

10 основных концепции, для админа Windows

<http://winitpro.ru/index.php/2010/04/12/10-osnovnyx-koncepcii-dlya-admina-windows-chast-1/>

<http://winitpro.ru/index.php/2010/04/12/10-osnovnyx-koncepcii-dlya-admina-windows-chast-2/>

<http://winitpro.ru/index.php/2010/04/12/10-osnovnyx-koncepcii-dlya-admina-windows-chast-3/>

<http://winitpro.ru/index.php/2010/04/12/10-osnovnyx-koncepcii-dlya-admina-windows-chast-4/>

Contents

10 основных концепции, для админа Windows	1
10 основных концепции, которые должен знать сетевой администратор Windows	1
Введение	1
1. DNS Lookup	1
2. Ethernet & ARP	2
3. IP-адреса и подсети	2
4. Шлюз по умолчанию	3
5. NAT и частная IP-адресация	4
6. Брандмауэры	4
7. LAN и WAN	4
8. Маршрутизаторы	4
9. Свитчи	4
10. Инкапсуляция в модели OSI	5
Резюме	5

10 основных концепции, которые должен знать сетевой администратор Windows

Введение

Недавно моя родственница проходила собеседование в качестве аналитика безопасности. Ей на интервью был задан целый ряд технических вопросов но те, с которыми у нее были самые большие проблемы – были именно вопросы о сети (она давно не работала именно с сетью. Я думаю, что эта статья может быть полезной для начинающих сетевых администраторов Windows, которым так нужна подборка вопросов, которые зачастую спрашивают на собеседованиях для сетевых администраторов, да и любой нормальный админ должен знать и понимать такие вещи).

Итак, вот мой список 10 основных сетевых концепции, которые должен знать каждый сетевой админ Windows (или тех, кто ищет такую работу):

1. DNS Lookup

Система доменных имен (DNS) является краеугольным камнем любой сетевой инфраструктуры. DNS преобразует IP-адреса в имена и имена в IP-адреса (прямое и обратное преобразование соответственно). Таким образом, когда вы переходите на веб-страницу, например www.winitpro.ru, без DNS, это имя не будет разрешено в IP адрес, и вы не увидите веб-страницу. Таким образом, если DNS не работает — для конечных пользователей «ничего не работает».

DNS-сервер разрешения IP адресов задается либо вручную или получаться с помощью DHCP. Если вы наберете **IPCONFIG / ALL** в Windows, вы увидите, DNS сервер, установленный для вашего ПК.

```
Command Prompt
Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix . : wiredbraincoffee.com
Description . . . . . : Intel(R) WiFi Link 5100 AGN
Physical Address. . . . . : 00-22-FB-61-BE-94
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 10.0.1.107(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, January 01, 2010 2:15:15 AM
Lease Expires . . . . . : Monday, April 12, 2010 8:46:53 PM
Default Gateway . . . . . : 10.0.1.1
DHCP Server . . . . . : 10.0.1.1
DNS Servers . . . . . : 10.0.1.20
                          10.0.1.1
NetBIOS over Tcpip. . . . . : Enabled
```

IPCONFIG

DNS-серверы отображаются выполнением команды IPCONFIG

Итак, вы должны понимать, что такое DNS, и как важно что DNS-серверы должны быть настроены и работоспособны, и что DNS-серверы должны быть работоспособными что «почти все» к работало.

Когда вы выполняете пинг, вы можете легко увидеть, что доменное имя разрешается в IP-адресс.

```
C:\Users\david>
C:\Users\david>
C:\Users\david>ping www.windowsnetworking.com

Pinging www.windowsnetworking.com [147.202.51.254] with 32 bytes of data:
Request timed out.

Ping statistics for 147.202.51.254:
```

DNS резолвинг

: DNS имя разрешается в адрес IP

2. Ethernet & ARP

Ethernet представляет собой протокол для вашей локальной сети (LAN). Вы имеете сетевые карты Ethernet (NIC), подключенные к Ethernet кабелям, которые объединяются Ethernet-коммутаторами, которые соединяют все вместе. Без горящего сетевого линка на сетевой карте и свиче(коммутаторе, концентраторе), ничего не выйдет.

