10.Специални IP адреси. NAT. Преобразуване на IP адреси и физически адреси – ARP. Протокол за мрежова диагностика ICMP. Динамично раздаване на IP адресиа. DHCP.

**Специални IP адреси**

В рамките на IPv4 адресното пространство има адресни сегменти, които са отделени за частно (локално) използване. RFC3330 прави "карта" на адресните сегменти за специално използване.

127.0.0.0/8 - Internet host loopback address. Пакет се зацикля вътре в хоста. И не се появява никъде в мрежата. 169.254.0.0/16 – това е "link local" блок. Хостовете получават такива адреси по “auto-configuration”, например не може да се намери DHCP сървър.

**Частни IP адреси**

Те не се маршрутизират глобално, а само локално, за локални (частни) цели. RFC3330 (първото указване е в RFC1918) указва кои от адресните ространства се използват за частни цели:

10.0.0.0/8 т.е 10.0.0.0 – 10.255.255.255 || 172.16.0.0/12 т.е 172.16.0.0 - 172.31.255.255 || 192.168.0.0/16 т.е 192.168.0.0 - 192.168. 255.255

**NAT (Network Address Translation) -** IP адреса може да се преобразува от една мрежа в друга – това е така наречения NAT – network address translation. Тази транслация се прави от специялен маршрутизатор на изхода на една локална мрежа. Той освен маршрутизация прави и транслация на адресите. От практическа гледна точка има две предимства – намалява се броя на използваните световни IP адреси. Под един адрес могат да се скрият много абонати. СЪс това скриване се прави и защита от неоторизиран достъп.

Преобразуване на мрежови адреси или Адресна транслация [[1]](http://bg.wikipedia.org/wiki/NAT#cite_note-debra-0). В областта на компютърните мрежи NAT (Network Address Translation, Native Address Translation или IP Masquerading ) е технологията, при която адресите на получателя и подателя в [IP пакета](http://bg.wikipedia.org/w/index.php?title=IP_%D0%BF%D0%B0%D0%BA%D0%B5%D1%82&action=edit&redlink=1) биват пренаписани от [маршрутизатор](http://bg.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80) или [защитна стена](http://bg.wikipedia.org/wiki/%D0%97%D0%B0%D1%89%D0%B8%D1%82%D0%BD%D0%B0_%D1%81%D1%82%D0%B5%D0%BD%D0%B0). По този начин множество хостове от частна мрежа могат да достигат до [Интернет](http://bg.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82), използвайки само един [Интернет адрес](http://bg.wikipedia.org/w/index.php?title=%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B0%D0%B4%D1%80%D0%B5%D1%81&action=edit&redlink=1)

**Статично преобразуване (static NAT):** на маршрутизатора са конфигурирани определен брой IP-адреси, които отговарят на друг определен брой адреси, използвани във вътрешната мрежа, така че между вътрешната и външната мрежи съществува ясна връзка.

**Динамично преобразуване (dynamic NAT):** на маршрутизатора са конфигурирани определен брой IP-адреси, които се вземат в употреба за вътрешните адреси според нужда, така че във вътрешната мрежа може да има най-много определен брой активни връзки към външната, но адресите на вътрешната мрежа могат да бъдат повече от този брой активни връзки.

**ARP (Address Resolution Protocol)**

За глобална адресация в Internet се използват 32-битови IP-адреси. В същото време хостовете, свързани към локална мрежа Ethernet, притежават уникални 48-битови MAC (физически) адреси. При опаковането в Ethernet кадър на IP пакет, който се отправя към крайна дестинация, например, IP адресът на хоста-получател е известен, но в полето “адрес на получателя” на Ethernet кадъра трябва да се запише Ethernet адреса на съответния хост. Иначе пакетът няма да пристигне. За целта, за установяване на съответствието между IP адреса и Ethernet адреса на хостовете в локалната мрежа се използва протокол за право преобразуване на адресите **ARP** (address resolution protocol).

**Как работи ARP**

Когато даден хост трябва да изпрати пакет (дейтаграма) към машина от локалната мрежа, чийто IP адрес е известен, но не е известен Ethernet адреса, мрежовият слой разпространява в локалната мрежа ARP пакет-заявка. Този пакет-заявка е от тип broadcast, т.е. предава се до всички машини. В полетата “Ethernet адрес на подателя” и “IP адрес на подателя” (т.е Source IP, MAC) са записани съответните адреси на хоста, който изпраща ARP заявката.

В полето “Данни” е записано ARP съобщение от вида “who is X.X.X.X tell Y.Y.Y.Y”, където X.X.X.X и Y.Y.Y.Y са IP адреси съответно на получателя и на подателя. Всички машини от локалната мрежа игнорират заявката с изключение на хоста, чийто адрес съвпада с X.X.X.X. Хост X.X.X.X изпраща ARP пакет-отговор само на подателя, тъй като вече знае неговия Ethernet адрес от получената заявка.

