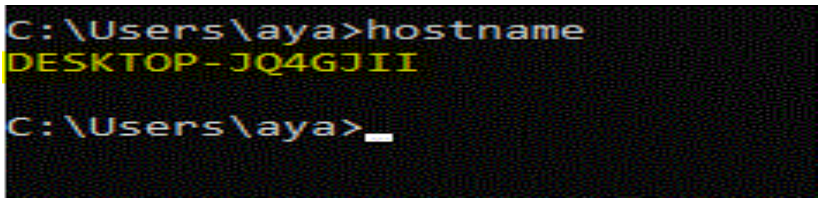
TP1

Objectifs :

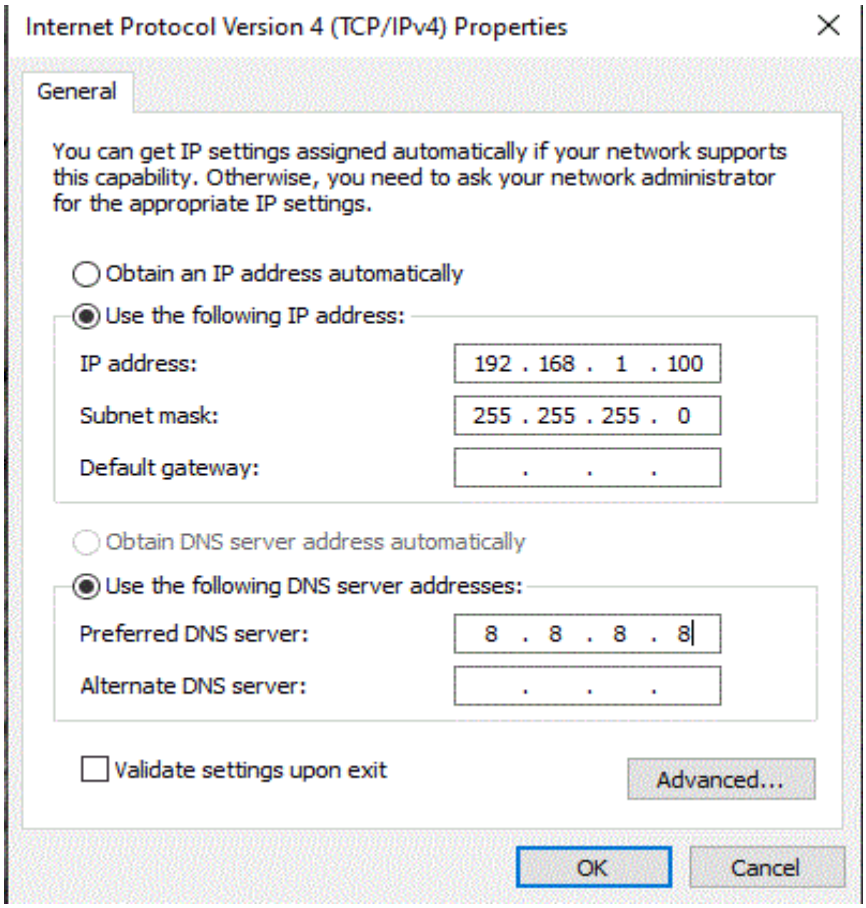
- Comprendre le fonctionnement d'un serveur DNS.
- Savoir le processus de résolution d'un nom de domaine en adresse IP et ses différentes étapes.
- Savoir créer un serveur DNS, ajouter des rôles et des fonctionnalités DNS...

