

МДК.01.01
Организация, принципы
построения и функционирования
компьютерных сетей
2-курс

Занятие 23

Прикладной уровень стека TCP/IP

Прикладной уровень стека TCP/IP

Прикладной уровень стека TCP/IP соответствует трем верхним уровням модели OSI:

- прикладному,
- представительному,
- сеансовому.

Он объединяет службы, предоставляемые системой пользовательским приложениям.

За долгие годы использования в сетях различных стран и организаций стек TCP/IP накопил большое количество **протоколов** и **служб** прикладного уровня.

Прикладной уровень стека TCP/IP

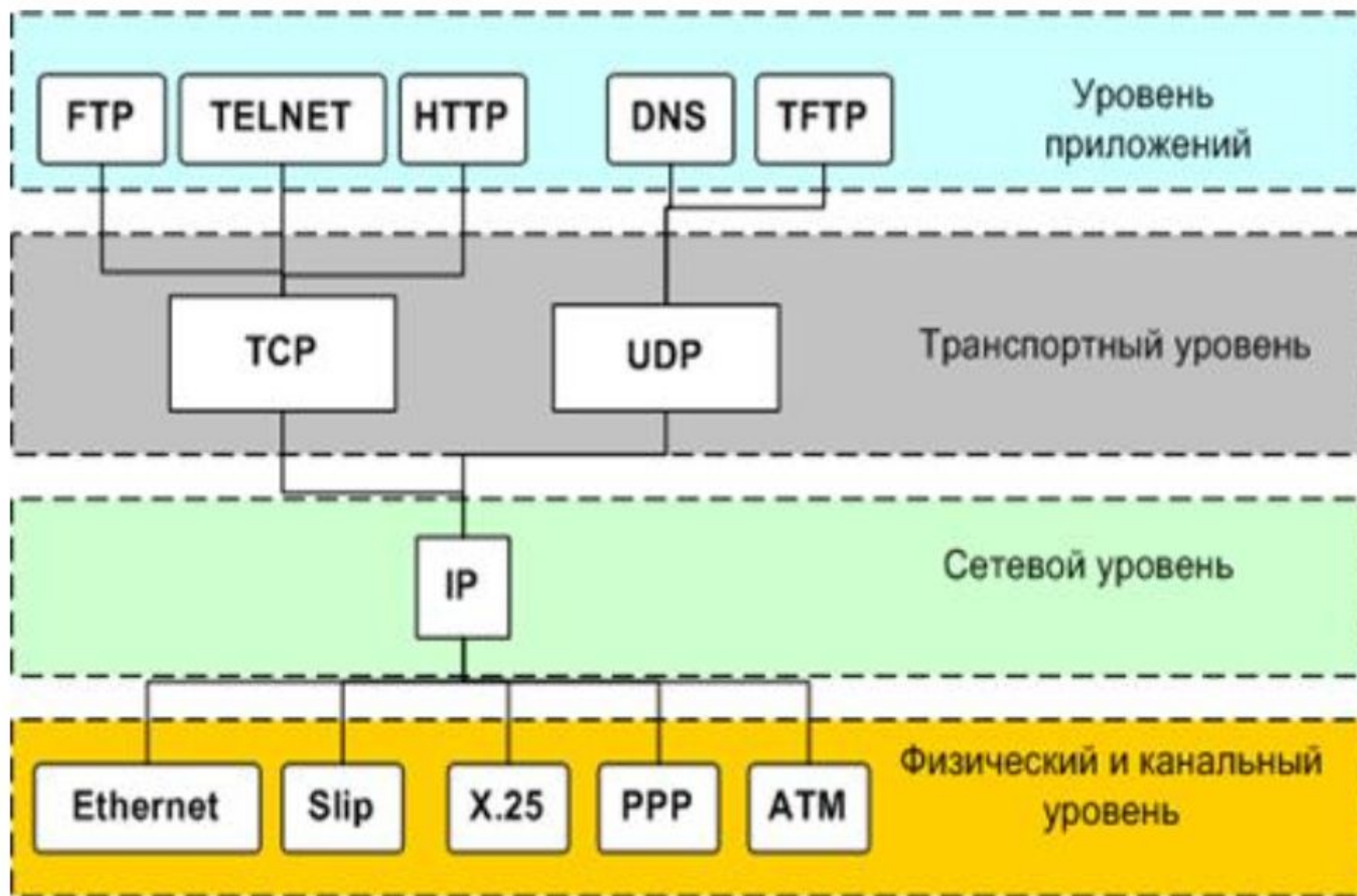
Протоколы прикладного уровня устанавливаются на хостах.

