
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

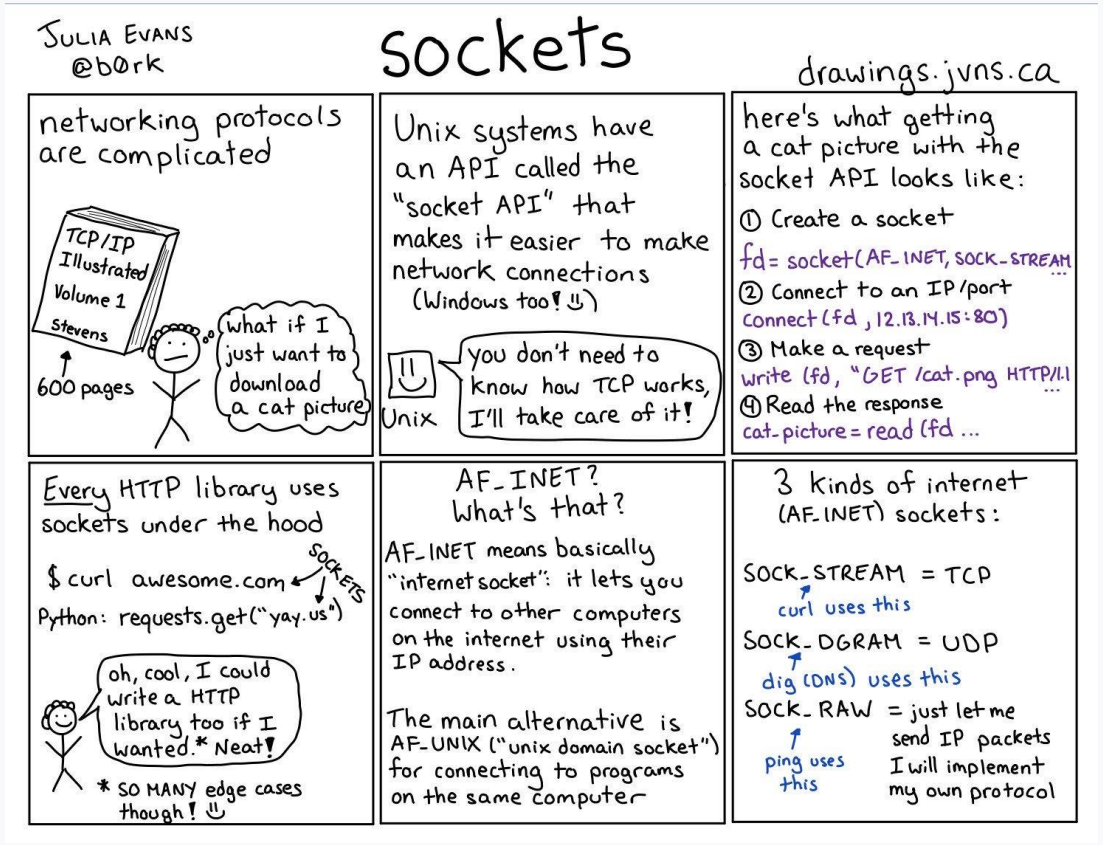
3. Провести практическую атаку на канальный уровень

