

Cisco Expo 2011



Как обеспечить контроль производительности сети и приложений ?

Патенко Владислав, Инженер-консультант, системы управления

vpatenko@cisco.com

innovate *together*

Оцени контент Cisco Expo и получи приз!

Призы ждут всех, кто:

- посетил 2 и более дней конференции
- заполнил общую анкету
- заполнил 5 и более сессионных анкет
- заполнил анкеты по 2 и более плановым демо

Онлайн-анкеты доступны на сайте www.ceq.com.ua.

Анкеты также можно заполнить, воспользовавшись терминалами в зоне общения на первом этаже.



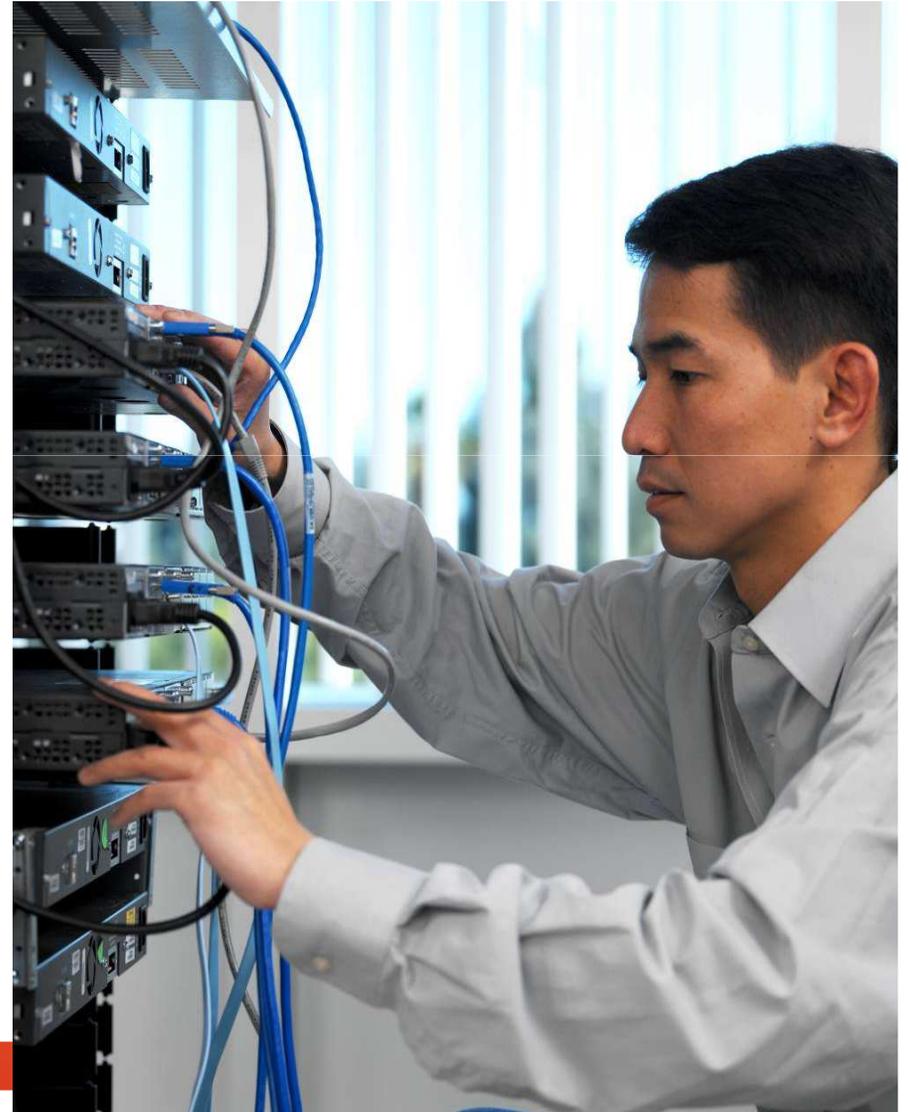
Потребность в контроле производительности

- В мире сетевых технологий ИТ часто является лицом компании
- Приложения должны обеспечивать простоту и надежность использования заказчиками
- Продуктивность компании часто зависит от ИТ
- Современные сети зачастую сложны в эксплуатации и диагностике
- Разные типы приложений (голос, видео, данные) имеют разные требования к сети



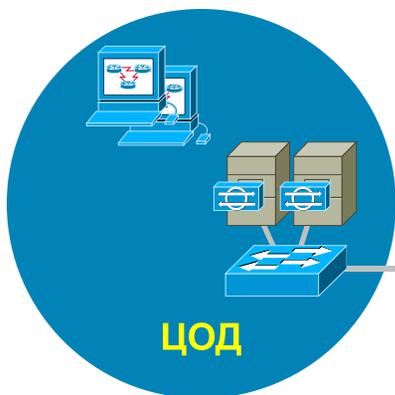
Тенденции в IT

- Часто источник проблем с производительностью неизвестен
- Требования по производительности приложений от удаленных пользователей
- Внедрение приложений без проведения анализа влияния на производительность других информационных систем
- Профиль работы приложения изменяется с централизацией ЦОДов.

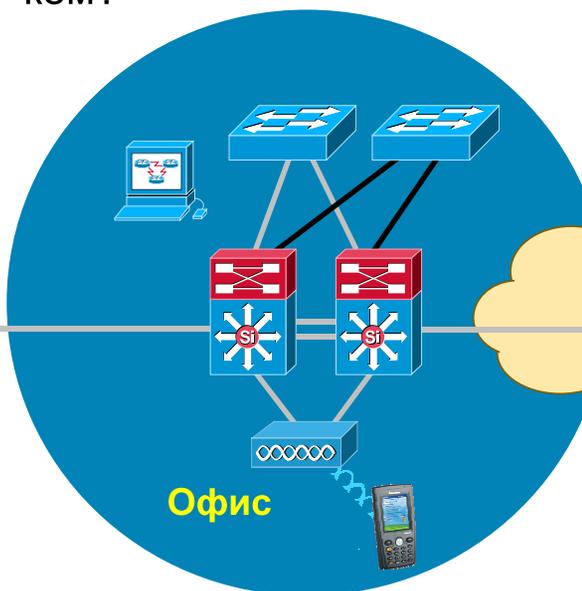


Какие решения для контроля производительности мне нужны?

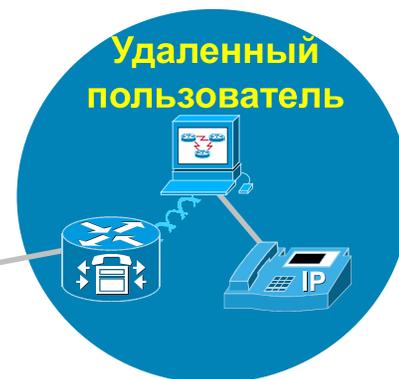
Что будет, если установить новое приложение?



Какие приложения используются на сети и кем?



Какая причина медленного ответа приложения?



Как управлять сетевым трафиком, учитывая требования каждого приложения?

Какая полоса пропускания канала между офисами будет оптимальной?

Удовлетворяет ли текущая ситуация потребности бизнеса?



Технологии измерения производительности

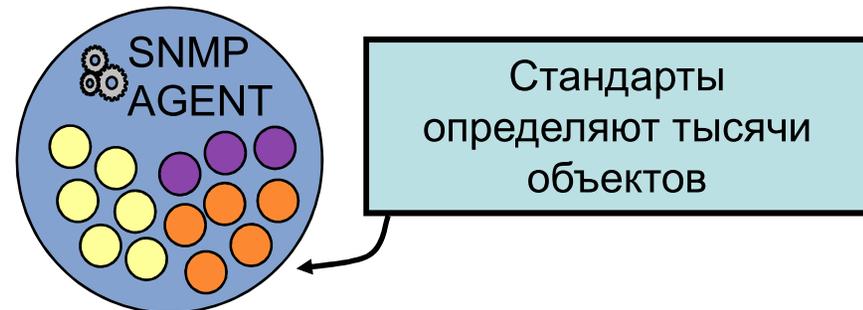


Технологии измерения производительности

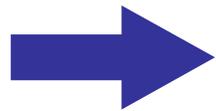
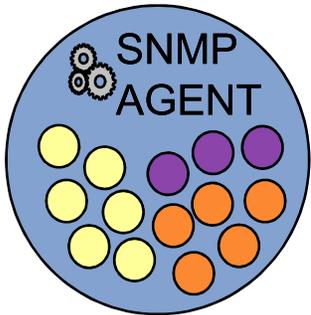


Технология измерения производительности: SNMP

- SNMP (Simple Network Management Protocol) – базовый протокол для получения данных с устройства
- SNMP MIB:
 - Набор переменных, определяющих состояние устройства (напр. темп = 85°)
 - Только факт — без выводов, хорошо это или плохо
 - Структура определена согласно стандартов
 - Каждый объект (переменная) идентифицируется уникальным ID (OID)
- MIB I/MIB II:
 - Стандартный MIB
 - Объекты используются в основном для мониторинга состояния и настройки
- Другие стандартные MIB:
 - RMON, host, router.
- MIB производителей:
 - Расширения стандартных MIB

