3. IP-kerroksen muita protokollia ja mekanismeja

- ICMP (Internet Control Message Protocol)
- ARP (Address Resolution Protocol)
- DHCP (Dynamic Host Configuration Protocol)
- CIDR (Classless InterDomain Routing)
- NAT (Network Address Translation)
- RIP (Routing Information Protocol)
- OSPF (Open Shortest Path First)
- BGP (Border Gateway Protocol)

3.1. ICMP (Internet Control Message Protocol)

- Verkkoinformaation välittämiseen isäntäkoneiden ja reitittimien välillä
  - reitittimet ilmoittavat verkon ongelmista toisilleen
  - reitittimet ilmoittavat lähetysten kohtalosta isäntäkoneille
    - "Destination network unreachable"
  - testauspakettien lähettäminen
- **Toteutettu IP-protokollan yhteyteen**

- ICMP-sanomat kapseloidaan IP-paketteihin
  - TCP- ja UDP-segmenttien tavoin
  - IP-paketin protokollakentässä 'ICMP'
  - => paketti annetaan ICMP:n käsiteltäväksi
- ICMP-sanomassa
  - tyyppi + koodi kertovat sanoman
  - 8 tavua sanoman aiheuttaneesta IP-paketista
    - jotta lähettäjä tietää, mikä paketti aiheutti sanoman

ICMP-sanomia

- Destination unreachable
- Time-To-Live exceeded
- Parameter problem
- Source quench
- Redirect
- Echo request, Echo reply
- Timestamp request, Timestamp reply

Summary of ICMP Message Types

- 0 Echo Reply
- 3 Destination Unreachable
- 4 Source Quench
- 5 Redirect
- 8 Echo
- 11 Time Exceeded
- 12 Parameter Problem
- 13 Timestamp
- 14 Timestamp Reply
- 15 Information Request
- 16 Information Reply

Type 3: Destination unreachable

Code

0 = net unreachable;

1 = host unreachable;

2 = protocol unreachable;

3 = port unreachable;

4 = fragmentation needed and DF set;

5 = source route failed.

6 = network unknown

7 = host unknown

Type 11:Time-To-Live exceeded

Sanoma hävitettiin, koska sen elinaika ehti kulua umpeen

Code

0 = time to live exceeded in transit;

1 = fragment reassembly time exceeded.

Type 12: Parameter problem

Virhe IP-otsakkeessa

- Sanomassa osoitin, joka kertoo virheellisen
- kohdan
  - ilmoittaa virheellisen tavun
  - esim. osoittimen arvo 1 kertoo, että vika on TOS-kentässä
- Sanoma lähetetään vain, jos IP-sanoma joudutaan virheen takia hävittämään

Type 4: Source quench

Tällä voidaan ilmoittaa lähettäjälle, että sen tulee vähentää lähettämistään

- reititin joutuu hävittämään paketteja puskuristaan
- vastaanottaja ei ehdi käsitellä paketteja sitä vauhtia kun niitä tulee

HUOM! Käyttöä ei suositella

- TCP-ruuhkanvalvonta
- TCP-vuonvalvonta

Type 5: Redirect

Reititin voi pyytää isäntäkonetta lähettämään sanoman toiselle reitittimelle

Code:

0 = Redirect datagrams for the Network.

1 = Redirect datagrams for the Host.

2 = Redirect datagrams for the Type of Service and Network.

3 = Redirect datagrams for the Type of Service and Host

Echo-sanomat

Type 0: echo reply
Type 8: echo request

Echo-pyynnön sanoma tulee palauttaa echo-vastauksessa

- **ping-ohjelma** lähettää echo-pyynnön koneelle ja pyynnön vastaanottanut kone palauttaa sen

Timestamp-sanomat

type 13: timestamp message
type 14: timestamp reply message

lähettäjä leimaa lähettäessään
ja vastaanottaja saadessaan ja
uudelleenlähettäessään

- The timestamp is 32 bits of milliseconds since midnight UT.

