

Echipa de retea
RFC: 950

J. Mogul (Stanford)
J. Postel (ISI)
August 1985

Internet Standard Subnetting Procedure
Procedura internet standard de subconectare

Pozitia(locul) acestui memo

Acest RFC specifica un protocol pentru comunitatea de internet - ARPA. Daca subconectarea e implementata, e recomandat ca aceste proceduri sa fie sa fie realizate. Distribuirea acestui memo este nelimitata.

Vedere de ansamblu

Acest memo discuta (prezinta) utilitatea "subretelelor" ale retelelor de internet, care sunt logic vizibile ca subsectiuni a unei singure retele de internet. Din cauza unor motive tehnice sau administrative, multe organizatii au ales sa divida o retea de internet in mai multe subretele, in loc sa-si insuseasca un set de numere de retele internet. Acest memo specifica procedurile pentru utilizarea subretelelor.

Aceste proceduri sunt pentru calculatoarele gazda (statii de lucru). Procedurile folosite in si intre portile (legaturile) retelelor nu sunt pe deplin descrise. O motivatie importanta si o informatie de fond pentru o subretea standard e oferita in RFC-940 [7].

Recunoastere(confirmare, certificare)

Acest memo e bazat pe RFC-917 [1]. Multi oameni au contribuit la dezvoltarea conceptelor descrise aici. J. Noel Chiappa, Chris Kent si Tim Man, in particular, au furnizat sugestii importante. Contributii suplimentare in configurarea acestui memo, au fost realizate de Zaw-Sing Su, Mike Karels si Algoritmi Portii si GADS.

1.Motivare

Planul (schita, rezumatul) original al universului (sistemului) Internet a fost o organizare ierarhica pe doua nivele: *nivelul superior* Internetul vazut ca un intreg si *nivelul inferior* retele individuale, fiecare cu numarul propriu de retea.

Internetul nu are o topologie ierarhica, mai degraba interpretarea adreselor este ierarhica. In acest model de doua nivele, fiecare gazda isi vede retea ca o singura entitate; adica retea poate fi tratata ca o "cutie neagra" la care un set(o multime) de gazde se conecteaza.

Atata timp cat aceasta schita s-a dovedit simpla si puternica, un numar de organizatii au gasit-o necorespunzatoare si au adaugat un al treilea nivel la interpretarea adreselor de internet. In aceasta schita, o retea de internet data, este divizata intr-o colectie de subretele.

Modelul cu trei nivele e util in retele care apartin unor organizatii destul de intinse (e.g., universitati sau companii care au mai mult de o cladire), unde e adesea necesar sa folosim mai mult de un cablu LAN pentru a acoperi o "retea locala". Fiecare retea LAN poate fi deci tratata ca o subretea.

Sunt asadar cateva motive pentru care o organizatie poate folosi mai mult de un cablu pentru a acoperi un campus universitar.

- tehnologii diferite: indeosebi intr-un mediu de cercetare, acolo ar trebui sa fie folosita mai mult de un tip de retea LAN; e.g., o organizatie poate avea echipament ce suporta fie reseaua Ethernet, fie cea de tip inel (ring network).
- limitele tehnologiei: majoritatea tehnologiilor LAN impun limite bazate pe parametri electrici, pe numarul de calculatoare gazda conectate si pe lungimea totala a cablului. Este usor sa depasesti aceste limite, in special pe cele legate de lungimea cablului.
- congestia retelei: este posibil ca pentru un mic subset al calculatoarelor gazda intr-o retea LAN, sa monopolizam majoritatea largimii de banda. O solutie obisnuita a acestei probleme este sa impartim gazdele in clici de inalta comunicare reciproca si sa punem aceste clici pe cabluri diferite.
- legaturi punct-la-punct: cateodata, o "suprafata locala", cum ar fi un campus universitar, este impartit in doua locatii prea deosebite pentru a se conecta utilizand preferata tehnologie LAN. In acest caz, legaturile punct-la-punct de viteza mare pot conecta mai multe LAN-uri.

O organizatie care a fost fortata sa foloseasca mai mult de o retea LAN are trei posibilitati pentru alocarea adreselor de internet.

