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 : **2 h 30** • Coefficient : **3,0**
(pondération indicative locale)

Sommaire

Cliquez sur une partie pour y accéder directement

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

2. Exploitation de la base de données des incidents (3 questions) **Page 6**

3. Analyse d'incident et durcissement de la sécurité (4 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/C3 - Administrer un réseau/2026/BUT Réseaux et Télécommunications - C3 - Administrer un réseau - Session 2026 - 1-Sujet.pdf

1. Architecture réseau, adressage et routage

Novalys Médical prépare la création des réseaux internes de Lyon et l'adressage du lien avec Grenoble à partir des besoins en hôtes, des VLAN et des préfixes IPv6 fournis. Il faut aussi préciser la segmentation, puis compléter les routes de SW-LYO à partir de la topologie et des paramètres OSPF.

Question 1.1. À partir du bloc IPv4 10.24.0.0/24, dimensionner les cinq sous-réseaux du tableau du plus grand besoin au plus petit. Pour chacun, donner le préfixe CIDR, le masque décimal, l'adresse réseau, la première et la dernière adresse utilisables ainsi que l'adresse de diffusion. Affecter les sous-réseaux successivement à partir de la plus petite adresse disponible, sans chevauchement.

Pour chaque besoin, on choisit le plus petit sous-réseau dont le nombre d'adresses utilisables est suffisant, puis on attribue les blocs dans l'ordre demandé. Les deux réseaux de 60 et 50 hôtes nécessitent chacun un /26. Les blocs suivants commencent à la première adresse disponible après le bloc précédent, en respectant l'alignement des préfixes.

Réseau	Préfixe	Masque	Adresse réseau	Première utilisable	Dernière utilisable	Diffusion
Utilisateurs, VLAN 20	/26	255.255.255.192	10.24.0.0	10.24.0.1	10.24.0.62	10.24.0.63
Serveurs, VLAN 30	/26	255.255.255.192	10.24.0.64	10.24.0.65	10.24.0.126	10.24.0.127
Administration, VLAN 10	/27	255.255.255.224	10.24.0.128	10.24.0.129	10.24.0.158	10.24.0.159
Invités, VLAN 40	/28	255.255.255.240	10.24.0.160	10.24.0.161	10.24.0.174	10.24.0.175
Lien Lyon-Grenoble	/30	255.255.255.252	10.24.0.176	10.24.0.177	10.24.0.178	10.24.0.179

Les capacités utilisables sont respectivement de 62, 62, 30, 14 et 2 adresses. Aucun bloc ne chevauche le suivant.

> **✓ RÉPONSE À RETENIR**
>
> 10.24.0.0/26, 10.24.0.64/26, 10.24.0.128/27, 10.24.0.160/28 et 10.24.0.176/30.

Question 1.2. Pour les VLAN 20, 30, 10 et 40, indiquer l'adresse IPv4 de passerelle selon la règle donnée et proposer l'adresse IPv6 de passerelle ::1 dans chaque préfixe attribué. Indiquer également le préfixe IPv6 utilisé pour le lien Lyon-Grenoble et les deux adresses d'interface choisies dans ce préfixe.

Chaque passerelle IPv4 reprend la première adresse hôte de son sous-réseau. Pour IPv6, l'adresse de passerelle demandée est ::1 dans le préfixe attribué à chaque VLAN. Le lien Lyon-Grenoble utilise le préfixe fourni et reçoit deux adresses d'interface distinctes, une pour chaque extrémité.

VLAN ou lien	Adresse IPv4	Adresse IPv6
VLAN 20, utilisateurs	10.24.0.1	2001:db8:24:20::1/64
VLAN 30, serveurs	10.24.0.65	2001:db8:24:30::1/64
VLAN 10, administration	10.24.0.129	2001:db8:24:10::1/64
VLAN 40, invités	10.24.0.161	2001:db8:24:40::1/64
Lien Lyon-Grenoble	Non demandé	Préfixe 2001:db8:24:ff::/64; Lyon : 2001:db8:24:ff::1/64; Grenoble : 2001:db8:24:ff::2/64

✓ RÉPONSE À RETENIR

Passerelles IPv4 : 10.24.0.1, .65, .129 et .161. Passerelles IPv6 : ::1 dans chaque VLAN. Lien : 2001:db8:24:ff::/64, avec ::1 à Lyon et ::2 à Grenoble.

