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 STAV, veuillez visiter :
bacstav.fr/annales-sujets-et-corriges

BAC STAV • CORRIGÉ DÉTAILLÉ

Bac STAV

Module C4 : Pratiques mathématiques et numériques, compétences en technologies de l'informatique et du multimédia

Session 2026 • Code sujet : **26-BTN-STAV-EP1** • Durée : **120 minutes** • Coefficient : **Sans coefficient autonome pour la TIM**

Sommaire

Cliquez sur une partie pour y accéder directement

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

2. Base de données relationnelle 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://bacstav.fr/assets/annales/bac-stav/Technologies de l'informatique et du multimédia/2026/Bac STAV - Technologies de l'informatique et du multimédia - Session 2026 - 1-Sujet.pdf

1. Architecture réseau, adressage et routage

La ferme expérimentale des Trois-Rivières utilise un réseau local segmenté en VLAN, relié à Internet par le routeur R1. À partir de sa topologie et de son plan d'adressage IPv4 et IPv6, il faut analyser les sous-réseaux et compléter des informations de routage.

Adressage IPv4 du VLAN 10

Question 1.1. Pour le préfixe 192.168.40.0/26, donner le masque en notation décimale pointée, l'adresse de diffusion, la plage des adresses utilisables pour les équipements et le nombre d'adresses utilisables.

Élément	VLAN 10 : 192.168.40.0/26
Masque	255.255.255.192
Adresse de diffusion	192.168.40.63
Adresses utilisables	192.168.40.1 à 192.168.40.62
Nombre d'adresses utilisables	62

Un /26 laisse 6 bits pour les hôtes, soit 64 adresses au total. L'adresse réseau, 192.168.40.0, et l'adresse de diffusion, 192.168.40.63, ne sont pas attribuables. Les équipements disposent donc des 62 adresses intermédiaires, de 192.168.40.1 à 192.168.40.62. Le masque correspondant comporte 26 bits à 1.

> ✓ **RÉPONSE À RETENIR**
>
> Masque : 255.255.255.192 ; diffusion : 192.168.40.63 ; plage utilisable : 192.168.40.1 à 192.168.40.62, soit 62 adresses.

Passerelle et appartenance au sous-réseau

Question 1.2. Pour PC-AGRI, configuré à l'adresse 192.168.40.20/26, indiquer sa passerelle par défaut selon DT 2 et expliquer pourquoi l'adresse 192.168.40.70 ne peut pas lui être attribuée.

DT 2 indique que la passerelle par défaut de PC-AGRI est 192.168.40.1, l'adresse de R1 dans le VLAN 10. Avec le préfixe /26, PC-AGRI appartient au sous-réseau 192.168.40.0/26. L'adresse 192.168.40.70 appartient au sous-réseau 192.168.40.64/27, affecté au VLAN 20 des serveurs. Elle ne peut donc pas être attribuée à PC-AGRI, car elle serait hors de son sous-réseau.

> ✓ **RÉPONSE À RETENIR**
>
> Passerelle : 192.168.40.1. L'adresse 192.168.40.70 appartient au VLAN 20, et non au sous-réseau du VLAN 10.

Adressage IPv6

Question 1.3. À partir du préfixe IPv6 du VLAN 10 dans DT 2, écrire l'adresse complète de la passerelle R1, qui se termine par ::1, et celle de PC-AGRI, qui se termine par ::20. Indiquer le rôle du préfixe /64.

Le préfixe IPv6 du VLAN 10 est 2001:db8:40:10::/64. En développant les groupes abrégés, la passerelle R1 s'écrit 2001:0db8:0040:0010:0000:0000:0000:0001 et PC-AGRI s'écrit 2001:0db8:0040:0010:0000:0000:0000:0020.

Le préfixe /64 désigne les 64 premiers bits du réseau. Les 64 bits restants identifient l'interface, ce qui permet de distinguer les équipements appartenant au même préfixe.

> ✓ **RÉPONSE À RETENIR**
>
> R1 : 2001:0db8:0040:0010:0000:0000:0000:0001 ; PC-AGRI : 2001:0db8:0040:0010:0000:0000:0000:0020. /64 fixe les 64 bits du préfixe réseau.

Table de routage et trunk

Question 1.4. Compléter dans DR 1 la table de routage de R1 pour les réseaux directement connectés et l'accès à Internet, en utilisant pour la route par défaut le prochain saut donné dans DT 2. Indiquer également la fonction du trunk entre SW1 et R1.

Les trois réseaux des VLAN sont directement connectés à R1 : les prochains sauts sont donc indiqués comme « Directement connecté ». Pour la destination par défaut 0.0.0.0/0, le prochain saut est l'adresse opérateur 203.0.113.1, et l'interface de sortie est WAN.

Le trunk entre SW1 et R1 transporte les VLAN 10, 20 et 30 sur une même liaison, en conservant l'identification de chaque VLAN. Les valeurs à inscrire dans les cases de DR 1 sont reportées sur l'annotation.

