********** DM **********

1. Routes et interfaces

La configuration "persistante" des interfaces réseaux et des routes est faite dans le fichier /etc/network/interfaces.
Par exemple votre fichier /etc/network/interfaces de m6 doit ressembler à :

```
auto lo
iface lo inet loopback

auto eth2
iface eth2 inet static
address 10.0.0.30
netmask 255.255.255.0
gateway 10.0.0.1

auto eth1
iface eth1 inet static
address 172.17.47.161
netmask 255.255.240.0

auto eth0
iface eth0 inet static
address 172.26.108.185
netmask 255.255.240.0
up ip route add 192.168.205.208/28 via 172.26.100.238 dev eth0
up ip route add 192.168.136.128/25 via 172.26.100.238 dev eth0
```

On doit mettre "auto eth0" pour demander le montage automatique de l'interface eth0 au démarrage.
Les commandes derrière "up" sont exécutées après le montage de l'interface correspondante. On a utilisé la commande "ip" pour créer les routes indirectes (on aurait aussi pu utiliser la commande "route").
L'argument gateway permet de spécifier la route par défaut, qu'il aurait aussi été possible de spécifier par

```
up ip route add default via 10.0.0.1/24 dev eth2
```

à la place de "gateway".
Sur m2 qui qui utilise DHCP pour acquérir ses données de connection, le fichier
/etc/network/interfaces doit être :

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp
```

2. Utilisation du serveur DNS de m7 sur les différentes machines

Il suffit de mettre la ligne suivante dans /etc/resolv.conf sur chaque machine (sauf m2 où le fichier est mis à jour par le client dhcp) :

```
nameserver 172.17.36.170
```

3. Activation du routage

Le routage doit être activé sur les routeurs m3 et m6 par l'une des commandes :

```
sysctl -w net.ipv4.ip_forward=1
```

ou

```
echo 1 >/proc/sys/net/ipv4/ip_forward
```

(attention, il faut un espace entre le 1 et le > sinon cela ne fonctionne pas).
Pour activer automatiquement le routage au démarrage de la machine il faut modifier
le fichier /etc/sysctl.conf en y ajoutant la ligne :

```
net.ipv4.ip_forward=1
```

(en fait elle y est déjà mais est commentée et il suffit d'enlever le #).

4. Serveur dns Cache unbound

Il faut dans le fichier /etc/unbound/unbound.conf :
-spécifier l'interface sur laquelle le serveur doit écouter en ajoutant la ligne suivante dans le fichier (au niveau où plusieurs lignes "interfaces" sont en commentaires) :

```
interface: 172.17.36.170
```

-autoriser l'utilisation du serveur par toutes les machines des différents réseaux en ajoutant des lignes "access-control" :

```
access-control: 192.168.136.128/25 allow
access-control: 192.168.205.208/28 allow
access-control: 172.26.96.0/20 allow
access-control: 172.17.32.0/20 allow
```

puis démarrer le serveur par :

```
/etc/init.d/unbound start
```

et vérifier qu'il a bien démarré.
Pour que le serveur soit démarré automatiquement au démarrage de la machine, vous auriez pu utiliser (ce qui n'était pas noté) :

```
update-rc.d unbound defaults
```

5. Serveur DHCP

Il faut mettre la configuration suivante dans le fichier /etc/dhcp/dhcpd.conf :

```
subnet 192.168.136.128 netmask 255.255.255.128 {
        range 192.168.136.214 192.168.136.233;
        option domain-name-servers 172.17.36.170;
        option routers 192.168.136.204;
        default-lease-time 3600;
        max-lease-time 7200;
}
host m2 {
    hardware ethernet 02:04:06:f2:3d:dd;
    fixed-address 192.168.136.167;
}
```

puis démarrer le serveur DHCP par :

```
/etc/init.d/isc-dhcp-server start
```

De même on aurait pu exécuter :

```
update-rc.d isc-dhcp-server defaults
```

pour que le serveur DHCP soit démarré automatiquement au démarrage de m1.

RESEAU

********** Configuration DHCP **********

- Fichier /etc/dhcp[3]/dhcpd.conf

```
# configuration du service dhcp du #serveur 1
# LACOUR Xavier

subnet 172.16.1.192 netmask 255.255.255.192 {
#adresse réseau 172.16.1.192 avec un #masque approprié.
     range 172.16.1.194 172.16.1.253;
#Ceci indique quelle est la plage d'adresses IP utilises
dans l'ensemble des adresses réservées aux clients.
#Les adresses comprises dans l'intervalle spécifié sont
alloues aux clients.
        option routeurs 172.16.1.254;
#Cette option définit la passerelle par défaut fournie aux
clients.
        option domain-name-servers 192.168.0.2;
#Cette option donne une liste de serveurs DNS que le client
devrait utiliser.
       default-lease-time 30;
#Un client peut demander un bail d'une dure bien précise.
#Sinon par défaut le serveur alloue un bail avec cette dure
avant expiration (en secondes).
        max-lease-time 60;
#C'est la dure maximale d'allocation autorise par le
serveur.
#Si un client demande un bail plus long, le bail sera accord
mais il ne sera
#valide que durant max-lease-time secondes.
        option broadcast-address 172.16.1.255;
#Cette option configure l'adresse broadcast qui sera fourni
aux clients.
}