1. Castigarea (dobandirea) unui numar de retea distinct pentru fiecare cablu; subretelele nu sunt folosite cu totul (la maxim).
2. Utilizati un singur numar de retea pentru intreaga organizatie, dar atribuiti (alocati, asignati) numere gazda fara a avea in vedere, la care LAN se afla o gazda ("subretele transparente").
3. Utilizati un singur numar de retea si partitionati spatiul de adresa al gazdei asignand numere de subretea retelelor LAN ("subretele explicite").

Fiecare dintre aceste abordari are dezavantaje. Prima, cu toate ca nu necesita protocoale noi sau modificate, rezulta intr-o explozie a marimii tabelelor de rutare. Informatii despre detaliile interne ale legaturii locale sunt raspandite oriunde, desi este de un ajutor nesemnificativ sau de nici un ajutor in afara organizatiei locale. Mai ales, cum unele implementari actuale ale porturilor nu au prea mult spatiu pentru tabelele de rutare, ar fi bine sa evitam aceasta problema.

A doua abordare necesita cateva conventii sau protocoale care fac ca colectia de LAN-uri sa fie considerata a fi o singura retea de internet. De exemplu, aceasta poate fi facuta pe LAN-urile in care fiecare adresa de internet e transferata la o adresa hard, utilizand un Protocol de Rezolutie a Adresei (ARP), avand punctele dintre LAN-urile care intercepteaza cererile ARP pentru tinte nelocale., vezi RFC-925 [2]. Oricum, nu este posibil sa facem aceasta pentru toate tehnologiile LAN, in special la acelea la care protocoalele ARP nu sunt curent folosite sau daca reseaua LAN nu suporta difuzarea. O problema mai importanta este aceea ca punctele trebuie sa descopere pe ce LAN se afla o gazda, probabil utilizand un algoritm de difuzare. Cu cat numarul de LAN-uri creste, cu atat creste si costul difuzarii; de asemenea, dimensiunea transferului de cache ceruta in puncti, creste o data cu numarul total de gazde din retea.

A treia abordare este sa suporte in mod explicit subretelele. Aceasta are insa un dezavantaj, care consta in modificarea protocolului de internet si prin urmare

se cer schimbări în implementarea IP-ului care este deja în funcțiune (dacă aceste implementări vor folosi într-o rețea subconectată). Oricum, aceste schimbări sunt relativ minore, și, odată făcute, produc o rezolvare simplă și eficientă a problemei. De asemenea, abordarea evită orice schimbări care pot fi incompatibile cu gazdele existente în rețele nesubconectate.

În plus, când alegeri de planuri adecvate sunt făcute, este posibil ca pentru gazdele care credeam că sunt într-o rețea nesubconectată, să fie folosite într-una subconectată, așa cum este explicat în RFC-917 [1]. Acest lucru este util atunci când nu este posibil să modificăm câteva dintre gazde pentru a suporta subrețele în mod explicit sau când o tranziție treptată este preferată.

2. Standardele pentru Adresarea Subrețelelor

Această primă secțiune descrie o propunere pentru interpretarea adreselor de internet pentru a suporta subrețele. Apoi sunt discutate schimbările la soft-ul gazdei pentru a suporta subrețele. La sfârșit, este prezentată o procedură pentru a descoperi ce interpretare a adresei este folosită într-o rețea dată (i.e., ce mască de adresă este folosită).

2.1. Interpretarea adreselor de internet

Presupunând că unei organizații i s-a asignat un număr de rețea și în plus a divizat acea rețea într-un set de subrețele și vrea să aloce (asigneze) adrese gazdei: cum ar trebui să fie făcută aceasta? Cum există restricții minimale la alocarea "adreselor locale", o parte a adreselor de internet, mai multe abordări au fost propuse pentru reprezentarea numărului de subrețea:

