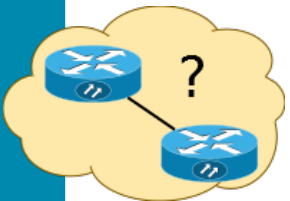


Labo réseau

I3030 – Administration et Sécurité des réseaux Labo Réseau



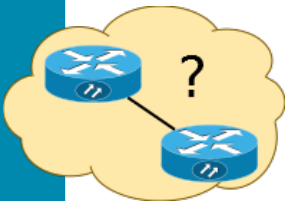
01 : Sommaire (1)

- Organisation et objectifs du cours
- Introduction (rappels)
- Modèle OSI
- Jeu
- Matériel réseau
- Commandes linux de base pour le réseau



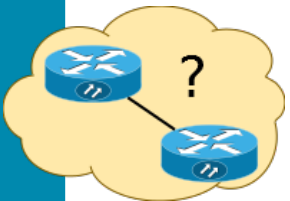
01 : Sommaire (2)

- ARP
- Ecoutes
- Netkit
- Rappel adressage IP

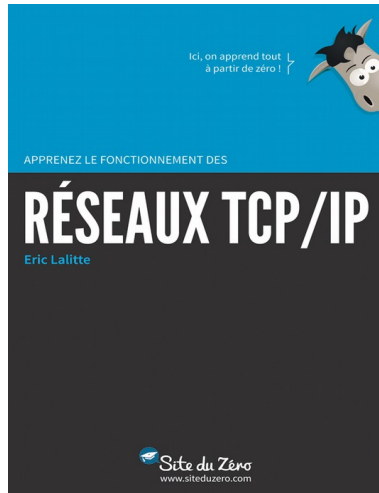


01 : Organisation et Objectifs du cours (1)

- Organisation
 - Ressources sur Moodle → 6I3030 → LaboReseau
- Objectifs et évaluation
 - 1 examen
 - Voir fiche UE

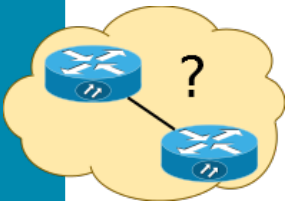
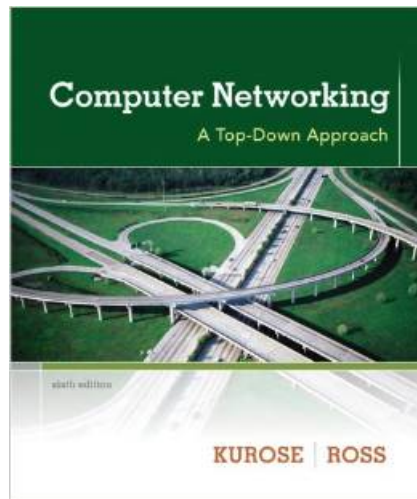


01 : Introduction (1)