Traceroute-ohjelma

- Lähettää kohdekoneelle ICMP-sanomia, joissa TTL on 1, 2, 3,... sekuntia
  - reititin, jolla jonkin sanoman TTL loppuu, lähettää tästä ilmoituksen, jossa on reitittimen osoite ja aikaleima
- Lähettäjä saa näin selville kiertoajan ja reitittimen eli kuljetun reitin lähettäjältä kohdekoneelle

3.2. ARP (Address Resolution Protocol)

- muuttaa IP-osoitteen siirtoyhteyskerroksen osoitteeksi
  - lähiverkkoon liitetyt laitteet ymmärtävät vain LAN-osoitteita
    - esim. eetteriverkon 48-bittisiä osoitteita
- yleislähetys lähiverkkoon
  - “Kenellä on IP-osoite vv.xx.yy.zz ?”
  - vastauksena osoitteen omistavan laitteen lähiverkko-osoite

- optimointia:
  - kyselyn tulos välimuistiin
    - talletetaan muutaman minuutin ajan
  - kyselijä liittää omat osoitteensa kyselyyn
  - alustettaessa jokainen laite ilmoittaa osoitteensa muille
    - kysyy omaa osoitettaan
    - jos tulee vastaus, niin konfigurointivirhe

- reitittimet eivät välitä ARP-kyselyjä
  - joko reititin vastaa itse ARP-kyselyihin (proxy ARP)
  - tai muihin verkkoihin menevät paketit lähetetään oletuspaikkaan, joka huolehtii niiden lähettämisestä

3.3. DHCP (Dynamic Host Configuration Protocol) (RFC 2131)

- **IP-osoitteen antaminen koneelle**
- **DHCP-palvelin**
  - antaa koneille IP-osoitteita
  - myös tilapäisiä IP-osoitteita
- **DHCP- välittäjä agentti** (reititin) **jokaisessa lähiverkossa**
  - tuntee DHCP-palvelim osoitteen
  - välittää oman verkon DHCP DISCOVER –paketit DHCP-palvelimelle

- **DHCP discover message:**
  - yleislähetyksenä
    - kohde: 255.255.255.255; lähde 0.0.0.0
- **DHCP offer message**
  - vastauksena DHCP-palvelimelta
    - voi tulla useita, jos useita palvelimia
  - IP-osoite ja sen vuokra-aika (lease)
- **DHCP request**
  - valittu osoite yleislähetyksenä
- **DHCP ACK**
  - palvelimen kuittaus

aikaisempia tapoja: RARP, BOOTP

- **RARP** (Reverse Address Resolution Protocol)
  - **muuttaa lähiverkko-osoitteen IP-osoitteeksi**
    - käynnistettäessä levytön työasema
    - asema kysyy IP-osoitettaan yleislähetyksenä
    - "Lähiverkko-osoitteeni on xxxxx..xx. Mikä on IP-osoiteeni?"
    - RARP-palvelin vastaa kertomalla laitteen IP-osoitteen

    ⇒kaikille laitteille voidaan käyttää samaa aloitustiedostoa
  - **reititin ei välitä RARP-viestejä**
    - joka verkossa oltava oma RARP-palvelin

- BOOTP**-protokollaa**
  - käyttää UDP-viestejä, jotka reititin välittää toisiin verkkoihin
  - lisäinformaatiota
    - tiedostopalvelimen IP-osoite
    - oletusreitittimen IP-osoite
    - aliverkkomaski

3.4. **CIDR** (Classless Inter Domain Routing)

- IP-osoitteiden riittävyys!
  - C-osoitteita paljon, mutta koneosoitteita vain 256
  - B-osoitteessa koneosoitteita riittävästi, mutta B-osoitteita vain 65536!
    - 100000 verkkoa jo 1996!
    - useassa B-verkossa alle 50 konetta
- reititystaulujen koon kasvaminen
    - reitittimien **tunnettava kaikki verkot**
  - => laskennan monimutkaisuus,
  - => tietojenvaihto vie paljon resursseja

CIDR-idea

- varataan C-osoitteet peräkkäisinä lohkoina
  - esim. 2000 osoitetta => varataan 8 peräkkäistä C-verkkoa (= 8*258 = 2048)
- jaetaan osoitteet neljään osaan, kukin osa varataan yhdelle maanosalle
- (Eurooppa, Pohjois-Amerikka, Etelä-Amerikka, Aasia+Pasific)
  - kullekin noin 32 miljoonaa osoitetta
  - 320 miljoona jää vielä varastoon
- reititetään myös maanosien mukaan
  - osoitteet: 194.0.0.0 - 195.255.255.255 Eurooppaan

