1. ***Назначение интерфейса Named Pipe***
2. ***Назначение и основные принципы работы Proxy-сервера***

**Прокси-сервер** — служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам.

***Использование***

1. Обеспечение доступа с компьютеров локальной сети в Интернет
2. Кэширование данных
3. Сжатие данных
4. Защита локальной сети от внешнего доступа
5. Ограничение доступа из локальной сети к внешней

1. ***Назначение интерфейса Mailslot***
2. ***Поясните понятие «Фальцовка » и «Расфольцовка»***

**Фальцовка** – разбиение значение поля на несколько строк с учетом ограничений на 998 и 78 символов (без учета CRLF).

**Расфальцовка** – процесс преобразования фальцованного многострочного представления поля в однострочное путем удаления всех последовательностей CRLF.

Если строка превышает 78 символов, ее желательно разбить на несколько строк. В некоторых реализациях значение превышающее 80 могут не восприниматься. Перед пробелом ставим сочетание CRLF и значение поля будет разбито на несколько строк.

1. ***Назначение и основные принципы работы (с указанием уровней модели ISO/OSI) межсетевого экрана***

**Межсетевой экран (сетевой) –** комплекс аппаратных или ПС, осущ-щий контроль и фильтрацию проходящий через него сетевых пакетов в соотв.с зад.правилами. Защищ. соединяемую с интернет корпорат.сеть от проникновения извне и сключ.возм-сть доступа к конфид.инфе.

Браундмауэр типа **пакетный фильтр** явл.наиб.простыми. Они раб.на сет.ур. модели OSI или на IP-уровне стека протоколов TCP/IP

**Шлюзы сеансового уровня** – брандмауэр, кот раб.на сеанс.ур.модели OSI или на TCP стека протоколов TCP/IP. Отслеживают процессы установл.TCP-соед.и позвол.опред., явл ли д-й сеанс легитимным.

**Шлюзы прикладного ур (proxy-сервер) –** функционир на прикл.ур модели OSI . Прикладной ур.отвеч.за доступ приложений в сеть. К задачам относ: перенос файлов, обмен почт.сообщ и упр-ние сетью.

**Stateful Packet Inspection** – объединяет в себе преим.пакетных фильтров, шлюзов сеанс.ур-ня и шлюзов прикладного ур. Т.е.фактически речь идет о многоур.брандмауэрах, кот.раб.одноврем.на сетевом, сеан и прикл.ур-нях.

1. ***Последовательное выполнение при вызове удаленной процедуры***
2. Процедура клиента вызывает клиентскую заглушку.
3. Клиентская заглушка создает сообщ.и вызывает службу RPC локальной операционной системы.
4. Служба RPC пересылает сообщение службе RPC удаленной операционной системе.
5. Служба RPC удаленной операционной системы вызывает серверную заглушку и передает ей сообщение.
6. Серверная заглушка извлекает из сообщения параметры и вызывает удаленную процедуру.
7. Удаленная процедура исполняет код и возвращает параметры и значение возврата серверной заглушке.
8. Серверная заглушка формирует сообщение и вызывает службу RPC своей локальной операционной системе.
9. Служба RPC своей локальной операционной системы сервера пересылает сообщение службе RPC локальной операционной системы клиента.
10. Служба RPC локальной операционной системы клиента возвращает сообщение клиентской заглушке.
11. Заглушка извлекает результаты и возвращает их.
12. ***Какие ограничения вносит спецификация REC5322(формат сообщения Internet) на размерность сообщений***

Сообщ включ.символы с десятич. кодами от 1 до 127 в кодировке ASCII.

Данная спецификация вносит **два ограничения** на число символов в строке:

* строка д.содерж.не более 998 символов (без учета CRLF)
* следует исп-ть строки р-ром не более 78 (без учета CRLF)

CR – возврат каретки (перем.курсор в нач.стр, не перев.на след. стр)

LF – перевод на новую строку.

Поля заголовков представл.собой строки, нач-ся с имени поля, за кот. лед.двоеточие, содерж.поля и знак завершения строки CLRF.

Имя поля д.сост.только из печа-мых символов исключая двоеточие.

Значение поля может включать печатаемые символы ASCII, символы пробела и гориз.табуляции.

1. ***Назначение и основные принципы работы NAT-устройства***

**NAT** (Network Address Translation) – процесс трансляции лок.адресов во внешн.

Существует 3 базовых концепции трансляции адресов:

**Стат.NAT –** отображ.незарег.IP на зарег. IP на осн.1к1.

**Динам.NAT** – отображ.незарег.IP на зарег.IP от группы зарег. IP.

**Перегруж.NAT** – форма динам.NAT, кот.отображ.неск незарег.IP в единств.зарег.IP, исп-я порты (известен как PAT). При перегрузке каждый пк в частной сети транслируется в тот же самый адрес, но с различн.№ порта.

