Ce document a été mis en ligne par l'organisme FormaV®.

Toute reproduction, représentation ou diffusion, même partielle, sans autorisation préalable, est strictement interdite.

Pour en savoir plus sur nos formations disponibles, veuillez visiter :
formav.co/explorer

BACHELOR UNIVERSITAIRE DE TECHNOLOGIE

**RÉSEAUX ET TÉLÉCOMMUNICATIONS**

# ÉVALUATION LOCALE : METTRE EN ŒUVRE UN SYSTÈME D'INFORMATION SÉCURISÉ POUR UNE PETITE STRUCTURE

SESSION 2026

Durée : 2 heures

| SPÉCIALITÉ / UNITÉ | COEFF |
|---|---|
| RÉSEAUX ET TÉLÉCOMMUNICATIONS | 3, INDICATIF |

Moyens de calculs et matériel autorisés :

**L'usage de calculatrice avec mode examen actif est autorisé. L'usage de calculatrice sans mémoire, « type collège », est autorisé.**

**Aucun document ou matériel autorisé en dehors de ceux fournis avec le sujet.**

Dès que le sujet vous est remis, assurez-vous qu'il est complet.

Ce sujet comporte 11 pages numérotées de 1/11 à 11/11.

Les documents réponses en fin de sujet sont à rendre avec la copie.

# DOSSIER SUJET

## MISE EN SITUATION PROFESSIONNELLE ET CAHIER DES CHARGES : ASSOCIATION LES ATELIERS DU CANAL, NANTES (LOIRE-ATLANTIQUE)

**Cadre de l'évaluation :** le programme national du BUT Réseaux et Télécommunications définit des compétences et des ressources, mais ne fixe pas d'épreuve nationale codifiée « C9 » portant ce libellé. Le présent sujet est construit pour une évaluation locale à partir de la situation professionnelle ci-dessous. La durée et le coefficient indiqués sont ceux retenus pour cette évaluation.

L'association Les Ateliers du Canal emploie 12 personnes dans des locaux comprenant un accueil, deux salles de réunion et un local technique. Elle souhaite remettre à niveau son système d'information sans interrompre durablement son activité. Le réseau actuel ne distingue pas les équipements internes de ceux des visiteurs. Un serveur de fichiers doit être installé dans le local technique. L'accès Wi-Fi visiteurs doit être isolé du réseau de l'association.

Le système à mettre en œuvre comprend une connexion Internet, un pare-feu, un commutateur administrable, deux points d'accès Wi-Fi, un serveur de fichiers et une alimentation secourue. Le réseau doit prendre en charge 12 postes ou équipements internes, jusqu'à 40 appareils visiteurs simultanés, 2 imprimantes réseau, 2 téléphones IP, 2 points d'accès, 1 serveur et les équipements d'administration.

Les réponses sont à reporter sur les documents DR 1 et DR 2 lorsqu'ils sont fournis. Toute hypothèse supplémentaire doit être clairement indiquée. Les prix et caractéristiques nécessaires aux calculs figurent dans le dossier technique.

## PARTIE 1 : Analyse fonctionnelle et exigences de sécurité (5 points)

***Qualifier les besoins, les actifs et les exigences applicables***

À partir du cahier des charges et des documents DT 1 à DT 3, analysez le besoin de l'association. Distinguez les exigences fonctionnelles des mesures de sécurité et justifiez vos choix au regard des informations fournies.

**1.1** (1,5 point) Relevez trois besoins fonctionnels du client et associez à chacun un équipement ou un service réseau qui contribue à le satisfaire. Présentez votre réponse sous forme de liste structurée.

**1.2** (2 points) Proposez une séparation logique des équipements en zones réseau. Pour chaque zone, indiquez les équipements ou usagers concernés et l'objectif de sécurité recherché. Votre réponse doit traiter au minimum le réseau interne, le réseau visiteurs, les serveurs et l'administration.

