ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Communication Systems

DHCP

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

Copyright Warning

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

Internet Protocol – the Universal Service

- By now: Link layer (second in OSI) networks provides delivery within the same network
- Typically includes its own addressing format (e.g. Ethernet), and maximum frame size (MTU)
- Network layer provides end-to-end delivery (routing)
- Provides consistent datagram abstraction:
  - best-effort delivery
  - no error detection on data
  - consistent maximum datagram size
  - consistent global addressing scheme
- Most prominent layer 3 implementation: IP version 4

Internet Protocol – the Universal Service

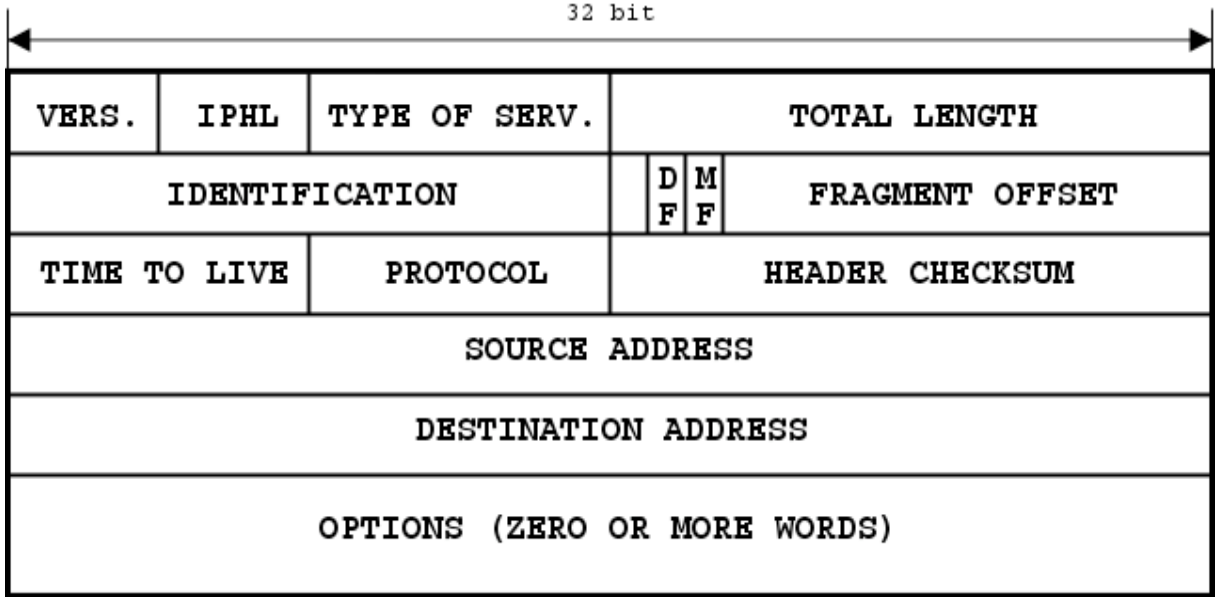
- **IPv6** forthcoming
  - solution to the address space exhaustion of IPv4
    - Predicted for a while, but limit not reached yet
    - Solutions for preserving numbers in IPv4 (masquerading, private networks ...)
  - at the moment nobody exactly knows when it will be used other then in backbone structures
  - predicted within the next 10 years
  - 3G/UMTS mobile telephone market may push IPv6
  - defined for a while

Internet Protocol Details

- **Protocol header** includes:
  - Version field
  - Source and Destination addresses
  - Lengths (header, options, data)
  - Header checksum
  - Fragmentation control
  - TTL, and TOS info
- But TOS info often ignored
  - easily changeable along the path (so what for?)

Internet Protocol Header Details

- **Version** field (4 standard, 5 STII, 6 next gen IP) and IP header length are of 4 byte
  - IP header normally consists of 20 Bytes, with options for more
  - Length needed to compute where next header starts



Internet Protocol Header Details

- **IP options** may sum up to 40Byte
- **Total length** field is 16bit, maximum packet length therefore may not exceed 64kByte
  - Minimum is 20Byte (just the IP header)
  - MTU of standard physical networks much smaller (e.g. 1500/9000Byte in Ethernet)
- 16bit identification field for fragments
  - Set for every packet by original sender of datagram
  - Sender can not know if fragmentation may occur
  - Initial message segmentation may not be small enough
  - Copied into each datagram during fragmentation

