

Сетевое оборудование ProCurve Networking by HP: безопасность и управление

Сергей Перроте

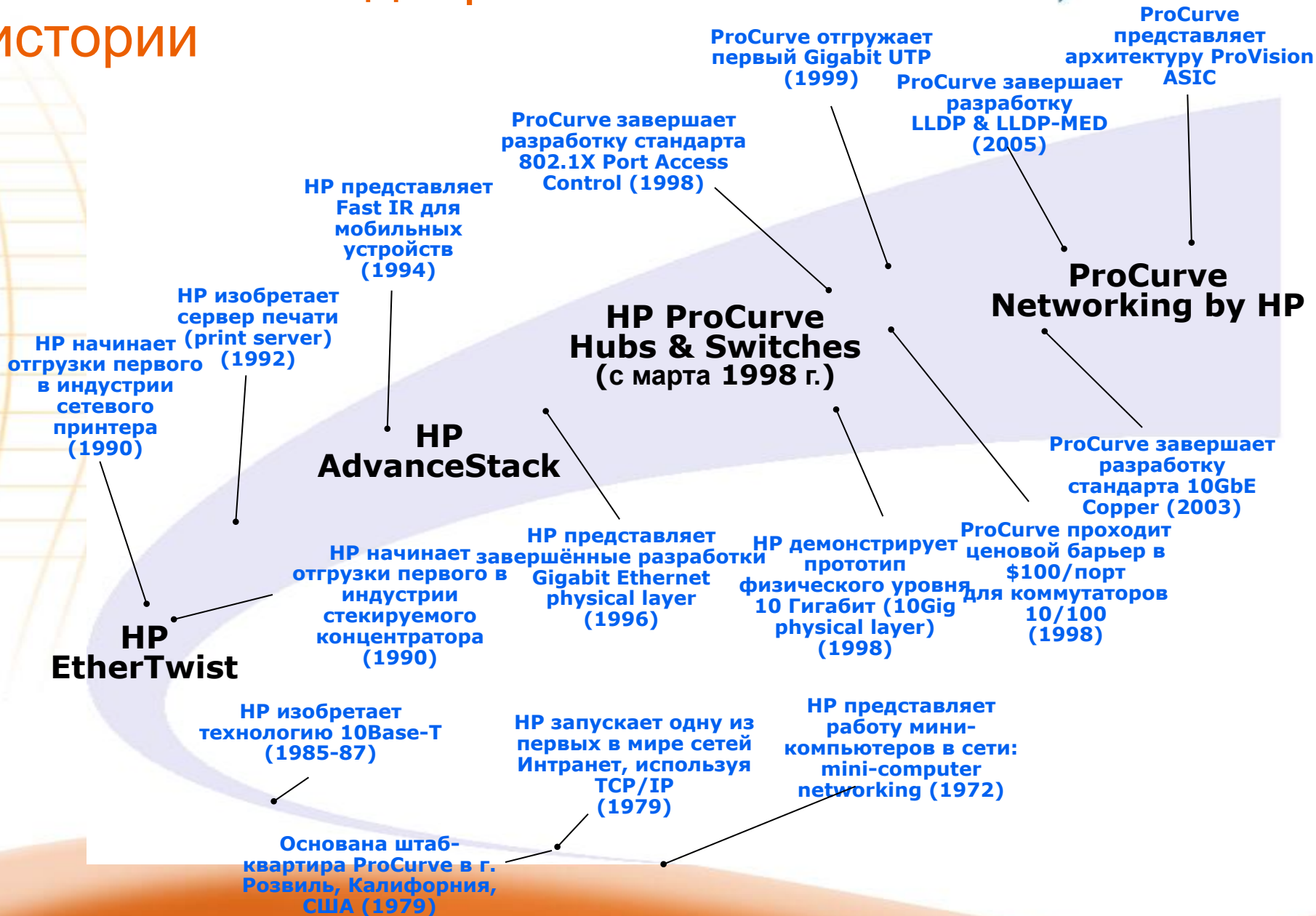
Менеджер по работе со стратегическими клиентами

Sergei.perrote@hp.com

+7 916 993 3480 ; +7 495 797 3576

ProCurve Networking by HP, Россия

Большой вклад в развитие сетевой истории

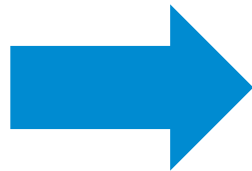


Предоставляем выбор через Стандарты

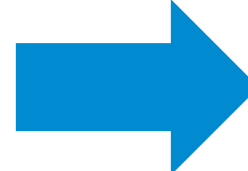
	ProCurve (открытые)	Патентованные
Маршрутизация	RIP/OSPF	EIGRP
Коммутация	802.1s	PVST+
VLANs	802.1Q	ISL
Агрегирование портов	802.3ad (LACP)	FEC
Обнаружение устройств	802.1AB (LLDP) LLDP-MED	CDP PDA - Phone Discovery Algorithm
Питание через Ethernet	802.3af	Cisco PoE
Роуминг	802.11(fast roaming)	WLCPP
Безопасность	802.1X	LEAP
Целостность клиента (Client Access Integrity)	Trusted Network Connect (TNC/TCG)	Cisco NAC
Беспроводные	802.11i	Cisco Compatible Extensions (CCX)

Знакомая эволюция ...

Mainframe Computing



Client/Server Computing

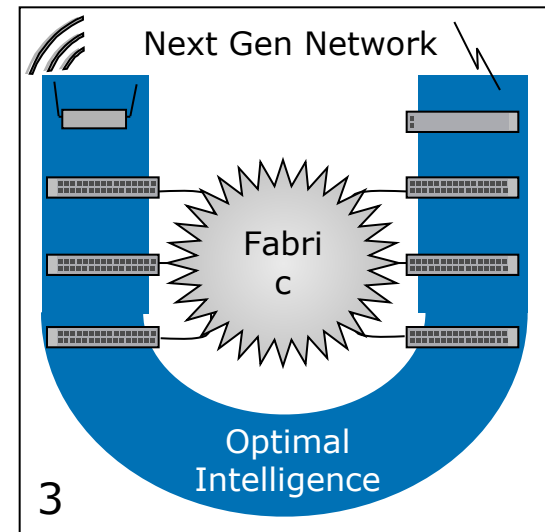
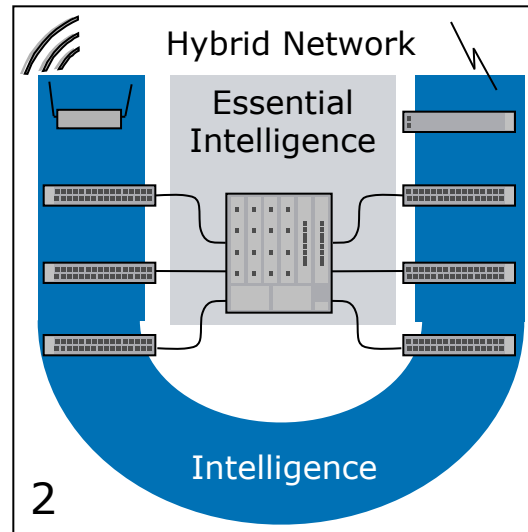
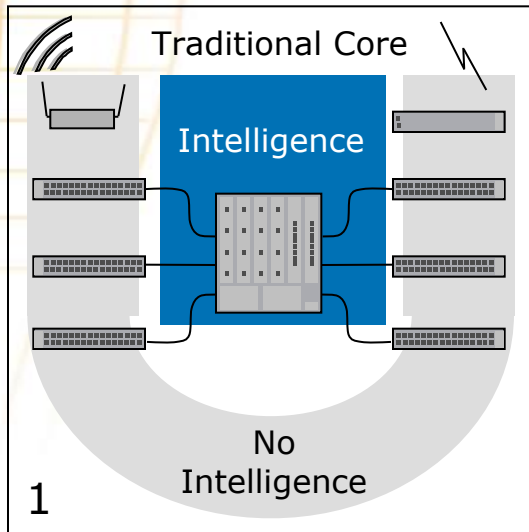


Distributed Computing

Centraled



Distributed



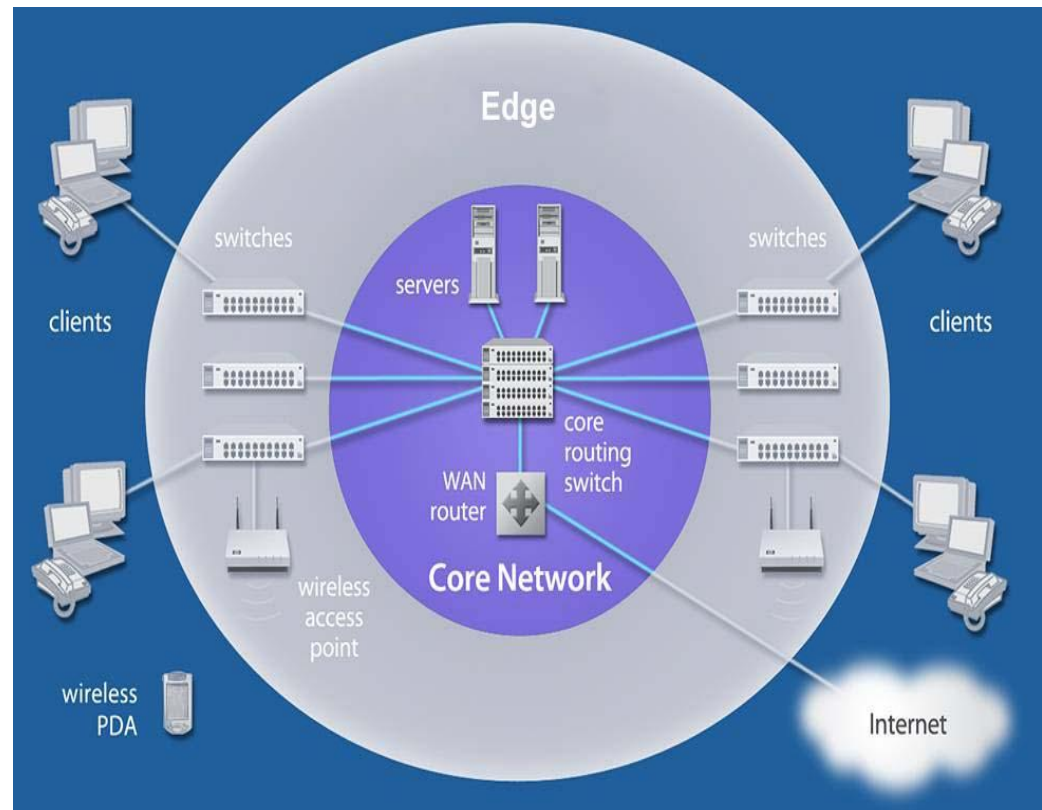
Smart Provisioning - ProCurve Adaptive EDGE Architecture

