



ВВЕДЕНИЕ В СЕТИ

ОБЩИЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СЕТЕЙ
АРХИТЕКТУРА И СТАНДАРТИЗАЦИЯ СЕТЕЙ

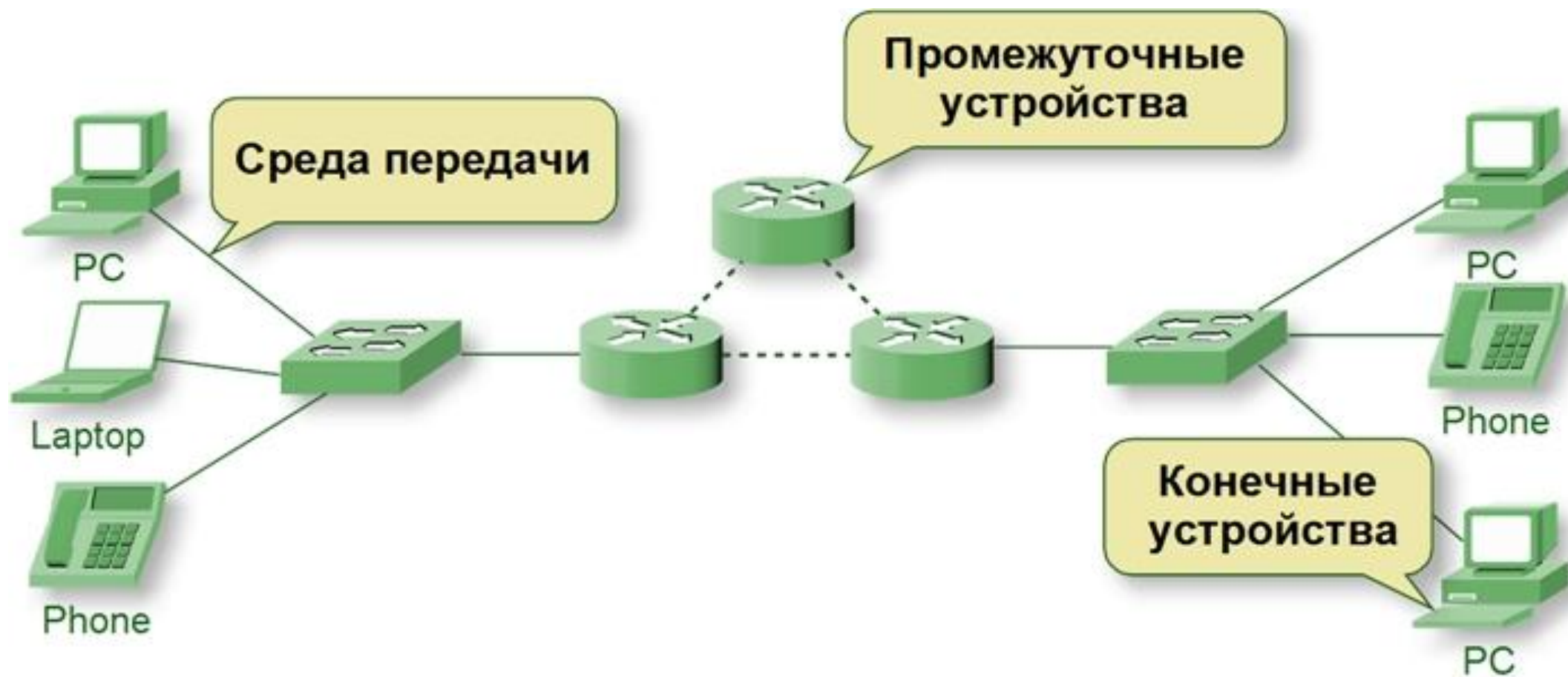
Компьютерные сети

- ▶ Компьютерные сети, сети передачи данных, Networks
- ▶ **Сеть** – группа компьютеров и/или других устройств, каким-либо способом соединенных для обмена информацией и совместного использования ресурсов.

Компоненты сети

- ▶ **Устройства** – физические элементы или оборудование сети
- ▶ **Среда передачи данных** – это физическая среда, по которой возможно распространение информационных сигналов в виде электрических, световых и т.п. импульсов
- ▶ **Сервисы - сетевые службы**, которые обеспечиваются специальными процессами сетевой операционной системы

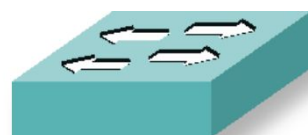
Компоненты сети



КОМПОНЕНТЫ СЕТИ

Промежуточные устройства

Устройства доступа к сети



Switch

Устройства сетевого взаимодействия



Router

Устройства безопасности

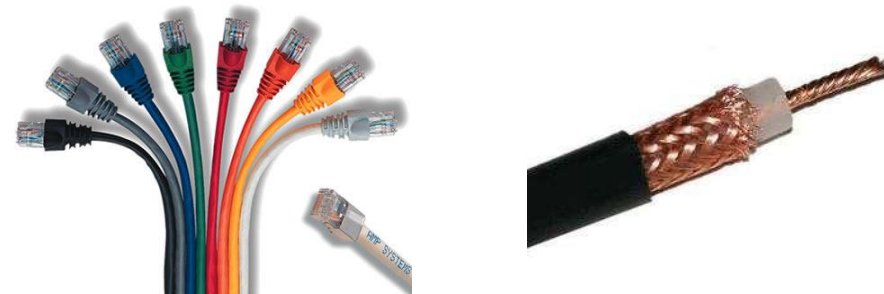


Firewall

Среда передачи данных

- ▶ Медная среда передачи данных

(витая пара, коаксиальный кабель)



- ▶ Оптическая среда передачи данных

(оптоволоконный кабель)



- ▶ Беспроводная среда передачи данных

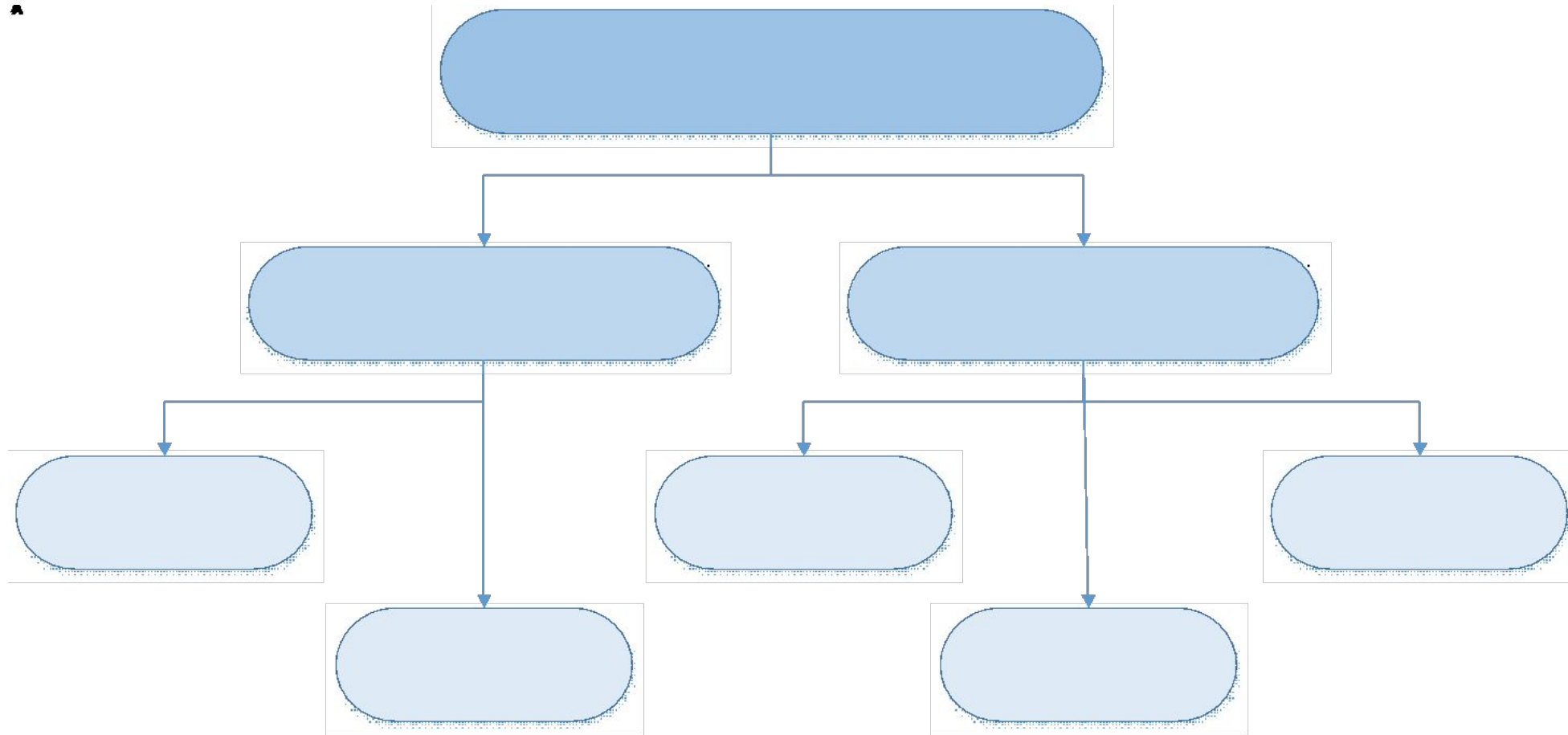
(Wi-Fi, Bluetooth, сотовая связь, спутниковая связь)