Internet Protocol Header – Fragmentation

- Content of 16bit **identification field** is computed by sender
  - Different OS use different computing schemes (e.g. tool “nmap”)
  - Might give away information on OS, internal network structure
  - Masqueraded machines could be identified by their fragmentation IDs
  - Counter on every machine will have different values (amount of traffic generated, computing scheme ...)
  - A private network may give more information away than intended

Internet Protocol Header – Fragmentation

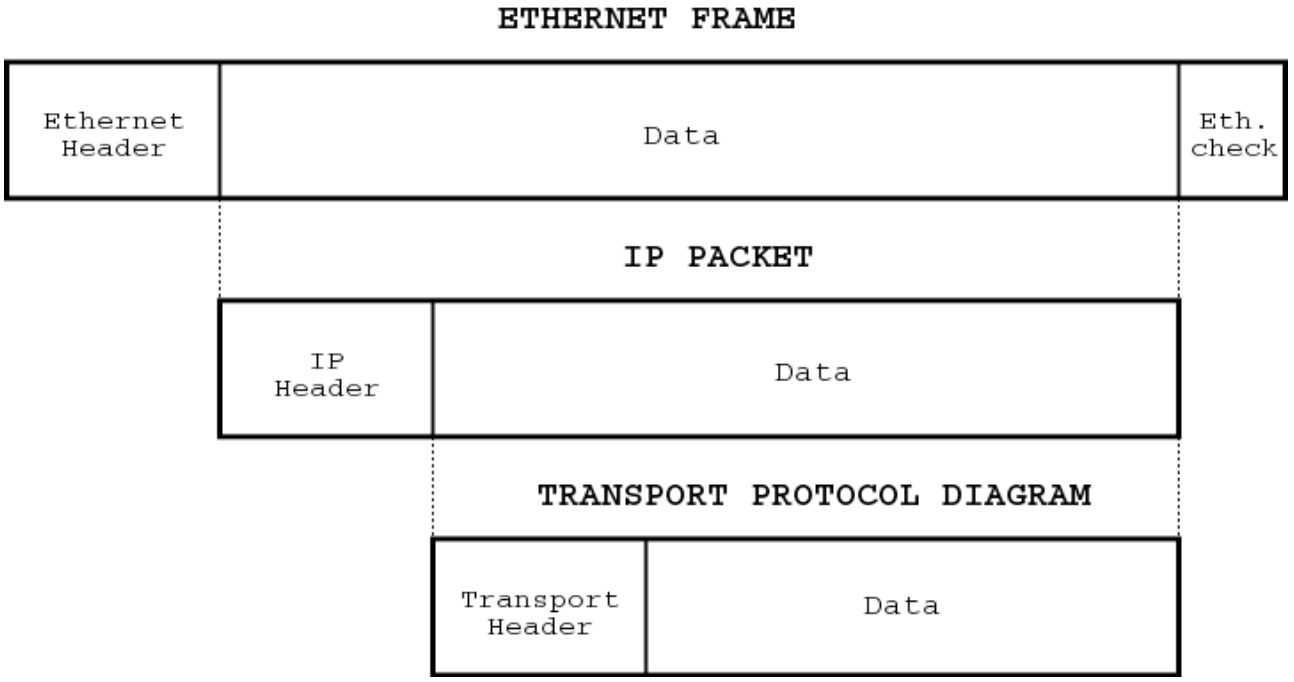
- **Flags for fragmentation control**
  - MF: more fragments (follow)
  - DF: dont fragment (some protocol implementation like DHCP in Boot-ROMs are not able to reassemble fragmented packets), feature may be used for MTU path discovery (increment packet size until ICMP error message is generated because of fragmentation need)
- **Fragmentation offset**
  - Offset of this fragment into the original datagram
  - Zero if no fragmentation used
  - why offset and not fragment number? - if further fragmentation is needed
- Fragmentation will be handled later

Internet Protocol Header – Protocol Field

- Protocol field – the payload with headers removed is passed to a higher layer in the networking stack -> where?
- There are different transportation layer protocols for different purposes
- 1: ICMP – discussed later
- 6: TCP – Transmission Control Protocol
- 17: UDP - User Datagram Protocol
- 50: ESP – Encapsulating Security Payload
- 51: AH - Authentication Header
- All protocol names and corresponding numbers are listed in (/etc/)protocols file (Linux operating system)

