Сеть в UNIX

Кулябов Д. С.

Российский университет дружбы народов

Содержание

Введение в сети

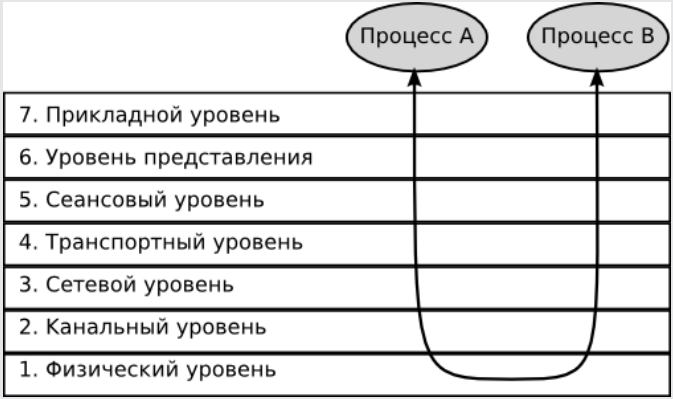
- Сети стали неотъемлемой составляющей современных вычислительных систем.
- Операционная система UNIX почти с самого рождения интегрировала в себя технологии организации локальных сетей, на её основе затем была построена сеть Internet, распространившаяся ныне по всему миру.
- Сеть объединяет разное оборудование, различные операционные системы и программы — их успешное взаимодействие было бы невозможно без принятия общепринятых правил, стандартов.
- В области компьютерных сетей существует множество международных и промышленных стандартов, среди которых следует особенно выделить международный стандарт OSI и набор стандартов IETF (Internet Engineering Task Force).

Протоколы

Протоколы

Семиуровневая модель OSI

Уровни ISO OSI



Протоколы

Протоколы Internet: TCP/IP

Соответствие стека TCP/IP модели OSI

OSI	TCP/IP
7. Прикладной уровень	WWW, SMTP, POP, SSH, ...
6. Уровень представления	
5. Сеансовый уровень	
4. Транспортный уровень	TCP, UDP
3. Сетевой уровень	IP
2. Канальный уровень	Ethernet, FDDI, PPP, ...
1. Физический уровень	UTP, радиоканалы

Сетевой интерфейс в UNIX

Сетевой интерфейс — это абстракция, связывающая канальный и сетевой (протокол TCP/IP) уровни сети в UNIX.

Интерфейс характеризуется следующими параметрами:

- уникальное имя, состоящее из типа устройства и номера (0 или больше для однотипных устройств).
- набор параметров, большая часть которых относятся к сетевому уровню (IP-адрес, маска сети и т. п.).
- аппаратный адрес (в случае Ethernet аппаратный адрес называется MAC-адрес и состоит из шести байтов, которые принято записывать в шестнадцатеричной системе счисления и разделять двоеточиями).

- Основной утилитой для просмотра и управления параметрами сетевых интерфейсов в UNIX служит ifconfig.
- В настоящее время в ряде систем наряду с ней используется более современная утилита ip.

Просмотр параметров сетевых интерфейсов (ifconfig)

```
desktop ~ # ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0D:60:8D:42:AA
          inet addr:192.168.1.5  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6160 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5327 errors:0 dropped:0 overruns:0 carrier:0
          collisions:1006 txqueuelen:1000
          RX bytes:3500059 (3.3 Mb)  TX bytes:2901625 (2.7 Mb)
          Base address:0x8000 Memory:c0220000-c0240000
desktop ~ # ifconfig lo
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:188 errors:0 dropped:0 overruns:0 frame:0
          TX packets:188 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:14636 (14.2 Kb)  TX bytes:14636 (14.2 Kb)
```

Конфигурация IP-сетей

Конфигурация IP-сетей

Сетевой адрес

Сетевой адрес I

- В IP-сетях каждому сетевому интерфейсу присваивается некоторый единственный на всю глобальную сеть адрес, который не зависит от среды передачи данных и всегда имеет один и тот же формат.
- Формат адреса зависит от версии протокола.
- В четвёртой версии протокола IP адрес состоит из четырёх байт, записываемых традиционно в десятичной системе счисления и разделяемых точкой.
- В шестой версии протокола IP адрес состоит уже из 16 байт и обычно записывается в шестнадцатиричной системе счисления.
- IP-адрес сетевого интерфейса eth0 из приведённого выше примера — 192.168.1.5.

