REQUETE ARP

PING / WIRESHARK

Postes :

172.21.255.22 et 172.21.255.21

Machine Virtuelle Windows 7x64

Réseau : VMware en « LAN SEGMENT »

1/ Arp –d * sur les 2 postes

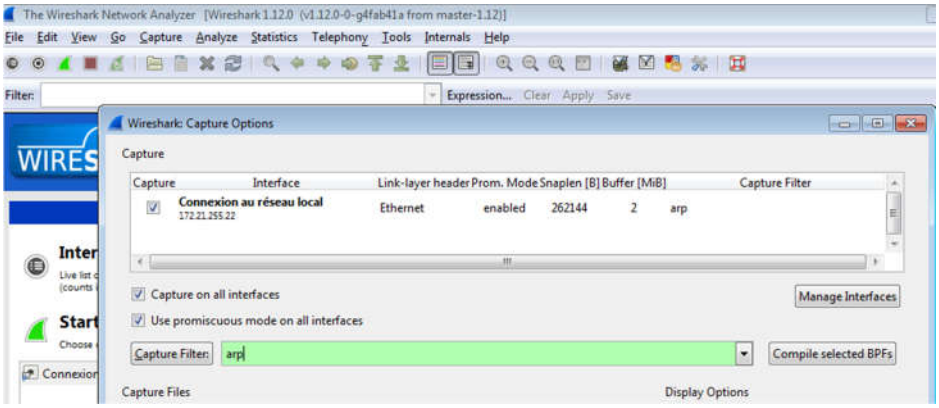
2/ installation sur « 22 » de wireshark

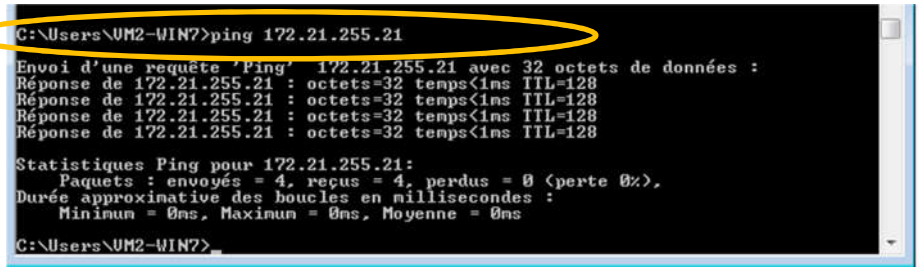
3/ lancement de wireshark sur « 22 »

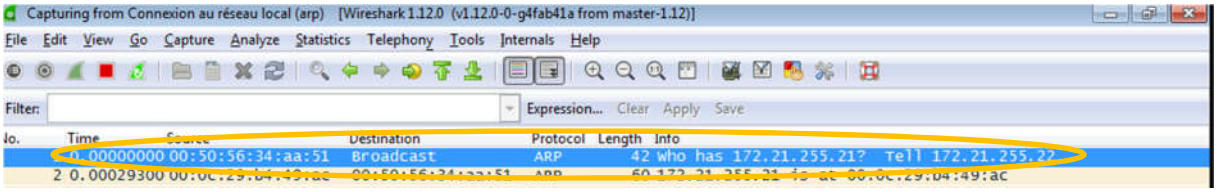
Erreur au lancement « msvcp140.dll » manquant

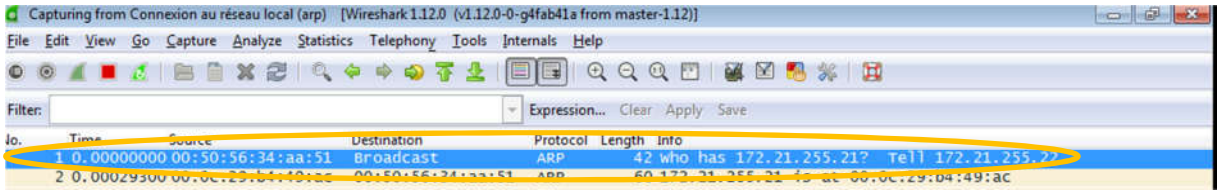
Téléchargement version ancienne x86 : 1.12 qui fonctionne

