

Компьютерные сети

Лекция №6

Прикладные протоколы

Контрольные вопросы

- Правила работы TCP
- Алгоритм работы DNS
- Резервированные IP-адреса

WORLD WIDE WEB – всемирная паутина

- WWW (World Wide Web, Всемирная паутина) состоит из компьютеров, которые предоставляют графический доступ к хранящейся на них информации.
- Протокол работы с WWW - HTTP (Hypertext Transfer Protocol, Протокол передачи гипертекста)

- URI (Uniform Resource Identifier, Идентификатор ресурса),
- URL (Uniform Resource Locator, Местонахождение ресурса),
- URN (Uniform Resource Name, Имя ресурса).

- Схема. (например FTP или WWW)
- Адрес. (например, cmc.cs.msu.su)
- Имя или путь доступа. (например, /curr/cn/mac.html)

- <http://cmc.cs.msu.su/curr/cn/mac.html>

- HyperText Markup Language (HTML) - это язык описания содержащейся на WWW информации.
- Common Gateway Interface (CGI) - это стандарт расширения функциональности WWW, позволяющий WWW-серверам выполнять программы, аргументами работы которых может управлять пользователь.

HTTP-соединение

- Методы запроса.
- "GET"
- "POST"
- "HEAD"
- "PUT"
- "DELETE"



проxy (промежуточный агент)



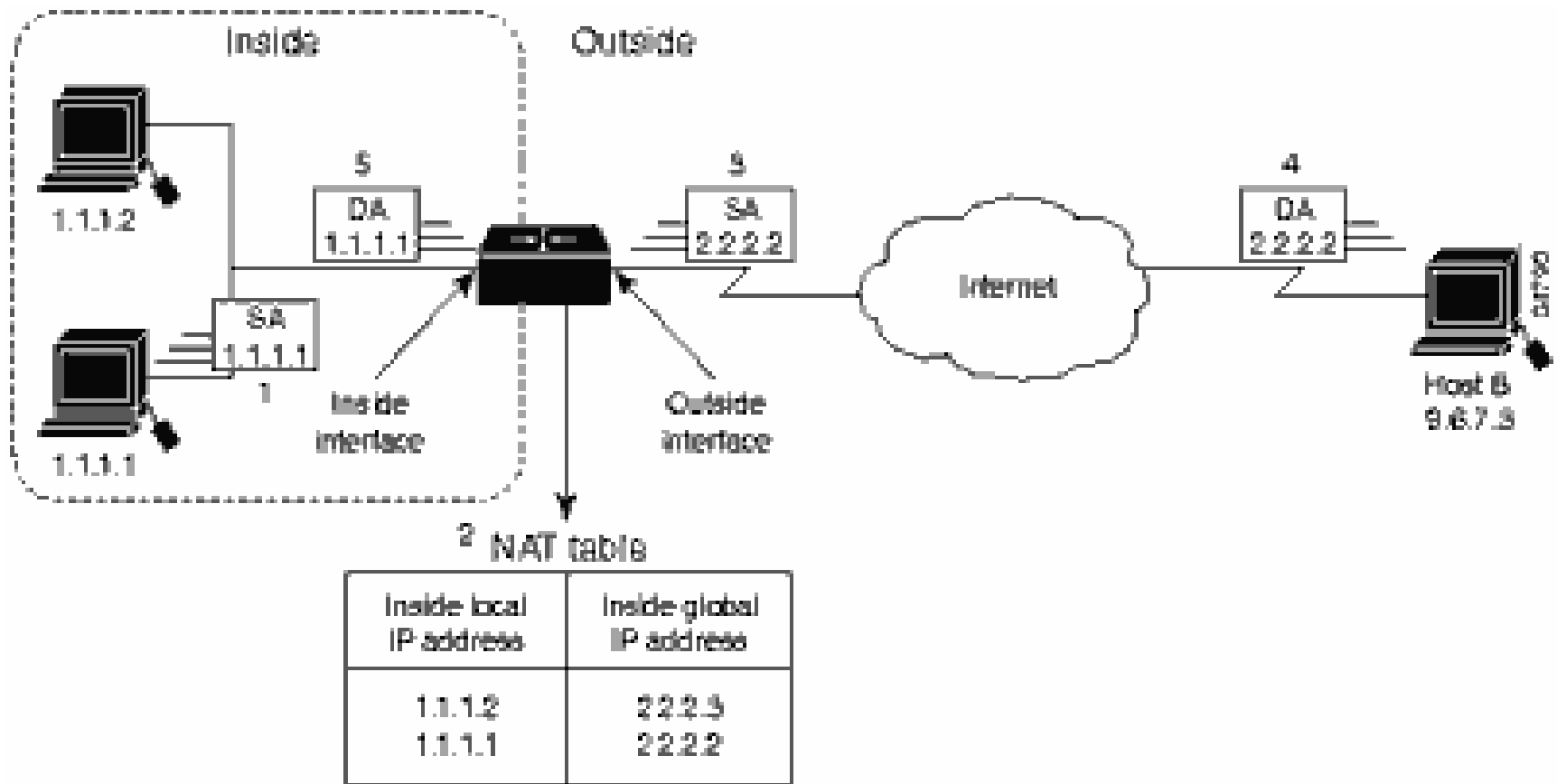
Технология трансляции сетевых адресов (NAT)

- Не все станции имеют глобальные уникальные имена
- Изменение внутренних адресов
- Распределение TCP-трафика