Сетевой адрес II

- Второй сетевой интерфейс из примера — lo — заглушка (loopback), которая используется для организации сетевых взаимодействий компьютера с самим собой: любой посланный в заглушку пакет немедленно обрабатывается как принятый оттуда. Заглушке обычно назначается адрес 127.0.0.1.

Конфигурация IP-сетей

Маршрутизация

Маршрутизация I

- IP-адрес включает две части: адрес подсети и адрес конкретного узла в рамках этой подсети.
- Маска подсети показывает, сколько бит в IP-адресе содержат адрес подсети (остальные — это адрес узла).
- Располагая IP-адресом узла назначения и маской подсети всегда позволяет определить, относится ли узел назначения к той же подсети.
- В этом случае пакеты к ним будет доставляться напрямую через канальный уровень.
- Если IP-адрес узла-адресата не входит в локальную сеть узла-отправителя, необходимо отослать какому-то абоненту локальной сети, с тем, чтобы тот перенаправил его дальше.
- Этот абонент, маршрутизатор, подключен к нескольким сетям, и ему вменяется в обязанность пересылать пакеты между ними по определённым правилам.

Таблицу, управляющую маршрутизацией пакетов, можно просмотреть с помощью утилиты netstat -r или route.

Вывод таблицы маршрутизации (route)

```
desktop ~ # route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 eth0
```

Конфигурация IP-сетей

Служебный протокол ICMP

Протокол ICMP

Служебный протокол ICMP (Internet Control Message Protocol), предназначенный для передачи служебных сообщений:

- сообщений об ошибках соединений
- сообщений об состоянии соединений
- сообщений об изменении маршрутов
- сообщений о фрагментации пакетов

Пример выполнения команды traceroute

```
desktop ~ # traceroute ya.ru
traceroute to ya.ru (213.180.204.8), 64 hops max, 40 byte packets
 1  195.91.230.65 (195.91.230.65)  0.890 ms  1.907 ms  0.809 ms
 2  cs7206.rinet.ru (195.54.192.28)  0.895 ms  0.769 ms  0.605 ms
 3  ix2-m9.yandex.net (193.232.244.93)  1.855 ms  1.519 ms  2.95 ms
 4  c3-vlan4.yandex.net (213.180.210.146)  3.412 ms  2.698 ms  2.654 ms
 5  ya.ru (213.180.204.8)  2.336 ms  2.612 ms  3.482 ms
```

Конфигурация IP-сетей

Информация о соединениях

Информация о соединениях I

- Основных транспортных протоколов в TCP/IP два — это TCP (Transmission Control Protocol, протокол управления соединением) и UDP (User Datagram Protocol).
- TCP заботится о том, чтобы передаваемые данные дошли до адресата в целости и сохранности. Для этого предпринимаются следующие действия:
  - установление соеднинения;
  - обработка подтверждения корректной доставки;
  - отслеживание состояния абонентов.

Для просмотра всех существующих в настоящий момент сетевых соединений можно воспользоваться командой **netstat**.

Пример выполнения команды netstat

```
desktop ~ # netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:32769           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:32770           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 192.168.11.5:34949      83.149.196.70:5223      ESTABLISHED
tcp        0      0 192.168.11.5:39833      213.248.55.180:5223     ESTABLISHED
tcp        0      0 192.168.11.5:59577      192.168.11.1:22         TIME_WAIT
udp        0      0 0.0.0.0:32768           0.0.0.0:*
udp        0      0 0.0.0.0:32769           0.0.0.0:*
udp        0      0 0.0.0.0:111             0.0.0.0:*
```

Службы Internet

Службы Internet

Служба доменных имён

- Когда-то имена всех компьютеров в сети, соответствующие IP-адресам, хранились в файле /etc/hosts.
- DNS (Domain Name Service, служба доменных имен). Она имеет иерархическую структуру. Если за какую-то группу абонентов домена отвечают не хозяева домена, а кто-то другой, ему выделяется поддомен (или домен второго уровня), и он сам распоряжается именами вида «имя_компьютера.поддомен.домен». Таким образом, получается нечто вроде распределенной сетевой базы данных, хранящей короткие записи о соответствии доменных имен IP-адресам.
- В самом простом случае для того, чтобы сказать системе, какой сервер доменных имён использовать, необходимо изменить файл /etc/resolv.conf. В более сложных системах можно установить и настроить собственный сервер доменных имён.

