Accès aux machines

Liens pratiques:

https://ent.univ-rennes1.fr/f/intranet/p/rssEtuEsirIstic.u27l1n88/max/render.uP?pCp

Portal VPN (depuis le navigateur):

https://istic-vpn.univ-rennes1.fr/

Depuis le réseau local de l'ISTIC

- En ligne de commande

  ssh zprojet@[VMS].istic.univ-rennes1.fr
- VMS:
  - ares1,ares2, ..., ares20

Compte utilisateur:

```
User : zprojet
Passwd: Zistic*!1
```

Passer en mode administrateur :

```
$ sudo su
```

Entrer votre mot de passe

En tant que administrateur, vous pouvez changer le mot passe :

```
# passwd
```

TP 1 : Introduction aux réseaux d'entreprise et services de base

Durée : 1h30

Objectif :

Se familiariser avec la configuration et la gestion des services réseau essentiels (DHCP, DNS) tout en introduisant des concepts avancés comme le DHCP Relay, le DNS dynamique, et la gestion des conflits d'adresses MAC. Vous allez apprendre à configurer ces services et à tester leur bon fonctionnement sur des hôtes virtuels.

Outils :

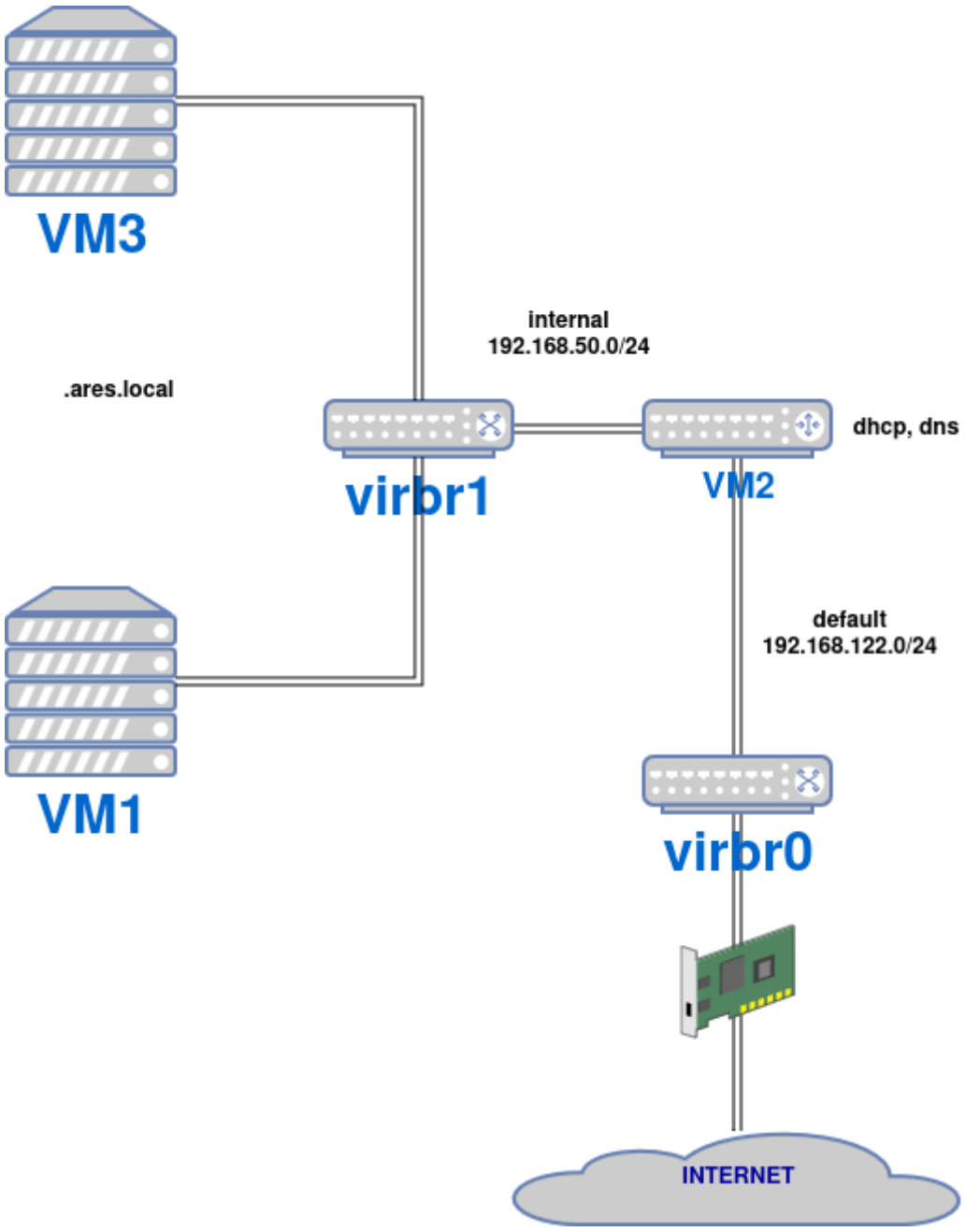
- **DNSMasq** : Outil léger pour la gestion du DHCP et du DNS.
- **isc-dhcp-relay** : Outil léger pour la gestion du relay DHCP.
- **Linux (Ubuntu)** : Système d'exploitation utilisé pour les configurations.

