Architecture Réseau VLAN

Bidouille — Équipe R&D | Router-on-a-Stick

1. Contexte

L'entreprise Bidouille vient de recruter 5 personnes pour son équipe R&D. Le réseau actuel est un réseau plat (flat network) : tous les équipements partagent le même sous-réseau, sans aucune séparation des flux. Cette situation pose deux problèmes majeurs :

- Les données sensibles R&D (prototypes, brevets) sont accessibles par tous les postes du réseau.
- Le trafic bureautique perturbe les serveurs industriels de la Production.
- L'Administration ne dispose d'aucun contrôle centralisé sur les accès entre services.

La solution retenue est une segmentation par VLANs avec routage inter-VLAN via un routeur unique (technique Router-on-a-Stick) et filtrage des flux par ACLs.

2. Infrastructure

Topologie — Router-on-a-Stick

Un switch L2 relie tous les postes. Un seul routeur, connecté au switch via un lien trunk 802.1Q, crée une sous-interface par VLAN et assure le routage inter-VLAN.

```
      |
 [ Routeur ]  Fa0/0.10 → passerelle VLAN 10
      |       Fa0/0.20 → passerelle VLAN 20
   (trunk)    Fa0/0.30 → passerelle VLAN 30
      |
 [ Switch L2 ]
  /    |    \
V10   V20   V30
Admin  R&D  Production
```

Équipements

Équipement	Rôle	Modèle (Packet Tracer)
Routeur principal	Routage inter-VLAN (sous-interfaces), ACLs	Cisco 1941 / 2901
Switch L2	Commutation, trunk vers routeur	Cisco 2960
Serveur Production	Service HTTPS interne (port 443)	Server-PT

3. VLANs et plan d'adressage

VLAN	Nom	Réseau	Passerelle	Hôtes DHCP	Hôtes
10	Administration	192.168.10.0/24	192.168.10.1	.10.10 – .10.30	5 postes
20	R&D	192.168.20.0/24	192.168.20.1	.20.10 – .20.15	5 postes
30	Production	192.168.30.0/24	192.168.30.1	.30.10 – .30.20	5 postes + 1 SRV

4. Règles de sécurité et ACLs

Matrice des flux

Source → Destination	VLAN 10 Admin	VLAN 20 R&D	VLAN 30 Prod
VLAN 10 — Administration	**OK**	**OK**	**OK (port 443 vers SRV)**
VLAN 20 — R&D	**BLOQUÉ**	**OK**	**BLOQUÉ**
VLAN 30 — Production	**BLOQUÉ**	**BLOQUÉ**	**OK**

5. Vérification et tests

Test	Résultat attendu	Commande
Poste Admin → poste R&D	**Succès**	ping 192.168.20.x
Poste R&D → poste Production	**Échec (ACL_VLAN20)**	ping 192.168.30.x
Poste Production → poste R&D	**Échec (ACL_VLAN30)**	ping 192.168.20.x
Admin → SRV-PROD port 443	**Succès**	telnet .30.100 443
R&D → SRV-PROD port 443	**Échec (ACL_SRV)**	telnet .30.100 443

Vérification des ACLs : show access-lists.