SIEMENS

SIMATIC NET

Industrial Ethernet Switches Web User Interface (Web UI) SINEC OS V2.1

Manuel de configuration

Pour SCALANCE XCH-300, XCM-300, XRH-300 et XRM-300

04/2022
C79000-G8977-C497-03

Mentions légales

Signalétique d'avertissement

Ce manuel donne des consignes que vous devez respecter pour votre propre sécurité et pour éviter des dommages matériels. Les avertissements servant à votre sécurité personnelle sont accompagnés d'un triangle de danger, les avertissements concernant uniquement des dommages matériels sont dépourvus de ce triangle. Les avertissements sont représentés ci-après par ordre décroissant de niveau de risque.

⚠ **DANGER**
signifie que la non-application des mesures de sécurité appropriées **entraîne** la mort ou des blessures graves.

⚠ **ATTENTION**
signifie que la non-application des mesures de sécurité appropriées **peut entraîner** la mort ou des blessures graves.

⚠ **PRUDENCE**
signifie que la non-application des mesures de sécurité appropriées peut entraîner des blessures légères.

IMPORTANT
signifie que la non-application des mesures de sécurité appropriées peut entraîner un dommage matériel.

En présence de plusieurs niveaux de risque, c'est toujours l'avertissement correspondant au niveau le plus élevé qui est reproduit. Si un avertissement avec triangle de danger prévient des risques de dommages corporels, le même avertissement peut aussi contenir un avis de mise en garde contre des dommages matériels.

Personnes qualifiées

L'appareil/le système décrit dans cette documentation ne doit être manipulé que par du **personnel qualifié** pour chaque tâche spécifique. La documentation relative à cette tâche doit être observée, en particulier les consignes de sécurité et avertissements. Les personnes qualifiées sont, en raison de leur formation et de leur expérience, en mesure de reconnaître les risques liés au maniement de ce produit / système et de les éviter.

Utilisation des produits Siemens conforme à leur destination

Tenez compte des points suivants:

⚠ **ATTENTION**
Les produits Siemens ne doivent être utilisés que pour les cas d'application prévus dans le catalogue et dans la documentation technique correspondante. S'ils sont utilisés en liaison avec des produits et composants d'autres marques, ceux-ci doivent être recommandés ou agréés par Siemens. Le fonctionnement correct et sûr des produits suppose un transport, un entreposage, une mise en place, un montage, une mise en service, une utilisation et une maintenance dans les règles de l'art. Il faut respecter les conditions d'environnement admissibles ainsi que les indications dans les documentations afférentes.

Marques de fabrique

Toutes les désignations repérées par ® sont des marques déposées de Siemens AG. Les autres désignations dans ce document peuvent être des marques dont l'utilisation par des tiers à leurs propres fins peut enfreindre les droits de leurs propriétaires respectifs.

Exclusion de responsabilité

Nous avons vérifié la conformité du contenu du présent document avec le matériel et le logiciel qui y sont décrits. Ne pouvant toutefois exclure toute divergence, nous ne pouvons pas nous porter garants de la conformité intégrale. Si l'usage de ce manuel devait révéler des erreurs, nous en tiendrons compte et apporterons les corrections nécessaires dès la prochaine édition.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
ALLEMAGNE

C79000-G8977-C497-03
Ⓟ 07/2022 Sous réserve de modifications

Sommaire

Avant-propos

1

Ce document décrit comment configurer et gérer SINEC OS. Le document s'adresse au personnel de l'assistance technique des réseaux qui sont familiers de l'exploitation de réseaux. Il est également recommandé pour les concepteurs de réseaux et systèmes ainsi qu'aux programmeurs de systèmes et techniciens de réseaux.

1.1 Security-Disclaimer

Siemens commercialise des produits et solutions comprenant des fonctions de sécurité industrielle qui contribuent à une exploitation sûre des installations, systèmes, machines et réseaux.

Pour garantir la sécurité des installations, systèmes, machines et réseaux contre les cybermenaces, il est nécessaire d'implémenter (et de préserver) un concept de sécurité industrielle global et moderne. Les produits et solutions Siemens constituent une partie d'un tel concept.

Il incombe aux clients d'empêcher tout accès non autorisé à leurs installations, systèmes, machines et réseaux. Ces systèmes, machines et composants doivent uniquement être connectés au réseau d'entreprise ou à Internet dans la mesure où cela est nécessaire et seulement si des mesures de protection correspondantes (p. ex. des pare-feux et/ou la segmentation du réseau) ont été prises.

Pour plus d'informations sur les mesures de protection pouvant être mises en œuvre dans le domaine de la sûreté industrielle, voir à l'adresse : (http://www.siemens.com/industrialsecurity).

Les produits et solutions Siemens font l'objet de développements continus pour être encore plus sûrs. Siemens vous recommande donc vivement d'installer les mises à jour dès qu'elles sont disponibles et de ne toujours utiliser que les versions de produit à jour. L'utilisation de versions obsolètes ou qui ne sont plus prises en charge peut augmenter le risque de cybermenaces.

Afin d'être informé des mises à jour produit dès qu'elles surviennent, abonnez-vous au flux RSS Siemens Industrial Security à l'adresse : (https://www.siemens.com/cert).

1.2 Assistance firmware/logiciel

Informez-vous régulièrement sur les nouvelles versions de firmware/logiciel ou sur les mises à jour de sécurité et appliquez-les. Dès qu'une nouvelle version est publiée, les versions précédentes et leur maintenance ne sont plus prises en charge.

1.3 Open Source

SINEC OS repose sur Linux®. Linux est mis à disposition conformément aux conditions GNU General Public Licence Version 2.0 (https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html).

SINEC OS contient d'autres logiciels Open Source. Vous trouverez la licence d'utilisation dans le document correspondant **Conditions de licence**.

Pour plus d'informations, voir "Informations sur les logiciels Open Source (Page 90)".

1.4 Marques déposées

Les désignations suivantes ainsi que d'autres désignations qui ne sont éventuellement pas repérées par le symbole de marque déposée ®, sont des marques déposées de Siemens AG :

- RUGGEDCOM
- SCALANCE
- SINEC

Linux® est la marque déposée de Linus Torvalds aux États-Unis et dans d'autres pays.

La marque déposée Linux® est, conformément à une sous-licence de LMI, utilisée au niveau mondial par le preneur de licence exclusif de Linus Torvalds, propriétaire de la marque.

1.5 Documents complémentaires

Les documents complémentaires suivants peuvent être utiles. Sauf indications contraires, les documents sont disponibles sous Siemens Industry Online Support (SIOS) (https://support.industry.siemens.com/cs/ww/fr/ps/15247).

Remarque

Les documents mentionnés sont ceux qui étaient disponibles au moment de la publication. Il se peut que des versions plus récentes de ces documents ou des produits correspondants soient disponibles. Pour plus d'informations, consultez le site SIOS ou adressez-vous au service après-vente Siemens.

Notes relatives au produit

Des notes relatives au produit sont disponibles sur le site du SIOS (https://support.industry.siemens.com/cs/ww/fr/ps/15247).

Manuels

Titre du document	Lien
Manuel de configuration SINEC OS CLI	Consultez (https://support.industry.siemens.com/cs/de/fr/ps/15296/man)
Instructions de service SCALANCE XCM-300	Consultez (https://support.industry.siemens.com/cs/de/fr/ps/15296/man)
Instructions de service SCALANCE XRM-300	Consultez

Titre du document	Lien
Instructions de service "SIMATIC NET Gestion de réseau SINEMA Server"	Consultez (https://support.industry.siemens.com/cs/ww/en/view/109748925)
Instructions de service "SIMATIC NET Gestion de réseau SINEC PNI"	Consultez (https://support.industry.siemens.com/cs/products?mfn=ps&pnid=26672&lc=fr-WW)
Manuel de diagnostic "SIMATIC NET Gestion de réseau Diagnostic et configuration avec SNMP"	Consultez (https://support.industry.siemens.com/cs/ww/fr/view/103949062)

1.6 Programme de formation

Siemens propose un programme de formation complet de stages standard sur les réseaux, commutateurs et routeurs Ethernet ainsi que des cours personnalisés sur site prenant en compte les besoins, l'expérience et les conditions d'application du client.

L'équipe de formation de Siemens fournit aux clients les compétences pratiques de base afin que les utilisateurs disposent des connaissances et de l'expertise appropriées pour comprendre les différentes technologies associées à l'infrastructure complexe d'un réseau de communication.

Grâce à ses vastes connaissances en matière d'informatique et de télécommunications, combinées à sa connaissance des marchés de l'énergie, des transports et de l'industrie, Siemens peut proposer des formations adaptées aux applications de ses clients.

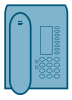
Pour plus d'informations sur le programme de formation et sur la disponibilité des cours, consultez le Programme de formation (https://support.industry.siemens.com/cs/ww/fr/sc/2226) ou contactez un représentant commercial Siemens.

1.7 Service après-vente

Le service se tient la disposition des clients Siemens- 24 heures sur 24, 7 jours sur 7. Pour l'assistance technique ou des informations générales, contactez Siemens par l'un des moyens suivants :

En ligne

Consultez (https://www.siemens.com/automation/support-request), pour nous adresser une demande d'assistance (Support Request, SR) ou pour connaître l'état d'avancement d'une demande d'assistance en cours de traitement.



Téléphone

Contactez un centre d'assistance téléphonique régional pour nous adresser une demande d'assistance (Support Request, SR) par téléphone. Pour trouver un centre d'assistant téléphonique régional, consultez (https://www.automation.siemens.com/aspa-db/fr/automation-techology/Pages/default.aspx).

Appli mobile

Installez l'appli mobile de l'Industry Online Support de Siemens AG sur un mobile Android, iOS ou Windows. L'application vous offre les possibilités suivantes :

- L'accès à la vaste bibliothèque de documents d'assistance Siemens y compris à la Foire aux questions (FAQ) et aux manuels.
- Adresser des demandes d'assistance ou consulter l'état d'avancement d'une demande d'assistance.
- Contacter un représentant commercial Siemens des domaines Ventes, Assistance technique, Formation, etc.
- Poser des questions ou partager des connaissances avec d'autres clients Siemens et la communauté d'assistance

Introduction

2

Bienvenue dans le manuel de configuration Web UI SINEC OS. Ce document explique comment configurer votre appareil via l'interface utilisateur Web de SINEC OS.

Remarque

L'interface utilisateur Web de SINEC OS offre des options de configuration limitées et un aperçu de caractéristiques de performance sélectionnées. Des informations complètes sur la configuration et l'exploitation sont disponibles via la Command Line Interface (CLI). Ce document ne décrit donc que les fonctions limitées de l'interface utilisateur Web.

Vous trouverez des informations sur la configuration complète de SINEC OS ainsi que sur les concepts et marches à suivre, dans le **manuel de configuration CLI SINEC OS**.