**1.3** (1,5 point) Indiquez deux mesures concrètes de protection des données personnelles et deux mesures de sécurisation des comptes ou des équipements. Pour chaque mesure, précisez le risque qu'elle réduit. Tenez compte des principes de minimisation des données, de limitation des accès et de protection des données applicables au traitement des fichiers de l'association.

## PARTIE 2 : Étude technologique et dimensionnement (6 points)

***Établir le plan d'adressage et vérifier les capacités matérielles***

Le bloc IPv4 privé attribué au projet est **192.168.40.0/24**. Les sous-réseaux doivent être distincts et respecter les effectifs indiqués dans le cahier des charges. Les premières adresses utilisables de chaque sous-réseau sont réservées à la passerelle. Utilisez les données du DT 2 pour les calculs de capacité, de stockage et de coût.

**Capacités à prendre en compte pour le dimensionnement**

| Zone | Besoin minimal en adresses utilisables, passerelle incluse |
|---|---|
| Visiteurs | 41 |
| Personnel | 15 |
| Serveurs | 6 |
| Administration | 6 |

*Données du cahier des charges et du DT 2.*

**2.1** (2,5 points) Complétez le tableau du DR 1 avec, pour chaque zone, le préfixe CIDR retenu, l'adresse réseau, le masque décimal, la première et la dernière adresse utilisables, l'adresse de diffusion et l'adresse de passerelle. Attribuez les sous-réseaux dans l'ordre décroissant des besoins à partir de 192.168.40.0/24, sans chevauchement. Justifiez le choix du préfixe de chaque zone en indiquant le nombre d'adresses utilisables.

**2.2** (1,5 point) Calculez la puissance PoE totale nécessaire aux équipements alimentés par le commutateur. Appliquez une réserve de dimensionnement de 20 %. Vérifiez si le budget PoE de 120 W indiqué au DT 2 est suffisant. Présentez les calculs avec les unités.

**2.3** (2 points) Calculez la capacité de stockage minimale à prévoir après prise en compte d'une croissance des données de 30 %. Déterminez si la configuration de deux disques de 2 To en miroir répond au besoin en capacité utile. Calculez ensuite le coût total des équipements de la nomenclature du DT 2, puis la marge budgétaire par rapport au plafond de 2 500 € HT. Détaillez les opérations.

## PARTIE 3 : Préparation de la mise en œuvre et protocole opératoire (5 points)

***Préparer les services, les filtrages et les contrôles de recette***

La mise en service doit préserver l'accès aux ressources internes tout en isolant les visiteurs. Les services d'adressage et de résolution de noms sont hébergés sur le pare-feu. Le serveur de fichiers utilise une adresse fixe dans le sous-réseau serveurs. Les flux nécessaires sont précisés au DT 3.

**3.1** (2 points) Complétez au DR 2 une configuration de principe indiquant, pour chaque zone, l'interface ou le VLAN à utiliser, la passerelle, le service DHCP attendu et l'accès DNS. Pour la zone serveurs, indiquez explicitement que le serveur de fichiers reçoit une adresse fixe. Les adresses à reporter doivent être cohérentes avec votre plan du DR 1.

**3.2** (1,5 point) Établissez une politique de filtrage minimale répondant aux flux autorisés du DT 3. Présentez au moins quatre règles ordonnées comprenant la source, la destination, le service ou port, l'action et une justification. La politique doit comporter un refus par défaut entre zones.

**3.3** (1,5 point) Rédigez un protocole de recette composé de trois contrôles vérifiables. Pour chaque contrôle, indiquez la manipulation, le résultat attendu et le critère permettant de conclure à la réussite. Au moins un contrôle doit vérifier l'isolement du réseau visiteurs et un autre l'accès autorisé au serveur de fichiers.

## PARTIE 4 : Prévention, exploitation et réaction à un incident (4 points)

***Réduire les risques d'exploitation et sécuriser les interventions***

Le système sera exploité par un salarié référent qui ne dispose pas d'une équipe informatique dédiée. Le local technique est accessible aux personnes autorisées uniquement. Les tâches de maintenance doivent être traçables et réalisées sans exposer les données de l'association.

