***Лекция 23.***

**Протоколы управления DNS, ICMP и SNMP**

***План:***

***1. Протокол DNS***

***2.*** ***Протокол ICMP***

***3.*** ***Протокол SNMP***

***Ключевые слова:*** *домен, хост, виртуальный сервер, доменное имя,* *зона, делегирование ответственности,* *агра,* *двухсимвольные домены, трехсимвольные домены, почтовый обменник, функции контроля, Ping, Traceroute, контроль подключенных к сети устройств, менеджер, агент*

**Протокол DNS**

*DNS* протокол (*Domain Name System* – система доменных имен) – это компьютерная четко распределенная система для получения информации о состоянии домена.

Часто его используют для получения IP-адреса по имени определенного хоста (устройства или компьютера), получения необходимой информации о пройденном маршруте почты, которая обслуживается узлами для протоколов в домене.

Такая распределенная база данных системы доменных имен поддерживается благодаря иерархии DNS-серверов, которые взаимодействуют согласно определенному протоколу.

Основой для *DNS* протокола служит представление об ее иерархической системе доменного адреса и зонах. Каждый отдельный сервер, которые в ответе за имя, может вполне делегировать свою ответственность на будущую часть домена другому серверу, что способствует возложению ответственности за популярность информации на серверы разнообразных предприятий, организация или людей, которые отвечают только за собственную часть доменного имени.

Недавно в систему DNS протоколов начали внедрять средства проверки целостности данных, которые передаются, эти средства получили название DNS Security Extensions (DNSSEC).

DNS была разработана Полом Мокапетрисом в 1983 году.

DNS протокол можно охарактеризовать такими функциями:

* Распределенность администрирования. Люди или разные организации несут ответственность за некоторые части иерархической структуры.
* Распределенность сохраненной информации. Каждый отдельный сетевой узел обязательно должен сохранять не только те данные, которые находятся в его зоне ответственности, но и адреса корневых серверов.
* Кэширование всей информации. Определенный узел способен сохранять некоторое количество данных из несобственной зоны ответственности для того, чтобы уменьшить сетевые нагрузки.
* Иерархическая структура, которая объединяет все узлы в одно дерево, каждый узел может сам определить работу нижестоящих узлов, или просто передать их другим узлам.
* Резервирование. За обслуживание и хранение собственных зон отвечают сразу несколько серверов, которые разделены на физические и логические, что в результате гарантирует сохранность данных и продолжение работы даже при сбое одного из узлов.

*Система доменных имен* очень важна в работе глобальной сети, поскольку для обычного соединения с узлом нужно вся информация о его личном адресе, а для людей легче запомнить адреса, написанные буквами, чем цифрами.

Изначально преобразование между доменными и IP-адресами проводилось с применением определенного текстового файла, составляющего в централизованном и автоматическом режиме, рассылался на каждую машину в личной локальной сети. С развитием глобальной сети появилась необходимость в эффективном и автоматизированном механизме, которым и стала система доменных имен - DNS.

В сети Интернет DNS выполняет важную задачу, для доступа к WEB-серверу необходимо знать его IP-адрес. Люди помнят буквенные (обычно осмысленные) адреса, чем последовательность цифр IP – адреса, компьютерам, в свою очередь, удобнее обрабатывать численное представление адреса (IP-адрес). Также наличие символьного имени сервера позволяет использовать так называемые *виртуальные серверы*, например, HTTP-серверы, отличающиеся друг от друга именем запроса (доменным именем), но использующие один и тот же IP-адрес.

*Протокол DNS* выполняет две основные функции. Он позволяет клиентским компьютерам запрашивать *DNS-сервер* об IP-адресе или имени какого-либо хоста в сети, а также позволяет производить обмен информацией между базами данных серверов DNS.

В этом протоколе используется стандартный формат типа "запрос-ответ", где клиент посылает пакет запроса, и сервер отвечает либо пакетом с информацией, полученной из базы данных, либо сообщением об ошибке, в котором указывается причина отказа в обработке запроса.

В своей работе этот протокол использует порт 53 и протоколы — TCP или UDP. Причем в последнее время UDP стал более распространенным методом транспортировки пакетов по сети Интернет.

В связи с тем, что число узлов Интернета растет с каждым днем, для эффективной работы DNS разработана распределенная база данных, поддерживаемая с использование иерархии DNS-серверов.

В основе иерархической структуры DNS лежит представление о доменном имени и зонах. Каждый DNS сервер, отвечающий за имя, может передать ответственность за дальнейшую часть домена другому серверу.

Система доменных именИерархия доменных имен начинается с корневого домена без имени (или еще как его называют «домен точка»), далее идут домены верхнего уровня или домены первого уровня. Домены верхнего уровня поделены на три зоны:

* *Аrpa* - это специальный домен, используемый для сопоставления адрес – имя.
* *Семь трехсимвольных доменов* называются общими (generic) доменами или организационными (organizational) доменами.
* *Двухсимвольные домены*, так называемые домены стран или географические домены (ru – Российская федерация, kz - Казахстан), основанные на кодах стран, в соответствии с ISO 3166.