2.1 Fonctions et avantages

Vous trouverez ci-après une description des nombreuses fonctions de SINEC OS et de ses avantages :

- **Sécurité du réseau**
  Dans de nombreux secteurs où des réseaux d'automatisation et de communication avancés jouent un rôle essentiel pour les applications critiques, la sécurité des réseaux est devenue un enjeu majeur. SINEC OS comprend les fonctions de sécurité suivantes pour répondre aux questions de sécurité au niveau du réseau local :

Mots de passe	Les mots de passe utilisateur multiniveaux protègent contre les modifications de configuration non autorisées.
SSH/SSL	La protection par mot de passe a été complétée par le cryptage des données et mots de passe transmis sur le réseau.
Activation/désactivation des interfaces	Il est possible de bloquer le trafic de données sur certaines interfaces.
VLAN (IEEE 802.1Q)	Le trafic de données est séparé logiquement sur des interfaces prédéfinies.
SNMPv3	Authentification et sécurité d'accès cryptées
CEI 62443-4-1	Conçu et certifié selon le processus SDL (Secure Development Lifecycle) de la norme CEI 62443-4-1 par le contrôle technique allemand TÜV SÜD.
HTTPS	Accès à l'interface utilisateur web (UI).
SFTP	Pour le transfert de données sécurisé
Management ACL	Restriction d'accès de gestion à des hôtes distants sélectionnés
RADIUS	Authentification de l'utilisateur basée UDP via des serveurs d'authentification distants

- **Command Line Interface (CLI)**
  Une CLI, utilisée en combinaison avec un interprète de commande distant permet d'automatiser les interrogations de données, les modifications de configuration et les mises à jour de firmware. Une CLI performante permet à des utilisateurs expérimentés d'interroger sélectivement n'importe quel paramètre disponible et de le modifier.
- **Web User Interface (Web UI)**
  SINEC OS propose une interface utilisateur graphique pour la configuration et la surveillance à l'aide d'un navigateur Internet standard.
- **NETCONF**
  Le protocole NETCONF (NETwork CONFiguration) permet de configurer et de surveiller à distance des appareils SINEC OS via SSH à l'aide du langage XML (Extensible Markup Language). Il permet d'exécuter diverses opérations telles que l'édition et l'interrogation de données de configuration et d'exploitation sur un appareil SINEC OS (ou un serveur NETCONF) à partir d'un client NETCONF, exécuté sur votre PC.
  NETCONF utilise une simple procédure de remote call (RPC). Certaines commandes RPC sont échangées entre serveur et client NETCONF en format XML. La communication étant basée session, un utilisateur peut bloquer certaines mémoires de données de configuration pendant qu'il édite un appareil.
  NETCONF peut être utilisé pour modifier ou interroger directement un appareil ou être intégré à des scripts de commande.
  Pour plus d'informations sur l'utilisation de NETCONF voir "NETCONF pour SINEC OS Manuel de référence".
  Pour plus d'informations sur la configuration de sessions NETCONF sous SINEC OS, voir "Configuration de l'interface utilisateur NETCONF (Page 53)".
- **Simple Network Management Protocol (SNMP)**
  SNMP propose une procédure standardisée permettant à des stations de gestion de réseau d'interroger des appareils de divers constructeurs. SINEC OS prend en charge les versions v1, v2c et v3. Il est, d'une manière générale, recommandé d'utiliser SNMPv3, cette version proposant des fonctions de sécurité (telles que l'authentification et la protection des données) qui n'existaient pas sur les versions précédentes.
  SINEC OS prend par ailleurs en charge de nombreuses MIB (Management Information Base) facilitant l'intégration dans n'importe quel système de gestion de réseau (NMS). La possibilité de générer des notifications lorsque surviennent des évènements système est une des fonctions de SNMP prise en charge par SINEC OS.
- **PROFINET**
  PROFINET (Process Field Network) répond à toutes les exigences de l'automatisation de procédés et constitue la base des installations de l'industrie des procédés. En tant que standard ouvert de la communication par bus de terrain, PROFINET réunit les avantages du standard de bus de terrain éprouvé qu'est PROFIBUS DP et ceux du standard de réseau Industrial Ethernet. PROFINET définit un modèle de communication, d'automatisation et d'ingénierie non propriétaire pour l'automatisation industrielle. Avec des topologies en ligne, en anneau, des topologies arborescentes et en étoile ainsi qu'avec des réseaux à multicontrôleurs, PROFINET propose des options individuelles d'architecture de réseau.

- **EtherNet/IP (EIP)**
  EtherNet/IP est un standard de bus de terrain ouvert basé sur le protocole d'application Common Industrial Protocol (CIP), conçu pour une mise en œuvre en environnement industriel et dans des applications à temps critique. Outre le protocole CIP, EtherNet/IP supporte également l'Ethernet standard, le protocole Internet ainsi que TCP et UDP. Cette compatibilité avec des protocoles établis permet une intégration facile d'EtherNet/IP dans les réseaux. EtherNet/IP assure la continuité entre le réseau bureautique et l'installation à commander.
- **Device Level Ring (DLR)**
  Device Level Ring est une procédure redondante de couche 2 pour EtherNet/IP. Elle permet de réaliser des topologies en anneau avec EtherNet/IP. En cas d'interruption de la chaîne de communication, la communication est maintenue via un chemin redondant.
- **Réseaux locaux virtuels (VLAN)**
  Les VLAN permettent de diviser un réseau physique en réseaux logiques distincts avec des domaines de diffusion indépendants. Un certain niveau de sécurité est fourni, car les hôtes ne peuvent accéder qu'à d'autres hôtes dans le même VLAN, les tempêtes de données étant ainsi isolées. SINEC OS prend en charge les trames Ethernet taguées selon IEEE 802.1Q et les trunks de VLAN. La classification en fonction des interfaces permet d'affecter les appareils au VLAN correct.
  Une prise en charge GVRP supplémentaire est disponible pour simplifier la configuration de commutateurs au sein du VLAN.
- **Classes de trafic**
  Les classes de trafic organisent les trames entrantes en fonction de la priorité qui leur est attribuée et les affectent à des files d'attente de classes de trafic où elles attendent d'être retransmises. Les trames possédant une priorité spécifique peuvent être placées dans une file d'attente de haute priorité, devant celles de la file d'attente suivante, où elles sont retransmises avant celles de la file d'attente suivante. Cette possibilité sert à réduire l'impact de la latence et de la gigue sur les applications temps réel critiques pour le système.
- **Network Time Protocol (NTP)**
  Network Time Protocol synchronise automatiquement l'horloge interne de tous les appareils compatibles NTP du réseau. Ceci permet, lors d'un diagnostic d'erreurs, d'utiliser des horodatages servant à analyser les relations entre les évènements.
- **Synchronisation d'horloge SIMATIC**
  La méthode de synchronisation d'horloges SIMATIC permet à un appareil de synchroniser sa date/heure système avec celle d'autres composants SIMATIC du sous-réseau Industrial Ethernet local.
- **Passage à l'heure d'été/hiver**
  Configurez la date/heure système pour le changement d'heure automatique si le fuseau horaire que vous avez choisi passe à l'heure d'été.
- **Limitation de la vitesse de transmission**
  La limitation de la vitesse de transmission ou de la vitesse de transmission au niveau des ports limite le flux de trafic de données sur des interfaces spécifiques. Cela peut s'avérer crucial pour la gestion de la précieuse bande passante du réseau pour les fournisseurs de services. Elle offre également une protection contre les attaques par déni de service (Denial of service, DoS).
- **Discovery and Basic Configuration Protocol (DCP)**
  DCP est utilisé par PROFINET pour définir à distance le nom et l'adresse IP de la station. DCP est utile pour les applications qui ne possèdent pas de serveur DHCP.

- **Domain Host Communication Protocol (DHCP)**
  DHCP permet d'intégrer et de configurer rapidement des appareils dans le réseau. Les appareils compatibles DHCP obtiennent leurs paramètres de configuration TCP/IP d'un serveur DHCP central dès qu'ils sont connectés au réseau.
- **Configuration d'interface et état**
  Vitesse, duplex intégral, autonégociation, contrôle de flux et autres paramètres peuvent être configurés pour différents ports de pont. Ceci permet à l'appareil d'établir des connexions opérationnelles avec des appareils sans négociation ou qui ne possèdent pas des paramètres par défaut.
- **Statistiques d'interface**
  Des statistiques mises à jour en continu sont disponibles via une interface, des compteurs détaillés pour trames (d'entrée et de sortie) et octets de trame ainsi que des nombres d'erreurs détaillés !
- **Journalisation d'évènements et alarmes**
  Tous les évènements importants sont enregistrés dans un journal système non volatile, ce qui permet un traitement complet des erreurs. Les évènements incluent notamment la défaillance et la restauration de liens, l'accès non autorisé et le diagnostic d'autotest. Les alarmes fournissent un instantané des évènements récents que l'administrateur réseau doit encore acquitter. Un relais matériel externe peut être mis hors tension en présence d'alarmes critiques afin qu'une commande externe puisse, si nécessaire, réagir.

2.2 Recommandations de sécurité

Conformez-vous aux recommandations de sécurité ci-après, pour mettre l'appareil et/ou le réseau à l'abri de toute intrusion.

Général

- Contrôlez régulièrement l'appareil pour vous assurer que ces recommandations et/ou autres stratégies de sécurité internes sont bien appliquées.
- Évaluez la sûreté de votre site et mettez en place un concept de protection cellulaire avec des produits appropriés.
  Pour plus d'informations, voir Site Web Industrial Security (https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security.html).
- Consultez la documentation utilisateur des autres produits Siemens que vous utilisez avec l'appareil pour voir s'ils contiennent d'autres recommandations de sécurité.
- Veillez, à l'aide de la connexion à distance, à ce que le journal système soit transmis à un serveur de connexion central. Veillez à ce que le serveur se trouve dans un réseau protégé et vérifiez régulièrement dans les journaux l'absence de violations de sécurité ou de points faibles.
  Pour plus d'informations, voir "Configuration de la journalisation système distante (Page 296)".

Authentification

IMPORTANT
Risque d'intrusion - risque de perte de données Ne perdez pas les mots de passe de l'appareil. L'accès à l'appareil peut être rétabli par restauration des paramètres d'usine, ce qui supprimera toutes les données de configuration.

- Remplacz les mots de passe par défaut de tous les comptes utilisateur, modes d'accès et applications (s'il y a lieu) avant d'utiliser l'appareil.
- Utilisez des mots de passe robustes. Évitez d'utiliser des mots de passe faibles (tels que motdepasse1, 123456789, abcdefgh) ou des caractères qui se répètent (tels que abcabc). Cette recommandation vaut également pour les mots de passe/clés symétriques configurés sur l'appareil.
- Veuillez vous assurer que les mots de passe sont protégés et uniquement communiqués au personnel habilité.
- N'utilisez pas des mots de passe identiques pour plusieurs noms d'utilisateur et systèmes.
- Conservez les mots de passe en un endroit sûr (pas en ligne) pour les avoir sous la main en cas de perte.
- Modifiez les mots de passe régulièrement et souvent.
- Si l'identification a lieu via RADIUS, veuillez vous assurer que toutes les communications ont bien lieu au sein du périmètre de sécurité ou sont protégées par une voie sûre.
- Méfiez-vous des protocoles Link-Layer qui ne possèdent pas de propre authentification entre les nœuds d'extrémité, tels que ARP ou Ipv4. Il se pourrait qu'une unité malveillante exploite les points faibles de ces protocoles pour attaquer les hôtes, commutateurs et routeurs connectés à votre réseau de couche 2 et pour empoisonner les caches ARP des systèmes du sous-réseau et intercepter ensuite le trafic de données. En présence de protocoles de couche 2 peu sûrs, il convient de mettre en place des mesures de sécurité appropriées pour empêcher toute intrusion dans le réseau. Il est possible entre autres d'empêcher un accès physique au réseau local ou d'utiliser des protocoles sûrs des couches supérieures.

Certificats et clés

- Si vous soupçonnez une violation de sécurité, modifiez immédiatement tous les certificats et toutes les clés.
- Des clés SSH et SSL sont à la disposition des utilisateurs Admin. Veuillez vous assurer que vous prenez bien des mesures de sécurité appropriées lorsque vous expédiez l'appareil hors de l'environnement habituel :
  - Remplacez les clés SSH et SSL par des clés jetables avant l'expédition.
  - Mettez les clés SSH et SSL existantes hors service. Créez et programmez au retour de l'appareil de nouvelles clés pour l'appareil.
- Utilisez des certificats au format "PKCS #12", protégés par mot de passe.
- Utilisez des certificats possédant une longueur de clé de 4096 bits.

- Avant de retourner l'appareil à Siemens pour réparation, remplacez les clés et certificats courants par des clés et certificats temporaires jetables que vous pourrez détruire lorsque l'appareil vous sera retourné.
- Contrôlez les certificats et empreintes digitales sur le serveur pour éviter ainsi toute attaque dite de l'homme du milieu (MitM, Man-in-the-Middle).

Accès physique/ distant

- Exploitez les appareils uniquement dans une zone protégée du réseau. Si le réseau interne est découplé du réseau externe, un attaquant n'a pas accès aux données internes.
- Réservez l'accès physique à l'appareil exclusivement au personnel digne de confiance. Un utilisateur malveillant qui se serait procuré les supports amovibles de l'appareil pourrait en extraire des informations sensibles telles que certificats, clés, etc. (les mots de passe des utilisateurs sont protégés par des codes de hachage) ou reprogrammer les supports.
- Contrôlez l'accès à la console série avec la même minutie que tout accès à l'appareil.
- Il est instamment recommandé de laisser la protection contre les attaques par force brute (BFA, Brute-force-attack) activée pour empêcher toute intrusion à l'appareil.
  Pour plus d'informations, voir "Prévention des attaques par force brute (Page 119)".
- Si vous communiquez via des réseaux non sûrs, utilisez des appareils complémentaires compatibles VPN, permettant de crypter et d'authentifier les communications.
- Si vous établissez une communication sécurisée à un serveur (pour une mise à niveau sûre par exemple), veillez à ce que le serveur utilise des méthodes de cryptage et des protocoles robustes.
- Mettez correctement fin aux liaisons de gestion (HTTP, HTTPS, SSH p. ex.).
- Veuillez vous assurer que l'appareil a été intégralement mis hors tension avant de le mettre hors service.
  Pour plus d'informations, voir "Mise hors service l'appareil (Page 74)".

