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

BUT Info

Informatique

Session 2026 • Code sujet : **26-BUT-INFO-EP1** • Durée : **2 h 30** • Coefficient : **3,0 (indicatif)**

Sommaire

Cliquez sur une partie pour y accéder directement

1. Analyse fonctionnelle et réglementaire (4 questions) **Page 3**

2. Étude technologique et dimensionnement (5 questions) **Page 5**

3. Préparation du déploiement et protocole opératoire (4 questions) **Page 8**

4. Prévention, sécurité et diagnostic (3 questions) **Page 11**

5. Ce qu'il faut retenir & Questions fréquentes (FAQ) (Synthèse & Q&A Examen) **Page 13**

Sujet officiel (PDF) : https://butinfo.fr/assets/annales/but-info/C3 - Administrer/2026/BUT Informatique - C3 - Administrer - Session 2026 - 1-Sujet.pdf

1. Analyse fonctionnelle et réglementaire

Atelier Nordik doit faire évoluer son réseau après des ralentissements et un accès non autorisé à un dossier partagé. L'étude porte sur les besoins, la segmentation en VLAN, la protection des données personnelles et les critères de recette de l'infrastructure cible.

Recueil des besoins

Question 1.1. Relevez quatre besoins fonctionnels ou contraintes d'exploitation du cahier des charges. Pour chacun, indiquez le service ou la population concernée.

1. **Segmentation :** isoler les postes administratifs, utilisateurs, serveurs et invités dans quatre VLAN, afin de limiter les ralentissements et les accès indus.
2. **Postes utilisateurs :** fournir DHCP, DNS interne et accès aux seuls services nécessaires, notamment le partage de fichiers.
3. **Administration :** permettre l'administration des équipements par SSH depuis le seul VLAN 10 et limiter l'interruption planifiée à 45 minutes.
4. **Invités et serveurs :** réserver Internet aux invités, isoler les serveurs et sauvegarder 120 Go chaque nuit.

> ✓ RÉPONSE À RETENIR
>
> Quatre VLAN isolés, services DHCP et DNS pour les postes, SSH réservé au VLAN d'administration, accès Internet seul pour les invités et sauvegarde nocturne de 120 Go.

Segmentation logique

Question 1.2. À partir du contexte et des documents DT 1 et DT 3, proposez une segmentation logique adaptée aux quatre populations décrites. Précisez la fonction de chaque segment et les communications qui doivent être interdites par défaut.

VLAN	Population et fonction	Interdictions par défaut
10	Administration : gestion des équipements et serveurs	Tout flux non nécessaire ou non autorisé
20	Postes utilisateurs : accès aux services internes nécessaires	Tout autre accès inter-VLAN
30	Serveurs : hébergement des services et du partage	Administration hors VLAN 10 et flux non autorisés
40	Invités : accès à Internet	Toute communication avec les VLAN internes

Autoriser seulement DNS vers 10.42.0.130, DHCP et SMB vers le serveur de fichiers pour les postes du VLAN 20. Le VLAN 10 peut administrer les équipements en SSH et les serveurs par les services nécessaires. Les invités accèdent à Internet, pas au réseau interne. Refuser et journaliser les autres flux inter-VLAN.

> ✓ RÉPONSE À RETENIR
>
> VLAN 10 administration, VLAN 20 utilisateurs, VLAN 30 serveurs, VLAN 40 invités. Seuls les flux nécessaires sont autorisés, les autres sont refusés par défaut.

Protection des données

Question 1.3. Pour les données personnelles présentes sur les postes et les serveurs, indiquez trois mesures techniques ou organisationnelles cohérentes avec les principes de protection des données. Reliez chaque mesure au risque qu'elle réduit.

Trois mesures adaptées aux données personnelles présentes sur les postes et les serveurs :

- **Limiter les droits selon les rôles et le besoin d'en connaître :** réduit les consultations, modifications ou divulgations par des personnes non autorisées.
- **Minimiser les données collectées et fixer une durée de conservation :** réduit l'exposition en cas de fuite et la conservation injustifiée.
- **Chiffrer les données stockées et les sauvegardes, et protéger les échanges :** limite leur exploitation en cas de vol d'équipement ou d'interception.

Les droits attribués et les durées de conservation sont revus périodiquement.

> **✓ RÉPONSE À RETENIR**
>
> Appliquer le moindre privilège, minimiser les données et leur durée de conservation, puis chiffrer les données, sauvegardes et échanges.

