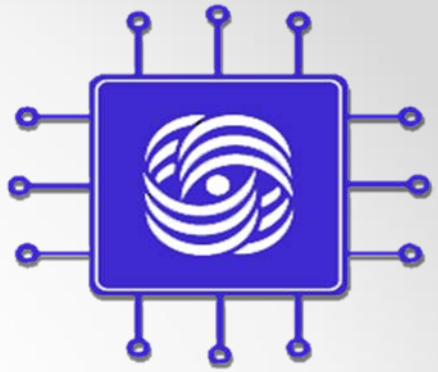


Прикладной уровень

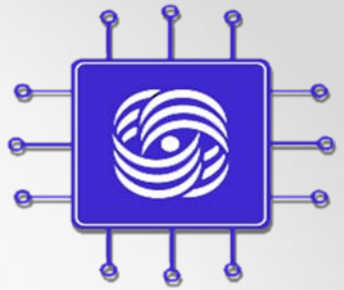
(Компьютерные сети т.2 стр.182-216)

Введение в компьютерные сети

чл.-корр. РАН Смелянский Р.Л.
Кафедра АСВК
ф-т ВМК МГУ

Прикладной уровень

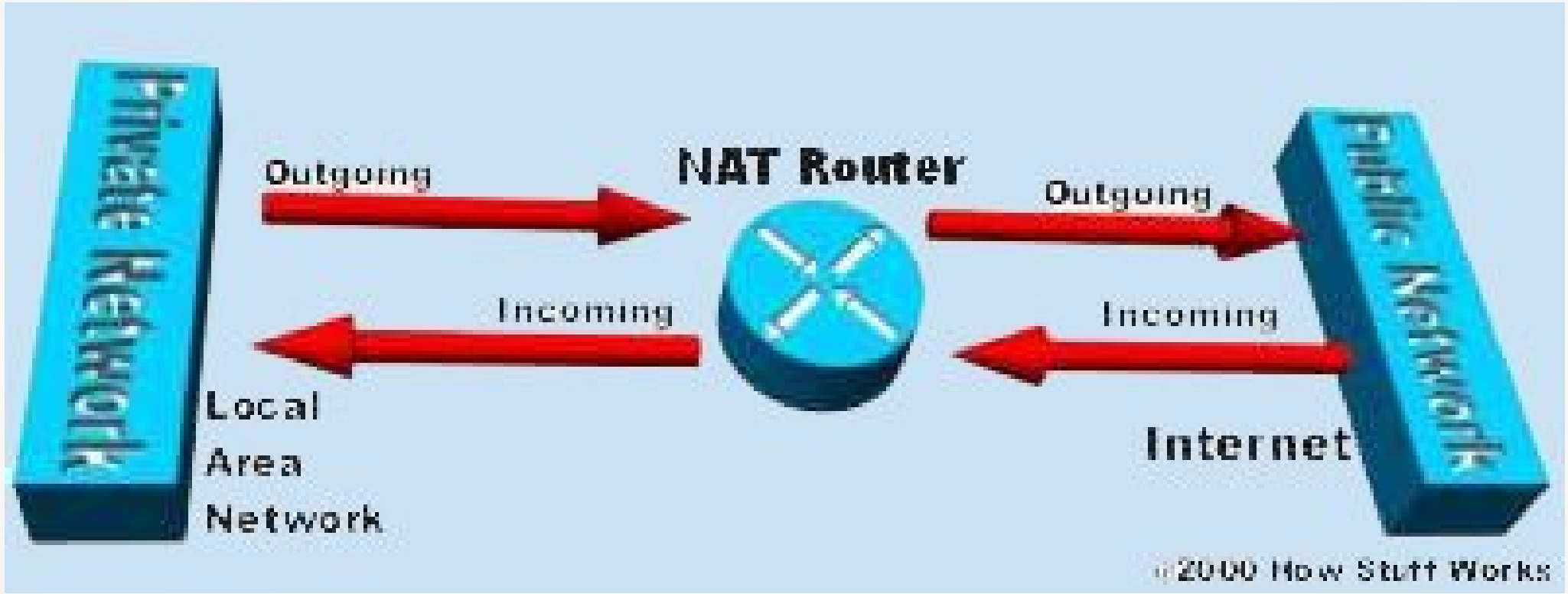
- NAT - Network Address Translation
- DNS - Domain Name Service
- HTTP - Hyper Text Transfer Protocol
- SNMP - Simple Network Management Protocol
- SMTP - Simple Mail Transfer Protocol
- FTP - File Transfer Protocol



NAT – Network Address Translation

(NAT описан в RFC 1631, RFC 3022)

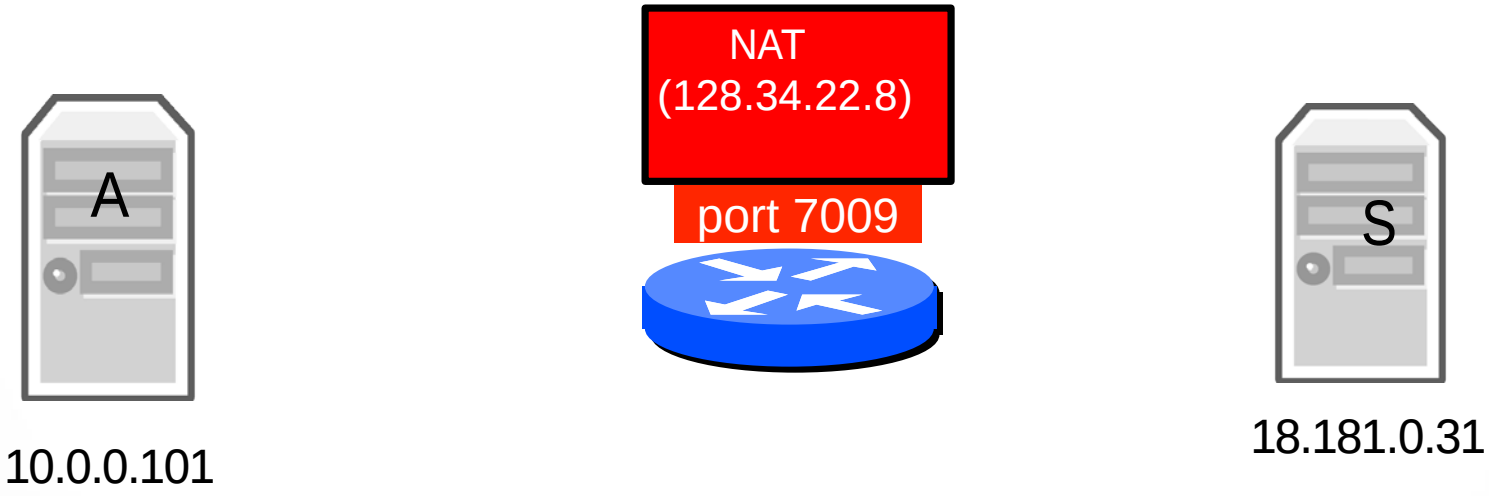
Как работает NAT



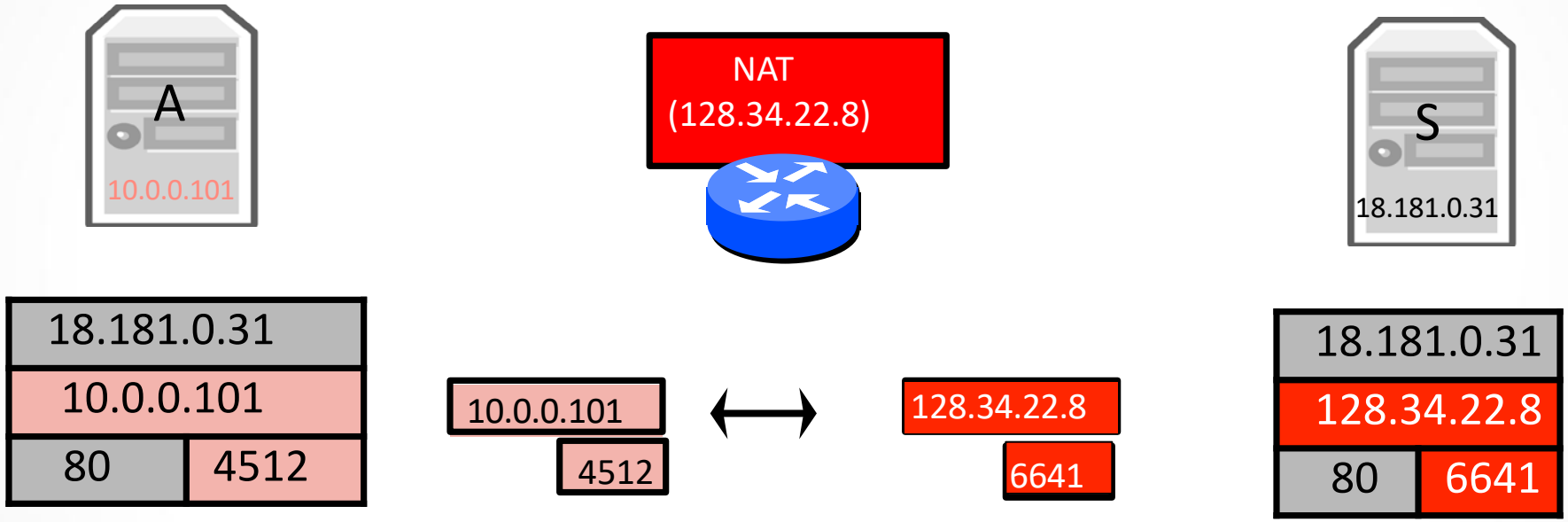
Виды отображения, реализуемые нагруженным NAT