Internet Protocol Header – Protocol Field

- In general: each layer has to provide the information of which upper layer should process given types of packets
- Each protocol adds its own header to the packet



Internet Protocol Header – Address Fields

- **Source address**
  - 32 bit length defines the IP address space
  - should never be changed through ordinary routing (there are some exceptions like network address translation (NAT))
  - protocol does not force authentication of source (often enforced by modern routers now)
- **Destination address**
  - 32 bit length defines the IP address space
  - should never be changed through ordinary routing
  - changes when source routing used (realised through IP option header)

Internet Protocol – Header Details

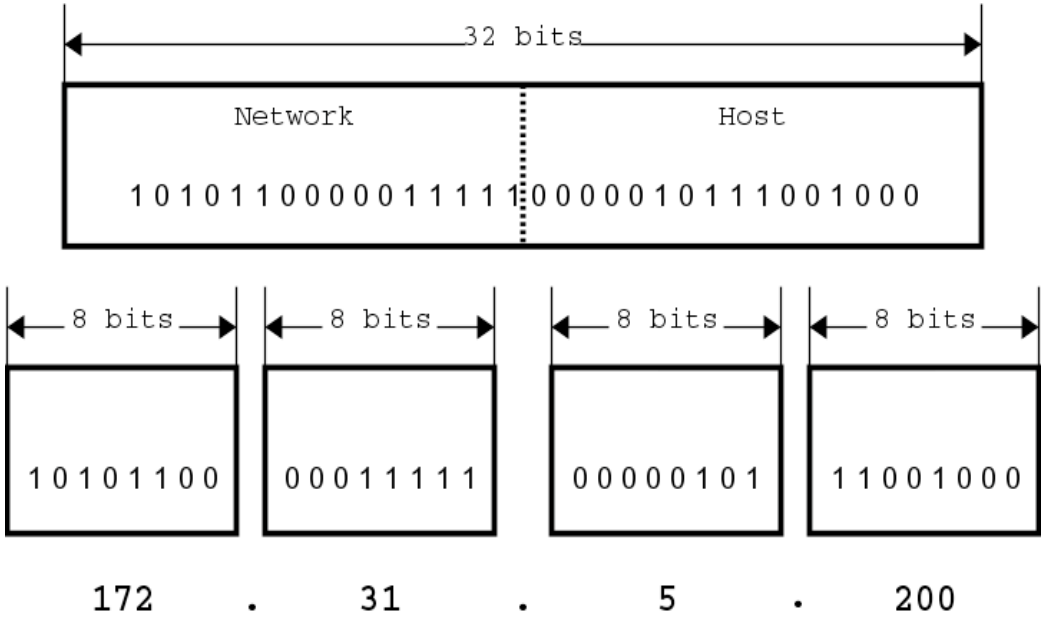
- **Source routing**
  - Special handling for particular datagrams, sometimes don't take router's "fast path"
  - Rarely used, but the more common are: Loose Source Routing, Strict Source Routing and Record Route
  - Timestamp
  - Must be copied on fragmentation
- Back to IPs basic routing principles and addressing

IP – Addressing Scheme

- We saw that IP packet header reserved two 32 bit fields for source and destination address
- For computation for delivery decisions the binary form is used only
- Programs and operating systems implementing IP automatically convert the addresses between the two representations
- IP addresses are topologically sensitive
  - Interfaces on same network share prefix
  - Prefix is assigned via ISP/local network administrator
  - 32-bit globally unique