В полето “Данни” на пакета-отговор е записано ARP съобщение от вида “X.X.X.X is hh:hh:hh:hh:hh:hh”, където hh:hh:hh:hh:hh:hh е Ethernet адреса (в 16-ен код) на хоста, изпращащ пакета-отговор. Обикновено хоста, който изпраща ARP заявката, запомня (кешира) получените 48- битови Ethernet адреси, за да могат да се използват при следващо предаване.

При определяне на Ethernet адреса на получателя на даден пакет първо се проверява дали този адрес не е вече кеширан Ако не е, се изпраща ARP заявка. Хостът може да използва и адреси, записани в конфигурационен файл. Освен това всеки хост при първоначалното си стартиране уведомява чрез broadcast съобщение от вида “I am X.X.X.X and my Ethernet address is hh:hh:hh:hh:hh:hh”, X.X.X.X и hh:hh:hh:hh:hh:hh са съответно IP адреса и Ethernet адреса.

Всички останали хостове в локалната мрежа ще запишат тази информация в своите кешове. Чрез ARP могат да се определят физическите адреси само на хостове, които са включени в локалната мрежа и имат IP адреси от IP мрежата (подмрежата) на изпращача. Пакетите, чийто получател е хост от друга IP мрежа (подмрежа), се изпращат към маршрутизатора, включен в локалната мрежа.

 Неговият Ethernet адрес се получава чрез ARP заявка, ако не е кеширан. Този маршрутизатор избира маршрут и препраща пакета към неговия получател.

**Proxy ARP**

**Proxy ARP** е метод, чрез който хост отговаря на ARP заявки за IP адреси, които не са конфигурирани на интерфейса му. “Проксирането” на ARP заявки за сметка на друг хост препраща целия LAN, предназначен за този хост, към прокси. Прихванатият трафик се “превключва” към другия интерфейс на проксито (обикновено маршрутизатор) или се препраща през серийна връзка (напр., dialup или VPN тунел), за да достигне хоста получател.

**RARP**

**RARP** (Reverse Address Resolution Protocol) е протокол за намиране на IP адреси по Ethernet адреси. Обикновено IP адресът на хоста е записан в конфигурационен файл, който се намира на твърдия диск на машината. При първоначално зареждане на операционната система файлът се прочита от твърдия диск и хостът научава своя IP адрес.

В случай, че в локалната мрежа е включена машина, която не притежава собствен твърд диск (diskless), за определяне на нейният IP адрес се използва RARP протоколът. За целта в мрежата трябва да е включен хост, който функционира като RARP сървър. Този сървър съхранява съответствието между Ethernet и IP адреси на станциите в мрежата.

Действието на RARP се основава на наличието на уникален физически Ethernet адрес на всяка система в локалната мрежа При инициализиране на diskless машината RARP протоколът прочита този адрес от интерфейсната карта и предава до всички станции в мрежата пакет-заявка. RARP сървърът отговаря на тази заявка, като в пакета-отговор се съдържа IP адреса, съответстващ на изпратения Ethernet адрес.

**DHCP -** се изпълнява за разпределяне на IP адреси при компютри в които няма статичен такъв. Единия начин за едно устройство да се определи IP адрес е той ръчно да се въведе, заедно със subnet mask и адрес на рутера. Ако не е хубаво този компютър да е със статично IP , то тогава се изпълнява DHCP протокола. За да работи това трябва да има DHCP сървър в конфигурация с него. Има пространство от динамични адреси, които той може да им раздава в определен срок. На този сървър трябва да се каже диапазона, който се раздава за статични IP адреси. Трябва да има DHCP агент, който знае къде е DHCP сървъра. Може да има повече от един DHCP сървър в конфигурацията.

Dynamic Host Configuration Protocol (DHCP) се използва за автоматично (динамично) конфигуриране на свързаността на даден хост към IP мрежата. За разлика от твърдото (ръчно или статично) конфигуриране. DHCP “раздава” не само IP адреси, но и всички други параметри на връзката – Default Gateway (изхода навън по подразбиране, DNS сървър/и, име на домейн и т.н.) DHCP улеснява процеса на добавяне на машина в мрежата, местене и т.н.

Днешната версия на DHCP за IPv4 е стандартизирана в RFC 2131 (1997 г.). DHCP за IPv6 (DHCPv6) е дефинирана в RFC 3315. DHCP е протокол от типа клиент-сървър. DHCP-конфигуриран клиент веднага след включването се свързва към мрежата и изпраща broadcast заявка, искайки необходимата информация от DHCP сървър.

