

# Rénovation & pérennisation du réseau « Grand Ouest »

Client : Tac&Tic Brother “avant qu’ils se séparent”  
(Import/Export — Nantes)

## 1. Présentation du client

**Tac&Tic Brother** est une société nantaise d’import/export. Son activité repose sur des échanges continus avec des partenaires en Europe et à l’international : commandes, suivi logistique, documents douaniers, contrats, catalogues produits, échanges avec transitoires, et communication commerciale.

L’entreprise opère sur le **Grand Ouest** (siège + implantation(s) régionales) et prépare le **déménagement** dans de **nouveaux locaux**. L’enjeu n’est pas seulement “que ça marche”, mais que le réseau soit **reproductible, documenté** et **maintenable** lors du transfert : architecture claire, procédure de bascule, capacité d’extension, et retour arrière possible.

Les usages attendus sont typiques d’une PME/ETI moderne :

- postes utilisateurs par division, imprimantes et services de partage,
- accès Internet sécurisé (web, visio, services cloud),
- besoins d’administration (accès restreint, traçabilité),
- hébergement de services internes (ex : intranet, VM applicatives),
- réseau “invités” pour partenaires, prestataires et visiteurs.

L’entreprise est structurée en **4 divisions** :

- **Commercial**
- **Développement**
- **R&D**
- **Marketing International**

Dans ce projet, chaque division est confiée à une **équipe (groupe de 5 étudiants)**.

Chaque équipe agit comme une équipe technique BAC+2 : **cadrage** → **conception** → **mise en œuvre** → **recette** → **documentation** de la zone dont elle a la charge, **en intégration** avec les autres équipes (interconnexions, flux partagés, règles communes).

## 2. Contexte & enjeux

Le réseau actuel est hétérogène, peu documenté, et doit être **rénové** pour :

- supporter le **déménagement** sans interruption majeure (architecture stable + procédures de bascule + sauvegardes),
- **séparer** les usages par division (confidentialité, maîtrise des flux, limitation des erreurs),
- garantir une **interconnexion** fiable entre divisions et services (et une méthode claire de routage),
- fournir une base **pérenne** (documentée, sauvegardée, maintenable) pour évoluer (ajout de VLAN, ajout de VM, ajout de service),
- permettre à l'exploitation (MCO) de diagnostiquer rapidement (logs, plan de tests, méthode de troubleshooting),
- réduire le risque "humain" : configuration lisible, règles explicites, et preuves de fonctionnement.

Les attentes du client sont donc doubles :

- **Technique** : un réseau fonctionnel, segmenté, sécurisé, avec services IP (DHCP/DNS) et interconnexions validées.
- **Exploitation** : un réseau "reprendable" (un autre technicien doit pouvoir le comprendre, le vérifier, et le restaurer).

Votre mission, si vous l'acceptez : **concevoir, déployer, sécuriser, tester et documenter** l'infrastructure réseau cible permettant d'**interconnecter tous les services** de Tac&Tic Brother en vous appuyant sur les compétences **CCNA 1**, et en allant **au-delà** (virtualisation ESXi, pare-feu OPNsense, segmentation, analyse de flux, MCO).

## 3. Parties prenantes & organisation (mode projet)

### 3.1 Parties prenantes (rôle "entreprise")

- **Client / Direction** : demande un réseau stable, sécurisé et documenté.
- **Référent métier** (par division) : exprime les besoins (accès, services, contraintes).
- **Équipe d'exploitation** : a besoin d'un runbook, de sauvegardes et de procédures.
- **Vous (équipes techniques)** : livrez un réseau conforme, prouvé par recette. Chaque équipe désigne un **chef d'équipe** (interlocuteur unique, coordination, arbitrages, suivi des livrables).

### 3.2 Répartition des équipes (divisions)

- **Groupe 1 = Commercial**
- **Groupe 2 = Développement**
- **Groupe 3 = R&D**
- **Groupe 4 = Marketing International**

Chaque groupe est responsable de :

- la conception + mise en œuvre de "sa" zone (LAN, VLANs, services, sécurité),
- la publication d'une **fiche d'interconnexion** (préfixes, next-hop, services exposés),
- l'intégration avec les autres groupes (interconnexion + tests croisés),
- la production des livrables (cadrage, conception, PV de recette, runbook, journal de changements).

