

# Internet Security [1]

VU 184.216

## *TCP/IP Part 1/2*

Paolo Milani Comparetti

[pmilani@seclab.tuwien.ac.at](mailto:pmilani@seclab.tuwien.ac.at)

Clemens Kolbitsch

[ck@seclab.tuwien.ac.at](mailto:ck@seclab.tuwien.ac.at)

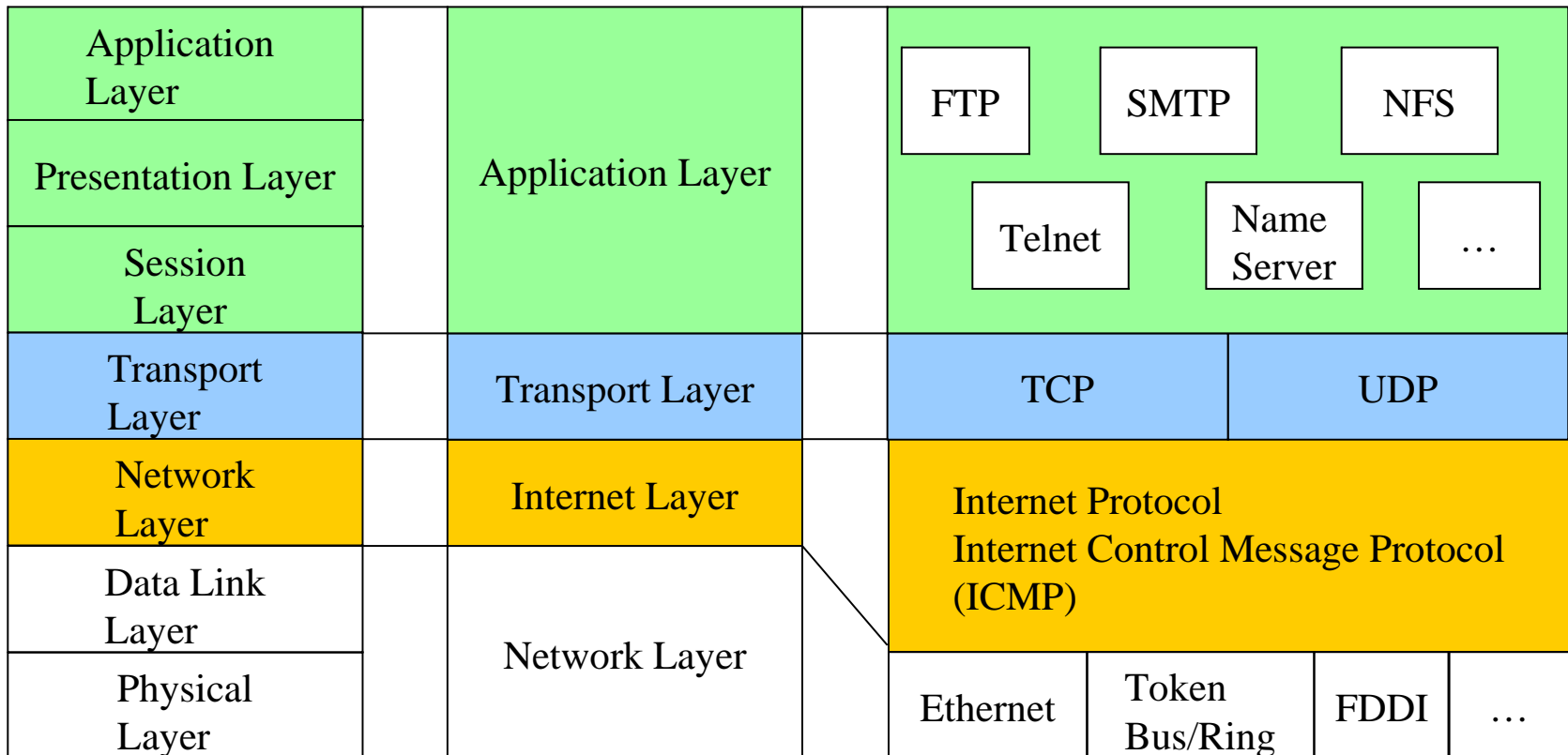
# News from the Lab

*Int. Secure Systems Lab  
Technical University Vienna*

- Registration web site is open
  - we had a down-time over the weekend, but the system is back up
  - registration open until 31.03
  - 1st challenge will start next week (24.03)
- This and the next lecture will give a quick overview of TCP/IP
  - focus on security-related aspects (attacks)
  - we will try to make everything comprehensible without prior knowledge
  - we suggest you take a networking/distributed systems class (if you haven't already, as listed in course prerequisites)

# Network Protocol Stack

*Int. Secure Systems Lab  
Technical University Vienna*

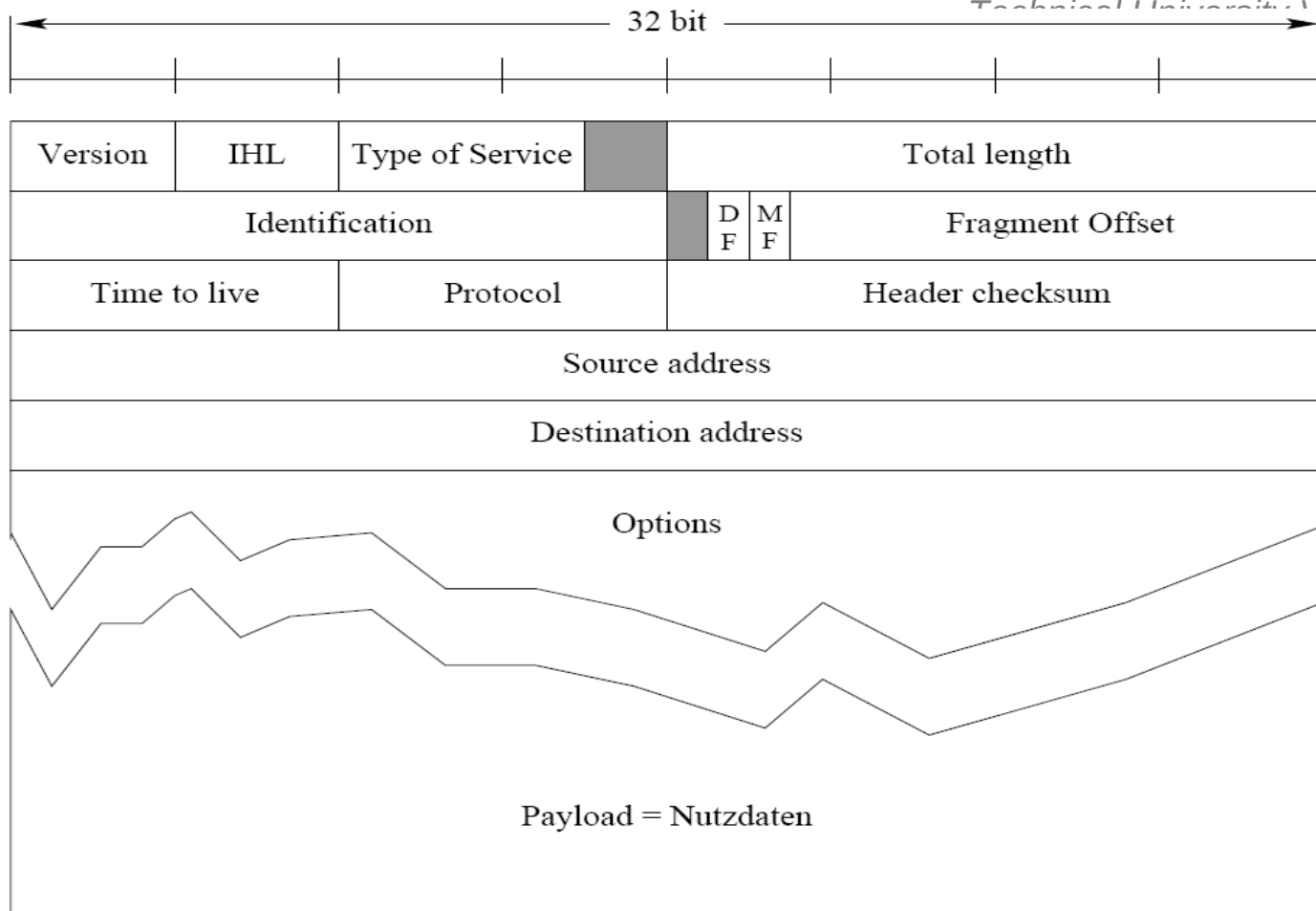


# Internet Protocol IP

*Int. Secure Systems Lab  
Technical University Vienna*

- IP address is 32-Bit Numbers (e.g. 128.130.2.3)
  - $2^{32}$  possible IP Addresses
- Limited (Local) Broadcast
  - not routed
- “Private” IP Addresses
  - 127.0.0.0 – 127.255.255.255 (callback)
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 172.17.255.255
  - 192.168.0.0 – 192.168.255.255

# IP Datagram



# Ethernet

*Int. Secure Systems Lab  
Technical University Vienna*

dest (48 bits)	src (48 bits)	type (16)	data (46-1500)	CRC (32)
----------------	---------------	-----------	----------------	----------

0x0800	IP Datagram
--------	-------------

## In Reality:

```
⊕ Frame 3 (66 bytes on wire, 66 bytes captured)
⊖ Ethernet II, Src: IntelCor_87:a1:eb (00:1d:e0:87:a1:eb), Dst: 00:22:43:42:78:91 (00:22:43:42:78:91)
  ⊕ Destination: 00:22:43:42:78:91 (00:22:43:42:78:91)
  ⊕ Source: IntelCor_87:a1:eb (00:1d:e0:87:a1:eb)
    Type: IP (0x0800)
0000  00 22 43 42 78 91 00 1d  e0 87 a1 eb 08 00 45 00  . "CBx... ..E.
0010  00 34 26 80 40 00 80 06  4c 5d 80 83 c3 ef 80 83  .4&.@... L].....
0020  c2 f0 60 e0 9e 79 c1 09  d7 8b 24 4f f9 8d 80 10  ..`..y.. ..$o....
0030  00 3f 0f ed 00 00 01 01  08 0a 00 4c 99 52 00 56  .?..... ...L.R.V
0040  8e e9  ..
```

# Direct IP delivery

*Int. Secure Systems Lab  
Technical University Vienna*

- hosts directly connected on a local network
- Problem:
  - Link layer uses 48 bit Ethernet addresses
  - network layer uses 32 bit IP addresses
  - we want to send an IP datagram
  - but we only can use the Link Layer to (really) do this
- Encapsulate IP datagram in Ethernet datagram
  - need to map destination IP address to Ethernet address

# Address Resolution Protocol (ARP)

*Int. Secure Systems Lab  
Technical University Vienna*

- Service at the link-level, RFC 826
  - maps network-addresses to link-level addresses
- Host A wants to know the hardware address associated with IP address of host B
  - A broadcasts ARP message on physical link layer including its own mapping
  - B answers A with ARP answer message
- Mappings are cached: `arp -a` shows mapping

# ARP

*Int. Secure Systems Lab  
Technical University Vienna*

dest (6 byte)	src (6 byte)	type (2)	data	CRC (4)
---------------	--------------	----------	------	---------

0x0800	IP Datagram
--------	-------------

<b>0x0806</b>	<b>ARP</b>
---------------	------------

# ARP Message Format

*Int. Secure Systems Lab  
Technical University Vienna*

hardware type (2 byte)		protocol type (2 byte)
hw.adr.size (1 byte)	prot. adr. size (1 byte)	opcode (2 byte)
sender Ethernet address (6 byte)		
sender IP address (4 byte)		
target Ethernet address (6 byte)		
target IP address (4 byte)		

# RARP

- RARP (Reverse Address Resolution Protocol)
- maps link-level addresses to network-addresses
  - for diskless stations to obtain their own IP address
  - Service at the link-level, RFC 903
- Host A wants to know its IP address (which is IP\_A)
  - A broadcasts RARP message on physical link
  - RARP server answers with RARP answer containing IP\_A
- Now mostly replaced by DHCP

# Reverse ARP (RARP)

*Int. Secure Systems Lab  
Technical University Vienna*

dest (6 byte)	src (6 byte)	type (2)	data	CRC (4)
---------------	--------------	----------	------	---------

0x0800	IP Datagram
--------	-------------

<b>0x0806</b>	<b>ARP</b>
---------------	------------

<b>0x8035</b>	<b>RARP</b>
---------------	-------------

# (R)ARP

- use same message format
- contain:
  - types and address sizes of hardware and protocol
  - type of message (=opcode, (R)ARP request/reply)
  - link-level and network level addresses of sender and target.
- depending on type, different fields are "empty"
  - ARP: target link level address
  - RARP: everything except source link-level address