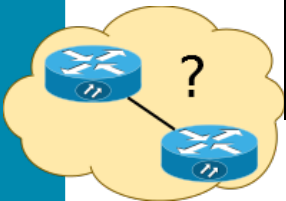
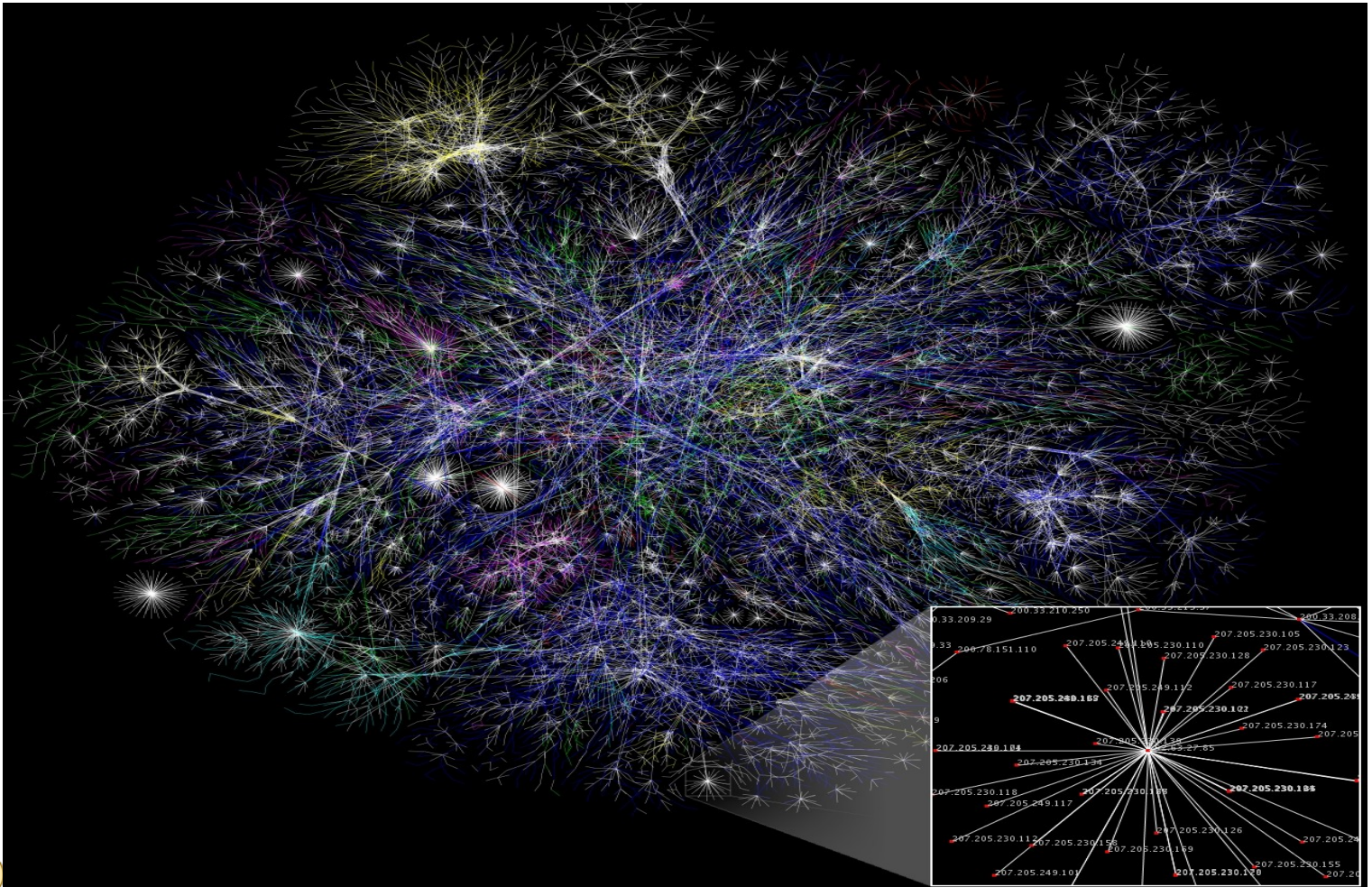