**4.1** (2 points) Identifiez quatre risques d'exploitation réalistes pour cette petite structure et associez à chacun une mesure de prévention adaptée. Incluez au moins un risque lié aux comptes, un risque lié aux sauvegardes et un risque lié au réseau sans fil.

**4.2** (2 points) Un poste du réseau interne présente un comportement anormal et plusieurs fichiers deviennent illisibles. Décrivez, dans l'ordre, quatre actions immédiates à conduire pour limiter l'incident et préserver les éléments utiles à son analyse. Précisez une action à éviter et indiquez comment vérifier ultérieurement que les données peuvent être restaurées.

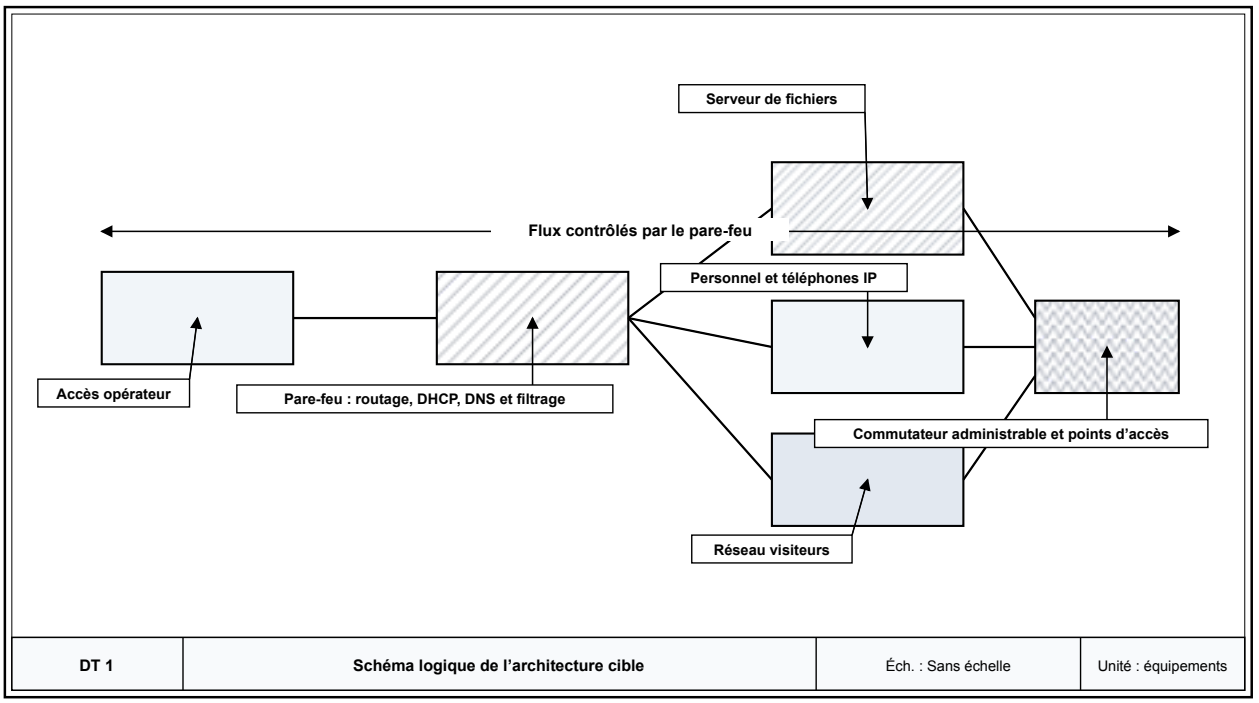
# DOSSIER TECHNIQUE ET RESSOURCES

Documents ressources nécessaires à la résolution du sujet

## **DT 1** : ARCHITECTURE LOGIQUE CIBLE ET EXIGENCES DU CLIENT

Les liens entre équipements représentent des liaisons Ethernet ou un accès opérateur. Le commutateur est administrable et prend en charge les VLAN. Le pare-feu assure le routage entre zones et le filtrage inter-VLAN. Les deux points d'accès diffusent un réseau Wi-Fi interne et un réseau Wi-Fi visiteurs distincts. Le serveur de fichiers ne doit pas être joignable directement depuis le réseau visiteurs.