Поскольку *DNS* поддерживает иерархию доменных имен, но никак не IP-адресов. Для решения “обратной” задачи есть специальный домен, структура которого совпадает со структурой IP-адресов. Называется этот домен *IN-ADDR.ARPA*.

*IN-ADDR.ARPA* — специальная доменная зона, предназначенная для определения имени хоста по его IPv4-адресу.

DNS использует несколько типов записей. Основные типы:

* A запись (address record [IPv4](http://just-networks.ru/seti-tcp-ip/protokol-ipv4) ) или запись адреса - основная запись, выполняет связующую роль между именем хоста (just-networks.ru) и IP адресом (5.101.153.37). Если меняется только А запись, то это значит, что сайт физически будет размещен на другом хостинге, а все остальные записи останутся работать на старом хостинге.
* AAA запись (address record [IPv6](http://just-networks.ru/seti-tcp-ip/protokol-ipv6)) или запись адреса - аналогична записи A, только для IPv6.
* CNAME запись (canonical name record) или каноническая запись имени (псевдоним) - используется для перенаправления на другое имя (по аналогии с ссылками), частным примером использования CNAME записи, является создание доменных имен для FTP, MAIL, SSH.
* TXT запись - текстовая запись, содержащая 254 байта любой текстовой информации, в основном используется для подтверждения принадлежности домена для сервисов YANDEX, GOOGLE.

**Протокол ICMP**

Протокол обмена управляющими сообщениями *ICMP (Internet Control Message Protocol)* позволяет маршрутизатору сообщить конечному узлу об ошибках, с которыми маршрутизатор столкнулся при передаче какого-либо IP-пакета от данного конечного узла.

Управляющие сообщения *ICMP* не могут направляться промежуточному маршрутизатору, который участвовал в передаче пакета, с которым возникли проблемы, так как для такой посылки нет адресной информации - пакет несет в себе только адрес источника и адрес назначения, не фиксируя адреса промежуточных маршрутизаторов.

*Протокол ICMP* - это протокол сообщения об ошибках, а не протокол коррекции ошибок. Конечный узел может предпринять некоторые действия для того, чтобы ошибка больше не возникала, но эти действия протоколом ICMP не регламентируются.

Коммуникация, использующая *протокол ICMP*, состоит в пересылке подходящих информаций об ошибках, раскроенных во время связи между двумя устройствами.

Одиночная информация существует в виде пакета, сформированного надлежащим образом (Datagram), которая, следовательно, будет подвергнутый инкапсуляции в рамке протокола IP. Протокол *ICMP* не использует в своей работе протоколы TCP и UDP.

Примеры работы протокола ICMP:

• Ping - один из инструментов, выступающих практически в каждой операционной системе, обслуживающей протокол TCP/IP. С его помощью пакеты ICMP ECHO\_REQUEST отправляются в целевой компьютер. Дистанционная машина, после получения такого сообщения должна ответить при помощи ECHO\_REPLY. Поэтому можно определить следующее: конфигурация сети делает возможной связь с дистанционной машиной, и оценку её нагрузки на основании информаций, касающихся количества потерянных пакетов и времени ответа.

• Traceroute – инструмент, делающий возможным определение, через какие маршрутизаторы проходит пакет по дороге к дистанционному компьютеру.

Существует несколько типов сообщений ICMP. Каждый тип сообщения имеет свой формат.

**Протокол SNMP**

*SNMP (Simple Network Management Protocol* — простой протокол сетевого управления) — стандартный Интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP.

К поддерживающим *SNMP* устройствам относятся маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры, модемные стойки и другие.

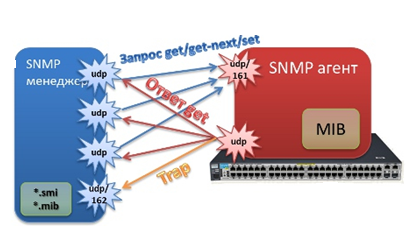
Протокол обычно используется в системах сетевого управления для контроля подключённых к сети устройств на предмет условий, которые требуют внимания администратора. SNMP определён Инженерным советом интернета (IETF) как компонент TCP/IP.

Он состоит из набора стандартов для сетевого управления, включая протокол прикладного уровня, схему баз данных и набор объектов данных.

Сеть, использующая *SNMP* для управления содержит три основных компонента:

1. *SNMP менеджер* – программное обеспечение, устанавливаемое на компьютер администратора (системы мониторинга)
2. *SNMP агент* - программное обеспечение, запущенное на сетевом узле, за которым осуществляется мониторинг.
3. *SNMP MIB* – MIB - это Management information base. Этот компонент системы обеспечивает структурированость данных, которыми обмениваются агенты и менеджеры. По сути - это некая база данных в виде текстовых фалов.

SNMP менеджер является прослойкой (интерфейсом) между оператором\администратором и сетевым узлом с запущенным SNMP агентом.



**Контрольные вопросы:**

1. Что такое DNS протокол?
2. Функции DNS протокола.
3. Кто и когда разработал DNS протокол?
4. Что такое виртуальный сервер?
5. Назначение протокола ICMP.
6. Утилита Ping и ее назначение.
7. Утилита Traceroute и ее назначение.
8. Назначение протокола SNMP.
9. Какие устройства поддерживают SNMP протокол?
10. Основные компоненты SNMP.