

R1.04 – Cours 6

Réseaux IP, Travail à distance

Département Informatique

IUT2, UGA

2023/2024

Plan du cours

- 1 Message pour le TP6
- 2 Introduction
- 3 Environnement réseau de l'IUT2
- 4 Adresses et ports dans les réseaux IP
- 5 Travail à distance
- 6 Utilisation de machines à distance
- 7 Partage et transfert de fichiers
- 8 Résumé

Plan du cours

- 1 Message pour le TP6
- 2 Introduction
- 3 Environnement réseau de l'IUT2
- 4 Adresses et ports dans les réseaux IP
- 5 Travail à distance
- 6 Utilisation de machines à distance
- 7 Partage et transfert de fichiers
- 8 Résumé

Message pour le TP6

- 2 séances de TP cette semaine
- TP6 Linux, 2h
- TP6 Windows, 1h30
- Si vous avez un ordinateur portable,
apportez-le cette semaine pour la séance de TP de 1h30

Plan du cours

- 1 Message pour le TP6
- 2 Introduction
- 3 Environnement réseau de l'IUT2
- 4 Adresses et ports dans les réseaux IP
- 5 Travail à distance
- 6 Utilisation de machines à distance
- 7 Partage et transfert de fichiers
- 8 Résumé

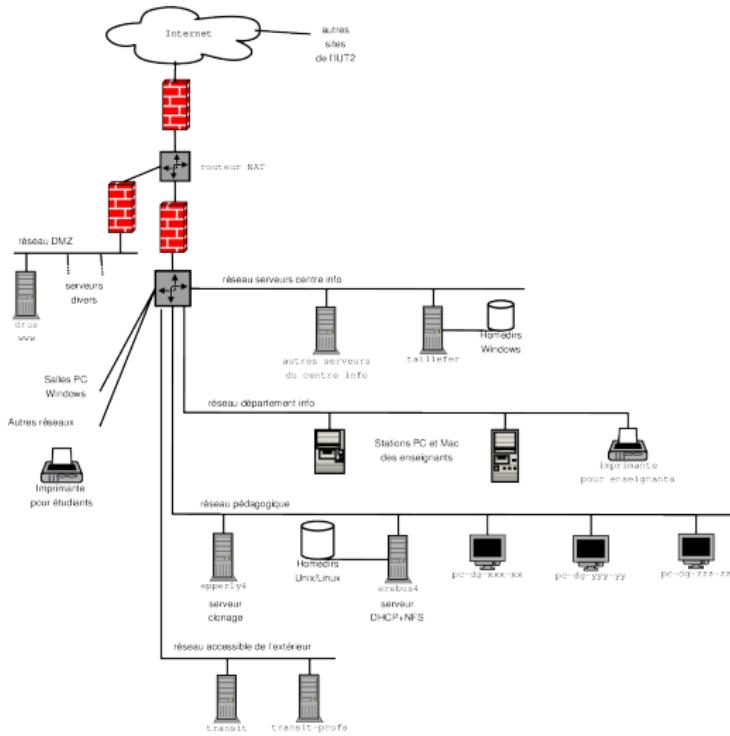
Buts et utilité des réseaux

- Réseaux : fonctionnalité essentielle d'un OS moderne
- Centralisation et partage de ressources
 - stockage (serveur de fichiers et/ou d'applications)
 - sauvegardes
 - imprimantes
 - puissance de calcul (CPU/RAM) : utilisation à distance
 - maintenance et support technique à distance
 - ...
- Accès à Internet
 - courrier électronique
 - Web
 - ...
- Applications client/serveur
 - bases de données (SGBD)
 - applications Web ou intranet
 - ...

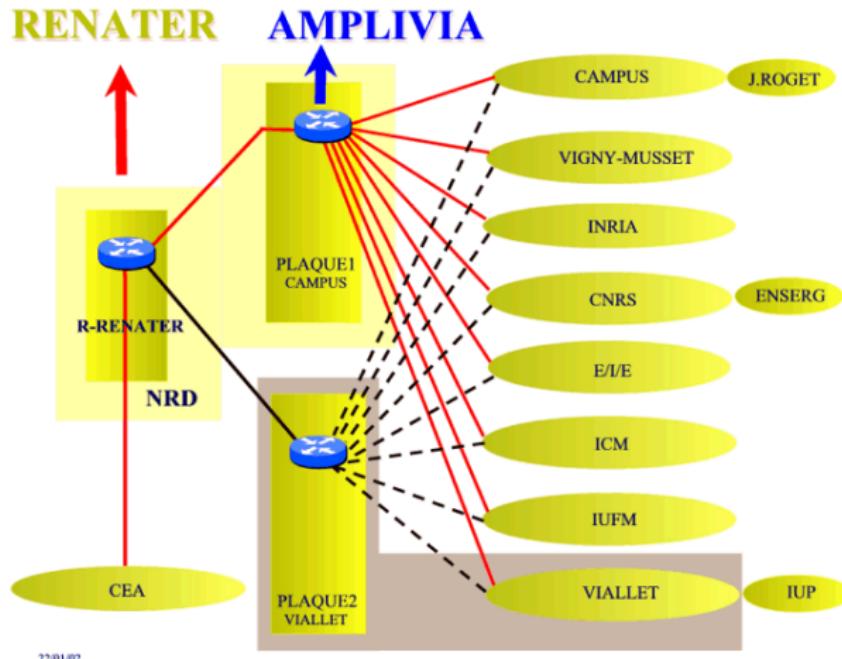
Plan du cours

- 1 Message pour le TP6
- 2 Introduction
- 3 Environnement réseau de l'IUT2
- 4 Adresses et ports dans les réseaux IP
- 5 Travail à distance
- 6 Utilisation de machines à distance
- 7 Partage et transfert de fichiers
- 8 Résumé

