SCS (Structured Cabling System, ISO 11801)

Structured Cabling System (SCS, структурированная кабельная система) – стандартизированная кабельная инфраструктура по ISO/IEC 11801 для унифицированного подключения телефонии, данных и систем управления в здании или кампусе. SCS обеспечивает гибкость и масштабируемость сети, поддержку разных сервисов и удобство обслуживания за счёт модульной структуры. В основе – магистральные и горизонтальные кабели, соединительные панели и розетки; используются медные кабели (витая пара Cat5e/Cat6/Cat6a/Cat7) и оптоволокно (типовые разъёмы RJ45 для витой пары, LC/SC для оптики).
Ключевые подсистемы SCS:

- **Entrance Facility** (точка ввода) – соединение с внешними линиями связи.
- **Equipment Room** (серверная/коммутационная) – размещение серверов и магистральных панелей.
- **Backbone Cabling** (магистраль) – магистральные связи между этажами и зданиями (обычно оптика или экранированная пара).
- **Telecommunications Room** (распределительное помещение) – узел перекрестной коммутации между магистральной и горизонтальной сетями.
- **Horizontal Cabling** (горизонтальная сеть) – кабели от распределительного шкафа к рабочим местам (чаще витая пара Cat6).
- **Work Area** (рабочая зона) – конечные точки сети: розетки и оборудование пользователя.
  Применение: SCS используется в офисах, дата-центрах и кампусных сетях для создания надёжной кабельной инфраструктуры.

LAN (Local Area Network)

Локальная сеть (LAN, Local Area Network) – сеть, объединяющая устройства (компьютеры, принтеры и т.д.) в пределах одного здания или кампуса. Цель LAN – обеспечить высокоскоростное взаимодействие и совместный доступ к ресурсам (файлы, принтеры, интернет) для устройств внутри сети. Основные технологии: Ethernet (IEEE 802.3) для проводного подключения и Wi-Fi (IEEE 802.11) для

беспроводной связи. Чаще используется «звезда»: устройства соединены через коммутаторы (switch), которые объединяют трафик, а маршрутизатор (router) обеспечивает выход в Интернет.
Основные компоненты LAN:

- **Сетевые карты (NIC)** – Ethernet- или Wi-Fi-адаптеры в каждом устройстве.
- **Кабели/среда** – витая пара Cat5e/Cat6, оптоволокно или Wi-Fi на 2.4/5/6 ГГц.
- **Сетевые устройства** – коммутаторы (switches) для обмена данными между узлами; маршрутизаторы (routers) для связи с другими сетями; точки доступа (access points) для Wi-Fi.
  LAN широко используется в офисах, домах и учебных учреждениях. Например, офисная LAN объединяет ПК и серверы через коммутаторы, а Wi-Fi роутер даёт доступ в Интернет. LAN обеспечивает высокую скорость (до 10 Гбит/с) и низкие задержки внутри локальной сети.

CAN (Campus Area Network)

Кампусная сеть (Campus Area Network, CAN) – частная сеть, объединяющая несколько локальных сетей (LAN) на территории кампуса (университет, офисный центр). Сеть принадлежит организации и охватывает несколько зданий. По размерам она больше обычной LAN, но меньше MAN/WAN. Назначение – объединить сети внутри кампуса для высокоскоростного обмена данными и централизованного администрирования (единая IP-схема, общие сервисы). Часто используется трёхуровневая архитектура (access/distribution/core) для масштабируемости и отказоустойчивости. Основные технологии: управляемые коммутаторы и маршрутизаторы предприятия; магистральные оптоволоконные/витопарные каналы 1–10 Гбит/с (Gigabit/10Gigabit Ethernet).
Характеристики CAN:

- Собственность организации, единое управление ИТ-отделом.
- Объединяет несколько LAN на одной территории.
- Высокопроизводительные магистрали (оптоволокно, агрегация каналов).
- Резервирование каналов и коммутаторов (STP, LACP) для надёжности.
- Поддержка общих служб (единая Wi-Fi, VoIP и др.).
  Примеры: университетские кампусы (связь корпусов и общежитий), офисные

кампусы (Googleplex, Microsoft). CAN объединяет сотни коммутаторов и тысячи устройств, обеспечивая низкие задержки и высокую пропускную способность внутри кампуса.