1. Adresse IP, et serveur DNS :

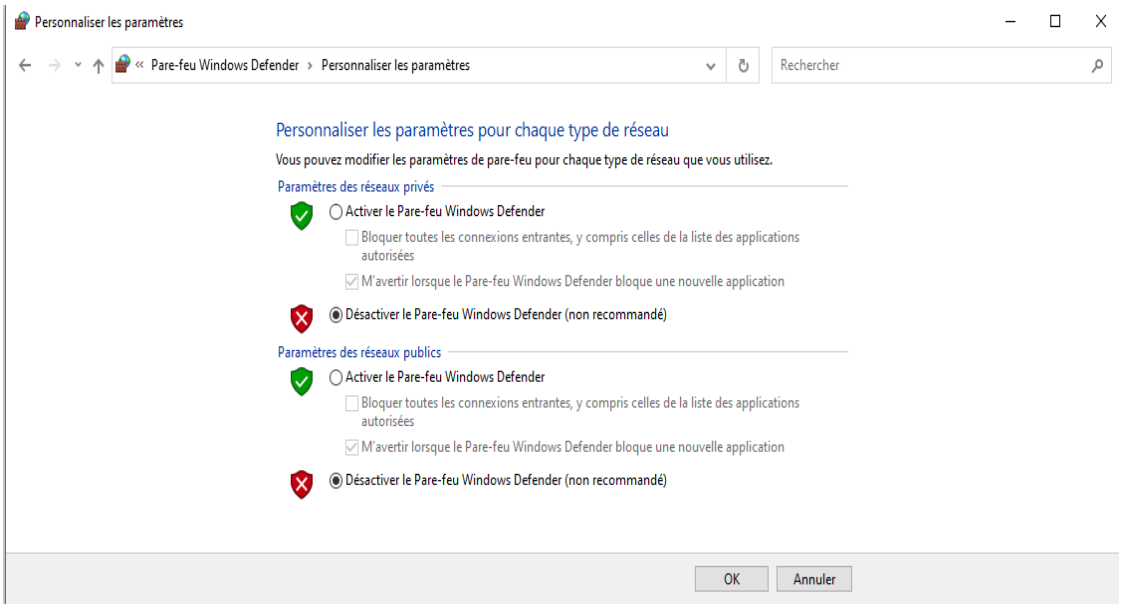
- Tapez cmd, puis afficher le nom de votre host par la commande :**hostname**



- Changer l'adresse IP de votre machine en 192.168.1.100, ainsi que l'adresse IP de votre DNS préféré en 8.8.8.8



- Désactiver la pare-feu Windows.



- Tapez Ping www.google.com. L'ordinateur doit convertir www.google.com en adresse IP pour savoir ou envoyer les paquets ICMP (Internet Control Message Protocol). La commande Ping est un type de paquet ICMP.

```
C:\Users\aya>ping www.google.com

Pinging www.google.com [142.251.37.164] with 32 bytes of data:
Reply from 142.251.37.164: bytes=32 time=633ms TTL=118
Reply from 142.251.37.164: bytes=32 time=579ms TTL=118
Reply from 142.251.37.164: bytes=32 time=178ms TTL=118
Reply from 142.251.37.164: bytes=32 time=92ms TTL=118

Ping statistics for 142.251.37.164:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 92ms, Maximum = 633ms, Average = 370ms
```

- **Quelle adresse IP s'affiche à l'écran ?**
  ⇨ **142.251.37.164**
- **Est-ce la même que celle de la capture d'écran ? Pourquoi ?**
  ⇨ **Non, il n'est pas la même car le DNS nous fournit une adresse IP proche à son adresse**
- **A l'invite de commandes, tapez la commande nslookup**

```
C:\Users\aya>nslookup
Default Server:  monrouteur.home
Address:  192.168.1.1
```

- **Quel est le serveur DNS par défaut utilisé ?**
  ⇨ **Le serveur monrouteur.home**
- Notez en quoi l'invite de commandes a changé. Il s'agit de l'invite nslookup. Dans cette invite, vous pouvez entrer des commandes liées au système DNS.