Прикладной уровень реализуется **программными системами**, построенными в архитектуре клиент-сервер.

В отличие от протоколов остальных трех уровней, протоколы прикладного уровня обрабатывают **логику приложений** и «не интересуются» способами передачи данных по сети.

Они обращаются к протоколам нижних уровней как к некоторому **набору инструментов**.

Так, клиентская часть протокола прикладного уровня для обмена сообщениями со своей серверной частью, установленной на отдаленном узле составной сети, **должна обратиться** с запросом к нижележащему транспортному уровню...



Наиболее известные протоколы каждого из уровней стека TCP/IP и взаимосвязь между ними.

Прикладной уровень стека ТСР/IP

Функции прикладного уровня обычно включают **идентификацию** партнеров по связи, определение наличия ресурса и синхронизацию связи.

При идентификации партнеров по связи прикладной уровень определяет **подлинность** и **наличие** партнеров по связи для прикладной программы, имеющей данные, готовые к передаче.

При определении **наличия ресурса** прикладной уровень должен принять решение, **существует ли** достаточное количество сетевых ресурсов для запрошенной связи.

При синхронизации связи весь обмен данными между прикладными программами **требует взаимодействия**, которое управлялось бы прикладным уровнем.

Прикладной уровень стека ТСР/ІР

Функции прикладного уровня:

- 1) **Идентификация и установление наличия** предполагаемых партнеров связи;
- 2) **Синхронизация** совместно работающих программ;
- 3) **Установление соотношения** по процедурам устранения ошибок;
- 4) **Управление целостностью** информации;
- 5) Протоколы прикладного уровня определяют, **имеется ли в наличии достаточно ресурсов** для предполагаемой связи;
- 6) Отвечает за то, чтобы **информация**, посылаемая из прикладного уровня одной системы, **была читаема** на прикладном уровне другой системы;

Прикладной уровень стека ТСР/ІР

7) При необходимости **осуществляет трансляцию** между множеством форматов представления информации путем использования общего формата и структур данных, а также **согласует синтаксис** передачи данных для прикладного уровня;

8) **Устанавливает и завершает сеансы** взаимодействия между прикладными задачами, **управляет этими сеансами, синхронизирует диалог** между объектами и управляет обменом информации между ними;

9) **Предоставляет средства** для отправки информации и уведомления об исключительных ситуациях передачи данных.

Прикладной уровень стека TCP/IP

Почему существуют два транспортных протокола TCP и UDP, а не один из них?

Дело в том, что они предоставляют **разные услуги** прикладным процессам.

Большинство прикладных программ **пользуются только одним** из них.

Вы можете **выбирать** тот протокол, который наилучшим образом соответствует вашим потребностям.

Если вам нужна **надёжная** доставка, то лучшим может быть TCP.

Если вам нужна доставка **датаграмм**, то лучше может быть UDP.

Прикладной уровень стека ТСР/IP

Если вам нужна эффективная доставка по **длинному** и **ненадежному** каналу передачи данных, то лучше может подойти протокол ТСР.

Если нужна **эффективность** на быстрых сетях с короткими соединениями, то лучшим может быть протокол UDP.

Если ваши потребности **не попадают** ни в одну из этих категорий, то выбор транспортного протокола **не ясен**.

Прикладной уровень стека ТСР/ІР

Однако **прикладные программы** могут устранять недостатки выбранного протокола.

Например, если вы выбрали UDP, а вам необходима **надежность**, то прикладная программа должна обеспечить надежность.

Если вы выбрали ТСР, а вам нужно **передавать записи**, то прикладная программа должна вставлять маркеры в поток байтов так, чтобы можно было различить записи.

Прикладной уровень стека TCP/IP

Прикладной уровень модели OSI **обеспечивает сопряжение** человека с сетевыми технологиями, что позволяет пользователям общаться между собой через сеть.

Другими словами, прикладной уровень **создает интерфейс** между приложениями конечных устройств при передаче сообщений по сети.

Прикладной уровень представляет собой комплекс программных средств, представленных в двух формах:

- в виде **приложений** (applications) и
- **программ служб сервиса** (services).

Прикладной уровень стека TCP/IP

Сопряжение человека с сетью обеспечивают **приложения**.

Широко известны такие приложения этого уровня, как **веб-браузеры** гипертекстовой информационной службы (World Wide Web – WWW), которые **позволяют** людям **готовить** сообщения для передачи по сети и **принимать** такие сообщения.

Наиболее известными веб-браузерами являются:

- Internet Explorer,
- Mozilla Firefox,
- Google Chrome,
- Opera.