MAN (Metropolitan Area Network)

Метрополитенная сеть (MAN, Metropolitan Area Network) – сеть, охватывающая город или регион и соединяющая локальные сети (LAN) нескольких офисных зданий/комплексов в единую инфраструктуру. По масштабу MAN больше LAN, но меньше широкополосных сетей (WAN); типичный диапазон охвата – 5–50 км. Назначение – объединение офисов или кампусов в пределах города для высокоскоростного обмена данными и выхода в интернет. Сети MAN часто реализуются операторами и могут выступать как общедоступная инфраструктура (муниципальные сети) или быть частными для группы компаний. Архитектура может быть кольцевая или разветвлённая со связью по магистрали.
Технологии MAN:

- **Оптоволокно (Metro Ethernet)** – Gigabit/10Gigabit Ethernet с арендованными или темными оптическими магистралями.
- **Беспроводные соединения** – технологии фиксированной беспроводной связи (радиорелейные линии, mmWave) или частные 4G/5G сети.
- **Другие носители** – точка-точка Wi-Fi, оптические кольца, интеграция MPLS/SDN для управления трафиком.
  Пример применения: объединение офисов разных районов, городские Wi-Fi-проекты или корпоративные сети оператора связи. MAN обеспечивает высокую пропускную способность и низкие задержки на городской территории.

WAN (Wide Area Network)

Глобальная сеть (WAN, Wide Area Network) – сеть, протянувшаяся на большие географические расстояния (регионы, страны, континенты). WAN соединяет локальные сети в разных местах, обеспечивая передачу данных между удалёнными офисами и филиалами. Часто WAN строятся с помощью арендованных магистральных линий связи и сетей операторов (leased lines). Интернет является примером самой большой

WAN, но WAN также могут быть частными (VPN/MPLS-сеть компании) или гибридными (VPN через интернет).

Технологии WAN:

- **Магистральные линии:** глобальное оптоволокно (межконтинентальные кабели, SDH/SONET, DWDM).
- **Сетевые сервисы:** MPLS/VPN, Ethernet VPN, выделенные линии провайдеров (leased lines).
- **Протоколы WAN:** MPLS, Carrier Ethernet, PPP; ранее Frame Relay и ATM.
- **Дополнительные каналы:** спутниковые (VSAT), мобильные (4G/5G) для удалённой связи или резервирования.

Примеры: корпоративные WAN (между офисами MPLS/VPN), сети операторов и сам Интернет. WAN обеспечивает надёжную глобальную связность, позволяя компаниям работать по всему миру. Современные решения включают SD-WAN (overlay-сети поверх Интернета) для гибкого управления трафиком и повышения отказоустойчивости.

RIR (Regional Internet Registry)

Региональный интернет-регистратор (RIR, Regional Internet Registry) – организация, управляющая распределением и регистрацией сетевых номеров (IP-адресов и AS-номеров) на определённой территории. RIR получают большие блоки адресов от IANA и делегируют их локальным регистраторам (LIR) – провайдерам и организациям, следуя региональным политикам.

Основные RIR:

- **ARIN** (American Registry for Internet Numbers) – США, Канада и часть Карибского региона.
- **RIPE NCC** (Réseaux IP Européens) – Европа, Россия, Ближний Восток.
- **APNIC** (Asia Pacific Network Information Centre) – страны Азии и Океании.
- **LACNIC** (Latin America and Caribbean Network Information Centre) – Латинская Америка и Карибы.
- **AfriNIC** (African Network Information Centre) – Африка (континент).

RIR ведут базы данных WHOIS и участвуют в глобальных организациях (NRO, ICANN) для координации политик. Например, IP-адрес выдаётся только одному пользователю благодаря системе RIR. Политика распределения адресов формируется сообща сообществом, и каждый RIR действует в рамках региональных рекомендаций. Кроме адресов, RIR распределяют AS-номера (Autonomous System numbers) для автономных сетей.

AS (Autonomous System)

Автономная система (AS, Autonomous System) – совокупность маршрутизируемых IP-префиксов, управляемых единой организацией и демонстрирующих единую политику маршрутизации. Каждой AS присваивается уникальный ASN (Autonomous System Number) для использования в протоколе BGP (Border Gateway Protocol). Изначально ASN были 16-битными (до 65535); с 2007 года IANA начала выдавать 32-битные номера (до 4 294 967 295). AS позволяют организовать обмен маршрутами между сетями в Интернете.

- **Типы AS:** транзитная AS (несколько провайдеров, передаёт трафик между сетями) и конечная AS (stub, один провайдер).
- **Маршрутизация:** меж-AS обмениваются маршрутами по BGP, где используется атрибут AS_PATH для предотвращения петель и выбора лучшего пути. Внутри AS часто применяются IGP (OSPF, IS-IS) для внутренних маршрутов.

