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-EP1** • Durée : **3 heures** • Coefficient : **3,0 (indicatif)**

Sommaire

Cliquez sur une partie pour y accéder directement

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

2. Base de données et requêtes SQL (3 questions) **Page 5**

3. Cybersécurité, analyse de journaux et durcissement (3 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/C4 - Concevoir un réseau/2026/BUT Réseaux et Télécommunications - C4 - Concevoir un réseau - Session 2026 - 1-Sujet.pdf

1. Architecture réseau, adressage et routage

Novalys Médical relie son siège de Lyon et son agence de Grenoble par un lien point à point, avec des VLAN dédiés aux postes, serveurs, téléphones IP et à l'administration. Les documents techniques donnent la topologie, les besoins, les préfixes IPv4 et IPv6, ainsi que les réseaux distants à joindre.

Question 1.1. Pour le VLAN 10 et le préfixe 10.24.0.0/25, déterminer le masque décimal pointé, l'adresse de diffusion, la plage complète des adresses utilisables et leur nombre maximal.

Élément	Valeur
Masque	255.255.255.128
Adresse de diffusion	10.24.0.127
Plage utilisable	10.24.0.1 à 10.24.0.126
Nombre maximal d'adresses utilisables	126

Un préfixe /25 laisse 7 bits pour les hôtes, soit 128 adresses au total. Le réseau est 10.24.0.0 et l'adresse de diffusion est 10.24.0.127. Les 126 adresses intermédiaires sont utilisables, passerelle comprise. Comme la première adresse utilisable est réservée à la passerelle, 125 adresses restent disponibles pour les autres équipements du VLAN.

> ✓ **RÉPONSE À RETENIR**
>
> Masque : 255.255.255.128 ; diffusion : 10.24.0.127 ; plage utilisable : 10.24.0.1 à 10.24.0.126, soit 126 adresses.

Question 1.2. Pour le VLAN 20 et le préfixe 10.24.0.128/26, déterminer l'adresse de diffusion, la première et la dernière adresse utilisables, puis vérifier si le sous-réseau peut accueillir les 40 serveurs indiqués dans le DT 1.

Le préfixe /26 comprend 64 adresses. Le bloc va de 10.24.0.128 à 10.24.0.191 : la première est l'adresse réseau et la dernière l'adresse de diffusion. Les adresses utilisables vont donc de 10.24.0.129 à 10.24.0.190, soit 62 adresses, passerelle comprise. La passerelle occupe la première adresse utilisable, laissant 61 adresses aux serveurs. Le réseau accueille donc les 40 serveurs et conserve 21 adresses pour d'autres équipements.

> ✓ **RÉPONSE À RETENIR**
>
> Diffusion : 10.24.0.191 ; adresses utilisables : 10.24.0.129 à 10.24.0.190. Après réservation de la passerelle, 61 adresses restent disponibles pour les 40 serveurs.

Question 1.3. **Compléter dans le DR 1 les routes statiques IPv4 manquantes de R-LYON et R-GRENOBLE. Pour chaque route, préciser le préfixe de destination et le prochain saut, en tenant compte des liaisons directement connectées déjà présentes.**

Routeur	Préfixe de destination	Prochain saut
R-LYON	10.24.1.0/24	10.24.0.242
R-GRENOBLE	10.24.0.0/24	10.24.0.241

Chaque route vise le réseau distant agrégé en /24. Le prochain saut est l'adresse de l'autre routeur sur le lien point à point : R-GRENOBLE utilise 10.24.0.242 et R-LYON utilise 10.24.0.241. Les réseaux directement connectés sont déjà présents dans les tables, donc aucune route supplémentaire n'est à ajouter pour eux.

Routes statiques complétées dans le DR 1

Routes statiques IPv4 à renseigner

Routeur	Préfixe de destination	Prochain saut
R-LYON	10.24.1.0/24	10.24.0.242 .....
R-GRENOBLE	10.24.0.0/24	10.24.0.241 .....

Une ligne par route statique à installer

> **✓ RÉPONSE À RETENIR**
>
> R-LYON : 10.24.1.0/24 via 10.24.0.242. R-GRENOBLE : 10.24.0.0/24 via 10.24.0.241.

Question 1.4. **À partir des préfixes IPv6 du DT 1, donner l'adresse IPv6 de la passerelle du VLAN 110, puis déterminer si 2001:db8:24:1:10::25 appartient au préfixe de ce VLAN. Justifier en indiquant le préfixe réseau commun utilisé pour la comparaison.**

Le préfixe du VLAN 110 est `2001:db8:24:1:10::/64`. Le document précise que la passerelle IPv6 de chaque VLAN se termine par `::1`. Pour tester l'appartenance, on compare les 64 premiers bits, soit les quatre premiers groupes hexadécimaux. Ils sont identiques pour le préfixe et l'adresse proposée : `2001:db8:24:1`. Les groupes suivants appartiennent à la partie hôte et ne changent pas le résultat de la comparaison.

- La passerelle est `2001:db8:24:1:10::1`.
- L'adresse donnée appartient au préfixe du VLAN 110.

