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 consulter tous nos sujets d'annales et corrigés du Bac Pro CIEL, veuillez visiter :
coursbacprociel.fr/annales-sujets-et-corriges

Sous-épreuve E31 : Mise en œuvre de réseaux informatiques

Session 2026 • Code sujet : **26-BCP-CIEL-E31** • Durée : **3 heures** • Coefficient : **5**

Sommaire

Cliquez sur une partie pour y accéder directement

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

2. Installation, configuration et validation (4 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://coursbacprociel.fr/assets/annales/bac-pro-ciel/Mise en œuvre de réseaux informatiques/2026/Bac Pro CIEL - Mise en œuvre de réseaux informatiques - Session 2026 - 1-Sujet.pdf

1. Architecture réseau, adressage et routage

Atelier Nord Services sépare son réseau entre les VLAN 10, 20 et 99, avec un routeur R1 chargé du routage inter-VLAN. À partir des plans d'adressage et des ressources techniques, le candidat détermine des paramètres IPv4 et IPv6 et complète la table de routage.

Question 1.1. Pour le VLAN 10, indiquez le masque IPv4 en notation décimale, l'adresse de diffusion et la plage d'adresses utilisables par les équipements. Déterminez si l'adresse 192.168.10.30 peut être attribuée à un équipement de ce VLAN.

Pour un préfixe /27, le masque décimal est 255.255.255.224 et les sous-réseaux avancent par blocs de 32 adresses. Le VLAN 10 couvre donc 192.168.10.0 à 192.168.10.31 : .0 est l'adresse réseau et .31 l'adresse de diffusion. Les hôtes utilisent les adresses intermédiaires, de .1 à .30. L'adresse 192.168.10.30 est utilisable ; elle est différente de l'adresse réseau, de l'adresse de diffusion et de la passerelle 192.168.10.1.

> ✓ RÉPONSE À RETENIR
>
> Masque : 255.255.255.224 ; diffusion : 192.168.10.31 ; plage utilisable : 192.168.10.1 à 192.168.10.30. 192.168.10.30 est attribuable.

Question 1.2. Proposez une adresse IPv4 utilisable pour un poste du VLAN 20, différente de l'adresse de la passerelle, de l'adresse réseau et de l'adresse de diffusion. Indiquez également le préfixe IPv6 de ce VLAN et l'adresse IPv6 de sa passerelle d'après les données de DT 2.

Paramètre VLAN 20	Valeur proposée
Adresse IPv4 du poste	192.168.20.2/27
Passerelle IPv4	192.168.20.1
Préfixe IPv6	2001:db8:42:20::/64
Passerelle IPv6	2001:db8:42:20::1

Le sous-réseau IPv4 s'étend de 192.168.20.0 à 192.168.20.31. L'adresse proposée est distincte de l'adresse réseau, de l'adresse de diffusion et de la passerelle. Selon DT 2, la passerelle IPv6 se termine par ::1 dans le préfixe du VLAN.

> ✓ RÉPONSE À RETENIR
>
> Poste : 192.168.20.2/27 ; préfixe IPv6 : 2001:db8:42:20::/64 ; passerelle IPv6 : 2001:db8:42:20::1.

Question 1.3. Complétez dans le DR 1 la table de routage attendue sur R1. Faites apparaître les trois réseaux directement connectés et la route par défaut vers l'opérateur, en précisant pour chaque entrée le préfixe de destination, le prochain saut ou la mention « direct », ainsi que l'interface de sortie.

Les sous-réseaux des VLAN 10, 20 et 99 sont directement connectés aux sous-interfaces 802.1Q de R1 sur Gi0/0. La route par défaut passe par le prochain saut opérateur 203.0.113.1 et sort sur Gi0/1.

Destination et préfixe	Prochain saut	Interface de sortie
192.168.10.0/27	direct	Gi0/0.10
192.168.20.0/27	direct	Gi0/0.20
192.168.99.0/28	direct	Gi0/0.99
0.0.0.0/0	203.0.113.1	Gi0/1

Les trois routes des VLAN sont connectées directement ; la route par défaut dirige le trafic vers l'opérateur.

DR 1 complété : table de routage de R1

Destination et préfixe	Prochain saut	Interface de sortie
192.168.10.0/27	direct	Gi0/0.10
192.168.20.0/27	direct	Gi0/0.20
192.168.99.0/28	direct	Gi0/0.99
0.0.0.0/0	203.0.113.1	Gi0/1

Document à compléter et à rendre avec la copie

✓ RÉPONSE À RETENIR

Routes VLAN directes via Gi0/0.10, Gi0/0.20 et Gi0/0.99 ; route par défaut via 203.0.113.1 sur Gi0/1.