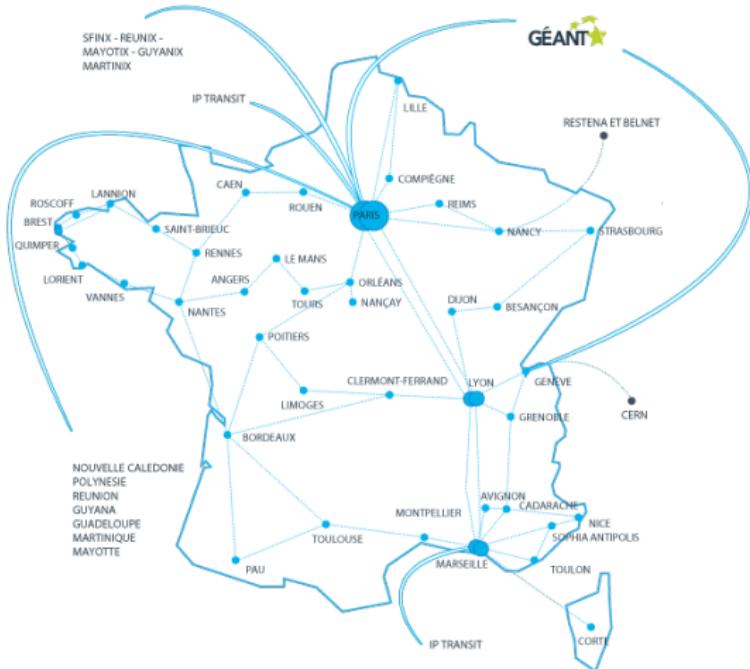
Réseau local de l'IUT2 : routeurs et filtrage



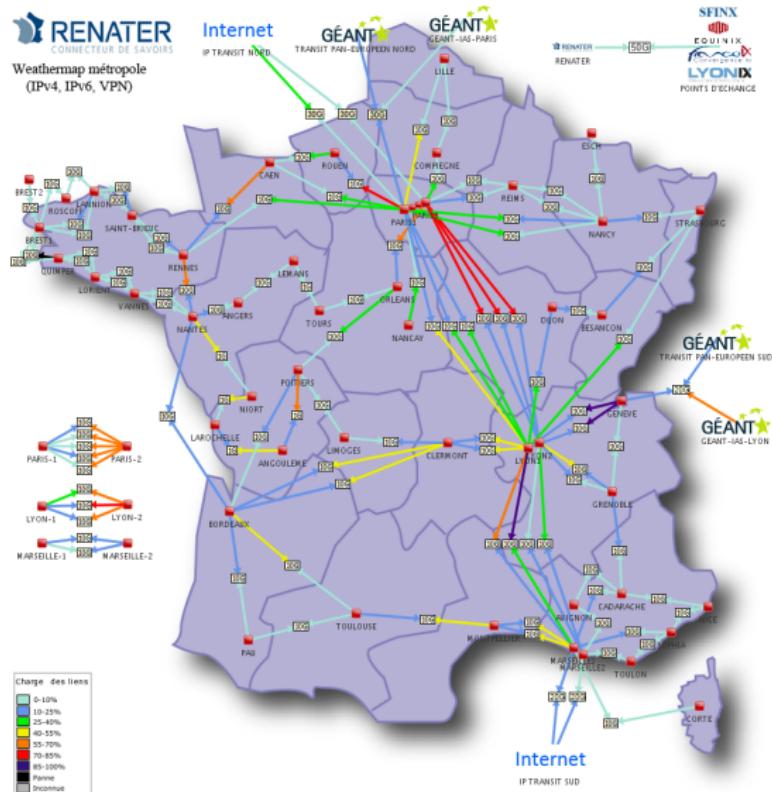
Maillage des sites académiques de Grenoble



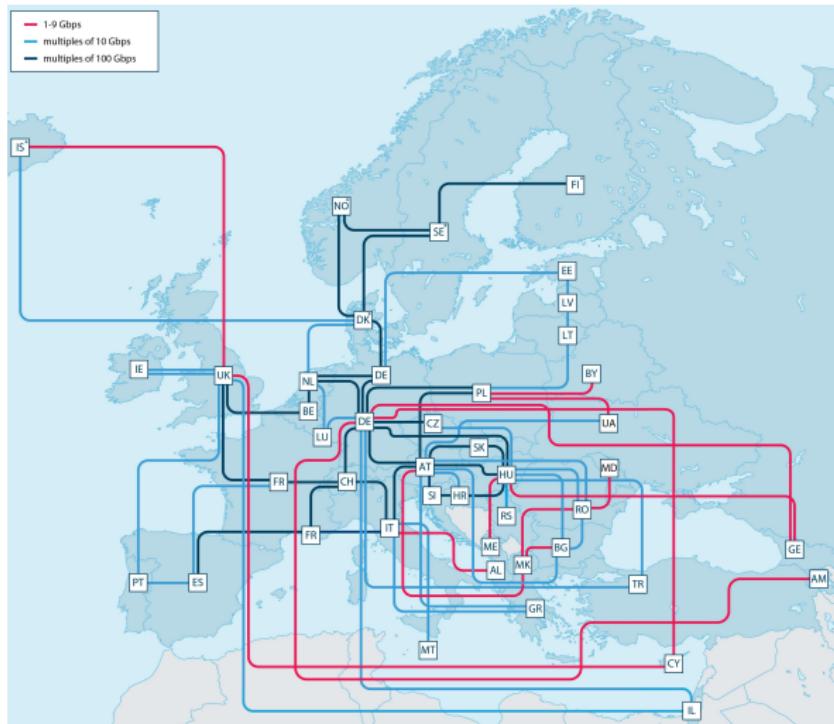
Maillage des sites académiques français (1)



Maillage des sites académiques français (2)