- **Статический NAT**
- **Cone NAT, Full Cone NAT**
- **Address-Restricted cone NAT (Restricted cone NAT)**
- **Port-Restricted cone NAT**
- **Симметричный NAT** (Symmetric NAT)
- Терминология и типизация NAT по RFC3489

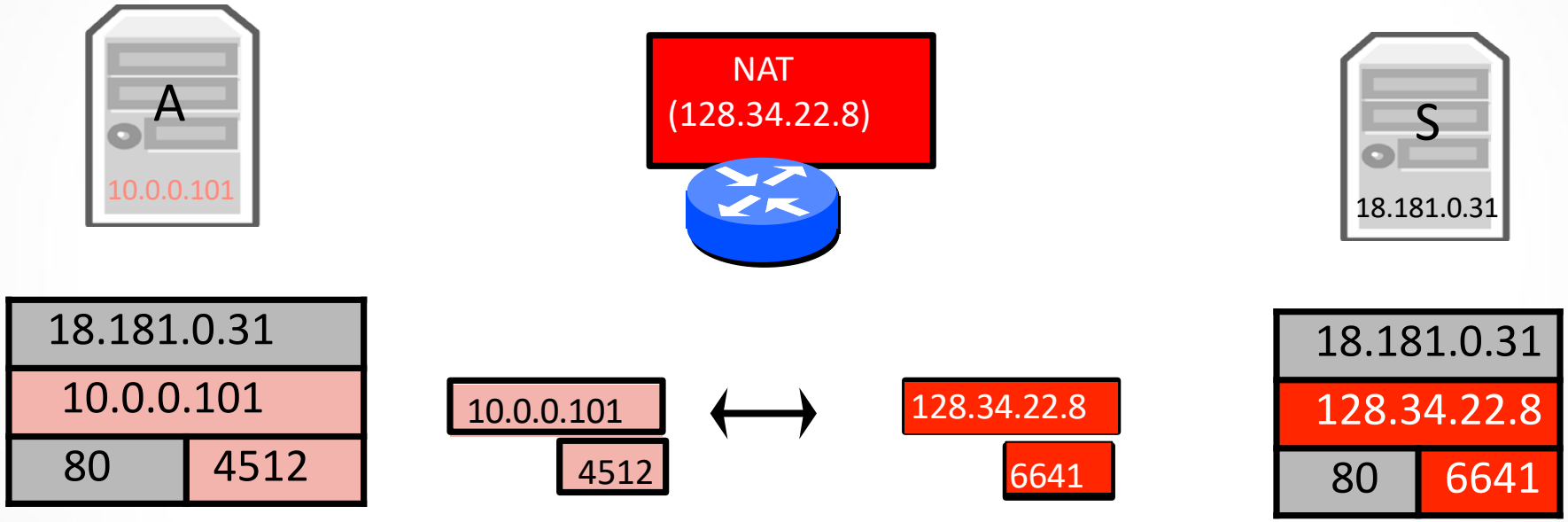
Статический NAT



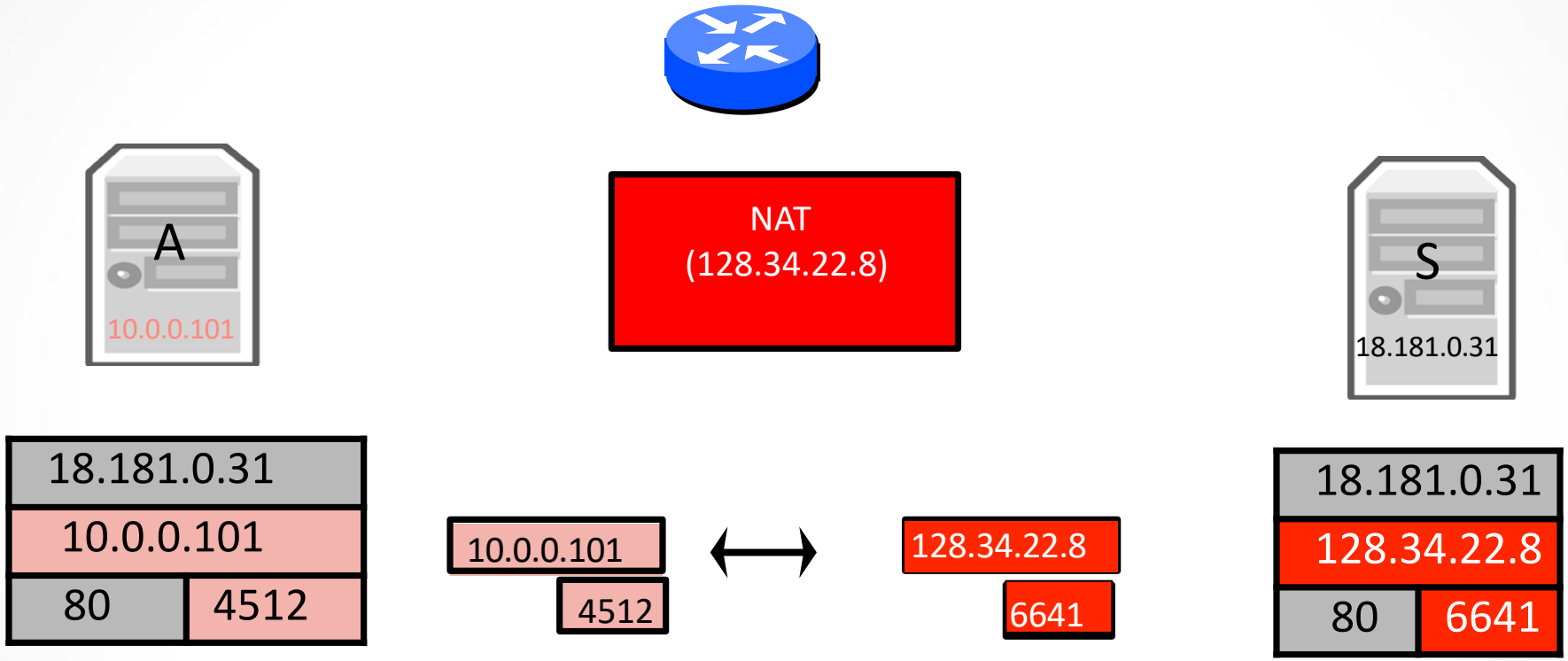
Full Cone (FC) NAT



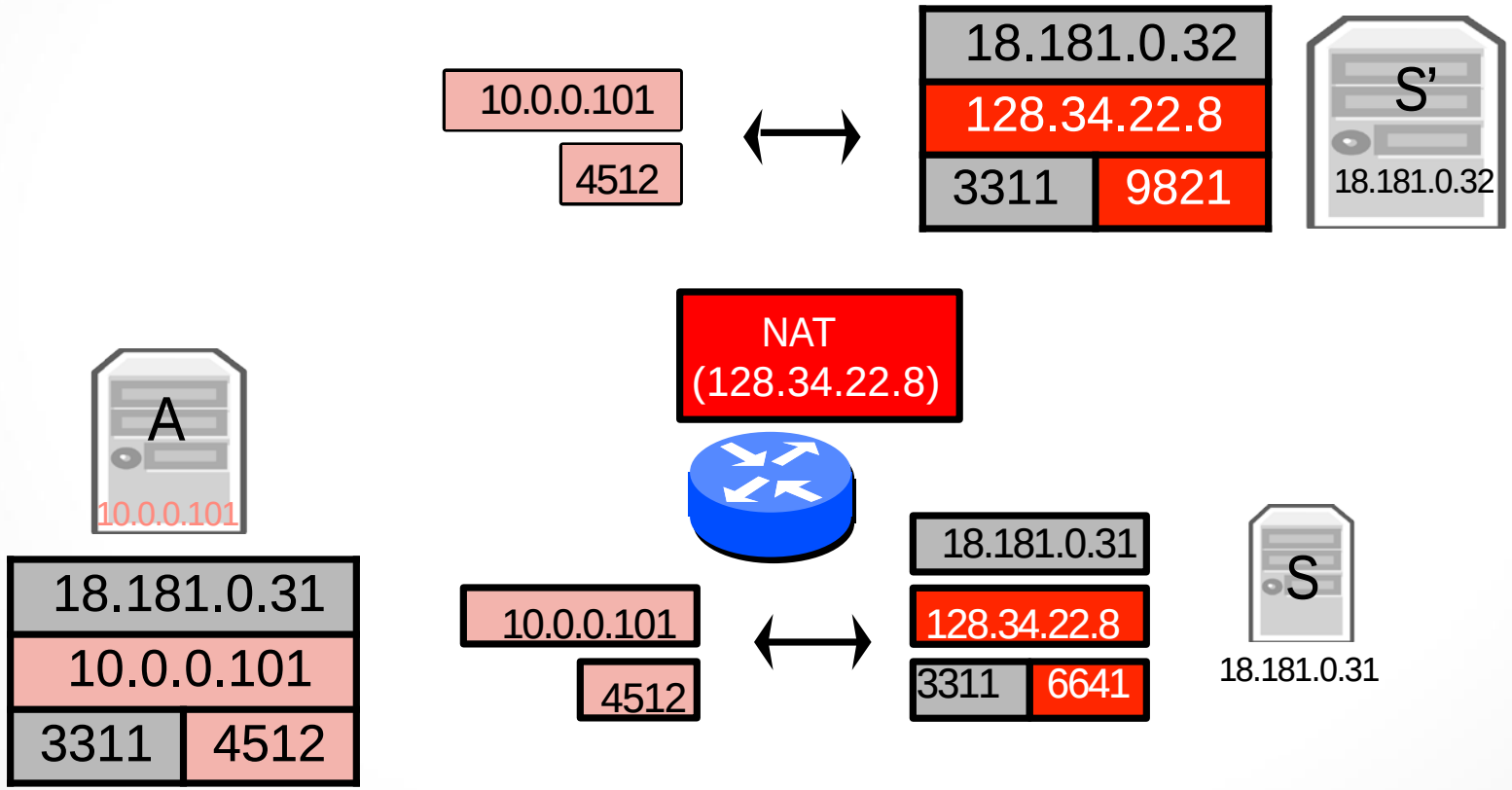
Restricted Cone (RC) NAT



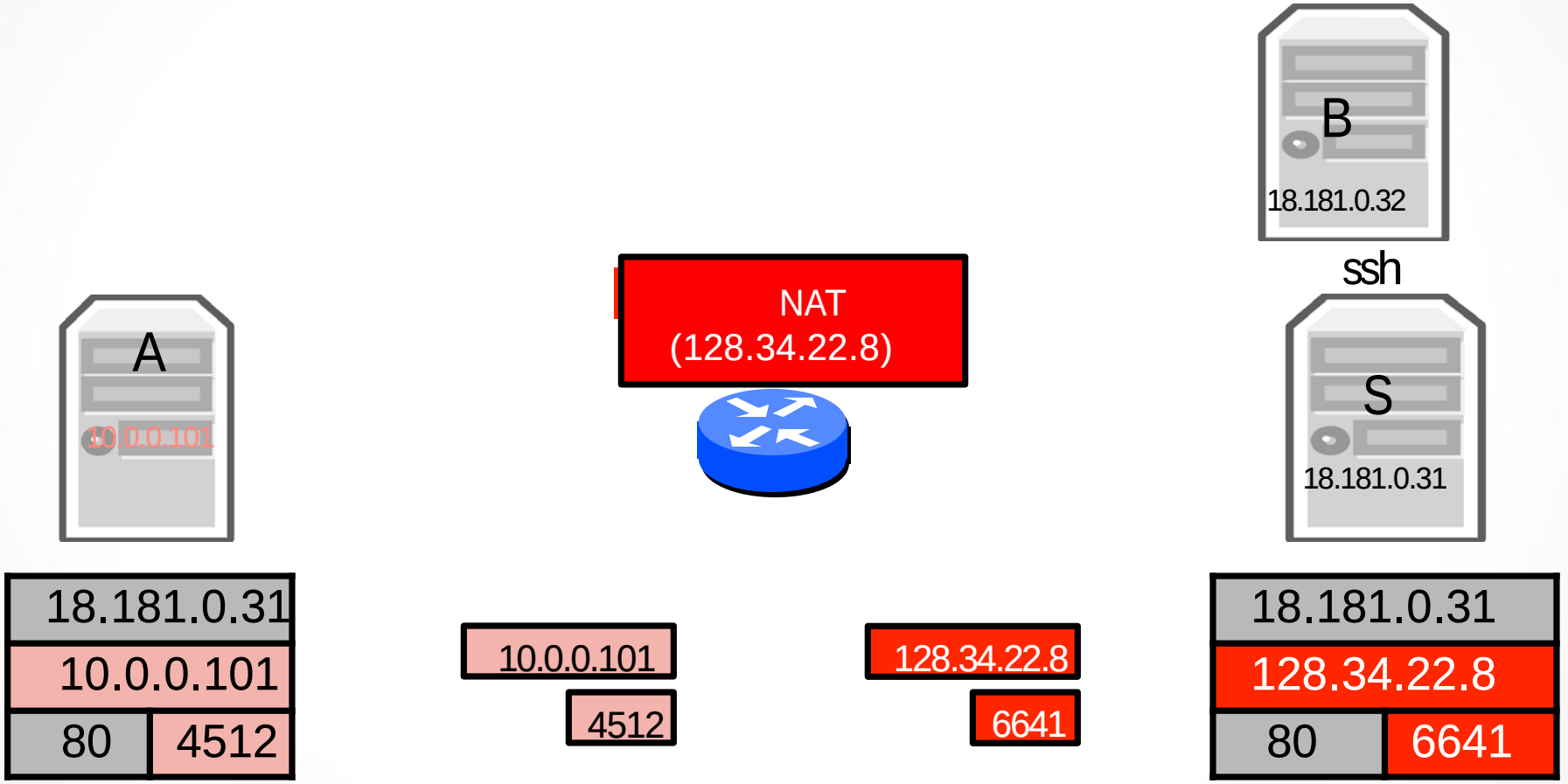
Port Restricted (PR) NAT



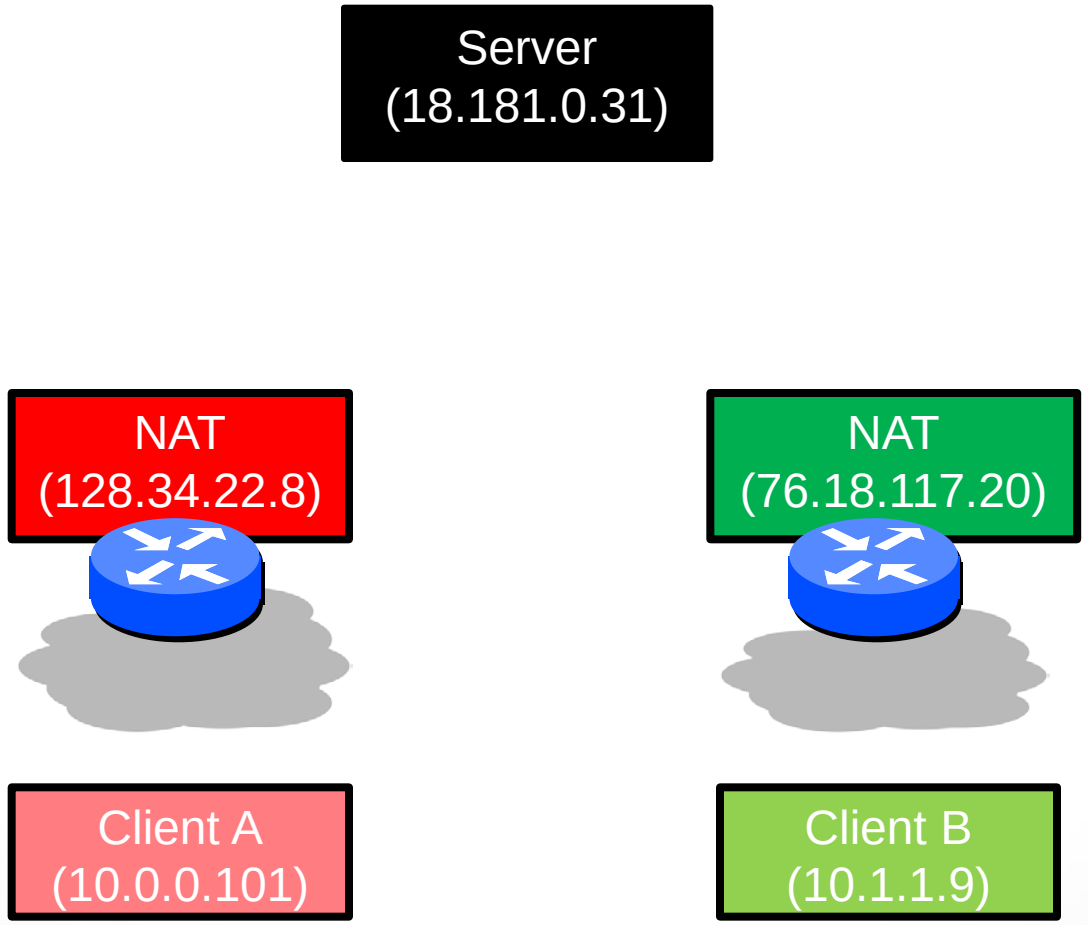
Symmetric NAT



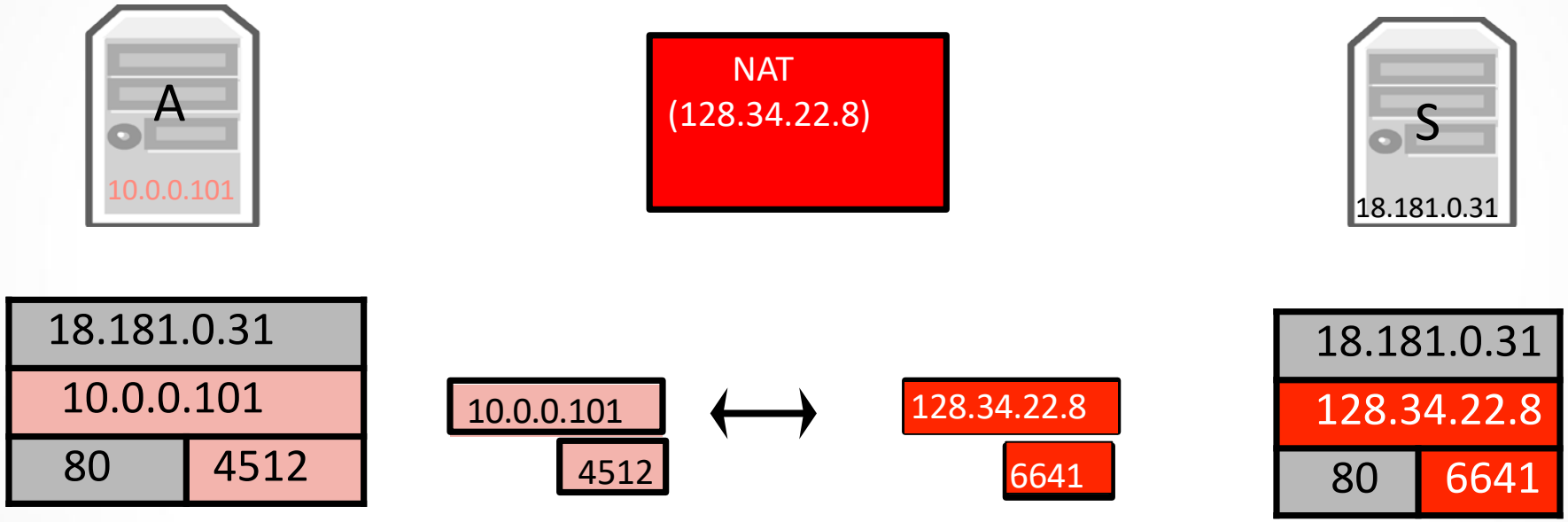
Влияние NAT на приложения: входящие соединения



Приложение: NAT перфоратор (hole-punching)

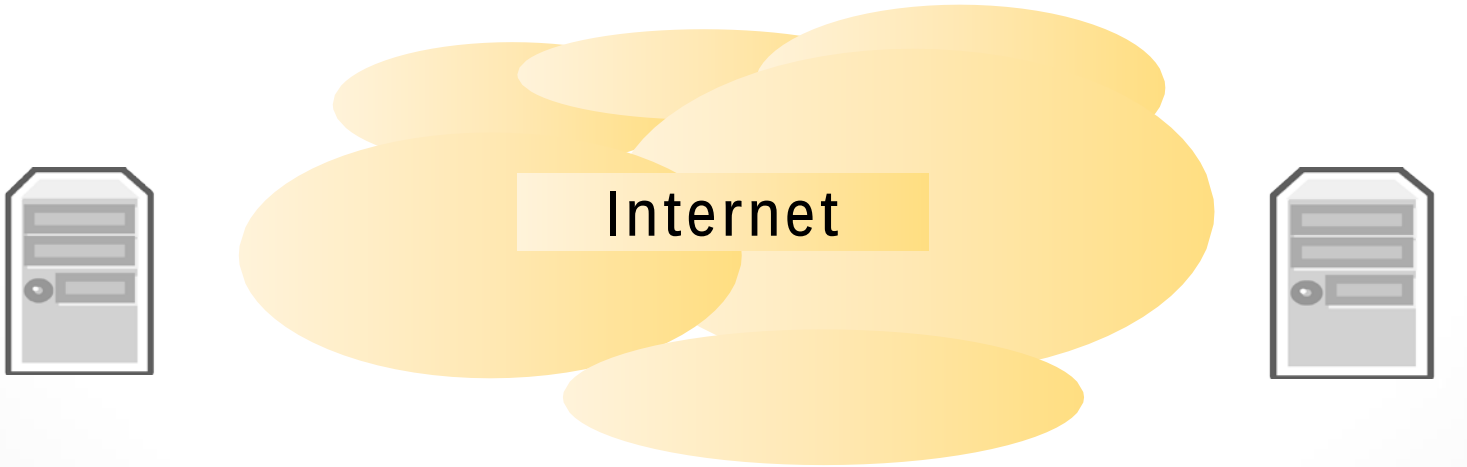


NAT = Нет новому Транспорту!



Strong End-to-End

