Мультисервисные защищенные сети ПД для промышленных предприятий

Гневанов Никита,
Системный инженер, CCIE R&S/Voice, #21926
ngnevano@cisco.com

Программа

1. Виртуализация сети ПД

- Предпосылки к виртуализации сети ПД
- Технологии виртуализации сети
- Управление доступом к ресурсам

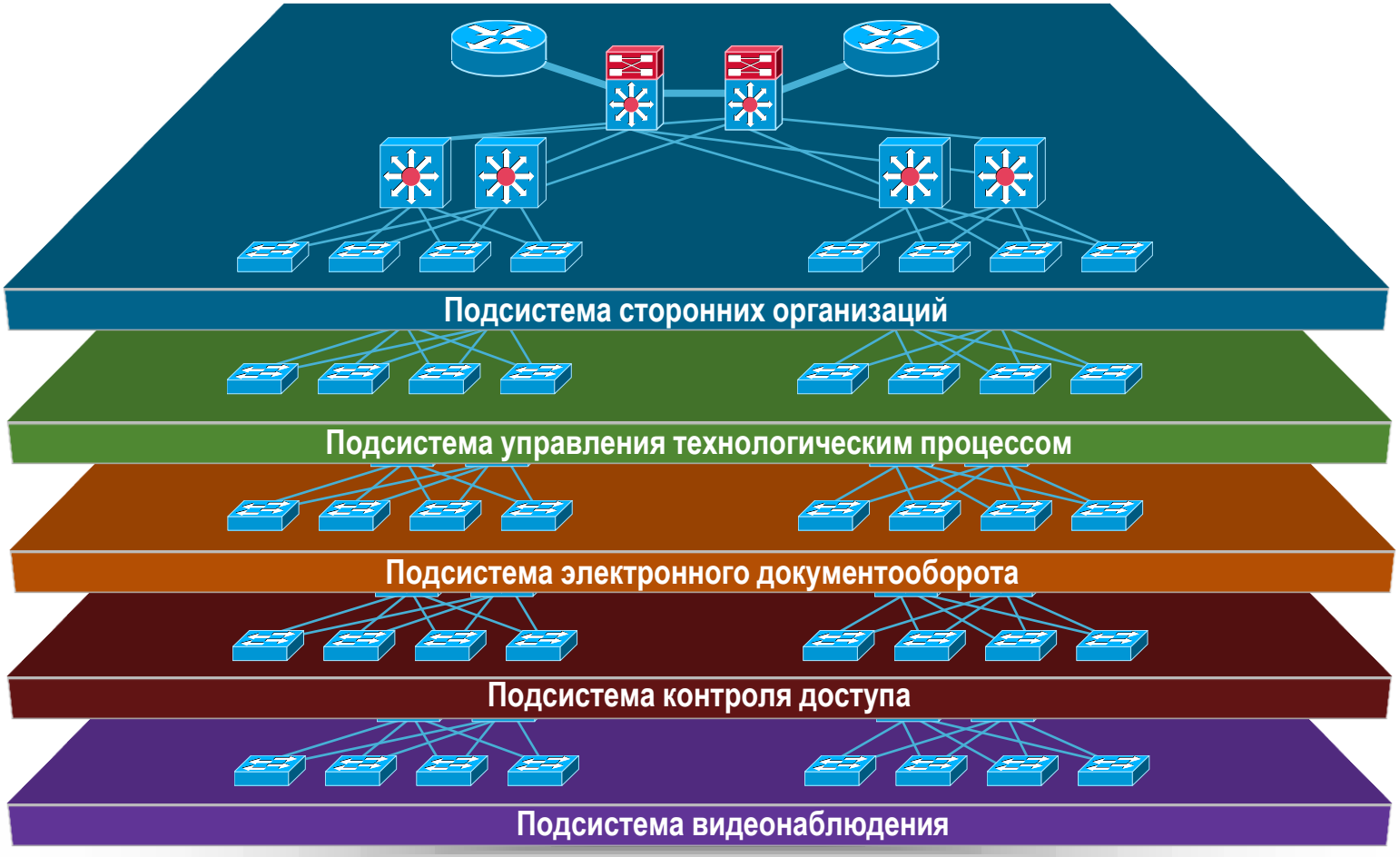
2. Особенности архитектуры сети ПД промышленных предприятий

- Модель сегментации современной промышленной сети
- Технологии обеспечения высокой доступности участка производственного процесса
- Особенности качества обслуживания

Предпосылки к виртуализации сети ПД

Современная сетевая инфраструктура

Типовой пример: много подсистем, которым нужно безопасное взаимодействие



Задачи предприятия

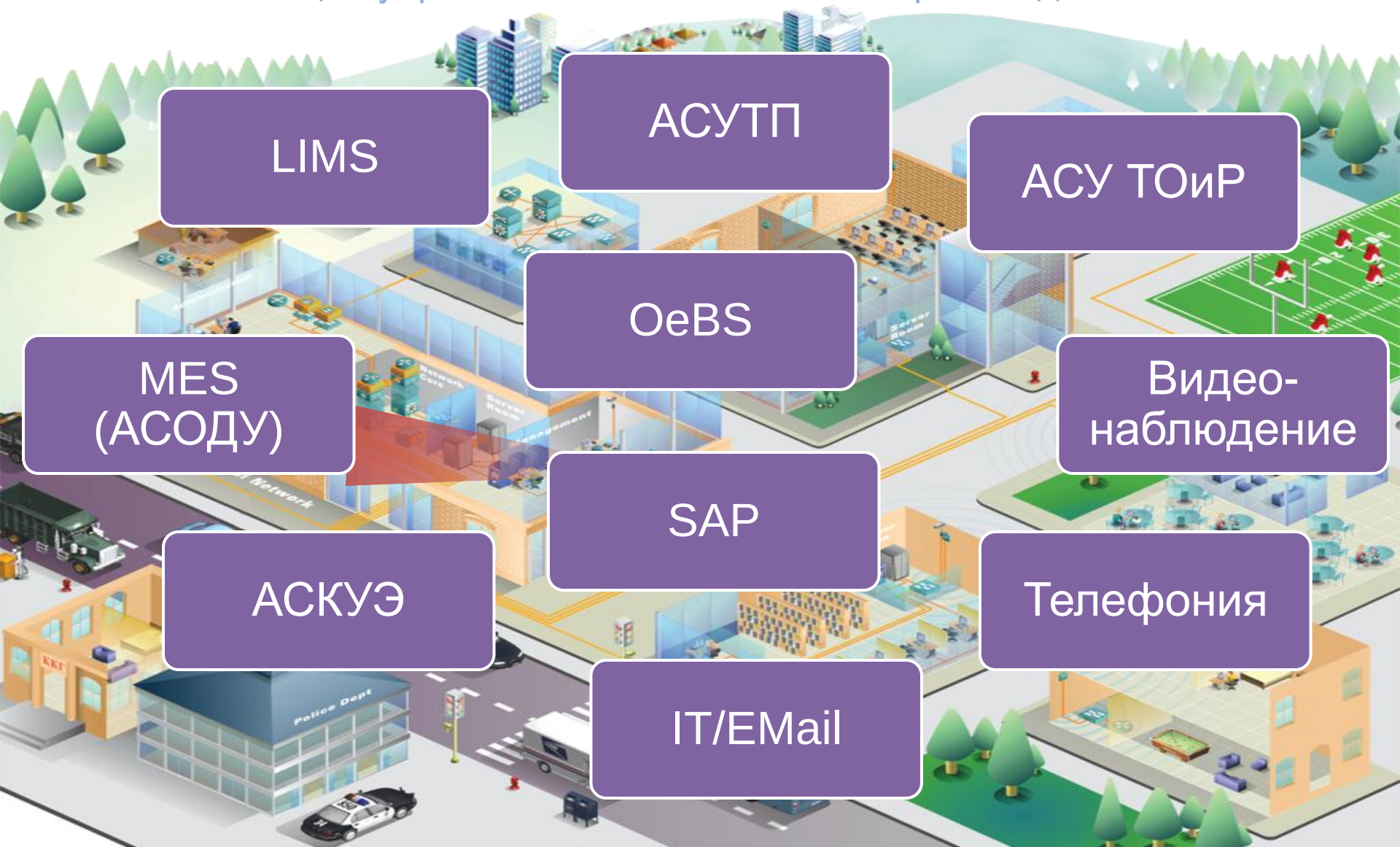
Одними из основных задач предприятия являются:

- **Контроль за расходами и их сокращение**
- **Повышение эффективности производства**
- **Рост доходов**
- **Рост удовлетворенности клиентов, партнеров, акционеров и всех других заинтересованных лиц**

Для достижения поставленных задач необходимо обеспечить прозрачность управления предприятием на всех этапах производства

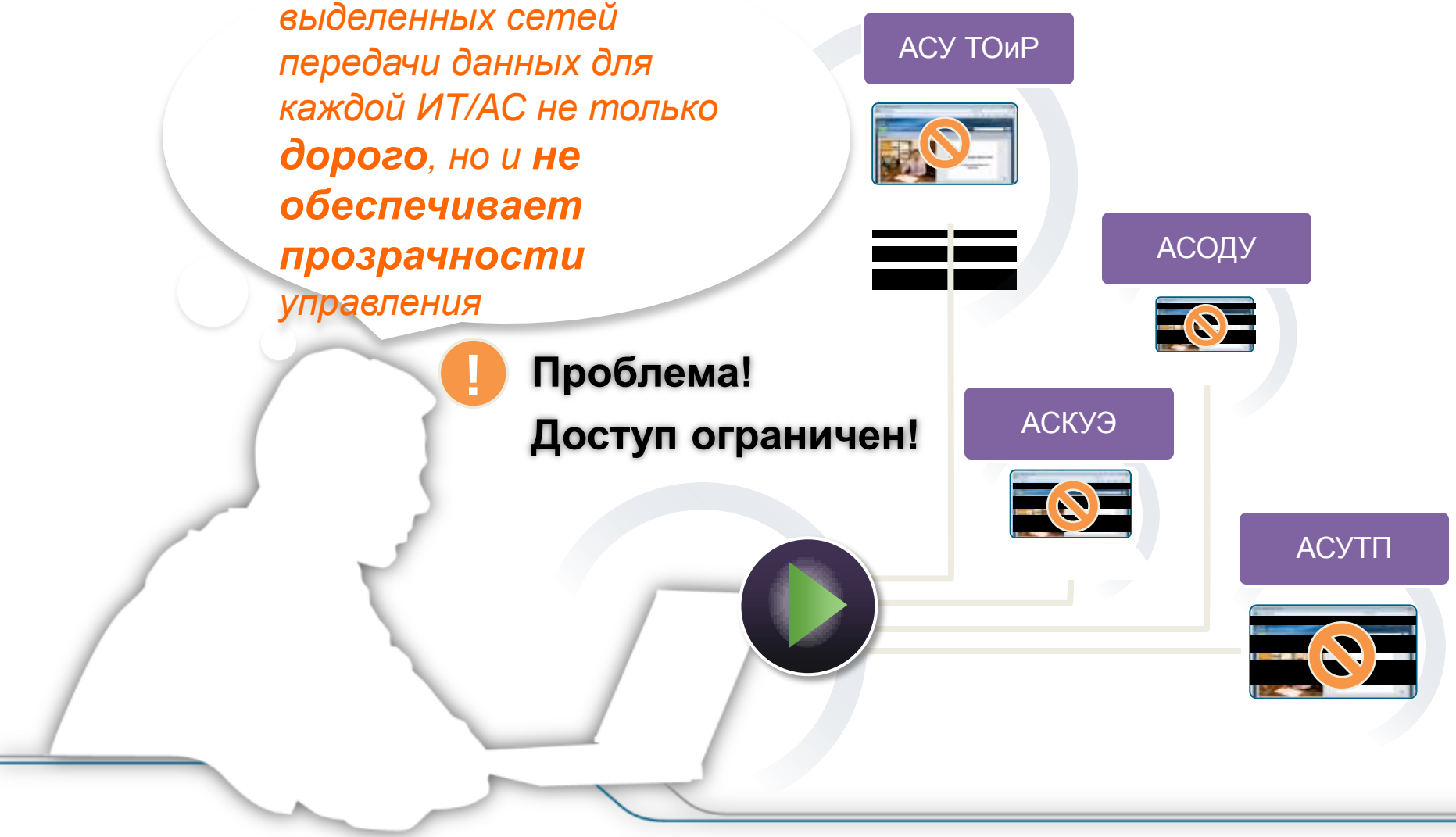
Прозрачное управление с помощью ИТ/АС

На промышленном предприятии существует множество систем автоматизации управления технологиями и производством