1. Câmpul lățime-variabilă: Orice număr de biți ai părții de adrese locale sunt folosiți pentru numărul de subrețea; mărimea acestui câmp, deși constantă pentru o rețea dată, variază de la o rețea la alta. Dacă lățimea câmpului este zero, atunci subrețelele nu sunt folosite.
2. Câmpul lățime-fixă: Un număr specific de biți (e.g., opt) este folosit pentru numărul de subrețea, dacă subrețelele sunt folosite.
3. Autocodificarea câmpului lățime-variabilă: Așa cum lățimea (i.e., clasă) câmpului numărului de rețea este codificată de ordinea mare (ridicată) a bitilor, tot așa este codificată și lățimea câmpului subrețelei.
4. Autocodificarea câmpului lățime-fixă: Un număr exact de biți este folosit pentru numărul de subrețea.
5. Bitii mascati (ascunși): Utilizati un bit mască ("mască adresei") pentru a identifica care biți ai câmpului adresei locale indică numărul de subrețea.

Care criteriu poate fi folosit pentru a alege una dintre aceste cinci scheme? Pentru început, ar trebui să folosim o schemă autocodificată? Și va fi posibil să se spună din examinarea unei adrese de internet dacă aceasta se referă la rețea subconectată, fără ajutorul nici unei alte informații?

O caracteristică interesantă a autocodificării este aceea că permite ca spațiul de adresă al unei rețele să fie divizat în subrețele de diferite mărimi, tipic o rețea la jumătate din spațiul de adrese și un set de mici subrețele.

De exemplu, considerand o retea de clasa C, care foloseste o schema de autocodificare cu un bit care sa indice daca este o subreteea mare sau nu, si in plus, trei biti care sa identifice subreteaua mica. Daca primul bit este zero, atunci aceasta este subreteaua mare, iar daca primul bit este unu, atunci urmatorii biti (trei in acest exemplu) dau numarul de subreteea.

Exista deci o subreteea cu 128 adrese gazda si opt subretele cu 16 gazde fiecare.

Pentru a stabili o subconectare standard, parametri si interpretarea schemei autocodificate, trebuie sa fie fiksi si consistenti prin internet.

Se poate presupune ca toate retelele sunt subconectate. Aceasta va trebui sa permita adreselor sa fie interpretate fara legaturi la alte informatii.

Acesta este un avantaj semnificativ, pentru ca, data adresa de internet, nici o alta informatie nu mai este necesara pentru o implementare pentru a determina daca doua adrese sunt pe aceeasi subreteea. Totusi, aceasta poate fi vazuta ca un dezavantaj: poate cauza probleme retelelor care au numere gazda existente si acestea folosesc biti imtamplator in partea de adrese locale.

Cu alte cuvinte, este necesar sa fii capabil sa controlezi daca o retea este subconectata independent de alocarea adreselor gazda.

Posibilitatea alternativa este sa stie faptul ca o retea e tinuta subconectata separat fata de adresare. Daca una afla, cumva, ca retea este subconectata, atunci regulile standard de autocodificare a adreselor retelei subconectate sunt urmate, altfel sunt folosite regulile de adresare ale retelei nesubconectate.

Daca o schema de autocodificare nu este folosita, atunci nu exista nici un motiv pentru a utiliza o schema a campului de latime fixa: de cand trebuie sa existe in orice caz, cateva "flag"-uri (stegulete) per-retea, care sa indice daca subretelele sunt folosite, costul suplimentar al folosirii unui intreg (latimea campului unei subretele sau masca de adrese) in locul unui boolean este nesemnificativ. Avantajul folosirii schemei mastii de adrese este acela ca permite fiecărei organizatii sa aleaga cea mai buna cale pentru a aloca in mod relativ putini biti ai adresei locale la subretele si numere gazda. De aceea, noi folosim schema mastii de adrese: este cea mai flexibila schema, care inca nu costa mai mult decat celelalte pentru a o implementa.

De exemplu, adresa de internet poate fi interpretata astfel:

<numar de retea><numar de subreteea><numar de gazda>

unde campul <numar-ul de retea> este definit de IP [3], campul <numar de subreteea> e de cel putin 1-bit latime si marimea campului <numar de gazda> e constanta pentru o retea data. Nici o alta structura nu este solicitata pentru campurile <numar de subreteea> sau <numar de gazda>. Daca latimea campului <numar de subreteea> este zero, atunci retea nu este subconectata (i.e., interpretarea lui [3] este folosita).

