TP SRWE : Réseau multi-sites — 4 agences, 40 VLANs, routage complet

TP complet SRWE (Cisco CCNA) : 4 groupes, chacun avec 1 routeur et 1 switch, 10 VLANs par groupe (40 au total), trunks, routage inter-VLAN Router-on-a-Stick, interconnexions Ethernet en chaîne R1-R2-R3-R4 et routes statiques.

Réseau Systèmes 90 min de lecture Niveau Intermédiaire

Document généré le 13/05/2026 à 11h17 · nouvy.fr/wiki/tp-srwe-reseau-multi-sites-4-agences-40-vlans

Sommaire

83 section(s) · 90 min de lecture

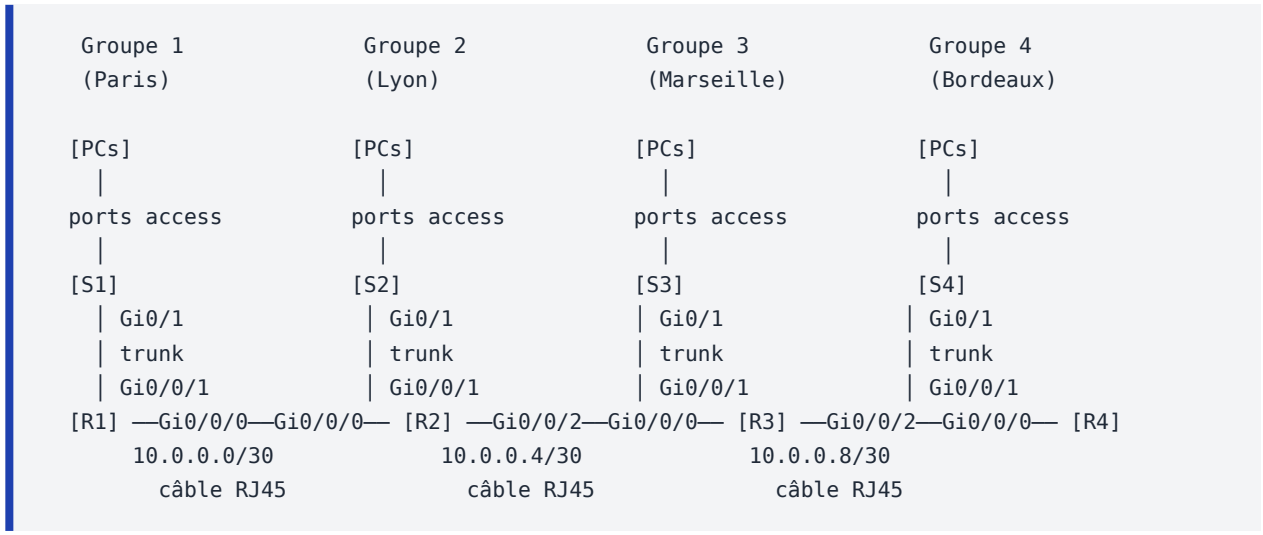
Objectifs du TP

- Configurer 4 routeurs et 4 switches avec les paramètres de base et la sécurité
- Créer et assigner 40 VLANs uniques répartis sur 4 sites
- Configurer les trunks 802.1Q entre chaque switch et son routeur
- Mettre en place le routage inter-VLAN (Router-on-a-Stick) sur chaque site
- Interconnecter les routeurs en chaîne (R1—R2—R3—R4) via des liens Ethernet /30 (câble RJ45 croisé)
- Configurer les routes statiques pour permettre la communication entre tous les sites
- Vérifier et dépanner la connectivité de bout en bout

Contexte

L'entreprise **NovaTech** possède 4 agences en France. Chaque groupe d'élèves configure **1 routeur + 1 switch + 10 VLANs**. À la fin, les 4 routeurs sont connectés en chaîne pour former le réseau complet.

Topologie



Copier

> *Chaque switch est relié **uniquement** à son routeur via un trunk. Les routeurs sont reliés entre eux en chaîne via des câbles RJ45 (croisés ou droit si Auto-MDIX est activé).*

Plan d'adressage complet

Groupe 1 — Paris (Siège) : R1 + S1

VLAN	Nom	Réseau	Passerelle	Ports S1
10	Direction-Generale	172.16.10.0/24	172.16.10.1	Fa0/1-2
11	Finance	172.16.11.0/24	172.16.11.1	Fa0/3-4
12	Juridique	172.16.12.0/24	172.16.12.1	Fa0/5-6
13	Communication	172.16.13.0/24	172.16.13.1	Fa0/7-8
14	Recherche-Dev	172.16.14.0/24	172.16.14.1	Fa0/9-10
15	Logistique	172.16.15.0/24	172.16.15.1	Fa0/11-12
16	Support-IT	172.16.16.0/24	172.16.16.1	Fa0/13-14
17	Serveurs-Siege	172.16.17.0/24	172.16.17.1	Fa0/15-16
18	VoIP-Paris	172.16.18.0/24	172.16.18.1	Fa0/17-18
19	Gestion-Paris	172.16.19.0/24	172.16.19.1	SVI