Прозрачное управление

Строительство выделенных сетей передачи данных для каждой ИТ/АС не только ***дорого****, но и* ***не обеспечивает прозрачности*** *управления*



Предпосылки к повышению доступности и надежности сети предприятия

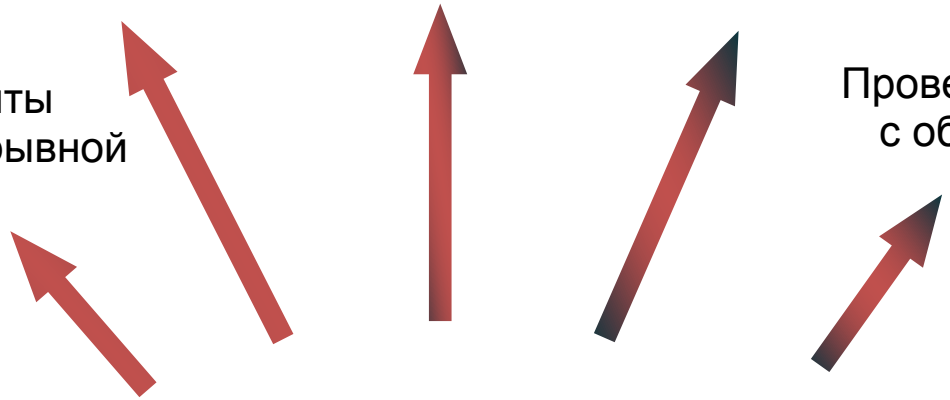
Человек замечает разницу в голосе при пропадании 10 пакетов G.711 или вариации задержки 150-200 мсек

Видео менее устойчиво к потерям пакетов и задержке

Эволюция бизнес приложений и решений Unified Communications

Промышленные сегменты (АСУТП) требуют непрерывной доступности сети

Проведение работ с оборудованием



Отказоустойчивость систем (SLA)

Отказоустойчивость сети

Возможные пути развития

1. Общая сетевая инфраструктура без виртуализации

Достоинства решения

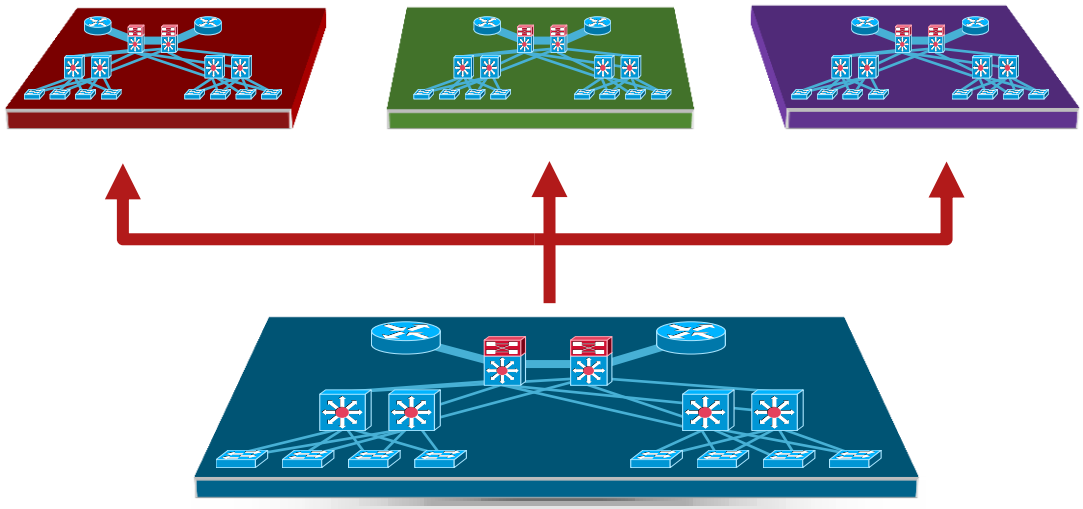
Общие устройства и каналы для всех подсистем

Минимальная стоимость оборудования

Недостатки решения

Трудности с обеспечением политик ИБ

Общие таблицы маршрутизации уменьшают гибкость настроек взаимодействия между подсистемами



Возможные пути развития

2. Общая сетевая инфраструктура с виртуализацией

Достоинства решения

Общие устройства и каналы для всех подсистем

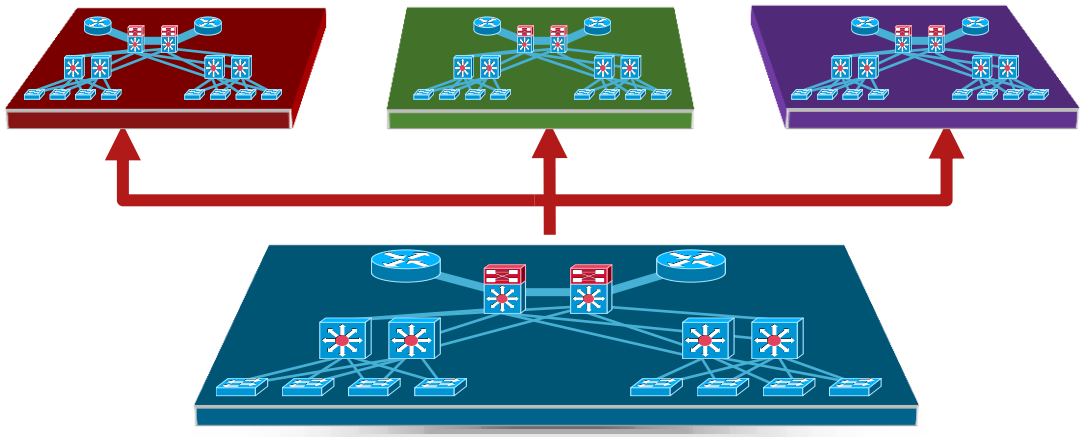
Изоляция подсистем на уровне сетевого оборудования и каналов

Экономия на стоимости оборудования и обслуживании

Гибкость настроек взаимодействия между виртуальными подсистемами

Недостатки решения

Нет



Технологии виртуализации сети

Компоненты виртуализации сети ПД

Виртуализация сетевого оборудования

- **Логическое разделение сетевой инфраструктуры между несколькими подсистемами**
- **Одна физическая инфраструктура обеспечивает работу нескольких логических подсистем**
- **Возможность обеспечения логического разделения сетевого оборудования для всех типов оборудования (коммутаторы, маршрутизаторы, МЭ)**

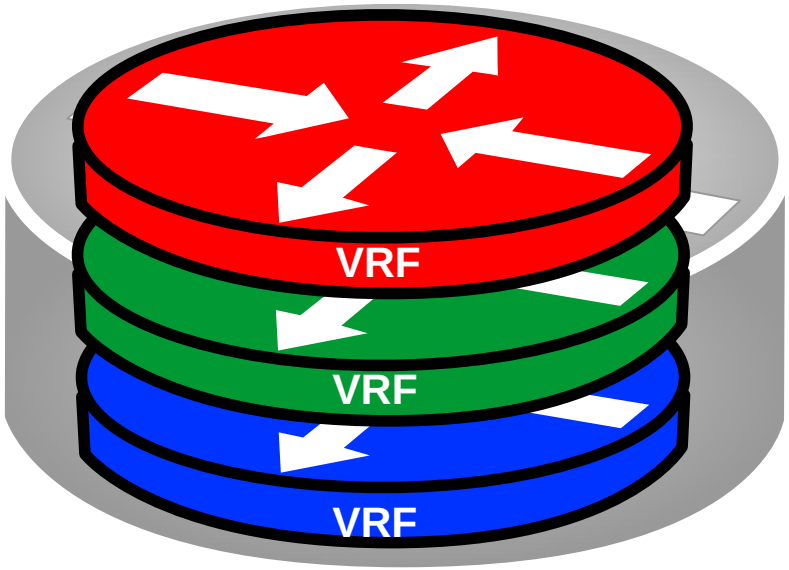
Виртуализация каналов

Технологии, позволяющие логическим подсистемам быть изолированными в пределах части/всей сети ПД

Компоненты - виртуализация устройств

Одно физическое устройство

- Коммутатор
- Маршрутизатор
- Межсетевой экран

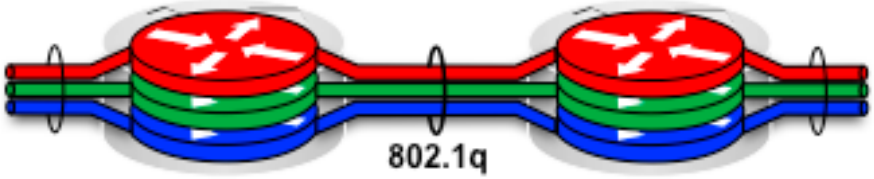


Несколько виртуальных устройств

- Виртуализация на L2 (VLAN’ы)
- Виртуализация на L3 (VRF’ы)
- Виртуализация экземпляров МЭ (контексты)
- Виртуализация сетевых сервисов

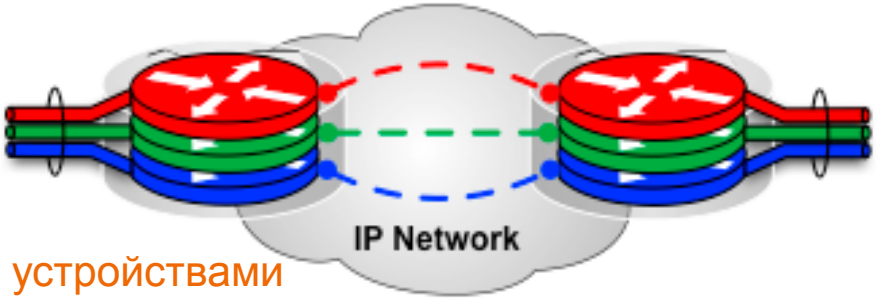
Компоненты - виртуализация каналов

- Hop-by-Hop (802.1Q)
  - VRF-Lite End-to-End
  - EVN (Easy Virtual Network)