Critères de recette

Question 1.4. Définissez trois critères de recette mesurables pour vérifier la conformité de l'installation au cahier des charges. Au moins un critère doit porter sur la segmentation, un sur l'accès d'administration et un sur la sauvegarde ou la continuité de service.

La recette est validée si ces trois critères sont satisfaits :

1. **Segmentation :** un poste invité accède à Internet, mais ses tentatives vers les VLAN 10, 20 et 30 sont bloquées ; les postes utilisateurs n'atteignent que DNS, DHCP et le partage autorisé.
2. **Administration :** SSH vers les équipements réseau réussit depuis le VLAN 10 et échoue depuis les VLAN 20 et 40 ; l'administration des serveurs est également réservée au VLAN 10.
3. **Sauvegarde et continuité :** la sauvegarde nocturne des 120 Go est vérifiée et un test de restauration est concluant ; l'interruption planifiée reste au plus égale à 45 minutes.

> **✓ RÉPONSE À RETENIR**
>
> Invités isolés des VLAN internes, SSH réservé au VLAN 10, sauvegarde de 120 Go restaurable et interruption planifiée limitée à 45 minutes.

2. Étude technologique et dimensionnement

Le bloc privé 10.42.0.0/24 doit être réparti entre les VLAN d'administration, des postes utilisateurs, des serveurs et des invités, en tenant compte des interfaces d'infrastructure. Les calculs portent aussi sur les débits, la sauvegarde nocturne et les règles de filtrage inter-VLAN.

Plan d'adressage VLSM

Question 2.1. À partir de 10.42.0.0/24, établissez un plan VLSM pour les quatre VLAN. Pour chacun, indiquez le préfixe, l'adresse réseau, la première adresse utilisable, l'adresse de diffusion et le nombre d'adresses utilisables. Justifiez chaque préfixe par la puissance de deux nécessaire, en tenant compte des deux adresses réservées. Attribuez les blocs par ordre décroissant des besoins, sans chevauchement.

Le nombre d'adresses du bloc doit couvrir les équipements et les deux adresses réservées. Les besoins de 48, 25, 12 et 10 équipements exigent donc des blocs de 64, 32, 16 et 16 adresses, soit /26, /27, /28 et /28. Ils sont placés dans l'ordre décroissant des besoins. Le DNS 10.42.0.130 impose de placer le VLAN 30 dans le bloc 10.42.0.128/28.

VLAN	Préfixe	Adresse réseau	Première utilisable	Diffusion	Adresses utilisables
10 Administration	/28	10.42.0.96	10.42.0.97	10.42.0.111	14
20 Postes	/26	10.42.0.0	10.42.0.1	10.42.0.63	62
30 Serveurs	/28	10.42.0.128	10.42.0.129	10.42.0.143	14
40 Invités	/27	10.42.0.64	10.42.0.65	10.42.0.95	30

Les besoins augmentés des deux adresses réservées sont respectivement 50, 27, 14 et 12. Ils tiennent dans 64, 32, 16 et 16 adresses. Les blocs attribués ne se chevauchent pas.

DR 2 complété : plan VLSM

VLAN	Besoin maximal	Préfixe	Adresse réseau	Première adresse utilisable	Adresse de diffusion	Nombre d'adresses utilisables	Flux principaux autorisés ou refusés
10 : Administration	12	.....	..... /28	..... 10.42.0.96	..... 10.42.0.97	..... 10.42.0.111 — 14	.....
20 : Postes utilisateurs	48	.....	..... /26	..... 10.42.0.0	..... 10.42.0.1	..... 10.42.0.63 — 62	.....
30 : Serveurs	10	.....	..... /28	..... 10.42.0.128	..... 10.42.0.129	..... 10.42.0.143 — 14	.....
40 : Invités	25	.....	..... /27	..... 10.42.0.64	..... 10.42.0.65	..... 10.42.0.95 — 30	.....

✓ RÉPONSE À RETENIR

VLAN 10 : 10.42.0.96/28 ; VLAN 20 : 10.42.0.0/26 ; VLAN 30 : 10.42.0.128/28 ; VLAN 40 : 10.42.0.64/27.

