Назначение и свойства сервера DNS. Взаимодействие клиента и серверов в иерархической структуре DNS. Сравнение статической и динамической реализации службы DNS. Проблемы безопасности.

Система доменных имен DNS (Domain Name System)

1) Domain Name System – пространство имен узлов сети с определенными понятиями свойствами как множества элементов.

2) Domain Name Service – служба или сервер, обслуживающий систему сетевых имен, с определенными понятиями, свойствами и программными реализациями как службы.

Поэтому, когда речь идет о понятиях и свойствах DNS, надо первым делом определить, что имеется в виду. Это важно, например, потому, что Domain Name System вполне может существовать без Domain Name Service. Хотя оба понятия тесно связаны и частенько объединяются.

Базовые свойства DNS.

Цель – сформировать пространство символьных имен с отображением на адреса хостов (как и в других системах именования). Возможно дополнительно нагрузить имена свойствами и сделать эту информацию общедоступной в сети.

Алфавит – латинские буквы прописные и строчные, цифры, дефис “-“. Дальнейшее расширение на UNICODE и подключение национальных алфавитов.

Синтаксис элемента пространства имен (DNS-имени) – строка структурного имени до 64 символов, состоит из полей (доменов), разделенных точкой. Расширена до 254 символов.

Структура пространства – связное дерево (иерархия с одним корнем), в котором узлы дерева, называемые доменами, образуют промежуточные части DNS-имени, а листья соответствуют компьютерам.

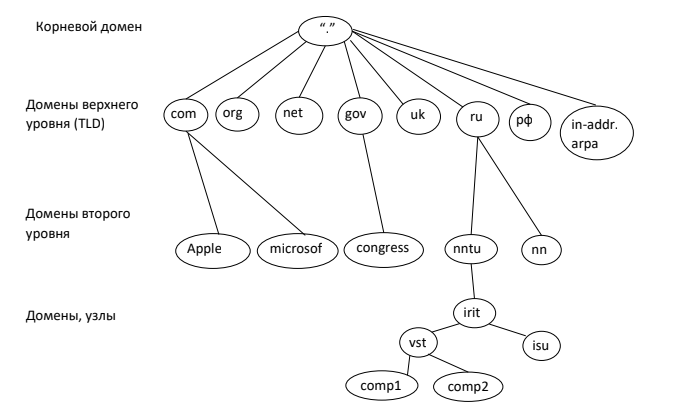
FQDN (Fully Qualified Domain Name) – полное квалификационное доменное имя хоста. Уникальное полное имя хоста, определяющее его положение в пространстве DNS. Обычно разделяется на две компоненты: локальное имя и dns-суффикс. Например, FQDN comp1.dom1.dom2.net включает comp1 – локальное имя, dom1.dom2.net – dns-суффикс. FQDN задает однозначный путь в дереве доменов от корня до данного хоста.

Основное требование – уникальность имен хостов во всем пространстве DNS.

Желаемые качества – информативность, эффективность для поиска, управляемость, надежность, масштабируемость в глобальной сети и много других обстоятельств.

Ради реализации требований и свойств DNS в Internet и разворачивается сложная международная система, сочетающая распределенность структуры с контролируемым распределением полномочий по уровням и доменам.

Основную роль играет система DNS в Internet, формируемая и контролируемая взаимосвязанной системой организаций – регистраторов DNS, аккредитованных ICANN.



Цель иерархии:

- быстрый поиск информации по дереву, когда FQDN задает прямой путь от корня;

- распределение административных полномочий по узлам дерева с подотчетностью. Владелец домена регистрирует поддомены и обеспечивает их уникальность на своем уровне. Если на каждом уровне это требование выполняется, то обеспечивается уникальность FQDN во всем пространстве DNS.

Динамические свойства DNS.

Работа DDNS основана на регистрации клиентов в базе данных предпочитаемого DNS-сервера, которую надо разрешить с клиентской и с серверной стороны. Регистрация записи имени и адреса клиента (A-запись и PTR-запись) может быть выполнена двумя путями:

- службой DHCP-клиента на узле при загрузке или конфигурировании от DHCP-сервера,

- службой DHCP-сервера после выдачи клиенту IP-адреса, то есть DHCP-сервер может сам связаться с DNS-сервером для регистрации клиента.

Варианты настраиваются и должны быть спланированы.

Протокол для обновления DNS описан в RFC 2136 и реализован, например, утилитой nsupdate. Со стороны DNS-сервера для безопасной аутентификации клиента можно использовать технологию TSIG, в которой используется заранее известный ключ. Ключ должен быть установлен на каждом клиенте и на сервере. Протокол TSIG (Transaction SIGnature) – идентификация и целостность данных во взаимодействиях между серверами DNS при передаче зоны и передаче динамических обновлений.

В динамическом режиме важна не только регистрация, но и удаление устаревших и некорректных записей. В DNS-сервер встроены механизм проверки актуальности ресурсных записей (aging resource record) и очистки БД (scavenging). Период стабильности (no-refresh interval) по умолчанию – 7 дней.

Безопасность DNS. DNSSecurity Extensions (DNSSEC)

Основная проблема состоит в том, что подмена правильных адресов, соответствующих DNS-именам, на ложные позволяет направить клиента на мошеннический сайт. Имитируя оригинальный интерфейс, злоумышленник может получить пароли, коды, какую-либо информацию о клиенте.

Сама информация DNS не секретна, поэтому ее не надо защищать от несанкционированного доступа. Надо защищать от несанкционированного изменения.

Цель DNSSEC –защита от подмены информации в ответах DNS-серверов на запросы клиентов.

Суть действий DNSSEC- подписывание адресной информации цифровой подписью с проверкой на клиентах.

Сложность реализации DNSSEC обусловлена распределенностью структуры и иерархической схемой обработки рекурсивных запросов. Необходимо развернуть иерархию доверия: регистраторы доменов должны ручаться за интернет-провайдеров, а те в свою очередь – за администраторов доменных имен.

Другая проблема безопасности, характерная для DNS, называется “ Отравление кэша резольвера” – подмена записей локального кэша DNS-клиента. Помним, что кэш работает в первую очередь. Самый простой и наглядный пример – влияние через файл hosts, которое можно сделать скрытно. Массовому пользователю невдомек регулярно проверять какой-то там файл.