ЧАСТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕДЛЬНОЕ УЧРЕЖДЕНИЕ «СЕВЕРО-КАВКАЗСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

ЛЕКЦИЯ 1. ТЕМА 1.1. ЭКСПЛУАТАЦИЯ ТЕХНИЧЕСКИХ СРЕДСТВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

1. Физические аспекты эксплуатации. Физическое вмешательство в инфраструктуру сети

Эксплуатация сетевой инфраструктуры предполагает поддержание работоспособности физических компонентов, обеспечивающих передачу данных. К физическим аспектам относят: контроль температурно-влажностного режима в серверных и кроссовых, обеспечение бесперебойного электропитания, защиту от электромагнитных помех, контроль доступа к оборудованию.

Физическое вмешательство в инфраструктуру — это любые действия, затрагивающие кабельные трассы, коммутационные панели, активное оборудование: монтаж/демонтаж кабелей, замена модулей, установка новых устройств, перекоммутация портов. Такие вмешательства несут риск нарушения связности, поэтому регламентируются процедурами Change Management.

Алгоритм действий при физическом вмешательстве:

1. Идентифицировать цель вмешательства (замена устройства, добавление порта, устранение неисправности).
2. Проверить актуальность физической и логической топологии, наличие свободных портов и ресурсов.
3. Оценить влияние на сервисы (время простоя, критичность, необходимость резервирования).
4. Оформить заявку на изменение (Change Request) с указанием даты, времени, ответственных, плана и плана отката.
5. Выполнить работы в согласованное окно обслуживания.
6. Провести проверку связности и основных метрик (ping, пропускная способность, ошибки на портах).
7. Зафиксировать изменения в документации и системах учёта активов.
8. Закрыть заявку и зафиксировать результаты.

2. Активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки

Активное сетевое оборудование содержит электронные схемы, обрабатывающие и перенаправляющие трафик: коммутаторы, маршрутизаторы, межсетевые экраны, точки доступа. Пассивное оборудование не обрабатывает сигналы, а лишь обеспечивает их передачу: кабели, патч-панели, коммутационные шкафы, кабельные каналы, розетки, коннекторы.

Кабельные каналы защищают кабели от механических повреждений и электромагнитных наводок. Кабель (чаще всего витая пара категории 5e/6/6A или оптоволокно) определяет пропускную способность и допустимую длину сегмента. Патч-панели обеспечивают удобную коммутацию: кабель от розетки заводится на панель, далее соединение выполняется патч-кордами. Розетки — конечные точки подключения пользовательских устройств.

Алгоритм проверки состояния пассивной инфраструктуры:

1. Визуальный осмотр кабельных каналов и розеток на предмет повреждений.
2. Проверка маркировки и соответствия схеме коммутации.
3. Тестирование кабельных сегментов тестером (длина, целостность, перекрестные наводки, затухание).
4. Проверка плотности контактов и отсутствия окисления.
5. Фиксация несоответствий и планирование устранения.

3. Полоса пропускания, паразитная нагрузка

Полоса пропускания (bandwidth) — максимальная скорость передачи данных по каналу связи, измеряется в бит/с. Эффективная пропускная способность зависит от качества среды передачи, уровня помех и эффективности протоколов.

Паразитная нагрузка (overhead) — служебный трафик, не относящийся к полезной нагрузке пользователя: заголовки пакетов, служебные протоколы (ARP, DHCP, STP, LLDP), повторные передачи при потерях, шифрование. В Ethernet паразитная нагрузка может составлять 10–30% от номинальной полосы в зависимости от размера кадров и типа трафика.

Для снижения паразитной нагрузки применяют: сегментацию сети (VLAN), ограничение широковещательного трафика, оптимизацию MTU, использование QoS для приоритизации полезного трафика.

4. Расширяемость сети. Масштабируемость сети. Добавление отдельных элементов сети (пользователей, компьютеров, приложений, служб)

Расширяемость — возможность добавления новых компонентов без полной замены существующей инфраструктуры. Масштабируемость — способность сети сохранять производительность и надёжность при увеличении нагрузки и количества узлов.

