SAÉ 21 : Construire un réseau informatique pour une petite structure

Guillaume Urvoy-Keller, Michaël Lance

8 avril 2024

Agenda

Objectifs selon PPN

- comprendre et construire une architecture de réseaux d'entreprise et d'Internet ;
- élaborer une méthode efficace pour tester progressivement la configuration réalisée ;
- construire un réseau local virtuel VLAN ;
- intercepter un trafic entre 2 ordinateurs et identifier le chemin utilisé ;
- construire une passerelle entre un réseau émulé et un réseau réel.

Déroulement

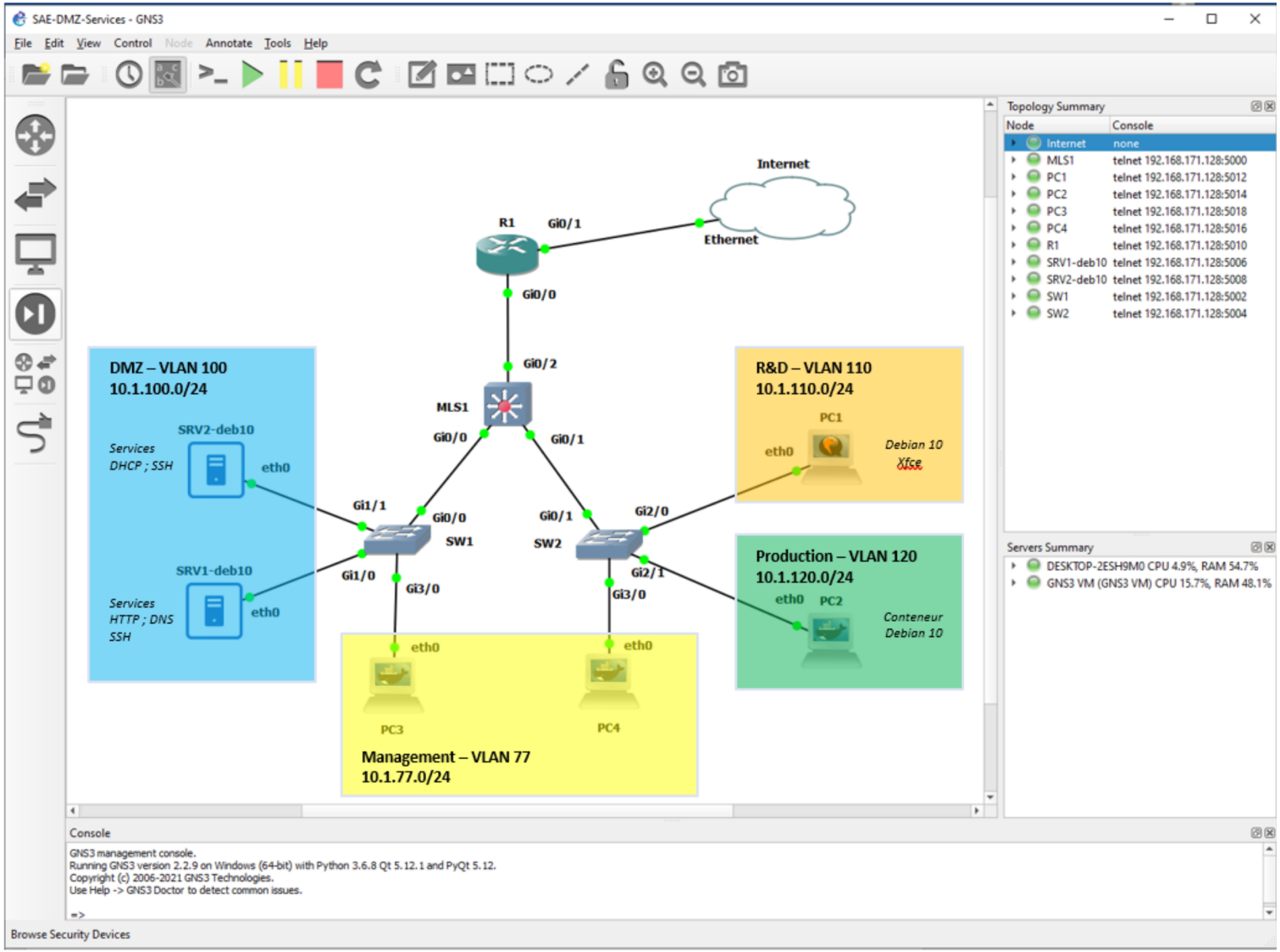
- Projet tuteuré
  - Débute .... dès cette semaine
  - Instructions précises envoyées par Michael Lance dans la semaine, *hopefully* demain
  - Deux visios avec Michael Lance pour discuter de *vos* problèmes $\Rightarrow$ il faut bosser avant !
    - La première la semaine prochaine (semaine 16)
      Il faudra avoir fait phase 1 et début phase 2 : routage inter-vlan, STP, DHCP, DNS interne
    - La seconde en semaine 20
  - Projet par groupe de 2
  - Rendu (a priori semaine 23) : compte-rendu écrit + vidéo de 3 min
    - Téléchargez les vidéos et rapport sur Moodle :
      `https://lms.univ-cotedazur.fr/2023/course/view.php?id=7013`

Vidéos et Rendu

- Utilisez le logiciel de capture d'écran (et votre voix) que vous souhaitez
- Lire `https://theshiftproject.org/guide-reduire-poids-video-5-minutes/`
- Diminuez la taille sans impact sur la qualité visuelle avec `https://handbrake.fr/`