DHCP сървърът разполага с пул от IP адреси и необходимата информация за конфигуриране на клиента: GW, SM, домейн, DNS сървър/и, NTP, WINS и др. При получаване на валидна заявка сървърът присвоява IP адрес, време за отдаване на aдреса (lease time – през което алокацията е валидна) и др. (гореспоменати) IP конфиг. параметри.

**Раздаване на IP адреси (allocation)**

DHCP сървърите раздават (алокират) IP адреси по 3 начина:

***Динамична алокация***: Обхват от IP адреси се дават за DHCP и всеки клиент си заявява IP адрес от DHCP сървъра при включване. Времето на отдаване (lease) е дефинирано, така че сървърът може да преотдаде адреса на друга машина.

***Автоматична алокация***: Подобн е на динамичната, но даден IP адрес е резервиран за даден клиент.

***Статична алокация***: DHCP раздава IP адреси на базата на таблица MAC адрес/IP адрес, ръчно попълнена от администратора. Само клиенти, чиито MAC адреси присъстват в тази таблица, ще получат IP адреси. Нарича се още *Static DHCP Assignment* (от DD- WRT, Linux-базиран фърмуер, Linksys), *fixed-address* (от dhcpd), *DHCP reservation* или *Static DHCP* (от Cisco/Linksys) или *IP reservation*, *MAC/IP binding* (други производитевли).

**ICMP**

**Internet Control Message Protocol** (**ICMP**) е част от протокола IP. Използва се от мрежовите ОС главно за откриване на грешки по мрежата и изпращане на съобщения за това. ICMP за IPv4 е известени като ICMPv4. IPv6 има подобен, ICMPv6. Дефиниран е в RFC 792. IP опакова ICMP съобщението с нов IP хедър, за а го върне на изпращача и го предава като обикновен пакет.

Например, всеки възел в мрежата (рутер, GW), която направлява IP пакета, трябва да декрементира TTL полето на IP хедъра с 1. Ако TTL достигне 0, ICMP съобщение Time to live exceeded in transit message се изпраща към източника. ICMP съобщенията се съдържат в стандартни IP пакети, но се обработват като специални случаи. Много мрежови средства за диагностика се базират на ICMP.

Командата traceroute изпраща UDP дейтаграми с определени IP TTL полета и очаква ICMP Time to live exceeded in transit, също изпраща "Destination unreachable" в отговор. Средството ping се реализира с ICMP "Echo request" и "Echo reply" съобщения.

**ping**

 Ping е инструмент за тестване на достижимостта на даден хост по IP мрежата. Изпраща ICMP “echo request” пакети към целта и очаква ICMP “echo response” отговори. Ping измерва round-trip time и регистрира загуби на пакети. Накрая разпечатва статистика: минималното, средното, максималното и (в някои версии) стандартното отклонение от round trip time. Mike Muuss е написал програмата през декември, 1983. Нарекъл я на звуковите импулси, издавани от локатор в подводница.

**traceroute**

**traceroute** е инструмент за определяне на маршрута на пакетите по мрежата. За IPv6 вариантът е **traceroute6**. traceroute го има за всички Unix-подобни ОС. Подобна функционалност имат **tracepath** на модерните Linux дистрибуции и **tracert** в Microsoft Windows. Traceroute инкрементира с 1 "time-to-live" (TTL) на всяка следваща “тройка” от изпратени пакети. Първата тройка е с TTL=1. Следващата е с TTL = 2 и т.н. Минавайки през хост, TTL на пакета се декрементира с 1 и се отправя към следващия хост. Хостът изхвърля пристигнал пакет с TTL = 1 и изпраща на подателя ICMP t ime exceeded (type 11). traceroute използва тези връщани пакети, за да създаде списък от хостове, през които пакетът е минал по маршрута до дестинацията.

Трите timestamp за всеки хост по пътя са закъснението - delay (latency) в ms за всеки пакет от тройката. Ако пакетът не се върне в рамките на очаквания timeout, разпечатва се звездичка (asterisk). Traceroute може и да не изброи реалните хостове. Само показва, че първият хост е на един хоп, вторият – на два, и т.н. Просто IP не гарантира, че всички пакети ще минат по един и същ път. Ако хост на хоп N не отговори, този хоп ще бъде пропуснат в разпечатката.

В съвременните Unix и Linux-базирани ОС traceroute използва по подразбиране UDP дейтаграми с номера на дестинационни портове 33434 - 33534. Но има опция да се използва ICMP echo request (type 8) както в Windows tracert.

**arping**

**arping** е подобна на ping, но използва ARP вместо ICMP. Затова, arping е използваема само в локалната мрежа В някои случаи отговорът може да идва от междинна система - proxy ARP (напр. рутер).