

DHCP

AUTOMATICKÉ PRIDEĽOVANIE IP ADRIES V POČÍTAČOVEJ SIETI

Z pohľadu histórie

- ▶ Používa sa od roku 1993
- ▶ Je rozšírením protokolu BOOTP
- ▶ Využíva rovnaké čísla portov ako BOOTP (UDP 67-server , 68-klient)
- ▶ Podporuje BOOTP klientov

Na čo sa používa a prečo je tak rozšírený?

- ▶ DHCP je preferovaný mechanizmus pre dynamické pridelenie IP adres
- ▶ Tvorba centrálného bodu na sieti, ktorý automaticky pošle zariadeniu IP adresu po pripojení do siete
- ▶ Výhody: 1. Centrálny bod pre administráciu
2. Jednoduchá konfigurácia na strane klienta
3. Flexibilita a škálovateľnosť

Bezpečnosť a DHCP?

- ▶ DHCP je nezabezpečený protocol
 - ▶ Využíva “nespolahlivý” UDP protocol
 - ▶ Je potrebné zabezpečiť pripájanie do siete
 - ▶ Pri nedostatočnom zabezpečení je priestor pre tvorbu DoS útokov

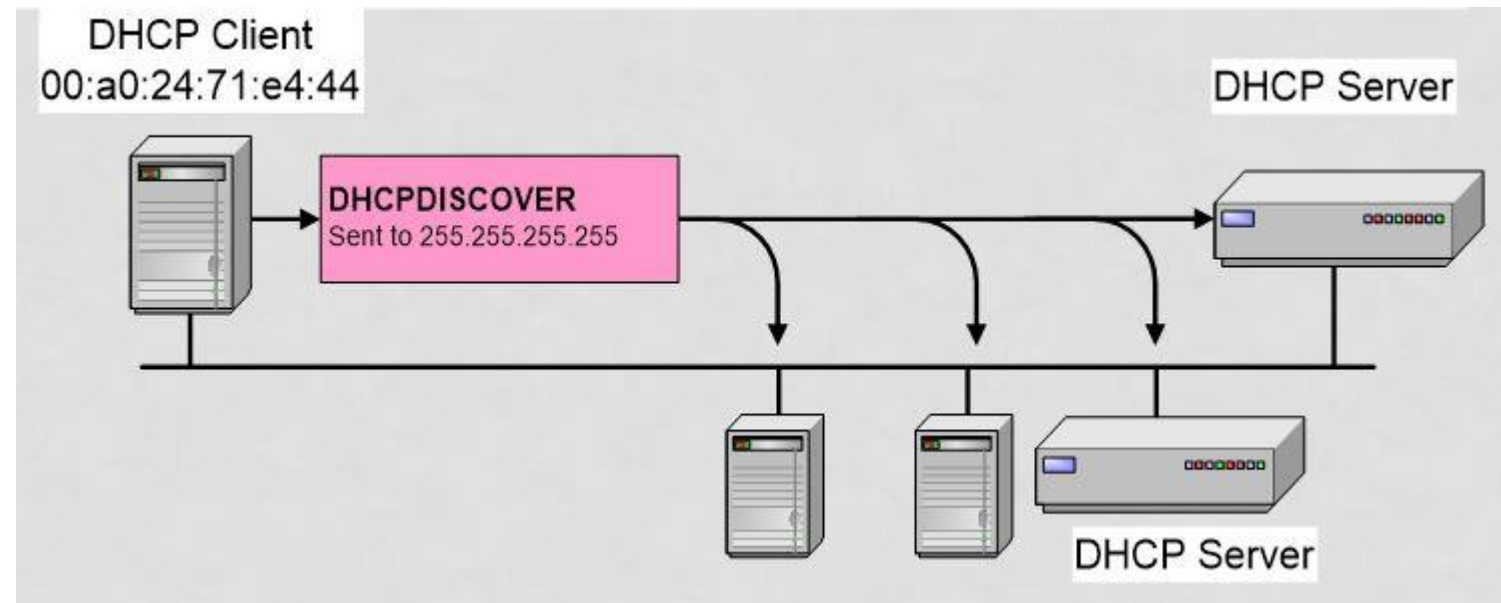
Proces dynamického pridelenia IP adresy

- ▶ 1. DHCPDISCOVER
- ▶ 2. DHCPOFFER
- ▶ 3. DHCPREQUEST
- ▶ 4. DHCPACK

- ▶ X. DHCPRELEASE
 - ▶ X. DHCPNAK
- ▶ X. DHCPDECLINE
- ▶ X. DHCPINFORM

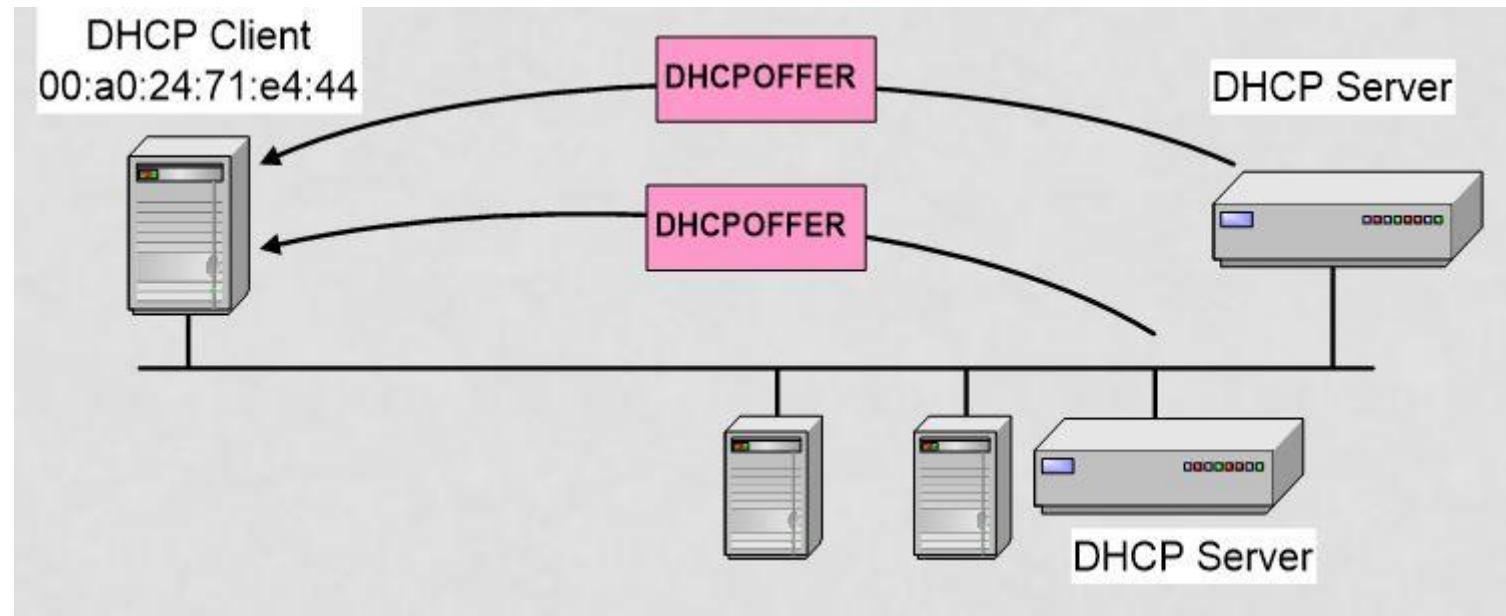
DHCPDISCOVER

- ▶ Prvá správa, ktorá začína komunikáciu medzi klientom a serverom
- ▶ Poslaná klientom
- ▶ Správa poslaná ako BROADCAST
- ▶ Smer: klient → server



