

Cisco Expo 2011



Использование маршрутизаторов ASR1000 в корпоративных сетях

Докладчик:
Дмитрий Шилов, системный инженер
dmishilo@cisco.com

innovate *together*

СОДЕРЖАНИЕ

- Обзор серии ASR1000
- Использование ASR1000 в сети предприятия
- Функционал Easy Virtual Network (EVN)



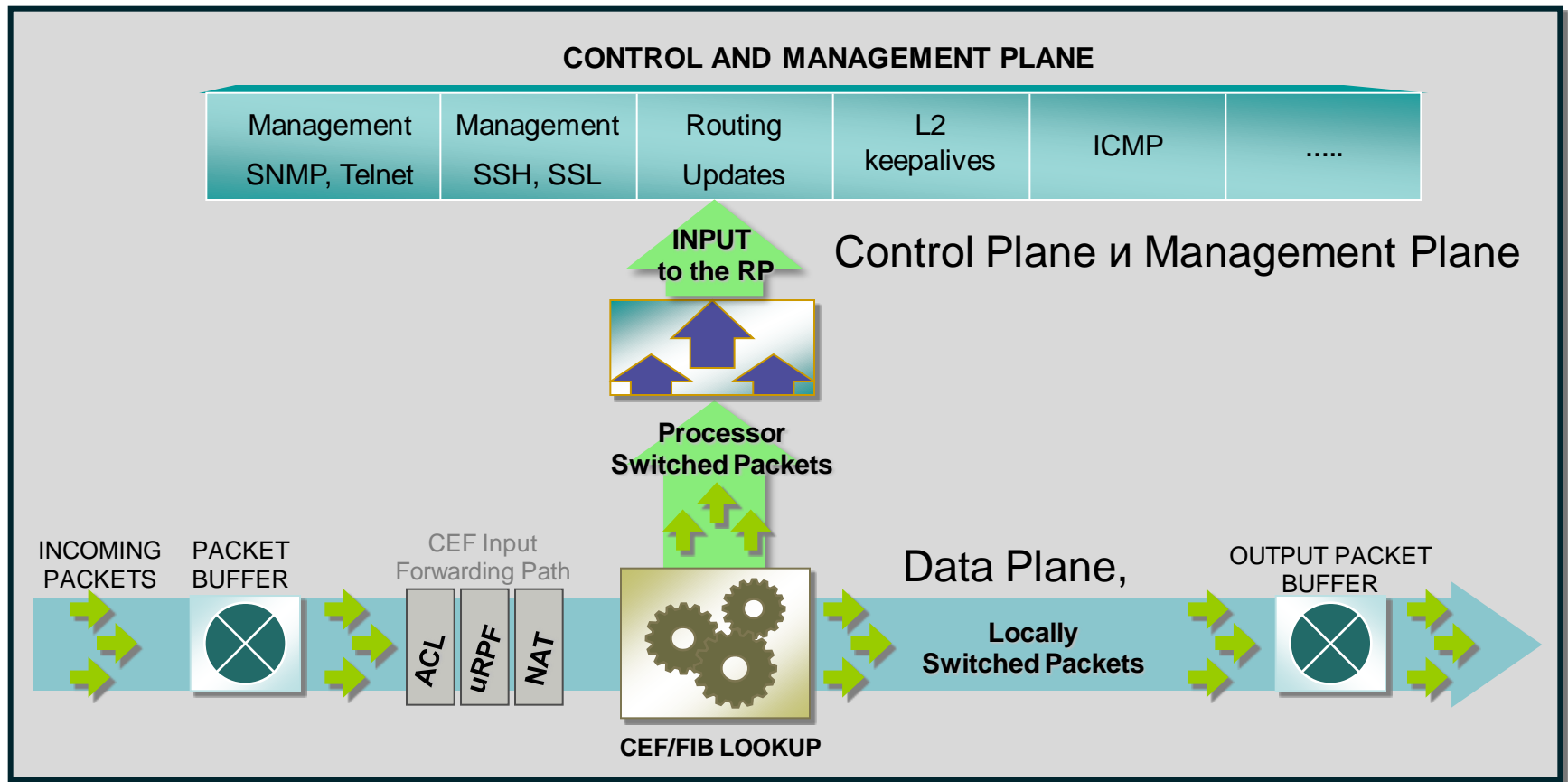
Обзор серии маршрутизаторов ASR1000



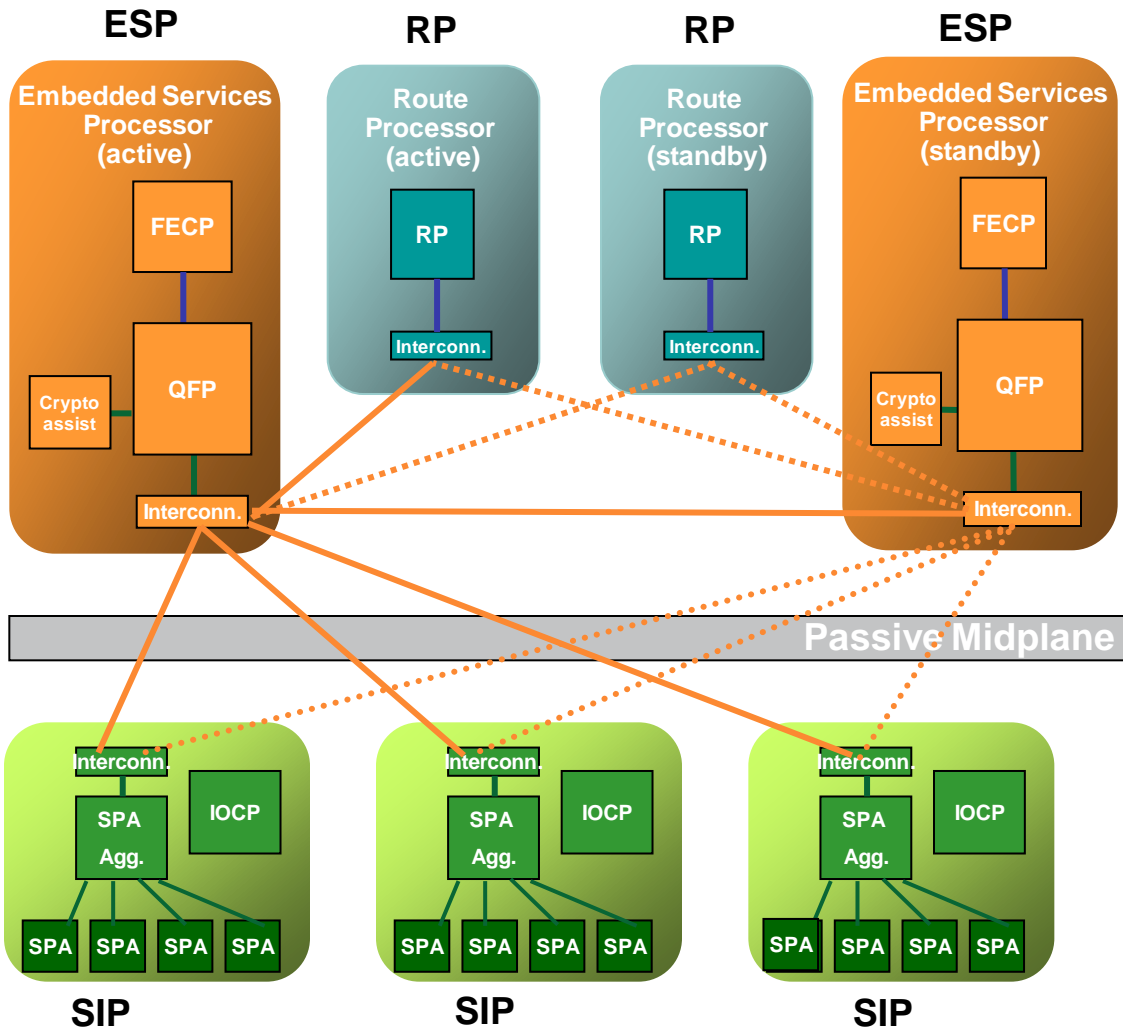
Основная задача маршрутизатора – обрабатывать трафик

Три типа обработки трафика:

Data Plane, Control Plane и Management Plane



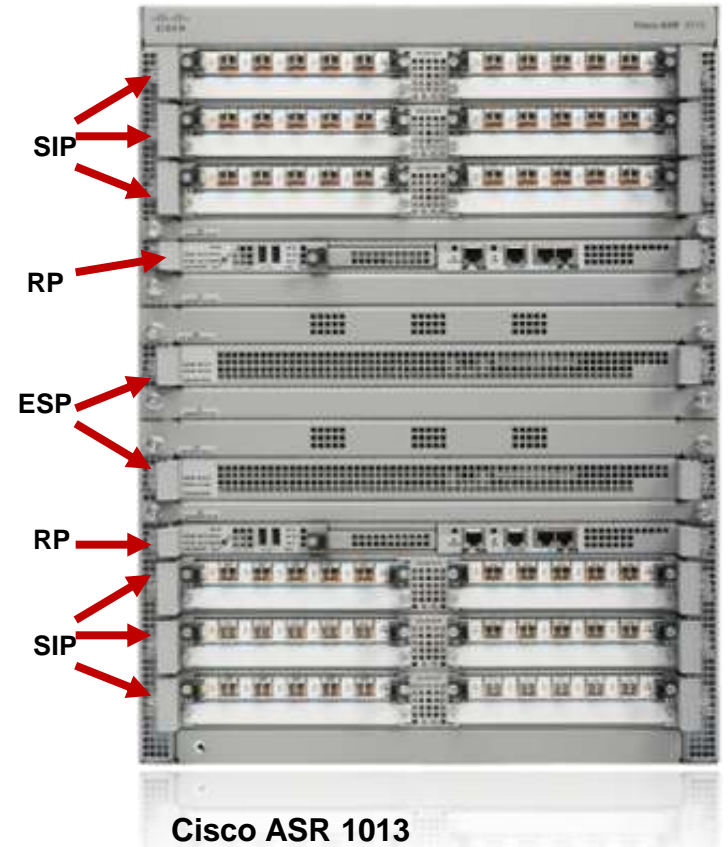
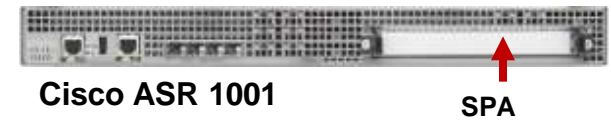
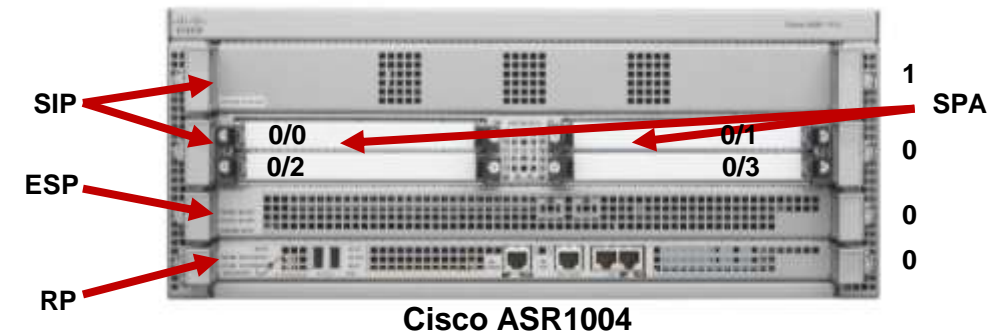
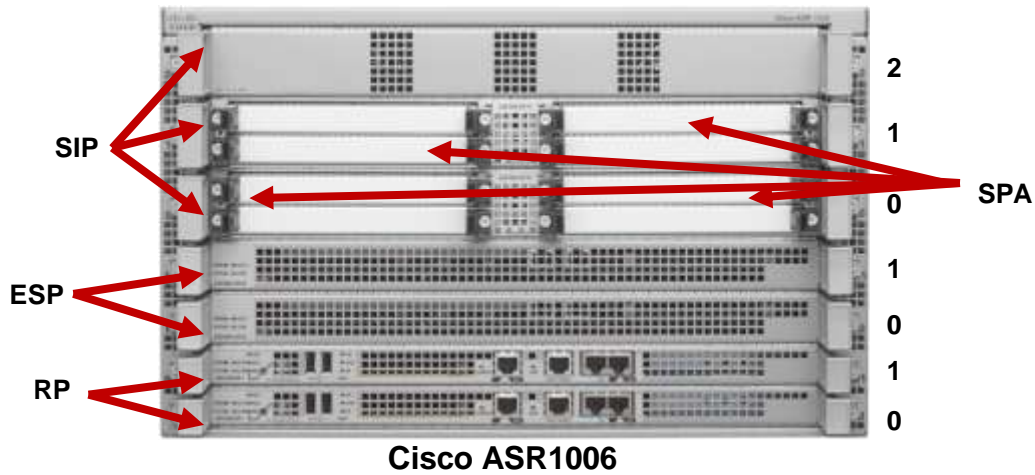
Архитектура ASR1000



- **RP (Route Processor)**
 - Работает на уровне control plane
 - управляет компонентами системы
- **ESP (Embedded Services Processor)**
 - Работает на уровне forwarding plane, выполняет форвардинг трафика
- **SIP (SPA Interface Processor)**
 - Установка и подключение Shared Port Adapters к системе
- **Централизованная архитектура обработки трафика**
 - Весь трафик проходит через активную ESP
- **Распределенная архитектура управления системой**
 - Все главные компоненты системы имеют выделенный контрольный процессор для функций управления элементом

— ESI, (Enhanced Serdes) 11.5Gbps or 23Gbps.
— SPA-SPI, 11.2Gbps
— Hypertransport, 10Gbps

Внешний вид маршрутизаторов Cisco ASR 1000



Процессорные карты RP

Route Processor – RP1 и RP2



	RP1	RP2
ЦПУ	1.5 GHz Freescale 8548	Dual-Core Intel Xeon 2.66 GHz
Память	4GB	От 8GB до 16GB
Встроенная bootflash	1GB (8GB на ASR-1002)	2GB
Порты управления	CON / AUX / ETH	CON / AUX / ETH
HDD	40HDD	80HDD
Поддержка внеш. USB	Да	Да

Коммутационные карты ESP

Сравнительные характеристики

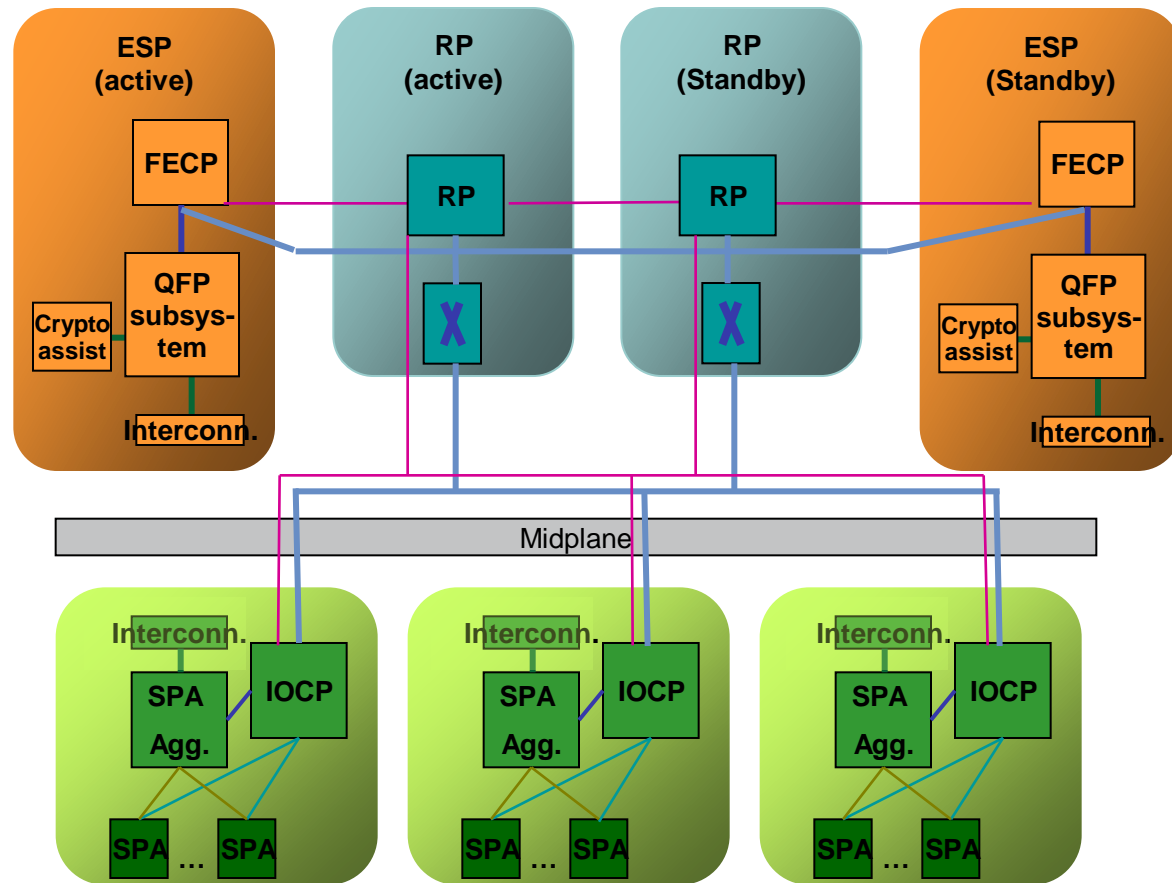
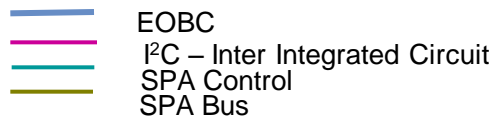


	ESP-5G	ESP-10G	ESP-20G	ESP-40G
Пропускная способность	5Gbps	10Gbps	20Gbps	40Gbps
Базовый ЦПУ	QFP 20	QFP 40	QFP 40	QFP 40
Частота синхронизации	900 MHz	900 MHz	1.2 GHz	1.2 GHz
Шифрование	~ 1Gbps	3 Gbps	8 Gbps	10 Gbps
Объем памяти QFP	256 MB	512 MB	1GB	1GB
Объем буфера	64 MB	128 MB	256 MB	256 MB
Объем TCAM	10 MB	10 MB	40 MB	40MB