Question 1.3. Le commutateur cœur SW-LYO assure le routage inter-VLAN. Préciser les informations nécessaires sur un port d'accès destiné à un poste du VLAN 20 et sur le lien trunk entre SW-LYO et le pare-feu FW-LYO. Indiquer les VLAN autorisés sur ce trunk et expliquer pourquoi le VLAN de gestion ne doit pas être confondu avec le VLAN des utilisateurs.

Le port destiné au poste doit être configuré en accès et affecté au VLAN 20. Le lien entre SW-LYO et FW-LYO doit transporter plusieurs VLAN : il est donc configuré en trunk 802.1Q aux deux extrémités, avec une liste de VLAN autorisés limitée à ceux prévus. Le VLAN 10 est réservé à l'administration des équipements; le séparer du VLAN utilisateurs réduit les possibilités d'accès non autorisé aux interfaces de gestion.

1. Port du poste : mode accès, VLAN 20.
2. Lien SW-LYO vers FW-LYO : trunk 802.1Q, VLAN autorisés 10, 20, 30 et 40.
3. Gestion : VLAN 10 distinct du VLAN 20 des utilisateurs.

✓ RÉPONSE À RETENIR

Port d'accès : VLAN 20. Trunk 802.1Q : VLAN 10, 20, 30 et 40 autorisés. VLAN 10 réservé à la gestion.

Question 1.4. Le routage entre les équipements de couche 3 est assuré par OSPF, aire 0. À partir du DT 1, compléter dans le DR 1 la table de routage de SW-LYO pour le réseau de Grenoble et la route par défaut. Indiquer le prochain saut de chaque route et expliquer brièvement comment le réseau de Grenoble est appris par OSPF.

R-GRE annonce le réseau 192.168.50.0/24 dans OSPF, aire 0. La route est apprise par SW-LYO avec le chemin retenu via FW-LYO; son prochain saut est donc 10.24.255.1, sur le lien de transit. La route par défaut est configurée sur SW-LYO vers ce même prochain saut. Les deux entrées et leurs types sont indiqués dans le DR 1 complété ci-dessous.

DR 1 complété, table de routage de SW-LYO

Table de routage de SW-LYO à compléter

Destination	Type ou source de la route	Prochain saut	Interface de sortie
192.168.50.0/24	OSPF, aire 0	10.24.255.1	Lien de transit vers FW-LYO
0.0.0.0/0	Route statique	10.24.255.1	Lien de transit vers FW-LYO

✓ RÉPONSE À RETENIR

192.168.50.0/24 : OSPF, prochain saut 10.24.255.1. 0.0.0.0/0 : route statique, prochain saut 10.24.255.1.

2. Exploitation de la base de données des incidents

Le service informatique de Novalys Médical suit les équipements et leurs incidents dans une base relationnelle dont le schéma et les données extraites sont fournis. Les tâches portent sur des requêtes SQL avec jointures, filtres, agrégats et prise en compte des sites sans incident correspondant.

Question 2.1. Écrire une requête SQL qui affiche, pour chaque incident de sévérité HAUTE encore au statut OUVERT, l'identifiant de l'incident, sa date et heure, le nom de l'équipement et son site. La requête doit utiliser une jointure entre les deux tables et trier les résultats du plus récent au plus ancien.

