**DHCP**

DHCP este folosit pentru a aloca automat adresele IP hosturilor dintr-o reţea; astfel se uşurează munca de configurare a acestora.

În afara de adresa IP, prin serviciul care rulează pe server DHCP se mai pot aloca şi alti parametri: adresa de default gateway, numele de domeniu, adresa serverului de DNS, etc.

Funcţionarea este urmatoarea:

* în reţea se instalează un server de DHCP;
* hosturile care au nevoie de adresa IP (pot fi la limita şi calculatoare fără hard disc sau alt mediu pe care să fie stocată configuraţia) trimit la pornire un mesaj în care cer un IP; adresa sursă a mesajului este adresa MAC a hostului,
* în timp ce adresa destinaţie este adresa broadcast a reţelei, întrucît ele nu cunosc adresa serverului de DHCP.
* serverul de DHCP răspunde, trimiţînd către adresa MAC de unde a venit mesajul, un mesaj în care îi comunică hostului doritor ce adresă IP (şi alti parametri) să folosească.
* această adresă poate fi aleasă aleator sau configurată dupa o tabelă de corespondenţă adresa MAC adresa IP, configurată manual de către administratorul rețelei.

La ora actuală majoritatea routerelor folosite acasă de cei mai mulți utilizatori au intergrat acest serviciu. Cu ajutorul acestui serviciu se pot conecta până la 254 calculatoare la acel router, fie prin cablu fie wireless. Dacă se dorește conectarea unui număr mare de calculatoare prin conexiune WiFi trebuie ca emițătorul să fie destul de puternic.

Pentru a extinde zona de acoperire trebuie să folosim un dispozitiv denumit “Range Extender wireless”.

Pentru a extinde numărul de calculatoare conectate prin fir trebuie să conectăm la porturile LAN ale routerelor switch-uri cu mai multe porturi. Deobicei routerele au 4 porturi LAN.

**Observație!** Numărul de calculatoare combinate pe fir sau wireless poate fi maxim 254.

**IP-uri private**

1. *Adresa IP Dinamica (Dynamic IP Address):* Reprezintă o adresa IP ce se poate schimba oricand fiind destinată echipamentelor ce nu necesita conexiune permanenta la Internet/Rețea. Aceasta adresa IP este alocată de către furnizorul tau de acces la internet (ISP) sau de catre un Server DHCP. Acest lucru este destinat unui numar mare de clienti ce nu necesită sa aibe aceeași adresă IP mereu, din mai multe motive. Calculatorul va prelua automat o adresa IP cand se conectează la rețeaua respectivă fără să fie nevoie să se cunoască detaliile rețelei respective privind configurarea. Aceasta adresa IP poate fi alocată oricui utilizează o conexiune dial-up, conexiuni wireless și conexiuni de mare viteză (Hight Speed Internet).

*Dacă se dorește a se realiza un server de email sau un server web, este recomandat să se aloce acelui calculator o adresă IP statică.*

1. *Adresa IP statica (Static IP Address):* Este o adresa IP fixă ce nu se schimbă niciodată fiind destinată echipamentelor ce necesită conexiuni permanante la Internet/Rețea. Este în contrast cu o adresa IP dinamică ce se poate schimba oricand. Majoritatea furnizorilor de acces la internet pot aloca o adresa IP statică sau un bloc de adrese statice pentru o taxa suplimentară la abonament.

**IP-uri publice (reale)** sunt acele adrese IP care sunt:

* vizibile în întregul Internet
* necesare pentru dispozitivele care ofera date.

**Utilitare folosite pentru aflarea unor informații cu ajutorul adreselor IP**

1. TRACERT

Cu ajutorul acestui utilitar aflăm informații legate de numarul de routere aflat între noi și destinatie se poate afla folosind comanda tracert. Rezultatul ofera adresele IP sau numele routerelor tranzitate.

Sintaxa pentru sisteme Windows este:

**tracert [-d][-h maximum hops][-j host\_list][-w timeout] target\_name**

target\_name este numele domeniului (de exemplu google.ro) sau adresa IP.

