LUCRAREA NR. 6
EASY IP: DHCP, NAT

1. Obiective

Obiectivele acestui laborator sînt: înțelegerea procesului de închiriere a unei adrese prin mecanismul DHCP, familiarizarea cu noțiunile: scop DHCP, interval de adrese, excluziuni, rezervare, superscopuri, relay agent, întelegerea procesului de translatare a adreselor, instalarea şi configurarea unui server DHCP, configurarea unui client DHCP, testarea configurării.

2. Considerații teoretice

2.1 DHCP – Dynamic Host Configuration Protocol

2.1.1 Introducere

DHCP este un protocol standardizat şi definit prin IETF RFC 2131 şi 2132. Prin DHCP, se pot aloca/modifica automat parametrii de configurare a unui host dintr-o rețea TCP/IP în timpul bootării sau în timpul funcționării. Adresele IP şi ceilalți parametrii de configurare (masca, adresele gateway, adresele serverelor DNS) sînt stocate într-o bază de date centralizată.

Serviciul DHCP şi serviciul DNS stau la baza infrastructurii unei rețele fiind o modalitate simplă dar puternică de a asigna adrese IP, măşti de rețea, adrese de gateway, adrese de servere DNS şi servere WINS - în rețele cu sisteme Windows, şi alte opțiuni.

2.1.2 Procesul de închiriere prin DHCP

Serviciul DHCP alocă informații de adresare IP hosturilor client. Procesul de alocare dinamică a unei adrese IP se numeşte închiriere DHCP. Procesul de închiriere DHCP se declanşează în următoarele cazuri:

- stiva TCP/IP este inițializată pentru prima dată pe un client DHCP;
- un client face o cerere pentru o adresă IP şi cererea e respinsă;

- un client care a cerut la un moment dat o adresă şi apoi a renunțat la aceasta adresă face o noua cerere pentru o adresă.

Procesul de închiriere DHCP se desfăşoară în patru faze.

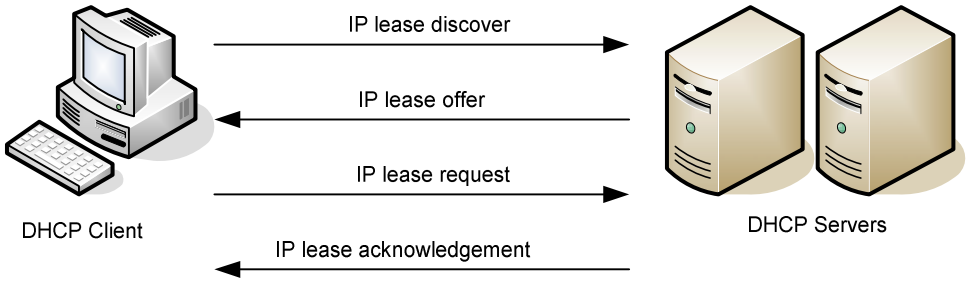

Figura 6.1 *Procesul de închiriere a unei adrese*

1. IP Lease Discover

În timpul procesului de boot al unui client, acesta face o cerere de închiriere a unei adrese IP prin trimiterea unui mesaj broadcast serverelor DHCP. În acest moment clientul nu are o adresă IP alocată si nici nu cunoaşte adresele IP ale serverelor DHCP de aceea utilizează adresa 0.0.0.0 ca adresă sursă şi 255.255.255.255 ca adresă destinație. Mesajul DHCPDiscover conține adresa hardware şi numele hostului client astfel încît serverele DHCP să identifice clientul de la care au primit cererea.

2. IP Lease Offer

Toate serverele DHCP care primesc cererea şi au o configurație validă pentru client trimit un mesaj broadcast, DHCPOffer, care conține următoarele informații:

- adresa hardware a clientului;
- adresa IP oferită;
- masca de rețea;
- durata perioadei de închiriere;
- identificatorul serverului (adresa IP a serverului DHCP care emite oferta).

