

5. Network Layer

5.1 Use of IP addresses

IP addresses and subnet masks are necessary to identify if the destination of a packet is within the own network or not.

5.2 IPv4 address

The IP address is a 32-bit number, thus there can be $4.294.967.296 = 2^{32}$ different IPv4-addresses. IPv4 = Internet Protocol version 4.

The IPv6-addresses are about to be implemented. IPv6 addresses are 128 bit numbers.

IPv4-addresses are usually written in 4 octets separated by dots. Each octet is often converted to a decimal number between 0 and 255.

Example:

1 octet = 8 bits = 1 byte

10101100	.	00010000	.	11111110	.	00000001
↓		↓		↓		↓
172	.	16	.	254	.	1

5.3 Subnet Mask

An IPv4-address is divided in two portions, the *network portion* and the *host portion*.

All hosts with the same network portion are forming one network which is the condition that the hosts can directly communicate between each other via hubs, switches or cross link cables. In one network no IP-address is allowed to appear twice.

For communications between two networks with different network portions a router (often also called gateway) is needed.

The *subnet mask* indicates which part of the IPv4-address forms the network portion and which part forms the host portion.

A subnet mask is a 32 bit number starting with a series of 1 followed by a series of 0.

Example:

	network portion	host portion
IPv4-address	10101100 . 00010000 . 10111	110 . 00000001
subnet mask	11111111 . 11111111 . 11111	000 . 00000000

5.4 CIDR syntax

The CIDR syntax (deut.: Schreibweise, franc.: notation) of an IPv4 address and its subnet mask is as follows:

192.168.0.34 / 24

The "/24" says that the first 24 bits of the IP address are forming the network portion. As a consequence the last 32-24=8 bits are forming the host portion.

5.5 Describing a network

There is a slight but important difference between the terms network portion and network address. *The network address* is the IP address of a network where all the bits of the host portion are 0. So the network address is the lowest possible IPv4 address in a network.

Example:

	network portion	host portion
a host address	10101100 . 00010000 . 10111	110 . 00000001
the subnet mask	11111111 . 11111111 . 11111	000 . 00000000
the network address	10101100 . 00010000 . 10111	000 . 00000000

network address = host address _____ subnet mask

To *describe a complete network* you write the network address and the subnet mask in CIDR syntax.

Example:

192.168.0.0 / 24 is describing the whole network with
the IP addresses 192.168.0.0 till 192.168.0.255

The first and the last IP-address in a network are always reserved and cannot be allocated to a host. The first IP-address (host portion=0) cannot be used as it corresponds to the network address. The last one is used for broadcast message. A broadcast message is a message addressed to all hosts on a network.

The default gateway is the router in the network that is responsible to treat all traffic to and from IP addresses that do not belong to the network of the host. So the default gateway needs to have one IP address of each network it belongs to.

Exercise 1:

Are the following host couples part of the same network? Justify your answer.

- a) 153.160.12.3/24 and 153.160.13.4/24
- b) 153.160.12.3/16 and 153.160.13.4/16
- c) 10.0.0.5/30 and 10.0.0.4/30
- d) 10.194.0.3 and 10.200.0.5 with subnet mask 255.192.0.0

Exercise 2:

How many hosts can be part of the following networks?

- a) 153.160.12.0/24
- b) 153.160.0.0/16
- c) 10.0.0.0/30
- d) 10.192.0.0/10

Exercise 3:

A host (172.16.50.53/16) wants to send a request for a web-page to the IP address 172.16.35.4. Does the request need to be forwarded to the default gateway? Justify your answer.

Exercise 4:

What is the logical condition that has to be checked between the 32 bits of the hosts IPv4 address IP-HOST, the 32 bits of the subnet mask MASK and the 32 bits of the destination IPv4 address IP-DEST in order to determine if the packet needs to be forwarded to the default gateway or not?

