ИРКУТСКИЙ ПОЛИТЕХ

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Лекция по дисциплине
«Сети и телекоммуникации»

Технологии AAA, NAT, ACL

Руководитель лаборатории сетевых технологий
института ИТиАД ИРНИТУ:
Аношко Алексей Федорович
Telegram: @a_anoshko

AAA (Authentication, Authorization, Accounting)

В организации сетей необходим механизм, который позволяет осуществлять аутентификацию, авторизацию и учет пользователей, то есть контролировать доступ и записывать производимые действия

Каждая из этих функций представляет собой модульный компонент, который может применяться в качестве компонентов инфраструктуры безопасности, реализуемой в корпоративной сети.

Как правило, управление данным механизмом реализуется посредством протоколов на базе клиент-сервер, таких как RADIUS и TACACS.

Внедрение AAA позволяет эффективно усилить безопасность корпоративной сети в целом.

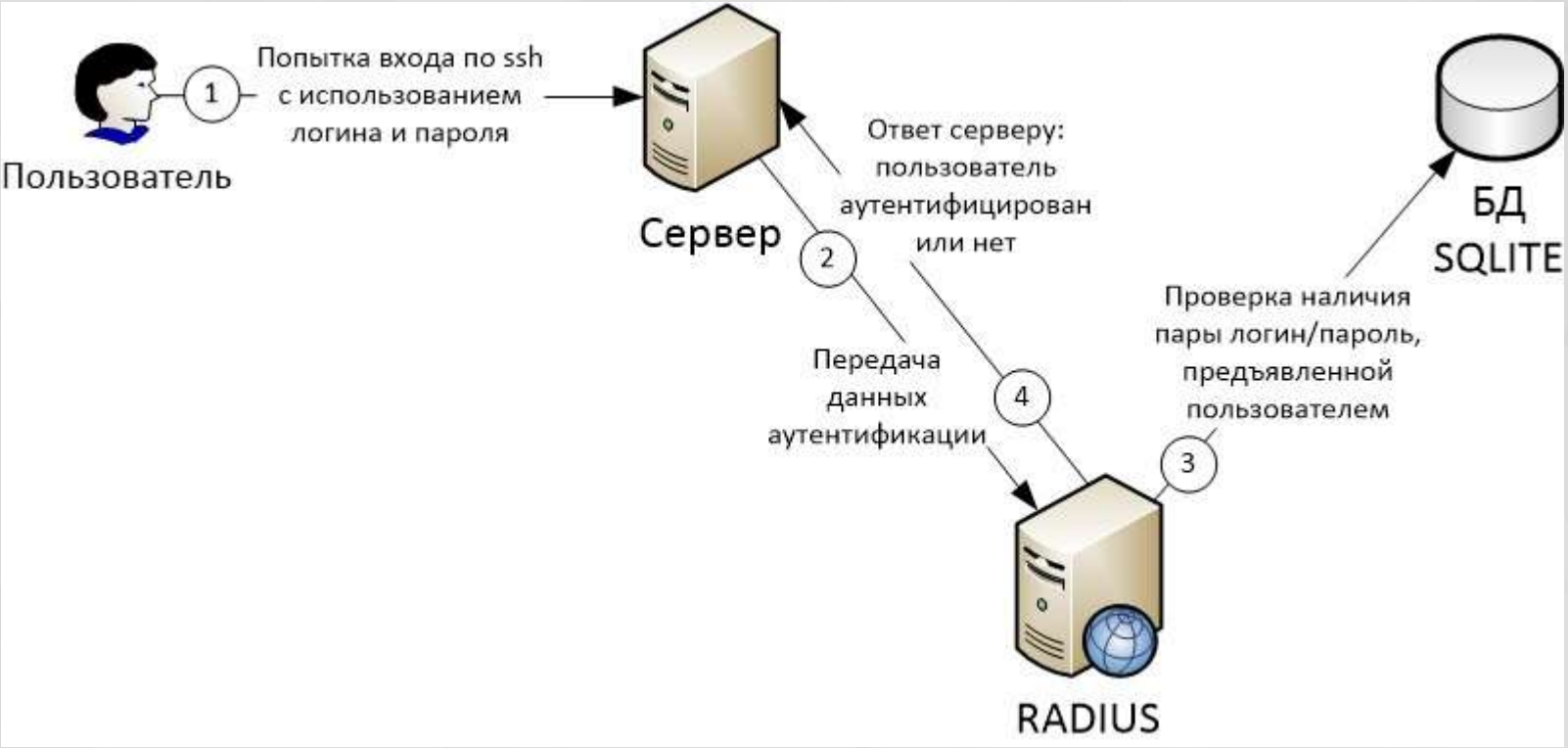
Authentication vs Authorization

Аутентификация — процедура проверки подлинности, например проверка подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базе данных.

Авторизация — предоставление определенному лицу или группе лиц прав на выполнение определенных действий.

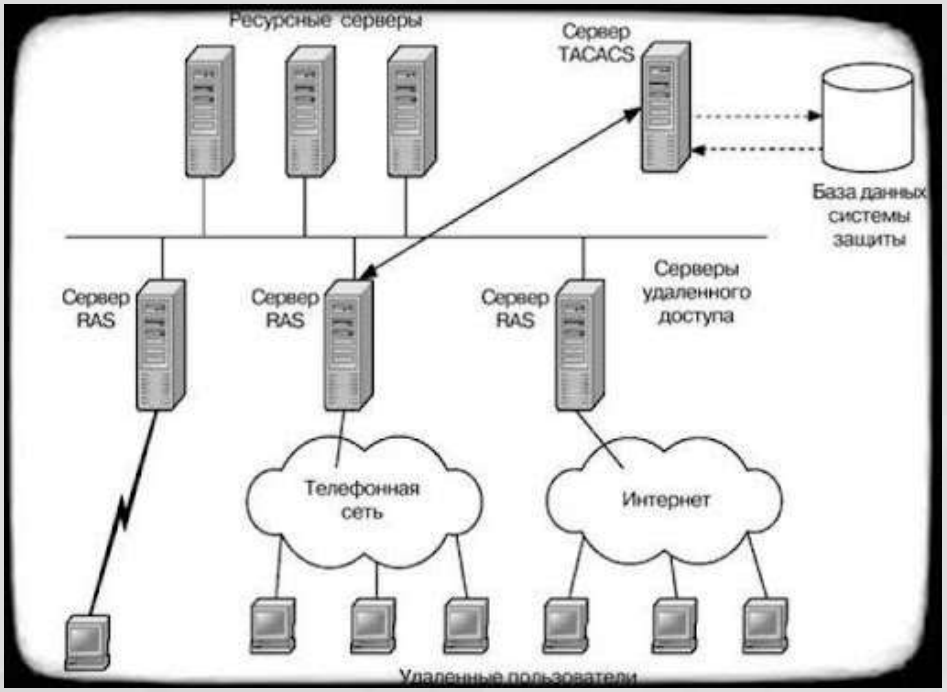
RADIUS (Remote Authentication in Dial-In User Service)