Сети сосредоточенные на ядре

Каждый коммутатор добавленный на границе увеличивает нагрузку «принятием решений» на ядре – **вынужденное наращивание мощности**

Цена/производительность для коммутаторов ядра не линейная – **дорогая и неизбежная модернизация**

Многие решаемые задачи НЕ МОГУТ перепоручаться ядру – **не отвечает требованиям критичным ко времени приложений**

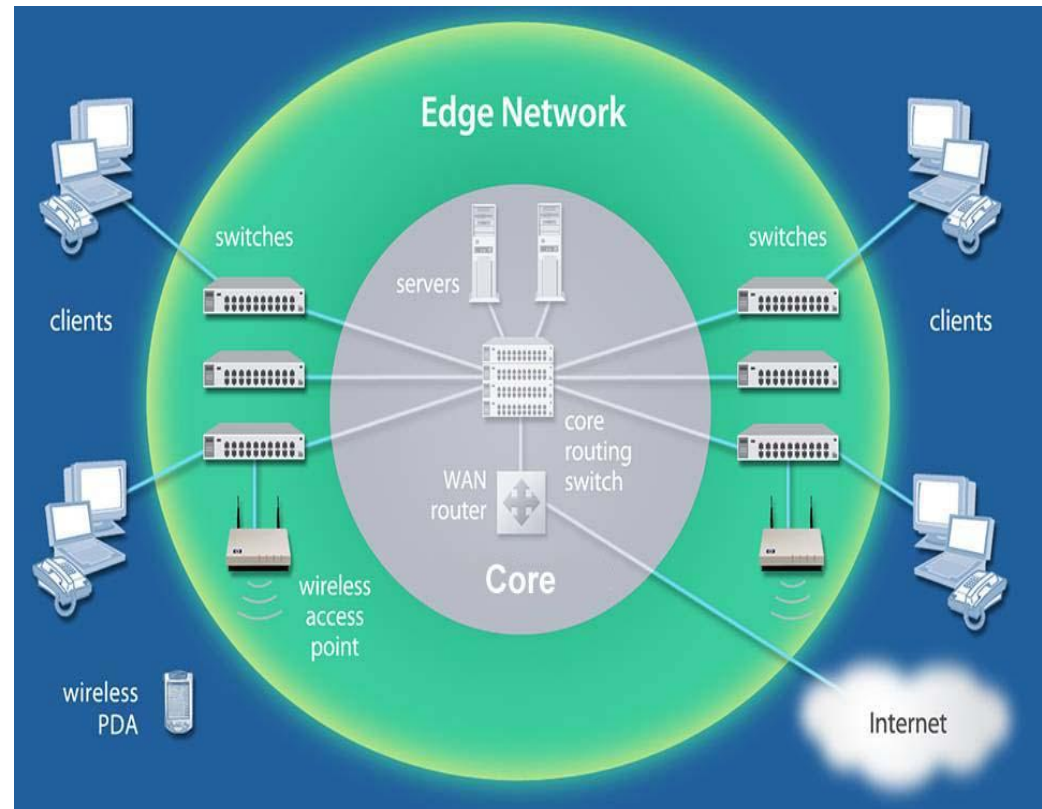


Adaptive EDGE сети

Каждый EDGE-коммутатор добавляет частицу "принятия решений" – **линейное масштабирование и соответствие критичным ко времени приложениям**

EDGE-коммутаторы границы сети основаны на стандартизованных компонентах – **недорогое расширение**

Коммутаторы ядра становятся проще (layer 2) и отвечают только за гарантию полосы пропускания и управление – **снижение цены и сложности**



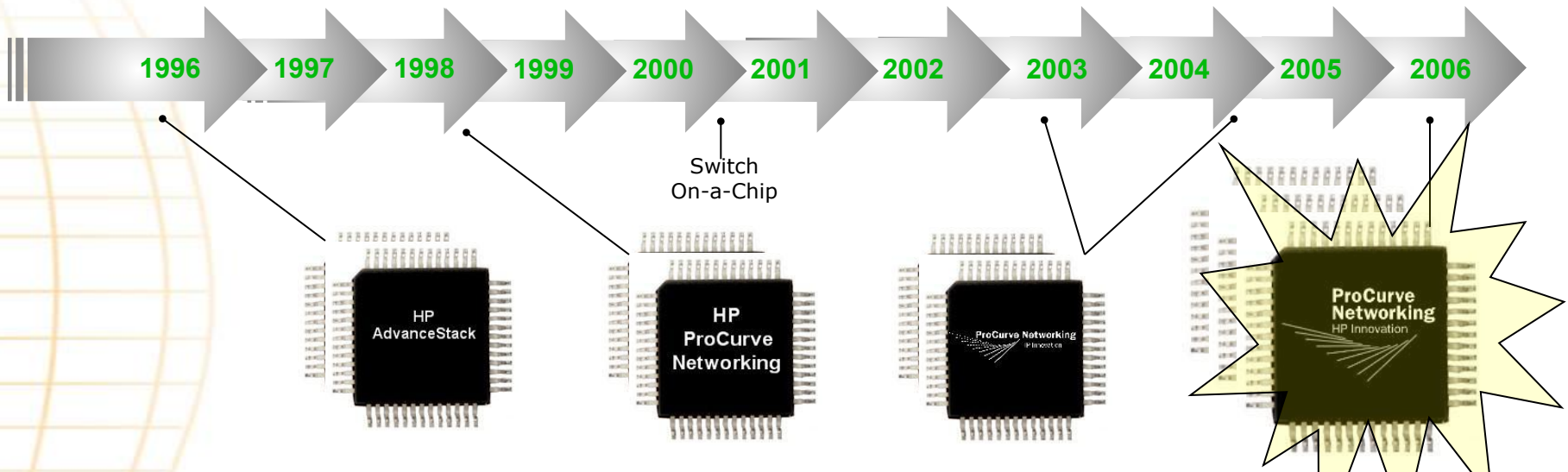
Создаём «умную» границу сети сегодня Да, но какой ценой?

- В своих решениях, конкуренты пытаются перепаковать коммутаторы для Ядра сети и поместить их в серверную комнату или этажный коммуникационный шкаф
- Сегодня конкуренты пытаются продавать коммутаторы для Ядра сети как граничные коммутаторы, чтобы удовлетворить потребность в интеллектуальных коммутаторах на границе
- Потребителям требуется экономичное по цене решение для построения интеллектуальной и управляемой границы сети!

Только HP ProCurve Networking разработал интеллектуальное решение для границы сети «с нуля», и корпоративные клиенты могут его позволить себе сегодня!

The ProVision ASIC

The Next Step in ProCurve Technology



ASIC Specs	1st	2 th	3 th	4 th
Product Family	2000	4000	5300	5400/3500
Process	0.5 μ	0.35 μ	0.25 μ	0.13 μ
Die Size (mm ²)	88	105	272	273
Gates	0.08 Million	0.4 Million	2.5 Million	6 Million
Data Path	Hard coded L2	Programmable	L3/L4 Flows	ACLs/IPv6/BMP
Throughput	1 Gbps	3.8 Gbps	76.8 Gbps	691 Gbps
Ports	4 10 1 10/100	8 10/100 1 GbE	24 10/100 4 1GbE & 16 1GbE	24 10/100/1000 4 10 GbE

Inside the ProVision ASIC

Gig-ASIC

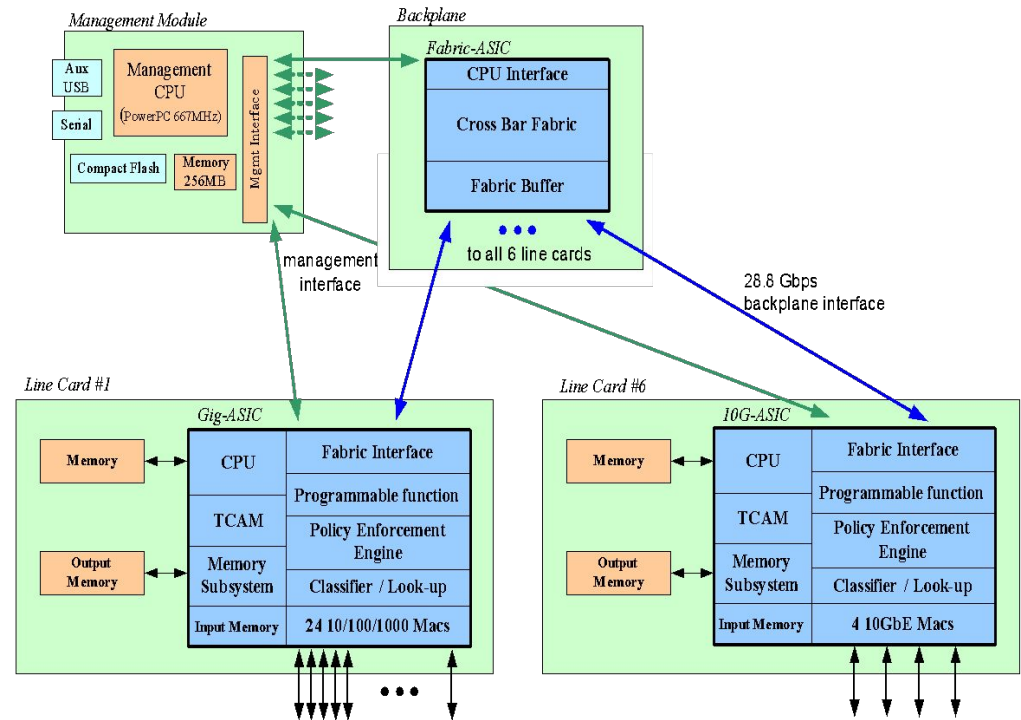
- 24 GbE ports per chip
- 28.8 Gbps Interface to fabric ASIC
- Management CPU interface
- Embedded MACs, classifier, various memory, packet processors