Serverul DHCP emite mesajul în maniera broadcast deoarece clientul nu are încă o adresă IP. Clientul DHCP alege prima ofertă pe care o recepționează.

3. IP Lease Request

După ce clientul DHCP a primit o ofertă de la un server DHCP emite un mesaj broadcast, DHCPRequest, adresat serverelor DHCP prin care anunță că a acceptat o ofertă. Mesajul DHCPRequest conține identificatorul serverului DHCP de la care a acceptat oferta. Celelalte servere DHCP îşi retrag ofertele şi păstrează adresa IP oferită pentru un proces de închiriere ulterior.

4. IP Lease Acknowledgement

4.1 Success

Serverul DHCP a cărui ofertă a fost acceptată răspunde cu un mesaj DHCPACK. După ce clientul primeste acest mesaj începe să utilizeze adresa IP alocată.

4.2 Eşec

Serverul DHCP a cărui ofertă a fost acceptată răspunde cu un mesaj DHCPNACK în următoarele situații:

- clientul încearcă să închirieze o adresă IP care este deja alocată;
- adresa IP nu e validă deoarece clientul şi-a modificat fizic locația într-o altă subrețea.

Clientul care primeşte un mesaj DHCPNACK va relua procesul de închiriere a unei adrese IP.

2.1.3 Reînnoirea unei închirieri, renunțarea la o adresă IP

După trecerea a 50% din timpul de închiriere alocat, clienții DHCP încearcă să-şi reînnoiască închirierea adresei prin trimiterea unui mesaj DHCPRequest adresat serverului DHCP de la care a obținut adresa. Dacă serverul DHCP este disponibil reînnoieşte închirierea şi emite un mesaj DHCPACK cu noua perioadă de închiriere şi parametrii de configurare actualizați.

Cînd un client DHCP este repornit în rețea încercă să închirieze aceaşi adresă IP. Dacă cererea de închiriere eşuează şi timpul de închiriere precedent nu a expirat, clientul utilizează vechea adresa IP pînă la următoarea încercare de închiriere a unei adrese.

Dacă un client DHCP nu-şi reînnoieşte închirierea prin serverul original la 50% din timpul de închiriere, la trecerea a 87.5% din timpul de închiriere clientul transmite un mesaj broadcast, DHCPRequest, pentru a contacta alte servere DHCP. Orice server DHCP disponibil răspunde cu un mesaj DHCPACK (reînnoirea închirierii) sau DHCPNACK (forțează clientul să reia procesul de închiriere a unei alte adrese IP).

Dacă perioada de închiriere expiră sau s-a recepționat un mesaj DHCPNACK clientul DHCP nu mai poate utiliza adresa IP şi trebuie să reia procesul de închiriere unei adrese IP.

2.1.3.1 Utilizarea comenzii Ipconfig pentru reînnoirea închirierii

Utilizați comanda `ipconfig` cu opțiunea `/renew` pentru transmiterea unui mesaj DHCPRequest serverului DHCP pentru actualizarea parametrilor şi perioadei de închiriere. Dacă serverul DHCP nu e disponibil clientul va utiliza în continuare aceiaşi parametrii de configurare.

2.1.3.2 Utilizarea comenzii Ipconfig pentru a renunța la o închiriere

Utilizatți comanda `ipconfig` cu opțiunea `/release` pentru transmiterea unui mesaj DHCPRelease serverului DHCP - clientul anunță că renunță la închiriere. Această metodă e utilă cînd hostul client e mutat în altă rețea şi nu mai are nevoie de închirierea anterioară. După lansarea comenzii, comunicarea TCP/IP cu hostul client este întreruptă.