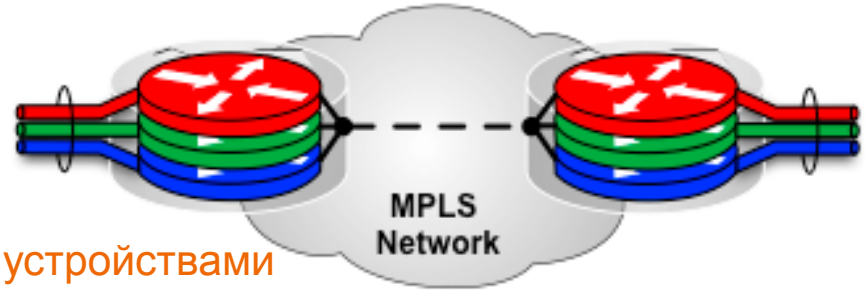
Тэг VLAN ID для виртуализации каналов
Виртуализация каналов между смежными устройствами

- Multi-Hop (GRE)
  - VRF-Lite + GRE



Туннель GRE для виртуализации каналов
Виртуализация каналов между удаленными устройствами

- Multi-Hop (MPLS)
  - MPLS-VPN



MPLS метки для виртуализации каналов
Виртуализация каналов между удаленными устройствами

Управление доступом к ресурсам

Доступ к ИТ ресурсам подсистем

Выделенный ресурс подсистемы

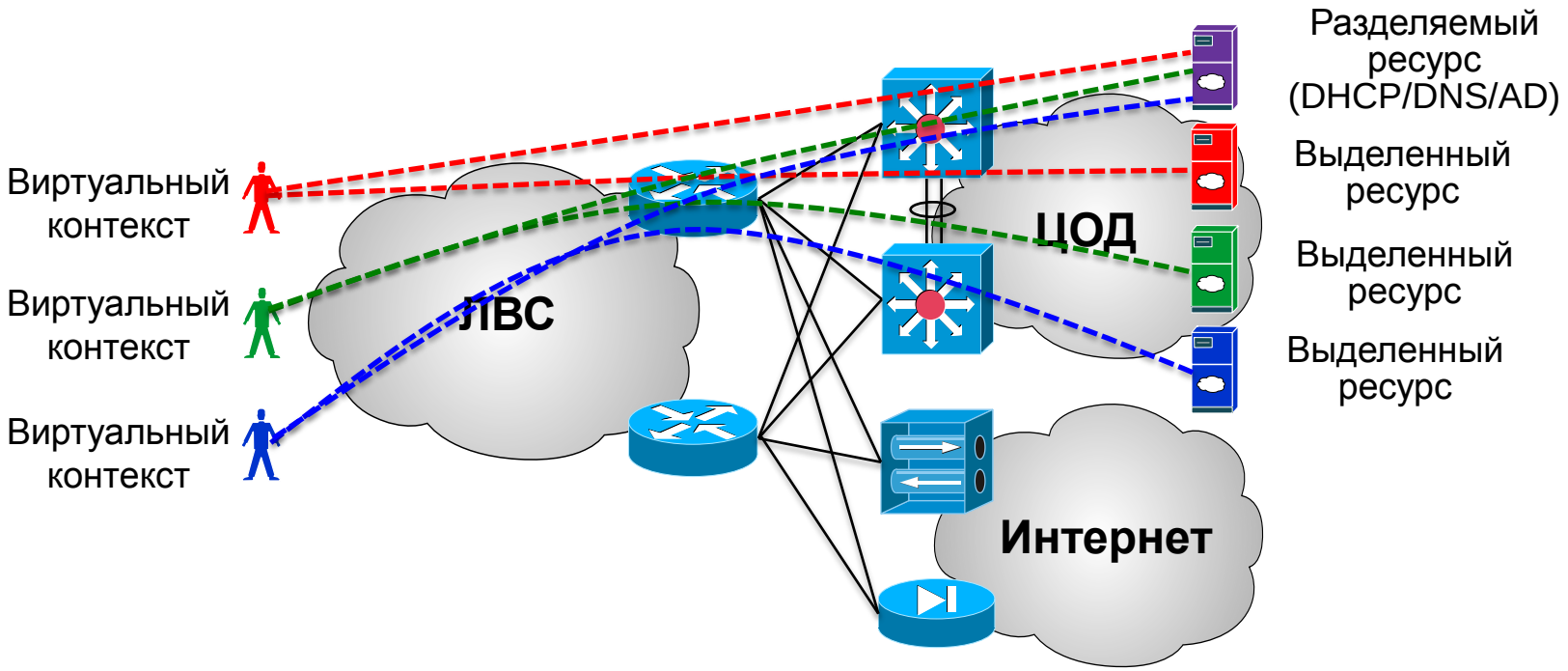
Только один контекст имеет доступ к ресурсу

Разделяемый ресурс для нескольких/всех подсистем

Несколько контекстов имеют доступ к ресурсу

Повышение экономической эффективности

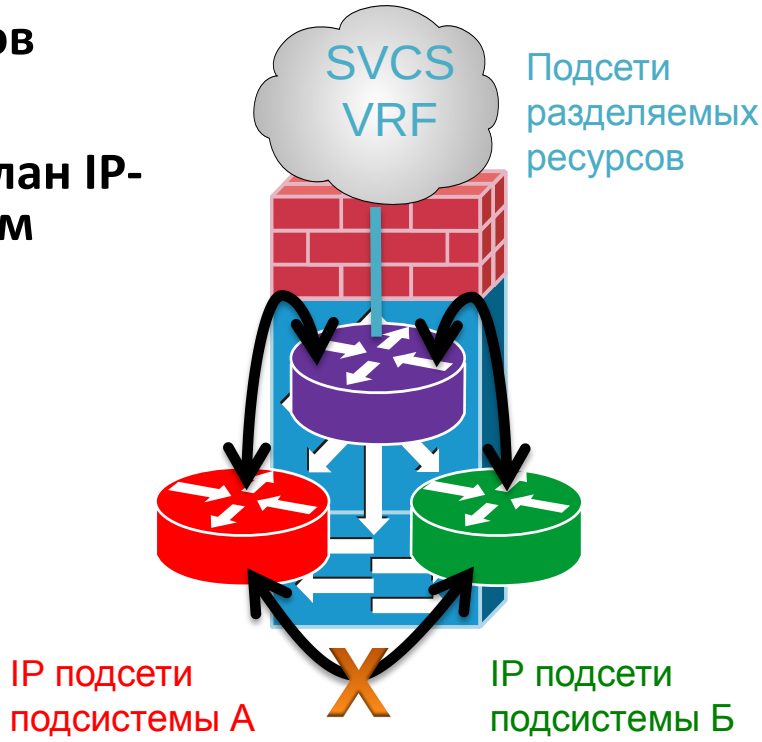
Централизованная политика информационной безопасности



Доступ к разделяемым ресурсам

Основные характеристики решения:

- **Нет межсетевого экранирования (но можно установить МЭ дополнительно)**
- **Используется для общих сервисов (DNS, DHCP, AD, …)**
- **Требуется не пересекающийся план IP-адресации для данных подсистем**



Программа

1. Виртуализация сети ПД

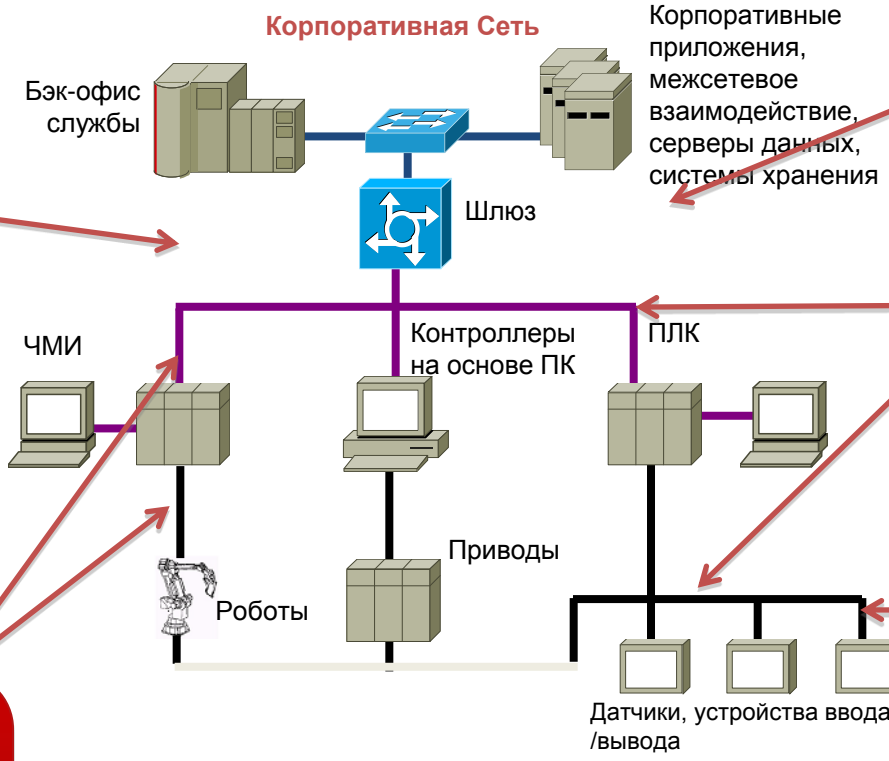
- **Предпосылки к виртуализации сети ПД**
- **Технологии виртуализации сети**
- **Управление доступом к ресурсам**

2. Особенности архитектуры сети ПД промышленных предприятий

- **Модель сегментации современной промышленной сети**
- **Технологии обеспечения высокой доступности участка производственного процесса**
- **Особенности качества обслуживания**