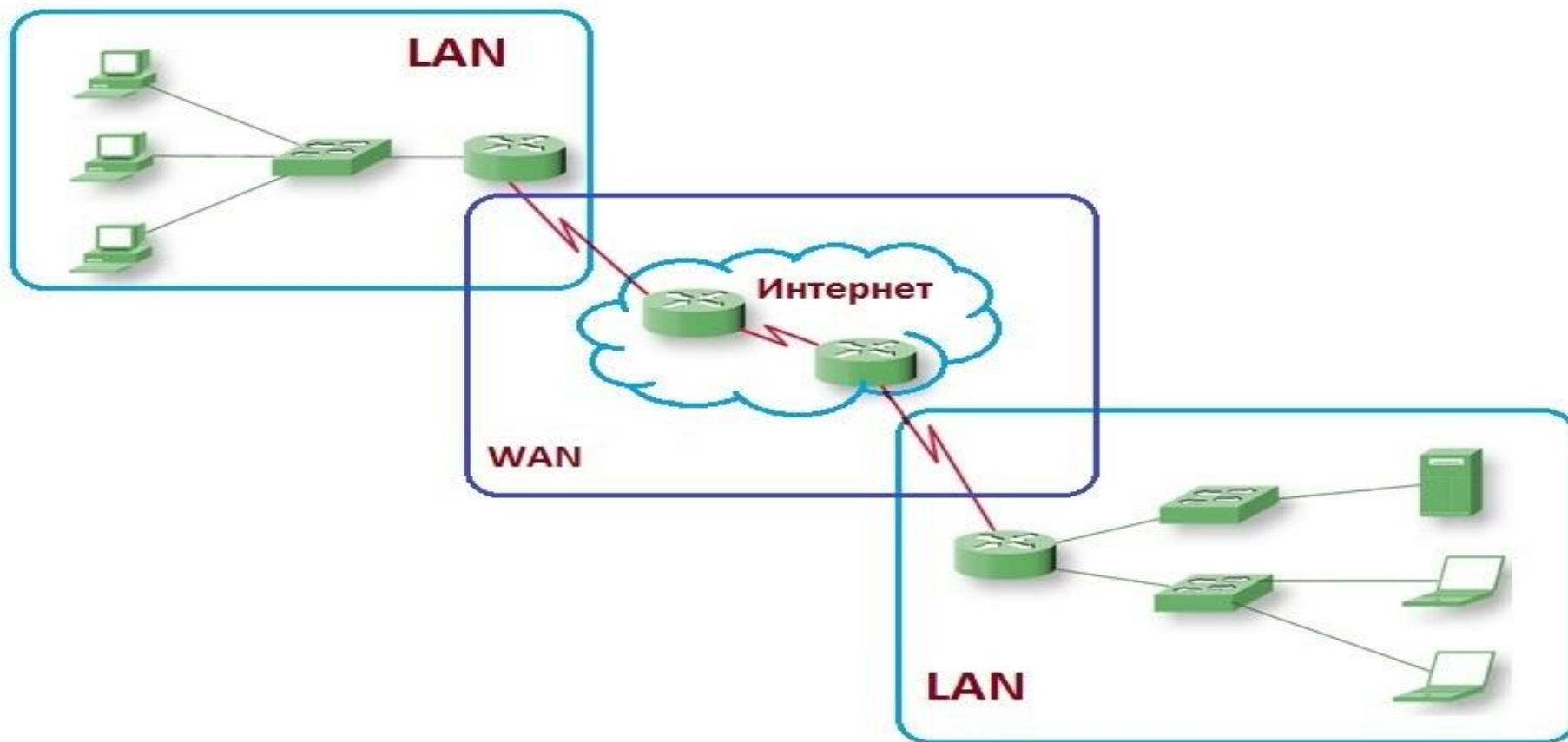
Классификация сетей

- ▶ Локальная сеть - Local Area Network, LAN
- ▶ Городская сеть, сеть мегаполиса – Metropolitan Area Network, MAN
- ▶ Глобальная сеть - Wide area network, WAN

Классификация сетей



Классификация сетей



Классификация сетей

Классификация сетей по распределению ролей между компьютерами:

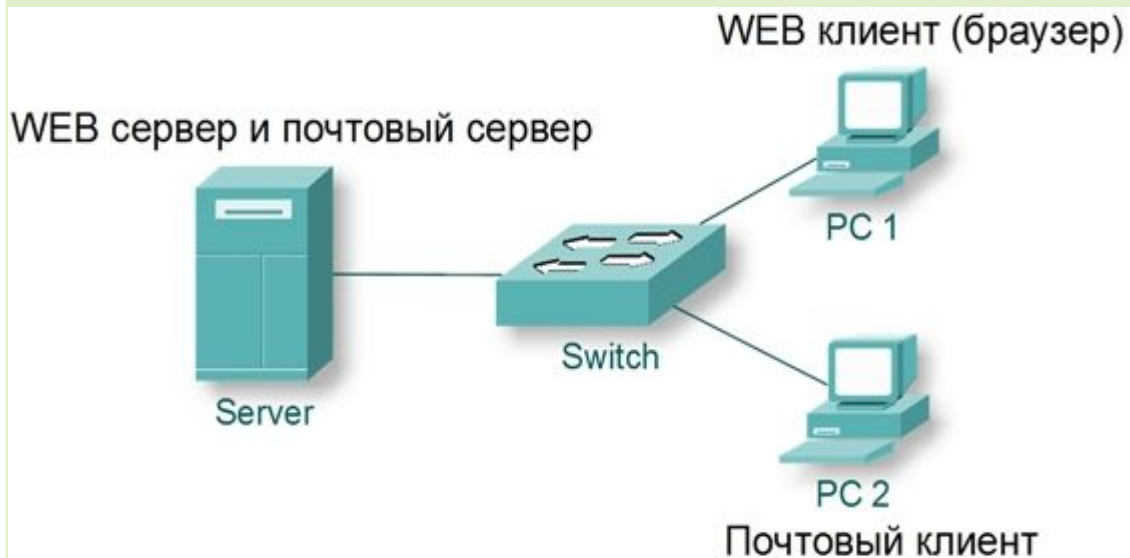
- ▶ Одноранговые сети
- ▶ Клиент-серверные