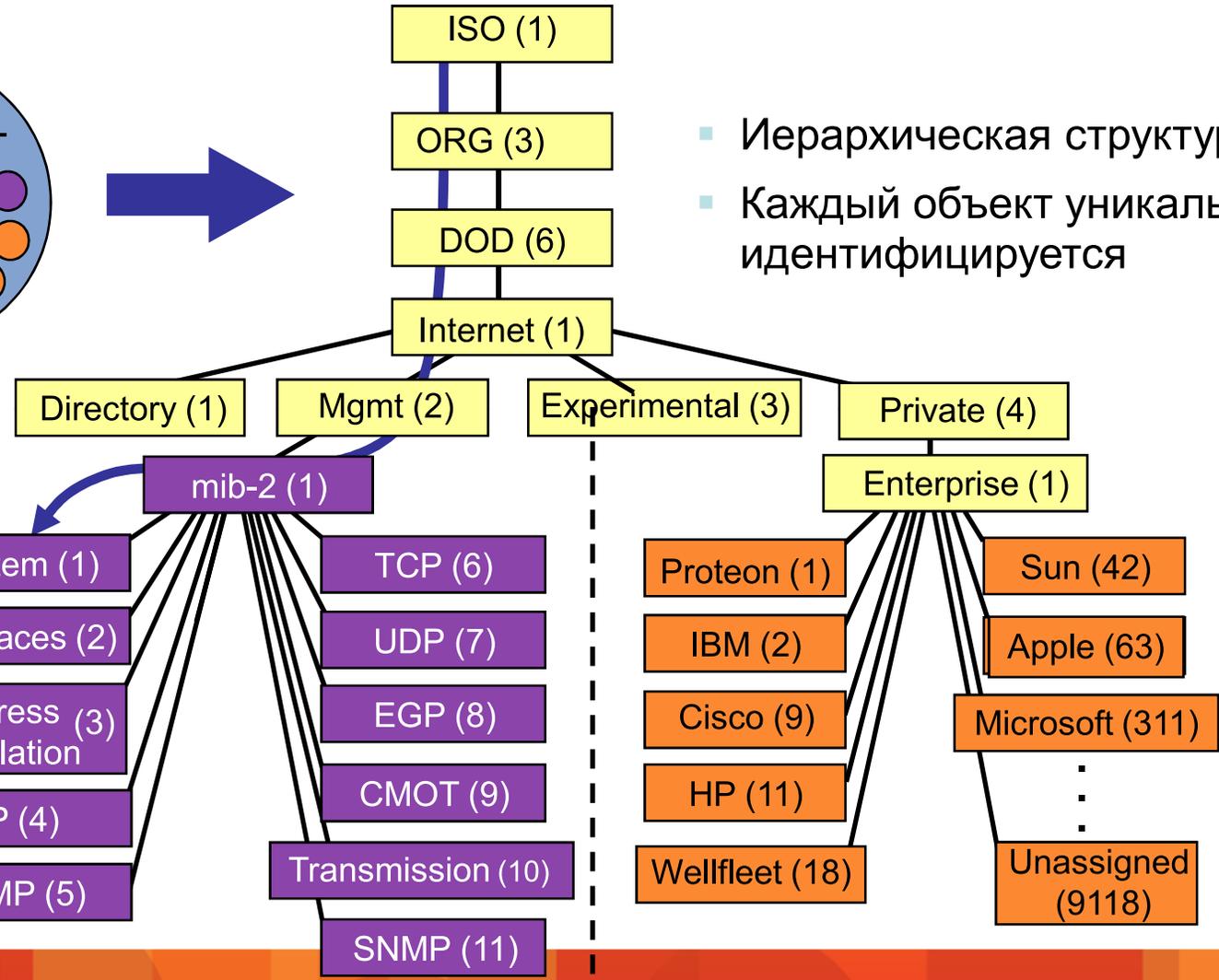


Идентификаторы объектов MIB



- Иерархическая структура
- Каждый объект уникально идентифицируется

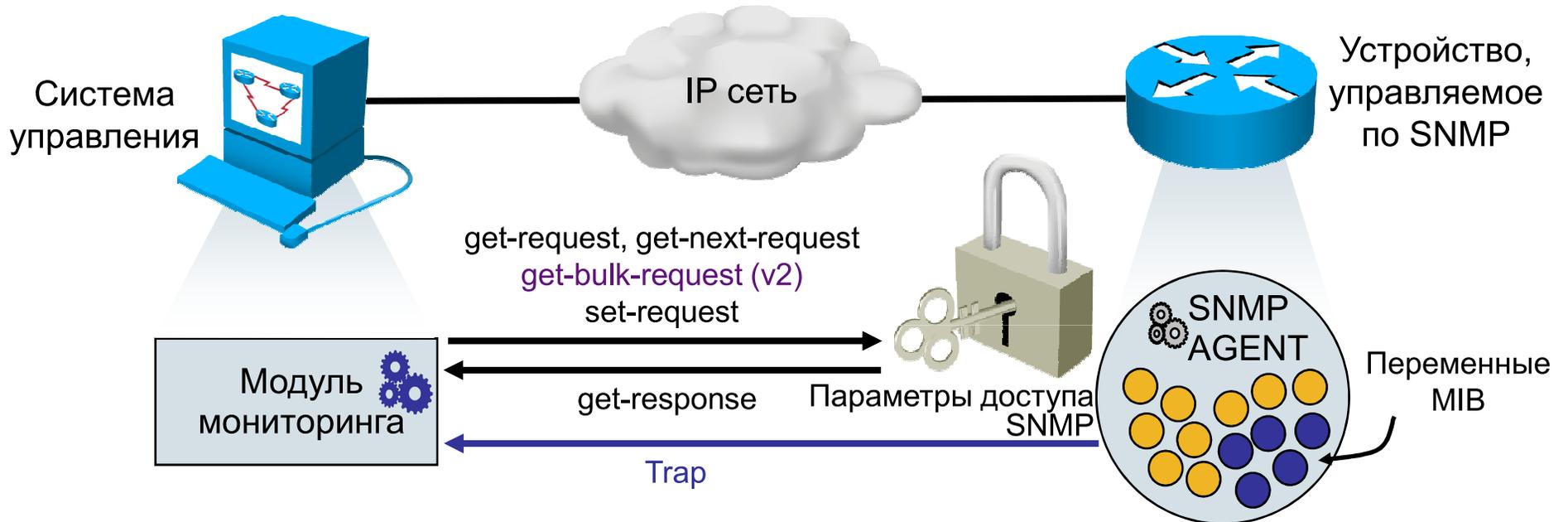
OID для system
1.3.6.1.2.1.1



Стандартные объекты

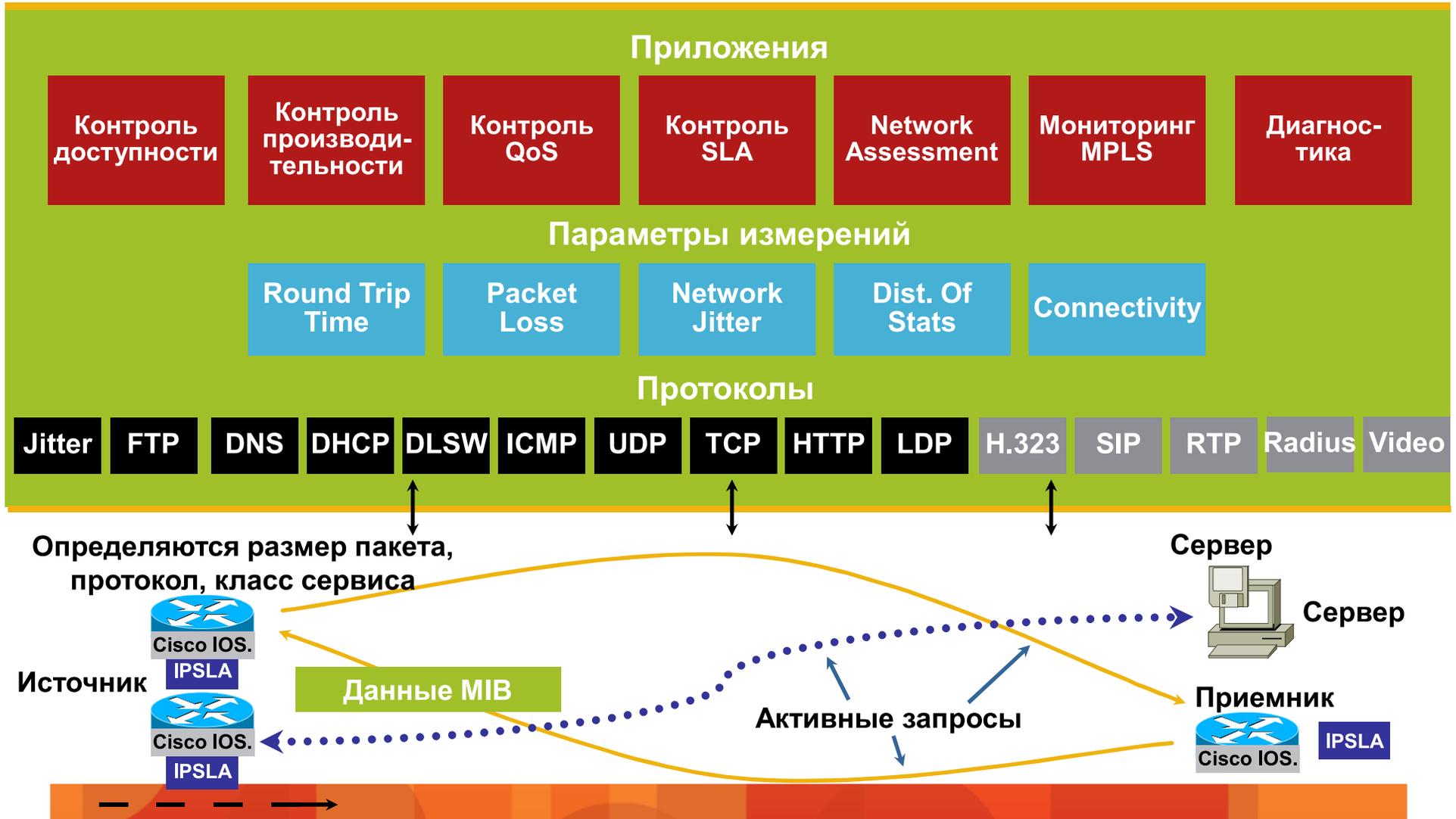
Объекты производителей

Взаимодействие по протоколу SNMP

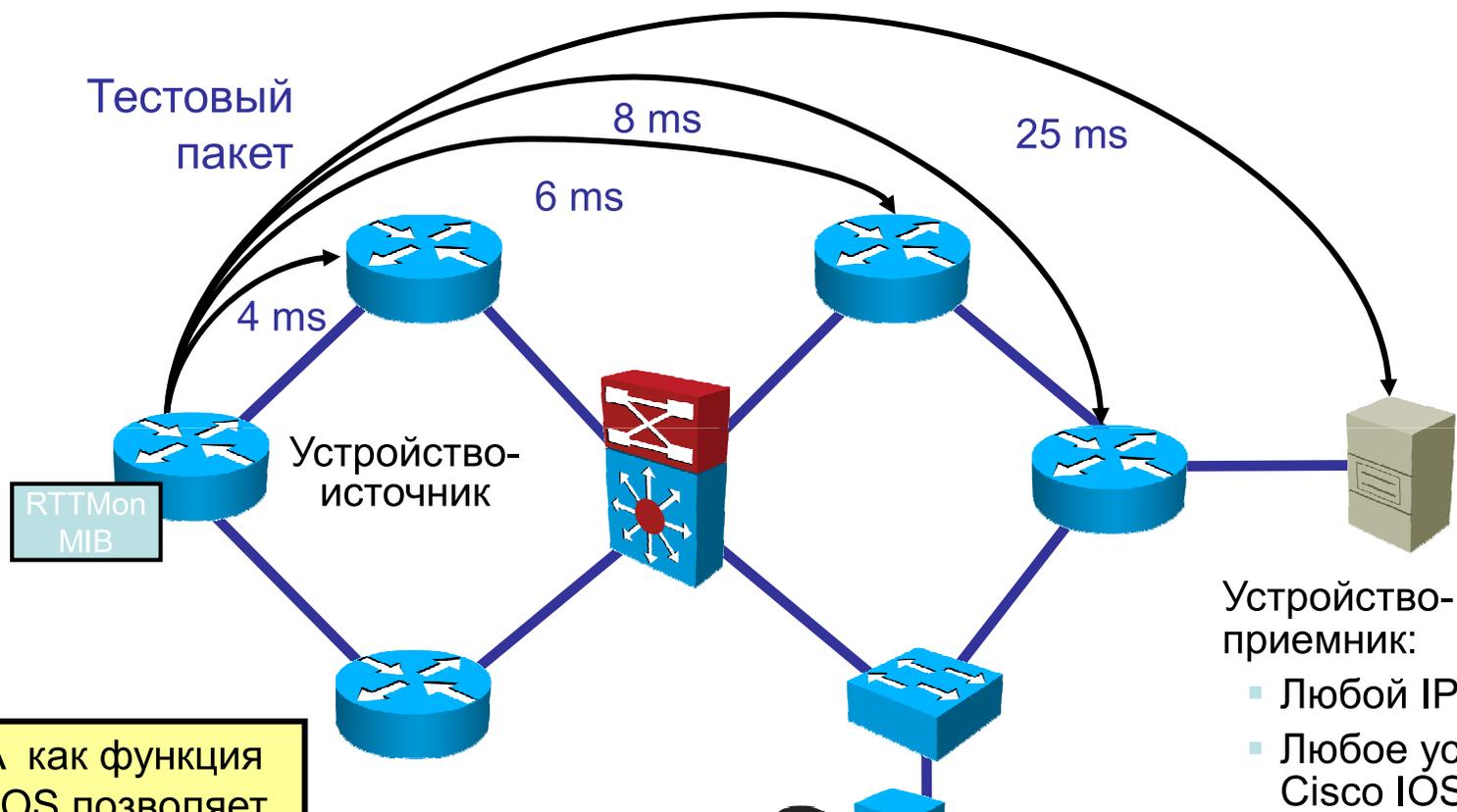


- Данные собираются с определенной периодичностью, обычно 5 мин.
- Типовые переменные: загрузка CPU, загрузка интерфейсов, ошибки
- SNMP обычно не дает возможность получить информацию о структуре трафика

Технология измерения: IPSLA



Как работает IP SLA?



