Для просмотра данной презентации наилучшим образом подходит бесплатный PDF Viewer “Sumatra PDF”, доступный для ОС Windows по следующей ссылке:

http://blog.kowalczyk.info/software/sumatrapdf/

Всё и больше

Возможности IOS, которые совсем не вредно использовать

Владимир Литовка
системный инженер
doka@cisco.com

CiscoExpo 2008

Содержание

- Безопасность
  - *Control Plane Protection (CoPP)*
  - *Network-based Application Recognition (NBAR)*
  - *VRF-Lite*
- Обслуживание
  - *Embedded Event Manager (EEM)*
  - *Remote Network Monitoring (RMON)*
- Качество сервиса
  - *IP SLA*
  - *Cisco Performance Routing (PfR)*

Безопасность
Control Plane Protection

Control Plane Protection

Защита устройства от внешних атак

- Сохранение работоспособности устройства в случае атаки, направленной на модуль управления (route processor, RP)

  потери управляющих пакетов (keepalive) и обновлений маршрутизации

  потеря управления устройством

- Приоритезация управляющего трафика

  например, OSPF важнее SSH

- Специальный интерфейс control-plane

  единая точка настройки политики защиты, независимо от количества интерфейсов в устройстве

- По умолчанию выключена

Control Plane Protection

Защита устройства от внешних атак

1. Разработка политики доступа к RP, например:
   a) *Critical (OSPF, BGP, LDP)*
   b) *Important (SSH, SNMP, NTP)*
   c) *Normal (ожидаемый трафик в небольших количествах – ping, пр.)*
   d) *Undesirable (нежелательный трафик)*

2. Определение критериев классификации трафика

```
router(config)# class-map <traffic_class_name>
router(config-cmap)# match <access-group>
```

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd805ffde8.html#wp9000040

Control Plane Protection

Защита устройства от внешних атак

3. Определение сервисной политики

```
router(config-pmap)# policy-map <service_policy_name>

router(config-pmap)# class <traffic_class_name>

router(config-pmap)# police <rate> conform-action
   transmit exceed-action drop
```

4. Применение сформированной политики

```
router(config)# control-plane

router(config-cp)# service-policy input
   <service_policy_name>
```

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd805ffde8.html#wp9000040

Безопасность

Network-based Application Recognition

Network-based Application Recognition

Интеллектуальное распознавание и контроль за трафиком

- Распознавание трафика не только по заголовкам пакета, но и по содержимому

  поддерживается около 60 протоколов

- Packet Description Language Module (PDLM)

  возможность добавлять сигнатуры без изменения версии IOS (файлы PDLM предоставляются Cisco)

- Использование для гибкого QoS и защиты сети от нежелательного использования

  выделение полосы / запрет на использование не только по портам/протоколам, а по типу приложения

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6558/ps6612/ps6653/prod_qas09186a00800a3ded_ps6616_Products_Q_and_A_Item.html

Network-based Application Recognition

Интеллектуальное распознавание и контроль за трафиком

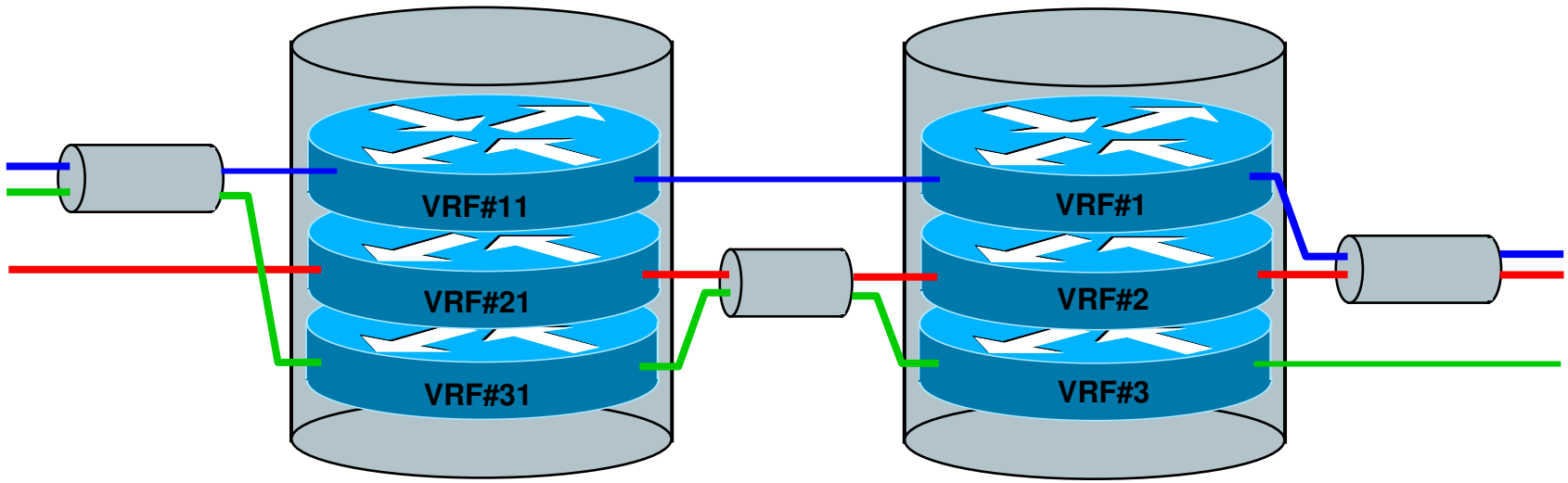
1. Включение NBAR на интерфейсе
   1. `router(config)# interface <intf_name>`
   2. `router(config-if)# ip nbar protocol-discovery`
2. Определение критериев классификации трафика
   1. `router(config)# class-map <traffic_class_name>`
   2. `router(config-cmap)# match protocol <protocol-name>`
3. Определение правил обработки
   1. `router(config-pmap)# policy-map <service_policy_name>`
   2. `router(config-pmap)# class <traffic_class_name>`
   3. `router(config-pmap-c)# [ … ]`
4. Применение сформированной политики
   1. `router(config)# interface <intf_name>`
   2. `router(config-cp)# service-policy input <service_policy_name>`