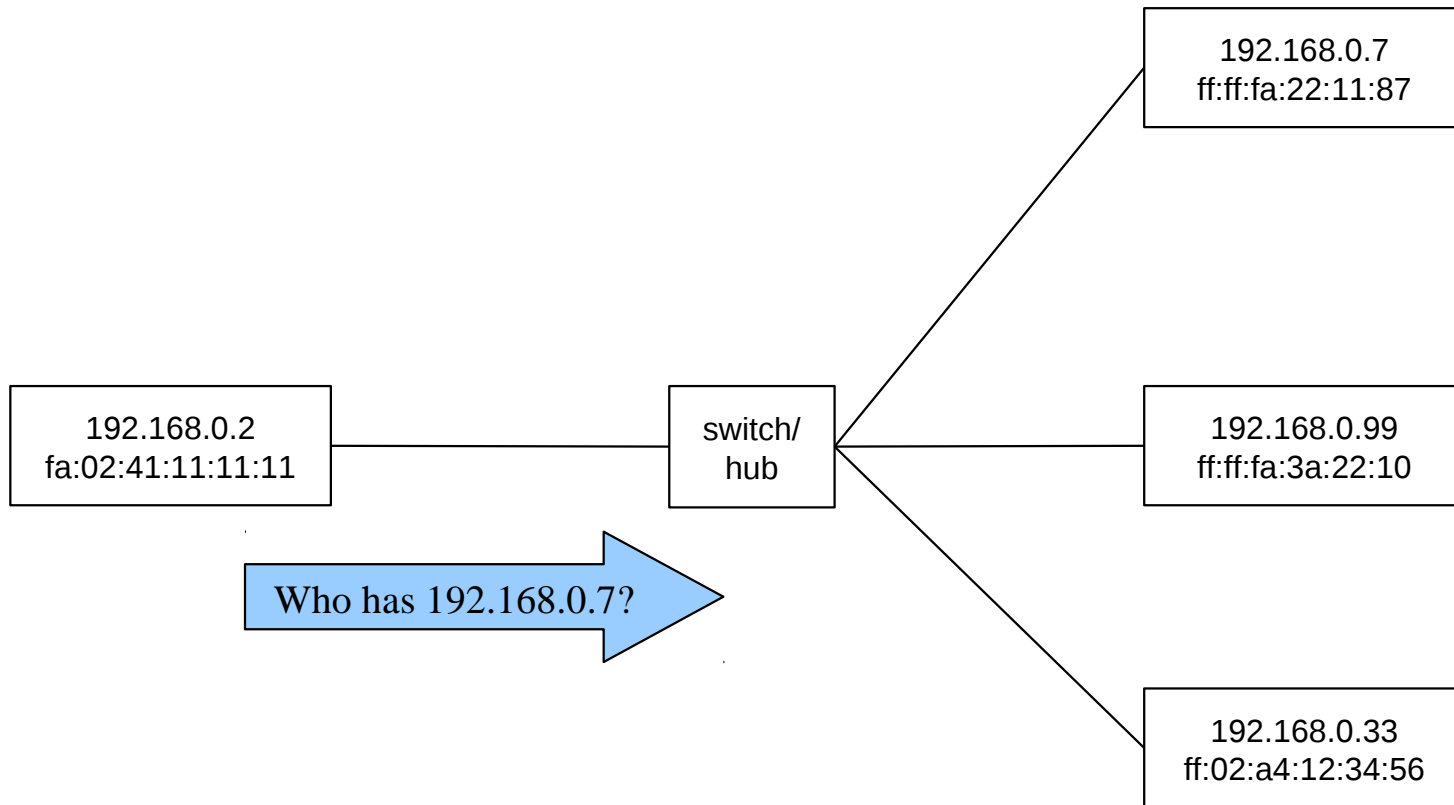
# Sending an IP Packet

*Int. Secure Systems Lab  
Technical University Vienna*

- Assume host A wants to send an IP packet to host B and that all ARP caches are empty
- A sends (broadcast) ARP request for IP-B
  - what is the Ethernet address associated with IP-B?
  - ARP cache in B is filled with mapping for IP-A
- B sends ARP reply to A
  - my Ethernet address is ...!
  - ARP cache on A is filled with mapping for IP-B
- A sends encapsulated IP datagram on link level to B

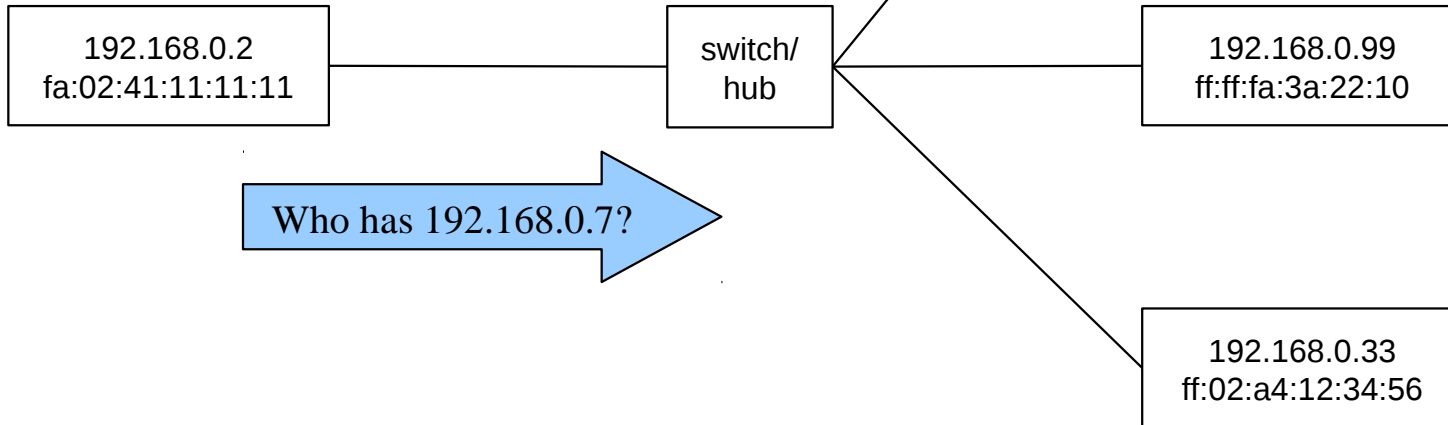
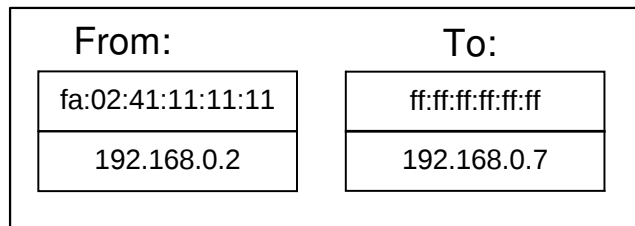
# Direct IP delivery

Int. Secure Systems Lab  
Technical University Vienna



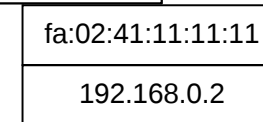
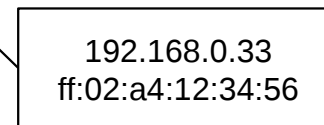
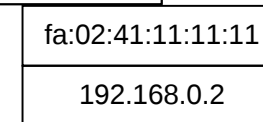
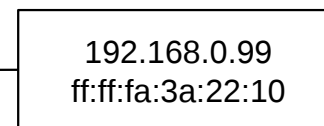
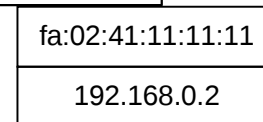
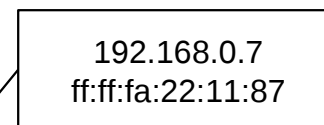
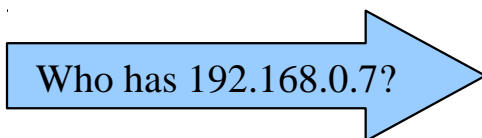
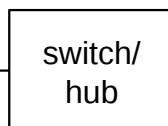
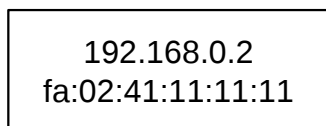
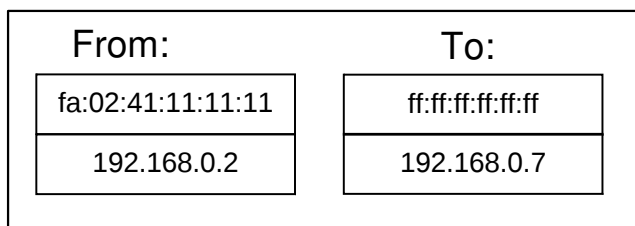
# Direct IP delivery