IP SLA как функция Cisco IOS позволяет проводить тесты между любыми устройствами в сети

- Система управления:
 - Настройка IP SLA
 - Просмотр результатов

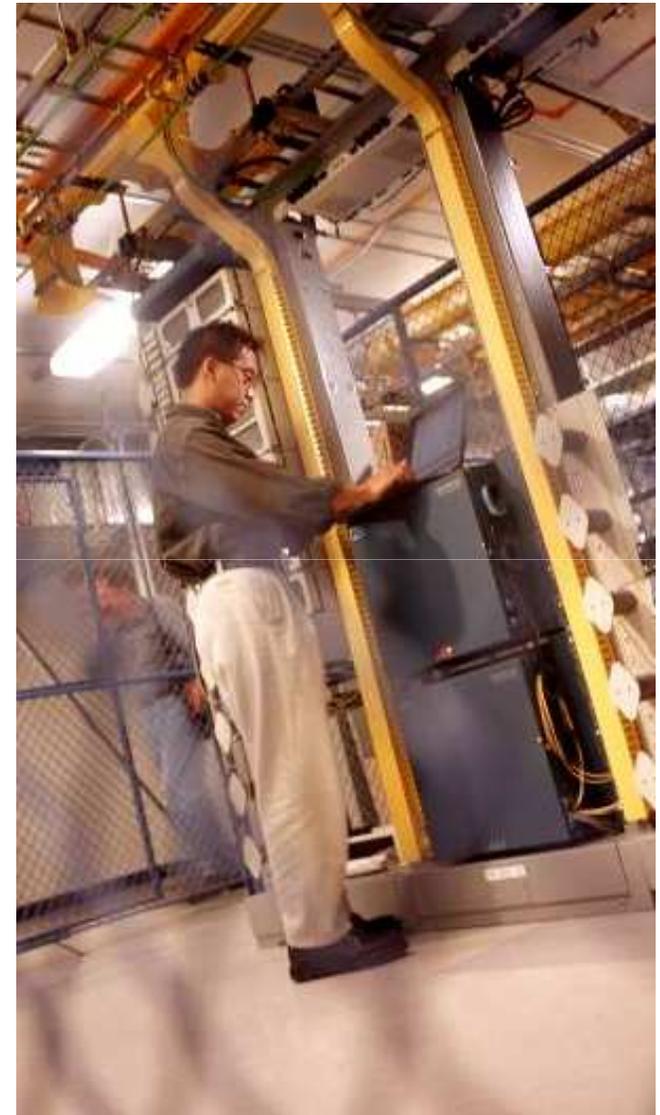


Технологии измерения производительности

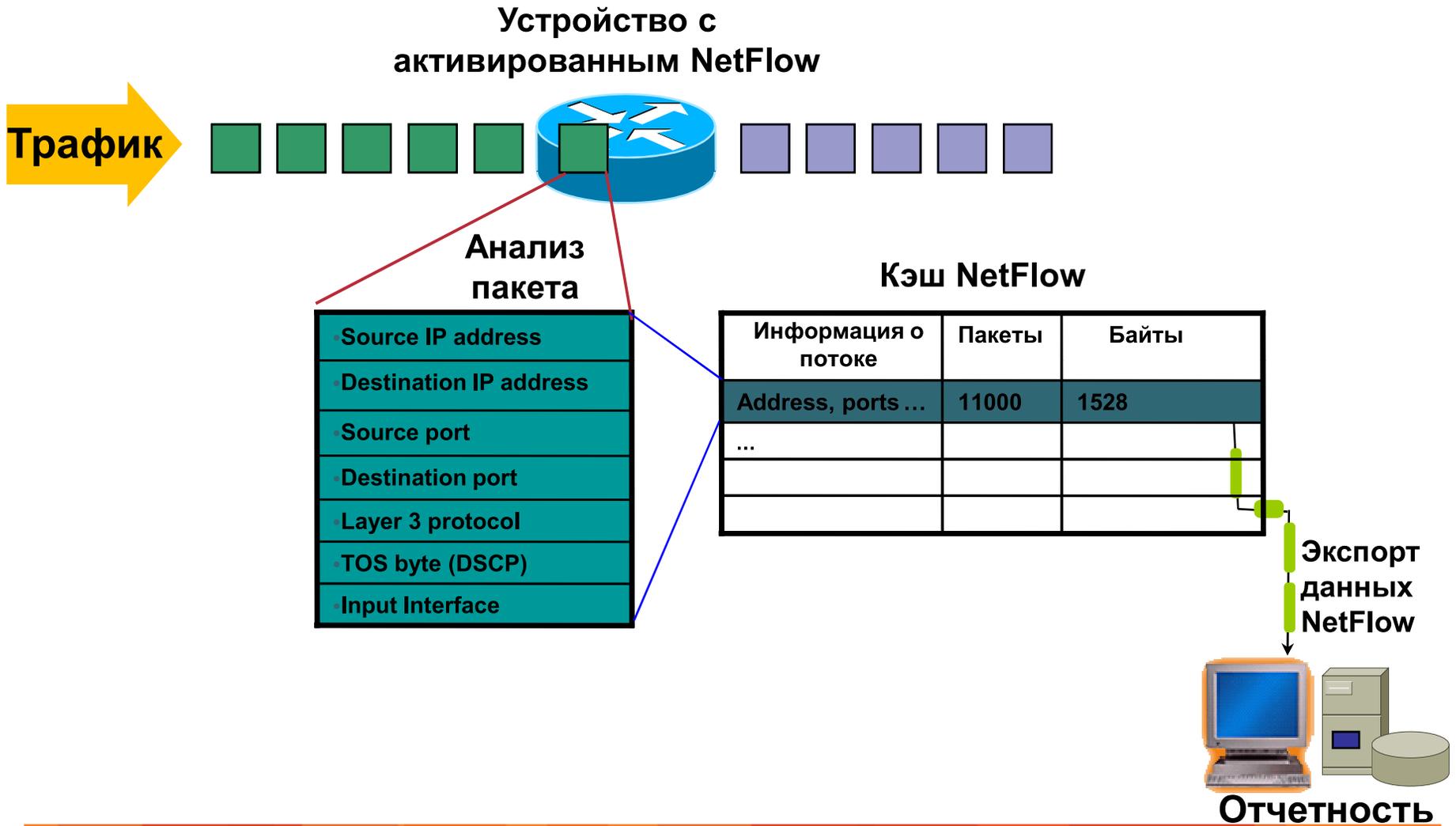


Что такое Cisco IOS NetFlow ?

- Технология, разработанная и запатентованная Cisco® Systems в 1996 году
- NetFlow - стандарт де факто для получения информации о потоках данных в сетях IP
- Предоставляет данные для мониторинга сети, планирования, анализа и учета



Определение потока Netflow



Примеры формирования потоков NetFlow

Пример 1



Анализ пакета

Key Fields	Packet 1
Source IP	1.1.1.1
Destination IP	2.2.2.2
Source Port	23
Destination Port	22078
Layer 3 Protocol	TCP - 6
ToS Byte	0
Input Interface	Ethernet 0

1. Анализ пакета и идентификация полей
2. Сравнение значений с кэшем NetFlow
3. Создание записи в кэше, если пакет уникальный
4. Проверка следующего пакета

Source IP	Dest. IP	Dest. I/F	Protocol	ToS	...	Pkts
1.1.1.1	2.2.2.2	E1	6	0	...	11000

Пример 2



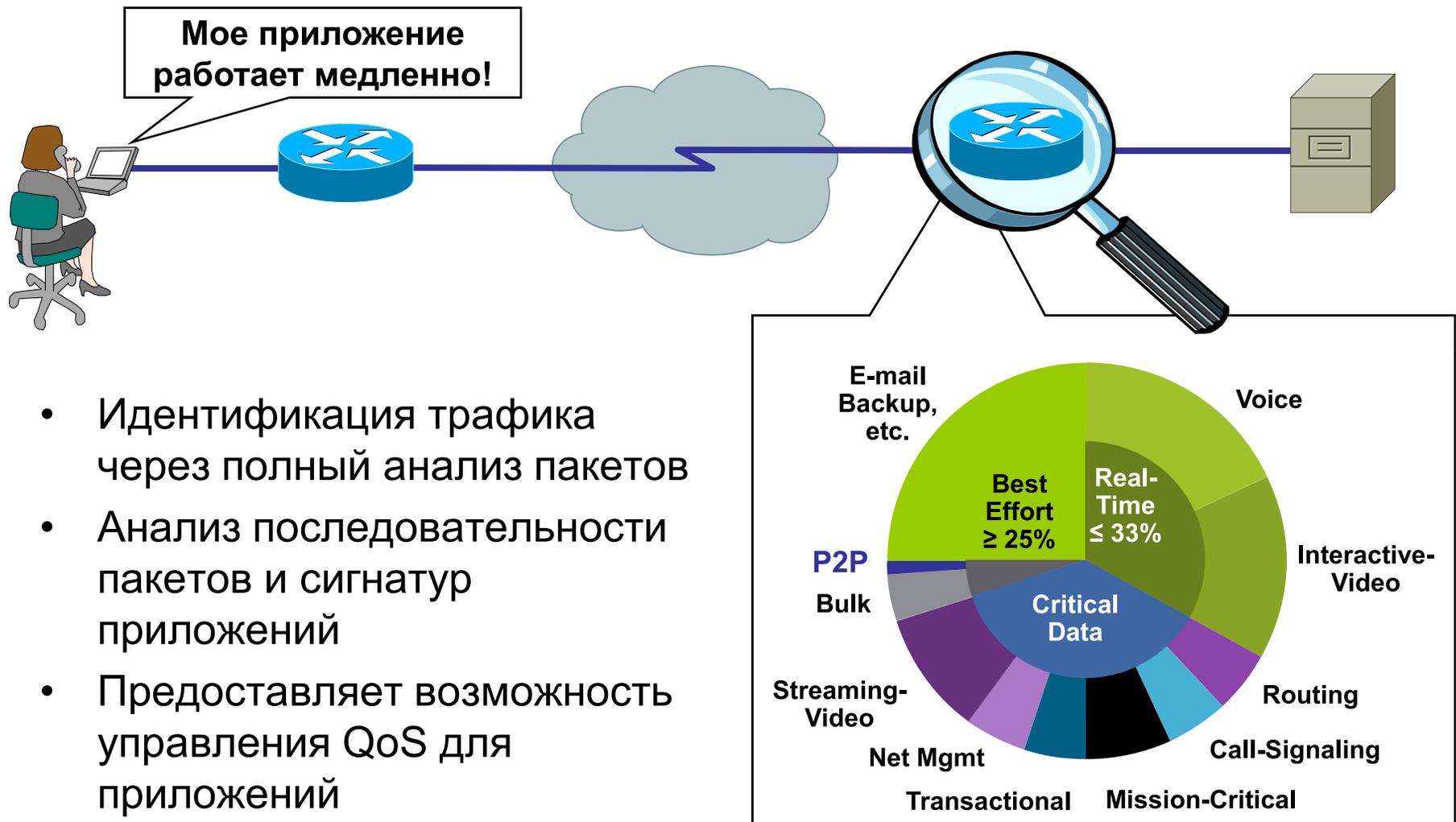
Анализ пакета

Key Fields	Packet 2
Source IP	3.3.3.3
Destination IP	2.2.2.2
Source Port	23
Destination Port	22078
Layer 3 Protocol	TCP - 6
ToS Byte	0
Input Interface	Ethernet 0

Source IP	Dest. IP	Dest. I/F	Protocol	ToS	...	Pkts
3.3.3.3	2.2.2.2	E1	6	0	...	11000
1.1.1.1	2.2.2.2	E1	6	0	...	11000

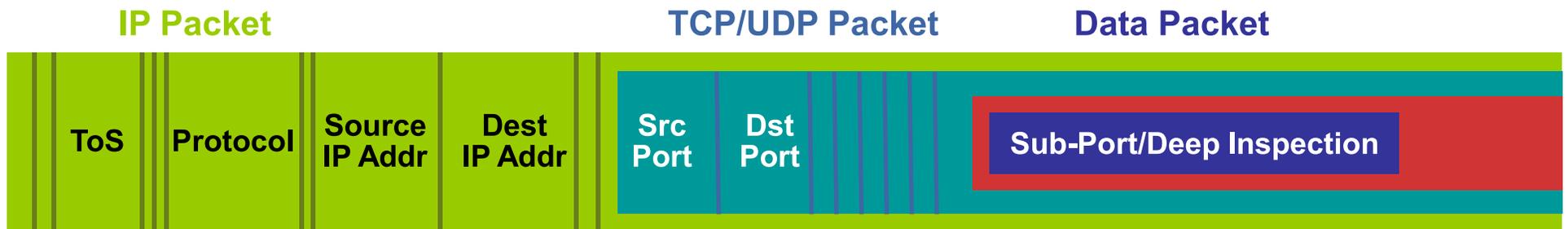


Технология измерения: NBAR



Загрузка канала связи

Технология NBAR: Deep Packet Inspection (DPI)