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/clsfy_traffic_nbar.html

Безопасность
VRF-Lite

VRF-Lite

- «Облегченная» версия MPLS VPN
  - *– не требуется MPLS*
  - *– VRF (логический маршрутизатор) неизвестен за пределами физического маршрутизатора*
  - *– вся информация о сконфигурированном VRF-Lite локальна для маршрутизатора*
- Защита абонентов и сервисов друг от друга непосредственно на границе сети



VRF-Lite

на примере коммутатора Catalyst ME4924

```
ip vrf Internet
 rd 1:101
!
ip vrf Voice
 rd 1:102
!
vlan 101
 name Access_Inet
!
vlan 102
 name Access_Voice
!
vlan 901
 name Aggregation_Inet
!
vlan 902
 name Aggregation_Voice
!
interface range GigabitEthernet 1/1 - 12
 switchport access vlan 101
!
interface range GigabitEthernet 1/13 - 24
 switchport access vlan 102
```

```
interface TenGigabitEthernet 1/29
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 900-1005
 switchport mode trunk
!
interface Vlan101
 ip address 1.2.2.1 255.255.255.0
 ip vrf forwarding Internet
!
interface Vlan102
 ip address 1.2.3.1 255.255.255.0
 ip vrf forwarding Voice
!
interface Vlan901
 ip address 1.3.2.1 255.255.255.0
 ip vrf forwarding Internet
 ip ospf network point-to-point
!
interface Vlan902
 ip address 1.3.3.1 255.255.255.0
 ip vrf forwarding Voice
!
ip route vrf Voice < … >
!
router ospf 101 vrf Internet
 [ … ]
```

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/44sg/configuration/guide/vrf.html

Обслуживание
Embedded Event Manager

Embedded Event Manager

Мониторинг и управление устройством

- Мониторинг событий

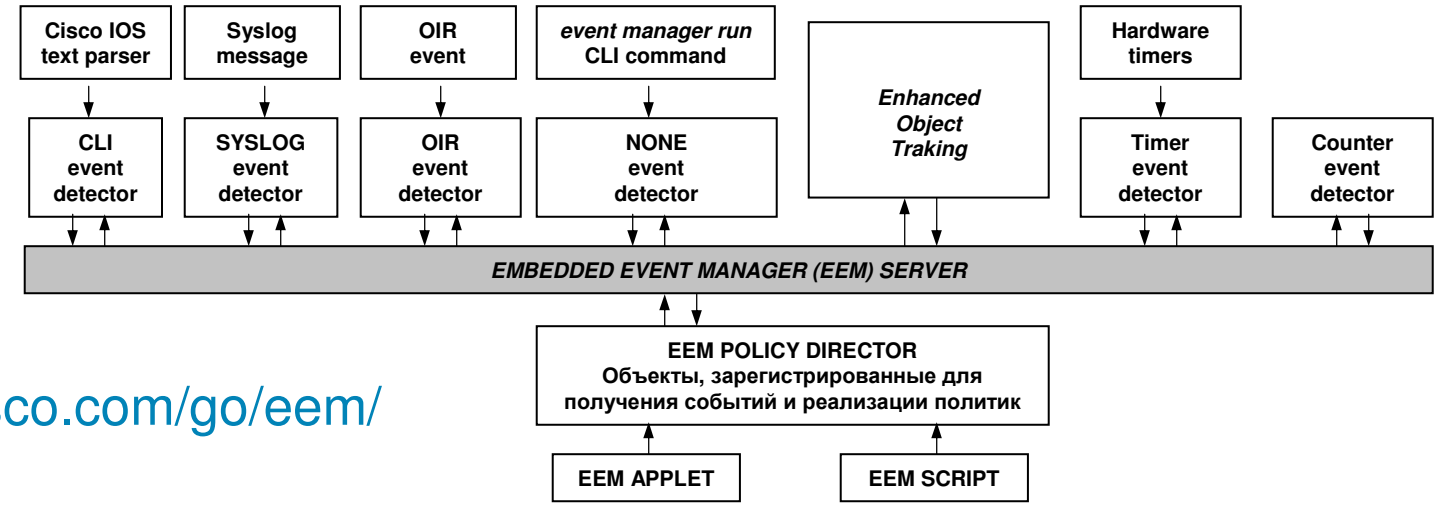
  например, падение интерфейса или критическая загрузка процессора