## ARP Request

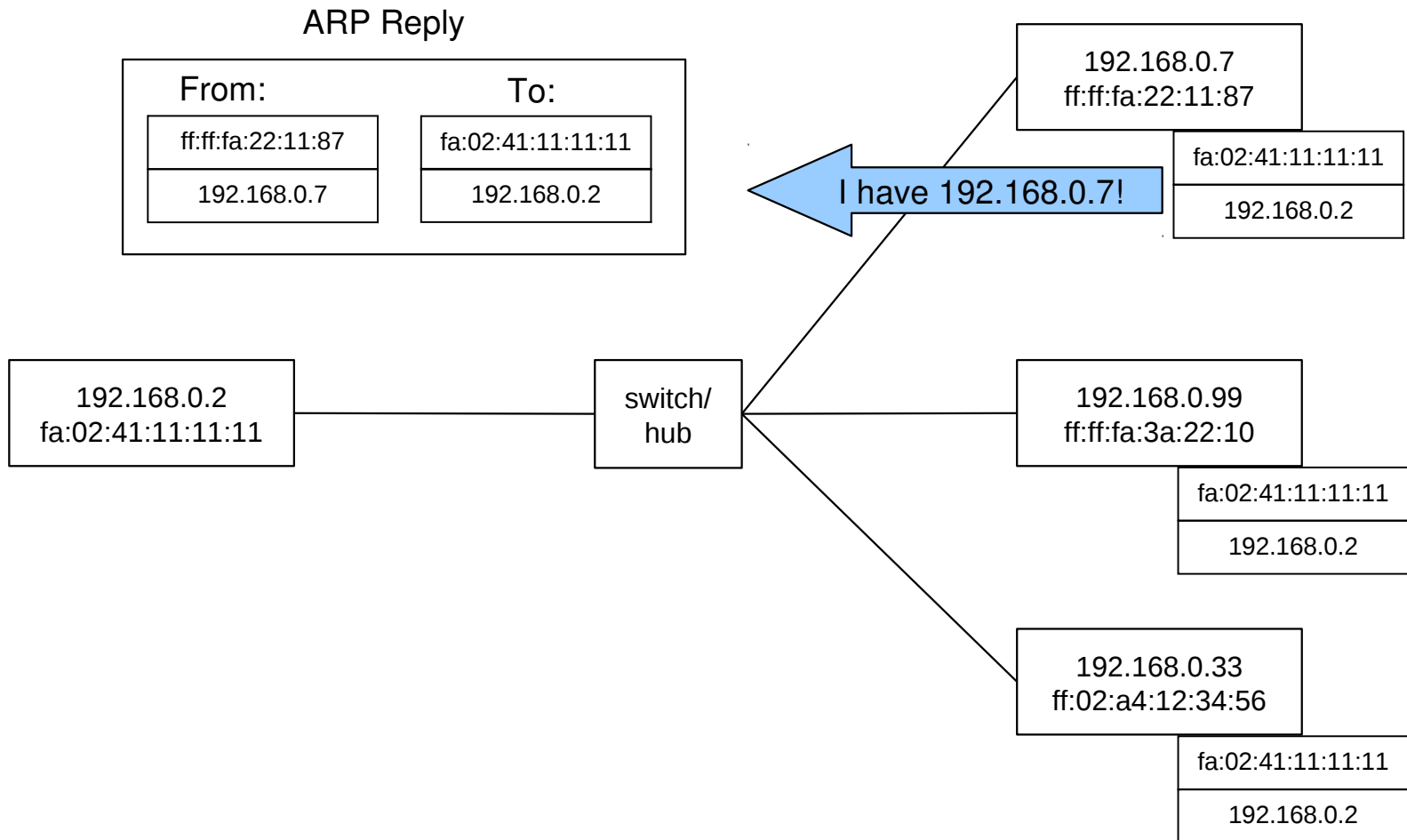


# Direct IP delivery

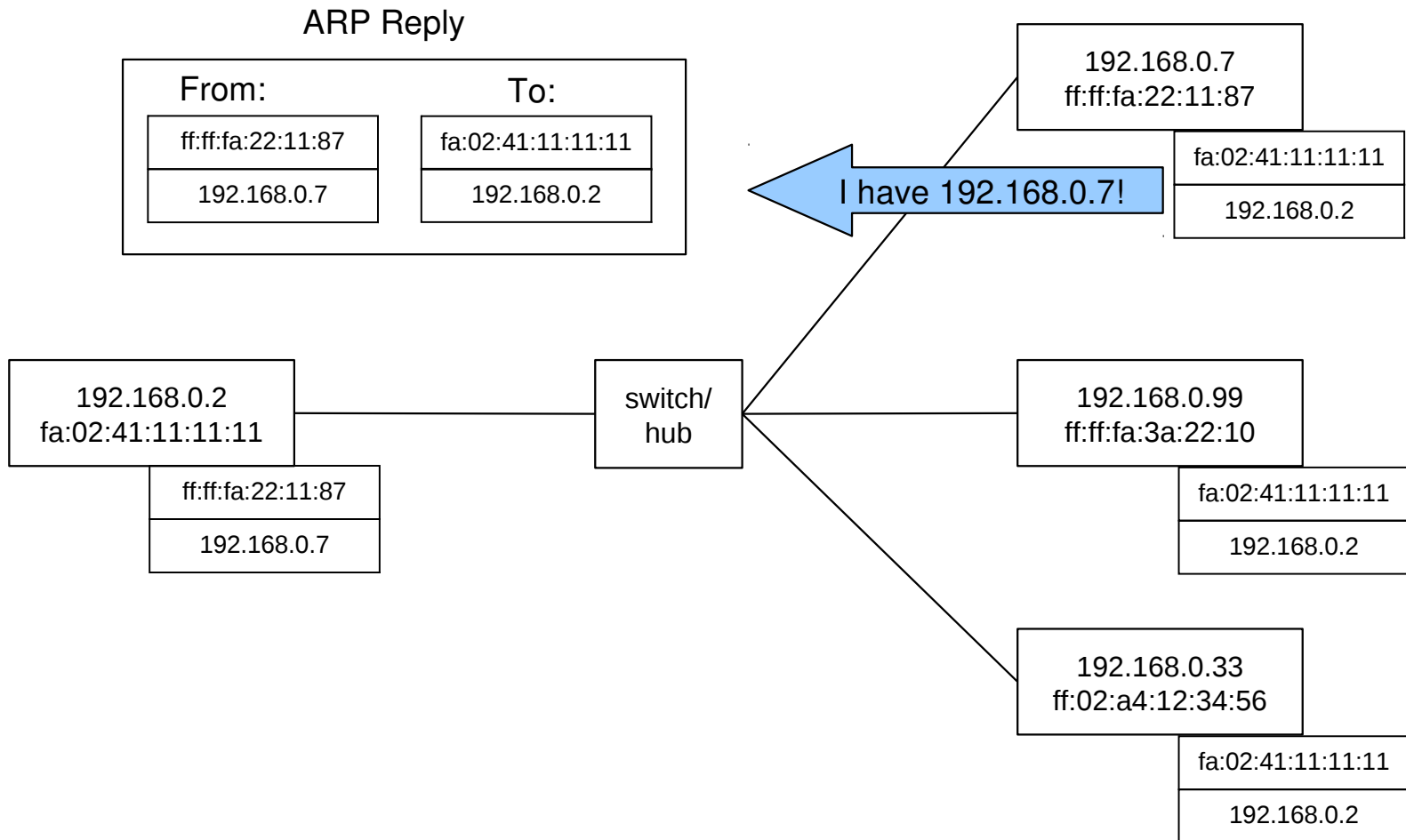
## ARP Request



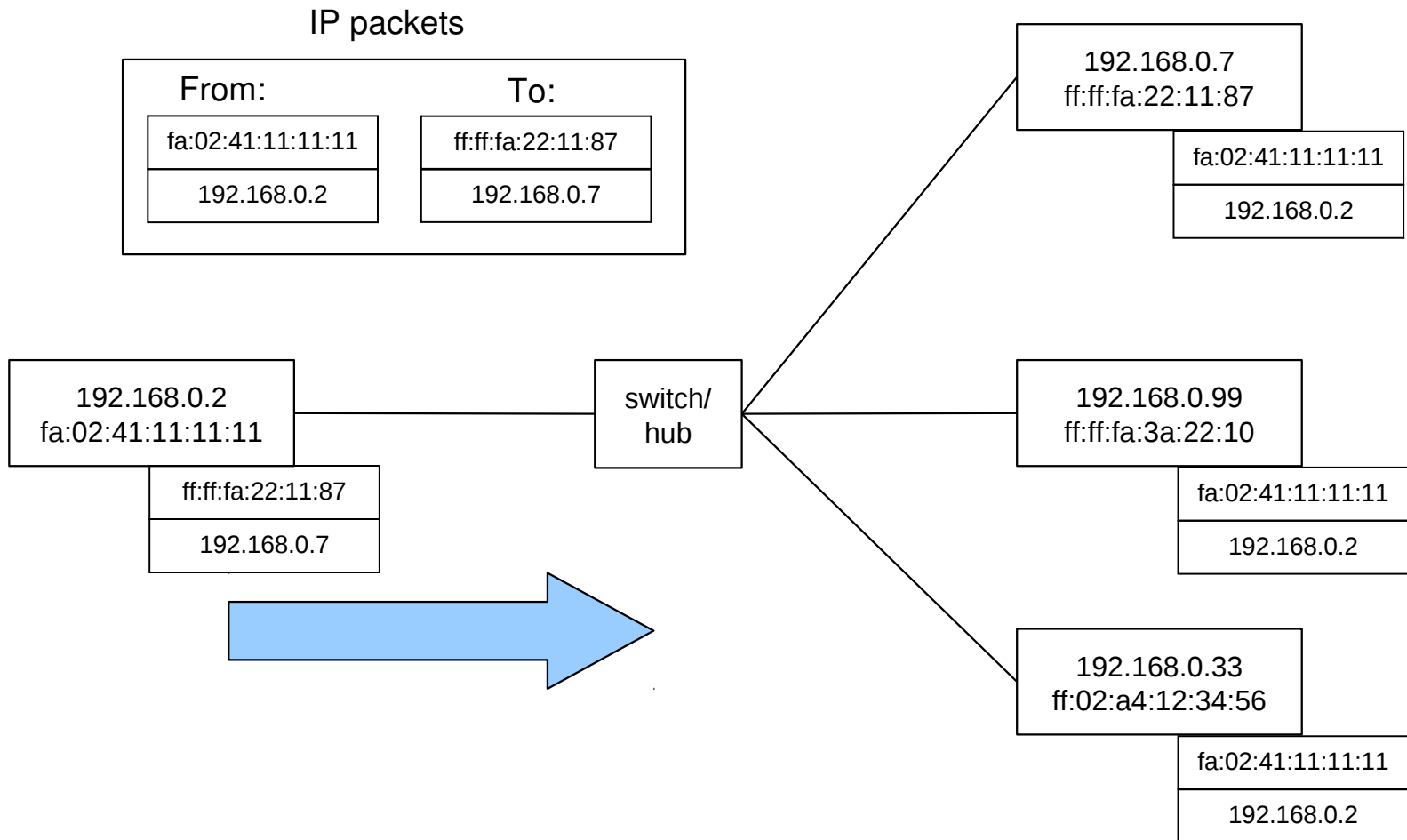
# Direct IP delivery



# Direct IP delivery



# Direct IP delivery



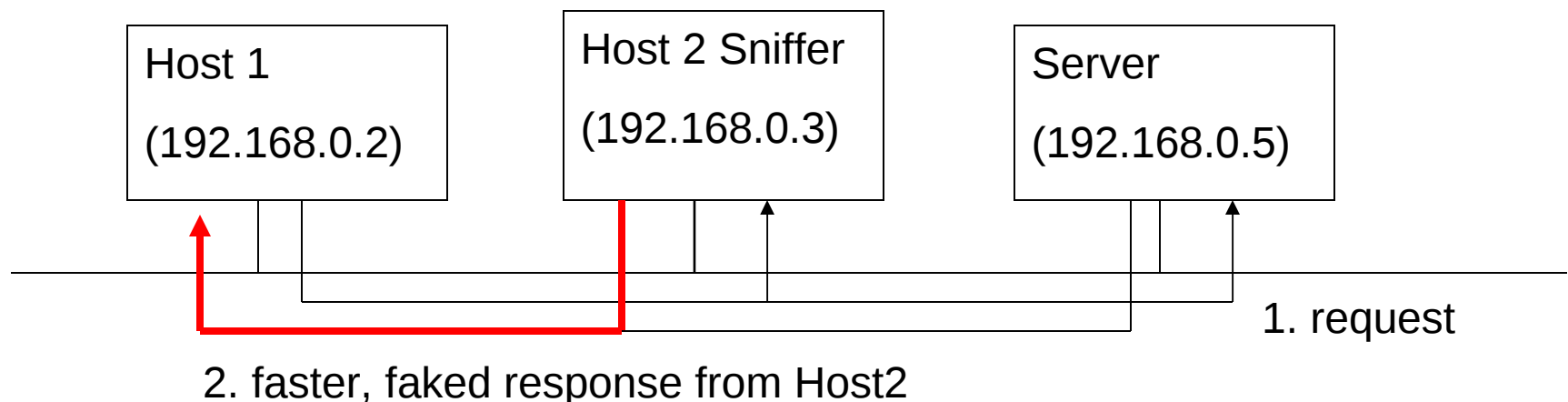
# LAN Attacks

*Int. Secure Systems Lab  
Technical University Vienna*

- Goals:
  - Information Recovery
  - Impersonate Host
  - Tamper with delivery mechanisms
- Methods:
  - Sniffing
  - IP Spoofing
  - ARP attacks

# IP Spoofing

- Impersonating another host by sending a datagram with a faked IP-address
  - IP addresses are NOT authenticated
  - used to impersonate sources of security critical info
  - address-based authentication
    - RPC, DNS



# IP Spoofing

*Int. Secure Systems Lab  
Technical University Vienna*

- How can you do it on your own?
- open a RAW socket
  - `socket(AF_INET, SOCK_RAW, IPPROTO_RAW)`
- craft the packet
  - with faked IP address
  - including all headers with all attributes set correctly
  - including data
  - including checksums
  - send the packet using the RAW socket

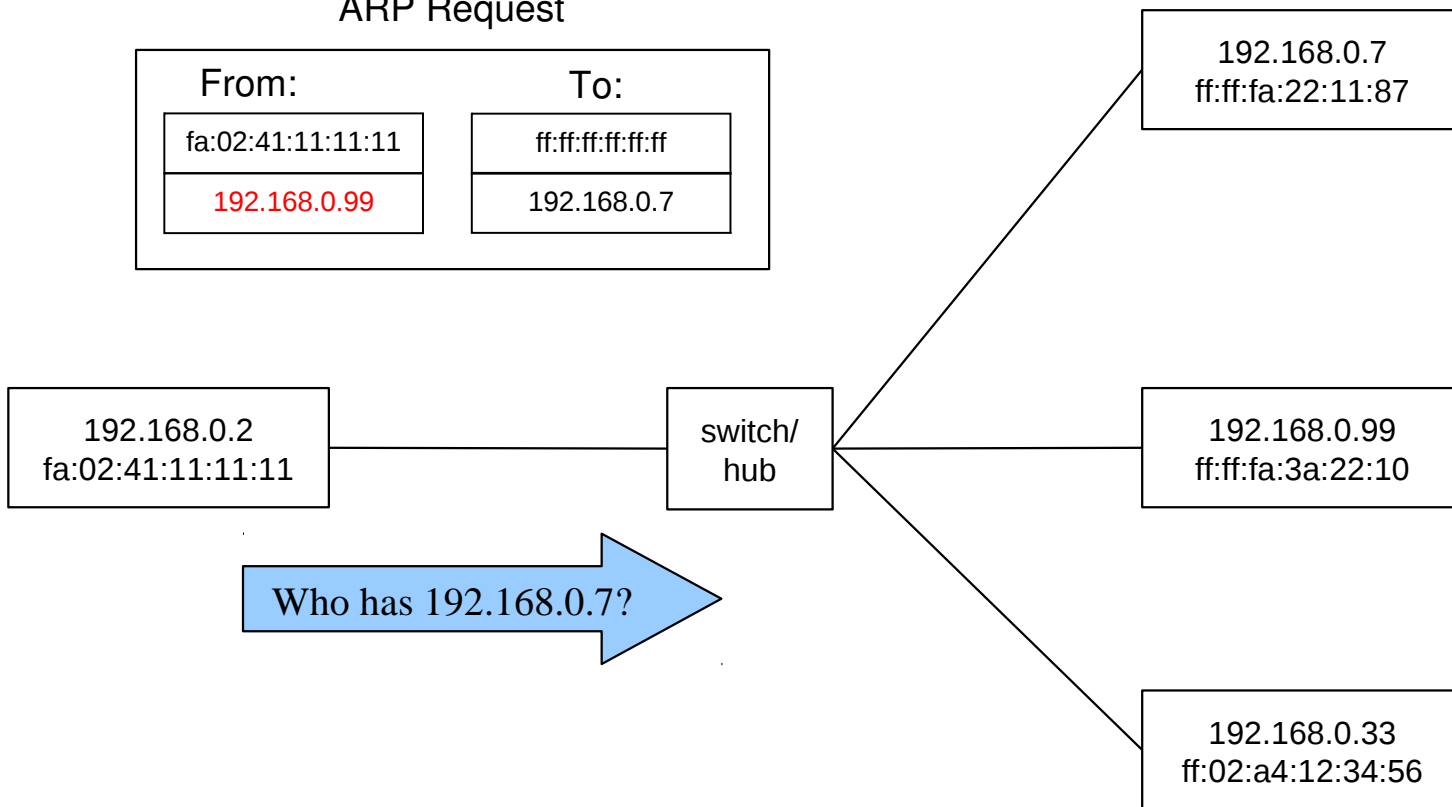
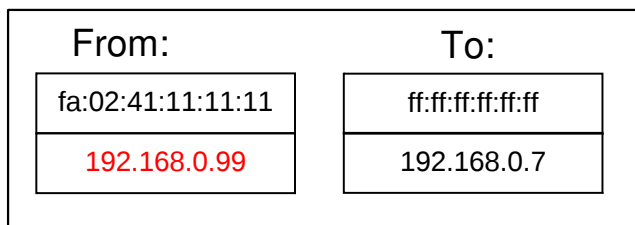
# ARP Poisoning

*Int. Secure Systems Lab  
Technical University Vienna*

- ARP does not provide any means of authentication
- Racing against the queried host is possible
  - provide false IP address/link-level address mapping
- Fake ARP queries
  - used to store wrong ARP mappings in a host cache
- Both can result in a redirection of traffic to the attacker
  - ARP messages are sent continuously to have caches keep the faked entries

