Table des matières

ÉTAPE 2 Si vous n'utilisez pas l'anglais, sélectionnez la langue souhaitée dans le menu déroulant Langue. Pour ajouter une nouvelle langue au périphérique ou mettre à jour une langue existante, reportez-vous à la section Mettre à niveau/sauvegarder micrologiciel/langue.

ÉTAPE 3 S'il s'agit de votre première ouverture de session avec l'ID utilisateur par défaut (**cisco**) et le mot de passe par défaut (**cisco**

Navigation dans les fenêtres

Cette section décrit les fonctions de l'utilitaire Web de configuration du commutateur.

En-tête d'application

L'en-tête d'application s'affiche sur toutes les pages. Il fournit les liens d'application suivants :

Nom du lien d'application	Description
	Une icône X rouge clignotante qui s'affiche à gauche du lien d'application **Enregistrer** indique que des

État et statistiques

Pour entrer des alarmes RMON :

ÉTAPE 1 Cliquez sur **État et statistiques > RMON** > **Alarmes** pour afficher les alarmes. Les ch

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les paramètres.

- **Entrée d'alarme** : affiche le numéro d'entrée de l'alarme.
-
  - a Tw Nom[(du c)-27 o(e)-7.mptaleugt55

État et statistiques

Afficher le journal

Administration : Journal système

Cette section décrit la fonction Journal système, qui permet à l'appareil de générer plusieurs journaux indépendants. Chaque journal correspond à un ensemble de messages décrivant les événements système.

L'appareil génère les journaux locaux suivants :

Administration : Journal système

Administration : Journal système

Affichage des journaux de la mémoire

Administration : Gestion de fichiers

Fichiers système

Administration : Gestion de fichiers

Administration : Gestion de fichiers

- **Global**

Administration : Gestion de fichiers

Si le

Administration : Gestion de fichiers

-

Paramétrage de la configuration automatique DHCP

Flux de travail

Pour paramétrer la configuration automatique DHCP :

Administration

Administration

Paramètres de console (prise en charge du débit de bauds automatiques)

Le débit du port de console peut être défini sur l'une des valeurs suivantes : 4 800, 9 600, 19 200, 38 400, 57 600 et 115 200 ou détection automatique.

Comptes d'utilisateur

Reportez-vous à la section **Définition d'utilisateurs**.

Définition du délai d'expiration en cas de session inactive

Le

Journal système

Reportez-vous à la section

Pour afficher les paramètres d'inté

- **Intervalle de Ping** : durée d'attente du système entre les paquets Ping. La

Administration : Paramètres horaires

Configuration de l'heure système

Administration : Paramètres horaires

Configuration de l'heure système

Administration : Diagnostic

Administration : Détection

Pour configurer Bonjour lorsque le périphérique fonctionne en mode système

- Fonctionnalités du système : fonctions principales du périphérique.

Cette page affiche les champs suivants :

Globale

- **Sous-type de l'ID du châssis**

Détails MAC/PHY

- **Négociation automatique prise en charge** : état de prise en charge de la négociation automatique du débit de port.
- **Négociation automatique activée**

- *État* : indique si les paquets de TLV 802.3 LLDP MED ont été envoyés ou si une surcharge est intervenue.

- **TLV LLDP facultatives**

  -

Gestion des ports

Définition de la configuration des ports

Gestion des ports

Gestion des ports

Agrégation de liaisons

Gestion des ports

Agrégation de liaisons

ÉTAPE 2 Sélectionnez un **port** puis cliquez sur **Modifier**.