"The network's job is to transmit datagrams as efficiently and flexibly as possible. Everything else should be done at the fringes."

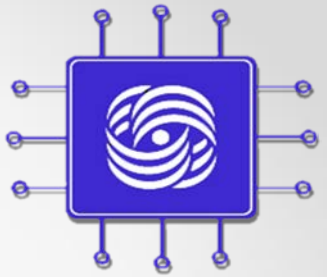


NAT выполняет три важных функции

- *Позволяет сэкономить IP-адреса, транслируя несколько внутренних IP-адресов в один внешний публичный IP-адрес (или в несколько, но меньшим количеством, чем внутренних).*
- *Позволяет предотвратить или ограничить обращение снаружи к внутренним хостам, оставляя возможность обращения из внутренней сети во внешнюю. Если для пакетов, поступающих из внешней сети, соответствующей трансляции не существует (а она может быть созданной при инициации соединения или статической), они не пропускаются.*
- *Позволяет скрыть определённые внутренние сервисы внутренних хостов/серверов. Тем самым, снаружи, на внешнем IP-адресе после трансляции адресов на сайт (или форум) для осведомлённых посетителей можно будет попасть по адресу http://dlink.ru:54055, но на внутреннем сервере, находящимся за NAT, он будет работать на обычном 80-м порту.*

Однако следует упомянуть и о недостатках данной технологии:

- *Не все протоколы могут "преодолеть" NAT.*
- *Из-за трансляции адресов "много в один" появляются дополнительные сложности с идентификацией пользователей и необходимость хранить полные журналы записей о трансляциях.*
- *Атака DoS со стороны узла, реализующего NAT – если NAT используется для подключения многих пользователей к одному и тому же сервису, это может вызвать иллюзию DoS-атаки на сервис (множество успешных и неуспешных попыток).*
- *Дебатировать NAT можно, но бесполезно – он есть!*



