ДІАГНОСТИКА СТАНУ МЕРЕЖІ НА ОСНОВІ TCP/IP

1 Мета роботи. Ознайомитися з мережними командами та навчитися використовувати їх при тестуванні комп'ютерних мереж різного призначення та архітектури

2 Ключові положення

2.1 Команда ipconfig

Команда ipconfig використовується для відображення всіх поточних параметрів мережі TCP/IP та оновлення параметрів DHCP і DNS. При виклику команди ipconfig без параметрів виводиться лише IP-адреса, маска підмережі і основний шлюз для кожного мережного адаптера:

а) синтаксис:

ipconfig [/all] [/renew[адаптер]] [/release [адаптер]] [/flushdns] [/displaydns][/registerdns][/showclassid_адаптер][/setclassid_адаптер [код_класса dhcp]];

б) параметри:

- **/all** - виведення повної конфігурації TCP/IP для всіх адаптерів. Без цього параметра команда ipconfig виводить тільки IP-адресу, маску підмережі та основний шлюз для кожного адаптера. Адаптери можуть бути фізичними інтерфейсами - встановлені мережні адаптери, або логічними інтерфейсами - підключення віддаленого доступу;

- **/renew** [адаптер] - оновлення конфігурації DHCP для всіх адаптерів (якщо адаптер не заданий) або для заданого адаптера. Цей параметр доступний тільки на комп'ютерах з адаптерами, налаштованими для автоматичного отримання IP-адрес. Щоб вказати адаптер, введіть без параметрів ім'я, введене командою ipconfig;

- **/release** [адаптер] - відправка повідомлення DHCPRELEASE серверу DHCP для звільнення поточної конфігурації DHCP і видалення конфігурації IP-адрес для всіх адаптерів (якщо адаптер не заданий) або для заданого адаптера. Цей адаптер відключає протокол TCP/IP для адаптерів, налаштованих для автоматичного отримання IP-адрес. Для того, щоб вказати адаптер введіть без параметрів ім'я, яке виведене командою ipconfig;

- **/flushdns** - скидання та очищення вмісту кеша порівняння імен DNS. Під час усунення негараздів DNS цю процедуру використовують для

видалення з кешу записів невдалих спроб порівняння та інших динамічно доданих записів;

- **/displaydns** - відображення вмісту кеша порівняння імен DNS, включає записи, попередньо завантажені з локального файлу Hosts, а також останні отримані записи ресурсів для запитів на порівняння імен. Ця інформація використовується службою DNS клієнта для швидкого порівняння імен, які часто зустрічаються, без звертання до вказаних в конфігурації DNS-серверам;

- **/registerdns** - динамічна реєстрація вручну імен DNS та IP-адрес, налаштованих на комп'ютері. Цей параметр корисний при усуненні проблем з DNS або при з'ясуванні причин перебоїв динамічного оновлення між клієнтом і DNS-сервером без перевантаження клієнта. Імена, зареєстровані в DNS, визначаються параметрами DNS у додаткових властивостях стеку TCP/IP; 10

- **/showclassid** (или /allcompartments) адаптер - відображення коду класу DHCP для зазначеного адаптера. Щоб переглянути код класу DHCP для всіх адаптерів, замість параметра адаптер вкажіть зірочку (*). Цей параметр доступний тільки на комп’ютерах з адаптерами, налаштованими для автоматичного отримання IP-адрес;

- **/setclassid** адаптер [код_класу] - присвоєння коду класу DHCP для зазначеного адаптера. Щоб задати код класу DHCP для всіх адаптерів, замість параметра адаптер вкажіть зірочка (*). Цей параметр доступний тільки на комп’ютерах з адаптерами, налаштованими на автоматичне отримання IP-адрес. Якщо код класу DHCP не задано, поточний код класу знищується;

- **/?** - відображення довідки в командному рядку.

2.2 Команда arp

Команда arp використовується для виводу і зміни записів кеша протоколу ARP, який містить одну або декілька таблиць, які використовуються для зберігання IP-адрес та відповідних їм фізичних адрес Ethernet або Token Ring. Для кожного мережного адаптера використовується окрема таблиця. Запущена без параметрів, команда arp виводить довідку:

а) синтаксис:

arp -a [inet_addr] [-N if_addr] [-v]

arp -d inet_addr [if_addr]

arp –s inet_addr eth_ addr [if_addr]

б) параметри:

-a [інет_адрес] [-Nін_адрес] - виведення таблиць поточного протоколу ARP для всіх інтерфейсів. Щоб вивести записи ARP для окремої IP-адреси, скористайтесь командою arp –a з параметром інет_адрес, де інет_адрес – це IP-адреса. Щоб вивести параметри таблиці кеша ARP для певного інтерфейсу, вкажіть параметр -N ін_адрес, де ін_адрес – це IP-адреса, яка призначена інтерфейсу. Параметр -N вводиться з урахуванням регістру;

-g [інет_адрес] [-Nін_адрес] - збігається з –a;

-d інет_адрес [ін_адрес] - видалення запису з певною IP-адресою, де інет_адрес - це IP-адреса. Щоб видалити запис таблиці для певного інтерфейсу, вкажіть параметр ін_адрес, де ін_адрес – це IP-адреса, яка призначена інтерфейсу. Щоб видалити всі записи, введіть зірочку (*) замість параметра інет_адрес;

-s інет_адрес е_адрес[ін_адрес] - додавання статичного запису, який співставляє IP-адресу інет_адрес з фізичною адресою е_адрес, в кэші ARP. Для додавання статичного запису кешу ARP в таблицю для певного інтерфейсу, вкажіть параметр ін_адрес, де ін_адрес – це IP-адреса, яка призначена інтерфейсу;

/? - відображення довідки в командному рядку.

Примітка. IP-адреси для параметрів інет_адрес записуються в точково-десятковій нотації. Фізична адреса для параметра е_адрес складається з шести байт, записаних в шістнадцятковому форматі і розділених дефісами (наприклад 00-AA-00-4F-2A-9C). Записи, додані з параметром -s, є статичними і не видаляються з кеша ARP після закінчення періоду часу. Записи видаляються, якщо зупинений і запущений протокол TCP/IP. Щоб створити постійні статичні записи кеша ARP, введіть відповідні команди arp та скористайтесь «планировщиком заданий» для виконання цього файлу при запуску. Ця команда доступна, тільки якщо у властивостях мережного адаптера в об’єкті "Сетевые подключения" в якості компонента встановлено протокол Интернета (TCP/IP).

2.3 Команда netstat:

Netstat - це утиліта командного рядка, яка дозволяє вивести статистику про поточні IP-з'єднання, стані портів, таблиці маршрутизації, стані активних TCP з'єднань і ін. Застосування команди netstat без параметрів відобразить тільки інформацію про поточні TCP з'єднаннях. Для отримання додаткової інформації необхідно вказати відповідні опції:

а) синтаксис:

netstat [-a] [- b] [- e] [- n] [- o] [- p *протокол*] [- r] [- s] [- v] [*інтервал*]

б) параметри:

-a	Виводить все подключени я і порт и , на котори е комп'ютер очікує з'єднання.
-b	Виводить ім'я виконуваного файлу, який бере участь у створенні кожного підключення або очікує порту.
-e	Виводить статистику Ethernet. Може застосовуватися разом з ключем -s.
-n	Відображення адрес і номерів портів в чис ловом форматі без спроб дозволу імен. Застосування даного ключа може прискорити роботу утиліти, а також спростити її висновок.
-p *протокол*	Відображення підключень для протоколу , що задається цим параметром. Можна вибрати зі значень tcp, udp, tcpv6, або udpv6. Може застосовувати разом з ключем -s.
-o	Відображає код (ID) процесу кожного підключення
-r	Висновок утримуючі імого таблиці маршрутів (таблиці маршрутизації).
-s	Виводить статистичні дані по протоколам. За замовчуванням дані відображаються для ip, ipv6, icmp, tcp, tcpv6, udp, udpv6.
інтервал	Повторний висновок статистичних даних через вказаний проміжок часу в секундах. Для припинення виведення даних використовується комбінація клавіш CTRL + C. Якщо команда застосовується без даного ключа, виводяться відомості про поточну конфігурацію і тільки один раз.

Примітка. TCP підключення в процесі установки і розриву з'єднань проходять певну процедуру. Висновок команди netstat дозволяє побачити поточну стадію процесу, що дозволяє більш точно інтерпретувати дані. З оединення в списку можуть знаходитися в наступних станах.

- *CLOSE_WAIT* - вказує на пасивну фазу закриття з'єднання, яка починається після отримання сервером повідомлення FIN від клієнта.
- *CLOSED* - з'єднання перервано і закрито сервером.
- *ESTABLISHED* - клієнт встановив з'єднання з сервером, отримавши від сервера повідомлення SYN.
- *FIN_WAIT_1* - клієнт ініціював закриття з'єднання (відправив повідомлення FIN).
- *FIN_WAIT_2* - клієнт отримав повідомлення ACK і FIN від сервера.
- *LAST_ACK* - сервер відправив повідомлення FIN клієнту.
- *LISTEN* - сервер готовий приймати вхідні з'єднання.
- *SYN_RECEIVED* - сервер отримав повідомлення SYN від клієнта і відправив йому відповідь.