Прикладной уровень стека TCP/IP

Программы служб сервиса **готовят данные** для передачи по сети, обеспечивая эффективное использование ресурсов сети.

Разные типы информации, такие как аудио-, видео-, текстовая информация, **требуют различных услуг.**

Это происходит потому, что всю эту разнотипную информацию необходимо передать **через общую сеть.**

Протоколы прикладного уровня **определяют правила** обмена данными между узлом источником информации и узлом назначения.

Прикладной уровень стека TCP/IP

Каждый вид приложений и сервиса использует **свои протоколы**, которые определяют стандарты и форматы передаваемых данных.

Протоколы и службы прикладного уровня обычно представлены соответствующими серверами.

Однако **сервер**, как отдельное устройство, может **объединять** функции нескольких служб сервиса.

Или наоборот, служба одного вида услуг может быть представлена **многими серверами** разного уровня.

Прикладной уровень стека TCP/IP

Наиболее распространенными протоколами и службами прикладного уровня являются:

- протоколы электронной почты:
 - Simple Mail Transfer Protocol – **SMTP**,
 - Post Office Protocol – **POP**,
 - Internet Messaging Access Protocol – **IMAP**;
- протокол передачи гипертекстовой информации, или веб-сервер (Hypertext Transfer Protocol – **HTTP**);

Прикладной уровень стека TCP/IP

- протокол передачи файлов (File Transfer Protocol – **FTP**);
- простой протокол передачи файлов (Trivial FTP – **TFTP**);
- система доменных имен (Domain Name System – **DNS**);
- протоколы удаленного доступа (**Telnet** и **SSH**), обеспечивающие виртуальное соединение с удаленными сетевыми устройствами;
- протокол динамического назначения адресов узлов (Dynamic Host Configuration Protocol – **DHCP**).

Прикладной уровень стека TCP/IP

Таким образом, приложения прикладного уровня обеспечивают интерфейс (сопряжение) **человека с сетью**.

Службы сервиса используют программные средства протоколов, чтобы **подготовить информацию** для передачи по сети.

Существуют две модели построения сети:

1. модель «**клиент-сервер**»;
2. модель соединения **равноправных узлов** сети (peer-to-peer).

Прикладной уровень стека TCP/IP

В сети **peer-to-peer** связанные через сеть конечные узлы разделяют общие ресурсы (принтеры, файлы) без выделенного сервера.

Каждое конечное устройство (peer) может функционировать либо как **сервер**, либо как **клиент**.

Компьютер может выполнять роль сервера для одного соединения и роль клиента для другого.

Прикладной уровень стека TCP/IP

Согласно модели «**клиент-сервер**» клиент запрашивает информацию, пересылая запрос выделенному серверу (**upload**), который в ответ на запрос посылает (**download**) файл, принимаемый клиентом.

Следовательно, клиент **инициирует** процесс обмена информацией в среде «клиент-сервер» и получает от сервера требуемую информацию.

Главным достоинством модели «клиент-сервер» является централизация управления сетью и **обеспечение безопасности**.

Протоколы передачи электронной ПОЧТЫ

Протоколы передачи электронной почты

При передаче электронной почты и взаимодействии почтовых серверов между собой используется простой протокол передачи почты (Simple Mail Transfer Protocol – **SMTP**).

Номер порта у него – **25** (по умолчанию). Этот порт не безопасен.

Порт **465** – порт для безопасного соединения.

Для получения клиентом сообщения с сервера используется протокол почтового отделения (Post Office Protocol – **POP**) с номером порта **110** (порт по умолчанию).

Этот порт не является безопасным.

Для безопасного соединения используется порт **995**.

Протоколы передачи электронной ПОЧТЫ

Либо возможно использование протокола доступа к сообщениям (Internet Messaging Access Protocol – **IMAP**).