Protocoles sûrs/peu sûrs

- Utilisez des protocoles sûrs si l'appareil n'est pas sécurisé par des mesures de protection physiques.
- Désactivez ou limitez la mise en œuvre de protocoles non sûrs. Certains protocoles sont effectivement sûrs (par ex, HTTPS, SSH, 802.1X, etc.), d'autre en revanche n'ont pas été développés dans le but de sécuriser des applications (par ex. SNMPv1/v2c, RSTP etc.).
  En présence de protocoles peu sûrs, il convient de mettre en place des mesures de sécurité appropriées pour empêcher toute intrusion dans l'appareil/e réseau.
- Si l'utilisation de protocoles peu sûrs s'impose, veuillez vous assurer que l'appareil est exploité dans une zone protégée du réseau.
- S'il existe une alternative sûre pour un protocole, utilisez cette dernière. Exemple :
  - Utilisez HTTPS au lieu de HTTP.
  - Utilisez SNMPv3 au lieu de SNMPv1/V2c.

- Évitez ou limitez la mise en œuvre de :
  - protocoles non authentifiés ou non cryptés
  - Link Layer Discovery Protocol (LLDP)
- Veuillez vous assurer, après la mise en service, que les droits d'accès paramétrés du Discovery and Configuration Protocol (DCP) sont "lecture uniquement".

Matériel/Logiciel

- Limitez la mise en œuvre d'applications critiques et l'accès aux services d'administration aux réseaux privés. La connexion d'un appareil SINEC OS à Internet est possible. Il faut cependant faire preuve des plus grandes précautions en protégeant l'appareil et le réseau auquel il est connecté par des mécanismes sûrs tels pare-feu ou IPsec.
- Utilisez autant que faire se peut des VLAN pour vous protéger contre les attaques de déni de service (DoS) et intrusions.
- Des services choisis sont activés par défaut dans SINEC OS. Il est recommandé de n'activer que les services qui sont indispensables pour votre installation.
  Pou plus d'informations sur les services disponibles, voir "Services disponibles (Page 28)".
- Utilisez la version de navigateur Web la plus récente compatible SINEC OS pour vous assurer que les méthodes de cryptage mises en œuvre sont les sûres. En outre, la répartition d'enregistrements 1/n-1 est activée dans les versions les plus récentes des navigateurs Web Mozilla Firefox, Google Chrome et Microsoft Edge ce qui réduit le risque d'attaques telles que SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST p. ex.).
- Veuillez vous assurer que vous avez installé la dernière version du firmware y compris tous les correctifs de sécurité.
  Vous trouverez les dernières informations en date sur les correctifs de sécurité des produits Siemens sur la page Web Industrial Security (https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security.html) ou ProductCERT Security Advisories (https://www.siemens.com/global/en/home/products/services/cert.html).
  Vous obtiendrez des mises à jour des Security Advisories pour produits Siemens en vous connectant au flux RSS de la page Web ProductCert Security Advisories ou en suivant @ProductCert sur Twitter.
- Activez uniquement les services qui sont utilisés sur l'appareil, y compris les ports physiques. Les ports physiques libres sont des points d'accès potentiels au réseau auquel l'appareil est connecté.
- Pour une sécurité optimale, utilisez toujours lorsque c'est possible les mécanismes d'authentification et de cryptage de SNMPv3 de même que des mots de passe robustes.

- Les fichiers de configuration peuvent être téléchargés de l'appareil. Veuillez vous assurer que les fichiers de configuration sont bien protégés. Vous pouvez les protéger par une signature numérique, les crypter, les enregistrer en un lieu sûr ou en ne transmettant les fichiers de configuration que par des voies de communication sûres.
  Les fichiers de configuration peuvent être protégés lors du téléchargement par mot de passe.
  Pour plus d'informations sur la protection par mot de passe des fichiers de configuration, voir "Enregistrement le la configuration courante sous forme de fichier sur un serveur distant (Page 84)".
- En cas d'utilisation de SNMP (Simple Network Management Protocol) :
  - Configurez SNMP de sorte qu'un message soit émis lorsque des erreurs d'authentification surviennent.
    Pour plus d'informations, voir "SNMP (Page 233)".
  - Veuillez vous assurer que les Standard-Community-Strings soient convertis en valeurs uniques.
  - Utilisez toujours SNMPv3 lorsque c'est possible. SNMPv1 et SNMPv2c sont considérés comme peu sûrs et ne devraient être utilisés qu'en cas d'absolue nécessité.
  - Évitez surtout autant que possible l'accès en écriture.

2.3 Capacités fonctionnelles

Vous trouverez ci-après un récapitulatif des valeurs limites des différentes fonctions de SINEC OS :

Sécurité des données

Fonction		Valeur limite
Clés et certificats	Paires de clés	5
	Certificats par paire de clés	2
	Portefeuilles de certificats	2
	Certificats par portefeuille de certificats	5
	Trousseaux de clés	5
	Hôtes connus par trousseau de clés	5
ACL de gestion	Entrées de règles	64

Administration système

Fonction		Valeur limite
Utilisateurs	Nombre d'utilisateurs	30
Sessions	Nombre de sessions CLI	8
	Nombre de sessions NETCONF	4
	Nombre de sessions SNMP	4
	Nombre de sessions d'interface utilisateur Web	4
	Taille de tampon (Octets) par session SSH	16834

Attribution d'adresses IP

Fonction		Valeur limite
DNS	Nombre de serveurs DNS	3
	Nombre de domaines DNS	6
DHCP	Nombre de clients DHCP	1

Administration d'interfaces

Fonction		Valeur limite
Adresses MAC	Nombre d'entrées de filtre d'adresses MAC unicast statiques	256
Table d'adresses MAC	Nombre d'adresses MAC apprises dynamiquement	4096

Découverte de réseau et gestion

Fonction		Valeur limite
SNMP	Nombre de paramètres cibles	16
	Nombre de cibles	16
	Nombre de notifications	16
	Nombre de communautés	16
	Nombre de vues	16
	Nombre de groupes	16
	Nombre d'utilisateurs	16
ARP	Nombre d'entrées ARP	512

Contrôle et classification de trafic de données

Fonction		Valeur limite
VLAN	Nombre de VLAN de couche 2	255
	Nombre de VLAN de couche 3	17
	Adresses IPv4 statiques par VLAN	1
	ID de VLAN disponibles	1 – 4094
Classes de trafic	Nombre d'affectations priorité/trafic par file d'attente	8
	Nombre d'affectations DSCP/classe de trafic par file d'attente	64

Services d'horloge

Fonction		Valeur limite
NTP	Nombre de serveurs NTP	1

Filtre Multicast

Fonction		Valeur limite
Général	Nombre de flux Multicast installés dans le système	1023
IGMP	Nombre d'entrées de retransmission de groupes IGMP de couche 2	256
	Nombre d'entrées de retransmission de groupes IGMP de couche 3	1024
GMRP	Nombre de groupes multicast appris	1024

Diagnostic

Fonction		Valeur limite
Journal système	Nombre d'entrées dans le journal d'incidents	1000
	Nombre de serveurs Syslog distants	5
SMTP	Nombre de serveurs SMTP	1
	Nombre de destinataires d'e-mail	20

2.4 Services disponibles

La liste ci-après récapitule tous les protocoles et services disponibles ainsi que leurs ports qui permettent d'accéder à l'appareil, y compris les informations ci-après :

- **Service**
  Service pris en charge par l'appareil.
- **Protocole**
  Protocole utilisé par le service.
- **Numéro de port**
  Numéro de port affecté au service.
- **État par défaut**
  État prédéfini du service (c.-à-d. ouvert, fermé, actif)
- **Service configurable**
  Indique si le service peut être configuré ou non.
- **Numéro de port configurable**
  Indique si le numéro de port peut être configuré.
- **Authentification**
  Indique si l'authentification du partenaire de communication a lieu ou si une authentification peut être configurée.
- **Cryptage**
  Indique si la transmission est cryptée ou si le cryptage est configurable.

Service	Proto-cole	Port numéro	État par défaut	Service configurable	Numéro de port configu-rable	Authentifica-tion	Cryptage
PROFINET	UDP	34964	Ouvert	-	-	-	-
SNMPv1/v2c	UDP	161	Fermé	✓	✓	Configurable	-
SNMPv3	UDP	161	Fermé	✓	✓	Configurable	Configurable
SSH	TCP	22	Ouvert	✓	✓	✓	✓
SSH/NETCONF	TCP	830	Ouvert	✓	✓	✓	✓
DCP	-	-	Actif	✓	-	-	-
LLDP	-	-	Actif	✓	-	-	-
Ping	ICMP	-	Actif	-	-	-	-
NTP	UDP	123	Fermé	✓	-	-	-
Ethernet/IP	TCP	44818	Fermé	✓	-	-	-
HTTP	TCP	80	Ouvert	✓	✓	✓	-
HTTPS	TCP	443	Ouvert	✓	✓	✓	✓

2.5 Droits d'accès

Un profil d'utilisateur qui définit les droits d'accès aux fonctions de l'appareil est attribué aux utilisateurs. Les droits d'accès s'appliquent de la même manière à toutes les interfaces utilisateurs.

Les utilisateurs possédant le profil d'utilisateur **Admin** disposent des pleins droits d'accès en écriture et en lecture aux fonctions de l'appareil. Les utilisateurs possédant le profil d'utilisateur **Guest** disposent de droits d'accès limités.

Les droits d'accès suivants sont disponibles :

- **Read (R)** - L'utilisateur peut consulter la configuration.
- **Create (C)** - L'utilisateur peut créer de nouvelles configurations.
- **Update (U)** - L'utilisateur peut modifier les configurations existantes.
- **Delete (D)** - L'utilisateur peut supprimer des configurations.
- **Execute (E)** - L'utilisateur peut exécuter des commandes.
- **No** - L'utilisateur ne possède pas de droits d'accès.

Le tableau ci-après montre les **droits d'accès de base** des profils utilisateurs. Les dérogations sont décrites dans des tableaux distincts.

	Droits d'accès par profil d'utilisateur	
	Admin	**Guest**
Toutes les actions	E	No
Toutes les données de configura-tion	R/C/U/D	R
Toutes les données opérationnel-les	R	R

Le tableau suivant présente les dérogations dans les **actions**. L'entrée "-" indique qu'il n'existe pas de dérogation par rapport aux droits d'accès de base.

Activité	Droits d'accès par profil d'utilisateur	
	Admin	Guest
Se connecter avec le compte utilisateur de débogage	No	-
Envoyer un ping sur une adresse IP/un hôte (ping)	-	E
Déterminer le chemin de données vers un hôte (Traceroute)	-	E

Le tableau suivant présente les dérogations dans les **données de configuration**. L'entrée "-" indique qu'il n'existe pas de dérogation par rapport aux droits d'accès de base.

Activité	Chemin admissible	Droits d'accès par profil d'utilisateur	
		Admin	Guest
Configurer le propre compte utilisateur	/system/authentication/user{OWN}	-	R/U
Configurer des utilisateurs locaux	/system/authentication/user	-	No
Configurer le compte utilisateur de débogage	/system/authentication/allow-debug-user	-	No
Configurer des utilisateurs SNMPv3 (USM)	/snmp/usm/local/user	-	No
Configurer des communautés SNMP	/snmp/community	-	No
Configurer des droits d'accès SNMP (VACM)	/snmp/vacm	-	No
Configurer des certificats	/keystore	-	No

Le tableau suivant présente des dérogations dans les **données opérationnelles**. L'entrée "-" indique qu'il n'existe pas de dérogation par rapport aux droits d'accès de base.

Activité	Chemin admissible	Droits d'accès par profil d'utilisateur	
		Admin	Guest
Surveillance de la prévention BFA.	/system/authentication/brute-force-prevention	-	No

2.6 Configuration d'appareil

SINEC OS prend en charge un concept de configuration en deux étapes, selon lequel la configuration en cours d'utilisation sur l'appareil reste inchangée jusqu'à ce que vous validiez les modifications de la configuration. SINEC OS possède pour ce faire de deux mémoires de données :

- **Mémoire de données Running**
  La mémoire de données Running contient la configuration actuellement exécutée sur l'appareil.
- **Mémoire de données candidate**
  La mémoire de données Candidate est une copie de la configuration en cours d'exécution. Vous pouvez créer, ajouter, supprimer et modifier des configurations sans que cela ait un impact sur la configuration en cours d'exécution. Si vous validez les modifications de la configuration, la configuration est transférée de la mémoire Candidate dans la mémoire Running où elle devient la configuration courante.

Une session de configuration typique

Pour pouvoir configurer un appareil, vous devez être connecté(é) avec des droits d'écriture et vous trouver en mode de configuration. Pour plus d'informations sur le mode de configuration, voir "Sélection d'un mode de configuration (Page 40)".