La jointure relie chaque incident à son équipement par la clé étrangère. Les filtres gardent les incidents de sévérité HAUTE au statut OUVERT ; le tri décroissant place les plus récents en premier.

```
SELECT i.id, i.date_heure, e.nom, e.site
FROM incident AS i
JOIN equipement AS e ON i.equipement_id = e.id
WHERE i.severite = 'HAUTE'
  AND i.statut = 'OUVERT'
ORDER BY i.date_heure DESC;
```

✓ **RÉPONSE À RETENIR**

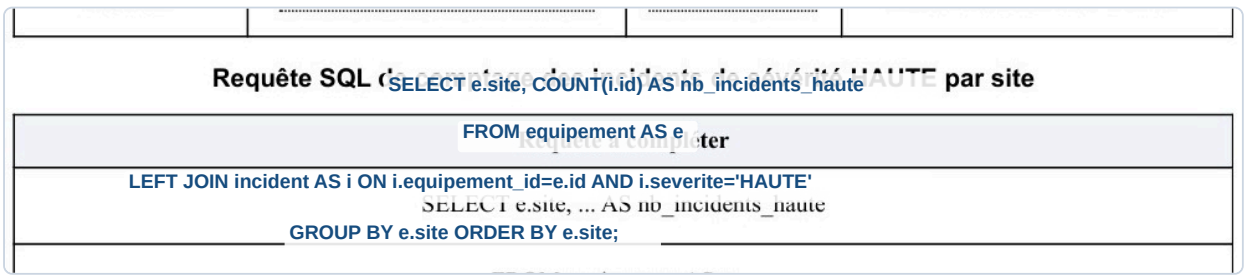
Incidents correspondants, du plus récent au plus ancien : 505, 502, 501.

Question 2.2. Écrire une requête SQL qui donne, pour chaque site, le nombre d'incidents de sévérité HAUTE enregistrés dans l'extrait du DT 2. Le résultat doit contenir les colonnes site et nb_incidents_haute, inclure également les sites pour lesquels ce nombre est nul et être trié par nom de site. Compléter la requête dans le DR 1.

Le `LEFT JOIN` conserve chaque site. Le filtre de sévérité reste dans la jointure pour inclure les sites sans incident HAUTE ; `COUNT(i.id)` leur attribue zéro. Le regroupement et le tri portent sur le site.

```
SELECT e.site, COUNT(i.id) AS nb_incidents_haute
FROM equipement AS e
LEFT JOIN incident AS i
  ON i.equipement_id = e.id AND i.severite = 'HAUTE'
GROUP BY e.site
ORDER BY e.site;
```

Requête SQL complétée dans le DR 1



✓ RÉPONSE À RETENIR

Grenoble : 1 incident HAUTE ; Lyon : 3 incidents HAUTE, dans cet ordre alphabétique.

Question 2.3. À partir des lignes fournies dans le DT 2, indiquer le nombre d'incidents ouverts de sévérité HAUTE au site de Lyon. Justifier le résultat par les filtres appliqués aux tables incident et equipement.

On filtre les incidents sur `severite = 'HAUTE'` et `statut = 'OUVERT'`, puis on joint `equipement` pour retenir le site de Lyon. Les incidents 501 et 502 satisfont ces critères ; le 506 est exclu car il est CLOS.

✓ RÉPONSE À RETENIR

2 incidents : 501 et 502 sont HAUTE et OUVERT, associés à des équipements du site de Lyon.

3. Analyse d’incident et durcissement de la sécurité

Une activité inhabituelle provenant du poste 10.24.0.131 est détectée en direction du serveur de fichiers FS-LYO. Les journaux système, le journal du pare-feu et une capture réseau servent à reconstituer les événements, interpréter les échanges et proposer des règles de filtrage et des mesures de durcissement.

Question 3.1. En vous appuyant sur les événements syslog et les paquets de la capture, reconstituer la chronologie de l’incident en trois étapes au minimum. Identifier l’équipement source, le serveur visé, les services sollicités et les éléments qui permettent de qualifier l’activité d’anormale.