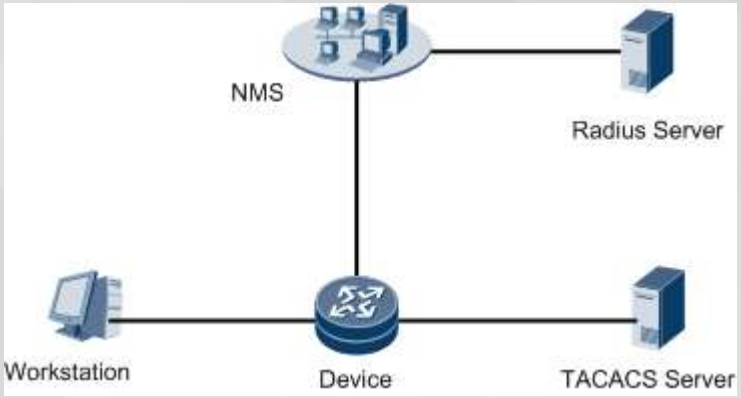
Аббревиатура «RADIUS» расшифровывается как «Remote Authentification Dial In User Services» — «аутентификация для удаленного доступа к пользовательским сервисам»



RFC 2865 – июнь 2000

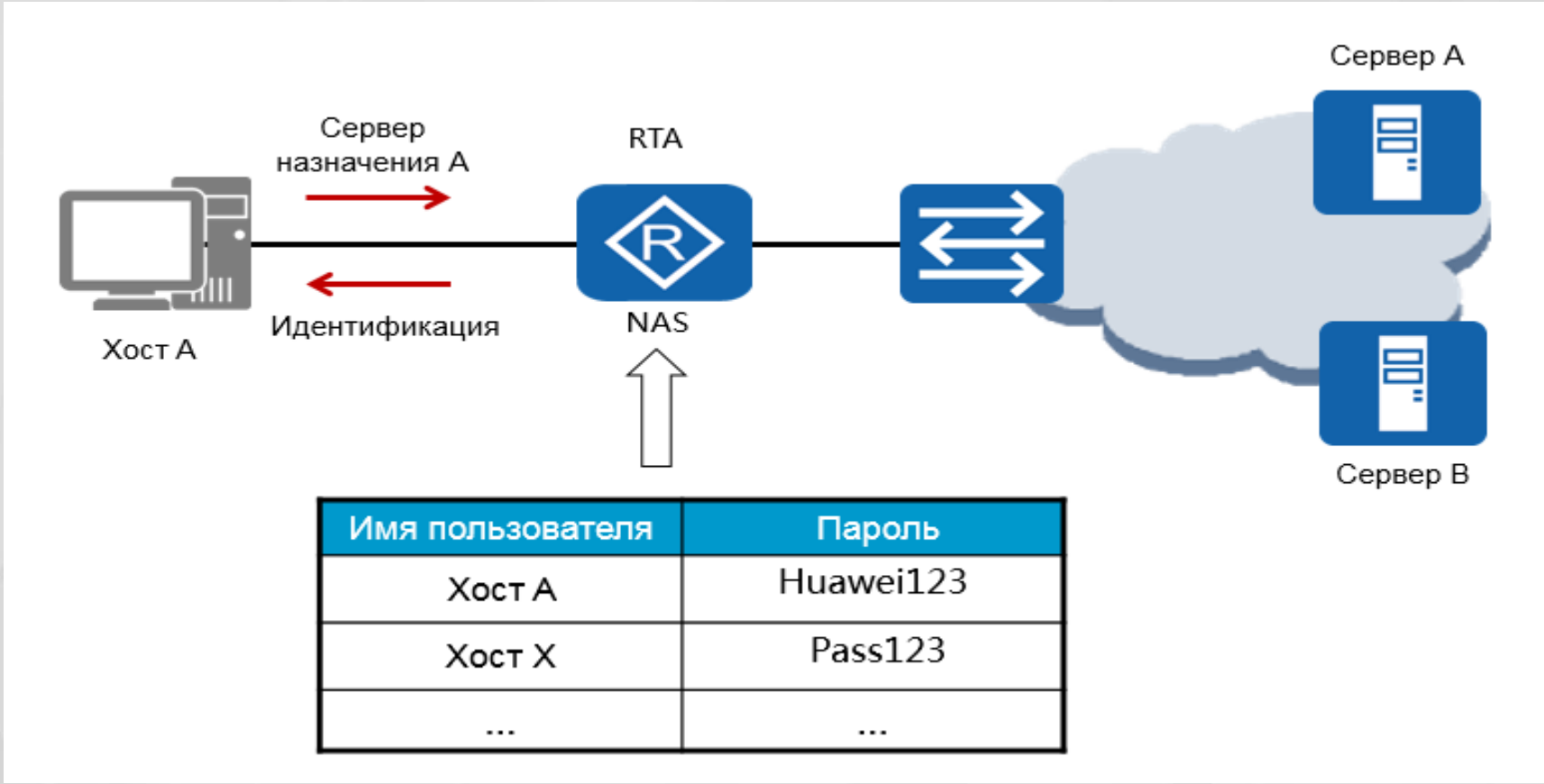
TACACS (Terminal Access Controller Access System)





