Facultatea de Electronică, Telecomunicații si Tehnologia Informației

**NET-Nivelul Network in Internet**

Coordonator: Studenți:

Conf. dr. ing. Ștefan Stăncescu Răducanu Marilena

Roșca Mihai

Grupa 441A

Universitatea Politehnica București

**Cuprins:**

1)Introducere(Răducanu Marilena)............................................................. 3

2)Protocolul IP(Răducanu Marilena)........................................................... 4

3)Adrese IP

3.1)Subrețele(Răducanu Marilena).................................................. 4

3.2)CIDR(Răducanu Marilena).......................................................... 5 3.3)NAT(Răducanu Marilena)........................................................... 6

4)Ipv6(Roșca Mihai).................................................................................... 6

5)Protocoale de control

5.1)ICMP(Roșca Mihai)...................................................................... 7

5.2)ARP(Roșca Mihai)........................................................................ 8

5.3)RARP(Roșca Mihai)...................................................................... 8

5.4)DHCP(Roșca Mihai)...................................................................... 9

6)Bibliografie(Răducanu Marilena,Roșca Mihai)......................................... 11

**1.Introducere**

Rolul layer-ului de rețea este de a transporta pachete intre host-uri, in timp ce se pune cat mai putina presiune pe rețea. Acest layer este nu este interesat sau conștient de tipurile de comunicații conținute de pachete. IP-ul este lipsit de conexiune, adică nici o conexiune dedicata end-to-end nu este creata înainte de trimiterea datelor. Comunicațiile fără conexiune sunt in principiu similare trimiterii de scrisori fără anunțarea destinatarului in prealabil.

Stratul de rețea, sau OSI Layer 3, oferă servicii pentru a permite dispozitivelor finale schimbul de date în întreaga rețea. Pentru a realiza acest transport, stratul de rețea utilizează patru procese de bază:

- Abordarea dispozitivelor finale de rețea – La fel cum un telefon are un număr unic, echipamentele finale de rețea trebuie sa aibă o adresa IP unica pentru identificarea in rețea. Un astfel de echipament cu adresa IP configurata se numește host.

- Încapsulare – Layer-ul de rețea primește o unitate protocol de data (PDU) din layer-ul de transport. Printr-un proces numit încapsulare, layer-ul de rețea adaugă informații din headerul IP, cum ar fi adresele IP ale sursei si ale destinatarului. Rezultatul acestei adăugări de date in PDU se numește pachet.

- Routare – Layer-ul de rețea oferă servicii de direcționare a pachetelor către un host destinație sau o alta retea. Pentru transmiterea in alte rețele, pachetul trebuie mai întâi procesat de un router. Un alt rol al routerului este de a selecta cai pentru transmiterea directa a pachetelor către host-urile destinație printr-un proces numit routare. Un pachet poate trece prin mai multe device-uri intermediare înainte de a ajunge la host-ul destinație. Fiecare cale pe care pachetul o parcurge pentru a ajunge la destinație, se numește hop.

- Decapsulare – Când pachetul ajunge la host-ul destinație, host-ul headerul IP al pachetului. Daca Ip-ul pachetul este același cu IP-ul expeditorului, headerul IP este înlăturat din pachet. Procesul de eliminare a headerelor din layer-ele de rang mic se numește decapsulare. După ce pachetul este decapsulat de layer-ul de rețea, layer 4 PDU rezultat este trimis către layer-ul de transport.

**2.Protocolul IP**

Exista mai multe protocoale de layere de rețea.Cu toate acestea, cele mai folosite doua sunt:

- Internet Protocol version 4 (IPv4)

- Internet Protocol version 6 (IPv6)

Ip-ul este serviciul de rețea implementat de protocolul TCP/IP.Ip-ul a fost gândit ca un protocol cu plafon scăzut. El oferă doar funcțiile necesare pentru transmiterea unui pachet dintr-o sursa către o destinație printr-un sistem interconectat de rețele. Protocolul nu a fost gândit pentru a urmări si a menegeria pierderile de pachete. Aceste funcții, daca sunt necesare, sunt îndeplinite de alte protocoale in alte layere.