10Gig-ASIC

- 4 10-GbE ports per chip
- 28.8 Gbps Interface to fabric ASIC
- Management CPU interface
- Embedded MACs, classifier, various memory, packet processors

Fabric ASIC

- Multi-stage capable cross-bar switching fabric
- Interface connections to management CPU, Gig-ASIC and 10Gig-ASIC

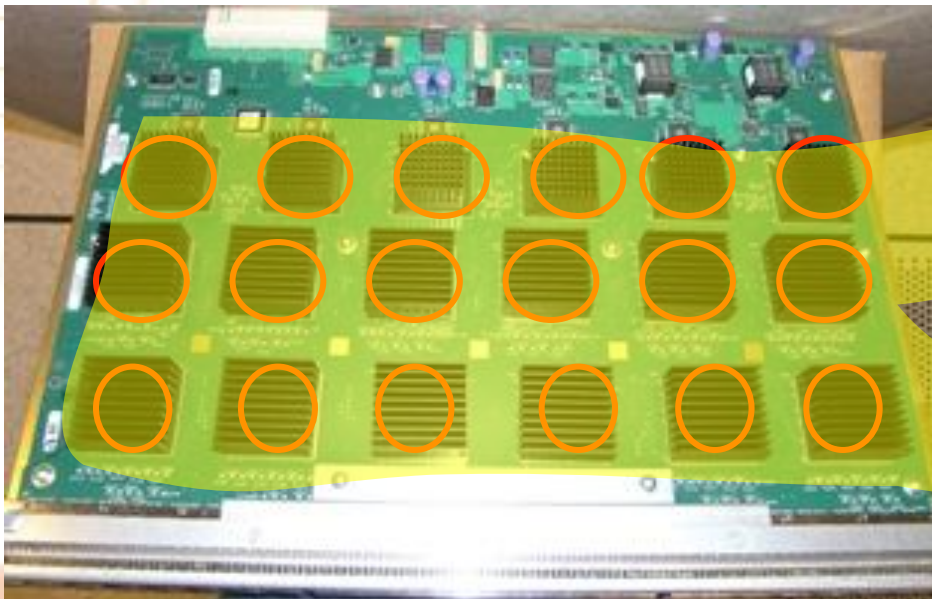


Architecture layout of a ProCurve 5406zl Switch

ProVision ASIC

Cisco 4506 vs ProVision

48 port 10/100/1000



ProCurve Networking



Edge Devices—LAN

Intelligent Edge Switches



ProCurve Switch 5406zl (J8697A)



ProCurve Switch 5406zl-48G (J8699A)



ProCurve Switch 5412zl (J8698A)



ProCurve Switch 5412zl-96G (J8700A)



ProCurve Switch 3500yl-24G-PWR* (J8692A)



ProCurve Switch 3500yl-48G-PWR* (J8693A)



ProCurve Switch 5304xl (J4850A)



ProCurve Switch 5304xl-32G (J8166A)



ProCurve Switch 5348xl (J4849B)



ProCurve Switch 5308xl (J4819A)



ProCurve Switch 5308xl-48G (J8167A)



ProCurve Switch 5372xl (J4848B)



ProCurve Switch 3400cl-24G (J4905A)



ProCurve Switch 3400cl-48G (J4906A)

*Power over Ethernet

Edge Switches—Managed



ProCurve Switch 4202vl-48G (J8771A)



ProCurve Switch 4202vl-72 (J8772A)



ProCurve Switch 4204vl (J8770A)



ProCurve Switch 4208vl (J8773A)



ProCurve Switch 4208vl-64G (J8774A)



ProCurve Switch 4208vl-96 (J8775A)



ProCurve Switch 4104gl (J4887A)



ProCurve Switch 4140gl (J8151A)



ProCurve Switch 4148gl (J4888A)



ProCurve Switch 4108gl (J4865A)



ProCurve Switch 4160gl (J8152A)



ProCurve Switch 4108gl Bundle (J4861A)



ProCurve Switch 2824 (J4903A)



ProCurve Switch 2848 (J4904A)



ProCurve Switch 2810-24G (J9021A)

NEW



ProCurve Switch 2810-48G (J9022A)

NEW



ProCurve Switch 2626 (J4900B)



ProCurve Switch 2626-PWR* (J8164A)



ProCurve Switch 2650 (J4899B)



ProCurve Switch 2650-PWR* (J8165A)



ProCurve Switch 2600-8-PWR* (J8762A)



ProCurve Switch 2510-24 (J9019A)

NEW



ProCurve Switch 2512 (J4812A)



ProCurve Switch 2524 (J4813A)

*Power over Ethernet

Edge Switches—Web Managed

NEW



ProCurve Switch 1800-8G (J9029A)

NEW



ProCurve Switch 1800-24G (J9028A)

ProCurve Networking



Edge Devices—LAN (continued)

Edge Switches—Unmanaged



ProCurve Switch
2708 (J4898A)



ProCurve Switch
2724 (J4897A)



ProCurve Switch
2312 (J4817A)



ProCurve Switch
2324 (J4818A)



ProCurve Switch
2124 (J4868A)



ProCurve Switch
408 (J4097B)

Edge Devices—WAN



ProCurve Secure Router
7102dl (J8752A)



ProCurve Secure Router
7203dl (J8753A)

Inter-connect Switches

Traditional Core Switches



ProCurve Routing
Switch 9408sl
(J8680A)



ProCurve Routing
Switch 9304m
(J4139A)



ProCurve Routing
Switch 9308m
(J4138A)



ProCurve Routing
Switch 9315m
(J4874A)

Interconnect Fabric Switches



ProCurve Routing
Switch 8108fl
(J8727A)



ProCurve Routing
Switch 8116fl
(J8728A)

Aggregators



ProCurve Switch
6400cl (J8433A)



ProCurve Switch
6410cl (J8474A)



ProCurve Switch
6200yl-24G-mGBIC
(J8992A)



ProCurve Switch
6108 (J4902A)

ProCurve Networking



Network Management Software



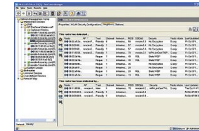
ProCurve Manager 2.1



ProCurve Manager Plus 2.1
(J8778A, J9009A, J8991A,
J8779A)



ProCurve Identity Driven
Manager 2.0 (J9012A,
J9013A, J9014A)



ProCurve Mobility
Manager 1.0
(J8990A)

ProCurve Networking

Edge Devices— Wireless LAN

Wireless Edge Services



ProCurve Wireless Edge Services xl Module (J9001A)



ProCurve Redundant Wireless Services xl Module (J9003A)



ProCurve Radio Port 210 (J9004A)



ProCurve Radio Port 220 (J9005A)



ProCurve Radio Port 230 (J9006A)

Secure Access



ProCurve Access Control Server 745wl (J9038A)



ProCurve Switch xl Access Controller Module (J8162A)

Access Points



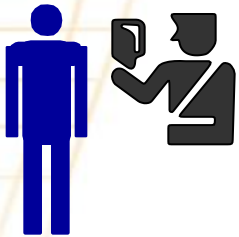
ProCurve Wireless Access Point 530 (J8986A/J8987A)



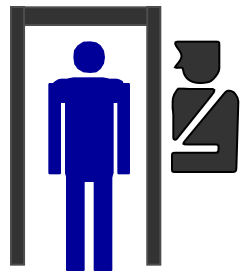
ProCurve Wireless Access Point 420 (J8130A/J8131A)

Аналогия: безопасность при авиаперелётах

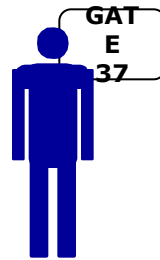
Проверка личности



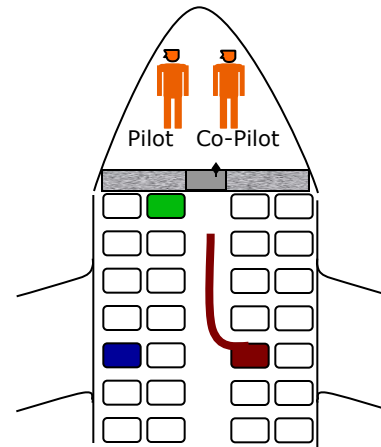
Сканирование на соответствие



Контроль Доступа



Мониторинг поведения

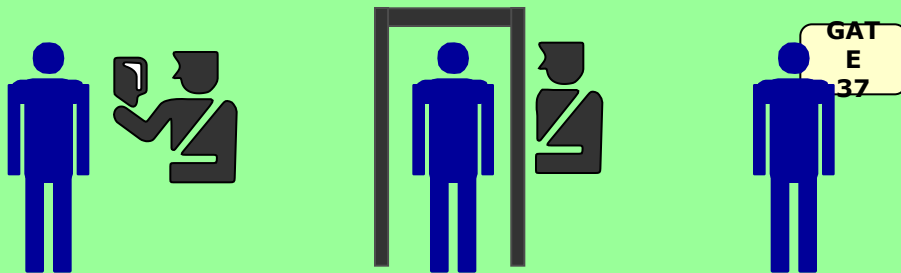


Изолирование подозрительных субъектов



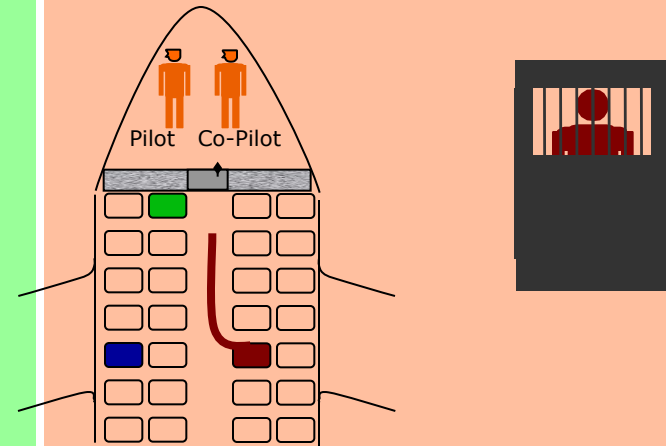
ПроАктивная защита ProCurve для сетевой инфраструктуры