RFC 1492 - июль 1993

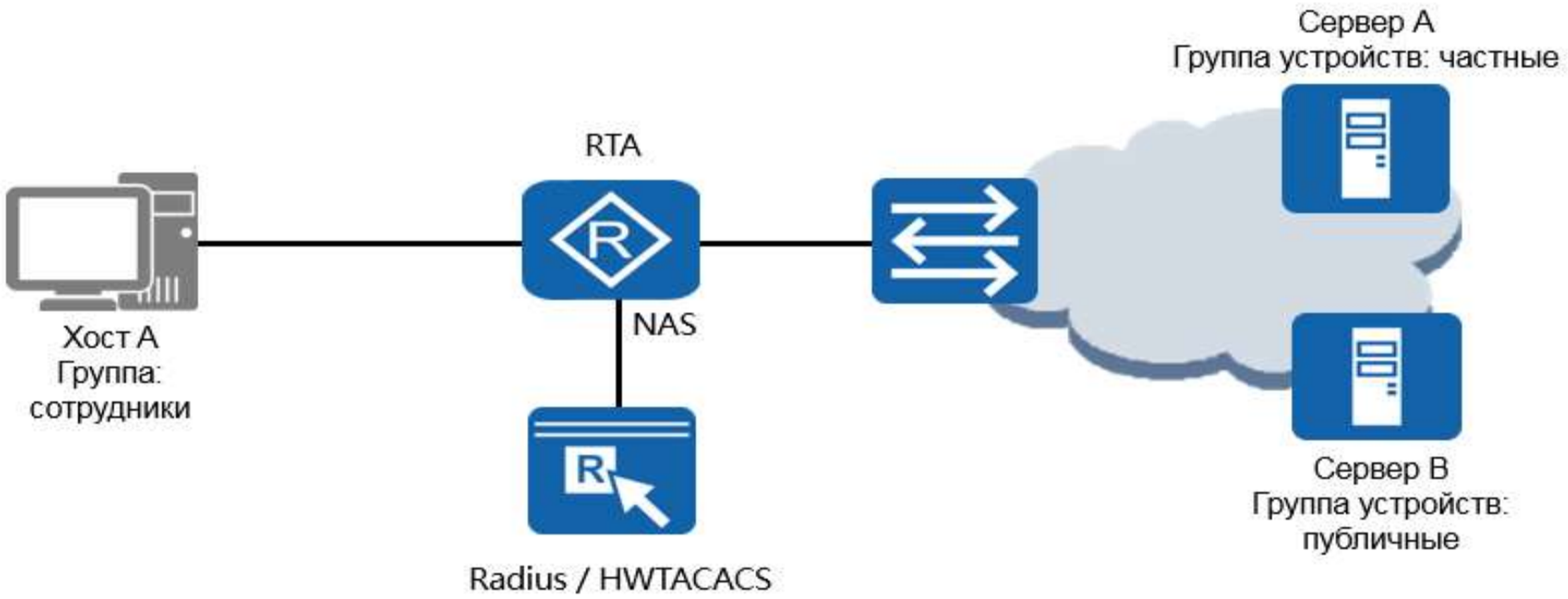
Аутентификация



Имя пользователя	Пароль
Хост A	Huawei123
Хост X	Pass123
...	...

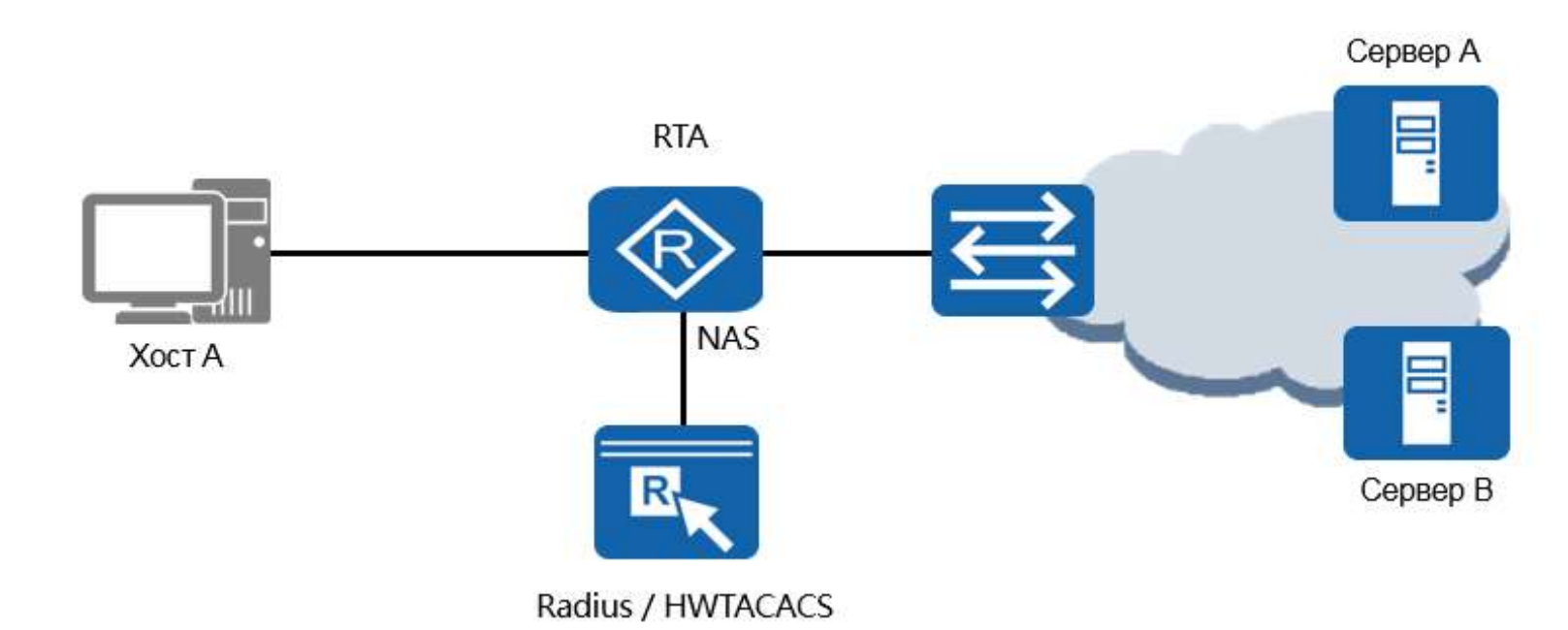
- Управление доступом пользователя осуществляется на базе схемы аутентификации.

Авторизация



Группа устройств	Группа пользователей	Время	Уровень привилегий
Частные	Администраторы	9:00–12:00	15
Публичные	Администраторы	9:00–18:00	15
Публичные	Сотрудники	9:00-18:00	2

Учет



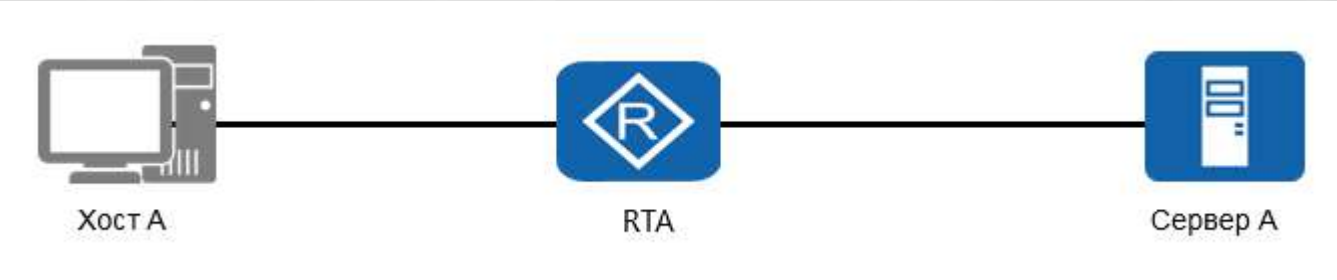
Время входа	Имя пользователя	Время работы	Полоса пропускания приема/передачи
1 мая 2021 г. 03:20:55	Хост А	01:22:15	496,2 КБ/21 МБ
16 апреля 2021 г. 12:40:51	Хост Х	00:30:12	123 КБ/1 МБ

Домены AAA

- Для пользователей в разных доменах

можно использовать различные схемы.

Локальная конфигурация AAA




```
[RTA]aaa
[RTA-aaa]local-user huawei password cipher hello123
[RTA-aaa]authentication-scheme auth1
[RTA-aaa-authen-auth1]authentication-mode local
[RTA-aaa-authen-auth1]quit
[RTA-aaa] authorization-scheme auth2
[RTA-aaa-author-auth2]authorization-mode local
[RTA-aaa-author-auth2]quit
[RTA-aaa]domain huawei
[RTA-aaa-domain-huawei]authentication-scheme auth1
[RTA-aaa-domain-huawei]authorization-scheme auth2
```

- На AR2200E можно сконфигурировать

схемы аутентификации и авторизации.