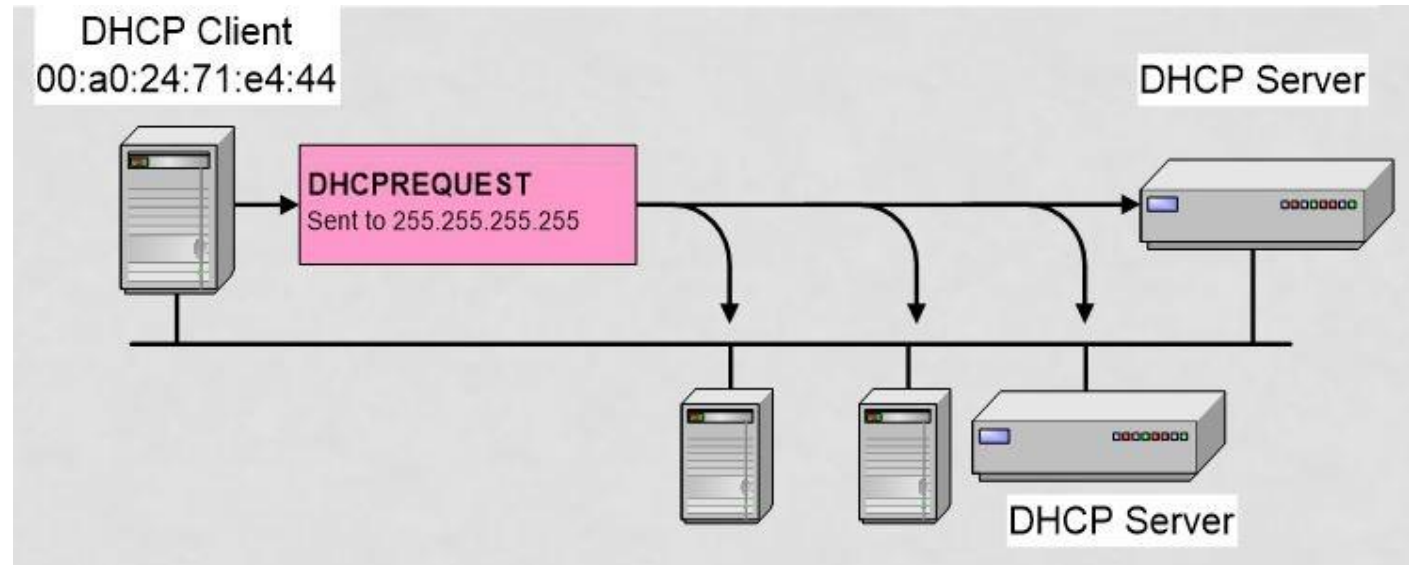
DHCPOFFER

- ▶ Odpoveď na správu DHCPDISCOVER zo strany servera
- ▶ Správa môže byť poslaná ako UNICAST (vďaka MAC adrese) alebo výnimočne BROADCAST
- ▶ Správa obsahuje sieťové nastavenia pre klienta (IP adresu, masku...)
- ▶ Smer: server → klient



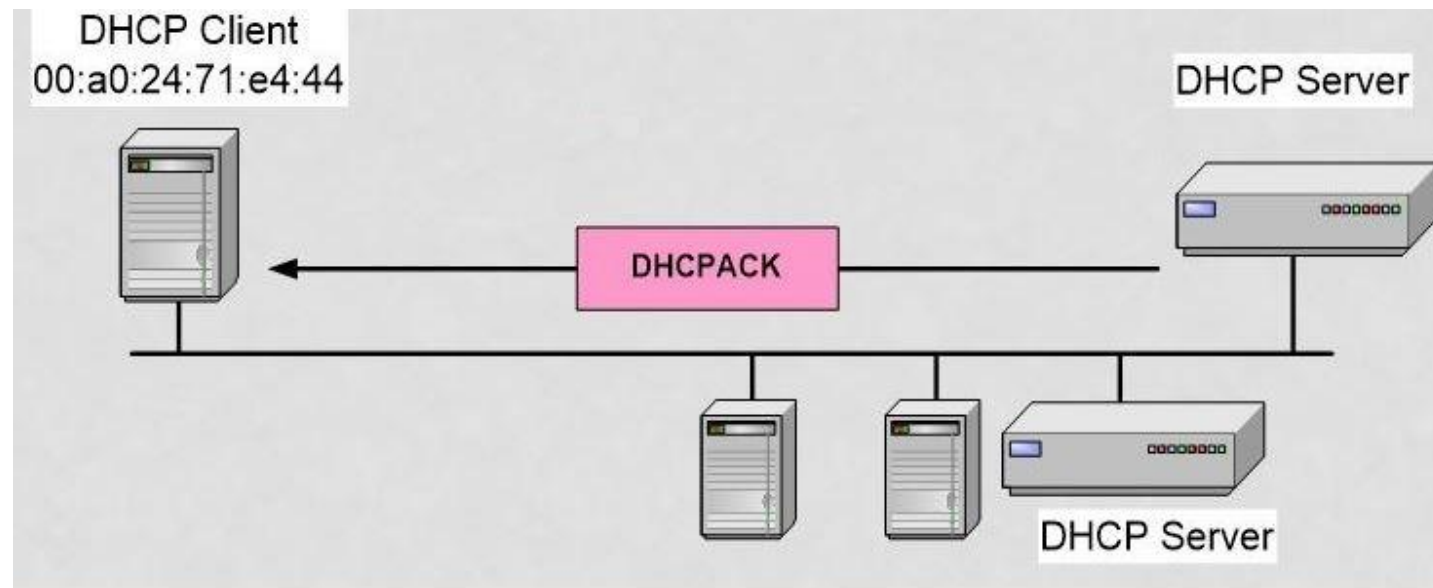
DHCPREQUEST

- ▶ Odpoveď na správu DHCPOFFER zo strany klienta
- ▶ Akceptačná správa, že klient použije sieťové nastavenia poslané v predchádzajúcej správe
- ▶ Správa poslaná ako BROADCAST (aby boli informované všetky DHCP servery)
- ▶ Smer: klient → server