Модель сегментации современной промышленной сети

Традиционная промышленная инфраструктура



Нет прямого доступа к информации

Затруднен удаленный доступ и обслуживание

Сложность интеграции

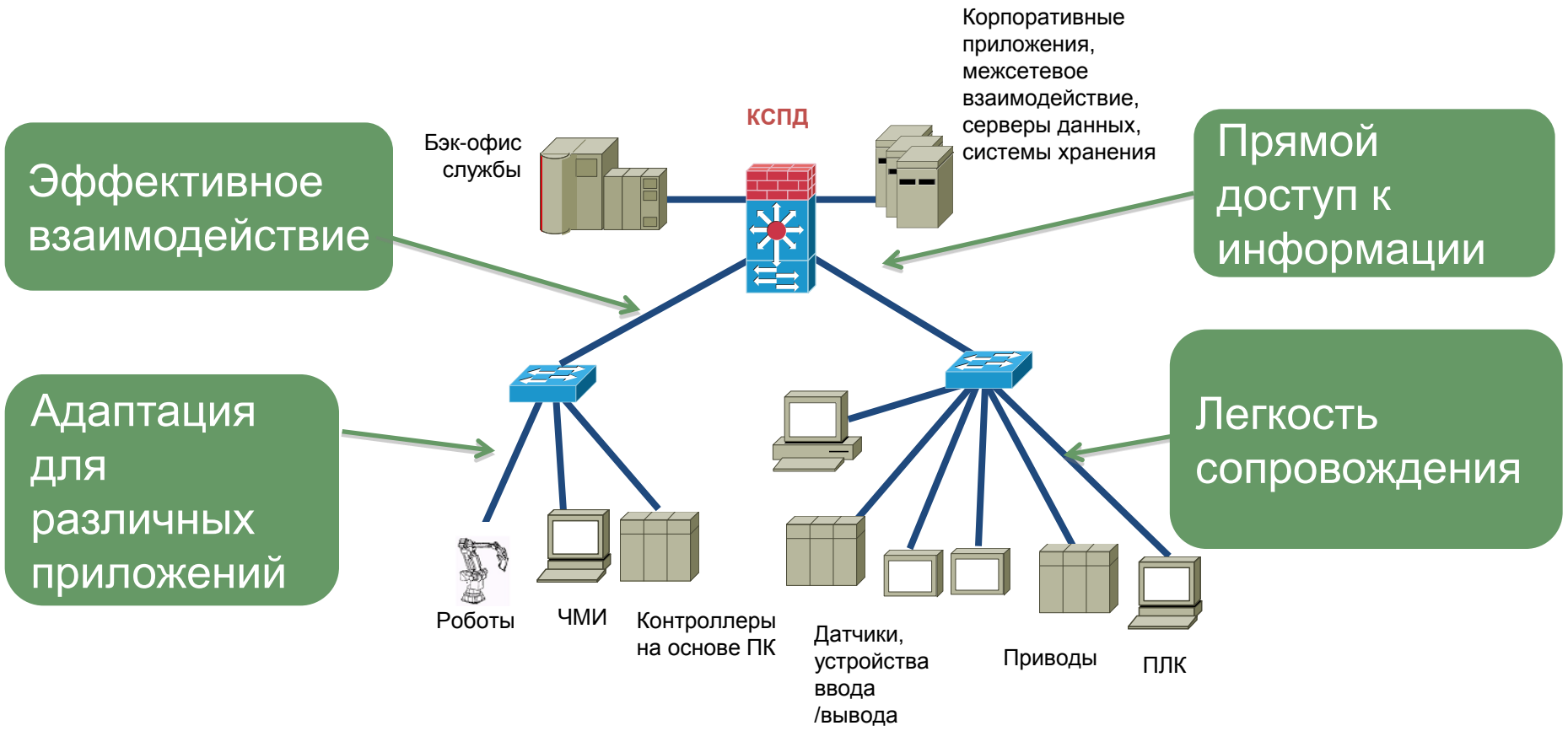
Ограниченная пропускная способность

Дорогое обслуживание множества сетевых инфраструктур

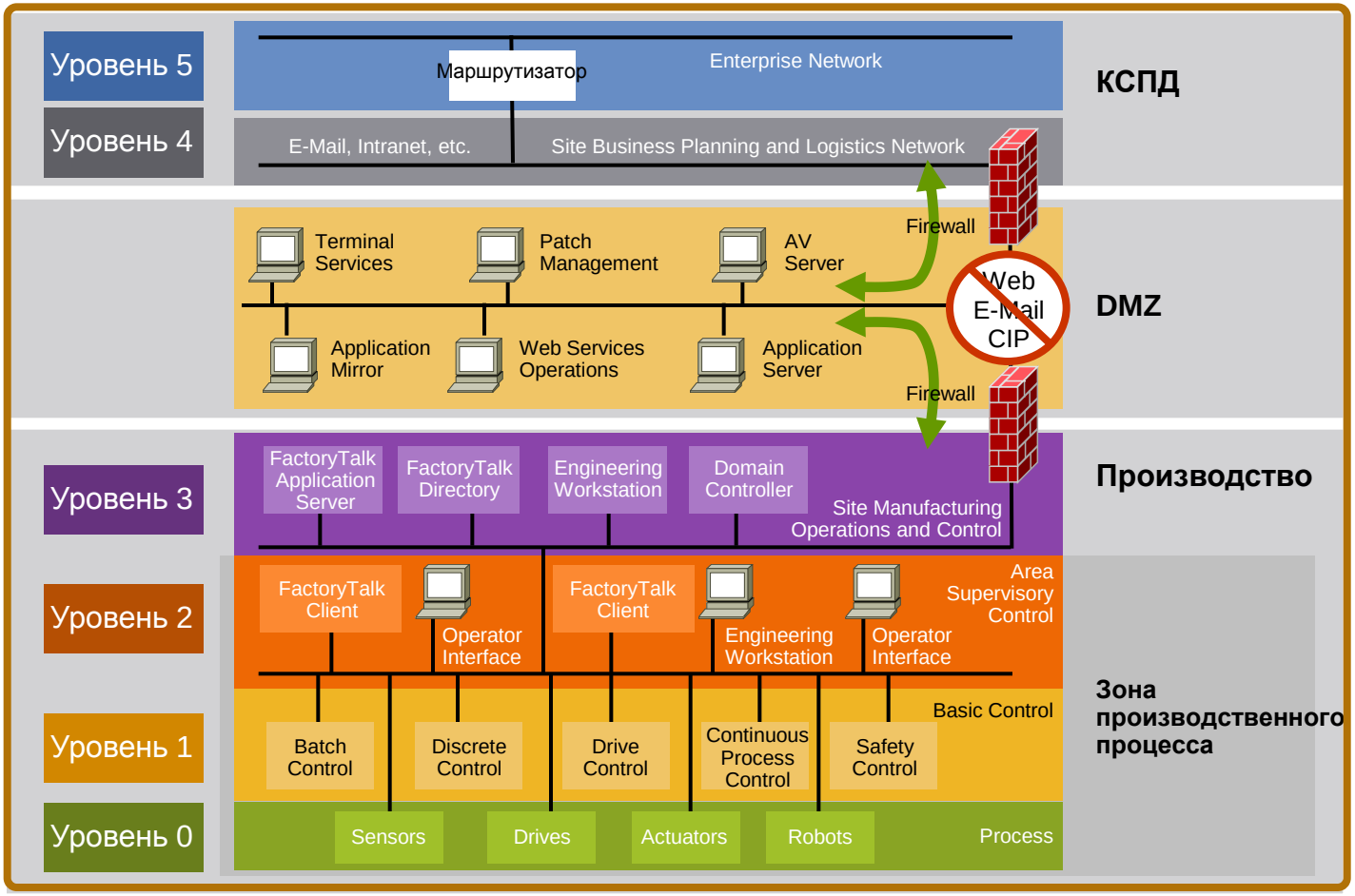
Традиционная сеть автоматизации

- Производственная сеть
- Сеть уровня устройств
- Ethernet

Система промышленной автоматизации, базирующаяся на Ethernet & IP



Логическая схема промышленной сети



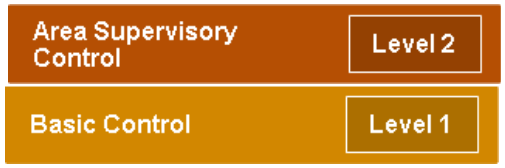
Типовые приложения и системы

- MES—Manufacturing Execution System, управление производством; отслеживает основные метрики, относящиеся к производственному процессу, такие как продукт, оборудование, труд, инвентаризация, дефекты и др.; требует интерфейс к приложениям корпоративного уровня.

- Исторический сервер—сбор, хранение данных и подготовка отчетов, относящихся к производственному процессу.

- SCADA—Supervisory Control and Data Acquisition; распределенная система контроля производственного процесса.

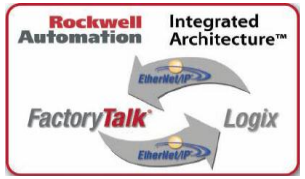
- ПЛК—Программируемый Логический Контроллер; контроль участка производственного процесса.

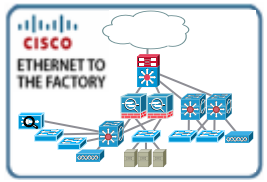


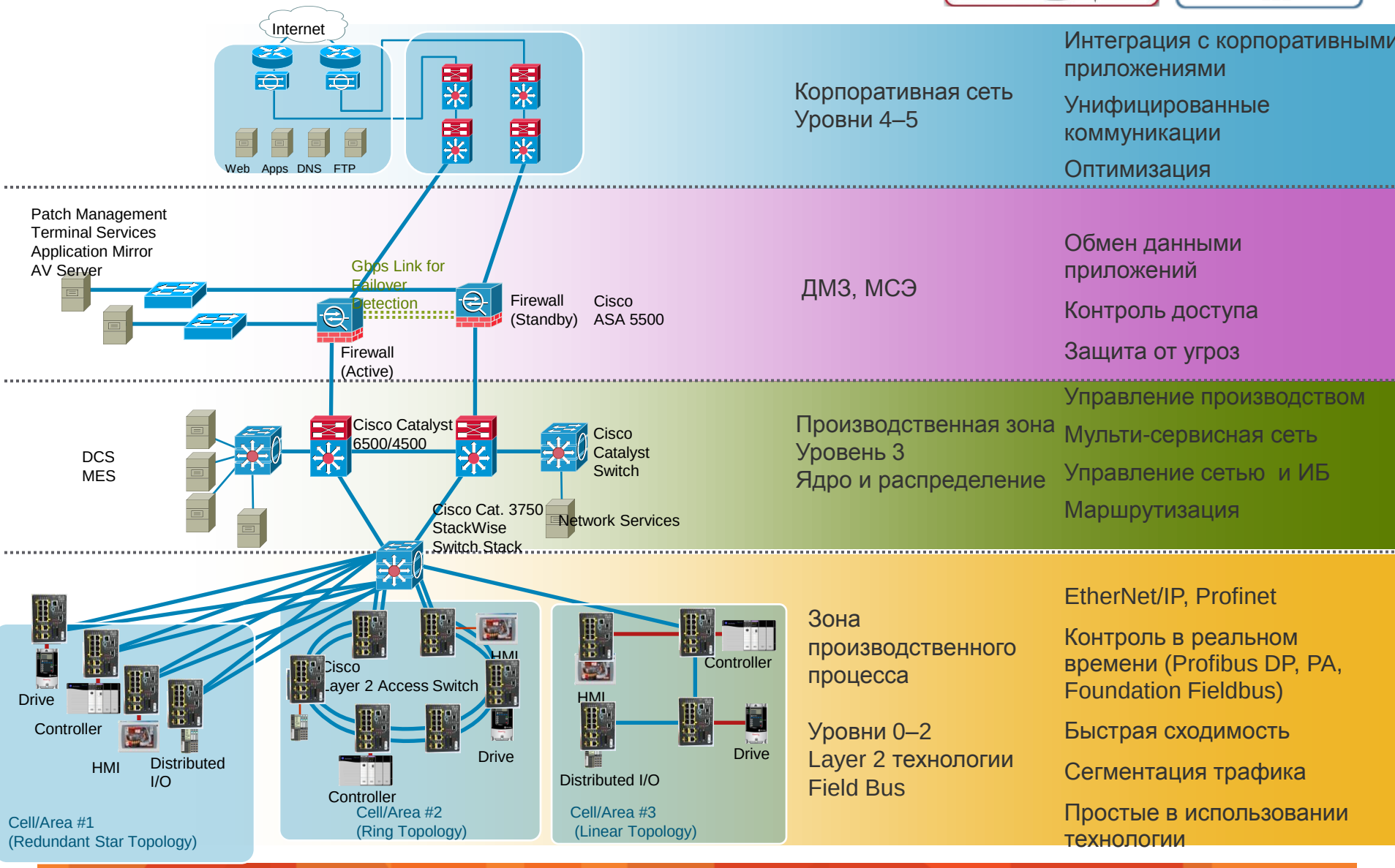
- ЧМИ—человеко-машинный интерфейс отображает состояние участка производственного процесса оператору и позволяет проводить простейшие операции (старт/стоп).