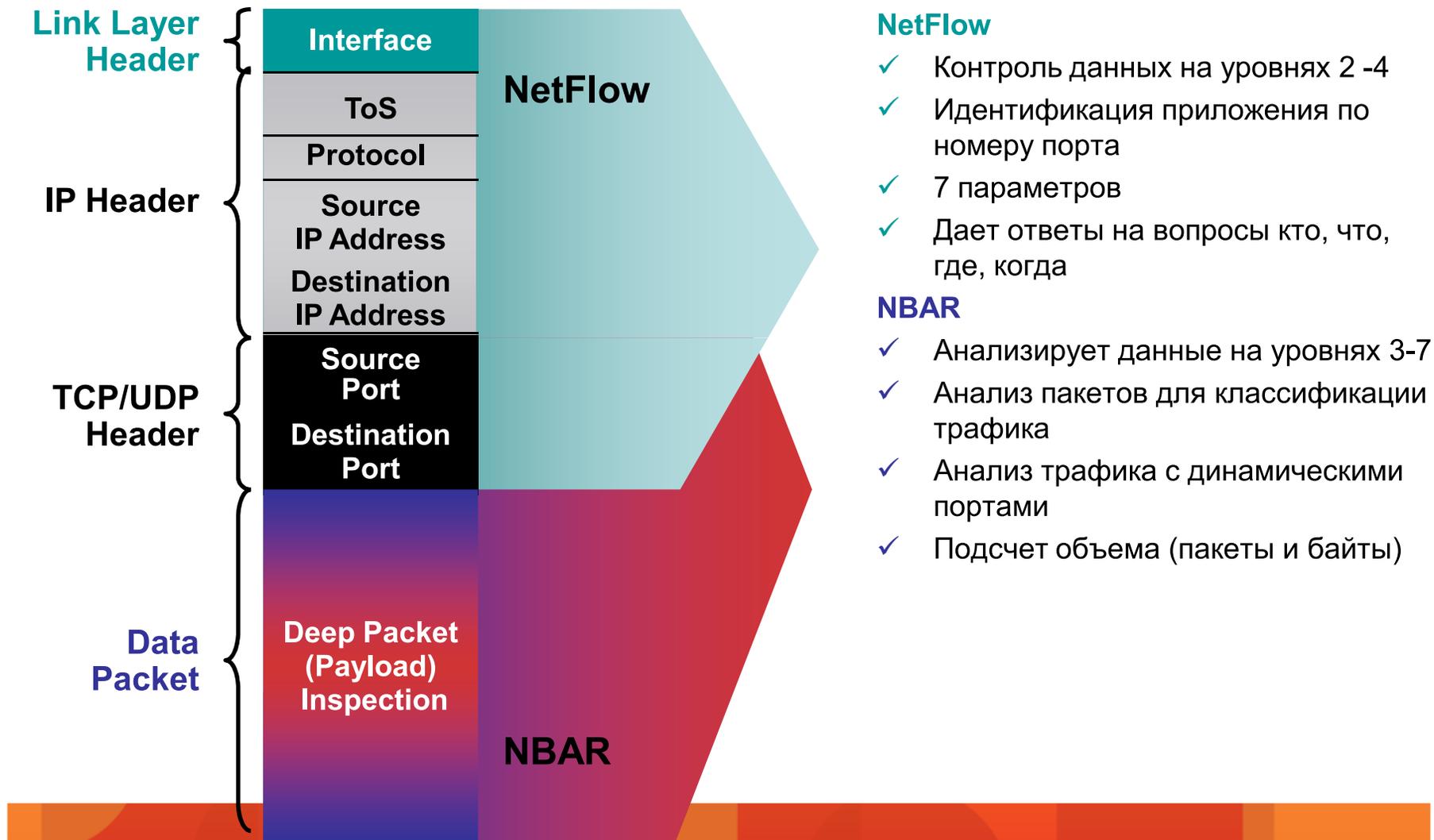


- Идентификация приложений и протоколов по номерам портов TCP и UDP которые
 - Назначены статически
 - Назначены динамически в процессе установления соединения
- Не-TCP и не-UDP протоколы
- Классификация заголовка
- Анализ данных в пакете

NBAR — примеры протоколов

Приложения	Туннели	Почтовые ИС	Интернет
Citrix ICA	GRE	IMAP	FTP
PCAnywhere	IPINIP	POP3	Gopher
Novadigm	IPsec	Exchange	HTTP
SAP	L2TP	Notes	IRC
Маршрутизация	MS-PPTP	SMTP	Telnet
BGP	SFTP	Каталоги	TFTP
EGP	SHTTP	DHCP/BOOTP	NNTP
EIGRP	SIMAP	Finger	NetBIOS
OSPF	SIRC	DNS	NTP
RIP	SLDAP	Kerberos	Print
Протоколы управления	SNMP	LDAP	X-Windows
ICMP	SPOP3	Потоковые протоколы	Peer-to-Peer
SNMP	STELNET	CU-SeeMe	BitTorrent
Syslog	SOCKS	Netshow	Direct Connect
RPC	SSH	Real Audio	eDonkey/eMule
NFS	Голосовые протоколы	StreamWorks	FastTrack
SUN-RPC	H.323	VDOLive	Gnutella
СУБД	RTCP	RTSP	KaZaA2
SQL *NET	RTP	MGCP	WinMX 2.0
MS SQL Server	SIP	Сигнализация	
	SCCP/Skinny	RSVP	
	Skype		
	MGCP		

Разница между NetFlow и NBAR



NetFlow

- ✓ Контроль данных на уровнях 2 -4
- ✓ Идентификация приложения по номеру порта
- ✓ 7 параметров
- ✓ Дает ответы на вопросы кто, что, где, когда

NBAR

- ✓ Анализирует данные на уровнях 3-7
- ✓ Анализ пакетов для классификации трафика
- ✓ Анализ трафика с динамическими портами
- ✓ Подсчет объема (пакеты и байты)

Инструментарий для измерения производительности приложений



Технологии измерения производительности

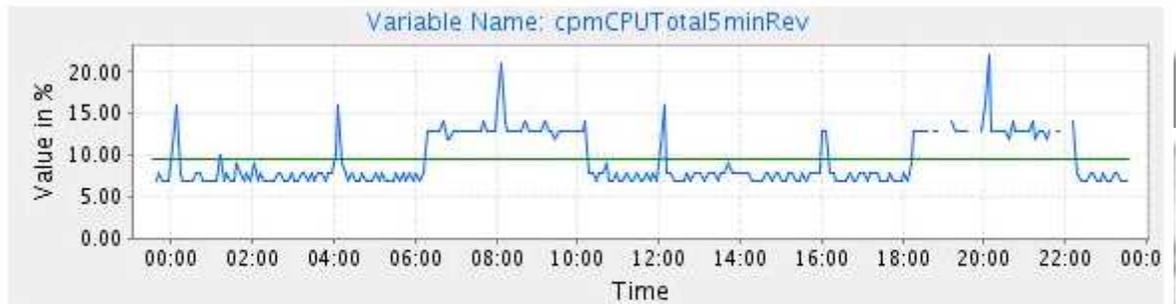


Обзор Prime LMS



Prime LMS: Сбор данных по производительности по SNMP

1. Добавить требуемый MIB
2. Выбрать требуемые переменные
3. Определить параметры сбора данных
4. Просмотреть отчет



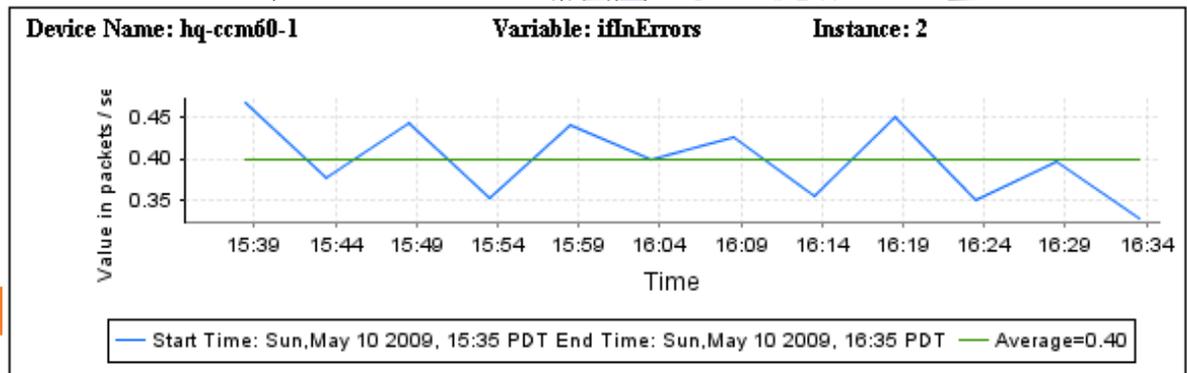
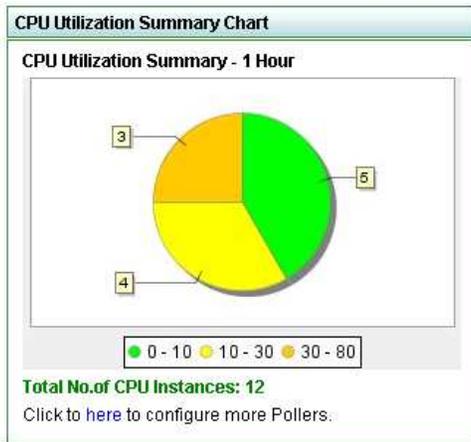
TOP-N CPU Utilization

Time Interval: 1 Hour

Device Name	CPU Instance	MIN %	MAX %	AVG %
10.77.208.108	1	39	39	39
10.77.209.19	CPU Utilization	29	34	32.15
10.77.209.209	CPU of supervisor	19	27	20.58
10.77.209.192	1	18	22	20.23
10.77.209.199	1	18	23	20.22

Legend: 0 - 10 (Green), 10 - 30 (Yellow), 30 - 80 (Orange), 80 - 100 (Red)

Click to [here](#) to configure more Pollers.



Prime LMS: Настройка граничных значений для мониторинга параметров

- Определить граничное значение и создать триггер
- При необходимости создать скрипт для выполнения какого-либо действия
- Получить аварийное событие или отчет о превышении граничных значений

The screenshot displays the 'Threshold Information' page in Prime LMS. It shows 3 configured thresholds and 48 critical violations in the last hour. A table lists threshold details for 'EnvMon' on device '20.20.110.11 - chassis', with violations at 27 and 38. A sidebar menu highlights 'Threshold Violations'. A 'Threshold Violation Summary' shows 1152 alarms, and a 'Critical Violation details' table lists specific violations for the 'EnvMon' rule.

Threshold Information			
No. of thresholds configured	3		
No. of violations in last 1 Hour	Low	Medium	Critical
	0	0	48
Threshold Details:			
Threshold Name	Device Name - Instance	Time	Violated Value
EnvMon	20.20.110.11 - chassis	Wed, Apr 22 2009, 10:02:48 PDT	27
	hassis Temperature Sensor	Wed, Apr 22 2009, 10:02:47 PDT	38

Threshold Violation Summary

Number Of Devices: 8
Number Of Thresholds: 1
Number Of Alarms: 1152

Severity	Count
Critical	1152

Critical Violation details

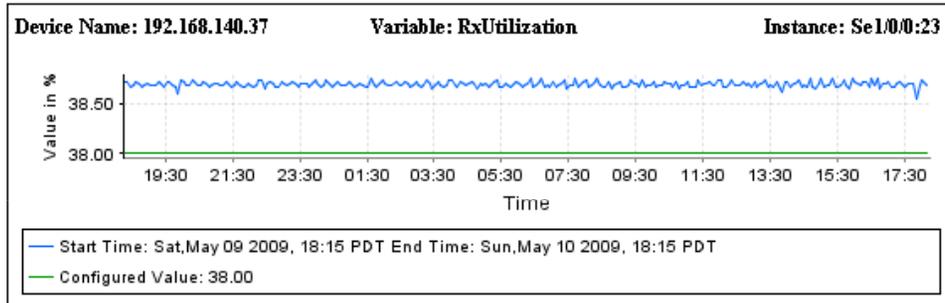
Threshold Name: EnvMon			
Rule: ciscoEnvMonTemperatureStatusValue >= 25.0Celsius			
DeviceName	Instance Name	Time Stamp	
20.20.3.2	Chassis Temperature Sensor	Sun, Apr 26 2009, 23:22	
20.20.110.11	chassis	Sun, Apr 26 2009, 23:22	
20.20.170.11	chassis	Sun, Apr 26 2009, 23:22	
20.20.150.11	chassis	Sun, Apr 26 2009, 23:22	