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



Основные понятия

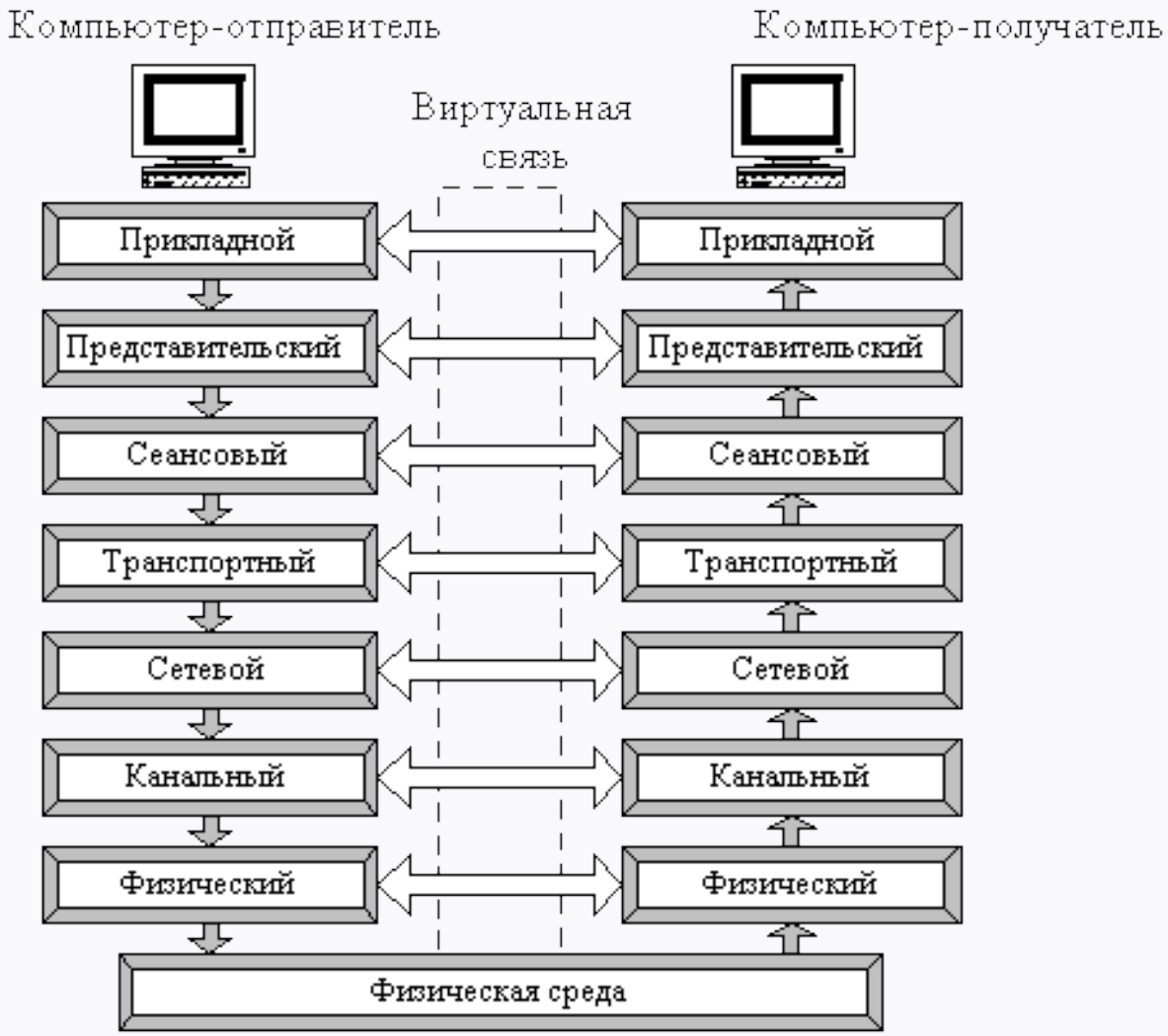
Типы сокетов:

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

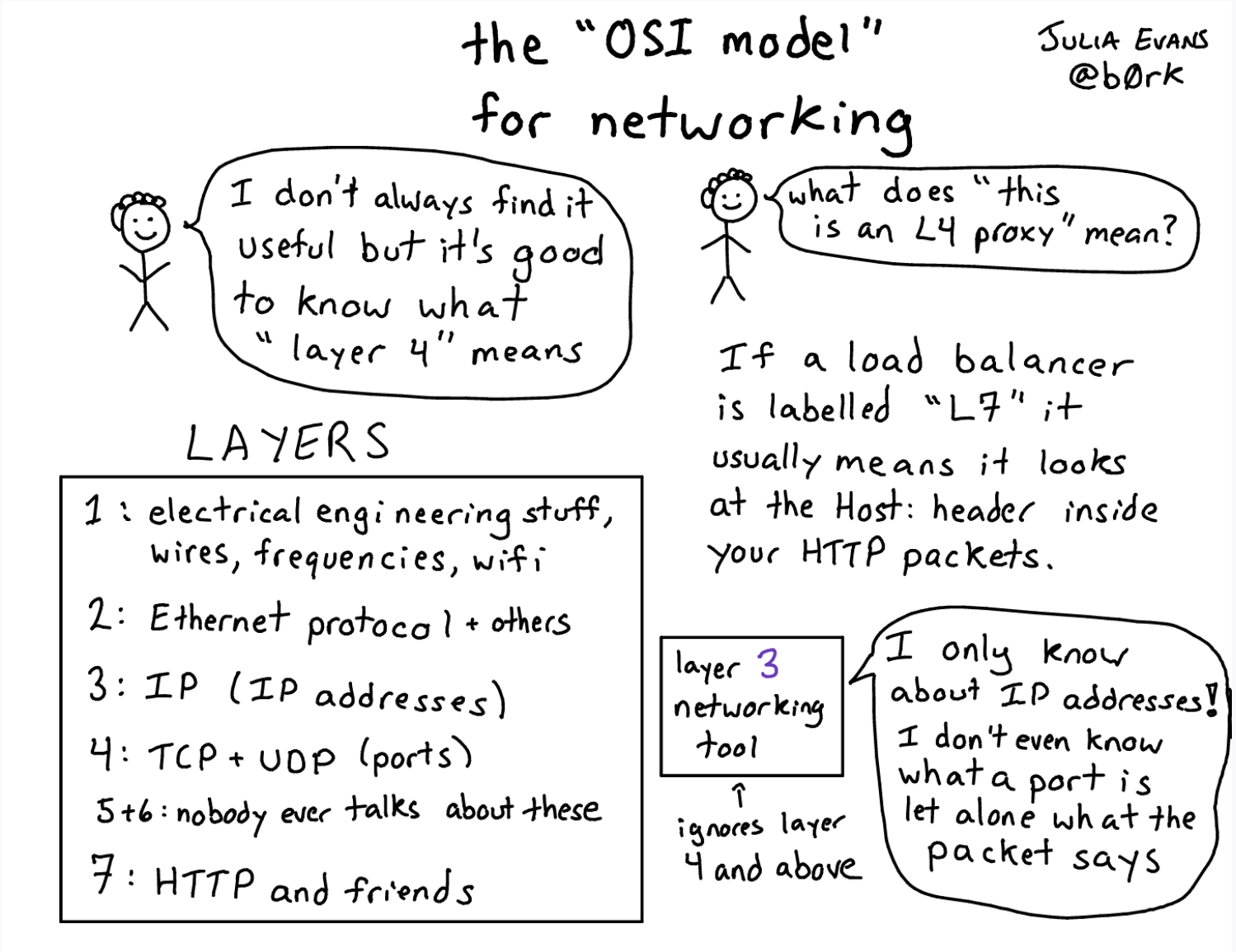
http://man7.org/linux/man-pages/man2/socket.2.html