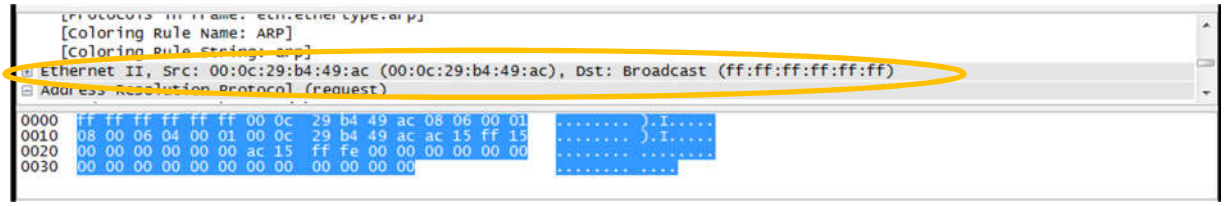
4/ ping 172.21.255.21 depuis le « 22 »



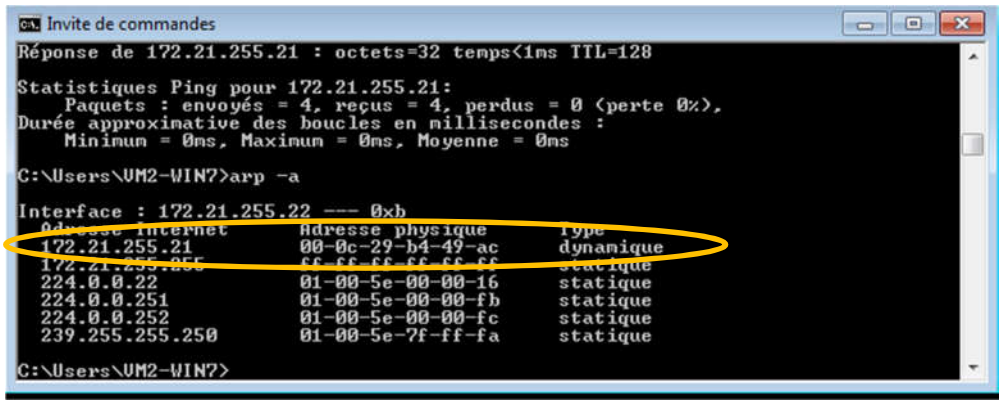








Vérification



5/ ping sur le nom « winSeven2 » du poste en « 21 » depuis poste en « 22 »

Un concurrent peu présent : le LLMNR

LLMNR, qui signifie **L**ink-**L**ocal **M**ulticast **N**ame **R**esolution, est un protocole de résolution de noms. Tout comme mDNS, LLMNR, développé par Microsoft, s'est basé sur le travail du protocole Multicast Domain Name Service.

Le principe de fonctionnement de ce protocole diffère très peu de mDNS. En effet, LLMNR s'appuie aussi sur le format standardisé des paquets DNS définis dans la RFC 1035. De plus, la similarité ne s'arrête pas là.

Le port utilisé pour envoyer les requêtes DNS est le port **UDP 5355** (pour rappel, mDNS utilise le port UDP 5353) et permet ainsi à un serveur DNS la possibilité d'implémenter en supplément le protocole LLMNR.

L'adresse de multicast est elle aussi très ressemblante puisqu'il a été choisi de communiquer sur l'adresse **224.0.0.252** ou son équivalent IPv6 **FF02::1:3** (mDNS : 224.0.0.251 ou FF02::FB).

La différence majeure entre les deux protocoles se situe au niveau de la gestion des noms de domaine. Là où mDNS n'autorise que des noms de domaine sur l'espace "**.local.**", LLMNR laisse la possiblité de choisir n'importe lequel. Ce qui, pour certains membres de l'IETF représente un grave problème de sécurité.

Dernier point de comparaison, le protocole LLMNR n'est pas compatible avec le protocole DNS-SD. Or, celui-ci est un élément essentiel du projet Zeroconf et l'incompatibilité avec DNS-SD a donc rendu LLMNR obsolète.