Добавление пользователей и устройств требует учёта: количества портов, доступной полосы пропускания, политик безопасности (ACL, VLAN, аутентификация), нагрузки на DHCP/DNS/NTP. Добавление приложений и служб требует выделения подсетей, настройки маршрутизации, балансировки нагрузки, резервирования.

Алгоритм добавления нового сегмента сети:

1. Определить требования к трафику (объём, тип, задержки, надёжность).
2. Выбрать топологию и уровень коммутации (L2/L3), выделить диапазон IP-адресов.
3. Спроектировать схему коммутации и маршрутизации, учесть отказоустойчивость.
4. Подготовить оборудование (настройка VLAN, STP/RSTP, агрегация каналов).
5. Настроить сервисы (DHCP, DNS, NTP, мониторинг).
6. Протестировать связность, задержку, пропускную способность.
7. Обновить документацию и схемы.

5. Наращивание длины сегментов сети; замена существующей аппаратуры

Наращивание длины сегментов ограничено физическими характеристиками среды передачи. Для витой пары максимальная длина сегмента — 100 м. Для увеличения протяжённости применяют промежуточные коммутаторы (каскадирование), медиаконвертеры (медь–оптика), SFP-модули, оптические линии.

Замена аппаратуры проводится при устаревании, выходе из строя, несоответствии требованиям производительности или безопасности. При замене учитывают совместимость, пропускную способность, поддержку необходимых протоколов, возможность интеграции с системами мониторинга.

Алгоритм замены сетевого устройства:

1. Собрать конфигурацию текущего устройства (бэкап).
2. Подготовить конфигурацию нового устройства (шаблоны, скрипты).
3. Проверить совместимость кабелей, SFP, питания.
4. Выполнить замену в окно обслуживания, подключить кабели, включить питание.
5. Проверить базовые функции (L1/L2/L3, связность).
6. Проверить расширенные функции (маршрутизация, ACL, QoS, STP).

7. Протестировать производительность и отказоустойчивость (failover, агрегация).
8. Обновить документацию, инвентаризацию, мониторинг.

6. Увеличение количества узлов сети; увеличение протяжённости связей между объектами сети

Увеличение количества узлов требует учёта масштабируемости L2-доменов (ограничение размера широковещательного домена), планирования IP-адресации, обеспечения отказоустойчивости. Рост протяжённости связей между объектами решается с помощью оптических линий, радиорелейных каналов, VPN.

При проектировании учитывают: задержки (latency), потери пакетов, синхронизацию времени, требования к шифрованию. Для распределённых сетей применяют иерархическую топологию (ядро–распределение–доступ), динамическую маршрутизацию (OSPF, BGP), резервирование каналов.

7. Техническая и проектная документация. Паспорт технических устройств

Техническая и проектная документация включает: схемы физической и логической топологии, планы кабельных трасс, спецификации оборудования, IP-план, политики безопасности, процедуры эксплуатации.

Паспорт технического устройства содержит: наименование и модель, серийный номер, MAC-адрес, версию ПО, конфигурацию, дату ввода в эксплуатацию, гарантийные данные, историю обслуживания и замен.

Ведение документации обеспечивает прозрачность, ускоряет устранение инцидентов, упрощает аудит и планирование модернизации.

8. Физическая карта всей сети; логическая топология компьютерной сети

Физическая карта сети отражает расположение оборудования, кабельных трасс, розеток, шкафов, источников питания. Логическая топология описывает пути передачи данных: VLAN, подсети, маршруты, политики маршрутизации и фильтрации.

Совмещение физической и логической топологий позволяет быстро локализовать неисправности, планировать изменения и оценивать риски. Для актуализации используют системы управления конфигурациями (CMDB), инструменты сетевого моделирования, автоматическую инвентаризацию.

9. Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры

Регламенты технических осмотров классифицируют по периодичности (ежедневные, еженедельные, ежемесячные, квартальные, годовые) и по содержанию (визуальные, функциональные, нагрузочные).