Durant une session de configuration, vous pouvez apporter une ou plusieurs modifications à la configuration. Les modifications de la configuration restent pour le moment inactives et sont enregistrées dans la mémoire de données Candidate. Elles n'ont pas d'effet sur la configuration en cours d'exécution.

Au cours de cette étape de configuration, vous pouvez consulter les modifications de la configuration et la configuration en cours d'exécution. Vous pouvez par ailleurs afficher l'aspect qu'aura la configuration cible après sa validation. Pour plus d'informations, voir "Affichage des modifications de la configuration (Page 40)".

Capacités fonctionnelles

Les capacités fonctionnelles décrites s'appliquent à la configuration enregistrée dans la mémoire de données Running. Pour plus d'informations, voir "Capacités fonctionnelles (Page 26)".

Dans la mémoire de données Candidate, les capacités fonctionnelles sont complétées comme suit : Valeur limite * 2. Ceci est affiché dans le tableau suivant à titre d'exemple pour le serveur DNS :

Fonction	Valeur limite	
	Mémoire de données Running	Mémoire de données Candidate
Nombre de serveurs DNS	3	6

Les capacités fonctionnelles étendues permettent d'échanger une configuration complète. Vous pouvez ajouter à 3 serveurs DNS existants 3 nouveaux serveurs DNS et les configurer avant de devoir supprimer les serveurs DNS existants. Si vous écrasez la valeur limite dans la mémoire de données Candidate, le message d'erreur suivant s'affiche :

Candidate configuration limit exceeded

Pour pouvoir valider les modifications de la configuration, les valeurs limites de la mémoire de données Running doivent être respectées. Le message d'erreur suivant s'affichera sinon dans l'exemple des serveurs DNS :

too many '/system/dns-resolver/server', 6 configured, at most 3 must be configured

Validation des modifications de la configuration

Pour appliquer les modifications de la configuration dans la configuration en cours d'exécution, vous devez les valider explicitement. Vous disposez de plusieurs options pour valider les modifications de la configuration. Pour plus d'informations, voir "Validation des modifications de la configuration (Commit) (Page 41)".

Vous pouvez, avant de valider les modifications de la configuration, vérifier l'absence de conflits avec la configuration en cours d'exécution.

Après la validation réussie des modifications de la configuration, les opérations suivantes sont exécutées :

1. La configuration utilisée avant la modification est horodatée puis sauvegardée afin de pouvoir la restaurer.
2. Une entrée est inscrite dans l'historique des configurations.
3. Une entrée est effectuée dans le journal.
4. Les modifications de la configuration sont intégrées dans la configuration en cours d'exécution. Les utilisateurs qui sont connectés à cet instant sont informés des modifications de la configuration.

Si des conflits surviennent lors de la validation des modifications de la configuration, aucune des modifications n'est appliquée. La configuration en cours d'exécution reste inchangée. Vous pouvez faire afficher les conflits par la commande **Validate**, voir "Vérification des modifications de la configuration (Page 41)".

Restaurer des configurations (Rollback)

Vous pouvez restaurer des valeurs de configuration écrasées et annuler ainsi les modifications précédemment validées. Pour plus d'informations, voir "Restauration d'une configuration (Rollback) (Page 43)".

2.7 Fonctions prises en charge

L'interface utilisateur Web ne permet de configurer et d'afficher que certaines fonctions. Pour toutes les autres fonctions, utilisez l'interface de ligne de commande (CLI) de SINEC OS.

Le tableau suivant donne un aperçu des fonctions disponibles via l'interface utilisateur Web :

◯ Pas pris en charge, ◐ partiellement prise en charge, ● entièrement prise en charge

Poste	Interface utilisateur Web	CLI
Configuration des interfaces utilisateur	◐	●
Paramètres de base	●	●
Firmware	◐	●

Poste	Interface utilisateur Web	CLI
Matériel de l'appareil	◐	●
Fichier de configuration	●	●
Contact de signalisation	●	●
Fonction de bouton-poussoir	●	●
Configuration License PLUG	●	●
Stratégie de mot de passe	●	●
Gestion des utilisateurs	●	●
Debug	◐	●
Prévention des attaques par force brute	●	●
Clés et certificats	◐	●
Authentification de l'utilisateur	●	●
Ports de pont	●	●
Interfaces VLAN	●	●
Table d'adresses MAC	●	●
Attribution d'adresses IP statiques	●	●
DNS statique	◐	●
DHCP	◐	●
Spanning Tree Protocol	○	●
Détection de boucles de réseau	●	●
LLDP	◐	●
DCP	●	●
PROFINET	◐	●
ARP	●	●
SNMP	◐	●
Limitation de la vitesse de transmission	●	●
VLAN	◐	●
Classes de trafic	●	●
Date et heure système	●	●
Décalage horaire et heure d'été	◐	●
NTP	●	●
SIMATIC Time	○	●
PTP	○	●

Poste	Interface utilisateur Web	CLI
Groupes multicast statiques	●	●
GMRP	◐	●
IGMP Snooping	●	●
Base de données de filtrage multicast	●	●
État du système	●	●
Gestion des évènements	◐	●
Ping	○	●
Traceroute	○	●
Journal système	◐	●
SMTP	●	●
Réplication de trafic de données	●	●
Diagnostic de câbles	●	●

2.8 Navigateurs Internet pris en charge

La représentation de l'interface utilisateur Web a été testée avec les navigateurs Internet suivants :

Navigateur Internet	Version
Google Chrome	77
Mozilla Firefox	70
Mozilla Firefox ESR	68

Remarque

L'utilisation de Microsoft Internet Explorer n'est pas autorisée.

SINEC OS Web UI n'est pas autorisé à être utilisé avec Microsoft Internet Explorer. N'utilisez SINEC OS Web UI qu'avec les navigateurs Internet mentionnés ci-dessus.

Interface utilisateur

3

Ce chapitre indique comment utiliser l'interface utilisateur Web SINEC OS (Web UI).

3.1 Interface utilisateur

Cette section décrit la structure de l'interface utilisateur graphique Web UI.

3.1.1 Page d'ouverture de session

La figure ci-après montre la page d'ouverture de session.

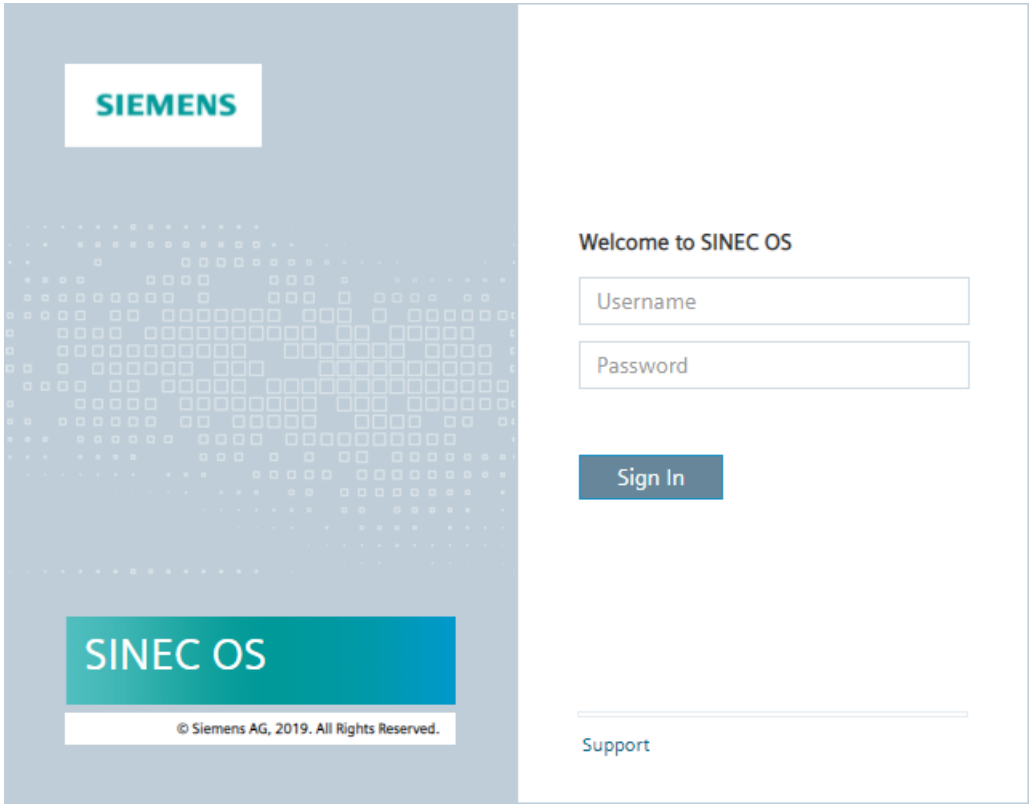


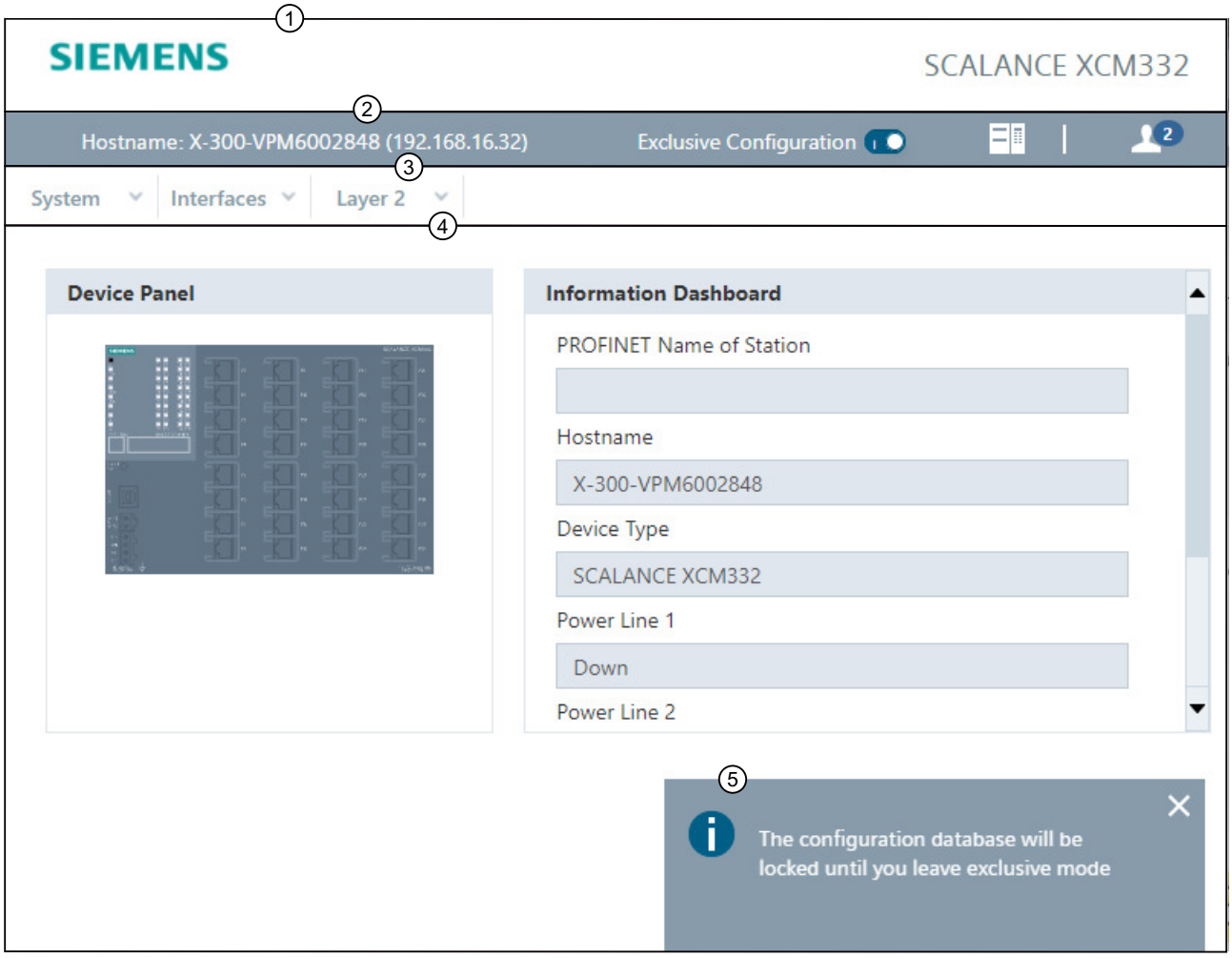
Figure 3-1 Page d'ouverture de session de l'IU Web de SINEC OS

Les éléments suivants sont disponibles sur la page d'ouverture de session :

- **Welcome to SINEC OS**
  Pour plus d'informations sur l'ouverture de session de l'IU Web, voir "Connexion (Page 66)".
- **Support**
  Si vous cliquez sur le lien **Support**, la page Internet du Siemens Industry Online Support s'ouvre dans un nouvel onglet.