Клиенты и серверы

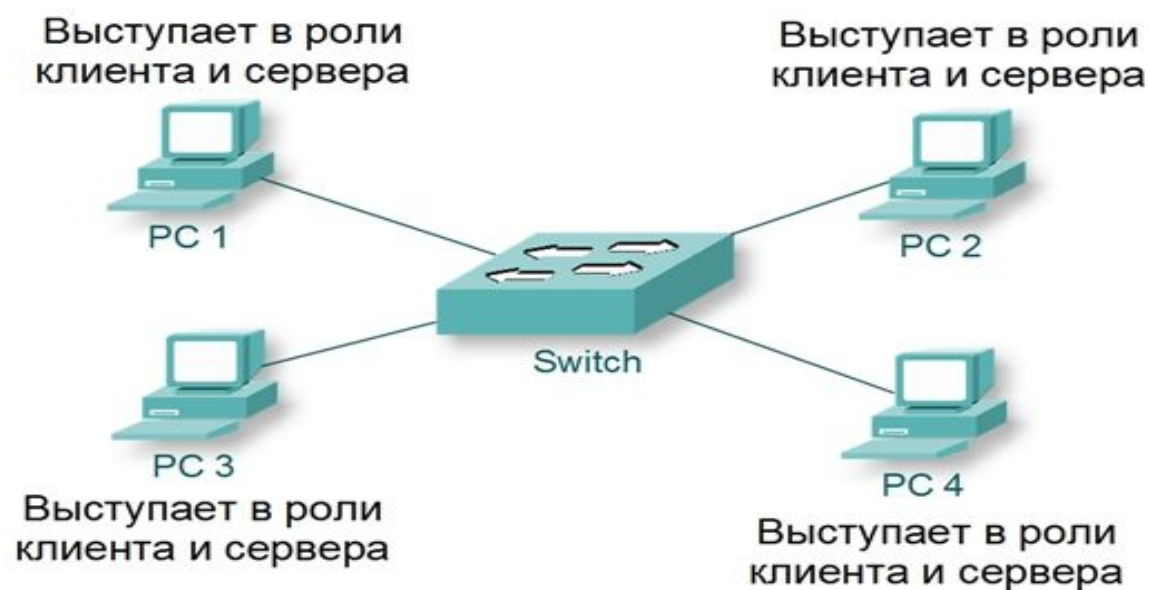
- ▶ **Серверы** – это узлы с установленным программным обеспечением, позволяющим предоставлять другим сетевым узлам информацию (например, доступ к электронной почте или веб-страницам)
- ▶ **Клиенты** — это компьютерные узлы с установленным программным обеспечением, позволяющим запрашивать и отображать полученную с сервера информацию.

Клиенты и серверы

Клиент-серверное взаимодействие (client-server)



Одноранговое взаимодействие (peer-to-peer)



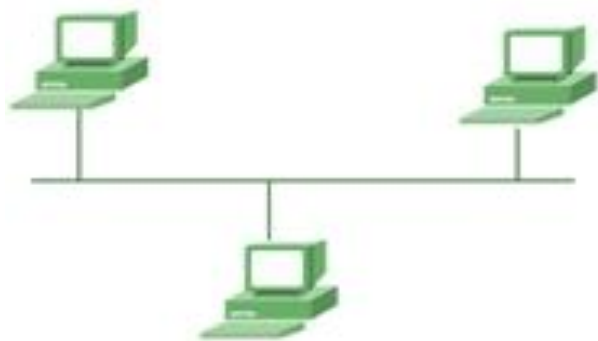
Топология сети

- ▶ **Топология сети** - это конфигурация графа, вершинам которого соответствуют конечные узлы сети (компьютеры) и коммуникационное оборудование (маршрутизаторы), а рёбрам — физические или информационные связи между вершинами.
- ▶ **Схемы физической топологии** — физическое расположение промежуточных устройств, настроенных портов и прокладки кабеля.
- ▶ **Схемы логической топологии** — определение устройств, портов и схемы IP-адресации.