Примеры: у крупных провайдеров и сервисов есть свои AS. Например, у Google ASN=15169, у других CDN – свои AS. ASN выдаются RIR (через IANA) локальным регистрам (LIR). AS обеспечивает глобальную маршрутизацию в Интернете; внутри каждой AS используется IGP для внутренней маршрутизации.

BGP (Border Gateway Protocol)

BGP – внешний протокол маршрутизации (EGP) для обмена маршрутами между автономными системами в Интернете. Это протокол «путь-вектор»: решения принимаются на основе путей AS и политик администрирования. Каждый маршрутизатор BGP устанавливает TCP-сессию (порт 179) с соседями (peers) для обмена UPDATE-сообщениями о маршрутах. Внутри одной AS действует iBGP, а между AS – eBGP.

- **Маршрутные атрибуты BGP:** AS_PATH (препятствует петлям – если ASN уже в пути, маршрут отвергается), NEXT_HOP (следующий хоп), LOCAL_PREF (приоритет внутри AS), MED (медианный приоритет внешних путей), communities (метки политик).
- **Принцип работы:** BGP-пиры передают анонсы префиксов, формируя глобальную таблицу маршрутов. При выборе маршрута учитываются политика (LOCAL_PREF), минимальная длина AS_PATH и другие атрибуты.

Примеры: BGP позволяет провайдерам обмениваться маршрутами и организовать связи между дата-центрами. Крупные сети обмениваются тысячами префиксов; компании настраивают iBGP full mesh или route-reflectors для распространения маршрутов.

RPKI (Resource Public Key Infrastructure)

RPKI – инфраструктура открытых ключей для защиты маршрутизации BGP. RPKI связывает ресурсы (IP-префиксы и AS) с цифровыми сертификатами – цепочка доверия повторяет схему IANA→RIR→LIR. Операторы регистрируют ROA (Route Origin Authorization) – заявление о том, какой AS имеет право анонсировать указанный префикс. BGP-маршрутизаторы, поддерживающие RPKI, выполняют проверку объявлений (Route Origin Validation): если фактический AS-источник не совпадает с ROA, маршрут считается недействительным. Это позволяет предотвращать поглощение трафика (route hijacking) и другие атаки на BGP.

- **Внедрение:** каждый RIR предоставляет платформу RPKI в портале для участников, LIR может использовать её или свой CA.
- **Поддержка роутерами:** современные маршрутизаторы Cisco, Juniper и др. поддерживают RPKI и протокол RTR (RFC 6810) для загрузки проверенных ROA.

Пример: провайдер, получив некорректное BGP-объявление (не совпадающее с ROA), отклоняет его. В мире всё больше сетей вводят ROV-фильтрацию для повышения доверия к BGP.

IGP: Distance Vector / Link State

Протоколы внутренних маршрутов (Interior Gateway Protocol) предназначены для обмена информацией между маршрутизаторами внутри AS. IGP делятся на два класса:

- **Distance Vector (DV):** каждый маршрутизатор периодически рассылает соседям всю свою таблицу маршрутов. Пример: RIP/RIPv2 – считает сети по количеству прыжков (hop count). Недостатки: медленная сходимость и проблемы «зацикливания» маршрутов.
- **Link State (LS):** каждый узел распространяет сведения о состоянии своих интерфейсов; все строят общую карту сети и вычисляют кратчайшие пути (алгоритм Дейкстры). Примеры: OSPF и IS-IS – быстро сходятся и хорошо масштабируются.

Примеры использования: RIP применялся в небольших сетях, OSPF/IS-IS – в крупных корпоративных и провайдерских сетях. Современные IGP (например, EIGRP) комбинируют элементы DV и LS. IGP работает внутри AS и взаимодействует с внешними протоколами (EGP/BGP) для глобальной маршрутизации.

Router Control Plane / Data Plane

Современный маршрутизатор разделяет функции на контролирующую (control plane) и пересылочную (data/forwarding plane) части. Control plane отвечает за протоколы маршрутизации (BGP, OSPF, EIGRP и др.) и построение таблиц маршрутизации. Data plane фактически пересылает пакеты: он использует таблицу пересылки (FIB), созданную контролирующим процессором, и быстро перенаправляет пакеты на соответствующие интерфейсы. В большинстве маршрутизаторов control plane работает на центральном CPU, а data plane – в специализированном оборудовании (ASIC/NPU) для высокой скорости. Например, при получении BGP-обновления маршрутизатор обновляет таблицу маршрутов через control plane, а data plane затем быстро пересылает IP-пакеты на основании обновлённого FIB. Контрольные пакеты (например, ICMP с истечением TTL, служебные объявления) обычно обрабатываются control plane, тогда как остальной трафик переключается data plane. Такое разделение функций оптимизирует производительность и надёжность работы маршрутизатора.