Dimensionnement du réseau interne

Question 2.2. **À l'heure de pointe, les 48 postes utilisateurs génèrent chacun un trafic moyen de 1,5 Mbit/s vers les services internes. Calculez le débit agrégé demandé, puis comparez-le au débit utile d'un lien interne nominal de 1 Gbit/s. Présentez la formule, le résultat et une conclusion sur la marge disponible.**

Le trafic agrégé demandé est le nombre de postes multiplié par le débit moyen de chacun : 48 × 1,5 = 72 Mbit/s. Le débit utile du lien interne est 1 000 × 0,80 = 800 Mbit/s. La marge disponible est donc 800 − 72 = 728 Mbit/s. Le trafic interne calculé peut être acheminé sans saturer le lien, selon les hypothèses données.

> ✓ **RÉPONSE À RETENIR**
>
> Trafic agrégé : 72 Mbit/s ; débit utile : 800 Mbit/s ; marge : 728 Mbit/s.

Dimensionnement de la sauvegarde

Question 2.3. **Une sauvegarde nocturne de 120 Go doit être transférée en 30 minutes. Calculez le débit moyen nécessaire en Mbit/s et comparez-le au débit utile d'un lien nominal de 1 Gbit/s. Utilisez les conversions fournies dans le contexte et détaillez les étapes du calcul.**

Le volume vaut 120 × 10^9 octets, soit 120 × 10^9 × 8 bits. La durée de transfert est 30 × 60 = 1 800 secondes. Le débit moyen nécessaire est donc :

1. 120 × 10^9 × 8 = 960 × 10^9 bits.
2. 960 × 10^9 ÷ 1 800 = 533 333 333,3 bits/s.
3. Soit environ 533,3 Mbit/s.

Le lien fournit 800 Mbit/s utiles : le transfert tient dans sa capacité, avec une marge d'environ 266,7 Mbit/s.

> ✓ **RÉPONSE À RETENIR**
>
> Débit nécessaire : environ 533,3 Mbit/s, inférieur aux 800 Mbit/s utiles.

Règles de filtrage

Question 2.4. **À l'aide des besoins de filtrage du DT 3, rédigez quatre règles de filtrage ordonnées sous la forme « source, destination, service, action ». Elles doivent autoriser l'administration SSH requise, l'accès des invités à Internet et les échanges indispensables des postes utilisateurs avec les services internes, tout en bloquant les autres communications non explicitement autorisées entre VLAN. Indiquez la règle finale de refus par défaut.**

Appliquer les règles dans l'ordre et journaliser les refus lorsque l'équipement le permet. Le DHCP des postes est autorisé selon le mécanisme prévu, notamment le relais si nécessaire. Les invités n'atteignent que les destinations Internet permises ; tout flux invité vers un VLAN interne tombe sous le refus par défaut.

Ordre	Source	Destination	Service	Action
1	VLAN 10 Administration	Équipements réseau et serveurs	SSH TCP/22 et services d'administration nécessaires	Autoriser
2	VLAN 20 Postes	10.42.0.130 ; serveur de fichiers VLAN 30 ; service DHCP	DNS UDP/TCP 53 ; SMB TCP/445 ; DHCP selon l'architecture	Autoriser
3	VLAN 40 Invités	Internet, destinations internes exclues	Services de navigation nécessaires	Autoriser selon la politique de sortie
4	Tout VLAN	Tout autre VLAN	Tout flux non explicitement autorisé	Refuser par défaut

La règle 4 bloque donc aussi les invités vers le réseau interne et les accès non autorisés entre les autres VLAN.

DR 2 complété : synthèse des flux

VLAN	Besoin maximal	Préfixe	Adresse réseau	Première adresse utilisable	Adresse de diffusion	Nombre d'adresses utilisables	Flux principaux autorisés ou refusés
10 : Administration	12	.....	.....	.....	.....	.....	..... VLAN 10 : SSH autorisé
20 : Postes utilisateurs	48	.....	.....	.....	.....	.....	..... VLAN 20 : DNS, DHCP, SMB
30 : Serveurs	10	.....	.....	.....	.....	.....	..... VLAN 30 : accès admin
40 : Invités	25	.....	.....	.....	.....	.....	..... VLAN 40 : Internet seul

✓ RÉPONSE À RETENIR

Autoriser SSH depuis le VLAN 10, les services requis du VLAN 20 et la navigation Internet du VLAN 40 ; refuser tout autre flux inter-VLAN.

Capacité Internet

Question 2.5. Le débit Internet est de 200 Mbit/s et le débit utile retenu vaut 80 % du débit nominal. Calculez ce débit utile. Indiquez si le trafic de pointe des 48 postes, calculé à la question 2.2, peut être entièrement acheminé simultanément vers Internet sans dépasser cette capacité. Justifiez votre réponse.

