UNIVERSITÉ DE NANTES

Direction des Systèmes d'Information

Manuel Utilisateur

Guide de connexion à internet en cité universitaire sous les environnements GNU/Linux Ubuntu - Standard IEEE 802.1X -

Version 1.2 du 29/08/2013

Avertissement

Tout usage abusif des ressources informatiques est susceptible de faire l'objet de poursuites judiciaires ou d'une coupure de votre accès à internet en cité. Chaque usager est tenu de respecter les termes de la charte RENATER dont une copie est disponible à l'adresse :

En français :

eduroam.univ-nantes.fr/charte/charte_fr.pdf

En anglais :

eduroam.univ-nantes.fr/charte/charte_en.pdf

Nous vous invitons à en prendre connaissance, soit en vous connectant au préalable à internet au travers des portails captifs du CROUS, soit à l'issue du présent mode opératoire.

Assistance technique

La Direction des Systèmes d'Information (DSI) de l'Université de Nantes est à votre écoute si des questions restent en suspens ou qu'un problème technique demeure insoluble. Pour vous assister, de nombreuses informations sont déjà disponibles sur le wiki de l'Université (choix du profil étudiants → Autres documentations).

Renseignements techniques :

wiki.univ-nantes.fr

Courriel d'échange avec la DSI :

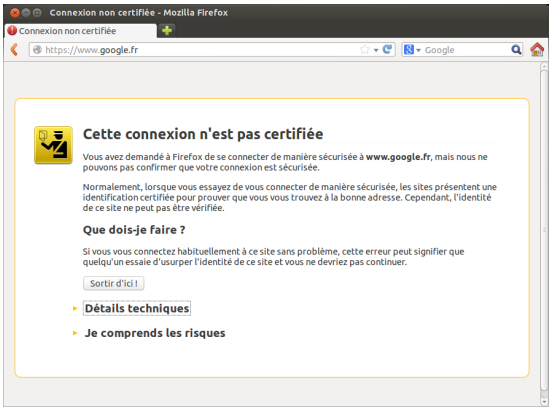
logement-u.informatique@univ-nantes.fr

Une nouvelle méthode de connexion à internet

En complément des traditionnels portails captifs, l'Université de Nantes propose une nouvelle méthode de connexion basée sur le standard IEEE 802.1x. C'est à votre système d'exploitation qu'incombe désormais la charge de vous authentifier auprès de l'infrastructure réseau. Là, une notification apparaît automatiquement après l'ouverture de votre session, vous demandant de saisir votre identifiant/mot de passe habituel à moins que ces informations ne soient déjà enregistrées dans votre profil de connexion.

La navigation sur internet se fait toujours au moyen de serveurs mandataires également appelés proxies. Alors que les portails vous refusaient l'accès au web sur un mauvais paramétrage de votre navigateur, la nouvelle méthode se montre plus flexible en rendant les proxies transparents. Ainsi, même sans configuration proxy adéquate, votre navigateur bénéficie d'un accès au web en http (sites dits non sécurisés) et https (sites dits sécurisés). Mais, en retour, un navigateur mal configuré (i.e. sans proxy) lèvera une alerte de sécurité lors de la visite d'un site web sécurisé. Un message du type "cette connexion n'est pas certifiée" ou encore "le certificat de sécurité de ce site web présente un problème" apparaîtra à chaque page https visitée :

– Avertissement généré par Firefox.



– Avertissement généré par Chrome/Chromium.

Il est juste de considérer la situation comme un risque potentiel à l'intégrité et la confidentialité de vos données, même si toutes les précautions de sécurisation sont prises sur les serveurs mandataires de l'Université. Le risque disparaît en paramétrant votre navigateur conformément aux recommandations rappelées dans le wiki.

Pré-requis

Ce mode opératoire concerne exclusivement les étudiants en cité universitaire disposant d'une connexion filaire au moyen d'une prise murale Ethernet/RJ45.

