1 часть
Спроектируем сеть для организации, обрабатывающей персональные данные (ПДн). Ключевые принципы: **сегментация**, **контроль доступа**, **логгирование** и **изоляция**.

Ключевые допущения:
*   **ЦОД:** Серверы размещены в основном ЦОДе.
*   **Пользователи:** Сотрудники работают из офисного сегмента.
*   **Интернет:** Выход осуществляется через центральный маршрутизатор.
*   **Хранилище ПДн:** Выделенный, физически или логически строго изолированный сегмент.

---

1. Детализация VLAN и политик

Таблица VLAN

ID VLAN	Имя VLAN	Назначение	Подсеть	Шлюз по умолчанию
10	`MGMT`	Управление сетевым оборудованием (коммутаторы, маршрутизаторы). Доступ строго ограничен.	`10.10.10.0/24`	`10.10.10.1`
20	`USERS_CORP`	Пользовательские рабочие станции сотрудников.	`10.20.20.0/23`	`10.20.20.1`
30	`SERVERS_CORP`	Корпоративные серверы (ERP, CRM, файловые серверы), не обрабатывающие ПДн.	`10.30.30.0/24`	`10.30.30.1`
40	`SERVERS_DMZ`	Публичные серверы (веб-портал, VPN-шлюз для удаленных сотрудников).	`172.16.40.0/24`	`172.16.40.1`
50	`SERVERS_PDN`	**Серверы обработки ПДн (прикладной уровень).** Доступ только из VLAN 60 и для администраторов.	`10.50.50.0/24`	`10.50.50.1`
60	`STORAGE_PDN`	**Изолированное хранилище ПДн (СУБД, системы хранения).** Доступ ТОЛЬКО из VLAN 50. Запрещен любой исходящий трафик.	`10.60.60.0/24`	`10.60.60.1`
99	`BLACKHOLE`	"Сегмент-ловушка" для неавторизованного трафика. Весь трафик здесь отбрасывается и логгируется.	`169.254.99.0/24`	-
100	`INFRASTRUCTURE`	Для транзитных линков между маршрутизаторами и коммутаторами (P2P links, Loopbacks).	`192.168.0.0/16`	-

---

Матрица доступа и правила (Zone-Based Firewall & ACL)

Концепция ZBFW: мы определяем "Зоны" (Zones) и политики между ними.

1. Определение Зон (Zones):
*   **Zone_PDN:** VLAN 50, 60 (критичные сегменты ПДн).
*   **Zone_Internal:** VLAN 20, 30 (пользователи и корпоративные серверы).
*   **Zone_DMZ:** VLAN 40 (демилитаризованная зона).
*   **Zone_Internet:** Внешний интерфейс маршрутизатора.
*   **Zone_MGMT:** VLAN 10 (управление).

2. Матрица доступа в виде правил ZBFW:

Источник	Назначение	Уровень	Разрешить?	Ограничения (Правила)	Логгирование
Zone_Internal	**Zone_PDN**	**L3**	**Нет**	По умолчанию запрещено.	**Full**
Примечание:				*Исключение: Специальные правила для конкретных пользователей (VLAN 20, IP/группа) к конкретным сервисам на SERVERS_PDN (VLAN 50, порт). Создается отдельное правило "Permit".*	
Zone_PDN	**Zone_Internal**	**L3**	**Нет**	Запрещено. Сервера ПДн не должны инициировать соединения внутрь корпоративной сети.	**Full**
Zone_PDN (VLAN 50)	**Zone_PDN (VLAN 60)**	**L3**	**Да**	**Правило:** `permit tcp <VLAN50_Subnet> <VLAN60_Subnet> eq 1433 5432 1521` (Разрешить только служебные порты СУБД от серверов приложений к хранилищу). **Deny Any** для всего остального трафика между этими подсетями.	**Full**
Zone_PDN (VLAN 60)	**Любая**	**L3**	**Нет**	**Правило:** `deny ip any any`. Сервера хранения ПДн не могут устанавливать исходящие соединения никуда.	**Full**
Zone_Internal	**Zone_DMZ**	**L3**	**Да**	**Правило:** `permit tcp <USERS_Subnet> <DMZ_Web_Server> eq 80 443` (Доступ пользователей к корпоративному порталу).	**Matches**
Zone_DMZ	**Zone_Internal**	**L3**	**Нет**	Запрещено.	**Full**
Zone_DMZ (VPN)	**Zone_Internal**	**L3**	**Да**	**Правило:** `permit ip <VPN_Pool> <USERS_CORP_Subnet>`, `permit ip <VPN_Pool> <SERVERS_CORP_Subnet>`. Удаленные сотрудники получают доступ к внутренним ресурсам после строгой аутентификации.	**Matches**
Zone_Internet	**Zone_DMZ**	**L3**	**Да**	**Правило:** `permit tcp any <DMZ_Web_Server> eq 80 443` (Публичный доступ к сайту).	**Matches**
Любая	**Zone_MGMT**	**L3**	**Нет**	По умолчанию запрещено.	**Full**
Примечание:				*Исключение: Разрешен доступ только с Jump Host в VLAN 30 по SSH (tcp/22) и HTTPS (tcp/443) для администраторов. Создается	