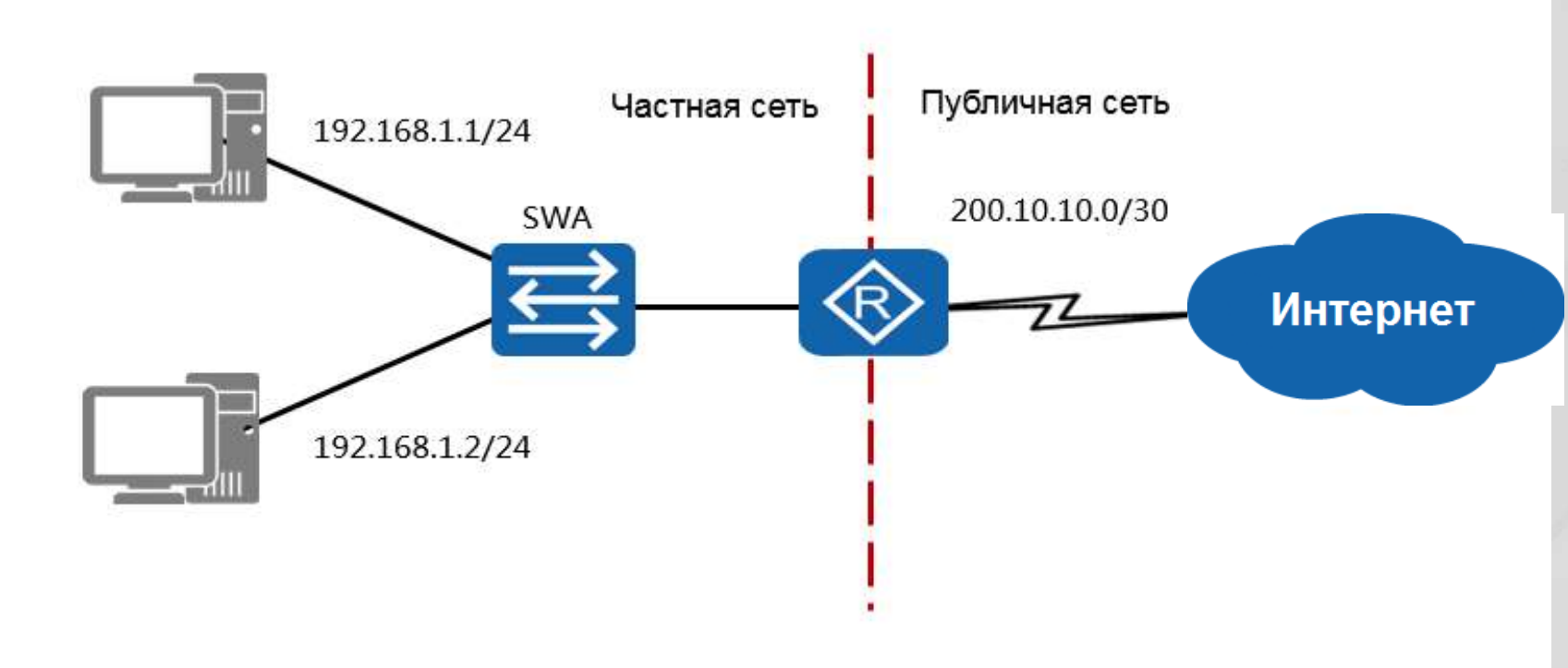
NAT (Преобразование сетевых адресов)

Непрерывное развитие IP-сетей стало причиной нехватки адресов IPv4.

Актуальность данной проблемы потребовала поиска долгосрочных решений. Хорошо зарекомендовавший себя механизм преобразования сетевых адресов (Network Address Translation; NAT) широко применяется в корпоративных сетях.

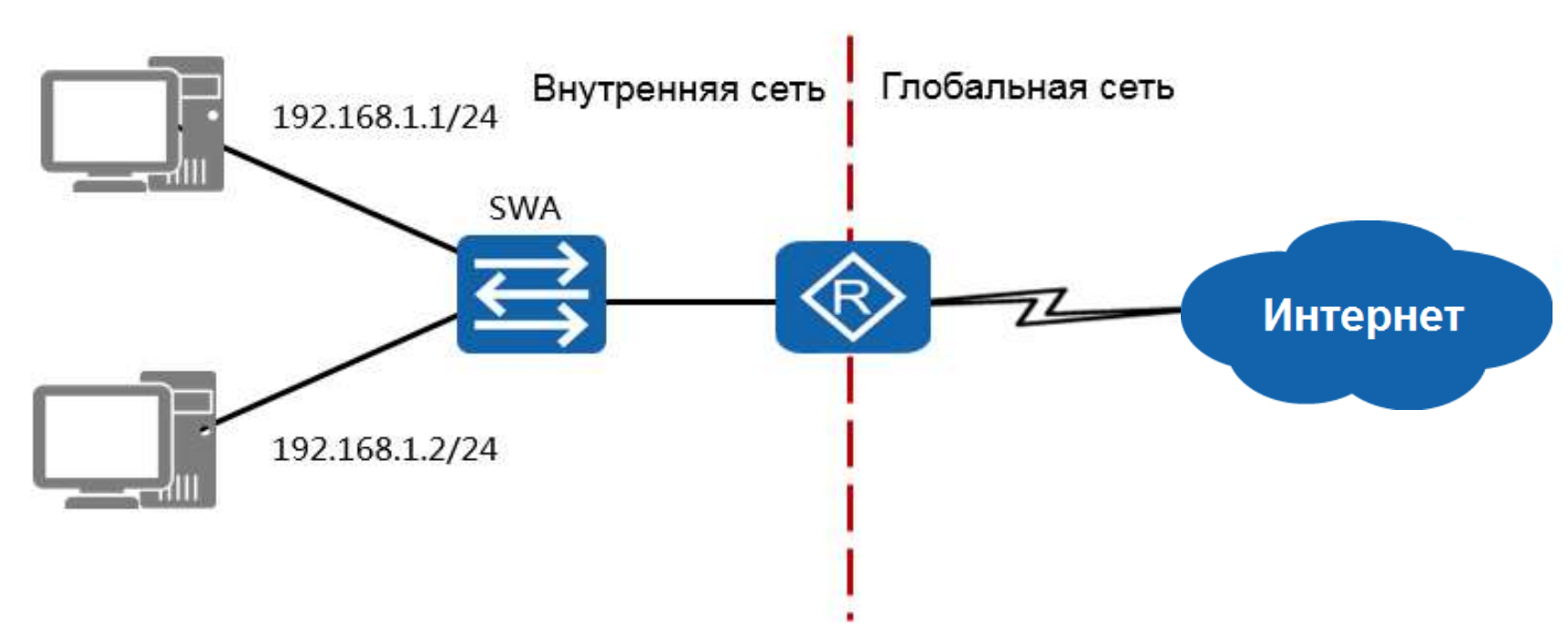
Многие методы NAT были разработаны таким образом, чтобы экономить пространство публичных адресов и в то же время поддерживать непрерывную связь с публичной сетью.