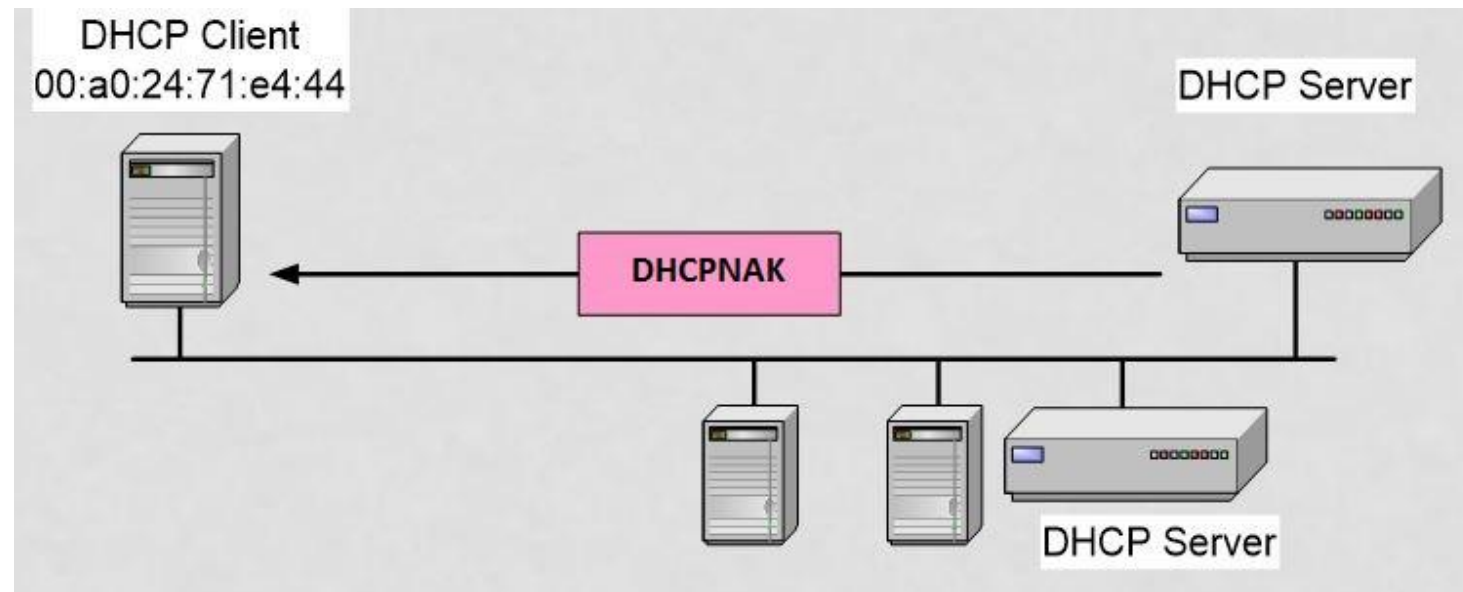
DHCPACK

- ▶ Odpoveď na správu DHCPREQUEST zo strany servera
- ▶ Správa, ktorá končí komunikáciu medzi serverom a klientom
- ▶ Táto správa neobsahuje nič, len server potvrdí klientovi, že ho autorizuje s danou IP adresou
- ▶ Správa poslaná ako UNICAST
- ▶ Smer: server → klient