Groupe 2 — Lyon (Pôle Technique) : R2 + S2

VLAN	Nom	Réseau	Passerelle	Ports S2
20	Dev-Backend	172.16.20.0/24	172.16.20.1	Fa0/1-2
21	Dev-Frontend	172.16.21.0/24	172.16.21.1	Fa0/3-4
22	DevOps	172.16.22.0/24	172.16.22.1	Fa0/5-6
23	QA-Tests	172.16.23.0/24	172.16.23.1	Fa0/7-8
24	Data-Science	172.16.24.0/24	172.16.24.1	Fa0/9-10
25	Cybersecurite	172.16.25.0/24	172.16.25.1	Fa0/11-12
26	Serveurs-Tech	172.16.26.0/24	172.16.26.1	Fa0/13-14
27	Wifi-Invite-Lyon	172.16.27.0/24	172.16.27.1	Fa0/15-16
28	VoIP-Lyon	172.16.28.0/24	172.16.28.1	Fa0/17-18
29	Gestion-Lyon	172.16.29.0/24	172.16.29.1	SVI

Groupe 3 — Marseille (Pôle Commercial) : R3 + S3

VLAN	Nom	Réseau	Passerelle	Ports S3
30	Commercial-France	172.16.30.0/24	172.16.30.1	Fa0/1-2
31	Commercial-Export	172.16.31.0/24	172.16.31.1	Fa0/3-4
32	Admin-Des-Ventes	172.16.32.0/24	172.16.32.1	Fa0/5-6
33	SAV	172.16.33.0/24	172.16.33.1	Fa0/7-8
34	Marketing-Digital	172.16.34.0/24	172.16.34.1	Fa0/9-10
35	Marketing-Event	172.16.35.0/24	172.16.35.1	Fa0/11-12
36	CRM-Serveurs	172.16.36.0/24	172.16.36.1	Fa0/13-14
37	Wifi-Invite-Marseille	172.16.37.0/24	172.16.37.1	Fa0/15-16
38	VoIP-Marseille	172.16.38.0/24	172.16.38.1	Fa0/17-18
39	Gestion-Marseille	172.16.39.0/24	172.16.39.1	SVI

Groupe 4 — Bordeaux (Pôle Formation) : R4 + S4

VLAN	Nom	Réseau	Passerelle	Ports S4
40	Formation-Salle1	172.16.40.0/24	172.16.40.1	Fa0/1-2
41	Formation-Salle2	172.16.41.0/24	172.16.41.1	Fa0/3-4
42	Formation-Salle3	172.16.42.0/24	172.16.42.1	Fa0/5-6
43	Formateurs	172.16.43.0/24	172.16.43.1	Fa0/7-8
44	Mediatheque	172.16.44.0/24	172.16.44.1	Fa0/9-10
45	Labo-Reseau	172.16.45.0/24	172.16.45.1	Fa0/11-12
46	Serveurs-Formation	172.16.46.0/24	172.16.46.1	Fa0/13-14
47	Wifi-Invite-Bordeaux	172.16.47.0/24	172.16.47.1	Fa0/15-16
48	VoIP-Bordeaux	172.16.48.0/24	172.16.48.1	Fa0/17-18
49	Gestion-Bordeaux	172.16.49.0/24	172.16.49.1	SVI

Liens inter-routeurs (chaîne R1—R2—R3—R4, câbles RJ45)

Lien	Réseau	Interface A	IP A	Interface B	IP B
R1 ↔ R2	10.0.0.0/30	R1 Gi0/0/0	10.0.0.1	R2 Gi0/0/0	10.0.0.2
R2 ↔ R3	10.0.0.4/30	R2 Gi0/0/2	10.0.0.5	R3 Gi0/0/0	10.0.0.6
R3 ↔ R4	10.0.0.8/30	R3 Gi0/0/2	10.0.0.9	R4 Gi0/0/0	10.0.0.10

Adresses IP des switches (SVI de gestion)

Switch	VLAN gestion	Adresse IP	Passerelle
S1-Paris	VLAN 19	172.16.19.2/24	172.16.19.1
S2-Lyon	VLAN 29	172.16.29.2/24	172.16.29.1
S3-Marseille	VLAN 39	172.16.39.2/24	172.16.39.1
S4-Bordeaux	VLAN 49	172.16.49.2/24	172.16.49.1

Adresses IP des PCs de test

PC	VLAN	Adresse IP	Masque	Passerelle
PC-Direction	10	172.16.10.10	255.255.255.0	172.16.10.1
PC-Finance	11	172.16.11.10	255.255.255.0	172.16.11.1
PC-DevBackend	20	172.16.20.10	255.255.255.0	172.16.20.1
PC-DevOps	22	172.16.22.10	255.255.255.0	172.16.22.1
PC-CommercialFR	30	172.16.30.10	255.255.255.0	172.16.30.1
PC-SAV	33	172.16.33.10	255.255.255.0	172.16.33.1
PC-FormSalle1	40	172.16.40.10	255.255.255.0	172.16.40.1
PC-LaboReseau	45	172.16.45.10	255.255.255.0	172.16.45.1