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

Теоретическая модель OSI

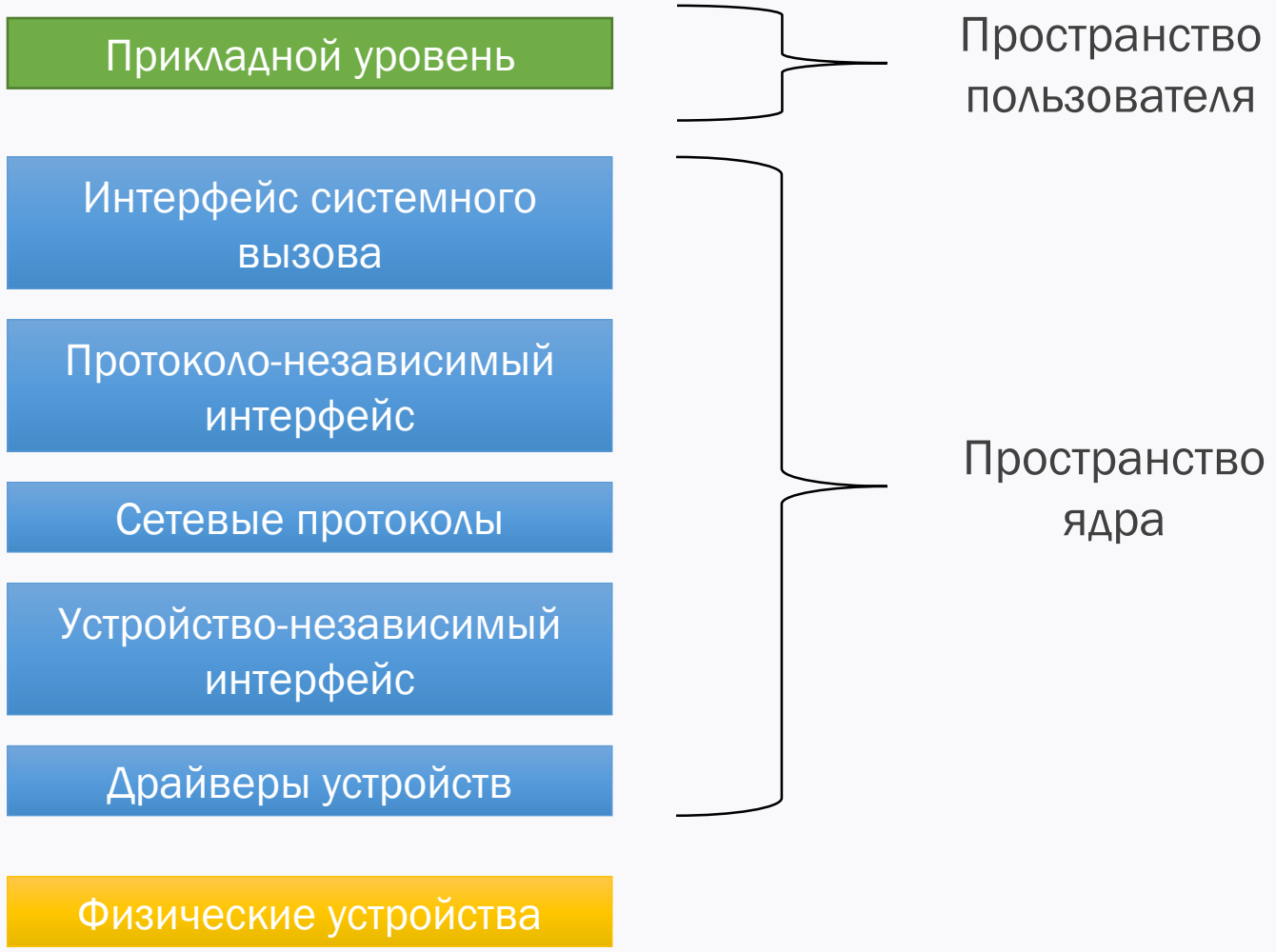


Теоретическая модель OSI



OSI 7 vs. TCP/IP

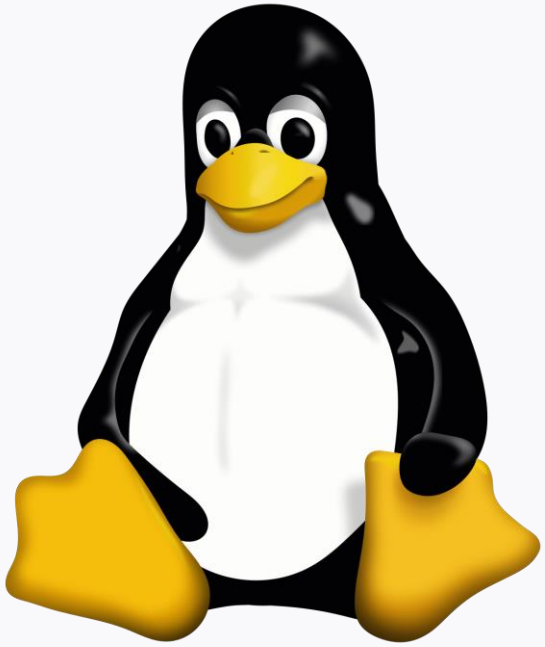
Сетевой стек Linux



Функциональность

Сетевая подсистема Linux обеспечивает следующую функциональность:

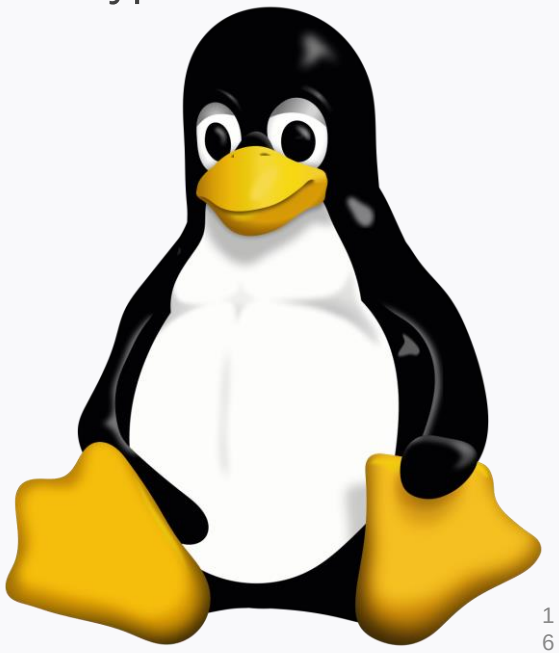
- абстракция сокетов,
- стеки сетевых протоколов (TCP/IP, UDP/IP, IPX/SPX, AppleTalk и мн. др.),
- маршрутизация (routing),
- пакетный фильтр (модуль Netfilter),
- абстракция сетевых интерфейсов.



Особенности реализации

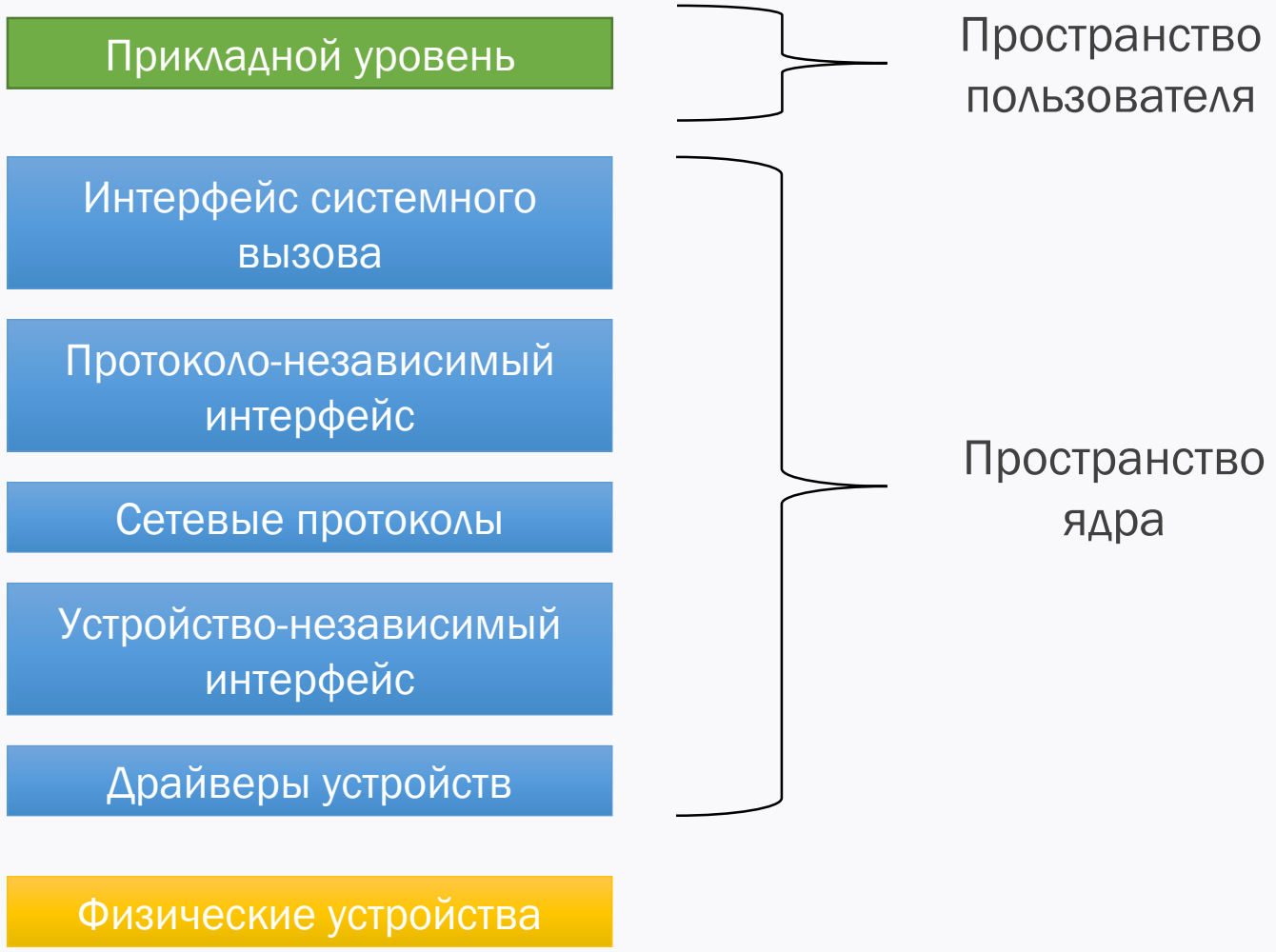
Основные особенности реализации:

- 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.



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):

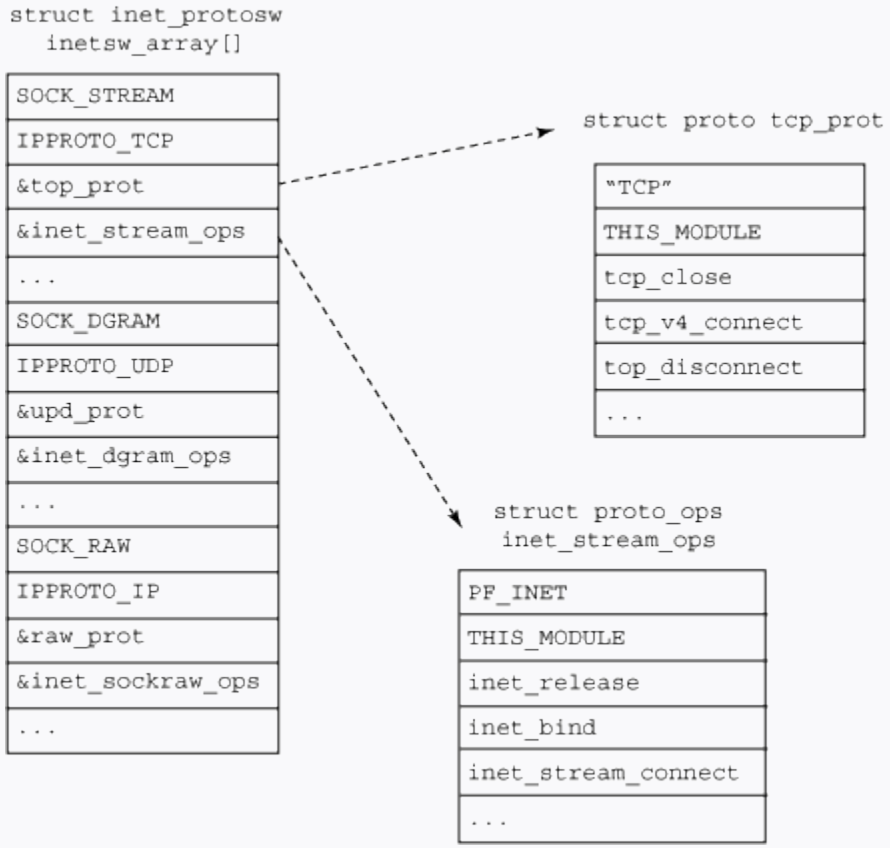
- уровень сокетов,
- набор стандартных функций для поддержки различных протоколов (TCP, UDP, Ethernet, SCTP),
- https://github.com/torvalds/linux/blob/master/include/net/sock.h

