

Passerelle

La passerelle (serveur DHCP, routage IP, ...)

- [Intro](#)
- [serveur DHCP](#)
- [Routage IP](#)
- [Portail captif](#)

Intro

La passerelle `proto.fablab.sorbonne-universite.fr` est un PC fonctionnant sous NetBSD, avec deux disques dur en RAID-1. Elle est accessible par ssh uniquement par clef publique/clef privée (pas de mot de passe).

- Elle assure les services DHCP pour les réseaux public et privés, et le routage pour les réseaux privés.
- Elle permet également de lancer idemake à travers un serveur vnc pour suivre les impressions à distance.
- Elle permet d'accéder aux interfaces de gestion des équipements réseau.
- Elle dispose d'un espace de stockage (accessible par samba: `smb://proto.fablab.sorbonne-universite.fr` ou `\\proto.fablab.sorbonne-universite.fr`) pour les sauvegardes de certains PCs (matériaux de la trotec, paramètres des impression 3d, réglages de galaad pour la CIF, ...).

Une deuxième machine identique `chimibio.fablab.sorbonne-universite.fr` est située dans l'espace chimie/biologie.

- Elle assure la continuité du vlan 3 (public) entre les deux espaces grâce à un tunnel l2tp.
- d'accéder aux interfaces de gestion de la borne wifi de l'espace chimie/biologie
- Elle dispose d'un espace de stockage pour les sauvegardes timemachine. L'accès à timemachine se fait par mot de passe.

serveur DHCP

La configuration du serveur DHCP se trouve dans le fichier */etc/dhcpd.conf*. Les logs du serveur sont dans */var/log/dhcp*. Dans le fichier de conf il est possible d'enregistrer les adresses ethernet des machines pour leur attribuer une adresse IP fixe. C'est le cas pour toute les imprimantes 3d et pour certaines machines fixes. Pour les vlans 205 et 3 il y a également une plage d'adresses dynamiques (la ligne *range*) permettant d'attribuer une adresse IP à une machine qui n'est pas enregistrée.

Routage IP

La passerelle assure le routage IP pour les vlans privés, avec filtrage et translation d'adresse (NAT) pour les communications extérieures. L'outil utilisé est npf (voir les pages de manuel *npf*, *npf.conf* sous NetBSD ainsi que <http://rmind.github.io/npf/>).

Pour pouvoir assurer le routage la machine doit avoir une adresse IP sur chaque vlan. Pour cela, la machine utilise l'encapsulation 802.1q pour envoyer des trames sur les différents vlan en utilisant une seule interface physique. Cela suppose que le port du switch en face soit configuré pour accepter ces trames.

L'interface physique est utilisée pour communiquer sur le vlan 1, qui permet de joindre les équipements réseau. Pour chaque autre vlan une interface vlan est créée avec l'adresse IP correspondante (voir les fichiers */etc/ifconfig.**).

Portail captif

Sur le réseau fablab (vlans 2 et 3), l'accès à l'extérieur est limité tant que la machine ou objet connecté n'a pas été authentifié. L'authentification se fait par la page <https://proto.fablab.sorbonne-universite.fr/gw/>. Un ordinateur ou téléphone devrait ouvrir automatiquement cette page; si ce n'est pas le cas il est toujours possible d'entrer l'URL ci dessus dans la barre d'adresse.

Certaines destinations sont accessibles sans authentification, en particulier les site web fablab.sorbonne-universite.fr et wiki.fablab.sorbonne-universite.fr, proxyweb.upmc.fr, les services DNS et NTP du campus.

Lors de la connection à <https://proto.fablab.sorbonne-universite.fr/gw/> il propose par défaut d'autoriser la machine qui se connecte. Mais il est possible d'autoriser une autre machine si on connaît son adresse IP, ou son adresse MAC. Il suffit pour cela de renseigner le champ correspondant (un seul des deux suffit), et de cliquer sur le bouton Rechercher correspondant. Si la machine est connectée au réseau elle apparaîtra.

Les autorisation sont remises à zero toute les nuits; mais une machine qui se déconnecte du réseau verra son autorisation supprimée après quelque minutes.

Certains équipements du lab ont une adresse IP fixe (imprimantes 3d, PCs associés au machines); la liste est dans le fichier `/etc/hosts` sur proto.fablab.sorbonne-universite.fr (accès par ssh pour ceux qui ont un compte).

La page <https://proto.fablab.sorbonne-universite.fr/gw/status> donne la liste des machines connectée au réseau, et si elles sont autorisées (et par qui).