Réseaux internet

Manche Open School

Paul Lecuq

9 novembre 2015

Paul Lecuq

- 26 ans
- DUT Services et réseaux de communication à Saint-Lô
- Licence professionnelle Administration et sécurité des réseaux à Saint-Malo
- Administrateur réseau chez FactorFX depuis 2011
- paul@paulbsd.com

Plan de cours

- Histoire et concepts
- Ethernet
- Internet
- Application
- Analyse
- Outils

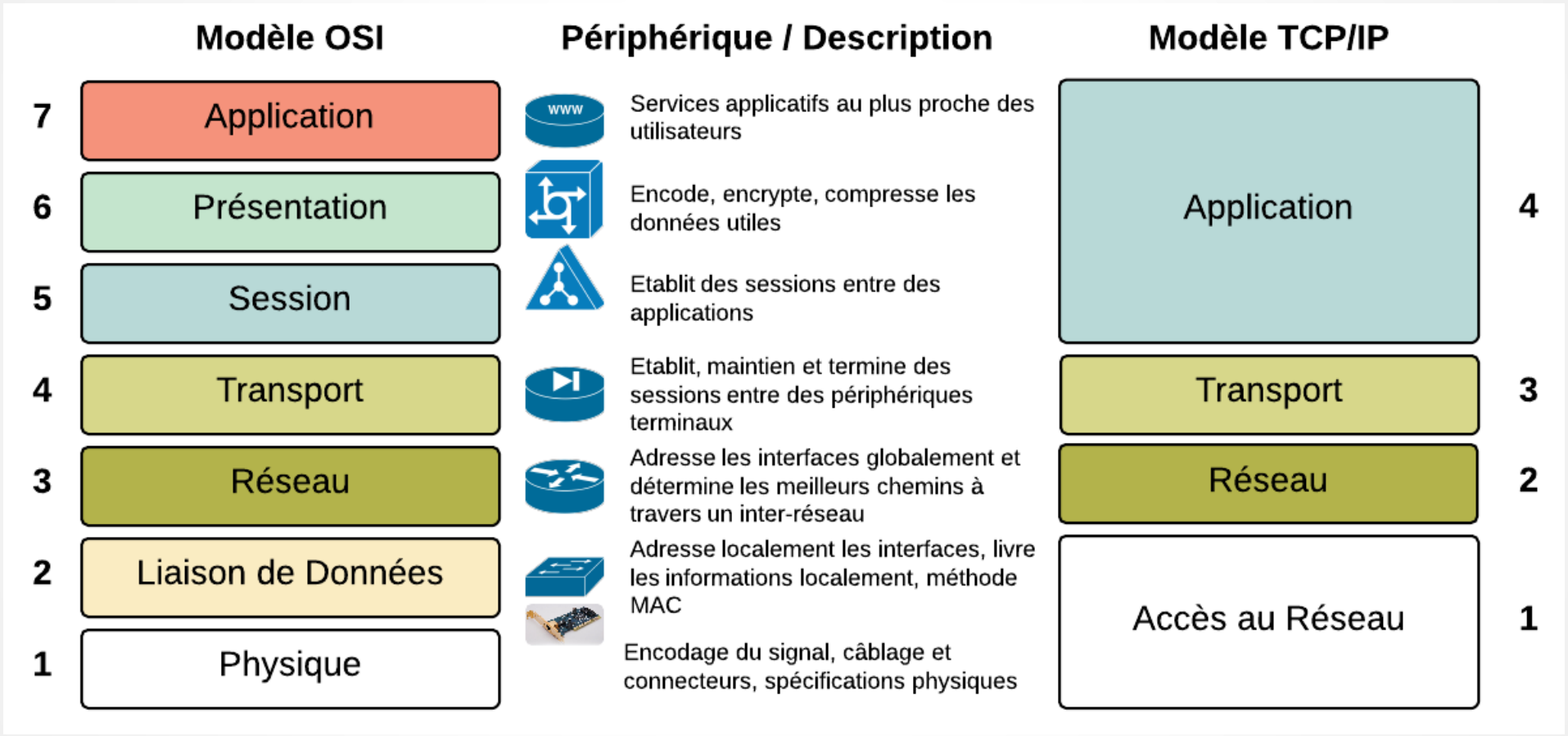
Histoire

- Arpanet, 1969 par des militaires US, maillage géographique, prémisses d'internet
- Ethernet en 1976 par Robert Metcalfe, développé au Xerox Parc, Palo Alto
- IP, base de l'internet en 1980 par Vint Cerf, décrit par RFC de l'IETF
- Implémentation de TCP/IP en 1984 par Bill Joy sur 4.2BSD