Exercise 5:

Suggest a network to which you can connect at least 1000 hosts without wasting unnecessarily IP addresses.

5.6 Private IP-addresses

No IP-address is allowed to appear twice in the Internet. That's why every IP-address used in the Internet has to be reserved at the IANA (Internet Assigned Numbers Authority). For local networks this approach is not practical. In addition the number of available IPv4-adresses is insufficient for all hosts in use today.

The solution for both problems is "private IP-addresses". These are ranges of addresses that can be freely used within private networks and that are not allowed to be used in the public Internet.

Three ranges of private IPv4-addresses have been defined. These ranges can of course be split into subnets.

1. 10.0.0.0/8
2. 172.16.0.0/12
3. 192.168.0.0/16 192.168.0.0 -192.168.255.255
 192.168.0.0-192.168.0.255
 192.168.1.0-192.168.1.255

Exercise 6:

Mark the private IPv4 addresses.

10.0.9.23	172.0.1.236	192.1.0.1
10.255.9.23	172.12.0.12	192.168.50.1
11.9.9.23	172.16.0.12	192.172.50.1
11.254.9.23	172.32.255.255	192.186.10.0
	172.63.0.1	192.255.50.1

Exercise 7:

Determine the lowest and highest IPv4-address of every private IPv4-address range as well as the total number of IPv4-addresses in every range.

Exercise 8:

- Into how many /24 subnets can you split the network 192.168.0.0/16?
- Into how many /24 subnets can you split the network 10.0.0.0/8?
- Into how many /16 subnets can you split the network 10.0.0.0/8?
- Into how many /24 subnets can you split the network 172.16.0.0/12?
- Into how many /16 subnets can you split the network 172.16.0.0/12?
- Construct a formula to calculate the number of subnets if you know the length of the network portion and the length of the subnet portion.

5.7 A piece of history (classful routing)

(source: <http://www.netplanet.org/adressierung/subnetting.shtml>)

You might ask yourself why the private IP address ranges start and end in the middle of nowhere within the total IPv4 address range. This has a historical reason. Subnet masks were only introduced in 1985. Before that date it was the first bits of an IP-address that helped to determine if a destination IP-address was part of the same network or not.

Example:

If the first bit of your own IP address was a 0, then you were part of a so called *class A network*. In a class A network the network portion was defined to be 8 bit long. Thus if the first bit of your own IP address was a 0 AND the first 8 bits of the destination IP address were identical to the first 8 bits of your own IP address then the packet did not need to be sent to the default gateway.

This method was called *classful routing*.

Class definitions:

Class	Leading bits	Length of network portion	Number of possible networks of this class	IP addresses per network
Class A	0	8		
Class B	10	16		
Class C	110	24		

Exercise 9:

Complete the above table.

Exercise 10:

- What type of network class is the network 10.0.0.0/8?
- What type of network class is the network 172.20.0.0/16?
- What type of network class is the network 192.168.50.0/24?

Exercise 11:

- a) How many private class C networks do exist?
- b) How many private class B networks do exist?
- c) How many private class A networks do exist?

Already in 1993 the classful routing has been replaced by the *Classless Inter-Domain Routing* introducing the VLSM technique (variable length subnet mask). Unfortunately today the terms of Class A, B & C are still in use and even often misused. As an example the network 20.3.0.0/16 might be called by some as a class B network as the network portion has a length of 16 bits, but this is false as the leading bits of this network are not 10.

In order to avoid all misunderstandings the terms of network classes shouldn't be used anymore.

5.8 ipconfig command

With the ipconfig command you can question a host for its IP-addresses, subnet-masks and default gateway IP addresses of every network it is connected to.

Example:

```
C:\> ipconfig

Ethernet adapter Ethernet:

Connection-specific DNS Suffix:

Link-local IPv6 Address : fe80::e000:727:696c:8bfb%17
IPv4 Address : 192.168.99.5
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.99.19
```

If in addition to the IP addresses also the MAC addresses of the network cards are needed, then type ipconfig/all.