Le débit Internet utile est 200 × 0,80 = 160 Mbit/s. Le trafic de pointe des postes calculé en 2.2 vaut 72 Mbit/s. Il peut donc être acheminé simultanément vers Internet sans dépasser la capacité utile, si tout ce trafic est destiné à Internet. La marge restante est 160 − 72 = 88 Mbit/s.

✓ RÉPONSE À RETENIR

Débit utile : 160 Mbit/s. Oui, les 72 Mbit/s passent ; marge : 88 Mbit/s.

3. Préparation du déploiement et protocole opératoire

Le déploiement doit tenir dans une fenêtre de maintenance de 45 minutes, avec des équipements compatibles avec les VLAN 802.1Q, le routage inter-VLAN et les listes de contrôle d'accès. Le candidat prépare une intervention réversible, complète les paramètres DHCP et propose des contrôles automatisés ainsi que des tests de recette.

Ordre opératoire

Question 3.1. Établissez un ordre opératoire d'au moins six étapes, depuis la préparation jusqu'à la recette. Pour chaque étape, indiquez une action concrète et un contrôle permettant de décider si l'intervention peut se poursuivre. Prévoyez la sauvegarde de la configuration initiale et une procédure de retour arrière compatible avec la fenêtre de maintenance.

Avant la fenêtre, sauvegarder les configurations et préparer les commandes de restauration. Pendant l'intervention, poursuivre uniquement si le contrôle de l'étape est concluant.

1. 5 min : créer les VLAN et configurer les trunks 802.1Q ; vérifier les VLAN et l'état des liens.
2. 8 min : configurer les passerelles, le routage et les ACL ; vérifier routes et règles actives.
3. 7 min : activer les étendues DHCP ; contrôler une attribution et les options par VLAN.
4. 10 min : migrer les ports ; vérifier le VLAN de chaque équipement migré.
5. 7 min : tester DNS, SSH, partage et blocages ; consigner les résultats.
6. Réserver 8 min au retour arrière : restaurer les configurations par console si un contrôle échoue, puis vérifier le rétablissement du service initial.

Les opérations en fenêtre totalisent 45 minutes, retour arrière compris.

> **✓ RÉPONSE À RETENIR**
>
> Configuration initiale sauvegardée avant intervention ; déploiement et recette en 37 min, avec 8 min réservées au retour arrière.

Étendues DHCP

Question 3.2. Complétez le DR 1 pour les quatre étendues DHCP à partir du plan d'adressage établi à la question 2.1. Indiquez la passerelle, le masque ou préfixe, la plage dynamique proposée et le serveur DNS interne. Pour les VLAN 10 et 30, expliquez pourquoi les équipements d'infrastructure ou les serveurs concernés ne doivent pas recevoir une adresse dynamique non réservée.

VLAN	Réseau/préfixe	Masque	Passerelle	Plage dynamique	DNS
10 Administration	10.42.0.96/28	255.255.255.240	10.42.0.97	10.42.0.98-10.42.0.108	10.42.0.130
20 Postes	10.42.0.0/26	255.255.255.192	10.42.0.1	10.42.0.2-10.42.0.62	10.42.0.130
30 Serveurs	10.42.0.128/28	255.255.255.240	10.42.0.129	Aucune plage générale	10.42.0.130
40 Invités	10.42.0.64/27	255.255.255.224	10.42.0.65	10.42.0.66-10.42.0.94	10.42.0.130

Les plages excluent les passerelles. Le VLAN 10 dispose de 11 adresses dynamiques pour les équipements autres que la passerelle ; les adresses d'infrastructure doivent rester fixes ou réservées pour éviter les changements et les conflits. En VLAN 30, les serveurs conservent des adresses fixes ou réservées : le DNS 10.42.0.130 reste ainsi joignable à une adresse stable. Les plages proposées laissent des adresses inutilisées dans les VLAN 20 et 40.

DR 1 complété : paramètres DHCP

VLAN	Réseau et préfixe	Masque décimal	Passerelle	Début de plage dynamique	Fin de plage dynamique	DNS fourni aux clients
10 : Administration	10.42.0.96/28	255.255.255.24	10.42.0.97	10.42.0.98	10.42.0.108	10.42.0.130
20 : Postes utilisateurs	10.42.0.0/26	255.255.255.19	10.42.0.1	10.42.0.2	10.42.0.62	10.42.0.130
30 : Serveurs	10.42.0.128/28	255.255.255.24	10.42.0.129	Pas de plage dynamique générale	Pas de plage dynamique générale	10.42.0.130
40 : Invités	10.42.0.64/27	255.255.255.22	10.42.0.65	10.42.0.66	10.42.0.94	10.42.0.130

✓ RÉPONSE À RETENIR

Passerelles : .97, .1, .129, .65. Plages dynamiques : .98-.108, .2-.62, aucune plage générale, .66-.94. DNS : 10.42.0.130.