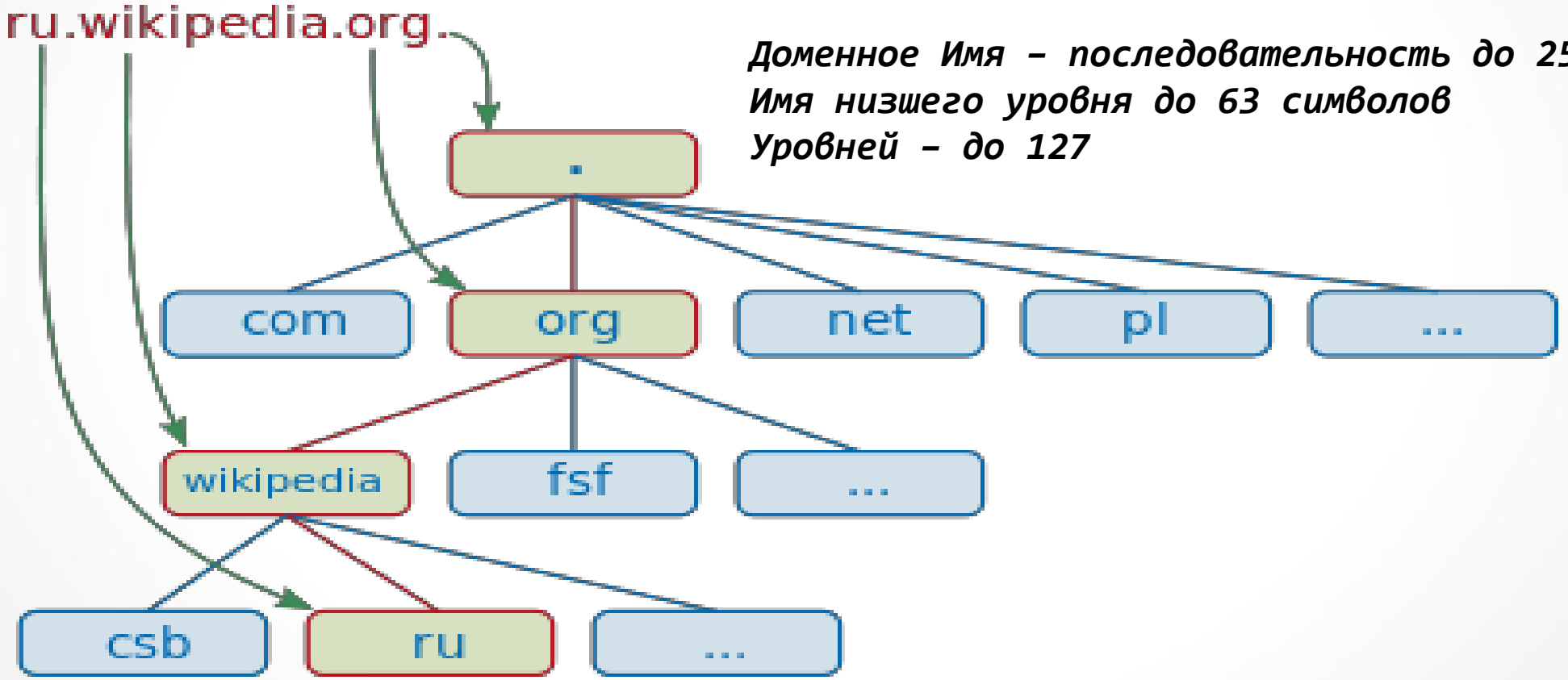
DNS – Domain Name Service

DNS

- *Задача:*
  - *сопоставление символического имени IP адресу*
  - *автоматическая резолюция адресов*
  - *DNS (Domain Name System)*
  - *распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Internet*
  - *механизм взаимодействия машин в сети Internet с этой базой данных*

DNS: структура имен

- Иерархическая древовидная структура имен

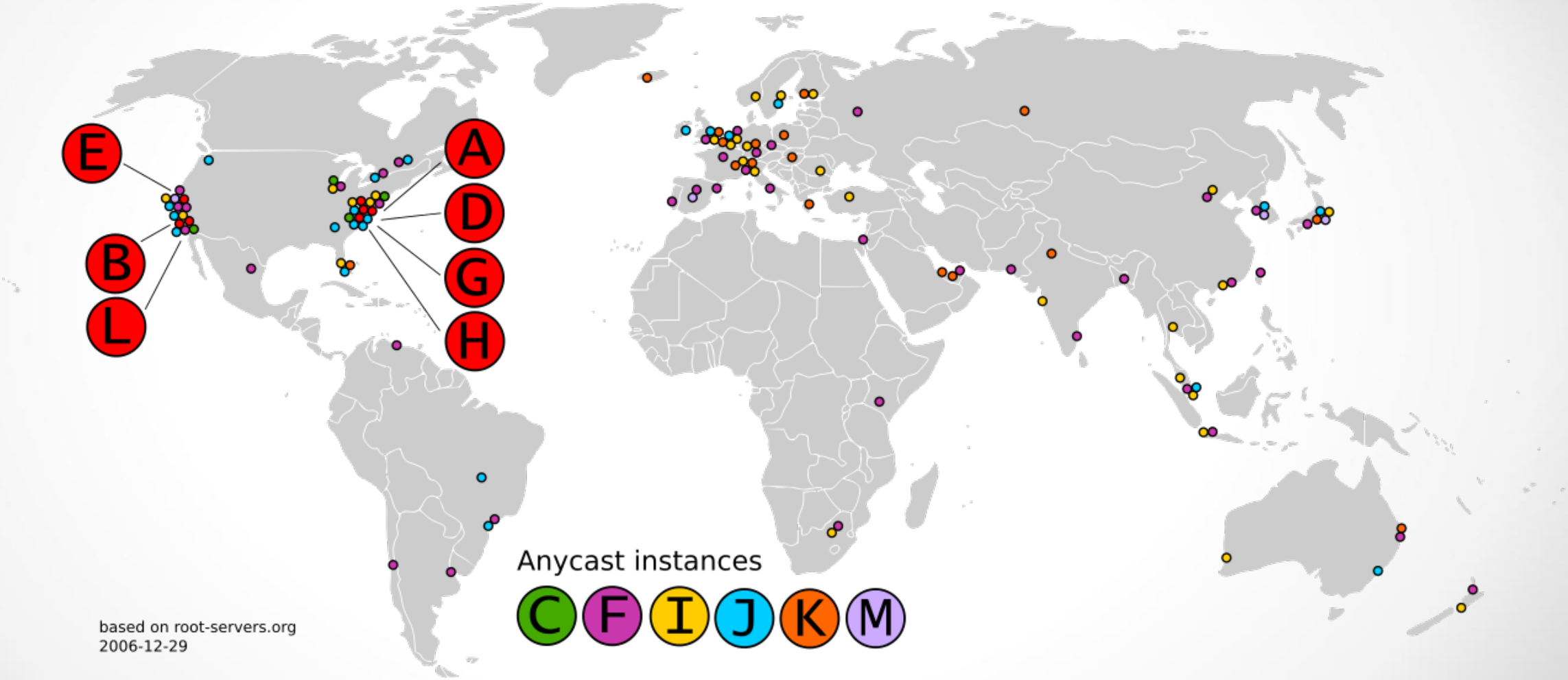


Доменное Имя – последовательность до 254 символов
Имя низшего уровня до 63 символов
Уровней – до 127

Стандартизованные суффиксы имен

Поле адреса	Тип сети
.aero	Фирма или организация, относящаяся к сфере авиации;
.arts	Культура и досуг;
.biz	Организация, относящаяся к сфере бизнеса;
.com	Коммерческая организация;
.coop	Кооперативная организация;
.firm	Коммерческое предприятие;
.gov	Государственное учреждение (США);
.info	Открытая TLD-структура (регистрация имен доменов)
.org	Бесприбыльная организация;
.edu	Учебное заведение;
.jobs	Работодатели;
.mil	Военное предприятие или организация (США);
.mobi	Сайты и сервисы, ориентированные на работу с мобильными телефонами и беспроводными устройствами
.museum	Имя домена музея
.name	Имя домена частного лица
.net	Большая сеть;
.pro	Профессионал, достойный доверия. Управляется RegistryPro (http://www.nic.pro/);
.int	Международная организация;
.rec	Развлечения;
.tel	Хранение и управление персональными и корпоративными контактными данными;
.travel	Турагенства;
.tv	Телевидение. Хотя существует домен bbc.tv, а регистрация в этой зоне в РФ процветает (см. Ru center, официального статуса в качестве TLD этот домен не получил. В базе данных IANA (см. Национальные коды доменов в Интернет этот домен записан попрежнему за TUVALU
.arpa	Специальный домен, используемый для преобразования IP-

