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

Réseaux et télécommunications

Session 2026 • Code sujet : **26-BUT-RT-C1** • Durée : **2 heures** • Coefficient : **3,0**
indicatif

Sommaire

Cliquez sur une partie pour y accéder directement

1. Architecture réseau, adressage et routage (3 questions) **Page 3**

2. Exploitation de la base de données d'inventaire (3 questions) **Page 5**

3. Analyse d'incident et sécurisation des accès (4 questions) **Page 7**

4. Ce qu'il faut retenir & Questions fréquentes (FAQ) (Synthèse & Q&A Examen) **Page 9**

Sujet officiel (PDF) : https://butrt.fr/assets/annales/but-rt/C1 - Administrer les réseaux et l'Internet/2026/BUT Réseaux et Télécommunications - C1 - Administrer les réseaux et l'Internet - Session 2026 - 1-Sujet.pdf

1. Architecture réseau, adressage et routage

Sur le site lyonnais de Novalys Services, R1 assure le routage inter-VLAN et relie le réseau local à Internet ainsi qu'à une plateforme hébergée par VPN. Les documents techniques précisent le plan IPv4 et IPv6, les interfaces logiques et les routes à utiliser.

Question 1.1. Pour le poste du VLAN 20 ayant l'adresse IPv4 10.24.20.77/25, déterminer l'adresse du réseau, l'adresse de diffusion et la plage d'adresses utilisables, puis préciser si cette adresse appartient au sous-réseau du VLAN 20 indiqué dans le DT 1.

Avec un préfixe **/25**, le dernier octet est découpé en blocs de 128 adresses. Comme 77 est dans le bloc 0 à 127, le réseau est **10.24.20.0** et l'adresse de diffusion **10.24.20.127**. Les adresses utilisables vont de **10.24.20.1** à **10.24.20.126**. L'adresse 10.24.20.77 appartient donc bien au réseau VLAN 20 du DT 1.

> ✓ **RÉPONSE À RETENIR**
>
> 10.24.20.0/25 ; diffusion : 10.24.20.127 ; plage utilisable : 10.24.20.1 à 10.24.20.126. 10.24.20.77 appartient au sous-réseau.

Question 1.2. À partir du plan du DT 1, indiquer pour le VLAN 30 son nom d'usage, son préfixe IPv4, l'adresse IPv4 de sa passerelle, son préfixe IPv6 et le nom de l'interface logique de R1 qui lui est associée.

Le plan d'adressage du DT 1 donne directement les paramètres du VLAN 30. La passerelle IPv4 est la première adresse utilisable du sous-réseau. L'interface logique G0/0.30 porte le routage de ce VLAN sur R1.

Élément	Valeur
Nom d'usage	Serveurs
Préfixe IPv4	10.24.30.0/27
Passerelle IPv4	10.24.30.1
Préfixe IPv6	2001:db8:24:30::/64
Interface logique R1	G0/0.30

> ✓ **RÉPONSE À RETENIR**
>
> VLAN 30 : Serveurs ; 10.24.30.0/27 ; passerelle 10.24.30.1 ; IPv6 2001:db8:24:30::/64 ; interface G0/0.30.

Question 1.3. Compléter la table de routage du DR 1 en indiquant, pour chaque destination, le prochain saut ou l'interface de sortie correspondant aux informations du DT 1. Distinguer la route par défaut de la route statique vers le réseau hébergé.

Les VLAN sont directement connectés à R1 : chacun sort par son interface logique. Le réseau hébergé utilise l'interface du tunnel VPN. La route par défaut, distincte de cette route statique, envoie les autres destinations vers la passerelle opérateur par le WAN.

Destination	Prochain saut ou interface de sortie
VLAN 10 Administration	G0/0.10
VLAN 20 Utilisateurs	G0/0.20
VLAN 30 Serveurs	G0/0.30
VLAN 40 Invités	G0/0.40
Réseau hébergé	ipsec0
Route par défaut	198.51.100.9 par interface WAN

Table de routage DR 1 complétée

Destination	Préfixe	Prochain saut ou interface de sortie
VLAN 10 Administration	10.24.10.0/26	G0/0.10
VLAN 20 Utilisateurs	10.24.20.0/25	G0/0.20
VLAN 30 Serveurs	10.24.30.0/27	G0/0.30
VLAN 40 Invités	10.24.40.0/26	G0/0.40
Réseau hébergé	172.20.0.0/16	ipsec0
Route par défaut	0.0.0.0/0	198.51.100.9 via WAN

Compléter le prochain saut ou l'interface de sortie à partir du DT 1.

✓ RÉPONSE À RETENIR

VLAN 10 : G0/0.10 ; VLAN 20 : G0/0.20 ; VLAN 30 : G0/0.30 ; VLAN 40 : G0/0.40 ; réseau hébergé : ipsec0 ; défaut : 198.51.100.9 via WAN.