host m2 {
  hardware ethernet 02:04:06:96:17:de;
  fixed-address 172.16.1.199;
}
```

- [serveur] Redémarrer serveur dhcp : /etc/init.d/isc-dhcp-server [re]start
- [serveur] Vérifier s'il est démarré avec : *ps ax* et *lsof -i -n*
- [serveur] LOG dhcp avec : tail -f /var/log/syslog
- [client] supprimer le fichier des bails /var/lib/dhcp/dhclient.leases

********** FIREWALL **********

- créer dans /root un executable iptables.sh (ne pas oublier chmod 755) :

```
#!/bin/bash

echo " Enlever toutes les règles existante"
iptables -F

echo "Politiques par default a DROP"
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

echo "Requete DNS et WEB depuis m1 permise"
iptables -A FORWARD --source 192.168.1.1 -protocol  UDP
--destination-port 53 -j ACCEPT
iptables -A FORWARD --source 192.168.1.1 --protocol
       TCP --destination-port 80 -j ACCEPT
iptables -A FORWARD  -d 192.168.1.1 -m state --state
       ESTABLISHED,RELATED  --jump ACCEPT

echo "REJECT pour machine en interne et DMZ"
iptables -A INPUT -i eth0 -j REJECT
iptables -A INPUT -i eth1 -j REJECT
#iptables -A FORWARD -i eth0 -j REJECT
iptables -A FORWARD -i eth1 -j REJECT
iptables -A OUTPUT -o eth0 -p icmp --icmp-type
       destination-unreachable -j ACCEPT
iptables -A OUTPUT -o eth1 -p icmp --icmp-type
       destination-unreachable -j ACCEPT

echo "LOG pour le reste"

iptables -A INPUT -m limit --limit 5/minute -j LOG
iptables -A OUTPUT -m limit --limit 5/minute -j LOG
iptables -A FORWARD -m limit --limit 5/minute -j LOG

echo "Autoriser les requetes DNS depuis le routeur"
iptables -A OUTPUT -o eth2 --protocol UDP
       --destination-port 53 -j ACCEPT
echo "Requete web depuis le routeur"
iptables -A OUTPUT -o eth2 --protocol TCP
       --destination-port 80 -j ACCEPT

echo "Requete DNS depuis m1 permise"
#iptables -A INPUT -i eth2 --protocol UDP
       --source-port 53 -j ACCEPT

echo "Etablissement d'un suivi de connexion"
iptables -A INPUT  -i eth2 -m state --state
       ESTABLISHED,RELATED  --jump ACCEPT
```

********** DNS **********

- /etc/hosts : correspondance entre @IP et nom de domaine.
- /etc/resolv.conf : adresse du serveur dns « nameserver 10.0.0.3 »
- /etc/nsswitch.conf : ligne « hosts : files dns » importante.
- Installation du dns : *sudo apt-get update* puis *sudo apt-get install unbound*
- Configuration du serveur dans /etc/unbound/unbound.conf
- IPV4 : dig google.com A / IPV6 : dig google.com AAAA /

********** PANNE **********

Panne 1 : pas d'interface on modifie le fichier de config /etc/network/interfaces :

auto eth0
iface eth0 inet static
address 10.1.0.9
netmask 255.255.255.0

les deux lignes qui suivent permettent à panne1 d'aller vers lextérieur

gateway gateway 10.1.0.2
up ip route add 172.17.135.128/26 via 10.1.0.100 dev eth0
up ip route add 10.2.0.0/30 via 10.1.0.100 dev eth0
up ip route add 192.168.68.0/24 via 10.1.0.100 dev eth0

On peut voir les routes qui étaient sur ok1, on a juste a les copier

Panne 2 : Un cable croisé utilisé, il faut un cable droit parce que c'est vers un switch

Panne 3 : Problème de route

On redemarre la machine pour que le changement des route ait été bien pris en compte.
ip route del pour supprimer une route.
contenu du fichier /etc/network/interfaces de panne 3

Panne 4: Fonction de routage de panne 3 : pas activé
Activer la fonction de routage sysctl -w net.ipv4.ip_forward=1
et de manière persistance /etc/sysctl.conf
on décommente la ligne correspondante net.ipv4.ip_forward=1
/etc/resolv.conf : adresse du server DNS incorrect la vraie est 172.17.135.129

Panne 5: fichier /etc/nsswitch
files DNS etait collé ensuite, nano /etc/unbound/unbound.conf le /25 etait un /30

access-control: 172.17.135.128/25 allow