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



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

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-y5CFADo6Mn
```

Материалы для дополнительного чтения

Название	Ссылка
Creating sockets	https://idea.popcount.org/2019-11-06-creating-sockets/
Программирование сокетов в Linux	https://rsdn.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

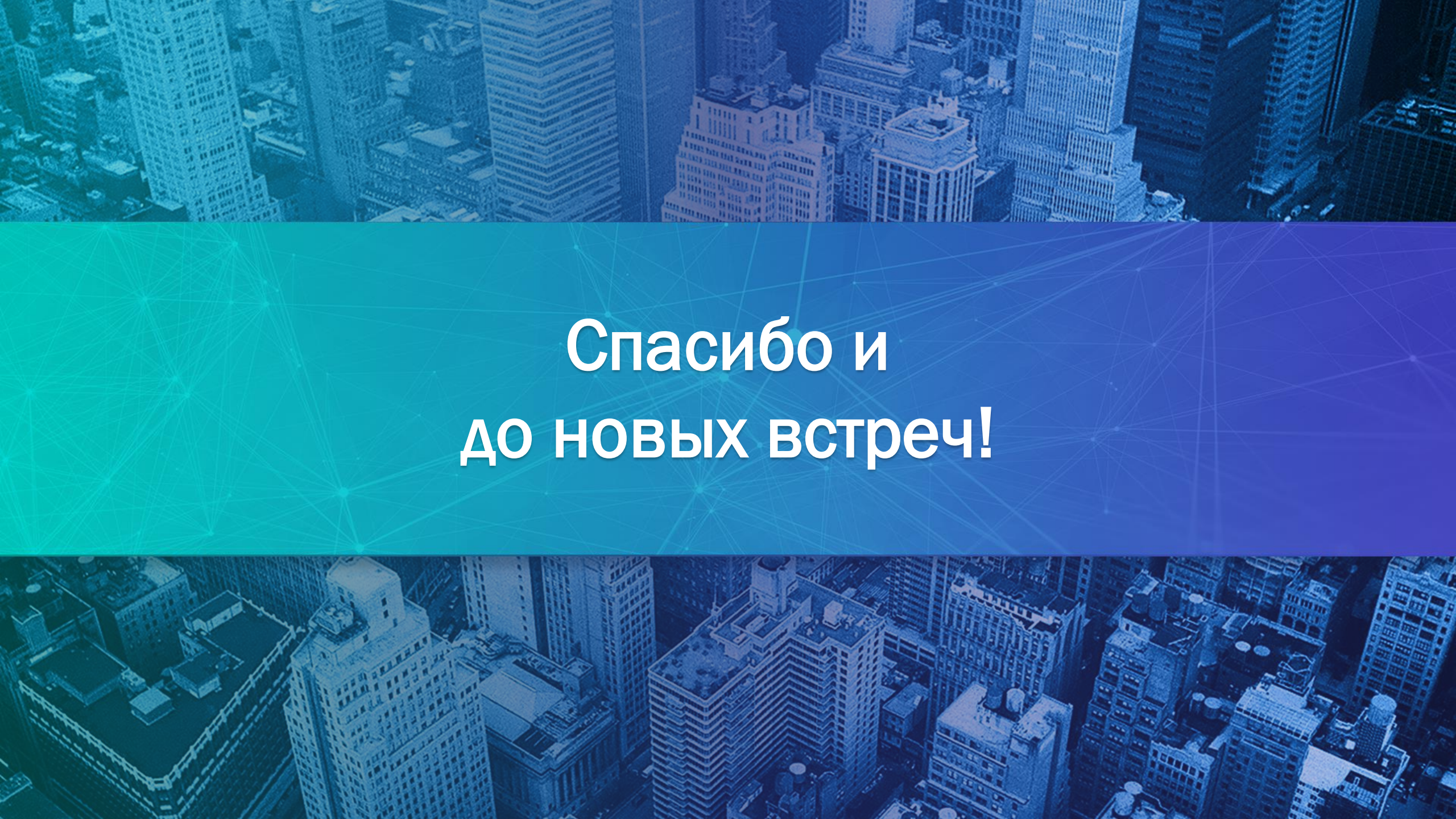
Тема: «Сетевая подсистема ОС Android»

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


Спасибо и
до новых встреч!