-*d* Do not resolve addresses to hostname

-*h maximum\_hops* Maximum number of hops to search for target

-*j host-list* Loose source route along host-list

-*w timeout* Wait timeout miliseconds for each repply

**Exemplu:** dintr-o fereastra DOS (Start -> Run -> tastati: cmd -> OK) tastati:

**tracert google.ro.** Rezultatul va fi ca cel din figura 3.2.



*Fig. 3.2. Rezultatul folosirii utilitarului TRACERT*

1. PING

Prescurtare de la Packet InterNet Groper, este o comanda folosita pentru a verifica daca pachetele de date ajung la o adresa (destinatie) fara erori.

Sintaxa pentru sisteme Windows este:

**ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]**

 **[-r count] [-s count] [[-j host-list] | [-k host-list]]**

 **[-w timeout] destination-list**

**Exemplu:** dintr-o fereastra DOS (Start -> Run -> tastati: cmd -> OK) tastati:

ping google.ro. Veți obține informațiile din figura 3.3.



*Fig. 3.3. Rezultatul folosirii utilitarului PING*

Utilitarul PING se poate folosi simplu sau cu adaugarea unor terminații ca cele de mai jos care ne dau informații suplimentare:

**-t** Pings the specified host until stopped

 To see statistics and continue - type Control-Break

 To stop - type Control-C

**-a** Resolve addresses to hostnames

**-n count** Number of echo requests to send

**-l size** Send buffer size

**-f** Set Don't Fragment flag in packet

**-i TTL** Time To Live (TTL poate lua valori între 0 și 255)

**-v TOS** Type Of Service

**-r count** Record route for count hops

**-s count** Timestamp for count hops

**-j host-list** Loose source route along host-list

**-k host-list** Strict source route along host-list

**-w timeout** Timeout in milliseconds to wait for each reply



*Fig. 3.4. Rezultatul folosirii utilitarului* ***PING*** *și terminația* ***-i 255***

 **TTL (Time To Live)**

Este un camp de 8 biți din header-ul IP și este conținut de al 9-lea octet din cei 20.

Campul TTL este stabilit de computerul care trimite datagrama și este decrementat de fiecare host (echipament activ de rețea) aflat în ruta către destinație. Dacă acest camp ajunge la 0 înainte ca datagrama să ajungă la destinație datagrama va fi ștearsă și se va genera o eroare ICMP (11 - Time Exceeded) care va fi trimisă înapoi calculatorului sursă. Scopul campului TTL este de a evita situația în care o datagrama nelivrată continuă să circule prin Internet.

**TTL reply** este valoarea afișată ca raspuns la executarea comenzii ping.

**Exemplu:** daca între noi si destinatie sunt 7 routere si valoarea originala pentru TTL este 64 vom primi raspunsul 64-(7\*1)=57, ca în figura 3.5.



*Fig. 3.4. Informații pentru TTL (timpul de viață al datagramei)*

De notat că, în anii furnizării accesului internet către clienţii de tip “home users” prin reţeaua telefonică, DHCP a fost şi o soluţie de economisire a adreselor IP, deoarece clienţii care se conectau telefonic nu stăteau conectaţi tot timpul; prin urmare, un ISP putea avea un milion de clienţi, din care doar 10% să fie conectaţi simultan, fiind suficient numărul corespunzător de adrese.

Odată cu trecerea la accesul internet prin tehnologii de tipul “always on” (ISDN, cablu, ADSL, etc) nu se mai pot face economii de adrese pe această cale, iar DHCP este folosit doar pentru simplificarea administrării alocării de adrese IP.

**NAT**

NAT (Network Address Translation) este principala tehnologie care a permis Internetului să se dezvolte chiar dacă adresele IP sunt limitate ca număr. În interiorul unei organizaţii se pot folosi adrese IP private, nerutabile (din RFC1918), dar calculatoarele (hosturile) cu aceste adrese nu sînt vizibile în Internet. NAT rezolvă această problemă ca în figura 3.5.