Контроль доступа



- Оценить Личность пользователя
- Оценить целостность клиента
- Динамически применить тэги VLAN, ACL основываясь на политиках
- Enable mitigation

Защита инфраструктуры



- Мониторинг поведения сети
- Автоматически ответить на угрозы основываясь на политиках
- Карантин
- Алерты
- Аномалии
- специфические виды трафика

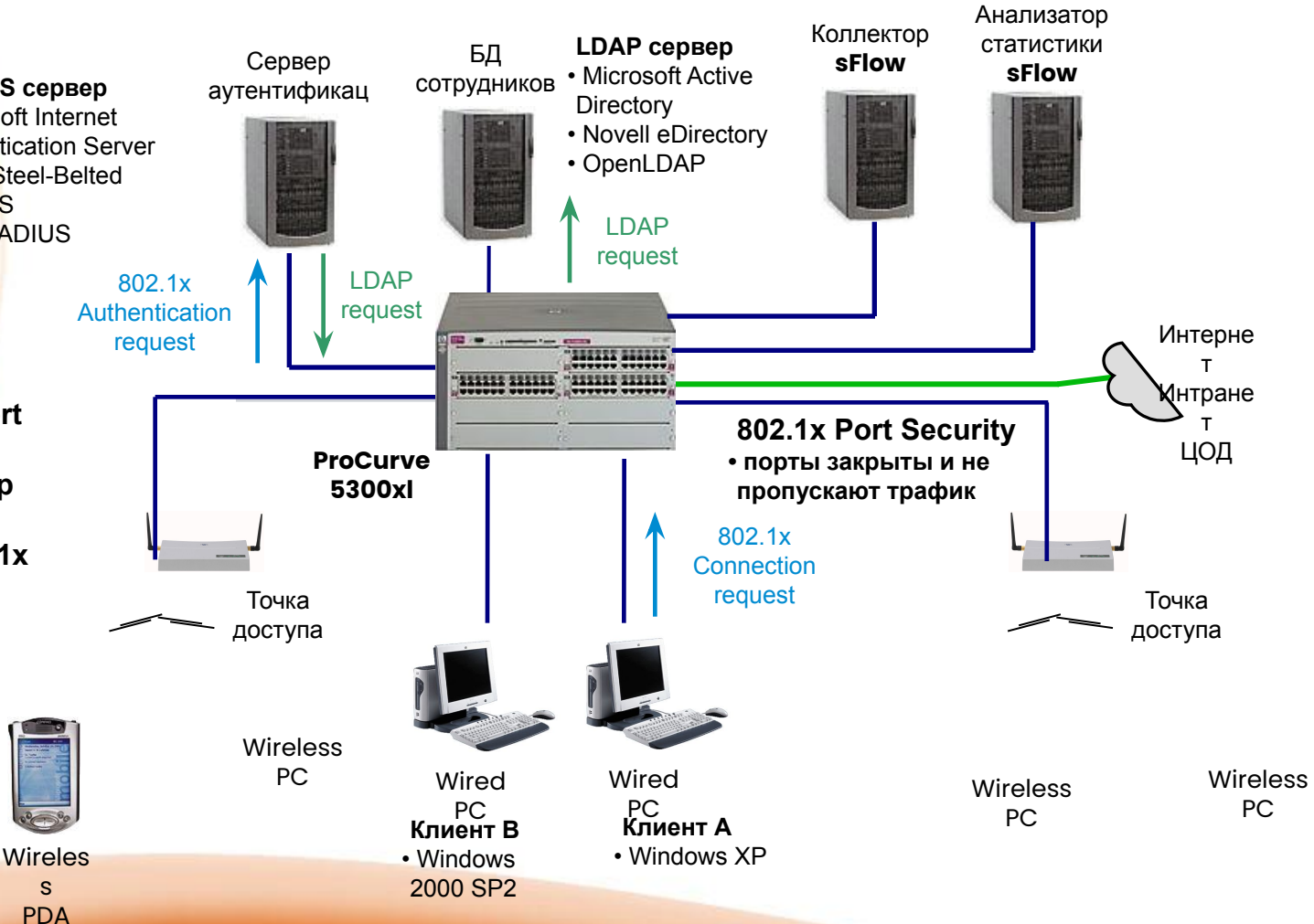
Аутентификация на основе 802.1x для проводных и беспроводных клиентов

RADIUS сервер

- Microsoft Internet Authentication Server
- Funk Steel-Belted RADIUS
- FreeRADIUS

Ключевые технологии:

- IEEE 802.1x Port Security
- RADIUS сервер
- сервер LDAP
- Multi-host 802.1x
- Mac Lockdown



Аутентификация на основе 802.1x для проводных и беспроводных клиентов

RADIUS сервер

- Microsoft Internet Authentication Server
- Funk Steel-Belted RADIUS
- FreeRADIUS

Сервер аутентификац



БД сотрудников



LDAP сервер

- Microsoft Active Directory
- Novell eDirectory
- OpenLDAP

LDAP response

Коллектор sFlow



Анализатор статистики sFlow



Ключевые технологии:

- IEEE 802.1x Port Security
- RADIUS сервер
- сервер LDAP
- Multi-host 802.1x
- Mac Lockdown

802.1x Authentication response (Port Open/Close)

LDAP response

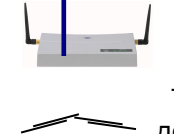
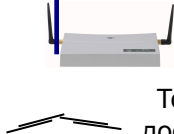
802.1x Port Security
• открывается порт для Клиента А

802.1x Connection response (Port Open/Close)

Интернет
Интранет
ЦОД

ProCurve 5300xl

Точка доступа



Точка доступа

Wireless PC



Wired PC
Клиент В
• Windows 2000 SP2



Wired PC
Клиент А
• Windows XP

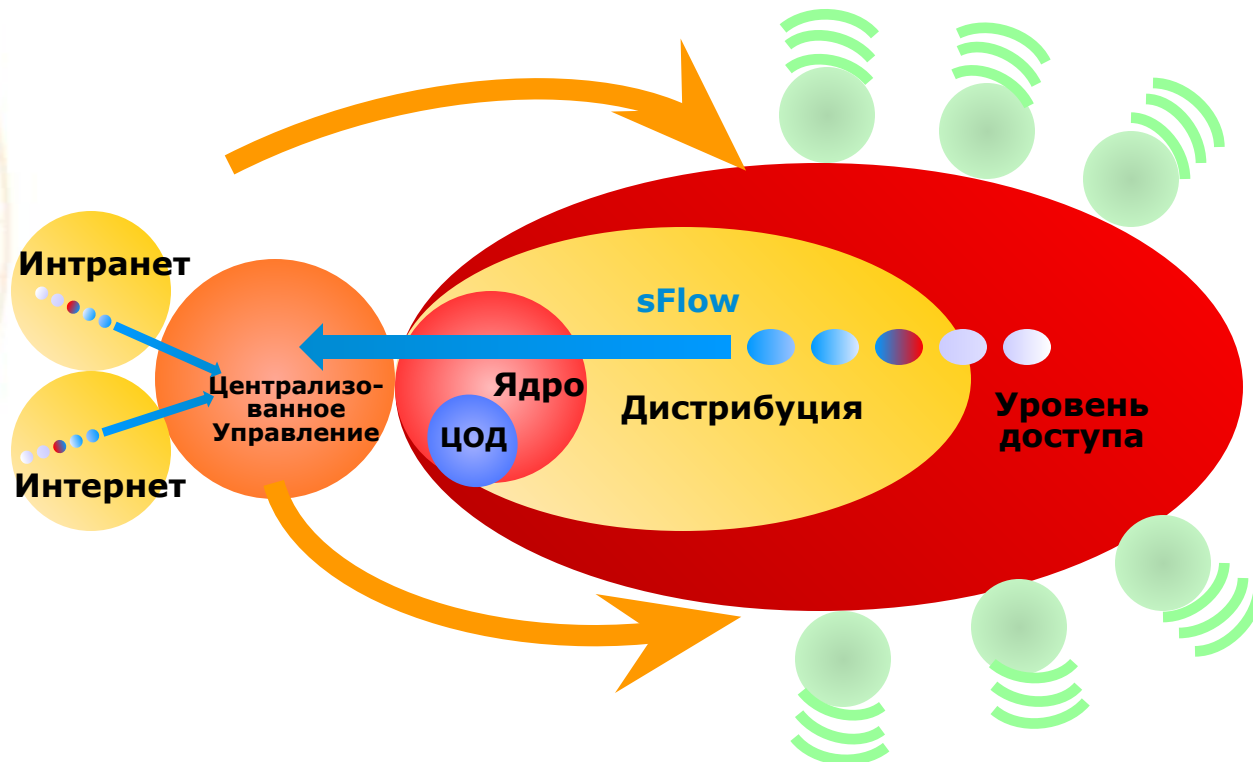
Wireless PC

Wireless PC



Wireless PDA

Промышленный стандарт для мониторинга трафика в сложных, многоуровневых сетях с коммутацией и маршрутизацией

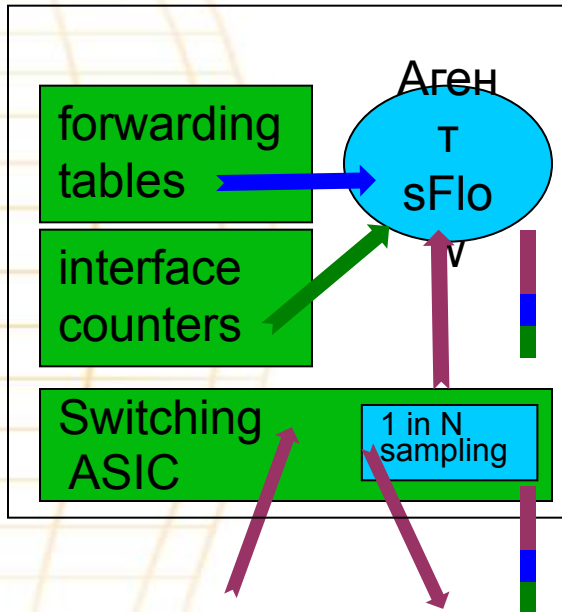


Измерения доступны на каждом порту, всё время = сеть видна целиком и «прозрачна»