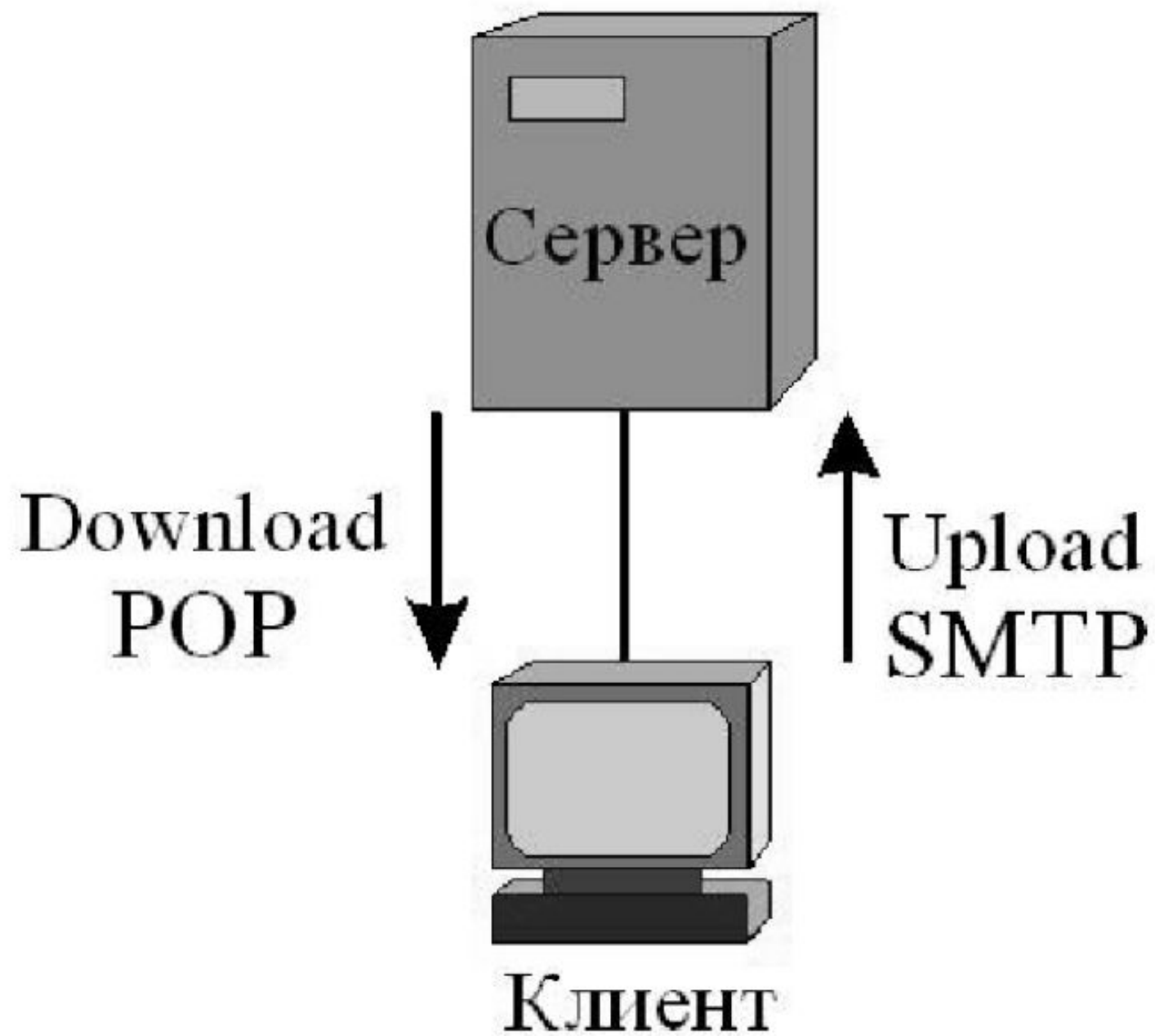
В то время как POP позволяет доступ к почте только с **одного приложения**, IMAP позволяет доступ из **множества клиентов**.

По этой причине, IMAP наиболее **адаптивен** в тех случаях, когда доступ к одному почтовому аккаунту необходим для **нескольких пользователей**.

По умолчанию, протокол IMAP использует следующие порты:

Порт **143**. Не безопасен.

Порт **993** – для безопасного соединения.



Протоколы передачи электронной ПОЧТЫ

На рисунке приведена модель «клиент-сервер» в службе электронной почты.

При пересылке почты от клиента на сервер используется протокол **SMTP**.

При этом происходит процесс **upload**.

Когда почтовый сервер получает сообщение, предназначенное для клиента, он хранит это сообщение и ждет, когда адресат назначения заберет свою почту.

Почтовые клиенты забирают сообщения (процесс **download**), используя один из сетевых протоколов.