1. **09:14:02 :** le poste `10.24.0.131` envoie des SYN vers FS-LYO (`10.24.0.66`) en TCP/22. Syslog signale plusieurs tentatives SSH avec des comptes différents.
2. **09:14:19 :** l’authentification SSH est refusée, car le compte utilisé n’existe pas.
3. **09:15:11 :** le poste tente TCP/445. Le pare-feu journalise un refus inter-VLAN ; la capture montre un RST, ACK.
4. **09:16:03 puis 09:19:44 :** SW-LYO détecte une adresse MAC non inventoriée sur un port du VLAN 20, puis la supervision signale une hausse des connexions vers le VLAN 30.

Les essais avec plusieurs comptes, la sollicitation de deux services et l’équipement non inventorié rendent l’activité suspecte.

> **✓ RÉPONSE À RETENIR**
>
> `10.24.0.131` cible FS-LYO en SSH puis en SMB ; comptes multiples, refus inter-VLAN et MAC inconnue signalent une activité anormale.

Question 3.2. La capture montre un SYN vers TCP/22 sans réponse visible, puis une tentative vers TCP/445 suivie d’un RST, ACK. Expliquer ce que permettent de conclure ces observations et préciser une limite de l’analyse d’une capture réalisée sur un seul point du réseau.

Le SYN retransmis vers TCP/22 sans réponse visible ne prouve pas qu’une connexion SSH a été établie. Il peut s’agir d’un filtrage, d’une perte de paquets ou d’une réponse absente de l’extrait. Le syslog confirme néanmoins des tentatives d’authentification, toutes deux refusées.

Le RST, ACK vers TCP/445 indique que la tentative SMB a été réinitialisée ; aucun échange SMB établi n’est montré. Le pare-feu journalise un refus, mais la capture attribue le RST à l’adresse de FS-LYO : on ne peut donc déterminer avec certitude qui l’a émis. Une capture sur un seul point ne montre pas tout le trajet ni ne localise sûrement le filtrage.

> **✓ RÉPONSE À RETENIR**
>
> SSH : aucune connexion établie visible, malgré les tentatives confirmées par syslog. SMB : tentative réinitialisée. La capture ne permet pas d’identifier sûrement l’émetteur du RST ni le point de filtrage.

Question 3.3. **Proposer une règle de filtrage qui autorise l'administration SSH du serveur FS-LYO uniquement depuis le poste d'administration 10.24.0.130, tout en interdisant aux postes utilisateurs l'accès SSH et SMB aux serveurs. Indiquer les adresses, les protocoles ou ports et l'ordre logique des règles. Le pare-feu applique une politique implicite de refus.**

Ordre	Action	Source	Destination	Protocole
1	Autoriser	`10.24.0.130`	FS-LYO `10.24.0.66`	TCP/22
2	Refuser	VLAN 20, préfixe prévu `10.24.0.0/26`	VLAN 30, préfixe `10.24.0.64/26`	TCP/22 et TCP/445
3	Refus implicite	Toutes les autres sources	Toutes destinations	Tous

L'autorisation SSH ciblée précède les refus. Attention : selon le plan d'adressage, `10.24.0.131` appartient au VLAN 10 (`10.24.0.128/27`), alors que le journal SW-LYO situe ce poste sur le VLAN 20. Il faut vérifier cette incohérence et appliquer le refus utilisateurs selon le VLAN réel, pas uniquement selon l'adresse IP.

> **✓ RÉPONSE À RETENIR**
>
> Autoriser `10.24.0.130` vers `10.24.0.66` en TCP/22, puis bloquer le VLAN 20 vers le VLAN 30 en TCP/22 et TCP/445 ; appliquer le refus implicite au reste.

Question 3.4. **Formuler trois mesures complémentaires de durcissement adaptées à l'incident. Les propositions doivent couvrir au moins deux domaines parmi la gestion des comptes, la journalisation et la supervision, le cloisonnement réseau, la sécurisation des postes et la réponse à incident. Pour chaque mesure, préciser brièvement le risque qu'elle réduit.**

- **Comptes :** privilégier les comptes nominatifs, les clés SSH et l'authentification multifacteur ; limiter les essais. Cela réduit les attaques par identifiants et l'usurpation de comptes.
- **Supervision :** centraliser les journaux SSH, pare-feu et commutateurs, avec des alertes sur les échecs répétés et les scans. Cela accélère la détection et facilite l'analyse.
- **Cloisonnement et réponse :** limiter les flux inter-VLAN et prévoir l'isolement rapide des postes non inventoriés. Cela réduit les déplacements latéraux et la propagation d'une compromission.

