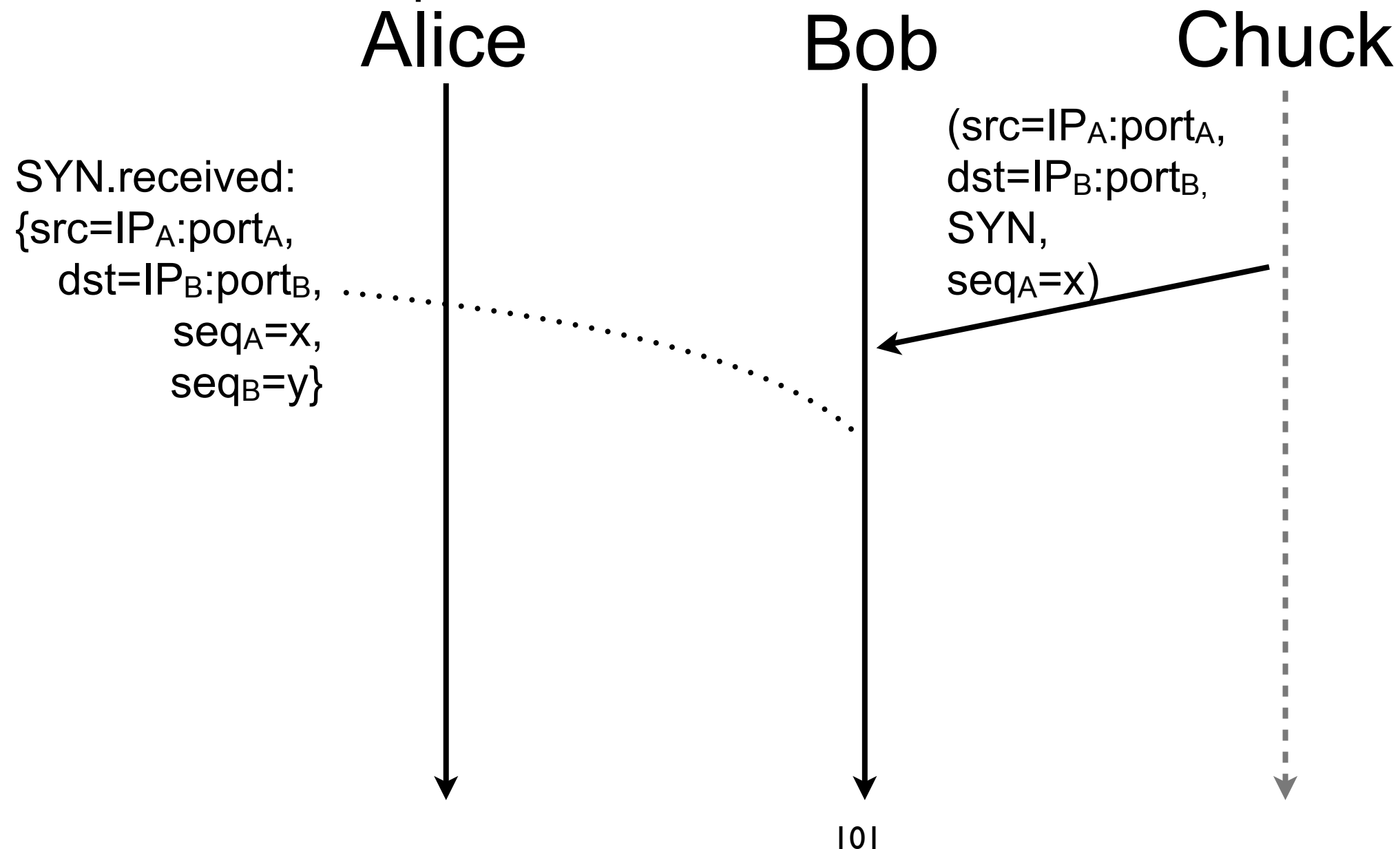
Danger of state (contd.)

- TCP relied on a state machine started upon reception of a SYN packet



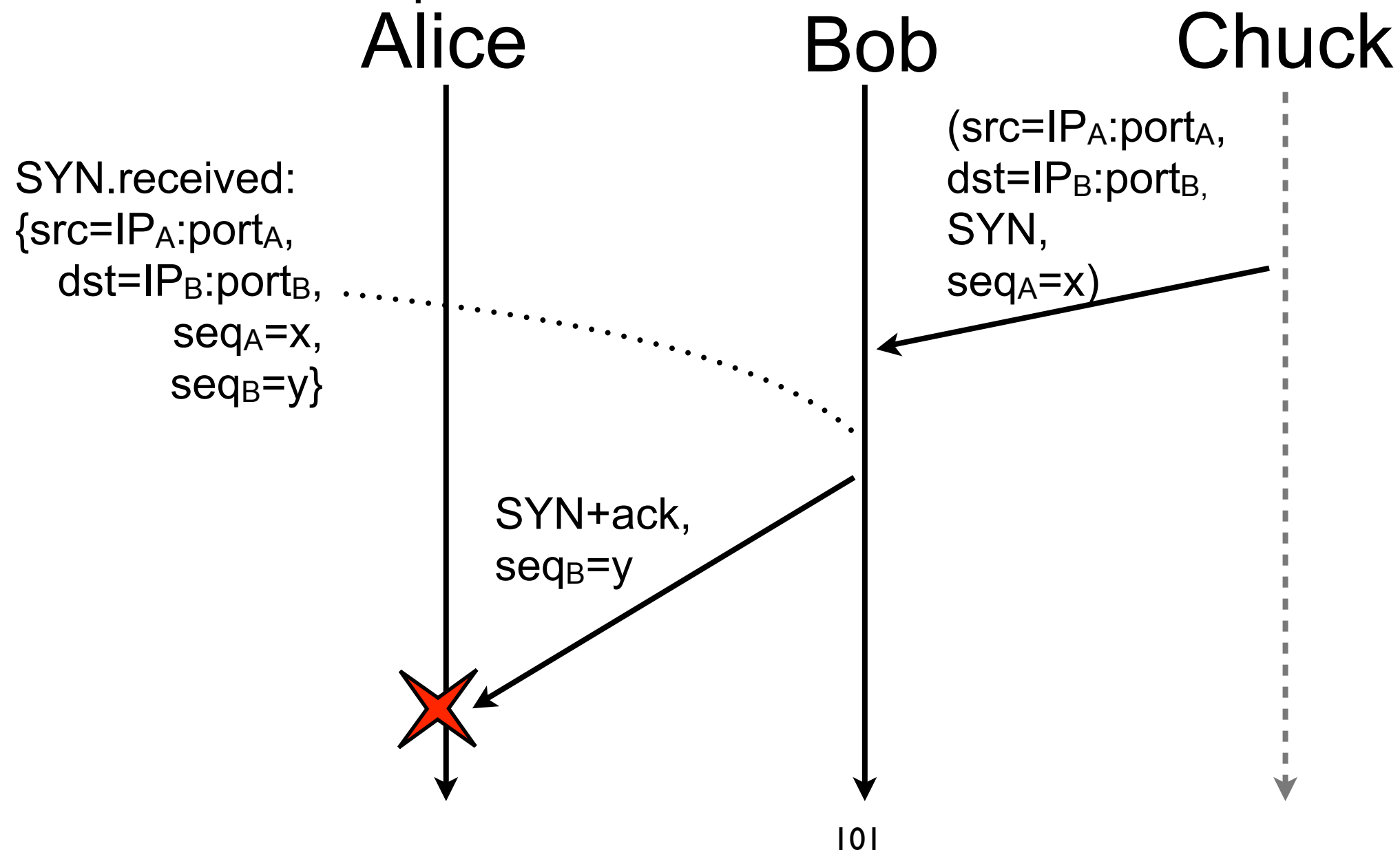
Danger of state (contd.)

- TCP relied on a state machine started upon reception of a SYN packet



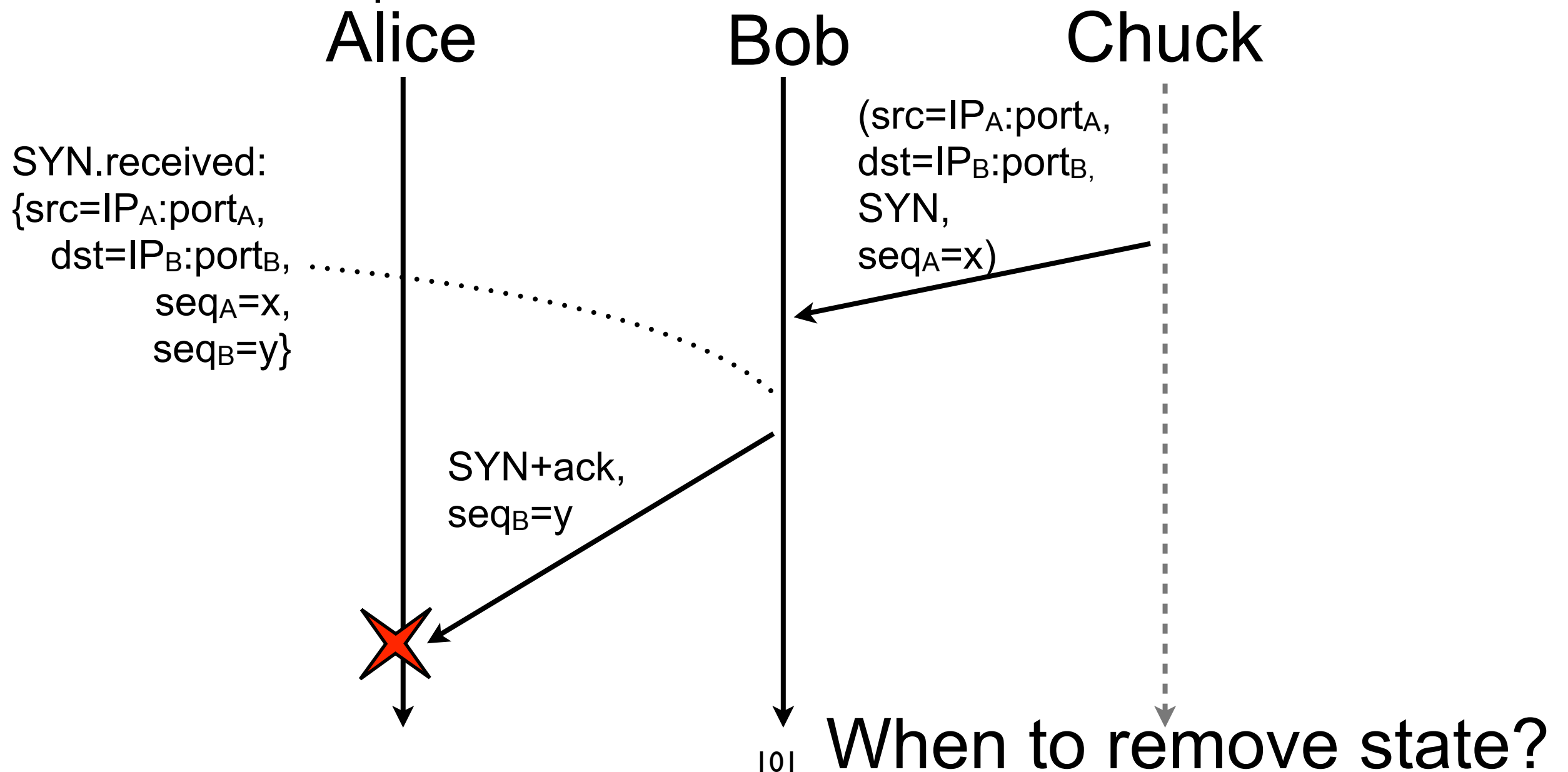
Danger of state (contd.)

- TCP relied on a state machine started upon reception of a SYN packet



Danger of state (contd.)

- TCP relied on a state machine started upon reception of a SYN packet



Danger of state (contd.)

- Always create state at the end of session establishment (e.g., TCP SYN cookie)

Alice



Bob

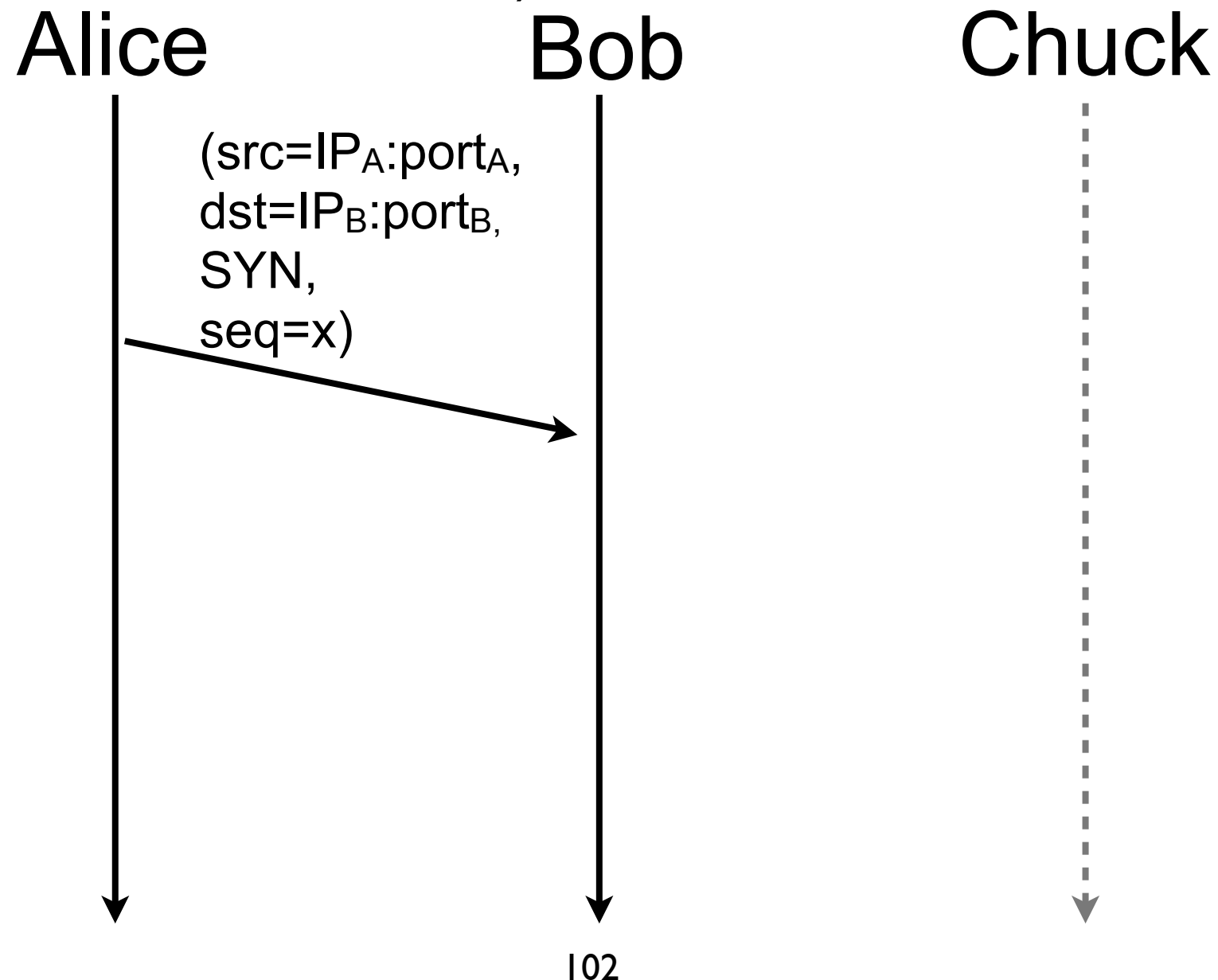


Chuck



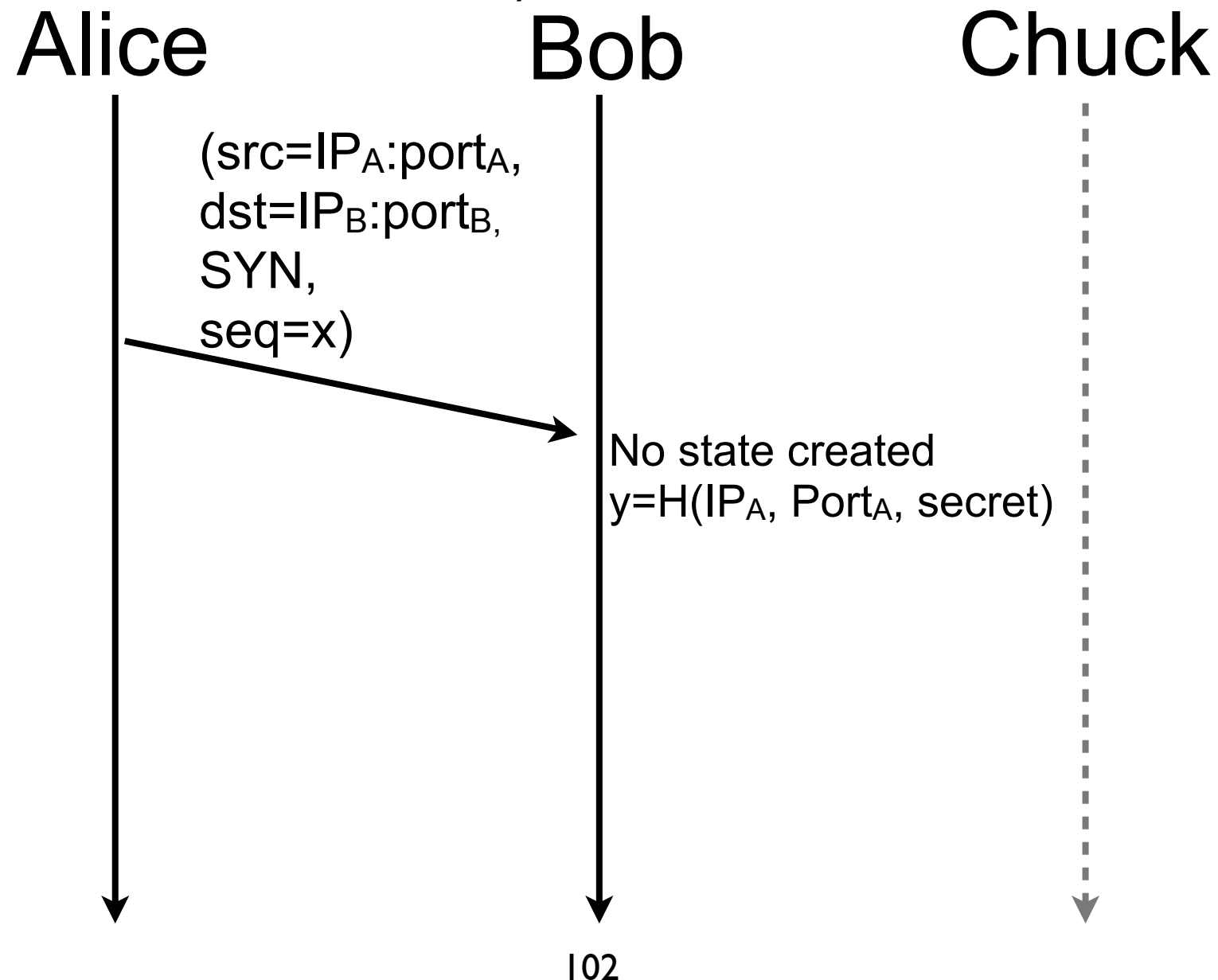
Danger of state (contd.)

- Always create state at the end of session establishment (e.g., TCP SYN cookie)



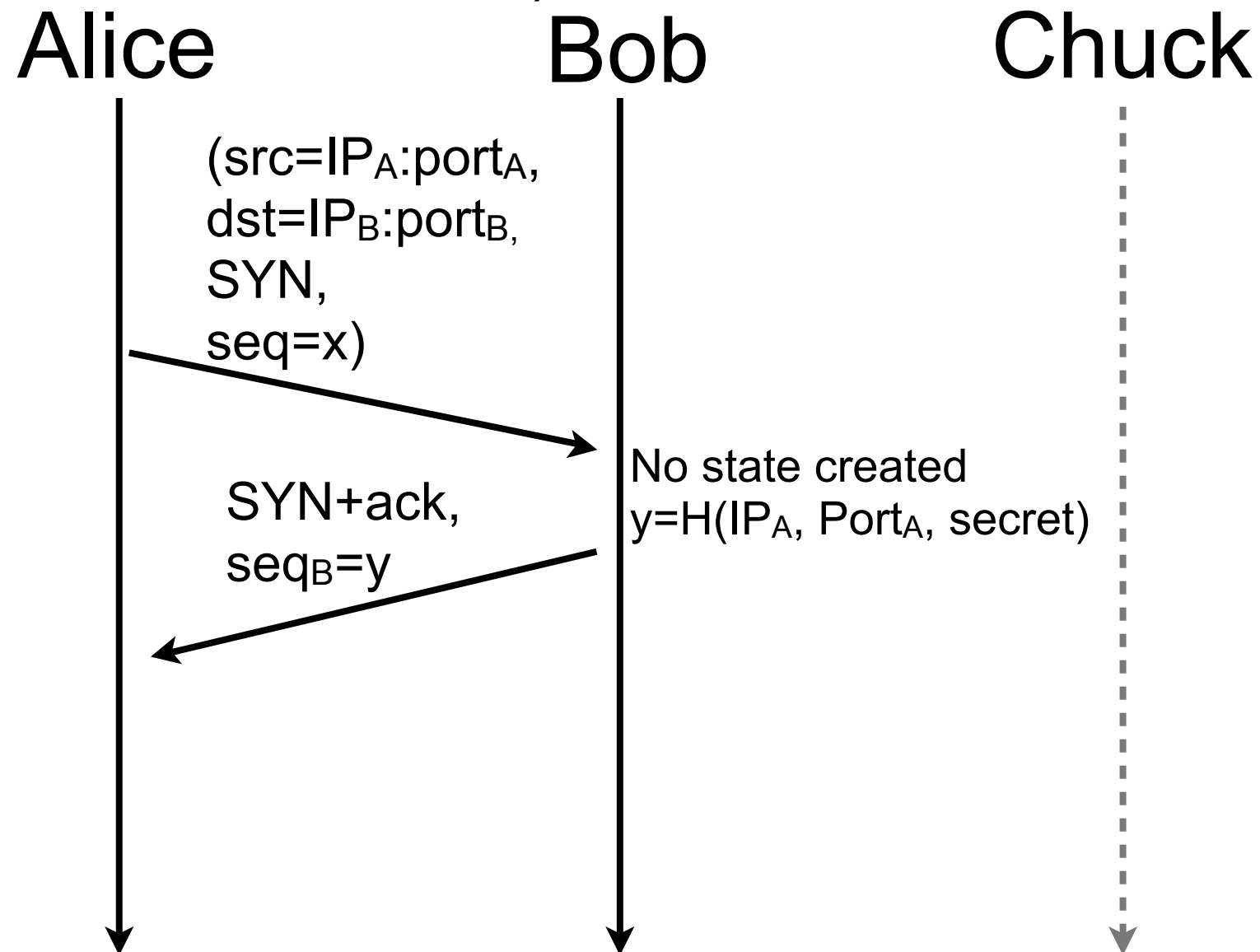
Danger of state (contd.)