- *Реакция на события*

  генерация сообщений или внесение изменений в конфигурацию

- *Варианты конфигурирования*

  - *Command Line Interface (CLI) Applet*
  - *скрипт TCL*



http://www.cisco.com/go/eem/

Embedded Event Manager

Мониторинг и управление устройством

Реакция на событие в Syslog

```
event manager applet OSPF
event syslog pattern “Neighbor Down: Dead timer expired”
action 1.0 cli command “enable”
action 1.1 cli command “sh proc cpu | append flash:cpu_info”
action 1.2 cli command “show interface | append flash:interface_info”
```

Мониторинг состояния объекта

```
track 2 interface GigabitEthernet0/0 line-protocol
!
event manager applet GE-DOWN
event track 2 state down
action execute1 cli command "enable"
action execute2 cli command "conf t"
action execute3 cli command "interface Gi0/1"
action execute4 cli command "shutdown"
```

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6815/config_guide_eem_configuration_for_cisco_integrated_services_router_platforms.html

Embedded Event Manager

Мониторинг и управление устройством

Изменение состояния объекта

```
track object 8 stub
!
interface FastEthernet2/0
 ip address 10.1.99.2 255.255.255.0
 duplex full
 standby 1 ip 10.1.99.10
 standby 1 preempt
 standby 1 track 8
!
event manager applet memory-demo
event snmp oid 1.3.6.1.4.1.9.9.48.1.1.1.6.1 get-type
 exact entry-op lt entry-val 5120000 poll-interval 10 action 1.0 syslog priority
   critical msg "Memory exhausted; current available memory is $_snmp_oid_val_bytes"
action 2.0 track set 8 state down
```

Как только счетчик ciscoMemoryPoolEntry станет менее 5Mb, переключить HSRP на резервный (standby) узел

Ищите готовые скрипты:

- **http://www.cisco.com/go/ciscobeyond**

Пишите свои скрипты:

- **http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_policy_tcl.html**

Обслуживание
Remote Network Monitoring

Remote Network Monitoring

Инфрастуктура контроля и управления

- Формализована в стандартах RFC
- Выполняет мониторинг, обработку и пересылку информации о состоянии сети и устройств в ней
- Информация разбита на группы
- В реализации RMON допускается поддержка любого подмножества групп
- Структура поддерживаемой группы должна соответствовать стандарту
- В Cisco IOS поддерживается подмножество групп RMON 1
- *Специальный модуль Network Analysis Module (NAM) поддерживает группы и форматы RMON2 и др.*

- Описывает группы:
  - ✓ *The Ethernet Statistics Group*
  - ✓ *The History Control Group*
  - ✓ *The Ethernet History Group*
  - ✓ *The Alarm Group*
  - ✓ The Host Group
  - ✓ The HostTopN Group
  - ✓ The Matrix Group
  - ✓ The Filter Group
  - ✓ The Packet Capture Group
  - ✓ *The Event Group*

http://www.faqs.org/rfcs/rfc1757.html
http://www.faqs.org/rfcs/rfc3577.html

Remote Network Monitoring

Использование групп Event и Alarm

Реакция на абсолютное значение

```
rmon event 1 log trap public description "CPU utilization hit 75%"
rmon event 2 log trap public description "CPU utilization recovered"
rmon alarm 3 cpmCPUTotalTable.1.8.1 300 absolute rising-threshold 75 1 falling-
  threshold 30 2
```

Реакция на разницу значений

Для Ethernet 0/1 (ifEntry.10.3) 10% за 60сек составляет 7864320 (0.1 * 10Mbps / 8 * 60):

```
rmon event 1 log trap public description "Ethernet utlization is more than 10%"
rmon event 2 log trap public description "Ethernet utlization is below 5%"
rmon alarm 1 ifEntry.10.3 60 delta rising-threshold 7864320 1 falling-threshold
  3932160 2
```

Качество сервиса

IP Service Level Agreement

IP Service Level Agreement

Каково состояние и производительность сети между любыми двумя ее точками?

- Идентификация состояния сети в реальном времени позволяет быстро реагировать на возникающие проблемы и прогнозировать развитие ситуации

- Измерения доступны по каждому классу трафика (в соответствии с параметром DiffServ), а также по каждому VRF

- Для проверки работы сервиса может быть сгенерирован трафик со свойствами, присущими проверяемому сервису (размер пакета, класс QoS, протокол и порты, частота посылок)

- Высокая точность проверки (до 0.1мс) в режимах round-trip и unidirectional

http://www.cisco.com/en/US/technologies/tk648/tk362/tk920/technologies_white_paper09186a00802d5efe.html

IP Service Level Agreement

Каково состояние и производительность сети между любыми двумя ее точками?