- ➔ Эффективный контроль позволяет достигнуть высокой производительности сети и повысить надёжность

sFlow в действии

Коммутатор /
Маршрутизатор



sFlow Datagram

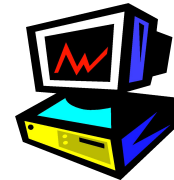
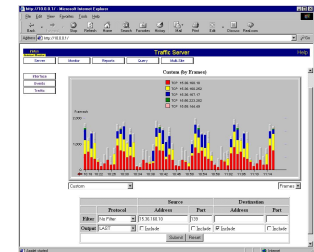
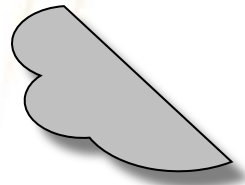


eg 128B

rate
pool

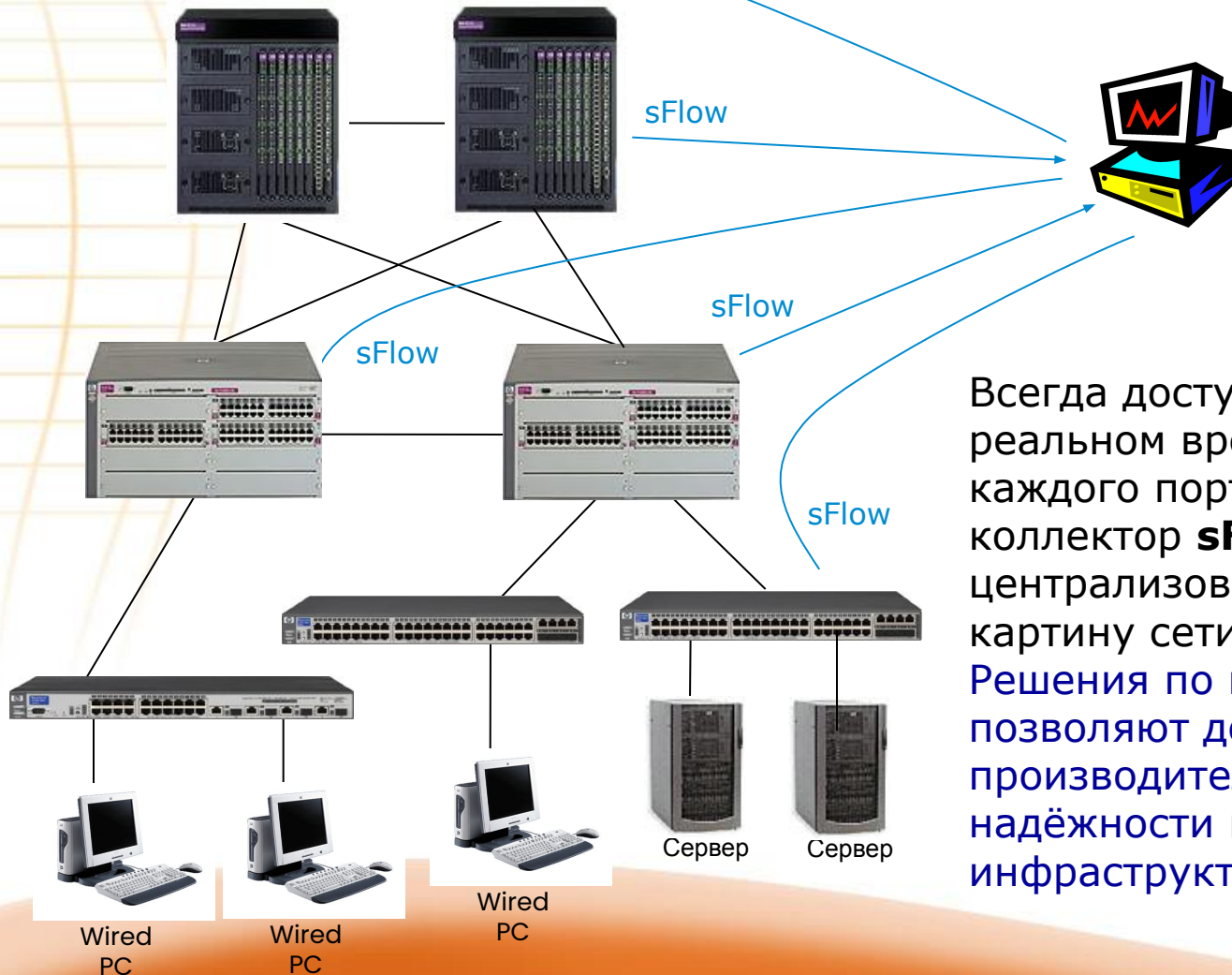
src 802.1p/Q
dst 802.1p/Q
next hop
src/dst mask
AS path
communities
localPref

src/dst
Radius
TACACS



Коллектор и анализатор
sFlow

«Прозрачная сеть» sFlow с данными на каждом порту коммутатора, поступающими всё время



Коллектор /
Анализатор sFlow

Всегда доступные, поступающие в реальном времени измерения с каждого порта пересылаются в коллектор **sFlow**, и формируют централизованную, «прозрачную» картину сети.

Решения по контролю сети позволяют достигнуть высокой производительности и высокой надёжности всей сетевой инфраструктуры.

Определение различных угроз и контроль производительности и надёжности сети

Идентификация угроз безопасности

- Подозрительное и аномальное поведение
- Вторжения в сеть
- Нарушение политик (Policy violation)
- Неавторизованный трафик
- Попытки сканирования
- Атаки типа «Отказ в обслуживании» (DoS)
- ARP-штормы

Обеспечение качества обслуживания (QoS) в сетях VoIP и мультисервисных сетях (converged networks)

Определение проблем с сетью (network troubleshooting) и проблем с приложениями

- Почему моя сеть такая медленная?

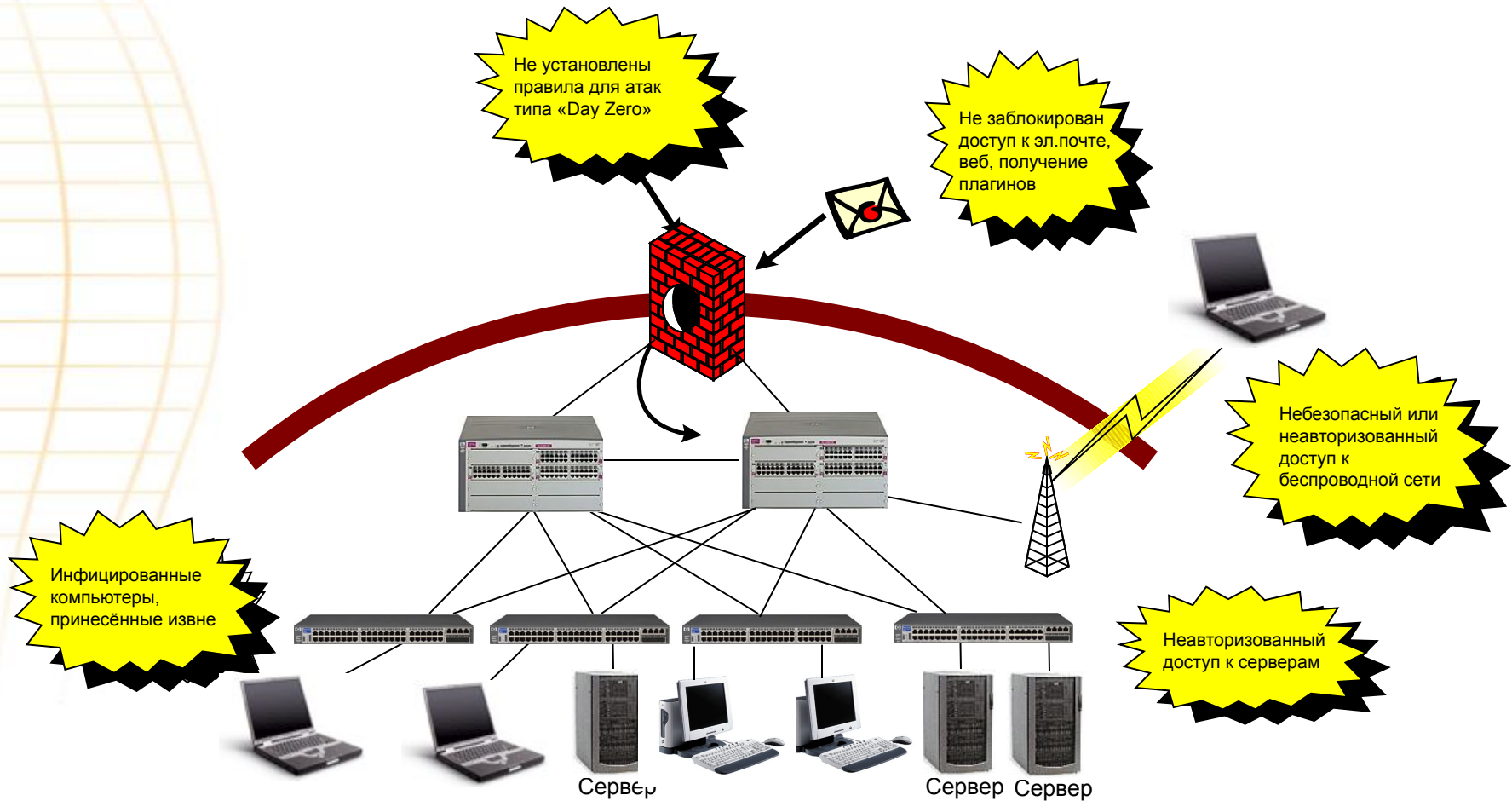
Учёт трафика (аккаунтинг) и выставление детализированных счетов, для «пристыжения» пользователей за использование сети не по назначению

Оптимизация маршрутов BGP

Управление широковещательным трафиком (multicast traffic)

