**netstat** (**net**work **stat**istics) is a [command-line](http://en.wikipedia.org/wiki/Command_line_interface) [tool](http://en.wikipedia.org/wiki/Computer_software) that displays [network connections](http://en.wikipedia.org/wiki/Transmission_Control_Protocol) (both incoming and outgoing), routing tables, and a number of network interface statistics. It is available on [Unix](http://en.wikipedia.org/wiki/Unix), [Unix-like](http://en.wikipedia.org/wiki/Unix-like), and [Windows NT](http://en.wikipedia.org/wiki/Windows_NT)-based [operating systems](http://en.wikipedia.org/wiki/Operating_systems). **Netstat –** показва информация за мрежовите сесии(активни връзки) на съответния компютър.Сесията е от порта на един хост до порта на друг хост.За диагностика на IP,ICMP,TCP,UDP It is used for finding problems in the network and to determine the amount of traffic on the network as a performance measurement.

**iproute2** is a collection of utilities for controlling [TCP](http://en.wikipedia.org/wiki/Transmission_Control_Protocol) and [UDP](http://en.wikipedia.org/wiki/User_Datagram_Protocol) [IP](http://en.wikipedia.org/wiki/Internet_Protocol) networking and [traffic control](http://en.wikipedia.org/wiki/Network_traffic_control) in [Linux](http://en.wikipedia.org/wiki/Linux), in both [IPv4](http://en.wikipedia.org/wiki/IPv4) and [IPv6](http://en.wikipedia.org/wiki/IPv6) networks. iproute2 is intended to replace[[1]](http://en.wikipedia.org/wiki/Iproute2#cite_note-0) an entire suite of legacy Unix networking tools (often called “net-tools*”)*

|  |  |  |
| --- | --- | --- |
| **purpose** | **legacy "net-tools"** | **iproute2** |
| Address and link configuration | [ifconfig](http://en.wikipedia.org/wiki/Ifconfig) | ip addr, ip link |
| Routing tables | route | ip route |
| Neighbors | arp | ip neigh |
| Tunnels | iptunnel | ip tunnel |
| Multicast | ipmaddr | ip maddr |
| Statistics | [netstat](http://en.wikipedia.org/wiki/Netstat) | ss |

**iptables** is a [user space](http://en.wikipedia.org/wiki/User_space) application program that allows a [system administrator](http://en.wikipedia.org/wiki/System_administrator) to configure the tables provided by the [Linux kernel](http://en.wikipedia.org/wiki/Linux_kernel) [firewall](http://en.wikipedia.org/wiki/Firewall_%28computing%29)(implemented as different [Netfilter](http://en.wikipedia.org/wiki/Netfilter) modules) and the chains and rules it stores. Different kernel modules and programs are currently used for different protocols; *iptables* applies to IPv4, *ip6tables* to IPv6, *arptables* to ARP, and *ebtables* as a special for Ethernet frames.

**Longest prefix match**

Пример: **192.168.20.16/28 ; 192.168.0.0/16**

When the address 192.168.20.19 needs to be looked up, both entries in the routing table "match". That is, both entries contain the looked up address. In this case, the longest prefix of the candidate routes is 192.168.20.16/28, since its [subnet mask](http://en.wikipedia.org/wiki/Subnet_mask) (/28) is higher than the other entry's mask (/16), making the route more specific.

**ifconfig** (short for **i**nter**f**ace **config**uration) is a system administration utility in [Unix-like](http://en.wikipedia.org/wiki/Unix-like) operating systems to configure, control, and query [TCP/IP](http://en.wikipedia.org/wiki/TCP/IP) [network interface](http://en.wikipedia.org/wiki/Network_card) parameters. Common uses for ifconfig include setting an interface's [IP address](http://en.wikipedia.org/wiki/IP_address) and [netmask](http://en.wikipedia.org/wiki/Netmask), and disabling or enabling a given interface.