Agenda

Projet


SAE-DMZ-Services - GNS3
File Edit View Control Node Annotate Tools Help
Internet
Ethernet
R1
Gi0/1
Gi0/0
Gi0/2
MLS1
Gi0/0
Gi0/1
DMZ – VLAN 100
10.1.100.0/24
SRV2-deb10
Services
DHCP ; SSH
eth0
SRV1-deb10
Services
HTTP ; DNS
SSH
eth0
Gi1/1
Gi0/0
SW1
Gi1/0
Gi3/0
Gi0/1
Gi2/0
SW2
Gi2/1
Gi3/0
R&D – VLAN 110
10.1.110.0/24
PC1
eth0
Debian 10
Xfce
Production – VLAN 120
10.1.120.0/24
eth0 PC2
Conteneur
Debian 10
eth0
PC3
eth0
PC4
Management – VLAN 77
10.1.77.0/24
Topology Summary
Node Console
Internet none
MLS1 telnet 192.168.171.128:5000
PC1 telnet 192.168.171.128:5012
PC2 telnet 192.168.171.128:5014
PC3 telnet 192.168.171.128:5018
PC4 telnet 192.168.171.128:5016
R1 telnet 192.168.171.128:5010
SRV1-deb10 telnet 192.168.171.128:5006
SRV2-deb10 telnet 192.168.171.128:5008
SW1 telnet 192.168.171.128:5002
SW2 telnet 192.168.171.128:5004
Servers Summary
DESKTOP-2ESH9M0 CPU 4.9%, RAM 54.7%
GNS3 VM (GNS3 VM) CPU 15.7%, RAM 48.1%
Console
GNS3 management console.
Running GNS3 version 2.2.9 on Windows (64-bit) with Python 3.6.8 Qt 5.12.1 and PyQt 5.12.
Copyright (c) 2006-2021 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.
=>
Browse Security Devices

Projet

- Environnement de travail : packet tracer (simulation) et non émulation GNS3
- Plus facile pour travailler chez vous
- Partie système, notamment DNS, moins riche (mais vue dans d'autres modules)
- Full cisco...avantage (vous connaissez) et inconvénient (vous ne connaissez que ça)

Projet

Ce que vous devrez faire :

- Plan d'adressage réseau interne
- VLAN et Multi-Layer Switch
- Serveurs DNS, DHCP et ajout PC "portable"
- Routage interne
- Connexion externe et redistribution de route
- NAT
- Sécurisation et DMZ

Projet

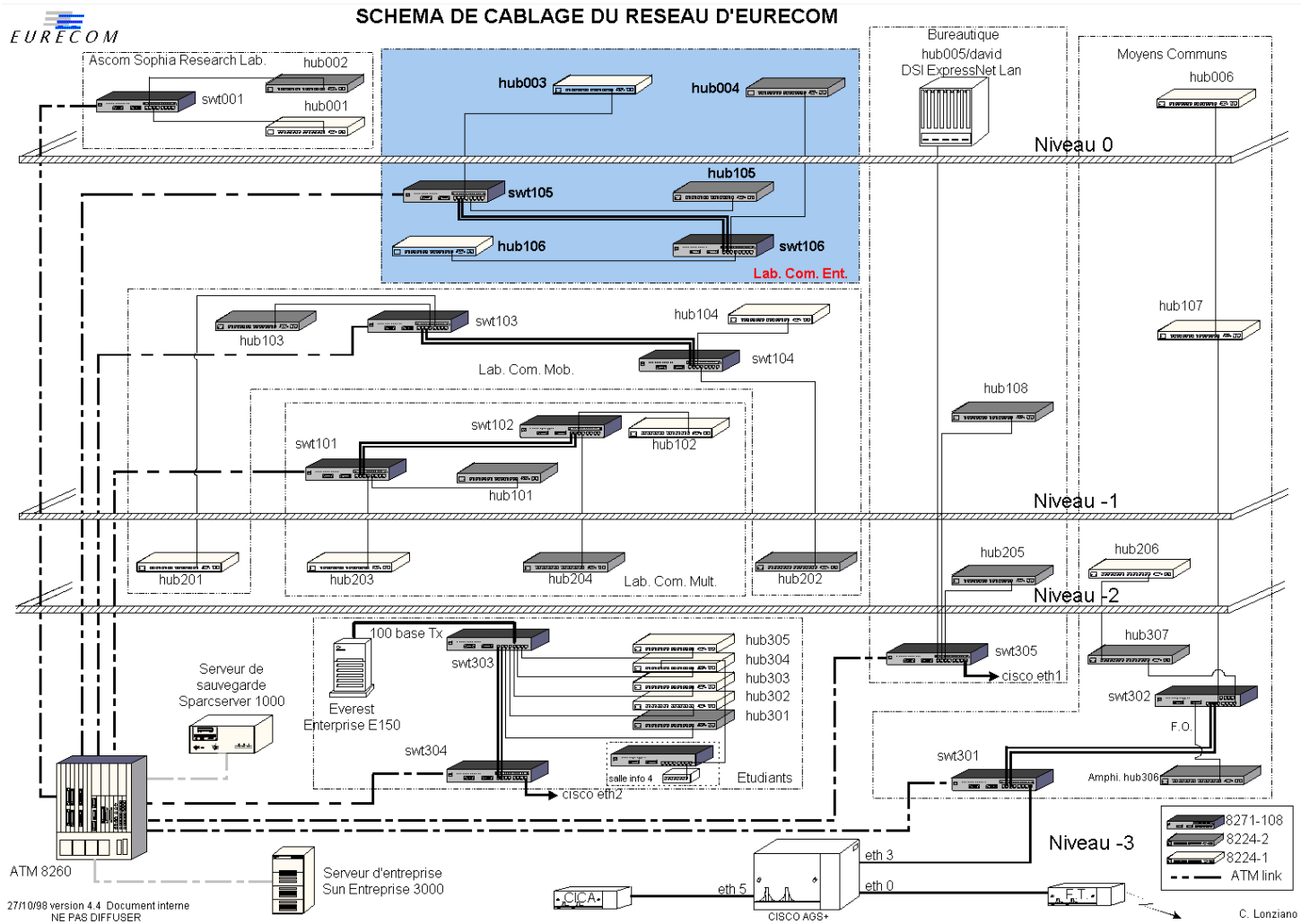
- DMZ = vos serveurs exposés à l'extérieur (Web, DNS, Mail)
- Principe sécurisation = si "quelqu'un" parle au serveur Web, il lui parle sur le port 80 ou 443 et aucun autre (Mail, port 25 seulement, etc).→ pare-feu externe
- Si un paquet IP est destiné à une machine client en interne, alors il faut que la machine client lui ait parlé avant : → pare-feu interne
- DMZ entre pare-feu externe et interne
- Implémentation : pare-feu complet ou liste de contrôle d'accès (ACL, Access Control List)

