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 - BUT R&T, compétence C2

Session 2026 • Code sujet : **26-BUT-RT-EP1** • Durée : **2 heures** • Coefficient : **3,0**
indicatif

Sommaire

Cliquez sur une partie pour y accéder directement

1. Architecture, adressage et routage (4 questions) **Page 3**

2. Exploitation des données et automatisation (3 questions) **Page 6**

3. Diagnostic de sécurité et mesures de durcissement (3 questions) **Page 8**

4. Ce qu'il faut retenir & Questions fréquentes (FAQ) (Synthèse & Q&A Examen) **Page 10**

Sujet officiel (PDF) : https://butrt.fr/assets/annales/but-rt/C2 - Assister l'administrateur du réseau/2026/BUT Réseaux et Télécommunications - C2 - Assister l'administrateur du réseau - Session 2026 - 1-Sujet.pdf

1. Architecture, adressage et routage

Sur le réseau local de Novalys Services à Lyon, le commutateur de niveau 3 SW-L3 assure le routage inter-VLAN et rejoint le pare-feu FW-01 par un lien de transit. Il faut préparer l'ajout d'un réseau invité et diagnostiquer la connectivité à partir du plan d'adressage et des extraits de configuration.

Configuration de base du réseau local

Question 1.1. À partir du bloc 192.168.40.0/24, déterminez le plus petit préfixe IPv4 permettant d'adresser 24 postes clients et une passerelle. Indiquez le masque décimal, l'adresse réseau, l'adresse de diffusion et la plage d'adresses utilisables du premier sous-réseau en partant de 192.168.40.0. Complétez également les éléments correspondants du DR 1.

Il faut adresser 25 équipements : 24 postes et une passerelle. Cinq bits d'hôte donnent 32 adresses, dont 30 utilisables : un préfixe /27 suffit. Le premier sous-réseau commence à 192.168.40.0.

Élément	Valeur
Préfixe CIDR	192.168.40.0/27
Masque décimal	255.255.255.224
Adresse réseau	192.168.40.0
Adresse de diffusion	192.168.40.31
Adresses utilisables	192.168.40.1 à 192.168.40.30

DR 1 complété : plan d'adressage du VLAN 40

Élément	Valeur
Préfixe CIDR	192.168.40.0/27
Masque décimal	255.255.255.224
Adresse réseau	192.168.40.0
Adresse de diffusion	192.168.40.31
Plage d'adresses utilisables	192.168.40.1 à .30

✓ RÉPONSE À RETENIR

VLAN 40 : 192.168.40.0/27, masque 255.255.255.224, diffusion 192.168.40.31, plage utilisable 192.168.40.1 à 192.168.40.30.

Adressage IPv6

Question 1.2. Le VLAN 20 utilise le préfixe IPv6 2001:db8:1200:20::/64 et la passerelle 2001:db8:1200:20::1. Pour le poste adressé 2001:db8:1200:20::25/64, indiquez s'il appartient au sous-réseau de la passerelle en justifiant, puis donnez son adresse de réseau IPv6.

La passerelle et le poste ont le même préfixe /64 : ils appartiennent donc au même sous-réseau IPv6. En mettant à zéro la partie hôte de l'adresse du poste, on obtient l'adresse de réseau **2001:db8:1200:20::/64**.

> ✓ **RÉPONSE À RETENIR**
>
> Oui, même sous-réseau : 2001:db8:1200:20::/64.

Table de routage de SW-L3

Question 1.3. Complétez dans le DR 1 les routes directement connectées de SW-L3 pour les VLAN 10, 20, 30 et 40, en précisant l'interface logique ou le VLAN de sortie. Pour le VLAN 40, utilisez le sous-réseau calculé à la question 1.1 et sa première adresse utilisable comme passerelle. Indiquez aussi le prochain saut de la route par défaut vers le pare-feu.

Les réseaux des VLAN 10, 20 et 30 sont directement connectés à SW-L3. Le VLAN 40 utilise le sous-réseau calculé à la question 1.1 et sa première adresse utilisable comme passerelle. La route par défaut pointe vers l'interface de transit du pare-feu.

