Infrastructure réseau de travaux pratiques

Philippe Latu
philippe.latu(at)inetdoc.net

http://www.inetdoc.net

Ce document présente l'infrastructure réseau utilisée pour les enseignements pratiques sur les systèmes GNU/Linux et l'interconnexion réseau dans la filière STRI de l'Université Toulouse III - Paul Sabatier.

Table des matières

1. Copyright et Licence

1.1. Méta-information

Cet article est écrit avec *DocBook*[1] XML sur un système *Debian GNU/Linux*[2]. Il est disponible en version imprimable au format PDF : `infra.tp.pdf`[3].

2. Contexte d'utilisation de ce document

L'infrastructure présentée ici sert pour l'ensemble des séances de travaux pratiques aux niveaux L3, M1 et M2.

- En 3ème année de Licence, les équipements (commutateurs et routeurs) sont préconfigurés. L'objectif pour l'étudiant, est d'être capable de (re)configurer les interfaces réseau (LAN) d'un poste et de (re)brasser les connexions en fonction du plan d'adressage fourni dans ce document.

- En Master 1ère année, les équipements sont partiellement configurés. L'objectif pour l'étudiant, est d'être capable de (re)configurer les interfaces et l'interconnexion de réseaux étendus (WAN) et locaux (LAN). Ce document sert de base pour le plan d'adressage des réseaux locaux. Le plan d'adressage des réseaux étendus est fourni avec le document support de travaux pratiques.

- En Master 2ème année, les équipements sont libres de toute configuration. L'objectif pour l'étudiant, est d'être capable de construire une maquette d'infrastructure réseau reproduisant un scénario d'exploitation. Ce document sert de base pour le raccordement des maquettes aux réseaux locaux.

[1] http://www.docbook.org
[2] http://www.debian.org
[3] http://www.inetdoc.net/pdf/infra.tp.pdf

3. Étapes usuelles de configuration du poste de travail

Chaque début de séance de travaux pratiques consiste à répéter un certain nombre de tâches usuelles avant d'attaquer le vif du sujet. Voici une liste indicative.

Brassage par défaut
: Avant d'allumer le poste de travaux pratiques, il faut vérifier que l'interface (LAN|Ethernet) de ce poste est correctement brassée sur le réseau local «par défaut» ; celui qui bénéficie du service DHCP. Si ce n'est pas le cas, il faut brasser cette interface sur l'un des ports de la plage numérotée de 17 à 32 (`range Fa0/17 - 32`) du commutateur `swd2.infra.stri` en salle 211 ou du commutateur `swd1.infra.stri` en salle 213.

Restauration du poste
: Il se peut que la configuration du système d'exploitation ait été «modifiée» lors d'une séance de travaux pratiques précédente. Il est possible de restaurer le poste de travaux pratiques au démarrage en tapant **2** lorsque l'écran ci-dessous est affiché.

Téléchargement du support de travaux pratiques et des documents associés
: Comme les changements de connexion réseau sont fréquents lors des travaux pratiques, il n'est pas rare de perdre la connexion vers l'Internet. Il est donc judicieux de posséder une copie locale de l'ensemble des documents nécessaires au traitement des questions de travaux pratiques. Tous les supports étant disponibles au format PDF, c'est ce type de document qu'il faut télécharger.

Installation des paquets utiles
: Un fois les supports téléchargés il faut les parcourir et constituer une liste des paquets utiles à la réalisation des travaux pratiques. Si cette étape n'est pas correctement traitée, il peut être nécessaire de revenir à la connexion réseau «par défaut» dès que l'on constate qu'un outil est absent. C'est une perte de temps.

