



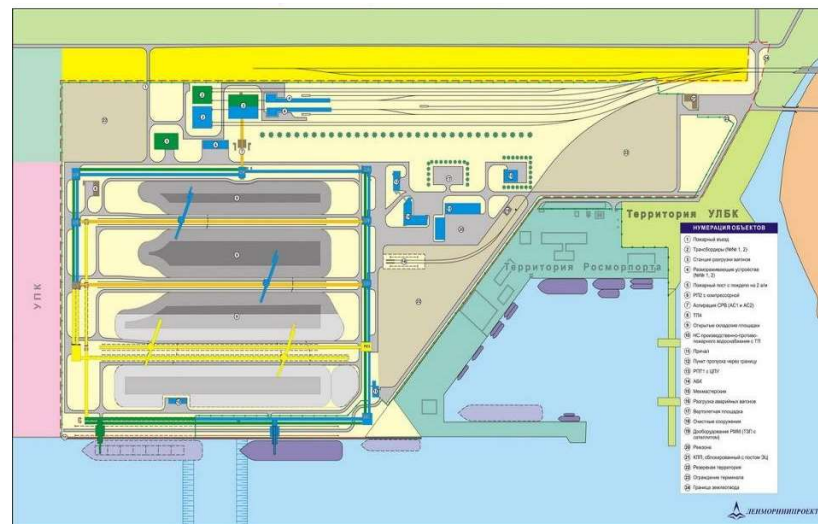
**ОАО «РОСТЕРМИНАЛУГОЛЬ»  
МОРСКОЙ ТОРГОВЫЙ ПОРТ УСТЬ-ЛУГА**

**Реструктуризация производственных сетей  
с реализацией работы в сложных  
эксплуатационных условиях**

**Начальник отдела информационных технологий  
Игнатъев Алексей Сергеевич**

# Общая информация

ОАО «Ростерминалуголь» – самый современный специализированный портовый технологический комплекс для перевалки угля в Российской Федерации. В число основных услуг входят погрузочно-разгрузочные работы, а также транспортно-экспедиторское обслуживание.



- Грузооборот ОАО «Ростерминалуголь» в 2015 году составил 17 468 525,993 тонн угля. Годовой план выполнен на 113%.
- За 12 месяцев 2015 года обработано 282 судна. Максимальное погруженное судно «UBC OTTAWA», дата коносаменты 31 августа 2015 года, приняло к перевозке 107 641 тонн угля. Судно было погружено за 52 часа.
- За двенадцать месяцев 2015 год выгружено 244 146 единиц подвижного состава, что на 9% больше чем в 2014 году.
- Максимальный показатель выгрузки за месяц достигнут в октябре 2015 года – выгружено 24 142 единиц подвижного состава с 1 707 689 тоннами угля.

В 2016 году Предприятию исполняется 20 лет!



## Проблемы

---

- ▶ Присутствие множеств вариантов точек отказа сети
- ▶ Отсутствие времени на техническое обслуживание
- ▶ Мультивендорная архитектура сетевых устройств
- ▶ Выход из строя сетевого оборудования в зонах № В/С
- ▶ Необходимость в зонах № В/С наличия компьютеров и работы Wi-Fi устройств
- ▶ Малая пропускная способность магистральных линий





## Задачи

---

- ▶ Реализация работы сетевого оборудования на производстве в сложных эксплуатационных условиях
- ▶ Увеличение надежности и масштабируемости систем с эксплуатационным сроком до 10 лет с сокращением простоев на техническое обслуживание
- ▶ Монобрендовая стратегии с оптимизацией расходов на эксплуатацию



# Среда

## ▶ Зона № А – кампус

- ▶ Степень загрязнения – малая
- ▶ Большая насыщенность клиентскими устройствами

Сеть ИТ

## ▶ Зона № В – пограничные здания

- ▶ Степень загрязнения – средняя
- ▶ Температурный диапазон – от +5\* до + 25\*

## ▶ Зона № С – промышленные объекты

- ▶ Степень загрязнения – большая
- ▶ Температурный диапазон – от -5\* до + 50\*(тепляк)
- ▶ Влажность – от 60% до 90% (море)
- ▶ Вибрация (вагоноопрокидыватель)