### 3.3 Organisation interne obligatoire (dans chaque groupe)

Chaque équipe (5 personnes) doit attribuer **des rôles clairs**. Une même personne peut cumuler 2 rôles si besoin, mais **le chef d'équipe est obligatoire**.

#### *Chef d'équipe / Coordinateur projet (obligatoire)*

- **Responsabilités** : planifier le travail sur la séance, distribuer les tâches, arbitrer, gérer les dépendances avec les autres groupes, valider les livrables avant rendu.
- **Rôle "SPOC"** : point de contact unique avec l'enseignant (client/exploitation) et avec les autres équipes.
- **Production** : mise à jour du **journal de changements**, suivi de l'avancement, consolidation du dossier final.

#### *Responsable Réseau (Routeur, routage, interconnexions)*

- **Responsabilités** : configuration routeur (interfaces, SSH), routes statiques IPv4/IPv6, vérification inter-divisions.
- **Production** : captures show ip int brief, show ip route / show ipv6 route, preuve ping/traceroute inter-groupes.

#### *Responsable Virtualisation / ESXi*

- **Responsabilités** : port groups, trunk 802.1Q (ou alternative), placement correct des VMs, dépannage "VM sur mauvais réseau".
- **Production** : schéma des réseaux ESXi (vSwitch/Port Groups), mapping VM ↔ VLAN/Port Group.

#### *Responsable Sécurité / OPNsense*

- **Responsabilités** : interfaces, VLANs, DHCP, DNS (Unbound), NAT, règles firewall stateful, logs.

- **Production** : captures de config (interfaces/VLAN/DHCP/DNS/NAT/règles) + preuves logs (ALLOW/BLOCK) + export backup.

*Responsable Recette & Qualité (tests, preuves, documentation)*

- **Responsabilités** : construire le **PV de recette**, exécuter le plan de tests, collecter les preuves, contrôler la conformité (exigences fonctionnelles + sécurité).
- **Production** : PV de recette complet + plan de tests + synthèse de conformité.

*Responsable Documentation / Runbook (peut être fusionné avec Qualité)*

- **Responsabilités** : rédiger le **runbook** (procédures, checklists, rollback), assurer la lisibilité du dossier (schémas, tableaux IP, conventions).
- **Production** : runbook exploitable + procédures testées (au minimum sauvegarde/restauration + ajout VM + ajout VLAN).

**Règles de fonctionnement recommandées :**

- Début de séance : 5 minutes de synchronisation (qui fait quoi, dépendances).
- Fin de séance : 10 minutes de recette rapide + sauvegardes + mise à jour doc.
- Toute modification "impactante" = sauvegarde avant/après + trace dans le journal de changements.

## 4. Objectifs pédagogiques (CCNA1 acquis + au-delà)

Le livrable final doit **prouver** l'acquisition de **toutes les compétences CCNA 1 (ITN)**, et démontrer une démarche **professionnelle** (virtualisation, segmentation, pare-feu, exploitation).

### 4.1 Compétences CCNA1

Vous devez fournir des preuves (captures, sorties show, explications courtes) pour :

1. **IOS & configuration de base** : nommage, sécurisation accès, SSH, sauvegarde.
2. **Adressage IPv4 + subnetting** : masques, passerelles, cohérence des plans IP.
3. **Ethernet / L2** : ARP/MAC (preuve + explication local vs distant / rôle gateway).
4. **Diagnostic** : ping / traceroute + méthode L1/L2/L3.
5. **Routage** : routes statiques IPv4 + lecture/explication show ip route.
6. **Services** : DHCP + DNS (résolution de noms prouvée).