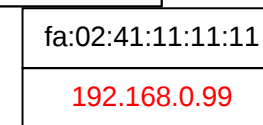
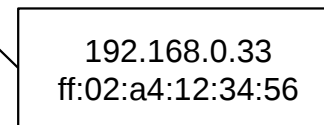
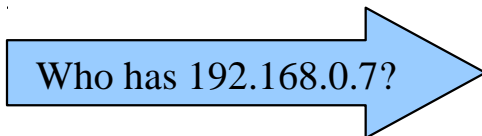
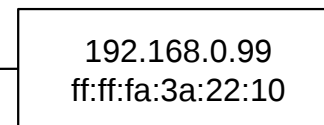
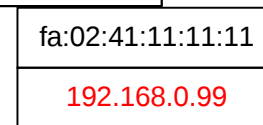
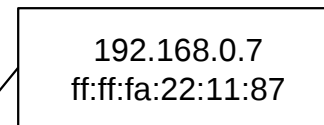
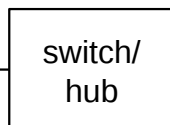
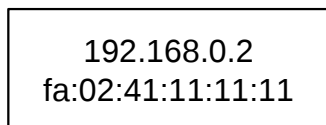
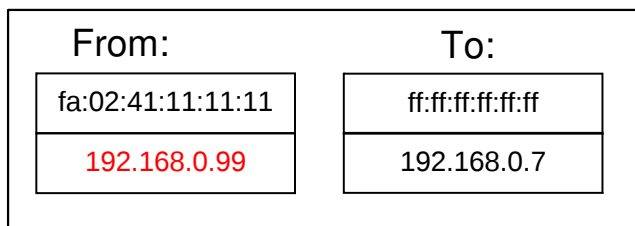
# ARP Poisoning

## ARP Request

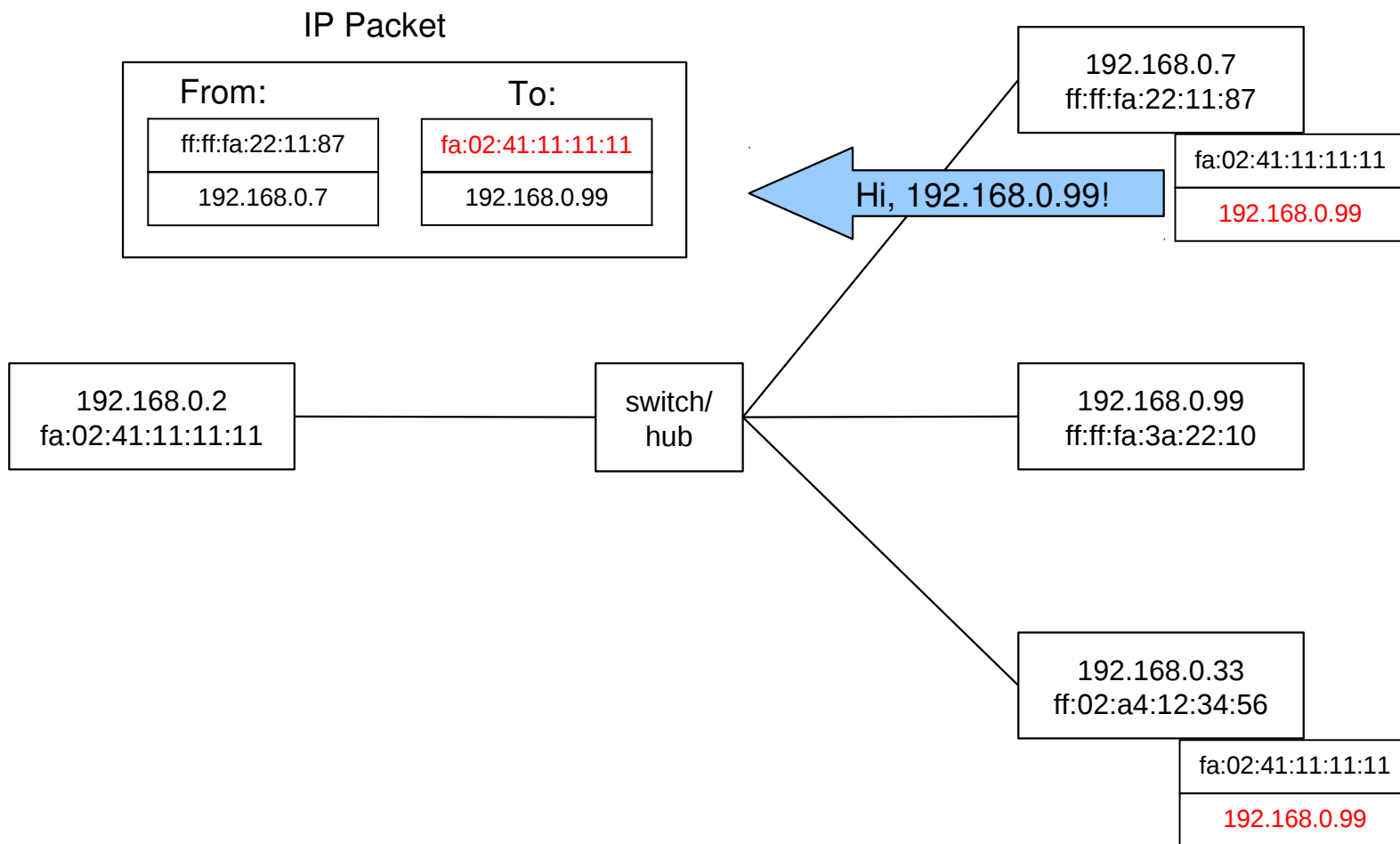


# ARP Poisoning

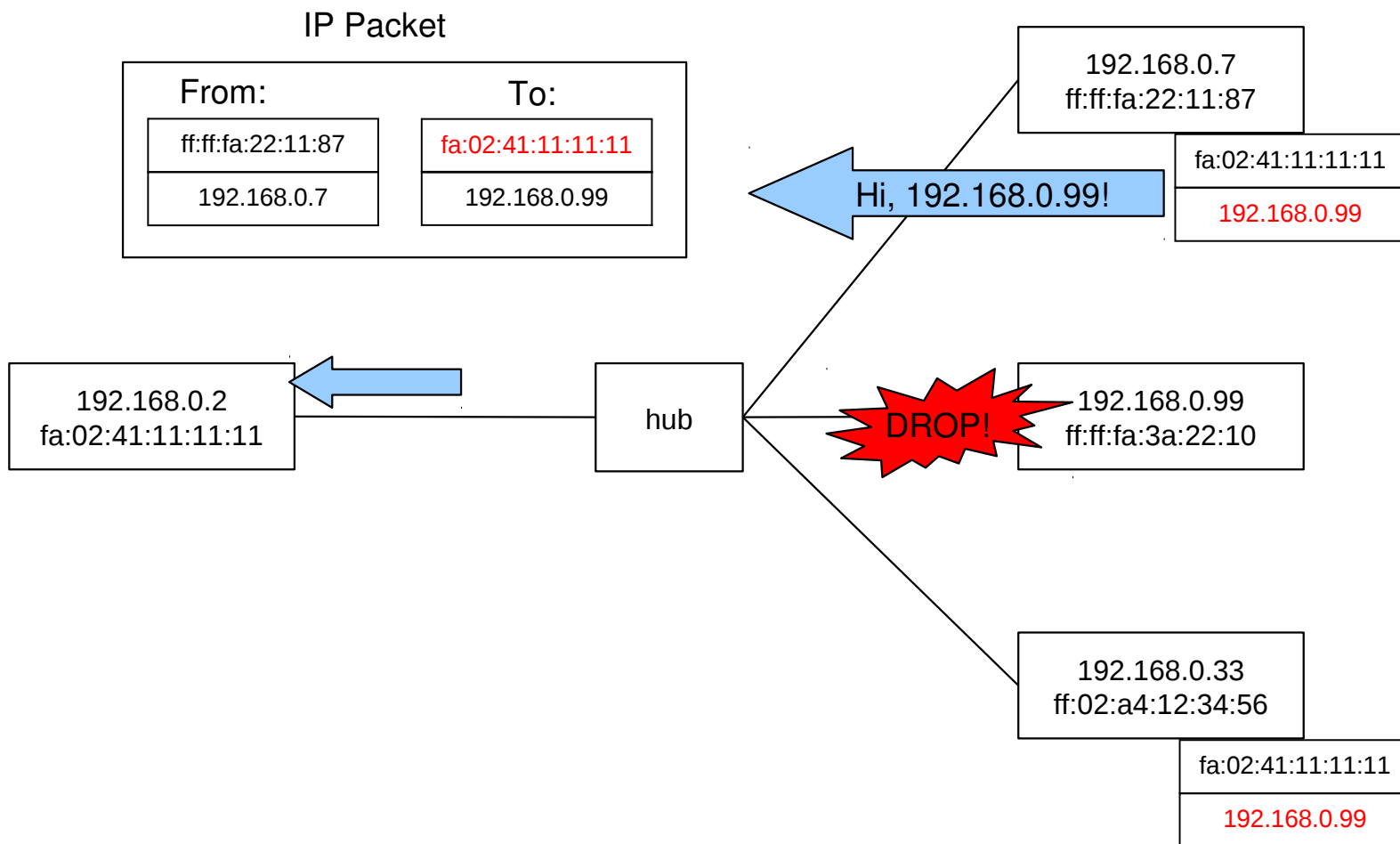
## ARP Request



# ARP Poisoning



# ARP Poisoning

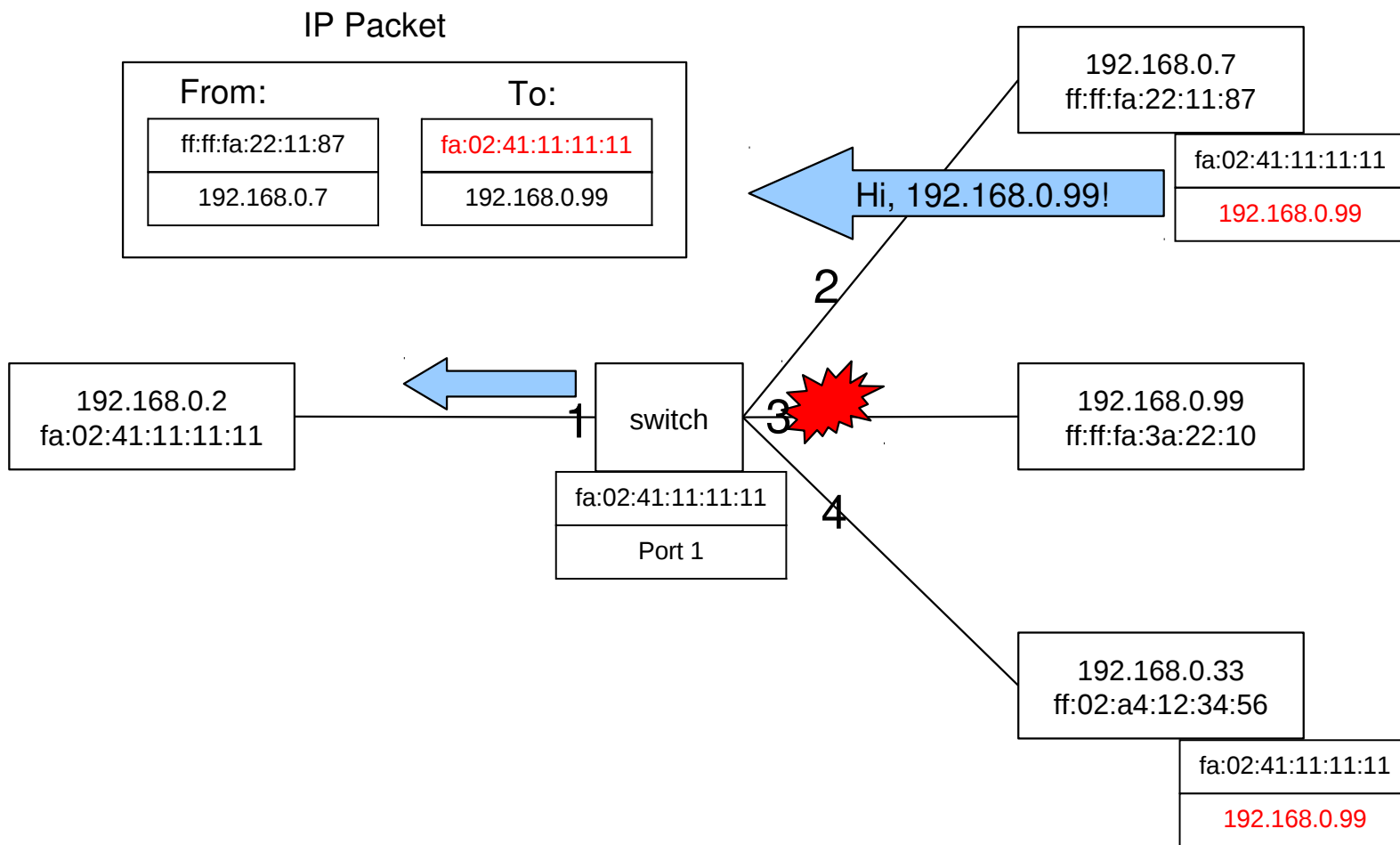


# Hub vs Switch

*Int. Secure Systems Lab  
Technical University Vienna*

- Hub is a physical layer device
  - has no address
  - forwards ALL incoming packets to all other ports
- Switch is a link-layer device
  - has a MAC address for each port
  - forwards incoming broadcast packets to all ports
  - keeps track of which Ethernet addresses can be reached through which ports