Les informations personnelles présentes sur le serveur sont limitées aux données nécessaires aux activités de l'association. Les accès doivent être accordés selon le besoin professionnel. Les exigences applicables comprennent notamment les principes de protection des données prévus par le RGPD et les recommandations de sécurité de la CNIL. Ces références ne remplacent pas l'analyse des traitements ni les procédures internes du client.




*Représentation de principe. Les identifiants VLAN sont définis au DT 2.*

## **DT 2** : PLAN D'ADRESSAGE DE DÉPART, ÉQUIPEMENTS ET DONNÉES DE DIMENSIONNEMENT

Le réseau privé disponible est 192.168.40.0/24. Les VLAN prévus sont : personnel VLAN 10, visiteurs VLAN 20, serveurs VLAN 30, administration VLAN 99. Le candidat détermine les sous-réseaux et les adresses des passerelles. Le premier hôte utilisable de chaque sous-réseau est réservé à la passerelle. Le serveur de fichiers reçoit une adresse fixe dans son sous-réseau.

Pour un sous-réseau IPv4 de préfixe /n, le nombre d'adresses utilisables pour les hôtes est égal à $2^{32-n} - 2$, hors cas particuliers non utilisés dans ce sujet.

### Équipements, caractéristiques et prix unitaires

| Équipement | Quantité | Caractéristique utile | Prix unitaire HT |
|---|---|---|---|
| Pare-feu | 1 | Routage inter-VLAN, filtrage avec état, DHCP et DNS relais | 420 € |
| Commutateur administrable PoE+ | 1 | 24 ports, budget PoE total 120 W | 360 € |
| Point d'accès Wi-Fi | 2 | Puissance maximale PoE 13 W par appareil | 110 € |
| Téléphone IP | 2 | Puissance maximale PoE 5 W par appareil | 75 € |
| Serveur | 1 | Deux baies de stockage, consommation maximale 100 W | 650 € |
| Disque dur | 2 | 2 To par disque, configuration miroir | 95 € |
| Onduleur | 1 | 900 VA, autonomie constructeur de 10 min à 180 W | 180 € |
| Câblage et accessoires | 1 lot | Lot forfaitaire | 160 € |

*Prix d'achat HT fournis pour les besoins du sujet.*

### Données de capacité

| Paramètre | Valeur |
|---|---|
| Données actuellement à conserver | 1,2 To |
| Croissance estimée des données | 30 % |
| Capacité utile d'un disque de 2 To en miroir à deux disques | 2 To |
| Plafond budgétaire | 2 500 € HT |
| Réserve de dimensionnement PoE | 20 % de la puissance calculée |

*Valeurs retenues pour les calculs de dimensionnement.*

## **DT 3** : SERVICES RÉSEAU, FLUX AUTORISÉS ET EXIGENCES DE MISE EN SERVICE

Les services du pare-feu sont fournis sur les passerelles des réseaux concernés. Les règles doivent être appliquées dans l'ordre et être accompagnées d'une politique de refus par défaut entre zones. L'accès Internet des visiteurs est autorisé, mais les visiteurs ne doivent accéder ni aux équipements du personnel, ni aux serveurs, ni à l'interface d'administration.

Le serveur de fichiers fournit le service de partage SMB sur TCP 445 uniquement aux postes du personnel autorisés. L'administration des équipements est réservée au réseau d'administration. Pour l'administration web sécurisée, TCP 443 est utilisé. Les requêtes DNS des clients sont destinées au service DNS du pare-feu sur UDP et TCP 53. L'accès Internet des clients utilise la traduction d'adresses du pare-feu. Les mises à jour du serveur peuvent sortir vers Internet selon la politique de l'association.