Частные и публичные сети



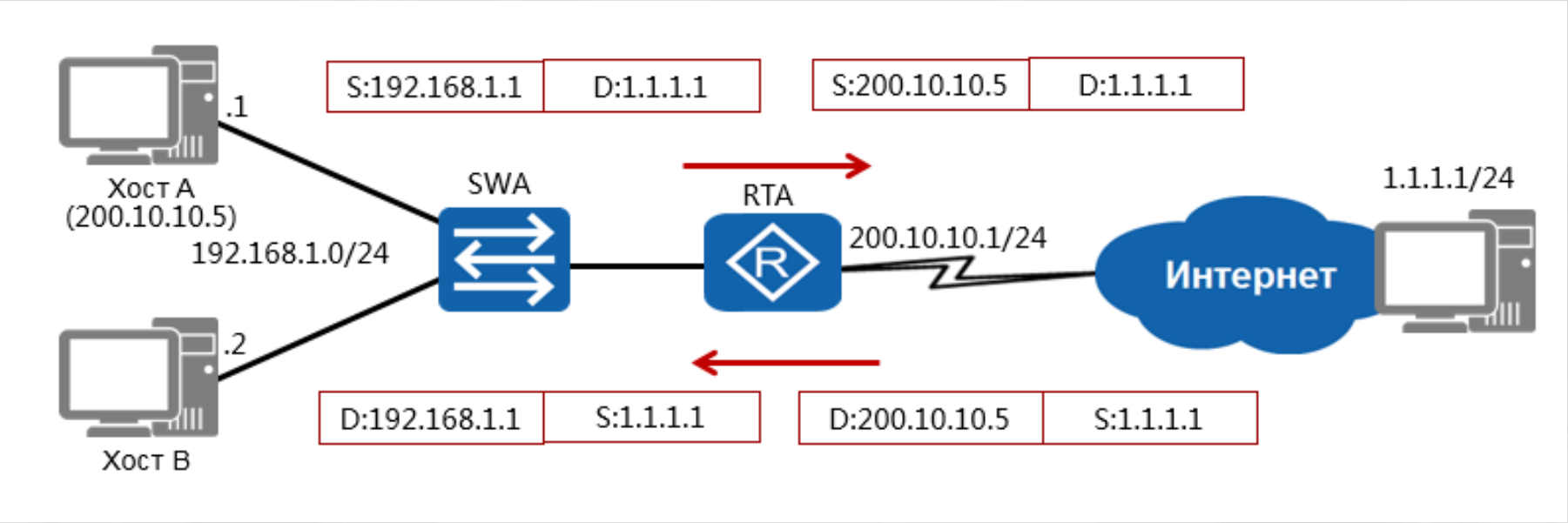
- Метод борьбы с быстрым исчерпанием пула IP-адресов.
- Шлюз работает на границе частной и публичной сетей.

Принцип работы NAT



- Границы NAT представлены как на уровне внутренней сети, так и на уровне глобальной сети.
- Преобразование адресов осуществляется между границами.

Статический NAT



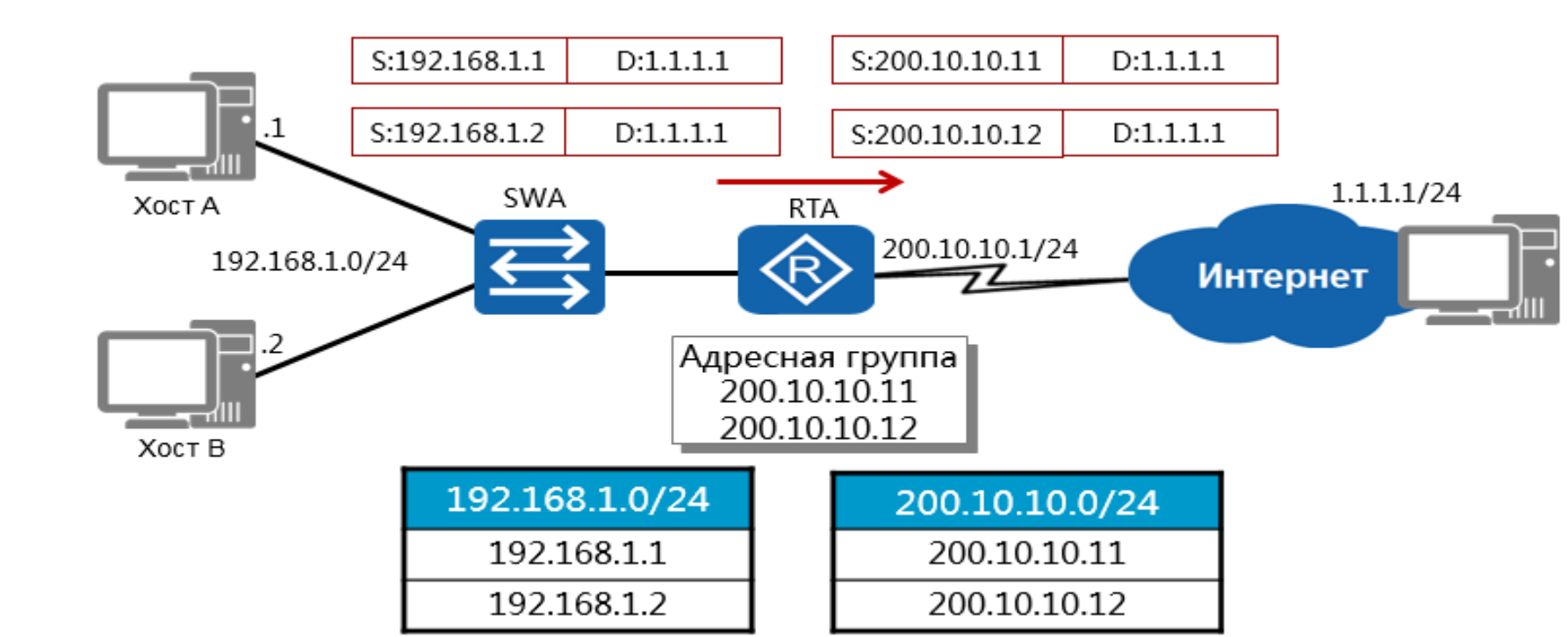
- Взаимно-однозначное (один к одному)

  преобразование частных и публичных адресов.