- *TIMED_WAIT* - клієнт відправив повідомлення FIN сервера і чекає відповіді на це повідомлення.
- *YN_SEND* - вказане з'єднання активно і відкрито.

2.4 Команда nslookup:

Nslookup - це утиліта командного рядка, призначені а для діагностики інфраструктури DNS . Даний засіб п озволяет задавати різні типи запитів до довільно указиваеми м сервера м DNS .

DNS *(Domain Name System - система доменних імен)* - розподілена база даних зберігає інформацію про домени мережі Інтернет . Система доменних име н заснована на ієрархічному принципі і має власний протокол взаємодії. Оскільки людині простіше оперувати літерними адресами (як правило носять смислове навантаження), ніж з послідовністю цифр ip-адреси, необхідний механізм для перетворення символьних записів в ip-адреси і навпаки. Записи про таку відповідність зберігаються на DNS-серверах, що відповідають за кожну доменну зону мережі Інтернет. Для отримання даних про яке-небудь адресу, клієнт посилає запит на відповідний DNS-сервер і отримує відповідь, що містить запитувану інформацію. Клієнтське програмне забезпечення, що посилає запити на перетворення імені в ip-адреси або навпаки, називає Резолвер (від англ. Resolve - вирішувати). Резолвер в тому чи іншому вигляді є частиною будь-якого програмного забезпечення працює з адресами мережі Інтернет, зокрема, будь-який браузер будь-якій операційній системи має власний вбудований Резолвер . Утиліта nslookup , також реалізує функції з перетворення ip-адрес і імен, однак є більш універсальним інструментом, що дозволяє отримати додаткову інформацію про інфраструктуру DNS.

Команда nslookup може працювати в двох режимах: інтерактивному і звичайному (автономному). Якщо потрібно висновок тільки невеликої частини інформації, слід використовувати звичайний режим. В якості першого параметра слід використовувати ім'я або IP-адреса комп'ютера, про який потрібно отримати дані. В якості другого параметра вводиться ім'я або IP-адресу сервера імен DNS , до якого необхідно надіслати запит . Якщо другий параметр не заданий, утиліта nslookup використовується сервер імен DNS, встановлений за замовчуванням для з'єднання з мережею . Якщо потрібно отримати більш повні відомості, слід використовувати інтерактивний режим. Запущена без параметрів, команда nslookup виводить довідку:

а) синтаксис:

nslookup [- *підкоманду ...*] { *іскомий_компьютер* | іскомий_адрес } [сервер]

б) параметри:

all	В Висновки відомості про сервер, що використовується за умовчанням, і про вузловому комп'ютері.
root	Вказує нове ім'я кореневого сервера
srchlist = N1 [/ N2 /.../ N6]	відправляє список адрес серверів домену, до яких

	необхідно відправити запит на дозвіл.
deb [ug]	включає режим налагодження. Виводитимуться більш докладні відомості про пакети, відправлених сервера, і про отримані відповідях. За замовчуванням використовується nodebug .
ti [meout] = *число*	Вказує число секунд для періоду очікування . Період очікування , що використовується по замовчуванням , становить 5 секунд. Якщо протягом зазначеного періоду часу відповідь на запит не отримано, інтервал буде подвоєний, а запит повторений. Є можливість встановити число повторних спроб за допомогою підкоманди retry
ret [ry] = *число*	Вказує нове значення числа повторних спроб. За замовчуванням число повторних спроб дорівнює 4. Якщо протягом зазначеного періоду часу відповідь на запит не отримано, інтервал буде подвоєний, а запит повторений. Заданий параметру значення визначає, скільки разів запит буде повторений. Є можливість змінити період очікування за допомогою підкоманди timeout .
rec [urse] | norec [urse]	Вказує (або скасовує) сервера імен DNS, що необхідно відправити запит інших серверів в разі, якщо він сам не має в своєму розпорядженні необхідною інформацією. За замовчуванням використовується синтаксис recurse .
ty [pe] = *min_zanici_ресурса*	Вказує тип запису ресурсу DNS. За замовчуванням використовується тип A. Можливі значення (найбільш використовувані): any - Вказує все типи даннях cname - Вказує канонічне ім'я для псевдоніма mx - запит адреси поштових серверів ns - запит даних про серверах імен

Приклад використання утиліти nslookup:

Отримання списку серверів імен для домену google.com без входу в командний режим (з використанням ключів).

```
C:\> nslookup -type=ns google.com
Server:  google.com
Address:  216.58.215.78
Non-authoritative answer:
google.com      nameserver = ns4. google.com
google.com      nameserver = ns1. google.com
google.com      nameserver = ns2. google.com
google.com      nameserver = ns3. google.com
```

3 Ключові питання

3.1 Укажіть призначення й основні параметри утиліти ipconfig

3.2 Укажіть призначення й основні параметри утиліти arp.