Agenda

Topographie (physique)

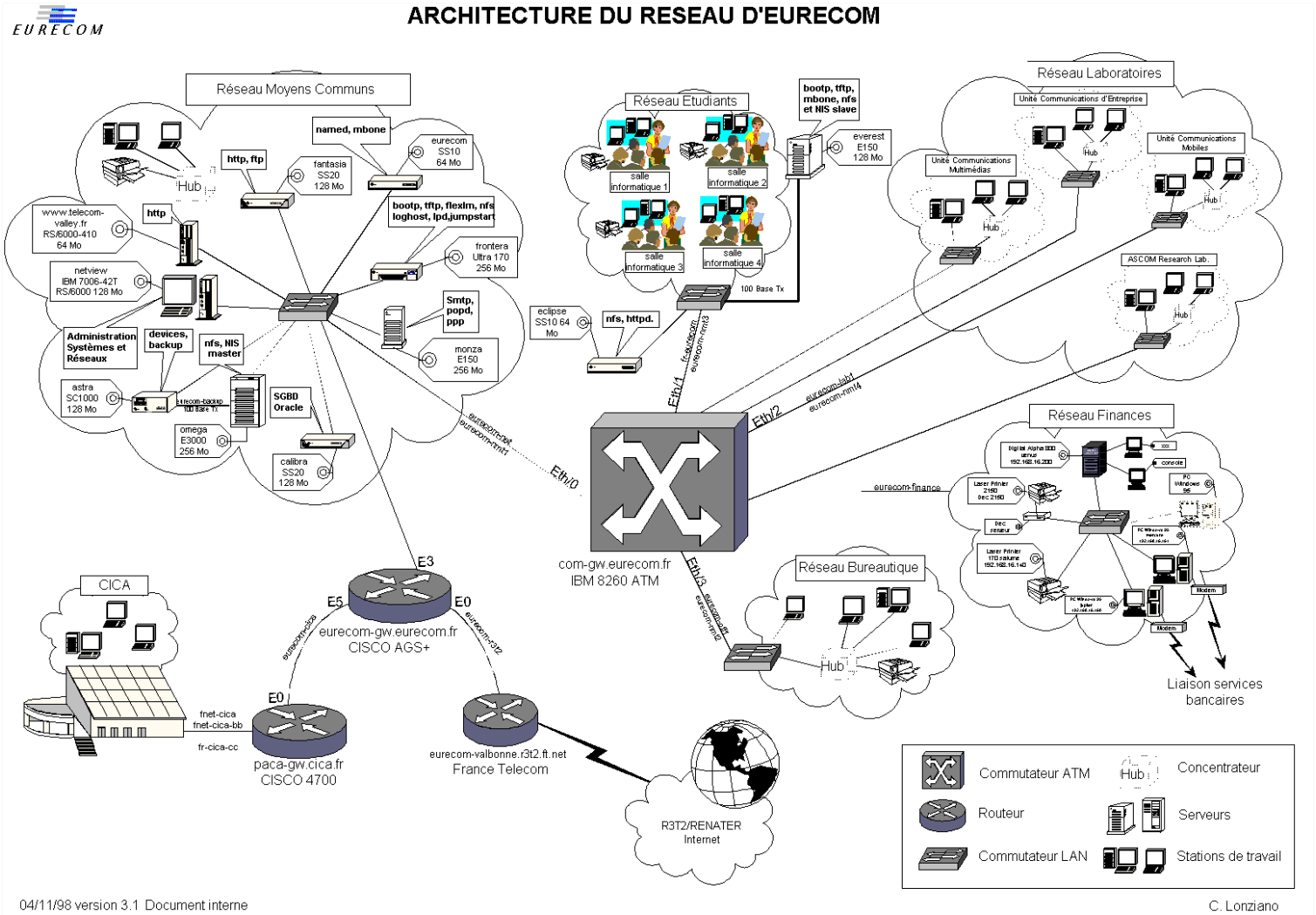
- Localisation physique des éléments du réseau
  - Salle serveurs avec racks
  - Salles techniques où arrivent les câbles (brassage)
- Des contraintes à prendre en compte :
  - Label clair sur les fils pour s'y retrouver ! (nom interface devra apparaitre dans vos schémas, et IP si applicable)
  - L'alimentation électrique des serveurs
  - L'alimentation électrique des climatiseurs
  - Notion de PUE : Power Usage Effectiveness.
    - Ratio entre électricité consommée par serveurs et réseau et électricité totale
    - Idéal PUE =1. En pratique entre 1 et 2.
    - Exemple : Data Center de Scaleway `https://pue.dc2.scaleway.com/fr/`