# ARP Poisoning



# ARP Poisoning: Applications

*Int. Secure Systems Lab  
Technical University Vienna*

- can be used for Man-in-the-Middle attack (MITM)
  - impersonate A with B, and B with A
  - sniff on a switched network
  - filter (modify) traffic
- can be used for Denial-of-Service (DoS):
  - map target IP to non-existent MAC address
- can target gateway
  - impersonate gateway to filter ALL the traffic
  - map gateway IP to non-existent MAC to drop all outgoing traffic
- can be targeted at a single host
  - destination Ethernet address specified (instead of broadcast)

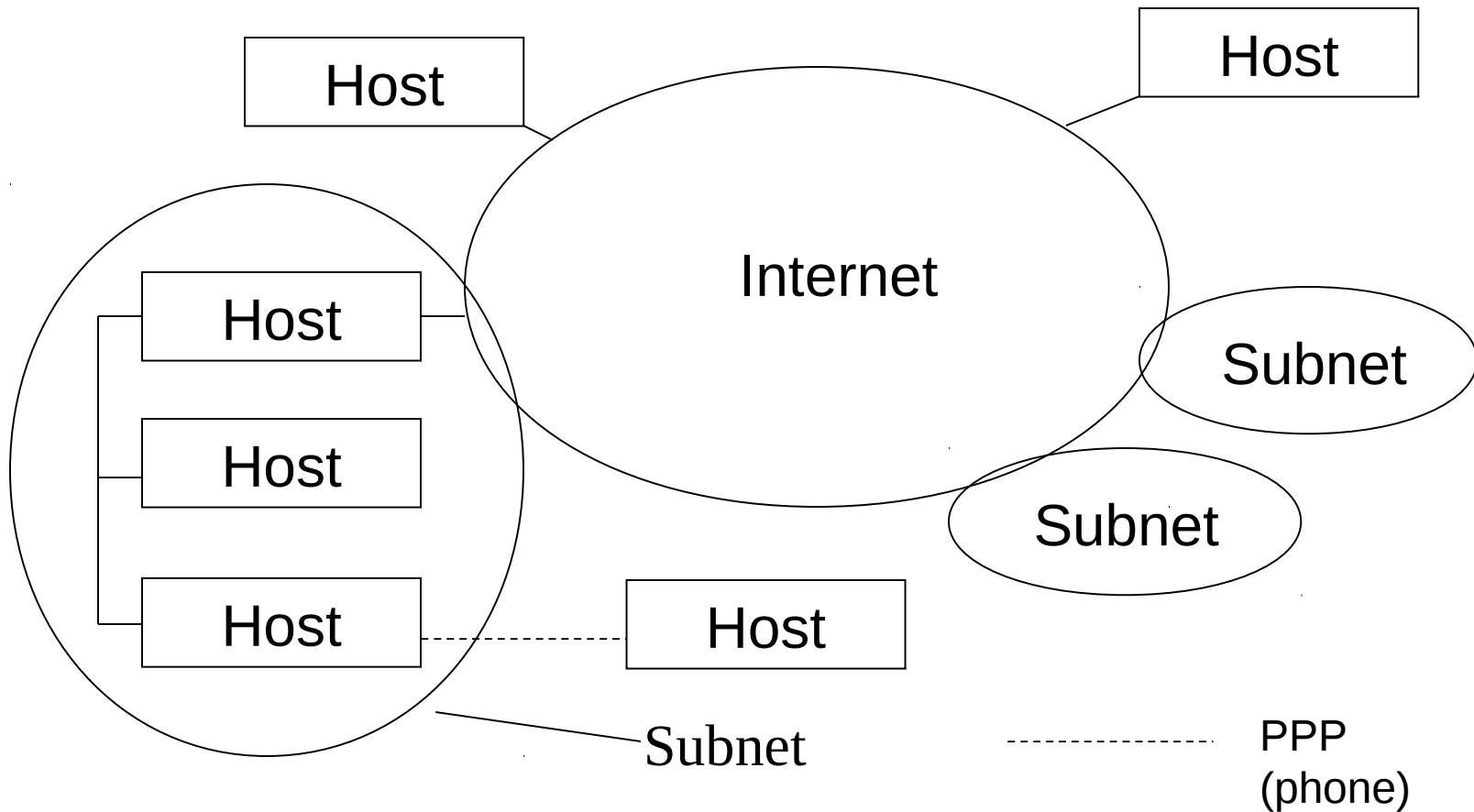
# Basic Networking Tools

*Int. Secure Systems Lab  
Technical University Vienna*

- ... everyone should know (do man <toolname> on UNIX/Linux)
- arp
  - service program for the ARP service
- ping
  - check whether a host is alive
- tcpdump
  - check what is going on on the net down to the packet level
- Ethereal / Wireshark
  - check what is going on on the net connection tracing, GUI
- nslookup / dig / host
  - DNS resolving

# The Internet

Int. Secure Systems Lab  
Technical University Vienna



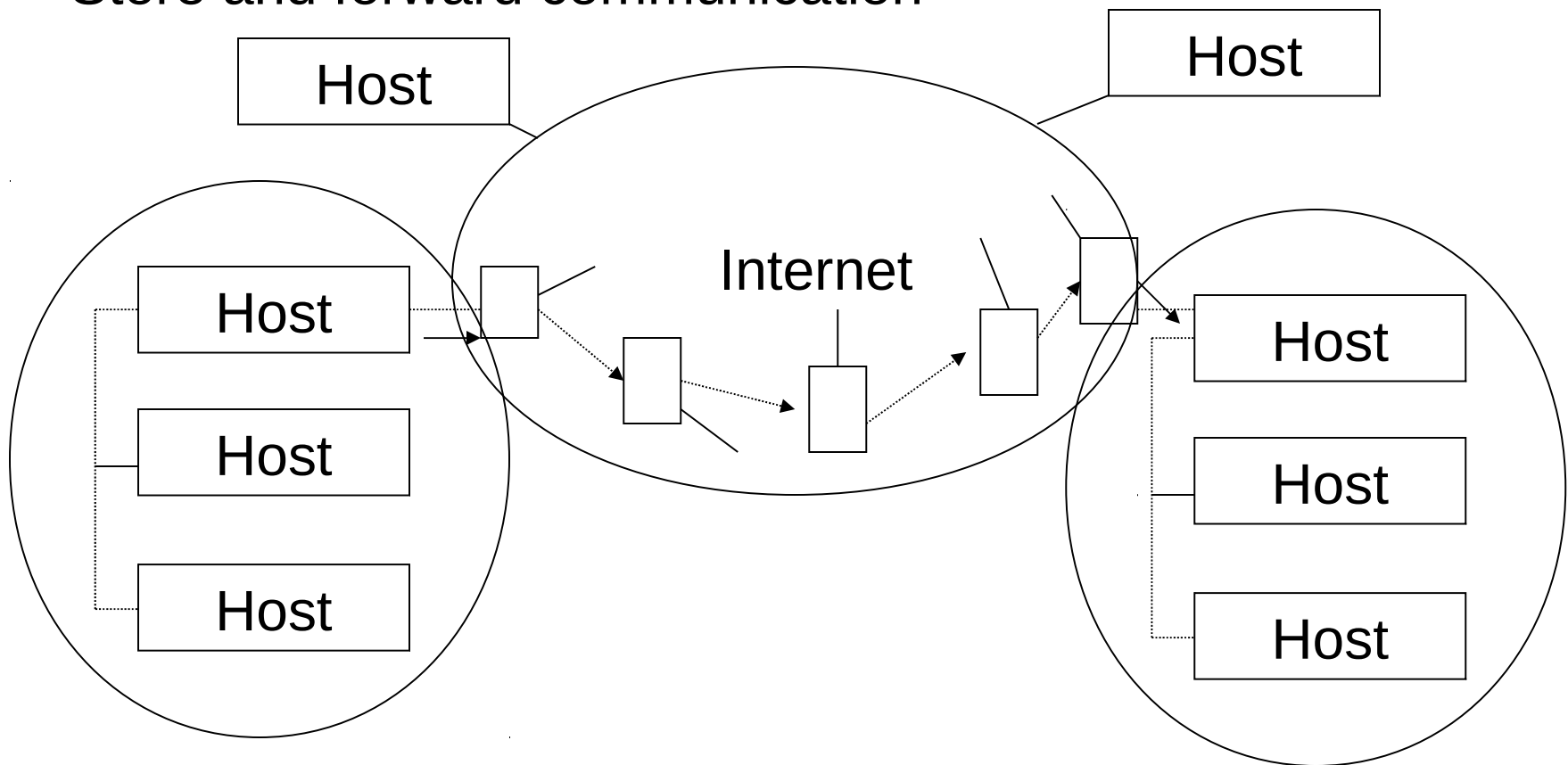
# Indirect Packet Delivery

*Int. Secure Systems Lab  
Technical University Vienna*

- If hosts are in different physical networks packet can't be delivered directly
- Packet is forwarded to a **gateway**
  - has access to other network(s)
  - decides where to send the packet next (based on its destination)
- this is repeated until packet arrives at network with target host
  - then direct delivery is performed
- link level addresses change at every step
  - TTL field is decreased by 1 at each hop
  - IP addresses remain the same!

# Routing

## Store and forward communication



# The Routing Table

- contains information how to do hop-by hop routing
  - what is the next hop?

```
% route -n
Kernel IP routing table
Destination      Gateway          Genmask         Flags         Iface
192.168.1.0      0.0.0.0         255.255.255.0   UH            eth0
127.0.0.1        0.0.0.0         255.0.0.0       U             lo
0.0.0.0          192.168.1.1    0.0.0.0         UG            eth0
```

- **Flags:**
  - U: the route is up
  - G/H: destination is a gateway/host

# Routing Mechanisms

*Int. Secure Systems Lab  
Technical University Vienna*

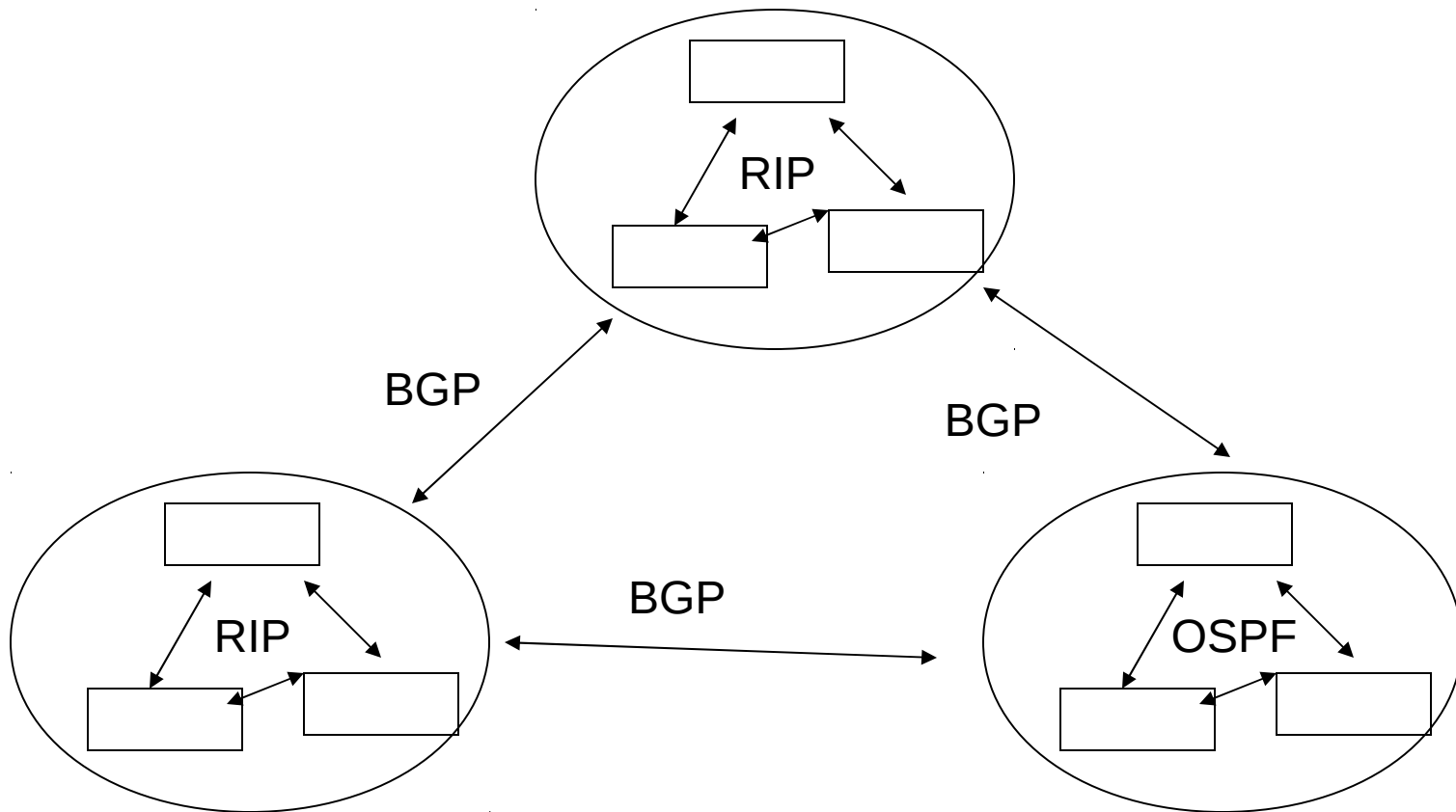
- Route-daemon searches for
  - matching host address
  - matching network address
  - default entry
- If no route can be found: ICMP message „Host unreachable“ is sent back to originator
- Routing tables can be set
  - statically
  - dynamically (using routing protocols)