Paketin reititys

- Reititys verkko-osoitteen perusteella
  - Kun paketti saapuu reitittimeen, sen kohdeosoitteen verkko-osoite etsitään reititystaulusta ja nähdään, minne porttiin paketti tulee lähettää

Muihin verkkoihin

Verkko-osoite, 0	portti

Omaan (omiin) verkkoihin

Oma verkko, host	portti

- kun paketti saapuu, sen kohdeosoite etsitään reititystaulusta
  - jos etäverkko => seuraavalle reitittimelle
  - jos sama verkko => kohdekoneelle
- jos ei löydy reittitaulusta, ohjataan reitittimelle, joka tietää enemmän

- Osoitteen luokka kertoi verkko-osoitteen bitit ja koneosoitteen bitit
- CIDR => verkko-osoitteen koko vaihtelee
- CIDR:n käyttö vaatii maskin, joka kertoo, mitkä bitit kuuluvat verkko-osoitteeseen ja mitkä koneosoitteeseen
- samoin aliverkko-osoitteita käytettäessä tarvitaan aliverkkomaski

Esimerkki CIDR:n käytöstä

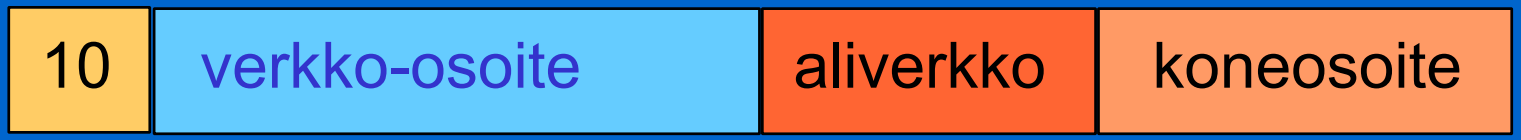
- varataan osoitteet
  - Turun yliopisto 2048 osoitetta
    - 194.24.0.0 - 194.24.7.255 ja maski 255.255.248.0
  - Helsingin yliopisto 4096 osoitetta
    - 194.24.16.0 - 194.24.31.255 ja maski 255.255.240.0
  - Tampereen yliopisto 1024 osoitetta
    - 194.24.8.0 - 194.24.11.255 ja maski 255.255.252.0
- talletetaan reititystauluihin
    - jokaisesta osoitteen alku eli kantaosoite ja maski
- saapuva paketti esim. 194.24.17.4
    - AND-operaatio ensin Turun maskilla
    - jos tuloksena Turun kantaosoite, menossa Turkuun
    - muuten yritetään muita

Reititys aliverkko-osoitteita käytettäessä

- Reititystaulussa
  - (muu_verkko, 0)
  - **(oma_verkko, muu _aliverkko, 0)**
  - **(oma_verkko, oma_aliverkko, kone)**
- kukin reititin tietää
  - oman aliverkkonsa koneet,
  - kuinka päästä muihin aliverkkoihin/verkkoihin
- aliverkon maski
  - kertoo mitkä bitit ovat koneosoitetta, mitkä aliverkko-osoitetta

aliverkkomaski

11111111111111111111111111111000000000000



Reitittimen reititystaulussa:

verkko1,0	**ulosmeno a**
…...	
verkkon,0	**ulosmeno l**
0, aliverkkoi, 0	**ulosmeno u**
……..	
0, aliverkkok, 0	**ulosmeno v**
0, tämä aliverkko, kone1	**ulosmeno k**
……	
0, tämä aliverkko, konen	**ulosmeno m**