- I/O—устройство ввода/вывода; контроль основных параметров участка производственного процесса; Уровень 0.

Архитектура ‘Converged Plantwide Ethernet’







Корпоративная сеть
Уровни 4–5

- Интеграция с корпоративными приложениями
- Унифицированные коммуникации
- Оптимизация

ДМЗ, МСЭ

- Обмен данными приложений
- Контроль доступа
- Защита от угроз

Производственная зона
Уровень 3
Ядро и распределение

- Управление производством
- Мульти-сервисная сеть
- Управление сетью и ИБ
- Маршрутизация

Зона производственного процесса

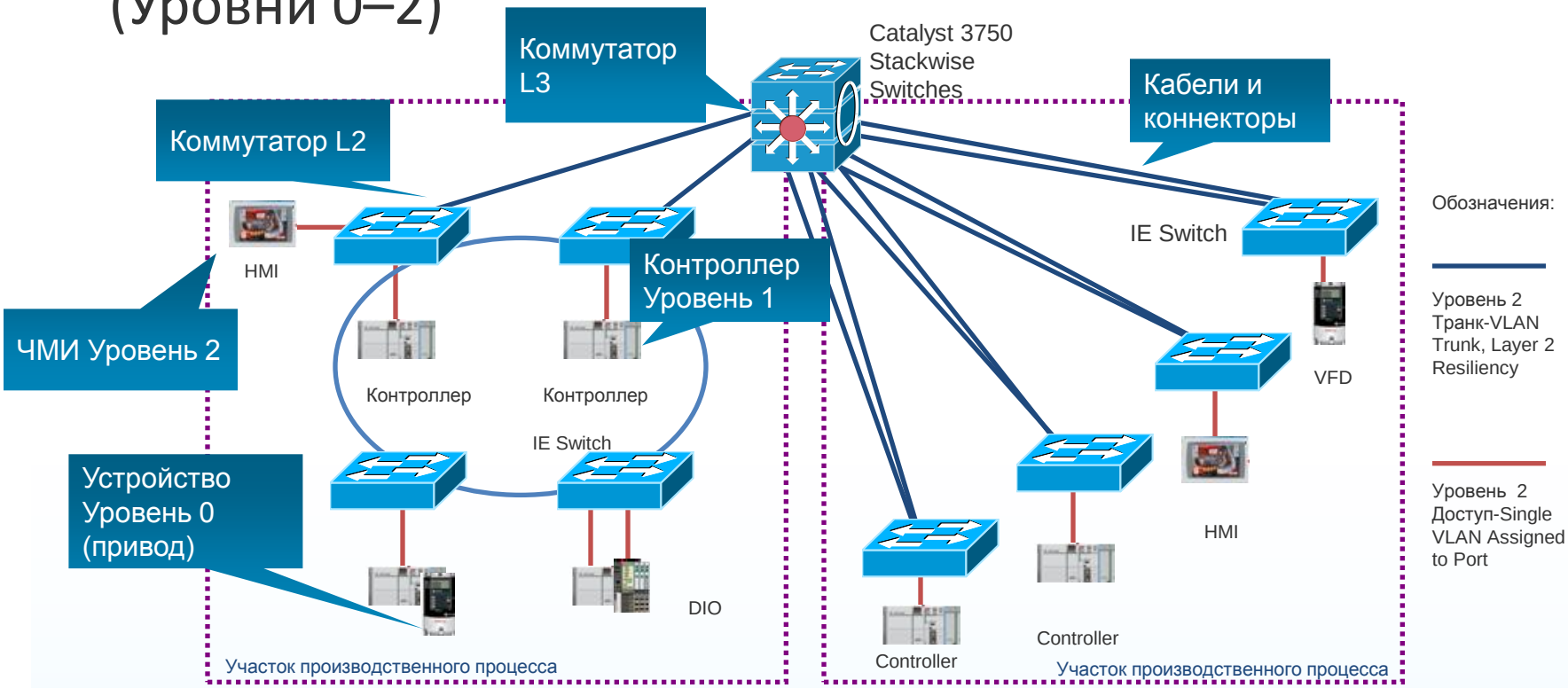
Уровни 0–2
Layer 2 технологии
Field Bus

- EtherNet/IP, Profinet
- Контроль в реальном времени (Profibus DP, PA, Foundation Fieldbus)
- Быстрая сходимость
- Сегментация трафика
- Простые в использовании технологии

Технологии обеспечения высокой доступности участка производственного процесса

Участок производственного процесса

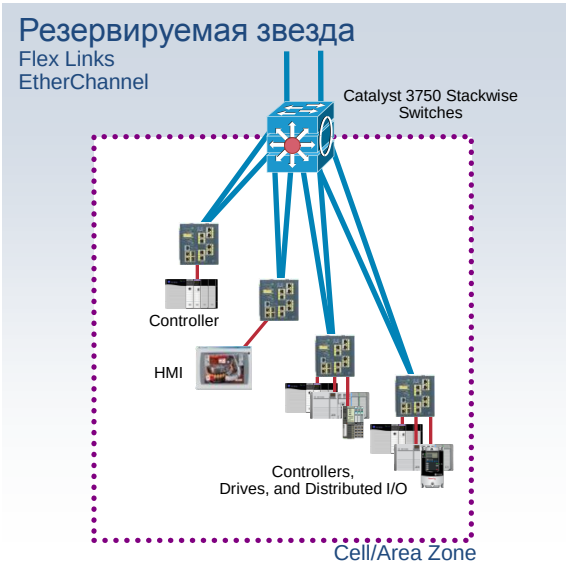
(Уровни 0–2)

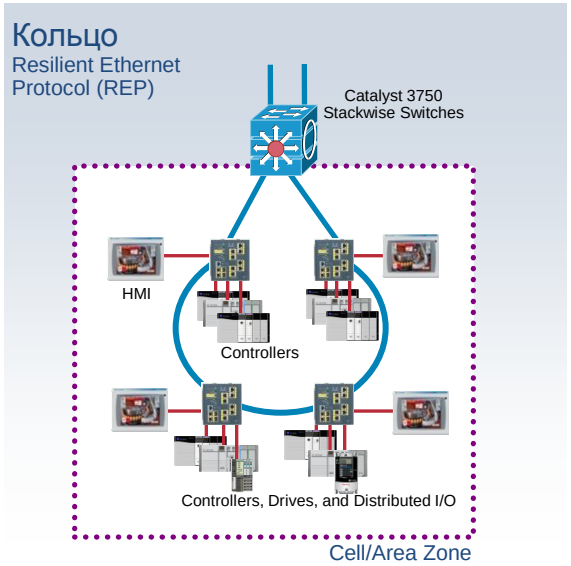


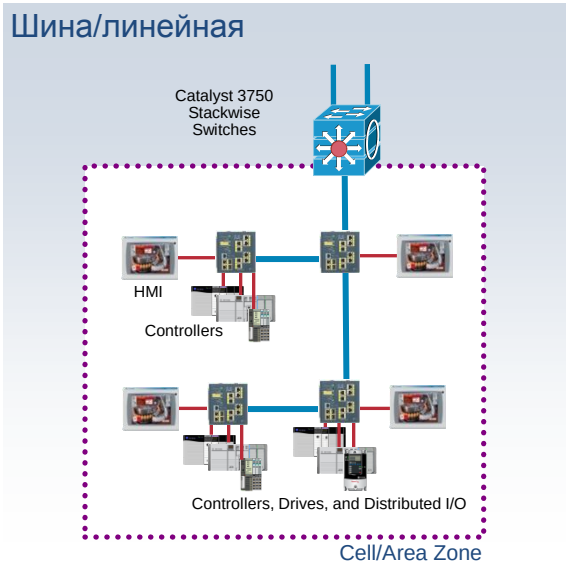
Участок производственного процесса – сеть Layer 2.
Требования к коммутаторам участка производственного процесса:

- Возможность работы в более жестких условиях эксплуатации
- Функциональности устройств, поддержка технологий быстрой сходимости в случае возникновения аварий на сети

Обзор возможных топологий сети участка производственного процесса





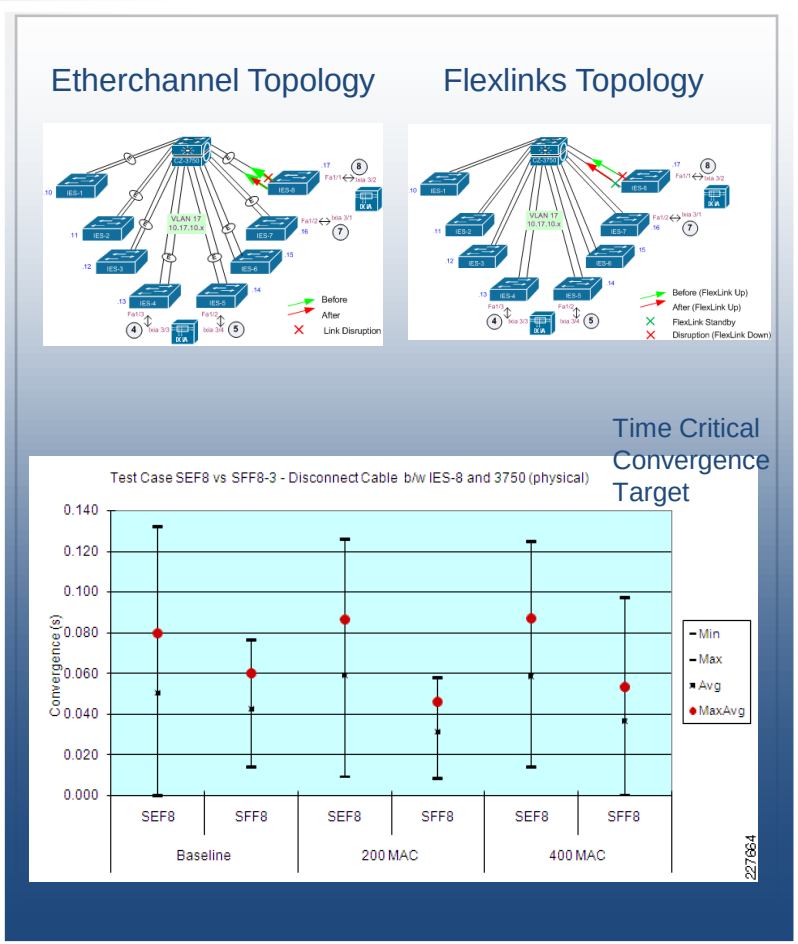


	Звезда	Кольцо	Линейная
Кабельная сеть			
Простота конфигурации			
Стоимость			
Полоса пропускания			
Резервирование и сходимость			
Прерывания при модернизации			
Интеграция с другими сегментами			
С точки зрения TCO	Best	OK	Worst