# Routing Protocols

*Int. Secure Systems Lab  
Technical University Vienna*

- automatically distribute information about delivery routes
- hierarchically organized with different scope
- divided in:
  - exterior gateway protocols (EGPs)
    - distribute information between different autonomous systems
    - e.g. Border Gateway Protocol (BGP) for Internet backbone
  - interior gateway protocols (IGP)
    - distribute information inside autonomous systems
    - e.g. Routing Information Protocol (RIP)
    - autonomous is loosely defined as: under a single administrative control

# Routing Protocols

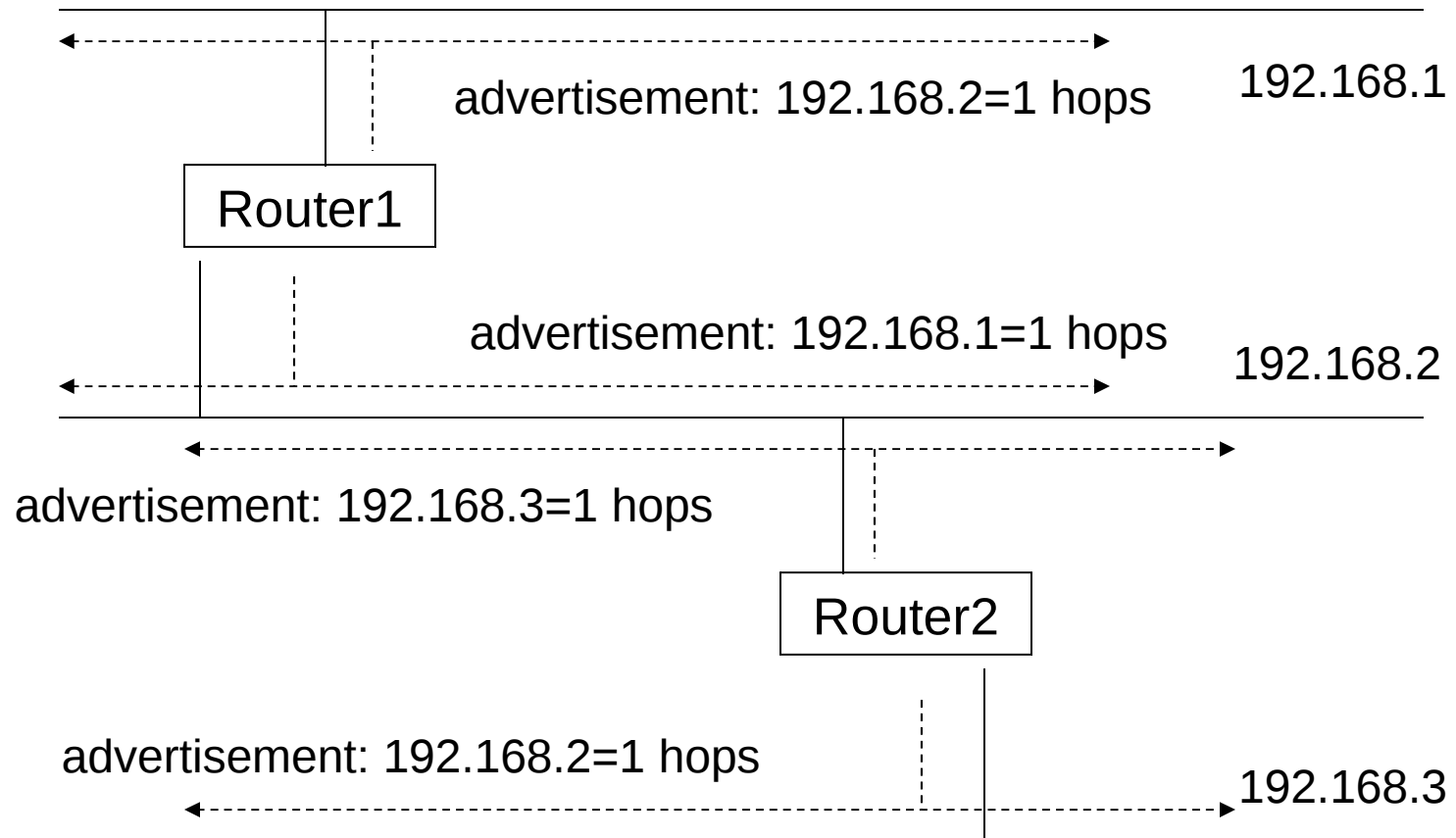


# RIP (Routing Information Protocol)

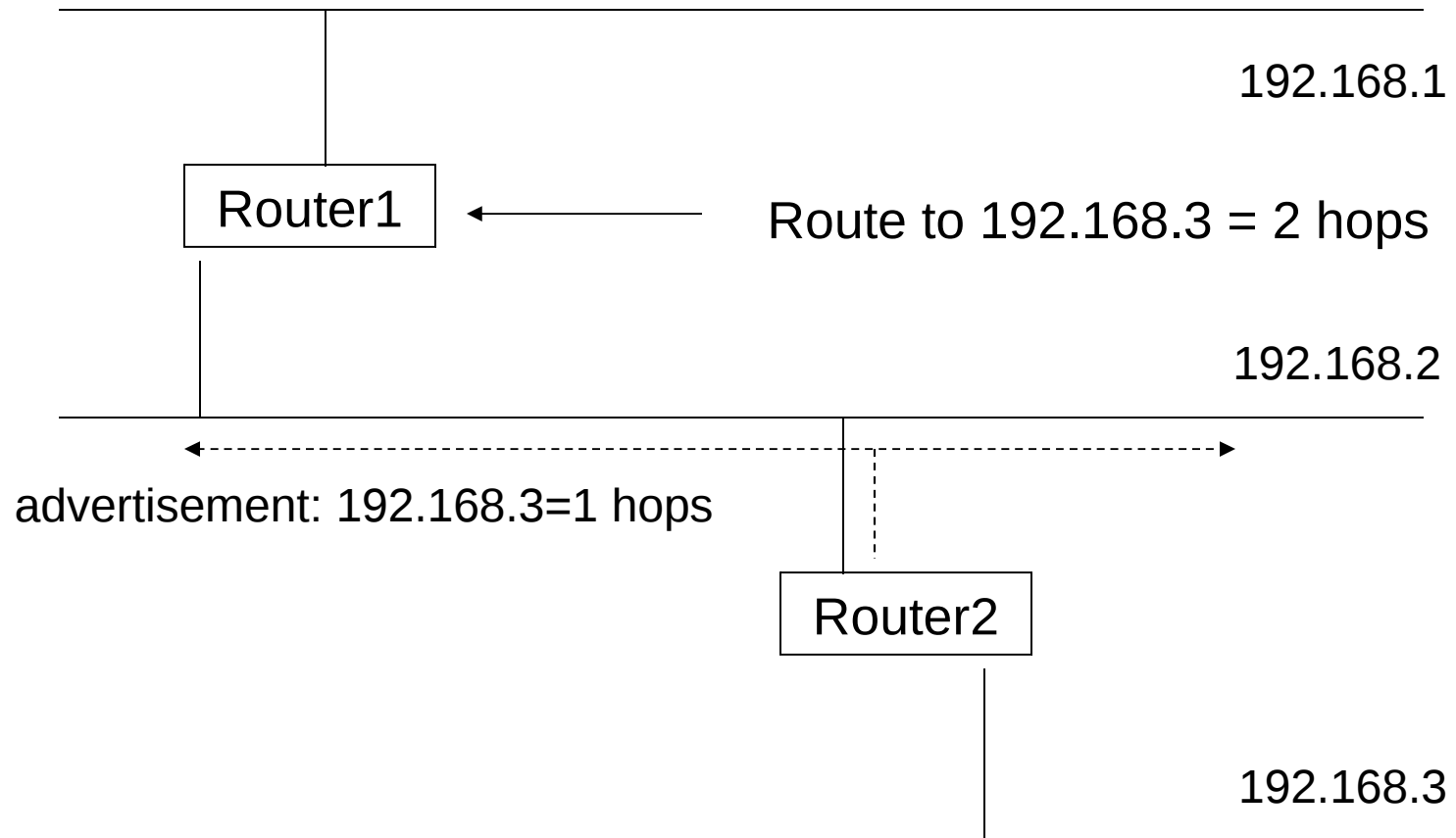
*Int. Secure Systems Lab  
Technical University Vienna*

- uses UDP to transport messages (520)
- no authentication (RIPv1), password in the clear (RIPv2)
- distance vector routing protocol
- router knows which nets it is connected to
- routers broadcast RIP messages every 30 seconds
  - contains route advertisements (all its knowledge)
  - each advertisements contains metric: hop count
  - only route with smallest hop count is stored in the router
  - timeout for routes (3 minutes) if not advertised again

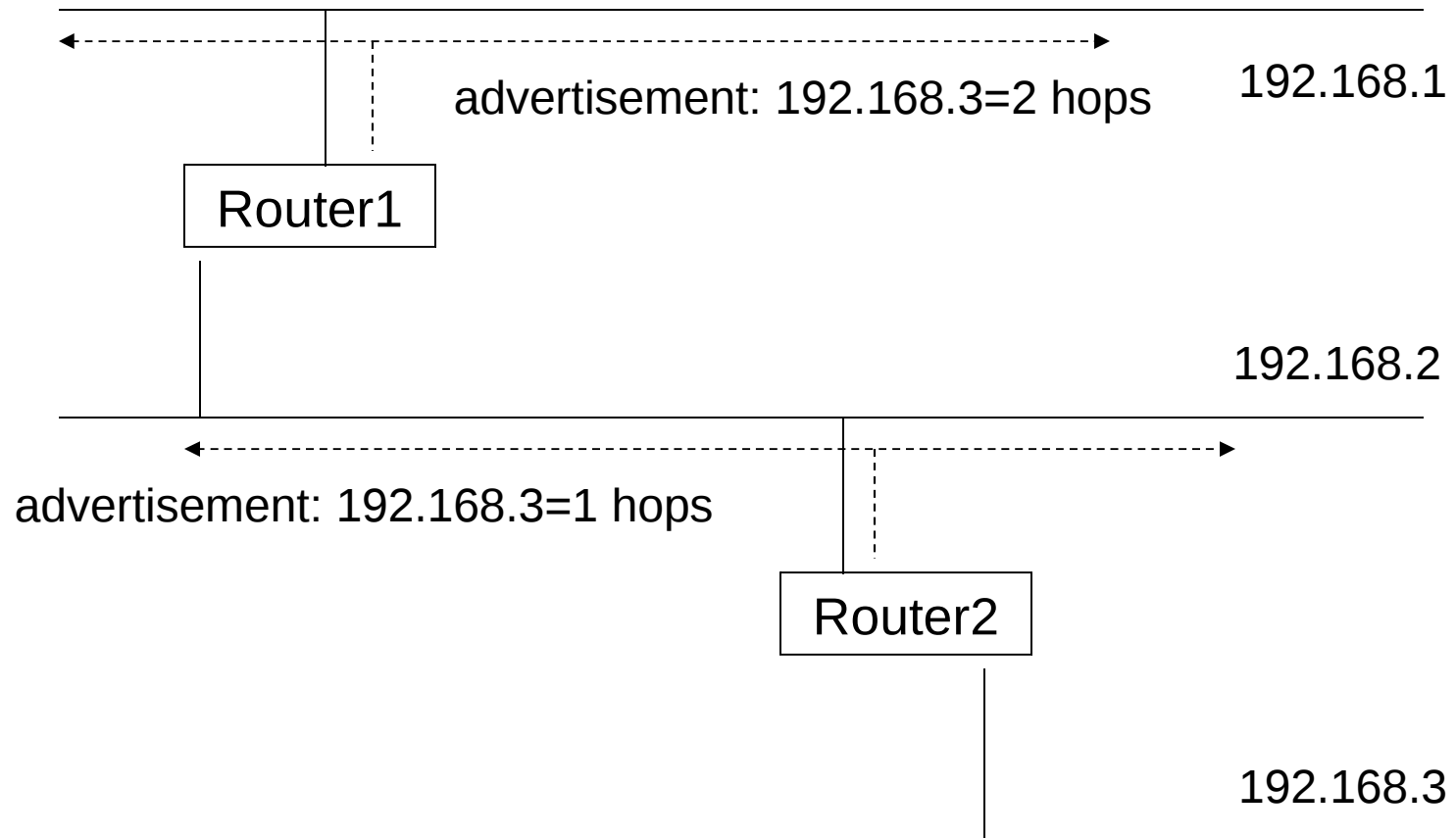
# RIP



# RIP



# RIP



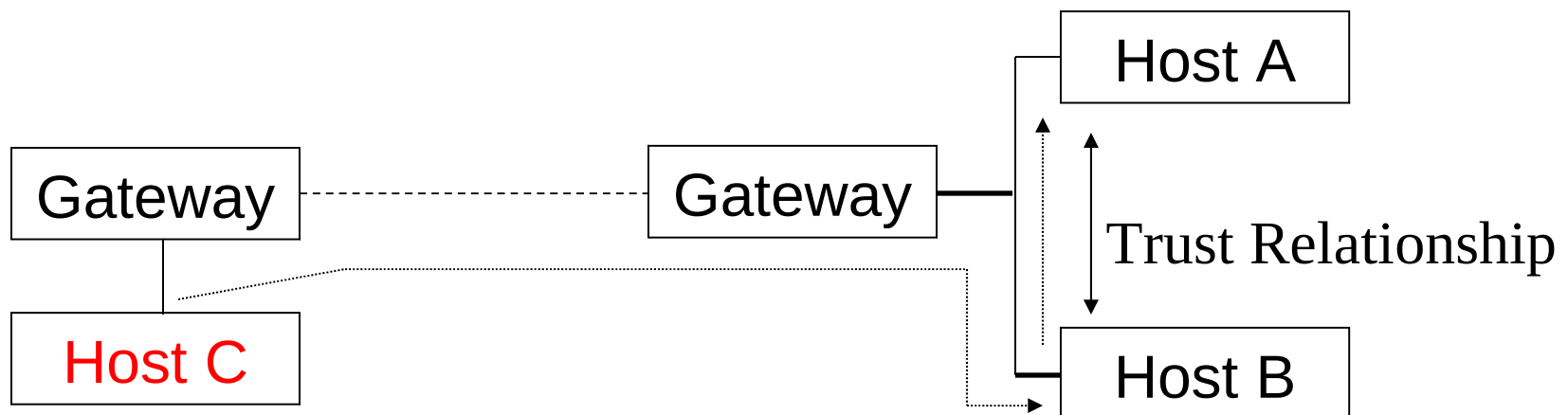
# Attacks involving Multiple Networks

*Int. Secure Systems Lab  
Technical University Vienna*

- Blind IP spoofing
- Man-in-the-middle-attacks
- Attacks concerning the routing mechanism
  - e.g. RIP attacks