3.1.2 Page d'accueil

Si vous vous êtes connecté avec succès, la page accueil s'affiche. La figure ci-après qui prend pour exemple la page d'accueil, montre les différentes zones de l'IU Web.



① Barre d'entête
② Barre d'état
③ Barre de navigation
④ Volet de contenu
⑤ Messages

Figure 3-2 Page d'accueil de l'IU Web de SINEC OS

Le tableau suivant décrit les zones de l'IU Web.

	Zone	Description
①	Barre d'entête	Les éléments suivants sont disponibles dans la barre d'état : • **Logo de Siemens AG** Si vous cliquez sur le logo SIEMENS, vous chargez la page d'accueil de l'IU Web. • **Nom de l'appareil** Le nom d'appareil indique à quel appareil vous êtes connecté. Vous ne pouvez pas modifier ce nom d'appareil.
②	Barre d'état	Pour plus d'informations, voir "Barre d'état (Page 38)".
③	Barre de navigation	La barre de navigation vous propose plusieurs menus. Cliquez sur les différents menus pour afficher les sous-menus. Les sous-menus contiennent des pages qui vous permettent de vérifier et de modifier la configuration de l'appareil. Ces pages sont toujours affichées dans le volet de contenu.
④	Volet de contenu	Le volet de contenu affiche les pages d'information et de configuration.
⑤	Messages	Les messages s'affichent au bord inférieur droit de l'IU Web. Les symboles indiquent s'il s'agit de conseils ou de questions de sécurité.

3.1.3 Barre d'état

Les fonctions suivantes sont disponibles dans la barre d'état :

Désignation	Symbole		Description
Hostname	-		Le nom d'hôte est un code qui facilite l'identification de l'appareil au sein du réseau. Le nom d'hôte forme également l'invite de commande de la CLI (p. ex. localhost#). Pour plus d'informations sur le nom d'hôte, voir "Modification du nom d'hôte (Page 69)".
Adresse IP	-		L'adresse IP du VLAN par défaut (VLAN 1) est affichée entre parenthèses à la suite du nom d'hôte.
Exclusive rights on/off		Désactivée (par défaut)	Le curseur permet d'activer ou de désactiver la configuration exclusive : • **Désactivée** Le mode configuration partagée est actif. • **Activé** Le mode configuration exclusive est actif. Pour plus d'informations sur le mode de configuration, voir "Sélection d'un mode de configuration (Page 40)".
		Activé	

Désignation	Symbole		Description
Transactions de configuration		Pas de modifications de la configuration (par défaut)	Lorsque vous cliquez sur l'icône, la zone des transactions de configuration s'affiche dans le volet de contenu à partir du bord droit de la fenêtre du navigateur. Les pages d'information et de configuration sont toujours disponibles. Dès que vous modifiez la configuration actuelle de l'appareil, ces changements apparaissent sur l'icône des transactions de configuration. Vous pouvez effectuer plusieurs modifications avant de les valider. Ce chiffre indique le nombre de modifications effectuées depuis la dernière confirmation. La zone des transactions de configuration contient les fonctions suivantes : • Liste de candidats • Boutons pour vérifier, valider ou rejeter les modifications Pour plus d'informations, voir "Transactions de configuration (Page 39)".
		Avec des changements de configuration non validés	
		Une erreur s'est produite lors de la vérification ou de la confirmation des modifications de configuration.	
		Les modifications de la configuration sont valables.	
Profil d'utilisateur			Si vous cliquez sur l'icône, les informations suivantes s'affichent : • **Username** - Nom de l'utilisateur connecté. • **IP Address** - Adresse IP du PC client par lequel l'utilisateur accède à l'IU Web • **System Time** - Date/heure système actuelle • **Session Timer** - Temporisation jusqu'à la déconnexion automatique de l'utilisateur Si l'utilisateur n'utilise pas l'IU Web, la session IU Web est automatiquement fermée au bout de 15 minutes. Vous pouvez modifier ou désactiver la temporisation. • **Log in/out Messages** - Si cette fonction est activée, des messages s'affichent lorsque les utilisateurs se connectent ou se déconnectent de l'appareil. Cela vaut également pour les accès via SNMP. Si la fonction est désactivée, ces messages ne s'affichent pas. • **Logout** - Bouton de déconnexion Ce chiffre indique le nombre d'utilisateurs connectés à l'appareil.

3.2 Transactions de configuration

Cette section décrit comment gérer les modifications de configuration. Par transactions de configuration, on entend toutes les activités ayant lieu dans le contexte de la configuration, telles que le contrôle, la validation ou l'annulation de modifications de la configuration.

3.2.1 Sélection d'un mode de configuration

Vous pourrez alterner pour la configuration entre un mode configuration partagée et un mode configuration exclusive.

- **Mode configuration partagée**
  Plusieurs utilisateurs peuvent accéder à l'appareil. Toutes les modifications sont occultées pour les autres utilisateurs tant qu'elles n'ont pas été validées.
  Les modifications doivent être validées pour qu'elles puissent être appliquées à la configuration active.
  Ce mode est activé par défaut.
- **Mode configuration exclusive**
  Un seul utilisateur peut activer la configuration exclusive sur un appareil. D'autres utilisateurs peuvent accéder à l'appareil en parallèle. Tant qu'un utilisateur a activé la configuration exclusive, les autres utilisateurs ne peuvent pas appliquer leurs modifications.
  Toutes les modifications de la session de configuration exclusive sont occultées pour les autres utilisateurs jusqu'à ce qu'elles soient validées. Les modifications doivent être validées pour qu'elles puissent être appliquées à la configuration active.
  Dès qu'un session de configuration exclusive est fermée par une déconnexion manuelle, un timeout ou une coupure de la connexion, le blocage est levé.
  Si vous activez ou désactivez la configuration exclusive comportant des modifications en suspens, un message qui vous demande si vous voulez annuler les modifications s'affiche dans la zone de notification.

Pour plus d'informations sur le changement de mode de configuration, voir "Barre d'état (Page 38)".

3.2.2 Affichage des modifications de la configuration

Pour afficher les modifications non validées de la configuration, cliquez sur le bouton **Transactions de configuration**.

La zone des transactions de configuration s'affiche, à partir du bord droit de la fenêtre du navigateur, dans le volet de contenu. Les pages d'information et de configuration sont toujours disponibles.

Le tableau affiche les informations suivantes :

Paramètres	Description
Component	Affiche le chemin d'accès à la page sur laquelle la modification a été effectuée. Pour accéder à la page, cliquez sur le chemin.
Operation	Affiche la modification qui a été effectuée. Valeurs possibles : • **created** - L'élément a été créé. • **deleted** - L'élément a été supprimé. • **value_set** - L'élément a été modifié. • **default_set** - Le paramétrage par défaut de l'élément a été restauré.
New Value	Affiche la nouvelle valeur après la modification.

Paramètres	Description
Old Value	Affiche la valeur antérieure à la modification.
Validation	Indique si la modification est valide. Valeurs possibles : • **Coche bleue** - La vérification du type de données de la modification a constaté qu'il était correct. • **Coche verte** - La vérification par rapport à la configuration existante révèle que la modification est valide. • **Point d'exclamation rouge** - La modification n'est pas valide. La vérification par rapport au type de données ou à la configuration a échoué. Pour plus d'informations, voir "Retours d'information visuels (Page 50)".

3.2.3 Vérification des modifications de la configuration

Pour vérifier les modifications de la configuration, procédez comme suit :

1. Dans la barre d'état, cliquez sur le bouton **Transactions de configuration**.
2. Cliquez dans le menu **Commit** sur **Validate**.
   Options disponibles :
   – Il n'y a pas de conflit entre la configuration actuelle et les modifications de la configuration.
   Les modifications valides sont marquées d'une coche verte.
   Vous pouvez valider les modifications. Pour plus d'informations, voir "Validation de modifications contrôlées de la configuration (Page 42)".
   – Il y a des conflits entre la configuration actuelle et les modifications de la configuration.
   L'appareil signale le premier conflit détecté.
   Les modifications non valides sont repérées par un point d'exclamation rouge.

3.2.4 Désactivation d'une fonction

Pour désactiver une fonction dans l'IU Web, procédez comme suit :

1. Naviguez vers une fonction.
2. Modifiez le paramètre correspondant en **Disabled**.
3. Validez la modification.

3.2.5 Validation des modifications de la configuration (Commit)

Pour valider des modifications de la configuration, utilisez dans la zone **Transactions de configuration** la commande **Commit**.

Vous n'êtes pas obligé de valider individuellement chaque modification de la configuration. Vous pouvez réaliser plusieurs modifications de la configuration et les valider ensemble.

Lorsque vous validez les modifications de la configuration, la validation est marquée par un identifiant. Cet identifiant vous permet ultérieurement de faire afficher dans la CLI les modifications et de rétablir la configuration précédente. L'identification dans l'IU Web est automatique.

Vous disposez de plusieurs options pour valider les modifications de la configuration.

Remarque

Si vous validez les modifications de la configuration et si, ce faisant, l'appareil est arrêté ou l'alimentation coupée, contrôlez les modifications de la configuration dès que l'appareil est de nouveau accessible.

3.2.5.1 Contrôle et validation des modifications de la configuration en une opération

Pour contrôler et valider les modifications de la configuration en une opération, procédez comme suit :

1. Dans la barre d'état, cliquez sur le bouton **Transactions de configuration**.
2. Pour contrôler et valider les modifications en une opération, cliquez sur le bouton **Commit**. Options disponibles :
   - Il n'y a pas de conflit entre la configuration actuelle et les modifications de la configuration. Les modifications de la configuration sont validées ensemble par un identifiant généré automatiquement.
   - Il y a des conflits entre la configuration actuelle et les modifications de la configuration. L'appareil signale le premier conflit détecté.
     Les modifications non valides sont repérées par un point d'exclamation rouge.

3.2.5.2 Validation de modifications contrôlées de la configuration

Pour valider des modifications déjà contrôlées de la configuration, procédez comme suit :

1. Dans la barre d'état, cliquez sur le bouton **Transactions de configuration**.
2. Contrôlez les modifications.
   Pour plus d'informations, voir "Vérification des modifications de la configuration (Page 41)".
3. Pour valider les modifications, cliquez dans le sous-menu **Commit** sur **Commit Only**.
   Les modifications de la configuration actuelle sont validées ensemble par un identifiant généré automatiquement.

3.2.6 Suppression de modifications de la configuration

Pour supprimer individuellement des modifications de la configuration, procédez comme suit :

1. Dans la barre d'état, cliquez sur le bouton **Transactions de configuration**.
2. Cliquez, dans la ligne de la modification, sur l'icône de suppression figurant dans la dernière colonne.

3.2.7 Annulation de toutes les modifications de la configuration

Pour annuler les modifications de la configuration, procédez comme suit :

1. Dans la barre d'état, cliquez sur le bouton **Transactions de configuration**.
2. Cliquez sur le bouton **Abort**.

3.2.8 Restauration d'une configuration (Rollback)

Avant la validation des modifications de la configuration, un horodatage est créé pour sauvegarder la configuration courante avant sa modification. Il en résulte une liste continue de configurations que vous pouvez restaurer.

Si vous restaurez une configuration, la configuration courante devient une version antérieure. L'appareil enregistre un nombre limité d'anciennes configurations. Lorsque le nombre maximal de configurations est atteint, l'enregistrement d'une nouvelle configuration efface la configuration la plus ancienne de la liste.

Remarque

Après le chargement d'un fichier de firmware d'une autre version, toutes les versions de configuration enregistrées sont supprimées. La configuration actuelle est conservée et n'est pas modifiée.

La restauration d'une configuration s'effectue via la CLI. Pour plus d'informations, voir le Manuel de configuration SINEC OS CLI.

3.3 Opérations de base

Cette section décrit les opérations de base sur l'IU Web.

3.3.1 Utilisation de tableaux

De nombreuses configurations de l'IU Web figurent dans des tableaux. Cette section décrit comment utiliser des tableaux dans l'IU Web.

3.3.1.1 Ajout d'une nouvelle ligne

Pour ajouter une nouvelle ligne, procédez comme suit :

1. Cliquez sur le bouton **Add**.
2. [Facultatif] Configurez les paramètres de la ligne.
3. Validez les modifications.

3.3.1.2 Sélection d'une ligne

Pour sélectionner une ligne, cliquez sur la coche dans la première colonne. Une ligne sélectionnée est affichée sur fond bleu.

Pour annuler la sélection, cliquez à nouveau sur la coche dans la première colonne.