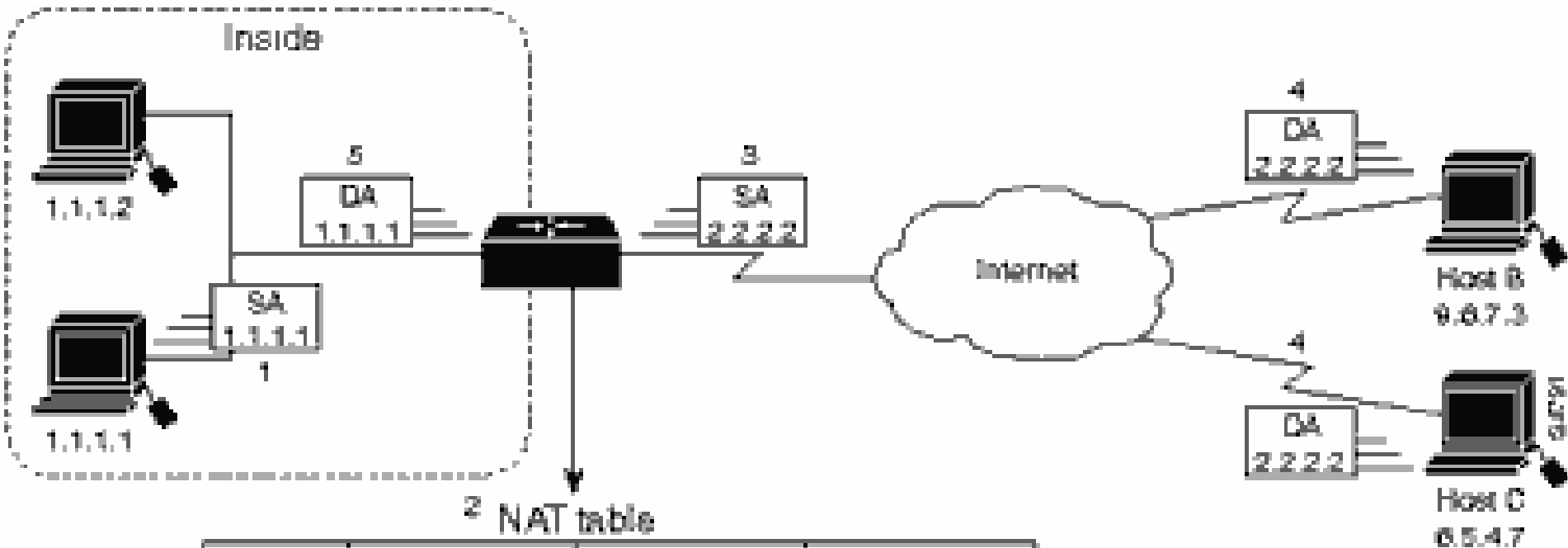
NAT

- Трансляция внутренних адресов источника
- Перекрывание глобальных адресов
- Трансляция при перехлесте адресов
- Распределение TCP-трафика

Трансляция внутренних адресов источника



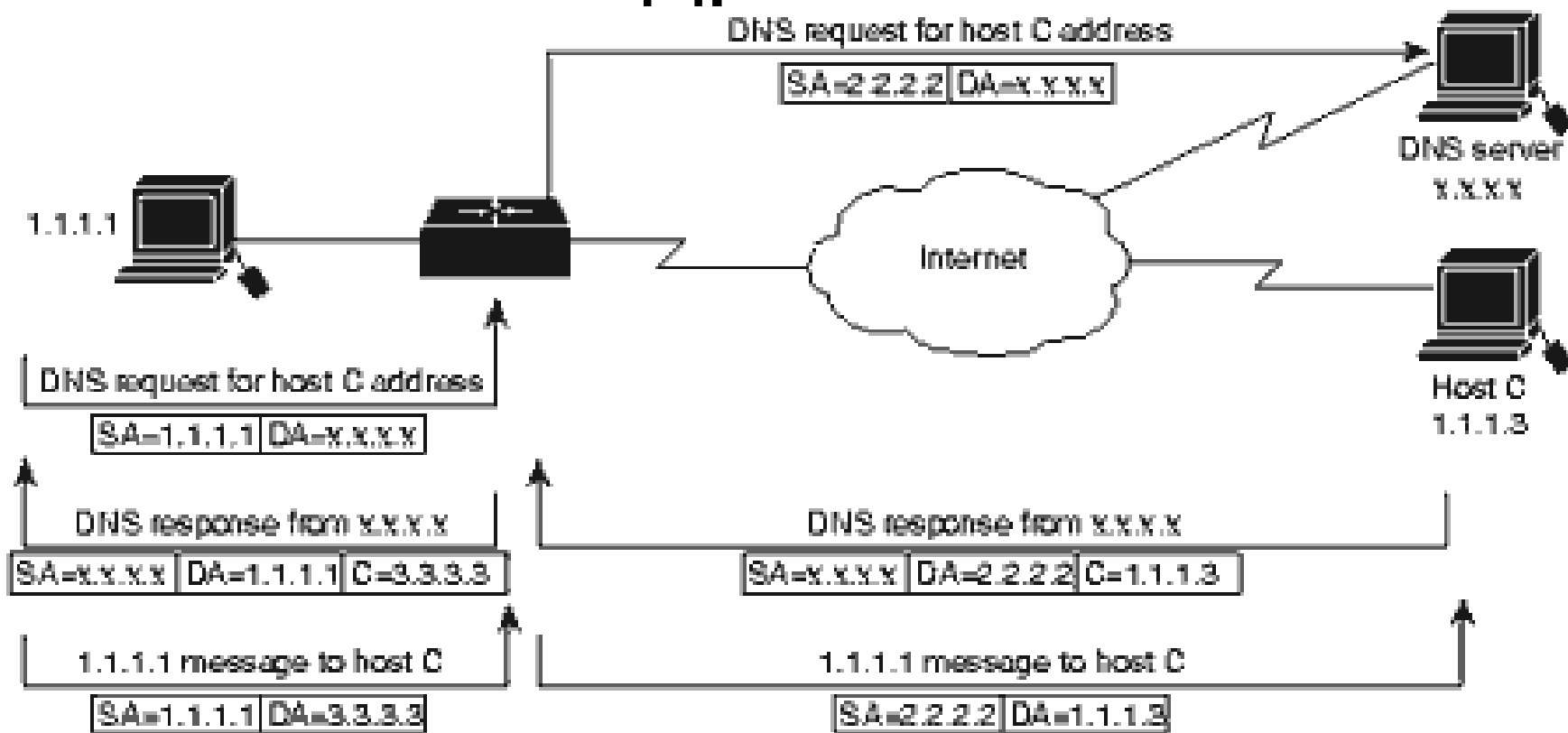
Перекрывание глобальных адресов в NAT



NAT table

Protocol	Inside local IP address:port	Inside global IP address:port	Outside global IP address:port
TCP	1.1.1.2:1723	2.2.2.2:1723	6.5.4.7:23
TCP	1.1.1.1:1024	2.2.2.2:1024	9.6.7.3:23