> **✓ RÉPONSE À RETENIR**
>
> Passerelle : 2001:db8:24:1:10::1. L'adresse appartient au préfixe 2001:db8:24:1:10::/64, dont les 64 bits réseau communs sont 2001:db8:24:1.

2. Base de données et requêtes SQL

Le service informatique veut produire des indicateurs par site à partir de la base relationnelle de suivi des incidents de Novalys Médical. Le DT 2 présente les tables SITE, TECH et INCIDENT, leurs relations et un extrait de données.

Question 2.1. Écrire une requête SQL standard qui relie les tables SITE et TECH, sélectionne le nom de chaque site et dénombre les techniciens qui y sont rattachés. Le résultat doit comporter une ligne par site et être ordonné par nom de site dans l'ordre alphabétique.

La jointure relie chaque technicien à son site par `id_site`. Le `LEFT JOIN` conserve aussi les sites sans technicien, et `COUNT(T.id_tech)` ne compte pas les lignes sans technicien. Le regroupement par identifiant et nom garantit une ligne par site, puis le tri alphabétique classe les noms.

```
SELECT S.nom, COUNT(T.id_tech) AS nombre_techniciens
FROM SITE S
LEFT JOIN TECH T ON T.id_site = S.id_site
GROUP BY S.id_site, S.nom
ORDER BY S.nom ASC;
```

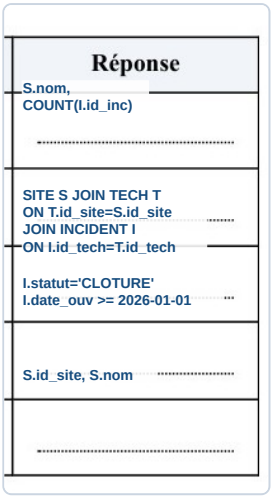
> **✓ RÉPONSE À RETENIR**
>
> Grenoble : 1 technicien. Lyon : 2 techniciens.

Question 2.2. Compléter dans le DR 1 la requête SQL qui joint SITE, TECH et INCIDENT, filtre les incidents dont le statut est CLOTURE et dont la date d'ouverture est postérieure ou égale au 1er janvier 2026, puis regroupe les résultats par site.

Les clés étrangères relient les trois tables de SITE à TECH, puis de TECH à INCIDENT. Le filtre inclut les incidents clôturés ouverts le 1er janvier 2026 ou après. Le regroupement par site permet d'obtenir un décompte distinct pour chaque site.

```
SELECT S.nom, COUNT(I.id_inc) AS nombre_incidents
FROM SITE S
JOIN TECH T ON T.id_site = S.id_site
JOIN INCIDENT I ON I.id_tech = T.id_tech
WHERE I.statut = 'CLOTURE'
  AND I.date_ouv >= DATE '2026-01-01'
GROUP BY S.id_site, S.nom;
```

DR 1 complété, éléments SQL de la question 2.2



✓ RÉPONSE À RETENIR

La requête compte les incidents clôturés ouverts depuis le 1er janvier 2026 inclus, par site.

Question 2.3. Ajouter à la requête de la question 2.2 la condition qui ne conserve que les sites ayant au moins deux incidents correspondants. Indiquer la clause SQL à utiliser et le test d'agrégation complet.

La clause `HAVING` s'applique aux groupes après le `GROUP BY`, tandis que `WHERE` filtre les incidents avant le décompte. Le test complet porte sur l'identifiant de l'incident, qui est non nul pour chaque ligne comptée :

```
HAVING COUNT(I.id_inc) >= 2
```

Dans les données fournies, Lyon a deux incidents qui satisfont les filtres, contre un pour Grenoble.

DR 1 complété, condition HAVING de la question 2.3



✓ RÉPONSE À RETENIR

Après le `GROUP BY` : `HAVING COUNT(I.id_inc) >= 2`. Seul Lyon est retenu.

3. Cybersécurité, analyse de journaux et durcissement

Les journaux du serveur d'authentification et du pare-feu du siège montrent des tentatives SSH depuis une adresse Internet, puis des événements d'authentification et des connexions acceptées sur le port 22. Les documents précisent la signification des événements, l'ordre d'application des règles du pare-feu et la synchronisation des horodatages.

Question 3.1. À partir des journaux du DT 2, relever l'adresse source des tentatives répétées, le compte visé et le résultat de la tentative d'accès enregistrée à 09:18:43. Citer les événements justificatifs et établir la durée entre la première tentative et cet accès.

Les journaux SSH indiquent trois échecs pour le compte **admin**, depuis **198.51.100.77**, à 09:16:02, 09:16:19 et 09:17:05. À 09:18:43, l'événement « Accepted password for admin » confirme que l'authentification par mot de passe a réussi. Entre le premier échec et cette authentification réussie, il s'écoule 2 min 41 s : 18 min 43 s moins 16 min 02 s, soit 161 secondes. Les événements attestent une connexion réussie, mais ne suffisent pas à établir ce qui a été fait après l'accès.