Сеть АСУ





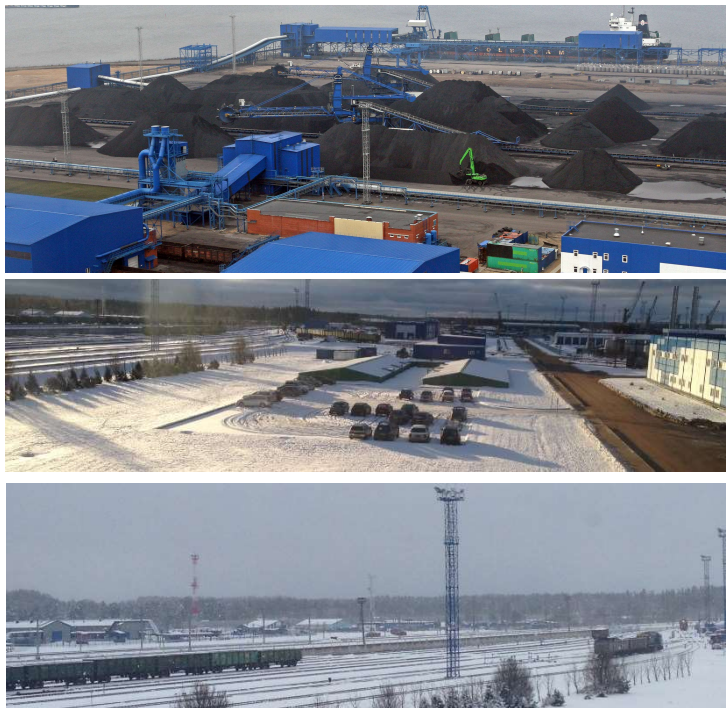
# Визуализация зон

A



Кампус, серверные

B



Ангары, склады, причалы, тех. помещения

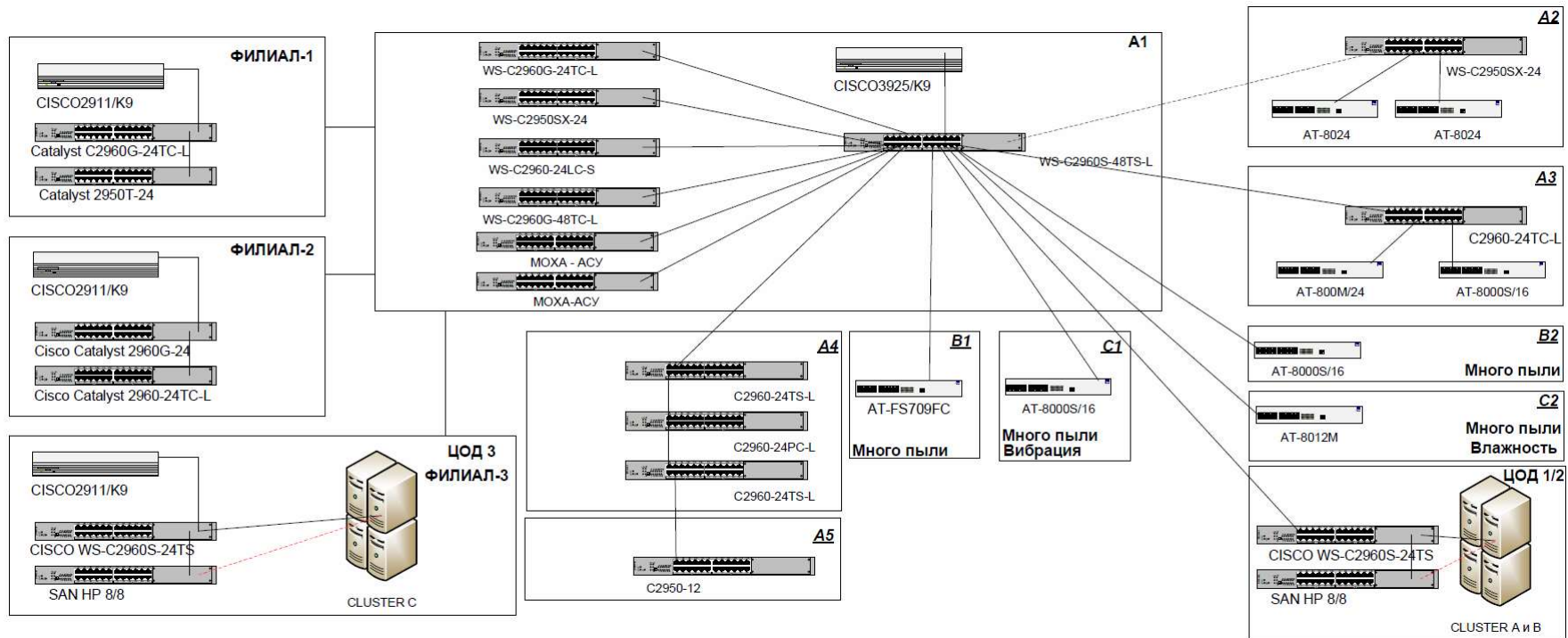
C



Вагонопрокидыватель, тепляк, магнитный сепаратор, конвейерные линии



# Укрупненная схема зон





## Варианты и выбор компании-поставщика

---

### ▶ Проработка:

- ▶ требований к работе
- ▶ сетевой архитектуры

### ▶ Выбор:

- ▶ полнота и целостность архитектуры
- ▶ совместимость с текущими и будущими проектами и опытом работы специалистов
- ▶ вопрос импортозамещения\*

### ▶ Решение:

- ▶ стоимости оборудования
- ▶ количества оборудования
- ▶ затрат на внедрение и обучение



