5. Протоколы и услуги сетей

- TCP/IP и основные протоколы (HTTP, FTP, SMTP, SSH, DHCP, DNS)

- Работа с службами и их настройка

Протоколы и услуги сети

# ТСР/IP и основные протоколы

*С эталонной моделью ТСР/IP вы ознакомились в первой теме нашего курса. Но в рамках этой темы рассмотрим некоторые важные аспекты, которые необходимы для дальнейшего понимания. (ССЫЛКА НА ТЕМУ 1)*

TCP/IP (Transmission Control Protocol/Internet Protocol) — это основной набор сетевых протоколов, который обеспечивает обмен данными в современных компьютерных сетях, включая Интернет.

TCP/IP основан на принципах модели OSI, но имеет свою упрощённую четырехуровневую структуру:

* **Прикладной уровень.** Отвечает за взаимодействие пользователем и приложениями с сетью, обеспечивая поддержку различных сетевых сервисов.
* **Транспортный уровень**. Обеспечивает надежную или быструю передачу данных между узлами сети с контролем целостности и порядка доставки.
* **Сетевой уровень**. Отвечает за логическую адресацию и маршрутизацию пакетов между различными сетями.
* **Канальный уровень**. Обеспечивает передачу кадров данных по физической среде и управление доступом к ней.

**Протоколы прикладного уровня:**

• FTP (File Transfer Protocol) — это протокол для передачи файлов между клиентом и сервером. Он позволяет пользователям загружать и скачивать файлы с удаленных серверов, поддерживает аутентификацию пользователей. Работает по умолчанию на портах 20 (для передачи данных) и 21 (для управления соединением).

• HTTP (Hyper Text Transfer Protocol)

HTTP — это основной протокол для передачи данных в интернете. Он используется для загрузки веб-страниц и работает по принципу "запрос-ответ". HTTP использует порт 80 по умолчанию и передает данные в открытом виде.

• HTTPS (HTTP Secure)

HTTPS — это защищенная версия HTTP, использующая шифрование через TLS (Transport Layer Security). Этот протокол обеспечивает безопасность передачи данных и используется для защиты конфиденциальной информации. HTTPS работает на порту 443 и предотвращает атаки типа "человек посередине".

• SMTP (Simple Mail Transfer Protocol) — это стандартный протокол для отправки электронной почты. Он обеспечивает передачу сообщений от клиента к серверу и между серверами. Работает на порту 25, поддерживает аутентификацию пользователей для повышения безопасности.

• SMTPS — это защищенная версия SMTP, которая использует шифрование. SMTPS обычно работает на портах 465 (для SMTPS с устаревшим SSL) или 587 (для современного шифрования STARTTLS).

• SNMP (Simple Network Management Protocol). Используется для управления и мониторинга сетевых устройств. Позволяет администраторам отслеживать состояние оборудования и получать информацию о производительности сети. Работает на порту 161.

• Telnet — это протокол для удаленного доступа к устройствам через командную строку. Позволяет пользователям управлять удаленными серверами, но не обеспечивает шифрование данных. Работает на порту 23.

• IMAP (Internet Message Access Protocol) — это протокол, который позволяет пользователям управлять своей почтой на сервере без ее загрузки на свое устройство. Поддерживает синхронизацию между несколькими устройствами, работает на порту 143.

• POP3 (Post Office Protocol version 3) — это еще один протокол для получения электронной почты, который загружает сообщения с сервера на устройство пользователя. В отличие от IMAP, обычно удаляет сообщения с сервера. Работает на порту 110.

• DHCP (Dynamic Host Configuration Protocol). Используется для автоматической настройки IP-адресов на устройствах в сети. Он позволяет динамически назначать IP-адреса клиентам и упрощает администрирование сети. Работает на порту 67 (сервер) и 68 (клиент).

• DNS (Domain Name System) — это система доменных имен, которая переводит удобные для человека доменные имена в IP-адреса. Позволяет пользователям легко находить веб-сайты. Работает на порту 53 и поддерживает как UDP (основной), так и TCP (для больших запросов).

• RTP (Real-time Transport Protocol) – используется для передачи аудио и видео в реальном времени, обеспечивая синхронизацию и доставку потоков данных. Обычно работает поверх UDP и использует динамические портовые диапазоны для передачи мультимедийного контента.

SSH (Secure Shell) — протокол, который обеспечивает безопасный доступ к удалённым системам по незащищённым сетям. Он широко используется для управления серверами, переноса файлов и выполнения удалённых команд. Обеспечивает шифрование данных и аутентификацию, что делает его более безопасным по сравнению с предыдущими протоколами, такими как Telnet.

**Протоколы транспортного уровня:**

• TCP (Transmission Control Protocol). Обеспечивает надежную передачу данных между устройствами, устанавливая соединение перед отправкой информации и гарантируя доставку пакетов в правильном порядке. TCP работает с портами, которые используются для идентификации приложений (например, порт 80 для HTTP, порт 443 для HTTPS).

• UDP (User Datagram Protocol) — это протокол без установления соединения, который не гарантирует доставку пакетов данных, но обеспечивает более быструю передачу информации. UDP также использует порты для адресации приложений (например, порт 53 для DNS).

**Сетевой уровень:**

• IP (Internet Protocol). Отвечает за адресацию и маршрутизацию пакетов данных в сети. Существует две версии: IPv4 и IPv6. Не использует порты, поскольку они являются атрибутом транспортного уровня.

• ICMP (Internet Control Message Protocol). Используется для передачи сообщений об ошибках и диагностики сетевых проблем. Например, команды ping используют ICMP для проверки доступности узлов в сети.

**Канальный уровень:**

• ARP (Address Resolution Protocol) отвечает за преобразование IP-адресов в физические адреса (MAC-адреса) в локальной сети, позволяя устройствам находить друг друга.

• RARP (Reverse Address Resolution Protocol) используется для определения IP-адреса устройства по его физическому адресу (MAC-адресу). Этот протокол менее распространен из-за использования DHCP.

**Работа со службами и их настройка**

Ниже приведены настройки для оборудования Cisco

Назначение IP адреса интерфейсу

* enable
* configure terminal
* interface GigabitEthernet0/0 #имя интерфейса
* ip address 192.168.0.1 255.255.255.0 #первый параметр – назначаемый адрес, второй – маска подсети
* no shutdown #включение интерфейса
* exit

Настройка DHCP сервера

* ip dhcp pool name #создается набор адресов с именем name
* default-router 192.168.0.1 #шлюз по умолчанию для клиентов
* network 192.168.0.0 255.255.255.0 #установка сетевого адреса и маски

Добавление DNS сервера

configure terminal

ip name-server 8.8.4.4 #добавляет публичный DNS сервер Google

exit

просмотр IP-адресов интерфейсов:

* show ip interface brief

Просмотр текущих маршрутов:

* show ip route

Просмотр настроек DNS:

* show hosts