De exemplu, la o retea de clasa B cu un camp de subreteea de 6-biti latime, o adresa va fi distrusa astfel:


```

THEN
    send_dg_locally(dg, dg.ip_dest)
ELSE
    send_dg_locally(dg,
        gateway_to(bitwise_and(dg.ip_dest, my_ip_mask)))

```

Desigur, parte a expresiei din conditie poate fi pre-evaluata.

Poate fi, sau poate sa nu fie necesar sa modificam functia "gateway_to", astfel incat prea ia in considerare bitii campului subretelei atunci cand efectuam comparatiile.

Pentru a suporta multiple gazde conectate, codul poate fi schimbat pentru a pastra dimensiunile "my_ip_addr" si "my_ip_mask" intr-o per-legatura de baza; expresia din conditie trebuie sa fie evaluata apoi pentru fiecare legatura.

2.3. Gasirea mastii de adrese

Cum poate o gazda sa determine ce masca de adrese este folosita intr-o subretea la care este conectata? Problema este asemanatoare cu alte cateva probleme legate de "pornirea calculatorului" pentru gazdele de internet: cum o gazda isi determina propriile adrese si cum isi localizeaza o poarta in retea ei locala. In toate aceste trei cazuri sunt doua solutii de baza: informatia "hardwired" si protocoale bazate pe difuzare.

Informatia hardwired este acea informatie disponibila unei gazde izolate de retea. Poate fi compiled-in sau (de preferat) stocata intr-un fisier de pe disk. Oricum, pentru cazul comun de crestere al unei statii de lucru fara discuri care este bootloaded over a LAN, nici solutia hardwired nu este satisfacatoare.

In schimb, de cand majoritatea tehnologiilor LAN suporta difuzare, o metoda mai buna este ca noua gazda bootata sa difuzeze o cerere pentru informatiile necesare. De exemplu, pentru a-si determina adresa de internet, o gazda poate utiliza "Reverse Address Resolution Protocol" (RARP) [4].

Oricum, cum o gazda nou bootata in general are nevoie sa adune cat mai multe informatii (e.g., adresa sa IP, adresa hard a unei porti, adresa IP a unui domeniu de server, masca de adrese a subretelei) ar fi bine sa capete toata aceasta informatie intr-o singura cerere daca este posibil, decat sa faca numeroase broadcast-uri la retea. Mecanismul destinat sa booteze statia de lucru fara discuri, poate de asemenea sa incarce per-gazda fisiere specifice de configurare care contin informatia ceruta.(e.g., vezi RFC-951 [8]). Este posibil si de dorit, sa obtinem toate informatiile necesare administrarii unei gazde de la un server de boot, folosind numai un mesaj difuzat.

In cazul in care este necesar pentru o gazda sa-si gaseasca masca de adrese, ca o operatie separata urmatorul mecanism este oferit:

Pentru a oferi informatii ale mastii de adrese, protocolul ICMP [5] este extins adaugand o noua pereche de tipuri de mesaje ICMP "Cereri ale mastii de adrese" si "Raspunsuri ale mastii de adrese", asemanator cu mesajele ICMP "Informatia ceruta" si "Informatia primita". Acestea sunt descrise in detaliu in Anexa I.

Intentia folosirii acestor noi mesaje ICMP este aceea ca, atunci cand booteaza, o gazda difuzeaza un mesaj de "Cerere a mastii de adrese". O poarta (sau o gazda jucand in locul unei porti) care primeste acest mesaj, raspunde cu un "Raspuns al mastii de adrese". Daca nu exista nici un indiciu in cererea pe care gazda a trimis-o (i.e., sursa de adrese a IP-ului este zero), raspunsul este difuzat de asemenea. Gazda emitatoare va auzi raspunsul si de aici va determina masca de adrese.