Topographie



Topologie

Vue logique du réseau avec groupes de travail = groupe utilisateur ou équipements



Adressage

- Utiliser les @ privées pour le réseau interne

Préfixe	Plage IP	Nombre d'adresses
10.0.0.0/8	10.0.0.0 – 10.255.255.255	2^{32-8} = 16 777 216
172.16.0.0/12	172.16.0.0 – 172.31.255.255	2^{32-12} = 1 048 576
192.168.0.0/16	192.168.0.0 – 192.168.255.255	2^{32-16} = 65 536

- Un groupe de travail $\rightarrow$ un (V)LAN
- Utilisation sous-réseaux, par exemple 10.0.0.0/8 en 10.0.1.0/24 $\rightarrow$ 10.0.255.0/24
- Toujours prévoir une bonne marge de sécurité si on ajoute des machines dans un VLAN

Volumétrie

- Pas à traiter dans le projet mais important
- Toujours difficile d'estimer le trafic car très variable
- Comme pour les FAIs, dimensionnement pour le trafic maximum, "prime time"
  - Pour un FAI, le prime time c'est 18h00-22h00
  - Pour un réseau d'entreprise, plusieurs périodes, par ex : 8h00 et 14h00 pour le serveur de mails, 2h00 à 4h00 du matin pour le serveur de backup
- Relation entre traffic et VLAN
  - Avec les LANs, c'était facile, le trafic restait beaucoup dans le LAN car les serveurs étaient par groupe de travail : règle des 80/20
  - Avec les VLANs et centralisation des serveurs : règles de 20/80 (80% inter VLAN)

Domaine de diffusion et de collision

Domaine de diffusion

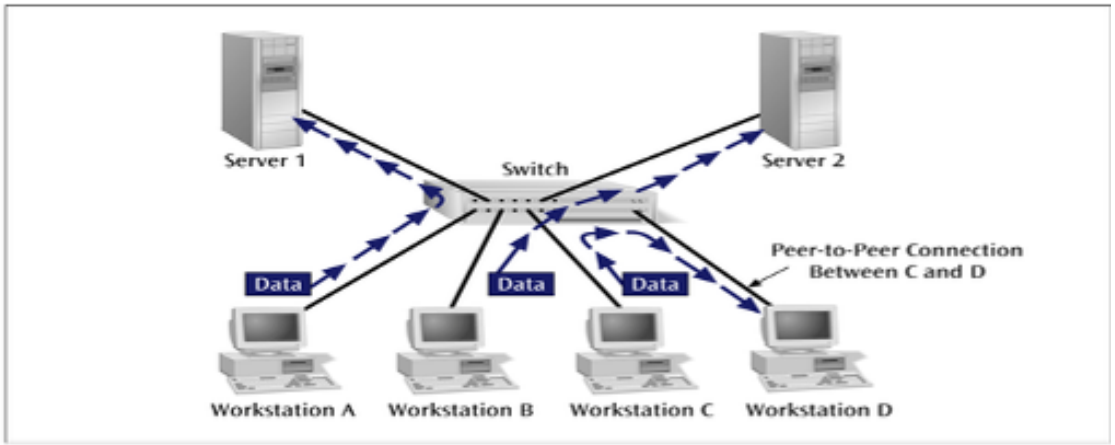
Les machines qui reçoivent un broadcast = un LAN ou un VLAN (=LAN distribué) = 1 sous réseau IP

Domaine de collision

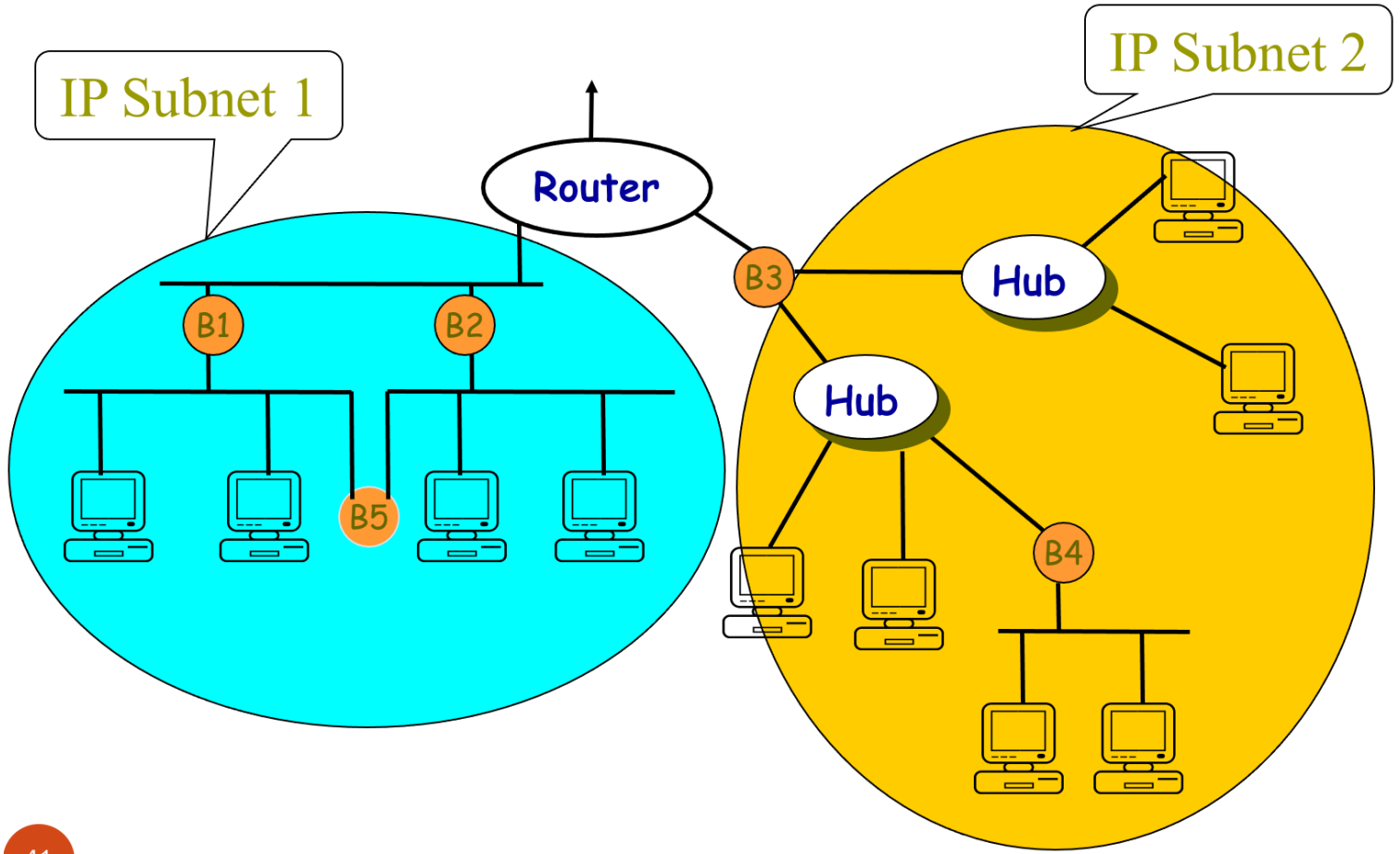
Les machines dont les trames, si elles sont envoyées en même temps se collisionnet → partage bande passante