- **KVM** : Environnement de virtualisation pour tester les configurations sur plusieurs machines virtuelles.

Prérequis :

- Partant du premier TP, nous utiliserons la machine routeur (VM2) pour ajouter les services DNS et DHCP.
- Tout se passe sur la machine virtuelle routeur (VM2). Vous devez installer et configurer DHCP et DNS à l'aide de **dnsmasq**.
- Il faudra s'assurer que le routage fonctionne correctement (voir TP précédent).
- Il n'est plus nécessaire d'avoir une adresse IP sur l'interface **virbr1**, vous pouvez la supprimer.
- Il est recommandé de bien établir son plan d'adressage et d'identifier correctement les interfaces réseau.
- Les noms des interfaces donnés dans ce TP sont à titre indicatif et peuvent ne pas correspondre aux vôtres.

Plan du TP



1. Installation de DNSMasq

> Par défaut, sur Ubuntu, **systemd-resolved** gère le fichier `/etc/resolv.conf` et un DNS local sur le port 53. Il est important de désactiver ce service pour la bonne marche du TP.

- Désactiver **systemd-resolved** :

```
sudo systemctl disable systemd-resolved.service
sudo systemctl stop systemd-resolved
```

- Mettre à jour le DNS en indiquant l'adresse IP du bridge (virbr0) :

```
echo nameserver 192.168.122.1 > /etc/resolv.conf
```

- **Q1** : Pourquoi faut-il mettre à jour la référence du DNS ?
- Mise à jour et installation de DNSMasq :

```
sudo apt update && sudo apt install dnsmasq -y
```

2. Configuration de DNSMasq pour DHCP et DNS de base

- Configurer le service DHCP dans le fichier de configuration `/etc/dnsmasq.d/ares.conf` :

  Remarque : Au préalable, `enp1s0` doit être configuré avec l'adresse IP `192.168.50.2`. Si ce n'est pas le cas, faites-le.

```
# Empêcher les requêtes DNS inversées pour les adresses IP privées d'être envoyées à des serveurs DNS publics
bogus-priv

# Configurer l'interface d'écoute
interface=enp1s0
listen-address=127.0.0.1,192.168.50.2

# Plage d'adresses pour DHCP
dhcp-range=192.168.50.3,192.168.50.5,12h
```

- Décommentez la ligne `conf-dir=/etc/dnsmasq.d` dans le fichier `/etc/dnsmasq.conf`.
- Redémarrer le service pour appliquer les changements :

```
sudo systemctl restart dnsmasq
```

- Effectuer les tests sur la machine VM1 pour vérifier le bon fonctionnement du DHCP :

```
dhclient -r <interface_réseau>   # Libérer l'ancien bail
dhclient -v <interface_réseau>   # Renouveler le bail
```

- Vérifier les adresses IP obtenues.

3. Paramétrage de la résolution DNS des machines virtuelles

Objectif : Permettre la mise à jour dynamique des enregistrements DNS par les hôtes lorsqu'ils obtiennent une adresse via DHCP.