SDN (Software-Defined Networking) overview

SDN – программно-определяемая сеть: архитектурный подход, отделяющий управление сетью (control plane) от физической инфраструктуры (data plane). Централизованный контроллер (сеть ОС) программно настраивает поведение

коммутаторов и маршрутизаторов через открытые интерфейсы (например, протокол OpenFlow). Это даёт гибкость и автоматизацию: администратор задаёт правила через API, а контроллер распространяет их по устройствам.

Основные компоненты SDN:

- **Application Layer:** сетевые приложения (QoS, балансировка нагрузки и др.) используют northbound API контроллера.
- **Control Layer:** централизованный контроллер (сетевой ОС) управляет трафиком и ресурсами, получает запросы от приложений и обновляет конфигурацию устройств.
- **Infrastructure Layer:** физические или виртуальные коммутаторы/маршрутизаторы, выполняющие пересылку по правилам контроллера (flow tables).
- **Протоколы:** OpenFlow и другие southbound API (NETCONF, gNMI) используются для управления устройствами.

Примеры: центры обработки данных (Google B4, Amazon Cloud WAN) используют SDN для управления глобальными соединениями; SD-WAN позволяет объединить филиалы через Интернет; современные дата-центры применяют SDN (VXLAN/EVPN) для гибкой виртуализации сети. SDN обеспечивает программное управление сетью, централизованный мониторинг и быструю адаптацию потоков.

WWW (World Wide Web)

Всемирная паутина (WWW, World Wide Web) – система взаимосвязанных гипертекстовых документов, доступных через Интернет по протоколу HTTP. WWW был разработан Тимом Бернерсом-Ли в 1989 году. Документы формата HTML содержат текст, изображения, видео и скрипты, а также гиперссылки (URL) для навигации.

Ключевые компоненты Web:

- **HTML/CSS/JavaScript:** языки разметки и сценарии для создания веб-страниц и приложений (содержат гипертекст и мультимедиа).
- **Web-серверы:** программы (например, Apache, Nginx), которые отвечают на HTTP-запросы и передают веб-страницы.
- **Браузеры:** клиенты (Chrome, Firefox, Edge), посылающие HTTP(S)-запросы к серверам и отображающие полученный контент.

- **Протоколы HTTP/HTTPS:** правила обмена данными по TCP (обычно порты 80/443) между браузером и сервером.
- **URL и DNS:** глобальные идентификаторы ресурсов. URL (например, `http://example.com/page`) указывает расположение ресурса; DNS переводит доменное имя в IP-адрес сервера.

Примеры: веб-сайты и веб-приложения любого назначения – от информационных (Wikipedia, новостные порталы) до сложных сервисов (Google Docs, социальные сети). WWW обеспечивает удобный доступ к данным через браузер, делая Интернет понятным для пользователей.

DNS (Domain Name System)

DNS – иерархическая распределённая система доменных имён, переводящая человекочитаемые имена (например, `example.com`) в IP-адреса компьютеров и сервисов. DNS организован по уровням: корневые серверы, зоны верхнего уровня (.com, .ru и др.), авторитетные серверы доменных зон и локальные резолверы. Система отказоустойчива: управление делегируется локальным NS-серверам, что обеспечивает распределённую архитектуру. Когда приложение запрашивает домен, локальный резолвер посылает запрос к DNS-серверам (обычно по UDP порт 53), постепенно получая нужную запись (A/AAAA или другую).

Основные типы записей:

- **A/AAAA:** связывают доменное имя с IPv4/IPv6-адресом.
- **CNAME:** задаёт псевдоним (alias) для другого домена.
- **MX:** указывает почтовые серверы домена.
- **NS:** определяет авторитетные DNS-серверы для зоны.
- **TXT:** служебная текстовая информация (например, SPF-записи для почты).

DNS необходим для работы Интернета: браузеры, почтовые клиенты и другие сервисы используют DNS для определения IP-адресов по именам. DNS-записи имеют TTL (time-to-live) – после заданного времени они кэшируются заново, что ускоряет последующие запросы. Разрешение имен может выполняться рекурсивно (через локальный резолвер) или итеративно (от корневого сервера к нужной зоне). В итоге DNS превращает сложную иерархию адресов в понятные человеку доменные имена.

DNSSEC (DNS Security Extensions)

DNSSEC – набор расширений DNS, вводящий криптографическую подпись для защиты ответов DNS от подмены. С помощью DNSSEC авторитетный сервер подписывает записи зоны, добавляя цифровые подписи (RRSIG) с приватным ключом. Публичный ключ зоны (DNSKEY) доступен в DNS, а цепочка доверия организована через делегирующие записи DS в родительской зоне.