Типовой регламент включает: визуальный осмотр, проверку индикации, контроль температуры и питания, тестирование связности, анализ журналов событий, проверку резервных копий, обновление ПО.

10. Проверка объектов сетевой инфраструктуры и профилактические работы

Проверка включает: контроль состояния портов (ошибки, коллизии, отброшенные пакеты), анализ журналов (ошибки, события безопасности), тестирование резервирования, проверку актуальности ПО и лицензий.

Профилактические работы: очистка оборудования от пыли, проверка креплений и заземления, контроль АКБ ИБП, обновление микропрограмм, ротация ключей и паролей, тестирование процедур восстановления.

Алгоритм профилактического осмотра коммутатора:

1. Проверить индикаторы питания и портов.
2. Собрать статистику по ошибкам и отброшенным пакетам.
3. Проверить температуру и нагрузку CPU/памяти.
4. Проверить журналы событий на критические ошибки.
5. Проверить состояние резервных конфигураций и бэкапов.
6. Проверить наличие обновлений ПО.
7. Зафиксировать результаты и спланировать доработки.

11. Проведение регулярного резервирования. Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удалённого оповещения о неполадках

Регулярное резервирование включает: бэкапы конфигураций, образов ПО, баз данных, журналов. Резервные копии хранят на отдельном носителе, проверяют возможность восстановления.

Обслуживание физических компонентов: чистка, проверка креплений, контроль питания и охлаждения. Контроль состояния аппаратного обеспечения — мониторинг температуры, напряжения, скорости вентиляторов, состояния дисков и блоков питания.

Удалённое оповещение организуют через SNMP-трапы, syslog, интеграцию с системами мониторинга (Zabbix, Prometheus, Grafana), настройку алертов по пороговым значениям.

12. Программное обеспечение мониторинга компьютерных сетей и сетевых устройств

ПО мониторинга собирает метрики, визуализирует состояние, формирует алерты, хранит историю. Примеры: Zabbix, Nagios, PRTG, SolarWinds, Grafana.

Функционал: сбор метрик по SNMP/WMI/API, построение графиков, настройка порогов и алертов, интеграция с ITSM, автоматическое обнаружение устройств, отчётность.

13. Протокол SNMP, его характеристики, формат сообщений, набор услуг

SNMP (Simple Network Management Protocol) — протокол управления сетевыми устройствами. Версии: SNMPv1, SNMPv2c, SNMPv3 (с улучшенной безопасностью).

Характеристики: работает поверх UDP, использует MIB (Management Information Base) для описания управляемых объектов, поддерживает операции GET, SET, WALK, TRAP, INFORM.

Формат сообщений: PDU (Protocol Data Unit) содержит тип операции, OID (Object Identifier), значения. Трапы (TRAP/INFORM) — уведомления от агента к менеджеру.

Набор услуг: сбор статистики, управление конфигурацией, мониторинг состояния, уведомления об ошибках, сбор инвентарных данных.

14. Задачи управления: анализ производительности и надёжности сети

Анализ производительности включает: измерение пропускной способности, задержек, потерь пакетов, загрузки CPU/памяти устройств, анализ очередей и буферов.

Анализ надёжности: оценка времени простоя, частоты отказов, эффективности механизмов резервирования, тестирования отказоустойчивости, анализа журналов ошибок.

Инструменты: NetFlow/sFlow, IP SLA, синтетические тесты, системы мониторинга. Результаты используют для оптимизации, планирования мощностей, улучшения SLA.

15. Оборудование для диагностики и сертификации кабельных систем. Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры

Оборудование для диагностики:

- Кабельные тестеры — проверяют целостность, длину, перекрестные помехи, затухание.
- Сертификационные приборы — измеряют параметры в соответствии со стандартами (TIA/ISO), выдают отчёты о соответствии категории кабеля.
- Сетевые мониторы — анализируют трафик, выявляют аномалии, помогают локализовать проблемы.
- Кабельные сканеры — определяют местоположение повреждений, коротких замыканий, обрывов.

Применение: при вводе в эксплуатацию, модернизации, устранении неисправностей, аудите инфраструктуры.