- IP SLA позволяет генерировать SNMP-посылки (traps) для извещения о переходе параметров за граничные состояния (+/- thresholds)

- Параметры, которые возможно измерить:
  - ✓ UDP: round-trip / one-way time, вариация задержки, потери, доступность удаленного узла
  - ✓ ICMP: пошаговое и round-trip время ответа, доступность удаленного узла
  - ✓ оценочные параметры голосовых сервисов (MOS/ICPIF)
  - ✓ DNS lookup, TCP connect, HTTP transaction time, время ответа DHCP-сервера
  - ✓ время отклика сетевых устройств

- Реакция на события:
  - ✓ верхняя и нижняя границы параметра
  - ✓ извещение оператора путем посылки SNMP trap
  - ✓ запуск другого IP SLA процесса для выполнения более детального анализа

http://www.cisco.com/en/US/technologies/tk648/tk362/tk920/technologies_white_paper09186a00802d5efe.html

IP Service Level Agreement

Компоненты

Источник запросов *Source*	Ответная часть *Responder*
▪ маршрутизатор с IOS ▪ периодическая посылка запросов ▪ сохранение результатов в MIB	▪ устройство с IP-стеком ▪ для некоторых операций требуется Cisco IOS

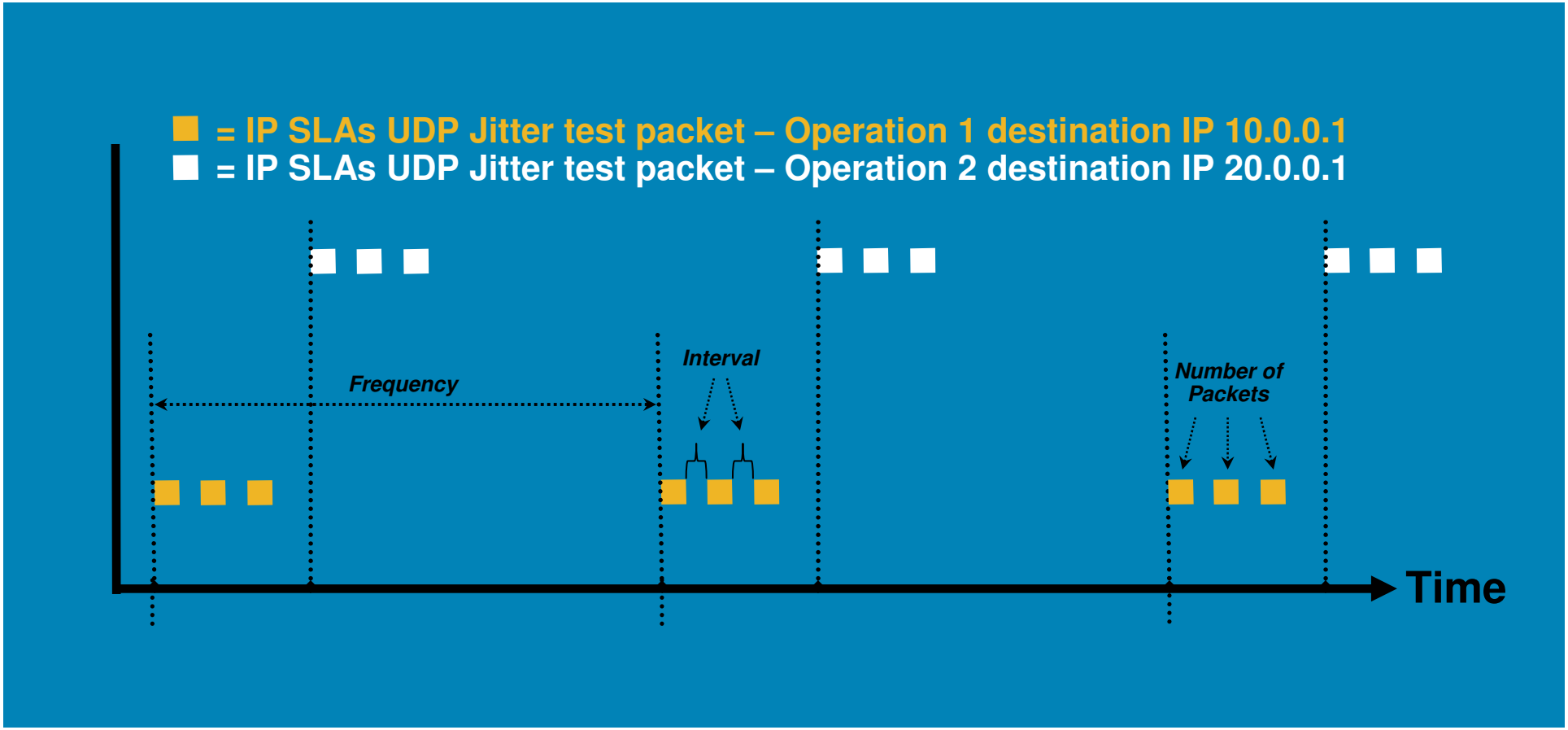
Протокол управления

- источник посылает сигнал о начале теста (1967/udp)
  - ✓ тип теста
  - ✓ порт для теста
  - ✓ количество, частота проб
- ответная часть
  - ✓открывает соответствующий порт
  - ✓ заполняет timestamp в ответе (*)