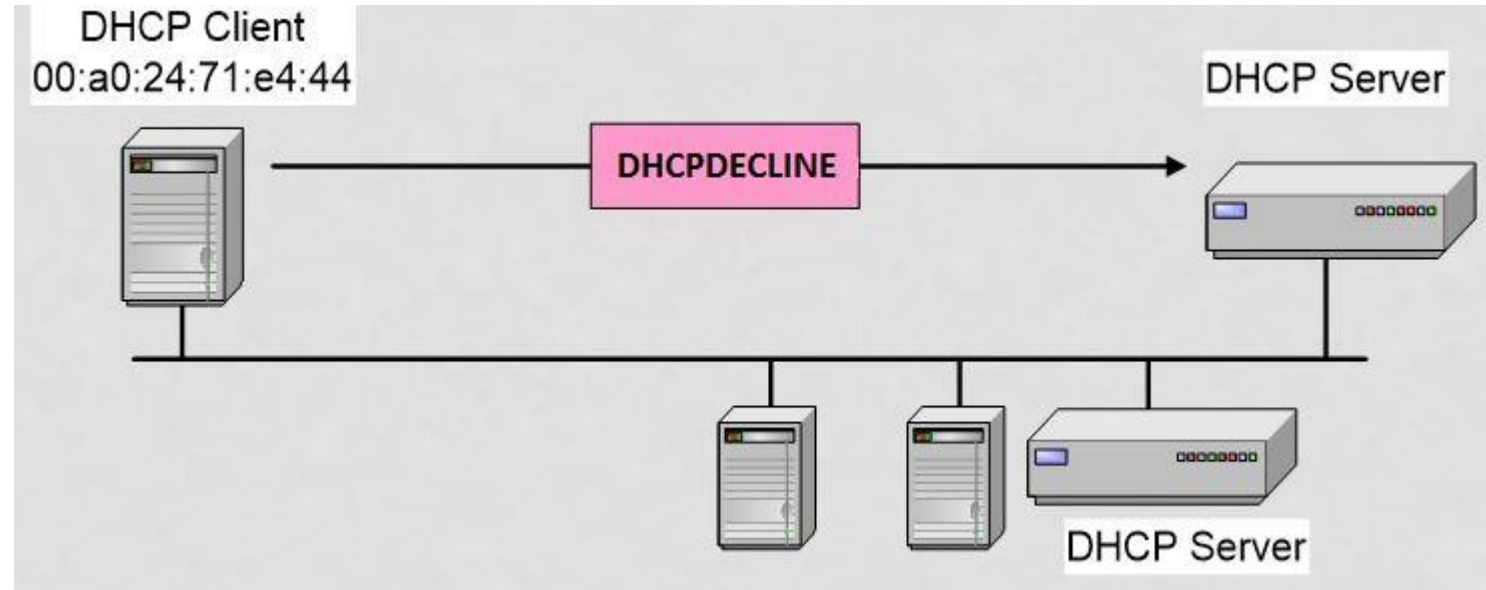
DHCPNAK

- ▶ Odpoveď na správu DHCPREQUEST zo strany servera
- ▶ Presný opak správy DHCPACK
- ▶ Správa je poslaná ak server nie je schopný splniť sieťové nastavenia klienta
- ▶ Správa poslaná ako UNICAST
- ▶ Smer: server → klient



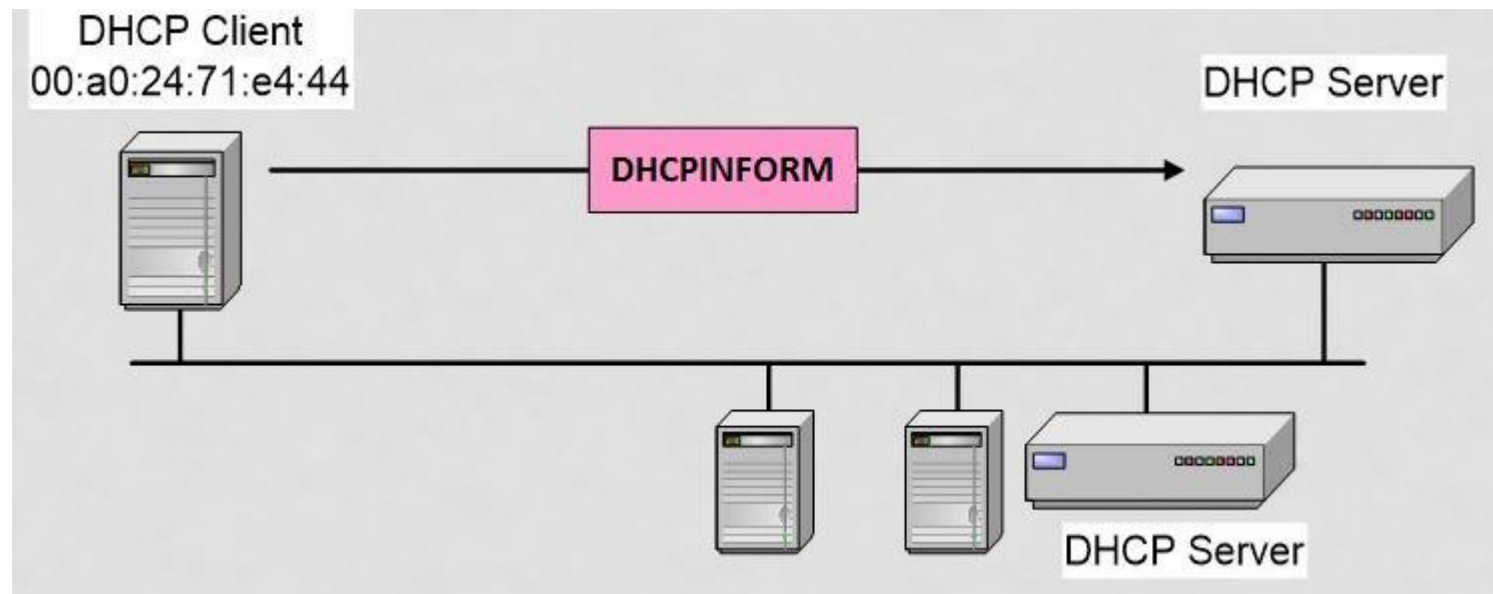
DHCPDECLINE

- ▶ Odpoveď na správu DHCPOFFER zo strany klienta
- ▶ Správa je poslaná, ak klient zistí, že sieťové nastavenie, ktoré mu server ponúka už používa iné zariadenie na sieti
- ▶ Správa poslaná ako UNICAST
- ▶ Smer: klient → server