- Éditer le fichier `/etc/dnsmasq.d/ares.conf` comme suit :

```
bogus-priv
interface=enp1s0
listen-address=127.0.0.1,192.168.50.2
dhcp-range=192.168.50.3,192.168.50.5,12h
server=8.8.8.8   # Utiliser ce DNS pour la résolution des domaines publics

# Donner le DNS aux clients
dhcp-option=6,192.168.50.2,4.2.2.2

# Gestion du domaine, mettre les VMs dans le domaine ares.local
domain=ares.local
dhcp-option=15,ares.local
```

Redémarrez le service **dnsmasq** sur VM2 et refaites les tests sur les machines clientes (VM1). Confirmez que le fichier `/etc/resolv.conf` a été mis à jour avec les informations du domaine local des VMs. Dans VM1, effectuez un ping vers VM1 et observez le résultat de la commande :

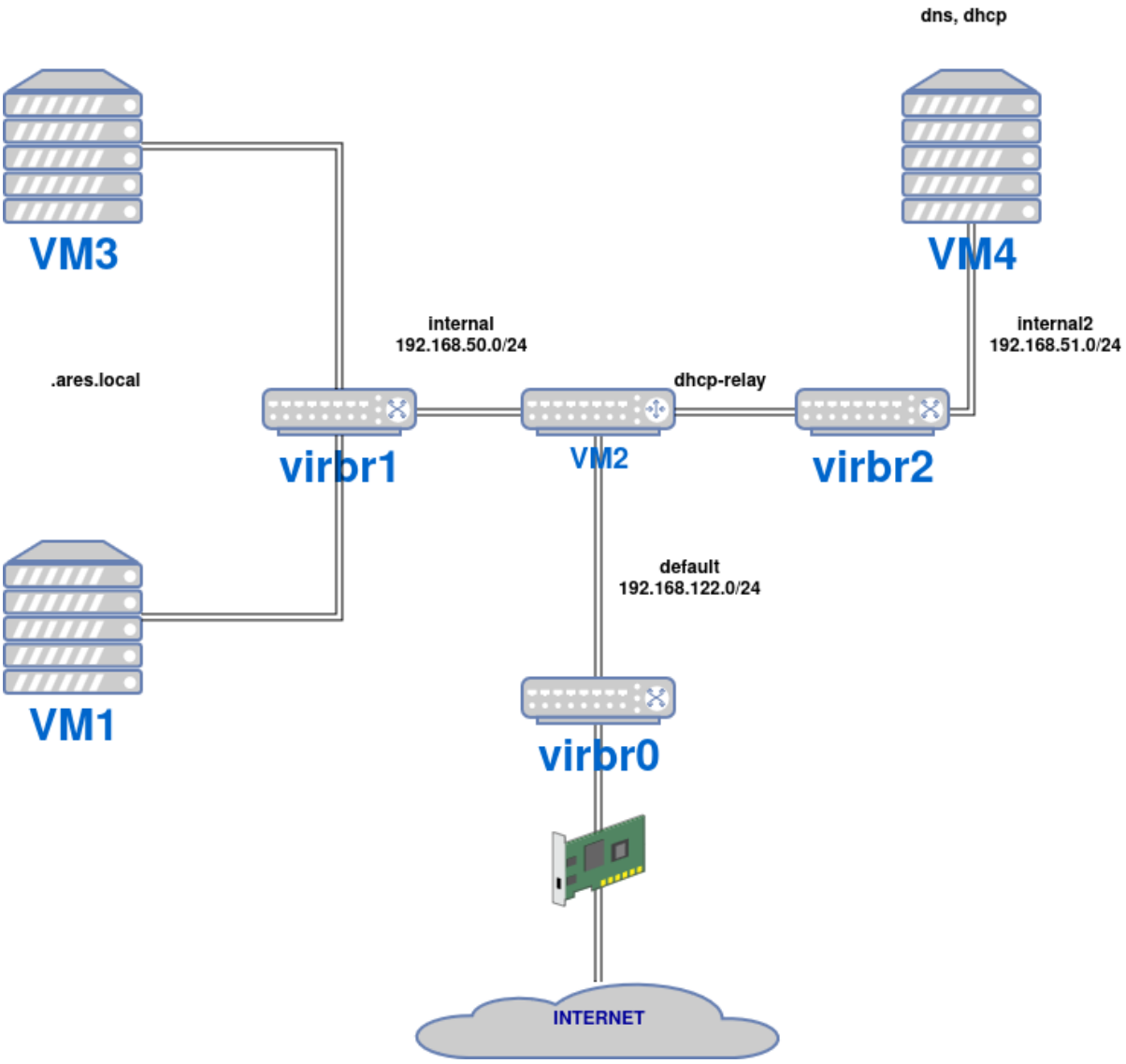
```
ping vm1
```

Exemple de résultat :

```
PING vm1.ares.local (192.168.50.4) 56(84) bytes of data.
64 bytes from vm1.ares.local (192.168.50.4): icmp_seq=1 ttl=64 time=0.078 ms
```

4. DHCP Relay

Objectif : Configurer un relais DHCP pour transmettre les requêtes DHCP vers un autre sous-réseau.



- Sur VM2, vous devez désinstaller **dnsmasq** et installer un relais DHCP (**isc-dhcp-relay**).

Avant de commencer, assurez-vous d'établir un plan d'adressage clair, d'identifier les interfaces réseau et leur connexion aux switches virtuels.

Le switch **virbr2** devra être créé comme dans le TP précédent. Faites le nécessaire pour relier VM2 au switch virtuel.

- Suppression de dnsmasq :

```
sudo systemctl stop dnsmasq
sudo apt-get remove dnsmasq && sudo apt-get purge dnsmasq
```

- Installation de isc-dhcp-relay dans VM2 :

```
sudo apt-get install -y isc-dhcp-relay
```

- Configuration du relais DHCP dans `/etc/default/isc-dhcp-relay` :

```
SERVERS="<adresse IP du serveur relay>"
INTERFACES="<interface_connectée_a_virbr1> <interface_connectée_a_virbr2>"
```

- Créer une nouvelle machine virtuelle (VM4) et y installer **dnsmasq** avec les configurations ci-dessus.
