ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Communication Systems

ARP

University of Freiburg
Computer Science
Computer Networks and Telematics
Prof. Christian Schindelhauer

CoNe Freiburg

IIF
INSTITUT FÜR INFORMATIK FREIBURG

Copyright Warning

- This lecture has already been stolen
- If you copy it again please ask the author
  - Prof. Dr. Gerhard Schneider
- like I did

Internet Working
Extensions: VLAN tagging and QoS

- **VLANs a means for complete virtualisation of broadcast domains**
  - Same characteristics as physical LAN, but allowing end stations to be grouped together independent of network switch location
  - Major advantage: reconfiguration done via switch software configuration instead of physically relocating hardware / changing cabling
  - Segmentation service traditionally provided by routers in a LAN
  - Provides a mean to expedite time-critical network traffic by setting transmission priorities for outgoing frames
  - Bridges and switches filter destination addresses and forward VLAN frames only to ports that serve the VLAN to which the traffic belongs
  - Multiple layer 3 networks within the same physical LAN

Extensions: VLAN tagging and QoS

- VLAN 802.1q tagging is a MAC option that provides capabilities not previously available to classical Ethernet networks (defined since Fast Ethernet standards)
- VLAN standard deploys internal tagging process modifying the Ethernet frame adding a 4 byte header extension
  - 2-byte tag protocol identifier (TPID)
  - plus 2-byte tag control information (TCI)

- TPID has a fixed value of 0x8100 indicating the frame is carrying 802.1q/802.1p tag
- TCI contains:
  - 3-bit user priority
  - 1-bit canonical format indicator (CFI)
  - 12-bit VLAN identifier (VID) – Uniquely identifies the VLAN the frame belongs to

Internet Working Extensions: VLAN handling

- If the MAC is installed in a switch port, the frame is forwarded according to its priority level to all ports that are associated with the indicated VLAN identifier
- If the MAC is installed in an end station, it removes the 4-byte VLAN header and processes the frame in the same manner as a basic data frame

PRE	SFD	DA	SA	VLAN type ID	Tag control information	Length/Type	Data	Pad	FCS	Extension
7	1	6	6	2	2	4	46 -	1500	4	

Field length in bytes

Internet Working Extensions: VLAN handling

- VLANs violate the old MTU restriction of 1518 Byte producing packets with a MTU of 1522 Byte
- Application:
  - Static – port based configuration: All machines connected to a port are in the same VLAN (invisible to them), standard scenario in campus setup
  - All VLAN tags added by these stations are silently dropped in switch (thus a reconfiguration of local device was required for producing the proper playground for the exercises)
  - Dynamic – using special software to create VLAN automatically e.g. grouping on source MAC address (e.g. putting all IP telephones in a specific LAN with higher forwarding priority)

Communication Systems
Ethernet and IP

- Flat addressing scheme of physical/data link layer Ethernet
- Why two addresses for a LAN connected host?
- IP addressing – higher layer, to overcome the flat addressing restrictions: routed/hierarchical
  - Changing places of many hosts (e.g. your laptop: connected at home to Ethernet and to different WLANs throughout the day, but the physical addresses of your machine do not change)
  - Manual setup/configuration needed (todays practical)
- How to encapsulate IP datagram within link-layer frame

Ethernet and IP

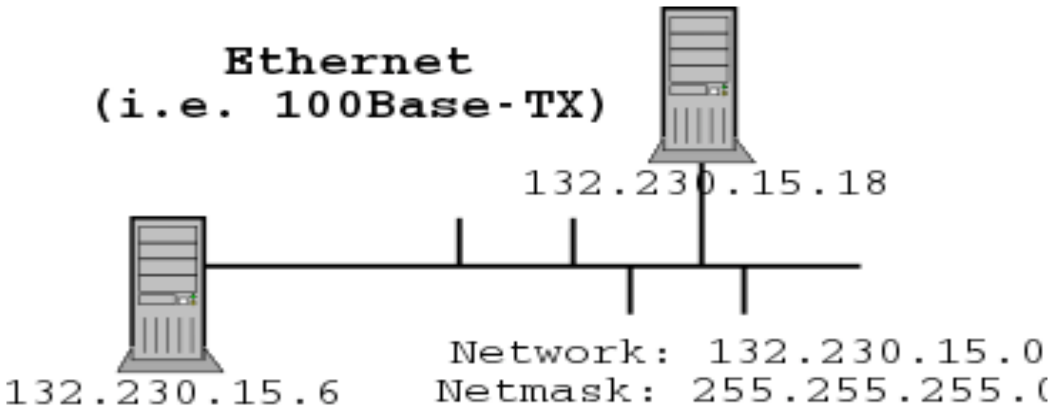
- What low level destination (MAC) address to use?
- Helper protocol is needed
  - IP has no feature to do mapping itself
  - Such mapping is not needed in PPP environments
  - This protocol is specific to the underlying hardware / software protocol
- Address Resolution Protocol (ARP) is for address mapping in Ethernets (and TokenRings, ATM, ...)
  - Fairly old protocol around for a while (RFC 826)