Deoarece exista numai o singura valoare posibila care poate fi trimisa intr-un "raspuns al mastii de adrese" in orice retea LAN data, atunci nu va mai fi nevoie ca gazda intrebatoare sa potriveasca raspunsurile pe care le aude cu cererile pe care trimite; la fel, nu este nici o problema daca mai mult de o poarta raspunde. Presupunem ca gazdele rebooteaza rareori, asa ca difuzarea incarcata pe o retea trebuie sa fie mica.

Daca o gazda este conectata la mai mult de o retea LAN, trebuie sa gaseasca masca de adrese pentru fiecare.

O problema posibila este ce ar trebui sa faca o gazda daca nu poate gasi masca de adrese, chiar dupa un numar mare de incercari. Trei interpretari pot fi amplasate situatiei:

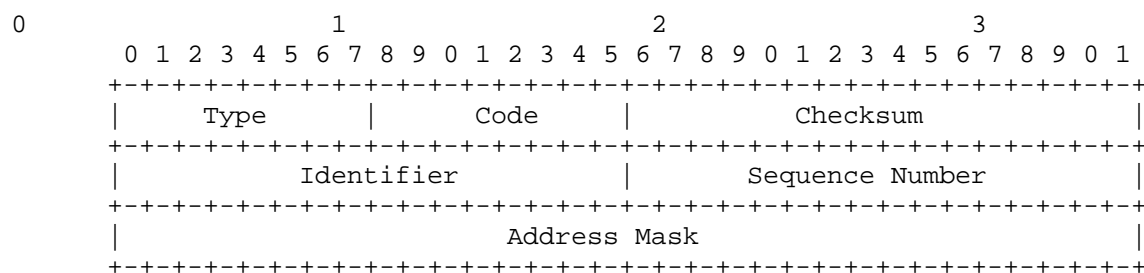
1. Reteaua locala exista in (permanenta) izolare fata de celelalte retele.
2. Subretelele nu sunt folosite, deci nici o gazda nu poate inlocui masca de adrese.
3. Toate portile din reseaua locala sunt (temporar) cazute.

Prima si a doua situatie implica ca masca de adrese este identica numarul de masca al retelei de internet. In a treia situatie, nu exista nici o posibilitate sa determini care este valoarea potrivita; cea mai sigura alegere este aceea ca masca sa fie identica cu numarul de masca al retelei de internet. Desi, aceasta s-ar putea dovedi a fi gresita mai tarziu, nu va impiedica transmisii, care altfel ar fi reusit. Este posibil pentru o gazda sa-si revina de pe urma unei alegeri proaste.: cand o gazda apare, ar trebui sa difuzeze un "Raspuns al mastii de adrese"; cand o gazda primeste un asemenea mesaj care nu este de acord cu presupunerea sa; ar trebui sa-si schimbe masca pentru a se pune in concordanta cu valoarea primita. Nici o gazda sau nici o poarta nu ar trebui sa trimita un "Raspuns al mastii de adrese" bazat pe o valoare presupusa.

In sfarsit, de notat, ca nici o gazda nu este solicitata sa foloseasca acest protocol ICMP pentru a descoperi masca de adrese; este de asteptat pentru o gazda cu memorie nevolatila sa foloseasca informatie inmagazinata (incluzand un fisier de configuratie de la un server de boot).

Anexa I. Masca de adrese ICMP

Cererea mastii de adrese sau Raspunsul mastii de adrese



Campurile IP-ului:

Adresele:

Adresa sursei intr-o cerere a mastii de adrese va fi destinatia mesajului de raspuns al mastii de adrese. Pentru a forma un mesaj de raspuns al mastii de adrese, adresa sursei a cererii devine adresa destinatiei a raspunsului, adresa sursei a raspunsului este setata la adresa destinatarului, tipul codului schimbat in AM2, valoarea mastii de adrese inregistrata in campul Mastii de Adrese si suma de control (checksum) recalculata. Oricum, daca adresa sursei in mesajul cererii este zero, atunci adresa destinatiei pentru mesajul de raspuns ar trebui sa indice o difuzare.