Pour finir, le protocole LLMNR n'a donc pas réussi à s'imposer comme standard de la résolution de noms sur un domaine local. Il dispose néanmoins d'une RFC informel : **RFC 4795**.

```
C:\Windows\system32>ping winseven2

Envoi d'une requête 'ping' sur winSeven2 [172.21.255.21] avec 32 octets de donné
es :
```

*Connexion au réseau local [Wireshark 1.12.0 (v1.12.0-0-g4fab41a from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	172.21.255.22	224.0.0.252	LLMNR	69	Standard query 0x4d1b A winSeven2
2	0.00088800	00:0c:29:b4:49:ac	Broadcast	ARP	60	who has 172.21.255.22? Tell 172.21.255.21
3	0.00088800	00:50:56:34:aa:51	00:0c:29:b4:49:ac	ARP	42	172.21.255.22 is at 00:50:56:34:aa:51
4	0.00625400	172.21.255.21	172.21.255.22	LLMNR	94	Standard query response 0x4d1b A 172.21.255.21
5	0.00643900	172.21.255.22	224.0.0.252	LLMNR	69	Standard query 0xca41 AAAA winSeven2
6	0.00817300	172.21.255.21	172.21.255.22	LLMNR	122	Standard query response 0xca41
7	0.00956800	172.21.255.22	172.21.255.21	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (repl
8	0.00968200	172.21.255.21	172.21.255.22	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=128 (requ
9	1.01392200	172.21.255.22	172.21.255.21	ICMP	74	Echo (ping) request id=0x0001, seq=16/4096, ttl=128 (no r
10	1.01449500	172.21.255.21	172.21.255.22	ICMP	74	Echo (ping) reply id=0x0001, seq=16/4096, ttl=128 (requ
11	2.02693200	172.21.255.22	172.21.255.21	ICMP	74	Echo (ping) request id=0x0001, seq=17/4352, ttl=128 (no r
12	2.02741700	172.21.255.21	172.21.255.22	ICMP	74	Echo (ping) reply id=0x0001, seq=17/4352, ttl=128 (requ
13	2.28598900	00:50:56:34:aa:51	Broadcast	ARP	42	who has 172.21.255.254? Tell 172.21.255.22
14	3.05990100	172.21.255.22	172.21.255.21	ICMP	74	Echo (ping) request id=0x0001, seq=18/4608, ttl=128 (no r
15	3.06052300	172.21.255.21	172.21.255.22	ICMP	74	Echo (ping) reply id=0x0001, seq=18/4608, ttl=128 (requ
16	4.77613500	00:50:56:34:aa:51	00:0c:29:b4:49:ac	ARP	42	who has 172.21.255.21? Tell 172.21.255.22
17	4.77644100	00:0c:29:b4:49:ac	00:50:56:34:aa:51	ARP	60	172.21.255.21 is at 00:0c:29:b4:49:ac

```
⊟ Ethernet II, Src: 00:0c:29:b4:49:ac (00:0c:29:b4:49:ac), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Source: 00:0c:29:b4:49:ac (00:0c:29:b4:49:ac)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
```

```
1 0.00000000 172.21.255.22    224.0.0.252     LLMNR    69 Standard query 0x4d1b  A winSeven2
```

```
Queries
  winSeven2: type A, class IN
    Name: winSeven2
    [Name Length: 9]
    [Label Count: 1]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
```

```
4 0.00625400 172.21.255.21    172.21.255.22   LLMNR    94 Standard query response 0x4d1b  A 172.21.255.21
5 0.00643900 172.21.255.22    224.0.0.252     LLMNR    69 Standard query 0xca41  AAAA winSeven2
6 0.00817300 172.21.255.21    172.21.255.22   LLMNR   122 Standard query response 0xca41
```

```
16 4.77613500 00:50:56:34:aa:51   00:0c:29:b4:49:ac   ARP   42 Who has 172.21.255.21?  Tell 172.21.255.22
17 4.77644100 00:0c:29:b4:49:ac   00:50:56:34:aa:51   ARP   60 172.21.255.21 is at 00:0c:29:b4:49:ac
```

Vérification

```
Administrateur : Invite de commandes

C:\Windows\system32>ping winSeven2

Envoi d'une requête 'ping' sur winSeven2 [172.21.255.21] avec 32 octets de donné
es :
Réponse de 172.21.255.21 : octets=32 temps<1ms TTL=128
Réponse de 172.21.255.21 : octets=32 temps<1ms TTL=128
Réponse de 172.21.255.21 : octets=32 temps<1ms TTL=128
Réponse de 172.21.255.21 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 172.21.255.21:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Windows\system32>arp -a

Interface : 172.21.255.22 --- 0xb
  Adresse Internet      Adresse physique      Type
  172.21.255.21         00-0c-29-b4-49-ac     dynamique
  172.21.255.255        ff-ff-ff-ff-ff-ff     statique
  224.0.0.252           01-00-5e-00-00-fc     statique
  239.255.255.250       01-00-5e-7f-ff-fa     statique

C:\Windows\system32>_
```