2. Exploitation de la base de données d'inventaire

La base relationnelle InventaireRT répertorie les équipements du site et les incidents qui leur sont associés. Les extraits fournis servent à rédiger des requêtes SQL de filtrage et d'agrégation, puis à vérifier un résultat à partir des lignes affichées.

Question 2.1. Rédiger une requête SQL complète affichant l'identifiant et le nom des équipements du VLAN 20 dont l'état est actif, avec un tri par identifiant croissant.

La requête filtre simultanément sur le VLAN 20 et l'état `actif`. Elle sélectionne uniquement l'identifiant et le nom, puis trie les lignes par identifiant croissant. Les noms de table et de colonnes respectent le schéma du DT 2.

✓ RÉPONSE À RETENIR

```
SELECT id_equipement, nom
FROM Equipement
WHERE vlan = 20 AND etat = 'actif'
ORDER BY id_equipement ASC;
```

Question 2.2. Rédiger une requête SQL complète affichant, pour chaque équipement, son identifiant, son nom et le nombre d'incidents de gravité critique qui lui sont associés. Les équipements sans incident critique doivent apparaître avec un total égal à zéro. Trier le résultat par identifiant croissant.

1. La jointure externe gauche conserve tous les équipements, même sans incident critique.
2. Le filtre `gravite = 'critique'` est placé dans la condition de jointure afin de préserver les équipements sans correspondance.
3. `COUNT(i.id_incident)` renvoie alors zéro pour ces équipements. Le regroupement produit un total par équipement et le tri respecte l'ordre croissant demandé.

✓ RÉPONSE À RETENIR

```
SELECT e.id_equipement, e.nom, COUNT(i.id_incident) AS nombre_incidents_critiques
FROM Equipement e
LEFT JOIN Incident i
  ON i.equipement_id = e.id_equipement AND i.gravite = 'critique'
GROUP BY e.id_equipement, e.nom
ORDER BY e.id_equipement ASC;
```

Question 2.3. À partir des lignes du DT 2, donner le nombre d'équipements correspondant au filtre VLAN 20 et état actif, préciser leurs identifiants et expliquer brièvement pourquoi l'équipement inactif n'est pas compté.

Les équipements 201 et 202 ont tous deux le VLAN 20 et l'état `actif`. L'équipement 203 est bien dans le VLAN 20, mais son état est `inactif` : il ne satisfait donc pas les deux conditions du filtre. L'équipement 301 est actif, mais appartient au VLAN 30 et n'est pas retenu.

> **✓ RÉPONSE À RETENIR**
>
> 2 équipements : identifiants 201 et 202. L'équipement 203 est exclu, car son état est inactif.

3. Analyse d’incident et sécurisation des accès

Le DT 2 rassemble un journal d’authentification SSH, un extrait de configuration SSH et une capture réseau effectuée sur le VLAN 20. Il faut interpréter les événements, identifier les informations exposées en clair et proposer des mesures de durcissement et de réponse à incident.

Question 3.1. Analyser les lignes du journal SSH du DT 2 : relever l’adresse source à l’origine de plusieurs échecs, identifier l’événement d’authentification réussi et indiquer les éléments qui justifient de traiter la situation comme un incident de sécurité à vérifier.

La source **203.0.113.44** provoque quatre échecs successifs d’authentification pour le compte root, de 08:11:02 à 08:11:20. À 08:12:03, l’événement *Accepted password* signale une connexion réussie de root depuis cette même adresse. Cette succession peut indiquer une tentative de deviner le mot de passe suivie d’un accès non autorisé, sans toutefois le prouver. Il faut vérifier si cette connexion était légitime et examiner les actions réalisées sur srv-admin-01 après l’authentification.

> **✓ RÉPONSE À RETENIR**
>
> Quatre échecs SSH pour root depuis 203.0.113.44, puis connexion réussie du même compte à 08:12:03 : incident à vérifier.

Question 3.2. À partir de l’extrait de capture réseau du DT 2, indiquer le type d’information exposé en clair et expliquer le risque associé à l’utilisation du protocole observé sur un réseau partagé.

La trame Telnet expose en clair les identifiants applicatifs : le nom de connexion **agent7** et le mot de passe. Telnet ne chiffre pas les échanges. Sur un réseau partagé, une personne capable de capturer le trafic peut lire ces données puis les réutiliser pour accéder au service, voire à d’autres comptes si le mot de passe est réemployé. Le mot de passe capturé doit donc être considéré comme compromis et remplacé. Il faut privilégier un protocole chiffré, tel que SSH, à la place de Telnet.

> **✓ RÉPONSE À RETENIR**
>
> Telnet expose login et mot de passe en clair, interceptables puis réutilisables sur le réseau partagé.

Question 3.3. Proposer quatre mesures de durcissement adaptées à l’extrait de configuration SSH du DT 2. Pour chacune, indiquer le paramètre ou le contrôle à modifier et l’effet de sécurité recherché.