(*) источник и ответная часть должны быть синхронизированы по времени

IP Service Level Agreement

Пример выполнения измерения UDP Jitter



UDP Jitter default settings:

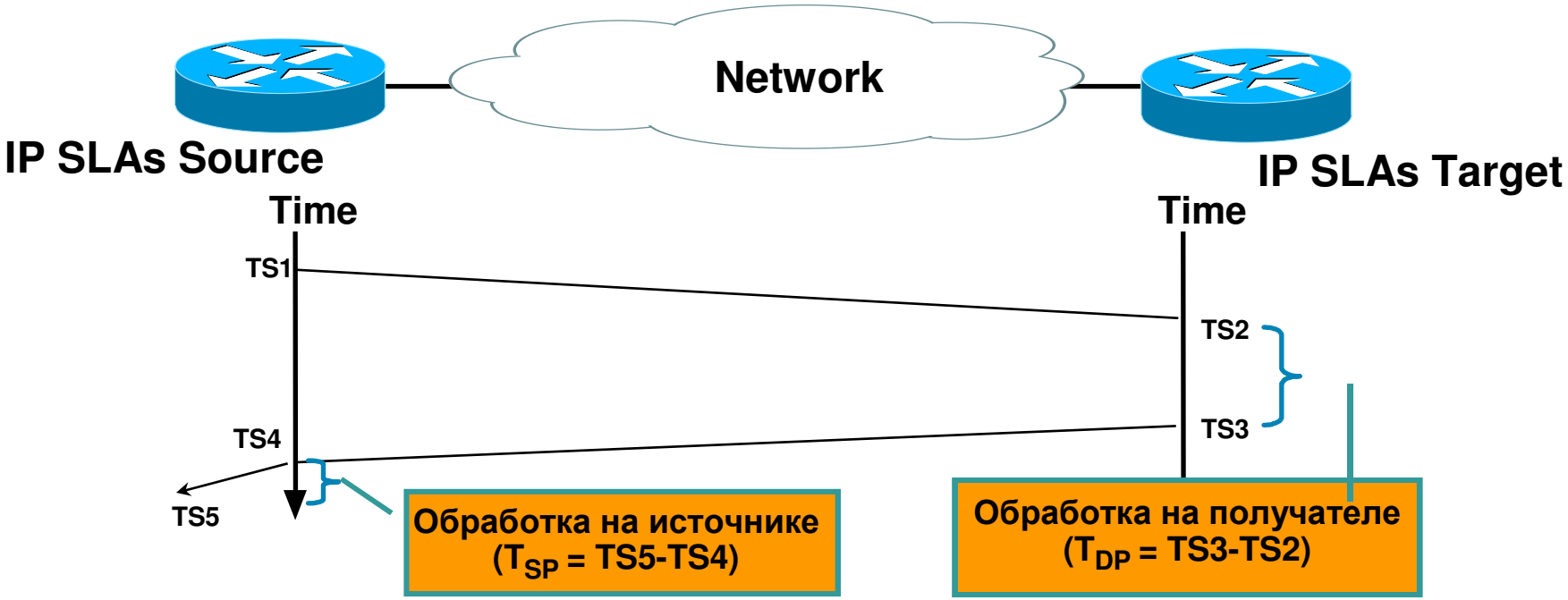
- **Frequency = 1 minute**
- **Interval = 20 milliseconds**
- **Number of Packets = 10**

Measurements:

- **Uni-directional Jitter**
- **Uni-directional Packet Loss**
- **Uni-directional Latency**

IP Service Level Agreement

Таймеры



- Round-Trip Delay (without Responder)

  TS5 - TS1 – T_{SP}
- Round-Trip Delay (with Responder)

  (TS5 – TS1) – T_{SP} – T_{DP}
- One-Way Delay (with Responder)

