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

BTS CIEL

Exploitation et maintenance de réseaux informatiques

Session 2026 • Code sujet : **26-BTS-CIEL-A-E5** • Durée : **3 heures** • Coefficient : **3**

Sommaire

Cliquez sur une partie pour y accéder directement

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

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

3. **Cybersécurité, analyse de traces et durcissement** (4 questions) **Page 8**

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

Sujet officiel (PDF) : https://coursbtsciel.fr/assets/annales/bts-ciel/E5 - Exploitation et maintenance de réseaux informatiques/2026/BTS CIEL - E5 - Exploitation et maintenance de réseaux informatiques - Session 2026 - 1-Sujet.pdf

1. Architecture réseau, adressage et routage

Le site Novalys Services de Valence est organisé en VLAN pour les utilisateurs, l'administration, les serveurs et la gestion des équipements. À partir de la topologie et du plan d'adressage, il faut vérifier les sous-réseaux IPv4 et IPv6 ainsi que les routes de R1.

Question 1.1. À partir du DT 1, décrire le rôle du VLAN 30 et du lien trunk entre SW1 et R1. Expliquer pourquoi le routage inter-VLAN est nécessaire pour qu'un poste du VLAN 10 communique avec le serveur du VLAN 30.

Le VLAN 30 regroupe les serveurs, dont le serveur applicatif et DNS. Le lien trunk entre SW1 et R1 transporte simultanément les VLAN 10, 20, 30 et 99 sur une liaison physique, en distinguant leur trafic grâce à 802.1Q. Le poste utilisateur et le serveur appartiennent à des VLAN et sous-réseaux différents : ils ne communiquent donc pas directement au niveau 2. R1 reçoit leur trafic sur ses sous-interfaces et réalise le routage inter-VLAN.

> ✓ **RÉPONSE À RETENIR**
>
> VLAN 30 : serveurs. Le trunk transporte les VLAN 10, 20, 30 et 99 ; R1 assure leur routage inter-VLAN.

Question 1.2. Pour le poste utilisateur 10.24.10.45/24, donner l'adresse du réseau, l'adresse de diffusion et la plage d'adresses utilisables. Indiquer si la passerelle 10.24.10.1 appartient au même sous-réseau et justifier la réponse.

Élément	Adresse
Réseau	10.24.10.0/24
Diffusion	10.24.10.255
Adresses utilisables	10.24.10.1 à 10.24.10.254

Avec le masque /24, les trois premiers octets identifient le réseau et le dernier identifie l'hôte. Les adresses d'hôte utilisables excluent l'adresse réseau et l'adresse de diffusion. La passerelle 10.24.10.1 appartient bien à ce sous-réseau et constitue une adresse utilisable.

> ✓ **RÉPONSE À RETENIR**
>
> Réseau : 10.24.10.0/24 ; diffusion : 10.24.10.255 ; plage utilisable : 10.24.10.1 à 10.24.10.254. La passerelle est dans le sous-réseau.

Question 1.3. **Compléter dans le DR 1 les routes IPv4 directement connectées à R1 et sa route par défaut. Pour la route par défaut, utiliser l'adresse du routeur opérateur indiquée dans le DT 1 et renseigner la destination avec son préfixe, le prochain saut et l'interface de sortie.**

Destination / préfixe	Prochain saut	Interface de sortie
10.24.10.0/24	direct	G0/0.10
10.24.20.0/24	direct	G0/0.20
10.24.30.0/24	direct	G0/0.30
10.24.99.0/24	direct	G0/0.99
0.0.0.0/0	198.51.100.9	G0/1

Les quatre réseaux des VLAN sont directement connectés aux sous-interfaces 802.1Q de G0/0. Le trafic destiné à toute autre destination utilise la route par défaut, transmise au routeur opérateur par l'interface WAN G0/1.

Table de routage IPv4 de R1 complétée

Destination / préfixe	Prochain saut	Interface de sortie
10.24.10.0/24	direct	G0/0.10
10.24.20.0/24	direct	G0/0.20
10.24.30.0/24	direct	G0/0.30
10.24.99.0/24	direct	G0/0.99
0.0.0.0/0	198.51.100.9	G0/1

✓ **RÉPONSE À RETENIR**

Quatre routes directes via G0/0.10, G0/0.20, G0/0.30 et G0/0.99 ; route par défaut via 198.51.100.9 sur G0/1.