7. **IPv6** : 1 VLAN en IPv6 + 1 reach inter-division en ICMPv6 via route statique.
8. **Sécurité de base** : accès admin propre (SSH/HTTPS), justification minimale.
9. **Encapsulation / OSI sur un flux imposé** (voir flux intranet) : en **8 lignes max**, expliquer ce qui relève de L2/L3/L4/L7 et ce qui change à chaque saut.
10. **Transport (TCP vs UDP)** : une capture montrant **DNS en UDP/53** et une capture montrant le début d'une session **HTTPS en TCP/443** (SYN/SYN-ACK/ACK).
11. **Switching** :
  - si switch Cisco disponible : show mac address-table + show interfaces status + justification access/trunk ;
  - sinon : preuve de diffusion/broadcast (ARP) + explication **broadcast domain vs collision domain** (5 lignes) + preuve d'isolement VLAN via tests.
12. **Justification de subnetting** : démontrer que les tailles de VLAN couvrent les besoins (hôtes), et fournir **au moins 1 calcul détaillé** (réseau, broadcast, plage utilisable, nb d'hôtes).

## 4.2 Au-delà CCNA1 — Attendus “technicien réseau prod”

- **Réseau virtuel ESXi** : port groups, trunk 802.1Q vers une VM firewall.
- **Pare-feu stateful (OPNsense)** : segmentation, règles minimales, preuves par logs.
- **Exploitation (MCO)** : runbook, sauvegardes, journal de changements, traitement de tickets.
- **Méthode** : mini-recette après changement, capacité à expliquer un incident et son correctif.

## 5. Besoins métier (exprimés par le client)

Ces besoins servent à justifier vos choix de segmentation, d'accès et de règles.

### 5.1 Commercial

**Profil** : équipes orientées relation client, mobilité, échanges rapides (mails, visio, CRM) et production de documents.

- Accès internet **stable** et **prioritaire** : CRM/SaaS, e-mail, visio (Teams/Meet), messagerie instantanée.
- Accès à un **serveur de fichiers / ressources internes** (catalogues, devis, contrats) avec droits de lecture/écriture.
- Accès au **portail intranet** hébergé par Développement (G2) : consultation procédures, actus, liens outils.

- Accès à un **service d'impression** interne (option) : imprimante réseau / file d'attente partagée.
- Besoin de **télétravail occasionnel** (option bonus) : accès sécurisé à certaines ressources (via VPN, si mis en place).

#### **Contraintes métiers :**

- Tolérance faible aux coupures (impact direct client).
- Pas d'accès direct aux données sensibles R&D.

## 5.2 Développement

**Profil** : héberge et maintient des services internes. A besoin d'accès d'administration et de séparation claire des priviléges.

- Accès à des dépôts/outils (CI/CD, Git) (simulés) + accès internet pour documentation.
- Hébergement d'un **serveur applicatif interne** (ex : VM web intranet dans VLAN30 SRV) exposé sous conditions aux autres divisions.
- Séparation "DEV" et "ADMIN" : seuls les admins ont accès aux interfaces d'admin (OPNsense/routeur/serveurs).
- Besoin d'accès "admin" vers SRV : SSH/HTTPS/RDP selon OS (à cadrer et documenter).
- Besoin de tests : possibilité de joindre certains ports internes (ex : 443 intranet) tout en gardant une politique restrictive.

#### **Contraintes métiers :**

- Traçabilité : les modifications doivent être documentées (journal de changements).
- Les services exposés doivent être minimisés (moindre privilège) et testés.

## 5.3 R&D

**Profil** : données à forte sensibilité (prototypes, specs, tests). Par défaut, R&D fonctionne "en bunker".

- Données sensibles (prototypes, specs, tests). Par défaut, **isolation renforcée**.
- Accès sortant internet **limité** aux besoins : documentation technique, mises à jour (HTTP/HTTPS + DNS).
- Accès entrant depuis les autres divisions : **interdit par défaut**, uniquement si justifié et contrôlé.

- Besoin de partage ponctuel : publication d'un livrable via un mécanisme contrôlé (ex : dépôt en SRV avec accès en lecture uniquement) (option).

#### **Contraintes métiers :**

- Priorité à la confidentialité : pas de "any/any", règles explicites, logs exploitables.
- Toute exception de flux doit être validée et documentée (analyse de flux + règle + test).

### 5.4 Marketing International

**Profil :** forte utilisation web/media + échanges avec partenaires externes + besoins "invités".

- Accès internet (outils campagnes, médias, réseaux sociaux, plateformes publicitaires).
- Réseau **invité** (prestataires / influence / partenaires) isolé (VLAN40 GUEST) avec accès Internet uniquement.
- Besoin de partager des contenus avec Commercial : accès à un **service** (ex : dossier partagé / VM SRV) et pas un accès complet au réseau.
- Besoin d'accès au portail intranet (G2) pour contenus internes (procédures, briefs, planning).