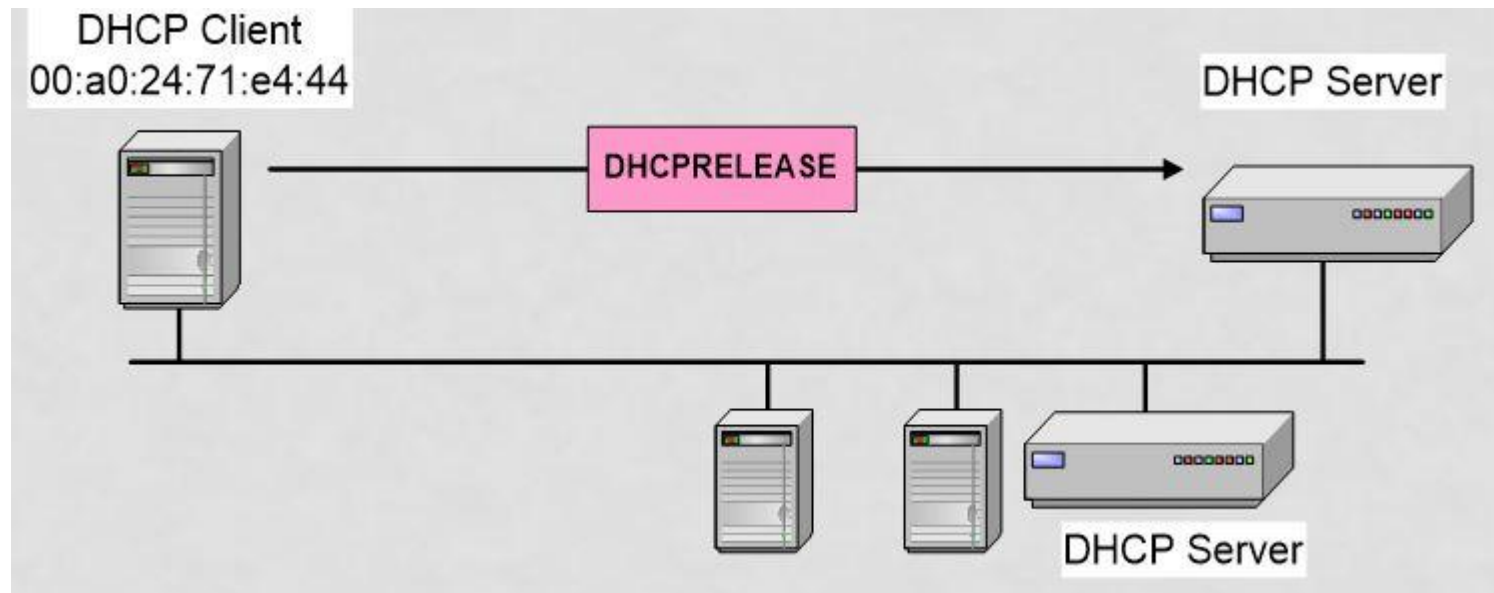
DHCPINFORM

- ▶ Správa je poslaná, ak má zariadenie staticky nakonfigurovanú IP adresu a od servera sú požadované len zvyšné sieťové nastavenia
- ▶ Smer: klient → server



DHCPRELEASE

- ▶ Správa je poslaná, ak už klient nepotrebuje sieťové nastavenia získané od servera
- ▶ Správa poslaná ako UNICAST
- ▶ Smer: klient → server