Топология сети

Физическая топология

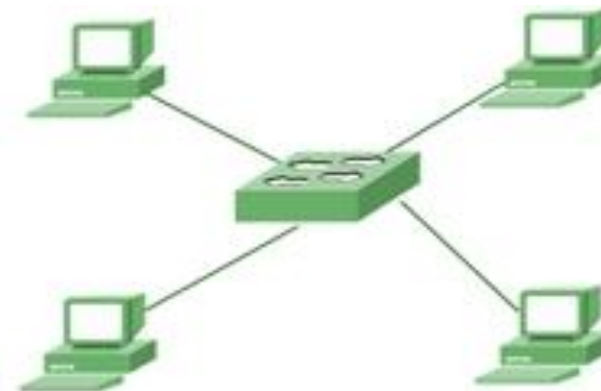
Шина



Кольцо

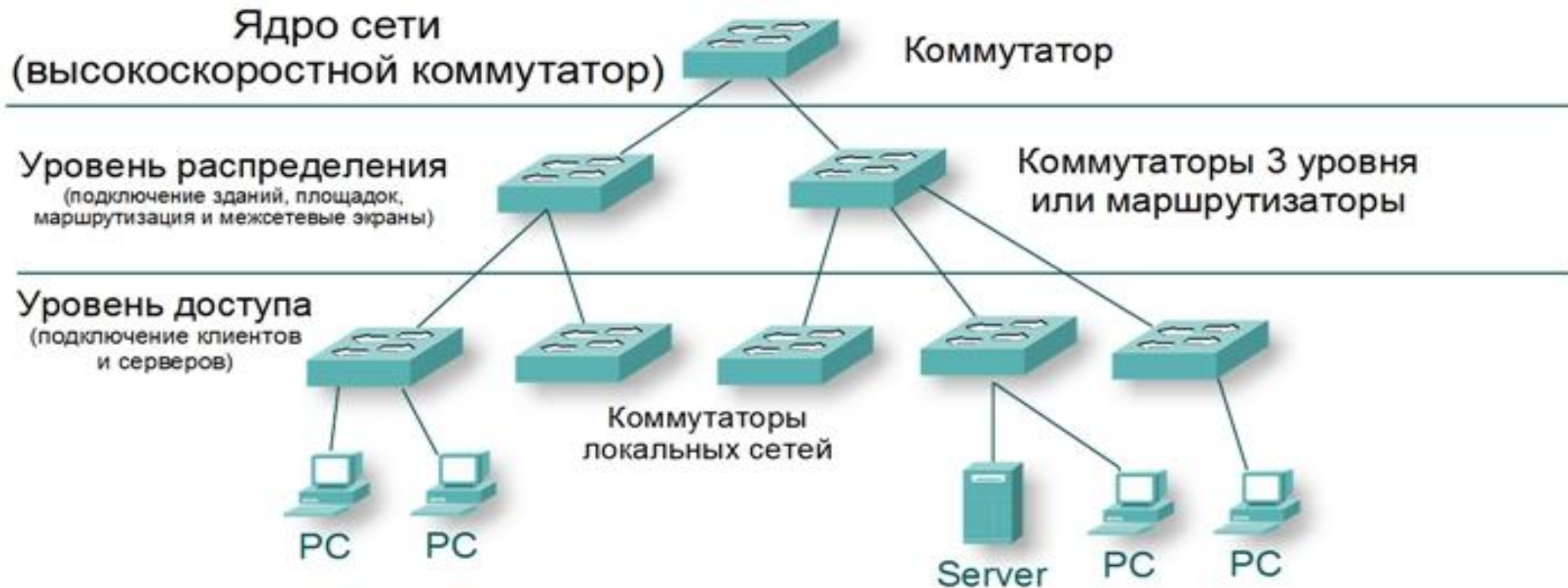


Звезда



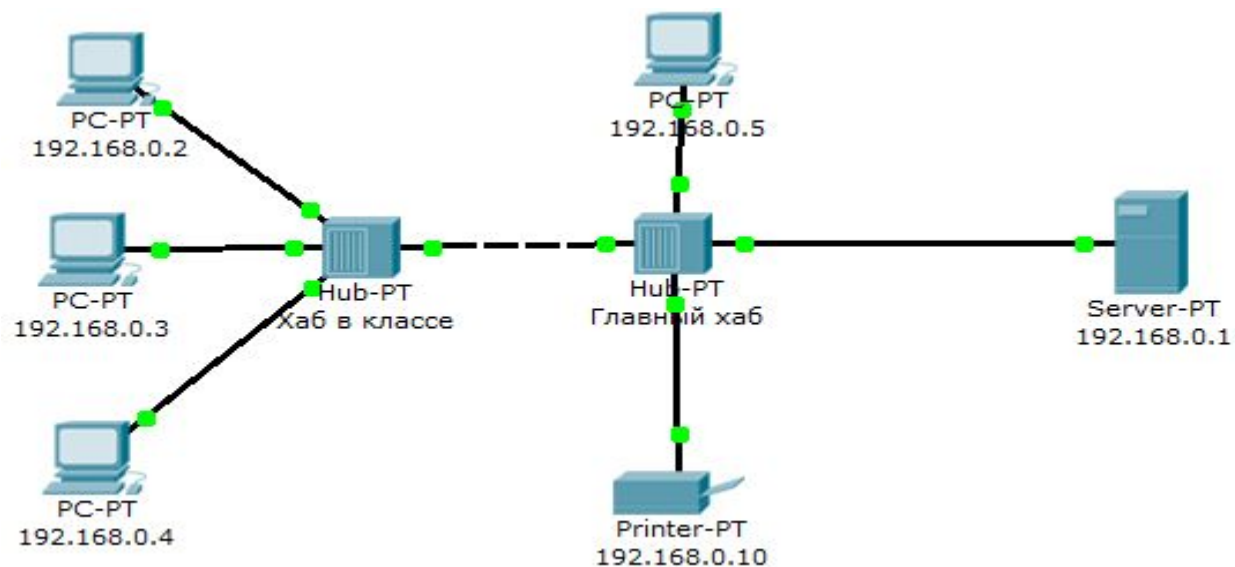
Топология сети

Физическая топология - Дерево



Топология сети

Логическая топология



Сетевой протокол

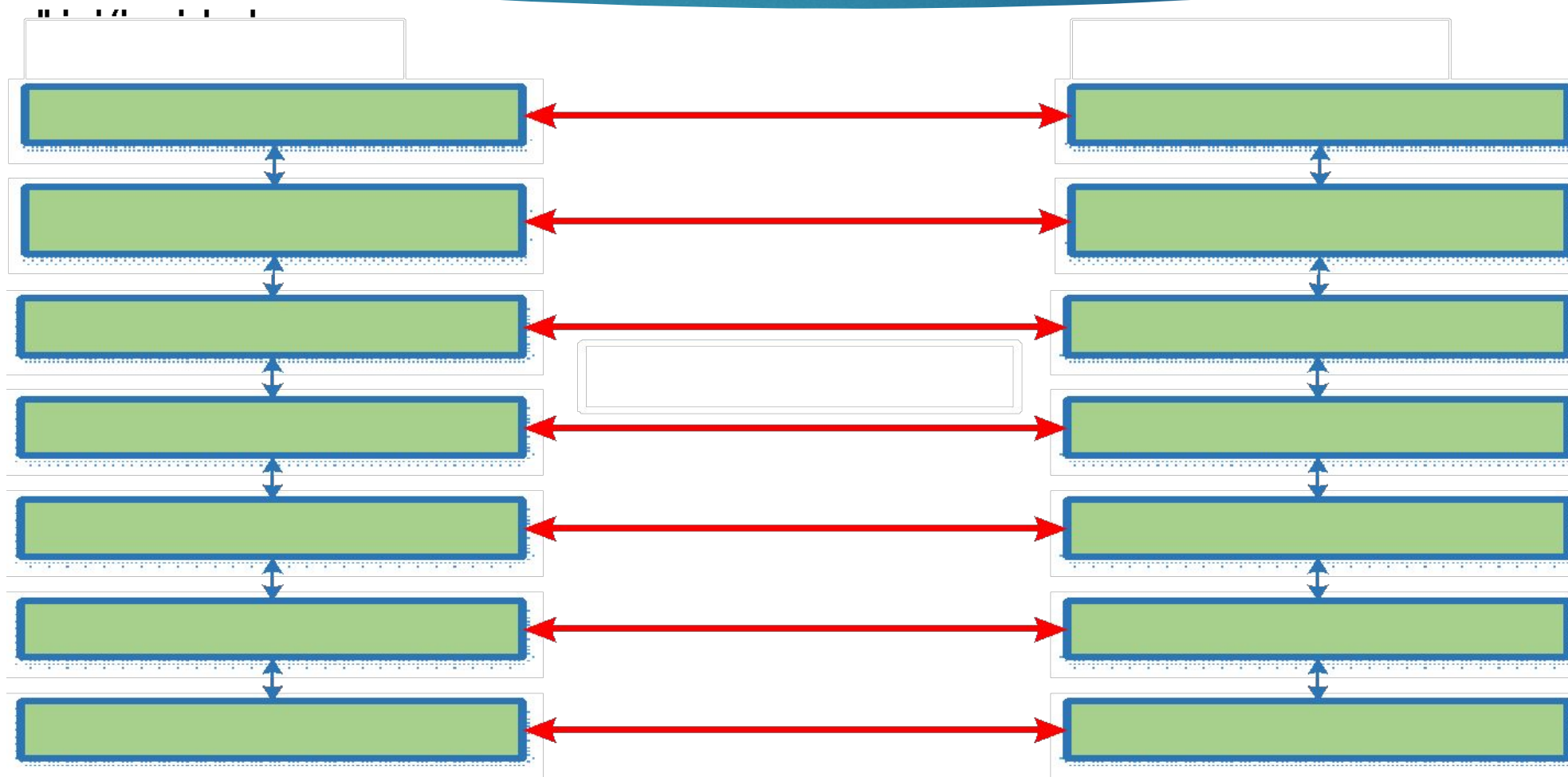
- ▶ **Сетевой протокол** – набор правил, позволяющий осуществлять соединение и обмен данными между двумя и более включёнными в сеть устройствами.

Эталонная модель OSI

- **Модель OSI** (*open systems interconnection basic reference model*) - сетевая модель стека сетевых протоколов OSI (ГОСТ Р ИСО/МЭК 7498-1-99).

Модель OSI	Функции	Протоколы
Уровень приложений	Доступ к сетевым службам	HTTP, FTP, SMTP
Уровень представления	Представление и шифрование данных	ASCII, EBCDIC, JPEG
Сеансовый уровень	Управление сеансом связи	RPC, PAP
Транспортный уровень	Прямая связь между конечными пунктами и надежность	TCP, UDP, SCTP
Сетевой уровень	Определение маршрута и логическая адресация	IPv4, IPv6, IPsec, AppleTalk
Канальный уровень	Управление доступом к среде. Физическая адресация	PPP, IEEE 802.2, Ethernet, DSL, L2TP, ARP
Физический уровень	Работа со средой передачи, сигналами и двоичными данными	USB, витая пара, коаксиальный кабель, оптический кабель

Взаимодействие между уровнями модели OSI



Движение данных по сети

- ▶ **Инкапсуляция данных** - процесс, который добавляет к данным содержимое заголовка дополнительного протокола перед передачей.
- ▶ **Деинкапсуляция данных** - процесс, который выполняется приёмным устройством, чтобы удалить один или несколько заголовков протоколов.

