



OTUS

ОНЛАЙН-ОБРАЗОВАНИЕ

Онлайн-образование

Не забыть включить запись!





Меня хорошо видно && слышно?

Ставьте , если все хорошо
Напишите в чат, если есть проблемы

СЕТЕВАЯ ПОДСИСТЕМА LINUX



Казанцев Анатолий

преподаватель

+7 (499) 110-61-65

Правила вебинара



Активно участвуем



Задаем вопрос в чат или ГОЛОСОМ



Off-topic обсуждаем в Slack `#general` или `#pentest-2019-09`



Вопросы вижу в чате, могу ответить не сразу

Маршрут вебинара

Основные понятия



Устройство сетевого стека.
Состав сетевого API



Атака с помощью Ettercap



Рефлексия

Цели вебинара

1

Рассмотреть архитектуру сетевой подсистемы ОС Linux

2

Научиться получать информацию
о состоянии сетевой подсистемы

3

Провести практическую атаку на канальный уровень

The image features a central horizontal band with a blue-to-purple gradient. This band is overlaid with a white network diagram consisting of interconnected nodes and lines. The background of the entire image is an aerial view of a city skyline, with buildings rendered in a monochromatic blue color. The text 'СЕТЕВАЯ ПОДСИСТЕМА' is centered within the blue band in a bold, white, sans-serif font.

СЕТЕВАЯ ПОДСИСТЕМА

ОСНОВНЫЕ ПОНЯТИЯ

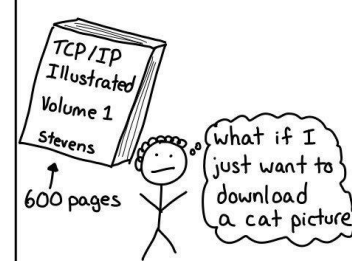
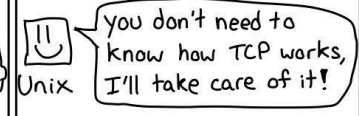
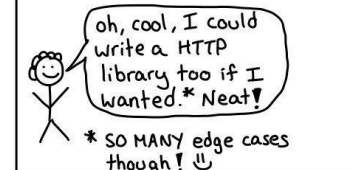
Сокет (socket) - объект, который используется операционной системой для предоставления доступа между приложениями локально или по сети.

<https://github.com/torvalds/linux/blob/master/net/socket.c>

JULIA EVANS
@b0rk

sockets

drawings.jvns.ca

<p>networking protocols are complicated</p> 	<p>Unix systems have an API called the "socket API" that makes it easier to make network connections (Windows too! 🙄)</p> 	<p>here's what getting a cat picture with the socket API looks like:</p> <ol style="list-style-type: none">1 Create a socket <code>fd = socket(AF_INET, SOCK_STREAM, ...)</code>2 Connect to an IP/port <code>connect(fd, 12.13.14.15:80)</code>3 Make a request <code>write(fd, "GET /cat.png HTTP/1.1")</code>4 Read the response <code>cat_picture = read(fd, ...)</code>
<p>Every HTTP library uses sockets under the hood</p> <p><code>\$ curl awesome.com</code> → sockets Python: <code>requests.get("yay.us")</code></p> 	<p>AF_INET? What's that?</p> <p>AF_INET means basically "internet socket": it lets you connect to other computers on the internet using their IP address.</p> <p>The main alternative is AF_UNIX ("unix domain socket") for connecting to programs on the same computer</p>	<p>3 kinds of internet (AF_INET) sockets:</p> <p>SOCK_STREAM = TCP ↑ curl uses this</p> <p>SOCK_DGRAM = UDP ↑ dig (DNS) uses this</p> <p>SOCK_RAW = just let me send IP packets ↑ ping uses this I will implement my own protocol</p>