2. Installation, configuration et validation

Le candidat intervient sur une maquette comprenant R1, SW1, un poste d'intervention et un serveur de supervision, conformément à la topologie et au plan d'adressage fournis. Il réalise les raccordements, configure le poste, vérifie les communications et exploite un journal d'authentification SSH.

Question 2.1. Sur le plateau, repérez R1, SW1, le poste d'intervention et le serveur. Réalisez les raccordements indiqués dans DT 1, notez dans le compte rendu les ports effectivement utilisés et signalez toute différence entre le câblage présent et le schéma.

Contrôlez les étiquettes avant chaque branchement et reportez les ports réellement utilisés sur le plateau. Le câblage de référence comprend le trunk R1 Gi0/0 vers SW1 Gi0/1, le lien opérateur sur R1 Gi0/1, puis les ports d'accès SW1 Fa0/2 pour le serveur, Fa0/3 pour le poste administratif, Fa0/4 pour le poste atelier et Fa0/5 pour le poste d'intervention. Les interfaces terminales indiquées dans DT 1 sont eth0. Signalez précisément tout port ou raccordement différent du schéma.

> **✓ RÉPONSE À RETENIR**
>
> Référence : R1 Gi0/0 - SW1 Gi0/1 ; R1 Gi0/1 - réseau opérateur ; SW1 Fa0/2 - serveur ; Fa0/3 - poste administratif ; Fa0/4 - poste atelier ; Fa0/5 - poste d'intervention. Ports réellement utilisés et écarts : à relever sur le plateau.

Question 2.2. Configurez le poste d'intervention conformément à son affectation au VLAN 99 : renseignez l'adresse IPv4, le préfixe ou masque, la passerelle et les paramètres IPv6 prévus dans DT 2. Relevez les commandes exécutées ou l'écran de configuration utilisé.

Avant modification, relevez la configuration existante avec `ip addr show eth0` et les routes. Pour le VLAN 99, configurez eth0 en IPv4 `192.168.99.12/28` (masque `255.255.255.240`), passerelle `192.168.99.1`, IPv6 `2001:db8:42:99::12/64` et passerelle IPv6 `2001:db8:42:99::1`. Les commandes ci-dessous conviennent à un poste Linux ; vérifiez ensuite les adresses et routes et consignez les commandes réellement exécutées.

```
sudo ip address replace 192.168.99.12/28 dev eth0
sudo ip route replace default via 192.168.99.1
sudo ip -6 address replace 2001:db8:42:99::12/64 dev eth0
sudo ip -6 route replace default via 2001:db8:42:99::1
ip addr show eth0
ip route
ip -6 route
```

> **✓ RÉPONSE À RETENIR**
>
> eth0 : 192.168.99.12/28, passerelle 192.168.99.1 ; 2001:db8:42:99::12/64, passerelle 2001:db8:42:99::1.

Question 2.3. Effectuez les quatre tests du tableau « Résultats de référence attendus pour la recette ». Pour chaque test, indiquez la commande utilisée et le résultat observé. En cas d'échec, précisez quelle étape de la chaîne de communication vérifier en premier à partir des données de DT 1 et DT 2.

Exécutez chaque commande depuis le poste affecté au VLAN indiqué. Les résultats ci-dessous sont les références attendues, pas des observations à déclarer sans avoir réalisé les essais. Consignez les réponses réellement reçues pour chaque test.

1. VLAN 10 : `ping -c 4 192.168.10.1`, réponses ICMP.
2. VLAN 20 : `ping -c 4 192.168.20.1`, réponses ICMP.
3. VLAN 20 vers le serveur : `ping -c 4 192.168.10.10`, réponses après activation du routage inter-VLAN.
4. Résolution DNS : `nslookup supervision.atelier.example 192.168.10.10`, adresse obtenue `192.168.10.10`.

En cas d'échec, vérifiez d'abord le lien et le port d'accès/VLAN, puis l'adresse et la passerelle. Pour la communication inter-VLAN, contrôlez aussi le trunk et le routage de R1.

> **✓ RÉPONSE À RETENIR**
>
> Attendu : réponses ICMP aux deux passerelles et au serveur après activation du routage inter-VLAN ; supervision.atelier.example est résolu en 192.168.10.10.