Hostnames et mots de passe

Groupe	Routeur	Switch
1 - Paris	R1-Paris	S1-Paris
2 - Lyon	R2-Lyon	S2-Lyon
3 - Marseille	R3-Marseille	S3-Marseille
4 - Bordeaux	R4-Bordeaux	S4-Bordeaux

Paramètre	Valeur
Enable secret	`Class123`
Mot de passe console	`Cisco123`
Utilisateur SSH	`admin` / `Admin123` (privilege 15)
Nom de domaine	`novatech.local`
Clé RSA	1024 bits
SSH	Version 2
Bannière	Accès autorisé uniquement

Phase 1 : Configuration de base

Consignes pour le routeur

1. Définir le hostname selon le tableau ci-dessus
2. Configurer une bannière de connexion
3. Sécuriser l'accès enable avec un mot de passe chiffré
4. Chiffrer tous les mots de passe en clair dans la configuration
5. Créer un utilisateur local avec le niveau de privilège maximum
6. Sécuriser la ligne console : mot de passe, login, synchronisation des logs, timeout de 5 minutes
7. Sécuriser les lignes VTY : authentification locale, autoriser uniquement SSH, timeout de 5 minutes
8. Configurer le nom de domaine, générer les clés RSA et activer SSH version 2
9. Sauvegarder la configuration

Consignes pour le switch

1. Mêmes étapes que le routeur (hostname, bannière, sécurité, SSH)
2. Sauvegarder la configuration

Phase 2 : Création des VLANs et assignation des ports

Consignes pour chaque switch

1. Créer les **10 VLANs** de votre groupe en leur donnant les noms indiqués dans le plan d'adressage
2. Créer un **VLAN 999** nommé `TrouNoir` pour les ports inutilisés
3. Configurer les ports indiqués en **mode access** et les assigner au VLAN correspondant (voir tableau)

4. Placer tous les **ports inutilisés** (Fa0/19 à Fa0/24) dans le VLAN 999 et les **désactiver**
5. Créer la **SVI de gestion** sur le VLAN de gestion de votre groupe (VLAN 19, 29, 39 ou 49) avec l'adresse IP indiquée dans le tableau
6. Configurer la **passerelle par défaut** du switch
7. Sauvegarder la configuration

Vérification attendue

- `show vlan brief` doit afficher vos 10 VLANs + le VLAN 999
- Chaque port doit apparaître dans le bon VLAN
- Les ports inutilisés doivent être dans le VLAN 999

Phase 3 : Configuration du Trunk

Consignes pour chaque switch

1. Configurer le port **GigabitEthernet 0/1** en mode **trunk**
2. Définir le **VLAN natif** sur le VLAN de gestion de votre groupe
3. **Limiter** les VLANs autorisés sur le trunk à vos 10 VLANs uniquement
4. **Désactiver la négociation DTP** sur le port trunk
5. S'assurer que le port est activé
6. Sauvegarder la configuration

Vérification attendue

- `show interfaces trunk` doit afficher Gi0/1 en trunking avec le bon VLAN natif
- Seuls vos 10 VLANs doivent être autorisés sur le trunk

Phase 4 : Routage Inter-VLAN (Router-on-a-Stick)

Consignes pour chaque routeur

1. Activer l'interface physique **GigabitEthernet 0/0/1** (connectée au switch)
2. Créer **10 sous-interfaces** (une par VLAN) sur cette interface physique :
    - Chaque sous-interface doit porter le numéro du VLAN (ex: Gi0/0/1.10 pour le VLAN 10)
    - Configurer l'**encapsulation 802.1Q** avec le numéro de VLAN correspondant
    - Attribuer l'adresse IP de **passerelle** indiquée dans le plan d'adressage
    - Ajouter une **description** avec le nom du VLAN
3. Pour la sous-interface du VLAN de gestion (19, 29, 39 ou 49), configurer l'encapsulation en mode **native**
4. Sauvegarder la configuration

Vérification attendue

- `show ip interface brief` doit afficher les 10 sous-interfaces en état **up/up**
- Depuis un PC, un **ping vers la passerelle** de son VLAN doit fonctionner
- Un **ping entre deux PCs de VLANs différents** du même site doit fonctionner (routage inter-VLAN)

Phase 5 : Liens inter-routeurs (câbles RJ45)

Consignes pour chaque routeur

Configurer les interfaces GigabitEthernet selon le tableau des liens inter-routeurs :

R1 (2 interfaces : Gi0/0/1 vers le switch, Gi0/0/0 vers R2) :

1. Configurer Gi0/0/0 avec l'adresse IP 10.0.0.1/30, ajouter une description vers R2, activer l'interface

R2 (3 interfaces : Gi0/0/1 vers le switch, Gi0/0/0 vers R1, Gi0/0/2 vers R3) :