Control Plane

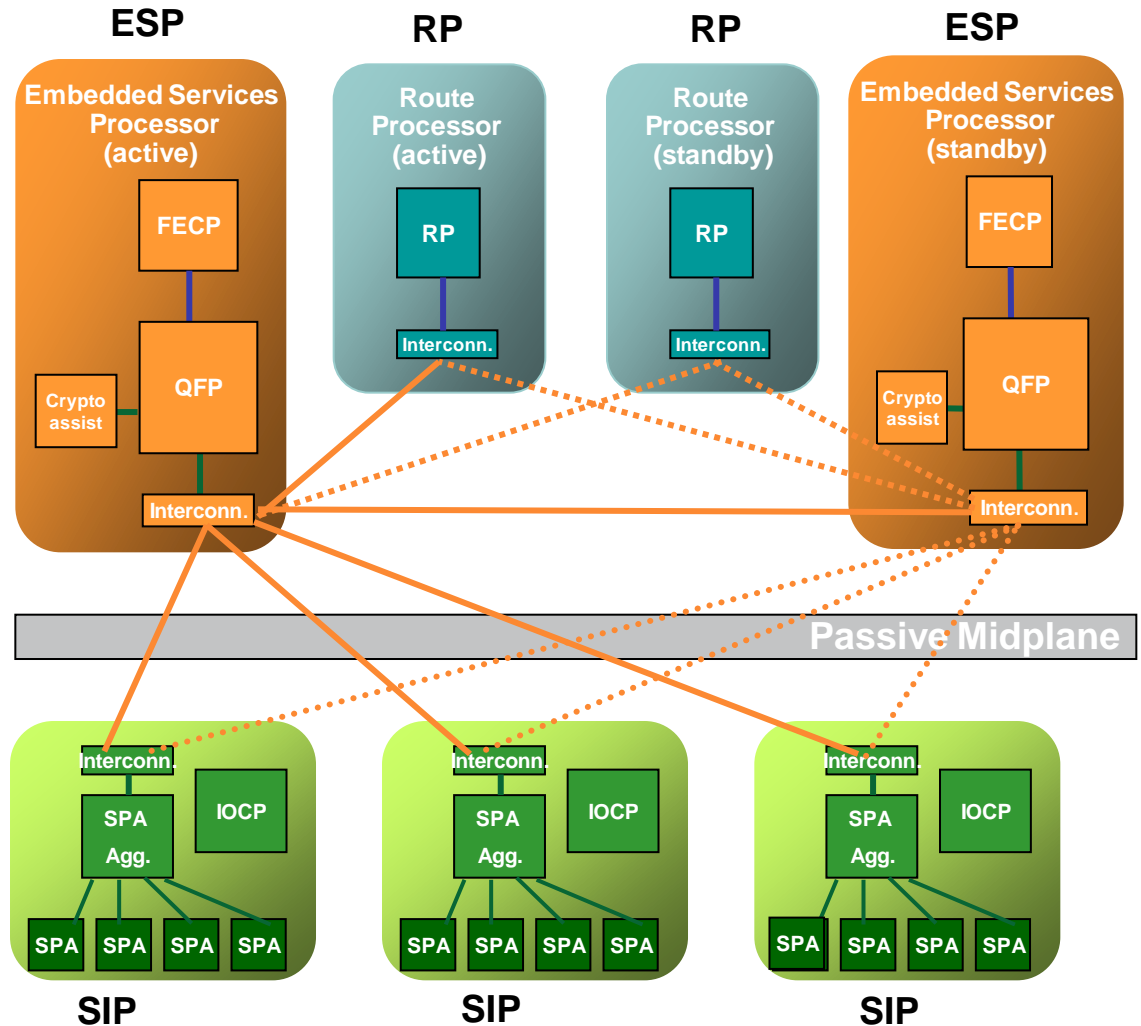
- Два различных соединения control plane не пересекающихся с dataplane соединениями
 - Ethernet out-of-band Channel (EOBC).
 - I²C – Мониторинг состояния компонент

- Управляющие соединения SPA
 - Между IOCP и SPA








Dataplane

- Весь трафик обрабатывается на ESP
- Исключение: Punt path для Legacy протоколов – обрабатывается RP
- Interconnect ASIC в каждом функциональном элементе обеспечивает соединение с backplane посредством ESI
- ESI (Enhanced Serdes Interconnect) используются для пересылки трафика
- SPA соединяются с backplane через SPA-Agg ASIC и SPA-SPI линки



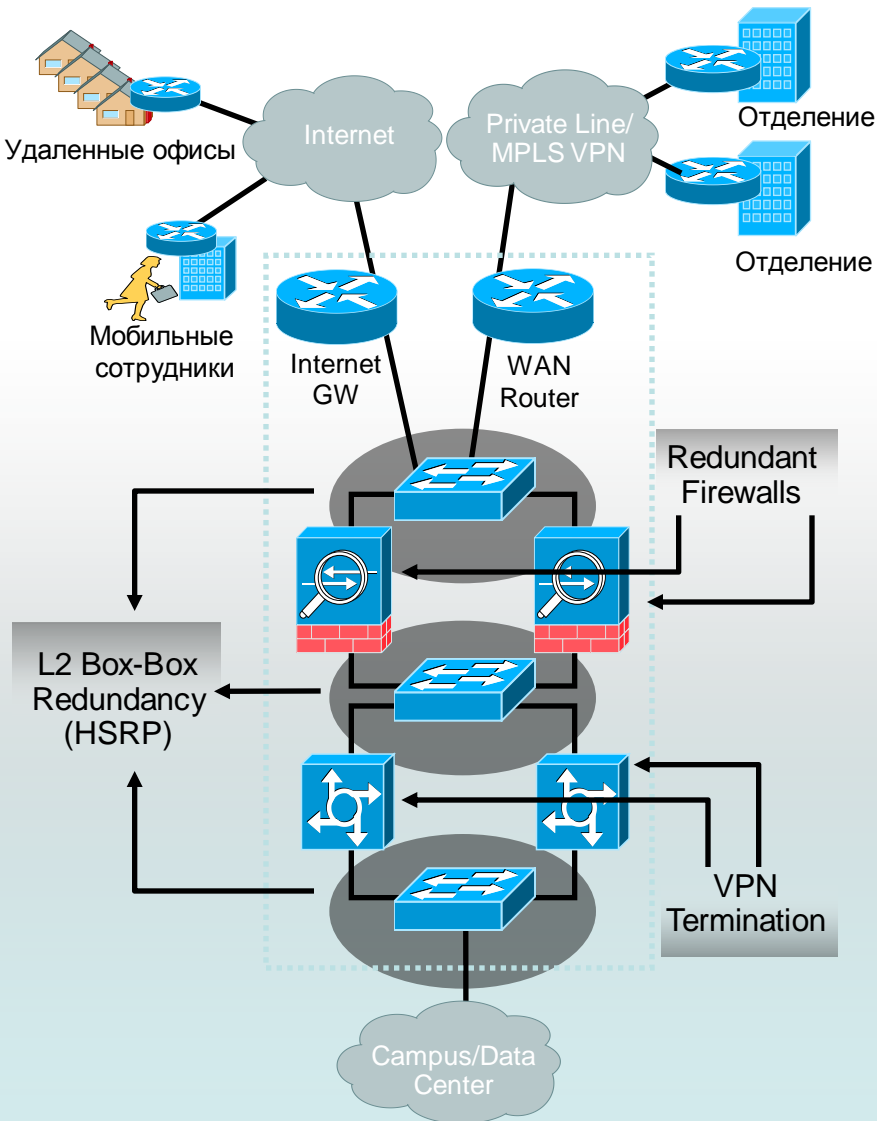
Номенклатура ASR 1000

	ASR1001	ASR1002	ASR1004	ASR1006	ASR1013
Шасси					
	От 2,5 до 5 Гбит/с 4 порта GE Программная отказоустойчивость	до 10 Гбит/с 4 порта GE Программная отказоустойчивость	До 40+ Гбит/с Программная отказоустойчивость	До 40+ Гбит/с Аппаратная отказоустойчивость	До 40+ Гбит/с Аппаратная отказоустойчивость
Embedded Services Processors (ESP)	Интегрированный ESP2.5/5 (один)	ESP5 (один)	ESP10 (один)	ESP10 (два)	
		ESP10 (один)	ESP20 (один)	ESP20 (два)	
			ESP40 (один)	ESP40 (два)	ESP40 (два)
Route Processor (RP)	Интегрированный RP (один)	Интегрированный RP1 (один)	RP1 (один)	RP1 (два)	
			RP2 (один)	RP2 (два)	RP2 (два)
SPA Interface Processor (SIP)	Интегрированный	Интегрированный	SIP10 SIP40	SIP10 SIP40	SIP10 SIP40
Кол-во SPA	1	3	8	12	24
	1 Интегрированная Дочерняя карта				

ASR1000: Сценарии применения



WAN-граница сети предприятия



Функционал WAN-границы

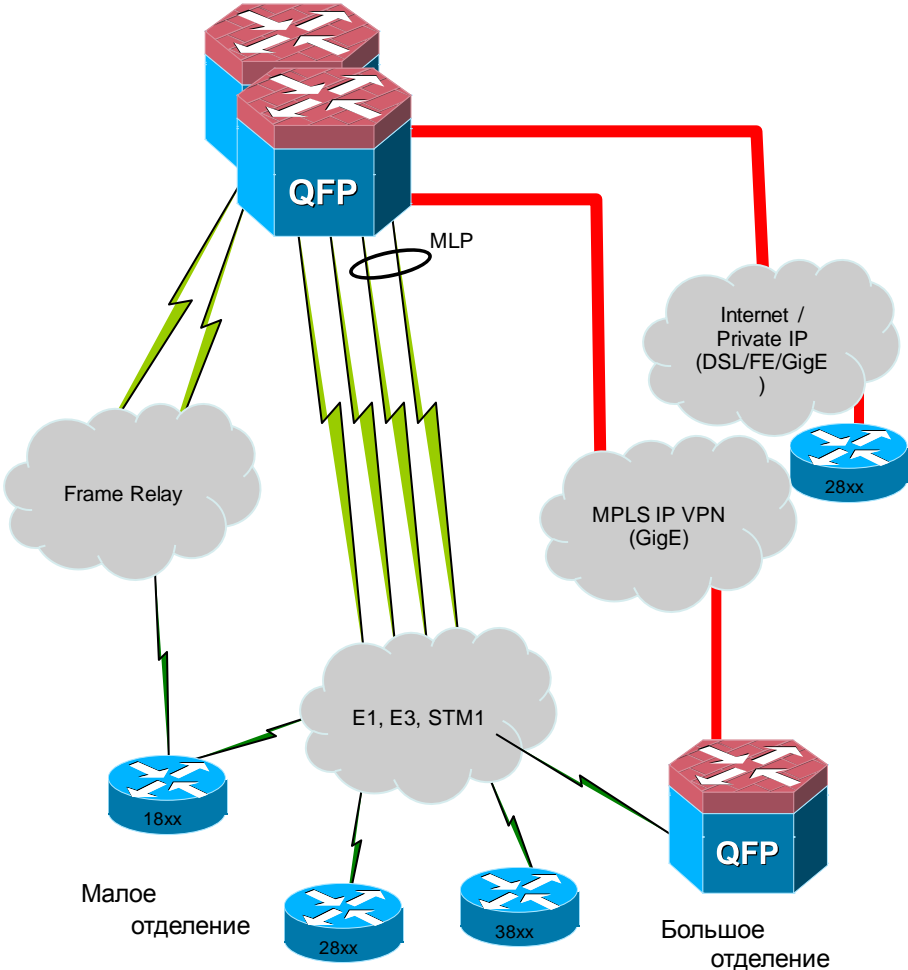
- Подключение WAN сервисов
- Безопасный доступ в Internet
- Подключение удаленных офисов
- Управление полосой пропускания
- Metro Ethernet сервисы