Question 1.4. **Pour le poste d'administration 10.24.20.77 utilisant le préfixe IPv6 2001:db8:24:20::/64, donner l'adresse de passerelle IPv6 configurée sur R1 pour ce VLAN. Expliquer en une phrase la signification de la longueur /64.**

La passerelle IPv6 du VLAN 20 est l'adresse de l'interface de R1 associée à ce VLAN, indiquée dans le plan d'adressage. Dans le préfixe /64, les 64 premiers bits identifient le préfixe réseau du sous-réseau ; les 64 bits restants sont disponibles pour identifier les interfaces. Le poste et sa passerelle utilisent ainsi des adresses appartenant au même préfixe IPv6.

✓ **RÉPONSE À RETENIR**

Passerelle IPv6 : 2001:db8:24:20::1. Le /64 réserve 64 bits au préfixe réseau et 64 bits à l’identifiant d’interface.

2. Exploitation et automatisation des contrôles

Le poste de diagnostic du VLAN 20 doit accéder à la passerelle, au serveur applicatif du VLAN 30 et au nom intranet.novalys.test. Les contrôles montrent une passerelle joignable, mais aucune réponse du serveur et aucun enregistrement DNS retourné.

Question 2.1. Rédiger, dans l'ordre, une séquence de commandes Linux permettant de vérifier la configuration IP du poste, la joignabilité de la passerelle, la route vers 10.24.30.20 et la résolution de intranet.novalys.test. Préciser l'information recherchée pour chaque commande et l'adapter aux adresses et au nom fournis.

Exécuter ces commandes dans l'ordre depuis le poste de diagnostic :

```
ip -br addr show
ip route
ping -c 2 10.24.20.1
ip route get 10.24.30.20
traceroute -n 10.24.30.20
dig @10.24.30.10 +short intranet.novalys.test
```

`ip -br addr show` affiche l'adresse et l'interface ; `ip route` présente la passerelle configurée. Le ping teste la passerelle. `ip route get` indique la route choisie vers le serveur, et `traceroute` les sauts observés. Enfin, `dig` interroge le DNS 10.24.30.10 pour obtenir l'adresse du nom applicatif.

> **✓ RÉPONSE À RETENIR**
>
> Séquence : configuration IP et routes, ping de 10.24.20.1, route vers 10.24.30.20, puis résolution via 10.24.30.10.

Question 2.2. Interpréter les résultats du tableau de contrôles. Indiquer ce qu'ils permettent de valider, où se situe vraisemblablement la rupture et proposer deux vérifications complémentaires sur SW1, R1 ou le serveur avant de modifier la configuration.

Le ping valide la joignabilité de la passerelle du VLAN 20. Le serveur applicatif ne répond pas et le nom ne se résout pas ; traceroute atteint 10.24.20.1, sans saut suivant. La rupture se situe probablement après R1, sur le routage inter-VLAN, le VLAN 30 ou les serveurs. Un filtrage ICMP peut toutefois expliquer l'absence de sauts affichés.

- Sur SW1 et R1, vérifier que le trunk transporte le VLAN 30 et que la sous-interface G0/0.30 est active et correctement associée.
- Vérifier l'adressage, la passerelle et le filtrage du serveur applicatif 10.24.30.20, puis le service DNS et l'enregistrement attendu sur 10.24.30.10.

> **✓ RÉPONSE À RETENIR**
>
> Passerelle joignable ; rupture probable sur l'inter-VLAN, le VLAN 30 ou les serveurs, à confirmer par des contrôles ciblés.

Question 2.3. Proposer une fonction Python nommée etat_service prenant les booléens passerelle_ok, serveur_ok et dns_ok. La fonction doit retourner « OK » si les trois tests sont vrais et « INCIDENT » dans les autres cas. Indiquer la valeur retournée pour les résultats observés.