Hubs vs Switchs vs Routeurs

Hub : 1 seul domaine de diffusion et de collision
Switch : 1 seul domaine de diffusion mais un domaine de collision par port
$\rightarrow$ plus de bande passante !
Routeurs séparent les domaines de diffusion

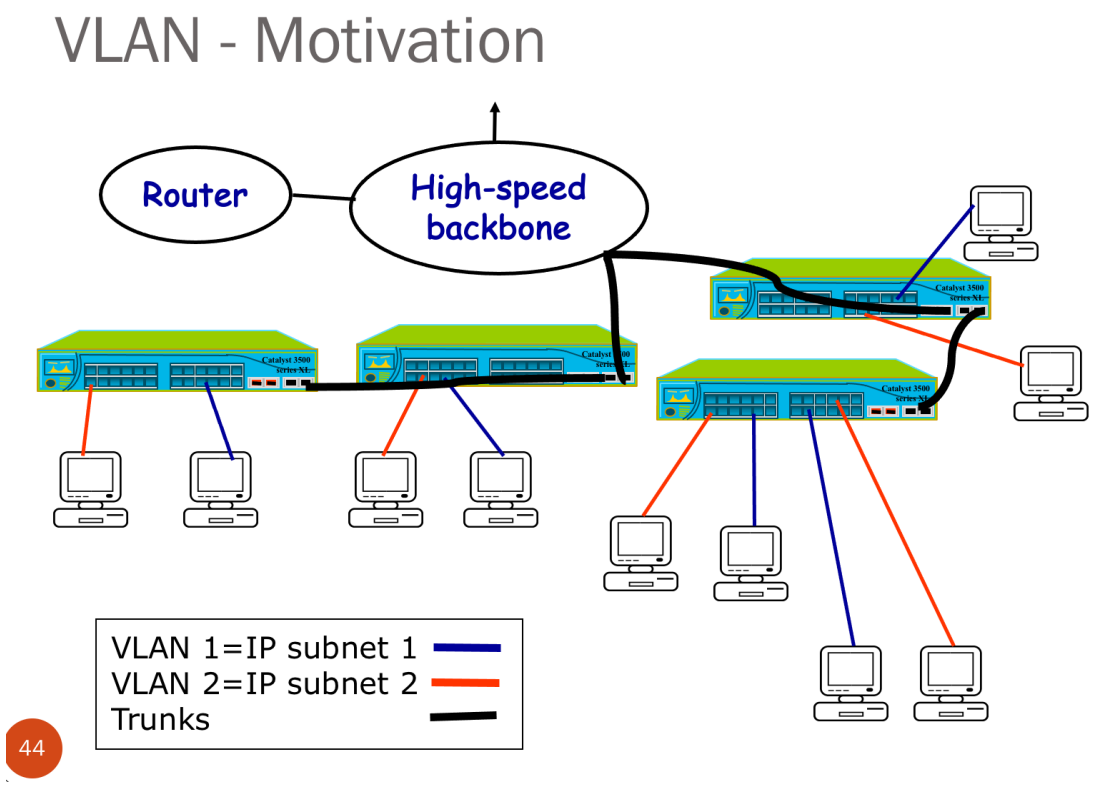


Routeur sépare les domaines de diffusion



VLANs et Multi-Layer Switch (MLS)