3.3.1.3 Suppression d'une ligne

Pour supprimer une ligne, procédez comme suit :

1. Sélectionnez la ligne que vous voulez supprimer.
2. Cliquez sur le bouton **Delete**.
3. Validez la modification.

3.3.1.4 Configuration simultanée des paramètres de toutes les lignes d'une colonne

Certains tableaux possèdent une première ligne contenant le mot-clé **All**. Les configurations que vous effectuez et validez dans la première ligne sont appliquées à toutes les lignes suivantes.

Vous pouvez aussi bien sélectionner une entrée dans une liste déroulante que saisir une valeur dans un champ de saisie. Les listes déroulantes affichent dans la ligne **All** le texte **Select...**. Dans la ligne **All**, les champs de saisie sont vides.

Si la configuration d'une ligne n'est pas possible, elle est repérée par un point d'exclamation rouge et un message d'erreur s'affiche.

Exemple

Dans cet exemple, on configure 2 paramètres de détection de boucles de réseau.

Pour configurer des paramètres de toutes les lignes d'un tableau, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Loop Detection**.
   Le tableau sous **Loop Detection** possède une première ligne avec l'entrée **All** dans la première colonne **Interface**.
2. Sélectionnez dans la première ligne sous **Transmission State** l'entrée voulue de la liste déroulante.
   Votre choix est appliqué à tous les ports de pont. Une coche bleue est affichée dans toutes les lignes à côté de la zone de liste déroulante.
3. Entrez la valeur voulue dans la première ligne sous **Transmission Interval**.
   La valeur est appliquée à tous les ports de pont. Une coche bleue est affichée dans toutes les lignes à côté du champ de saisie.
4. Validez les modifications.

3.3.1.5 Exécution simultanée d'actions sur toutes les lignes d'un tableau

Certains tableaux possèdent une première ligne contenant le mot-clé **All**. Si cette ligne contient un bouton, l'action correspondante sera exécutée pour toutes les lignes suivantes.

Exemple

Dans cet exemple, la détection des boucles réseau est réinitialisée manuellement sur tous les ports du pont.

Pour réinitialiser tous les ports du pont en même temps, procédez comme suit :

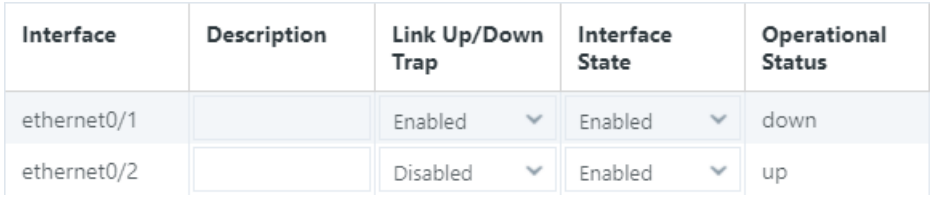
1. Naviguez vers **Layer 2** ≫ **Loop Detection**.
   Le tableau sous **Loop Detection** possède une première ligne avec l'entrée **All** dans la première colonne **Interface**.
2. Cliquez dans la dernière colonne de la première ligne sur **Reset**.
   Tous les ports de pont sont réinitialisés. Une coche verte est affichée dans toutes les lignes à côté du bouton.

3.3.1.6 Cellules éditables et cellules en lecture seule

Les cellules éditables et cellules en lecture seule se distinguent visuellement par une bordure.

Les cellules éditables possèdent une bordure. Dans l'exemple suivant, les cellules des colonnes **Description**, **Link Up/Down Trap** et **Interface State** sont éditables.

Les cellules en lecture seule ne possèdent pas de bordure. Dans l'exemple suivant, les cellules des colonnes **Interface** et **Operational Status** sont en lecture seule.



Interface	Description	Link Up/Down Trap	Interface State	Operational Status
ethernet0/1		Enabled	Enabled	down
ethernet0/2		Disabled	Enabled	up

Figure 3-3 Cellules éditables et cellules en lecture seule

3.3.1.7 Définition du nombre d'entrées affichées

Il existe des tableaux statiques avec un nombre fixe d'entrées, par exemple des tableaux avec des interfaces. Le nombre d'interfaces physiques d'un appareil est défini.

Les tableaux dynamiques varient dans le nombre de leurs entrées, par exemple les tableaux avec VLAN et le journal d'incidents.

Dans certains tableaux, les entrées statiques et dynamiques sont combinées. Un tableau de statistiques d'interface contient à la fois le nombre fixe d'interfaces physiques et le nombre variable de VLAN créés.

Si un tableau contient plus de 25 entrées, les informations suivantes s'affichent sur le bord inférieur droit du tableau :

- Le nombre d'entrées du tableau actuellement affichées (p. ex. **1 -25** of 29 items)
- Le nombre d'entrée que le tableau contient au total (p. ex. 1 -25 of **29** items)

Pour définir le nombre d'entrées affichées, sélectionnez au bord inférieur gauche du tableau le nombre voulu sous **items per page**.

Vous pouvez afficher 25, 50 ou 100 entrées. Pour afficher toutes les entrées, sélectionnez l'entrée **All**. Pour les grands tableaux, l'affichage de toutes les entrées peut prendre un certain temps. C'est pourquoi une demande de confirmation s'affiche.

Les tableaux statiques affichent par défaut 50 entrées.

Les tableaux dynamiques et les formes mixtes affichent par défaut 25 entrées.

3.3.1.8 Tableaux de plusieurs pages

Si un tableau contient plus d'entrées que ce qui est affiché sur une page, les entrées continuent sur une nouvelle page.

Les informations suivantes s'affichent au bord inférieur gauche du tableau :

- La page du tableau actuellement affichée (p. ex. **1**/3)
- Le nombre total de pages du tableau (p. ex. 1/**3**)

Les boutons suivants vous permettent de naviguer entre les pages du tableau.

Bouton	Description
	Ce bouton permet de passer à la page suivante.
	Ce bouton permet de passer à la dernière page.
	Ce bouton permet de passer à la page précédente.
	Ce bouton permet de passer à la première page.

3.3.2 Passage à la page d'accueil

Pour passer à la page d'accueil, cliquez sur le logo SIEMENS à gauche dans la barre d'entête.

3.3.3 Sélection multiple dans des zones de liste de déroulante

Il existe plusieurs types de zones de liste déroulante. Dans certaines zones de liste déroulante, vous ne pouvez sélectionner qu'une seule des entrées affichées, p. ex. Enabled ou Disabled. Toutefois, lorsqu'il s'agit de sélectionner p. ex. des interfaces ou des VLAN, une sélection multiple est possible dans certaines zones de liste déroulante. Vous reconnaissez ces zones de liste déroulante à l'entrée suivante dans l'état par défaut : 0 item selected.

Ouvrez la zone de liste déroulante et sélectionnez ou désélectionnez autant d'entrées que vous voulez.

Les entrées sélectionnées s'affichent dans l'ordre initial dans lequel elles ont été listées. Si le champ ne suffit pas pour afficher toutes les entrées sélectionnées, celles-ci sont abrégées par "...". Si vous faites glisser le pointeur de la souris sur le champ, toutes les entrées sélectionnées s'affichent sous forme d'infobulle.

Pour sélectionner plusieurs entrées en même temps, cliquez dans le champ et indiquez une plage. Par exemple, si vous souhaitez sélectionner les VLAN 3, 4, 5 et 6, saisissez "3-6" et

confirmez en appuyant sur la touche **Entrée**. Cette fonction n'est pas disponible pour les interfaces.

Certaines zones de liste déroulante sont extensibles. Vous pouvez par exemple indiquer les VLAN 6-10 comme plage, bien que le VLAN 10 n'existe pas encore. Cependant, les entrées ne sont pas créées automatiquement, vous devez créer vous-même les entrées correspondantes.

Pour désélectionner toutes les entrées sélectionnées en même temps, cliquez sur l'entrée supérieure "-".

3.3.4 Chargement et enregistrement de fichiers via un serveur distant.

Vous pouvez charger et enregistrer des fichiers via un serveur distant.

Pour le chargement et l'enregistrement via un serveur distant, vous avez besoin des informations suivantes :

- **Protocole**
  Les protocoles suivants sont pris en charge :
  - FTP
  - SFTP
    Pour établir une connexion à un serveur SFTP, il faut que l'empreinte de la clé publique soit enregistrée dans le Truststore de l'appareil.
    Une demande de confirmation est émise lors de la première connexion à un serveur SFTP. Si vous la confirmez, l'appareil enregistre automatiquement l'empreinte de la clé publique dans le Truststore. À compter de cet instant, le serveur SFTP est vérifié. Lors de nouvelles connexions à ce serveur SFTP, plus aucune demande de confirmation n'est émise.
  - TFTP

    Remarque

    TFTP n'étant pas un protocole basé TCP, des erreurs peuvent survenir durant le transfert de fichiers.

    Si vous constatez des erreurs lors du transfert de fichiers, configurez les paramètres du serveur TFTP avec les valeurs suivantes :
    - TFTP-Timeout : 300 secondes
    - Retransmissions TFTP : 100
  - HTTP
- **Nom d'utilisateur et mot de passe**
  La saisie du nom d'utilisateur et du mot de passe dépend du protocole.
  - Avec les protocoles FTP et SFTP, vous devez indiquer le nom d'utilisateur et le mot de passe.
  - Avec HTTP ces informations ne sont pas forcément nécessaires.
  - Avec TFTP, vous ne pouvez pas entrer ces indications.

- **Port**
  Le port ne doit être spécifié que si vous ne voulez pas utiliser le port par défaut :

Protocole	Port par défaut
FTP	Port TCP 21
SFTP	Port TCP 22
TFTP	Port UDP 69
HTTP	Port TCP 80

- **Chemin vers le fichier y compris le nom du fichier**
  Avec le protocole SFTP, vous devez indiquer le chemin complet sur le serveur distant jusqu'au fichier.

Pour charger ou enregistrer un fichier via un serveur distant, procédez comme suit :

1. Naviguer vers une page correspondante dans l'IU Web, par exemple **System** ≫ **Load & Save** ≫ **Firmware**.
2. Sous **Protocol**, sélectionnez un protocole.
3. Sous **Server Address / FQDN**, entrez l'adresse IP du serveur.
4. [Facultatif] Sous **Server Port** modifier le port si le serveur distant n'utilise pas le port préréglé.
5. [Facultatif] Si vous avez sélectionné sous **Protocol** l'option **FTP**, **SFTP** ou **HTTP**, entrez sous **Server User** le nom d'utilisateur.
6. [Facultatif] Si vous avez sélectionné sous **Protocol** l'option **FTP**, **SFTP** ou **HTTP**, entrez sous **Server Password** le mot de passe.
7. Saisissez sous **File Path / File Name** le chemin vers le fichier et le nom du fichier.
8. [Facultatif] Sous **File Protection** vous pouvez enregistrer le fichier en mode protégé.
   Options disponibles :

Option	Description
Disabled	**Par défaut** Le fichier est enregistré sans autres options.
Enabled	Le fichier est chargé en mode protégé. En mode protégé, le fichier est enregistré avec une somme de contrôle. La somme de contrôle permet de s'assurer que le fichier enregistré est resté inchangé lors du chargement sur un appareil. Lorsque le fichier enregistré est chargé, l'appareil vérifie la somme de contrôle. Si le fichier a été modifié, les sommes de contrôle ne concordent plus et le fichier n'est pas chargé.

9. [Facultatif] Si vous avez sélectionné sous **File Protection** l'option **Enabled**, attribuez sous **File Password** un mot de passe.
   Condition :
   - Il doit compter de 1 à 255 caractères.
   - Tous les caractères standard ainsi que les caractères spéciaux suivants sont autorisés : # $ % & ( ) * + , - . / : < = > @ [ ] ^ _ { } ~

10. [Facultatif] Si vous avez attribué un mot de passe sous **File Password**, répétez le mot de passe sous **File Password-Confirm**.
11. Cliquez sur **Load** ou **Save**.
    Lors de l'enregistrement sur un PC client local, le fichier sera enregistré directement dans un dossier prédéfini ou bien, selon le paramétrage de votre navigateur Internet, vous devrez d'abord choisir l'emplacement.

3.3.5 Indication d'une Durée

Pour indiquer une durée, composez les éléments requis de l'indication de durée (année à seconde) avec les caractères séparateurs voulus.

Le format de la durée est **nYnMnDnhnmns**.

Les diverses indications de temps et les caractères séparateurs sont définis comme suit :

- **nY** - Indique le nombre d'années.
- **nM** - Indique le nombre de mois.
- **nD** - Indique le nombre de jours.
- **nh** - Indique le nombre d'heures.
- **nm** - Indique le nombre de minutes.
- **ns** - Indique le nombre de secondes.