Quatre durcissements adaptés à la configuration :

- `PermitRootLogin no` : interdire la connexion SSH directe du compte root.
- `PasswordAuthentication no` : privilégier les clés SSH, après déploiement et vérification de leur bon fonctionnement.
- Configurer `AllowUsers` ou `AllowGroups` : limiter l’accès aux seuls comptes nécessaires.
- Filtrer le port 22 au pare-feu pour n’autoriser que les adresses d’administration et limiter les tentatives répétées, par exemple avec Fail2ban.

Appliquer et tester les changements en conservant une session d'administration active afin d'éviter de perdre l'accès au serveur.

> **✓ RÉPONSE À RETENIR**
>
> Interdire l'accès SSH root, privilégier les clés, limiter les comptes autorisés et filtrer le port 22 avec limitation des tentatives.

Question 3.4. Indiquer deux actions immédiates à mener après la détection de l'incident, en distinguant une action de limitation du risque et une action de préservation des éléments utiles à l'analyse.

Limitation du risque : bloquer temporairement la source `203.0.113.44`, sécuriser le compte root et désactiver son accès SSH direct. Remplacer également le mot de passe Telnet exposé et vérifier s'il est utilisé pour d'autres comptes.

Préservation des éléments : exporter et protéger les journaux SSH et système ainsi que la capture réseau. Conserver les horodatages et une copie non altérée, idéalement avec une empreinte permettant de vérifier son intégrité lors de l'analyse.

> **✓ RÉPONSE À RETENIR**
>
> Bloquer la source et sécuriser les comptes ; préserver les journaux et la capture réseau sans les altérer.

Ce qu'il faut retenir de ce sujet (Session 2026)

Bilan de l'épreuve : Épreuve de la compétence C1 du BUT Réseaux et télécommunications, session 2026, code 26-BUT-RT-C1, d'une durée de 2 heures et de coefficient indicatif 3,0. Elle porte sur le réseau du site lyonnais de Novalys Services et évalue l'adressage IPv4/IPv6, le routage, l'exploitation SQL d'un inventaire, l'analyse d'événements de sécurité et la sécurisation des accès.

Notions-clés, formules & règles à maîtriser

- Le préfixe IPv4 délimite le sous-réseau : l'adresse réseau et l'adresse de diffusion ne sont pas attribuables aux hôtes.
- Les réseaux directement connectés utilisent leurs interfaces logiques ; une destination distante peut passer par un tunnel ou un prochain saut.
- Pour conserver les équipements sans incident critique, filtrer la gravité dans la jointure externe et remplacer un total nul par zéro.
- Telnet transmet les données applicatives sans chiffrement ; SSH doit limiter les accès privilégiés et privilégier une authentification robuste.

Points de vigilance & attentes du jury

- Vérifier le préfixe, les bornes du sous-réseau et l'appartenance de l'adresse au VLAN demandé.
- Distinguer la route par défaut vers l'opérateur de la route spécifique vers le réseau hébergé par le tunnel.
- Dans la requête d'agrégation, conserver tous les équipements, y compris ceux sans incident critique, et trier par identifiant.
- Étayer l'analyse de sécurité avec les horodatages, les échecs répétés, la réussite observée et les paramètres de configuration fournis.

Questions fréquentes sur cette épreuve (Q&A Examen)

Q : Comment déterminer le réseau et la plage utilisable à partir d'une adresse IPv4 et de son préfixe ?

Convertissez le préfixe en masque, puis appliquez le masque à l'adresse pour obtenir le réseau. L'adresse de diffusion met à 1 les bits hôte. La plage utilisable se trouve entre ces deux adresses, sauf règles particulières du sous-réseau.

Q : Comment compter les incidents critiques sans exclure les équipements qui n'en ont aucun ?

Utilisez une jointure externe gauche entre Equipement et Incident, avec le filtre de gravité critique dans la condition de jointure. Comptez les identifiants d'incident, regroupez par équipement et remplacez les totaux nuls par zéro.

Q : Comment répartir les deux heures entre les parties ?

Le sujet attribue 7 points à la partie réseau, 6 à la base de données et 7 à la sécurité, sans fixer de durée par partie. Répartissez le temps selon ces pondérations, gardez une marge de relecture et vérifiez que le DR 1 est rendu.

Q : Que faut-il préciser pour chacune des mesures de durcissement SSH ?

Indiquez le paramètre ou le contrôle à modifier, puis l'effet de sécurité recherché. Les mesures doivent répondre aux risques visibles dans le sujet, notamment l'accès root, l'authentification par mot de passe et la transmission d'identifiants en clair.

Sujet officiel associé (PDF) : https://butrt.fr/assets/annales/but-rt/C1 - Administrer les réseaux et l'Internet/2026/BUT Réseaux et Télécommunications - C1 - Administrer les réseaux et l'Internet - Session 2026 - 1-Sujet.pdf
Ressources BUT Réseaux et Télécommunications : Toutes les annales & corrigés • Fiches de révision complètes • Simulateur de notes d'examen

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.