- Always create state at the end of session establishment (e.g., TCP SYN cookie)



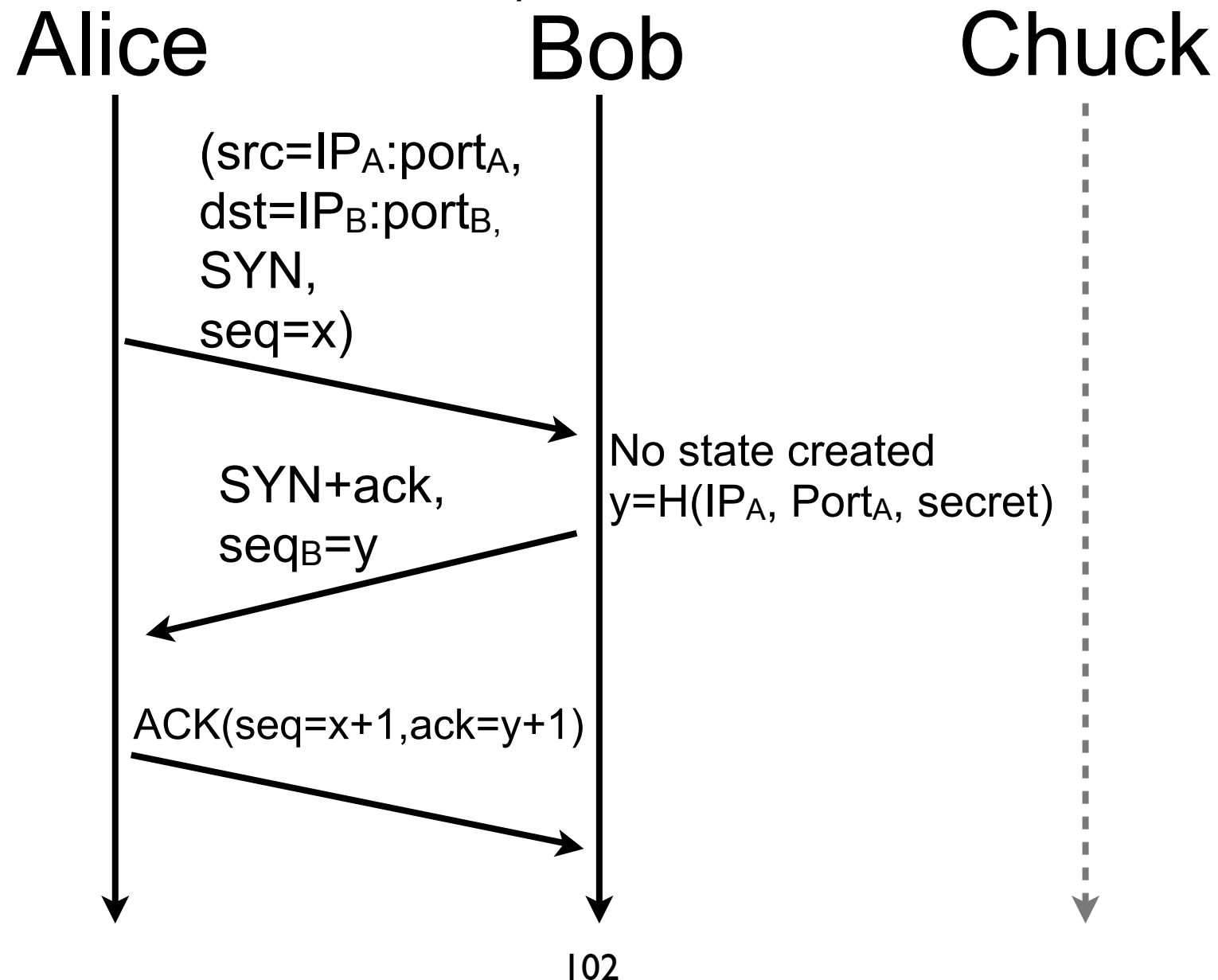
Danger of state (contd.)

- Always create state at the end of session establishment (e.g., TCP SYN cookie)



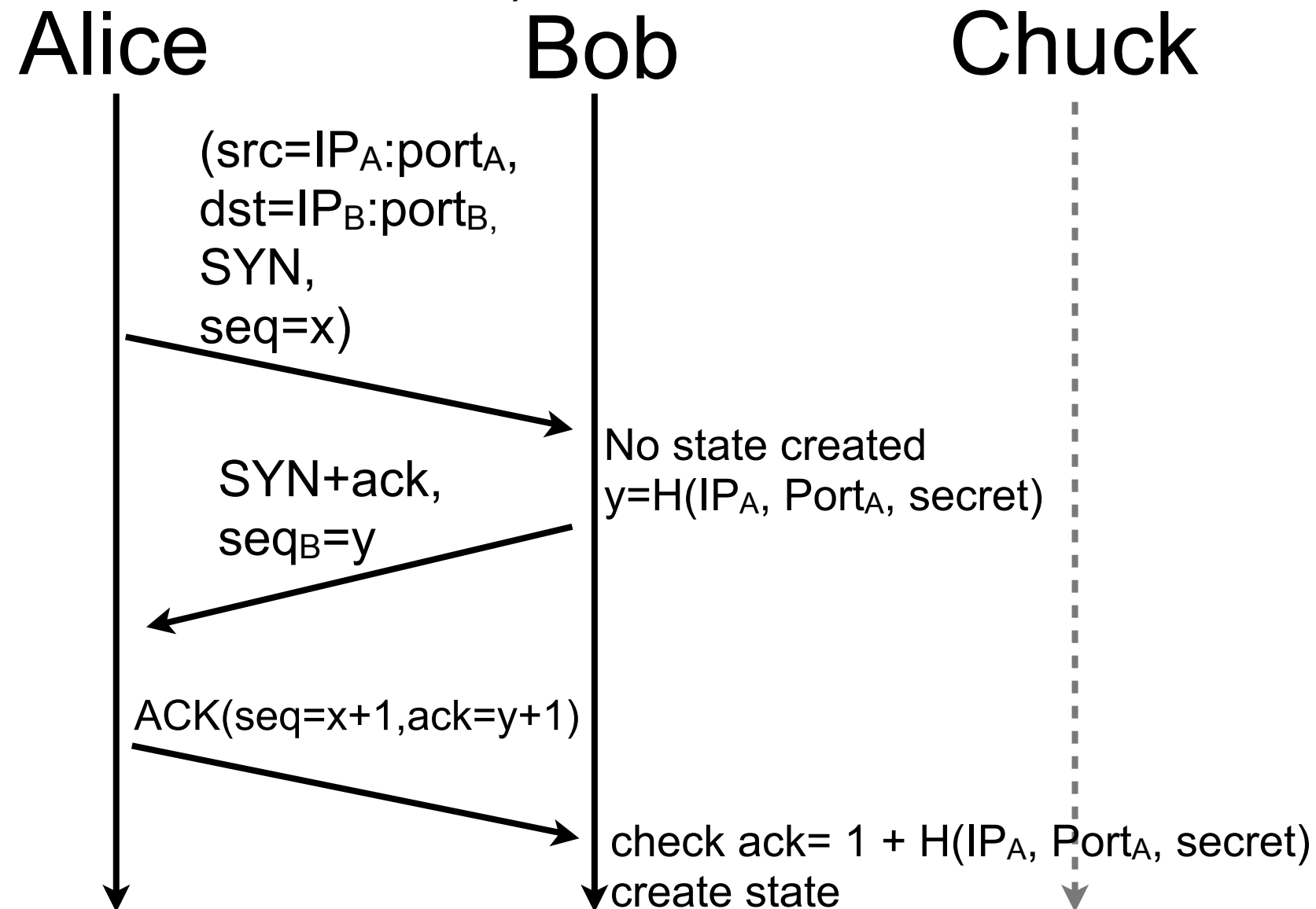
Danger of state (contd.)

- Always create state at the end of session establishment (e.g., TCP SYN cookie)



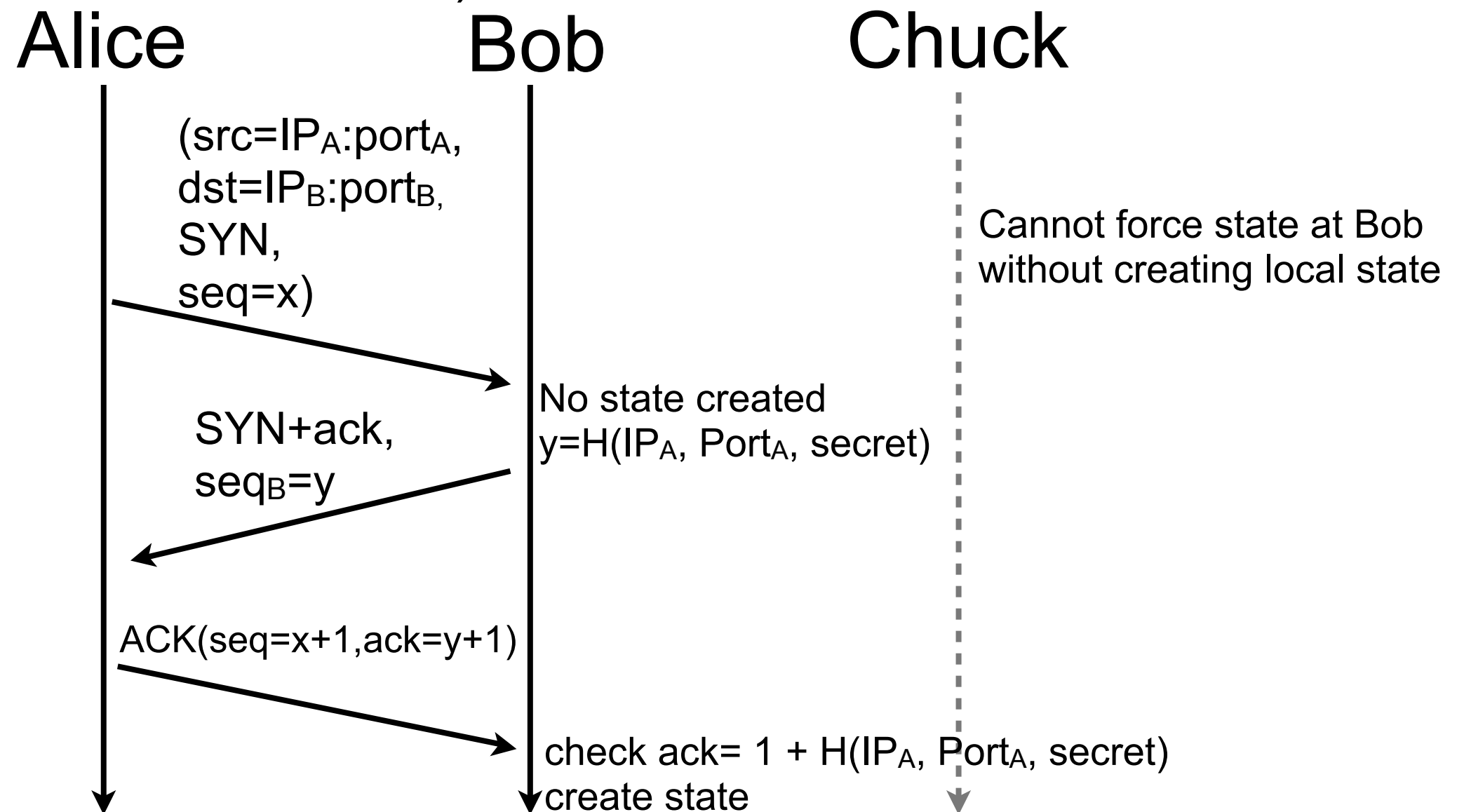
Danger of state (contd.)

- Always create state at the end of session establishment (e.g., TCP SYN cookie)



Danger of state (contd.)

- Always create state at the end of session establishment (e.g., TCP SYN cookie)



Danger of complexity

- Protection mechanism can be complex and can require important processing power
- An attacker can overwhelm her target CPU by triggering protection mechanisms
- Principle
 - require attacker to perform more processing than yourself
 - in general an attacker does not want to have to do heavy computation

Danger of complexity (contd.)

- Hard, if not impossible, to remove processing requirements but still possible to force the attacker to succeed some challenges to get access. This technique is usually called challenge-response
 - time challenges
 - when an attack is suspected, force the attacker to wait or slow down but the DoS protection can lead to a DoS
 - e.g., rate limiting
 - mathematical challenges
 - ask the initiator to solve a mathematical challenge that is hard to compute but easy to check, this might negatively impact legitimate clients
 - e.g., Bob asks Alice to find a J such that the K lowest order bits of $H((N,J))$ are zeros. N is a nonce and K sets the complexity of the puzzle, both parameters are decided by Bob [RFC5201]
 - human processing challenge
 - some services are reserved for users and don't want to be accessed by bots
 - ask Alice to succeed a challenge that is simple for a human but hard for a computer
 - e.g., CAPTCHA

Danger of complexity (contd.)

- Hard, if not impossible, to remove processing requirements but still possible to force the attacker to succeed some challenges to get access. This technique is usually called challenge-response
 - time challenges
 - when an attack is suspected, force the attacker to wait or slow down but the DoS protection can lead to a DoS
 - e.g., rate limiting
 - mathematical challenges
 - ask the initiator to solve a mathematical challenge that is hard to compute but easy to check, this might negatively impact legitimate clients
 - e.g., Bob asks Alice to find a J such that the K lowest order bits of $H((N,J))$ are zeros. N is a nonce and K sets the complexity of the puzzle, both parameters are decided by Bob [RFC5201]
 - human processing challenge
 - some services are reserved for users and don't want to be accessed by bots
 - ask Alice to succeed a challenge that is simple for a human but hard for a computer
 - e.g., CAPTCHA

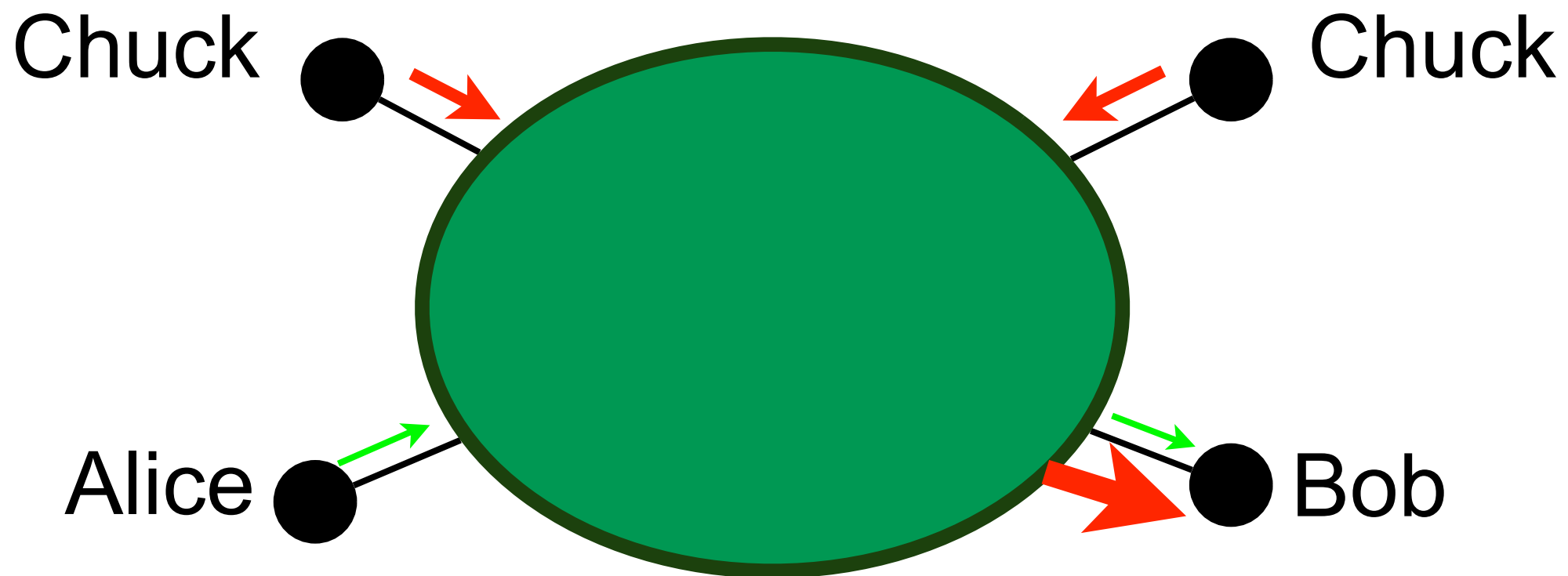


Link overloading

- Messages are sent to Bob by traversing links
- If an attacker can send packets at a high enough rate, she can saturate links toward Bob and make him unavailable
- Unfortunately, Bob cannot make anything to block packet before they reach him
- Principle
 - tweak the network to not suffer too much of such attacks

Link overloading (contd.)

- Example of Distributed Denial of Service (DDoS) attack



Link overloading (contd.)

- A first parade is to filter illicit traffic before it can harm the target
 - e.g., firewall, access lists
- A set of rules is specified a priori, if the traffic does not match the rules, it is discarded
 - always block everything but what is acceptable

Link overloading (contd.)

- Filtering based on origin
 - useful to avoid spoofing
 - e.g., block any packet which source address does not belong to the customer cone of a BGP neighbor
 - does not work so well as it depends on every network between the origin and the target
- Filtering based on traffic pattern
 - analyze the traffic and if it deviates from what is normal, drop it
 - e.g., drop malformed packets, rate limit a source if it sends too much SYN packets, ignore mails from well known SPAM servers, block any flow initiated by the outside if there is no server in the network

Network Intrusion Detection System (NIDS)

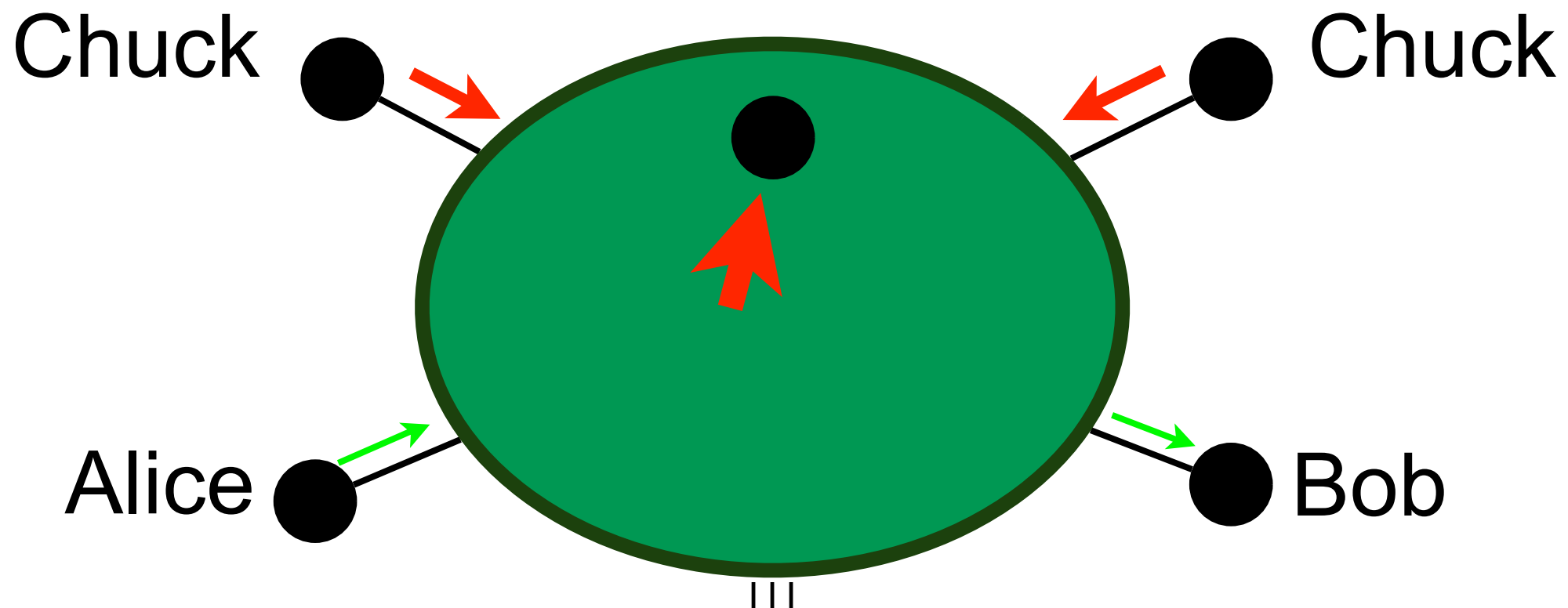
- An NIDS aims at discovering non-legitimate operations
- The NIDS analyses the traffic to detect abnormal patterns
- Upon anomaly detection, the NIDS triggers an alert with a report on the anomaly
- NOC follows procedures upon detection

Network Intrusion Detection System (contd.)

- Signature based detection
 - a database of abnormal behavior is maintained to construct a signature for each attack
 - if the traffic corresponds to a signature in the database, trigger an alarm
 - risk of false negative (0-day attack)
 - e.g., Snort, Bro, antivirus
- Outlier detection
 - the anomaly detector learns what is the normal behavior of the network
 - when an outlier is detected, an alarm is triggered
 - risk of false positive and false negative
 - e.g., cluster analysis, time series analysis, spectral analysis

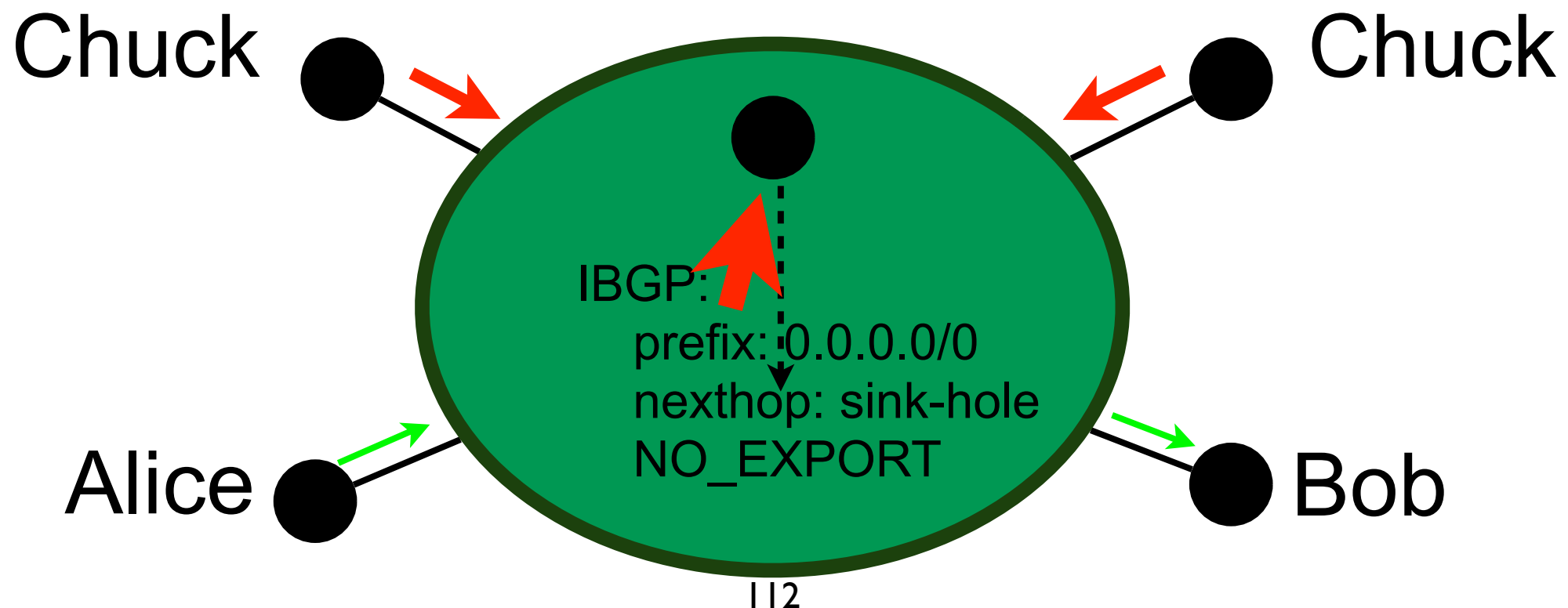
Link overloading (contd.)