- A l'invite, tapez pour afficher la liste de toutes les commandes disponibles pouvant être utilisées en mode nslookup

```
> ?
Commandes :   (les identificateurs sont en majuscules, [] signifie en option)
NOM             - affiche des infos concernant le NOM d'hôte/de domaine en
                  utilisant le serveur par défaut
NOM1 NOM2       - comme ci-dessus, en utilisant NOM2 en tant que serveur
help ou ?       - affiche des informations sur les commandes communes
set OPTION      - paramètre une option
    all             - affiche les options, le serveur actuel et l'hôte
    [no]debug       - affiche des informations de débogage
    [no]d2          - affiche toutes les informations de débogage
    [no]defname     - ajoute le nom de domaine à chaque requête
    [no]recurse     - donne une réponse récursive aux requêtes
    [no]search      - utilise la liste de recherche du domaine
    [no]vc          - toujours utiliser un circuit virtuel
    domain=NOM      - donne le nom NOM au serveur de domaine par défaut
    srchlist=N1[/N2/.../N6] - donne au domaine le nom N1 et liste de recherche
                          N1,N2, etc.
    root=NOM        - donne au serveur racine le nom NOM
    retry=X         - effectue X tentatives
    timeout=X       - définit la durée d'attente initiale à X secondes
    type=X          - définit le type de requête (ex. A,AAAA,A+AAAA, ANY,
                          CNAME, MX, NS, PTR, SRV)
    querytype=X     - identique à type
    class=X         - définit la classe de requête (ex. IN (Internet), ANY)
    [no]msxfr       - utilise le transfert de zone rapide MS
    ixfrver=X       - version à utiliser dans les requêtes de transfert IXFR
server NOM      - fixe le serveur par défaut en cours à NOM
lserver NOM     - fixe le serveur par défaut à NOM, avec le serveur initial
```

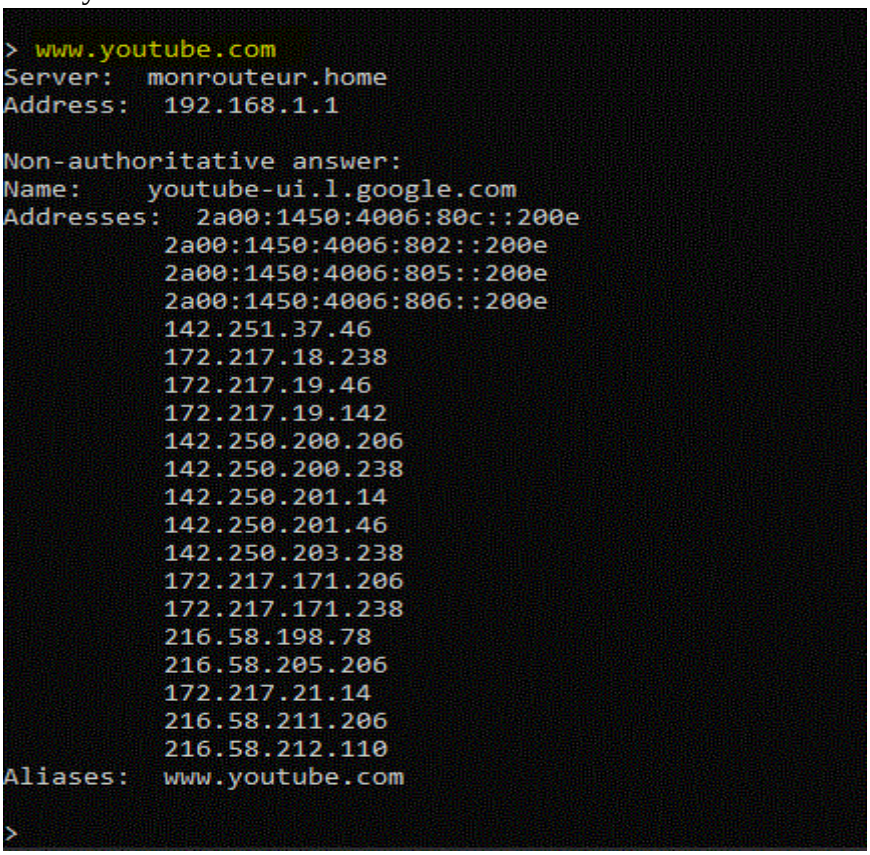
- A l'invite **nslookup**, tapez www.google.com. Quelle est l'adresse IP convertie ?

```
C:\Users\aya>nslookup
Default Server:  monrouteur.home
Address:  192.168.1.1

> www.google.com
Server:  monrouteur.home
Address:  192.168.1.1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2a00:1450:4006:811::2004
          142.251.37.164
```

- **Est-ce la même adresse IP que celle affichée avec la commande ping ?**
  ⇨ **Oui, on obtient la même adresse IP que celle affichée avec la commande ping.**
- A l'invite, tapez l'adresse IP du serveur Web google que vous venez de trouver. Vous pouvez utiliser nslookup pour obtenir le nom de domaine d'une adresse IP si vous ne connaissez pas l'URL

```
C:\Users\aya>nslookup 142.251.37.164
Server:  UnKnown
Address:  192.168.0.1

Name:    mrs09s14-in-f4.1e100.net
Address:  142.251.37.164
```