MAC-адреса (или физический адреса), уникальные строки, которые идентифицируют Ethernet устройство. ARP (Address Resolution Protocol) это протокол, который отображает Ethernet MAC адреса в IP-адреса. Когда вы открываете веб-страницу и получаете успешный поиск в DNS, вы узнаете IP адрес веб-сервера. Ваш компьютер затем выполнит по сети запрос ARP для того, что идентифицировать компьютер-сервер (который идентифицируется его MAC адресом, как показано на рисунке 1, как физический адрес- Physical address) имеет адрес IP.

3. IP-адреса и подсети

Каждый компьютер в сети должен иметь уникальный адрес 3-го уровня, называемый IP адресом. IP адресов представляет собой 4 числа, разделенных на 3 периода, типа 1.1.1.1.

Большинство компьютеров получают их IP адрес, маску подсети, шлюз по умолчанию и DNS-сервера от сервера DHCP. Естественно, чтобы получать эту информацию, ваш компьютер должен

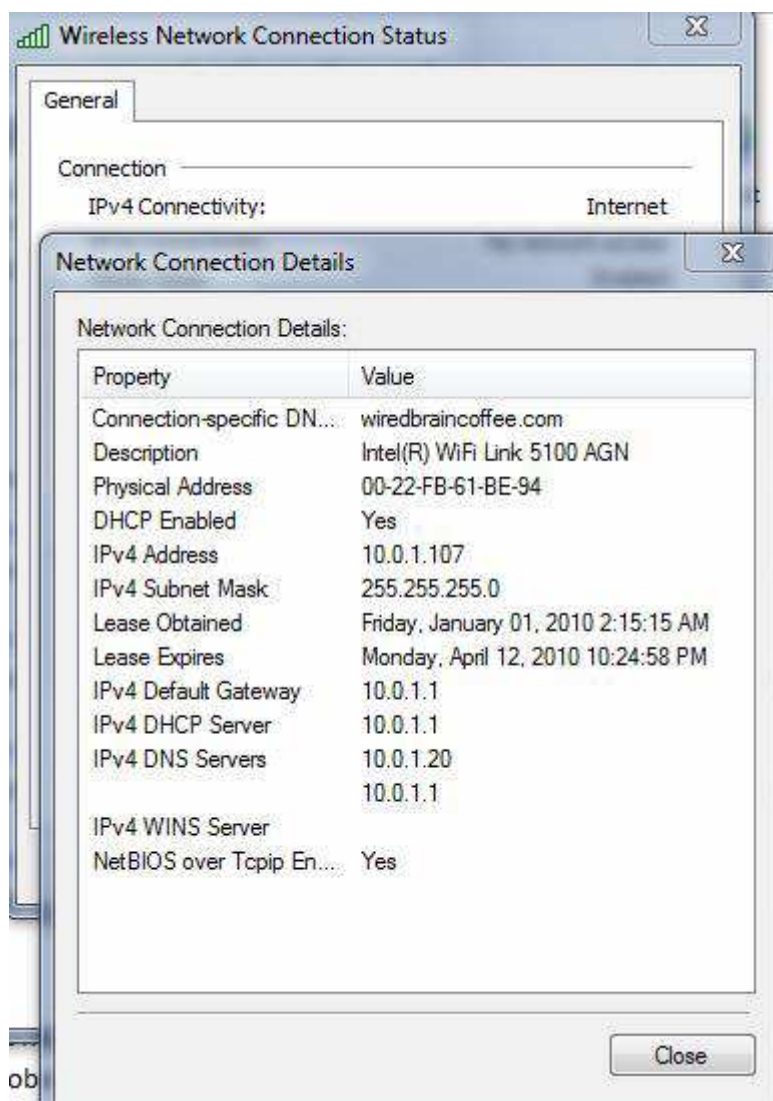
сначала иметь подключение к сети (горящий светодиод на сетевой карте и свиче) и должны быть настроен на DHCP-сервак.