<http://wiki.netkit.org>

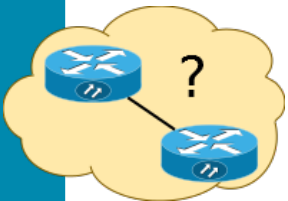
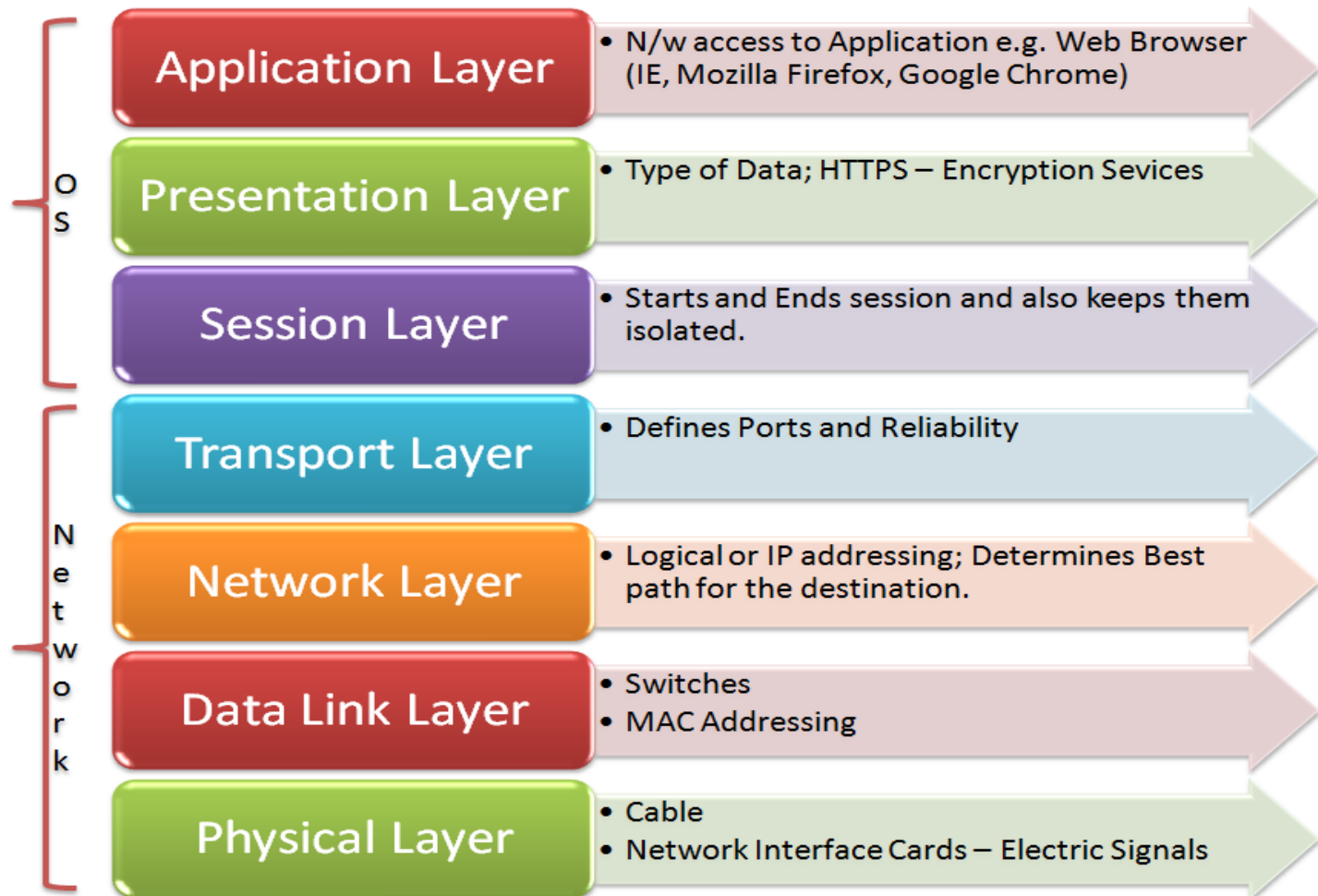
<http://www.lincoste.com/ebooks/pdf/informatique/fonctionnement-des-reseaux-tcp-ip.pdf>



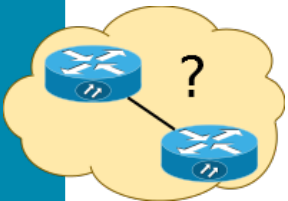
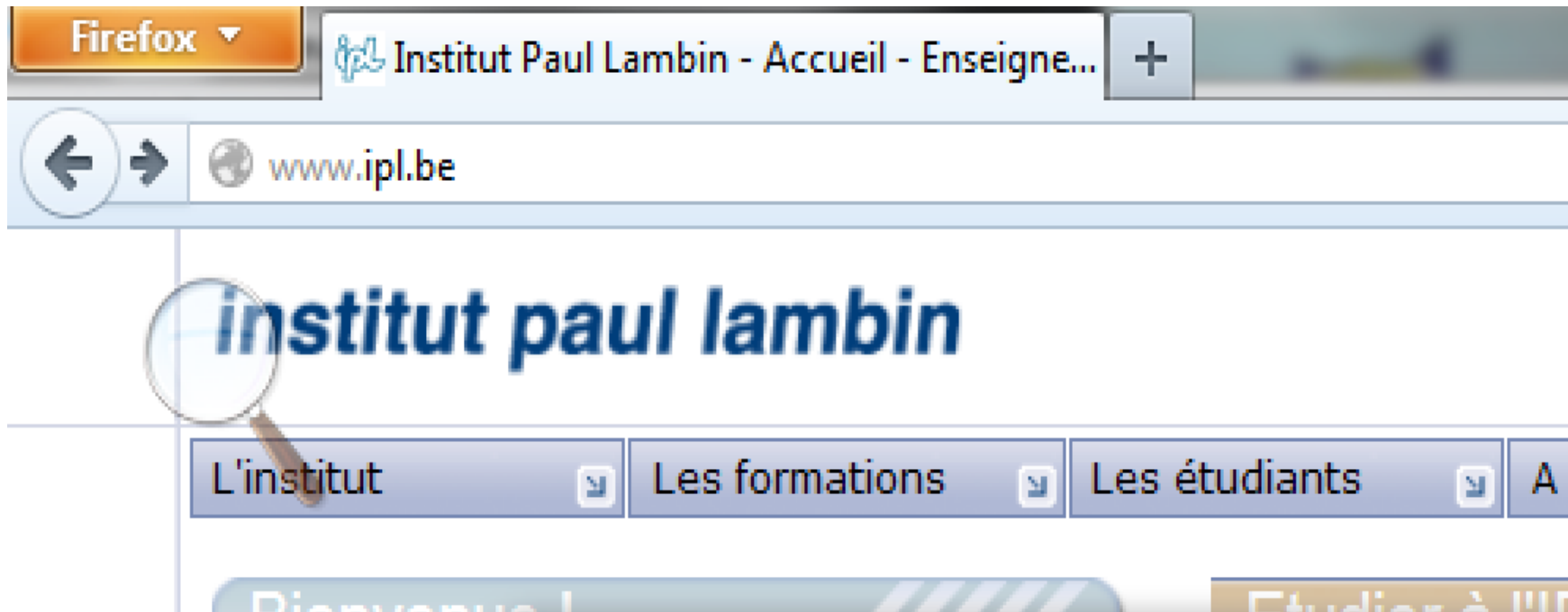
01 : Introduction (2)