- Attacks are often to random destinations or with random sources
- backscatter traffic to a sink-hole that can receive a lot of traffic attack without impacting the network



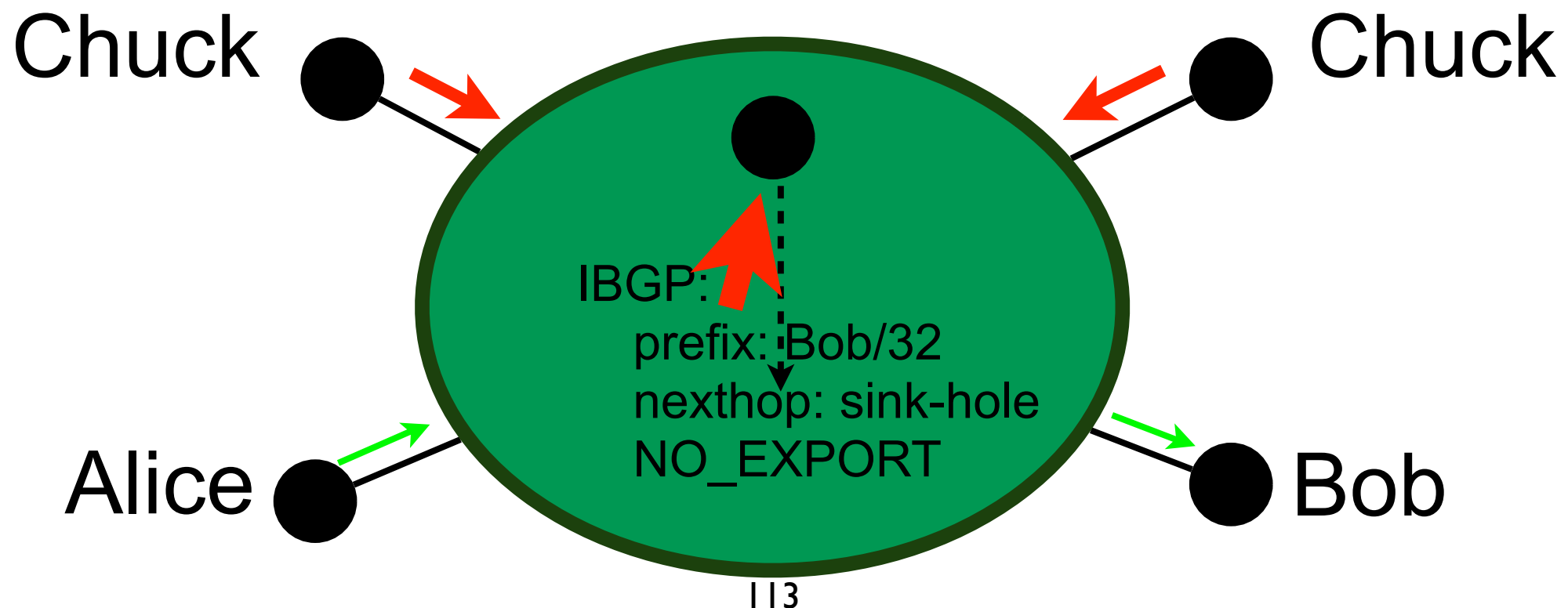
Link overloading (contd.)

- Use the sink-hole to attract bizarre packets



Link overloading (contd.)

- Use the sink-hole to protect the target



Problem solved?

- fill me
- fill me
- fill me

Problem solved?

- fill me
- fill me
- fill me

Relay attacks are still possible!

Relay attack

- In a relay attack, Chuck does not contact Alice directly but goes via Bob
- If the traffic from Bob to Alice is bigger than the traffic from Chuck to Bob, the attack is called amplification attack
- As for DoS, hard to protect correctly against relay attacks
 - use filters (e.g., deactivate ICMP)
 - authentication of the source
 - but correct spoofing protection that doesn't open a relay attack door is very hard to deploy in practice as it requires messages in both directions between parties

What did we miss?

What did we miss?

- To terminate the session!
 - with the same care as the opening of the session
 - this is often neglected

Perfect Forward Secrecy

- With perfect forward secrecy (PFS), Eve cannot decrypt messages sent between Alice and Bob
 - even if she captures every message
 - even if she breaks into Alice and Bob after the communication to steal their secrets (e.g., private keys)

Perfect Forward Secrecy (contd.)

- PFS is provided using ephemeral keys
 - the ephemeral key is generated and used only during the session
 - the session key is not stored after the communication
 - the session key is independent of stored information (e.g., good PRNG)
 - for long sessions, change the session key regularly

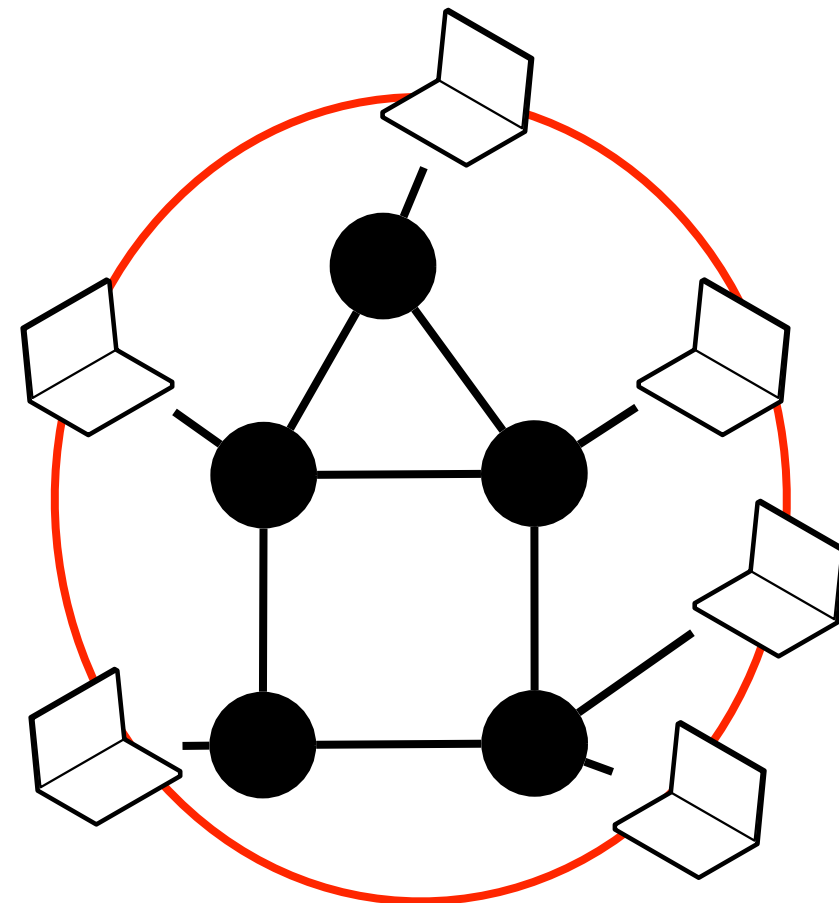
Perfect Forward Secrecy (contd.)

1. Initiate the communication between Alice and Bob
 - authenticity proven with public/private key pairs
2. Alice and Bob agree on a secret K
 - use Diffie-Hellman
 - authenticate DH messages with public/private key pairs
3. Encrypt/Decrypt messages with symmetric cryptography using K as the key
 - no need to sign as it is encrypted
 - be sure a nonce is used to avoid replay
4. If session is too long, back to 2.
5. Close the session correctly and be sure K is not stored anywhere

Overlay networking

Overlay network

- Constructed on top of another network, called the underlay
- Nodes in the overlay appear to be connected independently of the underlay



Definitions

- Peer
 - A node involved in forming the overlay (can be a computer, an end-user, an application...)
- Leecher
 - A peer that is both client and server
- Seed
 - A peer that is only server

Definitions (contd.)

- Peer-to-peer (P2P) application
 - No general definition
 - Specific to an application
 - Every peer is client and server
 - Peers form an overlay network
- In general, we define P2P application as overlay network formed by end-users

P2P

- P2P applications capitalize on any resource from anybody
 - CPU
 - Bandwidth
 - Storage
- In this course, we focus on file sharing (mostly BitTorrent)

P2P is still alive

	Upstream		Downstream		Aggregate	
Rank	Application	Share	Application	Share	Application	Share
1	BitTorrent	36.35%	Netflix	31.62%	Netflix	28.18%
2	HTTP	6.03%	YouTube	18.69%	YouTube	16.78%
3	SSL	5.87%	HTTP	9.74%	HTTP	9.26%
4	Netflix	4.44%	BitTorrent	4.05%	BitTorrent	7.39%
5	YouTube	3.63%	iTunes	3.27%	iTunes	2.91%
6	Skype	2.76%	MPEG - Other	2.60%	SSL	2.54%
7	QVoD	2.55%	SSL	2.05%	MPEG - Other	2.32%
8	Facebook	1.54%	Amazon Video	1.61%	Amazon Video	1.48%
9	FaceTime	1.44%	Facebook	1.31%	Facebook	1.34%
10	Dropbox	1.39%	Hulu	1.29%	Hulu	1.15%
		66.00%		76.23%		73.35%



Table 2 - Top 10 Peak Period Applications - North America, Fixed Access

<https://www.sandvine.com/downloads/general/global-internet-phenomena/2013/2h-2013-global-internet-phenomena-report.pdf>, 02/2014

P2P is still alive

Rank	Upstream		Downstream		Aggregate	
	Application	Share	Application	Share	Application	Share
1	BitTorrent	36.35%	Netflix	31.62%	Netflix	28.18%
2	HTTP	6.03%	YouTube	18.69%	YouTube	16.78%
3	SSL	5.87%	HTTP	9.74%	HTTP	9.26%
4	Netflix	4.44%	BitTorrent	4.05%	BitTorrent	7.39%
5	YouTube	3.63%	iTunes	3.27%	iTunes	2.91%
6	Skype	2.76%	MPEG - Other	2.60%	SSL	2.54%
7	QVoD	2.55%	SSL	2.05%	MPEG - Other	2.32%
8	Facebook	1.54%	Amazon Video	1.61%	Amazon Video	1.48%
9	FaceTime	1.44%	Facebook	1.31%	Facebook	1.34%
10	Dropbox	1.39%	Hulu	1.29%	Hulu	1.15%
		66.00%		76.23%		73.35%


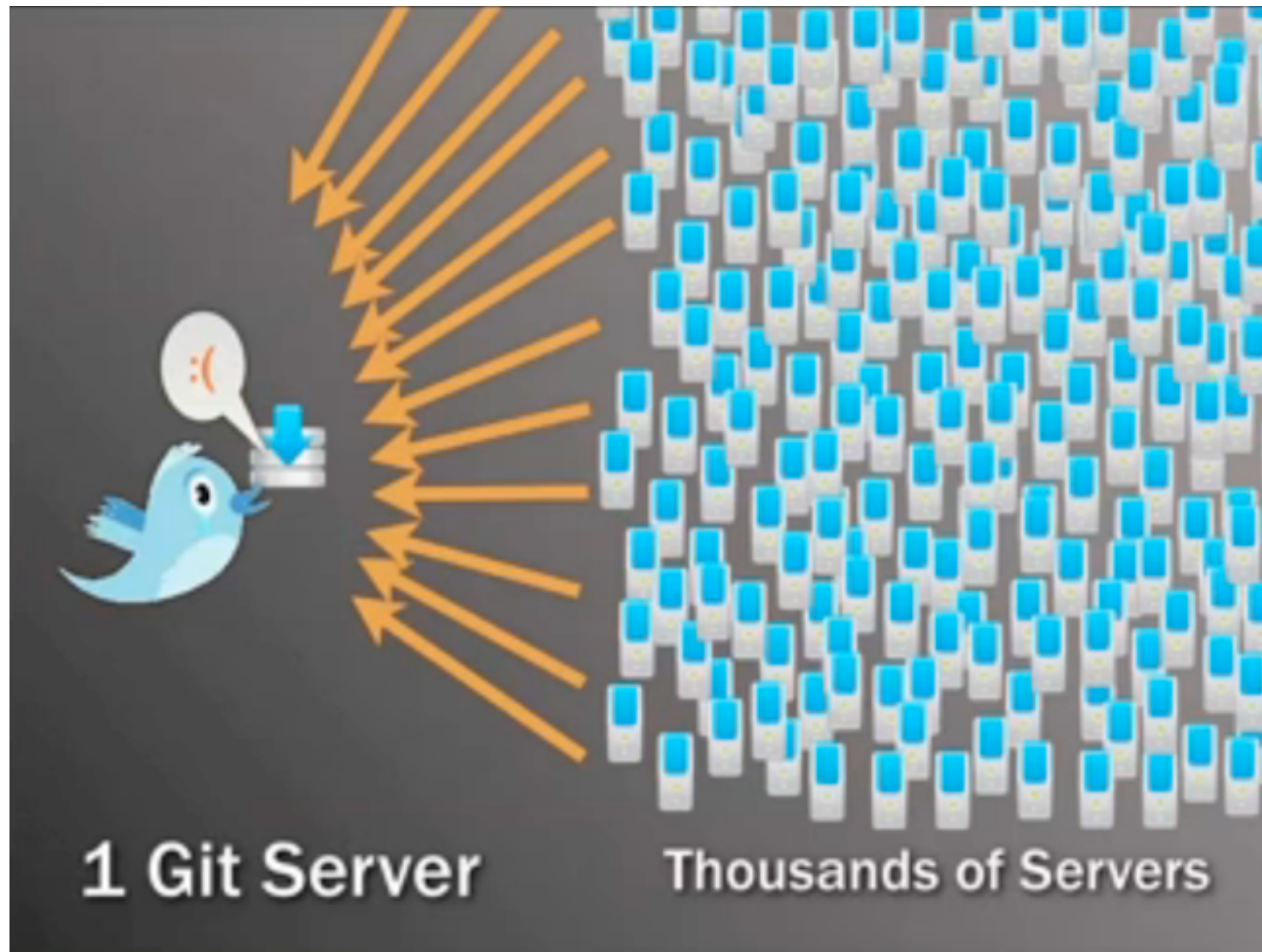
 sandvine

Table 2 - Top 10 Peak Period Applications - North America, Fixed Access

Why to study P2P

- When designed properly, P2P-based file sharing applications can be very efficient and fast to distribute contents
- e.g., Twiter uses Murder to update their servers since 2010
 - <https://blog.twitter.com/2010/murder-fast-datacenter-code-deploys-using-bittorrent>

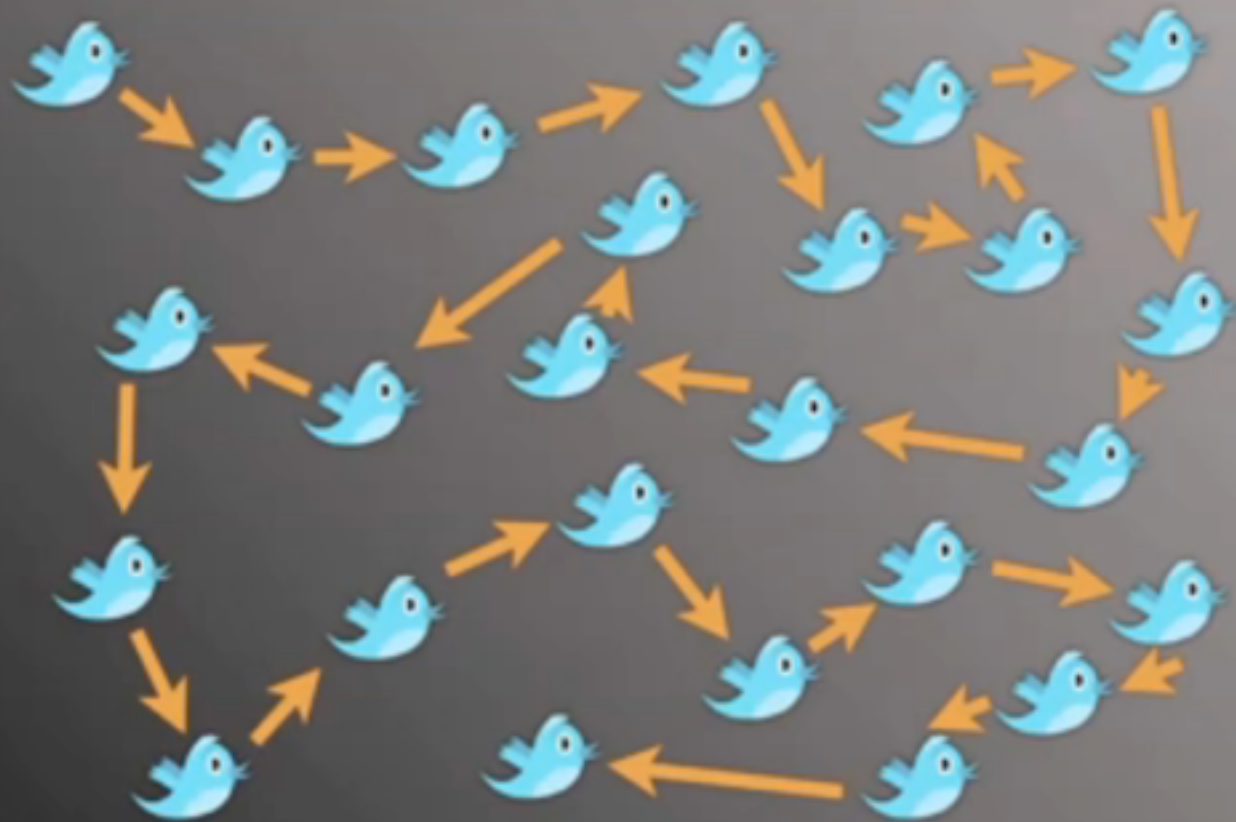
Before Murder



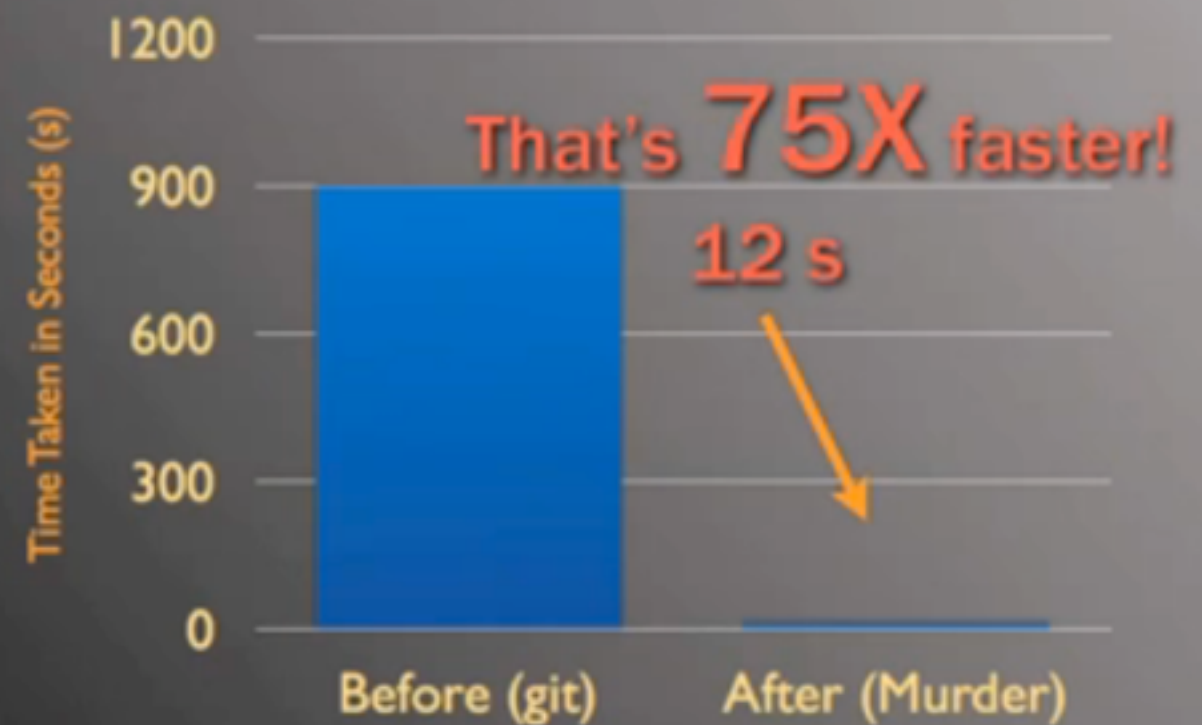
credit: <https://blog.twitter.com/2010/murder-fast-datacenter-code-deploys-using-bittorrent>

With Murder

How We Actually Distribute



Time to Deploy with Murder



credit: <https://blog.twitter.com/2010/murder-fast-datacenter-code-deploys-using-bittorrent>

Content replication

Definitions

- Service capacity
 - Number of peers that can serve a content
 - = 1 in client-server, constant with time
- Flash crowd of n
 - Simultaneous request of n peers (e.g., soccer match, iOS update...)
- Piece/chunk/block
 - Element of a partition of the content
 - Each piece can be independently retrieved
 - The union of pieces forms the content