2.1.4. Definirea noțiunilor: scop, interval de adrese, rezervare, excluziune, agent releu (relay agent)

2.1.4.1 Scopuri DHCP

Un scop DHCP este un pool de adrese IP dintr-o subrețea logică pe care serverul DHCP le poate aloca clienților. Scopul DHCP constituie elementul de bază al alocării dinamice de adrese şi parametrii de rețea clienților. Cînd se asignează o adresă IP, închirierea devine activă. Închiriere are loc pe o

perioadă de timp; clientul trebuie să-şi reînnoiască închirierea dacă vrea să utilizeze aceaşi adresă IP. Durata implicită a unei închirieri este de 8 zile.

2.1.4.2 Intervalul de adrese

Intervalul de adrese definit într-un scop trebuie să conțină adrese consecutive din aceaşi subrețea pentru care se activează serviciul DHCP. Deasemenea, din acest interval trebuie excluse adresele alocate static; aceasta se poate realiza prin simpla limitare a intervalului de adrese sau prin configurarea scopului şi definirea excluziunilor.

2.1.4.3 Mulțimea de excluziune

Mulțimea de excluziune conține una sau mai multe adrese IP care aparțin intervalului de adrese din scop dar pe care serverul de DHCP nu le închiriază clienților. Dupa definirea scopului şi a mulțimii de excluziune adresele rămase formează mulțimea de adrese disponibile pentru închiriere.

2.1.4.4 Regula 80/20

Pentru a asigura toleranța la erori într-o subrețea se configurează două servere cu serviciul DHCP. Dacă un server devine indisponibil celălalt server continuă procesul de închiriere de adrese şi de reînnoire a închirierilor. Pentru echilibrare se aplică regula 80/20: scopul este divizat între cele doua servere, primul server e configurat să aloce majoritatea adreselor (80% din numărul total de adrese), al doilea server e configurat să aloce restul de adrese (20%).

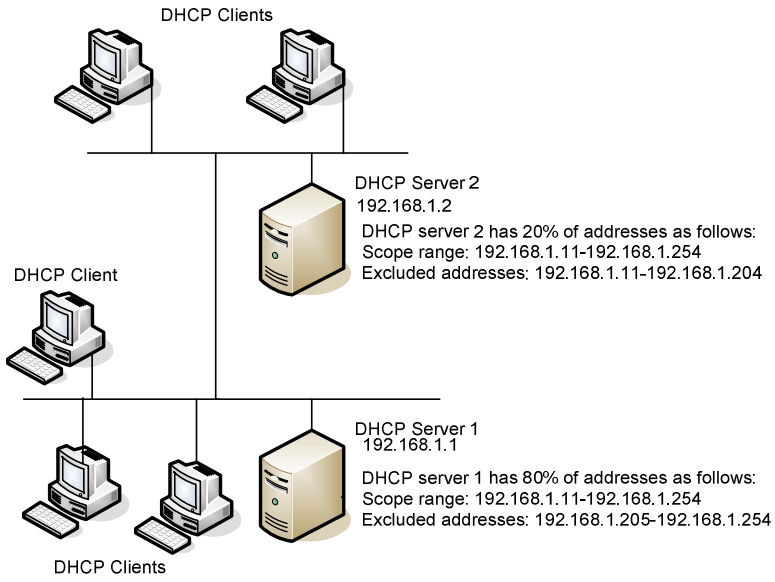

Figura 6.2 *Regula 80/20*

2.1.4.5 Rezervări

Printr-o rezervare se realizează o închiriere permanentă a unei adrese, un echipament din subrețea va avea întotdeauna aceaşi adresă IP. Procesul de rezervare e mutual exclusiv cu procesul de alocare statică a unei adrese IP.

2.1.4.6 Opțiuni DHCP

Opțiunile DHCP oferă clienților parametrii suplimentari de configurare. Opțiunile se definesc la nivel de rezervare, scop sau server. Există peste 60 de opțiuni standard ce pot fi configurate, cele mai importante fiind: 006 DNS Servers – adrese IP ale serverelor DNS ce pot fi contactate pentru rezolvarea de nume şi adrese, 015 Domain Name – numele de domeniu utilizat de client, 044 WINS/NBNS Servers – adresele IP ale serverului WINS primar şi secundar.