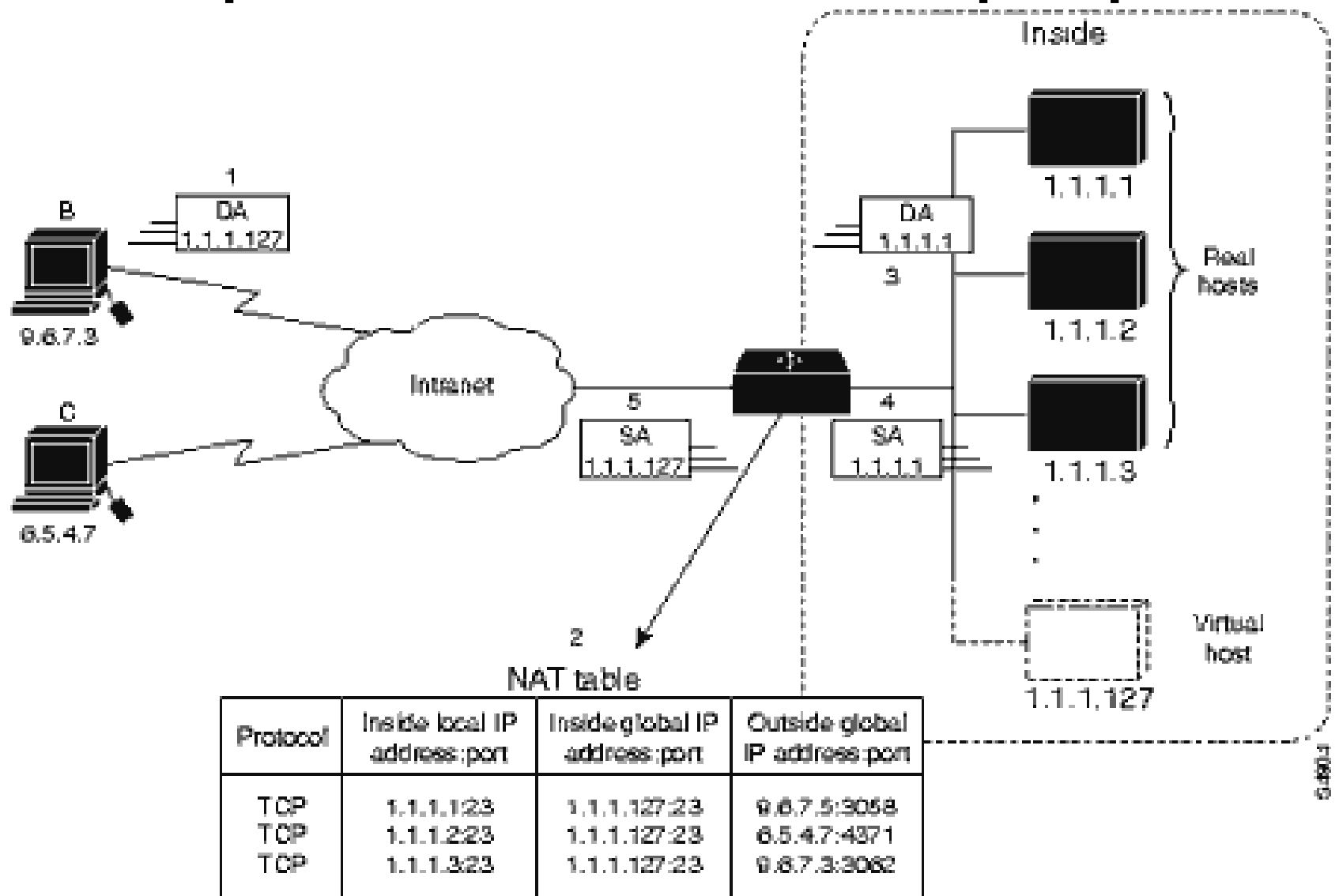
Трансляция при перехлесте адресов



NAT table

Inside local IP address	Inside global IP address	Outside global IP address	Outside local IP address
1.1.1.1	2.2.2.2	1.1.1.3	3.3.3.3

Распределение TCP-трафика

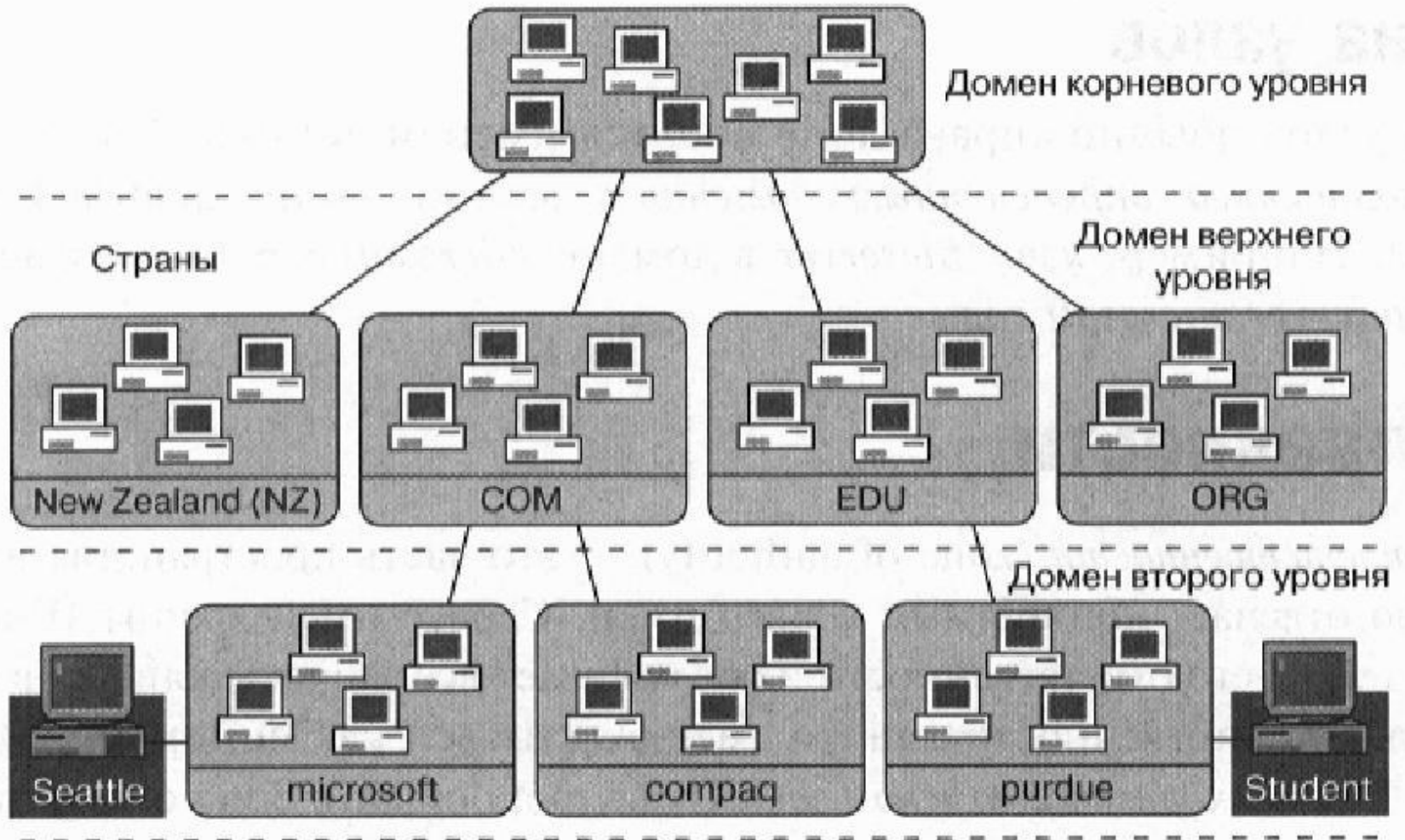


DNS

DNS доменная система имен. В работе DNS участвуют три основных компонента: клиенты DNS, или программы разрешения имен, серверы имен и пространство имен домена. Задача базы данных DNS - транслировать имена компьютеров в IP-адреса

Доменная система имен - это метод назначения имен путем передачи сетевым группам ответственности за их подмножество имен. Каждый уровень этой системы называется доменом. Домены в именах отделяются друг от друга точками: cs.msu.su, math.msu.su. В имени может быть различное количество доменов, но практически их не больше пяти.