- Уменьшение потребности в управлении

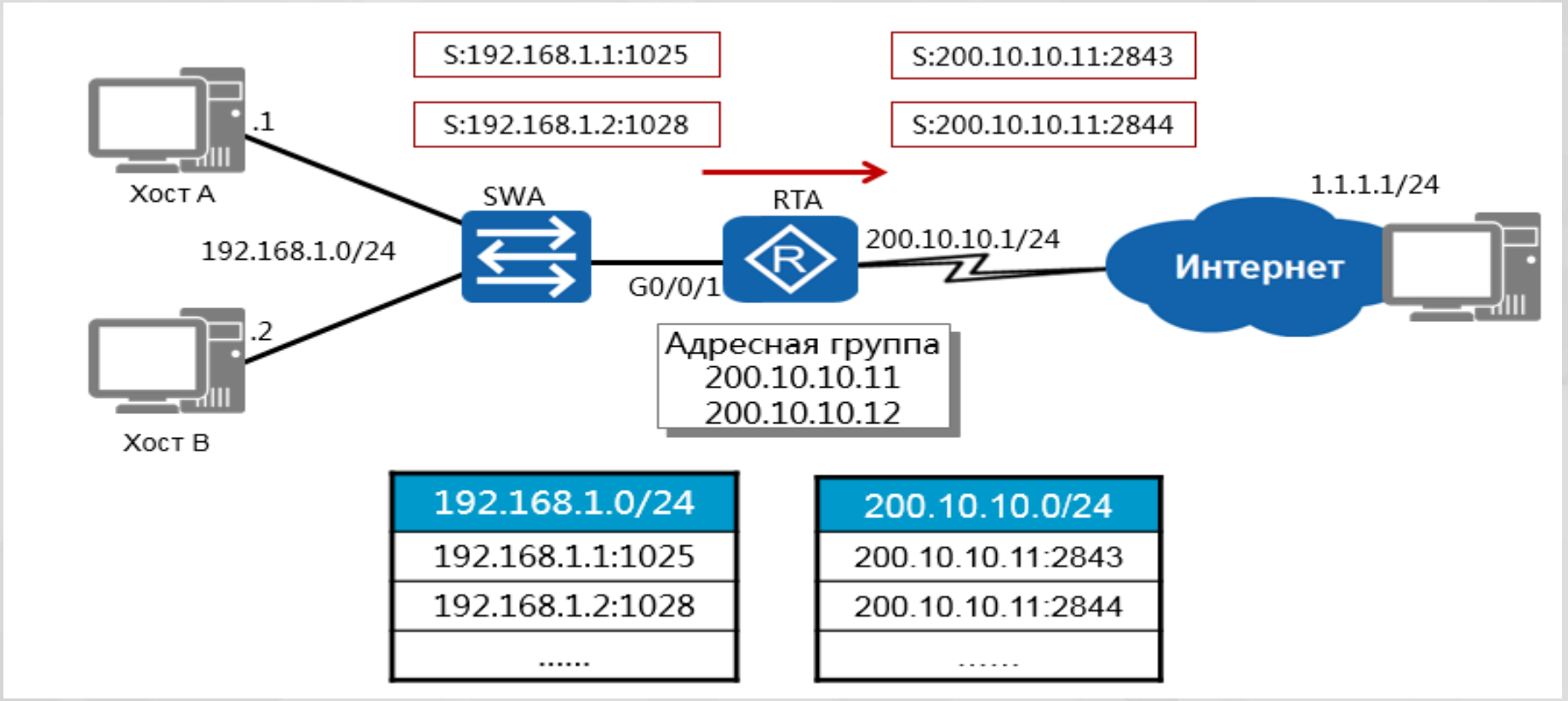
  адресами за счет сеансовых потоков.

Динамический NAT



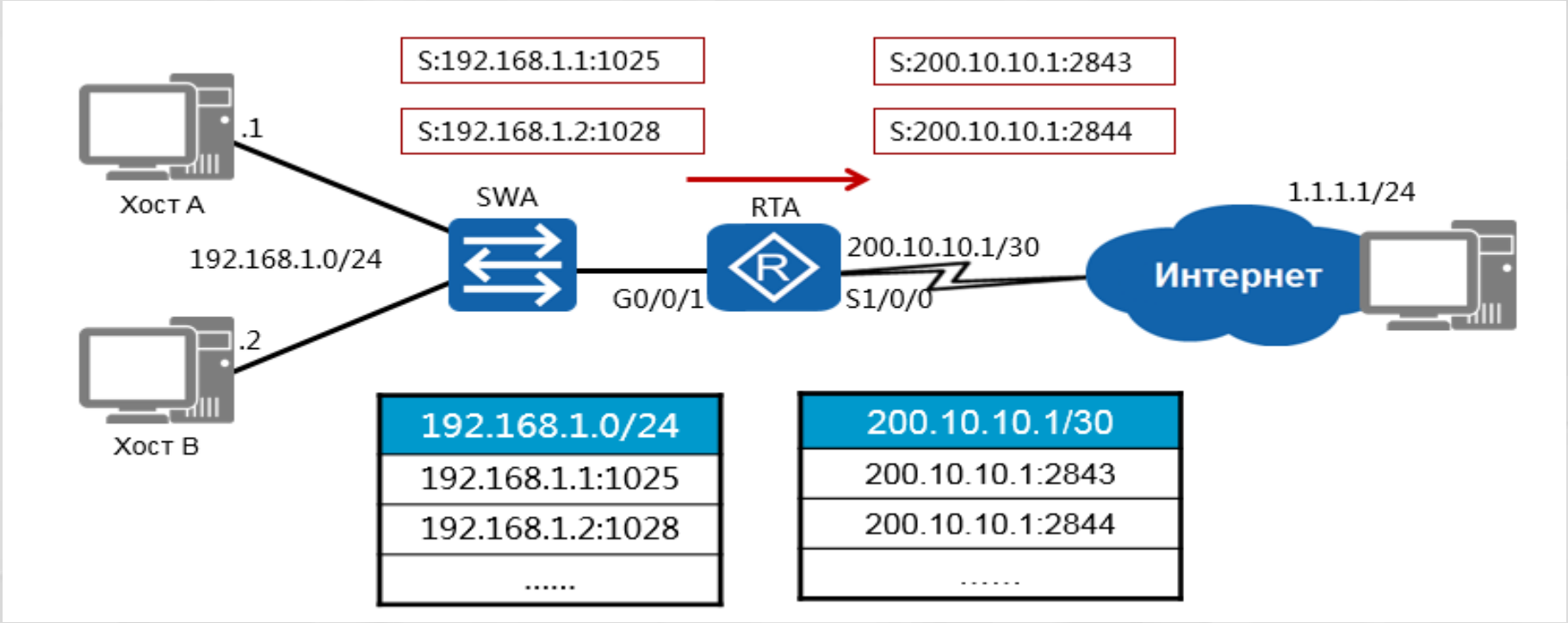
- Сопоставление частных адресов на базе пула адресных ресурсов.
- Пользователи могут использовать публичные адреса в соответствии с реальной потребностью.