Lors de l'indication d'une durée il faut respecter les règles suivantes :

- Il faut qu'il existe au moins une indication de temps avec caractère séparateur.
- Ne pas utiliser d'espaces entre les indications de temps.
- L'ordre des indications de temps est prédéfini et invariable.
- Si une indication de temps possède la valeur "0", on peut se passer de l'indication de temps et du caractère séparateur.
- Les indications de temps sont des entiers positifs. L'indication des secondes peut contenir des décimales.
- Pour représenter des durées négatives, la durée totale est précédée du signe moins.

Exemples positifs

Le tableau ci-après montre des durées correctement indiquées :

Durée	Description
2Y5M6D12h33m15s	2 ans, 5 mois, 6 jours, 12 heures, 33 minutes, 15 secondes
2D35m	2 jours, 35 minutes
1m30.5s	1 minute, 30,5 secondes
-6M	Moins 6 mois
20M	20 mois (l'indication des mois n'est pas limitée à 12.)

Exemples négatifs

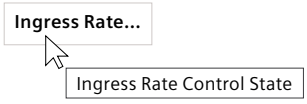
Le tableau ci-après indique des durées non valides.

Durée	Description
	Une entrée vide n'est pas admissible.
1M2Y	L'ordre des indications de temps doit être respecté.
1.5m	Les décimales sont uniquement autorisées pour les secondes.
1Y-6M	Le signe moins doit figurer en première position.

3.3.6 Retours d'information visuels

L'IU Web fournit les retours d'information visuels suivants sur les entrées, configurations, etc.

Retour d'information visuel	Description
	Les champs actifs sont encadrés en bleu.
	**Symbole de chargement** L'entrée est vérifiée.
	**Coche bleue** La vérification du type de données de la modification a constaté qu'il était correct. La vérification a lieu automatiquement lors de la saisie. Seules les modifications de configuration correctes sont intégrées à la liste de candidats. **Exemple** Dans cet exemple, la date/heure système a été saisie dans un format non valide : "2020-3-25 9:00" La vérification du type de données a échoué. Un point d'exclamation rouge et un message d'erreur s'affichent. **Exemple** Dans cet exemple, la date/heure système a été saisie dans un format valide : "2020-03-25 09:00:00" Le type de données a été vérifié avec succès. Une coche bleue s'affiche.
	**Coche verte** La vérification par rapport à la configuration existante révèle que la modification est valide. Pour lancer la vérification, utilisez la fonction **Validate** dans la zone Transactions de configuration. Pour plus d'informations, voir "Vérification des modifications de la configuration (Page 41)". Seules les modifications de configuration valide peuvent être validées.
	**Point d'exclamation rouge** Une entrée n'est pas valide. La vérification par rapport au type de données ou à la configuration a échoué.

Retour d'information visuel	Description
	**Note** Les notes s'affichent au bord inférieur droit de l'IU Web. Une seule note s'affiche à la fois. Toute nouvelle note remplace la précédente. Une note reste affichée jusqu'à ce que vous cliquiez sur l'icône de fermeture dans le coin supérieur droit de la note.
	**Demande de confirmation** Les demandes de confirmation s'affichent en bas à droite de l'IU Web lorsqu'une décision de l'utilisateur est nécessaire. La demande de confirmation reste affichée jusqu'à ce que vous y répondiez par **Yes** ou **No**. L'action qui a déclenché la demande de confirmation n'est exécutée qu'après votre confirmation ou bien annulée.
 	**Textes d'interface utilisateur abrégés** Si l'espace disponible n'est pas suffisant pour un texte d'interface, le texte est abrégé par "...". Cela s'applique aux titres et aux champs.
	**Infobulles** Si vous faites glisser le pointeur de la souris sur le champ, le texte abrégé s'affiche sous forme d'infobulle.

3.3.7 Adaptation de la mise en page

Lorsque la zone des transactions de configuration est ouverte, vous pouvez adapter la mise en page du volet de contenu.

Utilisez le curseur pour ajuster la répartition entre les pages d'information/de configuration et la zone des transactions de configuration.

3.3.8 Utilisation de l'IU Web avec le clavier

En fonction du navigateur, certains raccourcis clavier peuvent varier.

Action	Touche/Raccourcis clavier
Passser à l'élément suivant	Tabulateur
Actionner un bouton	Touche Entrée
Activer ou désactiver une case à cocher	Barre d'espacement
Naviguer parmi les options d'une liste déroulante	Flèches vers le haut et vers le bas
Passer à la page sélectionnée avant	[Alt] + [flèche vers la gauche]

Action	Touche/Raccourcis clavier
Passer à la page sélectionnée après	[Alt] + [flèche vers la droite]
Copier le contenu sélectionné	[Ctrl] + [C]
Coller le contenu	[Ctrl] + [V]
Couper le contenu sélectionné	[Ctrl] + [X]

3.4 Configuration des interfaces utilisateur

Cette section décrit la gestion des interfaces utilisateur SINEC OS CLI, Web UI et NETCONF.

Pour plus d'informations sur l'interface SNMP, voir "SNMP (Page 233)".

Vous pouvez configurer pour chaque interface utilisateur l'état (activé/désactivé), le timeout d'inactivité ainsi que les paramètres de protocole (tels qu'adresse IP et port, clé SSH ou TLS).

3.4.1 Ce qu'il faut savoir sur la configuration des interfaces utilisateur

La configuration de serveurs est réalisée sous SINEC OS via des nœuds d'extrémité. Un nœud d'extrémité est défini comme instance autonome d'un service de serveur.

Des nœuds d'extrémités sont prédéfinis par défaut sous SINEC OS pour les interfaces utilisateur et protocoles ci-après :

- CLI SSH
- Web UI HTTP
- Web UI HTTPS
- NETCONF SSH
- SNMP
  Pour plus d'informations sur la configuration de l'interface utilisateur SNMP, voir "Configuration de l'agent SNMP (Page 234)".

Il n'est possible de définir qu'un seul nœud d'extrémité de serveur par interface utilisateur et protocole.

Remarque

Les nœuds d'extrémité prédéfinis ne peuvent pas être renommés ni supprimés. Vous ne pouvez pas créer d'autres nœuds d'extrémité.

Les tableaux ci-après récapitulent les paramètres par défaut des nœuds d'extrémité.

CLI SSH

Nœud d'extrémité	Par défaut
Nom	default
Nœud d'extrémité activé	Oui

Nœud d'extrémité	Par défaut
Adresse IP	0.0.0.0
Port	22

Web UI HTTP

Nœud d'extrémité	Par défaut
Nom	unsecure
Nœud d'extrémité activé	Oui
Adresse IP	0.0.0.0
Port	80

Web UI HTTPS

Nœud d'extrémité	Par défaut
Nom	secure
Nœud d'extrémité activé	Oui
Adresse IP	0.0.0.0
Port	443

NETCONF SSH

Nœud d'extrémité	Par défaut
Nom	default
Nœud d'extrémité activé	Oui
Adresse IP	0.0.0.0
Port	830

3.4.2 Configuration de l'interface utilisateur NETCONF

Pour configurer l'interface utilisateur NETCONF, procédez comme suit :

1. Activez l'interface utilisateur NETCONF.
   Pour plus d'informations, voir "Activation de l'interface utilisateur NETCONF (Page 54)".
2. [Facultatif] Modifiez le timeout d'inactivité des sessions NETCONF.
   Pour plus d'informations, voir "Modification du timeout d'inactivité des sessions NETCONF (Page 54)".
3. Configurez un nœud d'extrémité de serveur pour NETCONF.
   Pour plus d'informations, voir "Configuration d'un nœud d'extrémité de serveur pour NETCONF. (Page 55)".
4. Activez un nœud d'extrémité de serveur pour NETCONF.
   Pour plus d'informations, voir "Activation d'un nœud d'extrémité de serveur pour NETCONF (Page 55)".

3.4.2.1 Activation de l'interface utilisateur NETCONF

Par défaut, l'interface utilisateur NETCONF est activée.

Seuls les utilisateurs possédant le profil utilisateur **Admin** sont habilités à activer l'interface utilisateur NETCONF.

Pour activer l'interface utilisateur NETCONF, procédez comme suit :

1. Naviguez vers **System** ≫ **Management Services** ≫ **Overview**.
2. Sous **NETCONF**, modifiez le paramètre **Status** en **Enabled**.
3. Validez la modification.

3.4.2.2 Modification du timeout d'inactivité des sessions NETCONF

Le timeout d'inactivité indique le temps pendant lequel une session NETCONF reste ouverte en cas d'inactivité. Lorsque le timeout d'inactivité est écoulé, le serveur termine automatiquement la session NETCONF.

Remarque

Si vous modifiez le timeout d'inactivité, la modification ne s'applique qu'aux nouvelles sessions NETCONF. Pour les sessions NETCONF en cours, le timeout d'inactivité n'est pas modifié.

Seuls les utilisateurs possédant le profil utilisateur **Admin** sont habilités à modifier le timeout d'inactivité.

Procédez comme suit pour modifier le timeout d'inactivité des sessions NETCONF :

1. Naviguez vers **System** ≫ **Management Services** ≫ **Overview**.
2. Sous **NETCONF**, modifiez le paramètre **Idle Timeout**.
   Conditions :
   - En format nYnMnDnhnmns, dans lequel n est un nombre personnalisé
   - Min. 0 seconde (0s)
   - Max. 49 jours 17 Heures 2 Minutes 47 secondes (49D17h2m47s)

   Par défaut : 5 m (5 minutes)
   Si vous entrez la valeur **0 s**, la déconnexion automatique est désactivée.
   Si vous paramétrez la valeur **1M** (1 Mois), l'appareil calcule le timeout d'inactivité comme suit : 365 jours/12 mois. C'est pourquoi une valeur de 30,4167 jours a été configurée.
3. Validez la modification.

3.4.2.3 Configuration d'un nœud d'extrémité de serveur pour NETCONF.

Configurez l'adresse IP locale et le port, via lesquels le nœud d'extrémité de serveur traite des requêtes NETCONF.

IMPORTANT
Risque de configuration - Risque de coupure de la liaison Si l'appareil obtient son IP dynamiquement par DHCP, tenez compte de ce qui suit : Si l'adresse IP que l'appareil obtient par DHCP ne concorde pas avec l'adresse IP que vous configurez pour le nœud d'extrémité de serveur NETCONF, l'appareil n'est pas accessible via le nœud d'extrémité de serveur NETCONF. Pour éviter une coupure de la liaison, vous disposez des possibilités suivantes : • Autorisez les requêtes de clients sur toutes les adresses locales (adresse IP par défaut : 0.0.0.0). • Attribuez à l'appareil une adresse statique. • Veuillez vous assurer que DHCP attribue toujours la même adresse IP.

Seuls les utilisateurs possédant le profil utilisateur **Admin** sont habilités à configurer un nœud d'extrémité de serveur.

Pour configurer un nœud d'extrémité de serveur, procédez comme suit :

1. Naviguez vers **System** ≫ **Management Services** ≫ **Overview**.
   Sous **NETCONF** ≫ **Endpoint** sont affichés les nœuds d'extrémité de serveur disponibles pour NETCONF.
2. Sous **Endpoint** sélectionnez un nœud d'extrémité et modifiez dans la colonne **TCP Port** le port, via lequel les requêtes NETCONF sont traitées.
   Conditions :
   – Le nombre 830
   – Un nombre compris entre 1024 et 49151
   – Un nombre compris entre 49500 et 65535

   Par défaut : 830
3. Sous **Endpoint** sélectionnez un nœud d'extrémité et modifiez dans la colonne **IP Address** l'adresse IP, via laquelle les requêtes NETCONF sont traitées.
   Par défaut : 0.0.0.0
   L'adresse IP par défaut autorise les requêtes de clients sur toutes les adresses locales.
4. Validez les modifications.

3.4.2.4 Activation d'un nœud d'extrémité de serveur pour NETCONF

Par défaut, le nœud d'extrémité de serveur pour NETCONF est activé.

Seuls les utilisateurs possédant le profil utilisateur **Admin** sont habilités à activer un nœud d'extrémité de serveur.

Pour activer un nœud d'extrémité de serveur pour NETCONF, procédez comme suit :

1. Naviguez vers **System** ≫ **Management Services** ≫ **Overview**.
   Sous **NETCONF** ≫ **Endpoint** sont affichés les nœuds d'extrémité de serveur disponibles pour NETCONF.
2. Sous **Endpoint**, sélectionnez un nœud d'extrémité et modifiez le paramètre **Status** en **Enabled**.
3. Validez la modification.