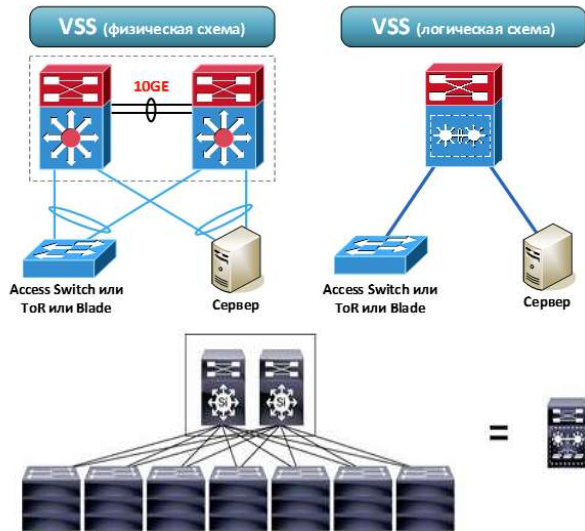
---

▶ \* <https://habrahabr.ru/post/277609/>



# Сеть ИТ\*

- ▶ Варианты работы (звезда/кольцо) и технологии виртуализации коммутаторов (VSS, IRF, стек)



Варианты:

VSS

- Cisco 4500E/4500X, 6500E/6800

Минусы:

- стоимость
- много нюансов к железу и версиям ПО

Cisco Catalyst Instant Access

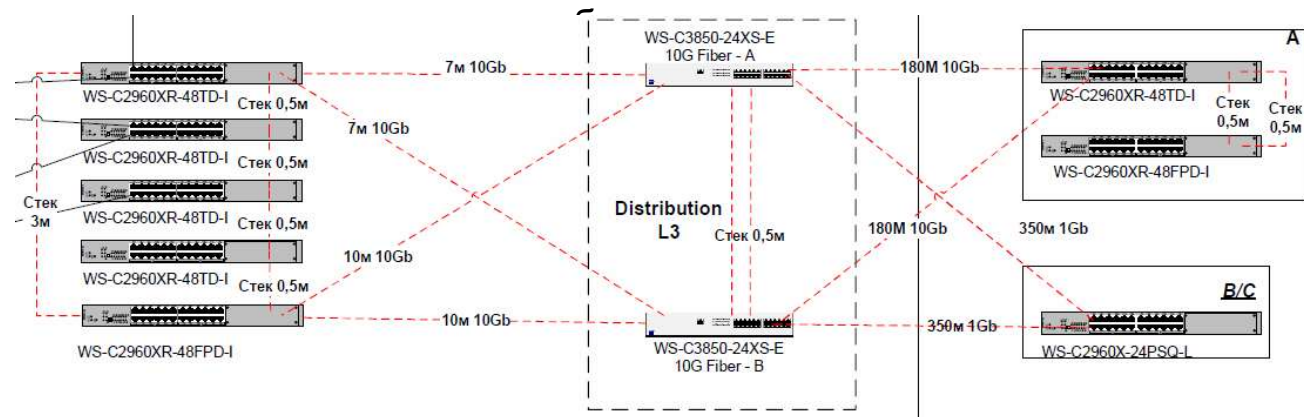
- 6500E/6800 с супервизорами Sup2T и линейными платами

Минусы:

- только коммутаторы Cisco 6800ia или 3560CX
- стоимость Cisco 6800ia приближается к стоимости свича

Решение:


- FlexStack+
- агрегация линков
- резервные блоки горячей замены
- возможность работы в зоне B
- две базовые модели
- масштабируемость до 3 уровня



▶ [\\*http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Oct2015/Campus\\_LAN\\_Wireless\\_LAN\\_Design\\_Oct2105.pdf](http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Oct2015/Campus_LAN_Wireless_LAN_Design_Oct2105.pdf)




# Решение сети ИТ



**Catalyst WS-C3850-24XS-E 10G Fiber**

- Терминирование беспроводных CAPWAP туннелей
- Интегрированный контроллер: до 50 точек доступа
- До 2000 клиентов на каждый стек
- Пропускная способность Wireless 40 Гб/с
- Пропускная способность восходящего канала (Uplink) 40 Гбит/с
- Пропускная способность стекирования 480 Гбит/с
- Поддержка питания POE+ на всех портах
- Вентиляторы и блоки питания с поддержкой горячей замены
- Granular QoS/Flexible NetFlow
- Стек по питанию Stackpower
- Модели с UPOE
- Скорость каналов line rate на всех портах



**Catalyst WS-C2960XR-48TD-I / Catalyst WS-C2960XR-48FPD-I**

- Dual Core CPU
- Отказоустойчивые источники питания с возможностью горячей замены (2960XR)
- Энергосберегающий режим Deep Sleep
- Обратная совместимость стека FlexStack с 2960-S
- FlexStack+ с пропускной способностью 80 Гб/с
- 2 x 10G или 4 x 1G
- Поддержка EEE на портах доступа
- 8 очередей на порт
- Буферы 4 Мб
- MacSec Ready
- Netflow Lite на всех портах

**Точка доступа Aironet 2600i**

- Для работы внутри помещений и в офисах



- Технология CleanAir
- ClientLink 2.0
- Привлекательный дизайн
- Внутренние встроенные двухдиапазонные антенны

AIR-CAP2602I-x-K9	Двухдиапазонная точка доступа 802.11 a/g/n с контроллерным управлением
AIR-CAP2602I-xK910	Точка доступа 802.11 a/g/n с контроллерным управлением, упаковка 10 шт.
AIR-SAP2602I-x-K9	Двухдиапазонная (802.11 a/g/n) автономная точка доступа
AIR-SAP2602I-xK9-5	Автономная точка доступа 802.11 a/g/n, упаковка 5 шт.