- **Mettre en place la configuration** qui correspond à votre architecture en termes d'adresses IP. Vous pouvez désormais supprimer l'adresse IP du switch **virbr2**.
- **Test** : Sur VM1, essayez d'obtenir un bail DHCP :

```
sudo dhclient -v <votre_interface_reseau>
```

- **Question** : Pourquoi ça ne marche pas ? Faites le nécessaire sur VM4 pour que cela fonctionne.

5. Sécurisation DNS avec DNSSEC

Objectif : Introduire **DNSSEC** pour sécuriser les résolutions DNS.

- Configurer DNSMasq pour supporter DNSSEC dans `/etc/dnsmasq.conf` :

```
conf-file=/usr/share/dnsmasq-base/trust-anchors.conf
dnssec
```

- **Test** : Vérifiez la signature des réponses DNS :

```
dig +dnssec example.com
```

- **Question** : À quoi sert DNSSEC ?

6. Vérification et supervision des logs

- Activer les logs sur le serveur **dnsmasq** en ajoutant les directives ci-dessous. Refaire les tests d'attribution DNS/DHCP (éditez `/etc/dnsmasq.d/ares.conf`) :

```
log-dhcp
log-queries
```

- Examiner les logs pour diagnostiquer les configurations :

```
tail -f /var/log/syslog
```

- Analyser les requêtes DHCP et DNS, ainsi que les mises à jour dynamiques des enregistrements DNS.

Compétences développées :

- Gestion des services réseau de base : Configuration d'un serveur DHCP, DNS, et de DNS dynamique avec DNSMasq.
- Gestion des services avancés : Utilisation de DHCP Relay et DNSSEC pour des environnements réseaux évolués.
- Routage de base : **iptables**, table de routage.

Questions à répondre :

1. Comment DNS dynamique facilite-t-il la gestion des noms d'hôtes dans un réseau avec des adresses IP dynamiques ?
2. Quelles sont les implications de la gestion du **DHCP Relay** dans un environnement réseau ?

Ce TP permet aux étudiants de se familiariser avec la gestion des services réseau tout en les confrontant à des problématiques plus avancées telles que la sécurité avec DNSSEC et la gestion des relais DHCP.