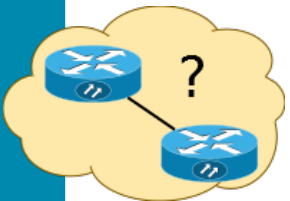
01 : Modèle OSI



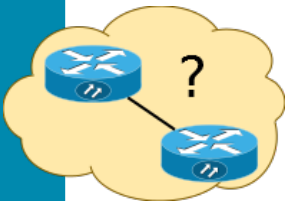
01 : Jeu (1)



01 : Jeu (2)



01 : Jeu (3)

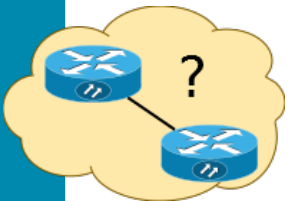


01 : Jeu (4)

```
/* AF_INET -> communication internet, AF_UNIX -> communication locale */  
/* création d'un socket TCP */
```

```
if ((sockfd = socket(AF_INET, SOCK_STREAM, 0)) == -1)  
{  
    perror("Erreur création socket");  
    exit(EXIT_FAILURE);  
}
```

```
/* no socket error */  
memset(&addr,0,sizeof(addr)); /* en System V */  
addr.sin_family = AF_INET;  
addr.sin_port = htons(portServeur);  
addr.sin_addr.s_addr = htonl(INADDR_ANY);  
if ((bind(sockfd,(struct sockaddr *)&addr,sizeof(addr))) == -1)  
{  
    perror("Erreur bind");  
    close(sockfd);  
    exit(EXIT_FAILURE);  
}
```



01 : Jeu (5)

```
C:\ Invite de commandes
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\olivier>ipconfig /all

Configuration IP de Windows

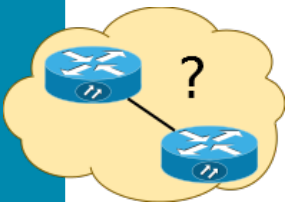
    Nom de l'hôte . . . . . : windevlicences
    Suffixe DNS principal . . . . . :
    Type de noud . . . . . : Hybride
    Routage IP activ   . . . . . : Non
    Proxy WINS activ   . . . . . : Non

Carte Ethernet Connexion au r  seau local:

    Suffixe DNS propre    la connexion :
    Description . . . . . : VMware Accelerated AMD PCNet Adapter

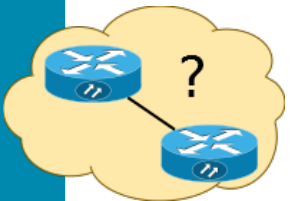
    Adresse physique . . . . . : 00-0C-29-F5-06-6B
    DHCP activ   . . . . . : Oui
    Configuration automatique activ  e . . . . . : Oui
    Adresse IP . . . . . : 192.168.1.98
    Masque de sous-r  seau . . . . . : 255.255.255.0
    Passerelle par d  faut . . . . . : 192.168.1.1
    Serveur DHCP . . . . . : 172.16.0.6
    Serveurs DNS . . . . . : 172.24.0.3
                             172.24.0.4
    Serveur WINS principal . . . . . : 172.24.0.3
    Serveur WINS secondaire . . . . . : 172.24.0.4
    Bail obtenu . . . . . : mardi 13 ao  t 2013 8:27:26
    Bail expirant . . . . . : mardi 13 ao  t 2013 8:37:26

C:\Documents and Settings\olivier>
```