Références de mise en œuvre : utiliser des protocoles sécurisés et des comptes nominatifs, supprimer les comptes et services inutiles, appliquer les mises à jour, protéger les configurations et réaliser des

sauvegardes testées. Les recommandations de l'ANSSI et de la CNIL constituent des ressources de bonnes pratiques. Le RGPD impose des obligations selon les traitements réellement effectués. Le périmètre d'application d'une réglementation spécifique doit être vérifié au regard de l'activité de l'organisme.

**Matrice minimale des flux interzones**

| Source | Destination | Service ou port | Décision |
|---|---|---|---|
| Visiteurs | Internet | DNS vers le pare-feu, puis navigation Internet | Autoriser selon filtrage |
| Visiteurs | Personnel, serveurs, administration | Tous les flux | Refuser |
| Personnel | Serveur de fichiers | TCP 445 | Autoriser pour les utilisateurs autorisés |
| Personnel et visiteurs | Pare-feu, service DNS | UDP/TCP 53 | Autoriser vers le service DNS désigné |
| Administration | Pare-feu, commutateur, points d'accès et serveur | HTTPS TCP 443 et protocoles d'administration nécessaires | Autoriser uniquement depuis les postes administrateurs |
| Serveur | Internet | HTTPS TCP 443 pour mises à jour | Autoriser selon la politique de mise à jour |

*Tout flux non explicitement autorisé entre zones est refusé.*

**Points de contrôle avant mise en production**

| Contrôle | Résultat attendu |
|---|---|
| Attribution d'adresse à un poste personnel | Adresse du sous-réseau personnel, passerelle et DNS cohérents |
| Connexion d'un client visiteur | Adresse du sous-réseau visiteurs et accès Internet |
| Tentative visiteur vers serveur ou administration | Connexion refusée |
| Accès d'un poste autorisé au partage | Partage accessible sur TCP 445 selon les droits du compte |
| Restauration d'un fichier de test | Fichier restauré lisible et contrôlé par le référent |

*Résultats attendus lors de la recette.*

**NE RIEN ÉCRIRE DANS CETTE PARTIE**

**DR 1** : Document réponse à rendre avec la copie : questions 2.1 à 2.3 **À RENDRE AVEC LA COPIE**

Compléter directement les tableaux. Pour la question 2.1, attribuer des sous-réseaux contigus à partir de 192.168.40.0/24, dans l'ordre décroissant des besoins, sans chevauchement. Les unités doivent figurer dans les résultats de calcul.

**Plan d'adressage à compléter**

| Zone et VLAN | Besoin en hôtes | Préfixe CIDR | Adresse réseau | Masque décimal | Première adresse utilisable | Dernière adresse utilisable | Adresse de diffusion | Passerelle |
|---|---|---|---|---|---|---|---|---|
| Visiteurs VLAN 20 | 41 | ..... | ..... | ..... | ..... | ..... | ..... | ..... |
| Personnel VLAN 10 | 15 | ..... | ..... | ..... | ..... | ..... | ..... | ..... |
| Serveurs VLAN 30 | 6 | ..... | ..... | ..... | ..... | ..... | ..... | ..... |
| Administration VLAN 99 | 6 | ..... | ..... | ..... | ..... | ..... | ..... | ..... |

*Inscrire les valeurs calculées pour chaque VLAN.*

**Calculs de puissance PoE et de capacité de stockage**

| Calcul | Expression et résultat | Conclusion |
|---|---|---|
| Puissance PoE nécessaire avant réserve | ..... | ..... |
| Puissance PoE avec réserve de 20 % | ..... | ..... |
| Capacité de stockage après croissance de 30 % | ..... | ..... |

*Justifier les résultats et conclure sur la capacité des équipements.*

## Nomenclature et vérification du budget

| Équipement | Quantité | Prix unitaire HT | Sous-total HT |
|---|---|---|---|
| Pare-feu | 1 | 420 € | ..... |
| Commutateur administrable PoE+ | 1 | 360 € | ..... |
| Points d'accès Wi-Fi | 2 | 110 € | ..... |
| Téléphones IP | 2 | 75 € | ..... |
| Serveur | 1 | 650 € | ..... |
| Disques durs | 2 | 95 € | ..... |
| Onduleur | 1 | 180 € | ..... |
| Câblage et accessoires | 1 lot | 160 € | ..... |
| Total HT et marge budgétaire | ..... | ..... | ..... |

*Calculer le total HT et la marge par rapport au plafond.*

**Cadre réservé aux justifications, calculs complémentaires ou schémas du candidat :**

.....