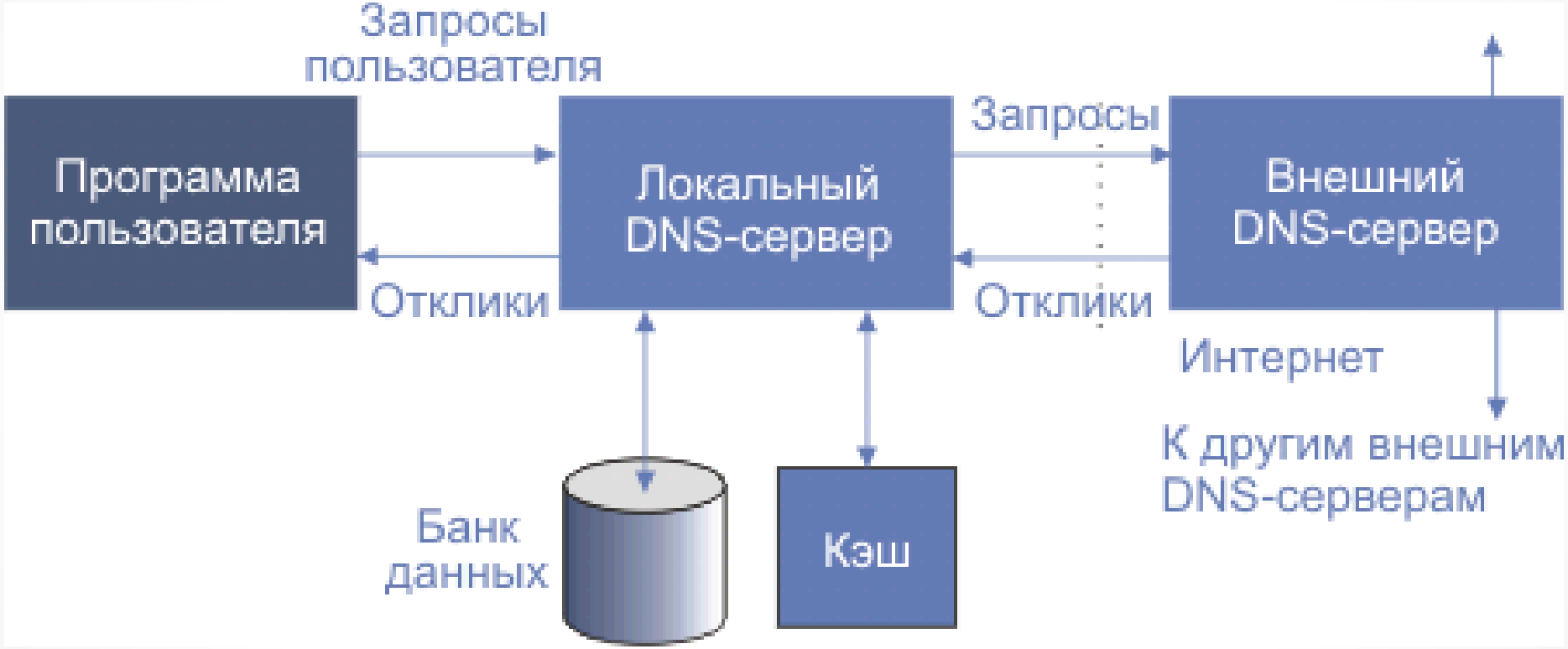
Географическое расположение корневых серверов DNS



DNS: основные понятия

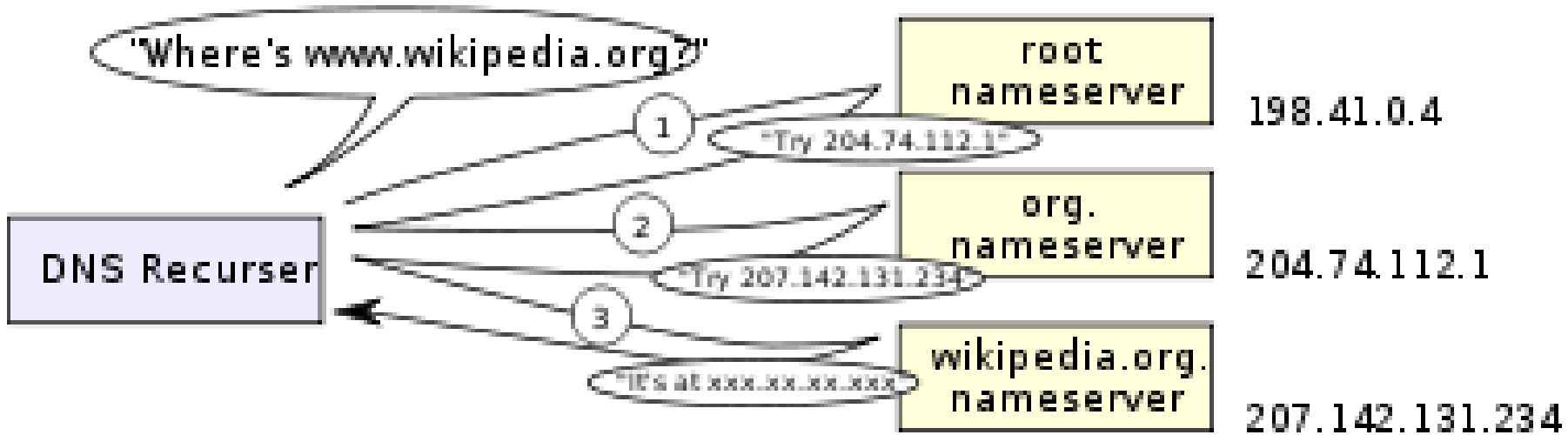
- ***Домен*** *– узел и связанное поддерево в иерархической структуре имен*
- ***Ресурсная запись*** *– единица хранения информации*
- ***DNS-сервер*** *и* ***DNS-клиент***
- ***DNS-запрос***
- ***Зона*** *– часть поддерева домена вместе с ресурсными записями*
- ***Делегирование*** *– передача ответственности за зону отдельному серверу*

Структура организации работы DNS приложения



DNS: пример рекурсивной резолюции адреса

Рекурсивное или итеративное поведение



DNS: ресурсная запись

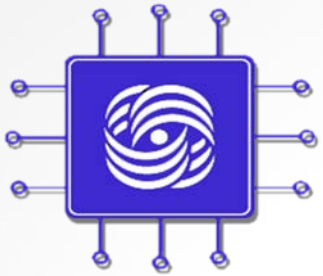
- *имя (NAME) – доменное имя, к которому привязана данная ресурсная запись*
- *TTL (Time To Live) – допустимое время хранения данной ресурсной записи в кэше неответственного **DNS-сервера***
- *тип (TYPE) ресурсной записи – определяет формат и назначение данной ресурсной записи*
- *поле данных (RDATA), формат и содержание которого зависит от типа записи.*

DNS: типы ресурсных записей

- ***Запись A*** *(address record) или* ***запись адреса*** *связывает имя хоста с адресом IP*
- ***Запись AAAA*** *(IPv6 address record) связывает имя хоста с адресом протокола IPv6*
- ***Запись CNAME*** *(canonical name record) или* ***каноническая запись имени*** *(псевдоним) используется для перенаправления на другое имя*
- ***Запись MX*** *(mail exchange) или* ***почтовый обменник*** *указывает сервер(ы) обмена почтой для данного домена*
- ***Запись NS*** *(name server) указывает на DNS-сервер для данного домена*
- ***Запись PTR*** *(pointer) или* ***запись указателя*** *связывает IP хоста с его каноническим именем*
- ***Запись SOA*** *(Start of Authority) или* ***начальная запись зоны*** *указывает, на каком сервере хранится эталонная информация о данном домене, содержит контактную информацию лица, ответственного за данную зону*
- ***Запись TXT*** *содержит не интерпретируемую текстовую информацию*

DNS: заключительные замечания

- *Доменная система именования указывает на то, кто ответственен за поддержку имени, но не где эта машина находится (несмотря на коды стран)*
- *Понятия доменного имени и адрес сети вообще говоря не связаны: две машины одного домена имен могут не принадлежать к одной сети*
- *У машины может быть много имен. В частности, это верно для машин, предоставляющих какие-либо услуги, которые в будущем могут быть помещены под опеку другой машины*



SMTP – Simple Mail Transfer Protocol

Организация служб в социуме и в цифровом пространстве

Архитектура и сервисы E-mail

- *Объединение агента пользователя (чтения/формирования сообщения) и агента передачи сообщений*
- *Основные функции почтовой службы*
  - ***Композиция*** *– обеспечивает создание сообщений и ответов*
  - ***Передача*** *– обеспечивает передачу сообщения от отправителя к получателю без вмешательства пользователей*
  - ***Отчет*** *перед отправителем о доставке*
  - ***Отображение*** *сообщения, включая вопросы форматирования и кодировки*
  - ***Размещение*** *– вопросы хранения сообщений, поиска среди них, повторной отправки или переадресации и т.п.*

E-mail: элементы краткого заголовка сообщения

- ***Return-Path*** *– обратный адрес*
- ***Received*** *– строчка журналирования прохождения письма. Каждый почтовый сервер (MTA) помечает процесс обработки этим сообщением*
- ***Формат тела: MIME-Version*** *– версия MIME, с которым это сообщение создано*
- ***From:*** *– Имя и адрес отправителя.*
- ***Sender:*** *– Отправитель письма. Добавлено для возможности указать, что письмо от чьего-то имени (from) отправлено другой персоной (например, секретаршей от имени начальника)*
- ***To:*** *– Имя и адрес получателя. Может содержаться несколько раз (если письмо адресовано нескольким получателям). Может не совпадать с полем SMTP RCPT TO*
- ***cc:*** *– (от carbon copy). Содержит имена и адреса вторичных получателей письма, к которым направляется копия*
- ***bcc:*** *– (от blind carbon copy). Содержит имена и адреса получателей письма, чьи адреса не следует показывать другим получателям. Это поле обычно обрабатывается почтовым сервером (и приводит к появлению нескольких разных сообщений, у которых bcc содержит только того получателя, кому фактически адресовано письмо).*