1. ***Опишите процесс получения элементов IP-адресов DHCP-сервера с указанием протоколов, адресов и получателей***

**DHCP –** Dynamic Host Configuration Protocol.

Передача д-х осущ.с пом.протокола **UDP**, при этом сервер приним. сообщ. от клиетов на порт 67 и откравл.сообщ.клиентам на порт 68.

**Распределение IP адресов:**

1. **Ручное** – сисадмин сопоставл MAC-адресу каждого пк клиента опрд.IP. Отлич от ручной настройки каждого пк лишь тем, что сведения хран. На DHCP сервере и их проще измен при необх-сти
2. **Авто** – каждому пк на пост.исп-ние выдел.произв.своб.IP из опред.админом диап
3. **Динам** – как авто, только выдается не на пост.пользование, а на произв.срок (аренда). По истеч.срока аренды ip сновь свободен и влиент обязан запросить новый.

## Взаимодействие клиента и сервера

* **DHCPDISCOVER** – широковещ.сообщ., отправл. от К в собств.физ.подсеть. в кач-ве отправителя все 0000. в кач-ве получателя 255.255.255.255.

Если в данной подсети сервер отсуств., сообщ.будет передано в др.посети ретранслир.агентами протокола BOOTP (они и вернут К сообщ от С).

К выдвиг.треб. С для установки IP с пар-ми (маска, время и т.д.). этот пакет рассылается по сети С.обязаны отреагировать ответом DCHPOFFER.

* **DHCPOFFER** – ответ сервера; посыл.клиенту с ip адресом (м содерж пар-ры конфигур).этот пакет также отсылается всем в сети. Вставляет также ключ, кот.был сформирован К. К смотрит его ключ или нет, и в завис от этого прин/ не прин IP.
* **DHCPREQUEST** –для устан.доп.пар-ров. Отправл в сеть широковещ.сообщ с id выбранного С + па-ры, кот.хотим получ.

(Клиента м.не устроить ни 1 из предлож., тогда он заново посыл. Request, а С так и не узнают, что их предлож.отклонены => поэтому при выдаче IP в offer С не резервирует его)

* **DHCPPACK** – получает DHCPREQUEST и смотрит был ли какой-то клиент, кот.быстрее запросил что-то, чем мы. Если такого не было, то запис.К (нас) в таблицу с выданными пар-ми. И выдаем это подтверждение клиенту. Клиент выставляет пар-ры и пользуется выделенным IP.
* **DHCPNACK** – если кто-то успел забрать IP-адрес быстрее нас, то он отправляет сообщ.К, что данный IP уже занят. Тогда К заново посыл. широковещ.запрос на получ.IP адреса и делает это до тех пор, пока не получит его.
* **DHCPDECLINE** – клиент отправляет запрос серверу, если в сети уже есть хост с таким же IP адресом и параметрами. Т.е. если клиент получил и пришел хост с уже установленными параметрами. Клиент в таком случае просит новый IP адрес и параметры.
* **DHCPRELEASE** – для долгосрочного прекращения аренды (все заново)  
  Если срок аренды закончился – посылаем request с просьбой продлить срок. Получ.положит.pack продолжаем работу.

1. ***Назначение записей «А» и «Мх» в таблице DNS***

|  |  |  |
| --- | --- | --- |
| **Тип** | **Функция записи** | **Описание испоьзования** |
| A | Host Address  Адрес хоста, или узла | Связ.домен.имя и ip  Если создать неск записей с одним и тем жже дом.именем но разными ip – развномерно распред.нагрузку. |
| MX | Mail Exchanger  Обмен почтой | Связ.имя почтового домена с именем хоста, содержащего почт С (неск – указ.приоритет) |

1. ***Назначение и основные принципы работы ремейтеров***

**Ремейлер** – сервер, кот.получ.сообщ.эл.почты и перенапрвл.его по адресу, указанному отправителем. В проц.переадресации вся инфа об отправителе уничтож., поэтому конечн.получатель лишен возм-сти выяснить, кто явл. автором сообщ.

**2 типа ремейлеров:**

\*псевдо-анонимные

Его оп-р знает адрес эл.почты, кот.необх.для получ.ответа на письмо. Тайна связи полностью завис.от оператора, кот.м.стать жертвой угорз, шантажа или соц.инженерии. Преимущество – юзабилити.

\*анонимные

Им.гораздо более выс.секретность, но при этом сложнее в исп-нии. Операторы не м.знать какие д-е пересыл.через них, а поэтому нет гарантии своеврем.доставки сообщ, кот.м.затеряться. Преимущество – надежно скрывают реальный адрес и содержимое сообщ.

1. ***Поясните понятие «Маршалинг параметров»***

Маршалинг пар-ров – процесс передачи параметров при вызове удаленных процедур.