Prochains sauts à inscrire dans la table de routage

Destination	Prochain saut	Interface de sortie
192.168.40.0/26	Directement connecté	VLAN 10
192.168.40.64/27	Directement connecté	VLAN 20
192.168.40.96/27	Directement connecté	VLAN 30
0.0.0.0/0	203.0.113.1	WAN

Utiliser le plan d'adressage de DT 2.

> ✓ **RÉPONSE À RETENIR**
>
> VLAN 10, 20 et 30 : directement connectés. Route par défaut : prochain saut 203.0.113.1 via WAN. Le trunk transporte les trois VLAN entre SW1 et R1.

2. Base de données relationnelle et requêtes SQL

Les techniciens enregistrent les mesures d'humidité et de nitrates des parcelles dans une base relationnelle composée des tables PARCELLE et MESURE. Les tâches portent sur la jointure et le filtrage de données, l'agrégation des concentrations en nitrates et l'interprétation de moyennes par parcelle.

Filtrage et tri SQL

Question 2.1. Écrire une requête SQL complète joignant PARCELLE et MESURE pour afficher le nom de la parcelle, la date et la teneur en nitrates des mesures du 8 avril 2026 dont la teneur est strictement supérieure à 20 mg/L. Trier les résultats par teneur en nitrates décroissante et utiliser les noms exacts des tables et colonnes de DT 2.

La jointure relie chaque mesure à sa parcelle par `id_parcelle`. Le filtre retient le 8 avril 2026 et les teneurs strictement supérieures à 20 mg/L ; le tri décroissant place la plus forte teneur en premier.

✓ RÉPONSE À RETENIR

```
SELECT PARCELLE.nom, MESURE.date_mesure, MESURE.nitrate_mg_l
FROM PARCELLE JOIN MESURE ON PARCELLE.id_parcelle = MESURE.id_parcelle
WHERE MESURE.date_mesure = DATE '2026-04-08' AND MESURE.nitrate_mg_l > 20
ORDER BY MESURE.nitrate_mg_l DESC;
```

Agrégation SQL par parcelle

Question 2.2. Compléter dans DR 1 la requête SQL qui affiche, pour chaque parcelle, son nom et la moyenne des teneurs en nitrates de ses mesures, sous l'alias moyenne_nitrates. Effectuer la jointure nécessaire et regrouper les résultats par parcelle et par nom.

AVG calcule la moyenne des teneurs en nitrates de chaque groupe. La jointure associe les mesures aux parcelles ; le regroupement par identifiant et par nom donne une moyenne distincte pour chaque parcelle.

Requête SQL complétée dans DR 1

Requête SQL à compléter pour la question 2.2

	Requête
AVG(MESURE.nitrate_mg_l) PARCELLE.id_parcelle = MESURE.id_parcelle PARCELLE.id_parcelle, PARCELLE.nom	SELECT PARCELLE.nom, ... AS moyenne_nitrates FROM PARCELLE JOIN MESURE ON ... GROUP BY ...;

Compléter les éléments manquants de la requête.

✓ RÉPONSE À RETENIR

```
SELECT PARCELLE.nom, AVG(MESURE.nitrate_mg_l) AS moyenne_nitrates
FROM PARCELLE JOIN MESURE ON PARCELLE.id_parcelle = MESURE.id_parcelle
GROUP BY PARCELLE.id_parcelle, PARCELLE.nom;
```

Calcul et interprétation des moyennes

Question 2.3. Sans écrire de requête, donner à partir de l'extrait fourni la moyenne des teneurs en nitrates pour chacune des trois parcelles, préciser l'unité et expliquer en une phrase pourquoi les résultats doivent être agrégés par parcelle.

Parcelle	Calcul	Moyenne
Nord (P01)	(18 + 24) / 2	21 mg/L
Sud (P02)	(12 + 30) / 2	21 mg/L
Est (P03)	27 / 1	27 mg/L

Le regroupement par parcelle permet d'obtenir une moyenne propre aux mesures de chacune.

✓ **RÉPONSE À RETENIR**

Nord : 21 mg/L ; Sud : 21 mg/L ; Est : 27 mg/L.

3. Cybersécurité, analyse de journaux et durcissement

Les journaux du pare-feu et du service SSH de SRV-DATA recensent des connexions refusées, des échecs d'authentification et une connexion réussie depuis le réseau interne. Il faut examiner les indices, proposer des protections du service SSH et indiquer des actions de réponse à l'événement.

Analyse des journaux

Question 3.1. Relever deux indices justifiant l'examen d'un incident de sécurité à partir des journaux. Distinguer les tentatives provenant de l'adresse extérieure 198.51.100.23 des événements concernant la connexion réussie du compte tech01.

Les journaux montrent des tentatives répétées depuis 198.51.100.23 : deux connexions SSH refusées par le pare-feu, puis deux échecs d'authentification sur SRV-DATA pour le compte admin. Ces échecs justifient l'examen d'un incident. Cette adresse est réservée aux exemples de documentation et ne désigne pas un organisme réel. La connexion réussie de tech01 à 09:17:10 provient de l'adresse interne 192.168.40.20 ; elle doit être vérifiée, sans être assimilée d'emblée à une attaque.