Требования к WAN-границе

- Полоса пропускания
- Совместимость устройств
- Уменьшение стоимости сервисов
- Уменьшение сложности и стоимости эксплуатации

WAN-граница сети предприятия

Центральный офис



Требования бизнеса

- Необходимость быстрой адаптации
- Сократить длительный период проверки нового решения
- Необходимость в проактивном и интегрированном сервисе по безопасности
- Отказоустойчивость и Надежность

Решение на основе ASR 1000

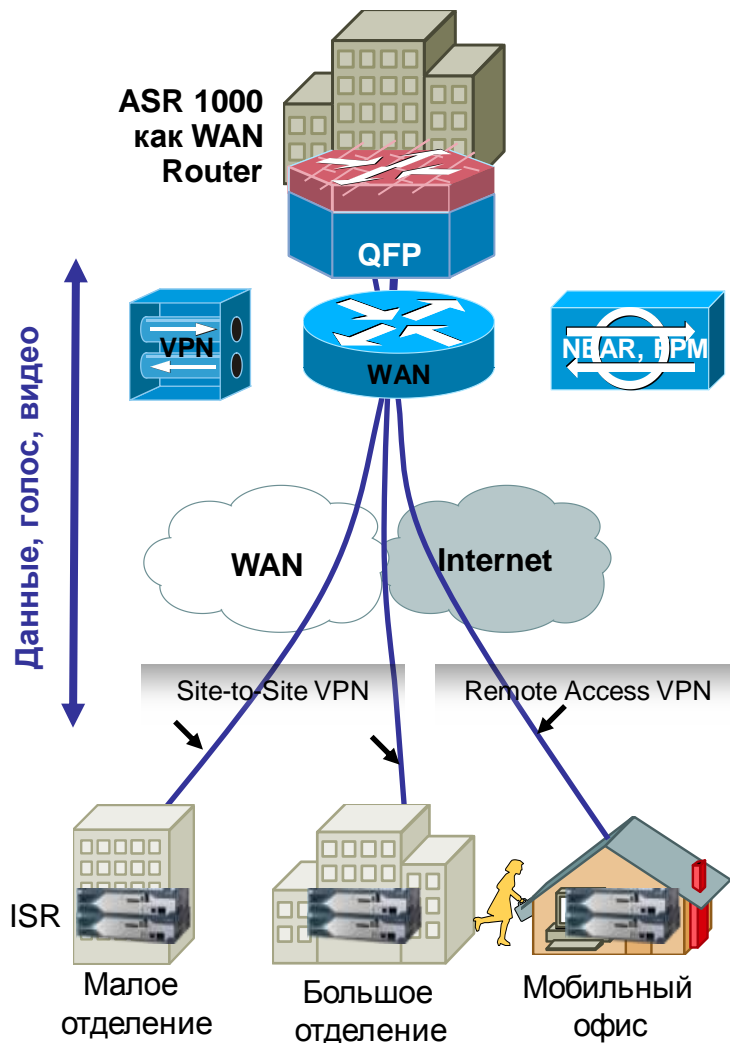
- Модульный, масштабируемый маршрутизатор для агрегации WAN
- Масштабируемость: ASR1000-ESP5, 10, 20, 40 ASR1000-RP1 и RP2
- Особенности: Модульные Control и Data plane с поддержкой ISSU, Интеллектуальные сервисы - NBAR, FPM, QoS

Преимущества

- Масштабируемость удовлетворяет требованиям бизнеса
- Сокращение расходов на внедрение и эксплуатацию одного устройства
- Простая адаптация с минимальным временем внедрения

WAN-граница сети предприятия

Центральный офис



Требования бизнеса

- Быстрое перестроение
- Необходимость в проактивном и интегрированном сервисе по безопасности
- Конфиденциальность связи

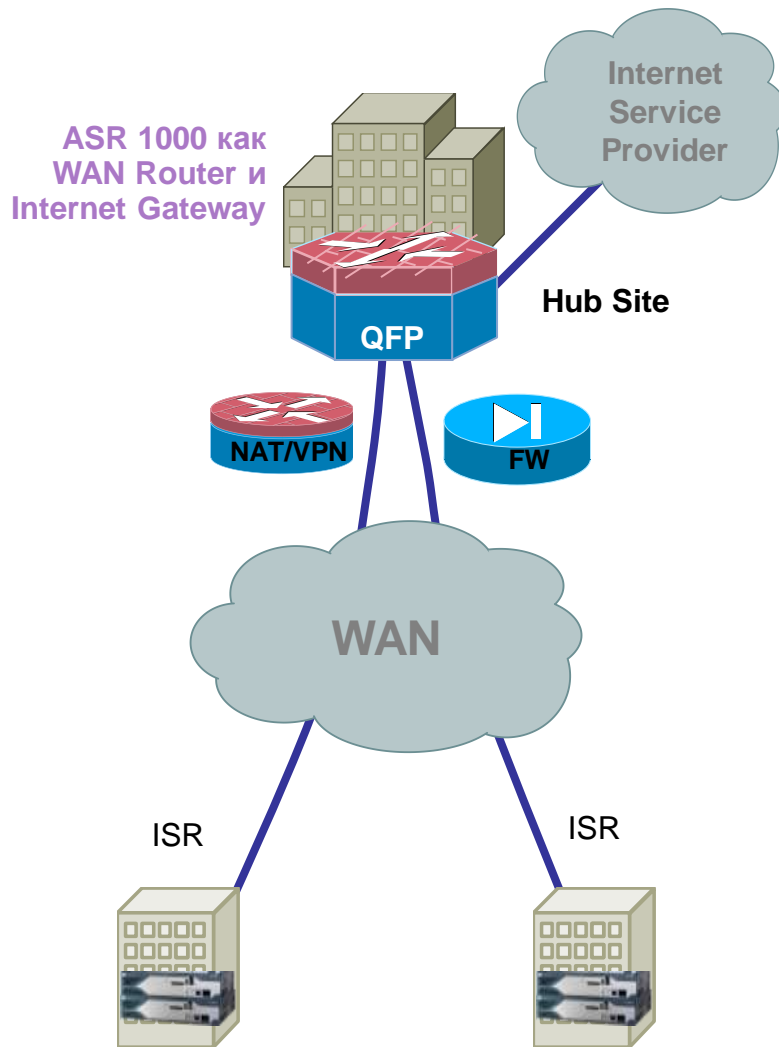
Решение на основе ASR 1000

- Пример с ESP-10: масштабируемый маршрутизатор агрегации WAN каналов с функциями безопасности
- Масштабируемость: 4 тыс. site-to-site и remote tunnels, шифрование IPsec до 8Гбит/с
- Возможности: IPsec, VPN services, Application Intelligence - NBAR, FPM

Преимущества

- Масштабируемость по полосе пропускания
- Сокращение эксплуатационных расходов
- Обеспечение конфиденциальности с минимальными потерями производительности
- Гибкая архитектура для добавления новых сервисов
- Простое управление и быстрое внедрение

WAN-граница сети предприятия



Требования бизнеса

- Обеспечение безопасности связи с удаленными офисами
- Эффективное управление трафиком
- Высокопроизводительный маршрутизатор для подключения к Интернет

Решение на основе ASR 1000

- Встроенные ф-ции безопасности: 40Гбит/с Firewall, 8Гбит/с шифрованного трафика, иерархический QoS
- Управление-Мониторинг: Netflow v9, Cisco Security Manager, LAN Mgmt Solution, ERSPAN
- Ключевые свойства: Firewall, NAT, NAC, NBAR, QoS, ACL