отдельное правило.* |
|
| **Любая** | **Любая** | **L3** | **-** | Неявный запрет. Весь трафик, не подпадающий под разрешающие правила, отбрасывается и направляется в `BLACKHOLE` VLAN для анализа.
| **Full** |

---

2. Разработка плана IP-адресации

Используем подсеть `192.168.0.0/16` для инфраструктуры.

Разбивка подсетей:

* **Для Loopback-интерфейсов:** `192.168.255.0/24`
  * Эти интерфейсы всегда доступны, используются для управления и динамической маршрутизации (e.g., OSPF Router-ID).
* **Для Point-to-Point линков:** `192.168.254.0/24`
  * Разбиваем на несколько подсетей `/30` или `/31` (если оборудование поддерживает).
* **Для управления оборудованием (In-Band):** Уже есть VLAN 10 (`10.10.10.0/24`).

Таблица IP-адресации для критических интерфейсов

Устройство	Интерфейс	Назначение / Описание	IP-адрес / Подсеть	Примечание
Core-Router-1	`Loopback0`	Router-ID, управление	`192.168.255.1/32`	
	`Gig0/0/0`	Связь с Core-Router-2	`192.168.254.1/30`	Peer IP: `192.168.254.2`
	`Gig0/0/1.10`	VLAN MGMT (10)	`10.10.10.1/24`	Шлюз для VLAN 10
	`Gig0/0/1.50`	VLAN SERVERS_PDN (50)	`10.50.50.1/24`	Шлюз для VLAN 50, здесь применяется ZBFW
	`Gig0/0/1.60`	VLAN STORAGE_PDN (60)	`10.60.60.1/24`	Шлюз для VLAN 60
Core-Router-2	`Loopback0`	Router-ID, управление	`192.168.255.2/32`	
	`Gig0/0/0`	Связь с Core-Router-1	`192.168.254.2/30`	Peer IP: `192.168.254.1`
	`Gig0/0/1.20`	VLAN USERS_CORP (20)	`10.20.20.1/23`	Шлюз для VLAN 20
	`Gig0/0/1.30`	VLAN SERVERS_CORP (30)	`10.30.30.1/24`	Шлюз для VLAN 30

	`Gig0/0/1.40`	VLAN SERVERS_DMZ (40)	`172.16.40.1/24`	Шлюз для VLAN 40
Agg-Switch-1	`VLAN10`	Management SVI	`10.10.10.10/24`	
	`Vlan50`	SERVERS_PDN SVI	`10.50.50.10/24`	
Agg-Switch-2	`VLAN10`	Management SVI	`10.10.10.11/24`	
	`Vlan20`	USERS_CORP SVI	`10.20.20.11/23`	

---

3. Проектирование физической топологии

Логическая схема: "Звезда" с двумя ядрами для отказоустойчивости.

Физическое размещение в стойках ЦОДа:

* **Стойка 1 (Сетевое ядро и агрегация):**
  * **Уровень 1:** `Core-Router-1`, `Core-Router-2`.
  * **Уровень 2:** `Agg-Switch-1` (подключен к Core-Router-1), `Agg-Switch-2` (подключен к Core-Router-2).
  * **Соединения:**
    * Между маршрутизаторами (P2P линк) — патч-корд 1-3 метра.
    * Каждый маршрутизатор подключен к обоим агрегационным коммутаторам для резервирования (LACP).
    * Агрегационные коммутаторы соединены друг с другом Multi-Chassis EtherChannel (MEC) или аналогичной технологией для создания единого логического блока.