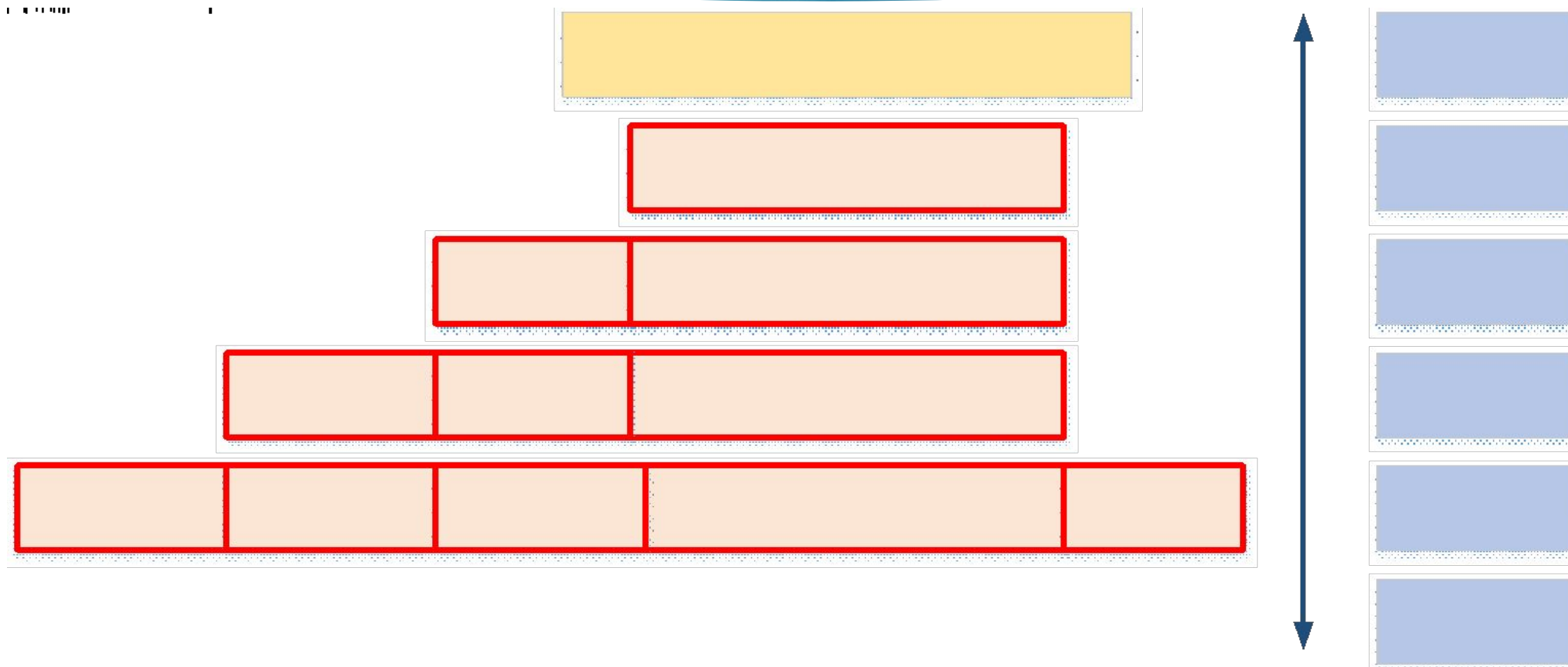
Движение данных по сети

- ▶ **Протокольный блок данных (PDU)** - фрагмент данных на разных уровнях моделей OSI, TCP/IP

Модель OSI	PDU
Уровень приложений	Данные
Уровень представления	
Сеансовый уровень	
Транспортный уровень	Сегмент
Сетевой уровень	Пакет
Канальный уровень	Кадр
Физический уровень	Биты

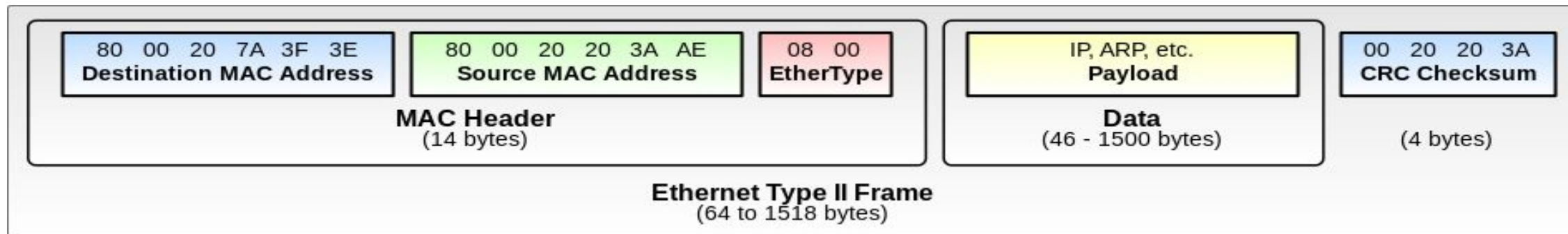
Движение данных по сети

1 2 3 4 5



Уровень 2 – Канальный (Data link)

- ▶ Канальный уровень обеспечивает два базовых сервиса :
 - принимает пакет уровня 3 и преобразует его в блок данных, который называется кадр;
 - контролирует управление доступом к среде и выполняет обнаружение ошибок.
- ▶ Протоколы — Ethernet, IEEE 802.11 Wireless Ethernet, SLIP, Token Ring, ATM и MPLS.
- ▶ Устройства — коммутаторы
- ▶ Блок данных — кадр



Уровень 3 – Сетевой (network)

**Адресация
конечных
устройств**

Маршрутизация

Протоколы - IPv4, IPv6, ICMP, BGP, RIP, IPSec

Оборудование - маршрутизаторы

Блок данных — пакет

4 уровень – Транспортный (transport)

Отслеживание отдельных сеансов передачи данных между приложениями на узле-источнике и узле-получателе

Сегментирование данных для управления ими, а также для их повторной компоновки в потоки прикладных данных на узле-адресате

Идентификация соответствующего приложения для каждого потока обмена данными

- ▶ Протоколы — TCP, UDP, SCTP
- ▶ Блок данных — сегмент

7 уровень – Прикладной (Application)

- ▶ Передача файлов : TFTP, FTP, NFS
- ▶ E-mail: SMTP
- ▶ Удаленный доступ: Telnet
- ▶ Управление сетью: SNMP
- ▶ Система имен: DNS

Стек протоколов

- ▶ **Стек протоколов** - это иерархически организованный набор сетевых протоколов, достаточный для организации взаимодействия узлов в сети.

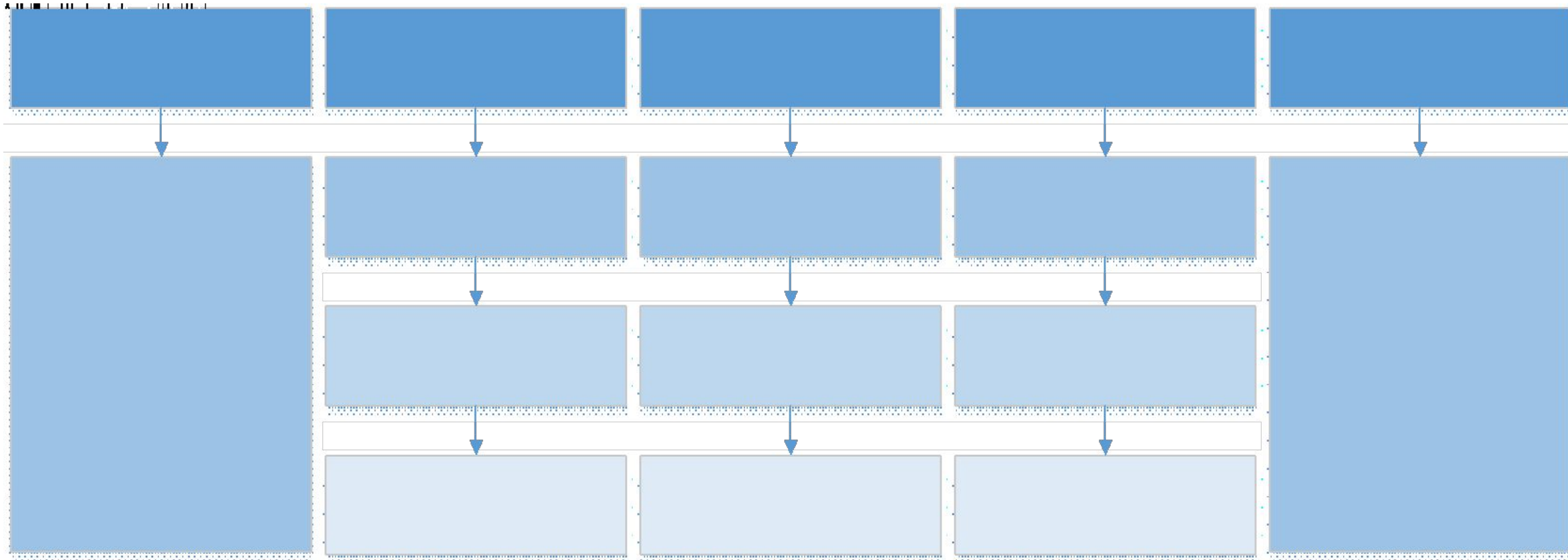
Стек протоколов TCP/IP

Стек протоколов TCP/IP	Функции	Протоколы
Уровень приложений	Работа большинства сетевых приложений	HTTP, RTSP, FTP, DNS
Транспортный уровень	Прямая связь между конечными пунктами и надежность	TCP, UDP, SCTP, DCCP
Межсетевой уровень	Определение маршрута и логическая адресация	IPv4, IPv6, ICMPv4, ICMPv6
Уровень сетевого доступа	Физическая адресация Работа со средой передачи, сигналами и двоичными данными	Ethernet, IEEE 802.11 Wireless Ethernet, SLIP, Token Ring, ATM и MPLS, физическая среда и принципы кодирования информации, T1, E1