Преимущества

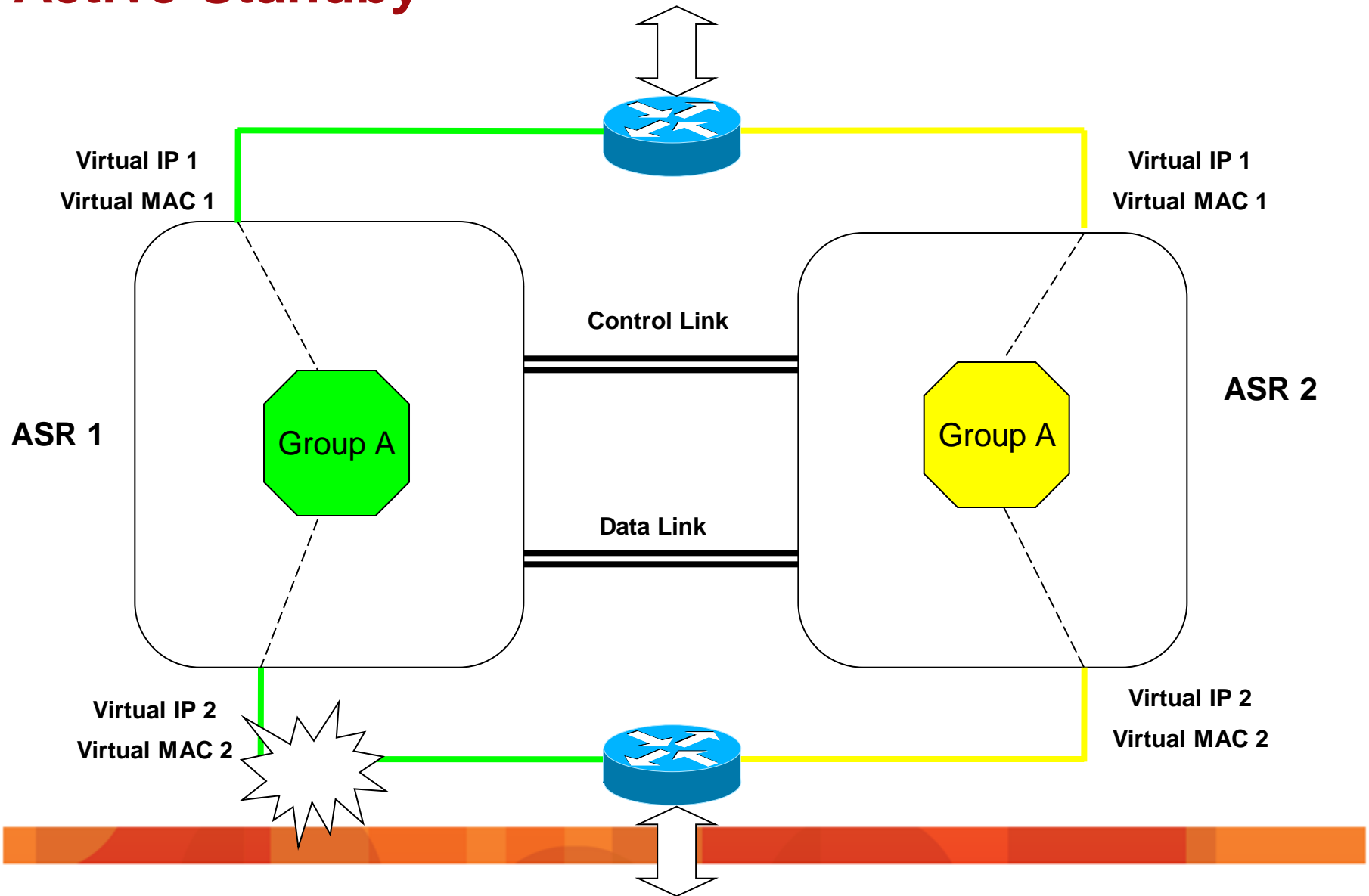
- Широкий спектр интерфейсов для подключения к ISP
- Отказоустойчивость операторского класса
- Быстрое внедрение
- Шифрование без ущерба для производительности

Firewall/NAT Box to Box Redundancy Active-Standby

Key

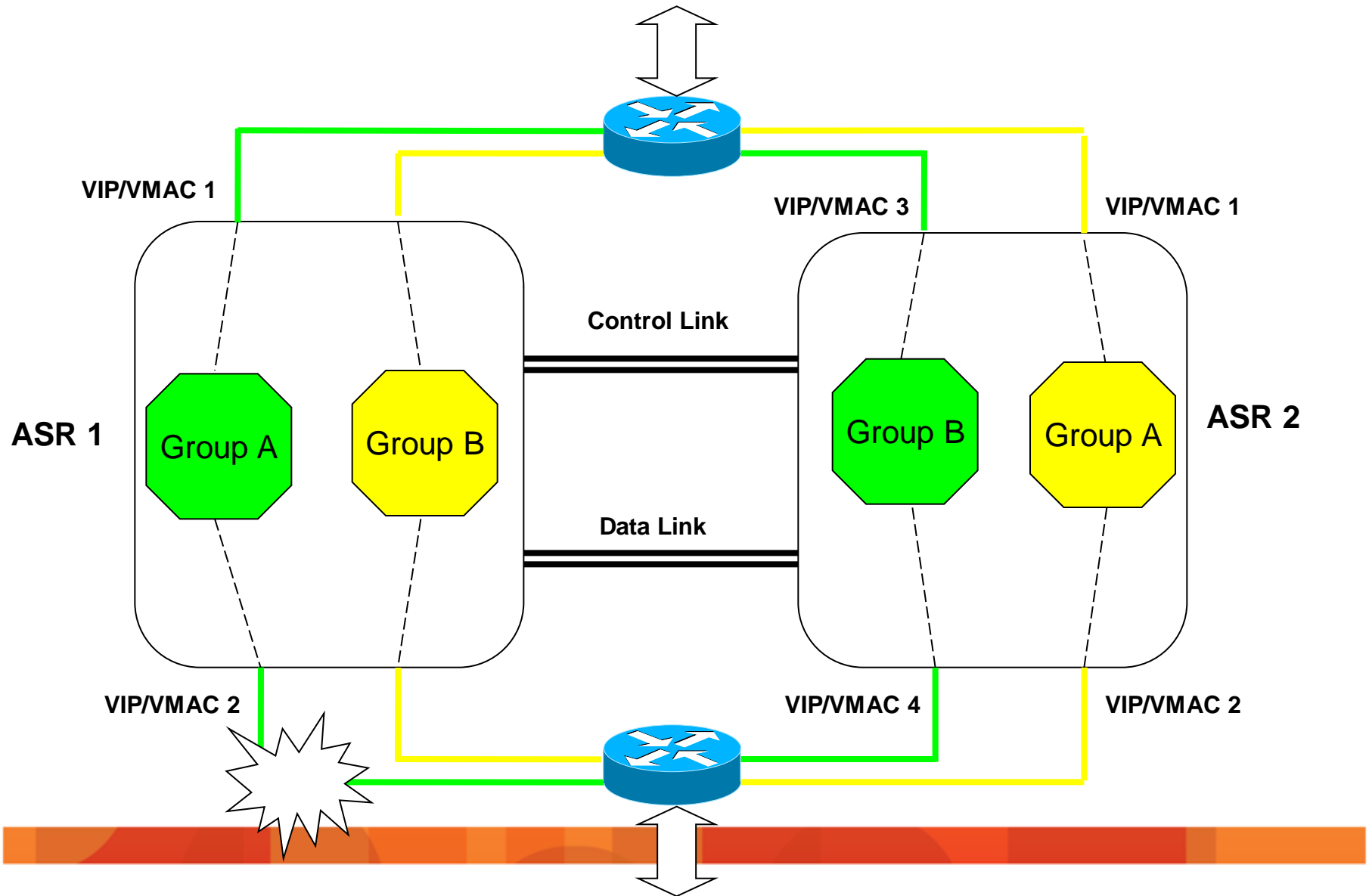
Green : Active

Yellow : Standby



ASR 1000 B2B – Active-Active

Key
Green : Active
Yellow : Standby



Firewall/NAT Box to Box Redundancy

- Поддерживаются сценарии Active-Standby и Active-Active
- Приложения– Firewall/NAT
- Субсекундное переключение
- Failover Control Interface
 - выделенное соединение для Failover Protocol
- Failover Data Interface
 - синхронизация состояния Firewall и NAT сессий
- Ограничения
 - ASR1006, ASR1013 не поддерживают Box to Box redundancy для Firewall/NAT
 - Только LAN to LAN сценарий поддерживается, LAN-WAN начинает поддерживаться
 - Ассиметричный роутинг будет поддерживаться в будущих релизах
 - Синхронизация конфигурации будет поддерживаться в будущих релизах



Пример конфигурации Voх-to-Vох Redundancy

Создать RG

```
redundancy
 application redundancy group
 mode none
 protocol 1
  name prot1
  timers hellotime msec 250 holdtime msec 750
 protocol 2
  name prot2
  timers hellotime 1 holdtime 3
```