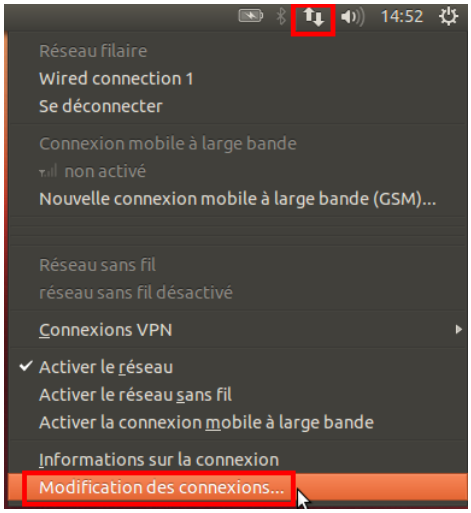
Vous disposez d'un nom d'utilisateur commençant par dw- délivré avant le 19/10/2012 ? Pour bénéficier de la nouvelle méthode d'authentification, vous devez changer votre mot de passe en vous rendant sur la page web `http://motdepasse.cites-u.univ-nantes.fr`. Les utilisateurs de l'Université de Nantes et ceux disposant d'un compte postérieur au 18/10/2012 ne sont pas concernés.

Description du mode opératoire

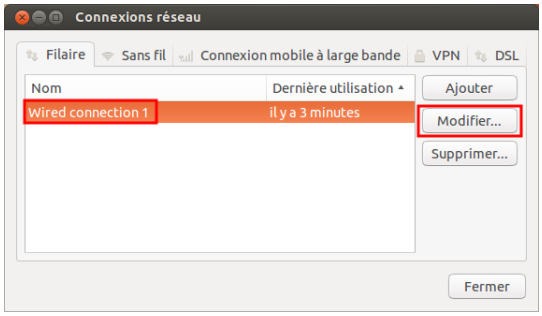
Nous décrivons, à présent, les phases successives de configuration des systèmes GNU/Linux Ubuntu 12.10 (Quantal Quetzal). Ce mode opératoire prévaut, à quelques différences mineures près, dans toutes les distributions basées sur l'environnement graphique Gnome.

1. Depuis votre chambre en cité, connectez le câble réseau à votre ordinateur.

2. Cliquez en haut à droite de la barre d'état sur l'icône réseau puis sélectionnez dans le menu **Modification des connexions**.