Prime LMS: Контроль тенденций

Summary	
TrendWatch Name:	MyUtilizationTrend
Rule:	HOURLY Avg of Interface Utilization.RxUtilization >= 38 and if it occurs atleast 3 Times
Syslog Group Name:	MySyslogGroup
Trap Group Name:	MyTrapGroup

1. Настройка механизма TrendWatch

2. Просмотр случаев выхода за граничные значения



TrendWatch			
No. of Trend-Watches configured 1			
No. of violations in last 1 Hour	Critical	Medium	Low
	1	0	0
Trend Watch Details:			
TrendWatch Name	Device Name / Instance	Severity Levels	TimeStamp
MyUtilizationTrend	192.168.140.37 / Se1/0/0:23	Critical	Sun, May 10 2009, 18:14:00 PDT

3. Отображение тенденций

5. Поддержка абсолютных и относительных значений

TrendWatch Details

TrendWatch Name: MyTrendThreshold Based on: Template Threshold

Template Name: Variable Name: Select Severity: Critical

Select Instances

<<Search Input>> All Search Results

TrendWatch Conditions

Group By: None Aggregate: None Condition: None Value: 1.0 % relatively

Trend

Occurred atleast 5 Times

Last 1 Days

From 09 May 2009 at 18:30

To 10 May 2009 at 18:30

Show Rule

4. Возможность установки граничных значений

TrendWatch Conditions

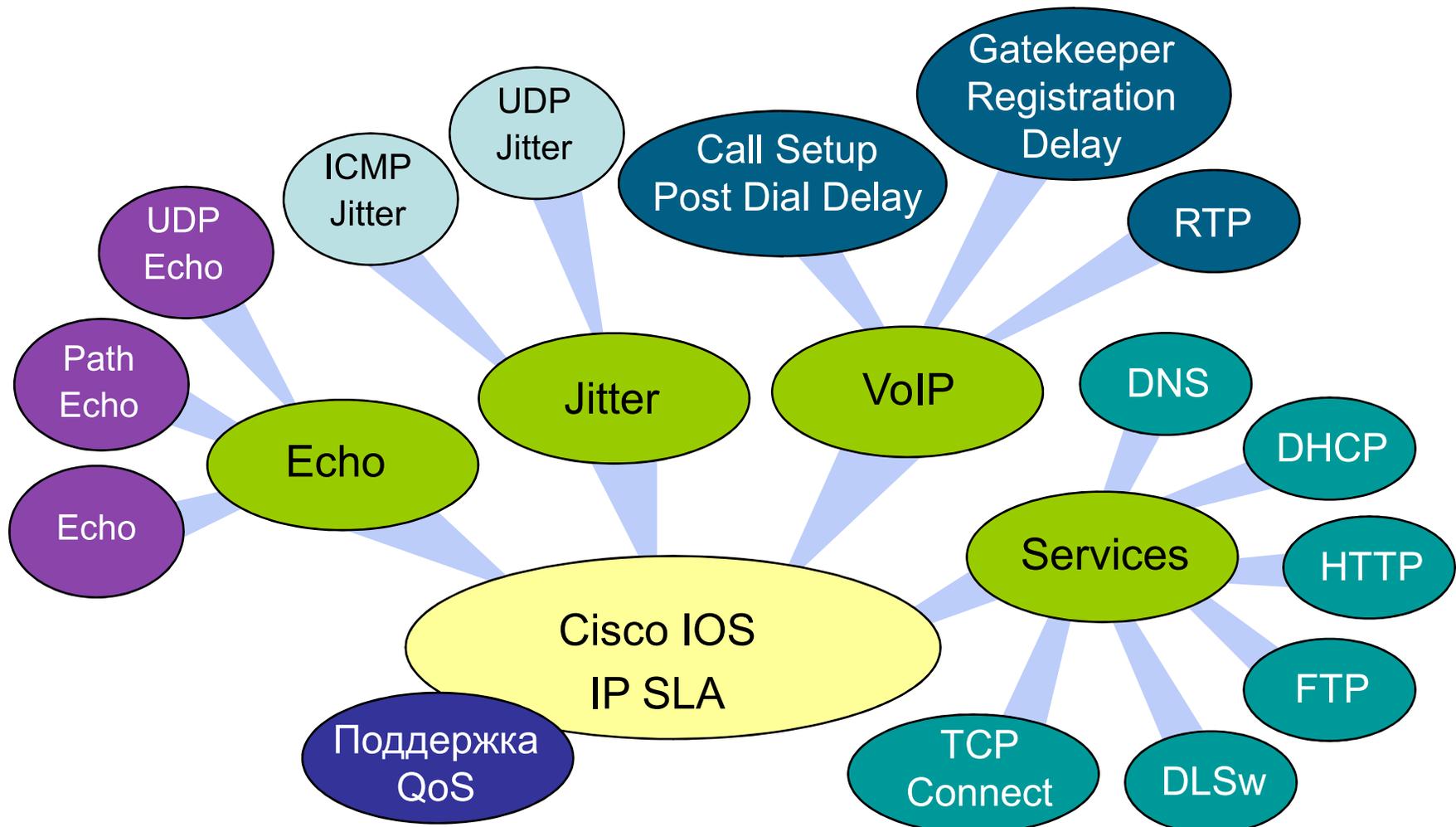
Group By: Hourly Aggregate: Avg Condition: >= Value: 1 % % relatively

Trend

Occurred atleast 5 %age of Times

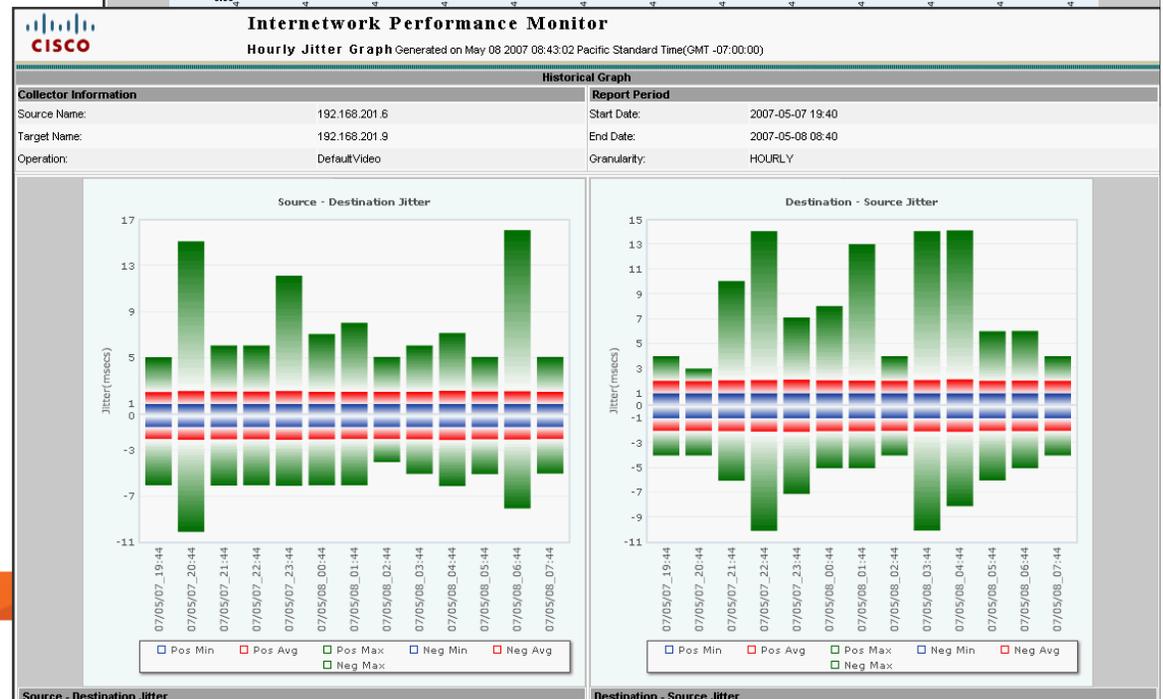
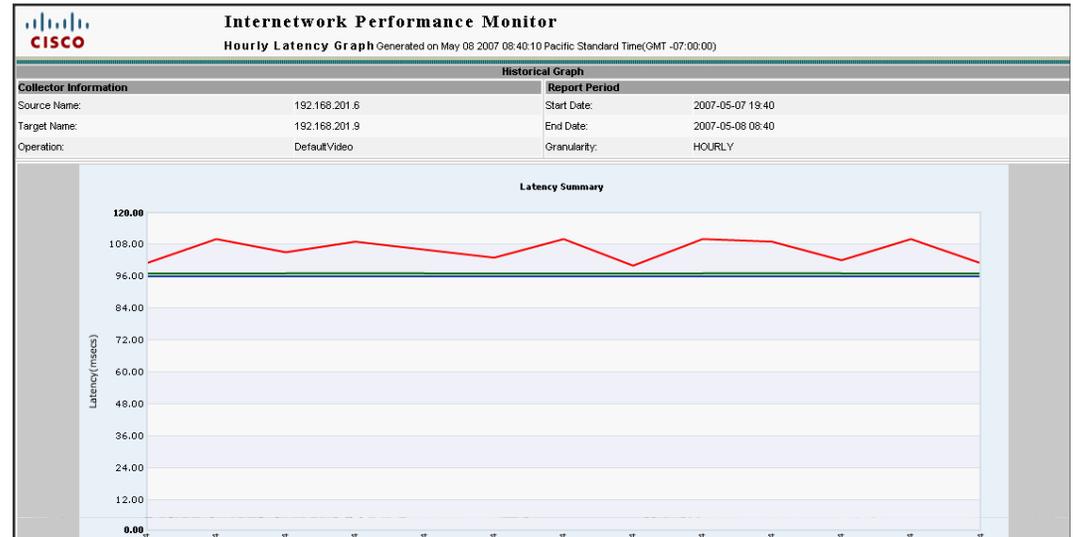
Last 1 Days

Prime LMS – Поддерживаемые тесты IP SLA



Prime LMS: Настройка IP SLA

- Создание теста.
Настройка основных параметров и типа.
- Настройка специфических параметров теста
- Настройка коллектора – выбор источника и приемника
- Настройка расписания
- Просмотр статистики



Технологии измерения производительности



Cisco NAM для контроля производительности

Контроль производительности приложений

- Мониторинг времени отклика приложений
- Анализ результатов оптимизации WAN
- Анализ качества голосового трафика

Анализ трафика

- Анализ трафика по приложениям, устройствам, DSCP/QoS, VLAN, VRF
- Анализ сети с наличием VM

Диагностика

- Захват пакетов, декодирование, фильтрация и поиск ошибок
- Статистика по портам и интерфейсам