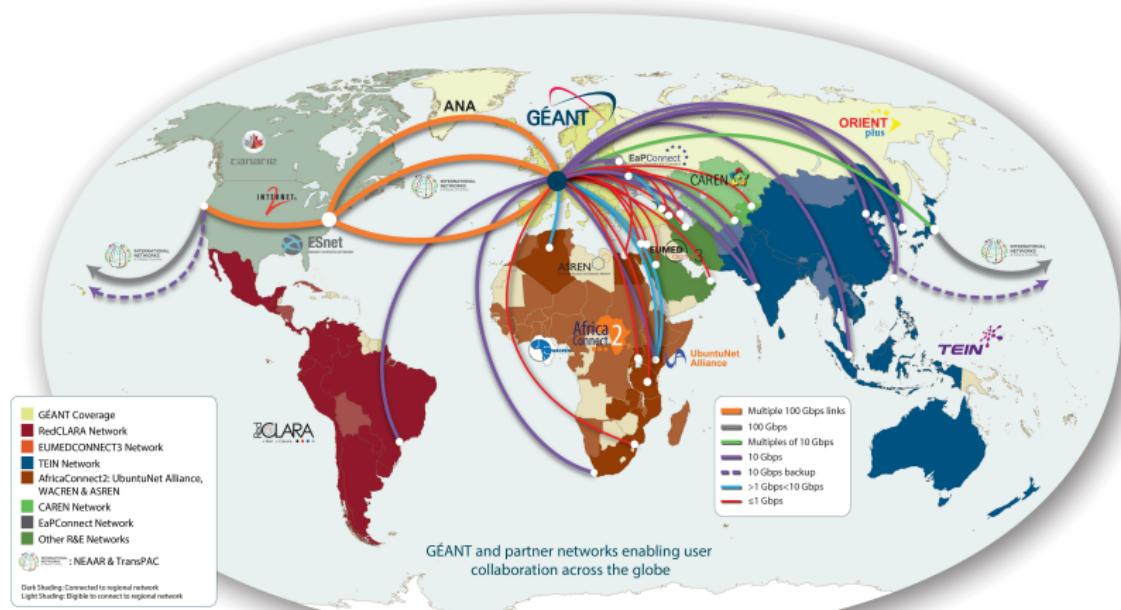
Maillage des sites académiques européens



Liens Europe ↔ Reste du monde



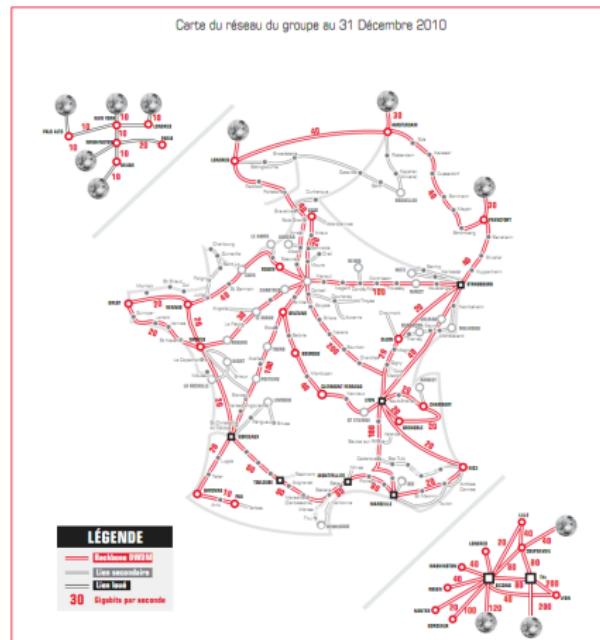
At the Heart of Global Research and Education Networking



This document is produced as part of the GÉANT Specific Grant Agreement GA4-2 (No. 731122), that has received funding from the European Union's 2020 research and innovation programme under the GÉANT2020 Framework Partnership Agreement (No 851998). In addition to GA4-2, the following projects have received funding from the European Union: AfricaConnect2, CAREN, AfriConnect (DG DEVCO), EaPConnect and EU-MEDCONNECT3 (DG NEAR). The content of this document is the sole responsibility of GÉANT and can under no circumstances be regarded as reflecting the position of the European Union.



Exemple de réseau d'un FAI



Interconnexion avec Renater à Paris (SFINX)

Plan du cours

- 1 Message pour le TP6
- 2 Introduction
- 3 Environnement réseau de l'IUT2
- 4 Adresses et ports dans les réseaux IP
- 5 Travail à distance
- 6 Utilisation de machines à distance
- 7 Partage et transfert de fichiers
- 8 Résumé

Adresses IP

- Une machine reliée à Internet nécessite une adresse IP
- Les machines sont identifiées sur Internet par un nom (*hostname*) ou une adresse IP
- Les adresses IP servent au routage → Toute machine reliée à Internet doit avoir une adresse IP propre
- **IPv4**
 - adresses sur **32 bits**
 - notation décimale pointée : 4×8 bits → 4 chiffres entre 0 et 255
 - exemples
 - une station Linux : 192.168.141.100
 - serveur Web de l'IUT2 : 193.55.51.242
- Actuellement : adresses IPv4 épuisées !
- **IPv6**
 - adresses sur **128 bits**
 - notation plus complexe
 - plusieurs adresses pour chaque machine.
 - exemple pour station Linux :
`fe80::260:67ff:fe37:2a9a`
`fd00::7ff`

Adresses privées (RFC1918)

- Utilisation libre par chaque site
- Adresses routées en interne du site mais pas hors du site
- Permet à un site d'avoir plus de stations que le nombre d'adresses publiques attribuées à ce site
- Les stations Linux ont des adresses privées → inaccessibles directement depuis l'extérieur !
- Utilisation d'un mécanisme de traduction d'adresses (NAT/PAT/Masquerading) pour l'accès à Internet → toutes les applications réseau courantes fonctionnent
- Tableau des adresses privées :

Classe	Intervalle d'adresses
A	10.x.y.z
B	172.16.x.y à 172.31.x.y
C	192.168.0.x à 192.168.255.x