1. Configurer Gi0/0/0 avec l'adresse IP 10.0.0.2/30, ajouter une description vers R1, activer l'interface
2. Configurer Gi0/0/2 avec l'adresse IP 10.0.0.5/30, ajouter une description vers R3, activer l'interface

R3 (3 interfaces : Gi0/0/1 vers le switch, Gi0/0/0 vers R2, Gi0/0/2 vers R4) :

1. Configurer Gi0/0/0 avec l'adresse IP 10.0.0.6/30, ajouter une description vers R2, activer l'interface
2. Configurer Gi0/0/2 avec l'adresse IP 10.0.0.9/30, ajouter une description vers R4, activer l'interface

R4 (2 interfaces : Gi0/0/1 vers le switch, Gi0/0/0 vers R3) :

1. Configurer Gi0/0/0 avec l'adresse IP 10.0.0.10/30, ajouter une description vers R3, activer l'interface

Récapitulatif des interfaces par routeur

Routeur	Gi0/0/0	Gi0/0/1	Gi0/0/2
R1	→ R2 (10.0.0.1)	→ S1 (trunk)	—
R2	→ R1 (10.0.0.2)	→ S2 (trunk)	→ R3 (10.0.0.5)
R3	→ R2 (10.0.0.6)	→ S3 (trunk)	→ R4 (10.0.0.9)
R4	→ R3 (10.0.0.10)	→ S4 (trunk)	—

Vérification attendue

- `show ip interface brief` : toutes les interfaces GigabitEthernet doivent être **up/up**

- Un **ping vers le routeur voisin** doit fonctionner :
    - R1 → 10.0.0.2
    - R2 → 10.0.0.1 et 10.0.0.6
    - R3 → 10.0.0.5 et 10.0.0.10
    - R4 → 10.0.0.9

Phase 6 : Routes statiques

Principe

La topologie est en **chaîne** :

```
R1 ——— R2 ——— R3 ——— R4
```

Copier

- **R1** n'a qu'un seul voisin (R2) → tout le trafic vers les autres sites passe par R2
- **R2** est au milieu → il envoie vers R1 (gauche) ou R3 (droite) selon la destination
- **R3** est au milieu → il envoie vers R2 (gauche) ou R4 (droite) selon la destination
- **R4** n'a qu'un seul voisin (R3) → tout le trafic vers les autres sites passe par R3

Consignes pour R1-Paris

1. Ajouter **30 routes statiques** (10 par site distant) vers les réseaux des 3 autres groupes
2. Toutes ces routes doivent pointer vers **10.0.0.2** (R2, seul voisin)
3. Ajouter les routes vers les liens WAN distants (10.0.0.4/30 et 10.0.0.8/30) via 10.0.0.2
4. Sauvegarder

Consignes pour R2-Lyon

1. Ajouter **10 routes** vers Paris (172.16.10-19.0/24) via **10.0.0.1** (R1)
2. Ajouter **10 routes** vers Marseille (172.16.30-39.0/24) via **10.0.0.6** (R3)
3. Ajouter **10 routes** vers Bordeaux (172.16.40-49.0/24) via **10.0.0.6** (R3, car le trafic doit transiter par R3)
4. Ajouter la route vers le lien WAN distant (10.0.0.8/30) via 10.0.0.6
5. Sauvegarder

Consignes pour R3-Marseille

1. Ajouter **10 routes** vers Paris (172.16.10-19.0/24) via **10.0.0.5** (R2, car le trafic doit transiter par R2)
2. Ajouter **10 routes** vers Lyon (172.16.20-29.0/24) via **10.0.0.5** (R2)
3. Ajouter **10 routes** vers Bordeaux (172.16.40-49.0/24) via **10.0.0.10** (R4)
4. Ajouter la route vers le lien WAN distant (10.0.0.0/30) via 10.0.0.5
5. Sauvegarder

Consignes pour R4-Bordeaux

1. Ajouter **30 routes statiques** vers les réseaux des 3 autres groupes
2. Toutes ces routes doivent pointer vers **10.0.0.9** (R3, seul voisin)
3. Ajouter les routes vers les liens WAN distants (10.0.0.0/30 et 10.0.0.4/30) via 10.0.0.9
4. Sauvegarder

Vérification attendue

- `show ip route static` doit afficher toutes les routes ajoutées
- `show ip route` doit afficher les routes C (connected), L (local) et S (static)

Phase 7 : Configuration des PCs

1. Dans Packet Tracer, configurer au moins **2 PCs par groupe** avec les adresses du tableau (Desktop → IP Configuration)
2. Chaque PC doit avoir :
    - Une **adresse IP** dans le bon réseau VLAN
    - Le bon **masque** (255.255.255.0)
    - La bonne **passerelle par défaut** (adresse .1 de son réseau)
3. Brancher chaque PC sur un port du switch correspondant à son VLAN

Phase 8 : Vérifications complètes

8.1 Checklist par groupe

#	Vérification	Commande à utiliser	Résultat attendu
1	VLANs créés sur le switch	`show vlan brief`	10 VLANs + VLAN 999
2	Ports dans les bons VLANs	`show vlan brief`	Correspondance avec le tableau
3	Trunk actif	`show interfaces trunk`	Gi0/1 en trunking, bon VLAN natif
4	Sous-interfaces routeur	`show ip interface brief`	10 sous-interfaces up/up
5	Liens inter-routeurs	`show ip interface brief`	GigabitEthernet up/up
6	Routes statiques	`show ip route static`	Routes vers les 3 autres sites
7	SVI switch	`show ip interface brief`	VLAN gestion up avec IP

8.2 Tests intra-site (routage inter-VLAN)

Depuis un PC, effectuer un **ping** vers un PC d'un **autre VLAN du même site**.