Cisco Nexus 1010 Appliance



Cisco Nexus 70xx series

Cisco Catalyst 65xx



Cisco 76xx



Cisco ISR / ISR G2



Cisco 7609



Cisco WAAS Appliances



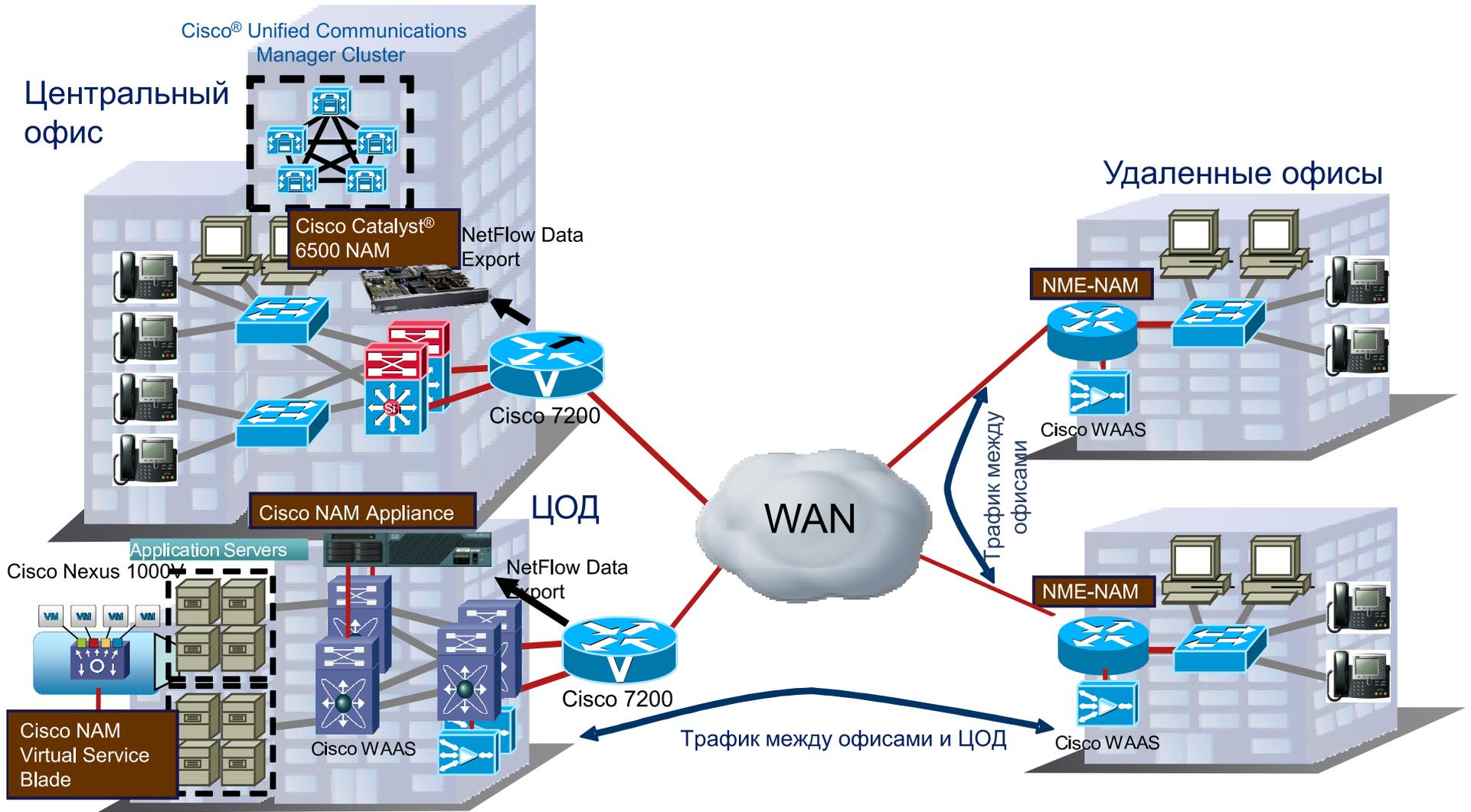
Cisco Catalyst 4K

Гибкость в выборе платформы



Оперативный сбор, агрегация данных и отчетность по производительности сети и услуг

Возможные точки контроля для Cisco NAM



Централизованные системы отчетности

Партнеры: Compuware, NetQoS, InfoVista, другие

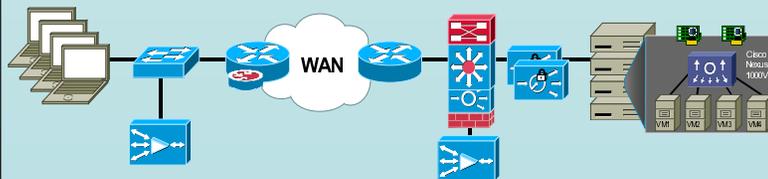


Data Roll-Up



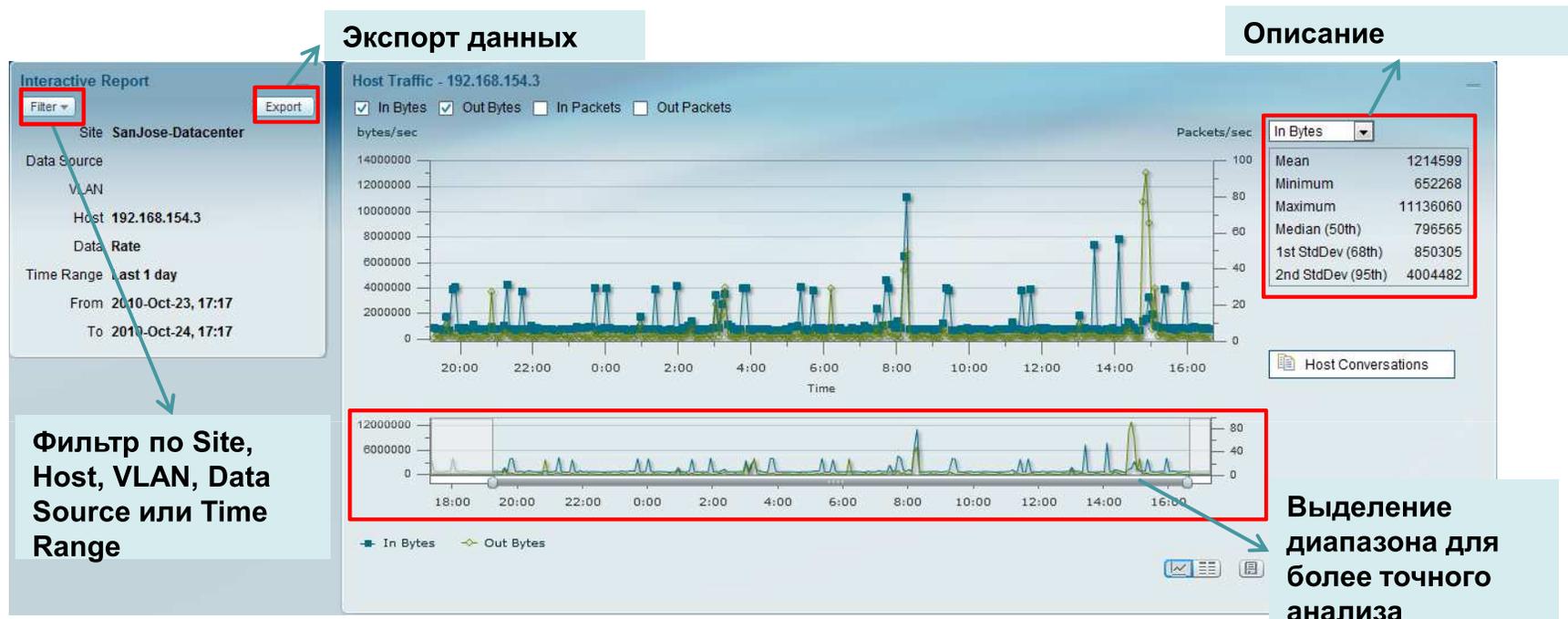
Data Drill-down

NAM Form-Factors



- Консолидация данных для контроля производительности сети
- Возможность получения детальных отчетов с NAM до уровня содержимого пакетов
- Диагностика

Интерактивная отчетность: Быстрый доступ к важной информации



- Уменьшение времени идентификации и решения проблемы:
 - Выделение требуемого диапазона (zoom) и получение детализации
 - Гибкие фильтры
 - Визуальная корреляция данных
- Идентификация повторяющихся проблем и сохранение фильтров
- Экспорт данных для более детального анализа другими инструментами

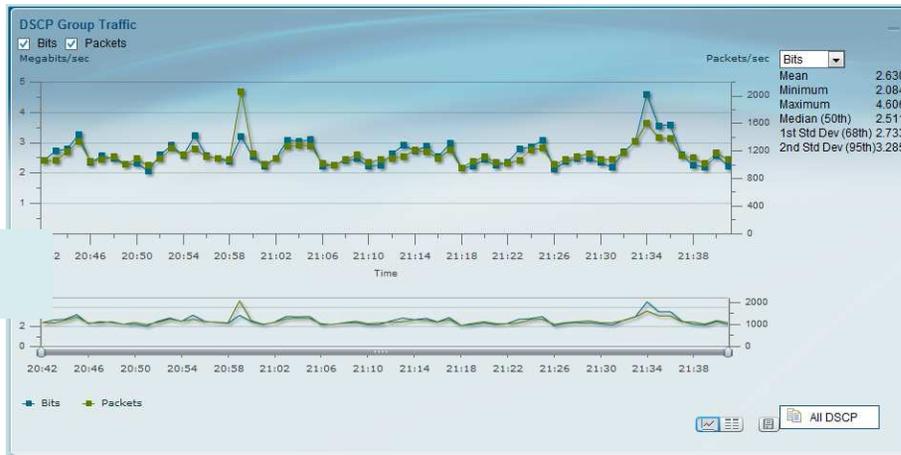
Анализ трафика в реальном режиме времени



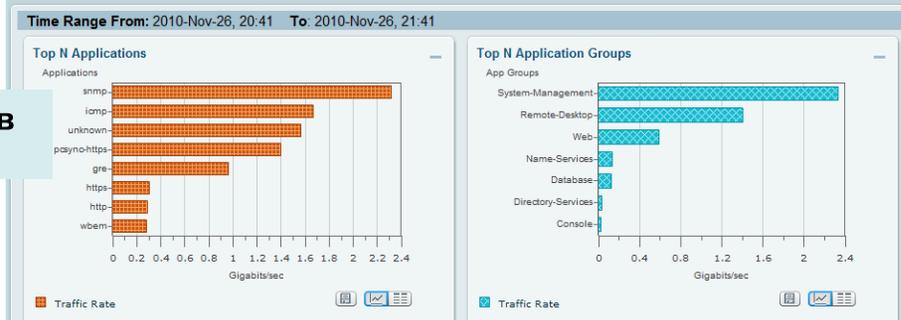
- Идентификация типов приложений, используемых в сети, кто из использует и сколько трафика они генерируют
- Идентификация удаленных узлов/офисов, VLAN и классов QoS с наибольшим количеством трафика
- Превентивный поиск узких мест в сети перед тем, как начнутся проблемы с производительностью
- Возможность зафиксировать поведение сети до и после изменений, например, изменения в ЦОД, оптимизация WAN, миграция виртуальных машин и внедрение VoIP

Анализ DiffServ

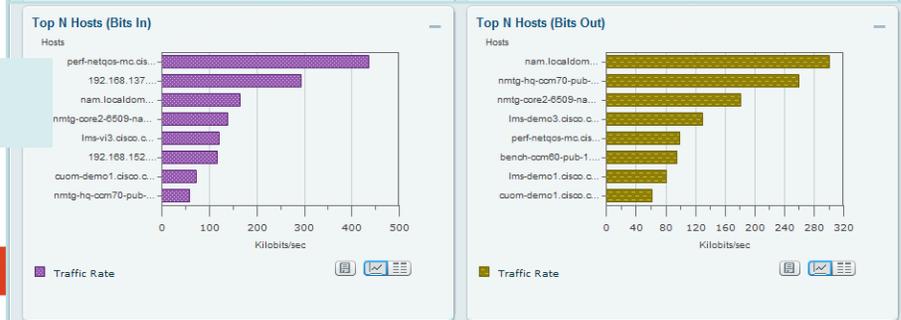
Трафик с DSCP0



Приложения в группе DSCP



Устройства в группе DSCP



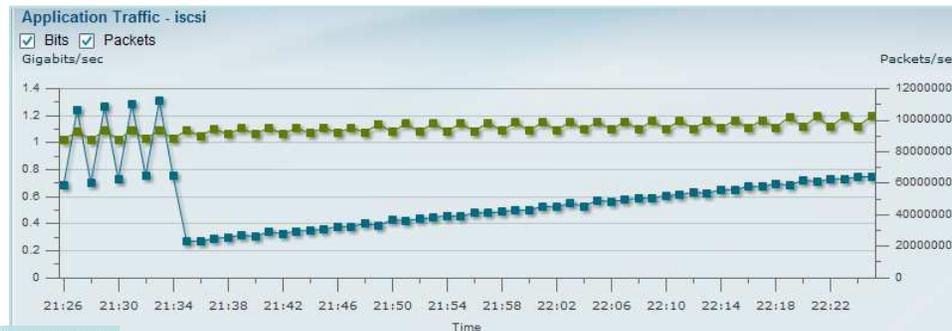
Функция:

- Визуализация трафика по узлам и приложениям для каждого DSCP
- Агрегация трафика по каждому DSCP

Возможности:

- Проверка правильности планирования и внедрения QoS
- Определение неучтенного трафика, или трафика с неправильным DSCP