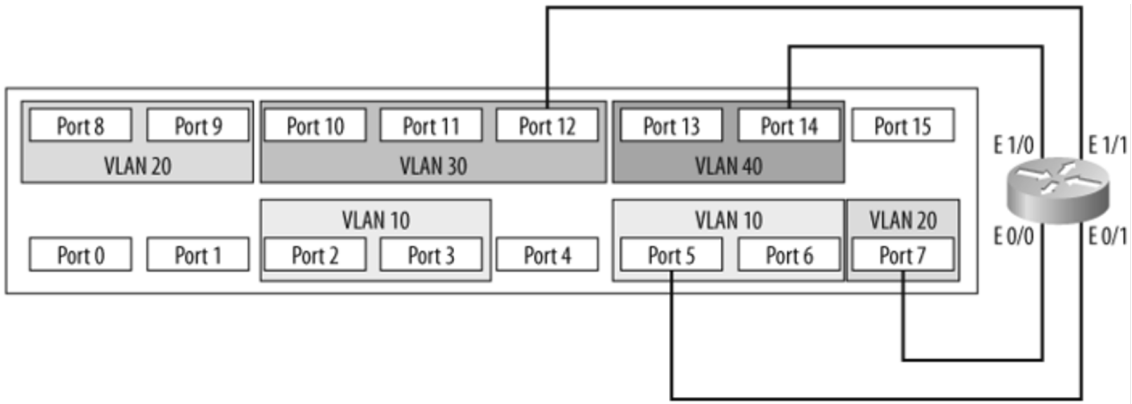
Motivation : les personnes d'un même groupe de travail peuvent être distribués géographiquement



VLANs et Multi-Layer Switch (MLS)

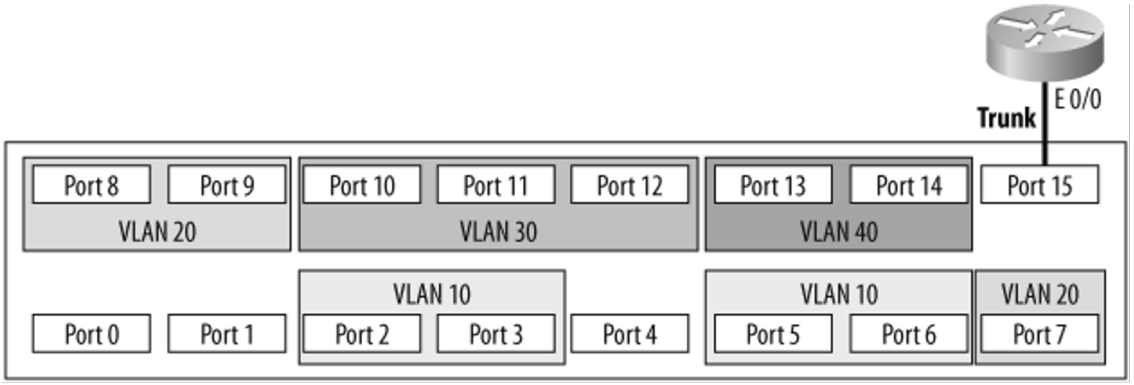
Problème : un routeur ne s'y retrouve plus car les domaines de collision ne sont plus séparés → invention du Multi-Layer Switch = Switch de niveau 3 = mélange routeur et switch

Option 1 : un routeur avec une interface dans chaque VLAN. Pas pratique



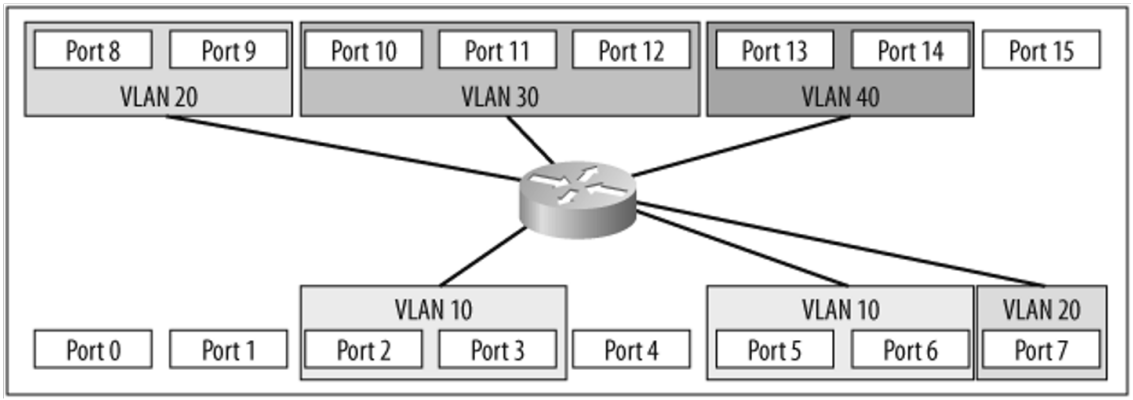
VLANs et Multi-Layer Switch (MLS)

Option 2 : "routeur on a stick". Utilisation de liens dits "trunks" sur lesquels on envoie le trafic de tout (ou partie) des VLANs