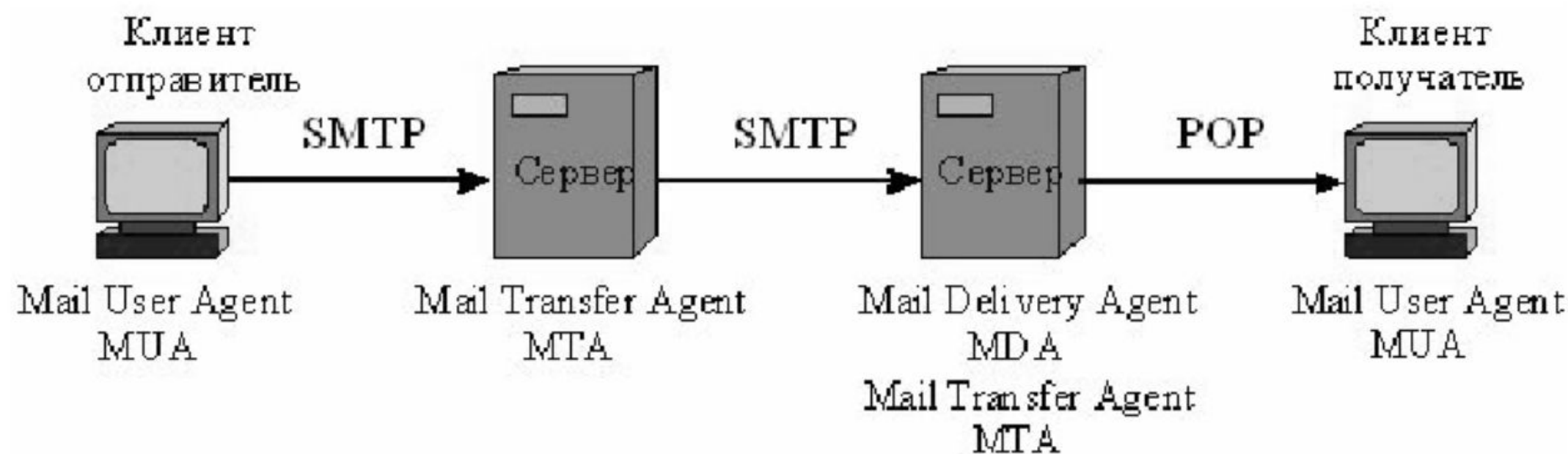
Протоколы передачи электронной ПОЧТЫ

Почтовые серверы общаются друг с другом, используя протокол **SMTP**, который транспортирует почтовые сообщения в текстовом формате, используя **TCP**.

Протокол **SMTP** характеризуется **низким** уровнем защиты информации, поэтому серверы предоставляют услуги только **пользователям своей сети**.

В процессе подготовки электронной почты люди применяют клиентское приложение, называемое **Агентом пользователя** (Mail User Agent – **MUA**).

Приложение **MUA** позволяет посылать сообщения и помещать полученные сообщения в почтовый ящик клиента.



Протоколы передачи электронной

При передаче сообщений **ПОИТЫ** между серверами используется **Агент передачи почты** (Mail Transfer Agent – **MTA**).

Агент передачи почты (MTA) получает сообщения от Агента пользователя (MUA) или от другого Агента передачи почты (MTA) и передает их по сети.

Агенты MTA применяют протокол SMTP для передачи электронной почты **между серверами**.

Если сообщение из сервера может быть отправлено сразу клиенту локальной сети, то подключается **Агент доставки почты** (Mail Delivery Agent – **MDA**).

Агент MDA **получает** прибывающую почту от MTA и **помещает** ее в соответствующие почтовые ящики пользователей, используя протокол POP.

Протокол HTTP

Протокол HTTP

Самым распространенным протоколом прикладного уровня в настоящее время является протокол передачи **гипертекстовой информации** (Hypertext Transfer Protocol – **HTTP**).

Он работает в сети Интернет.

Его основным приложением является веб-браузер.

Веб-браузер отображает данные на веб-страницах, используя:

- текст,
- графику,
- звук,
- видео.

Протокол HTTP

Веб-страницы создаются с применением языка разметки гипертекста Hypertext Markup Language (**HTML**).

Этот язык определяет местоположения для размещения текста, файлов и объектов, которые должны быть переданы от сервера по сети до веб-браузера.

Номер порта протокола HTTP – **80**.

Он функционирует совместно с протоколом транспортного уровня TCP.

Протокол HTTP

В ответ на запрос сервер посылает клиенту сети:

- текст,
- аудио- ,
- видео- ,
- графические файлы,

указанные в командах HTML.

Браузер клиента повторно собирает все файлы, чтобы создать изображение веб-страницы, которая представляется пользователю.

Протокол HTTP

Протокол HTTP характеризуется сравнительно невысоким уровнем безопасности, поскольку передаваемые по сети сообщения не зашифрованы.

Для **повышения уровня безопасности** передачи сообщений через Интернет был разработан протокол HTTP Secure (**HTTPS**).

В этом протоколе используется процесс **криптографирования** данных (encryption) и **аутентификации** (authentication), что существенно повышает уровень безопасности.

Номер порта протокола HTTPS – **443**.