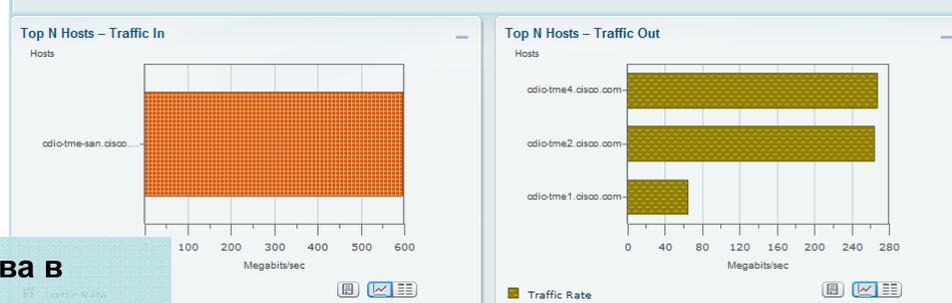
Анализ трафика VLAN



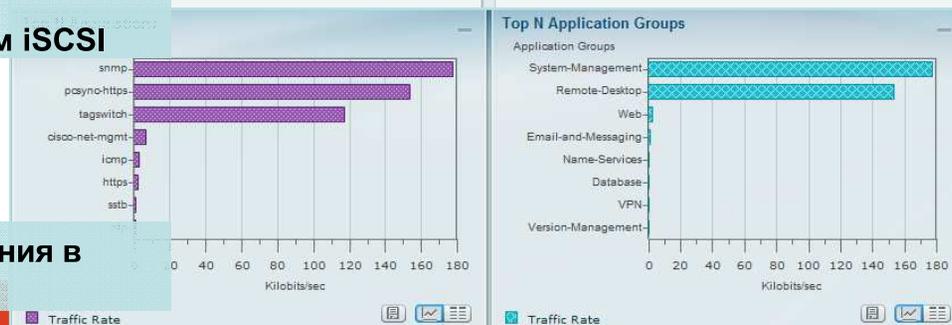
Трафик iSCSI в VLAN 0



Устройства в VLAN 0 с трафиком iSCSI



Приложения в VLAN 0



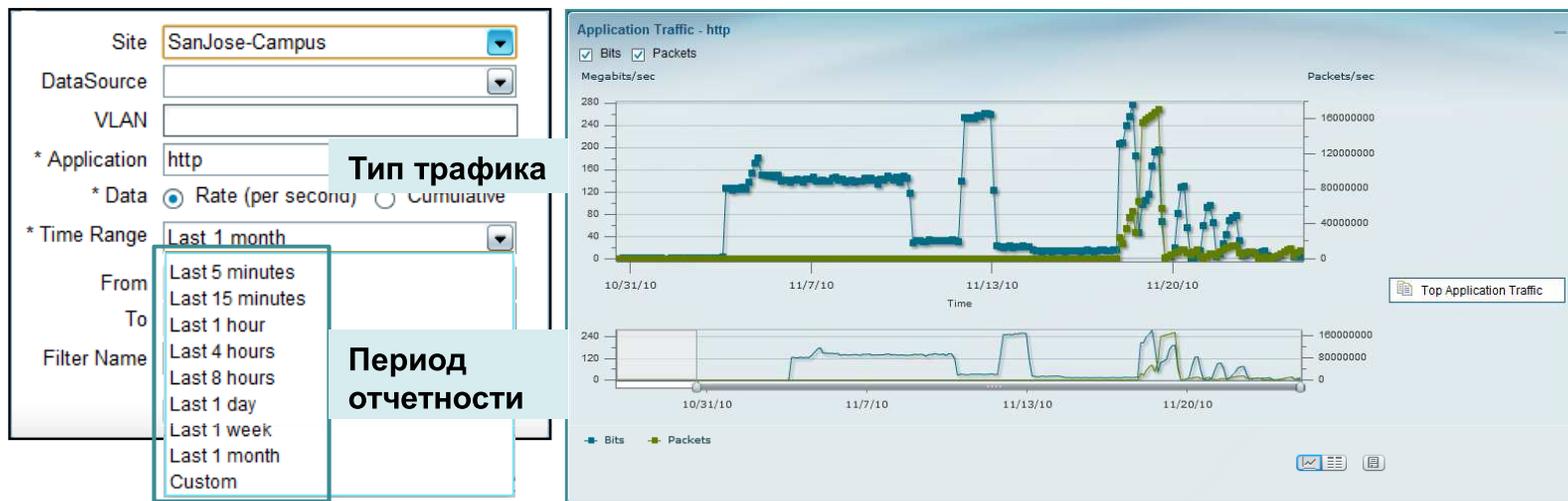
Функции:

- Просмотр всех VLAN по количеству трафика
- Анализ трафика VLAN :
 - Приложения
 - Узлы
 - Потoki
 - Качество голоса
 - Время отклика приложений

Возможности:

- Мониторинг трафика в каждом контролируемом VLAN
- Поиск некорректных назначений виртуальных машин (интерфейсов) и VLAN

Анализ исторических данных



Функция:

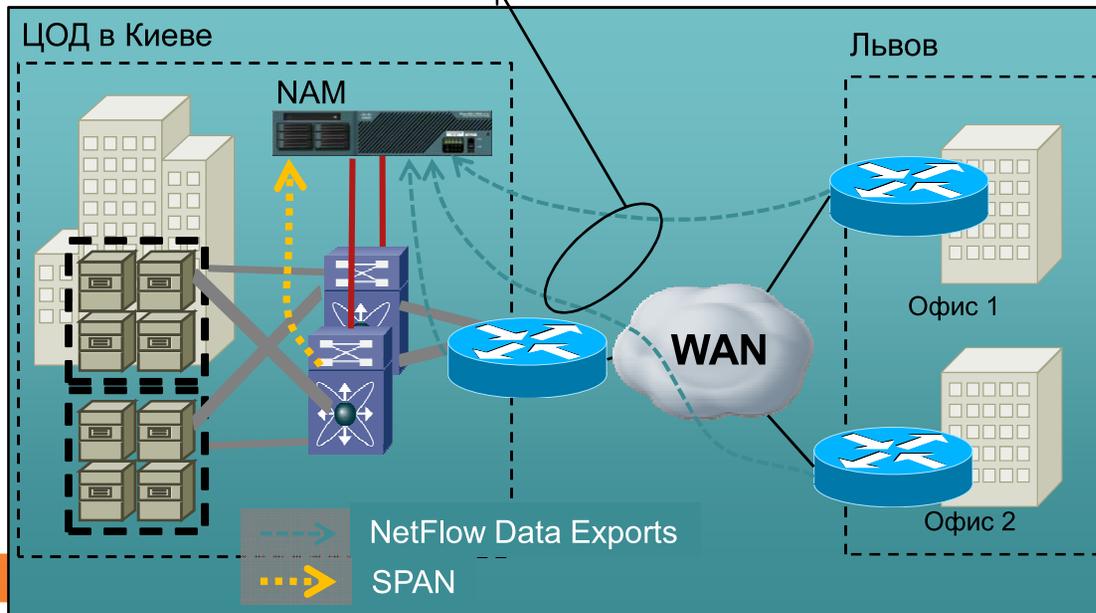
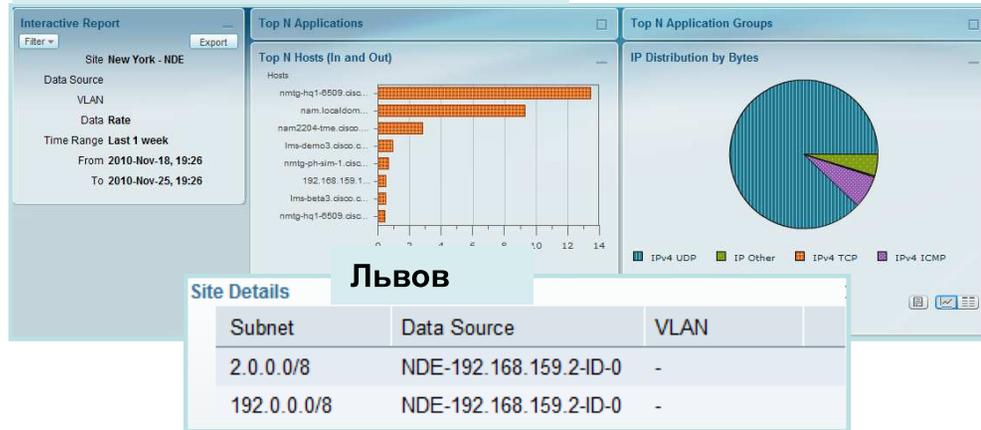
- Хранение всех данных до 72 часов с гранулярностью 1-5 мин и более длительный период с большей гранулярностью (1-2 часа)
- Интуитивно понятный интерфейс для дальнейшего анализа данных

Возможности:

- Анализ тенденций для диагностики проблем с производительностью
- Уменьшение времени поиска проблемы с доступом к детальным данным за последние 72 часа
- Надежный источник данных для принятия решений по оптимизации сети или настройке приложений.

Мониторинг удаленных офисов

Общая статистика по трафику



Функции:

- Создание офиса (Site) как группы узлов по IP адресу или сети, источника данных или VLAN
- Группировка данных по офису в одном окне (тип трафика, качество голоса, время отклика приложений, оптимизация WAN)

Возможности:

- Гибкая отчетность с группировкой данных по офисам, подразделениям
- Превентивное извещение о проблеме по граничным значениям для каждого офиса

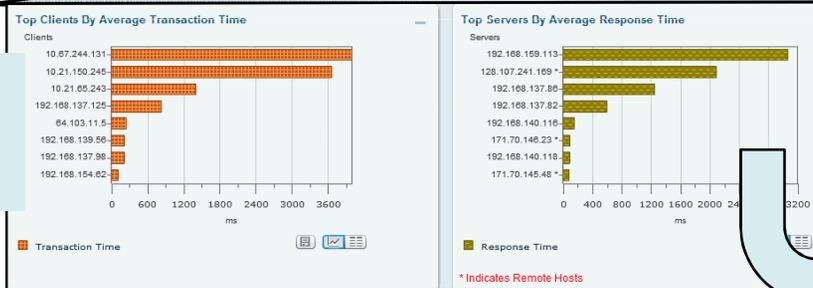
Пример сценария анализа проблемы: Анализ времени транзакции



1. Анализ производительности приложения за период времени

2. Получение детализации за интересующий период

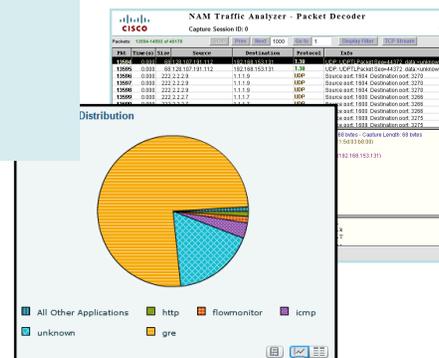
3. Идентификация наиболее пострадавших клиентов



4. Получение перечня серверов с большим временем выполнения транзакции

Возможности:

- Уменьшение времени поиска проблемы – все данные доступны в одном окне
- Анализ тенденций



5. Анализ всех приложений на сервере

Сканирование ошибок пакетов: Детальный анализ проблем

NAM Traffic Analyzer - Packet Decoder
Capture Session ID: 0

Packets: 13594-14593 of 40178

Pkt	Time (s)	Size	Source	Destination	Protocol	Info
13594	0.000	68	128.107.191.112	192.168.153.131	T.38	UDP: UDPTLPacket Seq=44372 data=<unknown>
13595	0.000	68	128.107.191.112	192.168.153.131	T.38	UDP: UDPTLPacket Seq=44372 data=<unknown>
13596	0.000	222	2.2.2.9	1.1.1.9	UDP	Source port: 1604 Destination port: 3270
13597	0.000	222	2.2.2.9	1.1.1.9	UDP	Source port: 1604 Destination port: 3270
13598	0.000	222	2.2.2.9	1.1.1.9	UDP	Source port: 1604 Destination port: 3270
13599	0.000	222	2.2.2.7	1.1.1.7	UDP	Source port: 1600 Destination port: 3266
13600	0.000	222	2.2.2.7	1.1.1.7	UDP	Source port: 1600 Destination port: 3266
13601	0.000	222	2.2.2.7	1.1.1.7	UDP	Source port: 1600 Destination port: 3266
13602	0.000	222	2.2.2.20	1.1.1.20	UDP	Source port: 1609 Destination port: 3275
13603	0.000	222	2.2.2.20	1.1.1.20	UDP	Source port: 1609 Destination port: 3275

Packet Number: 13594 - Arrival Time: Oct 20, 2010 11:48:26.000391000 - Frame Length: 68 bytes - Capture Length: 68 bytes

- + **ETH** Ethernet II, Src: 00:18:73:b5:7a:3f (00:18:73:b5:7a:3f), Dst: 00:11:5d:03:b8:00 (00:11:5d:03:b8:00)
- + **VLAN** 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 32
- + **IP** Internet Protocol, Src: 128.107.191.112 (128.107.191.112), Dst: 192.168.153.131 (192.168.153.131)
- + **UDP** User Datagram Protocol, Src Port: 5654 (5654), Dst Port: 6004 (6004)
- + **T38** ITU-T Recommendation T.38
- + **MALFOR** [Malformed Packet: T.38]
- **EXPERT** [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
- EXPERT [Message: Malformed Packet (Exception occurred)]
- EXPERT [Severity level: Error]
- EXPERT [Group: Malformed]

0000 00 11 5d 03 b8 00 00 18 73 b5 7a 3f 81 00 00 20 ..l.....s.z?..
0010 08 00 45 00 00 24 70 d2 00 00 77 11 38 ef 80 6b ..E..&p...w..8..k
0020 bf 70 c0 a8 99 83 16 16 17 74 00 10 06 c6 ad 54 ..p.....t.....T
0030 9b 82 75 6c 73 32 00 00 00 00 00 00 00 00 00 ..uls2.....