ÉTAPE 3 Choisissez d'activer ou de désactiver le mode **Détection d'énergie**

Gestion des ports : Unidirectional Link Detection

Instructions d'utilisation

ui ded'admin:=2.98(srat(ic

Port intelligent

Types de port intelligent

Fonctionnement de la fonction Port intelligent

Il est possible d'appliquer une macro Port intelligent à une interface par nom de macro ou par Type de port intelligent associé à la macro. L'application d'une macro Port intelligent par nom de macro s'effectue uniquement via l'interface de ligne de commande. Pour plus d'informations, reportez-vous au guide de

Port intelligent

Port intelligent automatique

REMARQUE La persistance des Types de port intelligent appliqués aux interfs es (s de)5.t efs0.4(r)-5e

Port intelligent

- **Nom de la macro** : affiche le nom de la macro Port intelligent actuellement associée au Type de port intelligent.
-

Port intelligent

Port intelligent

Macros Port intelligent intégrées

```
#
@
```

host

```
[host]
#macro description host
#macro keywords $native_vlan $max_hosts
#
```

Port intelligent

Gestion des VLAN

VLAN

Création d'un VLAN

Vous pouvez créer un VLAN mais cela n'a aucun effet tant que le VLAN n'est pas manuellement ou dynamiquement lié à au moins un port. Les ports doivent toujours appartenir à un ou plusieurs VLAN.

Le périphérique de la série 300 prend en charge jusà(9 é)-7à 4252.5(300.3(4(pr17.7(enéé

Gestion des VLAN

Configuration des paramètres d'interface VLAN

Gestion des VLAN

Gestion des VLAN

Flux de travail

Pour définir un groupe VLAN basé sur MAC :

1. Attribuez une adresse MAC à un ID de groupe VLAN (à l'aide de la page Groupes basés sur MAC).
2. Pour chaque interface requise :
    a. Attribuez le groupe VLAN à un VLAN (à l'aide de la page Groupes basés sur MAC aux VLAN). Les interfaces doivent être en mode Général.
    b. Si l'interface n'appartient pas au VLAN, affectez-la manuellement au VLAN à l'aide de la page Port vers VLAN.

- Longueur : préfixe de l'adresse MAC

- **ID de groupe**

VLAN voix automatique

Le mode VLAN voix automatique permet de gérer le VLAN voix, mais dépend de la fonction Port intelligent automatique pour gérer l'appartenance des ports VLAN voix. Le mode VLAN voix automatique offre les fonctions suivantes lorsqu'il est opérationnel :

Flux de travail 1 : pour configurer le VLAN voix automatique :

ÉTAPE 1 Ouvrez la page Gestion des VLAN > VLAN voix > Propriétés.

ÉTAPE 2 Sélectionnez l'ID du VLAN voix. Il ne peut pas être défini sur > Pro8(

Configuration du VLAN voix

Cette section explique comment configurer le VLAN voix. Elle couvre les rubriques suivantes :

- **Configuration des propriétés du VLAN voix**
-

Gestion des VLAN

Pour afficher les paramètres VLAN voix automatique :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN voix** > **VLAN voix automatique**.

Le bloc d'état opérationnel figurant sur cette page affiche des informations sur le

Cette rubrique aborde les points suivants :

- **Ajout de OUI à la Table des OUI de téléphonie**
-

Gestion des VLAN

VLAN voix

Gestion des VLAN

Gestion des VLAN

Gestion des VLAN

Pour définir l'état et les paramètres globaux STP :

- **Transitions de transfert** : affiche le nombre de fois où le port est passé de l'état **Blocage** à l'état **Transfert**.

Arbre recouvrant

- **Adresse IP de multidiffusion de groupe** : définit l'adresse IP de multidiffusion du nouveau groupe.
- **Propre à la source** : indique que l'entrée contient une source spécifique et ajoute l'adresse correspondante dans le champ Adresse IP source. Dans le cas contraire, l'entrée est ajoutée sous la foros Tw[4(n55 -1(o)-09(*,G)s)-2271(,c' e)-
  - dece(de gr).9(oup)98.5(e-5.6 ais)-15.8iséeoels iscec
    - **A5 -1(d)23()258.2(e-1.4ss(e)-73353It-19.1Pr)165**

Multidiffusion

Multidiffusion

Surveillance MLD

Pour activer le traçage MLD et le configurer sur un VLAN :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **MLD Snooping**.