**AIR-CAP2702I-R-K9\***

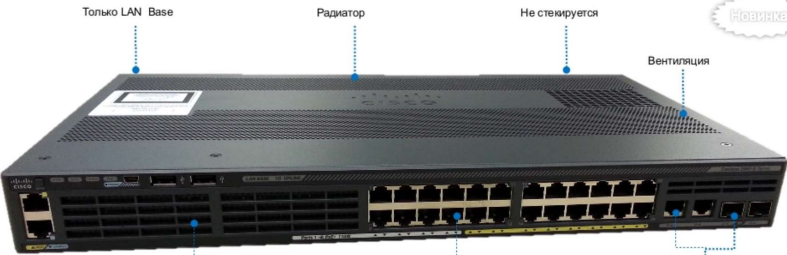
**Точка доступа Aironet 2600e**

- Для заводов, складов и других промышленных объектов



- Технология CleanAir
- ClientLink 2.0
- Корпус повышенной прочности
- 4 наружные двухдиапазонные антенны (продаются отдельно)
- Расширенный рабочий диапазон температур

AIR-CAP2602E-x-K9	Двухдиапазонная точка доступа 802.11 a/g/n с контроллерным управлением, с внешней антенной
AIR-CAP2602E-xK910	Точка доступа 802.11 a/g/n с контроллерным управлением, с внешней антенной, упаковка 10 шт.
AIR-SAP2602E-x-K9	Двухдиапазонная (802.11 a/g/n) автономная точка доступа, с внешней антенной
AIR-SAP2602E-xK9-5	Автономная точка доступа 802.11 a/g/n, с внешней антенной упаковка 5 шт.



**Catalyst WS-C2960X-24PSQ-L\*\***

- Только LAN Base
- Радиатор
- Не стекируется
- Новинка
- Вентиляция
- Фронтальная вентиляция
- Первые 8 портов PoE/PoE+ (110 Вт PoE бюджет)
- 4 апгрейд порта 2 \* SFP + 2 \* 1G BT

\* <http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-2700-series-access-point/datasheet-c78-730593.html>  
 \*\* <http://www.cisco.com/c/en/us/support/switches/catalyst-2960x-24psq-l-cool-switch/model.html>



# Решение сети ИТ



## iROBO-6000-Ni36CE\*:

- Встраиваемый компьютер с Intel Core i3-3120ME 2.4ГГц, 4ГБ DDR3 RAM, 320ГБ HDD, VGA, DVI-D, 2xDisplay Port, 2xGb LAN, 5xRS-232, 1xRS-232/422/485, 4xUSB 3.0, 2xUSB 2.0, 1xPCI-Express x4 слот, адаптер питания 120Вт
- Конструкция корпуса: Алюминиевый корпус
- Вид монтажа: Настольный, Монтаж на стене
- Тип установленного процессора: Intel Core i3-3120ME
- Тип: Безвентиляторный
- Температура эксплуатации: -5 ... 55 °С



## Наружная точка доступа Cisco Aironet серии 1530\*\*:

- 1530I: 3x3 MIMO, 3 пространственных потока (2,4 ГГц) и 2x3 MIMO, 2 пространственных потока (5 ГГц)
- 1530E: 2x2 MIMO, 2 пространственных потока (2,4 ГГц) и 2x2 MIMO, 2 пространственных потока (5 ГГц)
- 20 МГц (2,4 и 5 ГГц) и 40 МГц (5 ГГц только) каналы
- Скорость передачи данных PHY до 300 Мбит/с
- PoE (802.3at+) / (UPoE)
- Температура эксплуатации: -30° до 65°С

Плюсы: Mesh сеть

Проблемы: письма в ФСБ (разрешения на ввоз)



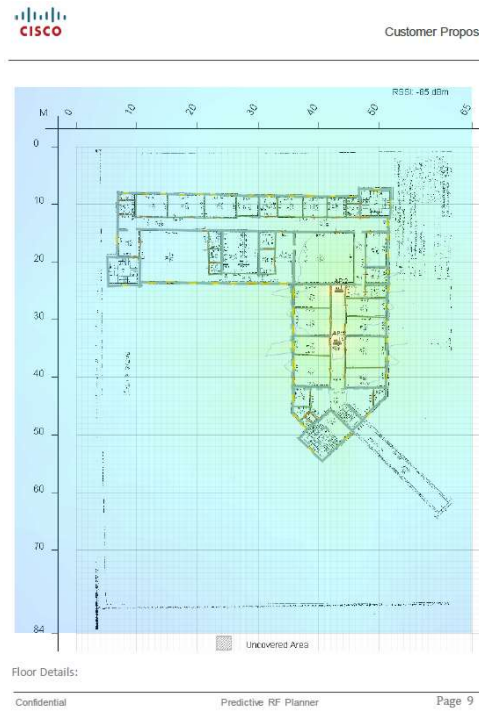
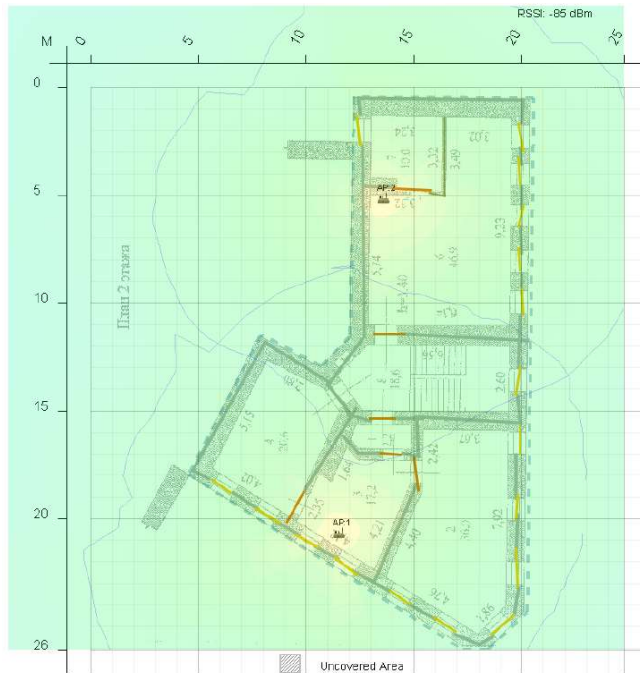
\* <http://irobo.ru/catalog/irobo-6000-ni36ce>