Сравнение стека протоколов TCP/IP с моделью OSI

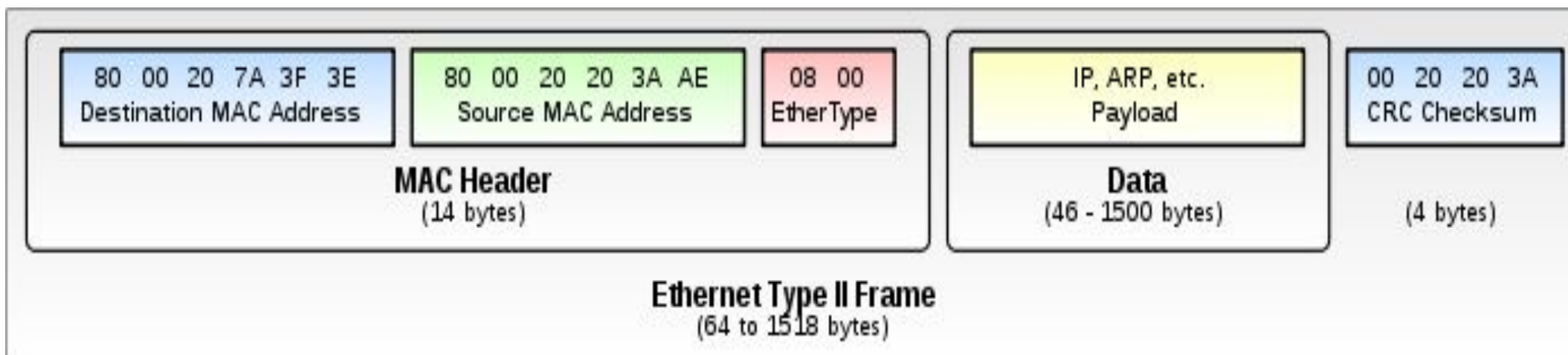
Модель OSI	Протоколы	Стек протоколов TCP/IP
Уровень приложений	HTTP, DNS, DHCP, FTP	Уровень приложений
Уровень представления		
Сеансовый уровень		
Транспортный уровень	TCP, UDP	Транспортный уровень
Сетевой уровень	IPv4, IPv6, ICMPv4, ICMPv6	Межсетевой уровень
Канальный уровень	PPP, Frame Relay, Ethernet	Уровень сетевого доступа
Физический уровень		

Адресация



MAC - адрес

- ▶ MAC – адрес – уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet - физический адрес.
- ▶ 48 бит



IP - адрес

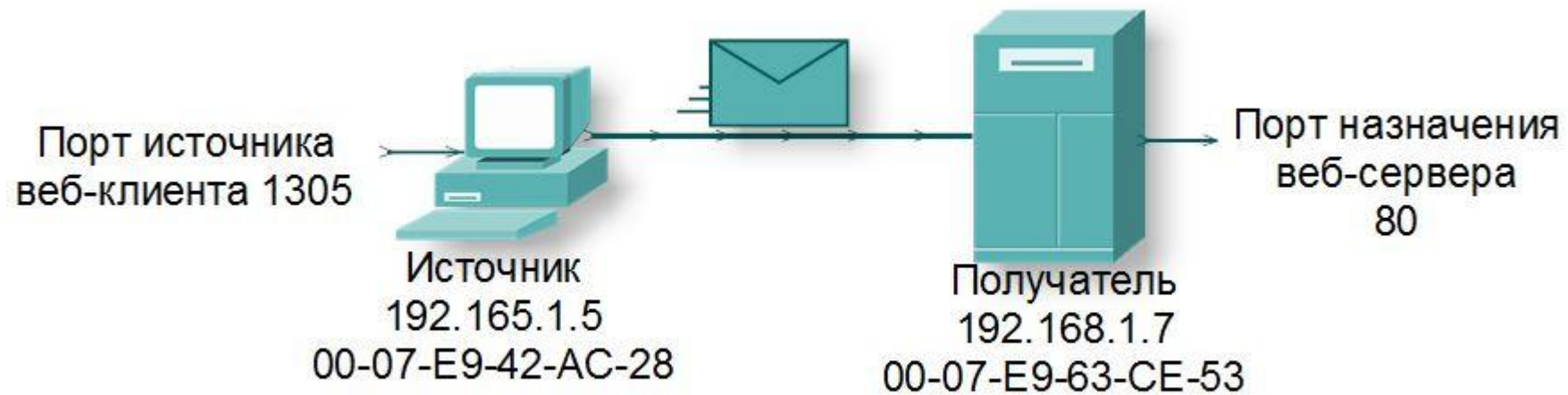
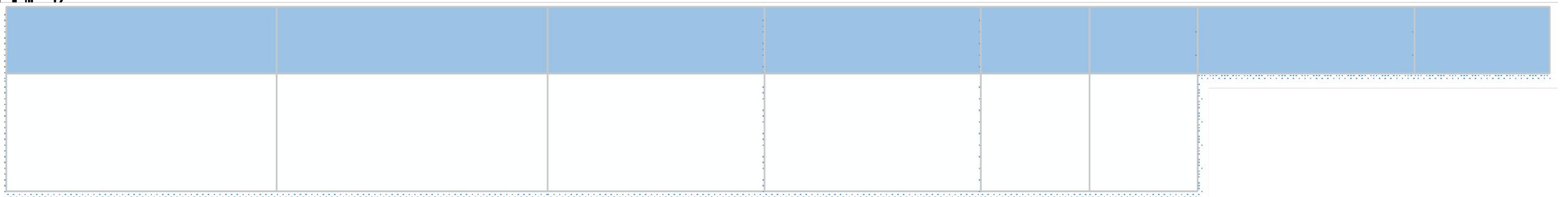
- ▶ IP – адрес - уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP.
- ▶ IPv4 – 32 бита IPv6 – 128 бит



Сетевой порт

- ▶ **Порт** — натуральное число, записываемое в заголовках протоколов транспортного уровня модели OSI (TCP, UDP, SCTP, DCCP). Используется для определения процесса-получателя пакета в пределах одного хоста.
- ▶ **Порт назначения** - клиент указывает номер порта назначения в сегменте, чтобы сообщить серверу назначения информацию о том, какой сервис запрашивается.
- ▶ **Исходный порт** - номер порта источника случайно генерируется устройством-отправителем для идентификации сеанса связи между двумя устройствами.