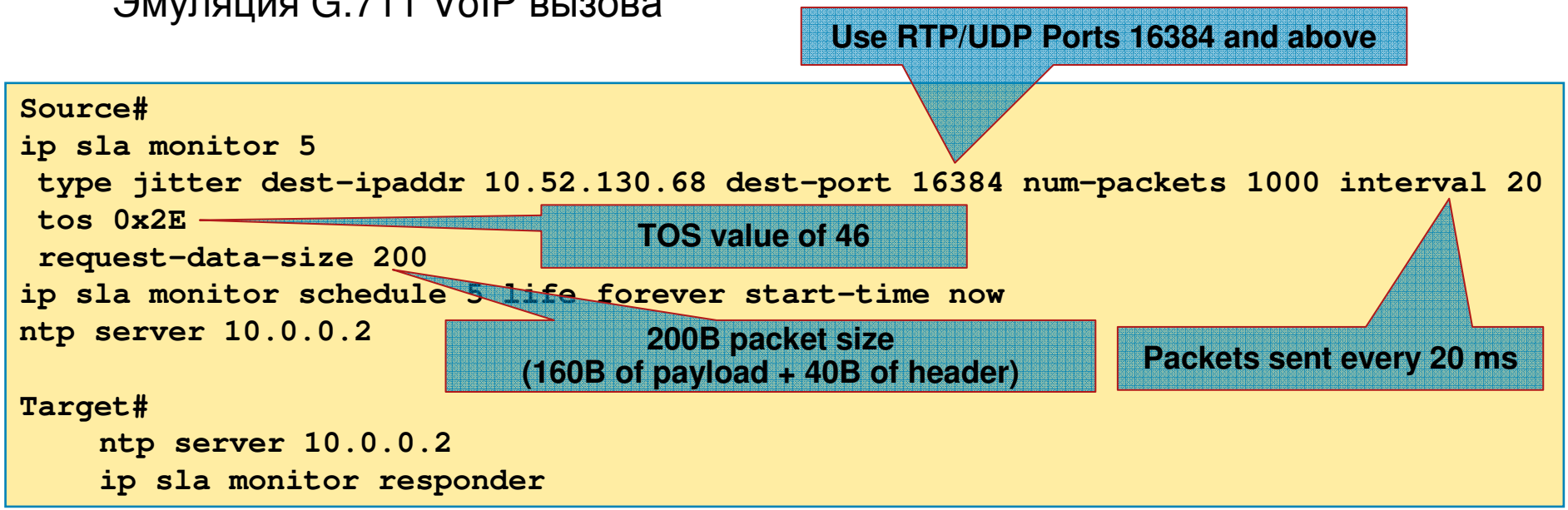
  TS2 – TS1

• Обработка пакетов IP SLAs поизводится так же, как и обработка трафика проверяемого класса

IP Service Level Agreement

Пример проверки UDP Jitter

Эмуляция G.711 VoIP вызова



NOTE: используйте Cisco Voice Codec Bandwith Calculator:

http://tools.cisco.com/Support/VBC/do/CodecCalc1.do

IP Service Level Agreement

Пример проверки UDP Jitter

```
Router#sh ip sla monitor op 5
        Current Operational State
Entry Number: 1
Modification Time: 08:22:34.000 PDT Thu Aug 22 2002
Diagnostics Text:
Last Time this Entry was Reset: Never
Number of Octets in use by this Entry: 1594
Number of Operations Attempted: 1
Current Seconds Left in Life: 574
Operational State of Entry: active
Latest Operation Start Time: 08:22:34.000 PDT Thu Aug 22 2002
Latest Oper Sense: ok
RTT Values:
NumOfRTT: 997   RTTSum: 458111  RTTSum2: 238135973
Packet Loss Values:
PacketLossSD: 3 PacketLossDS: 0
PacketOutOfSequence: 0  PacketMIA: 0    PacketLateArrival: 0
InternalError: 0        Busies: 0
(cont…)
```

3 packets lost S->D out of 1000 sent.

Average RTT was 458111/997 = 459ms.

IP Service Level Agreement

Пример проверки HTTP GET

Возможность запроса в форме RAW:

- *тип (HTTP/1.x), URL*
- *указание пароля*

Необязательная часть, для специфических задач

```
ip sla monitor 1
 type http operation raw url \
       http://www.cisco.com
http-raw-request
GET /lab/index.html HTTP/1.0\r\n
Authorization: Basic btNpdGT4biNvoZe=\r\n
\r\n

exit
ip sla monitor schedule 1 start-time now
```

IP Service Level Agreement

Синтаксис

```
Router(config)#ip sla monitor 1

Router(config-sla-monitor)#type ?
  dhcp         Perform DHCP Operation
  dlsw         Perform DLSw Keepalive Operation
  dns          Perform DNS Query
  echo         Perform Point to Point Echo Operations
  ftp          Perform ftp operation
  http         Perform HTTP Operations
  jitter       Perform Jitter Operation
  pathEcho     Perform Path Discovered Echo Operations
  tcpConnect   Perform TCP Connect Operations
  udpEcho      Perform UDP Echo Operations

Router(config-sla-monitor)#?
    [ ... ]
    threshold           Operation Threshold in msec

Router(config)#ip sla monitor reaction-configuration [ ... ]

Router(config)# ip sla monitor responder [ ... ]
```

Cisco Expo 2008

Проектирование управляемости

Патенко Владислав

Инженер-консультант, системы управления

Enable Your Network
Empower Your Business

Дополнительная информация об обслуживании и мониторинге сети доступна в презентации Владислава Патенко

«Проектирование управляемости в сервисно-ориентированных сетях»
CiscoExpo’2008

Качество сервиса

Cisco Performance Routing

Cisco Performance Routing

SP as Enterprise

- Традиционная маршрутизация основана на статических метриках (hop count, path cost, др.)