DNS (Domain Name System)



"организационные" зоны

- com - commercial (коммерческие)
- edu - educational (образовательные)
- gov - government (правительственные)
- mil - military (военные)
- net - network (организации, обеспечивающие работу сети)
- org - organization (некоммерческие организации)

"географические" зоны

- ae - United Arab Emirates
(Объединенные Арабские Эмираты)
- au - Australia (Австралия)
- be - Belgium (Бельгия)
- br - Brazil (Бразилия)
- by - Belarus (Белоруссия)

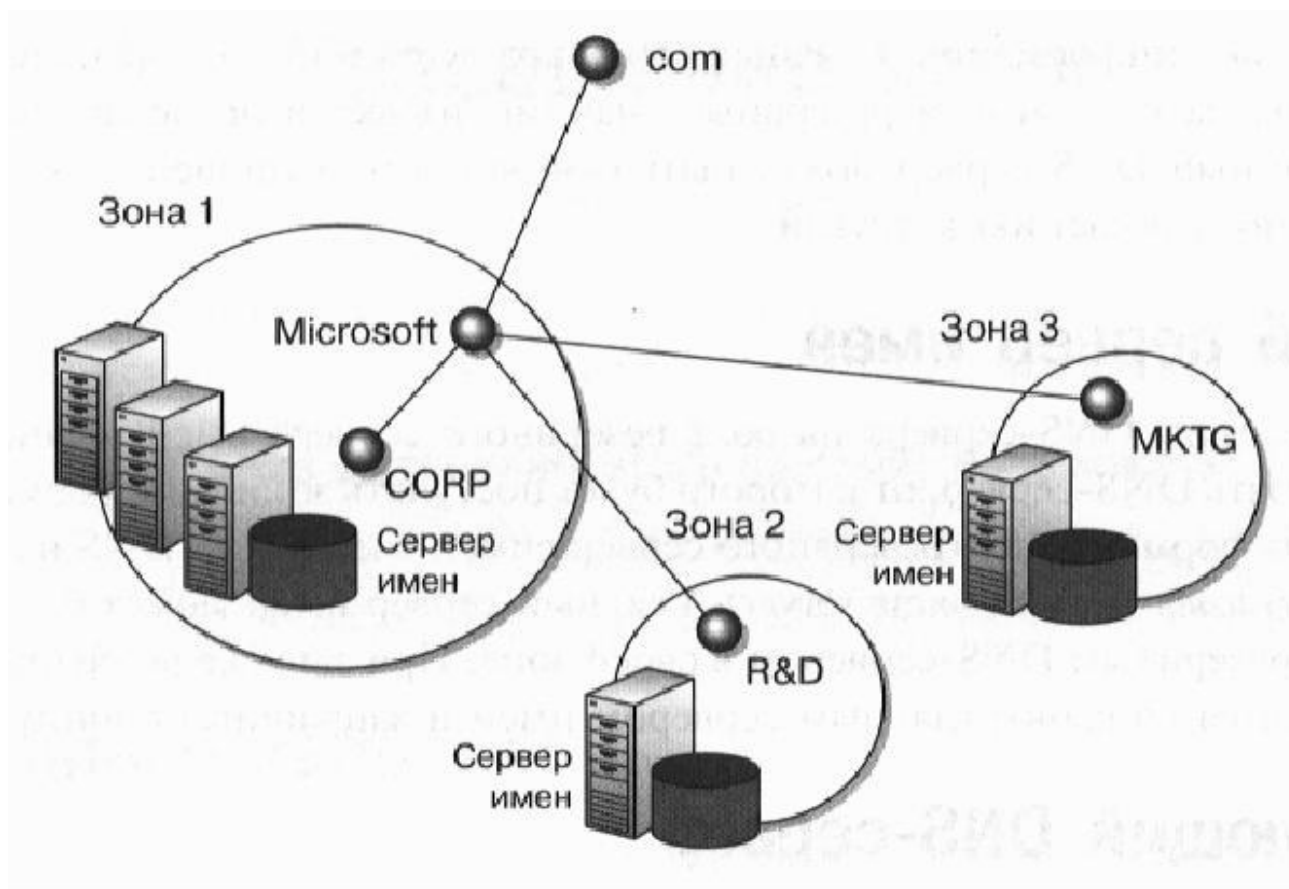
"функциональные" имена

- www - HTTP (WWW) сервер
- ftp - FTP сервер
- ns, nss, dns - DNS (Name) сервер
- mail - Mail сервер
- relay - Mail Exchanger
- проху - соответствующий Proху сервер

Зона ответственности

это часть пространства имен домена, за которую отвечает конкретный сервер имен.

Один DNS-сервер может управлять несколькими зонами. Каждая зона подчинена конкретному домену, который называют корневым доменом зоны.



Разрешение имен

Существует три типа запросов, которые клиент может направить к DNS-серверу: рекурсивный, итеративный и обратный.

Рекурсивные запросы

DNS-сервер обязательно отвечает на рекурсивный запрос, посылая либо запрошенную информацию, либо сообщение об ошибке. Последнее означает, что запрошенные данные отсутствуют или указанного имени домена не существует. При этом DNS-сервер не может перенаправить клиента к другому DNS-серверу

Итеративные запросы

На итеративный запрос DNS-сервер выдает наилучший ответ из имеющихся у него. В нем может содержаться разрешенное имя или ссылка на другой DNS-сервер.

Пример рекурсивного и итеративного запросов: клиент, находясь на работе, запрашивает у DNS-сервера IP-адрес, соответствующий узлу `www.whitehouse.gov`.

1. DNS-клиент посылает локальному DNS-серверу рекурсивный запрос, в котором просит определить IP-адрес для узла `www.whitehouse.gov`.

Локальный сервер имен отвечает за распознавание имени и не может перенаправить клиента к другому DNS-серверу.

2. Локальный DNS-сервер просматривает свои зоны и не находит зону, содержащую указанное имя домена. Тогда он посылает к корневому серверу имен итеративный запрос об узле `www.whitehouse.gov`.

3. Корневой DNS-сервер, ответственный за корневой домен, возвращает IP-адрес сервера имен для домена верхнего уровня - `.gov`.