\*\* [http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1530-series/data\\_sheet\\_c78-728356.html](http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1530-series/data_sheet_c78-728356.html)



## Расчет зон покрытия Wi-Fi в зависимости от внешних условий

- ▶ Проанализировать необходимость зон покрытия Wi-Fi на территории и в филиалах
- ▶ Программный расчет расположений AP по этажам с учетом материала стен и архитектуры здания посредством Cisco Prime Infrastructure\* на 2,4 Ghz и 5 Ghz
- ▶ Проверка покрытия с помощью инструментов Wifi Analyzer / AirMagnet WiFi Analyzer + AirCheck\*\*



### Точка доступа AP-2600

- ClientLink 2.0 – 3x4, 3SS, MIMO, формирование диаграммы направленности, система антенн
- Двухдиапазонный радиотракт с 3 передающими и 4 приемными каналами (дополнительный приемник радиосигнала для повышения пропускной способности восходящего канала)
- Использование архитектуры 3x4:3 (поддержка скорости до 450 Мбит/с)
- Поддержка новых скоростей 3-SS MCS 16-23
- Совместимость с существующими монтажными кронштейнами и PoE 802.3af
- Поддержка анализа радиочастотной среды по технологии Cisco CleanAir

RTP2	2	NA
KNPG	2	NA
RTP3	2	NA
KNPG2	2	NA
Grand Total		\$2,867.60

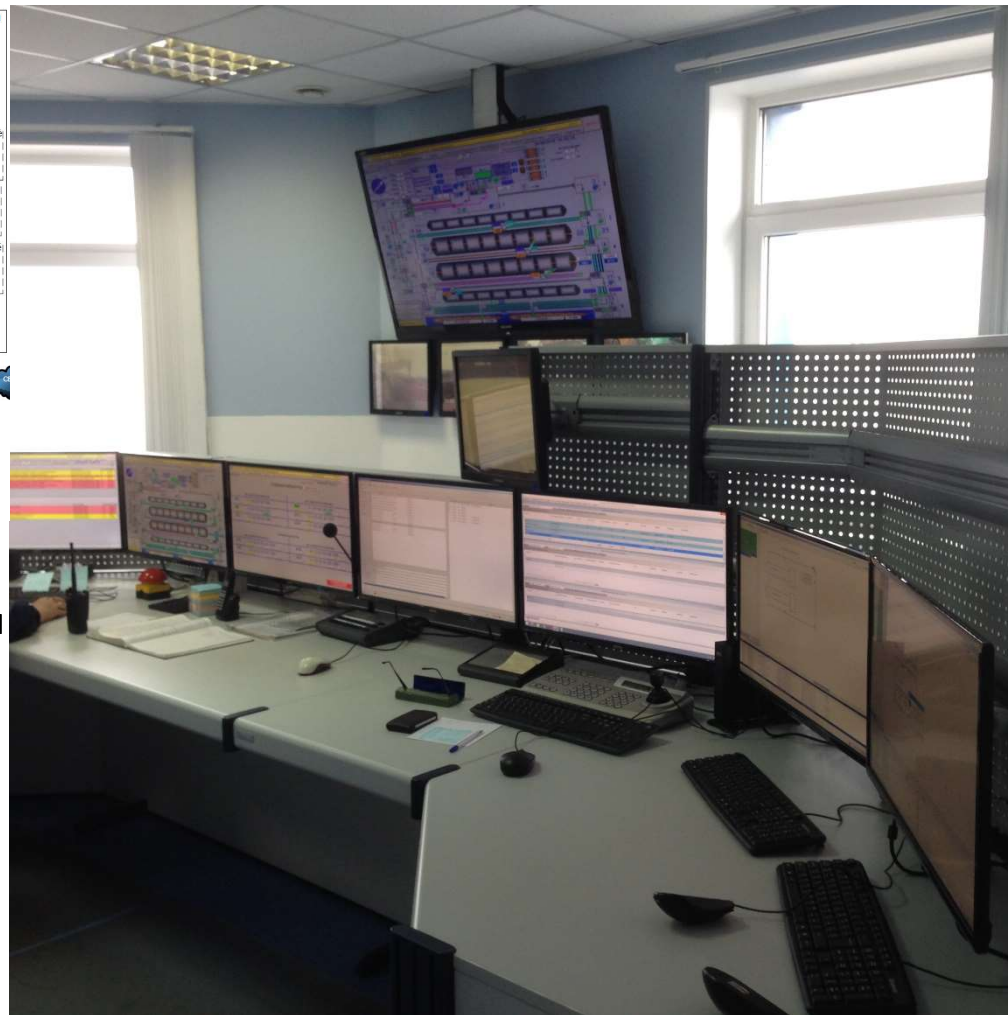
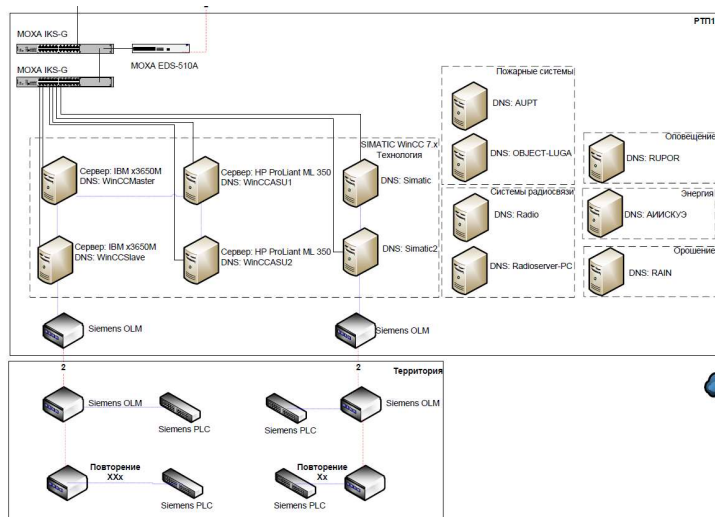
Product Image	Part Number	Quantity	Total Price
	L-LIC-CT5508-UPG: Primary SKU for CT5508 upgrade licenses (Delivery via Email)	1	\$2,495.00
Grand Total			\$2,495.00

