What routes are there in the tuxes? What are their meaning?

Algumas rotas são geradas automaticamente, “ligando” as máquinas às vlans a que pertencem: o tux31 tem uma rota para a vlan30, o tux32 tem uma rota para a vlan31, e o tux34 tem rota para as duas. O gateway para estas rotas é 0.0.0.0.

Para além disso, no tux31 adicionou-se a rota - route add -net [172.16.31.0/24](http://172.16.31.1/24) gw [172.16.30.254](https://l.messenger.com/l.php?u=http%3A%2F%2F172.16.30.254%2F&h=AT1sWhxRfO6ekCleYvfcp-sF-8VH3jV_ke9ySePTDoOWuDKbRg8lidb-GzV_Hn8Bew31Mes4CVPnGyaD-84vaCkAV_a03mEnIfUdj0QpiGDe8t2-b37iEQrgi_A5Vfnk99as04jtD40), isto é quando o tux31 ([172.16.30.1](https://l.messenger.com/l.php?u=http%3A%2F%2F172.16.30.1%2F&h=AT1sWhxRfO6ekCleYvfcp-sF-8VH3jV_ke9ySePTDoOWuDKbRg8lidb-GzV_Hn8Bew31Mes4CVPnGyaD-84vaCkAV_a03mEnIfUdj0QpiGDe8t2-b37iEQrgi_A5Vfnk99as04jtD40)) quer enviar um ping/mensagem para a vlan31 ([172.16.31.0](https://l.messenger.com/l.php?u=http%3A%2F%2F172.16.31.1%2F&h=AT1sWhxRfO6ekCleYvfcp-sF-8VH3jV_ke9ySePTDoOWuDKbRg8lidb-GzV_Hn8Bew31Mes4CVPnGyaD-84vaCkAV_a03mEnIfUdj0QpiGDe8t2-b37iEQrgi_A5Vfnk99as04jtD40)) ele vai utilizar como gateway o router que é o tux34 ([172.16.30.254](http://172.16.30.254/)), este

tux vai ter uma forwarding table que torna isto possível.

No tux34 fez-se algo similar ao que se fez no tux31 só que no sentido inverso, criou-se uma rota route add -net [172.16.30.1/24](http://172.16.30.1/24) gw [172.16.31.253](https://l.messenger.com/l.php?u=http%3A%2F%2F172.16.31.253%2F&h=AT1sWhxRfO6ekCleYvfcp-sF-8VH3jV_ke9ySePTDoOWuDKbRg8lidb-GzV_Hn8Bew31Mes4CVPnGyaD-84vaCkAV_a03mEnIfUdj0QpiGDe8t2-b37iEQrgi_A5Vfnk99as04jtD40), isto é quando queremos enviar um ping/mensagem para a vlan30 envia-se primeiro para o router ([172.16.31.253](http://172.16.31.253/)).

» What information does an entry of the forwarding table contain?

Na tabela de forwarding cada entrada possuí informação do tipo [Destination - Gateway - Interface], em que a destination é

o ip do computador/rede de destino, o gateway é o ip do computador para o qual vai ser mandada a mensagem e este é que vai dar

routing da mensagem para o destino, e a interface é a placa de rede usada para enviar a mensagem exemplo: eth0, eth1, etc.

Outras informações que também estão presentes para cada entrada na tabela são:

* Netmask => utilizado para determinar o ID da rede a partir do IP address do destino;
* Flags => informações sobre a rota.
* Metric => custo da rota.
* Ref => número de referências para esta rota (não usado no kernel do linux).
* Use => contador de pesquisas pela rota, dependendo do uso de -F ou -C (número de falhas da cache e número de sucessos, respetivamente).

3) What ARP messages, and associated MAC addresses, are observed and why?

* Ocorre uma troca de mensagens ARP quando um tux (tux1) envia um ping a outro tux (tux2), e o tux1 não conhece o MAC address de tux2. O tux1 envia uma mensagem ARP, na qual pede o MAC address de tux2, através do seu IP. Quando uma mensagem ARP é enviada, o tux que envia (neste caso, tux1) associa o seu MAC address à mensagem, para que o recetor esperado da mensagem (tux2) saiba a que tux responder ("Who has [IP de tux2]? Tell [próprio IP]"). Esta mensagem será enviada no modo broadcast (MAC address do recetor tem o valor 00:00:00:00:00:00), porque o MAC address de tux2 ainda é desconhecido. Quando recebe este broadcast, tux2 responde com uma mensagem ARP, na qual fornece o seu MAC address ("[IP de tux2] is at [MAC address de tux2]"). Esta mensagem é enviada apenas para o MAC address de tux1, e não em modo broadcast.  
    
  Esta troca de mensagens ARP ocorre sempre que uma mensagem é enviada de uma máquina para outra sendo que os endereços MAC não são conhecidos (por exemplo, da interface eth1 do tux4 para o tux2).

4) What ICMP packets are observed and why?

- Podemos observar pacotes ICMP do tipo request e reply, já que, estando todas as routes adicionadas, todos os tuxes reconhecem a presença uns dos outros. Se não reconhecessem, os pacotes ICMP enviados seriam do tipo Host Unreachable.

-> What are the IP and MAC addresses associated to ICMP packets and why?

Os endereços IP e MAC de origem e destino associados com os pacotes ICMP são os endereços MAC e IP das máquinas/interfaces que recebem/enviam os pacotes. Por exemplo, quando um pacote ICMP é enviado do tuxy1 para a interface do tuxy4 conectada à mesma subrede (no nosso caso foi utilizada a interface eth0), os endereços MAC e IP de origem serão os do tuxy1 (IP: 172.16.30.1 e MAC: 00:0f:fe:8b:e4:4d) e os endereços IP e MAC de destino serão os associados à interface eth0 do tuxy4 (IP: 172.16.30.254 e MAC: 00:21:5a:5a:7d:74).

Se as duas máquinas não estiverem conectadas à mesma virtual network (como é o caso do tuxy1 e tuxy2), não é possível efetuar o envio de informação entre as duas máquinas com apenas um pacote ICMP sem este ser modificado. Neste caso, o que acontece é: o tuxy1 irá enviar um pacote ICMP para a interface eth0 do tuxy4, uma vez que o tuxy4 está ligado a ambas as vlans e consegue interagir diretamente com o tuxy2; os endereços IP do pacote serão os IPs do tuxy1 e tuxy2 (origem e destino, respetivamente), e os endereços MAC serão os do tuxy1 e o da interface eth0 do tuxy4. Ao receber este pacote, o tuxy4 irá reencaminha-lo para o tuxy2, mantendo os endereços IP do pacote, mas os endereços MAC associados a este serão diferentes: o de origem será o da interface eth1 do tuxy4 (esta interface está conectada à vlan onde se encontra o tuxy2), e o de destino será o endereço MAC do tuxy2.