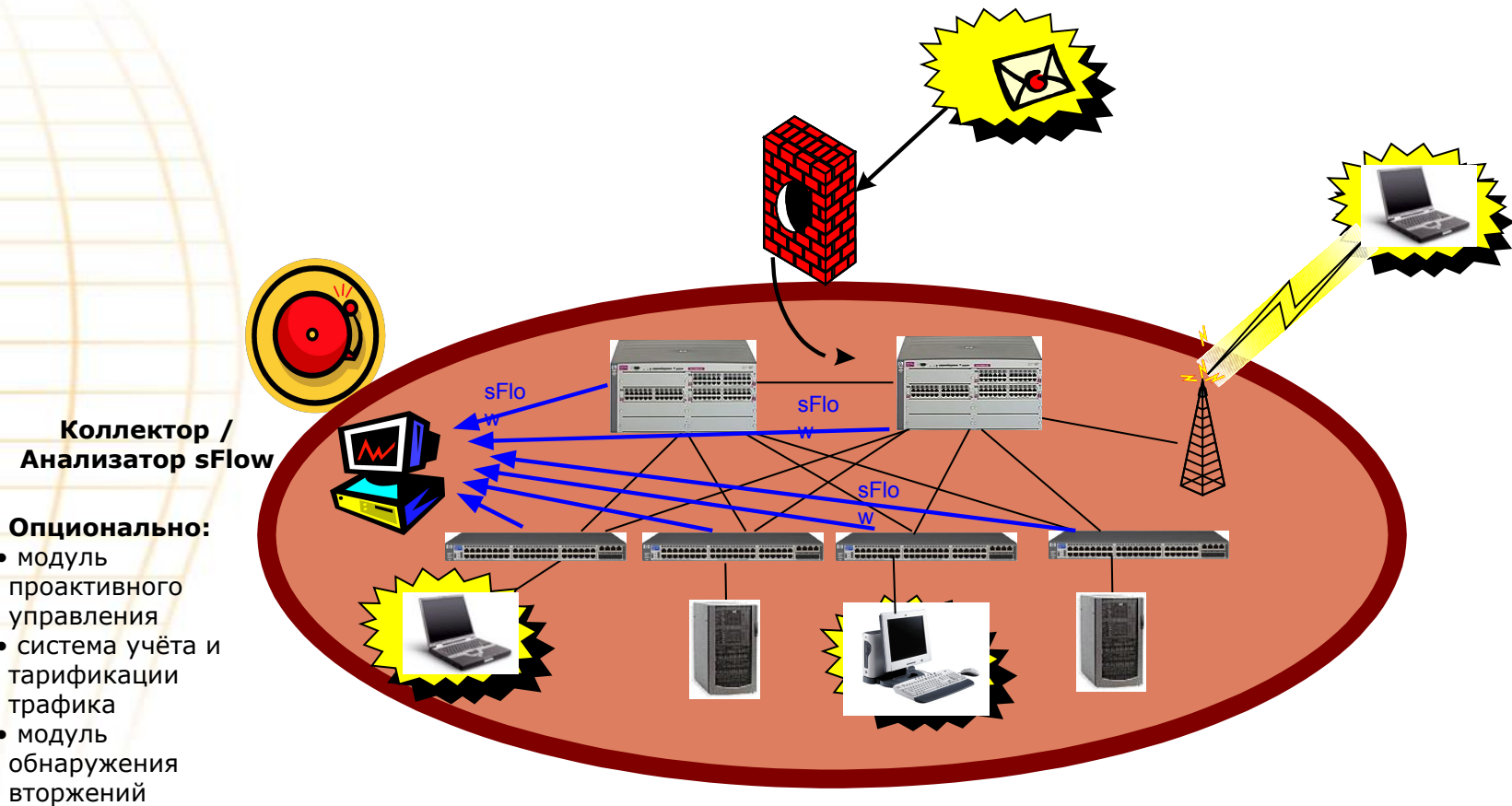
Анализирование трендов в использовании сети, для дальнейшего планирования развития сети

Межсетевой экран, IDS являются необходимыми для защиты периметра сети, но...



Защита периметра может быть нарушена или «прорвана». Нельзя полагаться на целостность защиты периметра или доступ ко всем хостам

Определение внутренних угроз и контроль безопасности с sFlow



Непрерывный, постоянный мониторинг всей сети с sFlow позволяет немедленно определить аномальное поведение и внутренние угрозы

*Мощнейшее решение самой острой и
наболевшей проблемы всех СІО и
системных администраторов в мире:*

**Больше защиты, обнаружения
и мгновенное реагирование с
интегрированным решением
Virus Throttling**

Больше защиты в локальной сети
(LAN)

ProCurve 5300xl Software Release 3

The Virus Problem ...

Антивирусные программы служат для защиты от вирусов

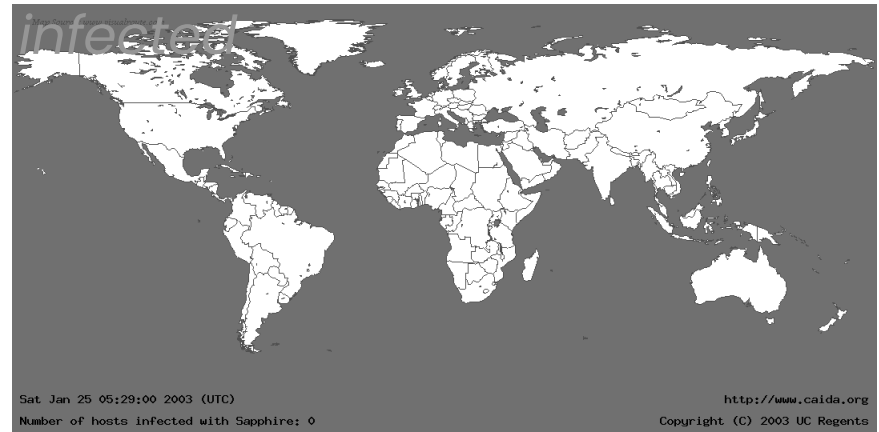
- Это помогает, но они не могут опознать "day zero" угрозы

Day zero, вирусы типа «червь» размножаются очень быстро и наносят массу вреда

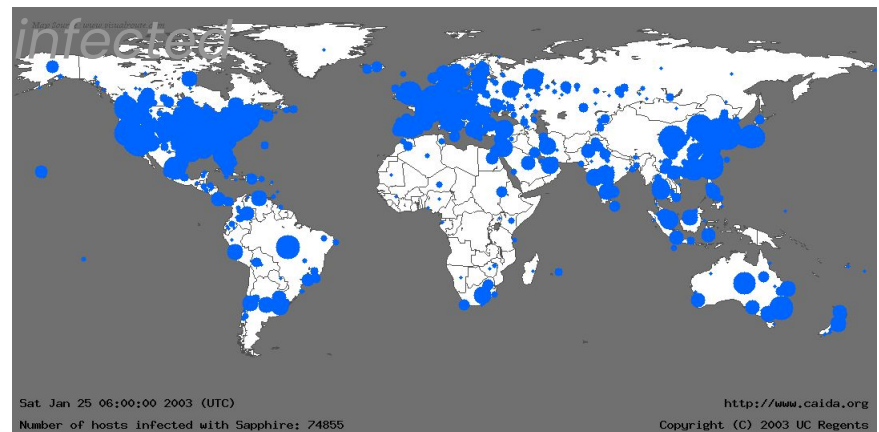
- Множество инфицированных компьютеров
- Перегрузка и блокировка сети

Примеры вирусов

05:29 Jan 25 - 0



06:00 Jan 25 - 74855



ProCurve 5300xl Software Release 3

Network Integrated Virus Throttling

Virus Throttling (ограничение распространения червей) - *встроенная* функция (*не отдельное устройство*) для построения гибкой сетевой инфраструктуры, без необходимости установки клиентского ПО

Обнаружение основано только на *поведении сети* для *защиты* от вирусов – против новых и неидентифицированных угроз – day zero

Предотвращает распространение вируса немедленно – «удушение» трафика на источнике

Занесение записи в журнал событий и предупреждающего SNMP trap-a на ProCurve Manager Plus для информирования ИТ для принятия дальнейших мер

Существует как бесплатное обновление микропрограммы, прост для повсеместного внедрения, защищая сеть от распространения вирусов

Изобретено и запатентовано в Лаборатории HP ProCurve Labs и реализовано для коммутаторов 5300xl by ProCurve Networking как элемент нашего портфолио по безопасности

ProCurve интегрированный Virus Throttling КАК это работает

Вирус распространяется от зараженной машины быстро контактируя с другими машинами (SQLSlammer: >800/sec)

Здоровые машины подключаются к меньшему количеству машин и значительно реже (1/sec)

Решение: ограничитель частоты на контакты с другими машинами

- Как только червь попытается распространиться, 5300 обнаружит аномальное поведение
- «Удушье» трафика от инфицированной машины на границы VLAN позволяет значительно замедлить распространение вируса... или ...
- Предотвращение маршрутизации всего трафика от инфицированной к другим членам сети




другие члены сети



Immediate machine speed response limits spread of virus until human action can be taken



ProCurve
5300xl Switch
*Virus
Throttling
Built In*

A woman with dark hair, wearing a dark green button-down shirt, stands in a server room. Behind her are several server racks with glowing green lights. To her left is a large monitor displaying a network diagram with blue nodes and lines. To her right is another large monitor displaying a blurred image of a person. The scene is dimly lit, with the primary light sources being the monitors and the server racks.