\* <http://www.slideshare.net/CiscoRu/cisco-prime>

\*\* <http://www.flukenetworks.com/enterprise-network/wireless-design-analysis-and-security#family-product-list-14>



# Сеть АСУ ТП

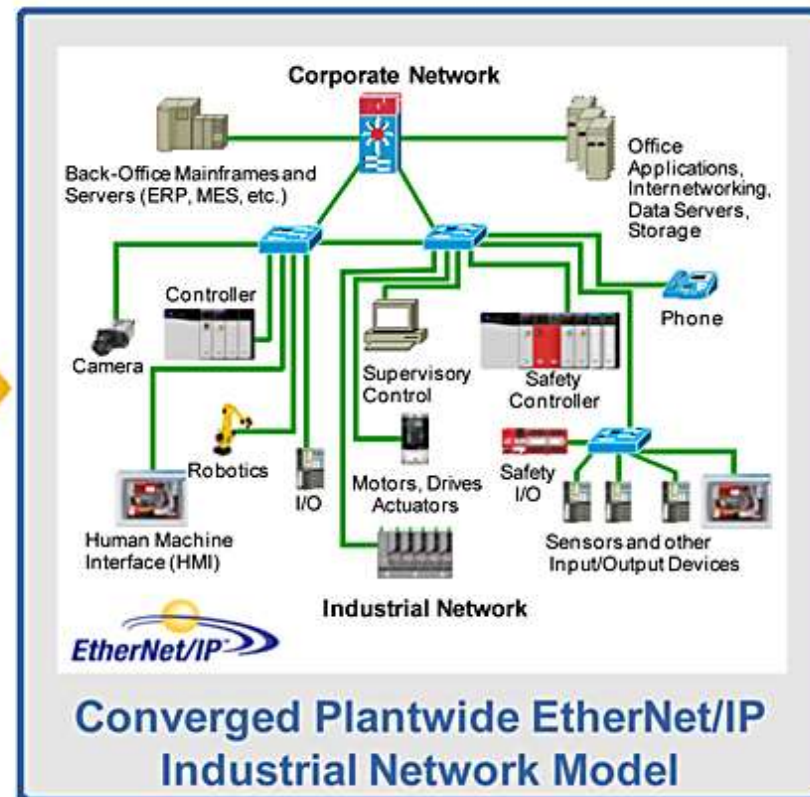
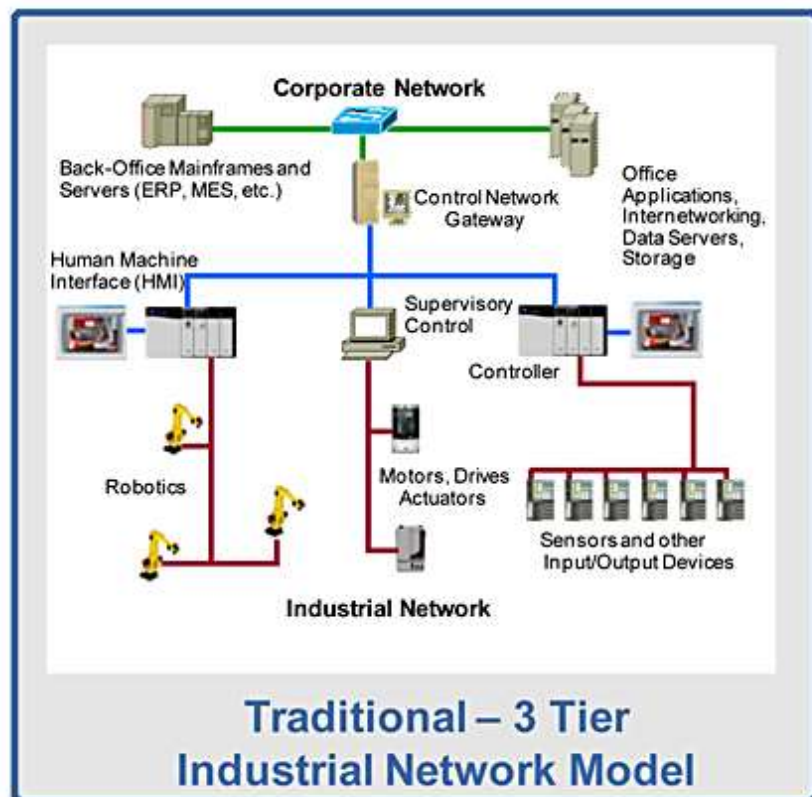