Campurile ICMP:

Tipul

AM1 pentru mesajul de cerere al mastii de adrese

AM2 pentru mesajul de raspuns al mastii de adrese

Codul

0 pentru mesajul de cerere al mastii de adrese

0 pentru mesajul de raspuns al mastii de adrese

Suma de control(checksum)

Suma de control este complementul celor 16-biti ai sumei complementare ai mesajului ICMP incepand cu Tipul ICMP. Pentru calcularea sumei de control, campul dumei de control ar trebui sa fie zero. Aceasta suma de control poate fi inlocuita in viitor.

Identificator

Un identificator care sa ajute in potrivirea cererilor si raspunsurilor, poate fi zero.

Sir de numere

Un sir de numere care sa ajute in potrivirea cererilor si raspunsurilor, poate fi zero.

Masca de adrese

O masca de 32-bitii.

Descriere

O poarta care primeste o cerere a mastii de adrese ar trebui sa se intoarca cu campul mastii de adrese setat la cei 32-bitii ai mastii bitilor identificand subretea si retea, pentru subretea pe care raspunsul a fost primit.

Daca gazda intrebatoare nu-si stie adresele IP, poate lasa campul sursa la zero; raspunsul ar trebui sa fie difuzare. Oricum, aceasta abordare ar trebui sa fie evitata de tot daca este posibil, de vreme ce creste inutil difuzarea incarcata in retea. Chiar si atunci cand raspunsurile sunt difuzate, de vreme ce exista o singura masca de adrese posibila pentru o subretea, nu este nevoie sa potrivim cererile cu raspunsurile. Campurile "Identificator" si "Sir de numere" pot fi ignorate.

Tipul AM1 poate fi primit de la o poarta sau o gazda.

Tipul AM2 poate fi primit de la o poarta sau o gazda jucand in locul unei porti.

Anexa II. Exemple

Aceste exemple arata cum o gazda poate gasi masca de adrese utilizand mesajele ICMP de Cerere a Mastii de Adrese si Raspuns al Mastii de Adrese. Pentru exemplele urmatoare, presupunem ca adresa 255.255.255.255. denota "broadcast la aceasta cale fizica" [6].

1. Cazul retelei de clasa A

Pentru acest caz, presupunand ca gazda emitatoare este in retea de clasa A 36.0.0.0, a adresat locatia 36.40.0.123, care este o poarta (de comunicare) la 36.40.0.62 si ca un camp al subretelei lat de 8-bitii este folosit adica, masca de adrese este 255.255.0.0.

Metoda cea mai eficienta si pe care noi o recomandam este ca un host (o gazda) sa-si descopere mai intai propria adresa (probabil utilizand "RARP" [4]) si apoi sa trimita cererea ICMP la 255.255.255.255:

Adresa sursei:	36.40.0.123
Adresa destinatiei:	255.255.255.255
Protocol:	ICMP = 1
Tip:	Cererea mastii de adrese = AM1
Cod:	0
Masca:	0

Poarta poate raspunde apoi direct gazdei emitatoare.

Adresa sursei:	36.40.0.62
Adresa destinatiei:	36.40.0.123
Protocol:	ICMP = 1
Tip:	Raspunsul mastii de adrese = AM2
Cod:	0
Masca:	255.255.0.0

Presupunand ca 36.40.0.123 este o statie de lucru fara discuri si nu-si cunoaste nici macar propriul numar de gazda. Va putea trimite urmatoarea datagrama(pachet de informatii):

```
Adresa sursei:          0.0.0.0
Adresa destinatiei:     255.255.255.255
Protocol:               ICMP = 1
Tip:                    Cererea mastii de adrese = AM1
Cod:                    0
Masca:                  0
```

36.40.0.62 va auzi datagrama(pachetul de informatii) si va trebui sa raspunda cu aceasta datagrama:

```
Adresa sursei:          36.40.0.62
Adresa destinatiei:     255.255.255.255
Protocol:               ICMP = 1
Tip:                    Raspunsul mastii de adrese = AM2
Cod:                    0
Masca:                  255.255.0.0
```

De notat ca poarta foloseste cea mai mica (ingusta) difuzare posibila pen tru a raspunde. Chiar si asa, suprasolicitarea transmisiei prezinta o incarcare care nu este necesara a tuturor gazdelor la subretea si asa folosirea adresei sursei anonime(0.0.0.0) trebuie sa fie utilizata la minim.