IP – Addressing Scheme

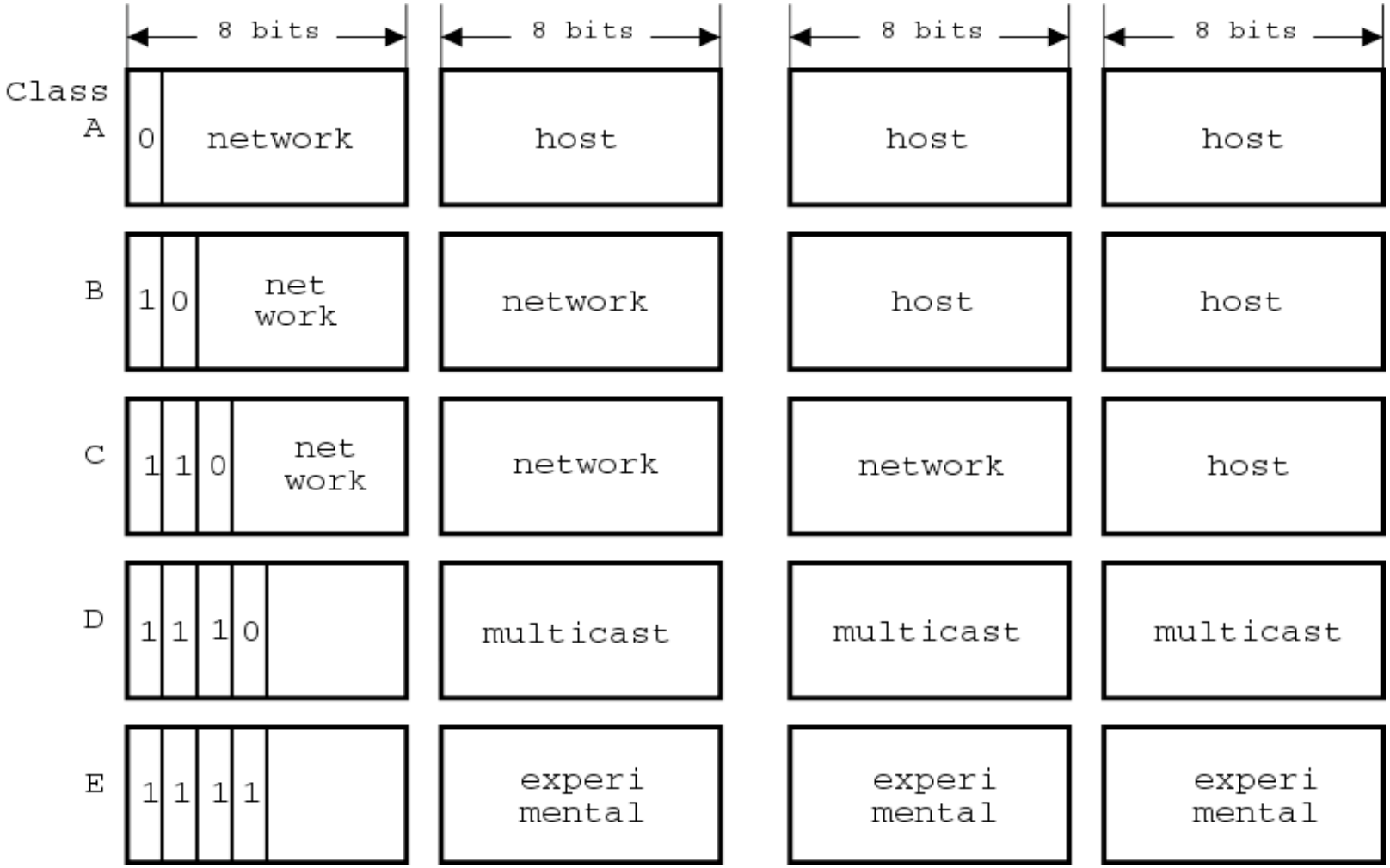
- Address is split into two virtual parts: network and host part
  - See later how division is done
- For better reading the binary representation could be split into four octets, which are transferred into the decimal system



IP – Addressing Scheme

- The **early** IP standard defined five address classes: A, B, C, D and E
- An IP address should be selfexplanatory, it should contain information on the networking sub structures
  - History by now (see early RFCs on IP)
- In this view the address consists of a pattern of high order bits, which shows their class, the network and the host component
- Machines in the same network share a common prefix (the class definition and network component of IP) and must a have unique suffix (the host component of IP)

IP – Historic Address Classes



IP – Historic Address Classes

- Class A: (high order bit: 0)
  - Large Organizations, few nets (127), huge number of hosts (16.7 million)
  - Address range in decimal notation 0.0.0.0 – 127.255.255.255
- Class B: (high order bits: 10)
  - Medium sized organizations and firms, e.g. University of Freiburg, some nets (16,384) and large number of hosts (65,536)
  - Address range 128.0.0.0 – 191.255.255.255
- Class C: (high order bits: 110)
  - Small organizations and firms, relatively large number of nets (2,097,152) with a small number of hosts per net (256)
  - Ranging from 192.0.0.0 – 223.255.255.255

IP – Historic Address Classes

- Class D: (high order bits: 1110)
  - Multicast addresses, but services are not very often used
  - Address range 224.0.0.0 – 239.255.255.255
- Class E: (high order bits: 1111)
  - Declared for experimental use only
  - Address range 240.0.0.0 – 255.255.255.255
- Theoretical address space is 4,294,967,296 (seems a lot :-) - but population on earth is higher by now)
- But the address space usable for the “Internet” is limited to addresses from 1.X.Y.Z up to 223.X.Y.Z