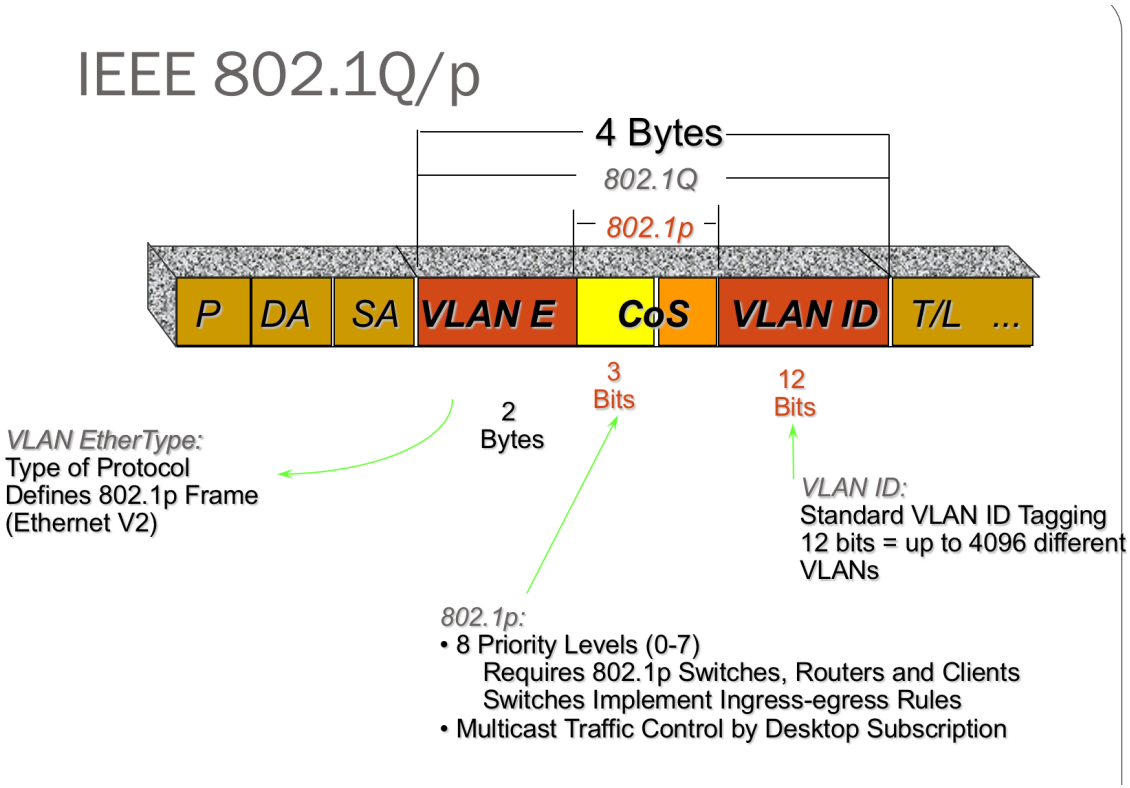
VLANs et Multi-Layer Switch (MLS)

Option 3 : MLS qui agit comme switch si le trafic reste dans le VLAN et comme routeur sinon



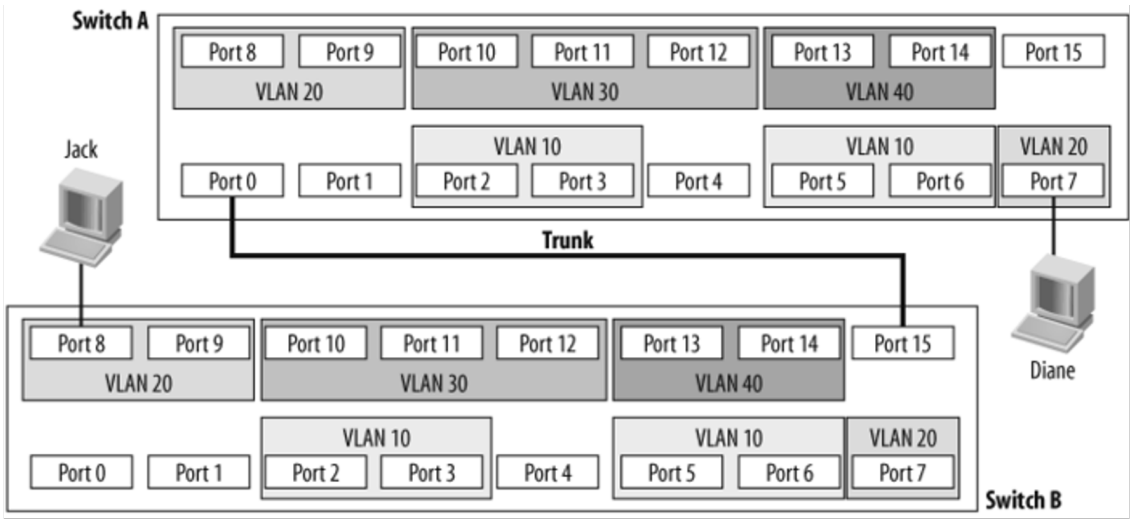
VLANs et trame Ethernet

Le numéro du VLAN doit transiter dans la trame Ethernet étendue avec option 802.1Q



VLANs et trunk

En langage CISCO, un lien d'un switch est en mode "accès" s'il transporte de des trames ethernet standard
.. et mode "trunk" si plusieurs trames 802.1Q qui contient numéro du VLAN.



Design

Evolution Historique

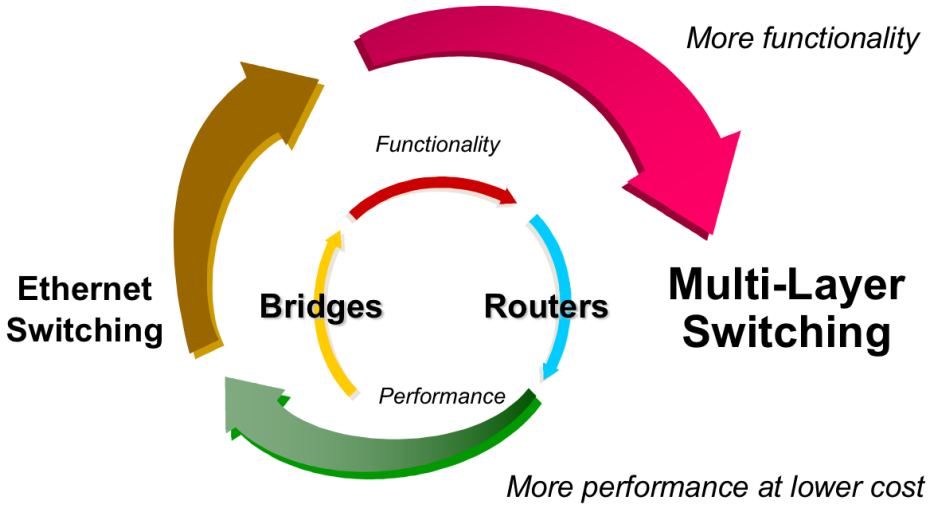
- Hubs . . . switches
- LAN Segmentation(1994-1995)
- High speed lan switching (1995-1996)
- Switching to the desktop (1996-1997)
- Scalable backbones – Multilayer switches (1997-1998)
- Giga to the desktop . . . . . .