Destination	Type	Interface ou prochain saut
192.168.10.0/24	Directement connectée	VLAN 10
192.168.20.0/24	Directement connectée	VLAN 20
192.168.30.0/24	Directement connectée	VLAN 30
192.168.40.0/27	Directement connectée	VLAN 40, passerelle 192.168.40.1
0.0.0.0/0	Route par défaut	192.168.254.1

DR 1 complété : routes de SW-L3

Table de routage de SW-L3

Destination	Type de route	Prochain saut ou interface de sortie
192.168.10.0/24	Directement connectée	VLAN 10
192.168.20.0/24	Directement connectée	VLAN 20
192.168.30.0/24	Directement connectée	VLAN 30
192.168.40.0/27	Directement connectée	VLAN 40, passerelle .1
.....	Directement connectée	192.168.254.1
0.0.0.0/0	Route par défaut	.....

✓ RÉPONSE À RETENIR

Routes connectées : VLAN 10, 20, 30 et 40. Route par défaut : 192.168.254.1.

Diagnostic de connectivité

Question 1.4. Un poste du VLAN 20 peut joindre sa passerelle, mais pas le serveur 192.168.30.10 du VLAN 30. En vous appuyant sur le DT 1, citez deux vérifications pertinentes à effectuer sur le commutateur ou le poste avant de conclure à une panne du serveur, et précisez le résultat attendu pour chacune.

Deux vérifications permettent de distinguer un défaut de routage ou de configuration d'une panne serveur :

- **Sur SW-L3 :** vérifier que `ip routing` est actif et que le réseau 192.168.30.0/24 apparaît comme directement connecté via l'interface VLAN 30 (192.168.30.1/24).
- **Sur le poste et le trunk :** confirmer l'adresse 192.168.20.45/24, la passerelle 192.168.20.1, l'affectation au VLAN 20 et le transport des VLAN 20 et 30 sur le trunk. Le DT 1 indique que ces VLAN sont autorisés dans l'état relevé.

✓ RÉPONSE À RETENIR

Vérifier le routage et le réseau directement connecté sur SW-L3, puis l'adressage du poste et les VLAN autorisés sur le trunk.

2. Exploitation des données et automatisation

La base relationnelle de suivi des incidents comprend les tables Devices et Incidents, reliées par l'identifiant de l'équipement. Les tâches portent sur des requêtes SQL qui exploitent ces tables sans modifier les données, puis sur le filtrage et le comptage de marqueurs dans un extrait de journal système.

Interrogation SQL des incidents ouverts

Question 2.1. Écrivez une requête SQL qui affiche, pour chaque incident de priorité « haute » encore ouvert, son identifiant, sa date, le nom de l'équipement concerné et sa localisation. Utilisez une jointure entre les deux tables, puis triez les résultats de la date la plus récente à la plus ancienne.

La jointure relie chaque incident à son équipement avec `device_id`. Les critères sélectionnent les incidents de priorité haute encore ouverts, puis le tri décroissant place la date la plus récente en premier.

```
SELECT i.incident_id, i.created_at, d.name, d.location
FROM Incidents AS i
JOIN Devices AS d ON d.device_id = i.device_id
WHERE i.priority = 'haute'
  AND i.status = 'ouvert'
ORDER BY i.created_at DESC;
```

Les colonnes affichées sont l'identifiant et la date de l'incident, puis le nom et la localisation de l'équipement.

> **✓ RÉPONSE À RETENIR**
>
> Afficher l'identifiant, la date, le nom et la localisation des incidents haute priorité ouverts, du plus récent au plus ancien.

Comptage des incidents par équipement

Question 2.2. Écrivez une requête SQL qui affiche, pour chaque équipement, son nom et le nombre total d'incidents enregistrés, y compris les équipements sans incident. Triez le résultat par nombre d'incidents décroissant.