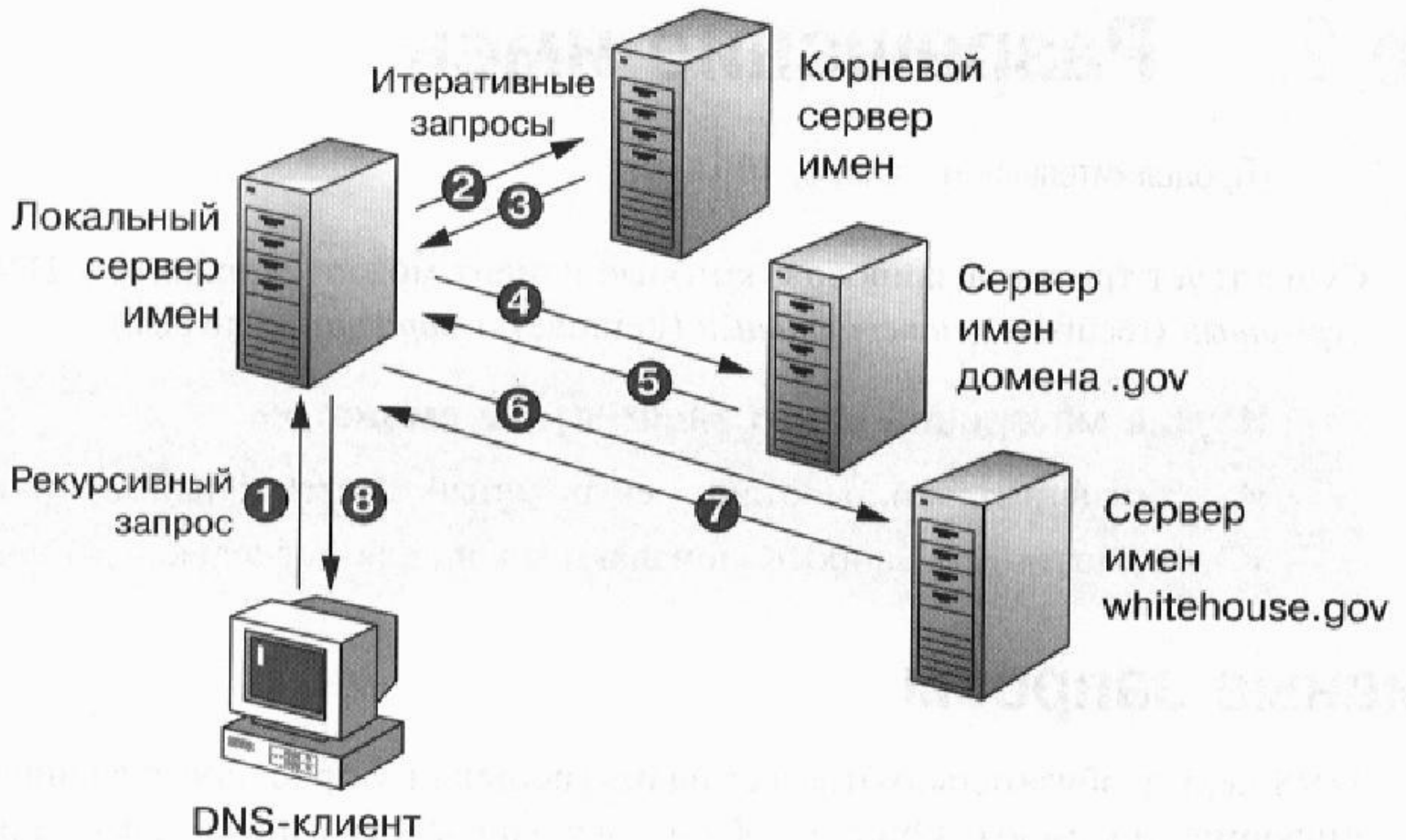
4. Локальный DNS-сервер посылает DNS-серверу домена `.gov` итеративный запрос о `www.whitehouse.gov`.

5. DNS-сервер домена `.gov` возвращает IP-адрес сервера имен, обслуживающего домен `whitehouse.gov`.

6. Локальный DNS-сервер посылает DNS-серверу домена `whitehouse.gov` итеративный запрос о `www.whitehouse.gov`.

7. DNS-сервер домена `whitehouse.gov` возвращает IP-адрес, соответствующий `www.whitehouse.gov`.

8. Локальный DNS-сервер посылает клиенту IP-адрес для `www.whitehouse.gov`.



Конфигурирование файлов DNS

Типичный DNS-сервер использует четыре конфигурационных файла.

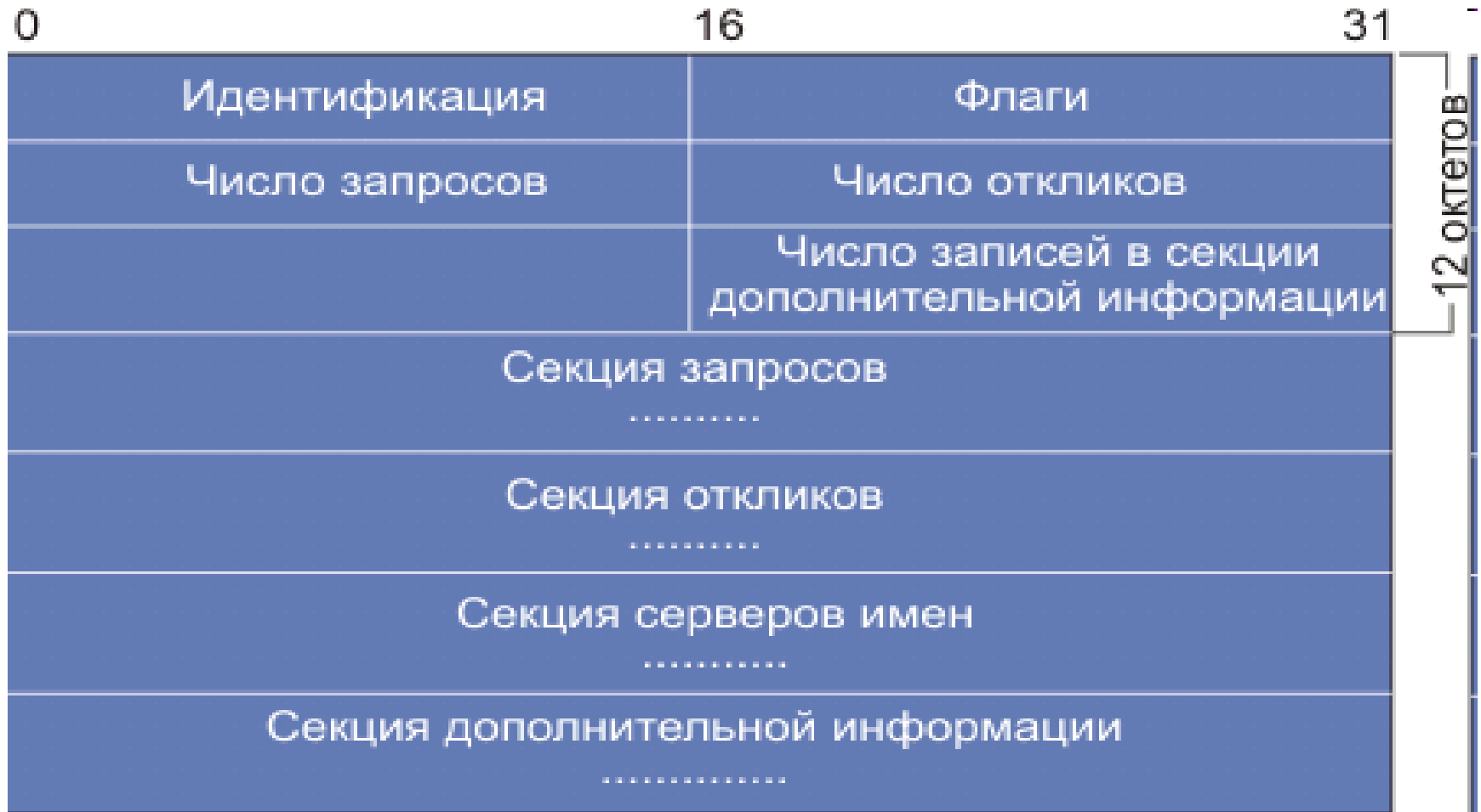
Файл базы данных - содержит исходные записи для домена.