Службы Internet

Удалённый терминал

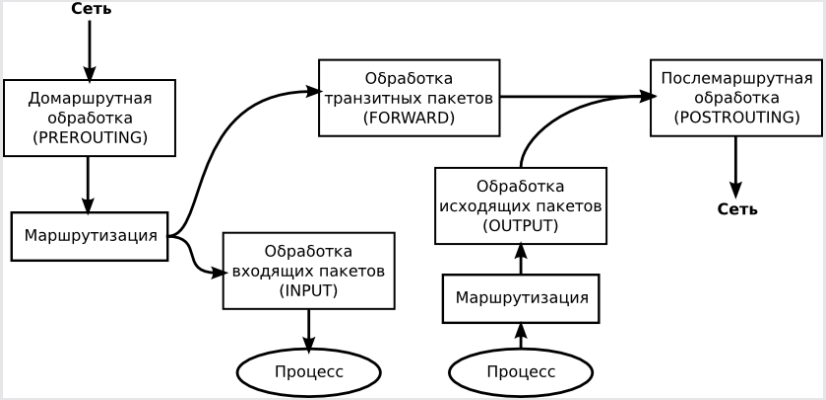
- Telnet — стандартное приложение, которое присутствует практически в каждой реализации TCP/IP.
- Оно может быть использовано для связи между узлами, работающими под управлением различных операционных систем.
- Клиент telnet взаимодействует и с пользователем, находящимся за терминалом, и с протоколами TCP/IP.
- Сервер telnet обычно взаимодействует с так называемыми псевдотерминальными устройствами в UNIX системах.
- Программа telnet обладает значительным недостатком — вся передаваемая информация (в том числе аутентификация пользователей) пересылается открытым текстом.

- В настоящее время для удалённого администрирования серверов в Internet повсеместно применяется ssh.

Межсетевой экран

Механизм анализа сетевых и транспортных пакетов, позволяющий избавляться от нежелательной сетевой активности, манипулировать потоками данных и даже преобразовывать служебную информацию в них.

Обработка пакета в iptables



Резюме

Резюме I

- Сеть состоит из различных аппаратно-программных узлов, для объединения которых используются стандартные протоколы. Эталонной моделью взаимодействия таких систем является семиуровневая модель OSI.
- Протокол TCP/IP частично реализует уровни OSI. Основные протоколы IP (сетевого уровня) и TCP (транспортного уровня) позволили объединить разрозненные локальные сети в глобальную сеть Internet.
- В UNIX основной сетевого взаимодействия является интерфейс, который находится между канальным и сетевым уровнем. Конфигурация TCP/IP включает в себя настройку интерфейса, маршрутизации и сервисов Internet, в первую очередь сервера доменных имен.

- Для удаленного управления компьютерами используется программа telnet и её современных защищённый аналог — ssh.
- Важным элементом сетевой инфраструктуры является межсетевой экран, который позволяет ограничить сетевой трафик и изменить его свойства. На лекции был рассмотрен межсетевой экран Linux — iptables.

Дополнительные материалы

Дополнительные материалы

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. — СПб.: Питер, 2002. — 672 с.: ил.
2. Курячий Г.В., Маслинский К.А. Операционная система Linux. — М.: Интуит.Ру, 2005. — 392 с.: ил.

Вопросы для самоконтроля

Вопросы для самоконтроля

1. Какие уровни входят в модель ISO OSI? Какие можно провести аналогии с реально существующими протоколами?
2. Что такое сетевой интерфейс в UNIX? Для чего он используется и каким образом настраивается?
3. Как управлять IP-маршрутизацией в UNIX?
4. Что такое служба доменных имён в UNIX? Как она конфигурируется?
5. Какие функции выполняет межсетевой экран? Каковы принципы управления межсетевым экраном iptables?