2.1.4.7 Utilizarea superscopurilor

Un superscop este o grupare administrativă de scopuri, definit pentru multinetting sau pentru gruparea logică a mai multor subrețele într-un singur

segment de rețea. Multinetting-ul defineşte situația în care numărul de hosturi dintr-un segment fizic de rețea creşte peste capacitatea scopului original definit. Prin crearea unui al doilea scop, adăugat scopului original pentru a defini un superscop, se poate dubla capacitatea de adresare a segmentului fizic. Astfel, serverul DHCP va aloca clienților dintr-o rețea adrese din mai multe scopuri.

2.1.4.8 Agent releu DHCP

Agentul releu DHCP (DHCP Relay Agent) este un protocol prin care se realizează închirierea unei adrese IP de la un server DHCP din altă subrețea. În mod normal, clientul transmite mesaje DHCPDiscover care sînt recepționate doar de serverele DHCP din subrețea. Deoarece ruterele blochează pachetele broadcast, clienții DHCP şi serverele DHCP trebuie să fie în aceeaşi subrețea fizică. Există definite două metode pentru a depăşi această limitare. Prima presupune ca ruterul ce separă subrețelele în care se află serverul DHCP şi clientul DHCP să fie RFC 1542-compliant, astfel ruterul poate fi configurat pentru transmisie BOOTP (Boot Protocol forwarding). Prin BOOTP ruterul transmite pachetele de broadcast între clienți şi servere şi infromează serverele despre subrețelele din care provin aceste pachete. Acest proces permite alocarea de adrese clienților remote. A doua metodă presupune configurarea unui agent releu în subrețeau în care sînt localizați clienții. Agentul releu interceptează mesajele DHPCDiscover şi le transmite unui server DHCP remote a cărui adresă a fost preconfigurată. Deşi agentul releu DHCP se configurează prin Routing and Remote Access, hostul pe care acesta e configurat nu trebuie sa fie un ruter între cele două subrețele.

2.2 Translatarea de adrese – NAT(Network Address Translation)

NAT este un mecanism de translatare a adreselor IP private dintr-o rețea în adrese publice. NAT este utilizat la granița dintre două rețele: una privată şi cealaltă publică.

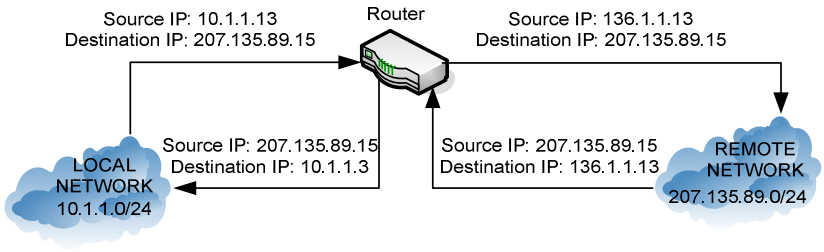

Figura 6.3 *Procesul de translatare a adreselor*

NAT a apărut ca o necesitate deoarece adresele publice disponibile au fost rapid alocate. NAT rezolvă această problemă prin:

- reutilizarea adreselor: mai multe rețele private pot folosi aceleaşi adrese. Rețelele private au adrese rezervate de IANA (Internet Assigned Numbers Authority) în acest scop: 10/8, 172.16/12, 192.168/16, adrese nerutabile. Rețelele private nu se pot conecta direct la Internet decît prin intermediul unui ruter sau a unui calculator configurat cu NAT astfel încît adresele nerutabile să fie translatate în adrese publice pentru rutarea în Internet;
- multiplexarea adreselor: mai multe adrese private dintr-o rețea pot fi cunoscute în Internet ca o singură adresă publică, crește securitatatea rețelei. Multiplexarea adreselor apare si sub denumirea NAPT (network address port translation).