* **Стойка 2 (Серверы ПДн):**
  * **Размещение:** Серверы приложений (`SERVERS_PDN`) и серверы СУБД (`STORAGE_PDN`).
  * **Подключение:**
    * Каждый сервер имеет 2 сетевых интерфейса (NIC).
    * `NIC1` (Data) подключается к `Agg-Switch-1` в соответствующих VLAN (50 или 60).
    * `NIC2` (Data/Management) подключается к `Agg-Switch-2` в тех же VLAN для отказоустойчивости.
  * **Требования к кабелям:** Патч-корды от стойки 2 до стойки 1. Длина зависит от планировки ЦОДа, но обычно в пределах 5-15 метров.

* **Стойка 3 (Корпоративные серверы и DMZ):**
  * Размещение серверов из VLAN 30 и VLAN 40.
  * Подключение по аналогичной с стойкой 2 схеме к обоим агрегационным коммутаторам.

*   **Офисный сегмент:**
    *   Доступные коммутаторы (Access Switches) размещаются в телекоммуникационных комнатах на этажах.
    *   Каждый доступный коммутатор "двойным лучом" (twin-axial cable или по оптоволокну) поднимается к обоим агрегационным коммутаторам (`Agg-Switch-1` и `Agg-Switch-2`) в стойке 1.
    *   Длина этих кабелей может быть значительной (до 100м по меди, значительно больше по оптоволокну).

Итог по физической топологии: Мы получаем отказоустойчивую, предсказуемую и легко обслуживаемую структуру, где критичные сегменты ПДн физически сгруппированы, а связь между всеми элементами дублирована. Длина патч-кордов минимизирована за счет размещения сетевого ядра и агрегации в центральной стойке ЦОДа.

Часть 2

1. Протокол маршрутизации

Выбор и обоснование

Для данного кейса однозначно рекомендуется к применению **протокол OSPF (Open Shortest Path First)**.

Обоснование:

1. **Скорость сходимости:** OSPF сходится очень быстро (обычно в пределах нескольких секунд). Для сети обработки ПДн, где критична доступность сервисов, это ключевое преимущество. EIGRP сходится сопоставимо быстро, но OSPF предсказуемее в больших сетях.
2. **Нагрузка на CPU:** OSPF использует алгоритм SPF (Dijkstra), который пересчитывается только при изменении топологии в области (Area). Это создает умеренную нагрузку, которая для современного оборудования некритична. EIGRP менее нагрузочный для малых изменений, но он проприетарный протокол Cisco, что снижает гибкость в гетерогенной среде.
3. **Простота администрирования и соответствие требованиям:** OSPF является открытым стандартом (IETF). Это критически важно для соответствия требованиям регуляторов по ПДн, которые часто предъявляют критерии прозрачности и отсутствия привязки к одному вендору. Логическая структура **Area** в OSPF идеально ложится на нашу концепцию зон безопасности (Zones), позволяя изолировать распространение LSA и содержать последствия сбоя в одной зоне.

EIGRP, несмотря на технические преимущества, исключается из-за закрытости, что может вызвать вопросы у аудиторов.

План внедрения OSPF

*   **Номер процесса:** `1` (локально значимый, может быть любым на каждом маршрутизаторе, но для единообразия используем везде `1`).
*   **Router-ID:** Будем задавать вручную через команду `router-id <address>` для стабильности. Используем IP-адреса из Loopback-интерфейсов.
*   **Назначение областей (Areas) и распределение сетей:**

    Мы используем многообластную структуру OSPF (Multi-Area) для повышения стабильности и масштабируемости.