Преобразование сетевых адресов на уровне портов



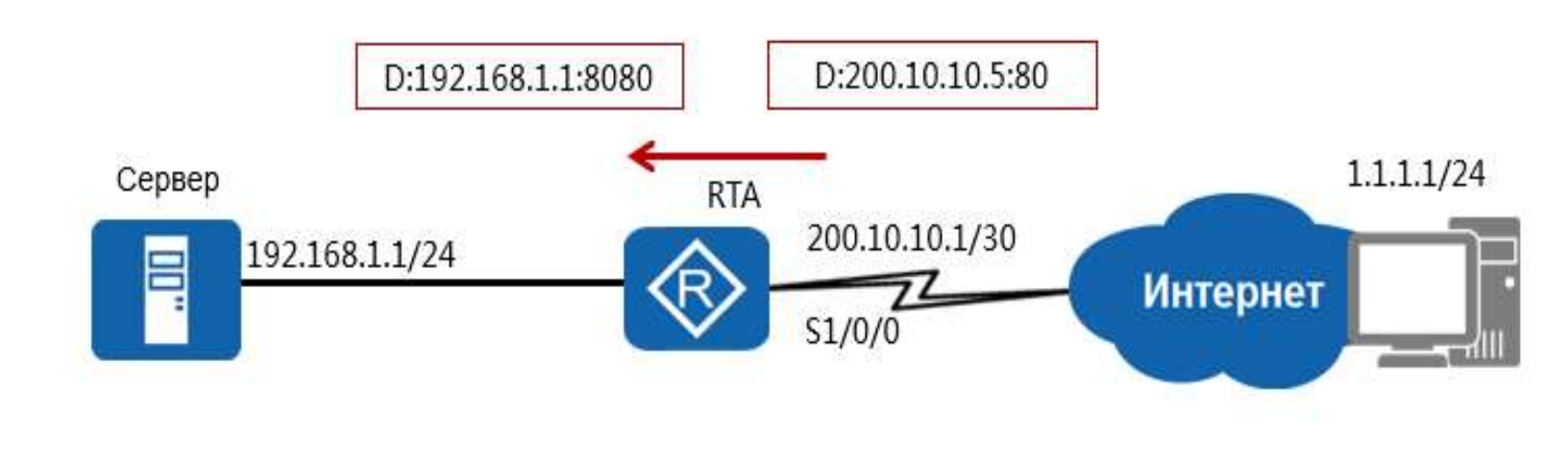
- Номера портов распознают привязку к одному и тому же публичному адресу.

Процесс «Easy IP»



- Адрес интерфейса WAN используется в качестве единого публичного адреса для всех внутренних пользователей, а номера портов используются для различения сеансов.

Внутренний сервер NAT

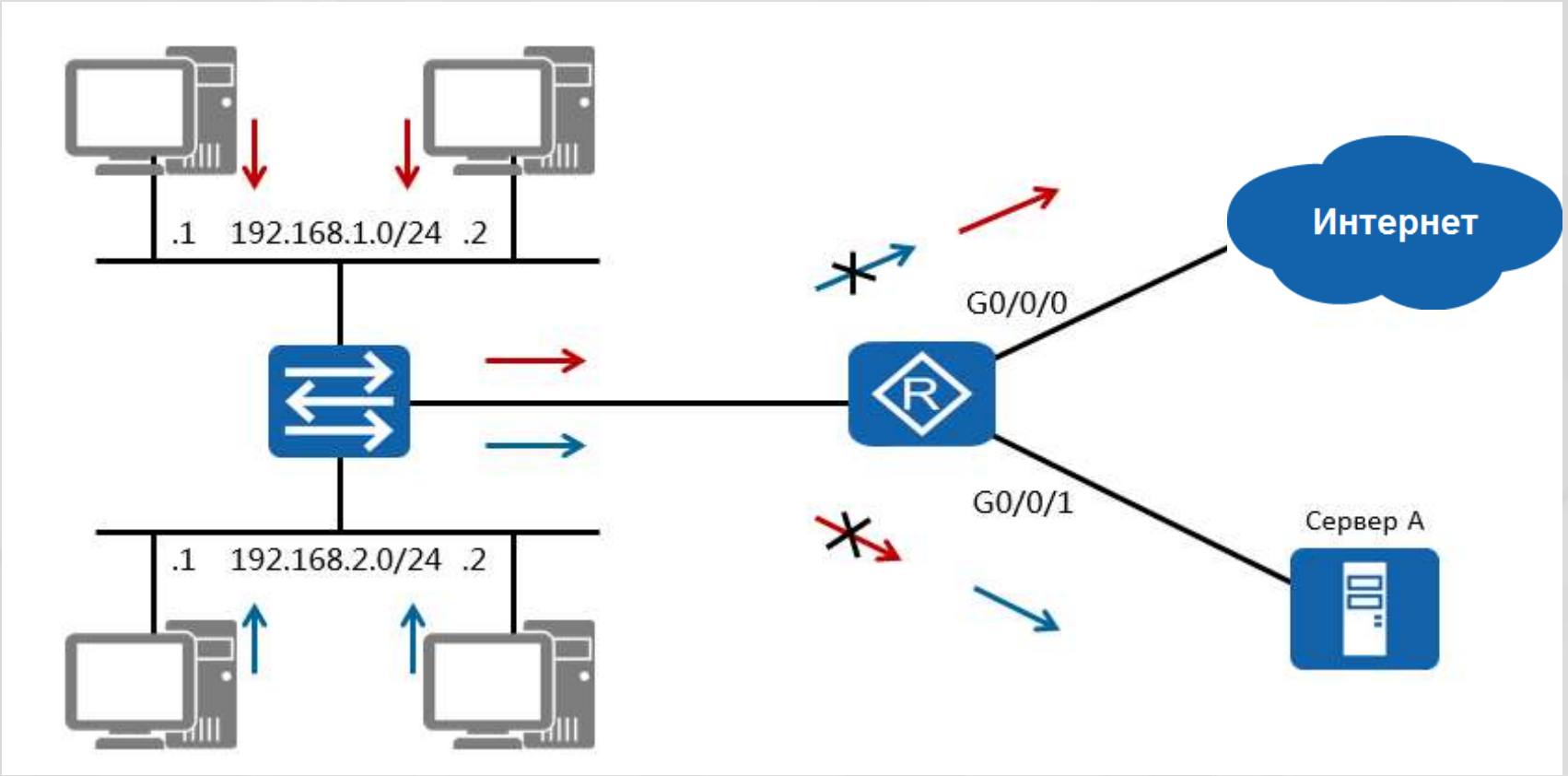


- Внутренние адреса достижимы с внешних источников.
- Сопоставляется как IP-адрес, так и номер порта.