Linux DHCP server

- ▶ ISC DHCP SERVER

- ▶ DNSMASQ

Inštalácia a konfigurácia ISC DHCP SERVERA

```
root@debian:~# apt-get install isc-dhcp-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
isc-dhcp-server is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
```

```
Terminal - peto@debian: ~
File Edit View Terminal Tabs Help
GNU nano 2.2.6 File: /etc/default/isc-dhcp-server

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPD_PID=/var/run/dhcpd.pid

# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACES="eth0"
```

```
Terminal - peto@debian: ~
File Edit View Terminal Tabs Help
GNU nano 2.2.6 File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.50.5
netmask 255.255.255.0
```

```
Terminal - peto@debian: ~
File Edit View Terminal Tabs Help
GNU nano 2.2.6 File: /etc/dhcp/dhcpd.conf Modified

# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

#subnet 10.254.239.32 netmask 255.255.255.224 {
#  range dynamic-bootp 10.254.239.40 10.254.239.60;
#  option broadcast-address 10.254.239.31;
#  option routers rtr-239-32-1.example.org;
#}

# A slightly different configuration for an internal subnet.
subnet 192.168.50.0 netmask 255.255.255.0 {
  range 192.168.50.80 192.168.50.200;
  option routers 192.168.50.1;
  option broadcast-address 192.168.50.255;
}
```



```
root@debian:~# systemctl status -n 200 isc-dhcp-server.service -l
```

```
● isc-dhcp-server.service - LSB: DHCP server
```

```
Loaded: loaded (/etc/init.d/isc-dhcp-server)
```

```
Active: active (running) since Thu 2017-04-20 15:06:26 CDT; 41s ago
```

```
Process: 1380 ExecStop=/etc/init.d/isc-dhcp-server stop (code=exited, status=0/SUCCESS)
```

```
Process: 1387 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS)
```

```
CGroup: /system.slice/isc-dhcp-server.service
```

```
└─1396 /usr/sbin/dhcpd -q -cf /etc/dhcp/dhcpd.conf -pf /var/run/dhcpd.pid eth0
```

```
Apr 20 15:06:24 debian systemd[1]: Starting LSB: DHCP server...
```

```
Apr 20 15:06:24 debian dhcpd[1393]: Internet Systems Consortium DHCP Server 4.3.1
```

```
Apr 20 15:06:24 debian dhcpd[1393]: Copyright 2004-2014 Internet Systems Consortium.
```

```
Apr 20 15:06:24 debian dhcpd[1393]: All rights reserved.
```

```
Apr 20 15:06:24 debian dhcpd[1393]: For info, please visit https://www.isc.org/software/dhcp/
```

```
Apr 20 15:06:24 debian dhcpd[1395]: Internet Systems Consortium DHCP Server 4.3.1
```

```
Apr 20 15:06:24 debian dhcpd[1395]: Copyright 2004-2014 Internet Systems Consortium.
```

```
Apr 20 15:06:24 debian dhcpd[1395]: All rights reserved.
```

```
Apr 20 15:06:24 debian dhcpd[1395]: For info, please visit https://www.isc.org/software/dhcp/
```

```
Apr 20 15:06:24 debian dhcpd[1395]: Wrote 2 leases to leases file.
```

```
Apr 20 15:06:24 debian dhcpd[1396]: Server starting service.
```

```
Apr 20 15:06:26 debian isc-dhcp-server[1387]: Starting ISC DHCP server: dhcpd.
```

```
Apr 20 15:06:26 debian systemd[1]: Started LSB: DHCP server.
```

```
Apr 20 15:06:37 debian dhcpd[1396]: DHCPRELEASE of 192.168.50.100 from 0a:00:27:00:00:0a (refoma-NB11) via eth0 (found)
```

```
Apr 20 15:06:42 debian dhcpd[1396]: DHCPDISCOVER from 0a:00:27:00:00:0a via eth0
```

```
Apr 20 15:06:42 debian dhcpd[1396]: DHCPOFFER on 192.168.50.100 to 0a:00:27:00:00:0a (refoma-NB11) via eth0