Obtention d'une adresse IP par une machine

Configuration manuelle

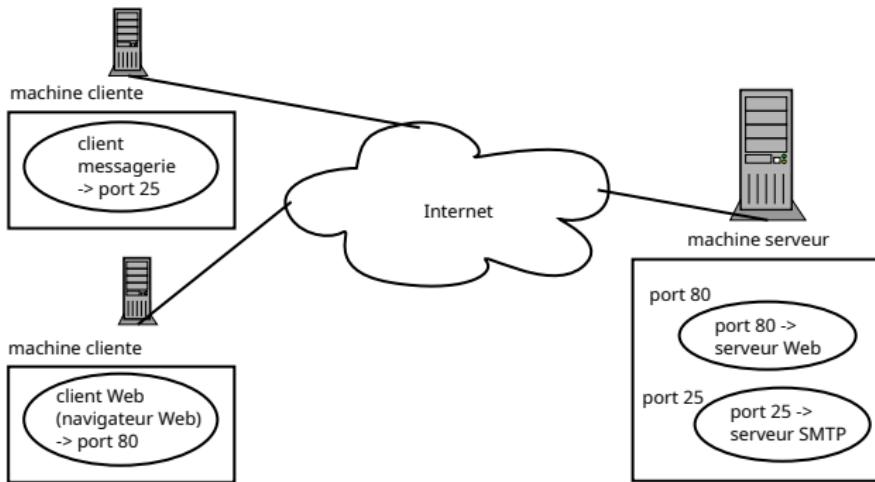
- configuration de chaque station par l'administrateur
- utilisé pour certains serveurs

Autoconfiguration

- utilisation d'un serveur d'adresses au niveau d'un site
- utilisé pour la plupart des stations
- Avec IPv4
 - autoconfiguration par protocole **DHCP**
 - utilisé à l'IUT2 pour les machines sous Linux et Windows, ...
 - utilisé dans les boxes des FAI, les réseaux mobiles (3G, 4G, 5G), ...
- Avec IPv6
 - autoconfiguration prévue dès la conception du protocole
 - utilisation possible de DHCPv6

Notion de port réseau

- Quand plusieurs logiciels serveurs tournent sur une même machine l'adresse IP n'est pas suffisante pour identifier la destination
- Port = numéro servant à distinguer les logiciels serveurs



Numéros de ports couramment utilisés

- port 80 pour contacter un serveur Web (protocole HTTP)
- port 25 pour contacter un serveur d'envoi des mails (SMTP)
- port 143 pour un serveur de réception de mails (IMAP)
- port 22 pour contacter un serveur SSH
- port 5432 pour contacter un serveur PostgreSQL
- port 5900 pour contacter un serveur VNC
- ...

Liste dans /etc/services

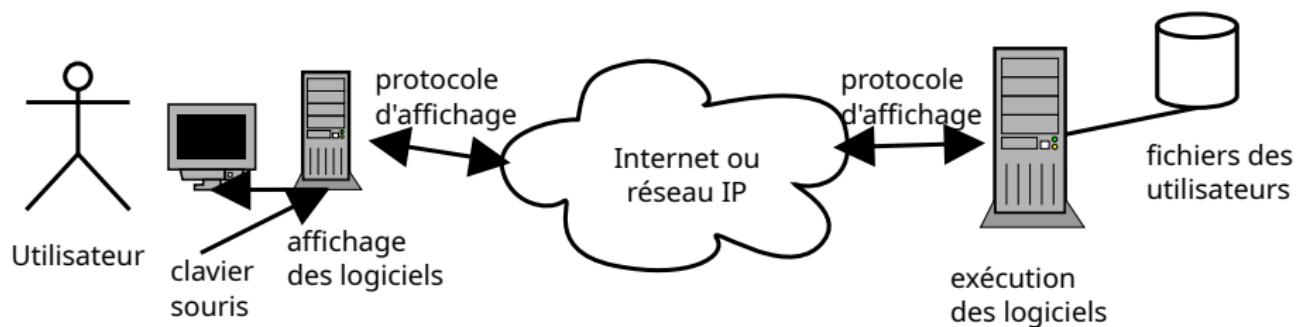
Plan du cours

- 1 Message pour le TP6
- 2 Introduction
- 3 Environnement réseau de l'IUT2
- 4 Adresses et ports dans les réseaux IP
- 5 Travail à distance
- 6 Utilisation de machines à distance
- 7 Partage et transfert de fichiers
- 8 Résumé

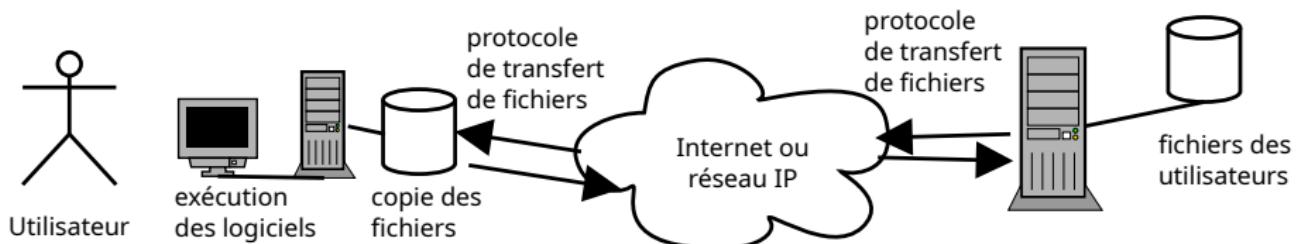
Travail à distance

- 2 formes de travail à distance
 - utilisation de machines à distance
 - transfert de fichiers
- Depuis 2 emplacements
 - le réseau local de l'IUT2
 - chez vous en utilisant Internet

Utilisation de machines à distance



Transfert de fichiers



Accès aux machines et fichiers de l'IUT2

Depuis l'IUT2

- Toutes les stations Linux sont utilisables à distance
- Les transferts de fichiers sont possibles avec tous les serveurs de fichiers

Depuis l'extérieur de l'IUT2

- Le pare-feu (*firewall*) interdit certains accès
 - L'accès aux fichiers ou aux machines ne peut se faire qu'avec un protocole sécurisé : SSH (*Secure SHell*)
- Les machines avec une adresse IP privée ne sont pas joignables directement
 - Il faut passer par une machine intermédiaire ayant une adresse IP publique : `transit.iut2.univ-grenoble-alpes.fr`
- On parle de «**bastion**»