ОСНОВНЫЕ ПОНЯТИЯ

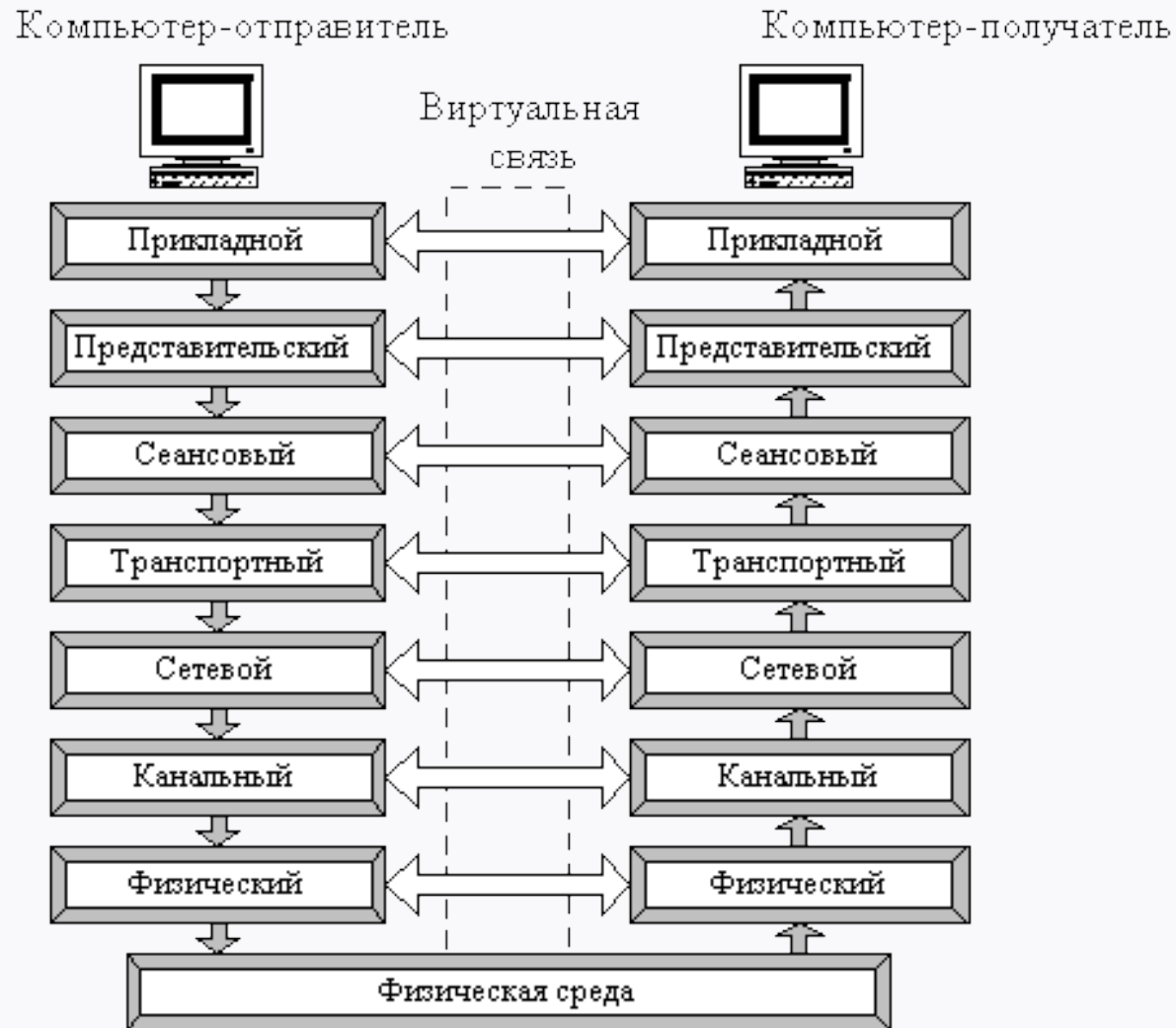
Типы сокетов:

- потоковые (stream),
- дейтаграммные (datagrams, messages),
- «сырые» (raw).

<http://man7.org/linux/man-pages/man2/socket.2.html>

<http://man7.org/linux/man-pages/man7/socket.7.html>

Теоретическая модель OSI



Теоретическая модель OSI

the "OSI model" for networking

JULIA EVANS
@b0rk



I don't always find it useful but it's good to know what "layer 4" means



what does "this is an L4 proxy" mean?

LAYERS

- 1: electrical engineering stuff, wires, frequencies, wifi
- 2: Ethernet protocol + others
- 3: IP (IP addresses)
- 4: TCP + UDP (ports)
- 5+6: nobody ever talks about these
- 7: HTTP and friends

If a load balancer is labelled "L7" it usually means it looks at the Host: header inside your HTTP packets.

layer 3
networking
tool

↑
ignores layer
4 and above

I only know about IP addresses! I don't even know what a port is let alone what the packet says

OSI 7 vs. TCP/IP

Прикладной уровень	Прикладной уровень
Представительский уровень	
Сеансовый уровень	
Транспортный уровень	Транспортный уровень
Сетевой уровень	Сетевой уровень
Канальный уровень	Уровень доступа к сети
Физический уровень	