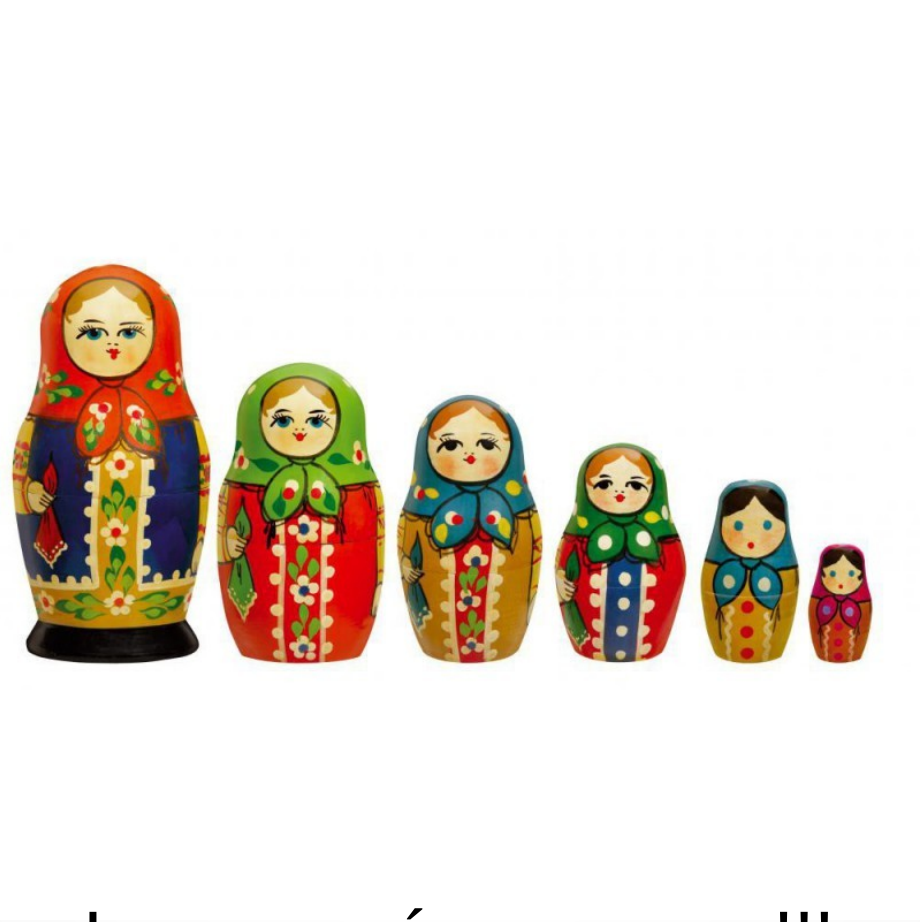
Couches modèle OSI

- 1 : Physique, c'est le médium physique
- 2 : Liaison, c'est le protocol de communication entre machines sur le même lien (Ethernet)
- 3 : Réseau, c'est ce qui permet de passer outre un réseau interne, on retrouve IP
- 4 : Transport, permet de transporter un protocole applicatif, on retrouve TCP et UDP
- 5 : Session, pour la communication entre applications
- 6 : Présentation, effectue des optimisations sur le canal
- 7 : Application, ce qui est présenté à l'utilisateur

Couches modèle OSI

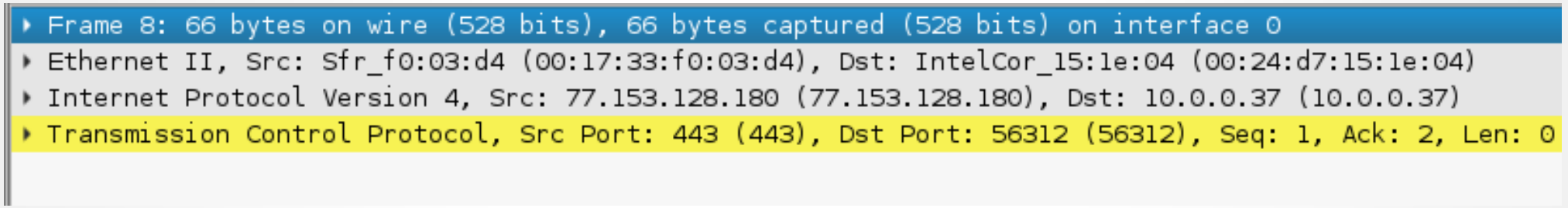


Notion essentielle de réseau



Les poupées russes !!!