IP to MAC and vice versa

- Address Mapping: IP to MAC – to get the host where to deliver a given packet locally
- Simple solution could just broadcast everything (and every machine listens to everything)
  - Unnecessary, burdens uninterested stations with others' traffic, congests the network
- IP to MAC address mapping mechanisms
  - Configured by hand [cumbersome]
  - Dynamic [learned by system automatically]
- Address Mapping IP to MAC: Learning

Address Mapping in Broadcast Nets

- **But what to do in broadcast nets with many connected hosts?**
  - In broadcast nets every host gets every packet sent out in the segment (switching may reduce traffic, but for some services packets to all are inevitable)
- **For local delivery, need to map network-layer address to link-layer address:**
  - Consider the machines 132.230.15.6 and 132.230.15.18 (netmask e.g. 255.255.255.0) ... [on same network/subnet]



Address Resolution Protocol (ARP)

- Dynamic approach
  - Each station runs Address Resolution Protocol (ARP)
  - Client/server architecture, each station is both client and server, routers have to implement the same mechanism too
  - Cache lookups with timeouts on each resolution
- Introduction of an intermediate protocol – operating between layer 2 & 3
- Address Resolution Protocol is basically address independent (at both network & link layer)
- Protocol is specialized for each particular network/link address pairing

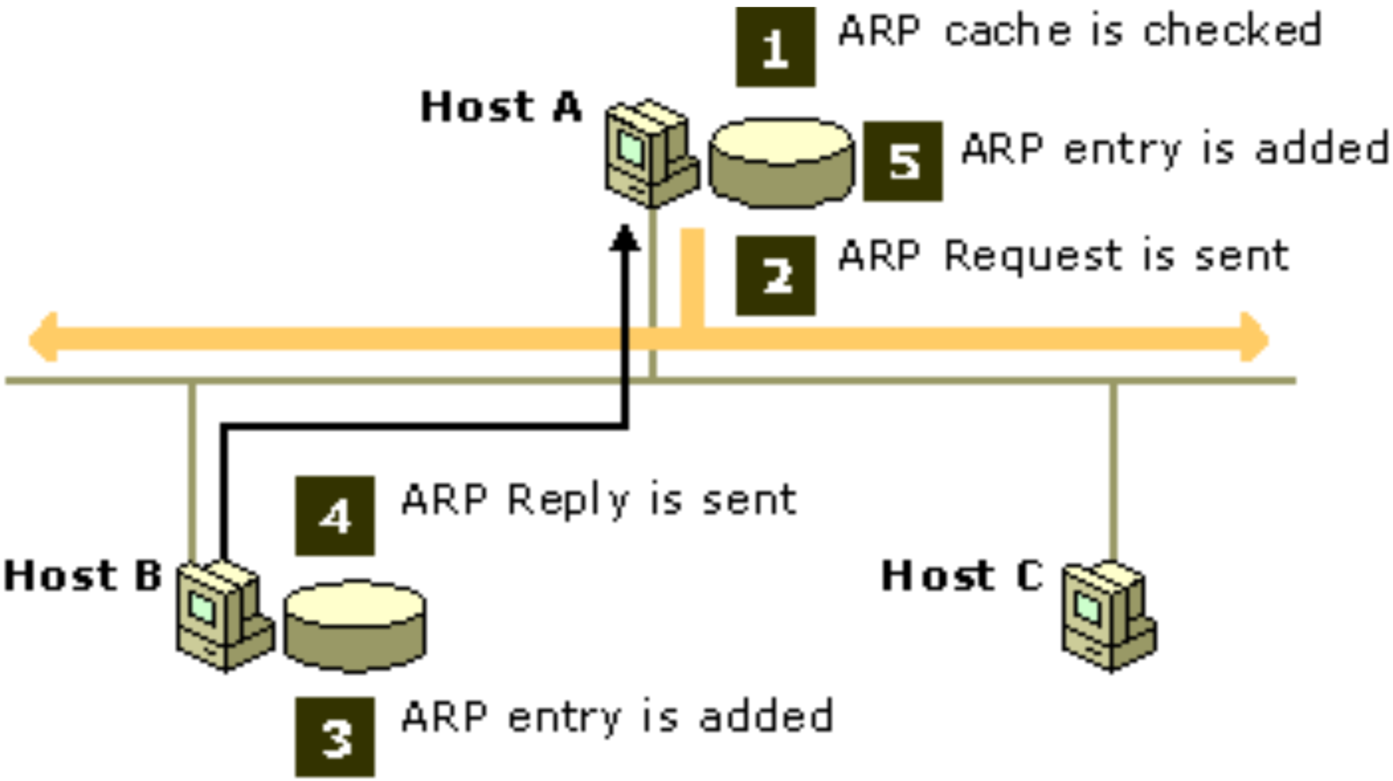
ARP

- The term address resolution refers to the process of finding an address of a computer in a network
- Address is "resolved" using a protocol in which a piece of information is sent by a client process executing on the local computer to a server process executing on a remote computer
- The information received by the server allows the server to uniquely identify the network system for which the address was required and therefore to provide the required address
- Procedure is completed when the client receives a response from the server containing the required address

ARP operation

- **Step-by-Step operation**
  - 0 - Requesting station A has IP address I, wants the associated MAC address M
  - 1 – Check the own ARP cache
  - 2 - A broadcasts the query: who has I? tell A
  - 3 – B adds MAC for A to its cache
  - 4 - Machine assigned address I responds directly to A with its MAC address M
  - 5 - A adds the (I,M) entry to its ARP cache

ARP operation cont.



ARP on ethernet with IP payload

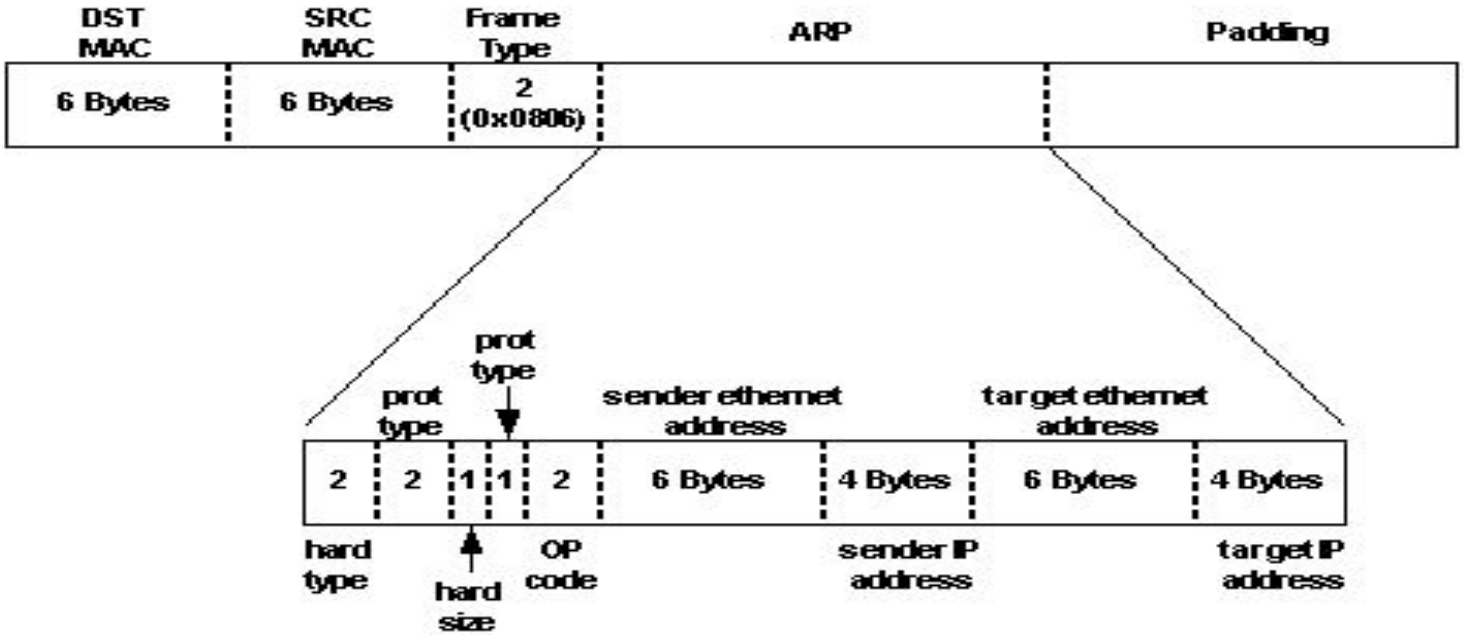
- **Common example is Ethernet/IPv4 (look at Ethernet/IPv6 in wireshark in upcoming practical)**
- **Ethernet MAC: 6Byte (48bit), IPv4: 4Byte (32bit), IPv6: 16Byte (128bit)**