**LAN**

**Internet**

**NAT**

**AS**

**192.168.0.25**

**AD**

**171.68.68.2**

**AS**

**171.68.68.2**

**AD**

**192.168.0.25**

**IP computer**

**192.168.0.25**

*Fig. 3.5. Serviciu NAT*

O organizaţie cumpără un număr redus de adrese IP rutabile de la un ISP, dar nu le alocă hosturilor interne; acestea primesc adrese private.

Un PC cu adresa privată (192.168.0.25) trimite un pachet cu această adresă sursă (**AS**) către un host din Internet. Ruterul de la graniţa organizaţiei schimbă această adresă cu o adresa rutabilă (171.68.68.2), dintre adresele cumpărate, şi trimite pachetul în Internet. De asemenea, el introduce această translaţie într-o tabelă locală.

Hostul destinaţie trimite pachetul de răspuns cu adresa destinaţie (**AD**) rutabilă, şi acesta ajunge înapoi la ruter. Ruterul işi consultă tabela de translaţie şi schimbă la loc adresa cu cea din interiorul organizaţiei, astfel ca PC-ul initial nici nu va detecta că “pe drum” adresa i-a fost translatata.

Adresa privată se numeste **inside address** iar cea publică, obtinuta prin translatare, se numeste **outside address**.

De notat că în general NAT poate face translaţia între orice fel de adrese, nu numai între private şi publice, aceasta fiind doar varianta cea mai raspândită (şi cea mai utilă).

**Variante de NAT:**

* NAT-ul simplu, “clasic”, este atunci când există suficiente adrese reale atfel ca toate hosturile interne să poata accesa, simultan, prin translatare, destinaţii externe. Această formă de NAT nu este utilă pentru rezolvarea crizei de adrese reale, ci doar pentru “mascarea” adreselor interne din diferite motive (de exemplu, de securitate).
* NAT-ul cu overload este atunci cînd numărul de adrese reale este mai mic decît umarul hosturilor interne (caz tipic). În acest caz, ruterul care face NAT va modifica şi portul sursă al pachetului, nu numai adresa sursă;
* **2 pachete cu aceeasi adresa outside vor putea fi diferenţiate prin numărul de port, şi la venirea pachetului de răspuns se refac adresa şi portul iniţiale.**

Această metoda funcţionează pentru că în aproape toate cazurile, portul sursă al unui pachet este ales la întîmplare de către sistemul de operare cînd trimite pachetul (nu va fi vizibil pentru utilizator), deci nu contează că este translatat. Numai portul destinaţie este important şi este binecunoscut (de exemplu, 80 sau 8080 pentru aplicațiile web). Există, totuşi, excepţii, care fac ca nu toate aplicaţiile să funcţioneze în spatele NAT.

* PAT (Port Address Translation) sau NAPT (Network Address Port Translation) este cazul precedent dus pînă la extrem, şi anume folosirea unei singure **adrese outside** rutabile şi diferenţierea între **adresele inside** numai după numarul de port. Această metodă este folosita pe scara largă de către organizațiile mici sau home-users, care cumpară un singur IP real. Sub Linux această varianta se mai numeşte şi IP Masquerading.
* Port Forwarding este un caz particular în care un port clar specificat de pe un host este translatat într-un alt port (cu acelaşi număr sau număr diferit) de pe alt host (cu adresa diferită).

O aplicaţie directă este instalarea de servere pentru anumite servicii (web, mail, etc) în interiorul unei organizaţii care foloseşte adrese private. Porturile destinaţie ale serviciilor respective, de pe adresa/adresele reale ale ruterului care face NAT, accesate din exterior, sînt translatate către porturile corespunzătoare ale serverelor din interior. Astfel, serviciul respectiv pare dinspre Internet că ruleaza pe ruter, cînd de fapt rulează pe un host din interior.

**PORT FORWARDING**

Dorim să permitem accesul dinspre Internet înspre un server (care oferă un serviciu oarecare: web, telnet, etc) din interiorul domeniului cu adrese private, ceea ce nu se poate în mod direct, căci adresele private nu sînt evident rutabile în Internet. Vom folosi adresa publică, de Internet, a lui R0 (1.1.1.1); accesul Telnet (port 23) de pe această adresă va fi redirectat către serverul de Telnet de pe R1 (192.168.1.2).