- A l’aide des procédures précédentes, recherchez une adresse IP associée à www.youtube.com



- A l’invite , tapez **ipconfig/all.**

```
C:\Users\aya>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-JQ4GJII
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : Home

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : Home
   Description . . . . . . . . . . . : Qualcomm Atheros AR8172/8176/8178 PCI-E Fast Ethernet Controller (NDIS 6.30)
   Physical Address. . . . . . . . . : 7C-05-07-D3-62-AA
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 16-FD-52-DE-EB-19
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : Home
   Description . . . . . . . . . . . : Qualcomm Atheros AR956x Wireless Network Adapter
   Physical Address. . . . . . . . . : 24-FD-52-DE-EB-19
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::fc62:f0a3:9fe0:56ec%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, March 30, 2022 9:05:51 PM
   Lease Expires . . . . . . . . . . : Thursday, March 31, 2022 9:47:01 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 103087442
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-21-89-7C-65-7C-05-07-D3-62-AA
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

2.Utiliser l'outil dig

- La commande dig peut offrir des informations très variées et détaillées dans différentes sections.

```
C:\Users\aya>dig

; <<>> DiG 9.16.27 <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60638
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       511252  IN      NS      e.root-servers.net.
.                       511252  IN      NS      k.root-servers.net.
.                       511252  IN      NS      d.root-servers.net.
.                       511252  IN      NS      j.root-servers.net.
.                       511252  IN      NS      c.root-servers.net.
.                       511252  IN      NS      l.root-servers.net.
.                       511252  IN      NS      h.root-servers.net.
.                       511252  IN      NS      b.root-servers.net.
.                       511252  IN      NS      m.root-servers.net.
.                       511252  IN      NS      a.root-servers.net.
.                       511252  IN      NS      f.root-servers.net.
.                       511252  IN      NS      i.root-servers.net.
.                       511252  IN      NS      g.root-servers.net.

;; Query time: 15 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Fri Apr 15 16:56:31 W. Europe Standard Time 2022
;; MSG SIZE  rcvd: 239
```

- Renvoie tout enregistrement A trouvé dans la zone du nom d'hôte interrogé.

  - dig www.usmba.ac.ma

```
C:\Users\aya>dig www.usmba.ac.ma

; <<>> DiG 9.16.27 <<>> www.usmba.ac.ma
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25142
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.usmba.ac.ma.               IN      A

;; ANSWER SECTION:
www.usmba.ac.ma.        2060    IN      A       196.200.146.77

;; Query time: 23 msec
;; SERVER: 192.168.1.254#53(192.168.1.254)
;; WHEN: Thu Mar 31 17:52:59 W. Europe Standard Time 2022
;; MSG SIZE  rcvd: 60
```

- Fournit une réponse courte, généralement une seule adresse IP.

  - dig www.usmba.ac.ma +short

```
C:\Users\aya>dig www.usmba.ac.ma +short
196.200.146.77
```

- L'ajout de l'instruction +trace indique à dig qu'il doit résoudre la requête vers le bas à partir du serveur de noms racine, puis signaler les résultats de chaque étape de la requête.

  - dig dyn.com +trace

```
C:\Users\aya>dig dyn.com +trace

; <<>> DiG 9.16.27 <<>> dyn.com +trace
;; global options: +cmd
;; connection timed out; no servers could be reached
```

- Recherche inversée d'adresses IP.

  - dig -x 137.254.16.101

```
C:\Users\aya>dig -x 137.254.16.101

; <<>> DiG 9.16.27 <<>> -x 137.254.16.101
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22425
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;101.16.254.137.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
101.16.254.137.in-addr.arpa. 10558 IN   PTR     bigip-ocoma-cms-adc.oracle.com.