Exemple pour le Groupe 1 : PC-Direction (VLAN 10) → PC-Finance (VLAN 11)

Le ping doit réussir. Si ce n'est pas le cas, vérifiez le trunk et les sous-interfaces.

8.3 Tests inter-sites

Effectuer les tests suivants et noter les résultats :

Test	Source	Destination	Nombre de sauts attendu
Paris → Lyon	172.16.10.10	172.16.20.10	1 saut (R1→R2)
Paris → Marseille	172.16.10.10	172.16.30.10	2 sauts (R1→R2→R3)
Paris → Bordeaux	172.16.10.10	172.16.45.10	3 sauts (R1→R2→R3→R4)
Lyon → Bordeaux	172.16.20.10	172.16.40.10	2 sauts (R2→R3→R4)
Marseille → Paris	172.16.30.10	172.16.11.10	2 sauts (R3→R2→R1)
Bordeaux → Lyon	172.16.45.10	172.16.22.10	2 sauts (R4→R3→R2)

Utiliser **tracert** (depuis le PC) ou **traceroute** (depuis le routeur) pour vérifier le nombre de sauts et le chemin emprunté.

8.4 Matrice de tests complète

Chaque groupe doit pouvoir pinger **au moins un PC de chaque autre site**. Remplir la matrice :

De \ Vers	Paris	Lyon	Marseille	Bordeaux
Paris	□	?	?	?
Lyon	?	□	?	?
Marseille	?	?	□	?
Bordeaux	?	?	?	□

Phase 9 : Dépannage

Si un test échoue, suivre cette démarche méthodique :

Étape 1 — Vérifier le PC

- L'adresse IP, le masque et la passerelle par défaut sont-ils corrects ?
- Le PC est-il branché sur un port du bon VLAN ?

Étape 2 — Vérifier le switch

- Le port du PC est-il bien en mode access dans le bon VLAN ? (`show vlan brief`)

- Le trunk vers le routeur est-il formé ? (`show interfaces trunk`)
- Le VLAN natif est-il identique des deux côtés ?
- Les VLANs autorisés sur le trunk sont-ils corrects ?

Étape 3 — Vérifier le routeur (inter-VLAN)

- L'interface physique Gi0/0/1 est-elle activée ?
- Les sous-interfaces sont-elles up/up ? (`show ip interface brief`)
- L'encapsulation dot1Q est-elle configurée avec le bon numéro de VLAN ?
- L'adresse IP de chaque sous-interface correspond-elle au plan d'adressage ?

Étape 4 — Vérifier les liens inter-routeurs

- Les interfaces GigabitEthernet vers les routeurs voisins sont-elles up/up ?
- Un ping vers le routeur voisin fonctionne-t-il ?
- Le câble RJ45 est-il bien branché des deux côtés ?

Étape 5 — Vérifier les routes statiques

- La route vers le réseau de destination existe-t-elle ? (`show ip route`)
- Le next-hop est-il correct (pas sa propre adresse) ?
- Les routes de **retour** existent-elles sur chaque routeur du chemin ?
- Les routeurs intermédiaires (R2, R3) ont-ils les routes vers **tous** les sites ?

Aide

- `ping` : tester la connectivité
- `traceroute` / `tracert` : visualiser le chemin hop par hop
- `show ip route` : voir la table de routage
- `show running-config` : vérifier la configuration complète

Phase 10 : STP (Spanning Tree Protocol)

Principe

Même avec un seul switch par site, il est essentiel de configurer STP pour :

- La **convergence rapide** (Rapid PVST+) — les ports passent en forwarding immédiatement
- La **sécurité** (PortFast + BPDU Guard) — empêcher qu'un switch non autorisé soit branché sur un port access

Consignes pour chaque switch

1. Activer Rapid PVST+

Configurer le mode **rapid-pvst** sur le switch.

2. Configurer le switch comme Root Bridge

Le switch étant le seul de son site, le configurer comme **Root Bridge primary** pour tous ses VLANs :

- S1 : Root Bridge primary pour les VLANs 10-19
- S2 : Root Bridge primary pour les VLANs 20-29
- S3 : Root Bridge primary pour les VLANs 30-39
- S4 : Root Bridge primary pour les VLANs 40-49

> *Cela garantit que si un jour un second switch est ajouté au site, le switch principal restera Root Bridge.*

3. PortFast sur les ports access

Activer **PortFast** sur tous les ports connectés à des PCs (ports access). Cela permet aux PCs de se connecter immédiatement sans attendre la convergence STP (30-50 secondes).