Example:

```
C:\> ipconfig /all

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Description . . . . . Realtek PCIe GBE Family Controller
Physical Address . . . . . 74-D4-35-B3-8E-E1
DHCP Enabled . . . . . No
Autoconfiguration Enabled . . . . . Yes
Link-local IPv6 Address . . . . . fe80::e000:727:696c:8bfb%17(Preferred)
IPv4 Address . . . . . 192.168.99.5(Preferred)
Subnet . . . . . 255.255.255.0
Default . . . . . 192.168.99.19
DHCPv6 . . . . . 292869173
DHCPv6 Client DUID . . . . . 00-01-00-01-1B-CA-DD-C2-74-D4-35-B3-8E-E1
DNS Servers . . . . . 192.168.99.19
NetBIOS over Tcpip . . . . . Enabled
```

5.9 Routing

5.9.1 Definition

A router is a network component that is connecting at least two separate networks together.

The default gateway is a router that will be used from the hosts by default (= as a standard).

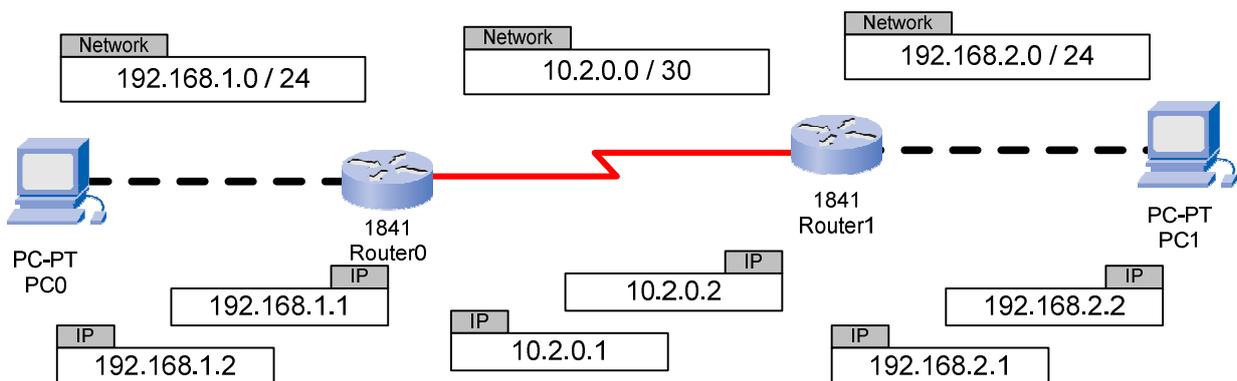
5.9.2 Routing table

The routing table tells the router what network is connected to which interface (plug) on the router. Every line in the routing table is called a route. The routing table is structured as follows:

Destination Network		Interface or next hop	Metric
network address	subnet mask		

Exercise 12:

Plan the IP-address ranges for the following internetwork:



5.9.3 Static routing

In *static routing* all routes are manually entered into the routers.

Example of the static routes for the internetwork in exercise 12:

Router0

Destination Network		Interface or next hop	Metric
network address	subnet mask		
192.168.2.0	24	10.2.0.2	

Router1

Destination Network		Interface or next hop	Metric
network address	subnet mask		
192.168.1.0	24	10.2.0.1	