    *   **Area 0 (Backbone):** Транзитная область для связи всех остальных областей.
        *   **Сети:** `192.168.254.0/30` (P2P линк между Core-Router-1 и Core-Router-2), Loopback-интерфейсы маршрутизаторов (`192.168.255.0/24`).
    *   **Area 10 (Internal Zone):** Объединяет пользовательские и корпоративные серверные сегменты.
        *   **Расположение:** На Core-Router-2.
        *   **Сети:** `10.20.20.0/23` (VLAN 20), `10.30.30.0/24` (VLAN 30).
    *   **Area 50 (PDN Zone):** **Критически важная изолированная область.** Содержит сегменты обработки и хранения ПДн.
        *   **Расположение:** На Core-Router-1.
        *   **Сети:** `10.50.50.0/24` (VLAN 50), `10.60.60.0/24` (VLAN 60).
        *   **Важно:** Для этой области можно и нужно настроить фильтрацию меж-area маршрутов (Area 50 Range с последующей фильтрацией в ABR - Core-Router-1), чтобы строго контролировать, какие сети оттуда видны в других областях.
    *   **Area 40 (DMZ Zone):** Выделенная область для демилитаризованной зоны.
        *   **Расположение:** На Core-Router-2.
        *   **Сети:** `172.16.40.0/24` (VLAN 40).

    Сеть управления (`10.10.10.0/24`) в OSPF анонсироваться **НЕ БУДЕТ**. Доступ к ней обеспечивается через статические маршруты, что является дополнительной мерой безопасности.

---

2. План обеспечения отказоустойчивости

Резервирование на канальном уровне: LACP

*   **Протокол:** IEEE 802.3ad (LACP - Link Aggregation Control Protocol).
*   **Режим:** Active-Active (LACP active на обеих сторонах канала).
*   **Ключевые точки агрегации:**
    1. **Между агрегационными коммутаторами (`Agg-Switch-1` и `Agg-Switch-2`):** Создается **Multi-Chassis Link Aggregation Group (MLAG/MC-LAG)**. Это формирует виртуальный логический коммутатор, что исключает петли (STP блокирует лишние линки) и обеспечивает активное использование всех каналов.
    2. **Между серверами (особенно в VLAN 50/60) и агрегационными коммутаторами:** Каждый сервер подключается двумя физическими линками (от двух независимых NIC) к разным агрегационным коммутаторам. Эти линки объединяются в **LAG (Link

Aggregation Group)** в режиме MC-LAG. Это обеспечивает отказоустойчивость на уровне канала и коммутатора.
3. **Между маршрутизаторами и коммутаторами:** Линки от Core-Router-1 к Agg-Switch-1 и Agg-Switch-2 также могут быть агрегированы для увеличения пропускной способности и отказоустойчивости.

Резервирование на сетевом уровне: FHRP

Используем протокол **HSRP (Hot Standby Router Protocol)** как наиболее распространенный в сресах Cisco.

* **Группа HSRP для пользовательских VLAN (VLAN 20):**
  * **Виртуальный IP (VIP):** `10.20.20.1`
  * **Реальный IP Core-Router-2:** `10.20.20.2`
  * **Реальный IP Core-Router-1:** `10.20.20.3` (Backup)
  * **Приоритет:** Core-Router-2 - `120` (Active), Core-Router-1 - `100` (Standby).
  * *Логика: Основной шлюз для пользователей - Core-Router-2.*

* **Группа HSRP для сегмента ПДн (VLAN 50):**
  * **Виртуальный IP (VIP):** `10.50.50.1`
  * **Реальный IP Core-Router-1:** `10.50.50.2`
  * **Реальный IP Core-Router-2:** `10.50.50.3` (Backup)
  * **Приоритет:** Core-Router-1 - `120` (Active), Core-Router-2 - `100` (Standby).
  * *Логика: Весь трафик к/от серверов ПДн идет через Core-Router-1, где применяется Zone-Based Firewall. В случае его падения, трафик пойдет через Core-Router-2, где должны быть настроены идентичные политики безопасности.*

* **Группа HSRP для сегмента хранения ПДн (VLAN 60):**
  * **Виртуальный IP (VIP):** `10.60.60.1`
  * **Реальный IP Core-Router-1:** `10.60.60.2`
  * **Приоритет:** Core-Router-1 - `120` (Active).
  * **Preempt:** Запрещен.
  * *Логика: Резервирование для этого сегмента может не требоваться, так как исходящий трафик из него запрещен. Шлюз остается единственным и статическим для максимальной предсказуемости. Можно добавить Core-Router-2 с приоритетом 90 как Standby, но без Preempt.*

---

3. План управления и мониторинга

Выбор протокола управления

Выбор: SNMPv3 (Simple Network Management Protocol version 3).