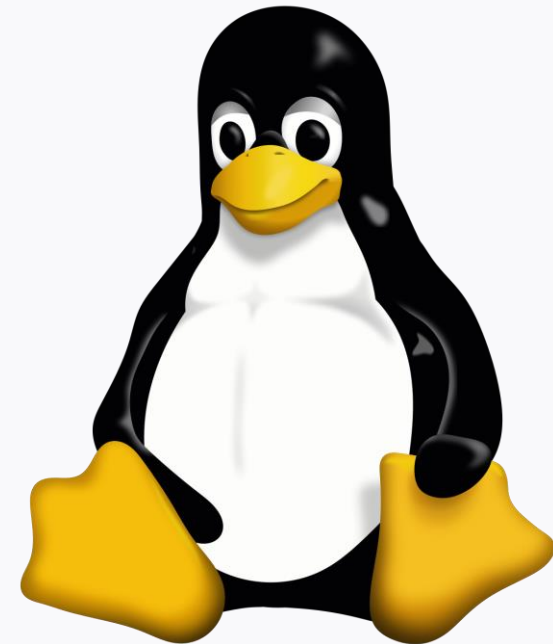
Сетевой стек Linux



Функциональность

Сетевая подсистема Linux обеспечивает следующую функциональность:

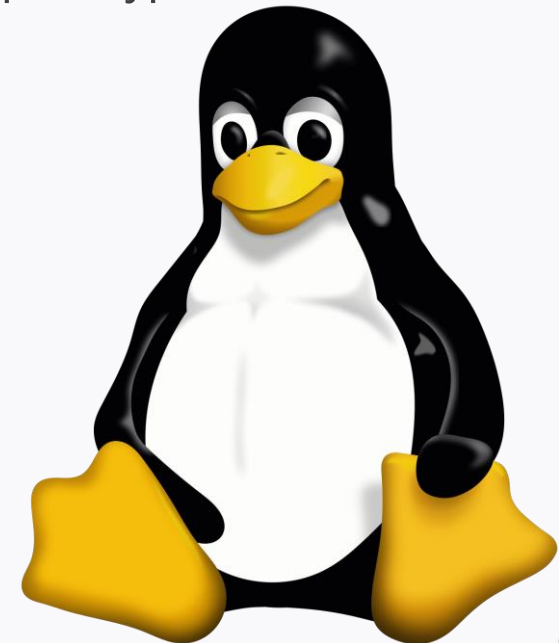
- абстракция сокетов,
- стеки сетевых протоколов (TCP/IP, UDP/IP, IPX/SPX, AppleTalk и мн. др.),
- маршрутизация (routing),
- пакетный фильтр (модуль Netfilter),
- абстракция сетевых интерфейсов.



Особенности реализации

Основные особенности реализации:

- стек строился в соответствии с четырехуровневой моделью TCP/IP,
- есть четкое разделение кода на обработчики (handler'ы), которые обрабатывают конкретный протокол,
- компоненты, которые отвечают за первые три уровня находятся в ядре. Четвертый уровень – в пользовательском режиме.



The image features a central horizontal band with a blue-to-purple gradient. Overlaid on this band is a white network diagram consisting of numerous interconnected nodes and lines. The background of the entire image is an aerial view of a city skyline, rendered in shades of blue and green. The text is centered within the network overlay.

ОПИСАНИЕ КОМПОНЕНТОВ

Сетевой стек Linux



Описание компонентов

Интерфейс системного вызова (system call interface):

- дает способ приложениям из пользовательского пространства получать доступ к сетевой подсистеме ядра,
- вызов `sys_socketcall` в `socket.c`
- <https://habr.com/ru/post/268145/> (Сетевые системные вызовы. Часть 3),
- <http://linasm.sourceforge.net/docs/syscalls/network.php> (Network system calls).

Описание компонентов

Протоколо-независимый интерфейс (Protocol agnostic interface):

- уровень сокетов,
- набор стандартных функций для поддержки различных протоколов (TCP, UDP, Ethernet, SCTP),
- <https://github.com/torvalds/linux/blob/master/include/net/sock.h>

Описание компонентов

Сетевые протоколы (Network protocols):

- определяет отдельные доступные сетевые протоколы (TCP, UDP и т.д.),
- определяет какие именно протоколы будут использоваться в сетевом взаимодействии.
Своеобразный список разрешенных и активных.
- инициализация в функции `inet_init`,
- https://github.com/torvalds/linux/blob/master/net/ipv4/af_inet.c (семейство протоколов PF_INET, например, TCP и UDP)

Описание компонентов

```
struct inet_protosw
  inetsw_array[]
```

SOCK_STREAM
IPPROTO_TCP
&top_prot
&inet_stream_ops
...
SOCK_DGRAM
IPPROTO_UDP
&upd_prot
&inet_dgram_ops
...
SOCK_RAW
IPPROTO_IP
&raw_prot
&inet_sockraw_ops
...

```
struct proto tcp_prot
```

"TCP"
THIS_MODULE
tcp_close
tcp_v4_connect
tcp_disconnect
...

```
struct proto_ops
  inet_stream_ops
```

PF_INET
THIS_MODULE
inet_release
inet_bind
inet_stream_connect
...