> **✓ RÉPONSE À RETENIR**
>
> Renforcer les comptes, centraliser les journaux avec des alertes, et cloisonner les VLAN avec une procédure d'isolement des postes suspects.

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

Bilan de l'épreuve : Cette évaluation BUT R&T, session 2026, code 26-BUT-RT-EP1, dure 2 h 30 et porte un coefficient indicatif local de 3,0. Dans le contexte de Novalys Médical, elle évalue l'adressage IPv4 et IPv6, les VLAN et le routage OSPF, les requêtes SQL sur les incidents, l'analyse de journaux et de captures réseau, ainsi que le filtrage et le durcissement de la sécurité.

Notions-clés, formules & règles à maîtriser

- Un sous-réseau IPv4 de préfixe /p contient 2^(32-p) adresses; réserver l'adresse réseau et l'adresse de diffusion pour le dimensionnement demandé.
- Le routage inter-VLAN s'appuie sur des interfaces de couche 3, tandis qu'un trunk transporte plusieurs VLAN entre équipements.
- Pour compter les incidents par site en conservant les sites sans correspondance, utiliser une jointure externe gauche et compter les identifiants d'incident.
- Un SYN sans réponse visible ne prouve pas à lui seul que le service est fermé; un RST, ACK signale un refus ou une connexion non acceptée à cette destination.

Points de vigilance & attentes du jury

- Dimensionner les sous-réseaux du plus grand besoin au plus petit et vérifier qu'ils ne se chevauchent pas dans le bloc attribué.
- Distinguer la route OSPF vers Grenoble de la route par défaut et utiliser les prochains sauts indiqués dans le DT 1.
- Pour conserver les sites ayant zéro incident, éviter de filtrer après la jointure externe les lignes sans incident correspondant.
- Ordonner les règles de pare-feu pour autoriser SSH depuis le seul poste d'administration et appliquer les refus ciblés aux postes utilisateurs.

Questions fréquentes sur cette épreuve (Q&A Examen)

Q : Comment dimensionner les sous-réseaux IPv4 demandés ?

Pour chaque besoin, choisir le plus petit bloc dont le nombre d'adresses utilisables suffit, en réservant réseau et diffusion. Classer les besoins du plus grand au plus petit, puis attribuer les blocs à partir de la première adresse disponible sans chevauchement.

Q : Que peut-on déduire d'un SYN retransmis sans réponse et d'un RST, ACK ?

Le SYN retransmis sans réponse visible indique seulement qu'aucune réponse n'apparaît dans cet extrait. Le RST, ACK reçu en réponse à TCP/445 signale que la connexion n'est pas acceptée à cette destination, sans déterminer à lui seul si le rejet vient du service ou d'un équipement.

Q : Comment gérer le temps et le barème de cette épreuve ?

Le sujet indique une durée de 2 h 30 et un coefficient de 3,0 à pondération indicative locale. Les parties valent respectivement 7, 6 et 7 points; répartissez le temps selon ces poids et gardez du temps pour vérifier les réponses et le DR 1.

Q : Quelles précautions de présentation et de notation faut-il retenir ?

Le sujet demande des réponses justifiées lorsque nécessaire, les alias SQL et tris demandés, ainsi que le DR 1 rendu avec la copie. Toute hypothèse ajoutée doit être explicitement justifiée; aucun barème plus détaillé n'est imprimé.

Sujet officiel associé (PDF) : https://butrt.fr/assets/annales/but-rt/C3 - Administrer un réseau/2026/BUT Réseaux et Télécommunications - C3 - Administrer 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.