**Arp(program)**manipulates the kernel's ARP cache in various ways. The primary options are clearing an address mapping entry and manually setting up one. For debugging purposes, the arpprogram also allows a complete dump of the ARP cache. **ARP-**използва се за визуализация и модификация на таблицата IP-към MAC адрес. **ARP** протоколът извършва съпоставяне м/у IP и MAC адреси.

**Rarpd(program)** is a daemon which responds to RARP requests. RARP is used by some machines at boot time to discover their IP address. They provide their Ethernet address and**rarpd** responds with their IP address if it finds it in the ethers database (either */etc/ethers* file or NIS+ lookup) and using DNS lookup if ethers database contains a hostname and not an IP address.

**RIPv1** работи с броадкаст съобщения, прилага само classful маршрутизация. Т.е периодичните updates не носят subnet информация. Не е възможно да имаме подмрежи от един и същи клас с различни маски. С други думи, всички подмрежи от даден клас трябва да бъдат с еднакви маски.

**RIPv2** има възможност да носи subnet информация, да поддържа CIDR. За поддържане на обратна съвместимост с версия 1 запазено е ограничението от 15 хопа. За сигурност е въведена аутентикация с явен текст, подобрена с MD5 (RFC 2082). За да не се товарят хостове, които не са участници в RIP, RIPv2 “мултикаства” обновленията на адрес 224.0.0.9, за разлика от RIPv1, който е broadcast.

**AUTONOMOUS SYSTEM:** On the Internet, an autonomous system (AS) is the unit of [router](http://searchnetworking.techtarget.com/sDefinition/0%2C%2Csid7_gci212924%2C00.html)policy, either a single network or a group of [network](http://searchnetworking.techtarget.com/sDefinition/0%2C%2Csid7_gci212644%2C00.html)s that is controlled by a common network administrator (or group of administrators) on behalf of a single administrative entity (such as a university, a business enterprise, or a business division).. An autonomous system is assigned a globally unique number - Autonomous System Number (ASN).

**Разлика RIPv1(broadcast) и RIPv2(multicast)** – RIPv1 не поддържа subnet маски.

**Routing table:** A routing table is a set of rules, often viewed in table format, that is used to determine where data [packet](http://whatis.techtarget.com/definition/0%2C289893%2Csid9_gci212736%2C00.html)s traveling over an [Internet Protocol](http://whatis.techtarget.com/definition/0%2C289893%2Csid9_gci214031%2C00.html) (IP) network will be directed. All IP-enabled devices, including [router](http://whatis.techtarget.com/definition/0%2C289893%2Csid9_gci212924%2C00.html)s and [switch](http://whatis.techtarget.com/definition/0%2C289893%2Csid9_gci213079%2C00.html)es, use routing tables

**хлъзгащия се прозорец**Те са по-ефективни от протокола спри и чакай, тъй като позволяват изпращане на повече от един кадър, преди да се чака за потвърждение. При тези протоколи всеки кадър се номерира с число от 0 до някакъв максимум, обикновено от вида 2^*n* - 1, така че номерът да се вмества точно в *n* бита.

The **maximum segment size** (**MSS**) is a parameter of the [TCP protocol](http://en.wikipedia.org/wiki/Transmission_Control_Protocol) that specifies the largest amount of data, specified in [bytes](http://en.wikipedia.org/wiki/Byte), that a computer or communications device can receive in a single, [unfragmented](http://en.wikipedia.org/wiki/IP_fragmentation) piece. It does not count the TCP header or the [IP](http://en.wikipedia.org/wiki/Internet_Protocol) header[[1]](http://en.wikipedia.org/wiki/Maximum_segment_size#cite_note-0). For optimum [communications](http://en.wikipedia.org/wiki/Information_transfer), the number of bytes in the data segment and the headers must not add up to more than the number of bytes in the [maximum transmission unit](http://en.wikipedia.org/wiki/Maximum_transmission_unit) (MTU).

**MSS –(**Maximum Segment Size) е опция на ТСР протокола,която определя най-голямото количество данни(в байтове) което компютър или комуникационно у-во може да получи в единичен,нефрагментиран сегмент.Всеки хост трябва да може да приема минимум 536 байта сегмент.