#### **Contraintes métiers :**

- Risque accru (fichiers externes, liens, prestataires) : isolation stricte + logs.
- Les invités ne doivent jamais atteindre les VLAN internes.

## 6. Périmètre

### 6.1 Inclus

- Interconnexion "Grand Ouest" via un **WAN commun** (segment de transit).
- Routeur Cisco : interfaces, routes statiques, administration sécurisée.
- ESXi : réseaux virtuels (port groups / trunk), VMs de test.
- OPNsense : VLANs, DHCP, DNS (Unbound), NAT sortant, règles firewall, logs.
- IPv4 complet + **IPv6 minimal obligatoire**.
- Recette (plan de tests + PV) + dossier d'exploitation + sauvegardes.

### 6.2 Hors périmètre (non requis)

- Routage dynamique (OSPF/EIGRP/BGP).
- Redondance matérielle (HSRP/VRRP), haute dispo firewall.

- Wi-Fi physique (non requis), mais **note de conception** demandée.

## 7. Contraintes techniques de réalisation (plateforme de TP)

Le projet est réalisé en réel avec :

- **Routeur Cisco** (WAN + transit local)
- **ESXi**
- **OPNsense** (VM)

Contraintes de mise en œuvre :

- Vous devez justifier vos choix (trunk vs port groups VLAN séparés, placement des services, etc.).
- Vous devez produire des **preuves** de fonctionnement (tests et commandes).
- Vous devez appliquer une **méthode de changement** : sauvegarde → modification → test → documentation.

## 8. Standards de configuration (exigences “qualité”)

### 8.1 Nommage & traçabilité

- Hostnames explicites : TTB-Gx-RTR, TTB-Gx-FW, TTB-Gx-CLI1, etc.
- Interfaces et réseaux documentés (qui est où, pourquoi).

### 8.2 Accès d'administration

- Administration routeur : **SSH** (user local), pas de Telnet.
- Administration OPNsense : **HTTPS** sur VLAN10 ADMIN.
- Comptes : au minimum 1 compte admin + 1 compte opérateur (si possible) et mots de passe cohérents.

### 8.3 Sauvegardes

- À la fin de chaque séance :
  - sauvegarde configuration routeur (preuve)
  - export config OPNsense (preuve)

## 9. Architecture cible imposée (macro)

### 9.1 WAN commun (interconnexion inter-groupes)

- Réseau WAN : **172.16.0.0/24** (imposé)
- Chaque groupe connecte son interface WAN routeur au switch WAN

- Adresses WAN :
  - G1 Commercial : **172.16.0.11/24**
  - G2 Développement : **172.16.0.12/24**
  - G3 R&D : **172.16.0.13/24**
  - G4 Marketing : **172.16.0.14/24**

## 9.2 Bloc LAN par division (imposé)

Chaque groupe **G** reçoit un bloc : **10.100.G.0/24**

Segmentation VLAN (modèle de base) :

- VLAN10 ADMIN : 10.100.G.0/26 (GW 10.100.G.1)
- VLAN20 USERS : 10.100.G.64/26 (GW 10.100.G.65)
- VLAN30 SRV : 10.100.G.128/27 (GW 10.100.G.129)
- VLAN40 GUEST : 10.100.G.160/27 (GW 10.100.G.161)
- VLAN99 MGMT (option) : 10.100.G.192/28 (GW 10.100.G.193)

## 9.3 ESXi / OPNsense (modèle recommandé)

- ESXi : **Port Group trunk** (VLAN 4095) vers la vNIC “TRUNK” de la VM OPNsense.
- OPNsense :
  - 1 vNIC **WAN** (vers routeur / transit local)
  - 1 vNIC **TRUNK** (porte VLAN10/20/30/40/...)
  - VLANs créés sur l’interface parent, puis interfaces VLAN assignées.

## 9.4 Architecture L3 de référence (Routeur ↔ OPNsense) — obligatoire

Cette section fixe le modèle de routage attendu pour éviter toute ambiguïté.