IP – Addressing Scheme

- But you will loose some more addresses:
- Special addresses like:
  - 0.0.0.0 defines the default route (explained later, route for the “whole Internet”) or the start address of a host searching for a dynamically provided IP (DHCP, last lecture)
  - 255.255.255.255 local broadcast address (and destination for hosts seeking an IP via DHCP)
  - 127.0.0.0 loop back network address (you will need only one address within this range and use typically 127.0.0.1). This address is used by every host implementing IP (software using IP for communication is usable without Internet connection)
  - 169.254.0.0 ... 169.254.255.255 is reserved address space for IP ad-hoc/auto configuration without a central server like DHCP (last lecture)

IP – “Private” Addresses

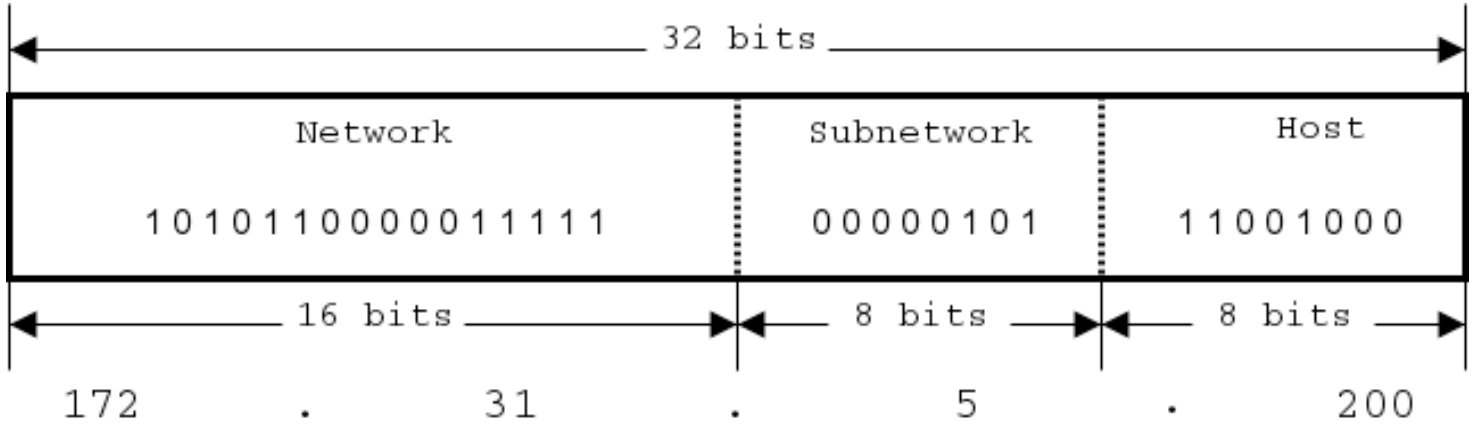
- Addresses reserved for “private” use – many organizations, enterprises, flat-sharing communities need IP communication for their applications without or restricted Internet access
  - 10.0.0.0 – 10.255.255.255 (within the class A range)
  - 172.16.0.0 – 172.31.255.255 (16 class B networks)
  - 192.168.0.0 – 192.168.255.255 (65,536 class C networks)
- University WLAN, private LAN is using 10.X.Y.Z addresses
- Addresses within these ranges should be discarded on Internet routers
- Address classifying helped in the beginning for faster network decision computation, routers had limited memory and CPU power

IP Addressing

- For addressing whole subnets or addressing all hosts within a given subnet (possibility depends on the underlying physical network) special IP addresses are introduced
  - Network number is the smallest IP address in a given (sub)network. It does not address a single machine and may not be assigned to a host. It is used with routing tables (explained later in detail)
  - Broadcast address is the largest possible IP in a network. It should be not assigned to a host, but allows the possibility to reach all hosts in a network with just one packet
- If we use the example class B address 172.31.5.200, this machine is a member of a network with the network number 172.31.0.0 and a broadcast address 172.31.255.255

IP Subnetting

- Networks with huge number of hosts could be split into subnets for better administration and considerations on physical topology and global spanning net
- The example class B network 172.16 with 65536 host IP numbers in it, allows 256 subnetworks with 256 hosts in it if split on the byte boundary
- But: The resulting 256 “class C networks” have the same high order bit like the original class B network