Создать Active-Active RG

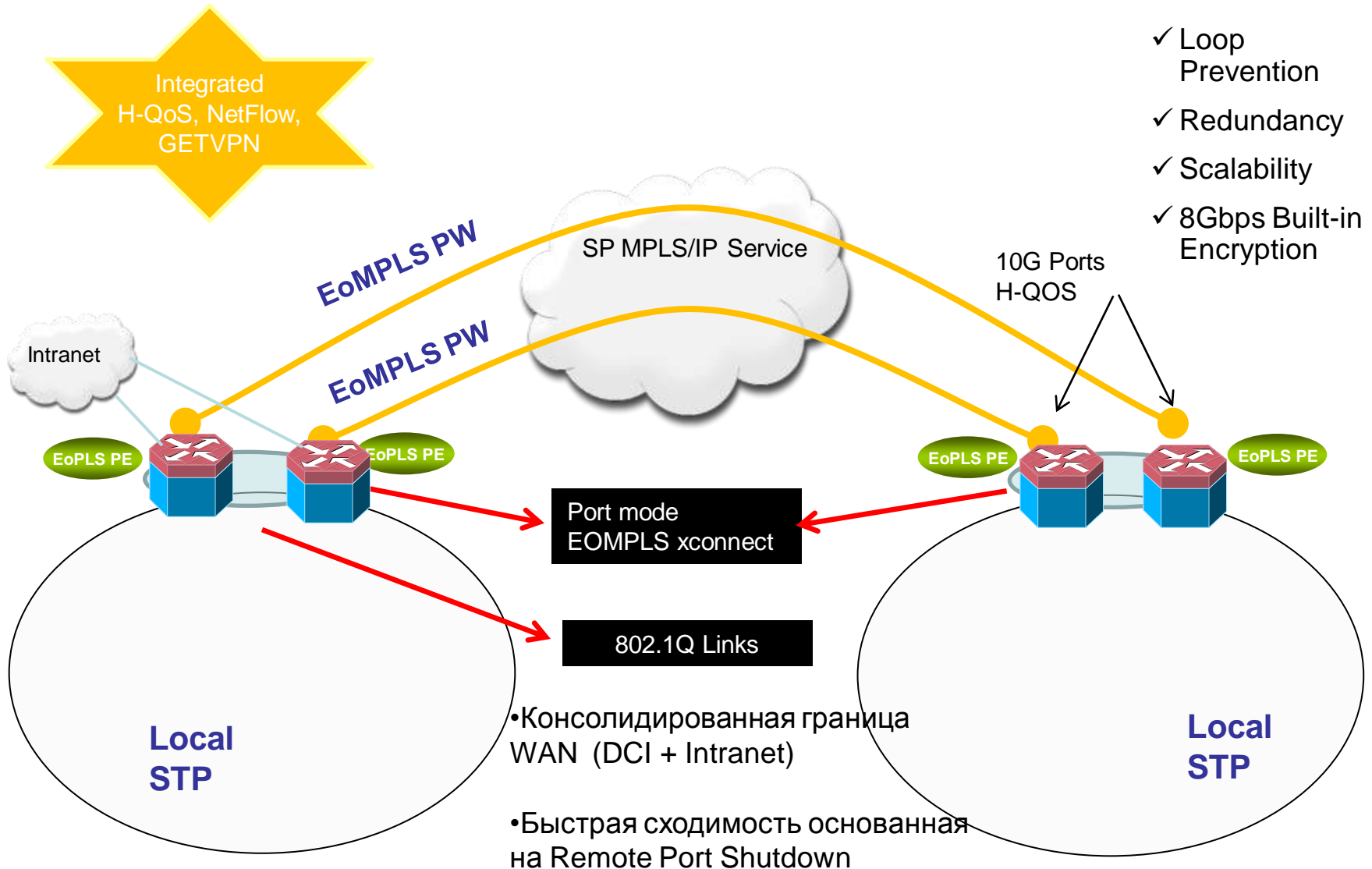
```
redundancy
 application redundancy group
  group 1
  name RG1
  preempt
  priority 205 failover-threshold 200
  #The other router has lower priority for this group
  control gi0/0/0 protocol 1
  data gigi0/0/1
  #Control and data links can be the same
  #For active-standby scenario, only one RG group is needed
  group 2
  name RG2
  priority 195 failover-threshold 190
  #The other router has higher priority for this group
  control gi0/0/0 protocol 2
  data gi0/0/1
```

Настроить Traffic Interface

```
interface gi1/0/0
 redundancy group 1 ip 10.1.1.1 exclusive
  decrement 50
  #Use the same virtual IP address for the same
  #group on the same LAN for both routers
  #For active-standby scenario, only one RG
  #group is needed
 redundancy group 2 ip 20.1.1.1 exclusive
  decrement 50
 redundancy rii 100
  #Rii should be the same across boxes for the
  #mapped interface
```

```
interface gi1/0/1
 redundancy group 1 ip 30.1.1.1 exclusive
  decrement 50
 redundancy group 2 ip 40.1.1.1 exclusive
  decrement 50
 redundancy rii 101
```

ASR1000: Объединение Центров Обработки Данных (DCI) + унифицированная граница WAN



ASR1000: Easy Virtual Network

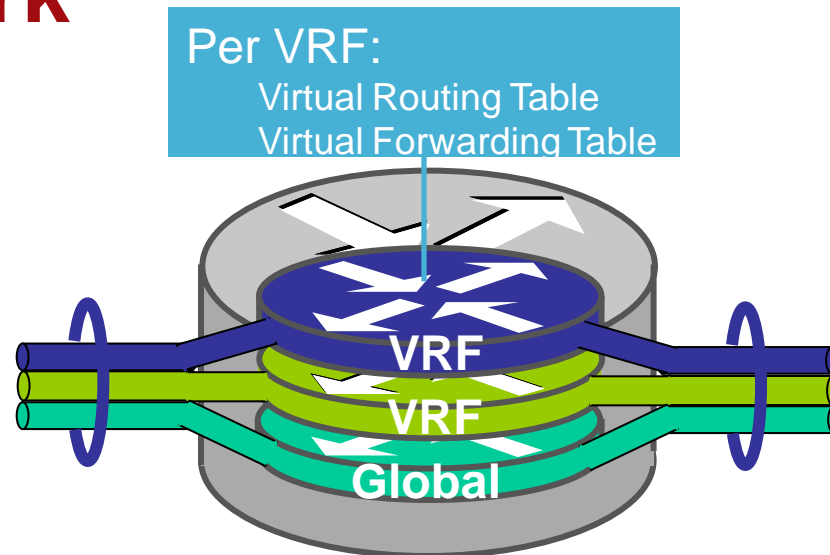


Easy Virtual Network

Компоненты EVN

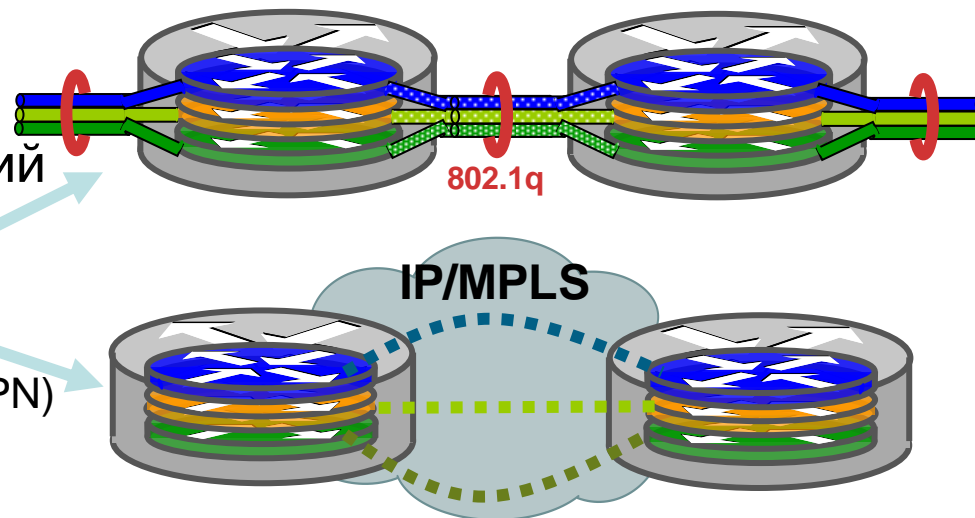
- Виртуализация устройства

- Control plane virtualization
- Data plane virtualization
- Services virtualization



- Виртуализация соединений

- Hop-by-Hop
-(EVN/VRF-Lite End-to-End)
- Multi-Hop
-(EVN/VRF-Lite+GRE, MPLS-VPN)



VRF: Virtual Routing and Forwarding

Easy Virtual Networks

На пограничных L3 устройствах создать VRFы и привязать L2 VLANы к соответствующим VRFам

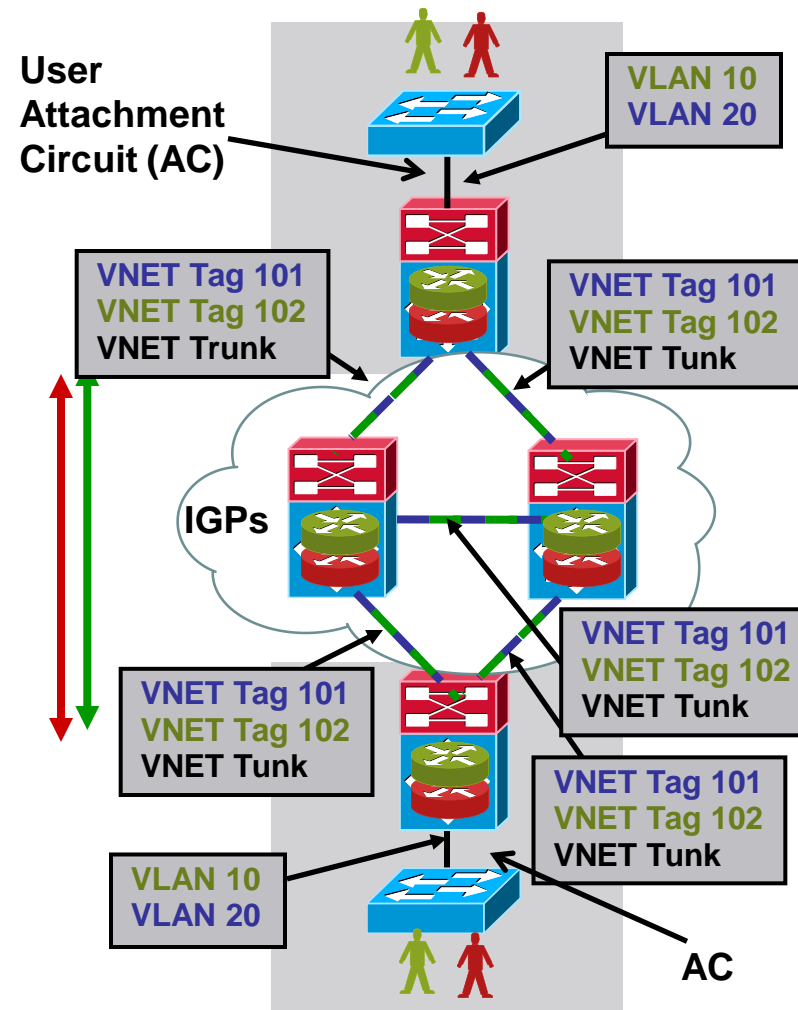
Создать VRFы на всех остальных L3 устройствах в сети