# Blind IP Spoofing

- usually the attacker does not have access to the reply, abuse trust relationship between hosts
  - e.g.
    - Host C sends an IP datagram with the address of some other host (Host A) as the source address to Host B
    - attacked host (B) replies to the legitimate host (A)

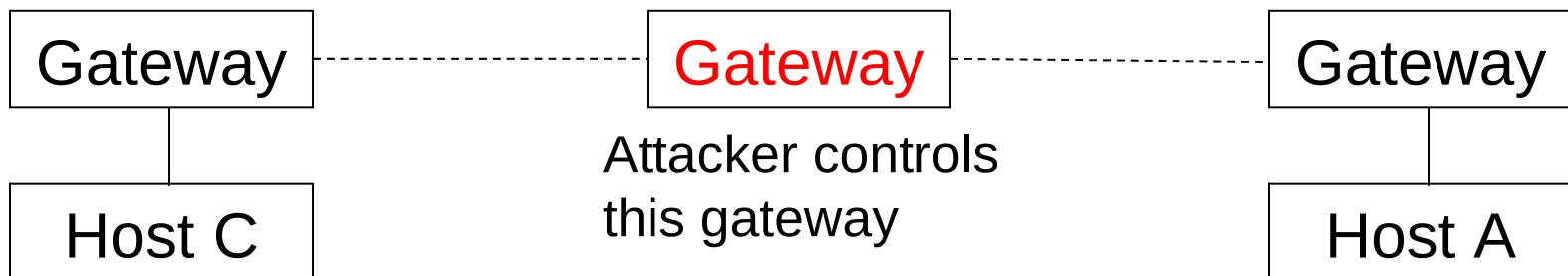


# Man-in-the-Middle Attack

Attacker who controls a gateway that is used in the delivery process can

- sniff the traffic
- intercept/block/delay traffic
- modify traffic

only works if attacker is on „best“ route

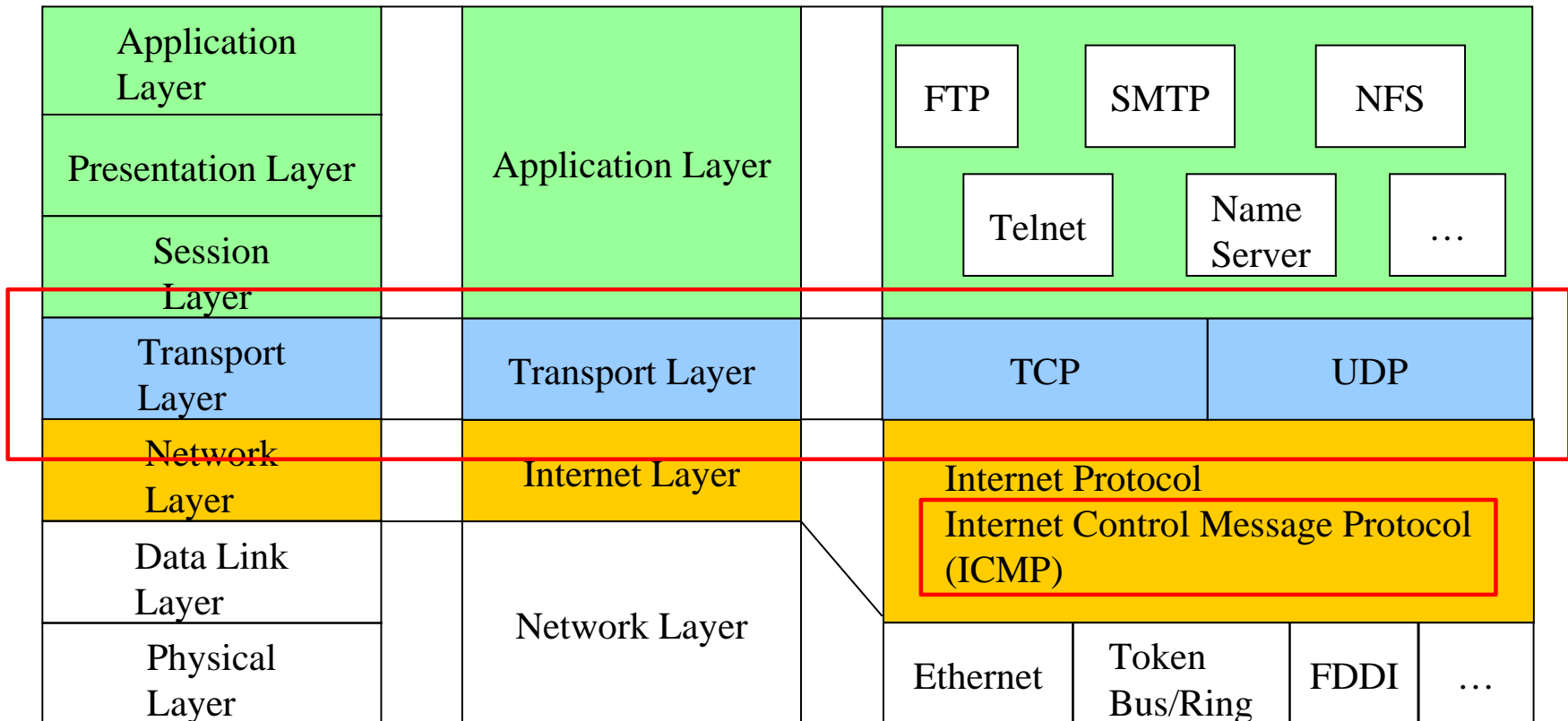


# RIP Attacks

- A host can send spoofed RIP packets in order to „inject“ routes into a host (requires only IP/UDP spoofing)
  - a route with a smaller hop count would be used
- This attack can be used for
  - MitM (sniffing, filtering, tampering)
  - DoS
- On a LAN with RIPv2 passwords have to be used for updating routes, but plaintext passwords are used
  - can be sniffed

# Transport Layer Protocols

*Int. Secure Systems Lab  
Technical University Vienna*



# ICMP (Internet Control Message Protocol)

*Int. Secure Systems Lab  
Technical University Vienna*

- Used to exchange control/error messages about the delivery of IP datagrams
  - is really at the network/internet layer
- ICMP messages are encapsulated inside IP datagrams
- ICMP messages can be:
  - Requests
  - Responses
  - Error messages:
    - include header and first 8 bytes of offending IP datagram

# ICMP Message Format

*Int. Secure Systems Lab  
Technical University Vienna*

type (1 byte)	code (1 byte)	header checksum (2 bytes)
data		

type field: specifies the class of the ICMP message

code field: specifies the exact type of message

# ICMP Messages

*Int. Secure Systems Lab  
Technical University Vienna*

- Address mask request/reply
  - used by diskless systems to obtain the network mask at boot time
- Timestamp request/reply
  - used to synchronize clocks
- Source quench
  - used to inform about traffic overloads
- Parameter problem
  - used for inform about errors in the IP datagram fields

# ICMP Messages

- Echo request/reply
  - used to test connectivity (ping)
- Time exceeded
  - used to report expired datagrams (TTL=0)
- Redirect
  - used to inform hosts about better routes (gateways)
- Destination unreachable
  - used to inform a host that it is impossible to deliver traffic to a specific destination

# ICMP Echo Request/Reply

- Used by the ping program

type (1 byte)	code (1 byte)	checksum (2 bytes)
identifier (2 bytes) = Process ID		sequence number (2 bytes)
data		

identifier is used by „ping“ to deliver back the packet to the right process (allowing more than one ping to run concurrently)