Тестирование: FlexLinks vs Etherchannel

Резервируемая звезда, оптоволоконные аплинки с Etherchannel и Flexlink с критичными производственными приложениями

- Измеренные значения сходимости в пределах 100 мс
  - Тестировались Multicast и unicast
- Практическое отсутствие влияния на работу приложения



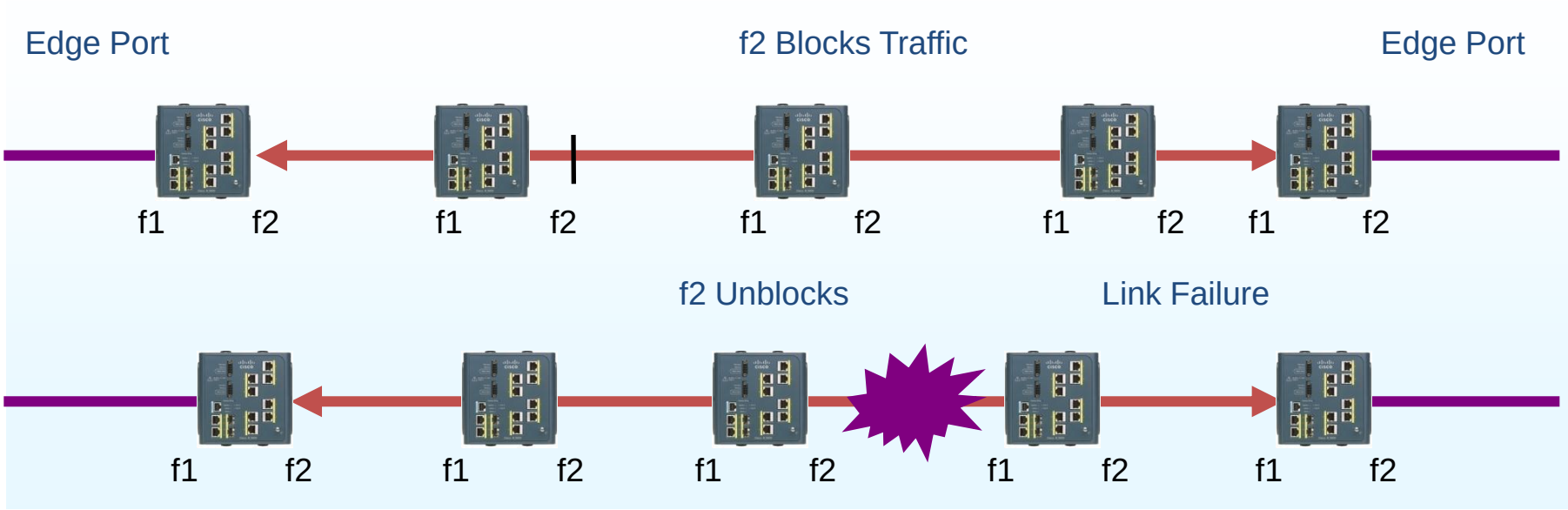
Resilient Ethernet Protocol

Протокол блокировки порта в колцевых топологиях

Когда все соединения активны, блокируется один из портов сегмента

При возникновении аварии порт переводится в активное состояние

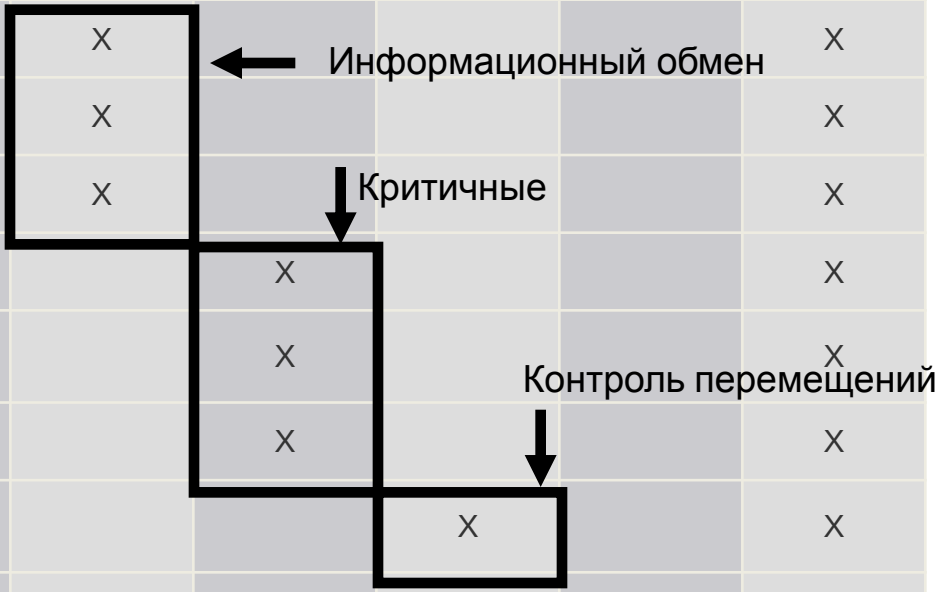
Типовое время сходимости в оптическом кольце ~ 50мс



Выбор технологии для отказоустойчивости сети

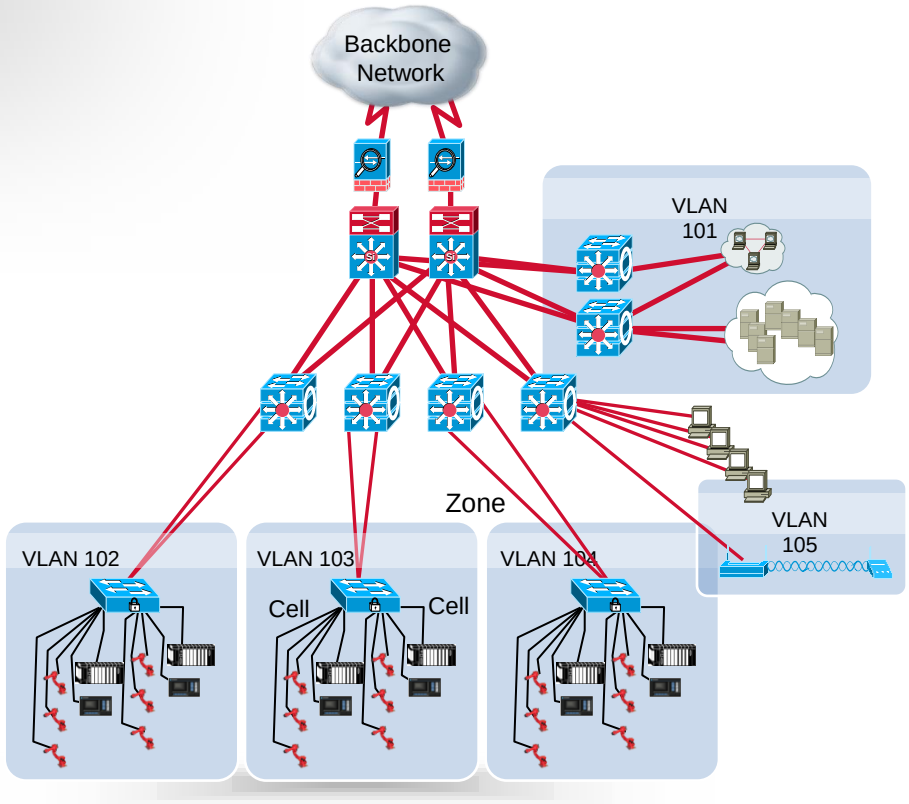
Выбор диктуется требованиями приложений

Протокол	Совместимость	Кольцо	Рез.звезда	Сходим. >250 мс	Сходим. 70-100 мс	Сходим. > 1 мс	Layer 3	Layer 2
STP (802.1D)	X	X	X					X
RSTP (802.1w)	X	X	X	X				X
MSTP (802.1s)	X	X	X	X				X
PVST+		X	X	X				X
REP		X			X			X
EtherChannel (LACP 802.3ad)	X		X		X			X
Flex Links			X		X			X
DLR (IEC & ODVA)	X	X				X		X
StackWise		X	X	X			X	X
HSRP		X	X	X			X	
GLBP		X	X	X			X	
VRRP (IETF RFC 3768)	X	X	X	X			X	



Дополнительные рекомендации сети производственного участка

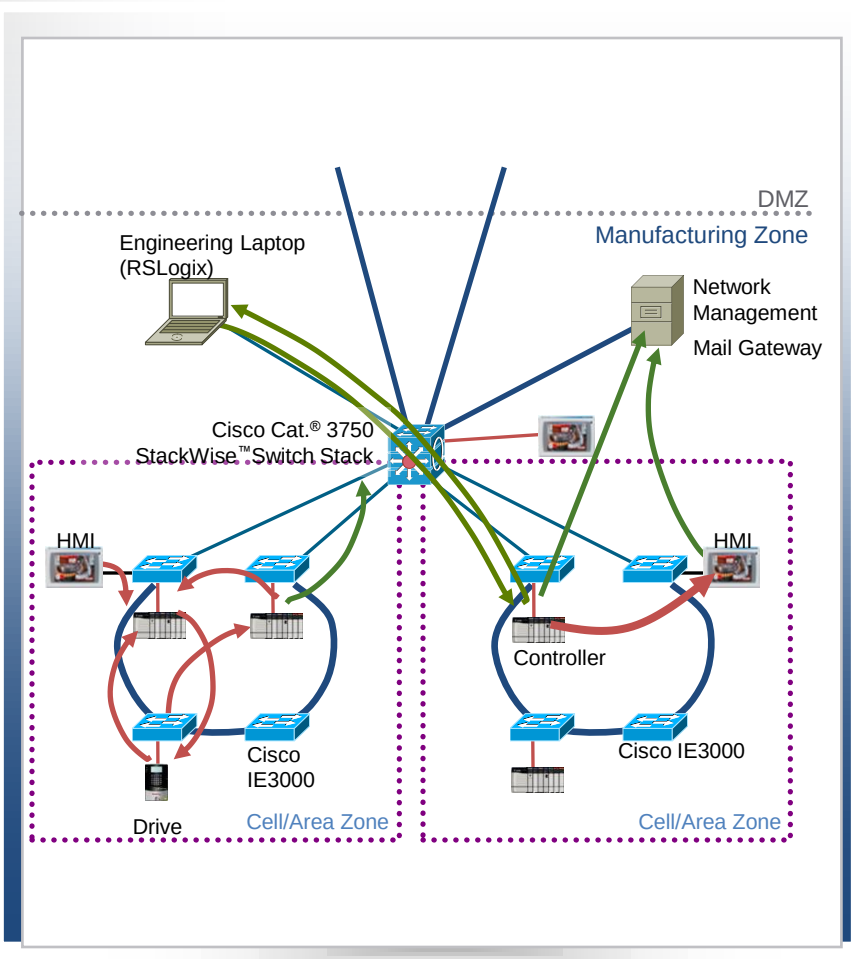
- Сегментация с использованием VLAN’ов (с учетом схемы взаимодействий)
- Использование оптики для уменьшения времени сходимости при обрыве канала
- Использование коммутатора L3, например, IE 3000 для маршрутизации между VLAN’ами