Все соединения в ядре сети настроить как VNET trunk. Каждое соединение будет использовать те же самые теги 802.1q

Включить протоколы маршрутизации внутри VRF на всех устройствах

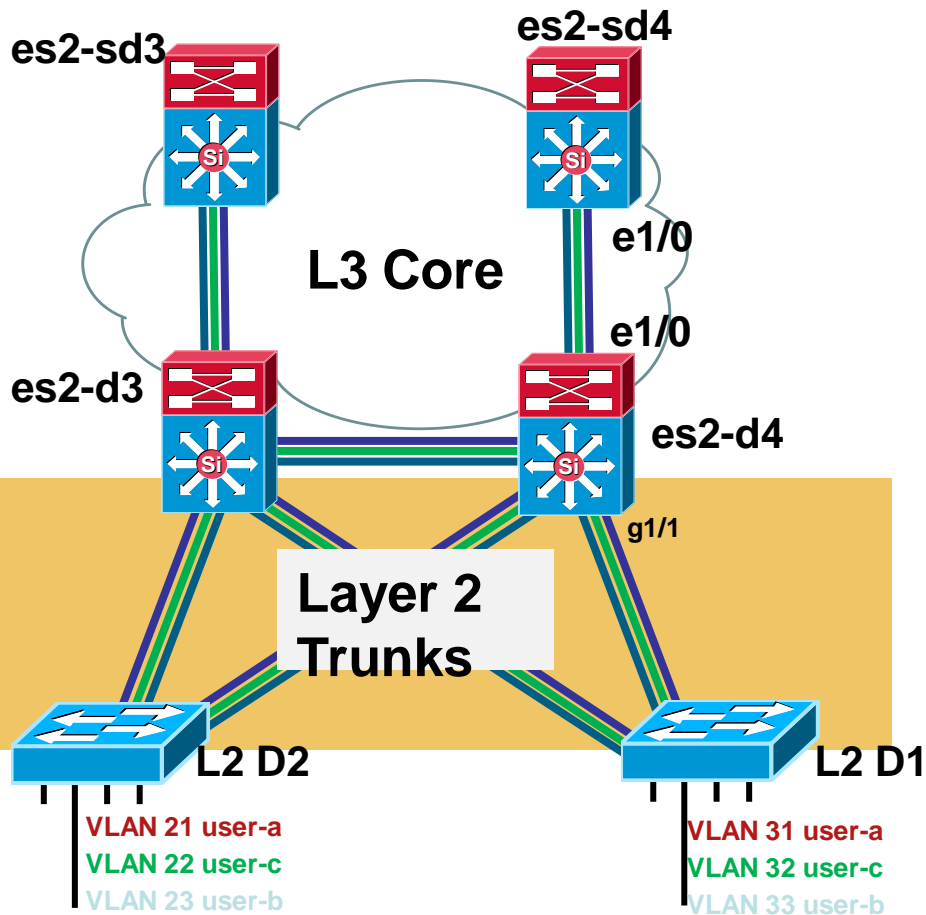
Теперь трафик проходит через сеть сохраняя логическую изоляцию между группами.

Один физический линк передает трафик нескольких VRF и готов к добавлению новых VRF



Конфигурация EVN :

Определение VRFs и привязка к интерфейсам



1. Create VRFs and allocate unique VNET tags for each VRF

```
vrf definition user-a
  vnet tag 11
vrf definition user-b
  vnet tag 12
vrf definition user-c
  vnet tag 13
```

2. Map VRFs to appropriate interfaces

```
!
interface Loopback11
  vrf forwarding user-a
!
interface e0/0.11
  vrf forwarding user-a
interface e0/0.12
  vrf forwarding user-c
interface e0/0.13
  vrf forwarding user-b
!
```

3. Transport all provisioned VRFs on Trunk interfaces

```
!
interface e1/0
  vnet trunk
```

Упрощение в настройке VRF – vnet trunk

VNET Trunk

```
!  
interface Ethernet1/0  
vnet trunk  
ip address 125.1.15.18 255.255.255.0  
ip pim sparse-mode  
!
```

Конфигурация
разворачивается в виде:



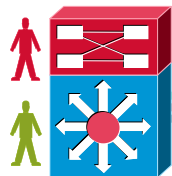
VRF Sub-interfaces

```
!  
interface Ethernet1/0.11  
description Subinterface for VNET services  
vrf forwarding user-a  
encapsulation dot1Q 11  
ip address 125.1.15.18 255.255.255.0  
ip pim sparse-mode  
!  
interface Ethernet1/0.12  
description Subinterface for VNET services  
vrf forwarding user-b  
encapsulation dot1Q 12  
ip address 125.1.15.18 255.255.255.0  
ip pim sparse-mode  
!  
interface Ethernet1/0.13  
description Subinterface for VNET user-c  
vrf forwarding user-c  
encapsulation dot1Q 13  
ip address 125.1.15.18 255.255.255.0  
ip pim sparse-mode  
!
```

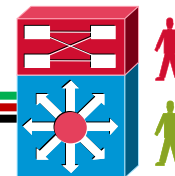
- Номер VNET Tag определен для каждого VRF и используется как часть номера подинтерфейса
- Каждый подинтерфес наследует характеристики от главного интерфейса
-одинаковый IP адрес на всех сабинтерфейсах
- Транковый интерфейс будет передавать трафик всех настроенных VRF
если не использовать фильтры

Совместимость VRF-Lite и VNET Trunk

VRF-Lite Device



EVN Device



VRF-Lite Config

```
!  
vrf definition user-c  
!  
vrf definition services  
!  
interface Ethernet1/0  
ip address 125.1.1.11 255.255.255.0  
ip pim sparse-mode  
!  
interface Ethernet1/0.10  
description Subinterface for VNET services  
vrf forwarding services  
encapsulation dot1Q 10  
ip address 125.1.1.11 255.255.255.0  
ip pim sparse-mode  
!  
interface Ethernet1/0.13  
description Subinterface for VNET user-c  
vrf forwarding user-c  
encapsulation dot1Q 13  
ip address 125.1.1.11 255.255.255.0  
ip pim sparse-mode
```

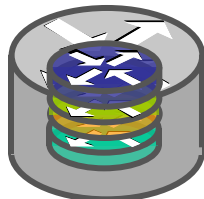
EVN config

```
!  
vrf definition services  
vnet tag 10  
!  
vrf definition user-c  
vnet tag 13  
!  
interface Ethernet1/0  
vnet trunk  
ip address 125.1.1.11 255.255.255.0  
ip pim sparse-mode  
!
```

•dot1Q tag и vnet tag
должны совпадать

Использование Routing Context для VRF Verification

Оригинальные команды CLI



Использование Routing context

```
es2-d4#show ip route vrf user-a
Routing table output for red

es2-d4#ping vrf user-c 10.1.1.1
Ping result using VRF red

es2-d4#telnet 10.1.1.1 /vrf user-a
Telnet to 10.1.1.1 in VRF red

es2-d4#traceroute vrf user-a 10.1.1.1
Traceroute output in VRF red
```

```
es2-d4#routing-context vrf user-a
es2-d4%user-a#

es2-d4%user-a# show ip route
Routing table output for red

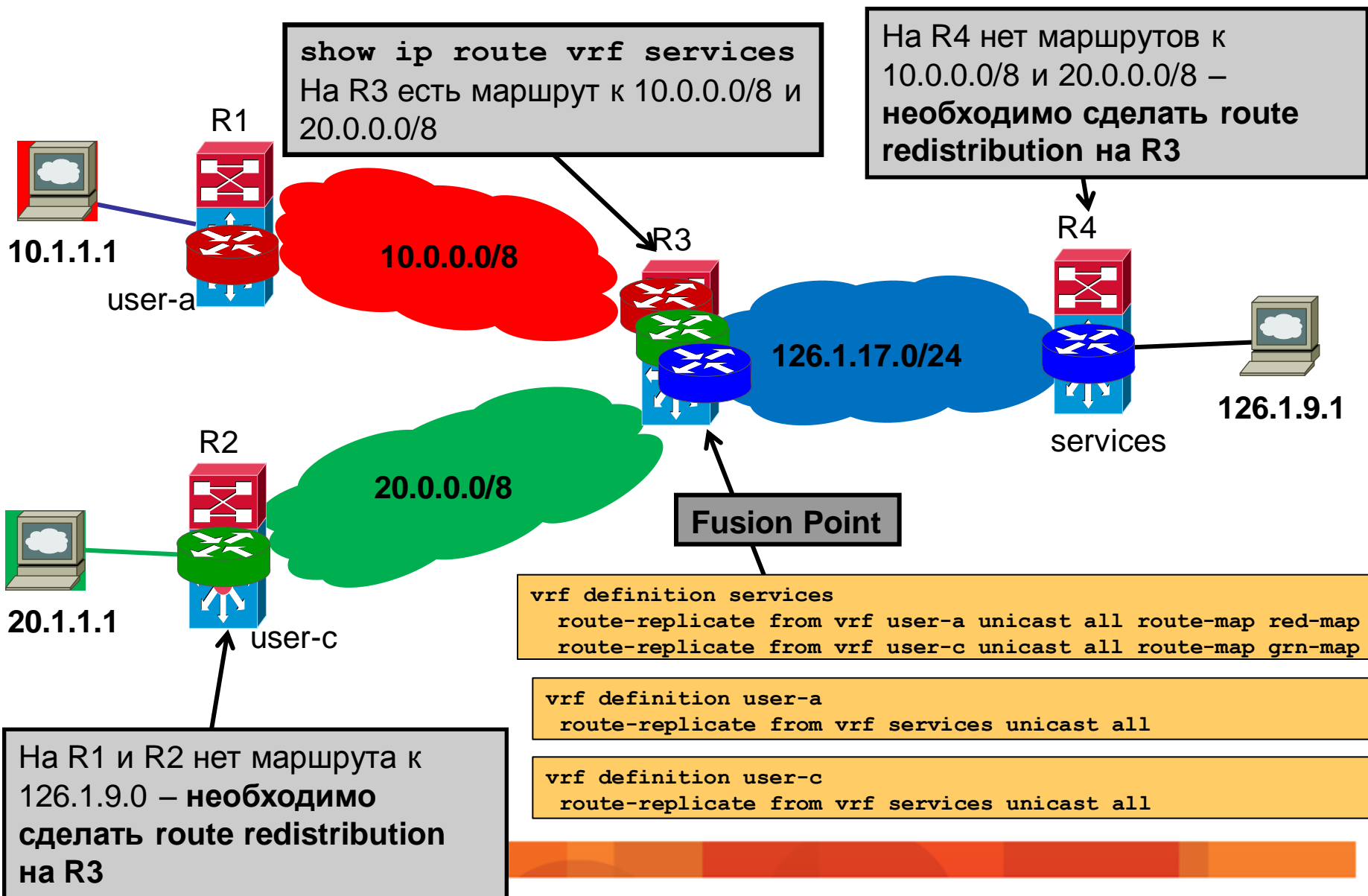
es2-d4%user-a# ping 10.1.1.1
Ping result using VRF red

es2-d4%user-a# telnet 10.1.1.1
Telnet to 10.1.1.1 in VRF red

es2-d4%user-a# traceroute 10.1.1.1
Traceroute output in VRF red
```