Caracteristicile de baza ale IP-ului sunt:

- Lipsa conexiunii – Nu se stabilește o conexiune cu destinația înainte de trimiterea pachetelor

- Best Effort (nu este de încredere) – Trimiterea pachetelor nu este garantata

- Independent de mediul de transmisie – Operația nu depinde de mediul care transporta datele

**3. Adrese IP**

3.1 Subretele

Un subnetwork sau subnet, este o subdivizie logica, vizibila a unei rețele IP. Metoda folosita pentru împărțirea unei rețele in doua sau mai multe rețele se numește subnetting.

Subnetting-ul este un proces de desemnare a biților de ordin mare din host si gruparea lor cu masca rețelei pentru a forma masca subnet. Acest lucru împarte rețeaua in diviziuni mai mici. Diagrama următoare prezinta un exemplu prin mutarea a 2 biți.

|  |  |  |
| --- | --- | --- |
|  | **Binary form** | **Dot-decimal notation** |
| IP address | 11000000.10101000.00000101.10000010 | 192.168.5.130 |
| Subnet mask | 11111111.11111111.11111111.11000000 | 255.255.255.192 |
| Network prefix | 11000000.10101000.00000101.10000000 | 192.168.5.128 |
| Host part | 00000000.00000000.00000000.00000010 | 0.0.0.2 |

Adrese speciale si subretele:

IPv4 folosește formate de adrese special create pentru o recunoaștere mai ușoara a adreselor de funcționalitate speciale. Prima si ultima subrețea aveau de obicei o desemnare speciala, care implica o folosire speciala. Mai mult de atât IPv4 folosește toate adresele de host.

IPv6 este următoarea generație de protocol de internet, cu adrese care vor suplimenta si eventual înlocui IPv4, protocolul cel mai folosit in zilele noastre.

3.2 CIDR

CIDR (Classless Inter-Domain Routing, câteodată numit supernetting) este un mod mai permisiv de acordare a adreselor IP decât era posibil cu sistemul original, pe clase. Ca rezultat, numărul de adrese disponibile a crescut foarte mult, ceea ce înseamnă ca durata de viată a IPv4 a crescut simțitor.

CIDR a redus problema spațiului de adrese pierdut inutil prin introducerea unui mod mai flexibil de a specifica adresele de rețea in routere. Sistemul este asemănător unuia de rețea publica de telefoane, unde apelurile sunt trimise către diferite parți ale rețelei. Acest mod este numit si supernet.

3.3 NAT

Network Address Translation (NAT) este un proces in care un device de rețea, de obicei un firewall, oferă o adresa publica unui computer (sau grup de computere) într-o rețea privata. Principala utilizare a NAT este de a limita numărul maxim de adrese IP publice pe care o companie sau o organizație pe poate folosii, din motive de securitate dar si economice.

Cea mai comuna forma de translatare implica o rețea privata mare cu adrese cuprinse intr-un interval mare (10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, or 192.168.0 0 to 192.168.255.255). Schema de adresare privata funcționează foarte bine pentru PC-uri care au acces la informații doar din interiorul rețelei. Routerele din interiorul rețelei private pot routa traficul intre adresele private fără probleme. Cu toate acestea, pentru a accesa resurse din afara rețelei, cum ar fi internetul, aceste computere trebuie sa primească o adresa publica înainte de a primi răspunsuri la cererile trimise. Aici intra in joc NAT.

NAT poate fi folosit pentru acordare selectiva a accesului in afara rețelei private. Stațiile de lucru sau pc-urile care cer acces special in afara rețelei pot primi adrese IP speciale pentru exterior, folosind NAT, oferindu-le posibilitatea de a comunica cu sisteme sau aplicații care necesita un IP public. Din nou, firewall-ul asigura intermedierea si poate bloca accesul in ambele direcții, restricționând porturile sau protocoalele.

Network Address Translation este un aspect foarte important al securitatii firewall. Acesta conserva numărul de adrese folosite de o organizație si oferă strictețe in controlul accesului in ambele direcții ale firewall-ului.

**4. IPv6**

IPv6 (Internet Protocol version 6) este un set de specificații de la Internet Engineering Task Force (IETF) care este in principiu un upgrade de IPv4. Funcțiile de baza ale IPv6 sunt similare cu cele ale lui IPv4 – device-urile pot folosi IPv6 ca sursa si destinație pentru pachetele trimise in rețea si ustensile ca ping pentru testarea rețelei.