E-mail: полный заголовок сообщения содержит

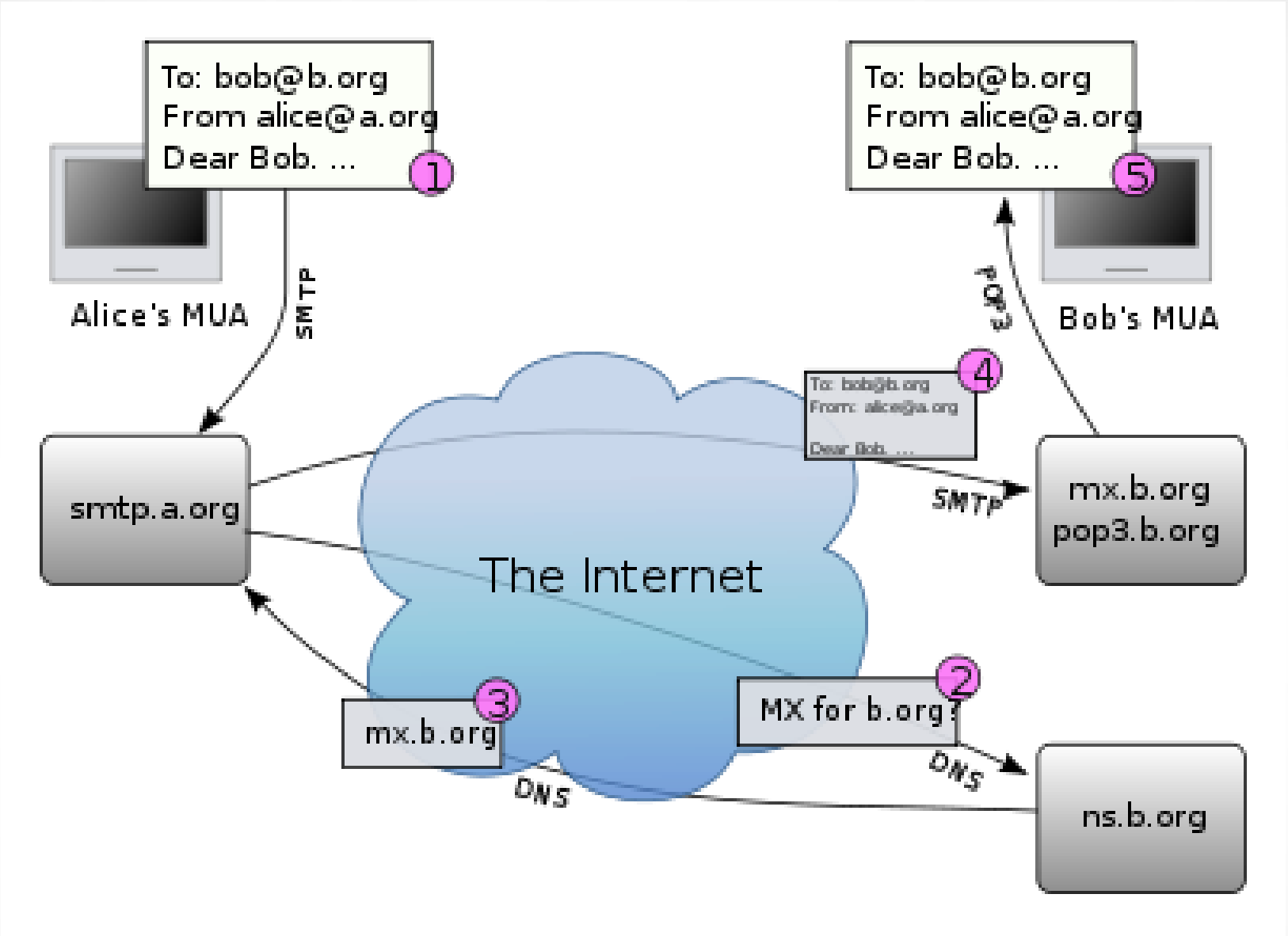
- ***Reply-To:*** *– имя и адрес, куда следует адресовать ответы на это письмо. Если, например, письмо рассылается ботом, то в качестве Reply-To будет указан адрес персоны, готовой принять ответ на письмо*
- ***Message-ID:*** *– уникальный идентификатор сообщения. Состоит из адреса узла-отправителя и номера (уникального в пределах узла). Выглядит примерно так: AAB77AA2175ADD4BACECE2A49988705C0C93BB7B4A@example.com. Вместе с другими идентификаторами используется для поиска прохождения конкретного сообщения по журналам почтовой системы и для указания на письмо из других писем*
- ***Content-Type:*** *– тип содержимого письма. С помощью этого поля указывается тип (HTML, RTF, Plain text) содержимого письма и кодировка, в которой создано письмо*
- ***In-Reply-To:*** *– указывает на Message-ID, для которого это письмо является ответом (с помощью этого почтовые клиенты могут легко выстраивать цепочку переписки)*
- ***Date:*** *– дата написания письма*

MIME – Multipurpose Internet Mail Extension

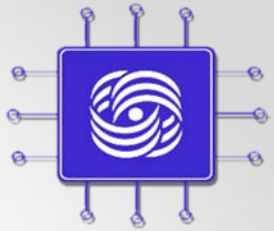
- *Поддержка*
  - *Различных алфавитов, включая нелатинские*
  - *Передачи нетекстовых данных*

E-mail: передача почтовых сообщений

- ***SMTP (Simple Mail Transfer Protocol)*** *– передача письма между почтовыми серверами*
- ***Для взаимождействия почтового агента с сервером:***
  - ***POP3 (Post Office Protocol)*** *– простой протокол для изъятия почты из удаленного почтового ящика . Он позволяет забирать почту с сервера и хранить ее на машине пользователя*
  - ***IMAP (Interactive Mail Access Protocol)*** *– позволяет одному и тому же пользователю заходить с разных машин на сервер, чтобы прочесть, отправить почту*
- ***Почтовый ящик*** *vs.* ***Почтовый терминал***
- *Сервера* ***передачи сообщений*** *vs. Сервера* ***хранения сообщений***



- PGP и PEM - распространенные безопасные почтовые системы



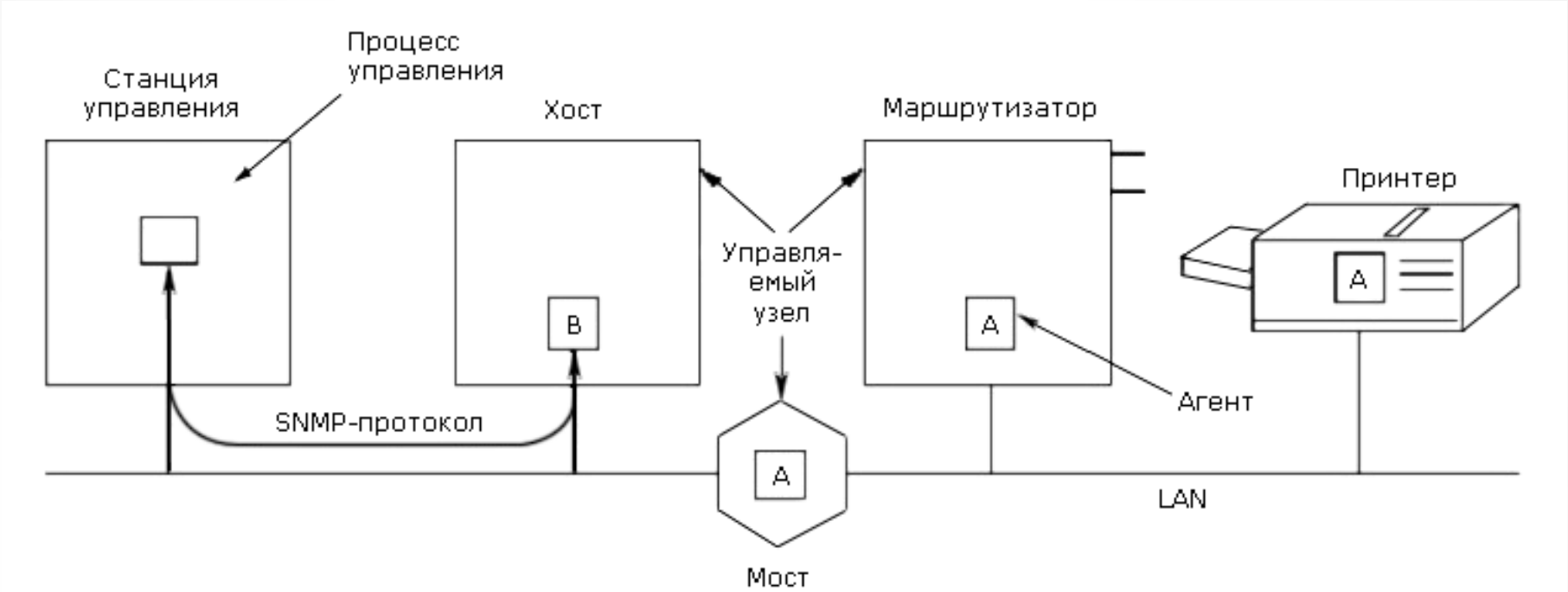
SNMP - Simple Network Management Protocol