Avertissement sur transit

- Le serveur transit a une capacité limitée
 - Il peut supporter quelques étudiants simultanément, mais pas 120
 - La **disponibilité** de ce serveur n'est **pas garantie**
 - Attention aux veilles de rendu de projets !
- Mieux vaut travailler sur votre propre ordinateur
- L'utilisation de ce serveur doit être vue comme un **dépannage ponctuel**
 - Nous verrons dans la SAÉ S1.03 l'installation d'un système Linux

Plan du cours

- 1 Message pour le TP6
- 2 Introduction
- 3 Environnement réseau de l'IUT2
- 4 Adresses et ports dans les réseaux IP
- 5 Travail à distance
- 6 Utilisation de machines à distance
- 7 Partage et transfert de fichiers
- 8 Résumé

Protocoles existants

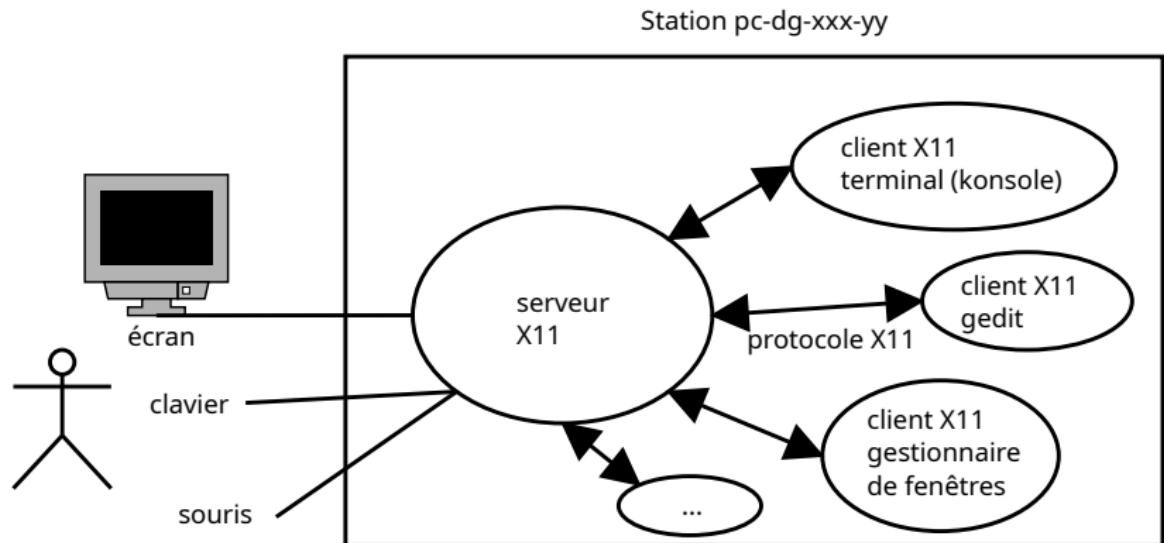
- Mode texte
 - telnet
 - SSH
- Mode graphique
 - X11
 - VNC
 - X2Go

Protocoles telnet, SSH

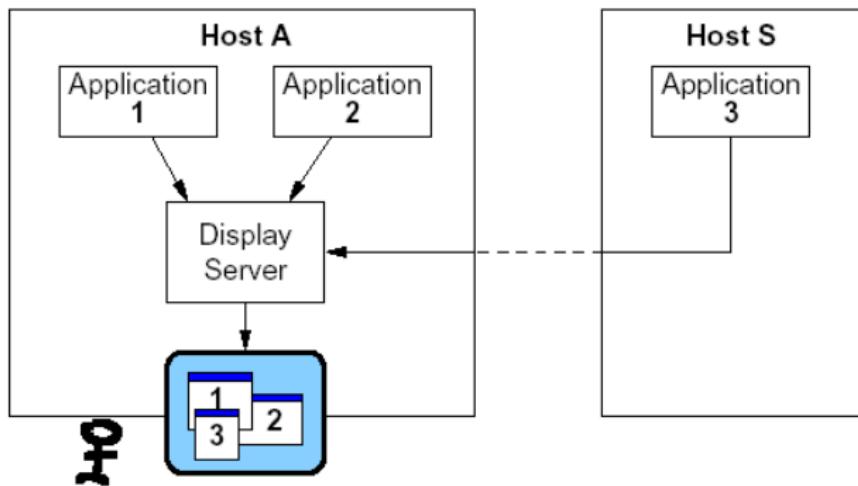
- Utilisation de machines en mode texte (dans un terminal)
- Protocole telnet
 - Protocole ancien, de moins en moins utilisé
 - Sans sécurité : le mot de passe est transmis en clair sur le réseau, ainsi que toute la session
- Pas de serveur telnet installé sur les machines de l'IUT2
- Protocole SSH (*Secure SHell*)
 - Sécurisé : le mot de passe et tout le reste est chiffré
 - 2 modes d'authentification : par mot de passe ou par clé SSH
 - Liste des clients sur l'intranet du département
 - Dispositif de sécurité (fail2ban) : 3 mots de passe erronés saisis
→ tous les paquets IP du client bloqués pendant 10 minutes

Protocole X11 : utilisation locale

X11 est un système graphique client/serveur



Protocole X11 : utilisation distante



- Le serveur graphique tourne sur la machine locale de l'utilisateur
- Les applications clientes tournent sur la machine distante
- Ce mode de fonctionnement est désactivé par défaut sous Linux car peu sûr