ÉTAPE 2 Activez ou désactivez l'option **État MLD Snooping**. Lorsque le traçage MLD 4227()-10.8(o

Multidiffusion

Multidiffusion

Définition de la multidiffusion Tout transférer

Multidiffusion

Définition des paramètres de multidiffusion non enregistrée

- **Longueur du préfixe**

Interactions entre la surveillance DHCPv4, le relais DHCPv4 et l'option 82

Les tableaux suivants décrivent le comportement du périphérique en fonction des différentes combinaisons entre dee 6(S01.7273t 500(illn c)-10.9ec)-216.7D5000.4DHCP1

Vous découvrirez comment les paquets de

La base de données de liaison de surveillance DHCP est également utilisée par les fonctionnalités de protection de la source IP et d'inspection ARP dynamique pour déterminer les sources légitimes des paquets.

Ports sécurisés DHCP

Configuration IP

IPv4 Management and Interfaces (Interfaces et gestion IPv4)

Configuration IP

IPv4 Management and Interfaces (Interfaces et gestion IPv4)

reçoivent une adresse IP du groupe configuré. Effectuez cette opération sur la page Configuration IP > Interface IPv4.

ÉTAPE 7

- **Nom d'hôte** : saisissez le nom de l'hôte qui peut être une chaîne de symboles et un entier.
- **Masque** : saisissez le masque de réseau de l'hôte statique.
  - Masque réseau : vérifiez et saisissez le masque réseau de l'hôte statique.
  - Longueur du préfixe : vérifiez et saisissez le nombre de bits compris dans le préfixe de l'adresse.

00e5s

Configuration IP

- **Type de la règle** : entrez la règle pour la liste de préfixes.
  - Autoriser : autorise les réseaux qui respectent la condition.
  - Refuser : refuse les réseaux qui ne respectent pas la condition.
  - Description : texte.
- **Préfixe IPv6** : préfixe de route IP.
- **Longueur du préfixe** : longueur du préfixe de route IP.
- **Supérieur à** : longueur minimale du préfixe devant être utilisée pour la correspondance. Sélectionnez une des options suivantes :
  - Aucune limite : aucune longueur minimale du préfixe ne doit être utilisée pour la correspondance.
  - Défini par l'utilisateur : longueur minimale du préfixe devant être respectée.
- **Inférieur à** : longueur maximale du préfixe devant être utilisée pour la correspondance. Sélectionnez une des options suivantes :
  - Aucune limite

Configuration IP

- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas

- **Préférence**

Configuration IP

Nom de domaine

Sécurité

Cette section décrit le contrôle d'accès et

- **Niveau d'utilisateur** : sélectionnez le niveau de privilèges de l'utilisateur que vous ajoutez/modifiez.

Si vous n'entrez pas de chaîne de clé dans ce champ, la clé de serveur

- **Port IP** : saisissez le numéro de port via lequel s'opère la session TACACS+.

Sécurité

Méthode d'accès de gestion

Sécurité

Authentification de l'accès de gestion

Sécurité

Les conneigpion interne)

Sécurité

- **« Trap »** : sélectionnez cette option pour activer les interceptions lorsqu'un

Sécurité

- **Mode Hôtes multiples**

  Un port est autorisé s'il y a au moins un client autorisé.

Sécurité : Authentification 802.1X

Tâches courantes

Flux de travail 1 : activer l'authentification 8021x sur un port

ÉTAPE 1 Cliquez sur **Sécurité > Authentification 802.1X/MAC/Web > Propriétés**.

ÉTAPE 2 Activez l'authentification basée sur les ports.

ÉTAPE 3 Sélectionnez la

Sécurité : Authentification 802.1X

- **Méthode d'authentification**

- **Contenu des termes et conditions** : saisissez le texte du message des conditions d'utilisation à afficher.