SNMP

- ***Задача:***
  - *удаленное унифицированное управление сетевыми устройствами*

- ***SNMP (Simple Network Management Protocol)***
  - *Сбор информации о параметрах конфигурации сетевых устройств*
  - *Изменение некоторых параметров конфигурации*

Модель управления в SNMP



Управляемое устройство

Агент – программное обеспечение, запускаемое на управляемом устройстве, либо на устройстве, подключенном к интерфейсу управления управляемого устройства

Система управления сетью (Network Management System - NMS) – приложение, отслеживающее и контролирующее состояние управляемого устройства с помощью своего агента

SNMP: Управляющая информация

- *SNMP не специфицирует, какая именно информация должна предоставляться управляемым устройством*
- *Используется расширяемая иерархическая система представления информации в ASN.1 нотации*
- *Агент обеспечивает:*
  - *Удаленное взаимодействие управляемого устройства с NMS сервером*
  - *Трансляцию и представление управляющей информации*

SNMP: протокол взаимодействия и его команды

Команды SNMP

Команда SNMP	Тип PDU	Назначение
GET-request	0	Получить значение указанной переменной или информацию о состоянии сетевого элемента;
GET_next_request	1	Получить значение переменной, не зная точного ее имени (следующий логический идентификатор на дереве MIB);
SET-request	2	Присвоить переменной соответствующее значение. Используется для описания действия, которое должно быть выполнено;
GET response	3	Отклик на GET-request, GET_next_request и SET-request. Содержит также информацию о состоянии (коды ошибок и другие данные);
TRAP	4	Отклик сетевого объекта на событие или на изменение состояния.
GetBulkRequest	5	Запрос пересылки больших объемов данных, например, таблиц.
InformRequest	6	Менеджер обращает внимание партнера на определенную информацию в MIB.
SNMPv3-Trap	7	Отклик на событие (расширение по отношению v1 и v2).
Report	8	Отчет (функция пока не задана).

FTP – File Transfer Protocol

FTP

- ***Задача:***
  - *доступ к файлам на удаленных машинах*
  - *надежная передача файлов*
  - *независимость клиента от файловой системы удаленной машины*
- ***FTP (File Transfer Protocol)***
  - *протокол передачи файлов по сети*

FTP: Протокол передачи файлов

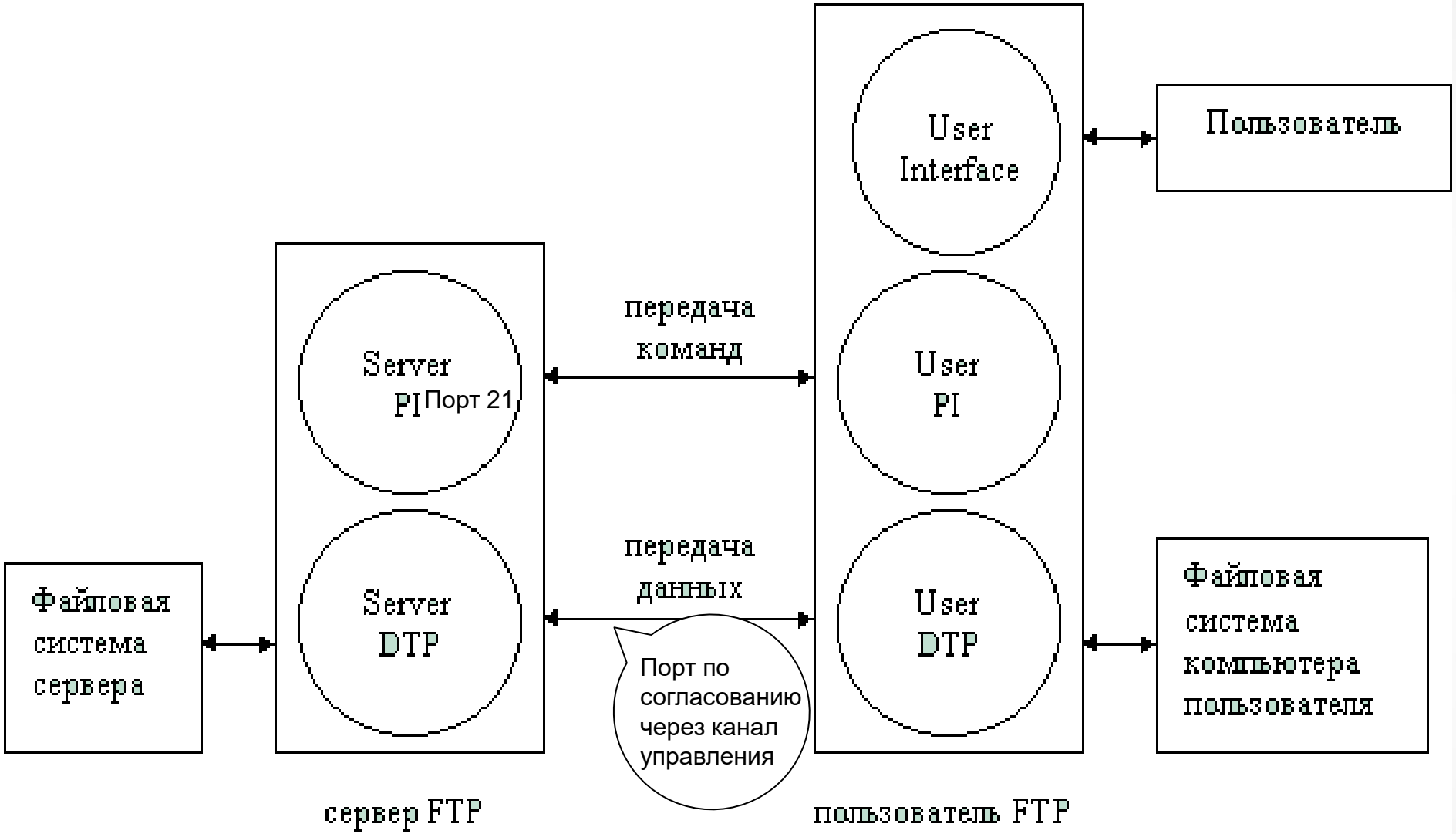
Алгоритм работы протокола FTP:

- Сервер FTP использует в качестве управляющего TCP соединение на порт 21, который всегда находится в состоянии ожидания соединения

- Устанавливают управляющее соединение по порту 21 между модулем "User-PI" и модулем сервера - "Server-PI«
- Клиент начинает отправлять на сервер команды согласования параметров канала передачи данных.
  - FTP-команды определяют параметры соединения передачи данных: роль участников соединения (активный или пассивный), порт соединения (как для "User-DTP", так и для "Server-DTP"), тип передачи, тип передаваемых данных, структуру данных и управляющие директивы, обозначающие действия, которые пользователь хочет совершить, например, сохранить, считать, добавить или удалить данные или файл

- Пассивный участник соединения(например, клиентский модуль "User-DTP") устанавливает режим ожидания открытия соединения на заданный для передачи данных порт.
- Активный модуль (например, "Server-DTP") открывает соединение и начинает передачу данных

- Окончание передачи данных:
  - соединение между "Server-DTP" и "User-DTP" закрывается, но управляющее соединение "Server-PI"-"User-PI" остается открытым.
  - Пользователь, не закрывая сессии FTP, может еще раз открыть канал передачи данных, передать необходимую информацию и т.д.


User Interface
Пользователь
Server PI
Порт 21
передача команд
User PI
передача данных
Server DTP
User DTP
Файловая система сервера
Файловая система компьютера пользователя
Порт по согласованию через канал управления
сервер FTP
пользователь FTP

Заключение

- Были рассмотрены:
  - **NAT – Network Address Translation**
  - **DNS – Domain Name Service**
  - **SNMP – Simple Network Management Protocol**
  - **SMTP – Simple Mail Transfer Protocol**
  - **FTP – File Transfer Protocol**

"The network's job is to transmit datagrams as efficiently and flexibly as possible. Everything else should be done at the fringes."