4. BPDU Guard sur les ports access

Activer **BPDU Guard** sur tous les ports access. Si un switch non autorisé est branché sur un port access, le port se désactive automatiquement.

Vérification attendue

- `show spanning-tree vlan X` doit afficher **"This bridge is the root"** pour chaque VLAN du groupe
- `show spanning-tree interface Fa0/1 detail` doit montrer PortFast activé
- Brancher un petit switch sur un port access → le port doit passer en **err-disabled** (BPDU Guard)
- Débrancher le switch intrus puis réactiver le port manuellement

---

Phase 11 : DHCPv4

Principe

Chaque routeur devient **serveur DHCP** pour les VLANs de son site. Les PCs n'ont plus besoin d'adresses IP statiques — ils les obtiennent automatiquement.

Consignes pour chaque routeur

1. Exclure les adresses réservées

Pour chaque réseau VLAN, exclure les adresses **.1 à .10** du pool DHCP (réservées pour la passerelle, les switches et les serveurs).

2. Créer un pool DHCP par VLAN

Pour chacun des 10 VLANs de votre groupe, créer un pool DHCP avec :

- Le **réseau** et le masque correspondant
- La **passerelle par défaut** (adresse .1)
- Le **serveur DNS** : 8.8.8.8 et 8.8.4.4
- Le **nom de domaine** : novatech.local
- La **durée du bail** : 7 jours

Exemple de nommage des pools :

Groupe	Pools à créer
Paris	POOL-VLAN10, POOL-VLAN11, ..., POOL-VLAN19
Lyon	POOL-VLAN20, POOL-VLAN21, ..., POOL-VLAN29
Marseille	POOL-VLAN30, POOL-VLAN31, ..., POOL-VLAN39
Bordeaux	POOL-VLAN40, POOL-VLAN41, ..., POOL-VLAN49

3. Configurer les PCs en DHCP

Dans Packet Tracer, sur chaque PC : Desktop → IP Configuration → sélectionner **DHCP** au lieu de Static.

Le PC doit obtenir automatiquement :

- Une adresse IP dans la plage .11 à .254
- Le masque 255.255.255.0
- La passerelle par défaut (.1)
- Le serveur DNS (8.8.8.8)

Vérification attendue

- Sur le routeur : `show ip dhcp pool` doit afficher les 10 pools avec le nombre d'adresses attribuées
- Sur le routeur : `show ip dhcp binding` doit afficher les baux actifs (adresse IP ↔ adresse MAC)
- Sur les PCs : l'adresse IP doit être dans la bonne plage et la passerelle correcte
- Les **pings inter-VLAN et inter-sites** doivent toujours fonctionner avec les adresses obtenues en DHCP
- Tester : libérer et renouveler un bail sur un PC (ipconfig /release puis ipconfig /renew)

Phase 12 : Port Security

Principe

Le **Port Security** limite le nombre d'adresses MAC autorisées sur chaque port access du switch. Si un appareil non autorisé est branché, le port réagit selon le mode de violation configuré.

Rappel des modes de violation

Mode	Trafic illégitime	Compteur violation	Notification	État du port
protect	Bloqué	Non incrémenté	Non	Up
restrict	Bloqué	Incrémenté	Oui (syslog)	Up
shutdown	Bloqué	Incrémenté	Oui (syslog)	err-disabled

Consignes pour chaque switch

1. Activer Port Security sur tous les ports access

Sur chaque port access (ceux assignés à un VLAN) :

- Activer le **port-security**
- Limiter le nombre d'adresses MAC à **2** (1 PC + 1 téléphone IP par exemple)
- Choisir le mode de violation **shutdown** (le port se désactive en cas de violation)
- Activer l'apprentissage **sticky** (le switch mémorise automatiquement les MAC apprises)

2. Configurer la récupération automatique

Configurer le switch pour **réactiver automatiquement** les ports en err-disabled après **300 secondes** (5 minutes). Cela évite qu'un port reste bloqué indéfiniment après une fausse manipulation.

Test de validation

1. Vérifier que le PC connecté fonctionne normalement
2. Brancher un **3ème appareil** sur un port access (via un mini-switch ou hub) → le port doit passer en **err-disabled**
3. Attendre 5 minutes → le port doit se réactiver automatiquement
4. Alternativement, réactiver le port manuellement (shutdown puis no shutdown)

Vérification attendue

- `show port-security` doit afficher un résumé de tous les ports protégés
- `show port-security interface Fa0/1` doit afficher : SecurityEnabled, MaxSecureAddr = 2, SecurityViolation = shutdown, Sticky
- `show port-security address` doit afficher les adresses MAC apprises en sticky
- `show interfaces status err-disabled` doit être vide si aucun port n'est en violation

Phase 13 : DHCP Snooping

Principe

DHCP Snooping protège contre les attaques **DHCP Spoofing** (faux serveur DHCP) et

DHCP Starvation (épuisement du pool). Le switch distingue les ports **trusted** (vers le routeur/serveur DHCP légitime) et les ports **untrusted** (vers les PCs).