Обоснование:

Требования к защите ПДн делают недопустимым использование старых версий SNMPv1/v2c, которые не имеют встроенного шифрования и используют простые строки сообщества (community strings), передающиеся по сети в открытом виде.

Преимущества SNMPv3 для нашего кейса:
*   **Аутентификация:** Гарантирует, что запросы приходят от доверенного источника.
*   **Шифрование (Privacy):** Шифрует данные, передаваемые между агентом (устройством) и менеджером (NMS), предотвращая перехват конфиденциальной информации (статусы интерфейсов, конфигурации).
*   **Авторизация:** Ограничивает доступ пользователей только к разрешенным объектам MIB.

Альтернативы (например, NETCONF/YANG) являются более современными, но их поддержка сильно зависит от модели и версии ПО оборудования. SNMPv3 — это отраслевой стандарт, поддерживаемый всем сетевым оборудованием, что соответствует принципу "проще и надежнее".

Стратегия резервного копирования конфигураций

Резервное копирование — критически важный процесс для быстрого восстановления в случае сбоя и для аудита изменений.

*   **Протокол: SFTP (SSH File Transfer Protocol).**
    *   **Обоснование:** TFTP небезопасен, данные передаются в открытом виде. SFTP использует SSH-туннель, обеспечивая аутентификацию по ключу/паролю и шифрование передаваемых данных. Это соответствует требованиям защиты ПДн.
*   **Сервер:** Выделенный безопасный сервер внутри корпоративного сегмента (VLAN 30) с ограниченным доступом.
*   **Частота копирования:**
    *   **Ежедневно (инкрементальное):** Автоматическое копирование измененных конфигураций каждую ночь.
    *   **Немедленно (по требованию):** Ручное копирование конфигурации на сервер после **ЛЮБОГО** изменения, влияющего на безопасность или стабильность сети (изменение ACL, правил фаервола, маршрутизации).
    *   **Ежемесячно (полное):** Полное архивирование всех конфигураций и связанных файлов (например, сертификатов).
*   **Верификация:** Раз в квартал необходимо проводить тестовое восстановление конфигурации на резервном оборудовании для проверки целостности бэкапов и корректности процедуры восстановления.
*   **Ведение журнала:** Все операции копирования должны логгироваться (кто, когда, какое устройство).

Часть 3

1. Детальное проектирование политик безопасности

Спецификации ACL (Access Control List)

ACL здесь применяются как дополнительный (и обязательный к логгированию) уровень контроля, дополняющий Zone-Based Firewall.

a) ACL для управления (VLAN 10 - MGMT)
*   **Наименование:** `ACL-MGMT-IN`
*   **Номер:** (Именованный ACL)
*   **Направление:** Входящий (inbound) на SVI интерфейсе VLAN 10.
*   **Описание правил:**

#	Action	Protocol	Source Address	Destination Address	Destination Port	Описание
10	Permit	TCP	`10.30.30.50/32`	`10.10.10.0/24`	`22 (SSH)`	Разрешить управление по SSH только с Jump-хоста.
20	Permit	TCP	`10.30.30.50/32`	`10.10.10.0/24`	`443 (HTTPS)`	Разрешить управление по HTTPS только с Jump-хоста.
30	Deny	IP	`any`	`10.10.10.0/24`	`any`	**Запретить весь остальной трафик. Запись для логгирования.**
						Неявный deny any (логируется по умолчанию, если включено logging)

b) ACL для изоляции хранилища ПДн (VLAN 60 - STORAGE_PDN)
*   **Наименование:** `ACL-STORAGE-PDN-IN`
*   **Номер:** (Именованный ACL)
*   **Направление:** Входящий (inbound) на SVI интерфейсе VLAN 60.
*   **Описание правил:**