Файл обратного просмотра - позволяет DNS-клиенту определять имя узла соответствующее заданному IP-адресу. Имя для файла обратного просмотра назначается в соответствии с названием зоны домена in-addr.arpa, для которой этот файл обрабатывает обратные запросы. Например, для обеспечения обратных запросов в IP-сети 157.57.28.0, необходимо создать файл обратного просмотра с именем 28.57.157.in-addr.arpa.

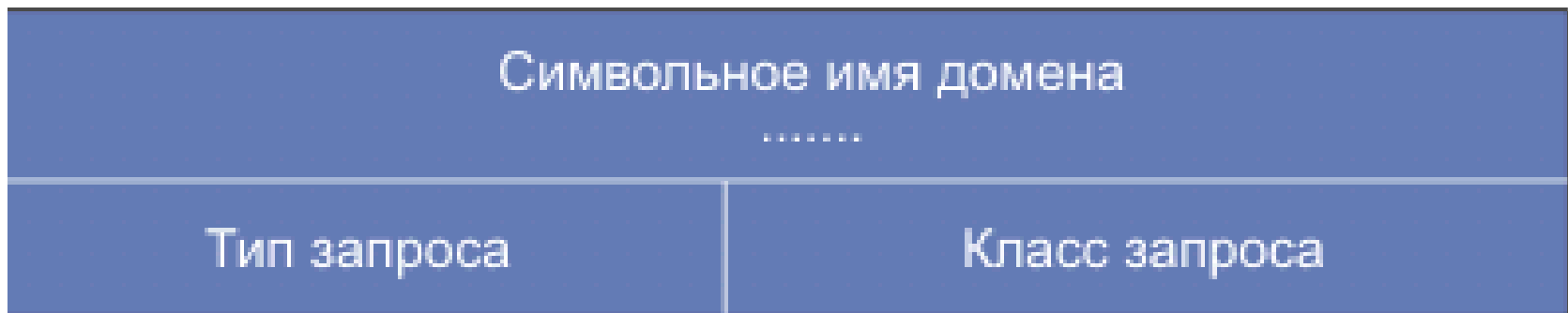
Кэш-файл

Файл Cache.dns содержит записи для серверов корневого домена. В кэш-файле хранится информация, необходимая для разрешения имен за пределами ответственных доменов. Он содержит имена и IP-адреса ~~корневых~~ DNS-серверов.

Формат DNS-сообщений



Формат секции вопросов DNS-запроса



- | Тип запроса | Код запроса | Описание |
|-------------|-------------|---|
| A | 1 | IP-адрес |
| NS | 2 | Сервер имен. |
| CNAME | 5 | Каноническое имя. |
| SOA | 6 | Начало списка серверов. Большое число полей, определяющих часть иерархии имен, которую использует сервер. |
| PTR | 12 | Запись указателя. |
| MX | 15 | Запись о почтовом сервере. Включает в себя значение приоритета обработчика почты. |
| * или ANY | 255 | Запрос всех записей. |

kemsu.ru

- IN SOA ns.kemsu.ru. demid.kemsu.ru.
- IN NS ns.kemsu.ru.
- IN NS prim.omskreg.ru.
- IN NS ns1.kuzstu.ru.
- IN NS ns.org.kemsu.ru.

- IN MX 10 mail.kemsu.ru.
- IN MX 30 mail.kuzstu.ru.

- kemsu.ru. IN A 82.179.1.10
- ns IN A 82.179.1.1

kemsu.ru

- ns IN A 82.179.1.1
- proxy IN A 82.179.1.1
- ban IN CNAME ns
- mrtg IN CNAME ns
- dwupdates IN CNAME ns
- demid IN CNAME ns

- oracle IN A 82.179.12.140

- school IN A 82.179.1.1
- mail.school IN CNAME school
- school IN MX 10 mail.school.kemsu.ru.

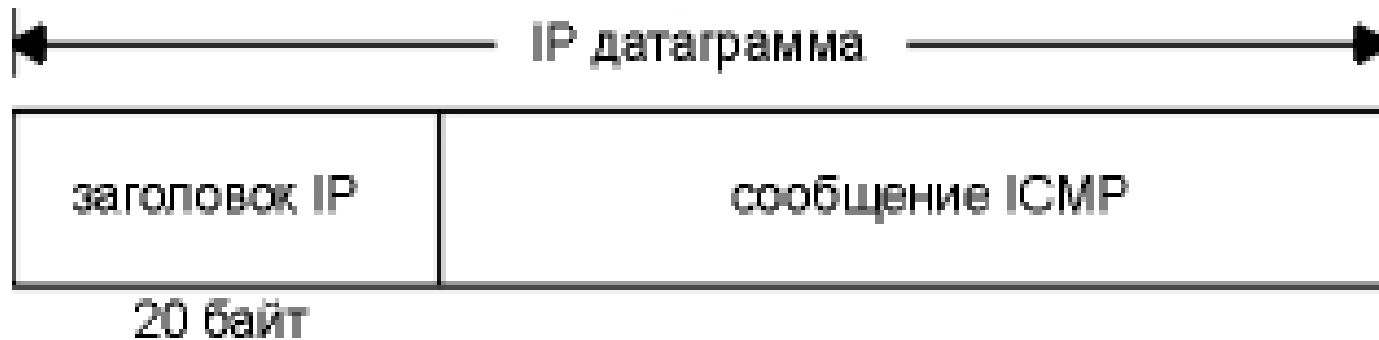
1.179.82.IN-ADDR.arpa

- IN SOA ns.kemsu.ru. demid.kemsu.ru.
- IN NS ns.kemsu.ru.
- IN NS prim.omskreg.ru.
- IN NS daemon.kuzstu.ac.ru.

- 1 IN PTR ns.kemsu.ru.
- 3 IN PTR www.kemsu.ru.
- 4 IN PTR mmedia2.kemsu.ru.
- 5 IN PTR mail.kemsu.ru.
- 6 IN PTR stat.kemsu.ru.
- 7 IN PTR domino.kemsu.ru.
- 8 IN PTR ultra10.kemsu.ru.

