Réseau fablab

description / adminitration du réseau (ethernet et wifi) du fablab

Architecture

organisation du réseau fablab

Les réseaux virtuels

Les réseaux virtuels, ou VLAN, permettent d'implémenter plusieurs réseaux ethernet distincts sur un même matériel physique. Cela permet d'isoler différentes machines sans multiplier les équipement réseau.

Un VLAN est identifié par un numéro, compris entre 1 et 1024 dans le cas des cisco. Chaque port d'un commutateur se voit affecté un numéro de vlan. Pour les communications entre équipements réseau, il est possible d'avoir un port appartenant à plusieurs vlans. Dans ce cas une en-tête est ajoutée aux trames ethernet contenant le numéro de vlan auquel appartient la trame: c'est l'encapsulation 802.1q.

Un port utilisant l'encapsulation 802.1q peut aussi émettre ou reçevoir des trames non encapsulées (ou ethernet native), il faut aussi associer un vlan au port pour ces trames natives.

Sur la plupart des équipements supportant les vlans 802.1q les ports sont par defaut dans le vlan 1.

Architecture

Les VLANs du fablab

Le fablab utilise les vlans pour isoler les traffics entre different équipements ou utilisateurs:

- 205 (fablabws ou fablabstaff): pour les machines des permaments du fablab et les rares équipement ayant besoin d'une connection internet directe. Le SSID wifi *fablabstaff* est connecté à ce vlan (rappel: ne pas donner accès à ce réseau aux étudiants, il est réservé aux permaments).
- 2 (imp): pour les imprimantes 3d et le PC associé. Elles sont sur un vlan distinct pour que les utilisateurs ne puissent pas communiquer directement avec les imprimantes depuis leur laptop,
- 3 (pub): pour les machines accessibles au public, et les machines perso du public. Le SSID wifi *fablab* est connecté à ce vlan.
- 4 (fablab-bad) pour les équipements à la sécurité douteuse
- 5 (imp restreint) pour les imprimantes 3d et PC associé de l'espace à accès restreint
- 1 (defaut) pour l'administration des équipements réseau.

Seul le vlan 205 est connu de la DSI, ce vlan peut donc être utilisé sur tout le campus. Une prise sur le vlan 205 peut être soit sur un switch de la DSI soit sur le notre.

Les autre vlans n'existent que sur les équipements réseau du fablab et ne sont donc accessible que sur les sites ou le fablab dispose d'un équipement réseau.

Connection internet

Chaque vlan utilise une plage d'adresse IP distincte:

- le vlan 205 utilise la plage 134.157.102.128/25, attribuée par la DSI. Le routeur de la DSI a pour IP 134.157.102.254. Notre passerelle proto.fablab.sorbonne-universite.fr est connectée à ce réseau et assure le service DHCP pour la configuration des postes clients. Sur ce vlan, les adresses IP 134.157.102.128->134.157.102.223 peuvent se connecter sans restriction à internet, les adresses 134.157.102.224->134.157.102.253 ne peuvent se connecter qu'a quelque machines du campus, dont le proxy http.
- Le vlan 2 (imp) utilise la plage d'adresses privées 10.0.2.0/24. Le routage avec translation d'adresse est assuré par notre passerelle, ainsi que le service DHCP. Les machines sur ce vlan ne peuvent se connecter à internet qu'au travers du proxy http du campus.
- Le vlan 3 (pub) utilise la plage d'adresses privées 10.0.3.0/24. Le routage avec translation d'adresse est assuré par notre passerelle, ainsi que le service DHCP. Les machines sur ce vlan ne peuvent se connecter à internet qu'au travers du proxy http du campus.
- Le vlan 4 (fablab-bad) utilise la plage d'adresses privées 10.0.4.0/24
- Le vlan 5 (imp restreint) utilise la plage d'adresses privées 10.0.5.0/24

Les paramètres pour le proxy sont: proxyweb.upmc.fr port 3128.