Rappel des menaces

Attaque	Description	Risque
DHCP Spoofing	Un attaquant branche un faux serveur DHCP qui distribue de mauvaises passerelles/DNS	Man-in-the-Middle, phishing
DHCP Starvation	Un attaquant envoie des milliers de requêtes DHCP pour épuiser le pool	Déni de service

Consignes pour chaque switch

1. Activer DHCP Snooping globalement

Activer DHCP Snooping sur le switch et le déclarer actif pour les **10 VLANs** de votre groupe.

> ⚠ *Désactiver l'option 82 (information option) car le routeur en tant que serveur DHCP local ne la gère pas dans Packet Tracer.*

2. Configurer le port trunk comme trusted

Le port **Gi0/1** (trunk vers le routeur) doit être marqué comme **trusted**. C'est par ce port que le serveur DHCP légitime (le routeur) répond.

3. Limiter le débit DHCP sur les ports access

Sur tous les ports access (untrusted par défaut), limiter le nombre de requêtes DHCP à **6 par seconde**. Cela empêche un attaquant d'inonder le serveur DHCP.

4. Tester le DHCP après activation

Les PCs doivent toujours obtenir une adresse IP en DHCP normalement après l'activation de DHCP Snooping. Si ce n'est pas le cas, vérifier que le port trunk est bien en trusted.

Vérification attendue

- `show ip dhcp snooping` doit afficher DHCP Snooping activé, les VLANs protégés et l'option 82 désactivée
- `show ip dhcp snooping binding` doit afficher la table des baux (MAC ↔ IP ↔ VLAN ↔ port) construite automatiquement
- Les PCs doivent continuer à recevoir des adresses DHCP normalement □
- Un PC faisant tourner un faux serveur DHCP sur un port untrusted sera bloqué □

Phase 14 : Dynamic ARP Inspection (DAI)

Principe

DAI protège contre les attaques **ARP Spoofing / ARP Poisoning**. Le switch vérifie chaque paquet ARP reçu sur les ports untrusted en le comparant avec la table **DHCP Snooping binding**. Si l'association IP ↔ MAC ne correspond pas, le paquet est rejeté.

> ⚠ ***Prérequis*** *: DHCP Snooping doit être activé (Phase 13). DAI utilise la table de binding DHCP pour valider les paquets ARP.*

Rappel de la menace

Attaque	Description	Risque
ARP Spoofing	L'attaquant envoie de faux ARP Reply pour associer sa MAC à l'IP de la passerelle	Man-in-the-Middle : tout le trafic passe par l'attaquant

Consignes pour chaque switch

1. Activer DAI sur les VLANs du groupe

Activer Dynamic ARP Inspection pour les **10 VLANs** de votre groupe.

2. Configurer le port trunk comme trusted

Le port **Gi0/1** (trunk vers le routeur) doit être marqué comme **trusted** pour l'ARP Inspection. Les paquets ARP venant du routeur ne sont pas vérifiés.

3. Activer la validation supplémentaire

Configurer DAI pour valider les champs suivants dans les paquets ARP :

- **src-mac** : la MAC source de la trame Ethernet correspond à la MAC dans le paquet ARP
- **dst-mac** : la MAC destination correspond à la MAC cible dans le paquet ARP
- **ip** : les adresses IP dans le paquet ARP sont valides (pas 0.0.0.0 ni 255.255.255.255 en source)

4. Limiter le débit ARP sur les ports access

Limiter le nombre de paquets ARP à **15 par seconde** sur les ports access pour éviter un flood ARP.

Vérification attendue

- `show ip arp inspection vlan X` doit afficher DAI activé pour chaque VLAN du groupe
- `show ip arp inspection interfaces` doit afficher Gi0/1 en **Trusted** et les Fa0/x en **Untrusted**
- `show ip arp inspection statistics` doit montrer des paquets Forwarded (trafic légitime) et éventuellement Dropped (trafic suspect)
- Les pings entre PCs et vers la passerelle doivent fonctionner normalement

Phase 15 : Protections complémentaires

15.1 Durcissement des trunks (protection VLAN Hopping)

Rappel de la menace

L'attaque **Double Tagging** exploite le VLAN natif : l'attaquant envoie une trame avec 2 tags 802.1Q. Le switch retire le premier tag (natif) et transmet la trame vers le VLAN cible.

Consignes

Vérifier que les mesures suivantes sont bien en place sur chaque switch (certaines ont déjà été configurées dans les phases précédentes) :

1. Le **VLAN natif** est bien le VLAN de gestion (19/29/39/49) et non le VLAN 1 (déjà fait en Phase 3)
2. La négociation **DTP est désactivée** sur le port trunk (switchport nonegotiate) — déjà fait en Phase 3
3. Les **ports inutilisés** sont dans le VLAN 999 (Black-Hole) et désactivés — déjà fait en Phase 4
4. Tous les ports inutilisés sont **explicitement en mode access** (pas en mode dynamic)

Consigne supplémentaire

Forcer le **tagging du VLAN natif** sur le trunk. Par défaut, les trames du VLAN natif ne sont pas taguées sur le trunk. En activant le tagging, une trame Double Tagging sera rejetée.