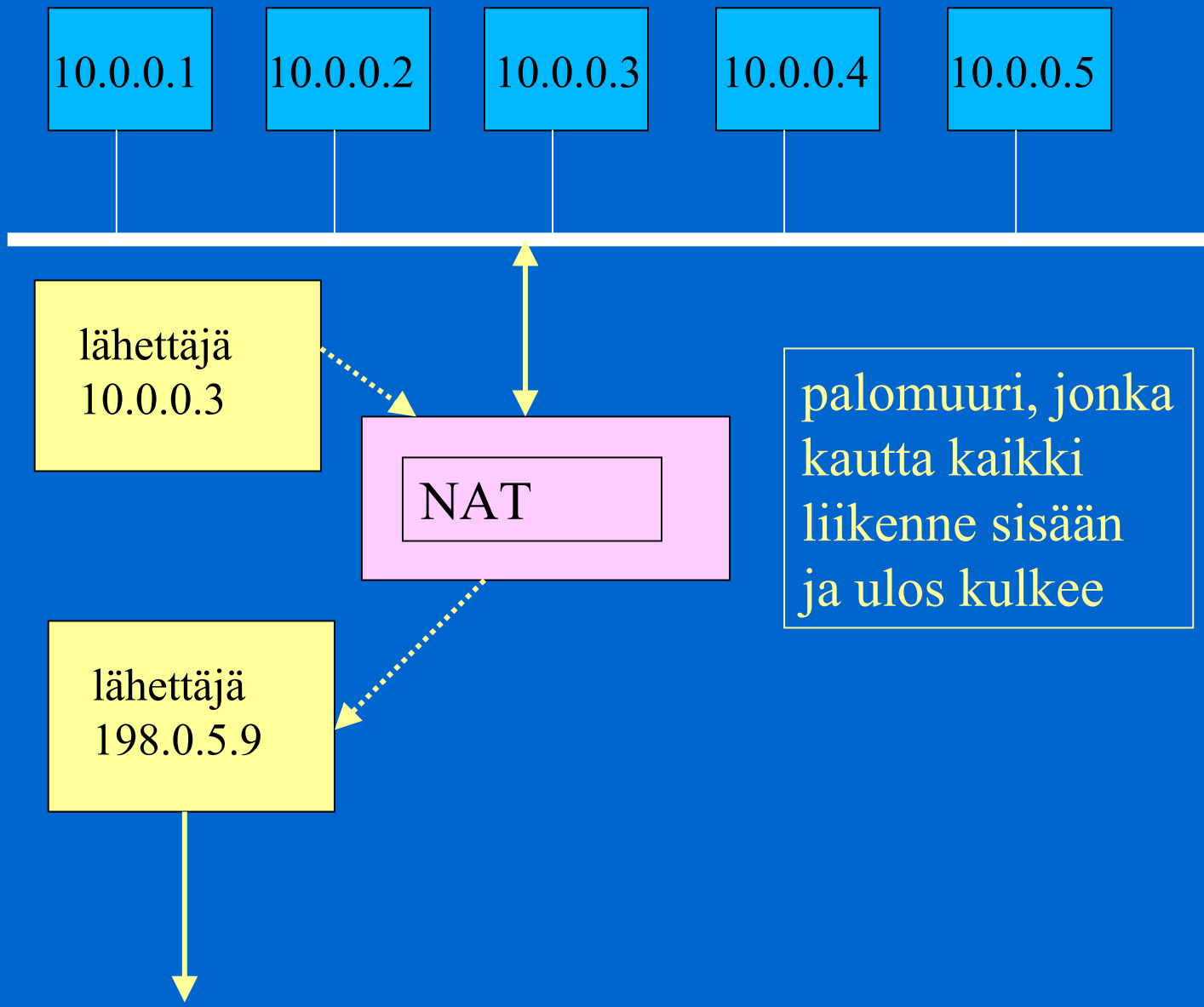
Aliverkkomaskin käyttö

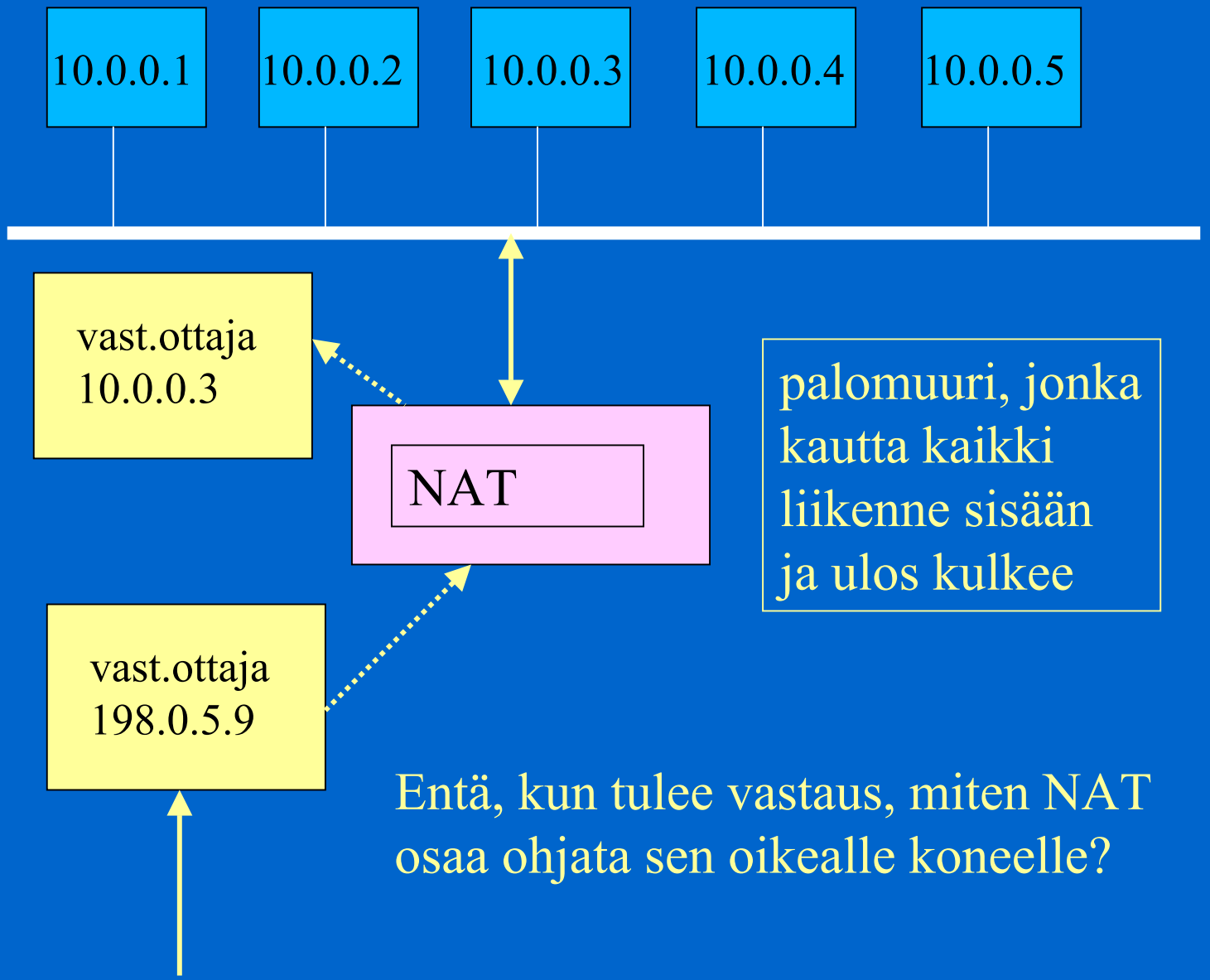
- maskin avulla osoitteesta poistetaan koneosoite
  - AND-operaatio
- etsitään verkko-osoite reititystaulusta
- esim.