Utilisation de X11 à l'IUT2 : combinaison avec SSH

Depuis l'IUT2

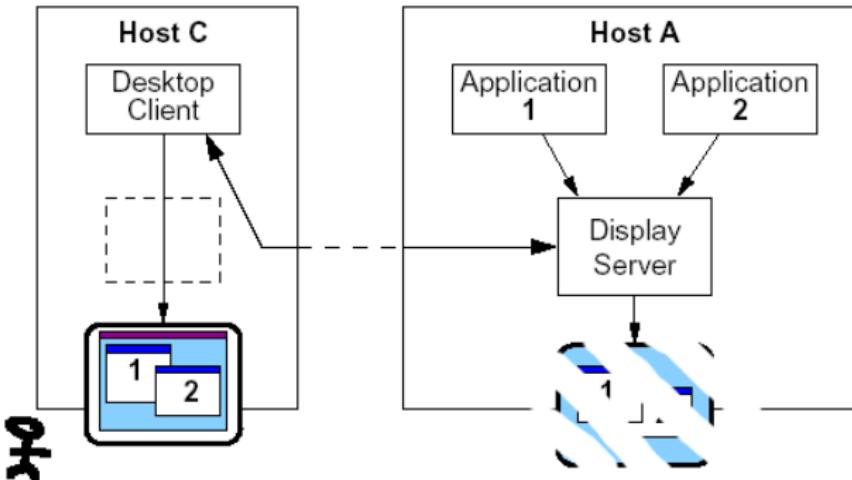
- Commande : `ssh -X pc-dg-xxx-xx`
- L'option `-X` (majuscule !) active le protocole X11

Depuis l'extérieur de l'IUT2

- Commande :
`ssh -X NOM_DE_LOGIN@transit.iut2.univ-grenoble-alpes.fr`
- Il faut faire tourner un serveur X11 sur la machine locale
 - Linux : serveur X11 natif
→ rien à faire
 - MacOS : serveur X11 pour MacOS
ex. : XQuartz
 - Windows : serveur X11 pour Windows
ex. : Cygwin

Protocole VNC (*Virtual Network Computer*)

- Un pseudo serveur graphique tourne sur la machine distante
- L'utilisateur fait tourner un client sur sa machine locale
- Avantages :
 - moins de latence que X11
 - un client VNC est très simple (un seul exécutable de ~300Ko)
- Inconvénient : en général plus de débit utilisé que X11



Utilisation de VNC à l'IUT2

Depuis l'IUT2

- Commande : `vncviewer pc-dg-xxx-xx`
- Résultat : on arrive sur un écran de connexion `lightdm`

Depuis l'extérieur de l'IUT2

- Passage par transit obligatoire, puis
 - utilisation directe de transit
 - utilisation d'une station Linux, quand les stations sont allumées
- Utilisation conjointe avec SSH
- 2 authentifications demandées (1 par SSH, 1 par `lightdm`)
- Détails dans l'intranet et en TP

X2Go

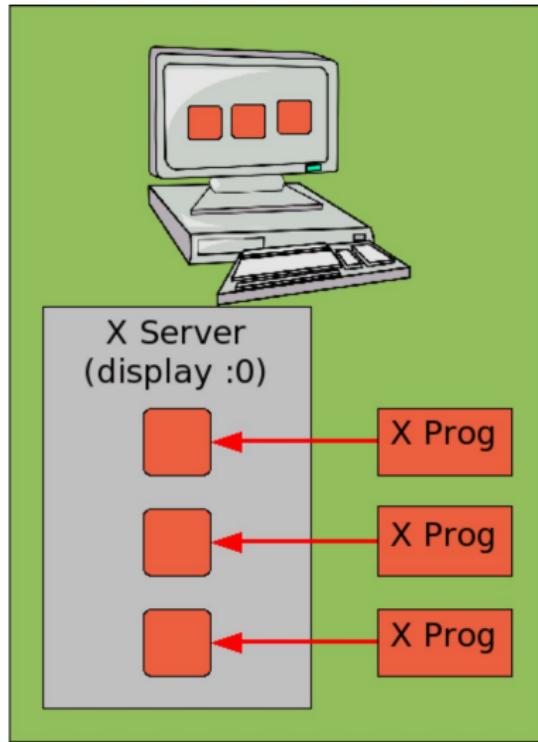
• Avantages

- plus simple à utiliser que X11 et VNC
- n'utilise qu'une connexion SSH
- utilise SSH de façon transparente
- une seule authentification demandée
- s'utilise de la même façon dans et hors IUT2

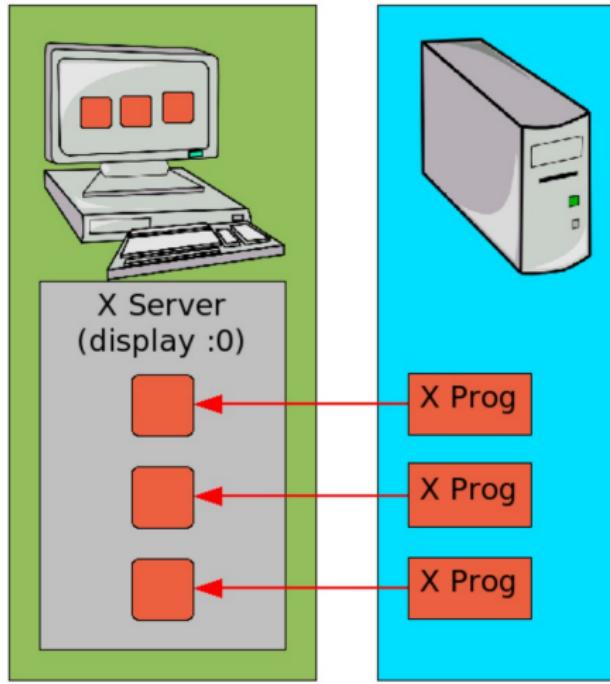
• Inconvénients

- client plus complexe qu'un client VNC
- un peu plus de latence que VNC
- ne fonctionne pas pour lancer Plasma