## Вводные данные:

- традиционная 3х уровневая модель сети АСУ ТП
- базирование на SIEMENS SIMATIC WINCC 7.X с спец. линейными платами
- сеть представляет гирлянду
- консервативный тип сети
- не требуются высокие скорости (100Base FX)
- высокая наработка на отказ



# Реструктуризация и типы сетей АСУ ТП

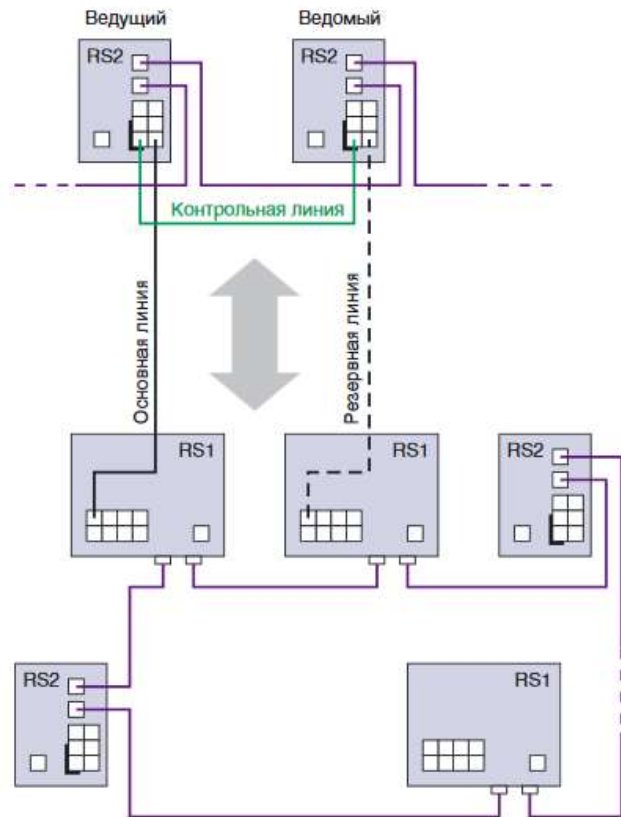


На текущий момент происходит постепенная интеграция ИТ инфраструктур производства и офиса в глобальные системы:

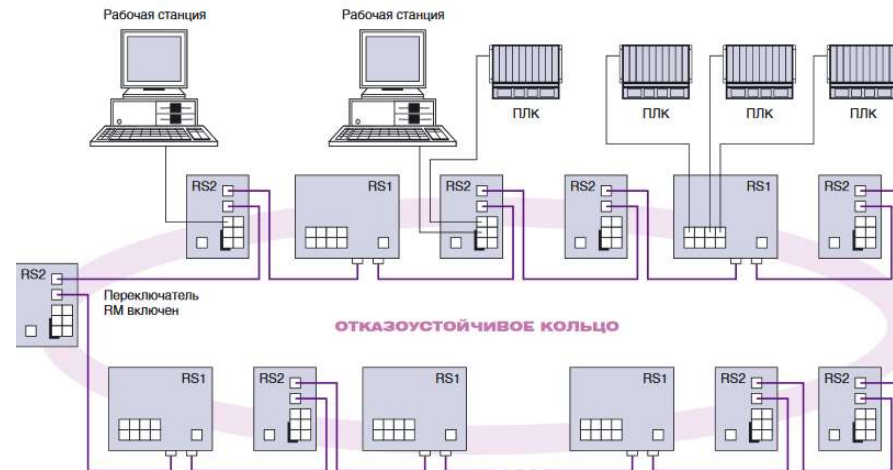
Текущие внутриконтроллерные сети с использованием Ethernet становятся все более популярными, постепенно вытесняя сети с технологиями ModBus, Profibus, COM и происходит постепенный переход от трех уровней к использованию только Ethernet/IP:



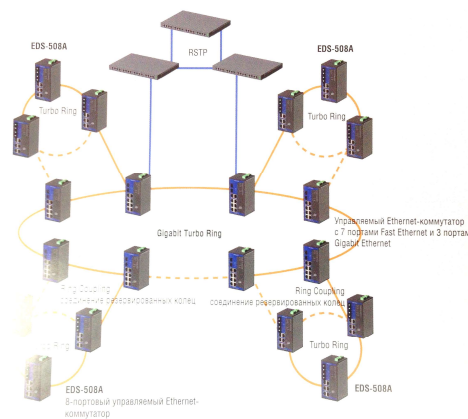
# Типовая структура АСУ ТП



Дублированное соединение сегментов сети с использованием коммутаторов



Кольцевая топология с использованием коммутаторов



## Варианты работы

- ▶ кольцо, двойное кольцо (Turbo Ring)
- ▶ Звезда
- ▶ RSTP



## Решение сети АСУ ТП



МОХА IKS-G6524A\*

- Управляемый коммутатор: 2 уровня с 24 портами: с 20 x 100/1000BaseSFP и 4 x 10/100/1000BaseTX/SFP (combo), с 2 изолированными источниками питания 110/220 В перем. (85 ~ 264 В перем.)
- Возможность резервирования связи: Резервированное кольцо Turbo Ring, "Связующее дерево" Spanning Tree, Turbo Chain (время восстановления соединения менее 20 мсек.)
- Возможность подключения резервного источника электропитания: Есть
- Рабочая температура, град.: -10 ~ +60 С



Серия EDS-510A\*\*

- Управляемый коммутатор: 7 x 10/100BaseTX, 3 x Gigabit SFP (оптика), с расширенным диапазоном температур
- Возможность резервирования связи: Резервированное кольцо Turbo Ring, "Связующее дерево" Spanning Tree, Turbo Chain (время восстановления соединения менее 20 мсек.)
- Возможность подключения резервного источника электропитания: Есть
- Рабочая температура, град.: -40 ~ +75 С

\* [http://www.moxa.ru/shop/ethernet/19\\_inch/iks/iks-g6524a/](http://www.moxa.ru/shop/ethernet/19_inch/iks/iks-g6524a/)

\*\*<http://www.moxa.ru/shop/ethernet/managed/gigabit/eds-510a/>





# Соединение сетей ИТ и АСУ ТП



Cisco ASA 5506H-X — NGFW для критичных инфраструктур и объектов. 5506H-X — особо защищенный МСЭ нового поколения (NGFW), специально ориентированный на защиту от угроз. Оборудован корпусом повышенной защищенности для работы в промышленных средах.



Индустриальный маршрутизатор IE3000-8TC, выполняющий функции межсетевого экрана (сертифицирован в ФСТЭК России)

Требования	ASA-X / ASA-SM	NGFW	IPS / NGIPS / wIPS	AMP / FireAMP	ISE / TrustSec	ESA	WSA	CTD	AC	VSG / ASA v
Идентификация и аутентификация	+	+	+		+	+	+		+	
Управление доступом	+	+	+	+	+	+	+	+	+	
Ограничение программной среды										
Защита машинных носителей					+					
Регистрация событий безопасности	+	+	+	+	+	+	+	+	+	+
Антивирусная защита				+						
Обнаружение вторжений		+	+	+			+	+		
Анализ защищенности		+			+			+		
Обеспечение целостности		+	+	+		+	+			
Обеспечение доступности	Обеспечивается любым решением компании Cisco, в т.ч. и не относящимся к решениям по информационной безопасности									
Защита среды виртуализации		+	+	+	+			+		+
Защита технических средств										
Защита АСУ ТП	+	+	+	+	+	+	+	+	+	
Безопасная разработка	Обеспечивается с помощью подхода Cisco к безопасной разработке (CSDL)									
Управление обновлениями					+					
Планирование мероприятий										
Обеспечение действий в нестандартных ситуациях										
Обучение пользователей										
Анализ угроз и рисков				+						
Управление инцидентами		+	+	+	+			+		
Управление конфигурацией	Обеспечивается системами управления сетью и информационной безопасностью									

**Примечание:**

ASA-X – Cisco ASA 5500-X (5512, 5515, 5525, 5545, 5565, 5585), а также IOS Firewall  
 ASA-SM – Cisco ASA Service Module для Catalyst 6500 / Catalyst 6800 / Catalyst 7800  
 NGFW – Cisco ASA NGFW, Cisco AVC, Sourcefire NGFW  
 IPS – Cisco IPS 4200/4300/4500, Cisco IOS IPS, Cisco IPS-AIM, Cisco AIP-IPS  
 NGIPS – Sourcefire NGIPS  
 wIPS – Cisco Wireless Adaptive IPS  
 AMP – Sourcefire Advanced Malware Protection  
 ISE – Cisco Identity Service Engine, включая Virtual ISE  
 ESA – Cisco E-mail Security Appliance, включая Virtual ESA  
 WSA – WSA – Cisco Web Security Appliance, включая Virtual WSA, а также Cisco Cloud Web Security  
 CTD – Cisco Cyber Threat Defense  
 AC – Cisco AnyConnect  
 VSG – Virtual Security Gateway  
 ASA v – Virtual ASA