Особенности качества обслуживания в промышленных сетях

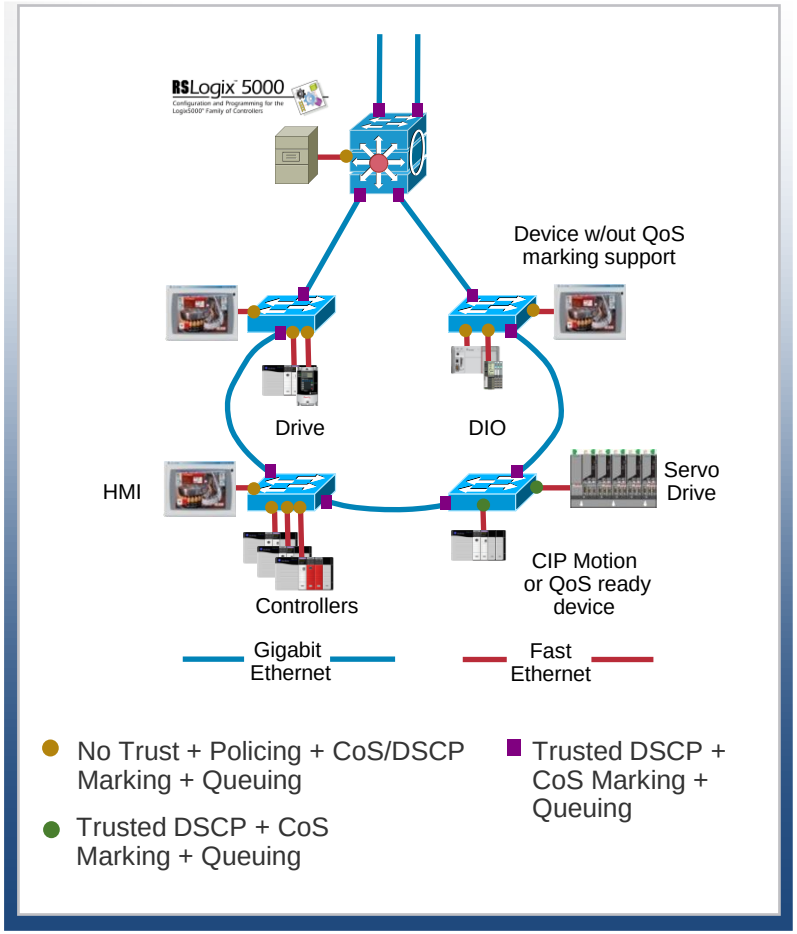
Обмен данными

- Трафик преимущественно (>80%) локализован, цикличный I/O (Скрытый)
  - Источники генерируют сообщения UDP multicast
  - Потребители генерируют сообщения UDP unicast
  - Малый размер пакета: 100-200 байт, высокая частота обмена (каждые 0.5 – 10 миллисекунд).
- Остальной трафик от систем управления (Направленный) направленный вовне
  - CIP, некритичный к/от системам управления
  - Диагностика через HTTP
  - Состояние и аварии через SNMP или SMTP
  - Большие пакеты ~500 байт, низкая частота обмена (сотни миллисекунд)



Рекомендации по дизайну QoS

- Приоритет для чувствительного к задержке трафику
  - Минимальный урон от атак DDoS
- QoS в рамках всей индустриальной сети
- Маркировка полей QoS может выполняться на производственном оборудовании
- Если производственное оборудование не поддерживает маркировку, то она может выполняться на портах коммутатора
  - CIP I/O UDP 2222
  - CIP Explicit TCP 44818

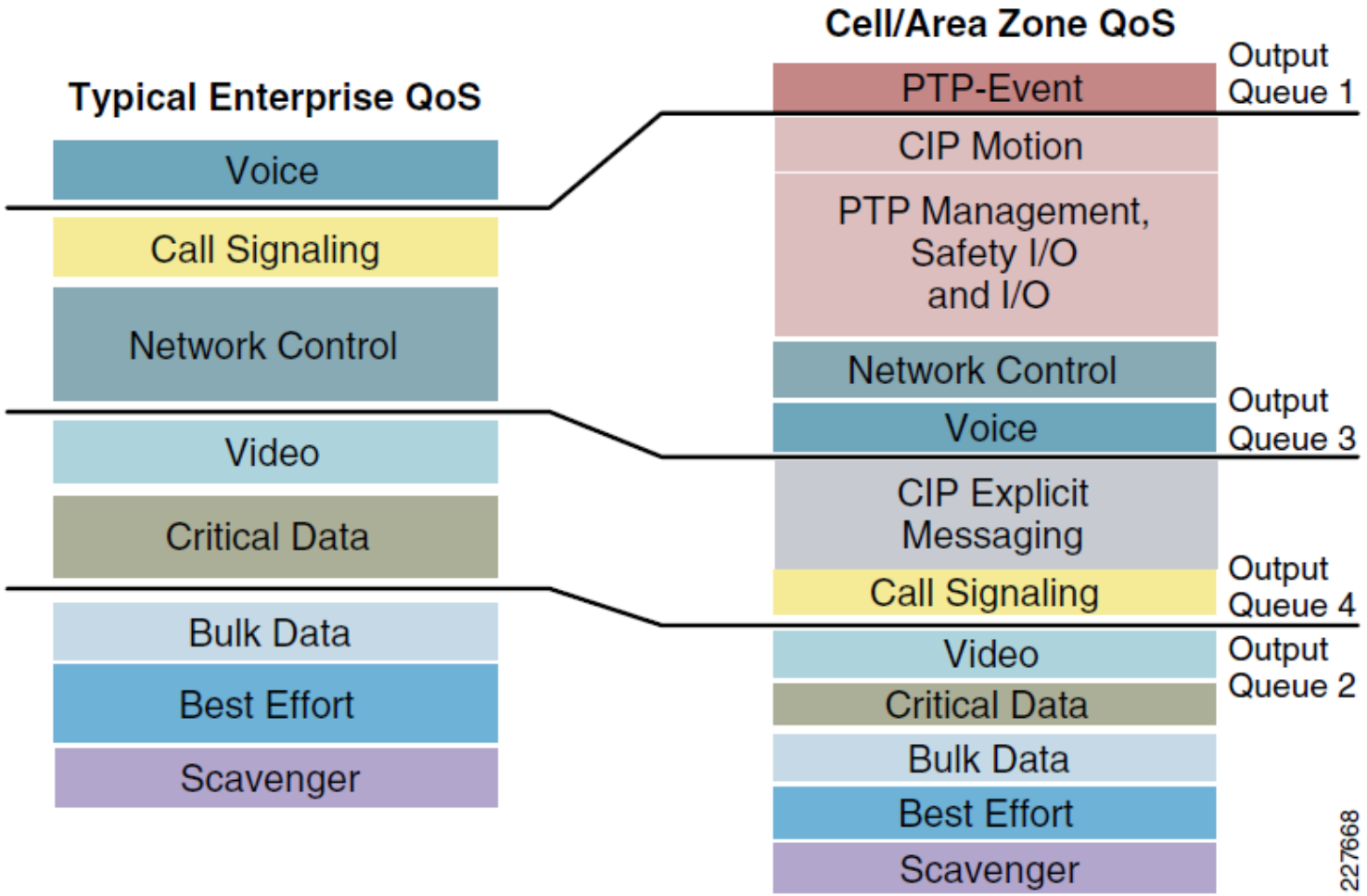


Качество обслуживания - QoS

Приоритезация в исходящих очередях

Модель корпоративной сети

Производственная сеть

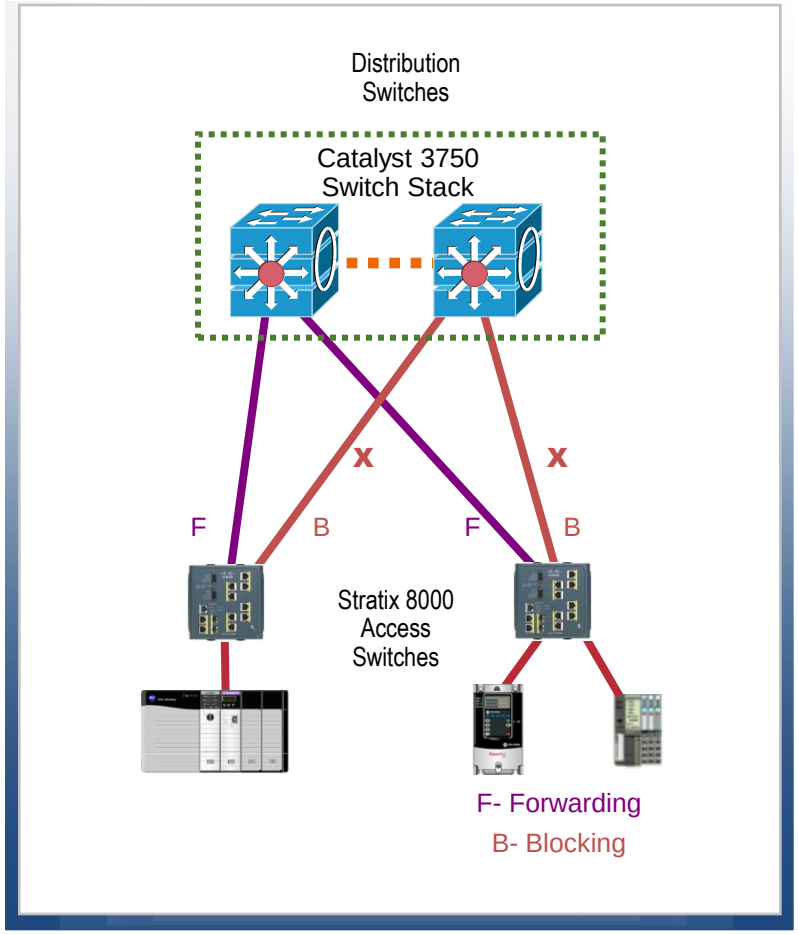


Вопросы

Спасибо за внимание

Spanning Tree Protocol (STP)

- Стандартное решение для обеспечения отказоустойчивости — IEEE 802.1D
- Резервируемая звезда/кольцо
- Контроль возникновения петель, выбор резервного пути
- Не поддерживается на ‘неуправляемых’ устройствах
- Реализации отличаются: STP, RSTP, MSTP and RPVST+
- Согласование с IT до момента реализации