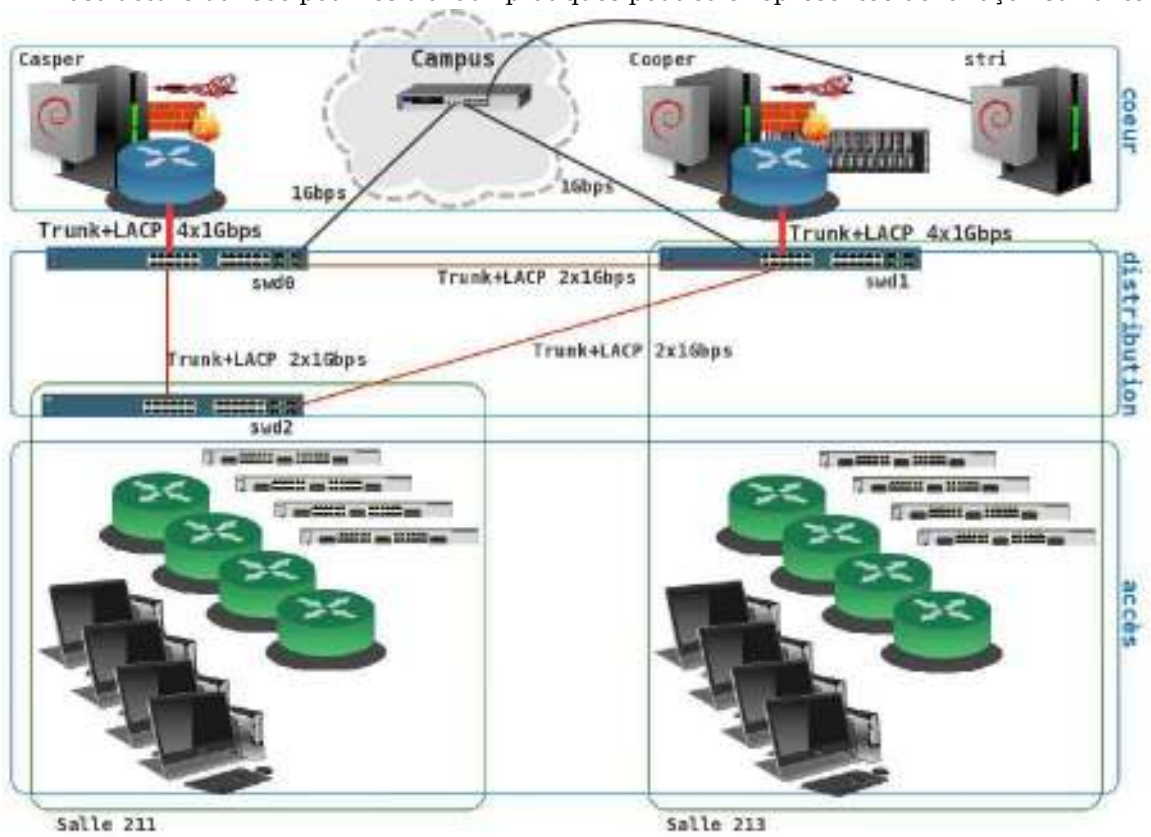
Brassage de la connexion et nouveau réseau local
: Chaque support de travaux pratiques impose une connexion à un réseau local différent du poste de travail. Il est donc nécessaire de reprendre manuellement la configuration de l'interface Ethernet. Il ne faut pas oublier de désactiver le client DHCP avant toute nouvelle configuration d'adresse IP à l'aide de la commande : **`# ifdown eth0`**.

Configuration de l'interface réseau et nom d'hôte
: Pour effectuer les opérations de configuration des interfaces réseau, il faut utiliser le support : *Configuration d'une interface réseau*

Enfin, n'oubliez pas de respirer profondément et ... de traiter les questions.

4. Interconnexion des équipements de l'infrastructure

L'infrastructure utilisée pour les travaux pratiques peut être représentée de la façon suivante :



Interconnexion des équipements de travaux pratiques - vue complète[4]

4.1. Passerelles du cœur de réseau

`cooper.infra.stri`, `casper.infra.stri`

Les passerelles *Casper* et *Cooper* assurent l'interconnexion entre le réseau du campus (que l'on assimile au réseau public) et les réseaux de travaux pratiques. Ces passerelles comprennent de nombreux services :

- *Le routage inter VLAN*. Au niveau réseau de la modélisation, tous les paquets IP passent nécessairement par l'une des deux passerelles pour être acheminés vers un autre réseau.

  Le mécanisme de routage utilisé est décrit dans le document *Routage Inter-VLAN*[5].

- *Le filtrage et la traduction d'adresses*. Les flux entrant et sortant sont filtrés par un pare-feu à état (*stateful firewall*) et les adresses IP des réseaux de travaux pratiques attribuées au début de chaque énoncé doivent être traduites avec les adresses des passerelles.

  La liste des réseaux de travaux pratiques est donnée dans la Section 5, « Plan d'adressage ». Toutes ces adresses sont dites privées ; elles appartiennent à l'un des trois super-réseaux définis dans le document RFC1918 *Address Allocation for Private Internets*[6].