Cea mai mare observație in IPv6 este ca lungimea adreselor a fost crescuta de la 32 de biți la 128 biți. Aceasta modificare anticipează o creșterea uriașa a internetului si oferă o scăpare pentru ceea ce se considera o lipsa a adreselor IPv4. IPv6 are de asemenea suport si pentru porțiunile in care IPv4 nu excela.

**Performante IPv6:**

- Suporta surse si destinații care au 128 biți.

- Necesita suport IPSec.

- Folosește câmp Flow Label pentru identificarea fluentei pachetelor pentru QoS prin router.

- Da voie host-urilor sa trimită pachete fragmentate dau nu routere.

- Nu include un checksum in header.

- Nu necesita o configurare manuala DHCP.

- Folosește adresele de host (AAAA) din resursele DNS pentru a face o harta de host pentru adresele IPv6.

- Folosește pointere pentru resursele din IPv6.ARPA, domeniu DNS, pentru maparea adreselor IPv6 la numele host-urilor.

- Suporta pachete de 1280 de byti (fără fragmentare).

- Muta datele opționale la extensiile header din IPv6.

- Folosește mesaje Multicast Neighbor Solicitation pentru a descompune adresele IP in layere de adrese.

- Folosește mesaje Multicast Listener Discovery (MLD) pentru a menegeria apartenenta intr-un grup de subrețea locala.

- Folosește ICMPv6 Router Solicitation si mesaje Router Advertisement pentru a determina adresa IP a celui mai bun gateway.

**5. Protocoale de control**

5.1 Internet Control Message Protocol (ICMP)

ICMP este un mecanist de raportare si diagnosticare a erorilor, parte necesara implementării unui IP. Înțelegerea ICMP si ce poate genera un anumit tip de ICMP este folositor in diagnosticarea problemelor de retea.ICMP-urile sunt folosite routere, device-uri intermediare sau host-uri pentru a comunica update-uri sau informații despre erori către routere, device-uri intermediare sau host-uri

Fiecare mesaj ICMP conține trei câmpuri care ii definesc scopul si asigura control. Acestea sunt TYPE, CODE si CHECKSUM.

Câmpul TYPE identifica mesajul ICMP.

Câmpul CODE oferă informații adiționale despre câmpul TYPE asociat.

Câmpul CHECKSUM oferă o metoda de determinare a integrității mesajului.

**Cerere si răspuns ECHO:**

ICMP-ul cel mai folosit pentru a testa conectivitatea IP, numita PING. Cererea ECHO ICMP va avea un câmp tip diferit de 8 si un câmp cod de 0. Răspunsurile ECHO vor avea un câmp tip de 0 si unul de cod, tot 0.

**Destinație inaccesibila:**

Când un pachet este netransmisibil, un ICMP, tip 3, Destinație Inaccesibila este generat. ICMP-urile de tip 3 pot avea in Code o valoare de la 0 la 15.

**Source Quench:**

Un mesaj ICMP Source Quench are un câmp tip de 4 si unul code de 0. Mesajele Source Quench sunt trimise când destinația este in incapacitate de procesare a traficului la viteza de trimitere a acestuia. ICMP-ul Source Quench comunica sursei sa scadă rata la care sunt trimise datele. Destinația va continua sa genereze acest ICMP pana când sursa oferă datele la o viteza acceptabila.

**Redirecționarea mesajului:**

Un device intermediar va genera un ICMP Redirect Message când va determina ca ruta dorita poate fi accesata fie local, fie printr-o cale mai buna. Aceste ICMP-uri sunt de tip 5 si sunt definite de următoarele valori ale câmpului 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

**Timp depășit:**

Daca un router sau un host decartează pachetul din cauza unui time-out, acesta va cenera un ICMP tip 11 Time Exceeded. Valoarea code-ului va fi ori 0 ori 1. Un code 0 este generat când hop-ul unui datagram este depășit si pachetul este decartat. Un code 1 este generat cand reasamblarea fragmentelor pachetului depășește valoarea de time-out.

5.2 Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) este un protocol de mapare a adresei IP a unui echipament fizic care este recunoscut in rețea. De exemplu, in IPv4, cel utilizat nivel de IP in zilele noastre, o adresa de 32 de biți lungime. Intr-o rețea locala Ehternet in schimb, adresele atașate device-urilor au o lungime de 48 de biți (Adresa fizica a unui device este numita adresa MAC). Un tabel, uzual nimic ARP cache, este folosit pentru a păstra o corelație intre fiecare adresa MAC si corespondentul IP. ARP asigura regulile de protocol pentru a face legătura si conversia in ambele sensuri a adreselor.