Vérification automatisée

Question 3.3. Rédigez un pseudo-code ou un script shell commenté qui vérifie la disponibilité du serveur DNS interne et du partage de sauvegarde, horodate les résultats et retourne un code d'erreur si l'un des deux contrôles échoue. Les commandes exactes peuvent être remplacées par des fonctions clairement définies.

Ce pseudo-script utilise des fonctions de contrôle clairement définies : la première interroge le DNS interne à 10.42.0.130 ; la seconde vérifie l'accès au partage de sauvegarde. Chacune renvoie un code nul en cas de succès. Les résultats sont horodatés séparément et le code final signale l'échec d'au moins un contrôle.

```
erreur=0
for controle in dns_disponible partage_disponible; do
    if "$controle"; then
        resultat=OK
    else
        resultat=ECHEC
        erreur=1
    fi
    printf '%s %s %s\n' "$(date -Is)" "$controle" "$resultat"
done
exit "$erreur"
```

✓ RÉPONSE À RETENIR

Code de sortie 0 si les deux contrôles réussissent, 1 si l'un au moins échoue ; chaque résultat est horodaté.

Tests de recette

Question 3.4. Citez deux tests de recette à effectuer depuis deux VLAN différents et précisez, pour chacun, le résultat attendu.

Réaliser les tests depuis des postes effectivement raccordés aux VLAN indiqués, puis consigner les résultats. Ils doivent confirmer les accès nécessaires et l'isolement des invités.

- **VLAN 20, postes utilisateurs :** interroger le DNS 10.42.0.130 et accéder au partage SMB du VLAN 30 ; les deux accès doivent réussir.
- **VLAN 40, invités :** vérifier l'accès Internet puis tenter l'accès au partage ou à une interface d'administration ; Internet doit fonctionner, tandis que les accès internes doivent être refusés et journalisés.

✓ RÉPONSE À RETENIR

VLAN 20 : DNS et partage accessibles. VLAN 40 : Internet accessible, ressources internes bloquées.

4. Prévention, sécurité et diagnostic

Après la mise en service, un poste invité a tenté d'accéder au partage de sauvegarde et l'interface d'administration d'un commutateur est joignable depuis le VLAN utilisateurs. Comme le partage contient des données de l'entreprise et des données personnelles, il faut qualifier et contenir l'incident, préserver les éléments de diagnostic et sécuriser les interventions et les comptes.

Qualification et confinement

Question 4.1. Indiquez les premières actions à mener pour qualifier et contenir l'incident, sans détruire les éléments utiles au diagnostic. Donnez au moins trois actions ordonnées.

1. Consigner l'heure, les adresses IP/MAC, les VLAN et les actions observées ; préserver les journaux du routeur, des commutateurs, du serveur et du partage.
2. Vérifier si des connexions ont abouti et si des fichiers ont été consultés ou modifiés. Ne pas effacer les journaux ni redémarrer les équipements ; conserver les éléments utiles au diagnostic.
3. Contenir l'incident en isolant le poste invité et en bloquant les flux non autorisés par ACL, sans interrompre les services nécessaires.
4. Documenter les actions et prévenir le responsable sécurité ; associer le délégué à la protection des données si une violation de données personnelles est suspectée.

> **✓ RÉPONSE À RETENIR**
>
> Préserver les journaux, qualifier les accès, isoler le poste invité, bloquer les flux non autorisés et alerter les responsables concernés.

Recherche des causes

Question 4.2. Proposez deux vérifications permettant d'identifier pourquoi le poste invité atteint le partage ou l'interface d'administration. Pour chacune, indiquez l'équipement ou la configuration à examiner et l'information recherchée.

Effectuer deux contrôles ciblés pour distinguer une erreur de segmentation ou de filtrage d'une exposition de l'interface de gestion :

- Sur le routeur et le commutateur cœur, vérifier l'affectation VLAN des ports, les VLAN autorisés sur les trunks 802.1Q et l'ordre des ACL. Rechercher une règle permettant au VLAN 40 d'atteindre le VLAN 30 ou un autre réseau interne.
- Sur le commutateur concerné, contrôler l'interface de gestion, ses ACL et les journaux. Rechercher si le VLAN 20 peut joindre cette interface ou si l'accès SSH n'est pas limité au VLAN 10.