32 bit

<table>
<tr><td colspan="2">HARDWARE ADDRESS TYPE</td><td colspan="2">PROTOCOL ADDRESS TYPE</td></tr>
<tr><td>HADDR LENGHT</td><td>PADDR LENGHT</td><td colspan="2">OPERATION</td></tr>
<tr><td colspan="4">SENDER HARDWARE ADDRESS (first 4 Byte)</td></tr>
<tr><td colspan="2">SENDER HADDR (last 2 Byte)</td><td colspan="2">TARGET HADDR (first 2 Byte)</td></tr>
<tr><td colspan="4">TARGET HARDWARE ADDRESS (last 4 Byte)</td></tr>
<tr><td colspan="4">TARGET PROTOCOL ADDRESS (all 4 Byte)</td></tr>
</table>

ARP on ethernet with IP payload cont.

- ARP frames marked with Frame Type 0x0806
- IPv4 frames marked 0x0800 (wireshark exercise)
- Ethernet frame on wire with all headers and ARP payload



ARP cache table (example)

- **Contains hostname or IP address, hardware type, MAC, flag (c for cached), interface (use of arp or ip neighbor commands presented in experimental part of the course)**

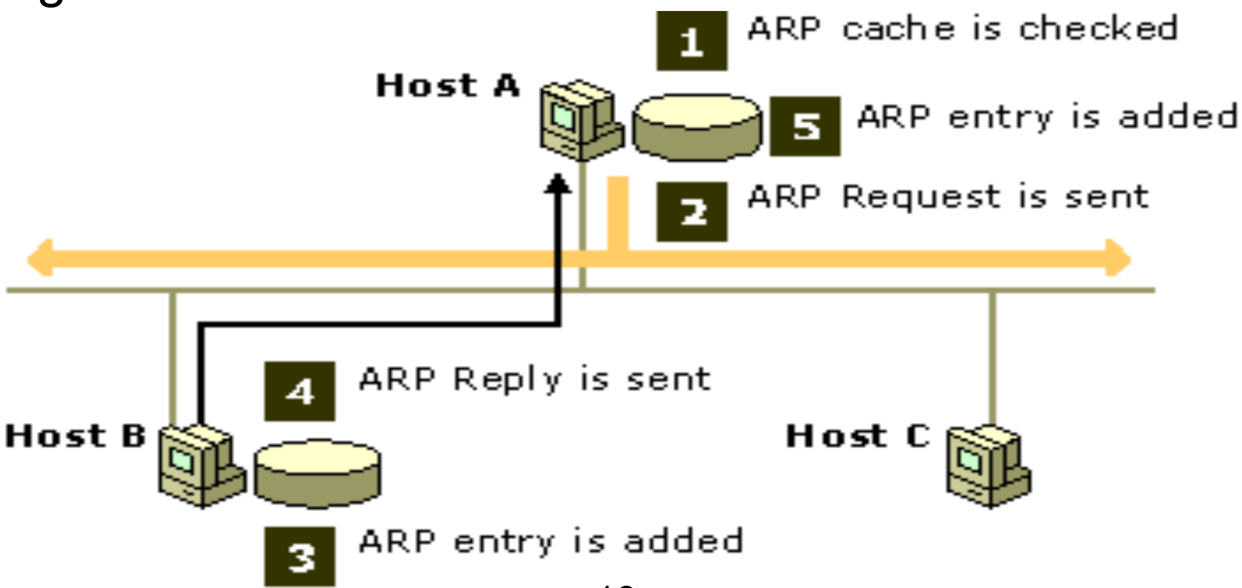
```
$
$ /sbin/arp
Address                  HWtype  HWaddress           Flags Mask            Iface
npserv2.ruf.uni-freibur  ether   00:09:6B:00:41:78   C                     eth0
fs1.ruf.uni-freiburg.de  ether   00:02:B3:4C:57:23   C                     eth0
mbone.ruf.uni-freiburg.  ether   08:00:20:88:96:76   C                     eth0
b1-9.ruf.uni-freiburg.d  ether   00:09:6B:00:40:DA   C                     eth0
npserv4.ruf.uni-freibur  ether   00:09:6B:00:41:BC   C                     eth0
b1-8.ruf.uni-freiburg.d  ether   00:09:6B:00:26:CF   C                     eth0
login9.ruf.uni-freiburg  ether   00:09:6B:00:3F:8D   C                     eth0
npserv1.ruf.uni-freibur  ether   00:02:B3:4C:57:37   C                     eth0
132.230.1.254            ether   00:09:97:30:3A:14   C                     eth0
mawa.ruf.uni-freiburg.d  ether   00:02:B3:B5:04:9A   C                     eth0
b2-7.ruf.uni-freiburg.d  ether   00:09:6B:00:41:72   C                     eth0
b2-6.ruf.uni-freiburg.d  ether   00:09:6B:00:40:4E   C                     eth0
b2-8.ruf.uni-freiburg.d  ether   00:09:6B:00:3B:08   C                     eth0
b1-6.ruf.uni-freiburg.d  ether   00:09:6B:00:41:88   C                     eth0
b1-7.ruf.uni-freiburg.d  ether   00:09:6B:00:54:B6   C                     eth0
ldap1.ruf.uni-freiburg.  ether   00:02:B3:4C:4D:5B   C                     eth0
$ █
```