Структура массива Internet-протокола

Описание компонентов

```
int fd = socket(AF_INET, SOCK_STREAM, 0);
```

<http://man7.org/linux/man-pages/man2/socket.2.html>

Name	Purpose	Man page
AF_UNIX	Local communication	unix(7)
AF_LOCAL	Synonym for AF_UNIX	
AF_INET	IPv4 Internet protocols	ip(7)
AF_AX25	Amateur radio AX.25 protocol	ax25(4)
AF_IPX	IPX - Novell protocols	
AF_APPLETALK	AppleTalk	ddp(7)
AF_X25	ITU-T X.25 / ISO-8208 protocol	x25(7)
AF_INET6	IPv6 Internet protocols	ipv6(7)
AF_DECnet	DECet protocol sockets	

Описание компонентов


Устройство-независимый интерфейс (Device agnostic interface):

- прослойка, которая соединяет логику работы протоколов с устройствами и их драйверами,
- New API (<https://wiki.linuxfoundation.org/networking/napi>),
- <http://unix-way.ru/index.php/poleznyashki-linux/118-linux-printsipy-raboty-s-setevoj-podsistemoj>
- <https://github.com/torvalds/linux/blob/master/include/linux/netdevice.h>

Описание компонентов

Драйверы устройств (Device drivers):

- драйверы, которые управляют сетевыми устройствами,
- <https://github.com/torvalds/linux/tree/master/drivers/net>

The image features a background of a dense city skyline, likely New York City, with numerous skyscrapers. The color palette is dominated by shades of blue and green, with a gradient from light green on the left to dark blue on the right. A network of thin, light blue lines connects various points across the image, creating a digital or data network aesthetic. The text is centered in the middle of the image.

ПОЛУЧЕНИЕ ИНФОРМАЦИИ О СЕТИ

Утилита ss

SS - another utility to investigate sockets. ss is used to dump socket statistics. It allows showing information similar to netstat. It can display more TCP and state information than other tools.

ss -6 state listening

```
root@Blinkenlights:/# ss -s
Total: 572
TCP:    2 (estab 0, closed 0, orphaned 0, timewait 0)

Transport Total      IP      IPv6
RAW       1          0       1
UDP       2          1       1
TCP       2          1       1
INET      5          2       3
FRAG      0          0       0
```

Утилита netstat

netstat - Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.

This program is mostly obsolete. Replacement for netstat is **ss**. Replacement for netstat -r is **ip route**. Replacement for netstat -i is **ip -s link**. Replacement for netstat -g is **ip maddr**.

```
root@Blinkenlights:~# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp6       0      0 :::111                 :::*                    LISTEN
udp        0      0 0.0.0.0:111             0.0.0.0:*               *
udp6       0      0 :::111                 :::*                    *
raw6       0      0 :::58                  :::*                    7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags               Type           State         I-Node      Path
unix   2      [ ACC ]              STREAM        LISTENING     26609       @/dbus-vfs-daemon/socket-seTy2r7B
unix   2      [ ACC ]              STREAM        LISTENING     23976       /tmp/ssh-XhPcqLiJe241/agent.859
unix   2      [ ACC ]              STREAM        LISTENING     24039       @/tmp/dbus-y5CEADo6Mn
```

Материалы для дополнительного чтения

Название	Ссылка
Creating sockets	https://idea.popcount.org/2019-11-06-creating-sockets/
Программирование сокетов в Linux	https://rdsn.org/article/unix/sockets.xml
Beej's Guide to Network Programming	http://beej.us/guide/bgnet/
Интервью с Алексеем Кузнецовым, одним из создателей сетевого стека Linux	https://www.opennet.ru/opennews/art.shtml?num=38016



Домашнее задание

Установить Android Studio.

Самостоятельно ознакомиться с материалами по предоставленным ссылкам.



Срок: 2 дня

Следующий вебинар

Тема: «Сетевая подсистема ОС Android»



Четверг 14 ноября 2019 г. в 20:00



Ссылка на вебинар будет в личном кабинете за 15 минут до начала



Материалы к занятию в ЛК — можно изучать



Обязательный материал обозначен красной лентой

The image features a central horizontal band with a blue-to-green gradient. Overlaid on this band is a white network of lines connecting various points, resembling a digital or social network. The background of the entire image is an aerial view of a city with numerous skyscrapers, tinted in shades of blue and green.

**Спасибо и
ДО НОВЫХ ВСТРЕЧ!**