### 9.4.1 Réseau de transit IPv4 (imposé)

Chaque groupe G utilise un transit dédié en /30 entre le routeur et l’OPNsense :

- Transit : **10.255.G.0/30**
  - Routeur (TRANSIT) : **10.255.G.1/30**
  - OPNsense (WAN) : **10.255.G.2/30**

### 9.4.2 Réseau de transit IPv6 (imposé)

- Transit : **2001:db8:G:ff::/64**
  - Routeur (TRANSIT) : **2001:db8:G:ff::1/64**
  - OPNsense (WAN) : **2001:db8:G:ff::2/64**

#### 9.4.3 Rôles de routage (attendus)

- **OPNsense** est la **passerelle des VLANs** (VLAN10/20/30/40/...) et porte les IP de GW.
- **Le routeur Cisco** est le **routeur d'interconnexion inter-divisions** via le WAN commun (172.16.0.0/24 + IPv6 WAN).

#### 9.4.4 Routes statiques minimales (attendues)

Sur le **routeur Cisco (groupe G)** :

- Route vers le LAN du groupe (tous VLANs) via OPNsense :
  - IPv4 : 10.100.G.0/24 **via** 10.255.G.2
  - IPv6 : 2001:db8:G::/48 **via** 2001:db8:G:ff::2
- Routes vers les autres groupes via leurs next-hop WAN (IPv4 obligatoire, IPv6 recommandé).

Sur **OPNsense (groupe G)** :

- Route par défaut :
  - IPv4 : 0.0.0.0/0 **via** 10.255.G.1
  - IPv6 : ::/0 **via** 2001:db8:G:ff::1
- Aucune route “complexe” n'est attendue : OPNsense envoie tout vers le routeur, qui se charge de l'inter-divisions.

**Implication** : les politiques de sécurité (filtrage) se font principalement sur OPNsense (flux entre VLANs + flux vers autres divisions), tandis que le routeur assure la connectivité globale.

### 10. Exigences fonctionnelles

#### 10.1 Connectivité inter-divisions (inter-groupes)

- Chaque division doit atteindre **au moins 2 autres divisions** en **IPv4** (ping + traceroute).
- Les routes doivent être **statique IPv4** (obligatoire) et documentées.
- Vous devez publier une **fiche d'interconnexion** :
  - préfixes IPv4/IPv6 utilisés
  - IP WAN du routeur
  - services exposés (si applicable)
  - règles d'accès demandées aux autres divisions (si applicable)

#### 10.2 IPv6 (obligatoire)

Objectif : prouver une mise en œuvre IPv6 **réaliste et structurée** (dual-stack minimal viable), cohérente avec l'IPv4.

## Plan d'adressage IPv6 (imposé)

- WAN inter-divisions (partagé) :  $2001:\text{db8}:0:16::/64$ 
  - G1 :  $2001:\text{db8}:0:16::11/64$
  - G2 :  $2001:\text{db8}:0:16::12/64$
  - G3 :  $2001:\text{db8}:0:16::13/64$
  - G4 :  $2001:\text{db8}:0:16::14/64$
- Préfixe "site" par groupe G :  $2001:\text{db8}:G::/48$  (G = 1..4)
- Un /64 par VLAN (imposé) :
  - VLAN10 ADMIN :  $2001:\text{db8}:G:10::/64$
  - VLAN20 USERS :  $2001:\text{db8}:G:20::/64$
  - VLAN30 SRV :  $2001:\text{db8}:G:30::/64$
  - VLAN40 GUEST :  $2001:\text{db8}:G:40::/64$
  - VLAN99 MGMT (option) :  $2001:\text{db8}:G:99::/64$
- Transit Routeur ↔ OPNsense (imposé) :  $2001:\text{db8}:G:\text{ff}::/64$ 
  - Routeur (TRANSIT) :  $2001:\text{db8}:G:\text{ff}::1/64$
  - OPNsense (WAN) :  $2001:\text{db8}:G:\text{ff}::2/64$

## Exigences IPv6 minimales (preuves obligatoires)

- IPv6 doit être opérationnel sur **au moins 1 VLAN** (USERS conseillé) : adresse + ping ICMPv6 vers la passerelle OPNsense.
- IPv6 doit être opérationnel **inter-divisions** : au minimum un ping ICMPv6 entre 2 divisions via **route statique IPv6** (preuve).
- Vous devez fournir `show ipv6 interface brief` et `show ipv6 route` (ou équivalent) + explication courte.