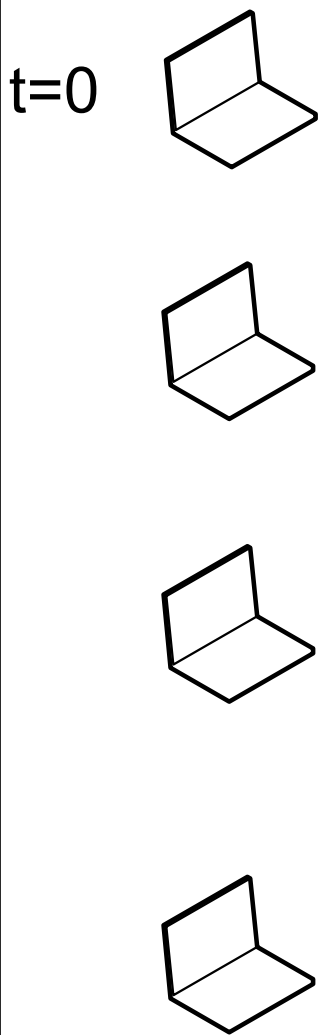
Interest of P2P to replicate contents

- Service capacity grows up exponentially with time
- Average download time for a flash crowd n is then in $\log(n)$
- Average download time decreases in $\frac{1}{\# \text{ of pieces}}$ when the number of pieces increases
 - if we ignore the overhead

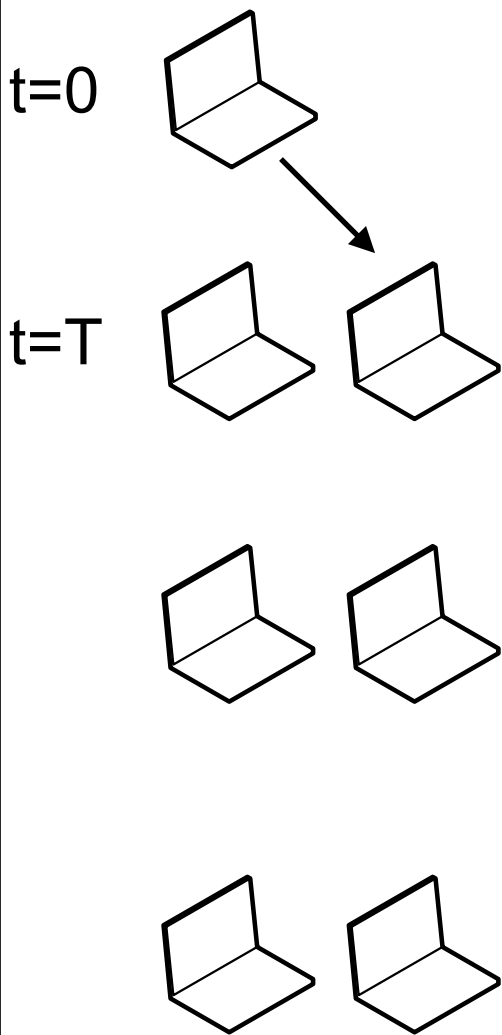
Content transfer model

- Simple deterministic model
 - Each peer serves only one peer at a time
 - The unit of transfer is the content
 - $n-1$ peers want the content, with $n=2^k$
- T is the time to complete an upload
 - $T=s/b$, s content size, b upload capacity
- Peer selection strategy with Binary tree
 - global knowledge

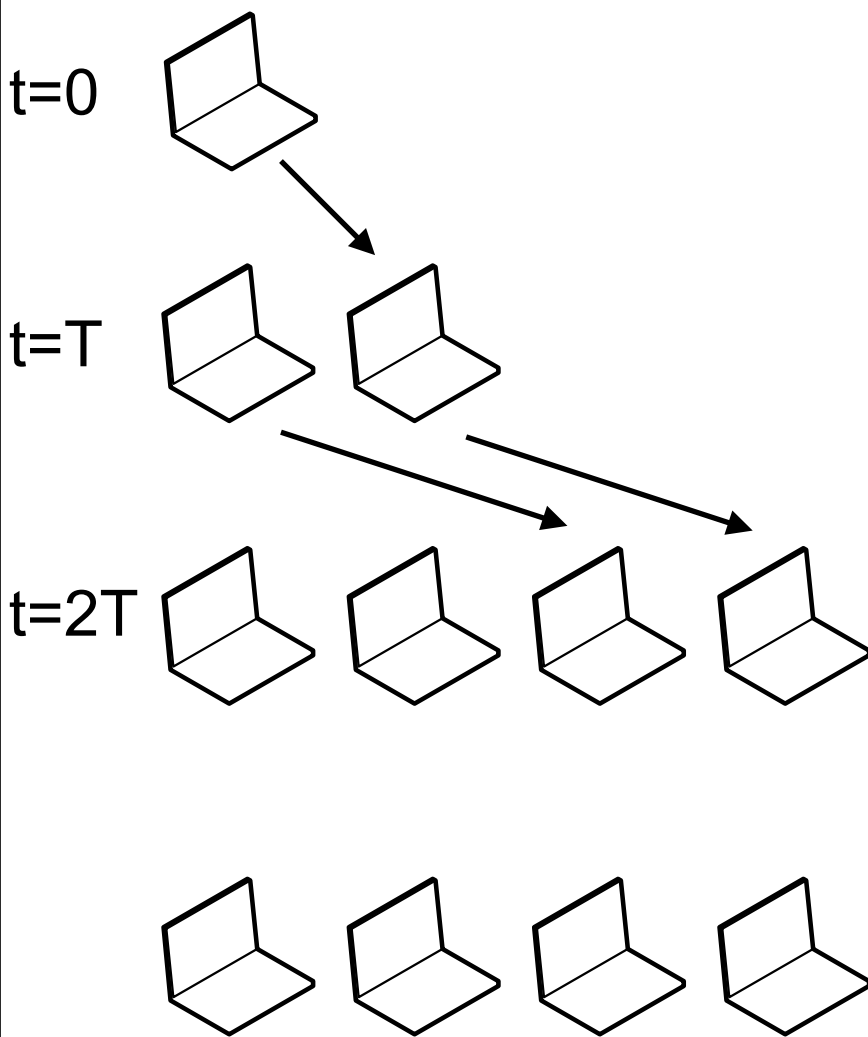
Capacity C of the service



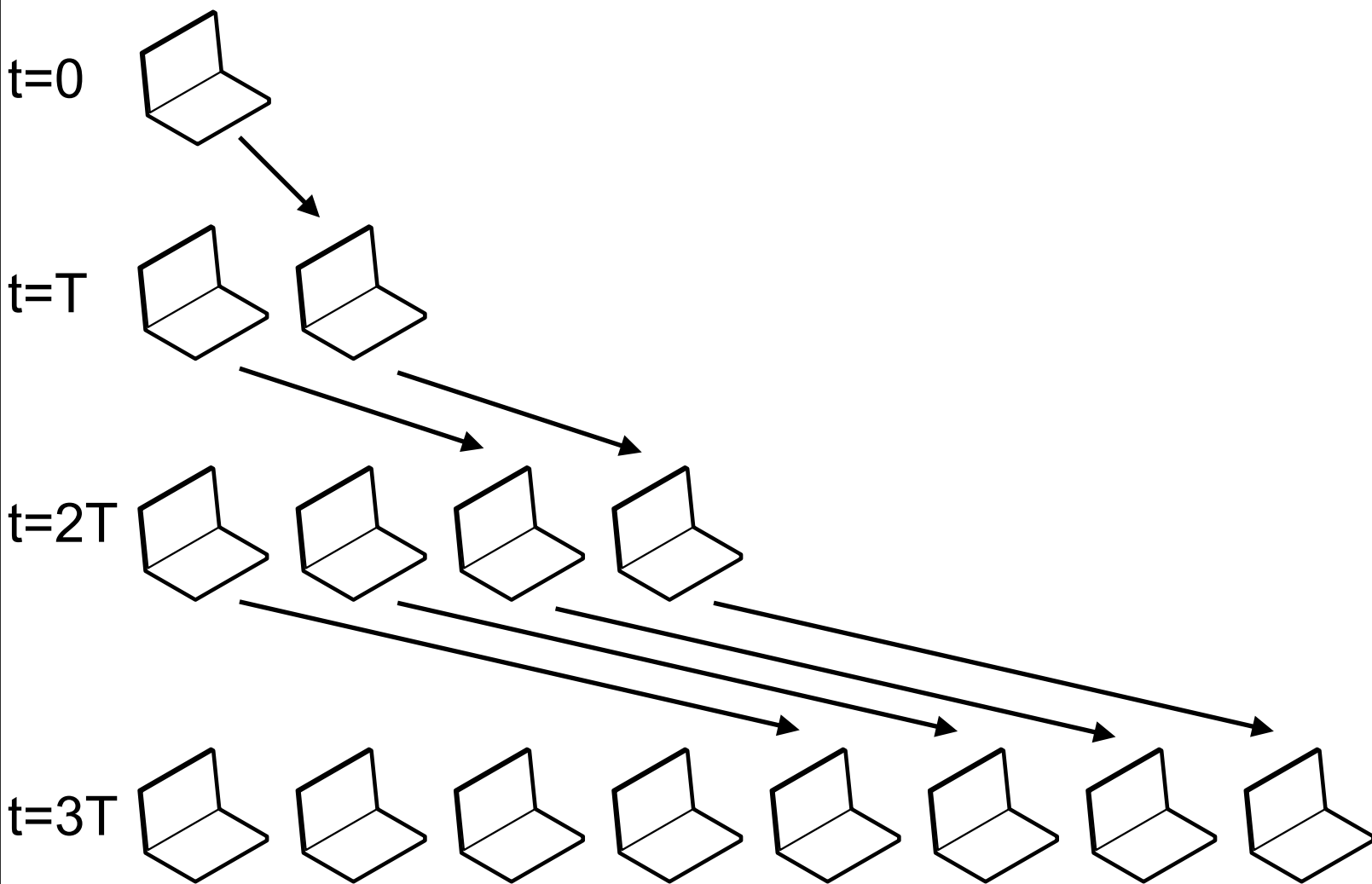
Capacity C of the service



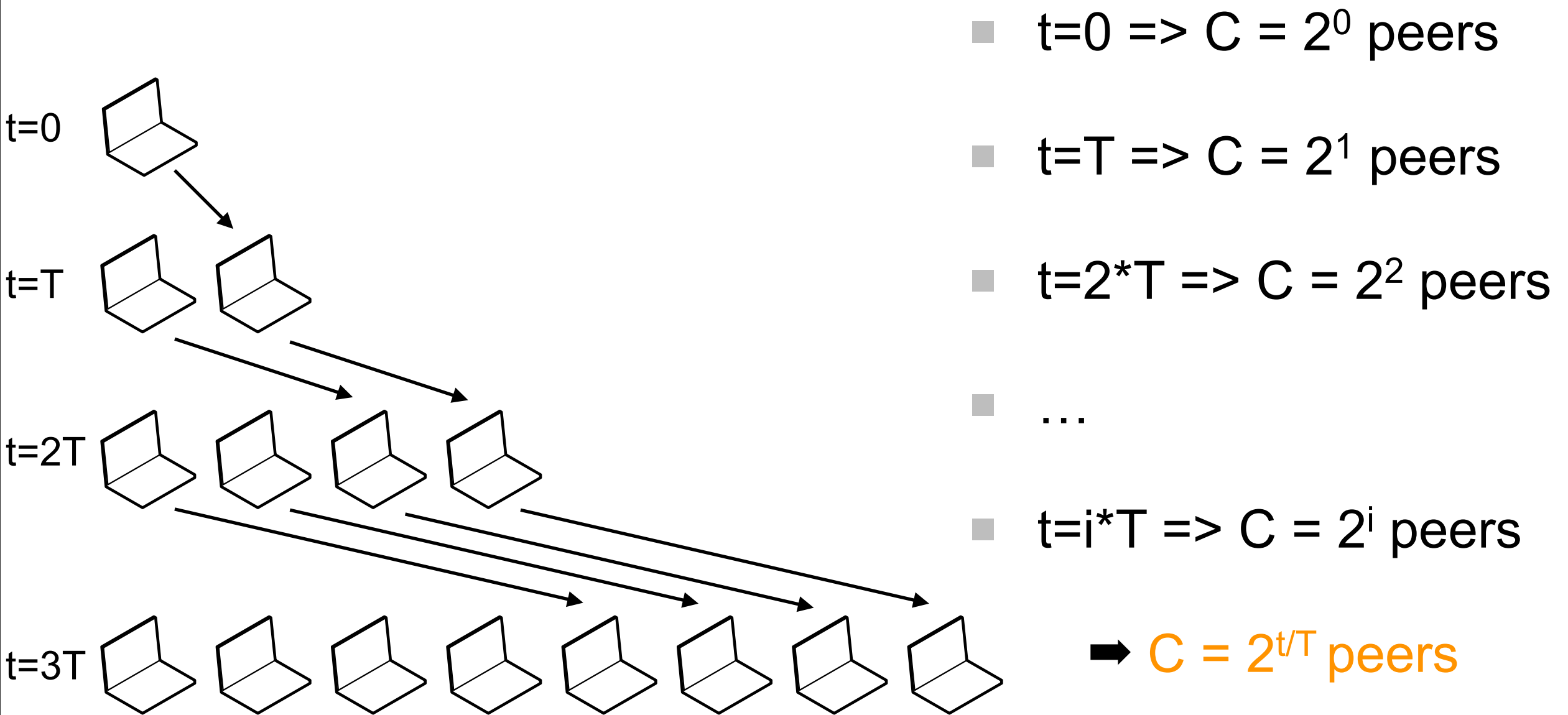
Capacity C of the service



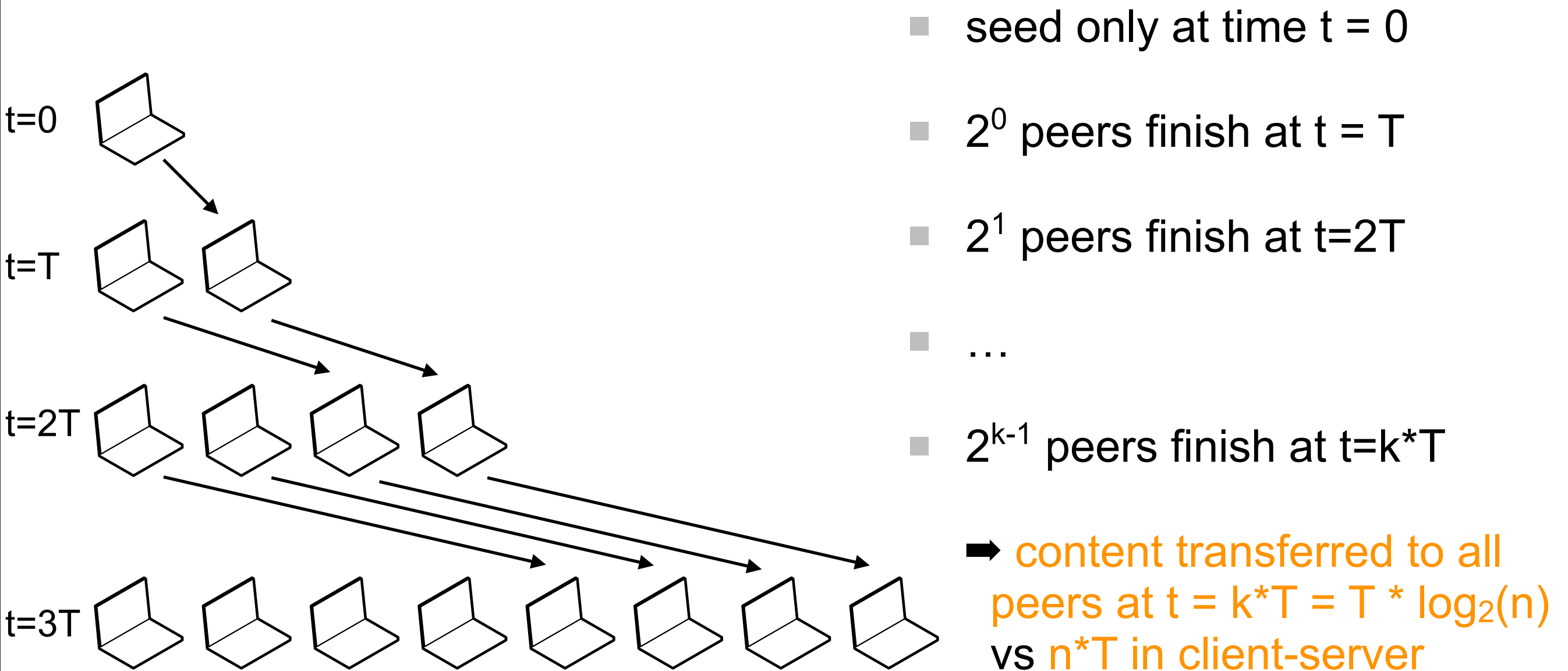
Capacity C of the service



Capacity C of the service



Finish time



Can we speed up
transfers?

Piece transfer model

- Same as before but the transfer unit is the piece instead of the content
 - a content is divided into m equal size pieces
 - $m > k$
 - Piece downloaded in T/m
- ➔ content transferred to all peers at $t = T * 1/m * \log_2(n) + T$
vs $T * \log_2(n)$ without piece transfer vs $n * T$ in client-server

Parallel downloads

- Download from several peers in parallel
- Strategy
 - request one piece from every server with the content
 - request another piece from the server as soon as the requested piece has been obtained
 - performance is optimal when servers are always busy delivering a piece of data

Parallel downloads (contd.)