. Вы можете видеть IP-адрес моего компьютера на рисунке 1, где говорится **IPv4 адрес 10.0.1.107**. Вы также можете увидеть, что он получил его через DHCP, о чем говорит запись **DHCP включен YES**.

Большие блоки адресов IP разбиваются на более мелкие блоки адресов IP, и это называется IP подсеть. Я не буду вдаваться в том, как это сделать, и вам не нужно знать, как сделать это по-памяти, (если вы не собираетесь сдавать сертификационный экзамен), поскольку вы можете использовать калькулятор IP подсетей, свободно и бесплатно загруженный из Интернета.

4. Шлюз по умолчанию

Шлюз по умолчанию, как показано на Рисунке 3, **10.0.1.1**, определяет, как ваш компьютер будет общаться с другим, который не в вашей локальной сети LAN. Этот шлюз по умолчанию – обычно ваш местный маршрутизатор. Адрес шлюза по умолчанию не требуется, но если он не настоящий момент не указан, Вы не могли бы обмениваться данными с компьютерами за пределами вашей сети (если вы не используете прокси-сервер).



Детали сетевого подключения

Рисунок : Детали сетевого подключения

5. NAT и частная IP-адресация

Сегодня почти в каждой местной локальной сети используют IP-адресация (на основе RFC1918), а для выхода в интернет эти частные IP-адреса переводятся в IP-адреса для общественности (публичные) с помощью NAT (Network Address Translation). Частные IP-адреса всегда начинаются с 192.168.xx или 172.16-31.xx или 10.xxx (это те блоки частные IP-адреса определены в RFC1918).

На рисунке 2 можно увидеть, что мы используем частные адреса, которые начинаются с «10». Это мой комплексный маршрутизатор, он же точка доступа, он же свитч, он же фаерволл, который также выполняет NAT и перевод моих частных IP адресов в публичные IP-адрес моего маршрутизатора, который был получен от моего Интернет-провайдера.

6. Брандмауэры

Защита вашей сети от злоумышленников занимаются брандмауэры. У вас могут быть программные брандмауэры на ОС Windows в вашем компьютере или сервере, а также у вас может быть аппаратные брандмауэры на вашем маршрутизаторе или в виде специального оборудования. Представьте, что брандмауэры – это такие гаишники для трафика, которые позволят определенным типам трафика проходить, а определенные блокировать.

7. LAN и WAN

Ваша локальная сеть (ЛВС), как правило, охватывает только ваше здание. Это может или не может быть только одна подсеть IP. Ваша локальная сеть связана свичами Ethernet и вам не требуется маршрутизатор для функционирования локальной сети. Итак, запомните, LAN означает «местно, локально».

Ваша широкая сеть (WAN) это «большая сеть», которая объединяет Ваши локальные сети. Интернет является глобальной общечеловеческой WAN. Тем не менее, большинство крупных компаний имеют свои собственные частные WAN. Глобальные сети охватывают несколько городов, государств, стран и континентов. Глобальные сети связаны между маршрутизаторами.

8. Маршрутизаторы

Маршрутизаторы разруливают трафик между различными подсетями IP.. Маршрутизатор работает на 3-ем уровне модели OSI. Как правило, маршрутизаторы определяют маршруты движения трафика от ЛВС к глобальной сети, но в более крупных предприятиях или кампусах зданий, маршрутизаторы обрабатывают трафик между несколькими подсетями IP в одной большой локальной сети.

В небольших домашних сетях, вы можете иметь комплексный и многофункциональный маршрутизатор, который также предлагает наличие встроенного брандмауэра, и многопортового коммутатора, а так же точку беспроводного доступа.