EVN:

Shared Services и использование Route Replication



EVN: Route Replication

RIB – VRF services			
Route	Type	Dest Int	NextHop
126.1.17.0/24	Connected	Gi0/1	
126.1.9.0/24	OSPF	Gi0/1	126.1.17.13
126.1.12.0/24	OSPF	Gi0/1	126.1.17.13
126.1.14.0/24	OSPF	Gi0/1	126.1.17.13

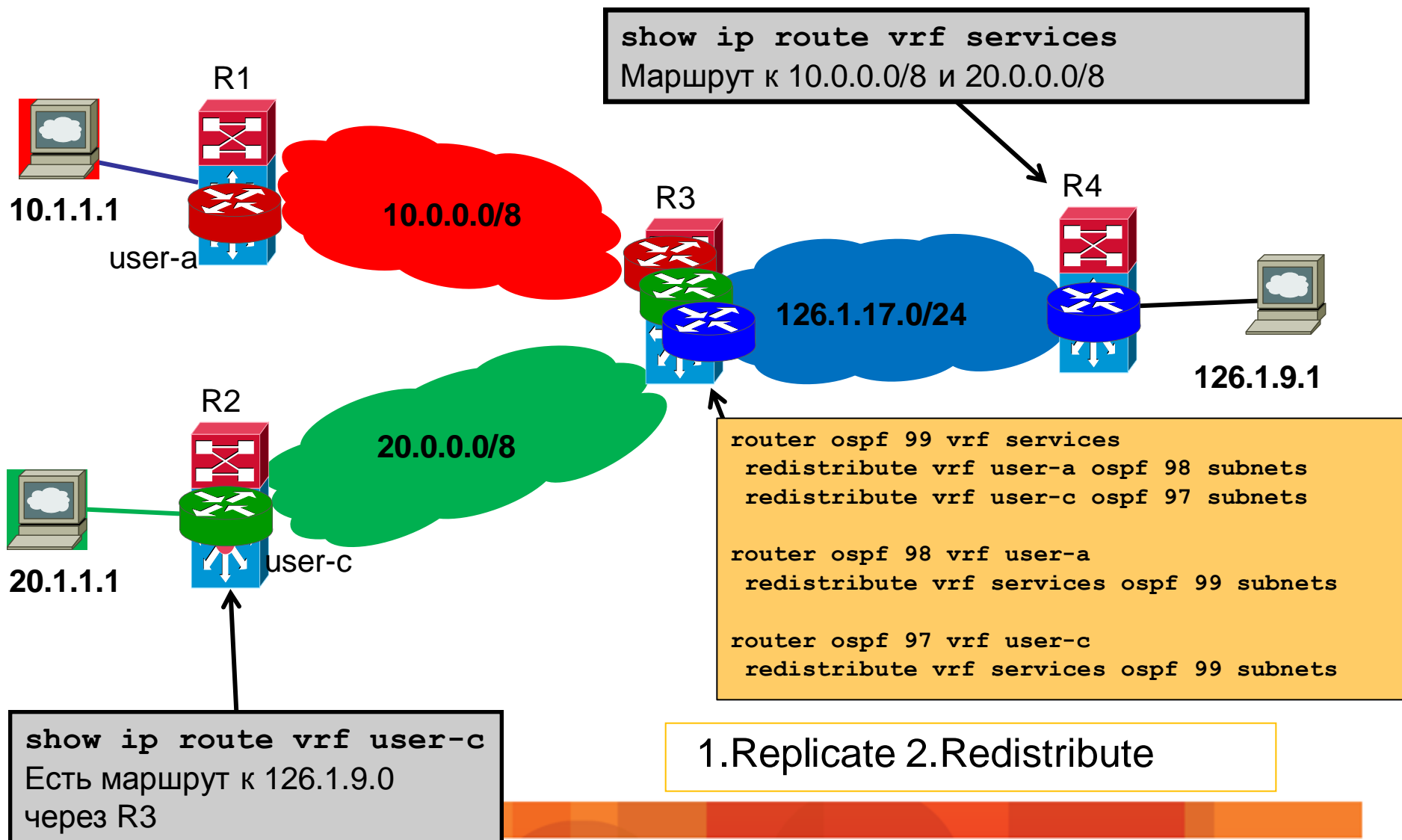
- Route Replication создает линк к маршруту в RIB из разных VRF

```
router ospf 99 vrf services
 network 126.1.0.0 0.0.255.255 area 0
!
router ospf 98 vrf user-a
 network 126.1.0.0 0.0.255.255 area 0
```

RIB – VRF user-a			
Route	Type	Dest Int	NextHop
126.1.9.0/24	OSPF	Gi0/1	126.1.17.13
126.1.12.0/24	OSPF	Gi0/1	126.1.17.13
126.1.14.0/24	OSPF	Gi0/1	126.1.17.13

```
vrf definition user-a
!
 address-family ipv4
  route-replicate from vrf services unicast all
 exit-address-family
```

Shared Services используя Route Replication и Redistribution



EVN: Управление разделяемыми сервисами

До: настройка shared services

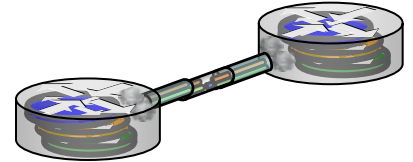
```
ip vrf services
  rd 3:3
  route-target export 3:3
  route-target import 1:1
  route-target import 2:2
!
ip vrf user-a
  rd 1:1
  route-target export 1:1
  route-target import 3:3
!
ip vrf user-b
  rd 2:2
  route-target export 2:2
  route-target import 3:3
!
router bgp 65001
  bgp log-neighbor-changes
  !
  address-family ipv4 vrf services
    redistribute ospf 3
    no auto-summary
    no synchronization
    exit-address-family
  !
  address-family ipv4 vrf user-a
    redistribute ospf 1
    no auto-summary
    no synchronization
    exit-address-family
  !
  address-family ipv4 vrf user-b
    redistribute ospf 2
    no auto-summary
    no synchronization
    exit-address-family
  !
```

После: с использованием Route Replication в EVN

- Не нужно BGP
- Не нужно Route Distinguisher
- Не нужно Route Targets
- Не нужно Import/Export
- Все проще

```
vrf definition services
!
  address-family ipv4
    route-replicate from vrf user-a unicast all
    route-replicate from vrf user-b unicast all route-
map userb
  exit-address-family
!
vrf definition user-a
  vnet tag 11
  !
  address-family ipv4
    route-replicate from vrf services unicast all
  exit-address-family
!
vrf definition user-b
  vnet tag 12
  !
  address-family ipv4
    route-replicate from vrf services unicast all
  exit-address-family
!
```

EVN: Резюме



- EVN – упрощает использование VRF Lite
- Работает с VRF Lite, MPLS VPN и MPLS VPN over mGRE
- Фаза I реализована на ASR1000 IOS XE 3.2S
- Новая концепция
 - VNET Tag
 - VNET Trunk
 - Sub-interface наследование номера vnet tag
 - Route Replication: Shared Services на протоколах IGP
 - routing-context: ping, traceroute, debug condition, cisco-vrf-mib

ASR1000: планы развития

- ESP-80G
 - Производительность до 32Млн.пак./сек, до 80Гбит/с
 - Установка в ASR1006 и ASR1013 с RP2 и следующим RP
 - Середина 2012 года
- ESP-160G
 - Производительность до 64Млн.пак./сек, до 160Гбит/с
 - Установка в ASR1013 с RP2 и следующим RP
 - Конец 2012 года
- ASR1002-х
 - Весна 2012 года
 - Производительность до 40Гбит/с
 - 6 встроенных интерфейсов Gigabit Ethernet SFP
 - 3 слота для SPA
 - 2 слота для PVDM

Cisco Expo 2011



Спасибо!

Просим Вас заполнить анкеты.
Ваше мнение очень важно для нас.

innovate *together*