```

```
Apr 20 15:06:42 debian dhcpd[1396]: DHCPREQUEST for 192.168.50.100 (192.168.50.5) from 0a:00:27:00:00:0a (refoma-NB11) via eth0
```

```
Apr 20 15:06:42 debian dhcpd[1396]: DHCPACK on 192.168.50.100 to 0a:00:27:00:00:0a (refoma-NB11) via eth0
```

Inštalácia a konfigurácia DNSMASQ

```
Terminal - peto@debian: ~
File Edit View Terminal Tabs Help
root@debian:~# apt-get install dnsmasq
Reading package lists... Done
Building dependency tree
Reading state information... Done
dnsmasq is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
```

```
Terminal - peto@debian: ~
File Edit View Terminal Tabs Help
GNU nano 2.2.6 File: /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.50.5
netmask 255.255.255.0
```

```

interface=eth0
dhcp-option=option:router,192.168.50.5
dhcp-range=192.168.50.150,192.168.50.200,255.255.255.0,12h
dhcp-authoritative

```

```

root@debian:~# systemctl status -n 200 dnsmasq -l
● dnsmasq.service - dnsmasq - A lightweight DHCP and caching DNS server
  Loaded: loaded (/lib/systemd/system/dnsmasq.service; enabled)
  Drop-In: /run/systemd/generator/dnsmasq.service.d
           └─50-dnsmasq-$named.conf, 50-insserv.conf-$named.conf
  Active: active (running) since Fri 2017-04-21 07:35:43 CDT; 23s ago
  Process: 1088 ExecStop=/etc/init.d/dnsmasq systemd-stop-resolvconf (code=exited, status=0/SUCCESS)
  Process: 1104 ExecStartPost=/etc/init.d/dnsmasq systemd-start-resolvconf (code=exited, status=0/SUCCESS)
  Process: 1096 ExecStart=/etc/init.d/dnsmasq systemd-exec (code=exited, status=0/SUCCESS)
  Process: 1094 ExecStartPre=/usr/sbin/dnsmasq --test (code=exited, status=0/SUCCESS)
  Main PID: 1103 (dnsmasq)
  CGroup: /system.slice/dnsmasq.service
           └─1103 /usr/sbin/dnsmasq -x /var/run/dnsmasq/dnsmasq.pid -u dnsmasq -7 /etc/dnsmasq.d,.dpkg-dist,.dpkg-old,.dpkg-new --local-service --trust-anchor=.,19036,8,2,49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5

Apr 21 07:35:43 debian systemd[1]: Starting dnsmasq - A lightweight DHCP and caching DNS server...
Apr 21 07:35:43 debian dnsmasq[1094]: dnsmasq: syntax check OK.
Apr 21 07:35:43 debian dnsmasq[1103]: started, version 2.72 cachesize 150
Apr 21 07:35:43 debian dnsmasq[1103]: compile time options: IPv6 GNU-getopt DBus i18n IDN DHCP DHCPv6 no-Lua TFTP contrack ipset auth DNSSEC loop-detect
Apr 21 07:35:43 debian dnsmasq-dhcp[1103]: DHCP, IP range 192.168.50.150 -- 192.168.50.200, lease time 12h
Apr 21 07:35:43 debian dnsmasq[1103]: reading /etc/resolv.conf
Apr 21 07:35:43 debian dnsmasq[1103]: using nameserver 192.168.1.1#53
Apr 21 07:35:43 debian dnsmasq[1103]: read /etc/hosts - 5 addresses
Apr 21 07:35:43 debian systemd[1]: Started dnsmasq - A lightweight DHCP and caching DNS server.
Apr 21 07:36:00 debian dnsmasq-dhcp[1103]: DHCPDISCOVER(eth0) 192.168.50.160 0a:00:27:00:00:0a
Apr 21 07:36:00 debian dnsmasq-dhcp[1103]: DHCPOFFER(eth0) 192.168.50.160 0a:00:27:00:00:0a
Apr 21 07:36:00 debian dnsmasq-dhcp[1103]: DHCPREQUEST(eth0) 192.168.50.160 0a:00:27:00:00:0a
Apr 21 07:36:00 debian dnsmasq-dhcp[1103]: Ignoring domain refoma.sk for DHCP host name refoma-NB11
Apr 21 07:36:00 debian dnsmasq-dhcp[1103]: DHCPACK(eth0) 192.168.50.160 0a:00:27:00:00:0a refoma-NB11