P



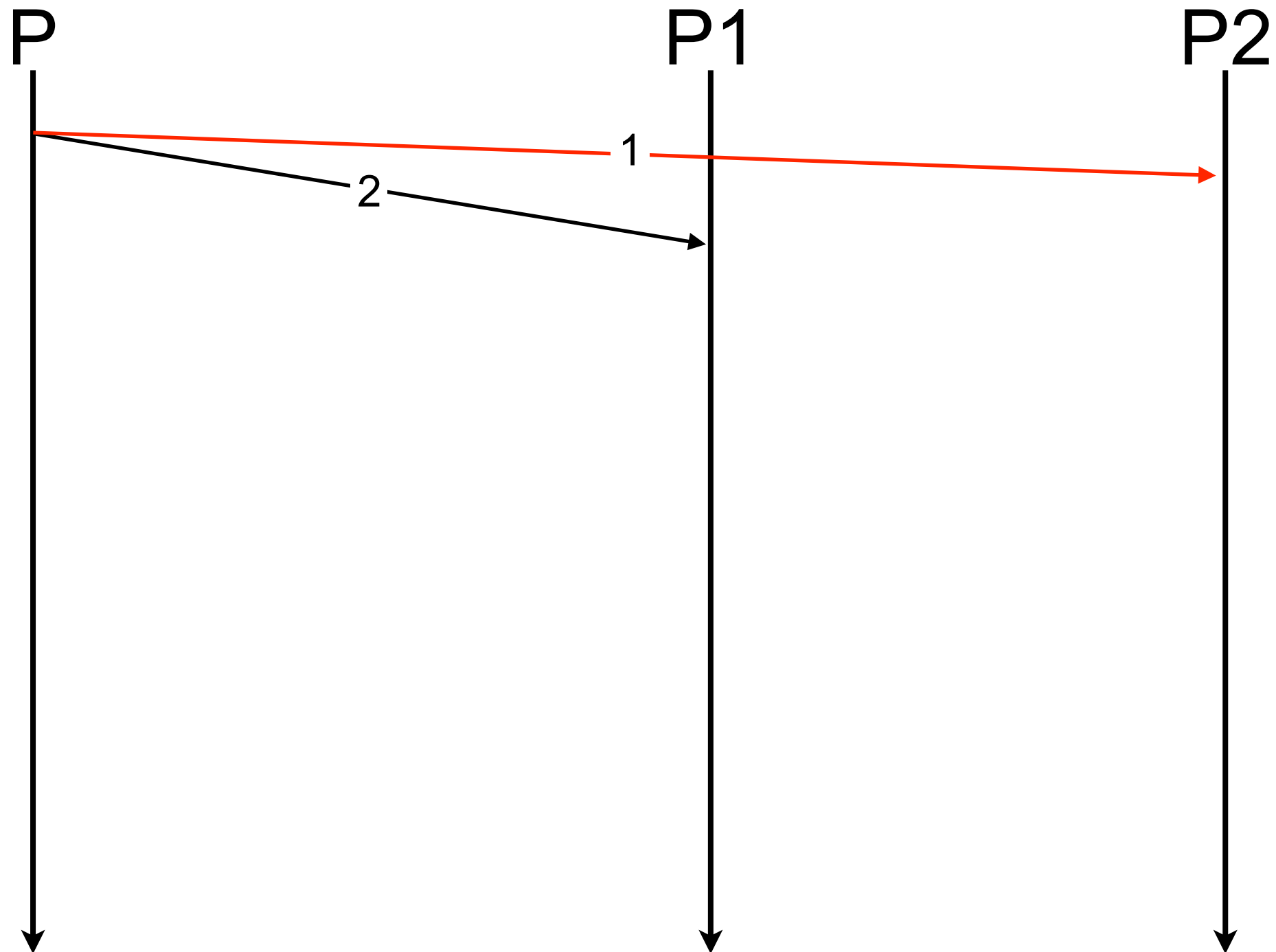
P1



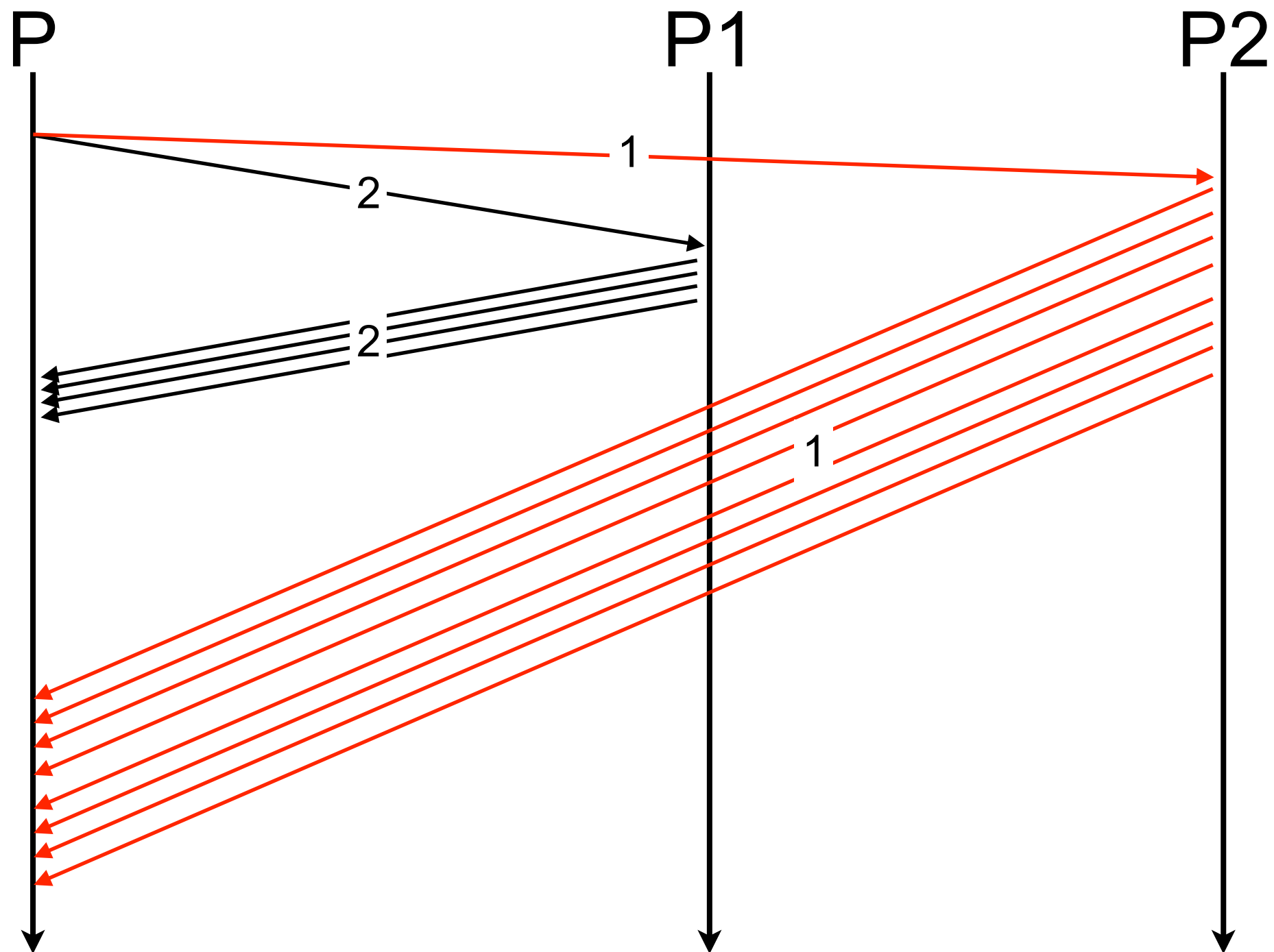
P2



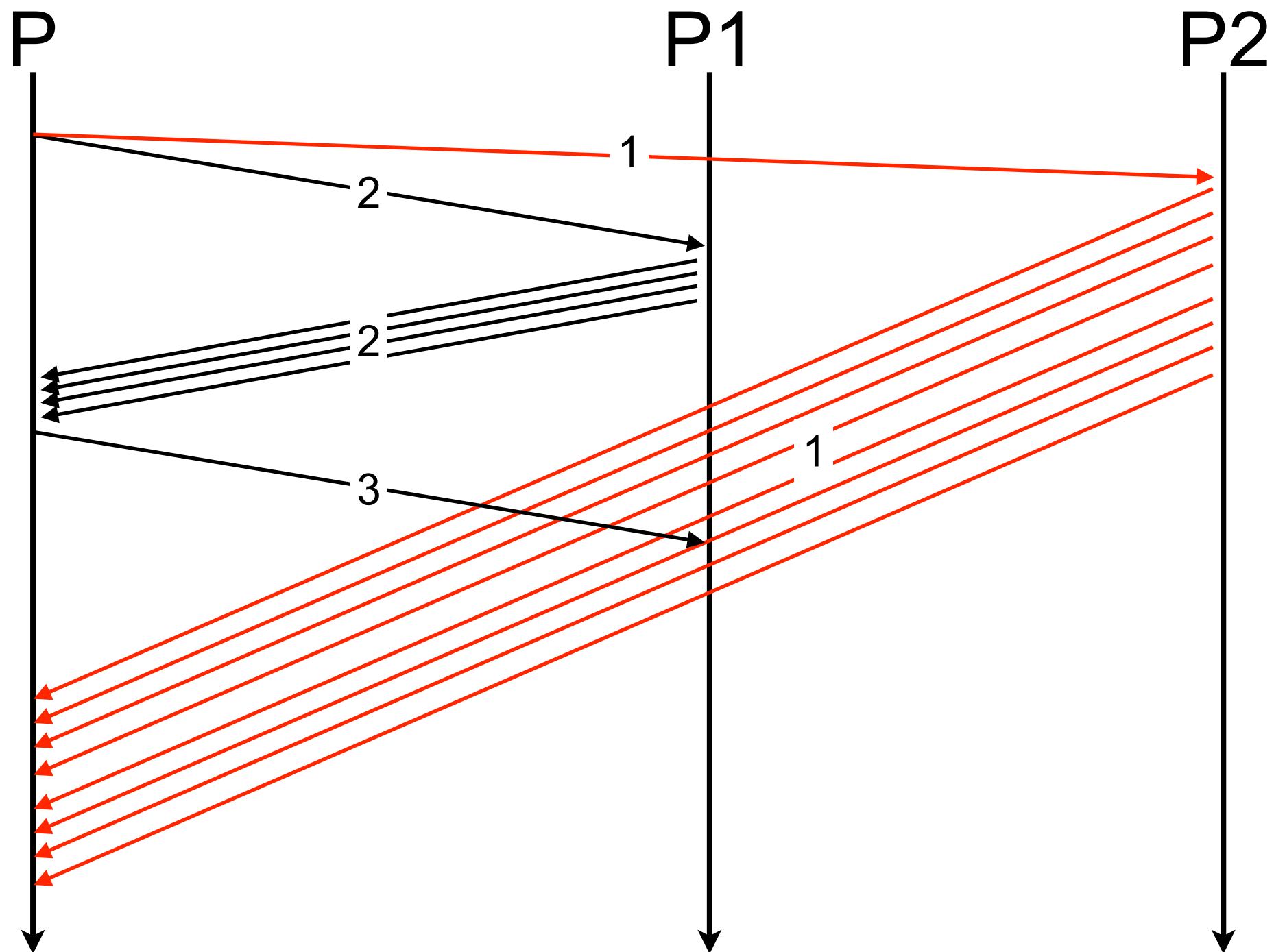
Parallel downloads (contd.)



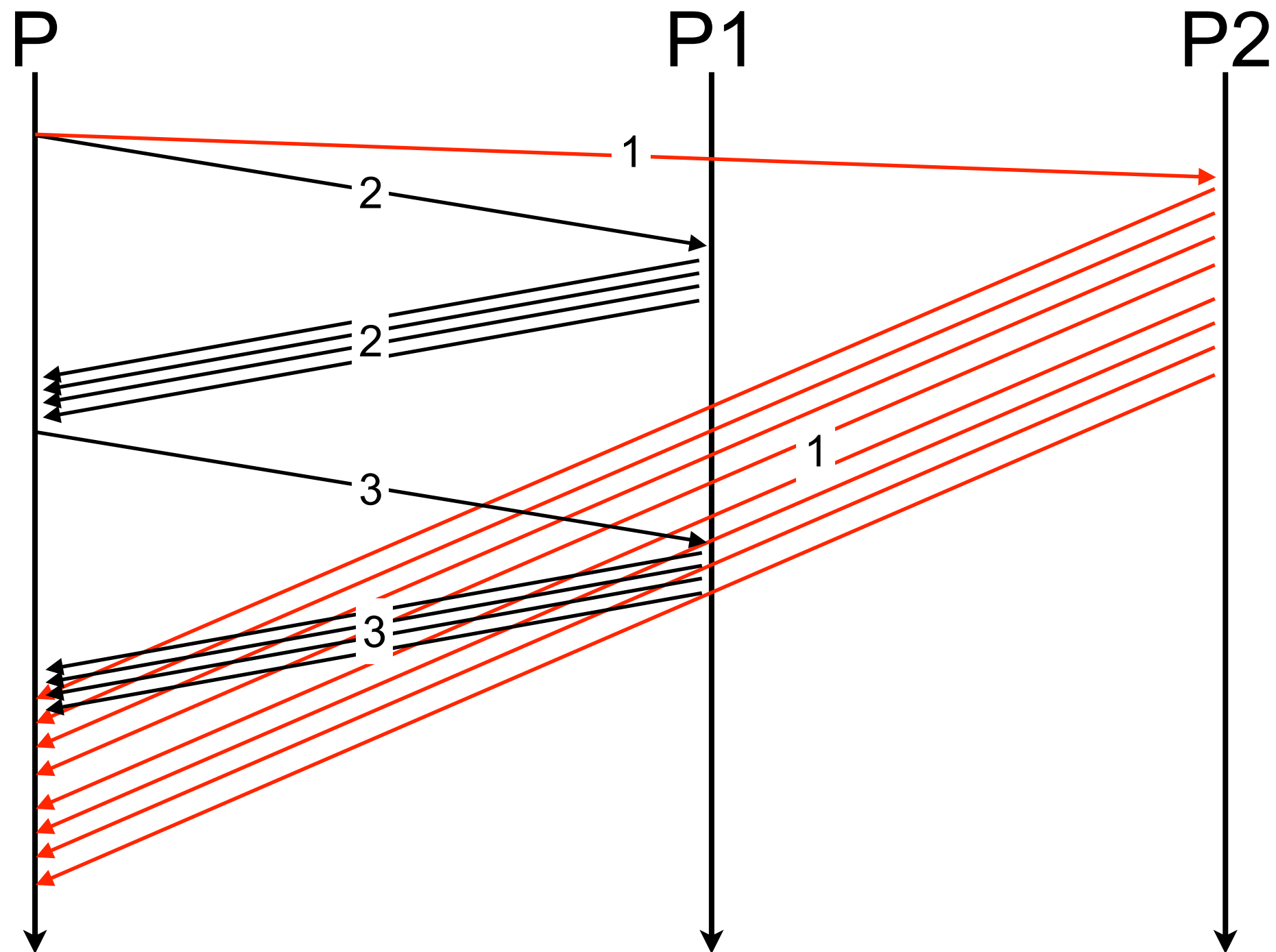
Parallel downloads (contd.)



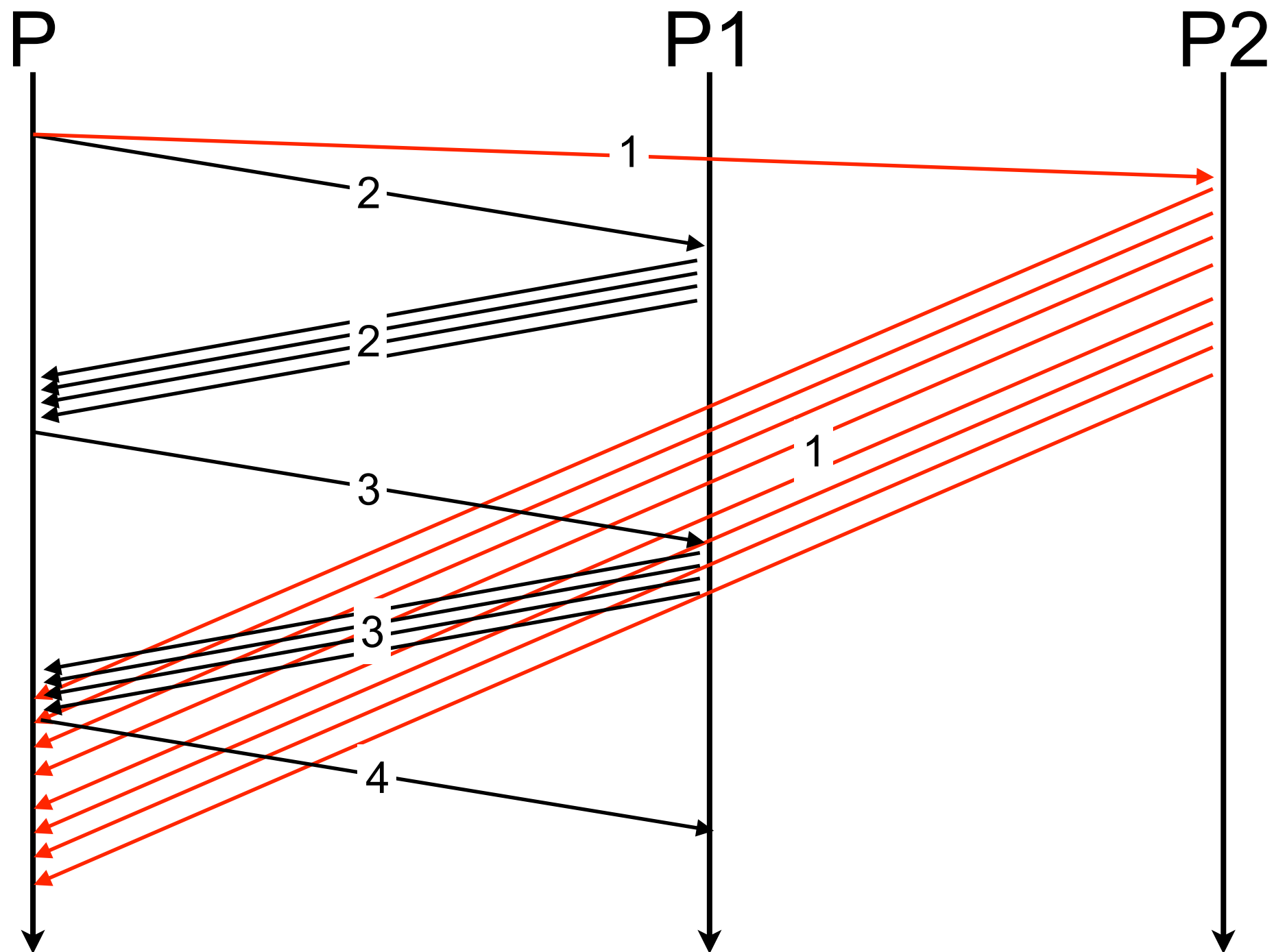
Parallel downloads (contd.)



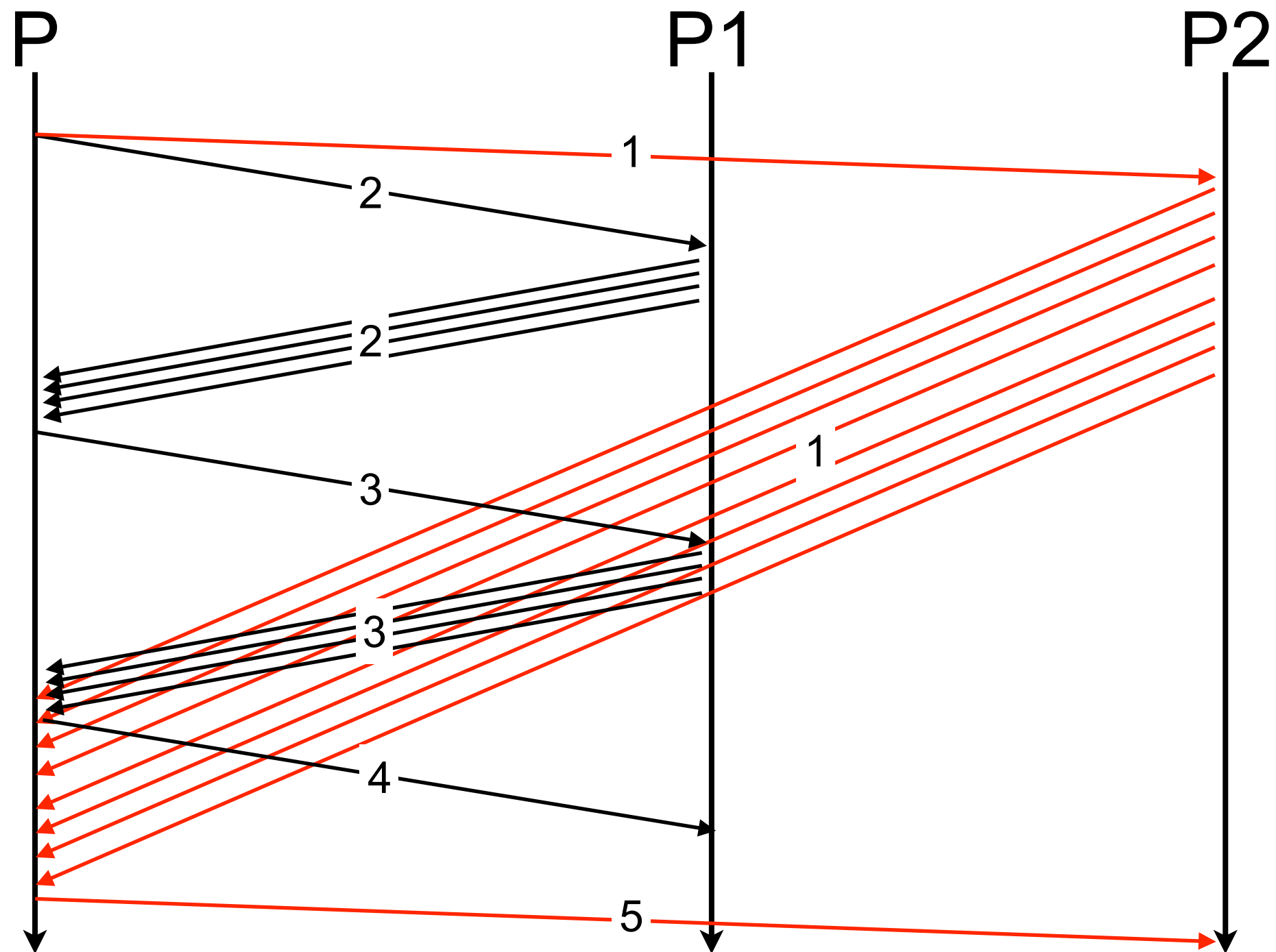
Parallel downloads (contd.)



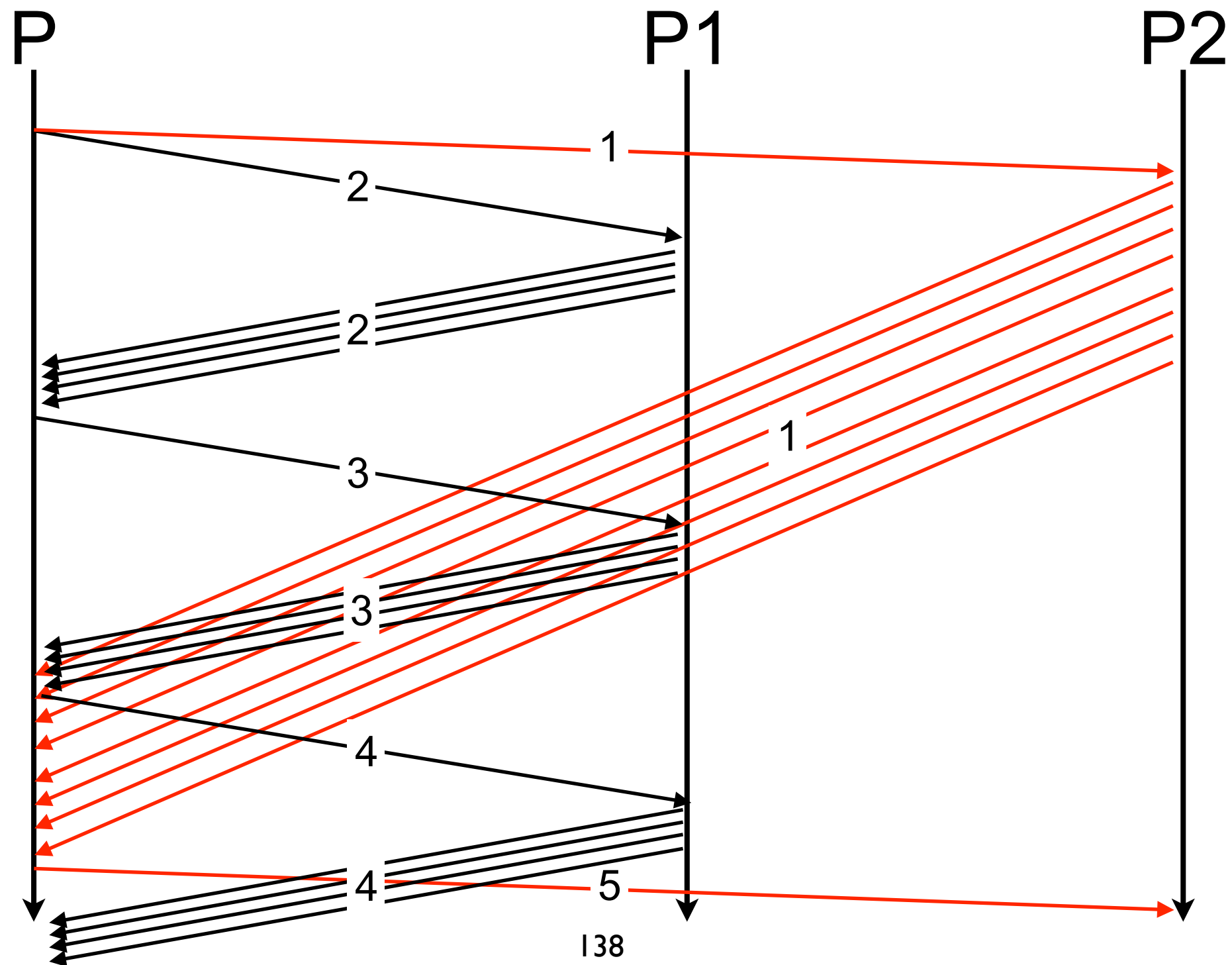
Parallel downloads (contd.)



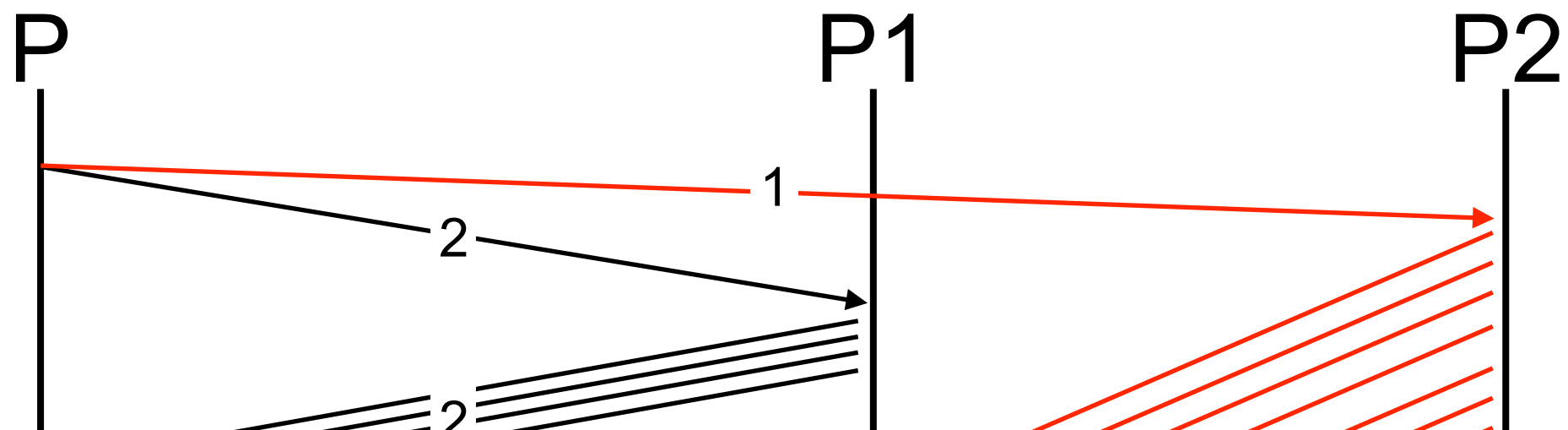
Parallel downloads (contd.)