- *La journalisation*. Tous les évènements sur les équipements réseau (état des interfaces, connexions, etc) sont consignés sur les services de journalisation (*logs* des deux passerelles.

- *Le service de noms de domaines* (DNS). Une arborescence factice ayant pour racine le nom *.stri*. (*Top Level Domain*) permet l'utilisation du service de noms de domaines dans les supports de travaux pratiques sur les services Internet : délégation DNS, courrier électronique, annuaires LDAP, etc. Le service DNS est implanté en redondance sur les deux passerelles.

  Les noms attribués aux postes de travail sont aussi utilisés par le service de restauration. Une image système est associée au nom d'hôte suivant la salle de travaux pratiques.

- *L'attribution automatique des adresses IP* (DHCP). Ce service est lié au service de noms de domaine. Une adresse MAC est associée à un nom d'hôte qui est lui-même associé à une adresse IP. Une instance DHCP est active sur chaque passerelle en mode tolérance de panne (*failover*). Si une première instance est défectueuse, la seconde peut prendre le relais de façon transparente.

[4] http://www.inetdoc.net/travaux_pratiques/infra.tp/images/infra.tp.pdf
[5] http://www.inetdoc.net/articles/inter-vlan-routing/
[6] http://www.faqs.org/rfcs/rfc1918.html

Comme dans le cas du service DNS, l'adresse MAC de l'interface réseau du poste de travail sert à désigner l'image système qui lui est attribuée.

- *La métrologie*. Le service SNMP est actif sur les deux passerelles ainsi que sur les trois commutateurs de couche distribution. Les informations sur les interfaces et les systèmes sont collectés par une instance de *Cacti: The Complete RRDTool-based Graphing Solution*[7].

- *Le service mandataire et le filtrage d'URLs*. Les logiciels *Squid*[8] et *SquidGuard*[9] sont installés sur les deux passerelles. Le service mandataire (*proxy*) utilise un cache partagé entre les deux passerelles. Le système de filtrage des URLs est alimenté quotidiennement par le dépôt de *Listes noires diffusées par l'université de Toulouse I*[10].

  La configuration de ces deux outils est décrite dans le guide *Proxy Squid & SquidGuard*[11]

4.2. Commutateurs de couche distribution

`swd0.infra.stri`, `swd1.infra.stri`, `swd2.infra.stri`

Les fonctions principales des ces commutateurs sont la redondance, la balance de charge et la fourniture de bande passante. Pour optimiser les temps de restauration système des postes de travaux pratiques, les ports numérotés de 17 à 32 (`range Fa0/17 - 32`) des commutateurs `swd1` et `swd2` sont associés aux VLANs sur lesquels le service DHCP de configuration automatique des interfaces est actif.

Les trois commutateurs utilisés appartiennent à la famille Cisco™ 2960G.

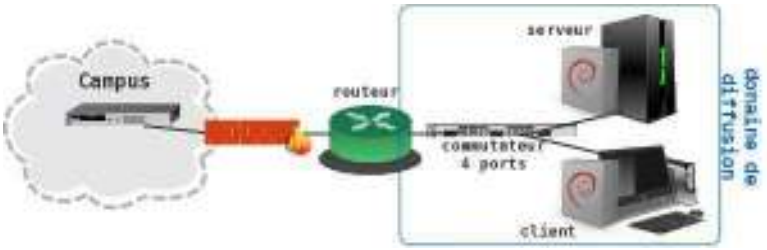
4.3. Commutateurs de couche accès

`sw2.infra.stri`, `sw3.infra.stri`, `sw4.infra.stri`, `sw5.infra.stri`, `sw6.infra.stri`, `sw7.infra.stri`, `sw8.infra.stri`, `sw9.infra.stri`, `sw10.infra.stri`, `sw11.infra.stri`

Sur chacun des commutateurs, 5 groupes de 4 ports sont configurés en mode accès. Les autres ports sont configurés en mode *trunk* pour les manipulations de routage inter-VLAN. Enfin le dernier port FastEthernet ou les deux derniers ports GigabitEthernet sont réservés pour communiquer avec le commutateur maître de la base de données des VLANs : le serveur *Virtual Trunking Protocol* (VTP).