HP ProCurve
Networking
Управление сетью

HP ProCurve Manager

Автораспознавание устройств

Конфигурирование и управление оборудованием

Модульная архитектура для будущего расширения

Понятный интерфейс в стиле Windows-Explorer («Проводник»)

Сбор данных и уведомление о возможных отказах

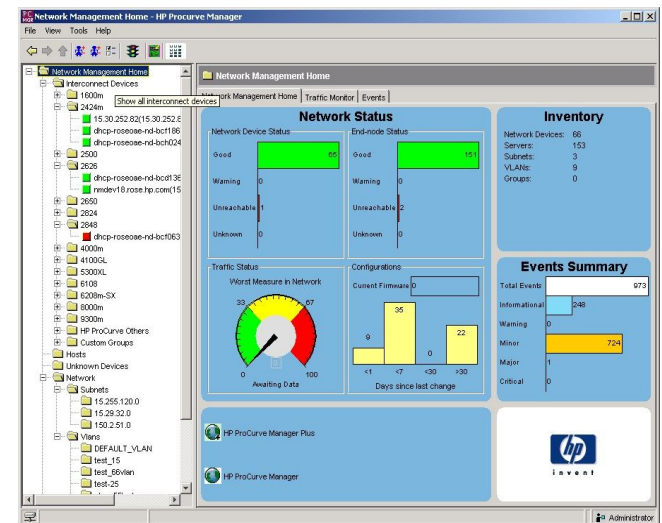
Поддержка неограниченного количества устройств

Построение карт и сетевых топологий

LLDP (802.1ab) discovery

Автоматическая регистрация продуктов ProCurve через web

Цена: \$0 (идет в комплекте с каждым управляемым коммутатором. Также доступна на веб-сайте: www.hp.com/go/hpprocurve)



HP ProCurve Manager Plus

Весь функционал HP ProCurve Manager ПЛЮС:

Гибкое управление политиками в группах, быстрое конфигурирование новых устройств

Расширенные функции по управлению безопасностью сети

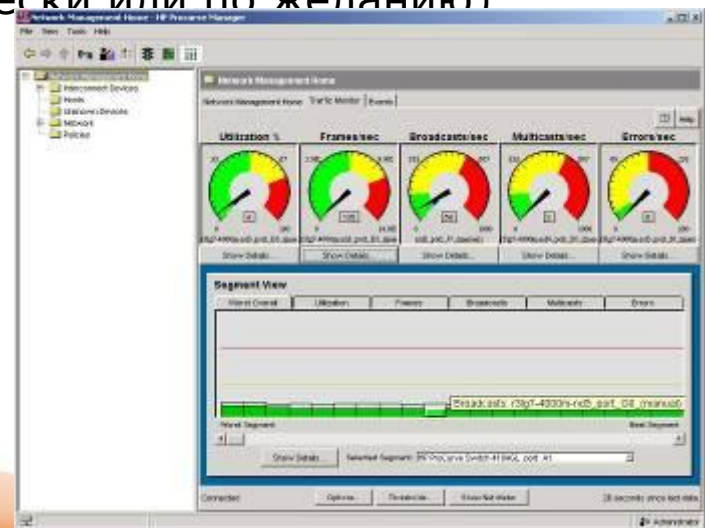
Управление конфигурацией группы устройств, загрузка готовых профилей

Создание и конфигурирование VLAN

Более детальный мониторинг и анализ трафика (XRMON, sFlow)

Обновление микропрограммы (автоматически или по желанию)

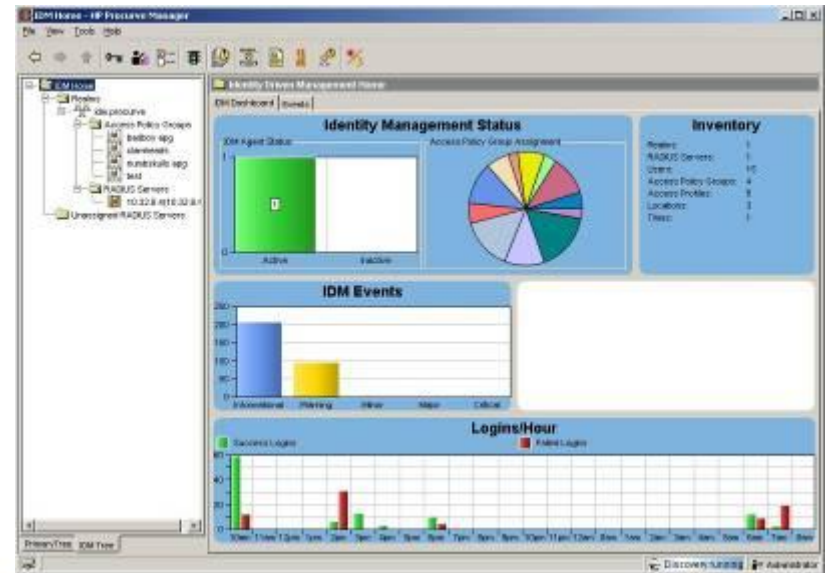
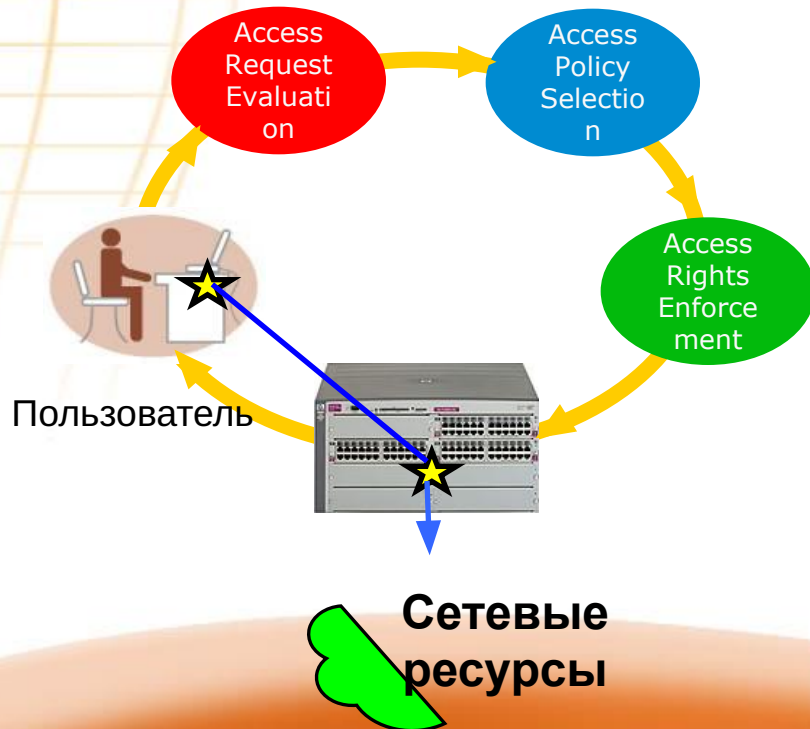
Бесплатная 30-дневная trial-версия идет в комплекте с HP ProCurve Manager.



IDM 2.0 - Identity Driven Management

Фундаментально новый подход для IT-Менеджеров по взаимодействию с сетью

- унификация границы сети (wire, wireless, WAN)
- управление ресурсами и политиками, не жели устройствами
- фокус на безопасность и интеграцию существующих приложений
- сеть адаптируется под приложения и/или бизнес потребности



Identity Driven Manager 2.0

- Динамическая установка параметров безопасности, доступа и производительности на основании пользователя, местоположения, времени, и теперь статуса «целостности» клиента
- Простое создание и управление группами пользовательских правил (политик доступа) для оптимизации производительности сети и повышения продуктивности пользователей, а также повышения общей эффективности (соответствующий доступ каждому)
- На основании прописанных правил будут установлены параметры сети для обеспечения желаемой функциональности

Установка значений =>



VLAN



Bandwidth Limit



QoS



ACLs



User ID

Device ID

Time

Location


Client Integrity Status

На основании =>

Identity Driven Per-Port ACL



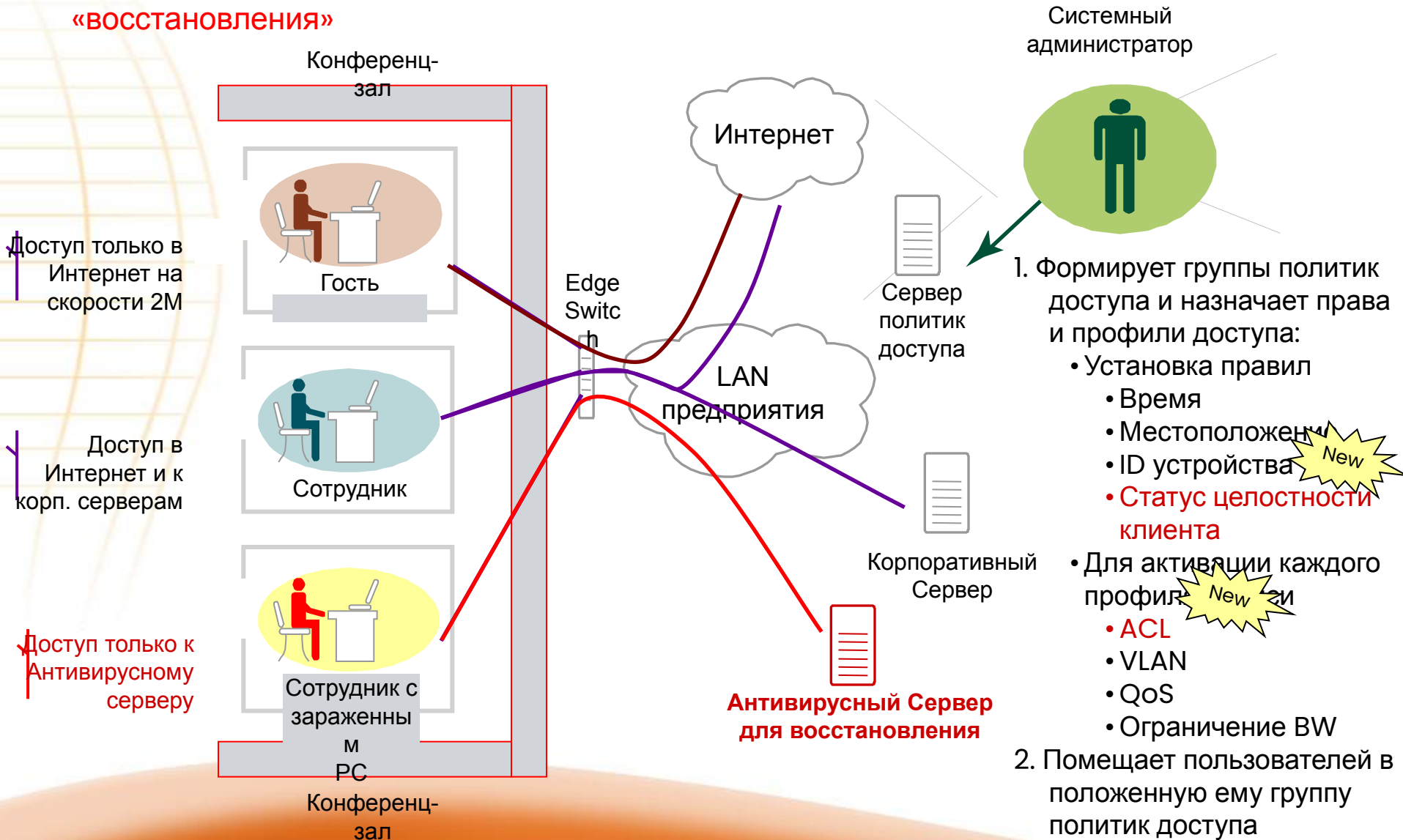
Наделяет сеть более детализированными и гибкими правилами безопасности доступа