Протоколы передачи файлов FTP и TFTP

Протоколы передачи файлов FTP и TFTP

Протокол передачи файлов (File Transfer Protocol – **FTP**) – служба, ориентированная на предварительное соединение (connection-oriented).

Она взаимодействует с протоколом транспортного уровня TCP.

Главная цель протокола FTP состоит в том, чтобы **передавать файлы** от одного компьютера другому или **копировать и перемещать файлы** от серверов клиентам и от клиентов серверам.

Протоколы передачи файлов FTP и

ТFTP
Это является главным **отличием** от протокола HTTP, который позволяет клиенту «скачивать» файлы с сервера, но не позволяет пересылать файлы на сервер.

Протокол передачи файлов FTP сначала устанавливает **соединение** между клиентом и сервером, используя команды запроса клиента и ответы сервера.

При этом номер порта – **21**.

Затем производится **обмен данными**, тогда используется номер порта **20**.

Протоколы передачи файлов FTP и

TFTP

Передача данных может производиться в режиме кода **ASCII** (American standard code for information interchange) или в двоичном коде.

ASCII – название таблицы (кодировки, набора), в которой некоторым распространённым печатным и непечатным символам сопоставлены числовые коды.

Эти режимы **определяют кодирование**, используемое для файла данных, которое в модели OSI является задачей **представительного (presentation) уровня**.

После завершения передачи файла соединение для передачи данных заканчивается автоматически.

Управление сеансом связи происходит на сеансовом (Session) уровне модели OSI.

Протоколы передачи файлов FTP и TFTP

Простой протокол передачи файлов (Trivial File Transfer Protocol – **TFTP**) — служба без установления соединения (connectionless).

Она работает совместно с протоколом транспортного уровня (User Datagram Protocol – **UDP**).

Протокол TFTP применяется на **маршрутизаторах**, чтобы передавать файлы конфигурации операционной системе Cisco IOS, а также для **передачи файлов** между системами, которые поддерживают TFTP.

Протоколы передачи файлов FTP и TFTP

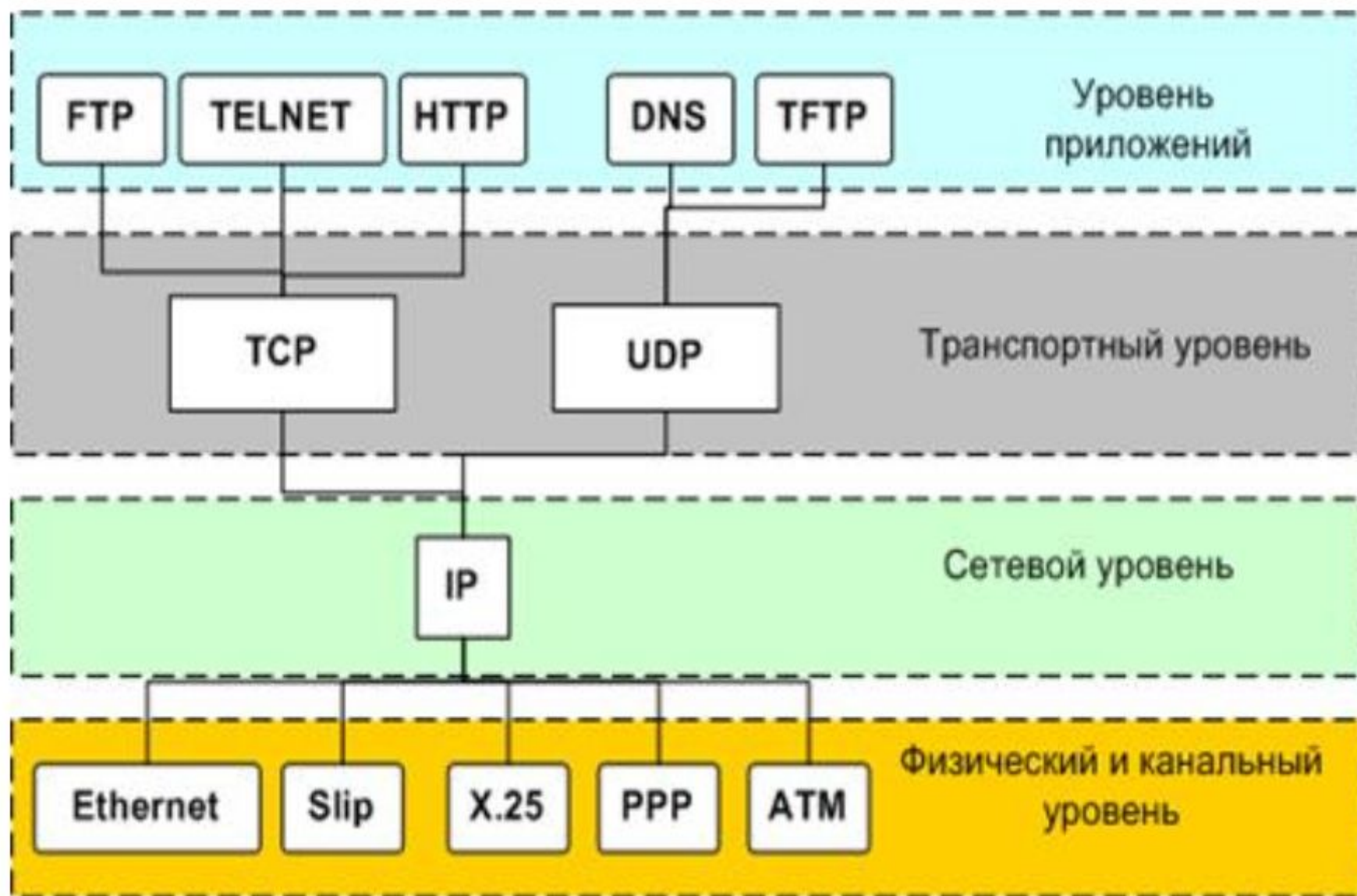
Протокол TFTP характеризует простота и малый объем программного обеспечения.