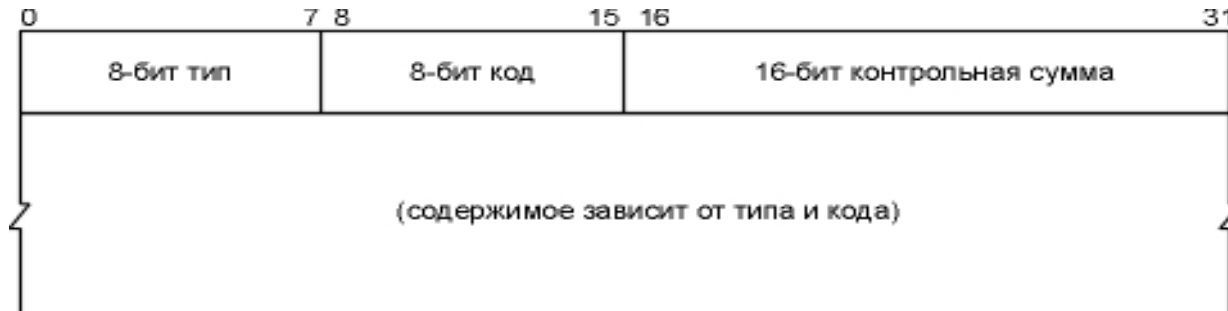
ICMP: протокол управления сообщениями Internet

ICMP сообщения передаются внутри IP датаграмм



С его помощью передаются сообщения об ошибках и сообщения о возникновении условий и ситуаций, которые требуют к себе особого внимания.

ICMP сообщение

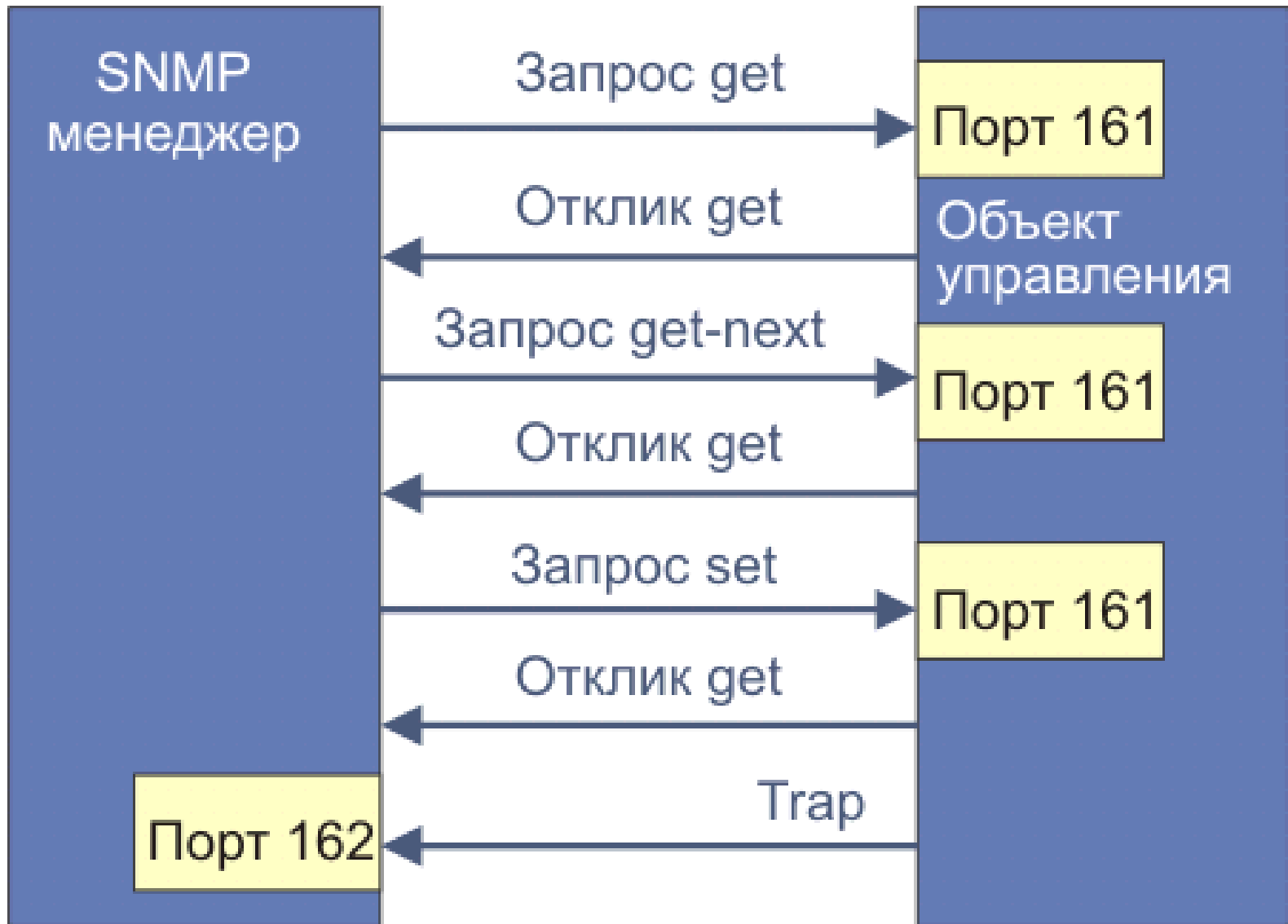


тип	код	Описание	запрос	ошибка
0	0	эхо-отклик (отклик-Ping, глава 7)	•	
3		назначение недоступно:		
	0	сеть недоступна - network unreachable (раздел "ICMP ошибки о недоступности хоста и сети" главы 9)		•
	1	хост недоступен - host unreachable (раздел "ICMP ошибки о недоступности хоста и сети" главы 9)		•
	2	протокол недоступен - protocol unreachable		•
	3	порт недоступен - port unreachable (раздел "ICMP ошибка недоступности порта (ICMP Port Unreachable Error)" главы 6)		•
	4	необходима фрагментация, однако установлен бит "не фрагментировать"- fragmentation needed but don't-fragment bit set (раздел "ICMP ошибки о недоступности" главы 11)		•
	5	не работает маршрутизация от источника - source route failed (глава 8, раздел "Опция IP маршрутизации от источника")		•