> **✓ RÉPONSE À RETENIR**
>
> Contrôler affectations VLAN, trunks et ACL, puis vérifier que l'interface de gestion est inaccessible depuis le VLAN 20.

Sécurisation des interventions et des comptes

Question 4.3. Citez deux mesures de prévention applicables aux interventions physiques dans la baie réseau et deux mesures de sécurisation des comptes d'administration. Distinguez clairement les mesures relatives aux personnes et celles relatives aux systèmes.

Domaine	Mesures à appliquer
Personnes et interventions physiques	Confier les manipulations au personnel habilité ; identifier les équipements et câbles avant intervention et respecter les consignes de sécurité électrique.
Systèmes et comptes d'administration	Attribuer des comptes nominatifs avec privilèges minimaux ; imposer l'authentification multifacteur et limiter SSH au VLAN 10.

Les premières mesures préviennent les erreurs de manipulation et les accès physiques non autorisés. Les secondes limitent l'usurpation d'identité et réservent l'administration réseau au VLAN autorisé.

> ✓ **RÉPONSE À RETENIR**
>
> Personnes : habilitation et identification des équipements et câbles. Systèmes : comptes nominatifs à privilèges minimaux, MFA et SSH limité au VLAN 10.

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

Bilan de l'épreuve : Cette évaluation de la compétence C3 du BUT Informatique, session 2026, code 26-BUT-INFO-EP1, dure 2 h 30 et affiche un coefficient indicatif de 3,0. Le cas Atelier Nordik étudie l'évolution d'un réseau d'entreprise : segmentation en VLAN, adressage, filtrage, déploiement et sécurisation. Les compétences évaluées couvrent le dimensionnement, l'exploitation documentée, la recette et le diagnostic d'incident.

Notions-clés, formules & règles à maîtriser

- Le nombre d'hôtes IPv4 utilisables d'un sous-réseau est 2^h - 2, où h est le nombre de bits réservés aux hôtes.
- Le débit utile retenu vaut 80 % du débit nominal : débit utile = débit nominal × 0,8.
- Pour calculer un débit de sauvegarde, convertir les Go en bits puis diviser par la durée en secondes.
- Le filtrage inter-VLAN autorise uniquement les flux nécessaires et documentés, puis refuse par défaut les autres communications.

Points de vigilance & attentes du jury

- En VLSM, dimensionner chaque bloc pour tous les équipements, dont la passerelle, puis vérifier l'absence de chevauchement.
- Réserver la première adresse utilisable à la passerelle et ne jamais attribuer les adresses réseau ou de diffusion.
- Dans chaque règle de filtrage, préciser source, destination, service et action, puis respecter l'ordre des règles.
- Prévoir une sauvegarde de configuration, des contrôles à chaque étape et un retour arrière compatible avec les 45 minutes.

Questions fréquentes sur cette épreuve (Q&A Examen)

Q : Comment choisir le préfixe d'un sous-réseau VLSM ?

Ajoutez deux adresses réservées au nombre d'hôtes requis, puis choisissez la plus petite puissance de deux qui couvre ce total. Le nombre de bits d'hôtes détermine le préfixe par soustraction à 32.

Q : Comment vérifier si un débit calculé est suffisant ?

Calculez d'abord le débit demandé dans la même unité que la capacité utile. La capacité est suffisante si elle dépasse le débit demandé ; la différence entre les deux valeurs donne la marge disponible.

Q : Comment organiser l'intervention dans la fenêtre de maintenance ?

Préparez les configurations et les contrôles avant l'interruption, sauvegardez l'état initial, puis appliquez les changements par étapes vérifiables. Gardez du temps pour la recette et pour restaurer la configuration si un contrôle échoue.

Q : Quels éléments rendent une règle de filtrage exploitable et vérifiable ?

Une règle identifie précisément source, destination, service et action, avec protocole et port si nécessaire. L'ordre préserve les autorisations explicites avant le refus par défaut, et les résultats doivent pouvoir être vérifiés.

Sujet officiel associé (PDF) : https://butinfo.fr/assets/annales/but-info/C3 - Administrer/2026/BUT Informatique - C3 - Administrer - Session 2026 - 1-Sujet.pdf

Ressources BUT Informatique : 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.