EtherChannel

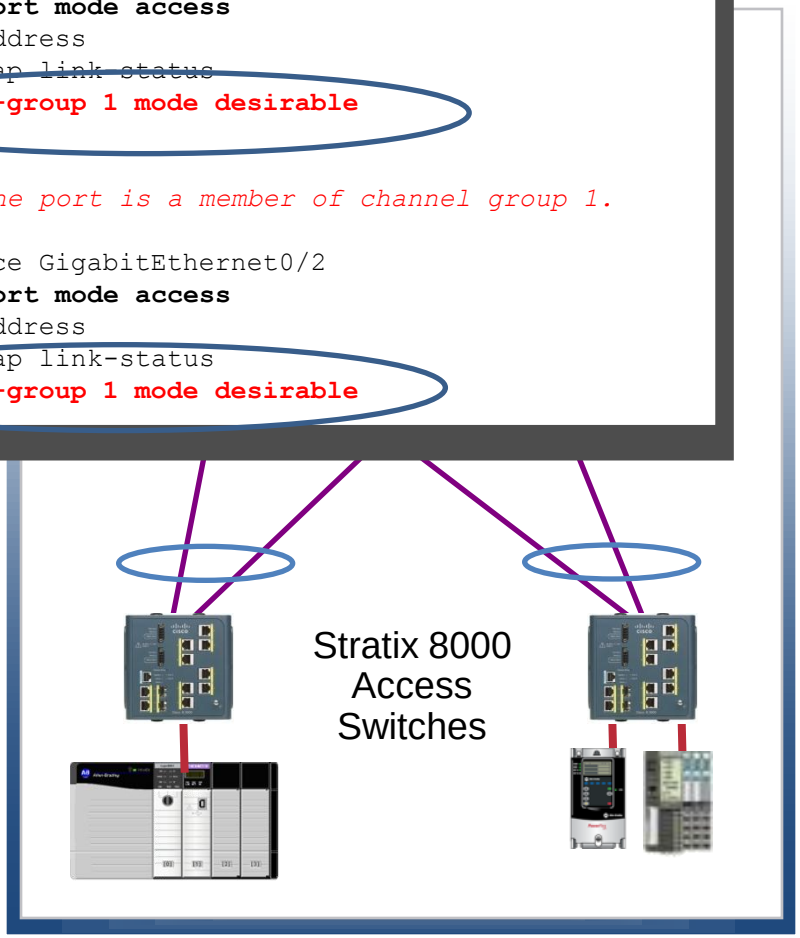
- Link Aggregation Control Protocc (LACP) port aggregation—IEEE 802.3ad
- Резервируемая звезда
- Несколько физических портов образуют логический (от 2 до 8 физических)
- Обеспечивает отказоустойчивость в транковых соединениях

```
!--- The port is a member of channel group 1.


interface GigabitEthernet0/1
switchport mode access
no ip address
snmp trap link-status
channel-group 1 mode desirable
!

 !--- The port is a member of channel group 1.

interface GigabitEthernet0/2
switchport mode access
no ip address
snmp trap link-status
channel-group 1 mode desirable
```



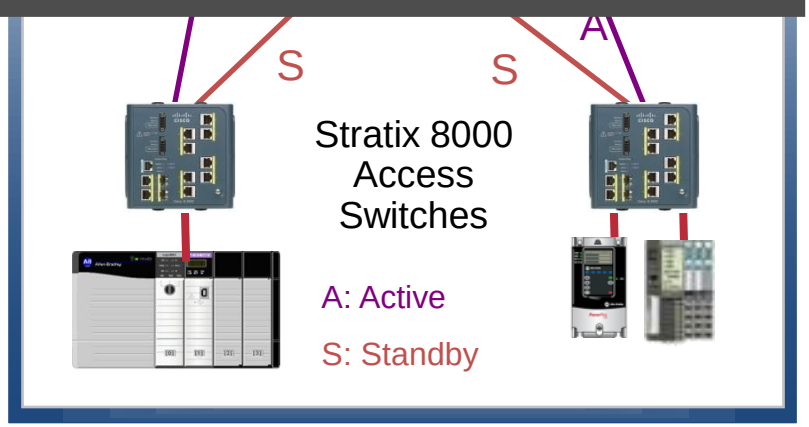
Flex Links

- Технологи
- Резервиру
- Схема осн
- Альтернат
  контроль в
- ‘Неуправл
  поддержив

```
Switch# configure terminal
Switch(conf)# interface fastethernet1/0/1
Switch(conf-if)# switchport backup interface fastethernet1/0/2
Switch(conf-if)# end
Switch# show interface switchport backup

Switch Backup Interface Pairs:


Active Interface Backup Interface State
--------------------------------------------------------------------------------
---
FastEthernet1/0/1       FastEthernet1/0/2       Active Up/Backup Standby
FastEthernet1/0/3       FastEthernet2/0/4       Active Up/Backup Standby
Port-channel1 GigabitEthernet7/0/1    Active Up/Backup Standby
```



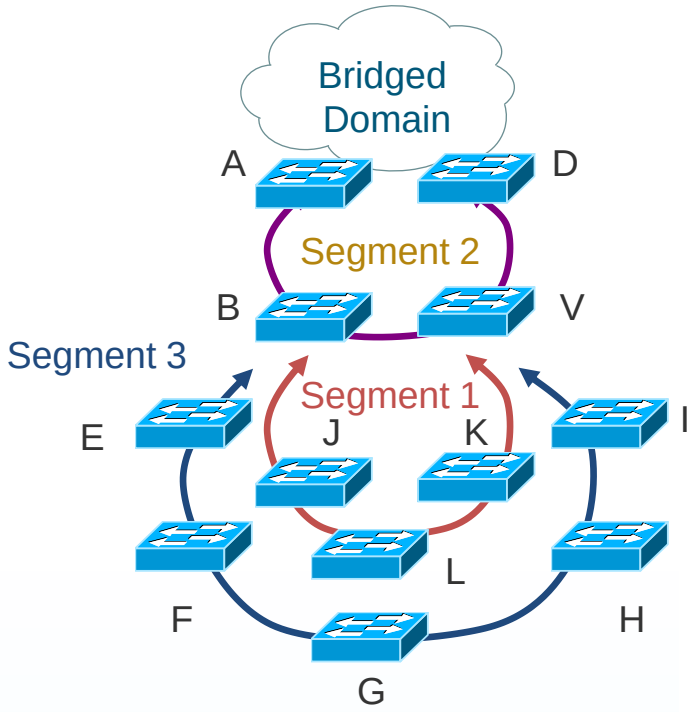
Resilient Ethernet Protocol

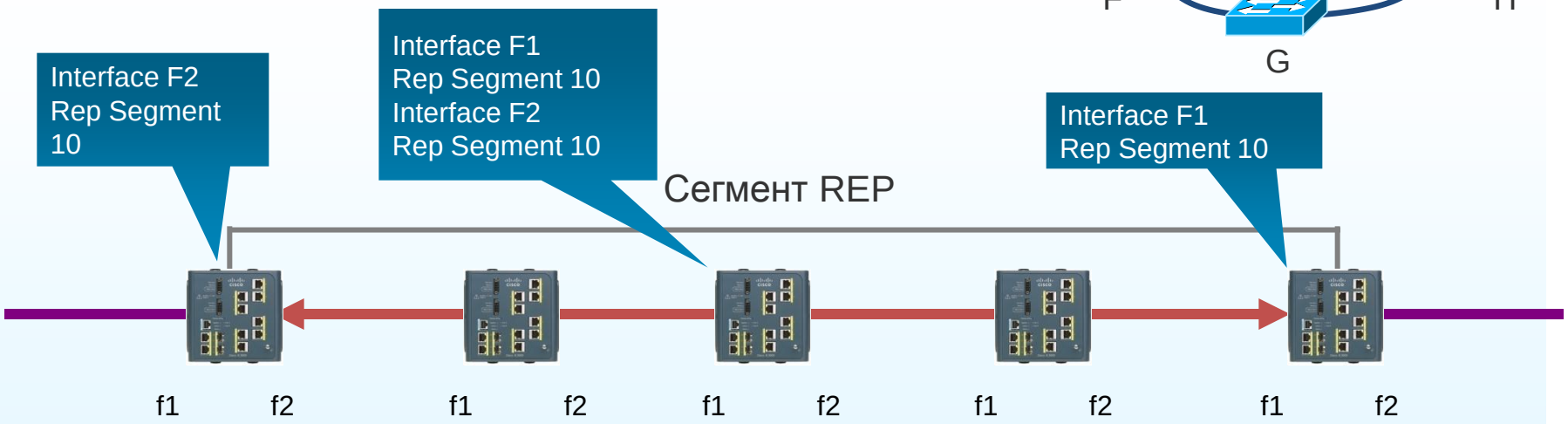
Протокол для сегментов

REP работает в цепочке коммутаторов образующих сегмент

Порт принадлежит уникальному сегменту

Сегменту может принадлежать до 2-х портов на устройстве





Resilient Ethernet Protocol

Кольцевая топология

```
!
rep admin vlan 4
!
vlan 101
 name wtg001
!
vlan 102
 name wtg002
```

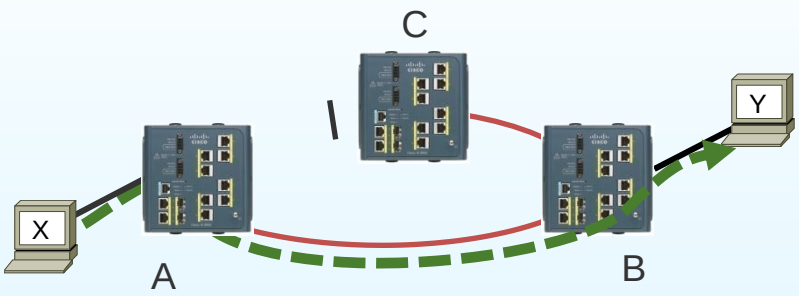
Сегме… …ь …

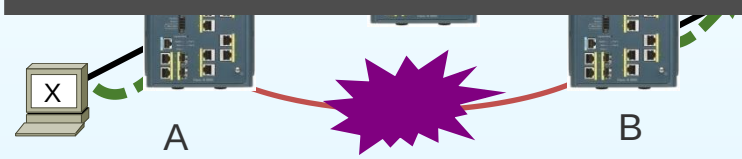
Образ… …ur…

Выбор edge port-a требует доп…
конфигурации

```
!
interface FastEthernet0/1
 description REP fiberloop1
 switchport trunk allowed vlan 4,101-120
 switchport mode trunk
 switchport nonegotiate
 duplex full
 priority-queue out
 rep segment 10 edge primary
 rep preempt delay 15
 rep block port 22 vlan 1-4094
 mls qos trust dscp

!
interface GigabitEthernet0/1
 description REP substation
 switchport mode trunk
 switchport nonegotiate
 priority-queue out
 rep segment 1 edge primary
 rep preempt delay 15
 rep block port 3 vlan 1-4094
 mls qos trust dscp
```





Resilient Ethernet Protocol

- **REP сегментный протокол**
  - Сегмент это цепочка коммутаторов
  - REP блокирует порт в нормальных условиях
  - REP разблокирует порт в случае аварии
- **С использованием сегментов REP можно строить масштабируемые резервные топологии**
- **Поддержка различных видов топологий**
- **Типовое время сходимости в оптическом кольце около 50 мс**
- **Инновация Cisco**