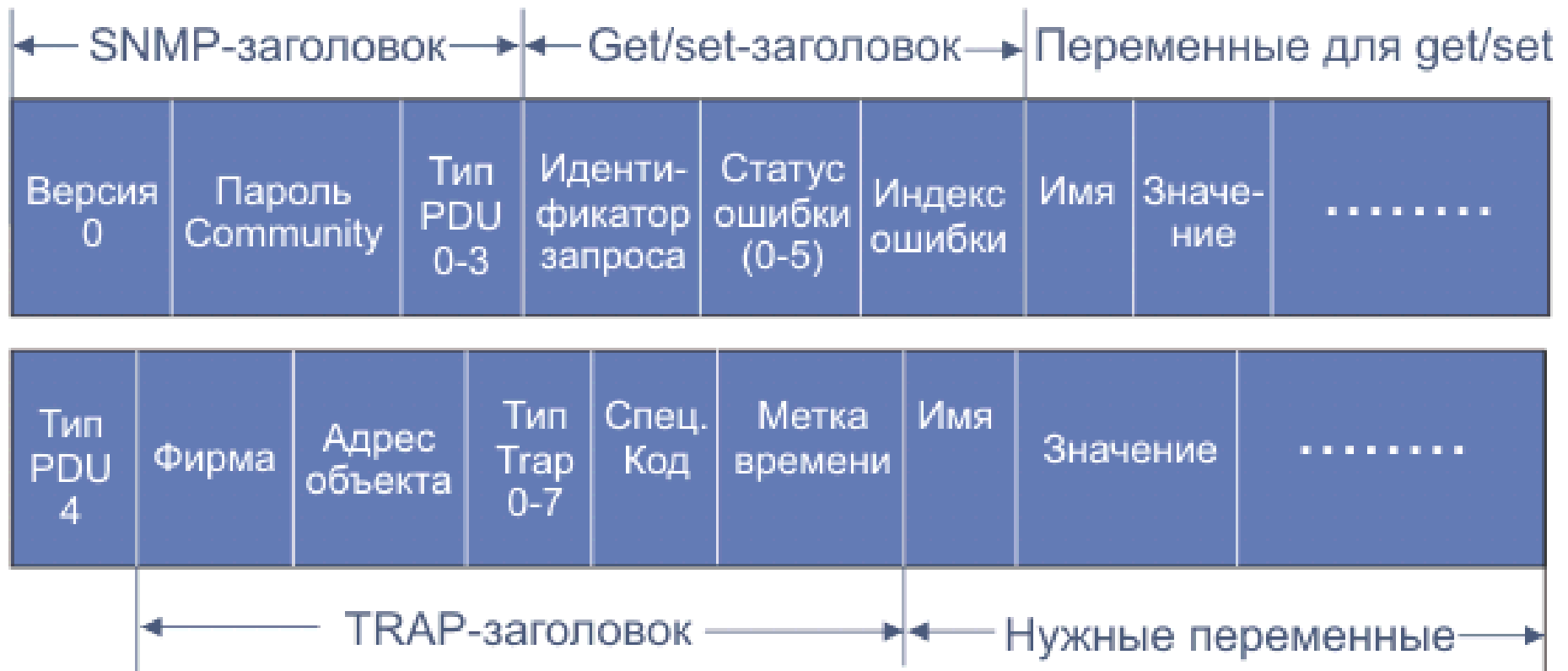
Протокол управления SNMP

- Работает на базе UDP
- Предназначен для использования сетевыми управляющими станциями
- Управляющая база данных - MIB

Схема запросов/откликов SNMP



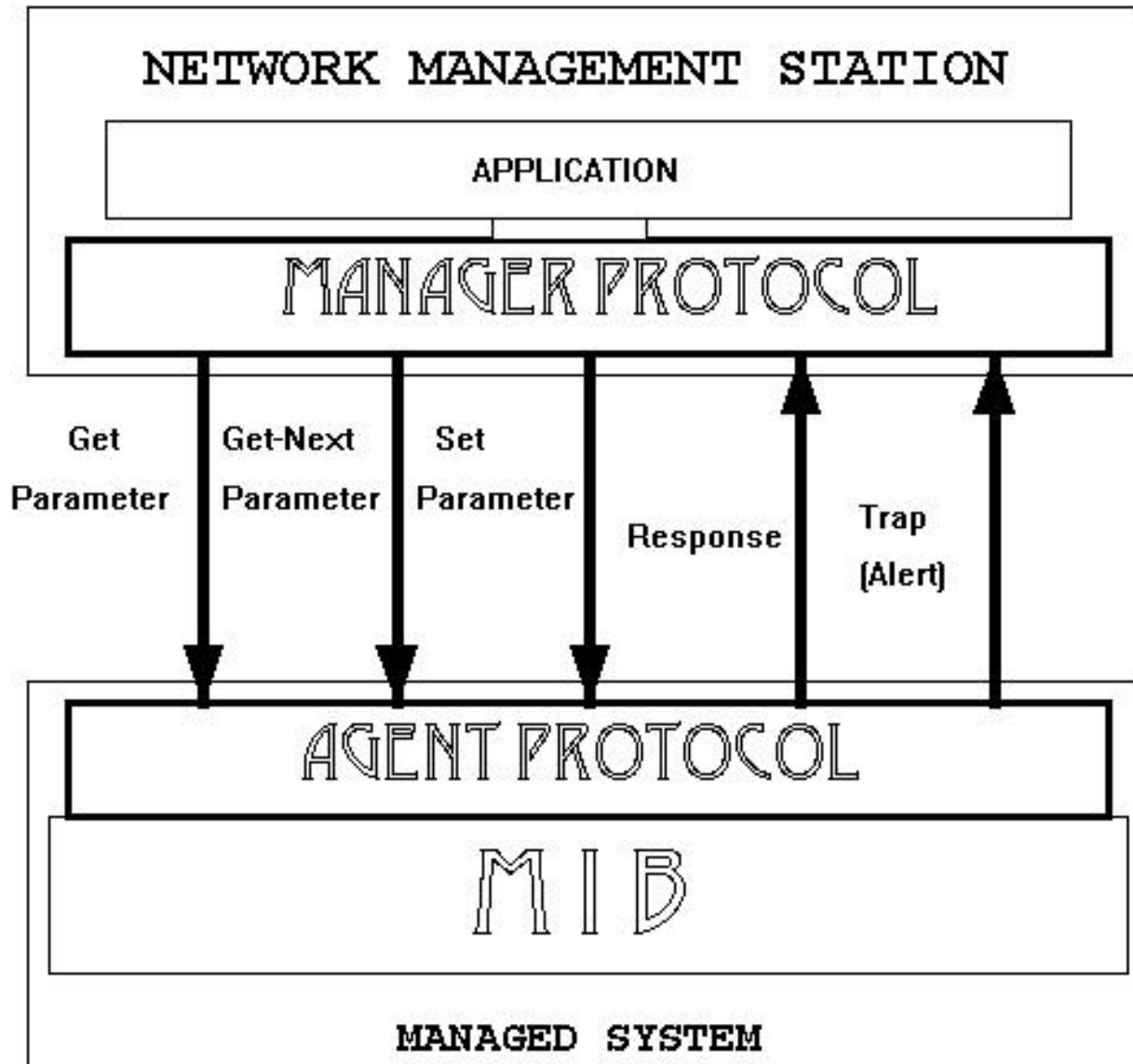
Формат SNMP-сообщений, вкладываемых в UDP-дейтограммы



Компоненты процессора SNMP

- Диспетчер
- Подсистема обработки сообщений
- Подсистема безопасности
- Подсистема управления доступом
- Генератор команд
- Обработчик команд
- Отправитель уведомлений
- Получатель уведомлений
- Прокси-сервер

MIB



SNMP версий 1,2 и 3

- Безопасность
- SNMP v.1 и SNMP v.2 авторизация пользователя выполняется посредством "строки сообщества«
- SNMP v.3 используют более сложный процесс авторизации

Traps

- Traps - сообщения, которые предупреждают о произошедших событиях при работе коммутатора.

Типы сообщений traps

- Cold Start
- Warm Start
- Authentication Failure
- Topology Change
- Link Change Event
- Port Partition
- Broadcast\Multicast Storm

Вопросы?