## 10.3 Services IP (obligatoires)

- DHCP obligatoire sur VLAN20 USERS et VLAN40 GUEST.
- DNS obligatoire via **Unbound** sur OPNsense (résolution de noms prouvée).
- Les clients doivent recevoir via DHCP : IP, masque, GW, DNS (preuves demandées).

## 10.4 Sécurité / segmentation (politique minimale imposée)

La sécurité doit être cohérente avec un contexte import/export (confidentialité, maîtrise des flux, limitation des surfaces d'attaque).

### 10.4.1 Politique "intra-division" (VLANs)

Règles minimales :

- **USERS (VLAN20)** → Internet : autoriser **DNS (53) + HTTP/HTTPS (80/443)**
- **USERS (VLAN20)** → **ADMIN (VLAN10)** : **interdire**
- **ADMIN (VLAN10)** → OPNsense : autoriser **HTTPS (443)** (et **SSH (22)** si vous l'activez)
- **GUEST (VLAN40)** → Internet uniquement : autoriser **DNS (53) + HTTP/HTTPS (80/443)**
- **GUEST (VLAN40)** → tout interne (VLAN10/20/30/...) : **interdire**
- **SRV (VLAN30)** : accès restreint (justifier les flux ; pas de “allow any”)

#### *10.4.2 Politique “inter-divisions” (par défaut : zéro confiance)*

- Par défaut : **interdire** les flux “division ↔ division”.
- N'autoriser que les flux explicitement demandés et justifiés (approche **moindre privilège**).

#### *10.4.3 Flux inter-divisions imposés (obligatoires)*

Pour rendre le projet concret et vérifiable, Tac&Tic Brother impose un besoin commun :

#### **Service métier imposé : Portail Intranet**

- Le **Développement (G2)** héberge un portail intranet accessible aux autres divisions.
- Le portail est hébergé dans **VLAN30 SRV** de G2.
- Service : **HTTPS TCP/443** (HTTP/80 optionnel si vous mettez une redirection)
- Nom DNS attendu : **intranet.ttb.local**

#### **Exigences d'accès**

- **Commercial (G1)** : accès **autorisé** au portail intranet (TCP/443)
- **Marketing International (G4)** : accès **autorisé** au portail intranet (TCP/443)
- **R&D (G3)** : accès **interdit par défaut** (sauf justification approuvée)

#### **Exigence DNS (pour forcer l'usage du service)**

- Chaque groupe doit permettre la résolution de **intranet.ttb.local** depuis VLAN20 USERS (au minimum) :
  - via un override/host dans Unbound, ou une zone locale **ttb.local**, ou une autre méthode documentée.

Les règles firewall doivent être écrites de façon lisible (alias, description) et prouvées par tests + logs.

#### *10.5 Journalisation & preuves*

- Vous devez être capable de produire :
  - 1 preuve d'autorisation (log ALLOW)
  - 1 preuve de blocage (log BLOCK)

- associées à vos règles (la règle doit être identifiable).

## 10.6 Exigences “au-delà” (recommandées)

- Centraliser la **journalisation** : syslog (OPNsense et routeur) vers une VM “LOG” (option).
- Mettre en place **NTP** (cohérence temps pour les logs) (option).
- Ajouter un petit service interne (VM web simple dans VLAN30 SRV) exposé sous conditions (option).

## 10.7 Analyse de flux (obligatoire)

Vous devez produire une **analyse de flux** qui servira de base à votre politique de filtrage.

**Format attendu (tableau) :**

- **Source** (division + VLAN + IP/plage)
- **Destination** (division + VLAN + IP/nom DNS)
- **Protocole/Ports**
- **Sens / Initiateur** (client → serveur)
- **Action** (ALLOW/DENY)
- **Justification métier**
- **Règle associée** (nom/ID/description)
- **Test de validation** (commande / résultat)

**Contenu minimum :**

- Tous les flux “intra-division” (USERS/ADMIN/GUEST/SRV) nécessaires au fonctionnement.
- Les flux vers Internet (DNS, HTTP/HTTPS).
- Les flux d’administration (ADMIN → équipements).
- Le flux inter-division imposé : accès au portail intranet (G1 & G4 → G2 SRV en TCP/443).
- Au moins 2 flux explicitement **refusés** et prouvés (ex : USERS → ADMIN ; GUEST → SRV).