L'interconnexion entre les différents réseaux est basée sur le routage inter-VLAN. Les passerelles *Casper* et *Cooper* partagent leurs routes via le protocole OSPF. Au delà de l'apprentissage des opérations de (re)configuration des interfaces de réseau local, l'objectif pédagogique est de fournir un domaine de diffusion cloisonné par groupe de postes de travail. De cette façon, la mise en pratique et le dépannage des services Client/Serveur est beaucoup plus facile.

Pour l'ensemble des travaux pratiques compris dans un réseau local, on se ramène à la topologie logique équivalente suivante :



Topologie logique type - vue complète[12]

[7] http://www.cacti.net
[8] http://www.squid-cache.org/
[9] http://www.squidguard.org/
[10] http://cri.univ-tlse1.fr/blacklists/
[11] http://www.inetdoc.net/guides/squid-guard/
[12] http://www.inetdoc.net/travaux_pratiques/infra.tp/images/infra.lab.png

4.4. Implantation des équipements

Les manipulations de travaux pratiques étant dupliquées pour accueillir un groupe complet d'étudiants, la topologie logique équivalente ci-dessus doit aussi être dupliquée. Voici une présentation de la topologie physique qui permet cette duplication.

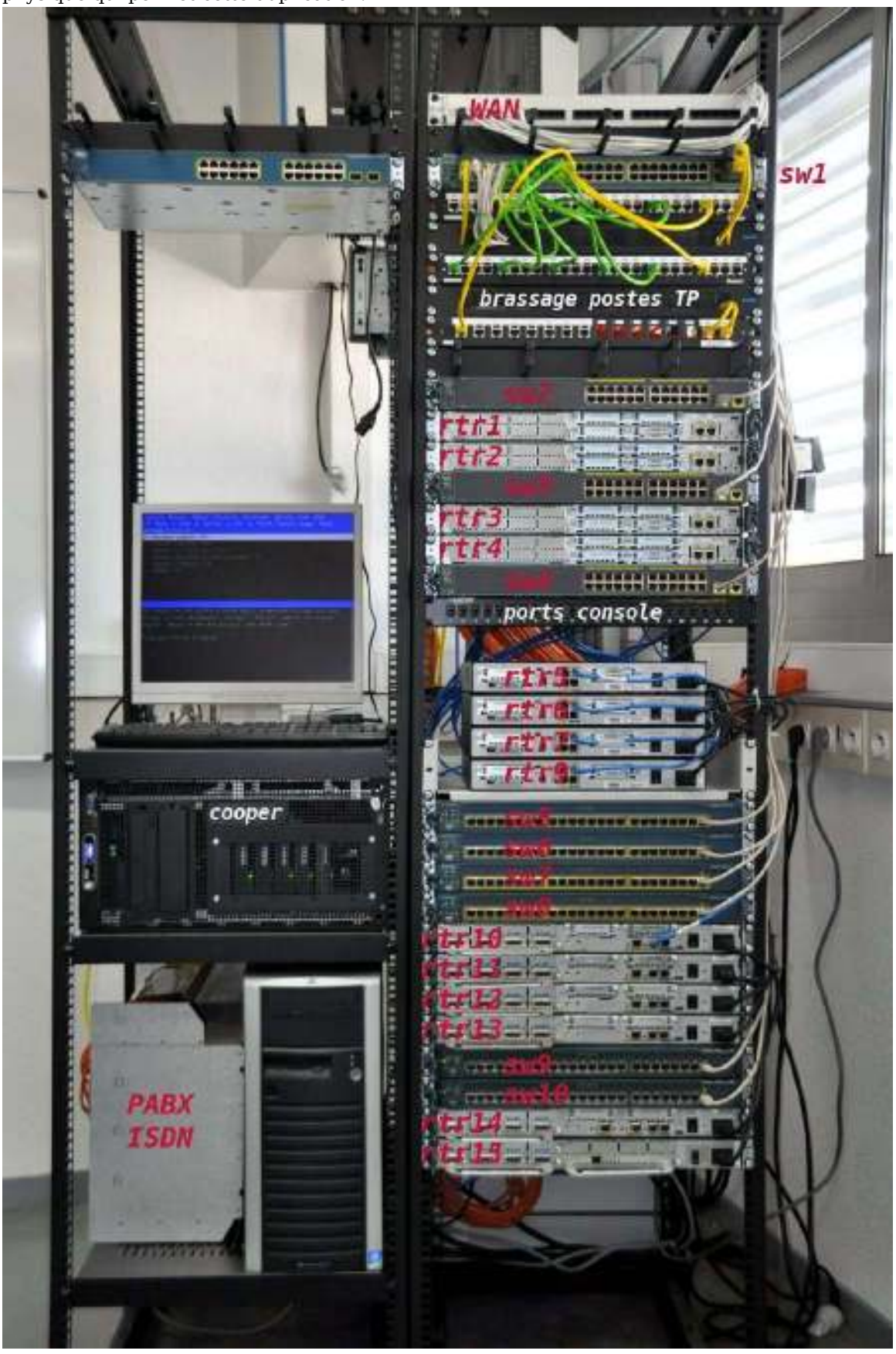


Photo bâtis U2-213 - vue complète[13]

[13] http://www.inetdoc.net/travaux_pratiques/infra.tp/images/rack.jpeg

5. Plan d'adressage

L'utilisation du routage inter-VLAN implique que l'on fasse correspondre à chaque réseau local virtuel (VLAN) un réseau IP différent. C'est la raison pour laquelle les tableaux ci-dessous font apparaître chaque numéro de VLAN en vis-à-vis d'une adresse IP indiquant la passerelle par défaut du réseau correspondant.

C'est ensuite à partir de cette adresse IP que l'on peut déterminer la plage des adresses réseau utilisables pour les postes de travail.

Note

Toutes les opérations de calcul sur les adresses IP sont traitées dans le document : *Adressage IPv4*

5.1. Base de données des réseaux locaux virtuels

Le tableau ci-dessous donne la liste des VLANs tels qu'ils sont implantés dans le commutateur maître de la base de données. Cette base de données de réseaux locaux virtuels est publiée vers les autres commutateurs à l'aide du protocole VTP (*Virtual Trunking Protocol*).