> ✓ RÉPONSE À RETENIR
>
> Source : 198.51.100.77 ; compte visé : admin ; authentification réussie à 09:18:43, après 2 min 41 s.

Question 3.2. Qualifier l'incident au vu des éléments disponibles et indiquer deux actions immédiates de traitement, l'une sur le compte et l'autre sur l'accès réseau. Pour chacune, préciser le risque réduit.

Les échecs répétés suivis d'une authentification SSH réussie depuis une source Internet signalent une **compromission probable** du compte. Les connexions au port 22 ensuite acceptées par le pare-feu, à 09:19:10 et 09:22:31, renforcent le soupçon d'accès non autorisé.

- **Compte :** désactiver admin, réinitialiser son mot de passe et fermer ses sessions actives afin d'empêcher la réutilisation des identifiants.
- **Accès réseau :** bloquer la source 198.51.100.77 et suspendre l'accès SSH depuis Internet afin d'interrompre les connexions distantes suspectes.

> ✓ RÉPONSE À RETENIR
>
> Compromission probable : désactiver et sécuriser le compte admin, puis bloquer la source et suspendre l'accès SSH depuis Internet.

Question 3.3. Proposer deux mesures préventives de durcissement pour l'administration distante du serveur. Elles doivent être distinctes des actions immédiates de la question 3.2 et adaptées aux informations du DT 2.

Les journaux montrent que l'authentification SSH par mot de passe et l'accès au port 22 depuis Internet sont possibles. Deux mesures préventives adaptées, distinctes du blocage immédiat de la source observée, sont :

1. Désactiver l'authentification SSH par mot de passe et imposer des clés cryptographiques ainsi qu'une authentification multifacteur, pour réduire les risques liés au vol ou au devinement des identifiants.

2. Faire passer l’administration par un VPN ou un bastion dédié, avec des règles d’accès limitées aux sources autorisées, sans exposer directement le port 22 à Internet.

> **✓ RÉPONSE À RETENIR**
>
> SSH par clés avec authentification multifacteur ; administration via VPN ou bastion autorisé, sans exposition directe du port 22.

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

Bilan de l'épreuve : Cette évaluation C4 de la session 2026, code 26-BUT-RT-EP1, dure 3 heures et porte un coefficient indicatif de 3,0. Elle étudie le réseau multi-sites de Novalys Médical, son adressage IPv4 et IPv6, ses routes, sa base de données d'incidents et ses journaux de sécurité. Les compétences évaluées couvrent le calcul réseau, SQL, l'analyse d'incident et le durcissement.

Notions-clés, formules & règles à maîtriser

- Pour un préfixe IPv4 /n, le nombre d'adresses hôtes utilisables est 2^(32-n) - 2, hors adresse réseau et adresse de diffusion.
- La première adresse utilisable est réservée à la passerelle : retranchez-la du nombre d'adresses disponibles pour les équipements.
- En SQL, WHERE filtre les lignes, GROUP BY forme les groupes et HAVING filtre les groupes selon un résultat agrégé.
- Un journal SSH « Accepted password » indique une authentification réussie, tandis que « Failed password » indique un échec.

Points de vigilance & attentes du jury

- Vérifier les bornes du sous-réseau et ne pas attribuer l'adresse réseau ni l'adresse de diffusion.
- Pour chaque route statique, distinguer le préfixe du réseau distant du prochain saut sur le lien intersite.
- Dans les jointures SQL, suivre les clés étrangères et regrouper par site avant d'appliquer le seuil d'incidents.
- Ne pas confondre une authentification SSH réussie et une action pare-feu ACCEPT, qui indique l'acceptation du paquet.

Questions fréquentes sur cette épreuve (Q&A Examen)

Q : Comment trouver rapidement les adresses utilisables d'un sous-réseau IPv4 ?

Le préfixe donne le nombre de bits hôte : 32 moins la longueur du préfixe. Calculez le nombre total d'adresses, retirez l'adresse réseau et l'adresse de diffusion, puis identifiez les deux bornes utilisables.

Q : Quelle différence y a-t-il entre WHERE et HAVING dans une requête SQL ?

WHERE filtre les lignes avant le regroupement, par exemple selon le statut ou la date. HAVING filtre les groupes après GROUP BY et permet de tester un résultat agrégé, comme un nombre minimal d'incidents.

Q : Comment déterminer le délai entre la première tentative et une authentification réussie ?

Relevez les deux horodatages concernés dans les journaux synchronisés, puis soustrayez l'heure de la première tentative de celle de l'authentification réussie. Ici, de 09:16:02 à 09:18:43, le délai est de 2 minutes et 41 secondes.

Q : Quelles attentes de notation sont indiquées pour les parties de cette épreuve ?

Le sujet attribue 8 points à l'architecture, l'adressage et le routage, 6 points aux requêtes SQL et 6 points à la cybersécurité. Il demande des réponses justifiées lorsque précisé et ne fournit pas de barème détaillé par sous-critère.

Sujet officiel associé (PDF) : https://butrt.fr/assets/annales/but-rt/C4 - Concevoir un réseau/2026/BUT Réseaux et Télécommunications - C4 - Concevoir un 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.