Механизм работы: резолвер, получая ответ с RRSIG, проверяет подпись с помощью DNSKEY и DS – если проверка не проходит, ответ отвергается. DNSSEC не шифрует данные (не обеспечивает конфиденциальность), но гарантирует их целостность и подлинность. Если ответ был изменён злоумышленником, подпись не пройдёт проверку, и такой ответ не будет использован.

Компоненты DNSSEC:

- **DNSKEY:** публичный ключ зоны (записывается в DNS).
- **RRSIG:** цифровые подписи для каждого RRset, созданные приватным ключом.
- **DS (Delegation Signer):** «хеш» публичного ключа дочерней зоны, публикуемый в родительской зоне.

DNSSEC широко применяется для защиты критичных доменов: корневой домен и многие TLD подписаны. Если DNS-ответ был изменён, DNSSEC-валидатор обнаружит несоответствие подписи и отклонит фальшивку. Это предотвращает типичные атаки DNS-подмены и повышает надёжность работы сервисов.

HA Cluster (High Availability)

Кластер высокой доступности – группа независимых компьютеров (узлов), работающих вместе, чтобы обеспечить непрерывность сервиса даже при сбое одного из них. Узлы в кластере постоянно отслеживают друг друга (heartbeat). Если основной узел выходит из строя, происходит переключение (failover) на резервный, и сервис продолжает работать без значительных простоев. Данные между узлами обычно синхронизируются или разделяются (через общий диск), чтобы каждый узел мог предоставить одинаковую информацию.

Кластеры HA могут быть построены по схеме active-passive (один активен, другой в резерве) или active-active (оба активны и балансируют нагрузку). Технологии HA включают программное обеспечение кластеризации (например, Pacemaker+Corosync в Linux, Windows Failover Clustering), виртуальные IP-адреса и выделенные каналы heartbeat для детектирования сбоев. Дополнительные механизмы (мультиплексирование каналов, дублирование оборудования, STONITH) помогают избежать «разделения мозга» и обеспечить непрерывную работу приложений.

Примеры: отказоустойчивые кластеры баз данных (MySQL, PostgreSQL), веб-серверов, почтовых и других критичных сервисов. Кластеры HA применяются в финансовых сервисах, дата-центрах и т.д., где недопустимы простои. Используемые решения достигают очень высокого времени безотказной работы (например, 99.99% и выше) за счёт избыточности на уровне сети, питания и узлов.

Mobile networks (Cellular networks)

Мобильная (сотовая) сеть – радиосеть, обеспечивающая беспроводную связь мобильных устройств через базовые станции оператора. Территория разбивается на соты (ячейки), каждая из которых покрывается определённым частотным диапазоном. При движении абонента между сотами происходит бесшовная передача (handover) связи на ближайшую станцию. Сотовые сети используют различные методы множественного доступа: FDMA/TDMA в 2G, CDMA в 3G, OFDMA в 4G/5G и современные MIMO/beamforming для повышения ёмкости.

Ключевые технологии:

- **Поколения связи:** 2G (GSM/CDMA – голос, SMS), 3G (UMTS/HSPA – мобильный интернет), 4G (LTE – высокоскоростной IP-трафик, VoLTE) и 5G (5G NR – сверхнизкая задержка, высокая пропускная способность, массовые IoT).
- **Сотовая структура:** соты связаны с ядром сети (MSC в 2G/3G, EPC в 4G, 5G Core в 5G). У каждого абонента есть уникальный IMSI, а аутентификация выполняется через SIM/USIM-карту.
- **Радиоинтерфейс:** применяется планирование частот и мощностей, используется распределение нагрузки по сотам. В 5G появились миллиметровые диапазоны и network slicing для создания виртуальных сетей под различные приложения.

- **Применение:** мобильный интернет (веб, видео, приложения), голосовые вызовы (через VoLTE/VoNR), обмен SMS, а также IoT-сервисы (NB-IoT, LTE-M) для «интернета вещей».

Примеры: операторы мобильной связи (МТС, Vodafone, Verizon) строят покрытие городов и регионов; устройства автоматически подключаются к ближайшей соте. Современные 5G-сети обеспечивают высокую плотность устройств и крайне низкие задержки, что критично для критичных приложений (AR/VR, автономные автомобили, массовые сенсоры).

Источники: Публичные документы и стандарты (ISO/IEC 11801, IEEE 802.x, IETF RFC, спецификации 3GPP и др.).