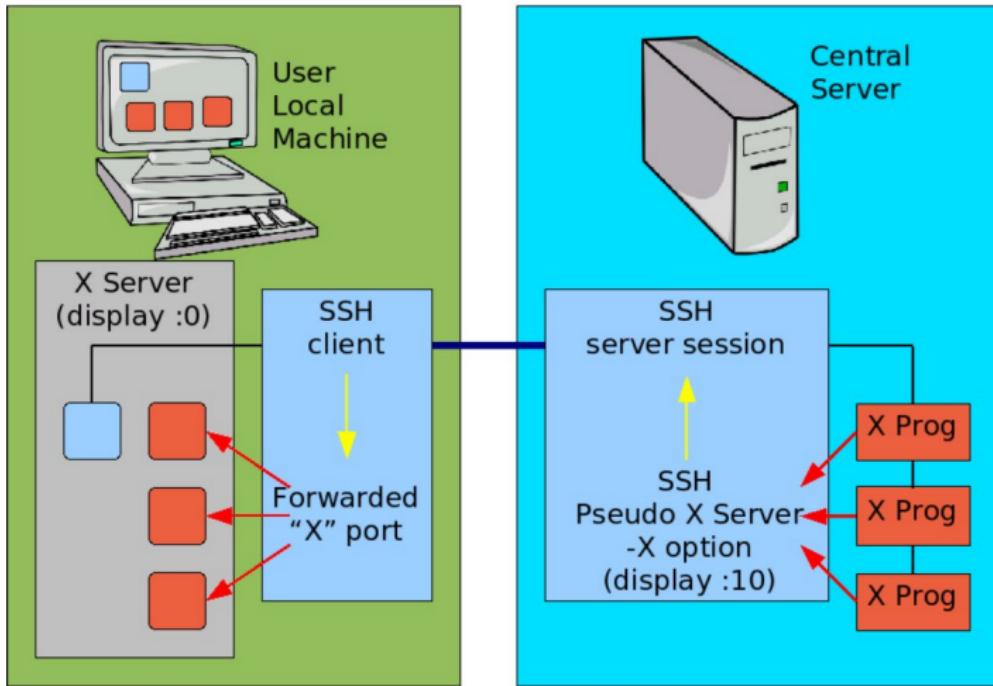
X11 en local



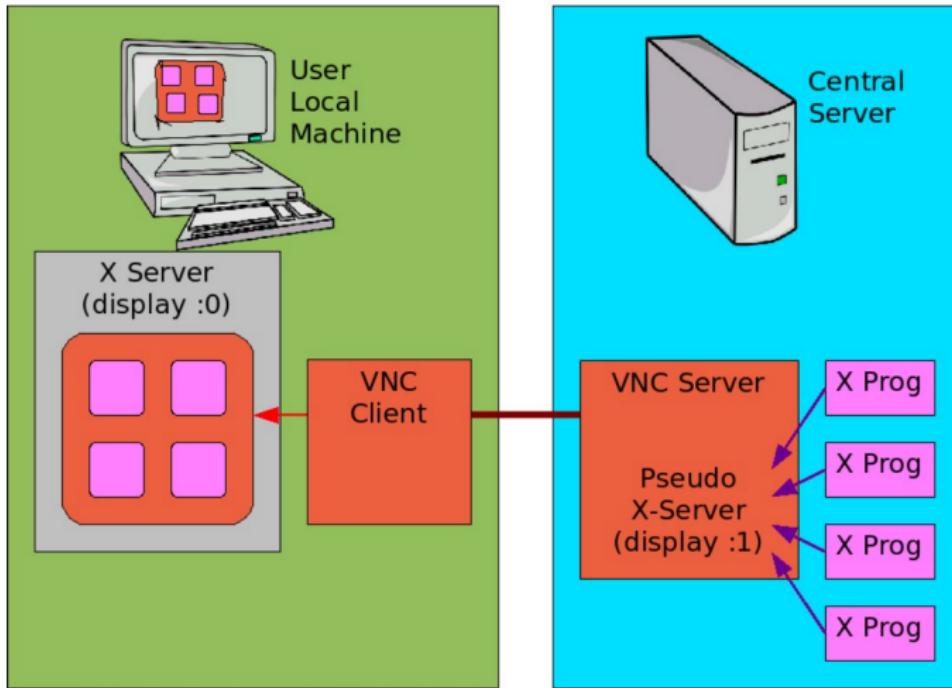
X11 en réseau



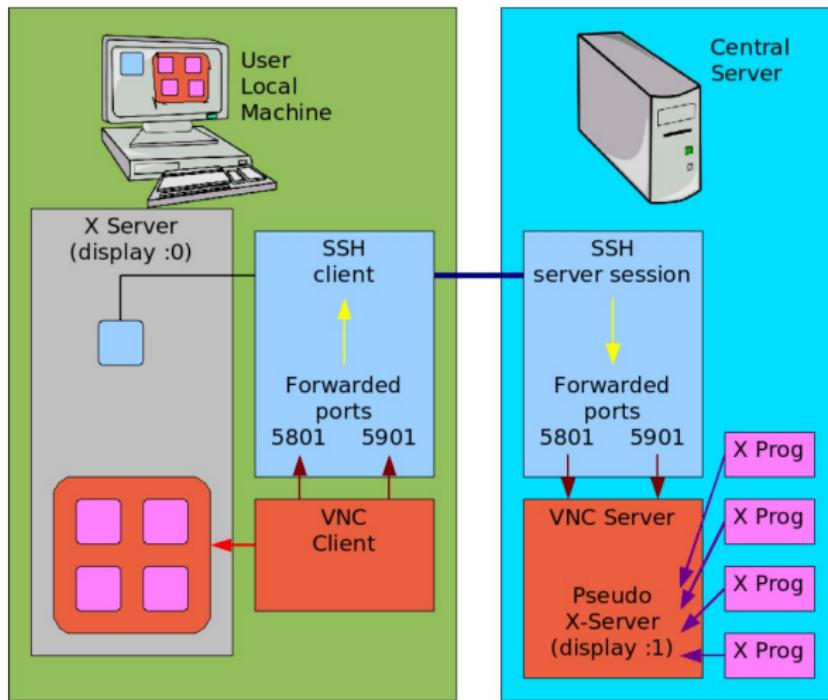
X11 en réseau sur SSH



VNC en réseau



VNC en réseau sur SSH



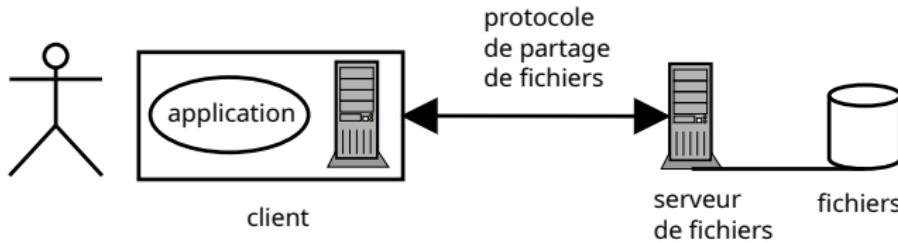
Plan du cours

- 1 Message pour le TP6
- 2 Introduction
- 3 Environnement réseau de l'IUT2
- 4 Adresses et ports dans les réseaux IP
- 5 Travail à distance
- 6 Utilisation de machines à distance
- 7 Partage et transfert de fichiers
- 8 Résumé

Partage de fichiers

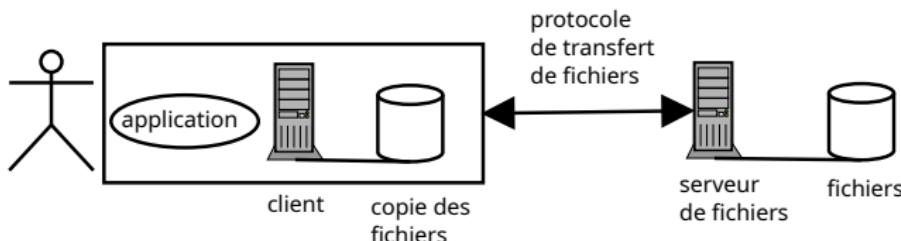
Répertoire partagé par un serveur

- Fichiers disponibles pour n'importe quelle application tournant sur les clients au même titre que des fichiers locaux
- Le système d'exploitation donne l'illusion que les fichiers distants sont locaux
- Ouverture et sauvegarde transparentes
- Il n'y a **pas de copie locale** des fichiers



Transfert de fichiers

- Il y a une **copie locale** des fichiers
- Travail en 3 temps :
 - copie serveur → client
 - ouverture, modification et sauvegarde par des logiciels
 - copie client → serveur



- L'utilisateur doit gérer 2 copies des fichiers

Protocoles de partage de fichiers

- Chaque système d'exploitation a son protocole natif
 - Unix/Linux : NFS (*Network File System*)
 - Windows : SMB (*Server Message Block*)
 - MacOS : AFP (*Apple Filing Protocol*), NFS
- L'opération qui rend les fichiers du serveur accessibles sur un client s'appelle un «montage»
- Des clients et serveurs existent pour d'autres OS que l'OS natif (certaines fonctionnalités particulières peuvent manquer)
 - Serveur SMB pour Unix/Linux : Samba
 - Client SMB pour Linux : intégré dans le noyau Linux ou gestionnaires de fichiers (Dolphin, Nautilus, ...)
 - Client SMB pour MacOS : intégré dans MacOS
- Ces protocoles ne sont en général pas autorisés à traverser les pare-feu (*firewalls*) car trop de risques de sécurité (protocoles complexes, failles de sécurité fréquentes)

Utilisation des protocoles de partage à l'IUT2

- Serveur NFS sous Linux : `erebus4`