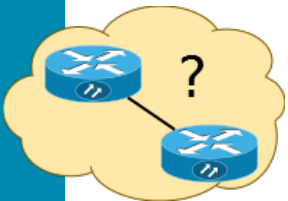
01 : Jeu (6)

```
<system.serviceModel>
  <services>
    <service behaviorConfiguration="WcfServiceLibrary1.Service1Behavior"
      name="WcfServiceLibrary1.Service1">
      <endpoint address="" binding="netTcpBinding" bindingConfiguration=""
        contract="WcfServiceLibrary1.IService1">
        <identity>
          <dns value="localhost" />
        </identity>
      </endpoint>
      <endpoint address="mex" binding="mexTcpBinding"
bindingConfiguration=""
        contract="IMetadataExchange" />
      <host>
        <baseAddresses>
          <add baseAddress="net.tcp://localhost:8523/Service1" />
        </baseAddresses>
      </host>
    </service>
  </services>
</system.serviceModel>
```



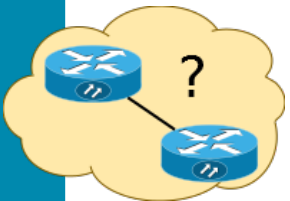
01 : Matériel réseau (1)

- Switch
 - Mac Address → table de mac address
 - Même réseau
- Routeur
 - IP Address
 - Connexion de réseaux



01 : Matériel réseau (2)

- Routeur vs PC (différences)
 - sans écran
 - Système exploitation propre (IOS par ex. si CISCO)
 - Plusieurs interfaces (min 2)
 - Routage activé !!!



01 : Commandes linux de base (réseau)

- *ifconfig* : permet de configurer et consulter une interface réseau d'une machine linux

Ex : `ifconfig eth0 192.168.1.1/24 up`

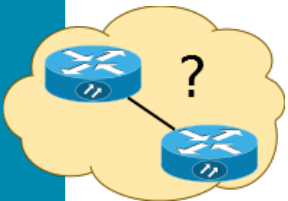
- *route* : permet de consulter ou adapter la table de routage

Ex : `route`

- *ping* : permet de tester l'accessibilité d'une adresse IP

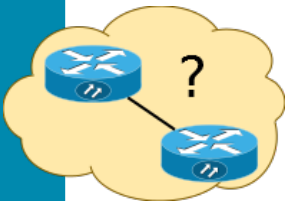
Ex : `ping 192.168.1.1`

- *traceroute* : permet de retrouver le chemin suivi par un paquet IP jusqu'à sa destination



01 : ARP (1)

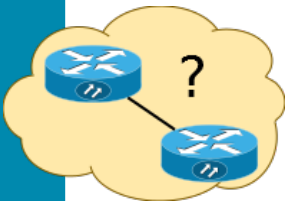
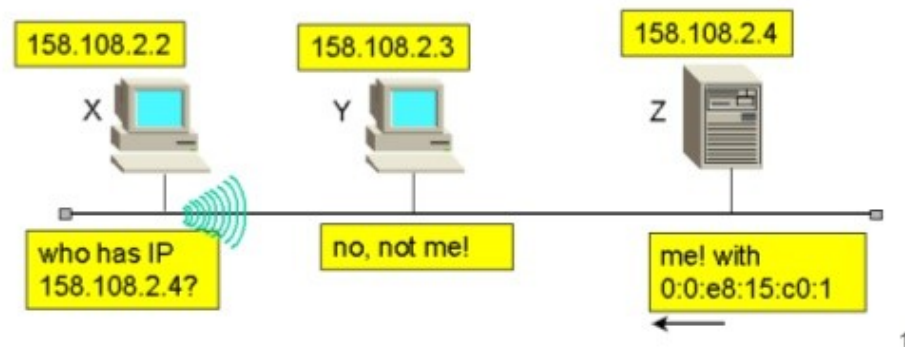
- Address resolution protocol
 - Quelle est l'adresse MAC du PC qui a l'adresse IP 192.168.1.1 ?
 - Broadcast – Unicast
 - Cache ARP
 - Commande arp pour manipuler le cache