```

DHCP Troubleshooting

- ▶ `systemctl status isc-dhcp-server.service`
- ▶ `systemctl status dnsmasq.service`
- ▶ `dhcpcdump -i eth0`
- ▶ `tcpdump -l eth0 port 67 or port 68 -n`
- ▶ `cat /var/lib/misc/dnsmasq.leases`
- ▶ `cat /var/lib/dhcp/dhcpd.leases`
- ▶ `cat /var/log/syslog | grep dhcp`

```
Terminal - peto@debian: ~
File Edit View Terminal Tabs Help
Password:
root@debian:~# dhcpcdump -i eth0
  TIME: 2017-04-22 08:27:01.037
  IP: 192.168.50.160 (a:0:27:0:0:a) > 192.168.50.5 (8:0:27:a9:fa:e1)
  OP: 1 (BOOTPREQUEST)
  HTYPE: 1 (Ethernet)
  HLEN: 6
  HOPS: 0
  XID: da518ed1
  SECS: 1024
  FLAGS: 0
CIADDR: 192.168.50.160
YIADDR: 0.0.0.0
SIADDR: 0.0.0.0
GIADDR: 0.0.0.0
CHADDR: 0a:00:27:00:00:0a:00:00:00:00:00:00:00:00:00:00
  SNAME: .
  FNAME: .
OPTION: 53 ( 1) DHCP message type          7 (DHCPRELEASE)
OPTION: 54 ( 4) Server identifier          192.168.50.5
OPTION: 61 ( 7) Client-identifier         01:0a:00:27:00:00:0a
-----

  TIME: 2017-04-22 08:27:05.452
  IP: 0.0.0.0 (a:0:27:0:0:a) > 255.255.255.255 (ff:ff:ff:ff:ff:ff)
  OP: 1 (BOOTPREQUEST)
  HTYPE: 1 (Ethernet)
  HLEN: 6
  HOPS: 0
  XID: 0d9f07ca
  SECS: 0
  FLAGS: 0
CIADDR: 0.0.0.0
```

```
Terminal - peto@debian: ~
File Edit View Terminal Tabs Help
root@debian:~# tcpdump -i eth0 port 67 or port 68 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
08:37:33.264256 IP 192.168.50.160.68 > 192.168.50.5.67: BOOTP/DHCP, Request from 0a:00:27:00:00:0a,
length 300
08:37:36.839217 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 0a:00:27:00:00:0a, leng
th 300
08:37:36.839408 IP 192.168.50.5.67 > 192.168.50.160.68: BOOTP/DHCP, Reply, length 300
08:37:36.840387 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 0a:00:27:00:00:0a, leng
th 329
08:37:36.846092 IP 192.168.50.5.67 > 192.168.50.160.68: BOOTP/DHCP, Reply, length 308
```

Porovnanie DHCP serverov

ISC DHCP SERVER

- ▶ Umožňuje Master-Slave nasadenie (veľká výhoda oproti DNSMASQ)
- ▶ Širšia škála funkcionalít ako DNSMASQ
- ▶ Podporujúce platformy: BSD, Solaris, Linux

DNSMASQ

- ▶ 10x Menej záťaže na pamäť a CPU ako ISC DHCP SERVER
- ▶ Podpora DNS a DHCP služieb jedným programom
- ▶ Jednoduchší z hľadiska inštalácie a následnej správy
- ▶ Menšia škála funkcionalít (vhodný pre menšie siete alebo do max. 1000 PC)
- ▶ Podporujúce platformy: BSD, Linux, MAC OS

Ďakujem za pozornosť 😊

PETER JANTÁK