La fonction renvoie « OK » uniquement si les trois paramètres valent `True` ; sinon, elle signale un incident.

```
def etat_service(passerelle_ok, serveur_ok, dns_ok):
    if passerelle_ok and serveur_ok and dns_ok:
        return "OK"
    return "INCIDENT"
```

D'après le tableau, le test de passerelle réussit, tandis que le ping du serveur et la résolution DNS échouent. Les arguments correspondants sont donc `True`, `False` et `False`.

> **✓ RÉPONSE À RETENIR**
>
> etat_service(True, False, False) = « INCIDENT » : le test passerelle réussit, mais les tests serveur et DNS échouent.

3. Cybersécurité, analyse de traces et durcissement

Les journaux du serveur srv-admin et une capture réseau rapportent des échecs d'authentification SSH depuis un poste d'administration, une connexion acceptée depuis le bastion autorisé et un TCP RST. Il faut distinguer les faits des hypothèses, sans conclure à une compromission non démontrée, puis proposer des mesures de protection.

Question 3.1. Relever deux faits établis par les journaux concernant les tentatives SSH et la connexion du compte ops. Distinguer ces faits d'une hypothèse sur l'origine ou l'objectif des tentatives.

Les journaux consignent plusieurs échecs SSH depuis 10.24.20.77 : les comptes admin, root, support et ops sont concernés. Ils consignent aussi, à 08:43:02, une connexion acceptée pour ops par clé publique depuis 10.24.20.50, le bastion autorisé. Ces faits ne révèlent pas l'identité de la personne utilisant le poste ni la raison des échecs. Une erreur de saisie, un test ou une tentative malveillante sont des hypothèses, non des conclusions établies par ces seules traces.

> ✓ **RÉPONSE À RETENIR**
>
> Échecs SSH depuis 10.24.20.77 ; connexion ops par clé acceptée depuis le bastion 10.24.20.50. L'origine et l'objectif des échecs restent inconnus.

Question 3.2. Interpréter la trace d'un TCP SYN suivi d'un RST vers le port 22. Indiquer ce qu'elle établit et ce qu'elle ne permet pas de conclure à elle seule, puis donner deux contrôles à effectuer sur le serveur ou son filtrage réseau pour expliquer l'absence de session SSH.

Le SYN suivi d'un RST vers 10.24.30.10:22 établit que la connexion TCP a été réinitialisée et qu'aucune session SSH n'a été établie dans cet échange. Cela ne permet pas, à lui seul, d'identifier la cause, ni de conclure à une compromission. Le RST peut notamment résulter d'un service non à l'écoute ou d'un filtrage configuré pour rejeter la connexion.

- Sur le serveur, vérifier l'état de sshd et son écoute sur TCP/22.
- Contrôler le pare-feu du serveur et les ACL réseau, ainsi que leurs journaux.

> ✓ **RÉPONSE À RETENIR**
>
> Connexion TCP/22 réinitialisée, sans session SSH ; vérifier l'écoute de sshd et les règles de filtrage du serveur et du réseau.

Question 3.3. Classer les échecs de connexion répétés selon une priorité faible, moyenne ou élevée. Justifier le classement à partir des traces et préciser une action immédiate de traitement qui préserve les éléments nécessaires à l'analyse.

Priorité moyenne. Les échecs répétés visent plusieurs comptes, dont root et ops, et proviennent de 10.24.20.77, qui n'est pas le bastion autorisé. Ces éléments justifient une investigation, mais aucune authentification réussie depuis ce poste n'est rapportée. La connexion ops acceptée provient du bastion déclaré : les traces ne démontrent donc pas une compromission.

Préserver immédiatement les journaux et la capture réseau avec leurs horodatages, puis consigner l'état initial avant toute modification. Vérifier ensuite l'activité du poste concerné sans effacer les traces.

> **✓ RÉPONSE À RETENIR**
>
> Priorité moyenne ; préserver les journaux et la capture horodatée, puis examiner le poste 10.24.20.77 sans altérer les traces.

Question 3.4. Proposer trois mesures de durcissement des accès SSH cohérentes avec le contexte, comprenant une mesure sur l'authentification, une restriction des sources réseau et une mesure de journalisation ou de supervision.