**MTU** (Maximum Transmission Unit) – В компютърните мрежи MTU в протокол на даден слой е размера(в байтове) на най-големия протоколен блок за данни(PDU),който може да понесе дадения слой.По-голям MTU означава по-голяма ефективност.

The **MTU (Maximum Transmission Unit) is** the size of the largest datagram that can be sent over a network.If a datagram is larger than an MTU, the datagram must be [fragmented](http://www.google.com/url?q=http%3A%2F%2Fwww.topbits.com%2Fpacket-fragmentation.html&sa=D&sntz=1&usg=AFQjCNG7CFso4guSzaPtm_4i3PVS6p6wfQ) into multiple smaller datagrams.

**OSPF** – OSPF e динамичен протокол за маршрутизация.Той е протокол със следене на на състоянието на връзката.Попада в протоколите за вътрешна маршрутизация.Приложим в големи корпоративно мрежи.Разпознава промени в мрежата.При отпадане примерно на възел за секунди се конвергира в нова топология без зацикляне.

**TCP** – Основен протокол на транспортния слой в TCP/IP модела.Той предоставя надеждно обслужване с установена връзка (connection oriented).Той внася допълнително закъснение заради спазване на реда за подаване на единиците с данни(сегментите) и функциите по надеждност.ТСР се ползва от най-популярните интернет приложения: FTP, E-mail,WWW. Не е подходящ за доставяне на съобщения в реално време.Всеки ТСР сегмент има 20 байта служебна информация.

**UDP** – Оснвен протокол на транспортния слой в TCP/IP модела.Той е по-опростен протокол с неустановена връзка(connectionless) и сесии не се установяват. Той е по-скоро транзакционен протокол тоест ако приложението има данни за предаване той ги предава.При изпращане на много дейтаграми те могат да поемат по различни пътища в мрежата и да пристигнат в различен ред.UDP не следи последователността на дейтаграмите при приемане като ТСР. Подходящ за доставяне на съобщения в реално време. UDP дейтаграмите са само 8 байта.

**BGP** –Основният протокол за маршрутизация в INTERNET. Поддържа таблица от IP мрежи(prefix), които определеят достижимостта на мрежите между автономните системи.Той е протокол с вектор на пътищата(path vector protocol) BGP не използва метрика на вътрешните протоколи,а взема решения за определяне на маршрути на база на пътя м/у ASs, мрежова политика и/или множество правила.

**IP(Internet Protocol) –** протокол за комуникация,стоящ в основата на Интернет.Задачата му е да извърши успешно предаване на пакети от източника до получателя,без значение дали те са в една и съща мрежа или не.IP се използва от транспортни протоколи като TCP и UDP

**Команди:**

**Ping**- служи за проверка на мрежовата свързаност, тестване на връзката с другите компютри.Използва протокола ICMP. Визуализира се времето за изпращане и получаване на пакет.

**IPCONFIG**- предоставя информация за ТCP/IP конфигурацията на всички мрежови карти, включени към компютъра.(В LINUX e ifpconfig)

**Nbtstat**-предоставя информация за имената на компютрите и групите известни на даден компютър

**Tracert**-проследява маршрута през мрежата до компютъра-местоназначение по даден IP адрес или име(Linux traceroute)

**RARP (Reverse)** превръща от MAC към IP

**RTT(Round Trip Time) –**времето на пакет да стигне от клиента до сървъра и обратно.Колкото е по-малка е стойността на RTT толкова мрежата е по-добра и по-бърза.

**На** **приложно ниво всеки процес се определя еднозначно от** **сокета** (IP адрес+номер на порт) ,а всяко съединение с двойка сокети.

**Анализатор на протоколи(функция)-**Програма или устройство чиято цел е да разбере съдържанието на капсулираната от протокола информация.

**Какво връща ARP** заявката: Връща МАС адреса.

**ROUTE**  С командата Route са възможни следните операции:да се добавят нови маршрути,да се трие запис на шлюз,да се изведе списък на съществуващи маршрути.

**Дейтаграмните** протоколи са UDP и IP.За тях е характерно че не установяват съсединение(connectionless)