Question 2.4. À partir des extraits de journal fournis dans DT 2, écrivez une commande Bash utilisant grep et awk pour afficher le nombre d'échecs d'authentification SSH par adresse source. Donnez le nombre d'échecs associé à chaque adresse IP présente dans les lignes marquées « Failed password ».

Sur le serveur de maquette, filtrez d'abord le journal sur les seules lignes `Failed password`, conformément à DT 2. Awk repère ensuite le champ `from` et compte le champ suivant, qui contient l'adresse source. La commande regroupe ainsi les échecs par IP, y compris si les champs précédant l'adresse varient selon le compte demandé. L'ordre d'affichage des adresses par awk n'est pas garanti.

```
grep 'Failed password' /var/log/auth.log | awk '{for (i=1; i<=NF; i++) if ($i=="from")
n[$(i+1)]++} END {for (ip in n) print ip, n[ip]}'
```

> **✓ RÉPONSE À RETENIR**
>
> 198.51.100.23 : 2 échecs d'authentification SSH dans les lignes « Failed password » fournies.

3. Analyse d’incident et sécurisation des accès

Le serveur de supervision a journalisé deux échecs SSH depuis une adresse externe réservée à la documentation, puis une connexion réussie du compte admin depuis le réseau d’administration. Le candidat interprète les traces disponibles, propose des mesures de durcissement et décrit le traitement de l’incident ainsi que les vérifications de conformité.

Question 3.1. Relevez les événements de sécurité dans l’ordre chronologique. Pour chacun des deux échecs SSH, indiquez l’adresse source et le compte demandé ; pour la connexion réussie, indiquez l’utilisateur et l’adresse source. Expliquez ce que ces seules lignes permettent de conclure et ce qu’elles ne permettent pas d’établir.

1. **09:14:02 et 09:14:09** : deux échecs SSH pour le compte demandé `support`, depuis `198.51.100.23`.
2. **09:16:31** : connexion SSH réussie par clé pour `admin`, depuis `192.168.99.12`.
3. **09:17:04** : `admin` lance avec sudo la commande `systemctl status ssh`.

Les lignes établissent ces événements et leurs horaires. L’adresse `198.51.100.23` appartient à une plage réservée à la documentation. Elles ne permettent pas d’identifier les personnes à l’origine des connexions, de prouver une compromission ni de relier les échecs à la connexion réussie. Le résultat de la commande sudo n’est pas indiqué.

> **✓ RÉPONSE À RETENIR**
>
> Deux échecs pour `support`, puis connexion par clé de `admin` depuis `192.168.99.12` et consultation de l’état de SSH.

Question 3.2. Proposez deux mesures de durcissement des accès SSH compatibles avec le besoin d’administration à distance. Pour chacune, indiquez le risque réduit et précisez comment éviter de verrouiller l’accès autorisé depuis le réseau d’administration 192.168.99.0/28.

- **Limiter SSH au réseau d’administration** par une ACL ou un pare-feu autorisant `192.168.99.0/28` et bloquant les autres réseaux. Cela réduit les tentatives depuis les réseaux non autorisés. Tester la règle depuis le réseau d’administration avant son activation définitive.
- **Imposer les clés SSH**, désactiver l’authentification par mot de passe et interdire la connexion directe de root. Cela réduit les attaques par devinette et force brute. Vérifier la clé autorisée, conserver une session active ou un accès console, puis tester une nouvelle connexion avant de fermer la session.

> **✓ RÉPONSE À RETENIR**
>
> Réserver SSH au réseau `192.168.99.0/28` et imposer les clés, après validation de l’accès autorisé et maintien d’un accès de secours.

Question 3.3. Décrivez, dans l'ordre, une procédure de traitement de l'incident comprenant la conservation des éléments de preuve, la vérification de l'état du compte admin, le contrôle des clés autorisées et la mise à jour de l'équipement. Indiquez les précautions à prendre avant de redémarrer le service SSH.

1. Copier les journaux et configurations utiles, préserver les originaux et noter la date ainsi que les empreintes des copies.
2. Vérifier que le compte `admin` est légitime et correctement protégé. Examiner les clés autorisées, leurs empreintes et leurs permissions; préserver toute clé suspecte avant de la révoquer.
3. Mettre à jour le système et les composants SSH depuis une source fiable, puis vérifier la configuration avec `sshd -t`.
4. Avant tout redémarrage, conserver une session active, prévoir un accès console ou un retour arrière et tester une nouvelle connexion depuis le réseau d'administration. Ne recharger ou redémarrer SSH que si la configuration est valide.