L’analyse de flux doit être cohérente avec vos règles OPNsense et votre PV de recette.

## 10.8 Extensions (optionnelles, bonus)

Ces extensions permettent d’aller vers un niveau **CCNA2 / SRWE** (switching, routage dynamique, services) tout en restant cohérent avec le projet Tac&Tic Brother.

Choisissez **au moins 1 extension** si vous visez le bonus. Chaque extension doit être **prouvée** (commandes show + tests + capture).

### *Extension A — Routage dynamique (OSPFv2) sur le WAN (très CCNA2)*

**But** : remplacer les routes statiques IPv4 inter-divisions par OSPF.

- Activer **OSPFv2 area 0** sur les interfaces WAN des routeurs.
- Annoncer le préfixe LAN du groupe : **10.100.G.0/24**.
- Conserver la route “LAN via OPNsense” sur le routeur (statique locale) si vous gardez le modèle Routeur↔OPNsense.

**Preuves attendues :**

- `show ip ospf neighbor` (adjacences)
- `show ip route ospf` (routes apprises)
- ping/traceroute vers 2 divisions (IPv4)

### *Extension B — OSPFv3 (IPv6) inter-divisions*

**But** : routage dynamique IPv6 (au lieu de routes statiques).

- OSPFv3 sur le WAN IPv6 (area 0)
- Annoncer `2001:db8:G::/48`

**Preuves attendues :**

- `show ipv6 ospf neighbor`
- `show ipv6 route ospf`
- ping ICMPv6 inter-divisions (2+ divisions)

### *Extension C — Switching “pro” (si switch Cisco dispo)*

**But** : se rapprocher des compétences switch CCNA2 (VLAN/trunks/Spanning-Tree/sécurité ports).

- Trunk 802.1Q propre (DTP désactivé si possible)
- **STP** : définir un root (ou expliquer l’élection) + activer **PortFast** sur ports access + **BPDUs Guard**
- (Option) **Port-Security** sur un port access (1 MAC, sticky, violation)

**Preuves attendues :**

- `show vlan brief`
- `show interfaces trunk`
- `show spanning-tree` (+ preuve PortFast/BPDUs Guard)
- (si port-security) `show port-security interface ...`

### *Extension D — Services centralisés (DHCP “serveur” + relay)*

**But** : introduire un scénario entreprise (un DHCP central, relay sur l'infra) + dépannage.

- Déployer une VM **DHCP** en VLAN30 SRV (ex : sur Dév G2)
- Mettre en place le **DHCP relay** (ip helper) depuis les VLANs USERS/GUEST
- Documenter les scopes (VLAN20/VLAN40) et les options (GW/DNS)

#### **Preuves attendues :**

- Client d'un autre groupe reçoit une IP depuis le DHCP central
- Capture du DORA (option) + logs DHCP
- Procédure “DHCP KO” dans le runbook

### *Extension E — ACL “défense en profondeur” côté routeur*

**But** : ajouter un filtrage L3 simple sur le routeur (en plus d'OPNsense) pour illustrer les ACL CCNA2.

- Exemple : empêcher toute communication inter-divisions sauf vers l'intranet (G2 SRV TCP/443) et/ou certains préfixes.

#### **Preuves attendues :**

- `show access-lists`
- Tests OK/KO alignés avec l'analyse de flux

## 11. Exigences non fonctionnelles

- **Documentation** obligatoire et exploitable (un autre technicien doit pouvoir reprendre).
- **Sauvegardes** : routeur + export OPNsense à chaque fin de séance.
- **Traçabilité** : journal de changements (date/heure, action, justification, résultat).
- **Qualité** : mini-recette après chaque changement impactant.
- **Lisibilité** : schémas et tableaux d'adressage compréhensibles sans oral.

## 12. Livrables attendus

Vous devez livrer un dossier projet complet, comme en entreprise. Le rendu est un **dossier unique** (PDF ou Markdown) avec captures intégrées.