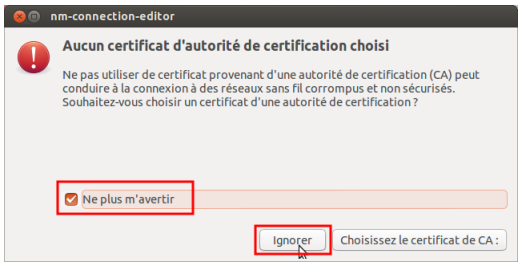


3. Sous l'onglet **filaire**, sélectionnez le réseau ethernet actif puis cliquez sur le bouton **Modifier**.

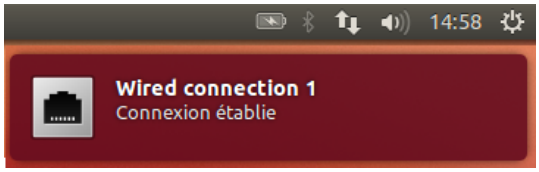


4. Sous l'onglet **Sécurité 802.1x**, cochez la case **Utiliser la sécurité 802.1x pour cette connexion** puis renseignez les paramètres suivants comme ceci : Authentification **Protected EAP (PEAP)** / Authentification interne **MSCHAPv2**. Saisissez ensuite les paramètres d'authentification comme précisé ci-dessous (il s'agit des mêmes que sur les portails captifs) puis cliquez sur le bouton **Enregistrer**.
   - Vous êtes un **étudiant** de l'Université de Nantes ? Le nom d'utilisateur à saisir se compose de votre identifiant intranet (ex. 'e990000') ou bien de votre adresse mail université (ex. 'jean.dupont@etu.univ-nantes.fr'). Le **mot de passe** est celui que vous saisissez à chaque connexion à l'intranet ou à l'ouverture de votre messagerie université.
   - Vous n'êtes pas inscrit à l'Université de Nantes ? Le nom d'utilisateur à saisir se compose de votre identifiant CROUS (ex. 'dw-dupont-j'). Cet identifiant, le **mot de passe** associé et la date de fin de validité du compte vous ont été transmis sous format papier par le CROUS lors de votre entrée en chambre universitaire.

5. Un tunnel sécurisé va s'établir en direction des serveurs d'authentification de l'Université de Nantes. L'Autorité de Certification employée, pourtant reconnue des principaux navigateurs web, ne l'est pas dans le système Ubuntu. Aussi, un avertissement est levé. Cochez la case **Ne plus m'avertir** puis cliquez sur le bouton **Ignorer**.



6. Le profil de connexion 802.1X est prêt à l'emploi. Le système va automatiquement tenter de s'authentifier auprès de l'équipement réseau d'accès de la cité. La notification suivante doit apparaître en l'espace d'une à deux secondes si les paramètres de configuration et d'authentification du profil 802.1X sont corrects.

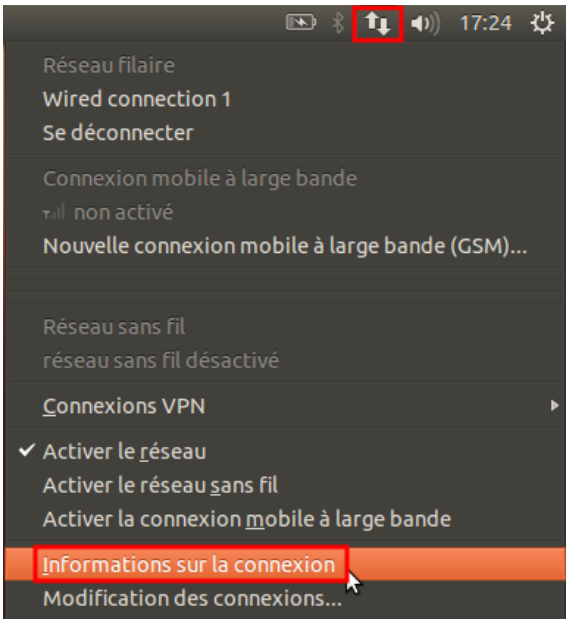


Désormais, le système Ubuntu vous authentifiera automatiquement au redémarrage de votre ordinateur ou encore au changement d'état de votre interface réseau (débranchement/branchement de votre câble Ethernet/RJ45). Sachez qu'en cas d'échec d'authentification, une fenêtre de ressaisie de votre mot de passe réapparaîtra au bout d'une vingtaine de secondes.

Contrairement aux systèmes Microsoft Windows, vous ne basculez pas automatiquement sur les portails captifs en cas d'échecs successifs d'authentification ou de défaut de paramétrage de votre profil de connexion 802.1x. Vous perdez toute connectivité sur internet... Le rétablissement de l'accès aux portails captifs nécessite seulement de rejouer les étapes 2, 3 et de décocher la case Utiliser la sécurité 802.1x pour cette connexion **à l'étape 4.**

Vérification de la connexion 802.1X

1. Cliquez à nouveau en haut à droite de la barre d'état sur l'icône réseau puis, sélectionnez cette fois-ci dans le menu, **Informations sur la connexion** pour obtenir de plus amples informations sur la connexion filaire en cours.



2. Vous devez voir apparaître **Sécurité : 802.1x, EAP-PEAP, MSCHAPv2**. En outre, vous remarquerez que votre adresse IP a changé par rapport à l'accès traditionnel via les portails captifs. Maintenant, elle est comprise dans la plage 192.168.100.x à 192.168.120.x.