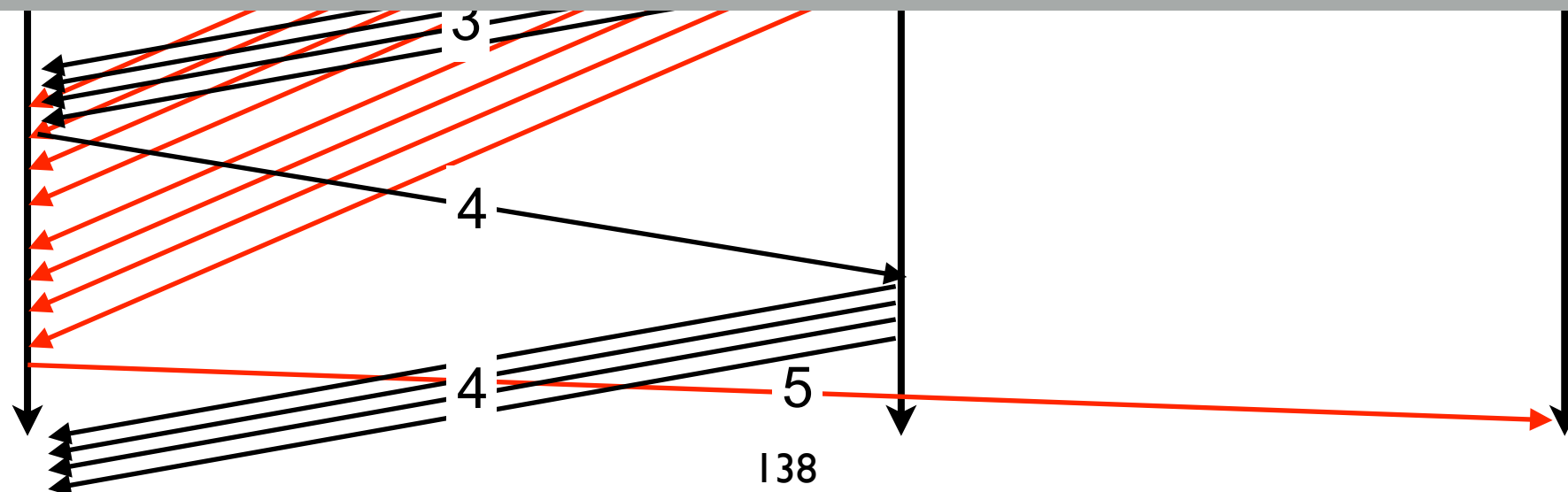
Parallel downloads (contd.)



Parallel downloads (contd.)



Peers are not always fully utilised!



Pipelining

P

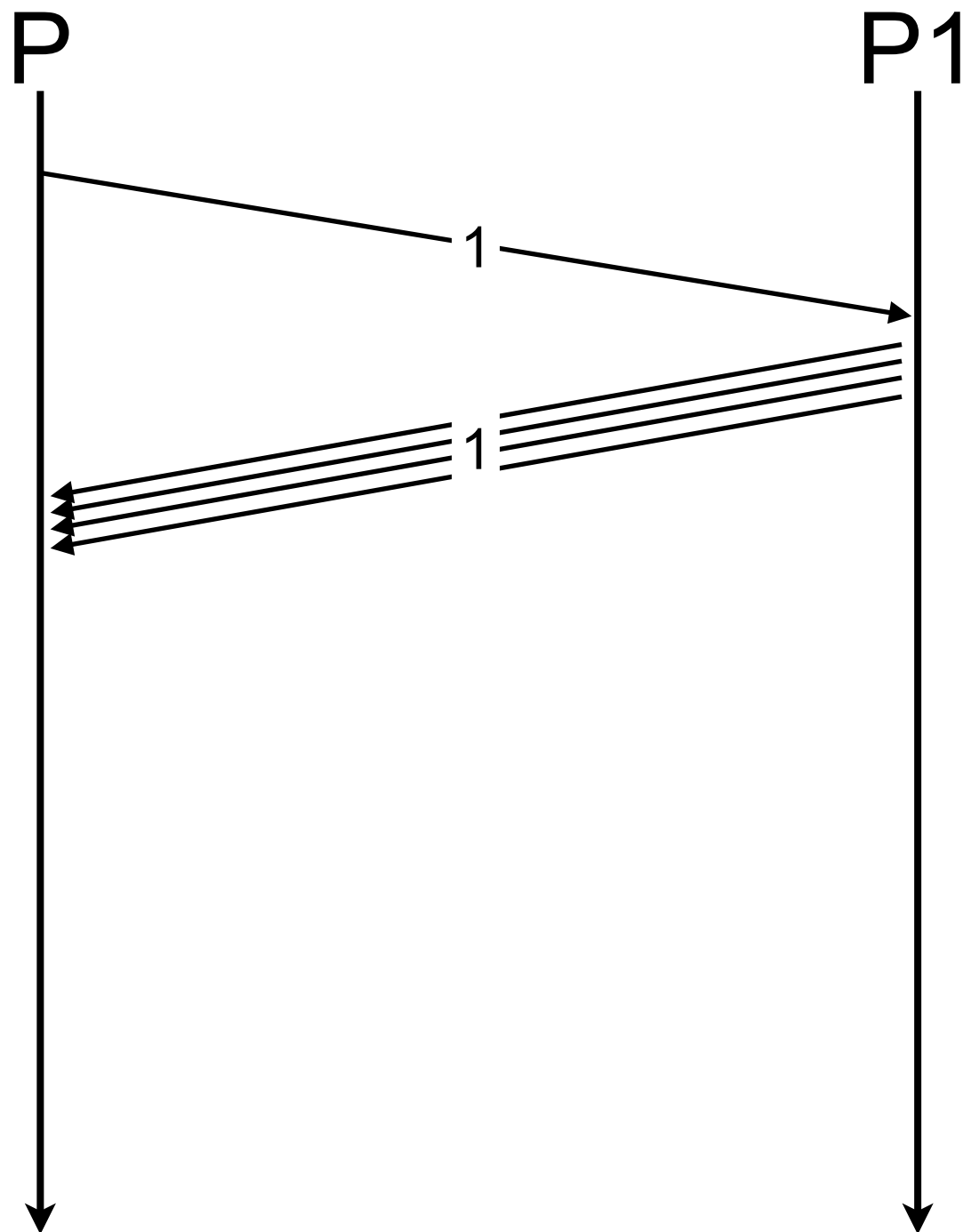


P1



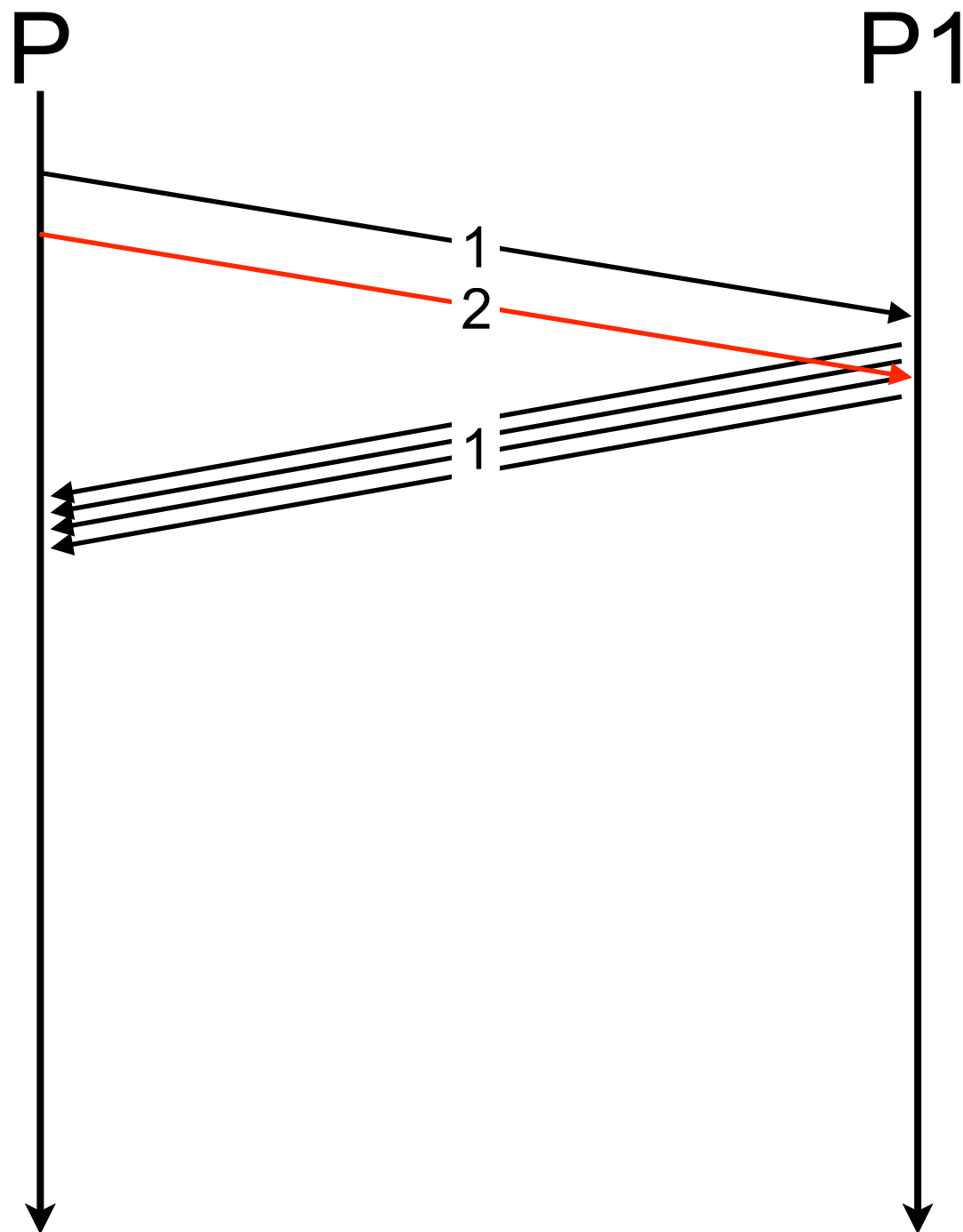
- Keep enough requests pending
- Send a new request before the end of the transmission of the piece being downloaded
- need to roughly estimate the RTT

Pipelining



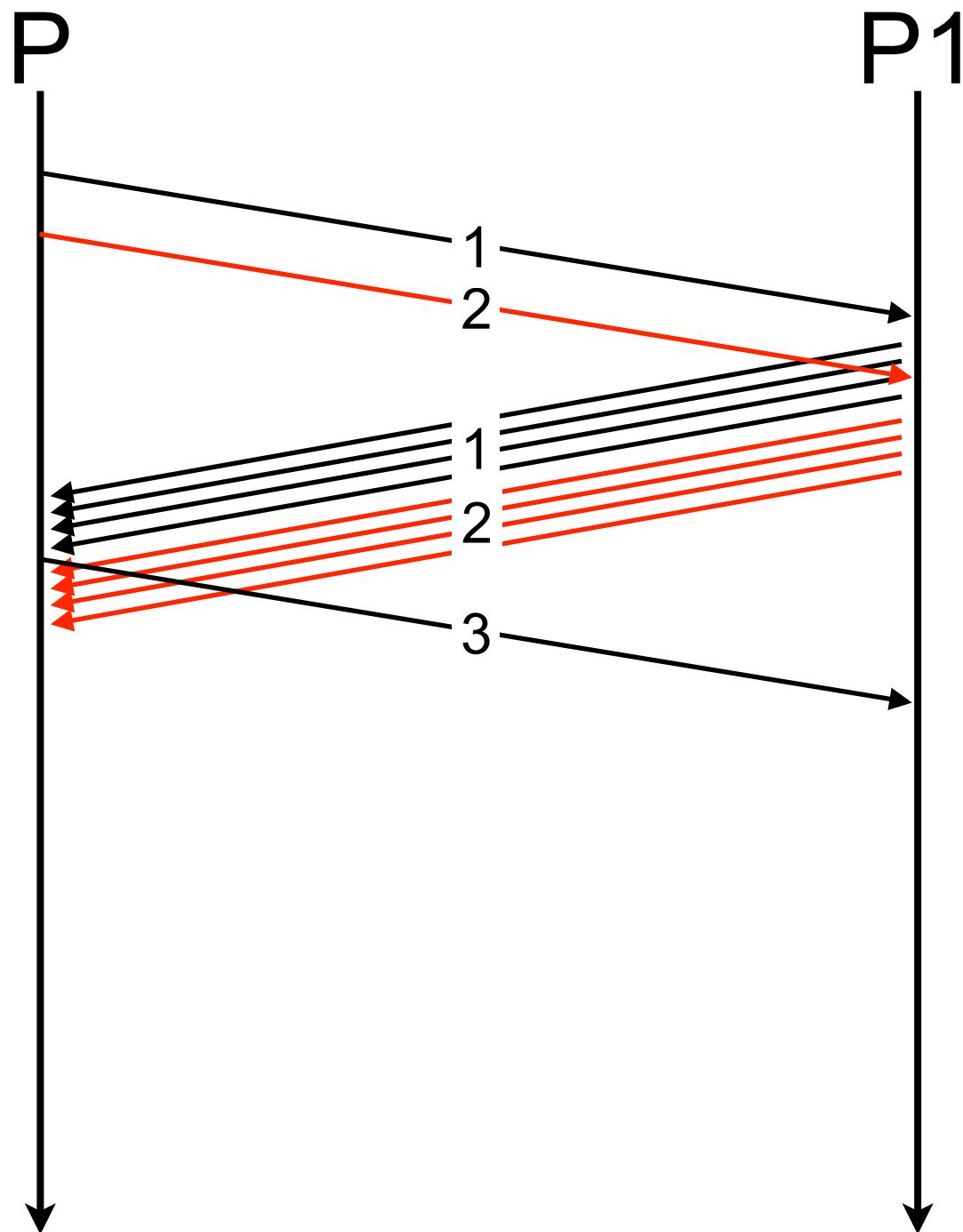
- Keep enough requests pending
- Send a new request before the end of the transmission of the piece being downloaded
- need to roughly estimate the RTT

Pipelining



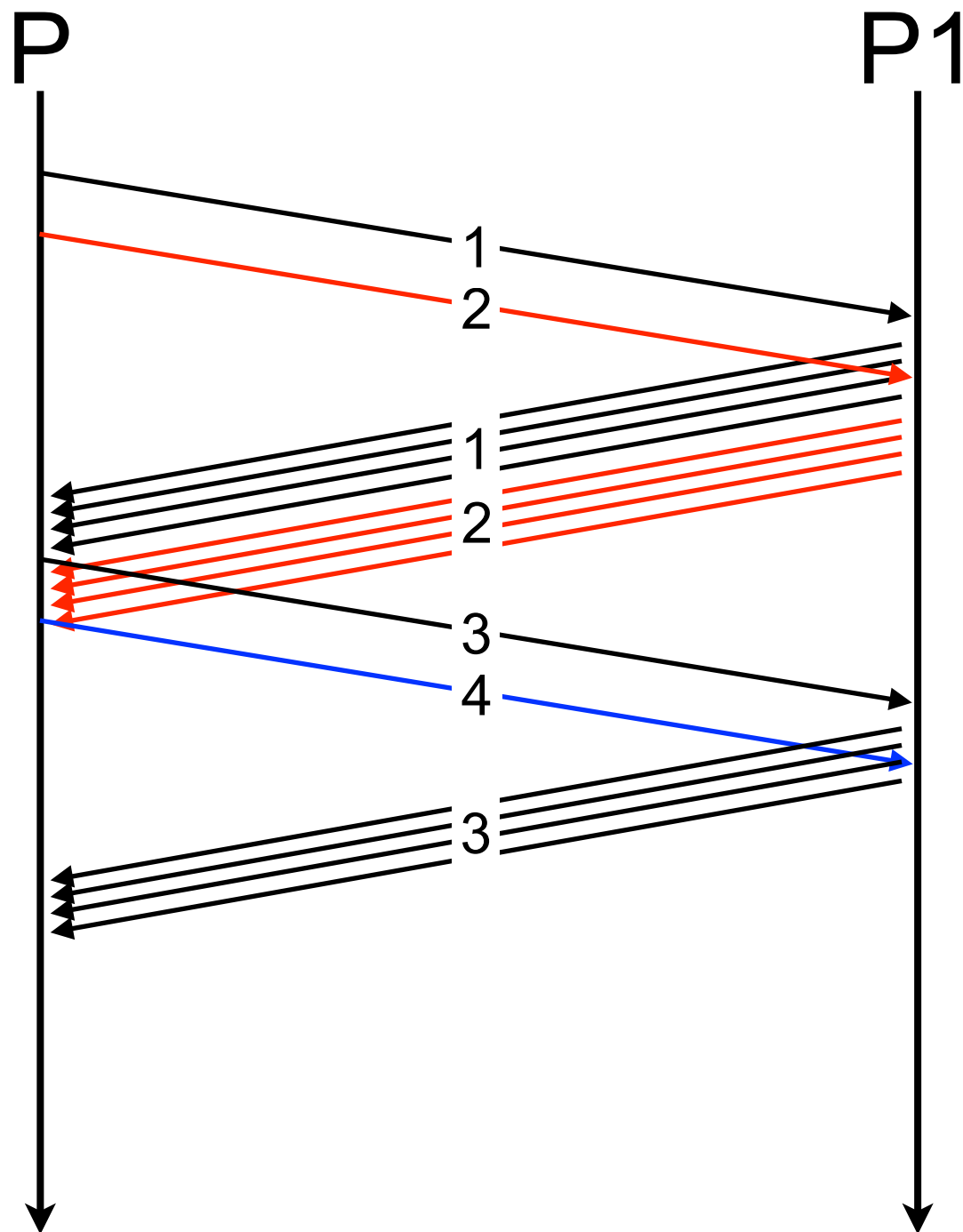
- Keep enough requests pending
- Send a new request before the end of the transmission of the piece being downloaded
- need to roughly estimate the RTT

Pipelining



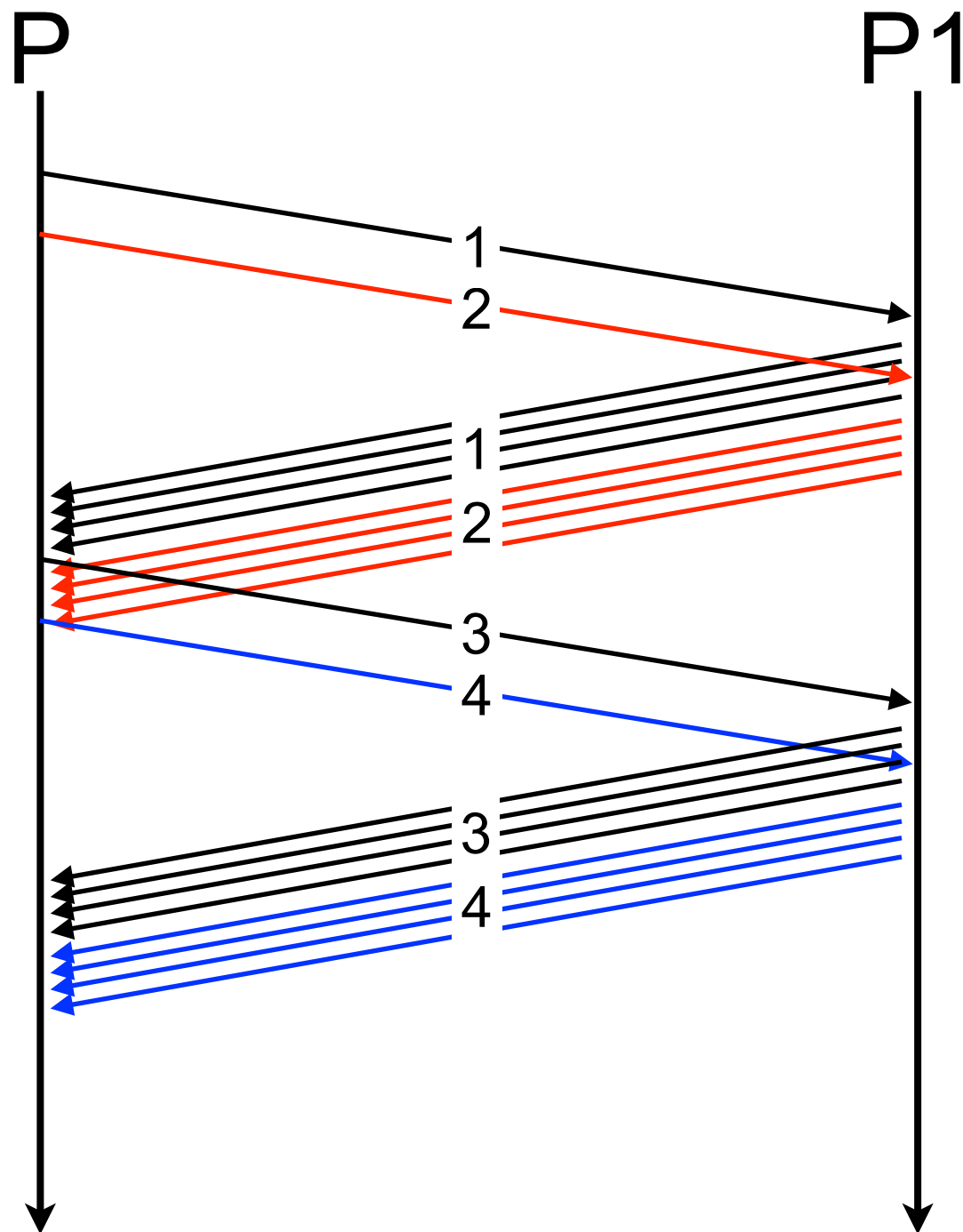
- Keep enough requests pending
- Send a new request before the end of the transmission of the piece being downloaded
- need to roughly estimate the RTT

Pipelining



- Keep enough requests pending
- Send a new request before the end of the transmission of the piece being downloaded
- need to roughly estimate the RTT

Pipelining



- Keep enough requests pending
- Send a new request before the end of the transmission of the piece being downloaded
- need to roughly estimate the RTT

Termination idle time

- In case of M servers, and P remaining pieces,
- when $P < M$, $M - P$ serving peers are idle
- End-game mode
 - when $P < M$, request pending blocks to all idle servers
 - speed of the fastest serving peers
 - some pieces are downloaded several times

Discussion

- Previous models have idealised view of the system
 - perfect peer selection (peers always select an available peer)
 - perfect piece selection (peers always select an available piece)
 - no dynamics (peers do not enter or leave the network)
 - no selfish behaviour (peers always answer at their maximal capacity)
 - a free rider is a peer that downloads without contributing
 - but to scale, each peer in a P2P system must act as a client and a server!