Evolution vitesse

- 10 Mb/s partagé
- 10 Mb/s dédié
- 100 Mb/s Dedicated
- 1 Gb/s ethernet (2003)
- 10 à 100 Gb/s de nos jours mais surtout pour serveurs, pas clients

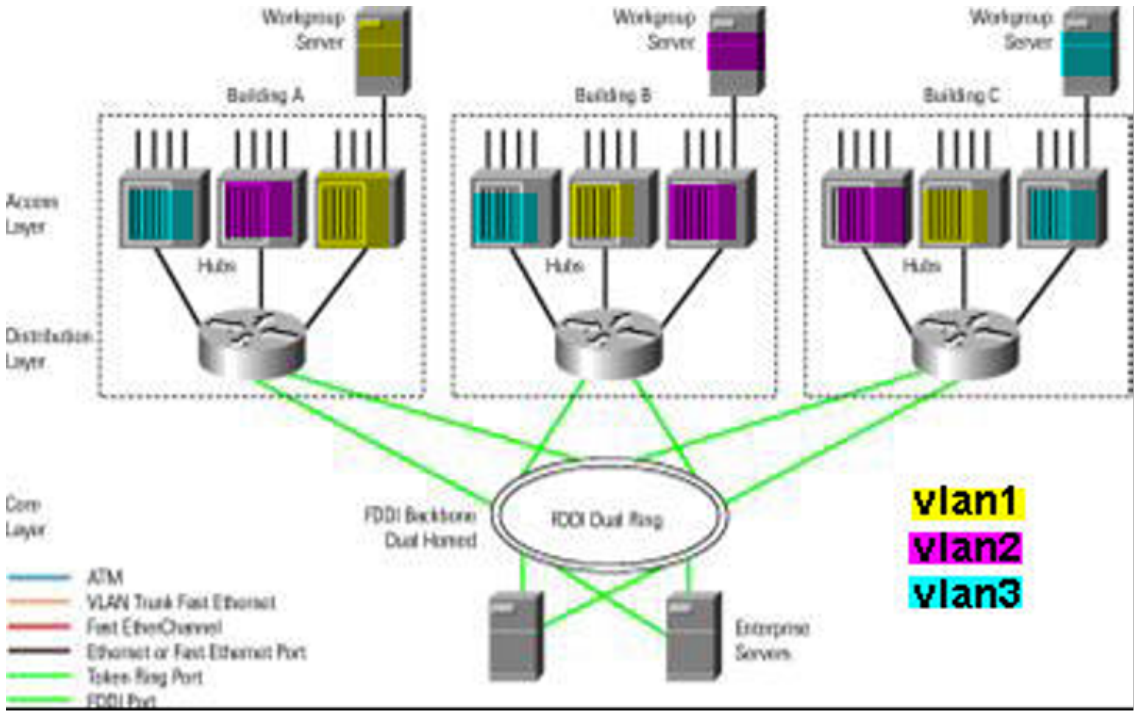
Design

- Hier : "switch when you can, route when you must"
- Aujourd'hui : "switch+route grâce aux MLS"



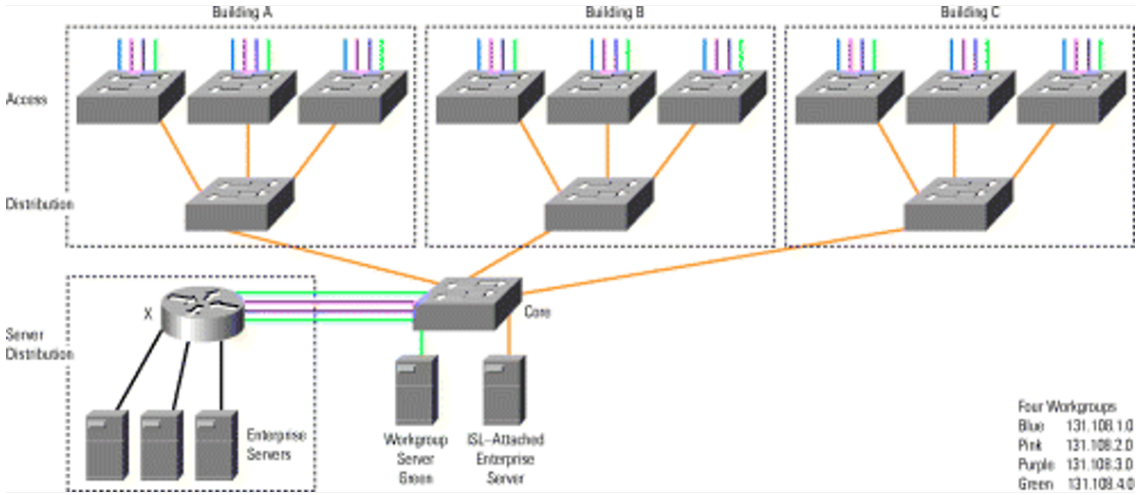
Structure historique Hub/Switch

- Un bloc = un groupe de travail
- Routage lent → on ne centralise pas les serveurs et règles 80/20 (20 passe par routeur)
- Contrainte physique sur localisation



VLANs

- Une couleur = un groupe → pas de contrainte physique
- Serveurs toujours par groupe car inter-VLAN lent



VLANs et MLS : design contemporain

- serveurs centralisés
- Règle 20/80