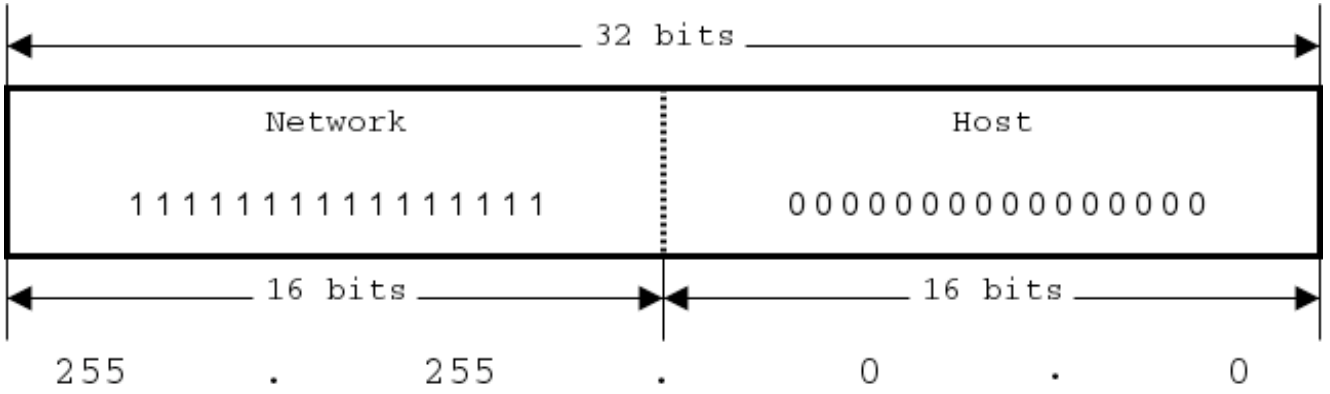


IP – the Subnetting Scheme

- The number of class B networks was much to small (Germany has around 100(?) universities and colleges and therefore would need for them at least 100 class B networks out of 16,384)
- There is no real need for class A networks (imagine a big company connecting all their machines to the Internet directly – e.g. IBM or HP had class A networks or a provider with over a million customers in a given area)
- There is great need for bigger networks than class C but much smaller then B
- The waste of addresses with the old scheme was enormous and the need for IP v6 seemed very urgent :-)
- Concept of subnetting and supernetting was introduced