Capture Errors and Warnings information

Packet Id	Protocol	Severity	Description
71938	eth.vlan.ip:udp:t38	Error	Malformed Malformed Packet (Exception occurred)
72263	eth.vlan.ip:udp:t38	Error	Malformed Malformed Packet (Exception occurred)
7528	eth.vlan.ip:tcp:ssl	Warn	Reassemble Unreassembled Packet (Exception occurred)
7529	eth.vlan.ip:tcp:ssl	Warn	Reassemble Unreassembled Packet (Exception occurred)
7530	eth.vlan.ip:tcp:ssl	Warn	Reassemble Unreassembled Packet (Exception occurred)
7531	eth.vlan.ip:tcp:ssl	Warn	Reassemble Unreassembled Packet (Exception occurred)
7535	eth.vlan.ip:tcp:ssl	Warn	Reassemble Unreassembled Packet (Exception occurred)
7536	eth.vlan.ip:tcp:ssl	Warn	Reassemble Unreassembled Packet (Exception occurred)

Функции:

- Анализ пакета и подсветка аномальных пакетов
- Получение детализации по пакетам одним щелчком мыши

Возможности:

- Повышение эффективности работы службы эксплуатации – возможность записи трафика по событию
- Подсветка ошибок позволяет сэкономить время на анализе данных

Анализ времени отклика приложения

Аналитика для анализа ТСР- приложений

- Детальная статистика по сессиям и транзакциям – более 45 параметров

- Data-transfer time
- Transaction time
- Connection duration
- Number of bytes and packets retransmitted
- Retransmission delay
- Acknowledgement delay
- Number of open connections
- Number of closed connections
- Number of refused connections
- Number of unresponsive connections
- And more...

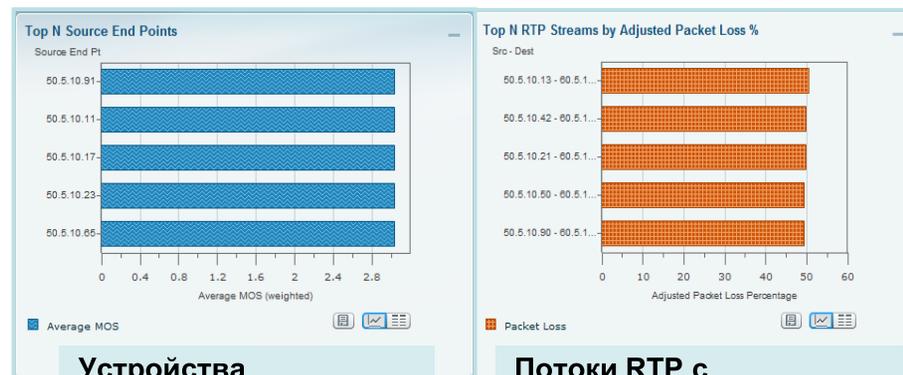


Мощное средство для мониторинга приложений

Анализ качества голосового трафика

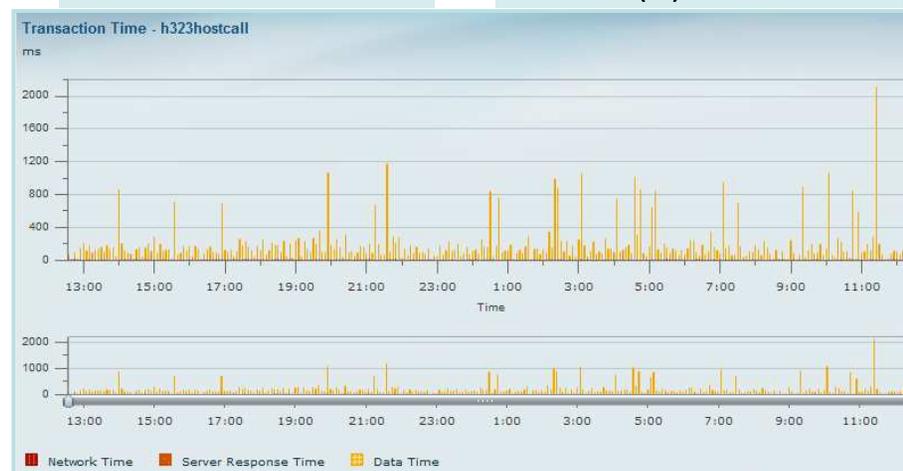
Мониторинг и диагностика в реальном режиме времени

- Мониторинг MOS (базируется на рекомендациях ITU-T G.107)
- Анализ потоков RTP в реальном режиме времени
- Быстрый поиск проблемных направлений
- Диагностика проблем с производительностью с использованием статистики по интерфейсам, DSCP, детальный анализ пакетов
- Время отклика для сигнальных протоколов на базе TCP, например SCCP, SIP



Устройства (телефоны) с низким MOS

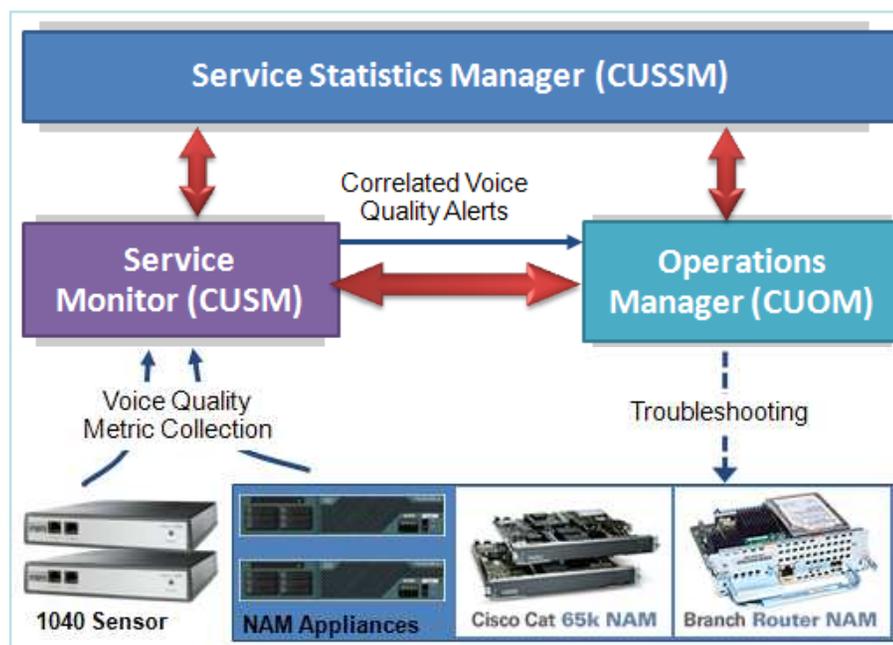
Потоки RTP с наибольшей потерей пакетов (%)



Время транзакции H.323 - последние 24 часа

Централизованная отчетность по качеству голосового трафика

- В реальном режиме времени по всей сети
- Превентивные извещения по проблемам с качеством голосовых услуг
- Детальная информация с NAM для диагностики
- Масштабируемые и гибкое решение – возможность снять статистику в любой точке сети



Cisco NAM дополняет CUCMS для получение комплексного решения по мониторингу услуг передачи голоса

Контроль виртуальных машин

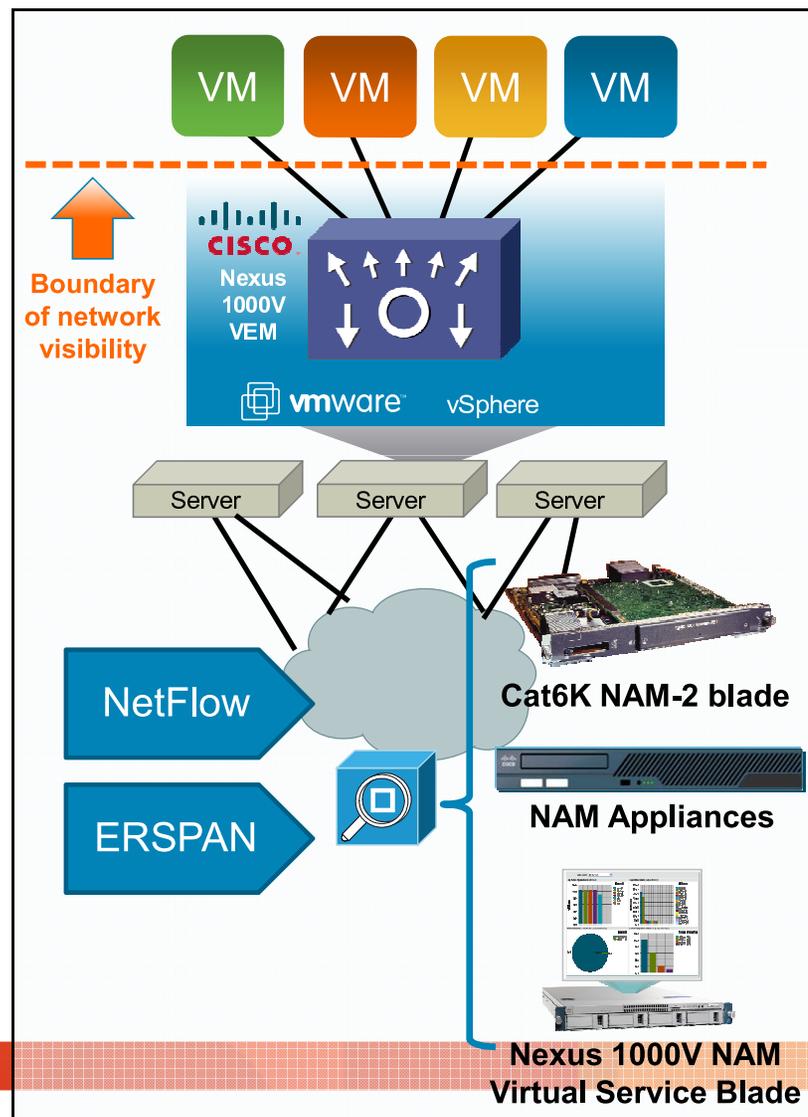
Интеграция NAM и коммутатора Nexus 1000V

Функции:

- Детальный анализ трафика по виртуальной машине, VLAN, DSCP, приложению, и т.д.
- Статистика как по физическим, так и виртуальным серверам
- Мониторинг виртуальных интерфейсов
- Мониторинг виртуальной машины во время миграции с VMotion

Возможности:

- Гибкие возможности по визуализации трафика с виртуальных машин
- Учет проблем с производительностью из-за миграции или изменений конфигурации.



Дополнительная информация

- Информация по технологиям
 - Netflow: <http://www.cisco.com/go/netflow>
 - IP SLA: <http://www.cisco.com/go/ipsla>
 - NBAR: <http://www.cisco.com/go/nbar>
- Prime LMS
 - Документация на сайте Cisco <http://www.cisco.com/go/nam>
- Prime NAM
 - Документация на сайте Cisco <http://www.cisco.com/go/nam>



Cisco Expo 2011



Спасибо!

Просим Вас оценить эту лекцию.
Ваше мнение очень важно для нас.

Онлайн-анкеты: www.ceq.com.ua

innovate *together*