.....

.....

.....

.....

.....

.....

**NE RIEN ÉCRIRE DANS CETTE PARTIE**

**DR 2** : Document réponse à rendre avec la copie : questions 3.1 à 3.3 **À RENDRE AVEC LA COPIE**

Compléter les champs avec les valeurs déterminées au DR 1. Les règles doivent être ordonnées. Indiquer explicitement la source, la destination, le service, l'action et la justification. Ajouter les contrôles de recette dans les cases prévues.

### Configuration logique des zones

| Zone | VLAN | Adresse de passerelle | Service DHCP | DNS utilisé | Remarque de configuration |
|---|---|---|---|---|---|
| Visiteurs | 20 | ..... | ..... | ..... | Isolation des autres zones : ... |
| Personnel | 10 | ..... | ..... | ..... | Accès au partage selon les droits : ... |
| Serveurs | 30 | ..... | Aucun bail pour le serveur | ..... | Adresse fixe du serveur de fichiers : ... |
| Administration | 99 | ..... | ..... | ..... | Accès réservé aux postes administrateurs : ... |

*Configuration de principe des VLAN et services réseau.*

### Règles de filtrage à compléter

| Ordre | Source | Destination | Service ou port | Action | Justification |
|---|---|---|---|---|---|
| 1 | ..... | ..... | ..... | ..... | ..... |
| 2 | ..... | ..... | ..... | ..... | ..... |
| 3 | ..... | ..... | ..... | ..... | ..... |
| 4 | ..... | ..... | ..... | ..... | ..... |
| Dernière règle | Toutes zones | Toutes destinations interzones | Tous services non précédemment autorisés | ..... | ..... |

*Classer les règles dans l'ordre d'application. Ajouter une règle de refus par défaut.*

## Protocole de recette à compléter

| Contrôle | Manipulation | Résultat attendu | Critère de réussite |
|---|---|---|---|
| Attribution DHCP d'un poste personnel | ..... | ..... | ..... |
| Isolement d'un client visiteur | ..... | ..... | ..... |
| Accès au partage depuis un poste autorisé | ..... | ..... | ..... |

*Décrire des tests reproductibles et leurs critères de réussite.*

**Cadre réservé aux justifications, calculs complémentaires ou schémas du candidat :**

.....

.....

.....

.....

.....

.....

.....

Copyright © 2027 FormaV®. Tous droits réservés.

FormaV® est une marque déposée auprès de l'INPI sous le numéro 5227897.

Ce document a été élaboré par FormaV® avec le plus grand soin afin d'accompagner chaque apprenant vers la réussite de ses examens. Son contenu (textes, graphiques, méthodologies, tableaux, exercices, concepts, mises en forme) constitue une œuvre protégée par le droit d'auteur.

Toute copie, partage, reproduction, diffusion ou mise à disposition, même partielle, gratuite ou payante, est strictement interdite sans accord préalable et écrit de FormaV®, conformément aux articles L.111-1 et suivants du Code de la propriété intellectuelle. Dans une logique anti-plagiat, FormaV® se réserve le droit de vérifier toute utilisation illicite, y compris sur les plateformes en ligne ou sites tiers.

En utilisant ce document, vous vous engagez à respecter ces règles et à préserver l'intégrité du travail fourni. La consultation de ce document est strictement personnelle.

Merci de respecter le travail accompli afin de permettre la création continue de ressources pédagogiques fiables et accessibles.