Security in ARP and Ethernet

- This lecture, first glimpse on security issues in broadcast networks using ARP
  - Traditional Ethernet uses shared medium – every packet is seen by every station, same applies to every wireless technology (okay – not every mobile station (phone) sees the messages of the others, but it is easy to “wiretap”)
  - Address Resolution Protocol is dynamic – Ethernets are “plug&play” because of ARP
  - ARP (and other protocols like DHCP – handled in a later lecture) needs to broadcast for station discovery
  - All exchanged messages are plain and not secured by any cryptographic methods (we might look at layer 2 security implementations for WLAN like WEP in a later lecture)

ARP Problems

- ARP is a very simple protocol (from the mid 1980s) – thus open to attacks
  - Remember ARP operation: Broadcast of information, no authentication of packets
  - Filling of the ARP cache completely depends on trust on the messages seen



ARP Problems

- We talked of “how switches secure Ethernets” in the beginning
  - Promiscuous mode of the hosts Ethernet adapter does not show the other packets any more
  - Communication between the default gateway (the Internet) and an arbitrary end system in a switched Ethernet is not visible to third party
  - But what to do to get access to packets exchanged between other stations in the net?
- ARP helps in packet routing by matching MACs to IP addresses
  - ARP cache is valid for a while, but not for ever (for obvious reasons)
  - If the relation is changed, IP packets will be delivered to the changed address

ARP Problems

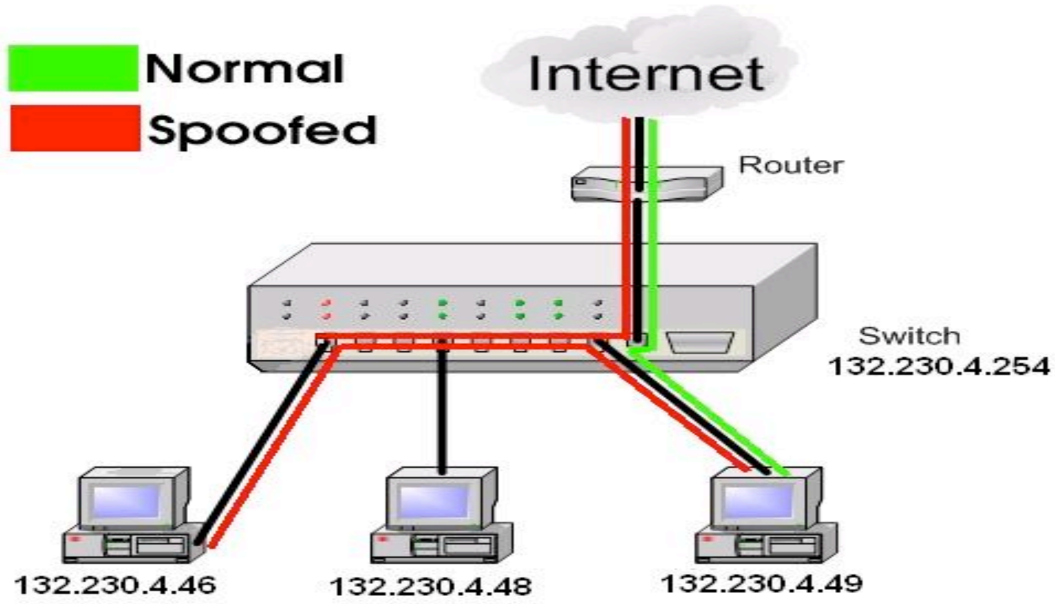
- Thus ARP could be used to force rerouting of IP packets
- So try this – send unsolicited ARP replies
  - Receiving system will cache the reply
  - Overwrites existing entry
  - Adds entry if one does not exit
- Why should systems cache replies for requests never seen?