Structure



Capture de paquets avec Wireshark

Ethernet

- Politesse !
- Remplace le token ring
- Adresse MAC, codée sur 48 bits, 6 octets
- $2.814749767 \times 10^{14}$ adresses
- Les 24 premiers bits identifie le constructeur, gérés par l'IANA
- Les autres sont générés aléatoirement par chaque constructeur

Ethernet : Datagramme

En octets

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14 … 1513	1514	1515	1516	1517
Adresse MAC destination						Adresse MAC source						Type de protocole		Données	FCS/CRC			

- Adresse destination : 00:17:33:f0:03:d4
- Adresse source : b8:27:eb:09:6c:62
- Type de protocole : définit le protocole utilisé en couche 3, IP par exemple
- Données, 1500 octets, correspond au MTU, qui peut être modifié (Jumbo frames)
- Checksum : Vérifie l'intégrité des données

IP : Internet Protocol

- Permet l'existence de l'internet
- Ethernet, n'a pas la capacité de passer un routeur, IP peut le faire
- Adresses codées en 32 bits (4o) en IPv4 de la forme : 128.232.212.36 (notation décimale)
- Adresses codées en 128 bits (8 * 2o) en IPv6 de la forme : 2a01:e35:2f6a:ecf0:8432:7654:4563:100 (notation héxadécimale)
- Rassurez-vous, les adresses en version 6 peuvent être raccourcies dans certains cas !!

Classes d'adresses et CIDR en IP

- Pour IPv4
- Classe A : premier octet de 1 à 127
- 126 réseaux d'environ 16 millions d'hôtes, découpé au premier octet

- Classe B : premier octet de 128 à 191
- 16384 réseaux de 65534 hôtes, découpé au second octet

- Classe C : premier octet de 192 à 223
- 2 millions de réseaux de 254 hôtes, découpé au troisième octet

Classes d'adresses et CIDR en IP

- Classe D : premier octet de 224 à 239
- Réservé pour le multicast

- Classe E : premier octet de 240 à 255
- Réservé pour des tests

http://www.tutorialspoint.com/ipv4/ipv4_address_classes.htm

Classes d'adresses et CIDR en IP

- Le CIDR a été inventé pour rendre plus souple le découpage de réseau qu'avec les classes traditionnelles
- 192.168.1.0/24 donne un réseau de 254 adresses disponibles de 192.168.1.1 à 192.168.1.254
- 192.168.1.0/26 donne un réseau 64 adresses disponibles : de 192.168.1.1 à 192.168.1.63
- Réprésentable comme un curseur
- Calcul de masque de sous-réseau

Adresse IP

- Classe d'adresse
- Découpage CIDR
- Calcul de masque de sous-réseau

- Démo

- Calcul binaire
- Tables de vérité (George Boole)

Multicast et broadcast IP

- Les adresses de classe D (224 à 239) sont définies pour le multicast
- Le multicast est utilisé dans certains cas pour limiter la bande passante que l'unicast sur des contenus spécifiques
- Exemples

- Le broadcast n'est pratiquement plus utilisé, et n'existe plus dans IPv6
- Pose beaucoup plus de problème qu'il n'apporte de solutions
- Peu d'applications aujourd'hui utilise le broadcast IP

Pénuries d'adresses

- IPv4, avec 4 milliards d'adresses disponibles, ne permet pas l'adressage de chaque machine qui existe sur Internet
- IPv6, tente de régler ce problème, mais la marche est encore longue
- Ipv6 comporte de nombreux avantages : exemples

- Des palliatifs ont été développés comme le NAT et le PAT, mais sont cependant imparfaits

NAT

- On réécrit l'adresse IP et le port TCP/UDP source, et l'équipement qui effectue cette transformation maintient une table de correspondance en mémoire
- Implémenté dans les box internet et routeurs
- Plusieurs machines pourront accéder à internet via une seule IP publique