01 : ARP (2)

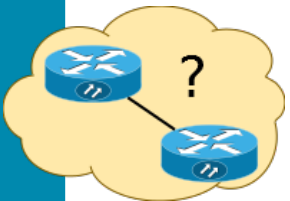
Address Resolution Protocol - ARP

IP over Ethernet



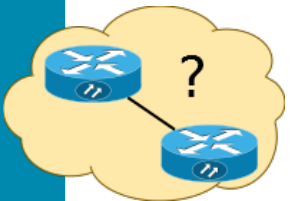
01 : Netkit (1)

- Machines virtuelles (User Mode Linux)
 - Routeurs
 - Switchs (commutateurs)
 - Serveur DNS , DHCP
 -



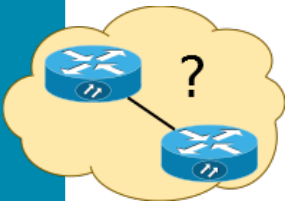
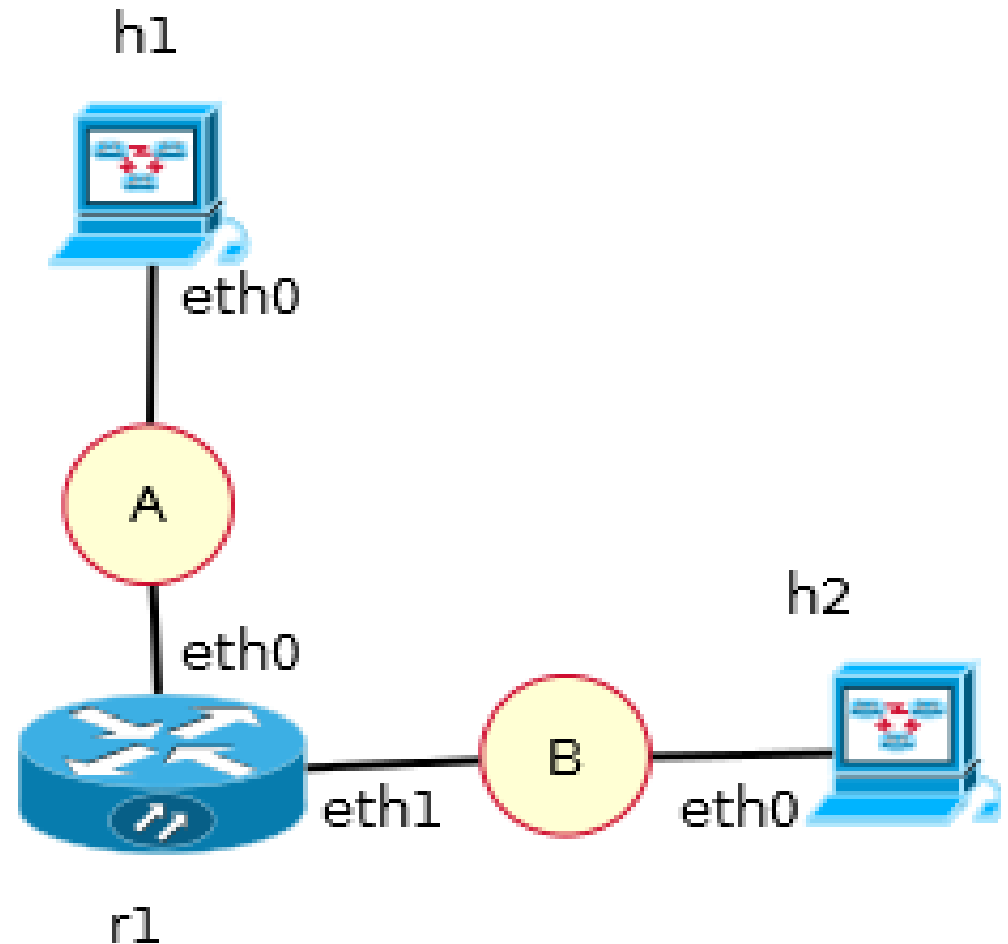
01 : Netkit (2)