ARP Problems

- Question of protocol design
  - Host C (in example of two slides before) could update its ARP cache from packets meant for other hosts – without further interaction the cache entries for certain hosts are up to date
  - Even if request is needed for adding an entry to ARP list, the reply of wrong host might be faster than of default router (or any other machine)
  - Just overload that system with bogus packets
- Flood the network with forged ARP replies, so other machines update their cache regularly with wrong entries

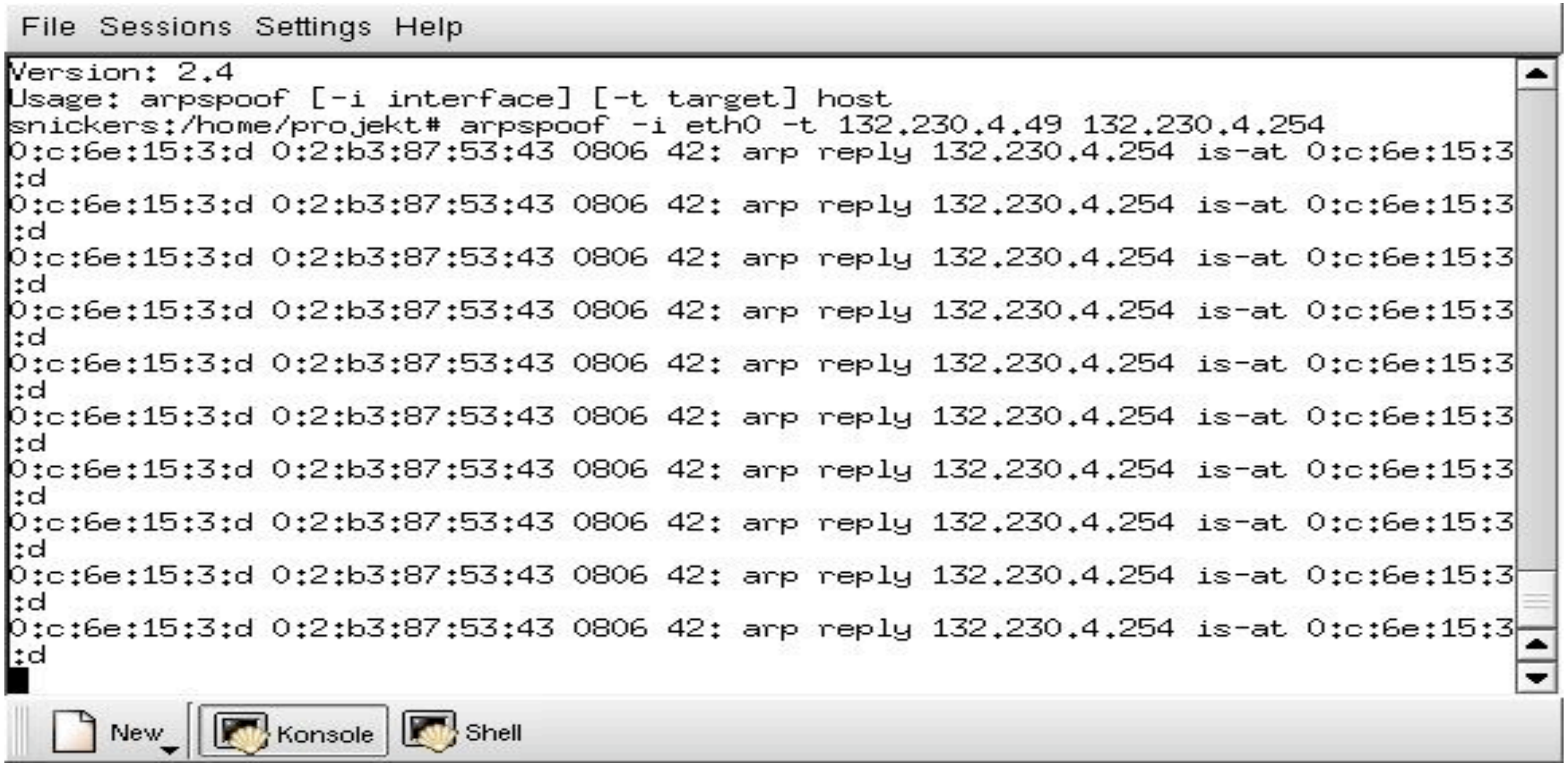
ARP Problems

- General idea: ARP could be used to force rerouting of IP packets, that communication between the Internet and 132.230.4.49 becomes visible to machine 132.230.4.46