- Методы аутентификации 802.1X, Web, MAC
- Позволяет всем быть подключенным к общему коммутатору разрешая доступ к общим сетевым ресурсам, в тоже время ограничивая доступ к закрытой информации на определенных портах
- Правило может применяться индивидуально для каждого порта на базе IP адресов хоста, подсети IP, приложения (номера TCP/UDP портов), или типа протокола IP
- Работает в режимах коммутации и маршрутизации

Применение Client Integrity

User Experience

Зараженные компьютеры получают права доступа к серверу «восстановления»



ProCurve Mobility Manager 1.0 (PMM) Расширение возможностей централизованного управления



Простые,
высокопроизводительные
средства для управления
беспроводными
локальными сетями
ProCurve

В сочетании с PCM Plus
образует экономичное
решение для
унифицированного
управления сетью

Начало продаж: декабрь 2005 г.
Цена в России 1752 долл. США

Сценарий для заказчика

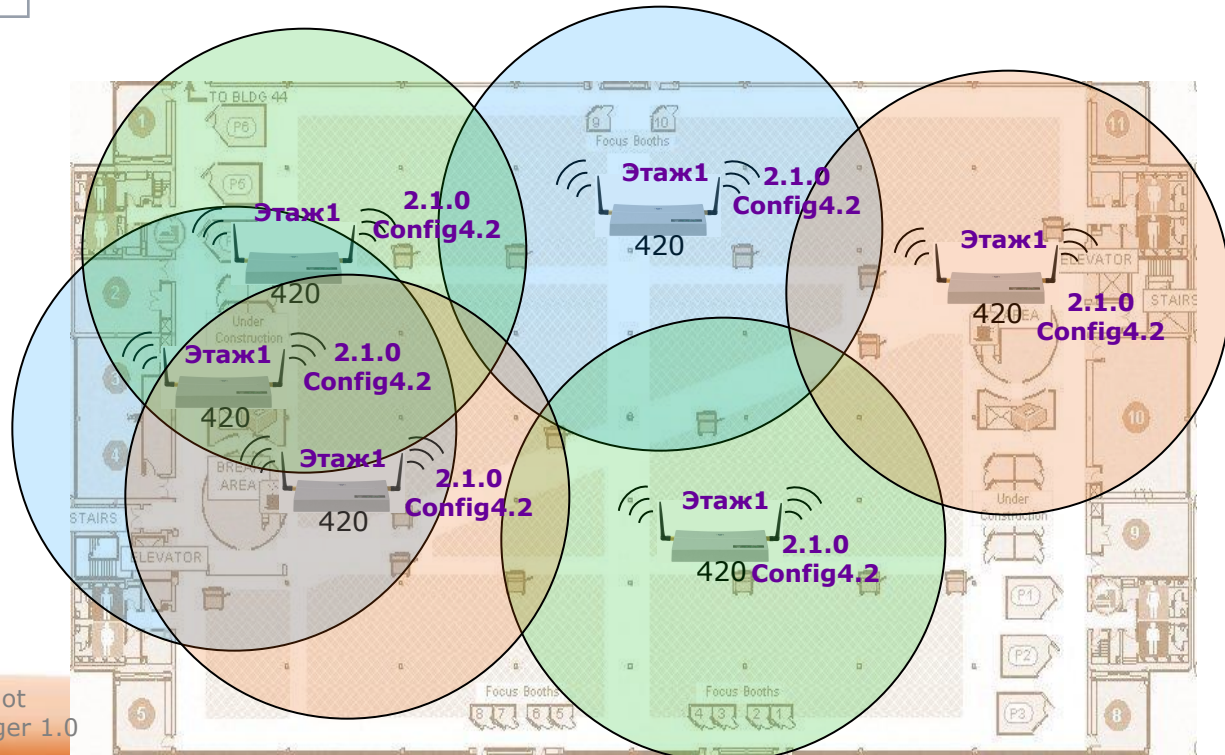
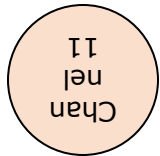
Применение и использование возможностей Deployment Assistance

Back Office



IT Manager

1. Подготовка объекта (определение мест для AP, установка мощности радиосигнала и др.) и установка
2. IT Manager создает конфигурационные шаблоны в PCM используя любые параметры настроек: установки безопасности (ключи WEP, WPA), dhcp ip lookup, SSIDs, и др.
3. PCM автоматически обнаруживает точки доступа, назначает их группе «Этаж1», применяет конфигурационные настройки, обновляет ПО (если нужно), активирует радиопередатчики, активирует механизм ACS (автоматический выбор частоты)
4. PCM глобально анализирует результаты ACS и прописывает значения каналов в конфигурацию точек доступа.



Note: Site survey and visualization not provided by ProCurve Mobility Manager 1.0

План этажа офиса

Сценарий для заказчика

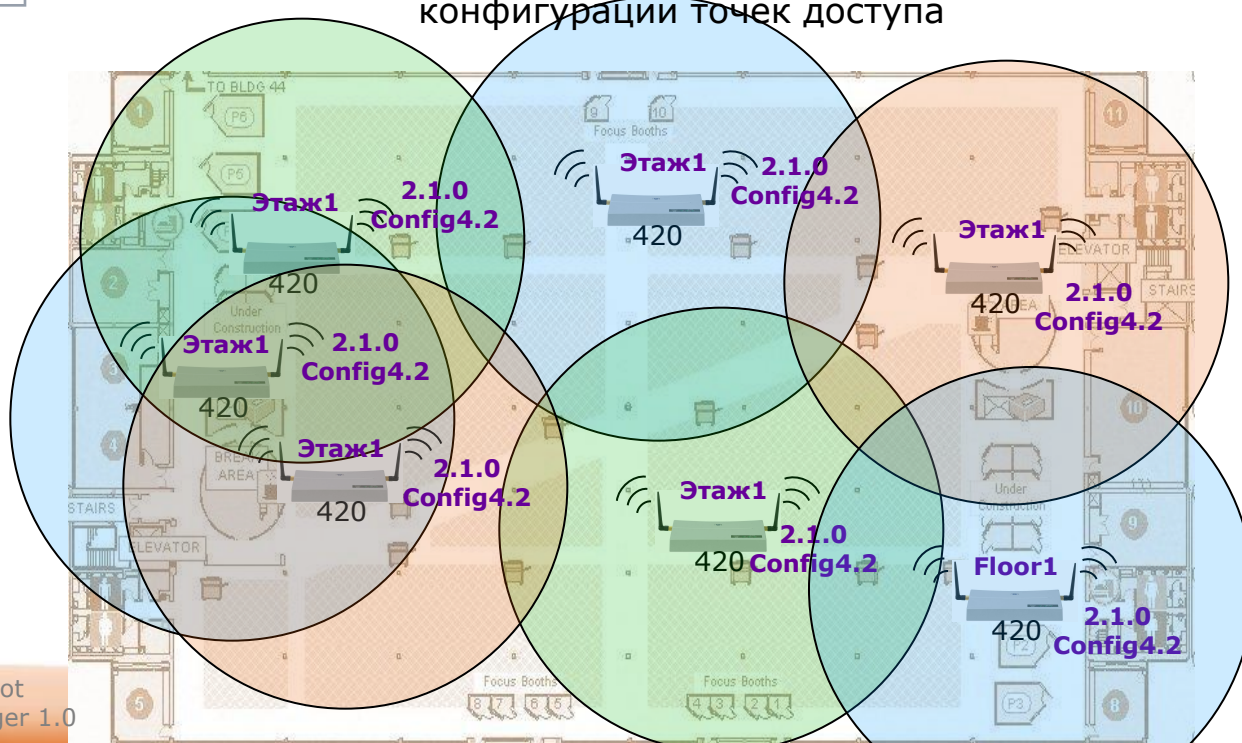
Расширение беспроводной сети

Back Office



IT
Manager

1. Добавились новые сотрудники, установлены дополнительные точки доступа для покрытия требуемых зон
2. РСМ обнаружил новые AP, назначил их существующей группе, применил желаемые настройки и обновил ПО
3. РСМ глобально ре-активировала ACS для всей группы
4. РСМ глобально провела ACS, зафиксировала выбранные каналы и прописала их значения в конфигурации точек доступа



Note: Site survey and visualization not provided by ProCurve Mobility Manager 1.0

Преимущества HP



Бесплатные обновления программного обеспечения (firmware) для всех коммутаторов

Бесплатное программное обеспечение для управления сетью
HP ProCurve Manager

- Интуитивный, лёгкий в использовании пользовательский интерфейс
- Авто-обнаружение устройств, карты топологии, запуск веб-агента
- Автопредупреждения и рекомендации по устранению неполадок

Пожизненная гарантия

- Бесплатная пожизненная гарантия* на весь срок владения оборудованием с заменой на следующий рабочий день!
- Без «подводных камней» - на весь период владения устройством, распространяется в т.ч. на все модули, вентиляторы, источники питания
- Высочайший показатель времени наработки на отказ (MTBF от 79 000 до 319 000 часов(>36 лет!))

*Все продукты – кроме серий 8100fl, 9300m, 9400sl и 700wl

ProCurve Networking by HP

Сергей Перротте

Менеджер по работе со стратегическими клиентами,
Сетевое подразделение ProCurve Networking by HP, Россия

Хьюлетт-Паккард
115054 Россия, Москва
Космодамианская наб., 52, строение 1

Тел. (495) 797-3576

Моб. (916) 993-3480

Эл. почта perrottet@hp.com