Într-un scenariu tipic, un ruter configurat cu NAT leagă o rețea privată de o rețea publică. Rețeaua internă (rețeaua privată) are hosturi cu adrese IP private, în timp ce ruterul are configurată pe interfața expusă spre rețeaua internă o adresă privată iar pe interfața expusă spre rețeaua publică are configurată o adresa publică (globală). Serviciul NAT examinează traficul ce trece prin ruter şi construieşte o tabelă de corespondență în care mapează conexiunile între hosturile din rețeaua internă şi hosturi din rețeaua externă. Pentru fiecare conexiune se păstrază următoarele informații:

- adresa IP originală şi portul sursă;
- adresa IP şi portul destinație;
- adresa IP translatată şi portul sursă;
- adresa IP translatată şi portul destinație;
- numerele de secvență TCP şi ICMP.

Implementarea NAT pe un ruter sau un firewall presupune crearea şi configurarea tabelei ce conţine mapările între adresele private şi adresele publice. Maparea poate fi realizată:

- manual: o tabelă NAT statică conţine regulile de translatare a adreselor. Tabelele definite static conţin doar mapări unu-la-unu între adresa actuală şi adresa translatată. Maparea statică nu este utilă în cazul legăturilor multiple între reţele private şi Internet, numărul mare de conexiuni create duce la cresterea excesivă a dimensiunilor tabelei NAT şi în consecinţă la degradarea performanţelor ruterului;
- dinamic: ruterele cu suport pentru NAT pot aloca dinamic adrese dintr-un interval de adrese specificat hosturilor dintr-o reţea privată. Maparile dinamice sînt unu-la-unu între adresa actuală şi adresa translatată. Acest proces este similar cu procesul de alocare dinamică a adreselor prin DHCP şi poate fi realizat aleator sau în manieră round-robin. Cînd se deschide o conexiune către o reţea externă, serviciul NAT asignează o adresă din intervalul de adrese predefinit şi informaţia de adresare din pachete este modificată în consecinţă.

O metodă mai avansată de translatare de adrese o reprezintă PAT (Port Address Translation), uneori denumită şi *NAT* overloaded sau masquerading. Această metodă permite un număr de aproximativ 64000 de conversaţii simultane de la orice host intern către exterior cu o singură adresă externă. Implementarea înlocuieşte pachetul din reţeaua locală cu adresa sursă S, adresa destinaţie D, portul sursă P, portul destinaţie Q, cu altul nou ce va avea adresa sursă M (adresa ruterului), adresa destinaţie D, portul sursa K. Portul destinaţie nu se schimbă. De asemenea se memorează asocierea (S,P) - K. Dacă un pachet ajunge pe ruter din exterior, având adresa destinaţie M, adresa sursă Q şi portul destinaţie K, atunci acest pachet va fi înlocuit cu un altul cu adresa destinaţie S, adresa sursă Q, portul destinaţie P şi va fi trimis în reţeaua locală. Portul sursă nu se schimbă.
Un caz special al PAT îl reprezintă redirectarea. În acest caz se va înlocui pachetul primit din reţeaua locală având adresa sursă S, adresa destinaţie D, portul P cu un altul având adresa sursă S, adresa destinaţie M (adresa ruterului), portul R (portul în care se face redirectarea, specificat de utilizator). Redirectarea este în general folosită pentru a implementa un proxy transparent, caz în care pe ruterul M portul R ascultă un proxy configurat pentru proxy transparent.

Marele dezavantaj al NAT constă în faptul că anumite protocoale (protocoale cu adrese criptate sau adrese embedded) nu lucrează cu adrese

IP translatate. Un alt dezavantaj derivă din pierderea conectivității end-to-end ceea ce face foarte dificilă depanarea problemelor de rutare.

3. Desfăşurarea lucrării

3.1 Instalarea serviciului DHCP

Implementarea unui server DHCP presupune instalarea serverului, autorizarea serverului; configurarea scopurilor, excluziunilor, rezervărilor şi opțiunilor şi verificarea configurării. Pentru a implementa DHCP, trebuie să se instaleze serviciul DHCP pe un calculator cu Windows 2000 Server din rețea. Înainte de instalarea serviciului DHCP, calculatorul trebuie să se configureze static cu o adresă IP, mască şi gateway.