- Сходимость сети основана на информации от соседних маршрутизаторов и состоянии линков (up/down)

- Маршрутизация работает на основании адреса получателя

- Эти механизмы не учитывают:
  - ✓ загрузку каналов
  - ✓ ухудшение качества транспорта
  - ✓ требования приложений для пропускной полосы

Сеть вроде бы работает. А приложения?

Cisco Performance Routing

SP as Enterprise

- Технология Cisco Performance Routing (PfR) реализует расширенные механизмы выбора пути, основанные на параметрах производительности сети
- Может быть использована для адаптации маршрутов под изменившиеся условия
- Критериями для изменения маршрута могут быть:
  - ✓ время отклика
  - ✓ потери пакетов
  - ✓ вариация задержки
  - ✓ Mean Opinion Score (MOS)
  - ✓ и др.
- Поставщиками этой информации являются:
  - ✓ IP SLA
  - ✓ Netflow v9

Cisco Performance Routing

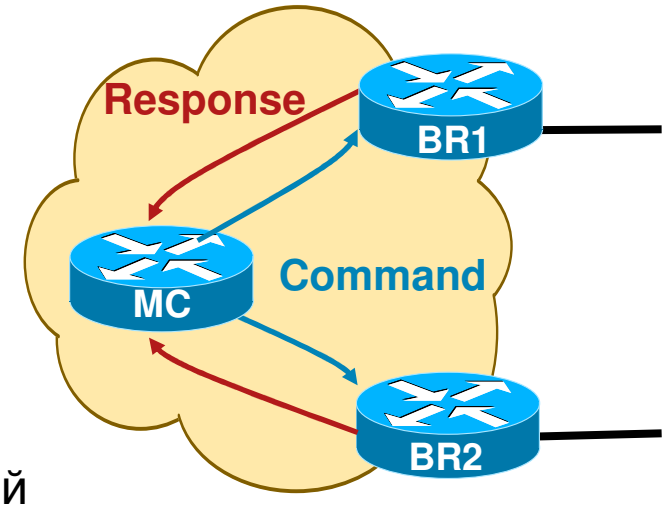
Определение классов трафика

Класс трафика		Например
Destination Prefix		10.0.0.0/8 20.1.1.0/24
Приложение	**ACL**	10.1.1.0/24 dscp ef 10.1.1.0/24 dst-port 50
	Well-known	10.1.1.0/24 telnet 20.1.0.0/16 ssh
	Dynamic Recognition	10.1.1.0/24 nbar RTP 20.1.1.0/24 nbar citrix

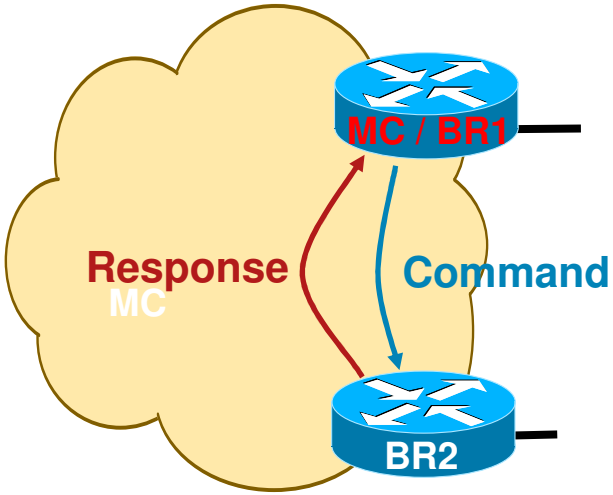
Cisco Performance Routing

Компоненты технологии

- Master Controller (MC)
  - Управляет BR
  - Содержит информацию о классах трафика
  - Сообщает о событиях
  - Сообщает о параметрах измерений
  - Принимает решения об изменении политик