Он может читать или записывать файлы при соединении с сервером.

При этом он не ведёт списки и каталоги.

Поэтому протокол TFTP работает быстрее, чем протокол FTP.

Система доменных имен DNS



Наиболее известные протоколы каждого из уровней стека TCP/IP и взаимосвязь между ними.

Система доменных имен DNS

Система доменных имен (Domain Name System – **DNS**) используется в Интернете для того, чтобы **переводить** имена сайтов или доменов в числовые значения IP-адреса.

Людам легче запомнить доменное имя, например, ссылка:

<http://www.cisco.com>,

чем числовой адрес:

198.133.219.25.

Система доменных имен DNS

Кроме того, числовые адреса могут со временем **меняться**.

Например, в настоящее время указанный выше числовой адрес сайта ссылка:

<http://www.cisco.com>

изменен на **72.163.4.161**.

Поскольку в ряде случаев требуется знание числового адреса, хост может обратиться к DNS-серверу и по имени получить соответствующий адрес.

DNS использует распределенный набор серверов разного уровня иерархии, чтобы получить соответствие между именем и числовым адресом.

Система доменных имен DNS

Операционные системы компьютеров содержат утилиту `nslookup`, которая позволяет пользователю вручную запрашивать имя сервера и идентифицировать название хоста.

Когда клиент делает запрос, локальный сервер сначала проверяет собственные записи.

Если соответствующих пар «**имя-адрес**» у него нет, то он связывается с другими серверами DNS более высокого уровня иерархии.

Чтобы воспользоваться утилитой `nslookup`, нужно войти в режим командной строки:

Пуск → Программы → Стандартные → Командная строка

Система доменных имен DNS

Рассмотрим пример выполнения команды `nslookup`, которая позволяет пользователю вручную запросить адрес DNS-сервера.

1. По команде `nslookup` был получен адрес DNS-сервера – 10.0.6.10.

```
C:\Documents and Settings\User1>nslookup
```

```
*** Can't find server name for address 10.0.6.10: Non-existent domain
```

```
**** Can't find server name for address 10.0.5.10: Non-existent domain
```

```
*** Default servers are not available
```

```
Default Server: UnKnown
```

```
Address: 10.0.6.10
```

Система доменных имен DNS

2. Затем был произведен запрос адреса сайта **www.cisco.com**, IP-адрес которого – 23.23.26.219.

> **www.cisco.com**

Server: UnKnoun

Address: 10.0.6.10

Non-authoritative answer:

Name: origin-www.cisco.com

Address: **23.23.26.219**

Aliases: **www.cisco.com**, **www.cisco.com.akadns.net**
wwwds.cisco.com.edgekey.net

Командная строка - nslookup

C:\Users\101>nslookup

ТхЃтхЃ яю ъюыўрэш■: s05-vad01.corp.kait20.ru

Address: 192.168.10.250

> 23.23.26.219

ТхЃтхЃ: s05-vad01.corp.kait20.ru

Address: 192.168.10.250

ℒ : ec2-23-23-26-219.compute-1.amazonaws.com

Address: 23.23.26.219

> 72.163.4.161

ТхЃтхЃ: s05-vad01.corp.kait20.ru

Address: 192.168.10.250

ℒ : www1.cisco.com

Address: 72.163.4.161

> _

Система доменных имен DNS

3. Был запрошен адрес сайта ссылка:
<http://www.cisco.netacad.net> – 72.163.6.223.