ÉTAPE10

Sécurité : Authentification 802.1X

Prise en charge des méthodes d'authentification et des modes de port

Sécurité : Sécurité du premier saut IPv6

Cette section décrit le fonctionnement de la Sécurité du premier saut (First Hop Security, FHS) et la façon de configurer cette fonction dans l'interface utilisateur graphique.

Elle couvre les rubriques suivantes :

- **Présentation de la Sécurité du premier saut**
- **Protection Router Advertisement**
-

Présentation de la Sécurité du premier saut

La Sécurité du premier saut IPv6 (IPv6 FHS) est une suite de fonctionnalités conçues pour sécuriser les opérations de liaison dans un réseau IPv6. Elle est basée sur le

Sécurité : Sécurité du premier saut IPv6

Protection DHCPv6

Protection contre l'usurpation de serveur DHCPv6

Un hôte IPv6 peut utiliser le protocole DHCPv6 pour :

- Configuration d'informations sans état
- Configuration d'adresse avec état

Un hôte malveillant peut envoyer des messages de réponse DHCPv6 qui l'annoncent lui-même comme serveur DHCPv6 et fournissant des adresses IPv6 et des informations sans état contrefaites. La protection DHCPv6 offre une protection contre ces attaques en configurant le rôle d'interface comme port client pour tous les ports auxquels les serveurs DHCPv6 ne peuvent pas être connectés.

Protection contre l'usurpation de cache NBD

Un routeur IPv6 prend en charge le cache NDP (Neighbor Discovery Protocol) qui mappe l'adresse IPv6 sur l'adresse MAC pour le routage du dernier saut.

Un hôte malveillant peut envoyer des messages IPv6 avec une autre adresse IPv6 de destination pour le transfert du dernier saut, générant ainsi un débordement du cache NBD.

Un mécanisme intégré à l'implémentation NDP, qui limi798TJ0..001é4a141 0.4(n)6 Tc 15(N

- **Autre drapeau de configuration** : ce champ spécifie la vérification du drapeau Autre configuration annoncé au sein d'une stratégie Protection RA IPv6.
  - Aucune vérification : ddration du

Sécurité : Sécurité du premier saut IPv6

Configuration de la Sécurité du premier saut via l'interface utilisateur graphique Web

- **Liste de VLAN**

Sécurité : Sécurité du premier saut IPv6

Configuration de la Sécurité du premier saut via l'interface utilisateur graphique Web

Sécurité : Sécurité du premier saut IPv6

SSD offre aux utilisateurs la flexibilité de configurer le niveau de protection souhaité pour leurs données confidentielles ; à savoir aucune protection des données confidentielles sous forme de texte en clair, une protection minimale avec un cryptage basé sur le mot de passe par défaut ou une protection améliorée avec un cryptage basé sur le mot de passe défini par l'utilisateur.

SSD accorde une autorisation en lecture sur les données confidentielles uniquement aux utilisateurs authentifiés et autorisés, et conformément aux règles SSD. Un appareil authentifie et autorise l'accès de gestion pour les utilisateurs par l'intermédiaire du processus d'authentification des utilisateurs.

Que vous utilisiez ou non SSpr.9(ormé0016 Tw-17(,)-4.41(')0.(1(è)-1.3(g.7(s)-2e du24r.)-2.8

uEn'é èe be su-11.3(oe-0.9(nsibl)-6.73s)sur lu apripd
é-11.9(a)-254.4(S)-21.53Sa r,ldunprié
uoJ.5(le)-6(73s)sr 73s

Sécurité : Gestion sécurisée des données confidentielles

Règles SSD

Sécurité : Gestion sécurisée des données confidentielles

Sécurité : Gestion sécurisée des données confidentielles

Sécurité : Gestion sécurisée des données confidentielles

Fichiers de configuration

Sécurité : Gestion sécurisée des données confidentielles

Interface de ligne de commande (CLI) et récupération du mot de passe

- Niveau 15 : indique que cette règle s'applique à tous les utilisateurs ayant le niveau de privilège 15.
- Tous : indique que cette règle s'applique à tous les utilisateurs.