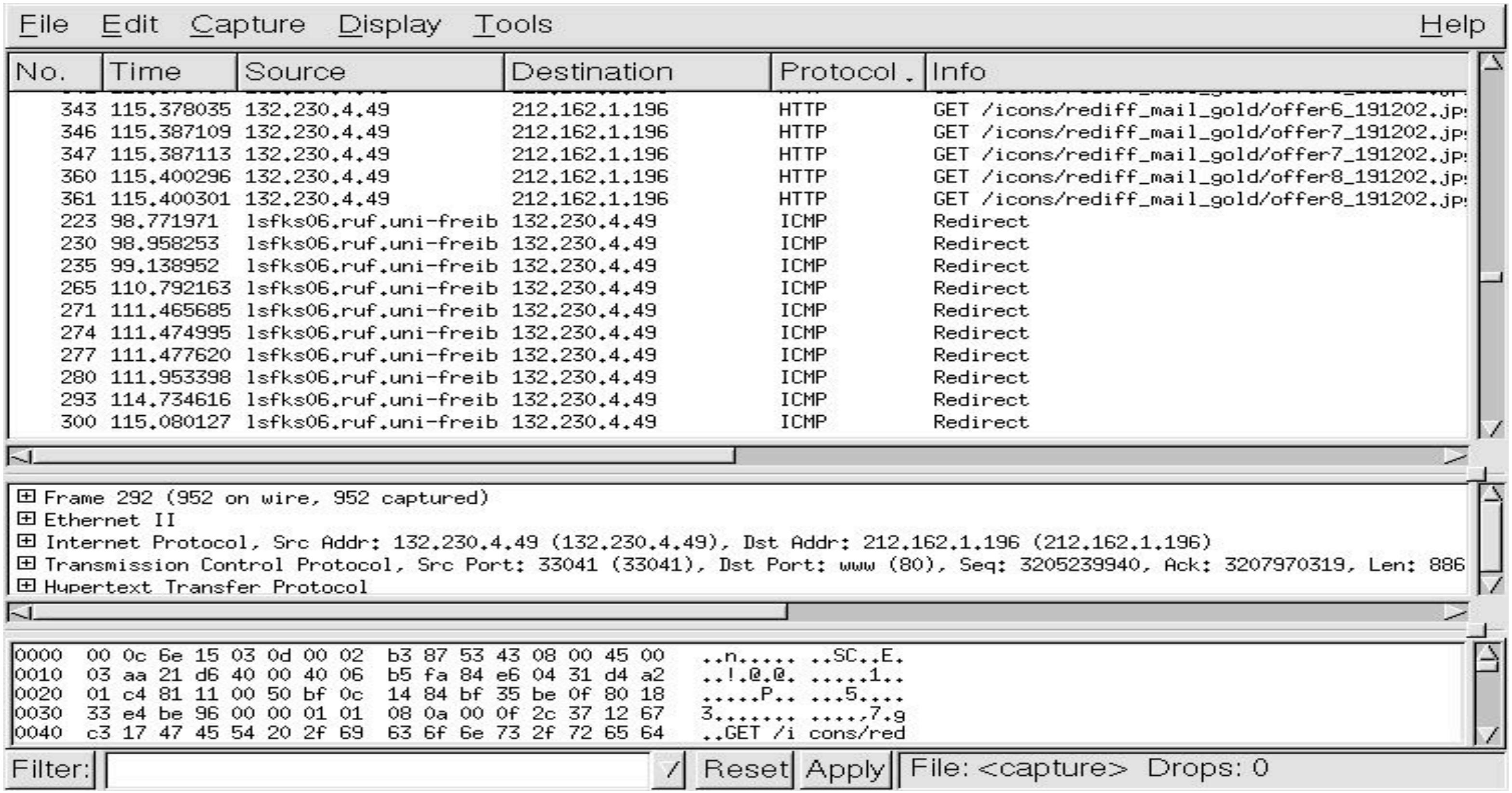
ARP Problems

- Target 132.230.4.49, attacker 132.230.4.46, default route is 132.230.4.254 (using arpspoof here)