Daca broadcasting-ul (difuzarea) nu-i permisa presupunem ca gazdele au asimilat informatii despre portile vecine; astfel, 36.40.0.123 poate trimite aceasta datagrama (acest pachet):

```
Adresa sursei:          36.40.0.123
Adresa destinatiei:     36.40.0.62
Protocol:               ICMP = 1
Tip:                    Cererea mastii de adrese = AM1
Cod:                    0
Masca:                  0
```

36.40.0.62 ar trebui sa raspunda exact ca in cazul precedent.

```
Adresa sursei:          36.40.0.62
Adresa destinatiei:     36.40.0.123
Protocol:               ICMP = 1
Tip:                    Raspunsul mastii de adrese = AM2
Cod:                    0
Masca:                  255.255.0.0
```

2. Cazul retelei de clasa B

Pentru acest caz, presupunand ca gazda emitatoare este in reseaua de clasa B 128.99.0.0, a adresat locatia 128.99.4.123, care este o poarta (de comunicare) la 128.99.4.62 si ca un camp al subretelei lat de 6-biti este folosit adica,masca de adrese este 255.255.252.0.

Poarta trimite cererea ICMP la 255.255.255.255.

```
Adresa sursei:          128.99.4.123
```

Adresa destinatiei: 255.255.255.255
Protocol: ICMP = 1
Tip: Cererea mastii de adrese = AM1
Cod: 0
Masca: 0

Poarta poate raspunde apoi direct gazdei emitatoare.

Adresa sursei: 128.99.4.62
Adresa destinatiei: 128.99.4.123
Protocol: ICMP = 1
Tip: Raspunsul mastii de adrese = AM2
Cod: 0
Masca: 255.255.252.0

In cazul statiei de lucru fara discuri gazda trimite:

Adresa sursei: 0.0.0.0
Adresa destinatiei: 255.255.255.255
Protocol: ICMP = 1
Tip: Cererea mastii de adrese = AM1
Cod: 0
Masca: 0

128.99.4.62 va auzi pachetul si vor raspunde cu acest pachet:

Adresa sursei: 128.99.4.62
Adresa destinatiei: 255.255.255.255
Protocol: ICMP = 1
Tip: Raspunsul mastii de adrese = AM2
Cod: 0
Masca: 255.255.252.0

Daca difuzarea nu este permisa, 128.99.4.123 trimite:

Adresa sursei: 128.99.4.123
Adresa destinatiei: 128.99.4.62
Protocol: ICMP = 1
Tip: Cererea mastii de adrese = AM1
Cod: 0
Masca: 0

128.99.4.62 ar trebui sa raspunda exact ca in cazul precedent.

Adresa sursei: 128.99.4.62
Adresa destinatiei: 128.99.4.123
Protocol: ICMP = 1
Tip: Raspunsul mastii de adrese = AM2
Cod: 0
Masca: 255.255.252.0

3. Cazul retelei de clasa C(prezentandbitii subretelei necontinuu)

Pentru acest caz, presupunand ca gazda emitatoare este in retea de clasa C 192.1.127.0, a adresat locatia 192.1.127.19, care este o poarta (de comunicare) la 192.1.127.50 si ca in retea, un camp al subretelei de 3-biti este folosit (01011000), adica, masca de adrese este 255.255.255.88.

Poarta trimite cererea ICMP la 255.255.255.255:

Adresa sursei: 192.1.127.19
Adresa destinatiei: 255.255.255.255
Protocol: ICMP = 1
Tip: Cererea mastii de adrese = AM1
Cod: 0
Masca: 0

Poarta poate raspunde apoi direct gazdei emitatoare.

Adresa sursei: 192.1.127.50
Adresa destinatiei: 192.1.127.19
Protocol: ICMP = 1
Tip: Raspunsul mastii de adrese = AM2
Cod: 0
Masca: 255.255.255.88.