1. Selectați Start, Settings, Control Panel, Add or Remove Programs.
2. În pagina Add or Remove Programs, alegeți Add/Remove Windows Components pentru a deschide Windows Component Wizard.
3. Selectați Networking Services.
4. Apăsați butonul Details pentru a deschide fereastra Networking Services.
5. Selectați Dynamic Host Configuration Protocol (DHCP) şi apăsați OK.
6. Înapoi în fereastra Windows Components Wizard, apăsați Next pentru începerea instalării.

După instalarea cu succes, verificați dacă serviciul Server DHCP a fost instalat prin deschiderea consolei de administrare. Pentru aceasta mergeți la Start şi selectați Administrative Tools, apoi DHCP. Consola DHCP este interfața din care configurați şi administrați serviciul DHCP al serverului.

Notă: Serverele DHCP trebuie autorizate daca urmează să fie integrate în rețele cu Active Directory; printr-un simplu click dreapta pe nodul server în consola DHCP şi alegerea opțiunii Authorized.

3.2 Configurarea scopurilor

1. Deschideți consola DHCP şi selectați New Scope din meniu.
2. Numiți scopul Scop Test.

3. În pagina IP Address Range, în Start IP Address scrieți 192.168.0.1, în End IP Address scrieți 192.160.0.10. Verificați valoarea măştii: 255.255.255.0.
4. În fereastra Excluded Address Range, excludeți adresa 192.168.0.1 şi intervalul 192.168.0.3 – 192.168.0.5.

Notă: Se poate configura durata închirierii unei adrese prin DHCP. Valoarea implicită este de 8 zile dar poate fi schimbată cu orice valoare de la 1 minut la 1000 zile (999 zile, 23 de ore, 59 de secunde, mai exact). Configurați durata închirierii la 10 minute.

5. În următoarea pagină, Configure DHCP Options, puteți configura acum/mai tîrziu informații suplimentare. Configurați în pagina Default Gateway, DNS Server cu datele furnizate de instructor.
6. În următoarea pagină, Activate Scope, se activează acum/mai tîrziu scopul configurat. În majoritata cazurilor activarea scopului se face acum. Selectați Yes, I Want to Activate This Scope Now şi apăsați Next pentru activarea scopului configurat.

3.3 Configurarea clientului

1. Deschideți Local Area Connection Properties şi Internet Protocol (TCP/IP) Properties.
2. În General, selectați Obtain An IP Address Automatically.
3. Selectați Obtain DNS Server Address Automatically.
4. În Local Area Connection Properties, apăsați Close.

3.4 Testarea configurării

1. Deschideti un command prompt.
2. Executați comanda `ipconfig /all`.

Configurația obținută prin DHCP este afişată: adresa IP, adresa gateway, adresa serverului DHCP şi adresa serverului DNS.

3.5 Testarea configurării prin alte exemple

1. Opriți serverul DHCP.
2. La client, executați `ipconfig/all.` Ce adresă IP are clientul?
3. Asteptați să expire perioada de închiriere a adresei (10 minute). Executați `ipconfig/all`. Care este noua adresă a clientului?

4. Reporniți serverul DHCP. La client, executați `ipconfig/all`. Care este adresa clientului acum?
5. Pe serverul DHCP faceți o rezervare pentru adresa 192.168.0.2.

Nota: Puteți configura o rezervare prin click dreapta pe Reservations şi alegeți New Reservation. Configurarea rezervării se poate face pentru orice echipament pentru care vreți să aveți o adresă asignată prin DHCP care nu expiră niciodata. Configurați rezervarea pentru o adresă MAC din laborator, aceasta va apărea în Reservations, în consola DHCP.

6. La client, executați `ipconfig/release` apoi `ipconfig/renew`. Care este adresa clientului acum?

Notițe