- LaboNetkit
 - lab.conf
 - h1
 - h1.startup
 - r1
 - r1.startup



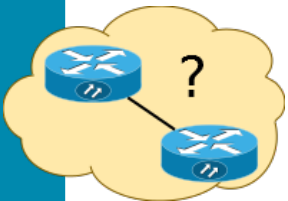
01 : Netkit (3)

- lab.conf
 - h1[0] = A
 - h2[0] = B
 - r1[0] = A
 - r1[1] = B



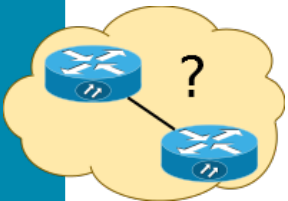
01 : Netkit (4)

- *vstart* : démarre une machine virtuelle
- *vhalt* : arrête une machine virtuelle
- *lstart* : charge un labo en démarrant toutes les machines virtuelles
- *lhalt* : termine proprement les machines virtuelles du laboratoire
- *lclean* : *supprime les machines virtuelles du laboratoire*



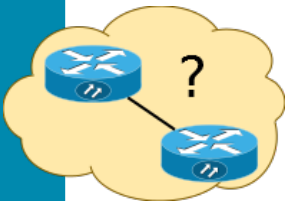
01 : Netkit (5)

- *Installation sur sa propre machine*
 - *Installer VirtualBox*
 - *Télécharger la VM sur*
<http://ochoquet.be/private/laborezo>
 - *Login : labo*
 - *Mdp : iplreseau*
 - *Dans VirtualBox → Importer un*
appareil virtuel (import appliance)



01 : Ecoutes (1)

- Ecoutes réseau
 - tcpdump -i <<interface>> -nt -s 0
 - Analyse avec wireshark (**installé sur Ubuntu**)
 - Vision par couches (modèles OSI)
 - tcpdump -i <<interface>> -nt -s **65535**
-w capture.cap
 - **cp capture.cap /hostlab/capture.cap**



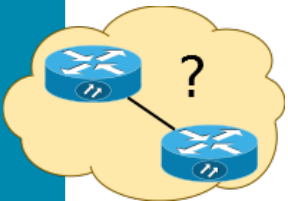
01 : Ecoutes (2)

capture.cap [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

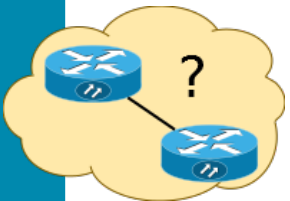
Filter: Expression... Clear Apply Enregistrer

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.1	192.168.0.2	ICMP	98	Echo (ping) reply id=0x2702, seq=1/256, ttl=64
2	0.952268	192.168.0.1	224.0.0.9	RIPv2	126	Response
3	0.999060	192.168.0.1	192.168.0.2	ICMP	98	Echo (ping) reply id=0x2702, seq=2/512, ttl=64
4	1.998255	192.168.0.1	192.168.0.2	ICMP	98	Echo (ping) reply id=0x2702, seq=3/768, ttl=64
5	3.001803	192.168.0.1	192.168.0.2	ICMP	98	Echo (ping) reply id=0x2702, seq=4/1024, ttl=64
6	4.001763	192.168.0.1	192.168.0.2	ICMP	98	Echo (ping) reply id=0x2702, seq=5/1280, ttl=64



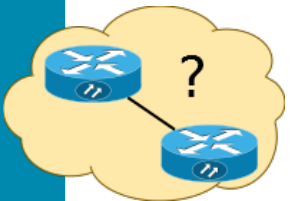
01 : Calculs réseaux (1)

- Réseaux avec 5 machines
 - $2^0 = 1$ KO
 - $2^1 = 2$ KO
 - $2^2 = 4$ KO
 - $2^3 = 8 - 2$ (adresse réseau/adresse broadcast) OK
 - $/32 - 3(2^3) = /29$
 - Adresse privée -> réseau 192.168.1.0/29



01 : Calculs réseaux (2)

- Suite
 - Adresse réseau : 192.168.1.0 (tous les bits hosts à 0)
 - Adresse broadcast : 192.168.1.0(tous les bits hosts à 1)
 - 192.168.1.00000111 $\rightarrow 2^2 + 2^1 + 2^0 = 7$
 - 192.168.1.7
 - Truc : adresse réseau tjs paire et adresse broadcast impair



01 : Calculs réseaux (3)

- Pq des adresses privées ?
- Adresse privée vs Adresse publique ?
- Ranges adresses privées
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/16