• **Canal** : définit le niveau de sécurité du canal d'entrée auquel la règle s'applique : Sélectionnez une des options suivantes :

- Sécurisé : indique que cette règle s'applique uniquement aux canaux

Guide d'admini772 0 natio4(i)-2 du commu(i)-2ti(776(at)25 l(eu(i)-2r)]TJ18.0.8(2D0034 T150 Tw4 T48[(Guidn)5.4(3.82.i(Tm 0 nable Cis)-15.2

Authentification du client SSH

Avant de commencer

Vous devez effectuer les actions suivantes avant d'utiliser la fonction SCP :

Sécurité : Client SSH

Configuration du client SSH via l'interface utilisateur graphique (GUI)

ÉTAPE 3 Connectez-vous à l'appareil B, puis ouvrez la page Authentification du serveur SSH. Sélectionnez la clé RSA ou DSA, cliquez sur **Modifier**, puis collez la clé de l'appareil A.

Pages de configuration du serveur SSH

Cette section décrit les pages utilisées pour configurer la fonctionnalité **Serveur SS7m5s9()**

Sécurité : Serveur SSH

Pages de configuration du serveur SSH

Contrôle d'accès

- Plage : sélectionnez une plage de ports source TCP/UDP avec lesquels le paquet est mis en correspondance. Huit plages de ports différentes peuvent être configurées (partagées entre les ports source et de destination). Les protocoles TCP et UD

- Non défini : une correspondance est établie si l'indicateur est Non défini.
- Sans importance : ignore l'indicateur TCP.

- **Type de service** : type de service du paquet IP.
- **ICMP** : si l'ACL est basée sur ICMP, sélectionnez le type de message ICMP à utiliser afin de filtrer. Sélectionnez le type de message en fonction de son

Qualité de service

Qualité de service

Qualité de service

Les contraintes suivantes s'appliquent à la

- **CoS/802.1p-DSCP** : sélectionnez cette option pour utiliser le mode CoS de confiance pour le trafic non IP et DSCP de confiance pour le trafic IP.

Pour utiliser l'action de dépassement DSCP hors profil, remappez la valeur DSCP dans la table Mappage DSCP hors profil. Sinon, l'action est Null, car la valeur DSCP de la table remappe le paquet sur lui-même, selon les valeurs par défaut définies en usine.

Cette fonction modifie les balises DSCP du trafic entrant commuté entre des domaines de QoS de confiance. En modifiant les valeurs DSCP utilisées dans un

Qualité de service

Mode de QoS avancé

Pour afficher les statistiques de file d'attente :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Statistiques de QoS** > **Statistiques de file**
Cl1quez 3stieiutie page.9(fle)-4.(i)-12.7s statt5tuivants-2.38.6(:9618 -7 0.563 rg 162 659.76 .5

ÉTAPE 3

ID d'objet du modèle

Ci-dessous figurent les ID d'objet (OID) du modèle de périphérique :

Nom du modèle	Description	ID d'objet
SG300-10	8 ports GE et 2 ports combinés spécifiques	

Pour créer un utilisateur SNMPv3, les éléments ci-dessous doivent exister au préalable :

- Un ID de moteur doit d'abord être

- **Adresse IP** : saisissez l'adresse IP de la station de gestion SNMP.
-

ÉTAPE 3

REMARQUE : le niveau de sécurité dépend du nom d'utilisateur qui a été sélectionné. Si le paramètre Aucune authentification a été défini pour ce nom d'utilisateur, le niveau de sécurité est uniquement Aucune authentification. Cependant, si le paramètre Authentification et confidentialité a été défini pour ce nom d'utilisateur sur la page Utilisateur,