La jointure externe gauche conserve tous les équipements, même sans incident associé. `COUNT(i.incident_id)` renvoie zéro pour ceux-ci, contrairement à `COUNT(*)`. Le regroupement s'effectue par identifiant et nom de l'équipement.

```
SELECT d.name, COUNT(i.incident_id) AS nombre_incidents
FROM Devices AS d
LEFT JOIN Incidents AS i ON i.device_id = d.device_id
GROUP BY d.device_id, d.name
ORDER BY nombre_incidents DESC;
```

Le résultat inclut les équipements sans incident et classe les nombres du plus grand au plus petit.

✓ RÉPONSE À RETENIR

Afficher le nom et le nombre d'incidents de chaque équipement, y compris zéro, par ordre décroissant du nombre.

Filtrage et comptage avec grep

Question 2.3. À partir de l'extrait de journal du DT 2, proposez une commande Bash utilisant grep pour afficher uniquement les lignes contenant le marqueur AUTH_FAIL, puis une commande permettant de compter ces lignes. Indiquez combien de lignes portent ce marqueur dans l'extrait.

Remplacez `journal.log` par le nom du fichier contenant l'extrait. La première commande affiche les lignes contenant le marqueur `AUTH_FAIL`. L'option `-c` de la seconde compte les lignes correspondantes.

```
grep 'AUTH_FAIL' journal.log
grep -c 'AUTH_FAIL' journal.log
```

L'extrait contient cinq lignes avec ce marqueur. La ligne `AUTH_OK` n'est pas comptée.

✓ RÉPONSE À RETENIR

`grep 'AUTH_FAIL' journal.log` ; comptage : `grep -c 'AUTH_FAIL' journal.log`. Total dans l'extrait : 5 lignes.

3. Diagnostic de sécurité et mesures de durcissement

Une alerte signale des échecs répétés d'authentification SSH sur un serveur. À partir des journaux et des éléments de configuration fournis, il faut caractériser et signaler l'incident, vérifier son origine et son impact, puis proposer des mesures de durcissement qui préservent l'accès d'administration légitime.

Signalement synthétique de l'incident

Question 3.1. Relevez dans l'extrait de journal le service visé, l'adresse IP source, le nombre d'échecs observés et la période concernée. Présentez ces éléments sous la forme d'un signalement synthétique.

Signalement : sur `srv-auth-01`, le journal montre des échecs d'authentification SSH pour le compte `admin`, depuis `203.0.113.77`.

Élément	Observation
Service	SSH (sshd)
Échecs observés	5 événements AUTH_FAIL
Période	18 juin 2026, de 08:41:12 à 08:45:10, heure locale

L'extrait ne montre aucune authentification réussie depuis cette adresse.

> ✓ **RÉPONSE À RETENIR**
>
> 5 échecs SSH pour le compte admin depuis 203.0.113.77, le 18 juin 2026 de 08:41:12 à 08:45:10.

Vérification de l'origine et de l'impact

Question 3.2. Le journal indique que les tentatives proviennent d'une adresse absente du plan d'adressage interne. Expliquez pourquoi cette observation ne suffit pas à prouver que l'adresse est malveillante, puis citez deux vérifications permettant de confirmer l'origine et l'impact des tentatives.

L'absence de `203.0.113.77` du plan interne signifie seulement que l'adresse n'est pas attribuée à un équipement interne. Elle peut provenir d'un accès externe autorisé, d'un VPN ou d'une traduction NAT. Dans cet extrait, les adresses peuvent aussi être anonymisées ou réservées à la documentation : cela ne prouve pas une activité malveillante.

- Vérifier l'origine dans les journaux du pare-feu, du VPN et les règles NAT, puis confronter le flux aux accès d'administration autorisés.
- Examiner les journaux SSH et système pour repérer une authentification réussie, une session ouverte ou des actions effectuées après les tentatives.

> ✓ **RÉPONSE À RETENIR**
>
> Contrôler l'origine dans les journaux pare-feu/VPN/NAT et rechercher une connexion SSH réussie ou des actions associées sur le serveur.