#### **Maquette fonctionnelle (MEP)**

- Maquette opérationnelle (routeur + ESXi + OPNsense + VLANs + services) conforme au cahier des charges.

- Preuves minimales : inter-divisions IPv4, IPv6 minimal, DHCP/DNS, politique firewall, logs.

### **Dossier de conception**

- Schéma logique (WAN + transit + OPNsense + VLANs + VMs)
- Plan d'adressage IPv4/IPv6 complet (tableaux)
- Stratégie de routage (routes statiques) + fiches d'interconnexion
- Architecture L3 Routeur↔OPNsense (transit /30 + /64, routes) appliquée
- Politique de sécurité (principes + exceptions)

### **Analyse de flux (obligatoire)**

- Tableau des flux (source/destination/ports/justification/règle/test) conforme à la section 10.7.
- Les flux refusés doivent être explicités (DENY) avec leur justification.

### **PV de recette**

- Plan de tests + résultats (captures) + commentaires.
- Synthèse de conformité : exigences respectées / non respectées + actions correctives.

## **13. Recette — Plan de tests minimal (obligatoire)**

Le PV de recette doit inclure résultats et preuves pour :

1. Client VLAN20 : DHCP OK + ping GW OK
2. Client VLAN20 : DNS OK (résolution)
3. Client VLAN20 : accès web/service externe OK (si service disponible)
4. Client VLAN20 : accès VLAN10 interdit (preuve)
5. Client VLAN10 : accès admin OPNsense (HTTPS) OK
6. Client VLAN40 : Internet OK ; accès interne interdit
7. Inter-divisions IPv4 : ping + traceroute vers 2 divisions
8. IPv6 : ping ICMPv6 local + ping ICMPv6 inter-division (1 minimum)
9. Logs : 1 preuve ALLOW + 1 preuve BLOCK associées à vos règles
10. Preuve L2 : ARP/MAC observé et expliqué (court)
11. Preuve routage : `show ip route` expliqué (au moins 5 lignes)
12. Flux imposé : depuis G1 et G4, accès au portail `intranet.ttb.local` (HTTPS) **OK** (preuve)
13. Flux imposé : depuis G3, accès au portail `intranet.ttb.local` **KO** (preuve)

**Recette CCNA1 — preuves supplémentaires (obligatoires)** 14. **Encapsulation/OSI (flux intranet)** : explication 8 lignes max + capture associée. 15. **Transport** : capture DNS (UDP/53) + capture début HTTPS (TCP/443 SYN/SYN-ACK/ACK). 16. **Switching** : preuve `show mac address-table` (si switch Cisco) **ou** preuve ARP/broadcast + explication broadcast domain vs collision domain. 17. **Subnetting** : 1 calcul détaillé (réseau/broadcast/plage/nb hôtes) prouvant que le VLAN choisi couvre le besoin.

## 14. Exploitation (runbook) — contenu minimum

Le runbook doit contenir :

- Inventaire (équipements, VMs, réseaux, VLANs)
- Procédure : ajouter une VM sur VLAN20 (ESXi + IP/DHCP)
- Procédure : ajouter un VLAN (ESXi + OPNsense + DHCP + règle de base)
- Procédure : sauvegarde/restauration OPNsense
- Procédure : sauvegarde routeur
- Checklists diagnostic : "DHCP KO", "DNS KO", "Pas d'accès inter-division", "Internet KO", "VM sur mauvais réseau ESXi"
- Points de contrôle (interfaces up, DHCP, DNS, NAT, logs)
- Rollback simple : comment revenir à la dernière config stable (routeur + OPNsense)

## 15. Gestion des demandes & anomalies (mode ticket)

Pendant le projet, l'enseignant joue le rôle du **client/exploitation** et peut transmettre **1 à 3 tickets** à traiter.

Pour chaque ticket :

- Symptômes → vérifications → cause racine → correctif → preuve → mise à jour doc/journal.

Un ticket "réussi" doit être reproductible : un autre technicien doit pouvoir relire et comprendre ce que vous avez fait.

## 16. Attendu final

À la fin, un autre technicien doit pouvoir **reprendre votre infra**, comprendre l'architecture, vérifier l'état, restaurer une configuration, et reproduire la recette — **comme en vraie prod.**