Peer selection

- Ideal, the peer selection algorithm should
 - always find a peer to upload from
 - prevent free riders
 - converge to the best upload-download match
 - peer selection should be based on capacity only (i.e., independent of pieces available)

Choke algorithm

- The peer selection of BitTorrent
- Different algorithm in leecher and seed states
- Peers are selected in the peer set (i.e., a subset of all peers)
- Choke status
 - A chokes B if A decides to NOT upload to B
- Interested status
 - A is interested in B if B has at least one piece A does not have
- All decision are performed locally

Choke algorithm: leecher state

- Every 10 seconds:
 - the peer list is sorted by download rate
 - the 3 fastest and interested peers are unchoked
- Every 30 seconds:
 - one interested peer selected at random is unchoked (optimistic unchoke)
- Maximum 4 interested unchoked peers at the same time

Choke algorithm: seed state

- Favor upload mode:
 - same as in leecher state but ordered by upload speed
- Round Robin mode:
 - Order peers in the list by their unchoked time, every 10 seconds
 - for two consecutive periods, unchoke the first 3 peers and a forth at random
 - for the third period, unchoke the first 4 peers

Choke algorithm discussion

- Leecher state is robust to free riders
 - must contribute to get good service
- Seed state is not robust to free riders
 - favors peers that download the fastest
- Tend to select the fastest peers, that it automatically detects

Piece selection

- Random piece selection
 - each peers selects at random a piece to download
 - poor entropy
 - hard to get the last pieces
- Global rarest first
 - select the globally rarest piece to download
 - piece replication is maximised
 - requires global knowledge

Piece selection (contd.)

- Local rarest first
 - select the rarest piece to download within the peer set
 - when peer selection is performed before piece selection, the piece is selected according to the availability on the selected peers
 - good entropy when the set is large and random enough

Network coding

- Encode pieces such that if
 - k is the number of original pieces
 - and n is the number of encoded pieces,
- any k among the $k+n$ pieces are enough to reconstruct the content

Network coding (contd.)

- Content $C = [x_1 \dots x_m]$
- Encode C as $E_i(\mathbf{A}_i) = \sum_{a_{i,j} \in \mathbf{A}_i} a_{i,j} \cdot x_j$
- Any linearly independent encodings $E_i(\mathbf{A}_i)$ can be combined to recover C

Network coding (contd.)

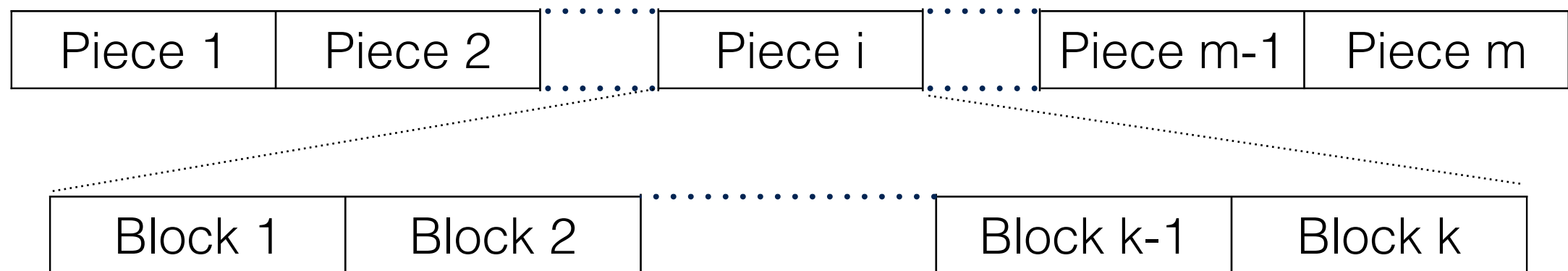
- No need for piece selection as any set of linearly independent encoded pieces can be used to recover the content
 - entropy is nearly optimal
- Encoding computation is heavy
- Integrity and security is easily broken as a single piece corruption propagates to the whole content

BitTorrent

- Get a .torrent file
 - describes the torrent (the unit of data)
 - content length in bytes
 - file name
 - piece length (256/512/1024/2048 KB)
 - all pieces signatures (SHA-1)
 - tracker address
 - creation date, comments...
 - torrents are independent (no link with the previous and current torrents)
- Get a random peer set from a tracker
- Retrieve the data

Pieces and blocks

- Contents are decomposed in pieces
- Pieces are split in blocks of 16 KB to allow pipelining
 - 5 pending requests



Torrent download (phase 1)

- The peer sends
 - torrent info hash
 - its peer ID
 - the port it listens on
 - the number of peers it expects in the list (default=50)
 - statistics

Torrent download (phase 2)

- The tracker returns
 - periodic statistics interval
 - randomised list of peers for the torrent
 - <peer id, peer IP, peer port>
 - statistics

Torrent download (phase 3)

- The peer connects to a subset of the peer list (40 outgoing sessions)
- The peer set (neighbour set) is limited to 80 connections in total
- Results in a graph with good properties for local rarest first
 - dense well connected random graph
 - low diameter
 - robust to churn (i.e., entering and leaving peers)

Tracker

- Peers periodically send statistics to the tracker (every 30 minutes)
- Peers request for new peers when peer list < 20
- Peers informs the tracker when they leave
- Tracker identify NATed peers and maintain peer list up-to-date
- To start a torrent
 - create a .torrent file and upload it to a discovery site
 - start a P2P client using the torrent file and the content to seed

Piece selection

- Strict priority
 - always request all the blocks of a piece before asking for other pieces
 - if no block available, start downloading other pieces, but come back to the pending blocks as soon as they are available
- Random first piece
 - to avoid spending time waiting to be unchoked and downloading hardly reachable piece, selects the first 4 pieces of a download at random
- Endgame mode
 - when all blocks have been requested, request all pending blocks to all peers

Cool, I am anonymous with P2P!

Are you sure?

Privacy

Sharing secrets

- Context
 - n student work on a top-secret project
 - They cannot trust each other
 - The project is in a digital safe
 - To open the digital safe, at least k out of the n students must be present

(k,n) threshold scheme

- $D = [x_1, \dots, x_n]$ is a data composed of n pieces
- When at least k pieces x_i of D are known
 - D can be computed
- otherwise D remains undetermined

(k,n) threshold scheme

- $D = [x_1, \dots, x_n]$ is a data composed of n pieces

A polynomial of degree $k-1$ is uniquely identified with k points

- D can be computed
- otherwise D remains undetermined

Shamir's (k,n) Threshold Scheme

- Let D be our secret (an integer), decomposed in n pieces
- Let p be a prime number $p > \max(D, n)$
- Generate $k-1$ random number a_i

$$\forall i \in [1; k-1] | a_i \in [0; p[$$

- Define the polynomial of degree $k-1$

$$g(x) = D + a_1 \cdot x^1 + \dots + a_{k-1} \cdot x^{k-1}$$

- Note that $g(0) = D$

Shamir's (k,n) Threshold Scheme (contd.)

- Generate n fragments of the secret

$$D_1 = g(1) \bmod p, D_2 = g(2) \bmod p, \dots D_n = g(n) \bmod p$$

- Distribute (x_i, D_i)
- Recompute D from k fragments (x_j, D_j) among n using Lagrange polynomial interpolation

$$g(0) = \sum_{i=1}^k D_i \left(\prod_{j=1, j \neq i}^k \frac{-x_j}{x_i - x_j} \right)$$
$$D \equiv g(0) \bmod p$$

Example $k=3$, $n=5$

- $p = 997$
- Make 5 groups
 - group 1: (1, 547)
 - group 2: (2, 629)
 - group 3: (3, 394)
 - group 4: (4, 839)
 - group 5: (5, 967)

Example $k=3$, $n=5$

- $p = 997$
- Make 5 groups
 - group 1: (1, 547)

Collaborate with 2 other groups to compute the secret D

- group 4: (4, 839)
- group 5: (5, 967)

Example $k=3$, $n=5$ (contd.)

- Group 1, 3, 4

$$g(0) = 547 \left(\frac{-3}{1-3} \frac{-4}{1-4} \right) + 394 \left(\frac{-1}{3-1} \frac{-4}{3-4} \right) + 839 \left(\frac{-1}{4-1} \frac{-3}{4-3} \right)$$

$$g(0) = 547 * 2 - 394 * 2 + 839 = 1145$$

$$g(0) \bmod 997 = 148$$

Example $k=3$, $n=5$ (contd.)

- To compute it, we took $D = 148$, $p = 997$ a prime number, and the polynomial $p=997$ (prime), $a_1=59$ (random), $a_2=340$ (random)
 $g(x)=148 + 59x + 340x^2$
- Such that
$$D_1 = g(1) \bmod 997 = 547$$
$$D_2 = g(2) \bmod 997 = 1626 \bmod 997 = 629$$
$$D_3 = g(3) \bmod 997 = 3385 \bmod 997 = 394$$
$$D_4 = g(4) \bmod 997 = 5824 \bmod 997 = 839$$
$$D_5 = g(5) \bmod 997 = 8943 \bmod 997 = 967$$

Shamir's (k,n) Threshold Scheme (contd.)

- The size of each fragment does not exceeds the size of the secret
 - as long as p is chosen of the same order as the secret
- Possible to generate new fragments at any time, without altering the others
- Possible to construct hierarchies by attributing more or less fragments
 - the boss has k fragments, the subaltern has $k/2$, ...
- No assumption as apposed to cryptographic functions

Anonymity

- Alice wants to send a message to Bob
 - Communications are unsecured
 - Nobody can know who is the sender (not even Bob)
 - Nobody can know who is the receiver
 - Nobody else Bob can retrieve the message

Mix

- Objectives of a mix
 - Hide correspondences between incoming and outgoing messages
 - Not possible to map a source and an outgoing message (apart for the mix)
 - No possible to map a receiver and an incoming message (apart for the mix)

Mix (contd.)

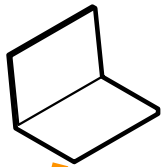
- If the mix cannot be fully trusted, use a cascade of mixes
- It works as long as untrusted mixes do not collaborate all together

Chaum-net

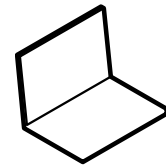
- Allow to send a sealed message via a cascade of mixes
- In an overlay, each participant has a private/public key pair
- Alice randomly chooses a few of them (e.g., 3) to be mixes
- Alice recursively encrypt the message with the public key of each mixes she selected