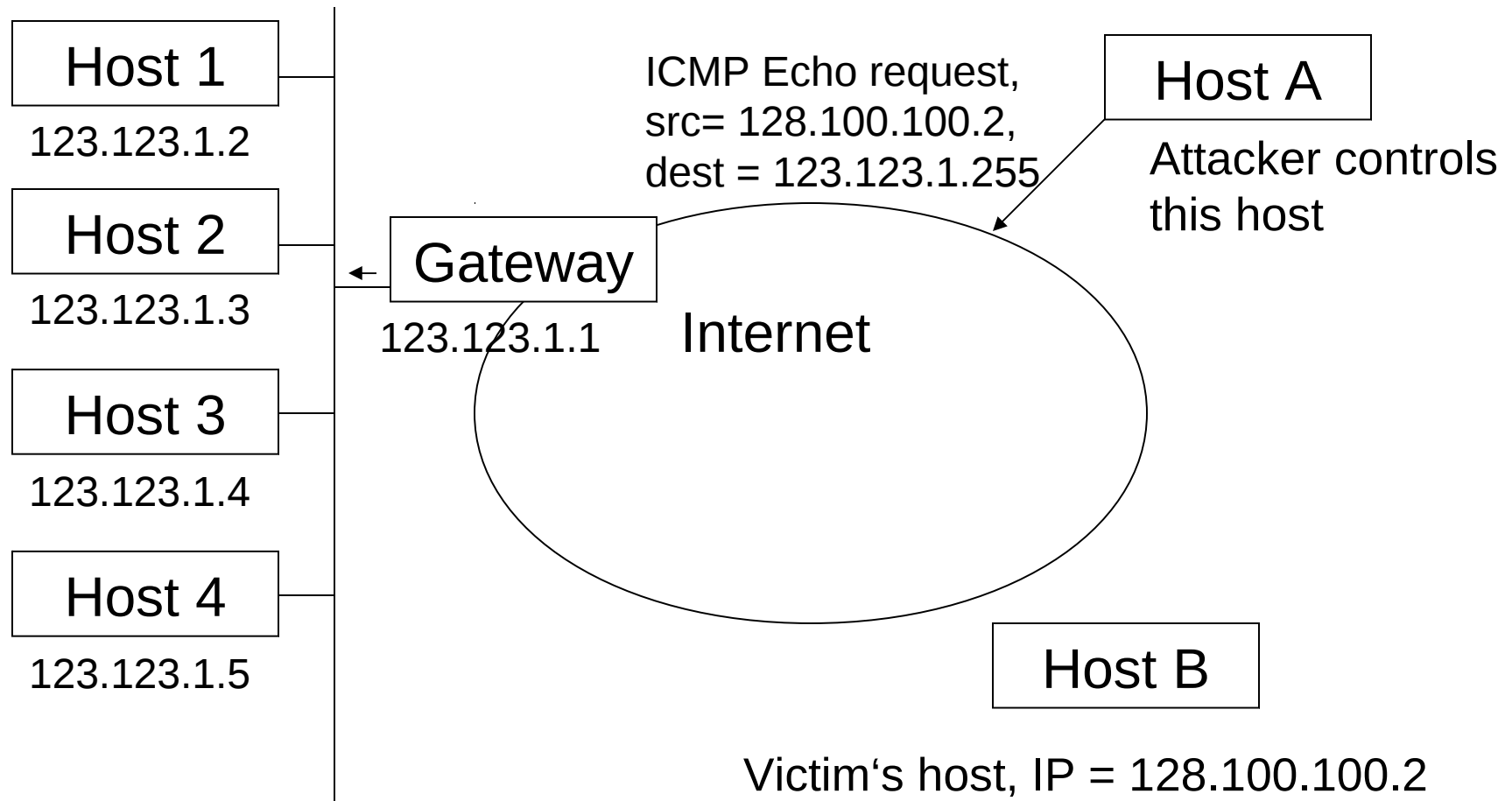
# ICMP Echo Attacks

*Int. Secure Systems Lab  
Technical University Vienna*

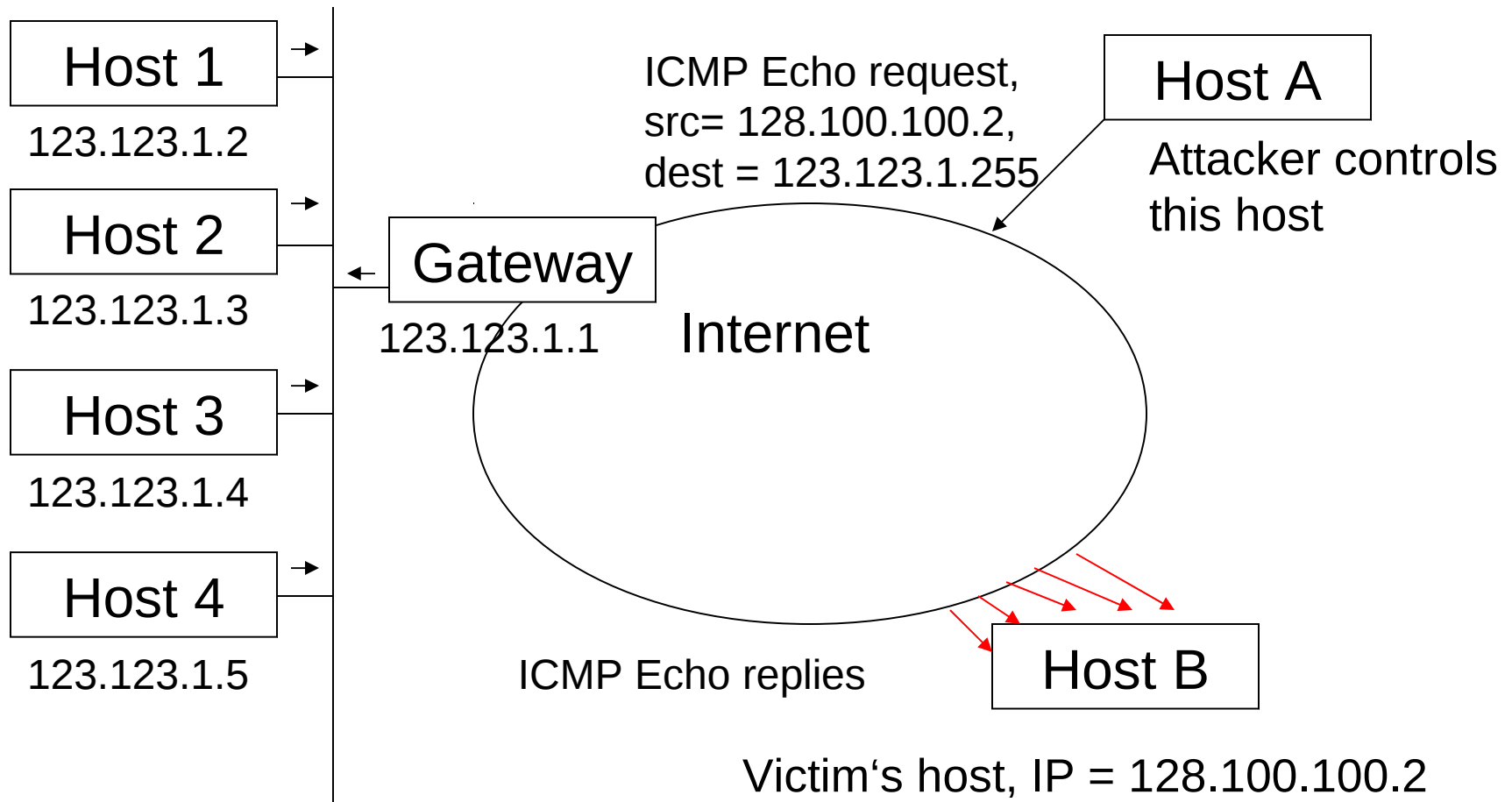
- Information gathering: map the hosts of a network
  - ICMP echo datagrams are sent to all the hosts in a subnet
  - attacker collects the replies and determines which hosts are alive
- Denial of Service attack (SMURF attack)
  - send spoofed (with victim's IP address) ICMP Echo Requests to subnets
  - victim will get ICMP Echo Replies from every machine

# ICMP Smurf Attack

Int. Secure Systems Lab  
Technical University Vienna



# ICMP Smurf Attack

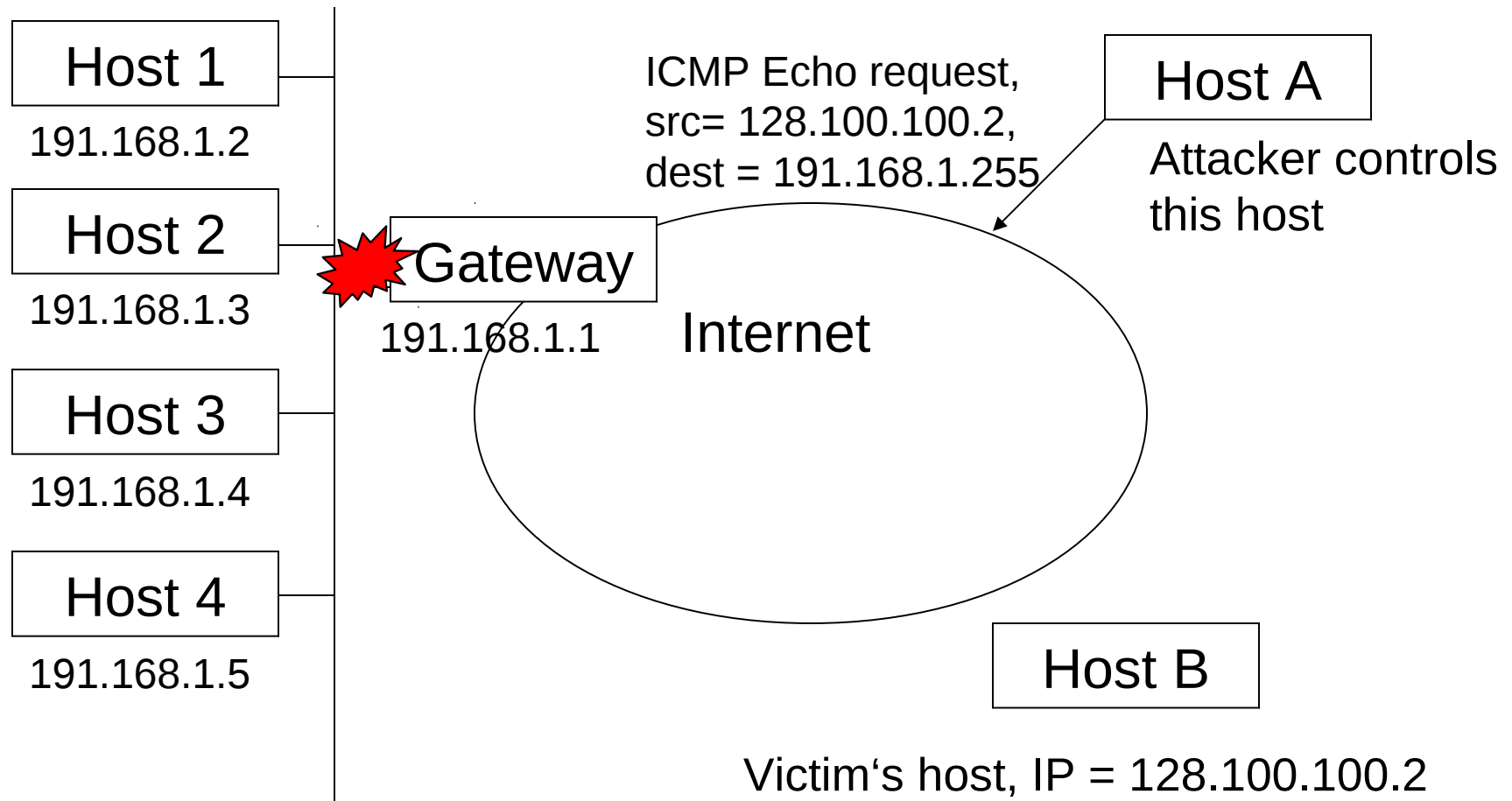


# ICMP Smurf Attack

*Int. Secure Systems Lab  
Technical University Vienna*

- Is a form of DoS amplification attack
  - attacker sends 1 packet, victim receives many packets
  - can cause more load on victim than attacker would be able to cause by directly flooding it with packets
- Should not work on real networks
  - except in the local network
  - gateway will NOT forward broadcast packets
  - **broadcast domain** ends at the router

# ICMP Smurf Attack

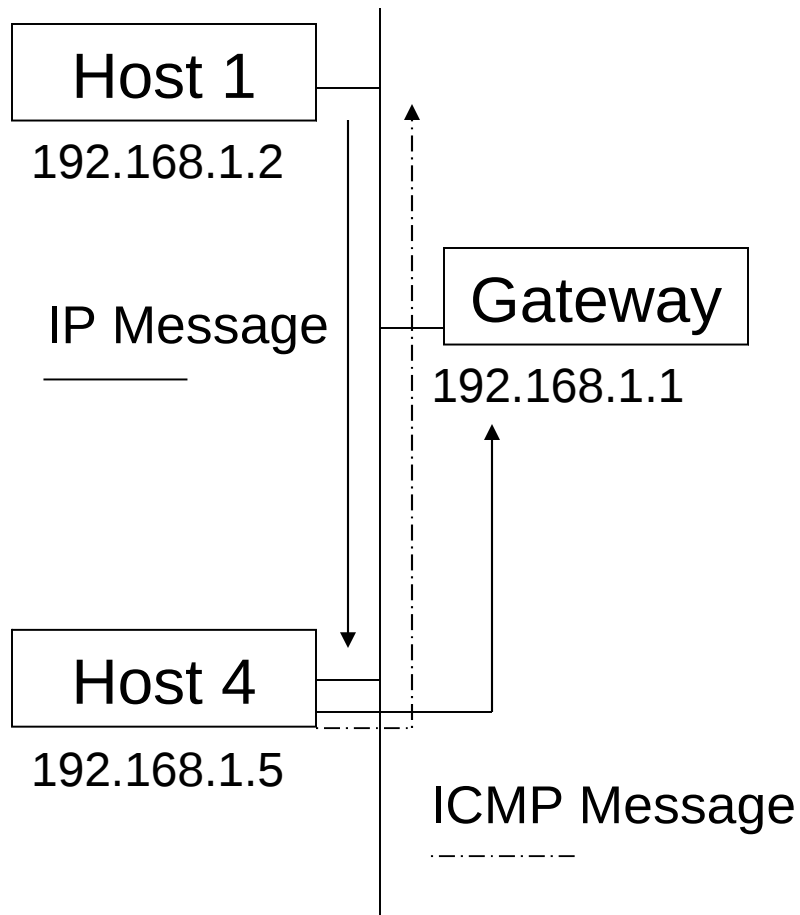


# ICMP Redirect

- is used for stating that there is a better route to a host/net
- is sent by a router that routes a packet over the same interface that was used for receiving this packet

type (=5)	code	checksum (2 bytes)
IP address of the router that should be used		
IP header + first 8 bytes of the original datagram		

# ICMP Redirect: Example



- 1) In Host1's configuration, it is stated to use Host4 as a gateway. So when Host1 sends a packet outside the subnet, this is forwarded to Host4.
- 2) Host4 gets the packet, but has to forward the packet to Gateway.
- 3) Additionally Host4 sends Host1 an ICMP redirect message. „The net xxx can be reached better via Gateway yyy.

# ICMP Redirect

- A host that receives an ICMP redirect message checks:
  - whether the new router is directly connected to the network
  - the redirect must be from the current router for this destination
  - the route that is being modified has to be an indirect route
- What cannot be checked
  - is message really sent by the current router?
  - IP spoofing!

# ICMP Redirect Spoofing

*Int. Secure Systems Lab  
Technical University Vienna*

- ICMP redirect messages can be used to re-route traffic on specific routes or to a specific host that is not a router at all
- The attack is very simple: just send a spoofed ICMP redirect message that appears to come from the host's default gateway
- Can be used to
  - Hijack traffic
  - Perform a denial of service attack

# ICMP Destination Unreachable

- ICMP message used by gateways to state that the datagram cannot be delivered
- Many subtypes
  - Network unreachable
  - Host unreachable
  - Protocol unreachable
  - Port unreachable
  - Fragmentation needed but don't fragment bit set
  - Destination host unknown
  - Destination network unknown etc.

# ICMP Destination Unreachable Spoofing

*Int. Secure Systems Lab  
Technical University Vienna*

- Can be used to „cut“ out nodes from the network
  - denial of service attack (DOS)
- If host A is sending traffic to B and receives a destination unreachable message, it will drop the connection
  - return an error to the application
- Attack: flood a network with destination unreachable messages for host B to ensure communication fails

# ICMP Time Exceeded

Used when

- TTL becomes zero (code =0)
- The reassembling of a fragmented datagram times out (code=1)

type (=11)	code (0 or 1)	checksum (2 bytes)
unused (4 bytes)		
IP header + first 8 bytes of the original datagram		

# Traceroute

- Utility program to determine the path to a specific host/net by soliciting ICMP Time Exceeded messages
- Traceroute:
  - sends a series of IP datagrams to the destination node
  - uses low TTL values
  - each datagram has an increasing TTL value (start at 1)
  - gets back ICMP Time Exceeded messages by the intermediate gateways
  - so the full path can be reconstructed by Traceroute
- Useful tool for topology mapping
  - (malicious) information gathering, but also admin

# Conclusion

*Int. Secure Systems Lab  
Technical University Vienna*

- We talked about:
  - IP networking and attacks
  - ARP protocol and spoofing attacks
  - ICMP protocol and attacks
- In the next lecture, transport layer
  - UDP, TCP protocols and attacks
- Any Questions?