> **cisco.netacad.net**

Server: UnKnoun

Address: 10.0.6.10

Non-authoritative answer:

Name: cisco.netacad.net

Address: 72.163.6.223

Служба прикладного уровня DNS характеризуется номером порта **53** и взаимодействует как с протоколом транспортного уровня TCP, так и с протоколом UDP.


```
Командная строка - nslookup
C:\Users\101>nslookup
тхѐтхѐ яю єьюѳрэш■: s05-vad01.corp.kait20.ru
Address: 192.168.10.250

> 23.23.26.219
тхѐтхѐ: s05-vad01.corp.kait20.ru
Address: 192.168.10.250

лб : ec2-23-23-26-219.compute-1.amazonaws.com
Address: 23.23.26.219

> 72.163.4.161
тхѐтхѐ: s05-vad01.corp.kait20.ru
Address: 192.168.10.250

лб : www1.cisco.com
Address: 72.163.4.161

> 72.163.6.223
тхѐтхѐ: s05-vad01.corp.kait20.ru
Address: 192.168.10.250

лб : cna-prod-nv.cisco.com
Address: 72.163.6.223

> -
```

Протокол динамического назначения адресов узлов DHCP

Протокол динамического назначения адресов узлов DNSP

Всем устройствам, которые обмениваются сообщениями через сеть Интернет, необходимы уникальные IP-адреса.

Эти адреса могут назначаться в статическом или динамическом режиме.

В статическом режиме адреса вручную назначает администратор при конфигурировании устройства.

Рекомендуется назначать **статические** IP-адреса на:

- маршрутизаторы,
- серверы,
- сетевые принтеры и другие устройства, адреса которых меняются редко.

Протокол динамического назначения адресов узлов DHCP

В то же время адреса рабочих станций могут изменяться достаточно часто.

Некоторые пользователи выходят в Интернет эпизодически, поэтому им нужны IP-адреса от случая к случаю.

Протокол динамического назначения адресов узлов (Dynamic Host Configuration Protocol – **DHCP**) позволяет автоматизировать процесс назначения IP-адресов рабочим станциям из диапазона, предоставленного администратору провайдером.

Протокол динамического назначения адресов узлов DHCP

Динамическое назначение адресов протоколом DHCP производится по запросу клиента на определенный **промежуток времени**, для продления которого пользователь должен периодически обращаться к серверу.

При освобождении IP-адреса возвращаются DHCP-серверу, который перераспределяет их.

При повторном запросе клиента, освободившего IP-адрес, сервер пытается назначить **ранее использовавшийся адрес**.

Помимо IP-адреса протокол DHCP предоставляет пользователю еще целый ряд параметров (маску подсети, шлюз по умолчанию, IP-адрес сервера DNS и

Контрольные вопросы

1. Что такое **DNS**? Для чего предназначена служба DNS? Что такое **домен**?
2. Что такое **маска** подсети? Зачем она нужна? Что называют **префиксом**?
3. Каково **максимальное количество** ip-адресов подсети с маской 255.255.255.0 и каково **максимальное количество** хостов подсети с этой маской? Почему?
4. Какова **маска** хоста подсети с ip-адресом 210.210.1.2/30? Сколько ip-адресов может быть в этой подсети? Как это определить?

Список литературы:

1. Компьютерные сети. Н.В. Максимов, И.И. Попов, 4-е издание, переработанное и дополненное, «Форум», Москва, 2015.
2. Компьютерные сети. Принципы, технологии, протоколы, В. Олифер, Н. Олифер (5-е издание), «Питер», Москва, Санкт-Петербург, 2016.
3. Компьютерные сети. Э. Таненбаум, 4-е издание, «Питер», Москва, Санкт-Петербург, 2003.
4. Построение сетей на базе коммутаторов и маршрутизаторов / Н.Н. Васин, Национальный Открытый Университет «ИНТУИТ», 2016.
5. Компьютерные сети : учебное пособие / А.В. Кузин, 3-е издание, издательство «Форум», Москва, 2017.
6. https://www.intuit.ru/studies/professional_retraining/942/courses/2/lecture/50?page=2
7. https://studwood.ru/1142167/informatika/prikladnoy_uroven_steka_tcpip

Благодарю за внимание!

Преподаватель: Солодухин Андрей Геннадьевич

Электронная почта: asoloduhin@kait20.ru