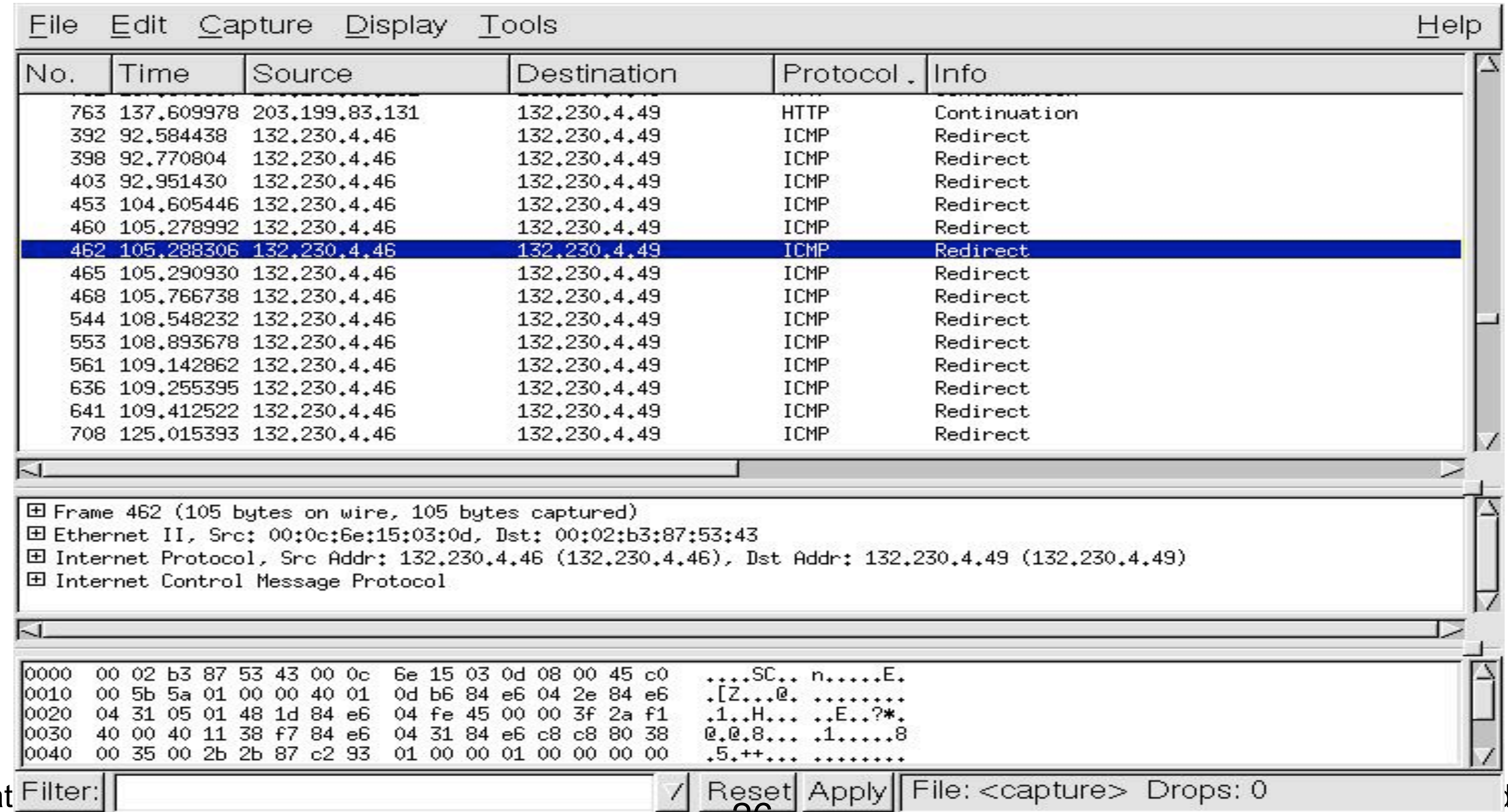
ARP Problems

- Wireshark capture of packets (as seen on the attacker machine 132.230.4.46 – sees the http connections of 132.230.4.49)



ARP Problems

- Ominous ICMP redirect messages on the target (132.230.4.49) of this attack (ICMP special helper protocol)



ARP Problems

- This concept of attack is called ARP poisoning
- You will try this in the exercise using ettercap or arpoison
  - Similar are dsniff, hunt, ...
- But beware – detection of tampering with ARP is easily detectable
  - Identify non-standard ARP- replies versus acceptable ones
  - Timeout issues, possibility of lost/dropped packets during setup and shutdown of ARP based redirect
- Security measures: Track and maintain ARP/IP pairings
  - Tools like arpwatch, snifftest, promisc, snort ...

ARP Problems

- Counter measures
  - Many OS allow for ARP caching to be made static instead of timing out every several minutes
  - Special treatment of router MAC addresses (do not allow update of this MAC, but of all others in network)
- Use static ARP entries
  - Option in special zones like DMZ with few servers and a rather static network setup
  - Otherwise: Who maintains lists of IPs and MACs?
- Or: use network or session layer encryption and authentication
- Does not help against spoofing, but attacks are less harmful (concept of the local WLAN)

ARP Special Scenarios

- ARP might be used in some special scenarios
- Proxy ARP
  - LAN extension: One machine responds to ARP requests in behalf of others
  - Network setup/configuration option
  - Can be used to hide underlying router infrastructure
- Reverse ARP (RARP)
  - Bootstrap method – machine starts without IP address
  - Send an ARP request for own IP address
  - Tells if address is already in use, also updates other's tables for own address
  - Mostly deprecated (replaced by DHCP – some future lecture)

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Communication Systems

Christian Schindelhauer

University of Freiburg
Computer Science
Computer Networks and Telematics
Prof. Christian Schindelhauer

CoNe Freiburg

IIF INSTITUT FÜR INFORMATIK FREIBURG