;; Query time: 66 msec
;; SERVER: 192.168.1.254#53(192.168.1.254)
;; WHEN: Thu Mar 31 18:10:10 W. Europe Standard Time 2022
;; MSG SIZE  rcvd: 100
```

3 .Processus de résolution d'un nom de domaine/adresse IP

Lorsqu'un client DNS exécutant Windows souhaite résoudre un nom de domaine en adresse IP, un processus décomposable en plusieurs étapes est exécuté :

3.1 Résolution DNS

Le client commence par vérifier si une adresse IP correspondant au nom d'hôte est présente dans le cache de noms DNS. Le cache de noms DNS contient tous les mappages noms d'hôte / adresses IP stockées en RAM.

⇨ Afficher le cache DNS de votre serveur local en exécutant

-ipconfig/displaydns

```
C:\Users\aya>ipconfig/displaydns

Windows IP Configuration

    safebrowsing.googleapis.com
    ----------------------------------------
    Record Name . . . . . : safebrowsing.googleapis.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 38
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 172.217.18.234


    245.137.168.192.in-addr.arpa
    ----------------------------------------
    Record Name . . . . . : 245.137.168.192.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live  . . . . : 411786
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    PTR Record  . . . . . : iPhone.mshome.net


    229.137.168.192.in-addr.arpa
    ----------------------------------------
    Record Name . . . . . : 229.137.168.192.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live  . . . . : 411786
```

⇨ Pour vider cette mémoire cache tapez la commande

- ipconfig/flushdns

```
C:\Users\aya>ipconfig/flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\aya>
```

Si l'adresse IP recherchée n'est pas présente dans le cache de noms DNS, alors le client consulte le fichier hosts. Ce fichier est situé dans le répertoire %SY ST EMROOT % \ system32 \ drivers \ etc Par défaut, il contient uniquement le mappage entre le nom d'hôte localhost et l'adresse IP 127.0.0.1. Si le mappage n'a pas été trouver dans le fichier hosts, alors le client va envoyer une requête DNS au premier serveur DNS dont l'adresse IP a été définie dans ses paramètres TCP/IP.

3.2 Résolution de nom NetBIOS

- Si le client n'a pas trouvé le mappage recherché alors il considère que l'adresse IP recherchée ne correspond pas à un nom d'hôte mais `a un nom NetBIOS et lance une résolution de nom NetBIOS. La résolution de noms NetBIOS se passe en plusieurs étapes :
- La Cache de noms NetBIOS : Vérification de la présence de l'adresse IP dans la cache de noms NetBIOS.
- Pour afficher le cache de noms NetBIOS en utilisant la commande **nbtstat -c**

```
C:\Users\aya>nbtstat -c

VMware Network Adapter VMnet8:
Node IpAddress: [192.168.44.1] Scope Id: []

    No names in cache

HMA! Pro VPN:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

VMware Network Adapter VMnet1:
Node IpAddress: [192.168.89.1] Scope Id: []

    No names in cache

Ethernet:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Wi-Fi:
```

- Pour vider cette mémoire cache grâce à la commande **nbtstat -r**

```
C:\Users\aya>nbtstat -r

    NetBIOS Names Resolution and Registration Statistics
    ----------------------------------------------------

    Resolved By Broadcast     = 0
    Resolved By Name Server   = 0

    Registered By Broadcast   = 115
    Registered By Name Server = 0
```

- Pour afficher le nom NetBios : **nbtstat -n**

```
C:\Users\aya>nbtstat -n

VMware Network Adapter VMnet8:
Node IpAddress: [192.168.44.1] Scope Id: []

               NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    DESKTOP-JQ4GJII<20>  UNIQUE      Registered
    DESKTOP-JQ4GJII<00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered

HMA! Pro VPN:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

VMware Network Adapter VMnet1:
Node IpAddress: [192.168.89.1] Scope Id: []

               NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    DESKTOP-JQ4GJII<20>  UNIQUE      Registered
    DESKTOP-JQ4GJII<00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered

Ethernet:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Wi-Fi:
Node IpAddress: [192.168.0.19] Scope Id: []

               NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    DESKTOP-JQ4GJII<20>  UNIQUE      Registered
    DESKTOP-JQ4GJII<00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
```

```
       Name                Type         Status
    -------------------------------------------
    DESKTOP-JQ4GJII<20>  UNIQUE      Registered
    DESKTOP-JQ4GJII<00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered

Local Area Connection* 1:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Local Area Connection* 12:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache
```