#	Action	Protocol	Source Address	Destination Address	Destination Port	Описание
10	Permit	TCP	`10.50.50.0/24`	`10.60.60.0/24`	`1433`	Разрешить доступ от серверов ПДн к MS SQL Server.
20	Permit	TCP	`10.50.50.0/24`	`10.60.60.0/24`	`5432`	Разрешить доступ от серверов ПДн к PostgreSQL.
30	Permit	TCP	`10.50.50.0/24`	`10.60.60.0/24`	`1521`	Разрешить доступ от серверов ПДн к Oracle DB.
40	Deny	IP	`any`	`10.60.60.0/24`	`any`	**Явный запрет всего остального входящего трафика. Логгировать.**

c) ACL для пользовательского сегмента (VLAN 20 - USERS_CORP)
*   **Наименование:** `ACL-USERS-CORP-OUT`
*   **Номер:** (Именованный ACL)
*   **Направление:** Исходящий (outbound) на SVI интерфейсе VLAN 20 (или входящий на интерфейсах доступа).
*   **Описание правил:**

    *   *Цель: Блокировать попытки пользователей инициировать соединение с сегментом ПДн, даже если маршрутизация есть.*
    *   `deny ip any 10.50.50.0 0.0.0.255 log`
    *   `deny ip any 10.60.60.0 0.0.0.255 log`
    *   `permit ip any any`

Политика безопасности портов (Port Security)

Применяется на всех **пользовательских портах доступа** (коммутаторы, к которым подключаются ПК сотрудников).

*   **Максимальное количество MAC-адресов:** `2`
    *   *Обоснование: К порту обычно подключен только ПК (1 MAC). Второй MAC разрешен для учетного IP-телефона (в режиме VoIP VLAN) или легального USB-адаптера.*
*   **Действие при нарушении (Violation Action):** **shutdown**
    *   *Обоснование: Наиболее безопасный вариант. При обнаружении несанкционированного устройства (например, подключенного свитча или хоста) порт переводится в error-disable (ошибочное отключение) состояние. Это требует ручного вмешательства администратора, что обеспечивает расследование инцидента.*
*   **Sticky MAC Address:** `enabled`
    *   *Обоснование: Позволяет автоматически "запомнить" первые 2 MAC-адреса, увиденные на порту, и добавить их в running-config. Это упрощает первоначальную настройку.*
*   **Исключения:** Политика **НЕ** применяется на портах, подключенных к серверам (VLAN 30, 50, 60) и на uplink-портах между сетевым оборудованием.

---

2. План реализации сервисов

Детальный план настройки DHCP

DH-сервер (располагается в VLAN 30) будет настроен со следующими scope (областями).

VLAN / Имя	Подсеть	Диапазон адресов	Исключения (резервации)	Шлюз по умолчанию	DNS-серверы	Примечания
20_USERS_CORP	`10.20.20.0/23`	`10.20.20.100` - `10.20.21.200`	`10.20.20.1` - `10.20.20.99`	`10.20.20.1` (HSRP VIP)	`8.8.8.8`, `1.1.1.1`	Для пользовательских рабочих станций.
30_SERVERS_CORP	`10.30.30.0/24`	-	-	-	-	**DHCP отключен.** Все адреса назначаются статически для стабильности серверов.

40_SERVERS_DMZ	`172.16.40.0/24`	-	-	-	-	**DHCP отключен.** Адреса назначаются статически.
50_SERVERS_PDN	`10.50.50.0/24`	-	-	-	-	**DHCP отключен.** Адреса назначаются статически. Критичная зона.
60_STORAGE_PDN	`10.60.60.0/24`	-	-	-	-	**DHCP отключен.** Адреса назначаются статически. Критичная зона.
10_MGMT	`10.10.10.0/24`	-	-	-	-	**DHCP отключен.** Адреса назначаются статически.

Схема приоритизации трафика (QoS)

Используем модель **DiffServ (Differentiated Services)**.

1. Классификация и маркировка:

* **Класс 1 - Голосовой трафик (EF - Expedited Forwarding):**
  * **Трафик:** VoIP (SIP, RTP).
  * **DSCP Marking:** `EF (46)` или `CS5 (40)`.
  * **Где маркируется:** На коммутаторах доступа по портам, на которых "сидят" IP-телефоны, или по доверенной DSCP-метке от телефона.

* **Класс 2 - Видео и бизнес-критичные приложения (AF4 - Assured Forwarding):**
  * **Трафик:** Видеоконференции (Webex, Zoom), трафик критичных ERP-систем.
  * **DSCP Marking:** `AF41 (34)`.
  * **Где маркируется:** На границе сети (коммутаторы доступа) с помощью ACL, идентифицирующих данный трафик.