I In cazul statiei de lucru fara discuri gazda trimite:

Adresa sursei: 0.0.0.0
Adresa destinatiei: 255.255.255.255
Protocol: ICMP = 1
Tip: Cererea mastii de adrese = AM1
Cod: 0
Masca: 0

192.1.127.50 va auzi pachetul si vor raspunde cu acest pachet:

Adresa sursei: 192.1.127.50
Adresa destinatiei: 255.255.255.255
Protocol: ICMP = 1
Tip: Raspunsul mastii de adrese = AM2
Cod: 0
Masca: 255.255.255.88.

Daca difuzarea nu este permisa, 192.1.127.19 trimite:

Adresa sursei: 192.1.127.19
Adresa destinatiei: 192.1.127.50
Protocol: ICMP = 1
Tip: Cererea mastii de adrese = AM1
Cod: 0
Masca: 0

192.1.127.50 ar trebui sa raspunda exact ca in cazul precedent.

Adresa sursei: 192.1.127.50
Adresa destinatiei: 192.1.127.19
Protocol: ICMP = 1
Tip: Raspunsul mastii de adrese = AM2
Cod: 0
Masca: 255.255.255.88

Punte - Bridge

Un nod conectat la doua sau la mai multe subretele insesizabile administrativ dar distincte fizic, care automat trimite pachete atunci cand este necesar, dar a carui existenta nu este cunoscuta de alte gazde. De asemenea, numit un "amplificator soft".

Poarta - Gateway

Un nod conectat la doua sau la mai multe retele distincte administrativ sau/si subretele, la care gazdele trimite pachete pentru a fi expediate.

Campul gazda - Host Field

Campul bit-ului intr-o adresa de internet folosit pentru a specifica o anumita gazda (host).

Internet

Colectia de retele conectate utilizand protocolul IP.

Adresa locala - Local Address

Restul campului din adresa de internet (asa cum am definit in [3]).

Retea - Network

O singura retea de internet (care poate sau nu sa fie divizata in subretele).

Numar de retea - Network Number

Campul retelei din adresa de internet.

Subretea - Subnet

Una sau mai multe retele fizice alcatuind un subset al unei retele de internet. O subretea este identificata explicit in adresa de internet.

Campul de subretea - Subnet Field

Campul bit-ului intr-o adresa de internet specificand numarul de subrete. Bitii care formeaza acest camp nu sunt neaparat continui in adresa.

Numarul de retea - Subnet Number

Un numar care identifica o subretea in interiorul unei retele.

Anexa IV. Numere asignate

Urmatoarele asignari sunt facute pentru parametrii protocolului folosit in sustinerea subretelelor. Singurele asignari necesare sunt pentru Protocolul Mesajelor de Control Internet -Internet Control Message Protocol (ICMP) [5].

Tipurile de mesaje ICMP

AM1 = 17

AM2 = 18

Referinte

- [1] Mogul, J., "Internet Subnets", RFC-917, Stanford University, Octombrie 1984.
- [2] Postel, J., "Multi-LAN Address Resolution", RFC-925, USC/Information Sciences Institute, Octombrie 1984.
- [3] Postel, J., "Internet Protocol", RFC-791, USC/Information Sciences Institute, Septembrie 1981.
- [4] Finlayson, R., T. Mann, J. Mogul, M. Theimer, "A Reverse Address Resolution Protocol", RFC-903, Stanford University, Iulie 1984.
- [5] Postel, J., "Internet Control Message Protocol", RFC-792, USC/Information Sciences Institute, Septembrie 1981.
- [6] Mogul, J., "Broadcasting Internet Datagrams", RFC-919, Stanford University, Octombrie 1984.
- [7] GADS, "Towards an Internet Standard Scheme for Subnetting", RFC-940, Network Information Center, SRI International, Aprilie 1985.
- [8] Croft, B., and J. Gilmore, "BOOTP -- UDP Bootstrap Protocol", RFC-951, Stanford University, August 1985.
- [9] Reynolds, J., and J. Postel, "Assigned Numbers", RFC-943, USC/Information Sciences Institute, Aprilie 1985.