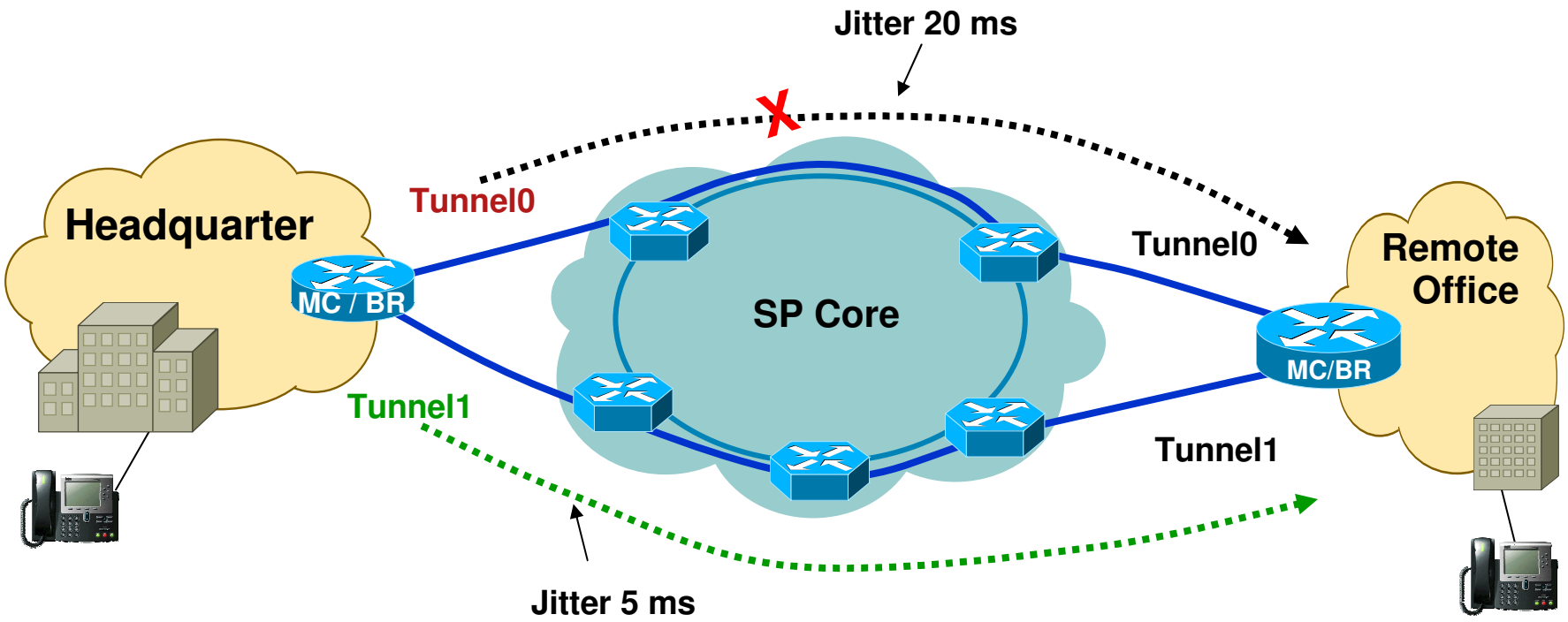


- Border Router (BR)
  - Управляется MC
  - Измеряет параметры производительности
    - ✓ классов трафика
    - ✓ каналов связи
  - Применяет политики, полученные от MC



Cisco Performance Routing

Пример оптимизации корпоративного VoIP



- Качество голосового соединения рассчитывается на основе MOS
- MOS вычисляется на основе задержки, вариации задержки и потерь трафика
- PfR выберет путь с наилучшим параметром MOS

  Tunnel1 – 95 из 100 проб с MOS >= 4.00 ← **Лучше**

  Tunnel0 – 80 из 100 проб с MOS >= 4.00

Cisco Performance Routing

Доступные ресурсы

- ***Стартовая страница***
  http://www.cisco.com/go/pfr

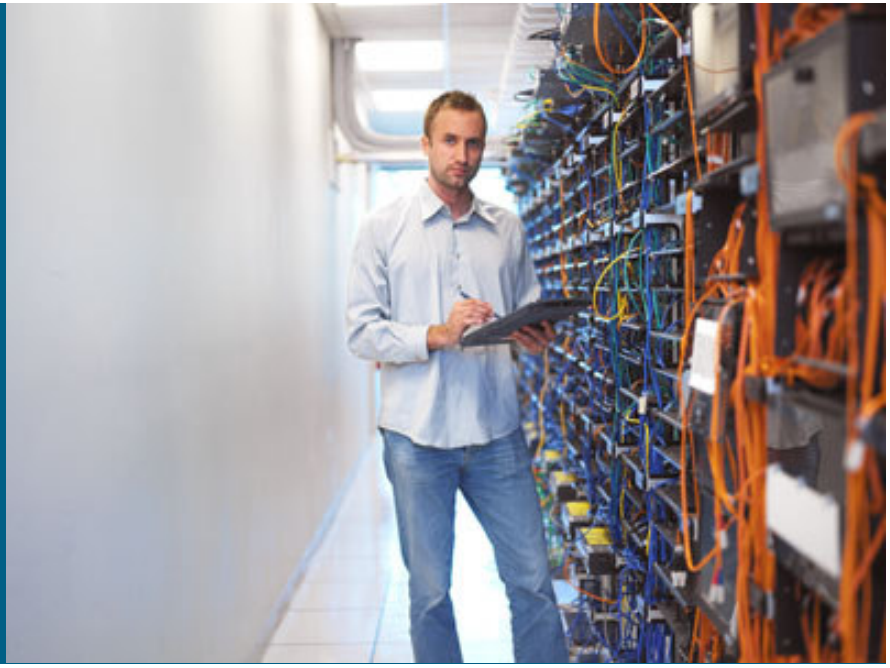
- ***Мифы и факты о Cisco Performance Routing:***
  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6554/ps6599/ps6628/prod_presentation0900aecd80608e97.pdf

- ***Performance Routing Design Guide:***
  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns483/c649/ccmigration_09186a008094e673.pdf

- ***Руководство по конфигурированию:***
  http://www.cisco.com/en/US/docs/ios/oer/configuration/guide/12_4t/oer_12_4t_book.html

Вопросы?

Не забудьте оставить нам свои комментарии! ☺




CISCO