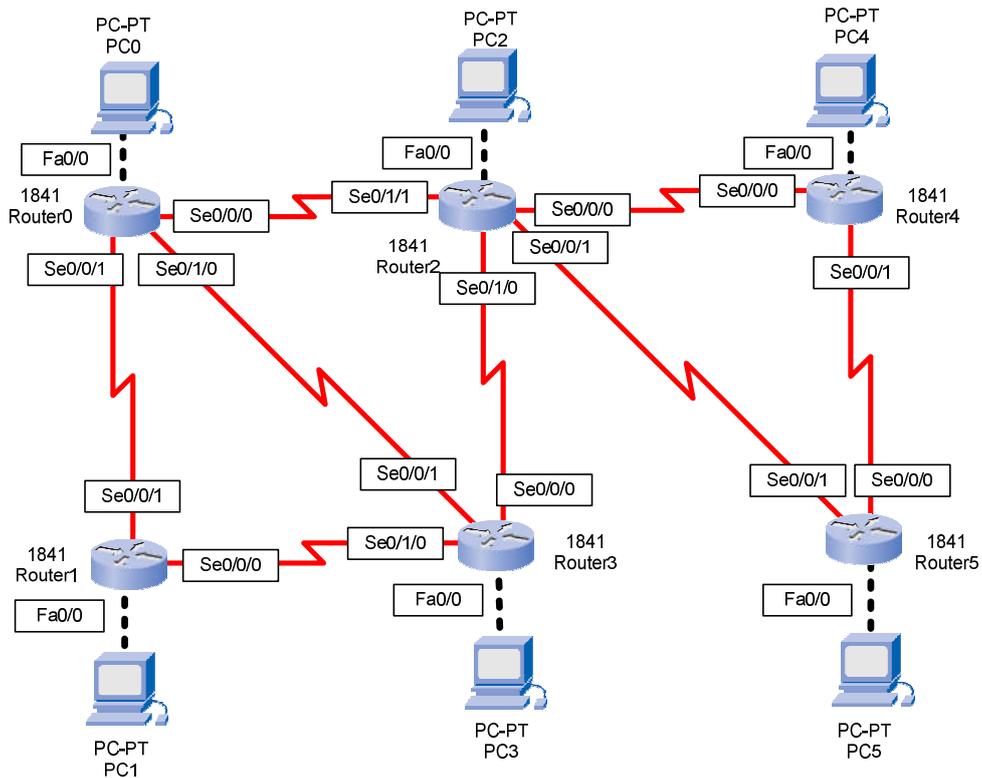
In static routing the routing table only contains routes to networks that are NOT connected to the router itself.

The *metric* is relevant when the internetwork allows several alternative routes to the same network.

The lower the value of the metric is the higher the priority of the route will be.

Exercise 13:

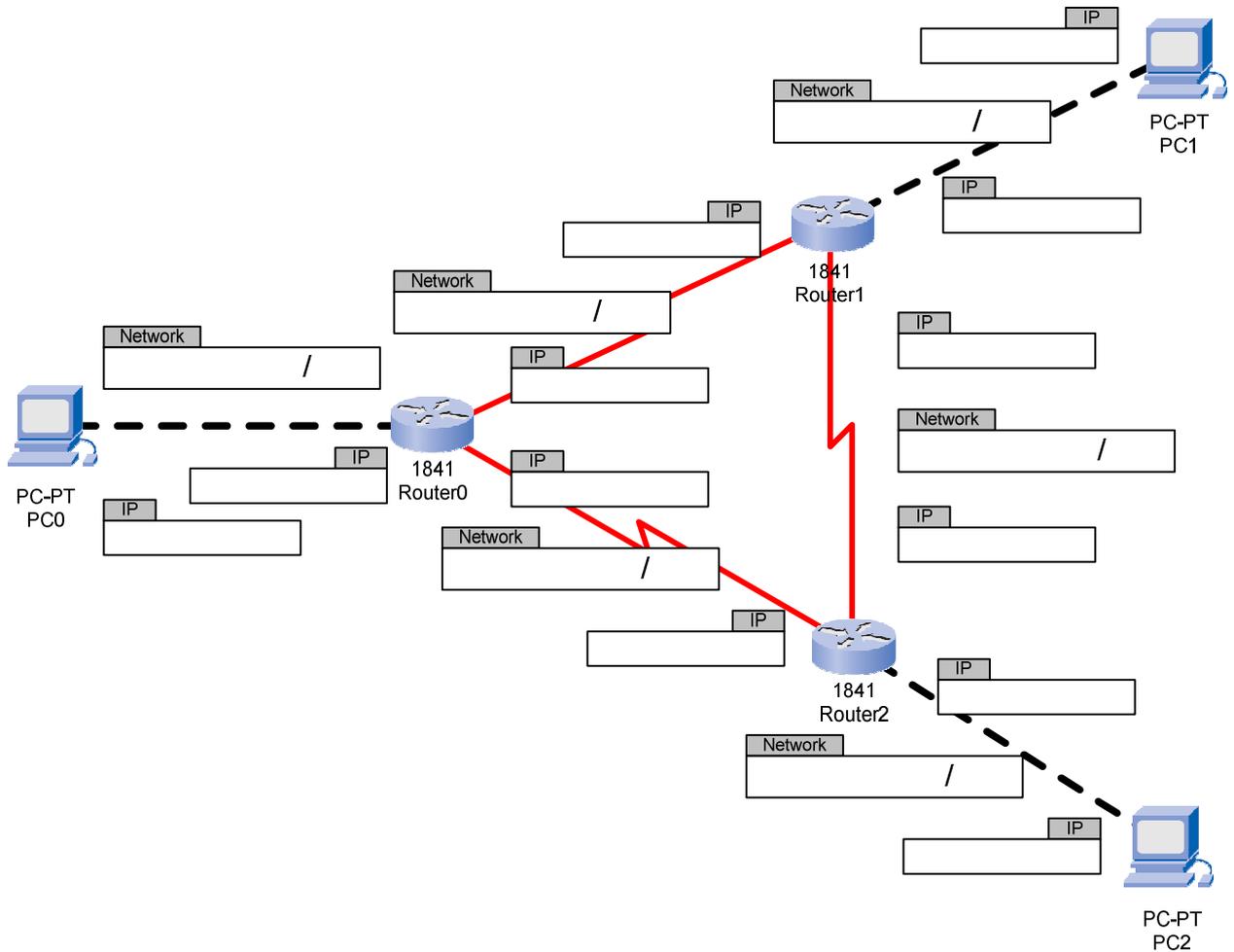
- Mark the way a ping will take from PC1 to the IPv4 address 15.150.0.10 through the following internetwork with the static routing tables below.
- Convert the destination IP address and the network addresses on the way to the destination in binary numbers.
- Mark the corresponding routes in the routing tables.



<u>Router0</u>			<u>Router2</u>			<u>Router4</u>		
network address	subnet mask	interface	network address	subnet mask	interface	network address	subnet mask	interface
0.0.0.0	/0	Se0/0/1	0.0.0.0	/0	Se0/1/1	15.160.0.0	/11	Se0/0/1
15.0.0.0	/11	Se0/0/1	15.0.0.0	/10	Se0/1/1	15.0.0.0	/9	Se0/0/0
15.64.0.0	/10	Se0/1/0	15.96.0.0	/11	Se0/1/1	15.128.0.0	/11	Fa0/0
15.128.0.0	/9	Se0/0/0	15.128.0.0	/9	Se0/0/1			
15.32.0.0	/11	Fa0/0	15.64.0.0	/11	Fa0/0			
<u>Router1</u>			<u>Router3</u>			<u>Router5</u>		
network address	subnet mask	interface	network address	subnet mask	interface	network address	subnet mask	interface
0.0.0.0	/0	Se0/0/0	0.0.0.0	/0	Se0/0/0	15.128.0.0	/11	Se0/0/0
15.32.0.0	/11	Se0/0/1	15.64.0.0	/11	Se0/0/0	15.160.0.0	/11	Fa0/0
15.0.0.0	/11	Fa0/0	15.92.0.0	/11	Fa0/0	15.0.0.0	/9	Se0/0/1
			15.0.0.0	/10	Se0/1/0			

Exercise 14:

Plan the following internetwork and prepare the static routing tables for all three routers.