9. Свитчи

Свитчи работают на Уровне 2 модели OSI и соединяют собой все устройства в сети. Свитч отправляет пакеты на основе информации в параметрах кадров, основываясь на MAC-адресе назначения для этого кадра. Switches come in all sizes from small home integrated router/switch/firewall/wireless devices, all the way to very large Cisco Catalyst 6500 series switches. Свитчи бывают разных размеров от небольших домашних многофункциональных маршрутизаторов / коммутаторов / Firewall / беспроводных устройств, вплоть до очень больших коммутаторов серии Cisco Catalyst 6500.

10. Инкапсуляция в модели OSI

Одна из основных концепций сетей это модель OSI. Это теоретическая модель, которая определяет, каким образом различные сетевые протоколы, которые работают на различных уровнях данной модели, работают вместе для достижения связи через сеть (например, Интернет).

В отличие от большинства других концепций, модель OSI является не совсем тем, что сетевые администраторы используют каждый день. Модели OSI для тех, кто хочет просертифицироваться как Cisco CCNA или при сдаче некоторых тестах в сертификации Microsoft Networking. Или, если у вас слишком рьяных интервьюер, который действительно хочет понять, что вы знаете.

Для выполнения тех, кто хочет это вкратце уяснить, приведем здесь модель OSI:

- **Application** — уровень 7 — любое приложение, использующее сеть, например FTP и веб-браузер (www)
- **Presentation** — уровень 6 — определит формат представления передаваемых данных, например JPG графика, ASCII, XML и
- **Session** — 5 — для приложений, оподдерживающих сессию активнойй – это Remote Procedure Calls (RPC), SQL и Exchange
- **Transport** — уровень 4- обеспечивает надежную связь по сети, позволяет убедиться, что ваши данные фактически попадают туда, куда вы их послали — TCP является наиболее распространенным протоколом транспортного уровня
- **Network** — уровень 3 — заботится о адрессации в сети, что позволяет направлять пакеты по протоколу IP, который является наиболее распространенным протоколом сетевого уровня. Маршрутизаторы работают на Уровне 3.
- **Data Link** — уровень 2 — передает кадры по сети, используя протоколы, такие как Ethernet и PPP. Свитчи функционируют на этом уровне.
- **Physical** — уровень 1 — контролирует фактические электрические сигналы, которые передаются по сети и включает в себя кабели, концентраторы и реальные физические связи в сети.

На этом этапе, позвольте мне остановиться и понять важность значения модели OSI, поскольку, даже несмотря на то, что она теоретическая, крайне важно, чтобы сетевые администраторы понимали и умели представить себе, как каждый кусочек данных, передаваемый по сети, путешествует вниз, а затем вверх по уровням этой модели. И как, на каждом уровне модели OSI, все данные из вышестоящего слоя инкапсулируется в нижестоящий слой с добавлением дополнительных данных из этого слоя. И, наоборот, как данные передаются обратно вверх от слоя к слою, и по дороге реинкапсулируются.

Понимая эту модель и то, как аппаратное и программное обеспечение сочетаются друг с другом, чтобы сделать сеть работоспособной (например, Интернет или локальной сети), вы сможете намного эффективнее диагностировать и устранять неполадки в любых сетях.

Резюме

Я не могу не сказать с уверенностью, что, если вы проводите собеседование на любую работу в сфере ИТ, значит, вы должны быть готовы отвечать на вопросы по сетям. Даже если вы идете на собеседование не как кандидат в сетевые администраторы, вы никогда не знаете наверняка, что они не попросят старшего администратора сети задать вам несколько вопросов для проверки ваших знаний. Я могу вам сказать из первых рук, что с высокой долей вероятности на все эти вопросы с вами поговорят на собеседовании на должность сетевого администратора Windows. И, если вы уже являетесь сетевым администратором Windows, надеюсь эта статья послужит отличным обзором основных концепций сетей, которые вы обязаны знать. Хотя вы не обязательно будете

пользоваться этим каждый день, знания об этих понятиях безусловно помогут вам в скорейшем устранении сетевых проблем.