Списки контроля доступа (ACL)

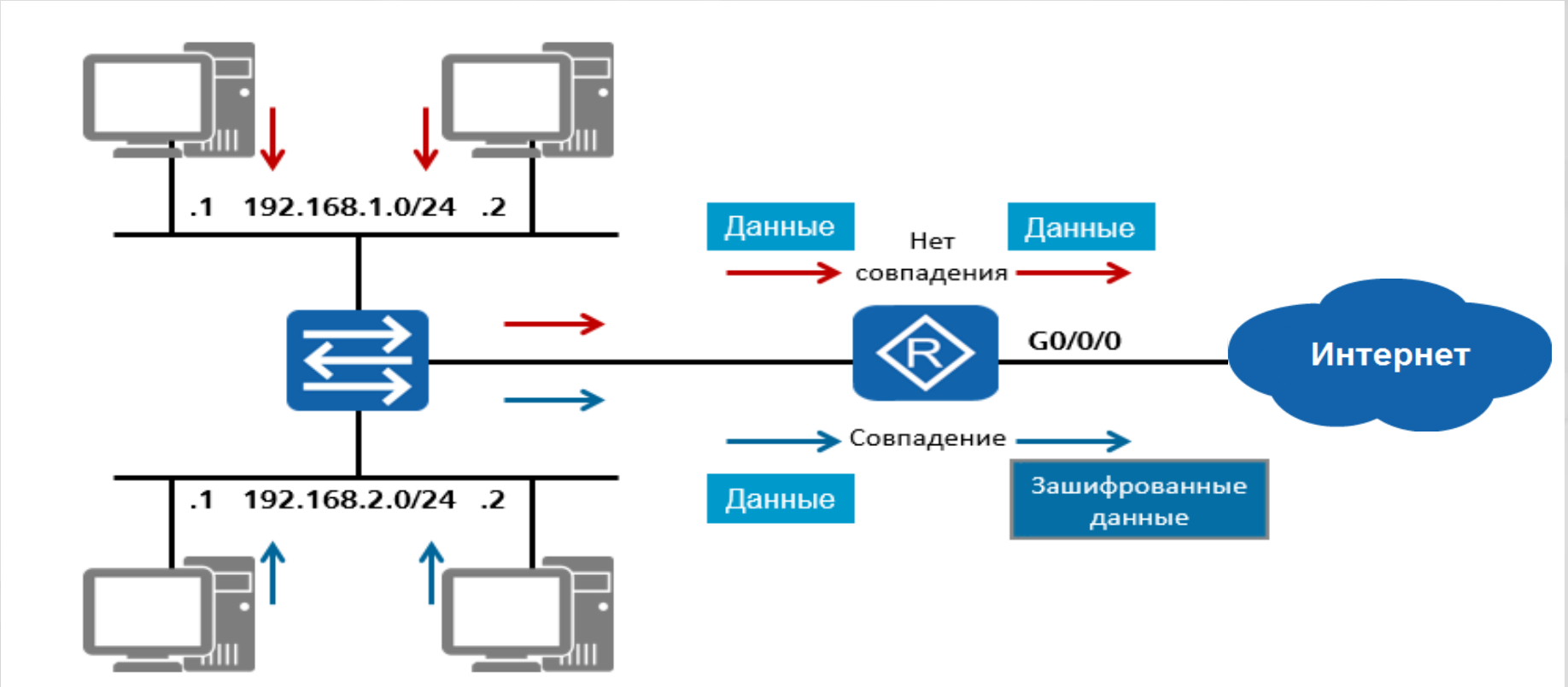
Работа многих технологий и протоколов опирается на списки контроля доступа (ACL), которые используются для более эффективного управления и фильтрации трафика в рамках применяемых мер безопасности или требований приложений. Реализация ACL в таких целях требует точного понимания данной технологии, поэтому этот раздел посвящен описанию общих решений ACL.

Фильтрация трафика



- Фильтрация пакетов осуществляется по адресам и параметрам.
- Правила разрешают или запрещают передачу пакетов в сети.

Фильтрация определенного типа трафика



- Для управления поведением и действиями применяется механизм фильтрации пакетов.
- В результате можно изменить параметры и поведение передачи.

Типы ACL

Типы	Диапазоны значений	Параметры
Basic	2000–2999	IP-адрес источника
Advanced	3000–3999	IP-адрес источника и пункта назначения, протокол, источник и порт назначения
Layer 2 ACL	4000–4999	MAC-адрес

- В маршрутизаторах серии AR2200 используется три типа ACL.
- У каждого типа ACL имеются свои параметры фильтрации пакетов.

СОРМ - система оперативно-розыскных мероприятий

«СОРМ-1» — система прослушивания телефонных переговоров, организованная в 1996 году;

«СОРМ-2» система протоколирования обращений к сети Интернет

«СОРМ-3» — обеспечивает сбор информации со всех видов связи и её долговременное хранение

ТСПУ - технические средства противодействия угрозам

№	Характеристики	Сервер Huawei (модель)
		Huawei 1288H v5 Тип S1, S2, S7, PostrgeSQL, промежуточного хранения данных, СПФС
1.	Тип и напряжение питания	Блок питания Platinum AC, 550 Вт (AC: от 100 В до 240 В) Блок питания Platinum DC, 1200W (DC: от 48 В до 60 В)
2.	Потребляемая мощность (1+1)	Блок питания Platinum AC, 550 Вт Блок питания Platinum DC, 1200W
3.	Размеры (В х Ш х Г)	Шасси с жесткими дисками 3,5 дюйма: 43×436×748 мм Шасси с жесткими дисками 2,5 дюйма: 43×436×708 мм
4.	Вес	8 x 2,5 HDD - 17,3 кг 4 x 3,5 HDD - 18,4 кг Вес упаковочных материалов: 5 кг
5.	Влажность среды эксплуатации	От 8% до 90%, без конденсации
6.	Температура среды эксплуатации	От 5°C до 30°C
7.	Температура среды хранения	От -40°C до +65°C
8.	Влажность среды хранения	От 5% до 95%, без конденсации
9.	Высота над уровнем моря	до 3000м Примечание: на высоте более 950 м максимальная температура эксплуатации уменьшается на 1°C каждые 300 м
10.	Описание интерфейсов (тип, кол-во)	LOM : 2 x 1Gb + 2 x 10Gb SFP+ 1 x PCIe : 2 x 10Gb SFP+

Коммутация ТСПУ

Коммутатор Eltex (модель)	
Ethernet-коммутатор MES3348, 48 портов 10/100/1000Base-T, 4 порта 10GBase-X(SFP+)/1000Base-X(SFP), L3, 2 слота для модулей питания	Ethernet-коммутатор MES5332A, 1x10/100/1000BASE-T (OOB), 32x10GBASE-R (SFP+)/1000BASE-X (SFP), коммутатор L3, 2 слота для модулей питания

Электропитание ТСПУ

Обходной переключатель (байпас), Silicom		
IBS Байпас модульный, 4 слота для внешних модулей, 2 резервируемых источника питания	**IS40** Байпас модульный, 2-го поколения, 3 слота для внешних модулей, 2 резервируемых источника питания	**IS100** Байпас модульный, 4-го поколения, 2 слота для внешних модулей, 2 резервируемых источника питания

Пропускная способность

Модуль оптический FT-QSFP28 LR4 (100Gb, SM, 10km, Tx1310nm, LC, DDM)	**Модуль оптический FT-QSFP28 SR4 (100Gb, MM, 100M, Tx850nm, MPO, DDM)**	**Модуль оптический FT-QSFP+-LR4-PSM (QSFP+, 40Gb/s, 10km, Tx1310nm, MPO/MTP, SM, DDM)**
QSFP28	QSFP28	QSFP+
10 km	100m,@OM4	10 km (SMF)