15.2 Désactivation de CDP/LLDP

Rappel de la menace

CDP (Cisco Discovery Protocol) et **LLDP** diffusent des informations sur les périphériques réseau (modèle, version IOS, adresses IP, VLANs). Un attaquant peut exploiter ces informations pour cartographier le réseau.

Consignes

1. **Désactiver CDP globalement** sur le switch et sur le routeur
2. **Désactiver LLDP globalement** sur le switch et sur le routeur
3. Si CDP est nécessaire entre le switch et le routeur pour le dépannage, le désactiver **uniquement sur les ports access** (côté PCs) et le laisser actif sur le trunk

15.3 IP Source Guard (optionnel / avancé)

Principe

IP Source Guard filtre le trafic sur les ports access en vérifiant que l'adresse IP source correspond bien à la table DHCP Snooping binding. Cela empêche un utilisateur de changer manuellement son adresse IP.

Consigne

Activer IP Source Guard sur les ports access de votre switch.

Vérification attendue

- `show cdp` doit afficher CDP désactivé (ou `show cdp interface` ne doit rien afficher sur les ports access)
- `show lldp` doit afficher LLDP désactivé
- `show ip verify source` doit afficher les ports avec IP Source Guard activé et les adresses IP autorisées

---

Phase 16 : Récapitulatif des protections de sécurité

Tableau synthétique

Menace	Protection	Phase	Port concerné
MAC Flooding	**Port Security** (max 2 MAC, shutdown, sticky)	Phase 12	Ports access
DHCP Spoofing/Starvation	**DHCP Snooping** (trust trunk, rate limit)	Phase 13	Tous
ARP Spoofing	**DAI** (validation ARP vs table DHCP)	Phase 14	Tous
STP Attack	**BPDU Guard** (err-disable si BPDU reçu)	Phase 10	Ports access
VLAN Hopping	**Trunk hardening** (natif dédié, nonegotiate, tag native)	Phase 15	Trunk
Reconnaissance réseau	**CDP/LLDP désactivés**	Phase 15	Tous
Usurpation IP	**IP Source Guard**	Phase 15	Ports access

Test global de sécurité

1. Vérifier que tous les PCs obtiennent leur IP en DHCP et peuvent se pinger entre eux et entre sites
2. Brancher un 3ème appareil sur un port access → **Port Security** doit bloquer le port
3. Brancher un switch non autorisé sur un port access → **BPDU Guard** doit désactiver le port
4. Vérifier que `show cdp neighbors` ne montre aucun voisin sur les ports access
5. Vérifier que `show ip dhcp snooping binding` et `show ip arp inspection statistics` affichent des données cohérentes

---

Récapitulatif général

Architecture finale

```
Groupe 1           Groupe 2           Groupe 3           Groupe 4
PARIS              LYON               MARSEILLE          BORDEAUX
VLANs 10-19        VLANs 20-29        VLANs 30-39        VLANs 40-49

[PCs]              [PCs]              [PCs]              [PCs]
  | Port Security     | Port Security     | Port Security     | Port Security
  | PortFast          | PortFast          | PortFast          | PortFast
  | BPDU Guard        | BPDU Guard        | BPDU Guard        | BPDU Guard
[S1]              [S2]              [S3]              [S4]
  | trunk             | trunk             | trunk             | trunk
  | DHCP Snooping     | DHCP Snooping     | DHCP Snooping     | DHCP Snooping
  | DAI               | DAI               | DAI               | DAI
[R1]═══RJ45═══[R2]═══RJ45═══[R3]═══RJ45═══[R4]
   10.0.0.0/30  10.0.0.4/30  10.0.0.8/30
        DHCP serveur par routeur (10 pools chacun)

STP Rapid PVST+ — Root Bridge par site
40 VLANs uniques — 0 chevauchement — Connectivité totale
```

Copier

Compétences évaluées

- Configuration de base sécurisée (hostname, SSH, mots de passe)
- Création et gestion de VLANs avec noms métiers
- Configuration de trunks 802.1Q avec VLAN natif dédié
- Routage inter-VLAN avec Router-on-a-Stick (sous-interfaces)
- Interconnexion inter-routeurs avec liens Ethernet /30 (câble RJ45)
- Routage statique multi-sites en topologie chaîne
- **STP** Rapid PVST+ avec PortFast et BPDU Guard (sécurité L2)
- **DHCPv4** avec pools par VLAN (attribution automatique d'adresses)
- **Port Security** : limitation des MAC, mode shutdown, sticky
- **DHCP Snooping** : protection contre les faux serveurs DHCP
- **DAI** : protection contre l'ARP Spoofing
- **Durcissement** : trunk hardening, CDP/LLDP désactivés, IP Source Guard
- Vérification et dépannage méthodique