Appliquer ces trois mesures en cohérence avec la politique du site :

- **Authentification :** imposer les comptes nominatifs et privilégier les clés SSH ; désactiver l'authentification par mot de passe et la connexion directe de root.
- **Sources réseau :** autoriser l'accès TCP/22 au serveur 10.24.30.10 uniquement depuis le bastion 10.24.20.50, avec filtrage réseau et pare-feu hôte.
- **Journalisation :** centraliser et conserver les événements d'authentification dans la supervision, avec une alerte sur les échecs répétés.

> **✓ RÉPONSE À RETENIR**
>
> Clés SSH et comptes nominatifs ; accès SSH limité au bastion 10.24.20.50 ; événements centralisés et alertes sur les échecs répétés.

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

Bilan de l'épreuve : L'épreuve E5 du BTS Cybersécurité, informatique et réseaux, électronique, option A, session 2026, porte le code 26-BTS-CIEL-A-E5, dure 3 heures et a un coefficient 3. À partir du réseau du site Novalys Services, elle évalue l'analyse des VLAN, de l'adressage et du routage, les contrôles Linux et leur automatisation en Python, puis le diagnostic des traces SSH et le durcissement des accès.

Notions-clés, formules & règles à maîtriser

- Un réseau IPv4 /24 utilise le masque 255.255.255.0 et comprend une adresse réseau, une adresse de diffusion et des adresses d'hôtes utilisables.
- Un trunk transporte plusieurs VLAN entre SW1 et R1 ; les sous-interfaces 802.1Q de R1 assurent le routage inter-VLAN.
- Une route directement connectée rejoint un réseau local ; une route par défaut dirige le trafic vers le prochain saut lorsque aucune route plus spécifique ne s'applique.
- Un TCP RST indique le refus ou la fermeture d'une connexion TCP, mais ne prouve pas à lui seul une cause précise ni une tentative SSH aboutie.

Points de vigilance & attentes du jury

- Vérifier que l'adresse réseau, l'adresse de diffusion et la plage d'hôtes correspondent au préfixe indiqué.
- Pour chaque route, renseigner le bon préfixe, le prochain saut et l'interface de sortie, en respectant les consignes du DR 1.
- Relier les résultats des commandes au diagnostic et ne pas confondre l'accès à la passerelle avec l'accès au serveur.
- Séparer les faits consignés dans les traces des hypothèses ; sauvegarder ou consigner l'état initial avant toute modification.

Questions fréquentes sur cette épreuve (Q&A Examen)

Q : Comment déterminer les adresses d'un sous-réseau IPv4 en /24 ?

Pour un réseau IPv4 en /24, le masque est 255.255.255.0 : les trois premiers octets identifient le réseau et le dernier l'hôte. L'adresse réseau et l'adresse de diffusion ne sont pas attribuables à des postes.

Q : Que peut-on conclure si la passerelle répond au ping, mais pas le serveur ?

La réponse de la passerelle valide la connectivité locale jusqu'à celle-ci, mais pas l'accès aux autres VLAN. Un traceroute qui s'arrête au premier saut oriente vers un problème après la passerelle, sans en localiser seul la cause.

Q : Quelle est la durée de l'épreuve et comment répartir son temps ?

L'épreuve dure trois heures et les trois parties totalisent 20 points, avec les pondérations indiquées dans le sujet. Répartissez le temps selon ces barèmes et réservez un moment pour vérifier les réponses et compléter le document DR 1.

Q : Quels critères de méthode sont importants pour l'analyse des traces ?

Il faut relier les interprétations aux observations, distinguer les faits des hypothèses et vérifier avant toute modification. Les changements doivent rester dans le laboratoire et être précédés d'une sauvegarde ou d'une consignation de l'état initial.

Sujet officiel associé (PDF) : https://coursbtsciel.fr/assets/annales/bts-ciel/E5 - Exploitation et maintenance de réseaux informatiques/2026/BTS CIEL - E5 - Exploitation et maintenance de réseaux informatiques - Session 2026 - 1-Sujet.pdf
Ressources BTS Cybersécurité, Informatique et réseaux, Électronique : 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.