Passerelle

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

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).

- Elles assure les services DHCP pour les réseaux public et privés, et le routage pour les réseaux privés.
- Elle permet également de lancer idemaker à travers un serveur vnc pour suivre les impressions à distance.
- Elle permet d'accèder 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 estsituée dans l'espace chimie/biologie.

- Elle assure la continuité du vlan 3 (public) entre les deux espaces grace à un tunnel l2tp.
- d'accèder 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 differents 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 créé 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 object connecté n'a pas été autentifié. L'autentification se fait par la page https://proto.fablab.sorbonne-universite.fr/gw/. Un ordinateur ou téléphonne 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 autentification, 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 connait 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 apparaitra.

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).

Equipements réseau

Accès aux équipements réseau

L'accès aux équipements réseau se fait uniquement sur le vlan 1, depuis proto.fablab.sorbonne-universite.fr pour les équipements en proto et chimibio.fablab.sorbonne-universite.fr pour fablab-wifi-3. Le login sur tout les équipements est admin.

Pour accès en ligne de commande:

- ssh proto.fablab.sorbonne-universite.fr
- pour le switch: telnet fablab-eth-1
- pour les bornes: telnet fablab-wifi-1 ou telnet fablab-wifi-2

Pour accès à l'interface web:

- ssh -D1234 proto.fablab.sorbonne-universite.fr
- dans firefox configurer un proxy SOCKSv5 sur localhost port 1234
- accéder à http://fablab-eth-1/ ou http://fablab-wifi-1/ ou http://fablab-wifi-2/

Pour fablab-wifi-3 (borne en chimie/biologie) il faut passer par chimibio.fablab.sorbonne-universite.fr

DLink dap-2680

Les bornes wifi du fablab sont des DLink dap-2680 (le manuel est en attachement). Elles sont alimentées par power over ethernet (POE), il faut donc les connecter soit sur un switch POE (les bornes consomment au max 17W) soit sur un injecteur POE, lui même connecté à un switch. Les bornes s'apellent fablab-wifi-1 (proche entrée) et fablab-wifi-2 (proche bureaux) en proto; fablab-wifi-3 en biologie/chimie

Ces bornes supportent les SSID multiples (8 en b/g/n et 8 en a/c), elles peuvent donc servir plusieurs réseau wifi en même temps. Chaque SSID peut être attaché à un vlan 802.1Q différent (il faut donc que la borne soit connectée à un switch supportant vlans 802.1Q). Actuellement ces bornes servent 2 SSIDs: *fablab* (pour le public) et *fablabstaff* (pour les permanents - ne pas donner accès aux étudiants à ce réseau) en chimie/biologie. Dans l'espace proto on trouve en plus *fablabo* (identique à *fablab* mais pour les équipements anciens ne supportant pas WPA2) et *fablab-bad* (pour les équipements à la sécurité douteuse).

Les bornes ont leur adresses IP sur le vlan 1, natif sur le lien ethernet (non taggué). Les vlans 3 (*fablab*), 4 (*fablab-bad*) et 205 (*fablabstaff*) sont taggués sur le port ethernet.

L'interface web de gestion est accessible uniquement depuis les passerelle proto.fablab.sorbonne-universite.fr. On peut y accéder de la manière suivante:

1. utiliser SSH pour créer un proxy socks sur le port 1234 (par exemple): *ssh -D1234 proto.fablab.sorbonne-universite.fr* (cela suppose d'avoir un accès ssh à la passerelle).
2. Configurer son navigateur web (firefox par exemple) pour utiliser un proxy socks sur la machine localhost, port 1234
3. entrer l'URL https://fablab-wifi-1/ (et accepter le certificat auto-signé). Le login est *admin*

Pour fablab-wifi-3 il faut passer par chimiebio.fablab.sorbonne-universite.fr

Les bornes sont également accessible en ligne de commande par telnet (depuis proto.fablab ou chimiebio.fablab), on peut les redémarer par la commande *reboot*