Cum funcționează ARP-ul:

Când un pachet destinat unei mașini host plasata într-o anumita zona a rețelei, ajunge la un gateway, acesta cere programului ARP sa găsească host-ul fizic sau o adresa MAC care sa se potrivească cu adresa IP. Programul ARP verifica ARP cache-ul; daca găsește o adresa care sa se potrivească, o oferă pachetului pentru a fi convertit la lungimea si formatul dorit si este trimis device-ului. Daca nu este găsita adresa IP, ARP-ul emite un pchet intr-un format special către toate device-urile din rețea ca sa vadă daca exista o potrivire. O mașina care recunoaște adresa IP ca fiind a ei, trimite înapoi un răspuns indicator. ARP-ul își updateaza cache-ul pentru referințe viitoare si trimite pachetul inițial către adresa MAC care a răspuns.

5.3 Reverse Address Resolution Protocol (RARP)

RARP (Reverse Address Resolution Protocol) este un protocol prin care o mașina fizica in rețeaua locala poate cere sa I se ofere propriul IP din gateway-ul server-ului ARP (tabel sau cache). Un administrator de rețea creează o tabela in router-ul gateway-ului unei rețele locale care mapeaza adresele mașinilor fizice (MAC). Când un now device este pus in funcțiune, clientul lui RARP programează cereri către server-ul RARP pentru a i se da adresa IP corespunzătoare lui. Presupunând ca a i s-a inițializat câmp in tabelul de routare, server-ul RARP va returna adresa IP a mașinii pentru a putea fi folosita si in viitor.

RARP este disponibil pentru Ethertnet, Fiber Distributed-Data Interface si token ring LANs.

5.4 Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) este un client/protocol de server care ofera automan un IP host propria adresa IP si alte lucruri legate de informațiile de configurare, cum ar fi subnet mas-ul si gateway-ul principal.

De ce sa folosim DHCP?

Orice device dintr-o adresa bazata pe TCP/IP are nevoie de o adresa IP unica pentru a accesa rețeaua si resursele ei. Fără DHCP, adresa ip a noilor computere care sunt mutate dintr-un subnet in altul trebuie configurata manual. Adresele IP pentru computere care sunt eliminate din rețea, trebuie repuse la uz manual.Cu DHCP, întregul proces este făcut automat si centralizat. Serverul DHCP conține toate adresele IP si la cerere “împrumuta” adresele oricărui device cu DHCP care intra in rețea. Deoarece majoritatea adreselor IP nu mai sunt statice, ci dinamice, după folosire adresele IP se întorc înapoi in lista de adrese disponibile pentru realocare.

Administratorul de rețea creează servere DHCP care conțin datele de configurare TCP/IP si care oferă adrese IP device-urilor DHCP care intra in rețea. Informațiile conținute de serverele DHCP sunt:

- Parametrii TCP/IP de configurare valizi pentru toți clienții rețelei.

- Adrese IP valide si adrese IP indisponibile.

- Adrese IP rezervate si device-ul căruia ii este atribuita. Acest lucru ajuta la nu acorda unui device mai multe adrese.

- Durata pe care o adresa IP poate sta in folosința pana când trebuie reînnoita.

Un client cu DHCP, in momentul achiziției unei oferte de adresa, primește:

- O adresa IP valida pentru rețeaua la care urmează sa se conecteze.

- Opțiunile DHCP ceruta, care semnifica parametrii DHCP suplimentari. Câteva exemple ar fi Router-ul, Serverul DNS, si numele de domeniu DNS.

**Beneficiile DHCP:**

- Adrese IP cu configurare de încredere

- Reducerea nivelului de administrare a rețelei

**6. BIBLIOGRAFIE**

<http://www.wildpackets.com/resources/compendium/tcp_ip/unreachable>

<http://whatismyipaddress.com/dhcp>

<http://www4.ncsu.edu/~kksivara/sfwr4c03/lectures/lecture3.pdf>

<http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html>

<https://www.digitalocean.com/community/tutorials/understanding-ip-addresses-subnets-and-cidr-notation-for-networking>

<http://www.webopedia.com/TERM/N/NAT.html>

<http://searchnetworking.techtarget.com/definition/subnet>