> ✓ **RÉPONSE À RETENIR**
>
> Tentatives SSH répétées et échecs du compte admin depuis l'adresse extérieure fictive ; vérifier la connexion interne réussie de tech01.

Réduction du risque SSH

Question 3.2. Proposer deux mesures techniques complémentaires pour réduire le risque d'accès non autorisé au service SSH et préciser, pour chacune, le risque qu'elle vise à réduire.

Deux mesures complémentaires réduisent des risques distincts :

- **Filtrer le SSH par pare-feu** pour n'autoriser que les adresses ou réseaux nécessaires : cela limite les tentatives de connexion depuis des sources non autorisées.
- **Imposer l'authentification par clé** et désactiver l'authentification par mot de passe : cela réduit les attaques par devinette ou réutilisation de mots de passe. Interdire en plus la connexion directe de root limite l'obtention immédiate de privilèges élevés.

> ✓ **RÉPONSE À RETENIR**
>
> Restreindre les sources SSH par pare-feu et imposer les clés, sans authentification par mot de passe.

Actions après détection

Question 3.3. Indiquer deux actions à réaliser après la détection des événements afin de préserver les éléments utiles à l'analyse et de limiter les conséquences possibles. Justifier brièvement chacune.

1. **Préserver les éléments d'analyse :** exporter les journaux du pare-feu et du service SSH, avec leurs horodatages, puis en conserver une copie intacte. Ils permettront de reconstituer la chronologie et d'analyser

les tentatives.

2. **Limiter les conséquences :** vérifier auprès de l'utilisateur la connexion réussie de tech01. Si elle est suspecte, suspendre temporairement le compte ou révoquer ses clés, et restreindre les accès SSH non autorisés. Cela réduit le risque de maintien ou de répétition d'un accès abusif.

> **✓ RÉPONSE À RETENIR**
>
> Conserver une copie intacte des journaux, puis vérifier tech01 et suspendre ou restreindre les accès jugés suspects.

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

Bilan de l'épreuve : Cette épreuve de TIM du bac technologique STAV, session 2026, porte le code 26-BTN-STAV-EP1 et dure 120 minutes, sans coefficient autonome pour la TIM. Située dans une ferme expérimentale, elle évalue sur 20 points l'analyse d'adressage et de routage, l'interrogation SQL de données agronomiques et l'analyse de journaux de cybersécurité.

Notions-clés, formules & règles à maîtriser

- En IPv4, un préfixe /26 correspond au masque 255.255.255.192 et partage le dernier octet en blocs de 64 adresses.
- Une adresse IPv6 /64 comprend 64 bits de préfixe réseau et 64 bits disponibles pour l'identifiant d'interface.
- Une route par défaut IPv4 a pour destination 0.0.0.0/0 et transmet les paquets vers un prochain saut.
- En SQL, AVG calcule une moyenne et GROUP BY regroupe les mesures pour obtenir une valeur par parcelle.

Points de vigilance & attentes du jury

- Distinguer adresse réseau, adresse de diffusion et adresses utilisables dans chaque sous-réseau.
- Utiliser les passerelles et le prochain saut tels qu'ils figurent dans DT 2, sans confondre adresse et interface.
- Respecter exactement les noms de tables et de colonnes, la condition de date, le seuil strict et le tri demandé en SQL.
- Dans l'analyse des journaux, séparer les tentatives externes de la connexion interne réussie et justifier les actions proposées.

Questions fréquentes sur cette épreuve (Q&A Examen)

Q : Comment déterminer rapidement les limites d'un sous-réseau IPv4 /26 ?

Un /26 laisse 6 bits pour les hôtes et forme des blocs de 64 adresses dans le dernier octet. Pour 192.168.40.0/26, le réseau est .0, la diffusion .63 et les adresses utilisables vont de .1 à .62.

Q : Pourquoi faut-il regrouper les mesures par parcelle pour calculer une moyenne ?

La jointure associe chaque mesure à sa parcelle, puis GROUP BY forme un groupe distinct pour chaque parcelle. AVG appliqué aux nitrates calcule une moyenne séparée pour chacune, au lieu d'une moyenne globale.

Q : Comment organiser les 120 minutes et que faut-il rendre sur DR 1 ?

Le sujet répartit 20 points entre trois parties : 7, 7 et 6 points. Gérez le temps en fonction de ces poids et gardez une vérification finale. Complétez directement DR 1 pour la table de routage 1.4 et la requête SQL 2.2.

Q : Quels éléments doivent apparaître dans la réponse sur l'incident SSH ?

Appuyez-vous sur les horodatages, les sources, les destinations et la nature des événements. Distinguez les tentatives externes des connexions internes, puis reliez chaque mesure ou action proposée au risque réduit ou à l'objectif de préservation des preuves.

Sujet officiel associé (PDF) : https://bacstav.fr/assets/annales/bac-stav/Technologies de l'informatique et du multimédia/2026/Bac STAV - Technologies de l'informatique et du multimédia - Session 2026 - 1-Sujet.pdf
Ressources Bac STAV : 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.