> **✓ RÉPONSE À RETENIR**
>
> Conserver les preuves, contrôler le compte et les clés, mettre à jour, valider la configuration et tester l'accès de secours avant le redémarrage.

Question 3.4. Après application des mesures, indiquez trois vérifications permettant de valider la conformité de l'installation : l'accès depuis le réseau d'administration, l'absence d'accès SSH depuis le VLAN atelier et le contrôle des journaux. Précisez le résultat attendu pour chacune.

Effectuer les trois contrôles après application des mesures et conserver leurs résultats :

- Depuis le réseau d'administration `192.168.99.0/28`, ouvrir une session SSH avec la clé autorisée : connexion réussie.
- Depuis le VLAN atelier, tenter une connexion SSH au serveur : accès bloqué et aucune session ouverte.
- Consulter les journaux : connexion autorisée depuis le réseau d'administration visible; tentative du VLAN atelier refusée ou bloquée si la règle de filtrage est journalisée; aucune connexion réussie inattendue.

> **✓ RÉPONSE À RETENIR**
>
> SSH est accessible depuis le réseau d'administration, bloqué depuis le VLAN atelier, et les journaux ne montrent aucun accès réussi inattendu.

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

Bilan de l'épreuve : L'épreuve E31 du baccalauréat professionnel CIEL, session 2026, porte le code 26-BCP-CIEL-E31 et dure 3 heures, coefficient 5. Elle porte sur le réseau d'Atelier Nord Services : segmentation en VLAN, adressage IPv4/IPv6, routage inter-VLAN, raccordement et tests de recette. Elle évalue aussi l'analyse de journaux SSH, le traitement d'incident et le durcissement des accès.

Notions-clés, formules & règles à maîtriser

- Un préfixe IPv4 /27 correspond au masque 255.255.255.224 et à des blocs de 32 adresses.
- L'adresse réseau et l'adresse de diffusion ne s'attribuent pas à un équipement ; les adresses utilisables se situent entre ces deux bornes.
- Un trunk 802.1Q transporte plusieurs VLAN entre le commutateur et le routeur ; les sous-interfaces de R1 assurent le routage inter-VLAN.
- Une route par défaut IPv4 utilise le préfixe 0.0.0.0/0 et dirige le trafic non autrement routé vers le prochain saut opérateur.

Points de vigilance & attentes du jury

- Vérifiez le préfixe avant de calculer le masque, l'adresse réseau, l'adresse de diffusion et les adresses utilisables.
- Associez chaque VLAN au bon sous-réseau, à sa passerelle et à son interface logique sur R1.
- Avant toute modification, relevez la configuration existante et vérifiez les étiquettes ainsi que les ports réellement utilisés.
- Dans l'analyse des journaux, distinguez les échecs, les connexions réussies et les actions sudo ; ne concluez pas au-delà des traces disponibles.

Questions fréquentes sur cette épreuve (Q&A Examen)

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

Repérez d'abord l'adresse réseau et l'adresse de diffusion à partir du préfixe. Les adresses utilisables se trouvent entre ces deux bornes. Vérifiez ensuite si une adresse est déjà réservée, par exemple pour la passerelle.

Q : Comment distinguer un trunk d'un port d'accès dans cette maquette ?

Un port d'accès relie un terminal à un seul VLAN. Le trunk entre SW1 et R1 transporte les VLAN 10, 20 et 99, afin que les sous-interfaces de R1 assurent le routage inter-VLAN.

Q : Comment sont répartis les points et combien de temps faut-il gérer ?

L'épreuve dure 3 heures et vaut 20 points : la partie 1 compte pour 6 points, la partie 2 pour 7 points et la partie 3 pour 7 points. Répartissez le temps entre préparation, manipulations et compte rendu.

Q : Qu'attend le jury pour l'analyse des journaux et la sécurisation SSH ?

Le sujet demande des conclusions fondées sur les événements fournis, des mesures compatibles avec l'accès d'administration autorisé et des vérifications explicites. Le dossier ne précise pas de norme supplémentaire ni de grille détaillée de notation.

Sujet officiel associé (PDF) : https://coursbacprociel.fr/assets/annales/bac-pro-ciel/Mise en œuvre de réseaux informatiques/2026/Bac Pro CIEL - Mise en œuvre de réseaux informatiques - Session 2026 - 1-Sujet.pdf
Ressources Bac Pro CIEL : 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.