Tableau 1. Base de données des réseaux locaux virtuels (VLANs)

VLAN	Nom	Périmètre
1	default	VLAN par défaut défini par le constructeur. Tout port non affecté à un réseau local appartient au VLAN1. Il est fortement déconseillé d'utiliser ce VLAN particulier même pour les opérations de gestion des équipements.
2	lan.UPS	«Nuage Internet» ou réseau public vu de l'infrastructure de travaux pratiques.
3	infra.stri	Réseau de gestion des équipements actifs de l'infrastructure de travaux pratiques. Il supporte les services de routage, de métrologie, de gestion des configuration, de journalisation et de supervision.
4	services.stri	Réseau d'hébergement des services Internet de l'infrastructure pédagogique. On y retrouve les services classiques : DNS, DHCP, HTTP, etc.
5	secu-grp1.stri	Réseau de déploiement de l'infrastructure d'entreprise fictive du premier groupe d'étudiants pour le projet sur la sécurité des systèmes d'information.
6	secu-grp2.stri	Réseau de déploiement de l'infrastructure d'entreprise fictive du second groupe d'étudiants pour le projet sur la sécurité des systèmes d'information.
100 - 199	lan-1[0-9]{2}.stri.sw[0-9]	Réseaux virtuels de travaux pratiques préconfigurés sur les commutateurs `sw1.infra.stri`, `sw2.infra.stri`, `sw3.infra.stri`, `sw4.infra.stri`, `sw5.infra.stri`, `sw6.infra.stri`, `sw7.infra.stri`, `sw8.infra.stri`, `sw9.infra.stri` et `sw10.infra.stri`. À chaque VLAN, on a fait correspondre un réseau IP particulier. Voir tableaux ci-après.
211	lan-211.stri	Réseau des postes de travaux pratiques de la salle 211 sur lequel le service DHCP est actif.
212	lan-212.stri	Réseau des postes de travaux pratiques de la salle 212 sur lequel le service DHCP est actif.
213	lan-213.stri	Réseau des postes de travaux pratiques de la salle 213 sur lequel le service DHCP est actif.
214	lan-214.stri	Réseau des postes de travaux pratiques de la salle «virtuelle» 214 sur lequel le service DHCP est actif.
300 - 399	lan-3[0-9]{2}.stri.sw[0-9]	Réseaux virtuels libres pour les travaux pratiques au cours desquels on doit effectuer des manipulations sur les numéros de VLANs.
999	***_Bit_Bucket_***	Réseau «trou noir» auquel on affecte les ports non utilisés des commutateurs.

Ceci est un exemple, cliquez sur le lien de téléchargement pour obtenir le cours complet.