IP – the Subnetting Scheme

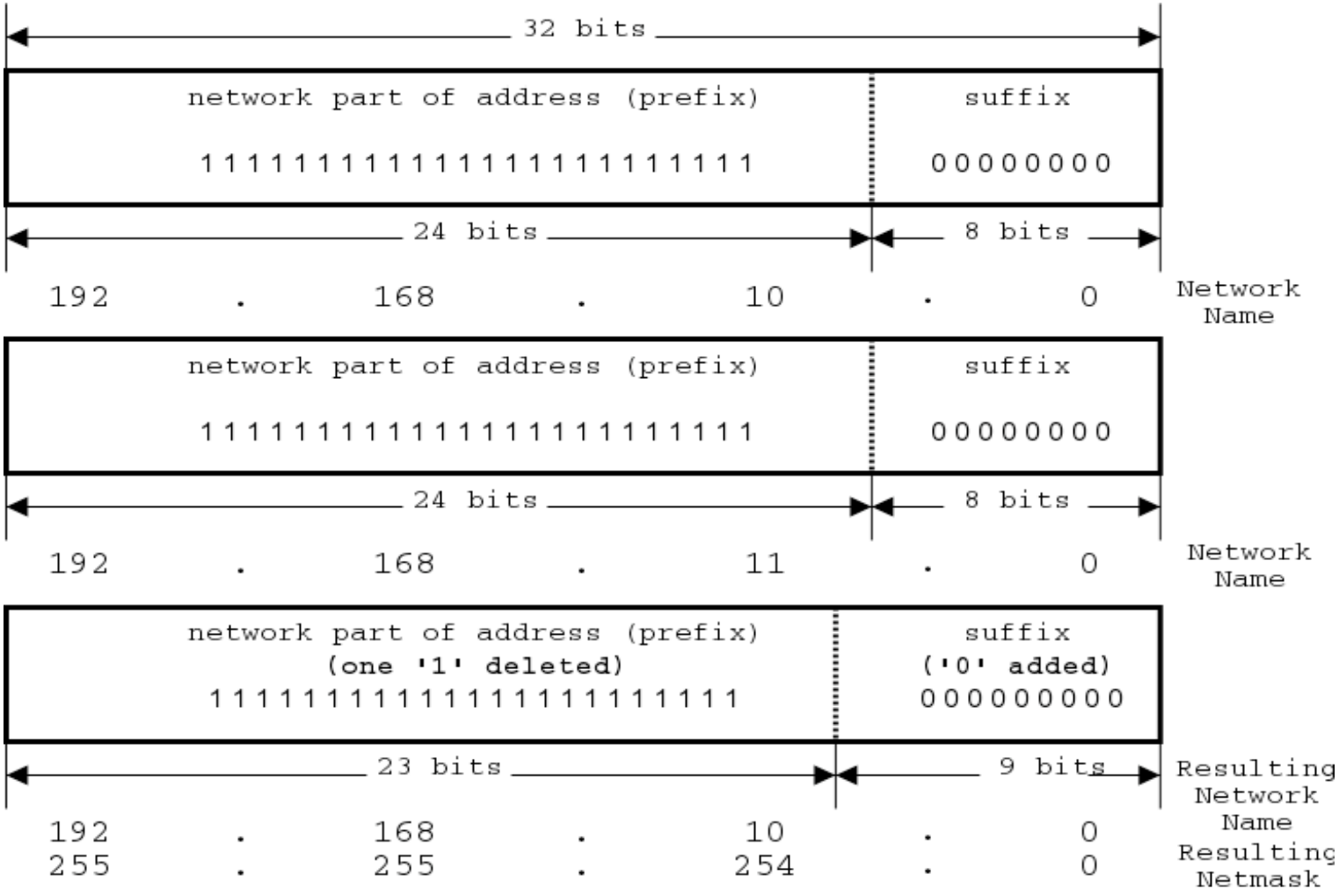
- Introduction of netmasks (were implicit with old addressing scheme)
- Supernetting means the combining of address ranges into larger ones with just one common network and broadcast address
- Result: IP addresses aren't self explanatory any more
- For the information of the span of subnetwork netmasks where introduced: “1” marks prefix part of IP (network) “0” marks suffix part of IP (host)



IP – the Subnetting Scheme

- The netmask of 255.255.0.0 just marks an old class B network
- 255.0.0.0 depicts class A and 255.255.255.0 class C
- The netmask may be abbreviated with the numbers of “1” in the netmask (e.g. class A: 8, B: 16, C: 24)
- If you combine two class C networks into a larger one, e.g.
  - network 192.168.10.0 with broadcast 192.168.10.255 and
  - network 192.168.11.0 with broadcast 192.168.11.255
- The result is:
  - network 192.168.10.0 with broadcast 192.168.11.255 and netmask 255.255.254.0

IP – the Subnetting Scheme



IP – the Subnetting Scheme

- Split of netmasks into prefix and suffix is done on the boundary between the “1” and “0”
- e.g. 1111 1111.1111 1111.1 000 0000.0000 0000 is 255.255.128.0 (some commands use abbreviation 17, first practical course)
- We would split that way the network 132.230.0.0/255.255.0.0 into two subnets: 132.230.0.0 – 132.230.127.255 and 132.230.128.0 – 132.230.255.255
- But we could split that network another way:
- e.g. 1111 1111.1111 1111.0000 0000.0000 0001 is 255.255.0.1 and get two subnets, one with the even (in the last octet) IP addresses and one with the odd IP addresses in it
- Managing networks that way implements a lot of risks :-)

IP – New Subnetting Scheme

- Networks may be combined into larger ones, large networks may be split
- Splitting networks means adding a “1” to the netmask (increasing prefix and decreasing suffix)
- Combining networks via removing “1” from the netmask and adding “0”
- Therefore at the moment there are enough blocks of class C networks still available for assignment (the need for IP v6 declined)
- Additional information is needed, routers need more memory to store netmasks in combination with net names
- Routing tables could be simplified through aggregation of routes

Literature/Reading

- Read and recap further on IP configuration
  - IP configuration and address structure of IPv4, general routing principles, classes, class-less routing, IP header
  - Packet fragmentation in IPv4 networks
  - NAT – network address translation
  - ICMP as an IP helper protocol
  - DHCP especially relay

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