3.3 Укажіть призначення утиліти nslookup.

3.4 Для чого використовується утиліта netstat ?

3.5 Який протокол необхідний для роботи з утилітами?

3.6 Який результат видасть утиліта netstat з параметрами –a, –s та –r?

3.7 Як можна за допомогою утілити оновити IP-адресу?

4 Домашнє завдання

4.1 Вивчіть, користуючись даними методичними вказівками, вбудовані засоби, що призначені для діагностики стану мережі на основі TCP/IP.

4.2 Підготуйте протокол лабораторної роботи, у якому вказана тема, мета роботи, відповіді на ключові питання п.3..

5 Лабораторне завдання

5.1 Виконайте наступні завдання:

- запишіть основні параметри мережної конфігурації PC, а саме фізичну адресу, IP-адресу, маску підмережі, основний шлюз та DHCP-сервер.
- для оновлення конфігурації IP-адреси, яка визначена DHCP-сервером, тільки для адаптера «Підключення по локальній мережі», введіть: ipconfig /renew;
- для того, щоб скинути кеш порівняння імен DNS за наявності несправностей у порівнянні імен, введіть: ipconfig /flushdns;
- для того, щоб вивести код класу DHCP для всіх адаптерів, які починаються зі слова Подключение, введіть: /allcompartments

5.2 Виконайте наступні завдання:

– для виведення таблиці кеша ARP для усіх інтерфейсів, введіть: arp –a;

– для того, щоб вивести таблицю кеша ARP для інтерфейсу, якому призначена IP-адреса 10.0.9.51, введіть: arp -a -N 10.0.9.51;

– додайте статичний запис кешу ARP, який порівнює IP-адресу 10.0.0.80 з фізичною адресою 00-AA-00-4F-2A-9C, введіть:

arp - 10.0.0.80 00-AA-00-4F-2A-9C.

5.3 Виконайте наступні завдання:

– для відображення статистики Ethernet та статистики по всіх протоколах введіть наступну команду: netstat -e –s;

– для відображення статистики лише за протоколами TCP і UDP введіть наступні команди: netstat -s –p tcp, або netstat -s –p udp;

– для відображення активних підключень TCP та кодів процесів кожні 5 секунд введіть наступну команду: netstat -o 5;

– для відображення активних підключень TCP та кодів процесів з використанням числового формату введіть наступну команду: netstat -n -o.

Примітка.

Діагностика проблем з низькою швидкістю закачування:

G:\>netstat -a

Якщо ви закрили всі додатки, які пов’язані з Інтернетом, а при цьому залишаються процеси зі станом ESTABLISHED, то саме з цим можуть бути пов’язані проблеми низької швидкісті (ці процеси без відома користувача завантажують частину каналу).

Побачити які це процеси можна за допомогою ключа -o.

G:\>netstat -o

Побачити, яку кількість інформації відправлено та отримано за певний період часу можна, запустивши команду з ключем -e, двічі з інтервалом 5 секунд і порівняти результати.

G:\>netstat -e

5.4 Виконайте наступні завдання:

– дізнайтеся ip-адреси вузлів: facebook.com, youtube.com, ukr.net;

– отримайте DNS-інформацію за допомогою команди nslookup -type=ns google.com, дізнайтесь назви серверів та дізнайтесь їх адресу.

5.5 Результати з виконання команд зафіксувати у звіті.

6 Зміст протоколу

1. Тема.
2. Мета роботи.
3. Результати виконання домашнього завдання.
4. Короткий опис виконання лабораторного завдання.
5. Висновки.

7 Література

1. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А.Олифер. // Учебник для вузов. – 5-е изд. – СПб.: Питер, 2016. – 992с.

2. Таненбаум Э. Компьютерные сети / Э. Таненбаум, Д.Уэзеролл. – 5-е изд. – СПб.: Питер, 2012. – 960 с.

3. Моримото Р. Microsoft Windows Server 2008 R2. Полное рук-во / Моримото Р., Ноэл М., Драуби О., Мистри Р., Амарис К. // Пер. с англ. — М. : ООО "И.Д. Вильямс", 2011. — 1456с. : ил.