* **Класс 3 - Best Effort (Обычные данные):**
  * **Трафик:** Веб-браузинг, почта, файловые передачи.
  * **DSCP Marking:** `DF (0)`.
  * **Примечание:** Это класс по умолчанию.

* **Класс 0 - Scavenger (Фоновий/Неважный):**
  * **Трафик:** Личный трафик, развлечения (YouTube, социальные сети) — если разрешено политикой.
  * **DSCP Marking:** `CS1 (8)`.
  * **Обработка:** Пропускная способность для этого класса ограничивается до минимума.

2. Организация очередей (на маршрутизаторах и uplink-портах):

Применяется политика **Low Latency Queuing (LLQ)**.

| # | Очередь | Тип очереди | Пропускная способность | Описание |

|-----|---------|--------------------|------------------------|---
--------------|
| 1 | Queue 1 | Priority Queue (LLQ) | 10% от полосы | Для голосового трафика
(EF). Гарантирует минимальную задержку и джиттер. |
| 2 | Queue 2 | Bandwidth Queue | 25% от полосы | Для видео и критичных
приложений (AF4). |
| 3 | Queue 3 | Bandwidth Queue | Остаток | Для Best Effort трафика (DF).
|
| 4 | Queue 4 | Bandwidth Queue | 1% от полосы | Для Scavenger трафика
(CS1). |

---

3. Формирование итогового документа и защита

Структура итогового документа «План конфигурации корпоративной сети»

1. **Титульный лист.**
2. **Введение.**
   * Цели проекта.
   * Обзор требований (защита ПДн, отказоустойчивость).
3. **Архитектура сети.**
   * Логическая схема (диаграмма).
   * Физическая схема (размещение в стойках).
4. **Детализация сети.**
   * Таблица VLAN.
   * План IP-адресации (включая P2P и Loopback).
   * Матрица доступа и политики ZBFW.
5. **Протоколы и сервисы.**
   * Проект OSPF (области, сети).
   * План отказоустойчивости (HSRP, LACP).
   * План DHCP.
   * Политика QoS.
6. **Безопасность.**
   * Спецификации ACL.
   * Политика безопасности портов.
   * Политика управления и мониторинга (SNMPv3, бэкапы).
7. **Приложения.**
   * Примеры конфигураций (образцы для маршрутизатора, коммутатора).

Ключевые тезисы для презентации (сложные и неочевидные решения)

1. **"Защита в глубину для сегмента ПДн"**
   * *Проблема:* Как обеспечить максимальную изоляцию, не теряя функциональность?
   * *Решение:* Многоуровневая защита:
     * **Уровень 1:** Физическая/логическая сегментация (VLAN 50/60).
     * **Уровень 2:** ZBFW с правилом "Deny Any" между зонами.

*   **Уровень 3:** Точные ACL на SVI интерфейсах, разрешающие *только* служебные порты БД.
*   **Уровень 4:** Отсутствие резервирования шлюза (HSRP) для VLAN 60 для исключения альтернативных путей.
*   *Вывод:* Нарушитель должен преодолеть 4 независимых рубежа защиты.

2. **"Соответствие требованиям регуляторов через технологический выбор"**
   *   *Проблема:* Требования прозрачности и независимости от вендора.
   *   *Решение:* Осознанный отказ от проприетарного EIGRP в пользу открытого OSPF. Использование SNMPv3 вместо v2c. Это не просто технический выбор, а стратегический, упрощающий аудит и валидацию.

3. **"Баланс между безопасностью и управляемостью в политиках безопасности портов"**
   *   *Проблема:* Полное блокирование порта (shutdown) создает операционную нагрузку на IT.
   *   *Решение:* Использование `sticky` + `maximum 2` + `shutdown`. Это автоматизирует легитимные подключения (ПК+телефон), но жестко пресекает любые попытки расширения сети пользователями, что критично для предотвращения утечек ПДн.

4. **"Логическое продолжение политик безопасности в QoS"**
   *   *Проблема:* Как гарантировать качество сервиса для VoIP, не усложняя модель безопасности?
   *   *Решение:* Маркировка трафика на границе сети (доверенная зона). Это позволяет внутренним устройствам (маршрутизаторам) просто применять политики очередей, не занимаясь глубокой инспекцией, что согласуется с принципом разделения ответственности.