 - Montage sur toutes les stations Linux
- Serveur SMB sous Windows : `taillefer`
 - Montage sur tous les PC sous Windows
 - Utilisation possible sous Linux
- Serveur SMB sous Linux : sur `erebus4`
 - Utilisation possible sous Windows

Protocoles de transfert de fichiers

- Indépendants du système d'exploitation
- Utiles pour des transferts
 - entre machines tournant sous des OS différents
 - entre réseaux séparés par des pare-feu
- FTP (*File Transfer Protocol*)
 - FTP anonyme / FTP authentifié (login + mot de passe)
 - protocole ancien, de moins en moins utilisé en mode authentifié
 - non sécurisé : mot de passe et fichiers transmis en clair sur le réseau
→ Pas de serveur FTP installé sur les machines de l'IUT2
- SCP/SFTP (*Secure CP, Secure FTP*)
 - repose sur le protocole SSH
 - même serveur que SSH
 - sécurisé : mot de passe et fichiers chiffrés

Utilisation à l'IUT2

- Serveur SSH/SCP/SFTP
 - sur transit
 - sur toutes les stations Linux
- Indispensable pour les transferts de fichiers chez vous ↔ IUT2

Logiciel scp

- Permet de copier des fichiers d'une machine à une autre
- Permet de copier des fichiers d'un compte à un autre
- Usage : `scp [-r] SOURCE DESTINATION`
- Source ou destination peut être sur une machine distante
- Exemples : copie d'un répertoire depuis chez vous
 - IUT2 → Chez vous
→ `scp -rp toto@transit...fr:REP_SRC REP_DEST`
 - Chez vous → IUT2
→ `scp -rp REP_SRC toto@transit...fr:REP_DEST`

Plan du cours

- 1 Message pour le TP6
- 2 Introduction
- 3 Environnement réseau de l'IUT2
- 4 Adresses et ports dans les réseaux IP
- 5 Travail à distance
- 6 Utilisation de machines à distance
- 7 Partage et transfert de fichiers
- 8 Résumé

Résumé

- Internet = sites + liaisons + routeurs
- Adresse IPv4 = a.b.c.d (32 bits)
- Serveur = (adresse ou nom) + numéro de port
- De l'**intérieur** de l'IUT2, **tout est accessible**
- De l'**extérieur**, je passe toujours par le bastion
transit.iut2.univ-grenoble-alpes.fr
- De chez moi, je ne peux utiliser que **SSH/SCP/SFTP**
- Attention, la **disponibilité** de transit n'est **pas garantie**