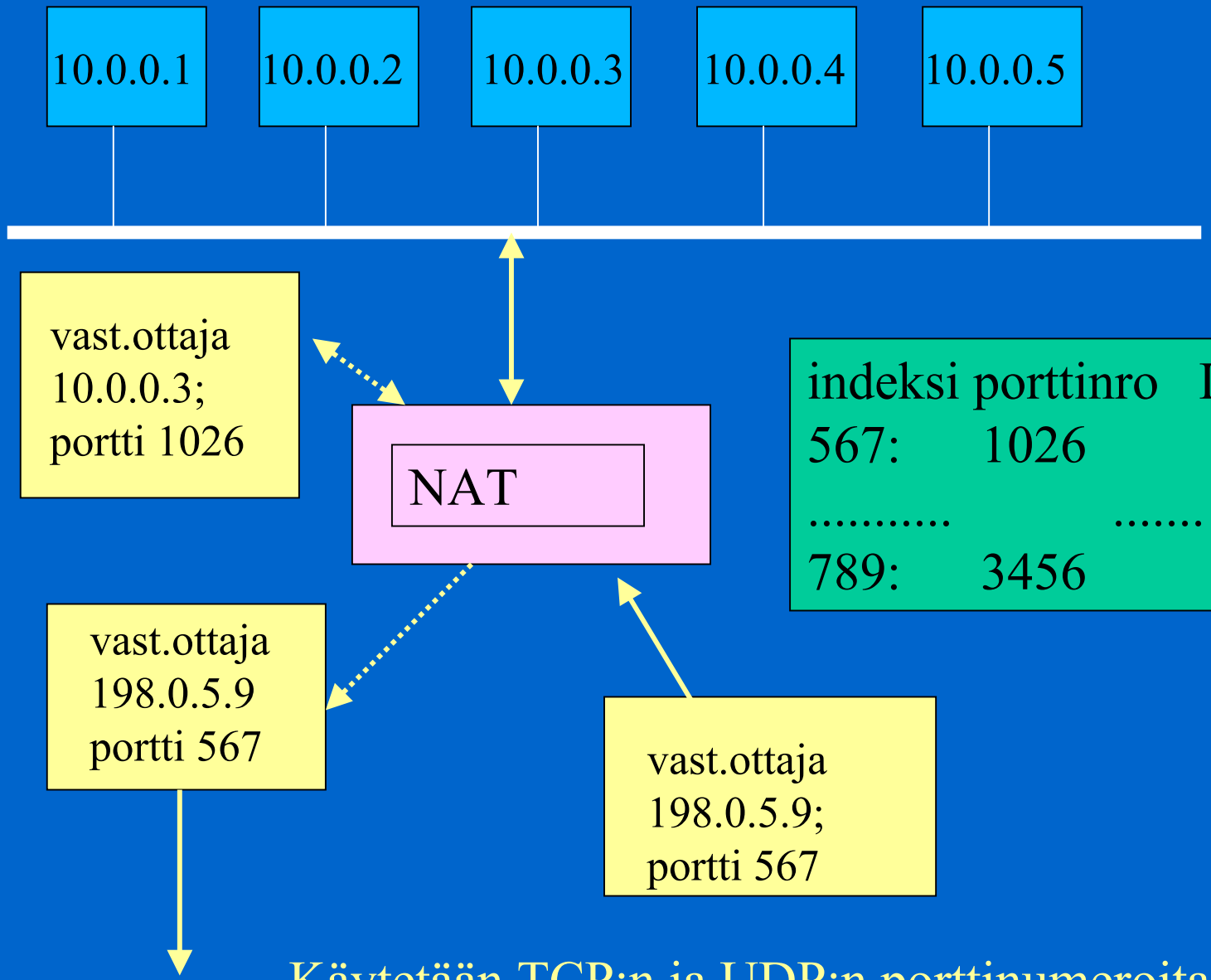
paketin kohdeosoite: 130.50.15.6
maski: 11 …1 11111100 00000000
osoite: 00001111 00000110
AND: 00001100 000000000
tuloksena verkko-osoite: 130.50.12.0

3.6. **NAT** (Network Address Translation, RFC3022)

- **yritykselle riittää muutama, jopa yksi IP-osoite, jolla kommunikoidaan ulkomaailmaan**
- **yrityksen sisällä koneilla on omat IP-osoitteet**
  - yksikäsitteisiä vain yrityksen sisällä
  - yksityiset osoitteet:
    - 10.0.0.0 – 10.255.255.255/8 (16 777 216 kpl)
    - 172.15.0.0 – (n. 1 miljoona)
    - 192.168.0.0 - (65536 kpl)


10.0.0.1
10.0.0.2
10.0.0.3
10.0.0.4
10.0.0.5
lähettäjä
10.0.0.3
NAT
palomuuri, jonka
kautta kaikki
liikenne sisään
ja ulos kulkee
lähettäjä
198.0.5.9


10.0.0.1
10.0.0.2
10.0.0.3
10.0.0.4
10.0.0.5
vast.ottaja
10.0.0.3
NAT
palomuuri, jonka
kautta kaikki
liikenne sisään
ja ulos kulkee
vast.ottaja
198.0.5.9
Entä, kun tulee vastaus, miten NAT
osaa ohjata sen oikealle koneelle?



Käytetään TCP:n ja UDP:n porttinumeroita, joilla tunnistetaan yhteyden prosessit

NAT:n ongelmia

- **jokaisella koneella pitäisi olla oma IP-osoite**
  - tuhansilla koneilla on osoite 10.0.0.1!
- **ei enää tilaton => yhtä haavoittuva kuin virtuaalipiiri**
    - Jos NAT kaatuu!
- **rikkoo protokollien kerrostamista**
    - nojaa ylemmän protokollan ominaisuuksiin
- **entä muut kuin TCP ja UDP?**
- **IP-osoite itse tekstissä säilyy ’vääränä’**
- **korkeintaan 65 536 konetta**