Mesures de durcissement

Question 3.3. Proposez trois mesures de durcissement adaptées à la situation, comprenant au moins une mesure relative au compte ou à l'authentification et une mesure portant sur l'exposition réseau du service. Pour chacune, indiquez le risque réduit et veillez à ne pas préconiser une action pouvant couper sans contrôle l'accès d'administration légitime.

Appliquer ces mesures progressivement, après vérification et test d'un accès d'administration légitime de secours.

1. **Authentification :** imposer les clés SSH et, si disponible, une authentification multifacteur. Ne désactiver l'accès direct au compte `admin` qu'après validation d'un compte nominatif de secours. Risque réduit : compromission par mot de passe.
2. **Exposition réseau :** limiter SSH au VPN ou aux adresses d'administration vérifiées, en conservant une voie de secours testée. Risque réduit : tentatives non autorisées depuis d'autres réseaux.
3. **Tentatives répétées :** mettre en place une temporisation ou un blocage progressif après plusieurs échecs, avec seuils contrôlés et procédure de déblocage. Risque réduit : attaques par essais répétés, sans verrouillage brutal des comptes légitimes.

> **✓ RÉPONSE À RETENIR**
>
> Renforcer l'authentification, restreindre SSH aux accès d'administration vérifiés et limiter progressivement les tentatives, après test d'un accès de secours.

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

Bilan de l'épreuve : L'évaluation de compétence C2 du BUT Réseaux et Télécommunications, session 2026, code 26-BUT-RT-EP1, dure 2 heures et porte un coefficient indicatif de 3,0. Dans le contexte du réseau de Novalys Services, elle évalue l'adressage et le routage IPv4 et IPv6, l'interrogation SQL, le traitement de journaux avec Bash, le diagnostic d'authentification SSH et le choix de mesures de sécurisation.

Notions-clés, formules & règles à maîtriser

- Le nombre d'hôtes IPv4 utilisables d'un sous-réseau classique est 2^(32 - préfixe) - 2.
- Une route directement connectée sort par l'interface du réseau local concerné ; la route par défaut utilise le prochain saut configuré.
- Une jointure relie des tables sur leurs clés ; une jointure externe gauche conserve aussi les équipements sans incident.
- grep filtre les lignes correspondant à un motif ; wc -l permet de compter les lignes filtrées.

Points de vigilance & attentes du jury

- Vérifier que le sous-réseau choisi fournit assez d'adresses utilisables, passerelle comprise.
- Pour un préfixe IPv6 /64, comparer les 64 premiers bits de l'adresse du poste et de la passerelle.
- Dans une requête de comptage, conserver les équipements sans incident et trier selon le nombre demandé.
- Distinguer faits observés et hypothèses dans le signalement, puis préserver un accès d'administration contrôlé.

Questions fréquentes sur cette épreuve (Q&A Examen)

Q : Comment choisir le préfixe IPv4 minimal pour des postes et une passerelle ?

Additionnez les hôtes nécessaires, passerelle comprise, puis choisissez le plus petit nombre de bits d'hôtes h tel que 2^h - 2 couvre ce total. Le préfixe est 32 - h ; calculez ensuite masque, réseau, diffusion et plage utilisable.

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

Partez de Devices et effectuez une jointure externe gauche vers Incidents sur device_id. Comptez une colonne d'incident non nulle, regroupez par équipement, puis triez selon le total décroissant.

Q : Comment gérer le temps dans cette épreuve de deux heures ?

Répartissez le temps entre les trois parties en tenant compte de leurs points : 7, 6 et 7. Commencez par les tâches maîtrisées, gardez du temps pour le DR 1 et relisez les réponses et justifications.

Q : Que doit contenir un signalement pour être évalué comme factuel ?

Relevez uniquement les éléments observables : service, source, nombre d'échecs et horaires. Distinguez-les des hypothèses, proposez des vérifications adaptées et justifiez les mesures de sécurité par le risque réduit.

Sujet officiel associé (PDF) : https://butrt.fr/assets/annales/but-rt/C2 - Assister l'administrateur du réseau/2026/BUT Réseaux et Télécommunications - C2 - Assister l'administrateur du réseau - 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.