Chaum-net example

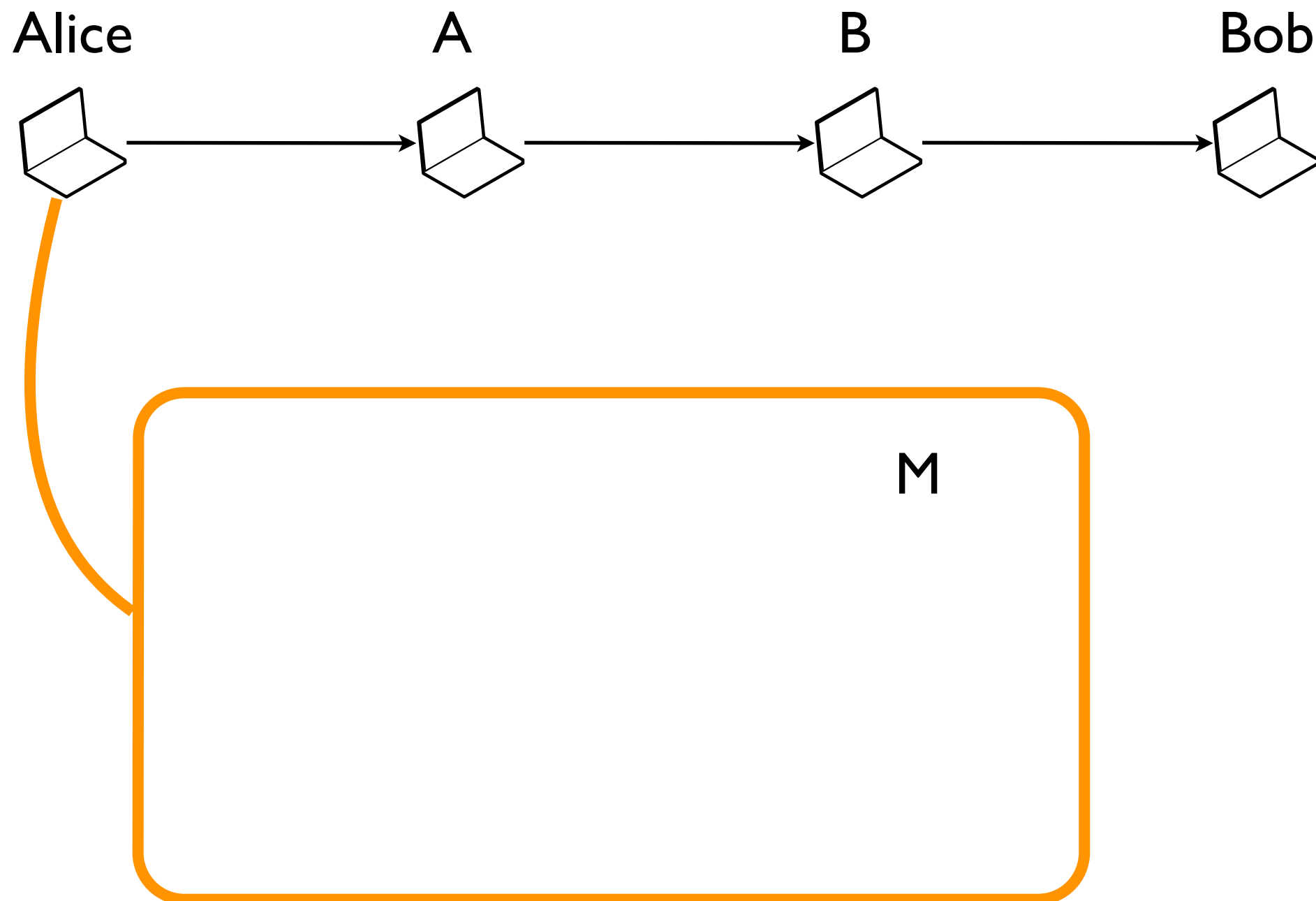
Alice



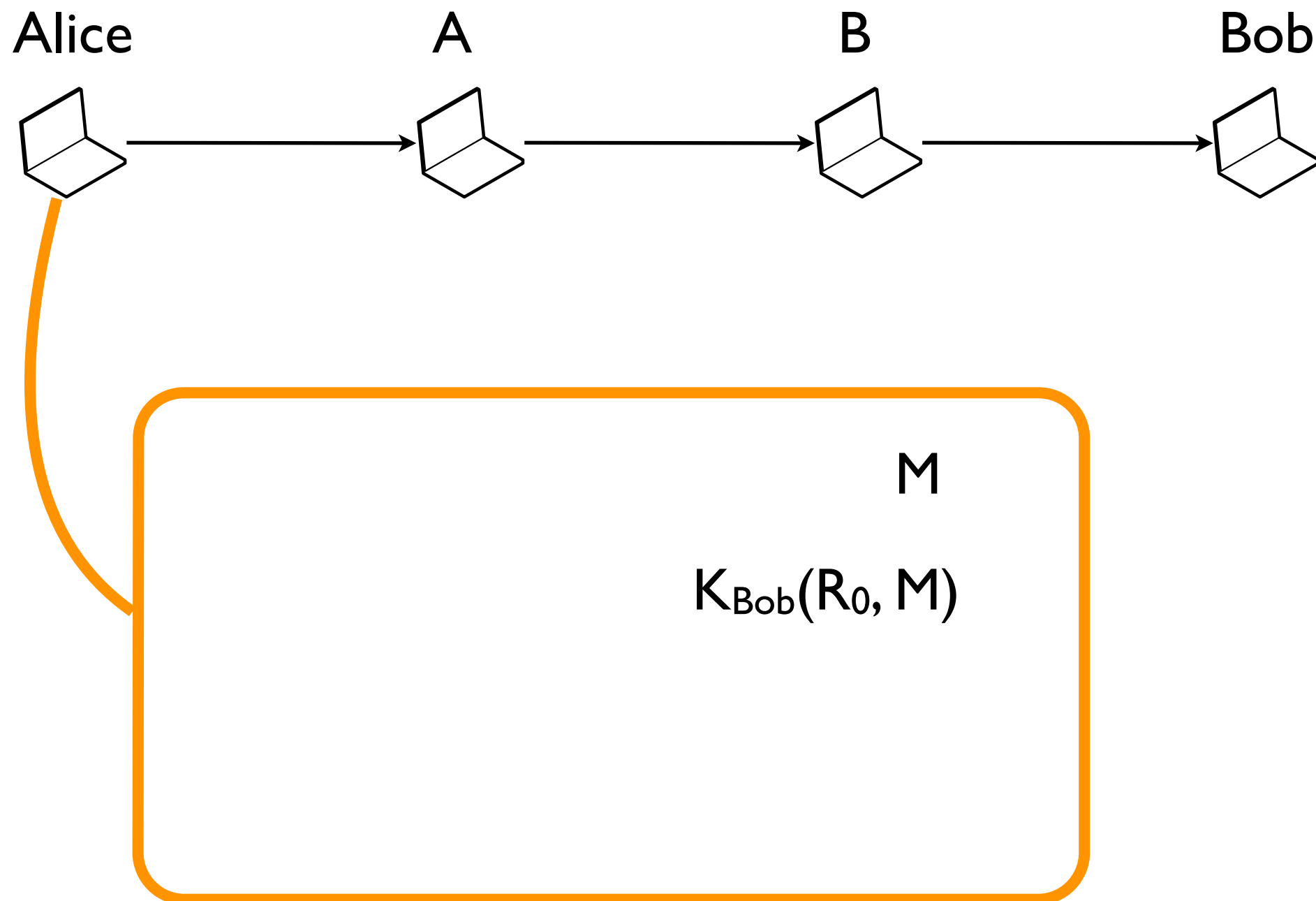
Bob



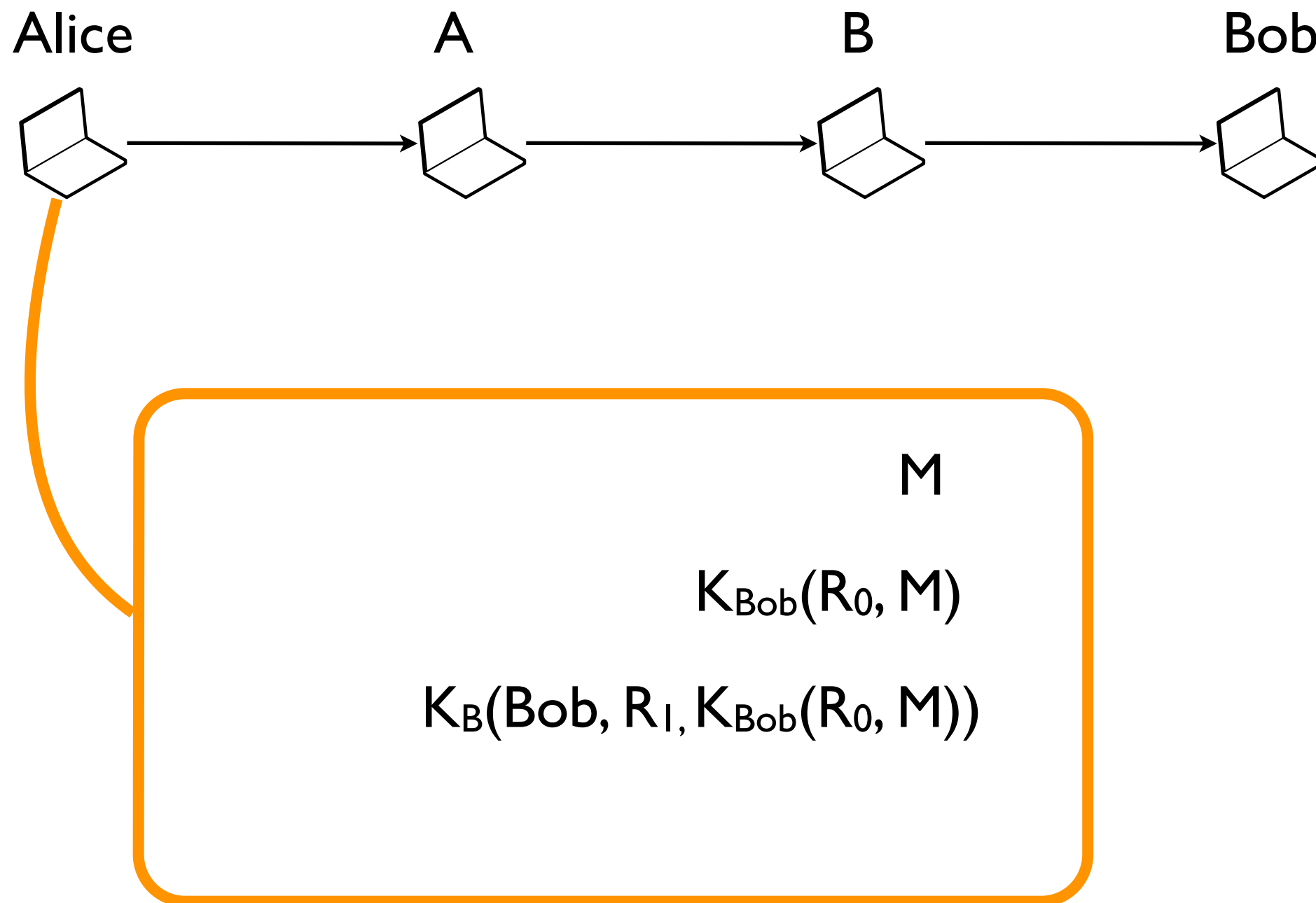
Chaum-net example



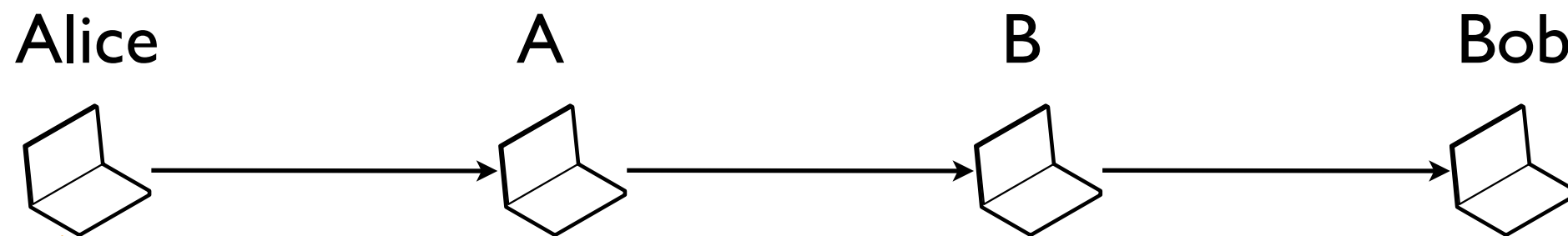
Chaum-net example



Chaum-net example



Chaum-net example



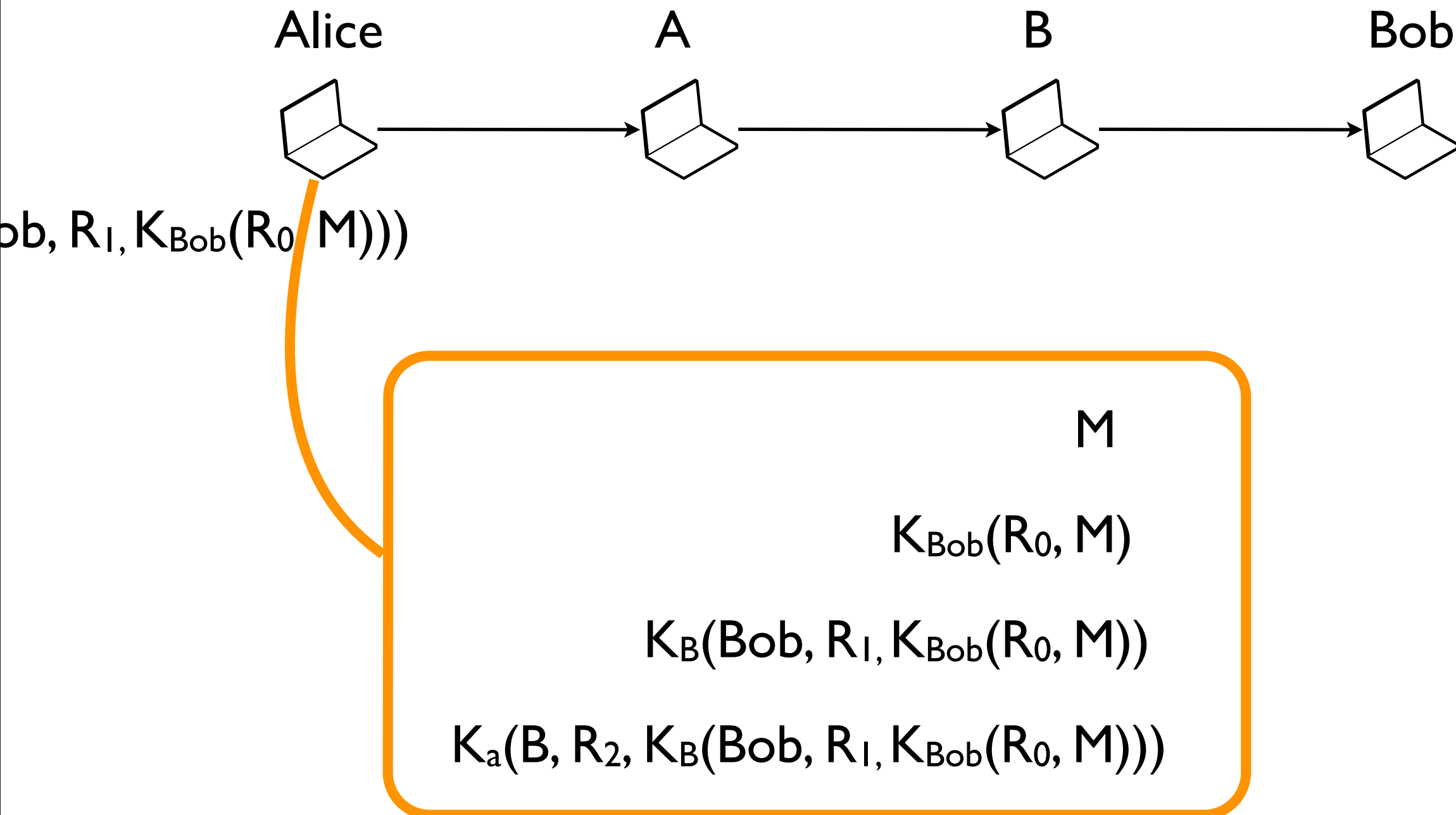
M

$K_{\text{Bob}}(R_0, M)$

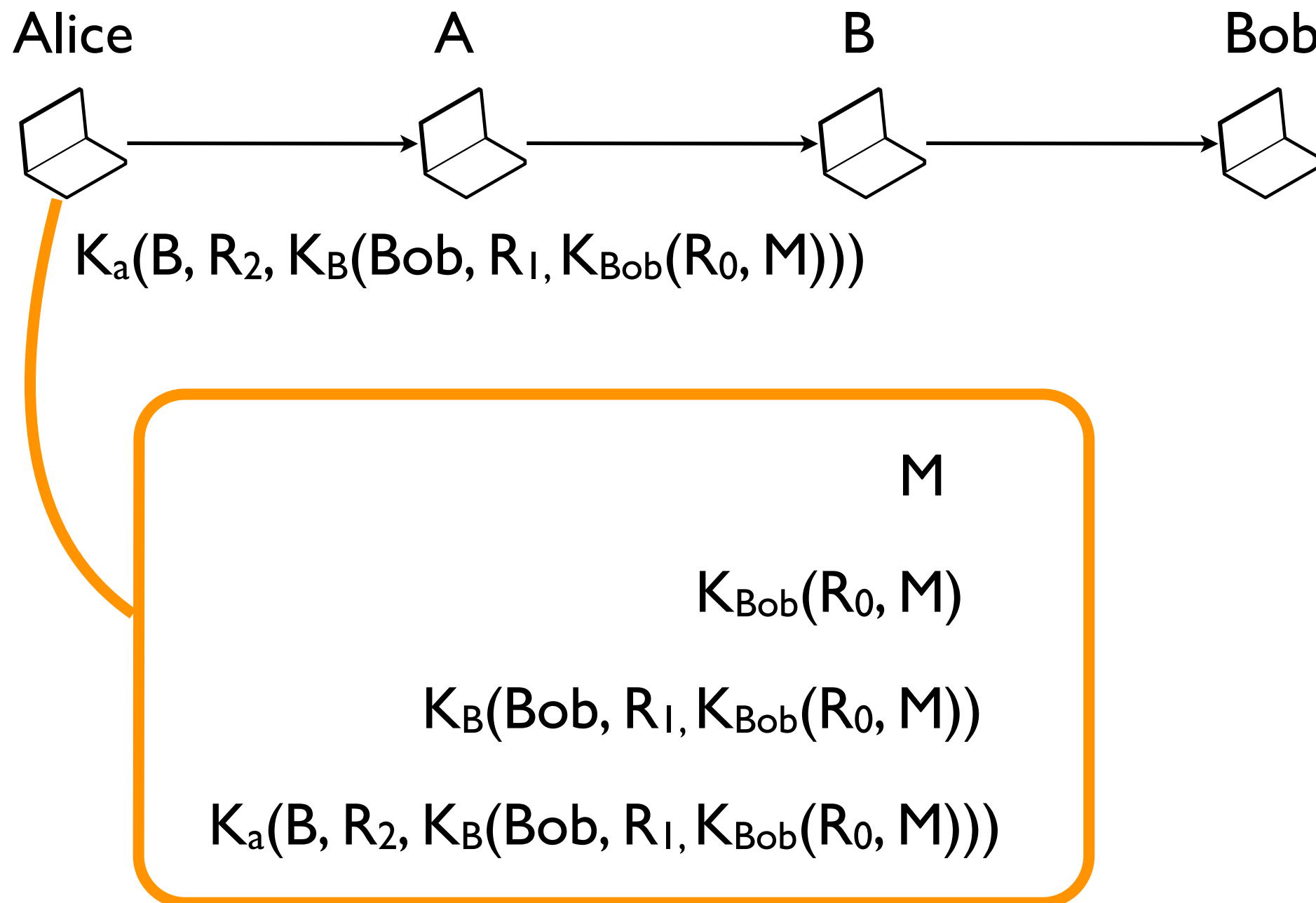
$K_B(\text{Bob}, R_1, K_{\text{Bob}}(R_0, M))$

$K_a(B, R_2, K_B(\text{Bob}, R_1, K_{\text{Bob}}(R_0, M)))$

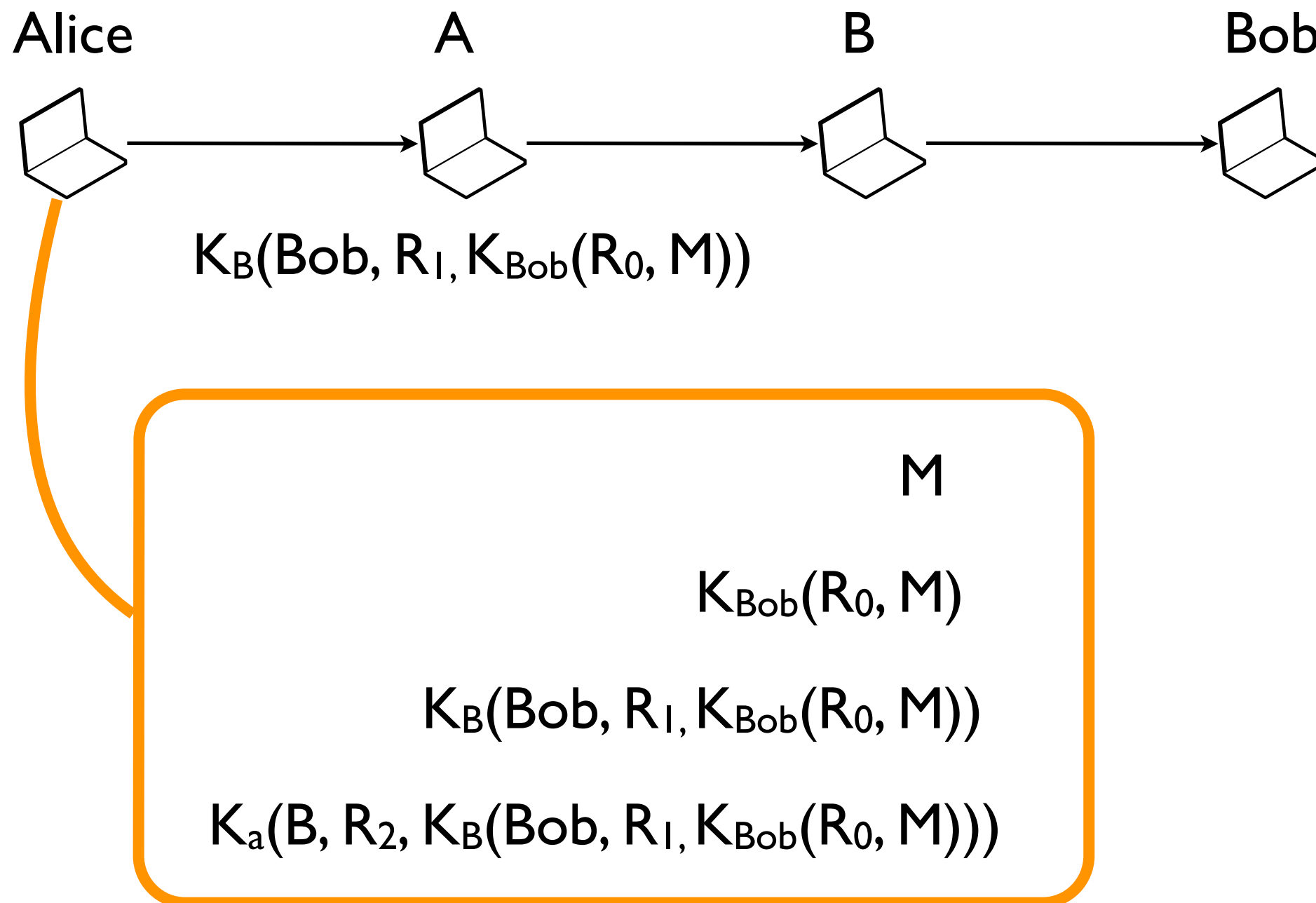
Chaum-net example



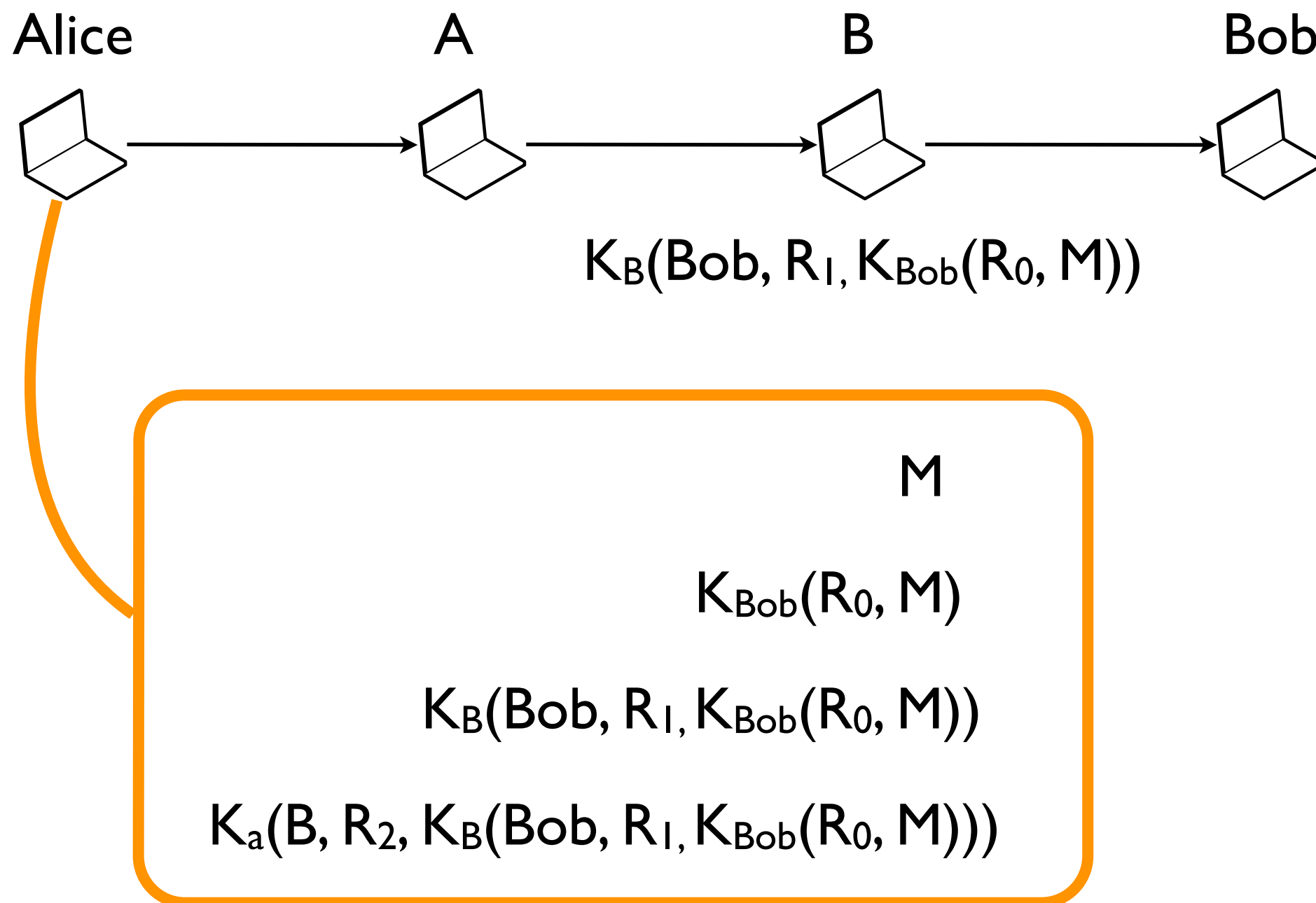
Chaum-net example



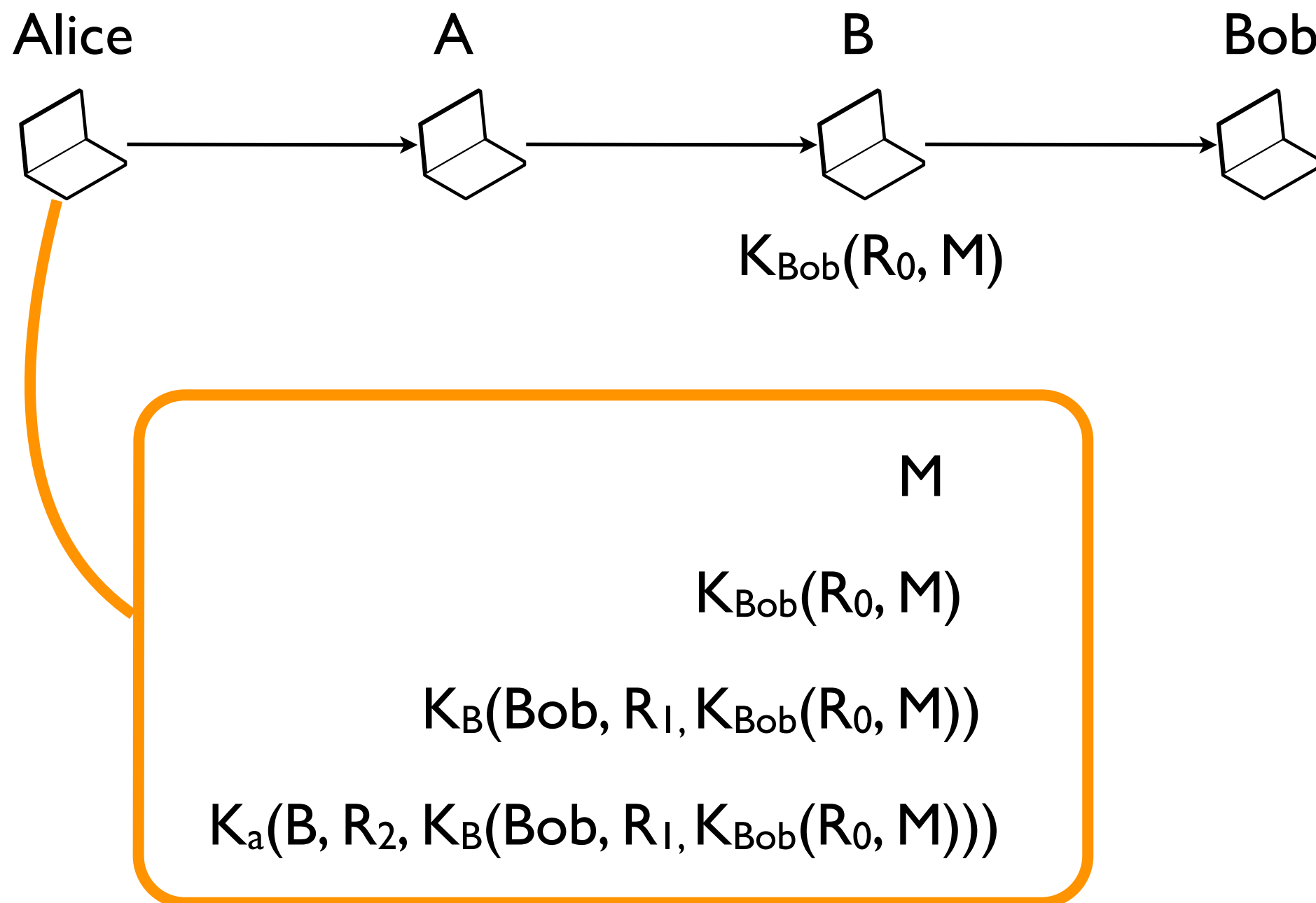
Chaum-net example



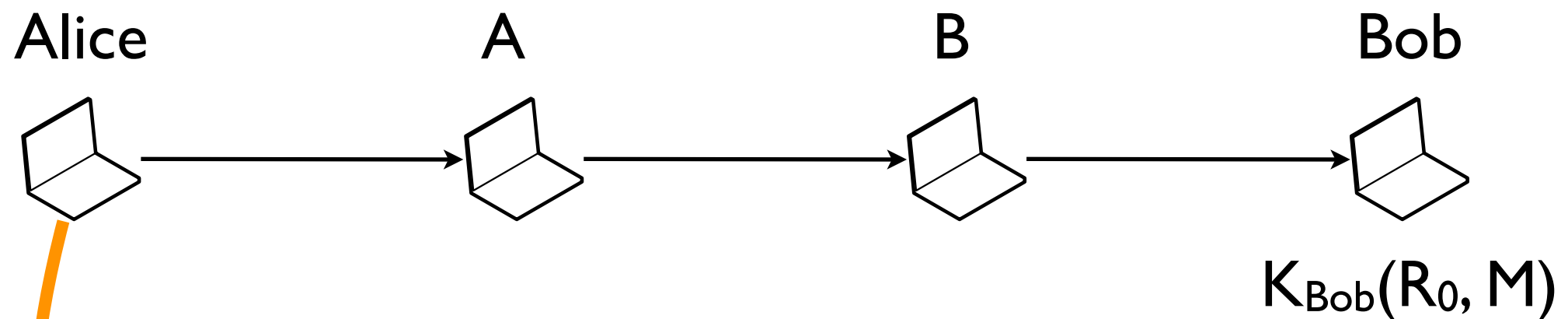
Chaum-net example



Chaum-net example

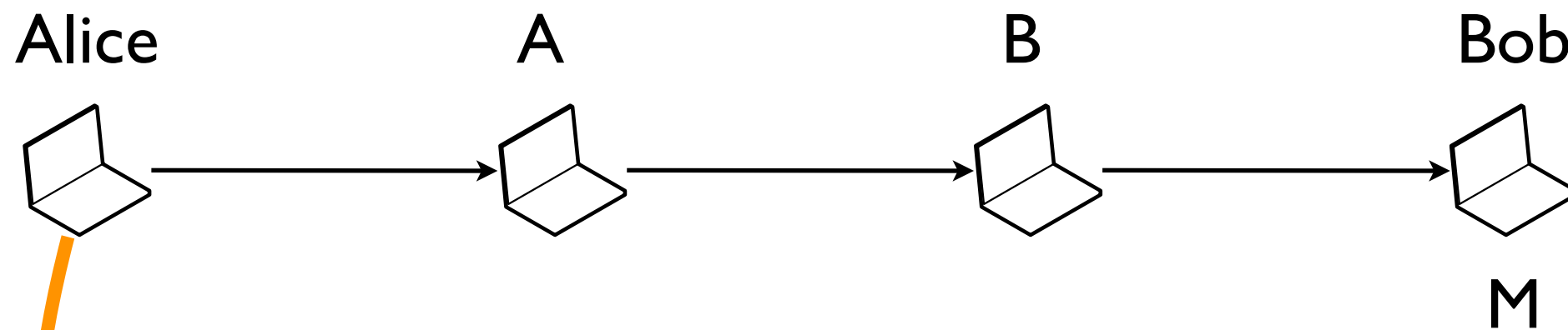


Chaum-net example



M
 $K_{\text{Bob}}(R_0, M)$
 $K_B(\text{Bob}, R_1, K_{\text{Bob}}(R_0, M))$
 $K_a(B, R_2, K_B(\text{Bob}, R_1, K_{\text{Bob}}(R_0, M)))$

Chaum-net example



M
 $K_{\text{Bob}}(R_0, M)$
 $K_B(\text{Bob}, R_1, K_{\text{Bob}}(R_0, M))$
 $K_a(B, R_2, K_B(\text{Bob}, R_1, K_{\text{Bob}}(R_0, M)))$

Chaum-net example

Alice

A

B

Bob

Cool, I am anonymous!

M

$K_{\text{Bob}}(R_0, M)$

$K_B(\text{Bob}, R_1, K_{\text{Bob}}(R_0, M))$

$K_a(B, R_2, K_B(\text{Bob}, R_1, K_{\text{Bob}}(R_0, M)))$

Chaum-net example

Alice

A

B

Bob

Are you sure?

M

$K_{\text{Bob}}(R_0, M)$

$K_B(\text{Bob}, R_1, K_{\text{Bob}}(R_0, M))$

$K_a(B, R_2, K_B(\text{Bob}, R_1, K_{\text{Bob}}(R_0, M)))$