NAT

- Utilisations d'adresses IP privées
- Important d'utiliser ces adresses pour des réseaux internes
- 10.0.0.0/8 → classe A
- 172.16.0.0/12 → classe B
- 192.168.0.0/16 → classe C
- RFC 1918
- Couplé avec le NAT, c'est une sécurité naturelle

PAT : le petit frère de NAT

- On réécrit l'adresse IP et le port TCP/UDP de destination
- Permet de rediriger les flux externes vers des IP internes
- Permet d'ajouter un serveur derrière votre box, et d'accéder à votre serveur
- Le module souvent appelé DMZ, redirige l'intégratilité des ports TCP/UDP vers une seule machine en réseau privé

TCP / UDP

- TCP : Transmission Control Protocol
- Transporte une application et gère des sessions et garantie une plus grande intégrité des flux
- Dispose de numéros de ports de 1 à 65535
- Ports connus 80 pour HTTP, 443 pour HTTPS par exemple
- Liste disponible : http://www.frameip.com/liste-des-ports-tcp-udp/

Applications

- DNS, résolution de nom internet, udp/53
- SMTP, échange de mails, tcp/25
- HTTP, pages internet, tcp/80
- HTTPS, pages internet sur SSL, tcp/443
- IMAP, consultations de mails, tcp/143
- LDAP, annuaires, tcp/389
- SSH, console à distance UNIX, tcp/22

Applications

- Bien que les ports de 1 à 1024 sont standards, il est possible de modifier ces ports suivant les applications
- Un serveur HTTP peut très bien écouter sur le port 8080, il faudra juste renseigner le navigateur :

  http://monserveur.tld:8080

Sécurité

- Pour protéger des machines d'internet, il est essentiel d'utiliser un firewall
- Permet de filtrer les flux sur des applications disponibles sur TCP/IP
- Chiffrer les données qui transitent : utilisation d'algorithmes de chiffrement
- Utilisation de réseaux privés virtuels

VPN

- Les VPN sont des réseaux virtuels qui permettent d'étendre géographiquement des réseaux physiques
- IPSec, L2TP, MPLS, OpenVPN sont des implémentations de VPN
- Nous utiliserons OpenVPN en TD/TP

Outils essentiels

- ping / ping6 : permet de savoir si l'on peut joindre une machine sur le réseau
- traceroute / traceroute6 : permet de tracer le chemin entre deux machines
- arp : permet de faire le lien entre les adresses MAC et les adresses IP sur un même réseau
- nmap : permet de connaitre les ports ouverts sur une machine

Outils essentiels

- netstat : permet de consulter la table de routage, et de savoir quelle connexions sont disponibles sur une machine
- pfctl : permet de controler le fonctionnement du firewall pf intégré aux principaux OS *BSD, comme opnsense
- tcpdump : analyse de trames et paquets en mode console
- wireshark : frère de tcpdump, en graphique
- J'insiste sur l'utilisation de tous ces outils pour bien appréhender les notions essentiels de réseau

Travaux dirigés

- Jouons ensemble
- 2 machines virtuelles virtualbox ou vmware
- Opnsense avec deux interfaces réseau virtuelles
- Une en bridge sur eth0 ou wlan0 : ce sera notre WAN (Wide area network)
- Une en vboxnet ou vmnet : ce sera notre LAN (Local area network)

Travaux dirigés

- Opnsense sera votre firewall !
- Nous ferons des règles de filtrage, de NAT/PAT
- Nous étudierons et analyserons le fonctionnement des protocoles
- Nous mettrons en place un VPN entre plusieurs
- Sur l'interface LAN de votre VM, je vous affecterais le troisième octet pour chacuns d'entre vous :

  192.168.x.0/24
- Votre tunnel VPN sera 10.50.x.0/24

Travaux dirigés

- Une seconde VM sur laquelle on installera des services à protéger
- Ce que vous voulez, du moment que c'est Open !

Travaux dirigés / Travaux pratiques

- Configuration réseau
- Filtrage TCP/IP
- NAT
- VPN
- Outils d'analyse et de sécurité

Si le temps nous le permet :

- QoS (Qualité de service et priorisations de flux)

Liens utiles supplémentaires

- Tutorial avec Opnsense
- http://www.scip.ch/en/?labs.20150409

- Pages de man, à chercher sur internet
- Ces pages sont essentielles

Fin

- Questions
- Contactez-moi si besoin