Адресация



Сетевое оборудование

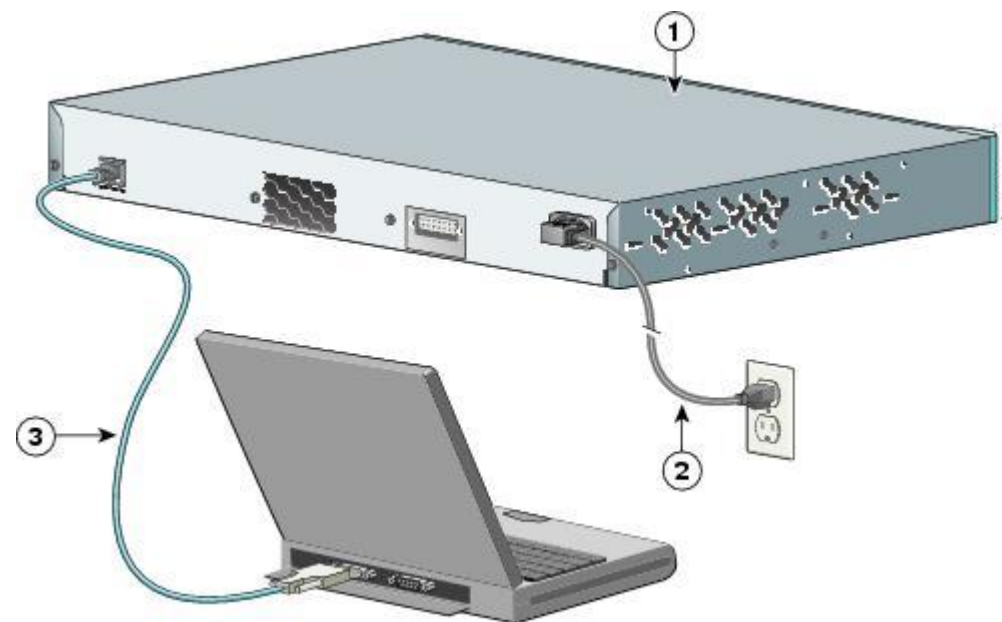
- ▶ **Маршрутизатор** - передает и получает пакеты данных из сети Интернет
- ▶ **Коммутатор** - соединяет конечные устройства с помощью сетевых кабелей
- ▶ **Точка беспроводного доступа** - состоит из радиопередатчика, который осуществляет беспроводное соединение конечных устройств
- ▶ **Устройство межсетевого экрана** - защищает исходящий и запрещает входящий трафик.

Методы доступа к сетевому оборудованию

- ▶ Консоль
- ▶ Telnet или SSH
- ▶ Порт AUX

Методы доступа к сетевому оборудованию

- ▶ Консоль
- ▶ Консольный порт — это порт управления, обеспечивающий возможность внеполосного доступа к устройству.
- ▶ Внеполосный доступ — это доступ через выделенный административный канал, который используется исключительно в целях технического обслуживания устройства.



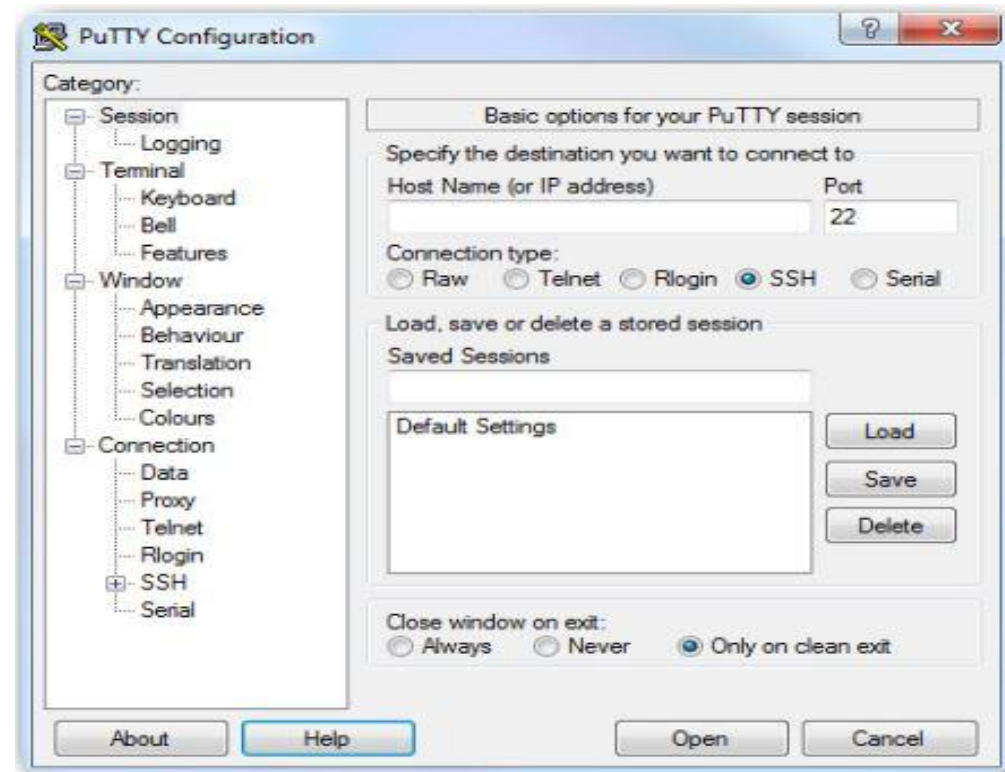
Методы доступа к сетевому оборудованию

- ▶ Telnet — это способ удалённого установления сеанса интерфейса командной строки (CLI) через виртуальный интерфейс по сети.
- ▶ SSH – способ удалённого входа в систему аналогично Telnet. Протокол SSH предоставляет более высокий уровень аутентификации на основе пароля, чем протокол Telnet, и при передаче информации о сеансе использует шифрование.
- ▶ Порт AUX - Устаревший метод установления сеанса интерфейса командной строки (CLI) — с помощью коммутируемого соединения по телефону к вспомогательному порту (AUX) маршрутизатора.

Методы доступа к сетевому оборудованию

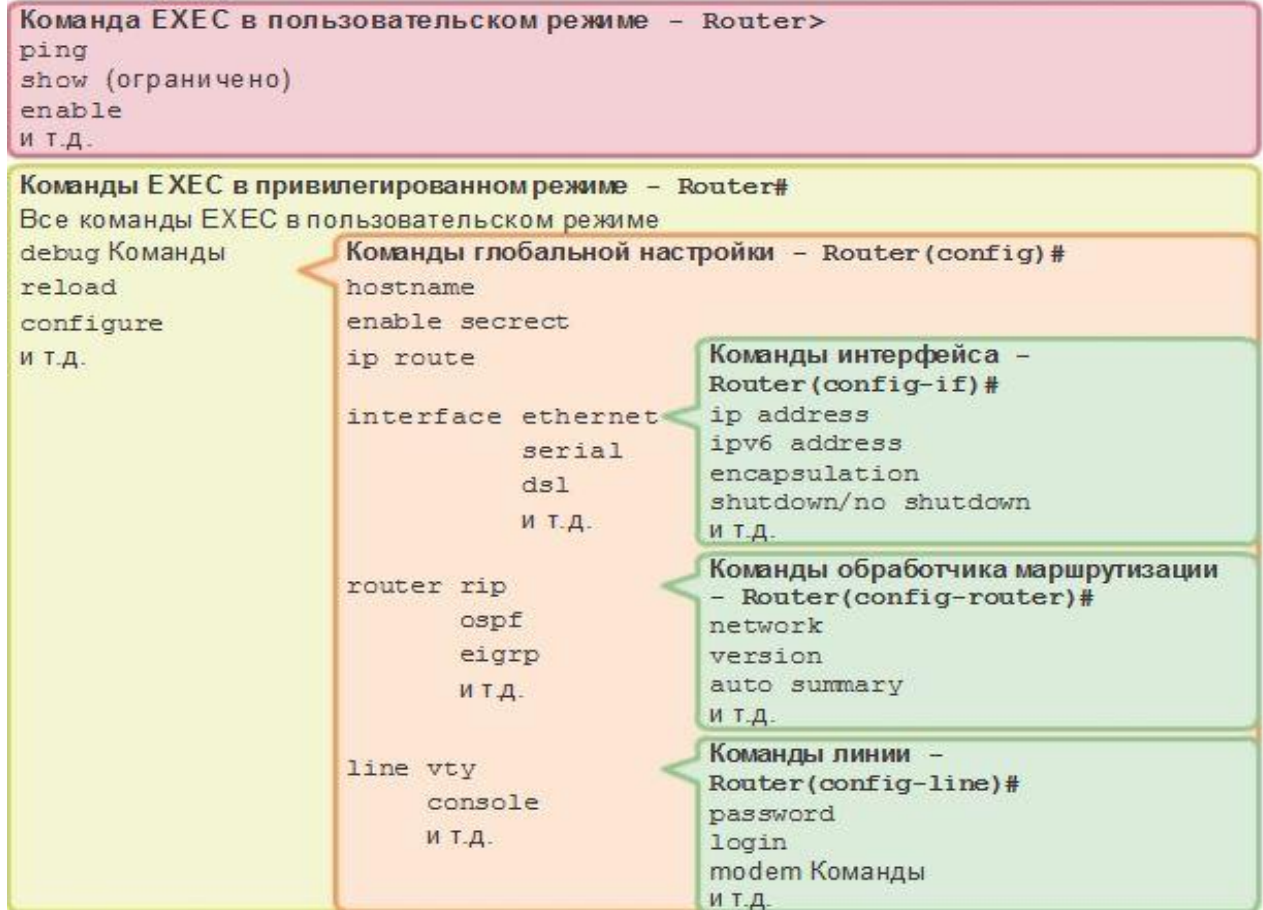
Программы эмуляции терминала:

- ▶ PuTTY
- ▶ Tera Term
- ▶ HyperTerminal
- ▶ Terminal OS X

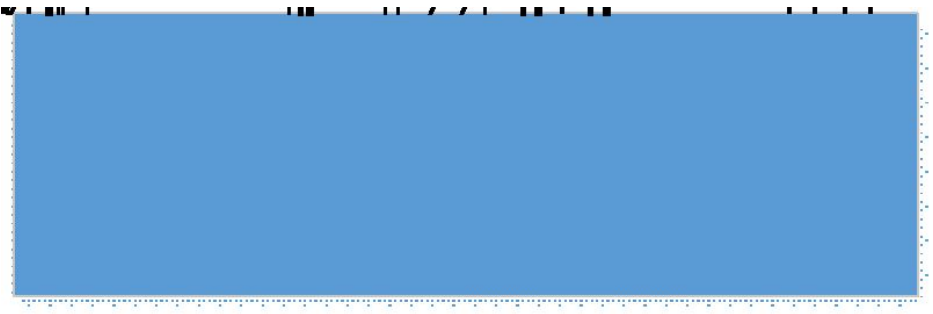


Режимы работы оборудования

- ▶ Пользовательский режим
- ▶ Привилегированный режим
- ▶ Режим глобальной конфигурации



Режимы работы оборудования

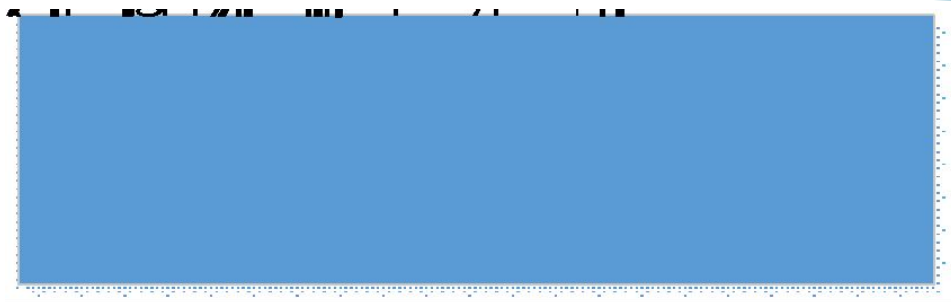


Переход в привилегированный режим:
Router> enable
Router#



Переход из привилегированного режима в пользовательский:
Router# disable
Router>

Режимы работы оборудования



Переход в режим глобальной конфигурации:
`Router# configure terminal`
`Router(config)#`



Выход из режима глобальной конфигурации:
`Router(config)# exit`
`Router#`

Структура команд

Синтаксис:

▶ Switch> **ping** *ip-address*

Пример со значениями:

▶ Switch> **ping 10.10.10.5**

Команда — **ping**, пользовательский параметр — **10.10.10.5**.

Синтаксис:

▶ Switch> **traceroute** *ip-address*

Пример со значениями:

▶ Switch> **traceroute 192.168.254.254**

Команда — **traceroute**, пользовательский параметр — **192.168.254.254**.

Базовые команды

Show - Базовая команда для проверки работы устройств

- ▶ **show interfaces** - служит для отображения статистических сведений по всем интерфейсам устройства

Пример: Switch# **show interfaces fastethernet 0/1**

- ▶ **show startup-config** - отображает сохранённую конфигурацию, расположенную в NVRAM.
- ▶ **show running-config** - отображает содержимое файла текущей конфигурации.

Базовые команды

- ▶ Switch# **show version** - отображает сведения о загруженной версии IOS, а также данные об устройстве и аппаратном обеспечении.
- ▶ **Software version** — версия программного обеспечения IOS (хранится во флеш памяти)
- ▶ **Bootstrap version** — версия программы начальной загрузки (хранится в загрузочном ПЗУ)
- ▶ **System up-time** — время с момента последней перезагрузки
- ▶ **System restart info** — способ перезапуска (например, цикл включения-выключения, сбой системы)
- ▶ **Software image name** — имя файла образа IOS, хранящегося во флеш памяти
- ▶ **Router type and processor type** — номер модели и тип процессора
- ▶ **Memory type and allocation (shared/main)** — ОЗУ главного процессора и буферизация ввода/вывода пакета
- ▶ **Software features** — поддерживаемые протоколы/наборы функций
- ▶ **Hardware interfaces** — доступные на устройстве интерфейсы
- ▶ **Configuration register** — спецификации загрузки, настройка скорости консоли и других параметров

Настройка узлов

Имена узлов должны:

- ▶ начинаться с буквы
- ▶ не содержать пробелов
- ▶ оканчиваться на букву или цифру
- ▶ содержать только буквы, цифры и тире
- ▶ содержать не более 64 символов

Настройка имени узла:

```
Switch> enable  
Switch# configure terminal  
Switch(config)# hostname Sw-HSE-1  
Sw-HSE-1 (config)#exit  
Sw-HSE-1#
```

Отмена действия команды:

```
Sw-HSE-1 (config)# no hostname  
Switch(config)#
```

Ограничение доступа к файлам конфигурации устройств

- ▶ **Пароль привилегированного режима** — ограничивает доступ в привилегированный режим
- ▶ **Секретный пароль** — зашифрованный пароль, ограничивающий доступ в привилегированный режим
- ▶ **Пароль консоли** — ограничивает доступ к устройствам через консольное подключение
- ▶ **Пароль для VTU** — ограничивает доступ к устройствам через Telnet

Защита доступа к привилегированному режиму

- ▶ Команды **enable password** и **enable secret** позволяют ограничить доступ в привилегированный режим EXEC и запретить посторонним вносить изменения в настройки маршрутизатора.
- ▶ Switch(config)# **enable password hsepass** – пароль незашифрован
- ▶ Switch(config)# **enable secret hsepass** – пароль зашифрован

- ▶ **service password-encryption** – шифрует незашифрованные пароли

Защита доступа к пользовательскому режиму

- ▶ Чтобы установить пароль для консоли строки в режиме глобальной конфигурации, нужно ввести следующие команды:
- ▶ Switch(config)# **line console 0**
- ▶ Switch(config-line)# **password hsepass**
- ▶ Switch(config-line)# **login**

Защита доступа к пользовательскому режиму

- ▶ Канал VTY – обеспечивает доступ к устройствам по протоколу Telnet
- ▶ VT – виртуальный терминал

Конфигурация:

```
Router(config) #line vty 0 4  
Router(config-line) #password hsepass  
Router(config-line) #login
```

login - предотвращает доступ по протоколу Telnet к устройству без аутентификации.

0 4 — это 5 пользовательских виртуальных терминалов = telnet сессий

По умолчанию многие коммутаторы Cisco поддерживают до 16 каналов VTY, пронумерованных от 0 до 15.

Конфигурация баннера

- ▶ Настройка баннера в режиме глобальной конфигурации:
- ▶ Switch(config)# **banner motd # message #**
- ▶ После выполнения команды баннер будет показан при всех последующих попытках доступа к устройству, пока он не будет удалён.

Сохранение конфигураций

- ▶ **show running-config** - для просмотра файла текущей конфигурации
- ▶ **copy running-config startup-config** - для сохранения файла текущей конфигурации в файл загрузочной конфигурации

Switch# **copy running-config startup-config**

После выполнения команды файл текущей конфигурации обновляет файл загрузочной конфигурации.

Сброс настроек

- ▶ **erase startup-config** – команда для сброса настроек

Switch# **erase startup-config**

После удаления начальной конфигурации из NVRAM необходимо перезапустить устройство:

Switch# **reload**

Устройство загрузит файл начальной конфигурации, встроенной по умолчанию, в текущую конфигурацию.