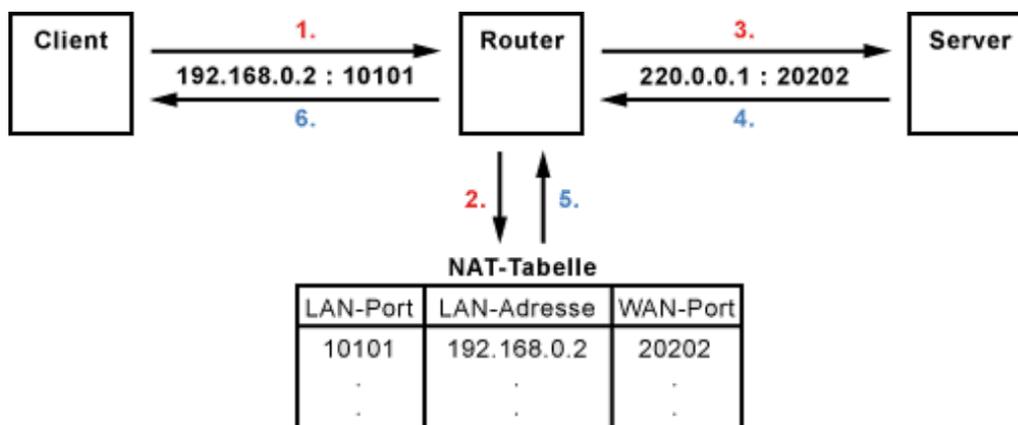
5.9.4 Dynamic routing

Static routing can get very complex in huge internetworks. In addition static routing with alternative routes is limited to internetworks with 3 routers, see lab 7.

Dynamic routing protocols allow routers to communicate between each other and to generate the routes automatically. An example of a dynamic routing protocol is EIGRP (Enhanced Interior Gateway Routing Protocol). All that needs to be done is to enter the networks that a router is connected to into the configuration of the router.

5.9.5 Network address translation (NAT) and Port address translation (PAT)

How NAT works:



As private IP-addresses are not allowed to appear in the header of whatever packet in the public Internet, a special technique has to be applied to exchange the private "in house" IP-addresses by the unique public IP-address of the default gateway once the packet is leaving the private network. This technique is called NAT (network address translation).

By doing NAT the information of the real source IP address is lost. If multiple clients are connected to the private network, the default gateway could not return the answer to a request when doing NAT only. Therefore it does a PAT too. The "private" port number of the request is changed to a public port number being synonym for the private IP address and port number pair.

The associations of the public port number with the private IP address and port number are saved in the so called NAT table within the router.

5.10 This and that

5.10.1 IPv4 loopback addresses

The IP addresses 127.0.0.1 to 127.255.255.254 refer all to the local host. When sending to one of these addresses the destination will be identical to the source.

If you type <http://127.0.0.1> or <http://localhost> in the browser of a host you are running a webserver on, you will always see the webpage hosted on this local webserver.

5.10.2 IPv4 Multicast addresses

The IPv4 multicast addresses 224.0.0.0 to 239.255.255.255 are reserved for multicast. Multicast allows to send information from one source host to many destination hosts simultaneously. This can be used to spread out a backup image to several hosts at the same time or to send the video stream of a TV station simultaneously to multiple TVs when using IP TV.

5.10.3 APIPA

With APIPA, DHCP clients can automatically self-configure an IP address and subnet mask when a DHCP server isn't available. When a DHCP client boots up, it first looks for a DHCP server in order to obtain an IP address and subnet mask. If the client is unable to find the information, it uses APIPA to automatically configure itself with an IP address. The IP address range is 169.254.0.1 through 169.254.255.254. The client also configures itself with a default class B subnet mask of 255.255.0.0. A client uses the self-configured IP address until a DHCP server becomes available.

5.10.4 Block diagram of an Integrated Services Router