3.4.3 Configuration de l'interface utilisateur CLI

Pour configurer l'interface utilisateur CLI, procédez comme suit :

1. [Facultatif] Modifiez le timeout d'inactivité des sessions CLI.
   Pour plus d'informations, voir "Modification du timeout d'inactivité pour les sessions CLI (Page 56)".
2. Activation d'un nœud d'extrémité de serveur pour la CLI
   Pour plus d'informations, voir "Configuration d'un nœud d'extrémité de serveur pour la CLI (Page 57)".
3. Activez un nœud d'extrémité de serveur pour la CLI.
   Pour plus d'informations, voir "Activation d'un nœud d'extrémité de serveur pour CLI (Page 58)".

3.4.3.1 Modification du timeout d'inactivité pour les sessions CLI

Le timeout d'inactivité indique le temps pendant lequel une session CLI reste ouverte en cas d'inactivité. Lorsque le timeout d'inactivité est écoulé, le serveur termine automatiquement la session CLI. La valeur vaut également pour les sessions pour lesquelles vous accédez à la CLI via une connexion série.

Remarque

Cette commande permet de modifier le timeout d'inactivité globalement pour toutes les sessions CLI. Vous pouvez écraser le timeout global pour les sessions CLI locales. Pour plus d'informations sur la configuration de sessions CLI locales, voir le **Manuel de configuration SINEC OS CLI**.

Remarque

Si vous modifiez le timeout d'inactivité, la modification ne s'applique qu'aux nouvelles sessions CLI. Pour les sessions CLI en cours, le timeout d'inactivité n'est pas modifié.

Seuls les utilisateurs possédant le profil utilisateur **Admin** sont habilités à modifier le timeout d'inactivité.

Procédez comme suit pour modifier globalement le timeout d'inactivité des sessions CLI :

1. Naviguez vers **System** ≫ **Management Services** ≫ **Overview**.
2. Sous **CLI**, modifiez le paramètre **Idle Timeout**.
   Conditions :
   - En format nYnMnDnhnmns, dans lequel n est un nombre personnalisé
   - Min. 0 seconde (0s)
   - Max. 49 jours 17 Heures 2 Minutes 47 secondes (49D17h2m47s)

   Par défaut : 15 m (15 minutes)
   Si vous entrez la valeur **0 s**, la déconnexion automatique est désactivée.
   Si vous paramétrez la valeur **1M** (1 Mois), l'appareil calcule le timeout d'inactivité comme suit : 365 jours/12 mois. C'est pourquoi une valeur de 30,4167 jours a été configurée.
3. Validez la modification.

3.4.3.2 Configuration d'un nœud d'extrémité de serveur pour la CLI

Configurez l'adresse IP locale et le port, via lesquels un nœud d'extrémité de serveur traite des requêtes CLI.

IMPORTANT
Risque de configuration - Risque de coupure de la liaison Si l'appareil obtient son IP dynamiquement par DHCP, tenez compte de ce qui suit : Si l'adresse IP que l'appareil obtient par DHCP ne concorde pas avec l'adresse IP que vous configurez pour le nœud d'extrémité de serveur NETCONF, l'appareil n'est pas accessible via le nœud d'extrémité de serveur NETCONF. Pour éviter une coupure de la liaison, vous disposez des possibilités suivantes : • Autorisez les requêtes de clients sur toutes les adresses locales (adresse IP par défaut : 0.0.0.0). • Attribuez à l'appareil une adresse statique. • Veuillez vous assurer que DHCP attribue toujours la même adresse IP.

Seuls les utilisateurs possédant le profil utilisateur **Admin** sont habilités à configurer un nœud d'extrémité de serveur.

Pour configurer un nœud d'extrémité de serveur, procédez comme suit :

1. Naviguez vers **System** ≫ **Management Services** ≫ **Overview**.
   Sous **CLI** ≫ **Endpoint** sont affichés les nœuds d'extrémité de serveur disponibles pour CLI.
2. Sous **Endpoint** sélectionnez un nœud d'extrémité et modifiez dans la colonne **TCP Port** le port, via lequel les requêtes CLI sont traitées.
   Conditions :
   - Le nombre 22
   - Un nombre compris entre 1024 et 49151
   - Un nombre compris entre 49500 et 65535

   Par défaut : 22
3. Sous **Endpoint** sélectionnez un nœud d'extrémité et modifiez dans la colonne **IP Address** l'adresse IP, via laquelle les requêtes CLI sont traitées.
   Par défaut : 0.0.0.0
   L'adresse IP par défaut autorise les requêtes de clients sur toutes les adresses locales.
4. Validez les modifications.

3.4.3.3 Activation d'un nœud d'extrémité de serveur pour CLI

Par défaut, le nœud d'extrémité de serveur pour CLI est activé.

Seuls les utilisateurs possédant le profil utilisateur **Admin** sont habilités à activer un nœud d'extrémité de serveur.

Remarque

Si vous désactivez le nœud d'extrémité de serveur de la CLI, vous pouvez continuer à accéder à la CLI via une connexion série.

Pour activer un nœud d'extrémité de serveur pour la CLI, procédez comme suit :

1. Naviguez vers **System** ≫ **Management Services** ≫ **Overview**.
   Sous **CLI** ≫ **Endpoint** sont affichés les nœuds d'extrémité de serveur disponibles pour CLI.
2. Sous **Endpoint**, sélectionnez un nœud d'extrémité et modifiez le paramètre **Status** en **Enabled**.
3. Validez la modification.

3.4.4 Configuration de l'interface utilisateur Web

Pour configurer l'interface utilisateur Web, procédez comme suit :

1. Activez l'interface utilisateur Web.
   Pour plus d'informations, voir "Activation de l'interface utilisateur Web (Page 59)".
2. [Facultatif] Modifiez le timeout d'inactivité des sessions Web UI.
   Pour plus d'informations, voir "Modification du timeout d'inactivité des sessions d'IU Web. (Page 59)".

3. Activation d'un nœud d'extrémité de serveur HTTP pour la iWeb UI.
   Pour plus d'informations, voir "Configuration d'un nœud d'extrémité de serveur HTTP pour l'IU Web (Page 60)".
4. Activez un nœud d'extrémité de serveur HTTP pour la Web UI.
   Pour plus d'informations, voir "Activation d'un nœud d'extrémité de serveur HTTP pour l'IU Web (Page 61)".
5. Configurez un nœud d'extrémité de serveur HTTPS pour la iWeb UI.
   Pour plus d'informations, voir "Configuration d'un nœud d'extrémité de serveur HTTPS pour l'IU Web (Page 62)".
6. Activez un nœud d'extrémité de serveur HTTPS pour la Web UI.
   Pour plus d'informations, voir "Activation d'un nœud d'extrémité de serveur HTTPS pour la Web UI (Page 62)".
7. [Facultatif] Référencez un certificat HTTPS personnalisé.
   Pour plus d'informations, voir "Utilisation d'un certificat HTTPS personnalisé. (Page 63)".

3.4.4.1 Activation de l'interface utilisateur Web

Par défaut, l'interface utilisateur Web est activée.

Seuls les utilisateurs possédant le profil utilisateur **Admin** sont habilités à activer l'interface utilisateur Web.

Pour activer l'interface utilisateur Web, procédez comme suit :

1. Naviguez vers **System** ≫ **Management Services** ≫ **Overview**.
2. Sous **WebUI (HTTP/HTTPS)**, modifiez le paramètre **Status** en **Enabled**.
3. Validez la modification.

3.4.4.2 Modification du timeout d'inactivité des sessions d'IU Web.

Le timeout d'inactivité indique le temps pendant lequel une session d'IU Web reste ouverte en cas d'inactivité. Lorsque le timeout d'inactivité est écoulé, le serveur termine automatiquement la session d'IU Web.

Remarque

Si vous modifiez le timeout d'inactivité, la modification ne s'applique qu'aux nouvelles sessions de l'IU Web. Pour les sessions IU Web en cours, le timeout d'inactivité n'est pas modifié.

Seuls les utilisateurs possédant le profil utilisateur **Admin** sont habilités à modifier le timeout d'inactivité.

Procédez comme suit pour modifier le timeout d'inactivité des sessions IU Web :

1. Naviguez vers **System** ≫ **Management Services** ≫ **Overview**.
2. Sous **WebUI (HTTP/HTTPS)** , modifiez le paramètre **Idle Timeout**.
   Conditions :
   - En format nYnMnDnhnmns, dans lequel n est un nombre personnalisé
   - Min. 0 seconde (0s)
   - Max. 49 jours 17 Heures 2 Minutes 47 secondes (49D17h2m47s)

   Par défaut : 15 m (15 minutes)
   Si vous entrez la valeur **0 s**, la déconnexion automatique est désactivée.
   Si vous paramétrez la valeur **1M** (1 Mois), l'appareil calcule le timeout d'inactivité comme suit : 365 jours/12 mois. C'est pourquoi une valeur de 30,4167 jours a été configurée.
3. Validez la modification.

3.4.4.3 Configuration d'un nœud d'extrémité de serveur HTTP pour l'IU Web

Configurez l'adresse IP locale et le port, via lesquels un nœud d'extrémité de serveur HTTP traite des requêtes IU Web.

IMPORTANT
Risque de configuration - Risque de coupure de la liaison Si l'appareil obtient son IP dynamiquement par DHCP, tenez compte de ce qui suit : Si l'adresse IP que l'appareil obtient par DHCP ne concorde pas avec l'adresse IP que vous configurez pour le nœud d'extrémité de serveur NETCONF, l'appareil n'est pas accessible via le nœud d'extrémité de serveur NETCONF. Pour éviter une coupure de la liaison, vous disposez des possibilités suivantes : • Autorisez les requêtes de clients sur toutes les adresses locales (adresse IP par défaut : 0.0.0.0). • Attribuez à l'appareil une adresse statique. • Veuillez vous assurer que DHCP attribue toujours la même adresse IP.

Seuls les utilisateurs possédant le profil utilisateur **Admin** sont habilités à configurer un nœud d'extrémité de serveur.

Pour configurer un nœud d'extrémité de serveur HTTP, procédez comme suit :

1. Naviguez vers **System** ≫ **Management Services** ≫ **Overview**.
   Sous **WebUI (HTTP/HTTPS)** ≫ **Endpoint** sont affichés les nœuds d'extrémité de serveur disponibles pour HTTP.
2. Sous **Endpoint** sélectionnez un nœud d'extrémité et modifiez dans la colonne **TCP Port** le port, via lequel les requêtes CLI sont traitées.
   Conditions :
   - Le nombre 80
   - Un nombre compris entre 1024 et 49151
   - Un nombre compris entre 49500 et 65535

   Par défaut : 80
3. Sous **Endpoint** sélectionnez un nœud d'extrémité de serveur HTTP et modifiez dans la colonne **IP Address** l'adresse IP, via laquelle les requêtes IU Web sont traitées.
   Par défaut : 0.0.0.0
   L'adresse IP par défaut autorise les requêtes de clients sur toutes les adresses locales.
4. Validez les modifications.

3.4.4.4 Activation d'un nœud d'extrémité de serveur HTTP pour l'IU Web

Par défaut, le nœud d'extrémité de serveur HTTP pour l'IU Web est activé.

Seuls les utilisateurs possédant le profil utilisateur **Admin** sont habilités à activer un nœud d'extrémité de serveur.

Pour activer un nœud d'extrémité de serveur HTTP pour l'IU Web, procédez comme suit :

1. Naviguez vers **System** ≫ **Management Services** ≫ **Overview**.
   Sous **WebUI (HTTP/HTTPS)** ≫ **Endpoint** sont affichés les nœuds d'extrémité de serveur disponibles pour HTTP.
2. Sous **Endpoint**, sélectionnez un nœud d'extrémité de serveur HTTP et modifiez le paramètre **Status** en **Enabled**.
3. Validez la modification.

3.4.4.5 Configuration d'un nœud d'extrémité de serveur HTTPS pour l'IU Web

Configurez l'adresse IP locale et le port, via lesquels un nœud d'extrémité de serveur HTTPS traite des requêtes de l'IU Web.

IMPORTANT
Risque de configuration - Risque de coupure de la liaison Si l'appareil obtient son IP dynamiquement par DHCP, tenez compte de ce qui suit : Si l'adresse IP que l'appareil obtient par DHCP ne concorde pas avec l'adresse IP que vous configurez pour le nœud d'extrémité de serveur NETCONF, l'appareil n'est pas accessible via le nœud d'extrémité de serveur NETCONF. Pour éviter une coupure de la liaison, vous disposez des possibilités suivantes : • Autorisez les requêtes de clients sur toutes les adresses locales (adresse IP par défaut : 0.0.0.0). • Attribuez à l'appareil une adresse statique. • Veuillez vous assurer que DHCP attribue toujours la même adresse IP.

Seuls les utilisateurs possédant le profil utilisateur **Admin** sont habilités à configurer un nœud d'extrémité de serveur.

Pour configurer un nœud d'extrémité de serveur HTTPS, procédez comme suit :

1. Naviguez vers **System** ≫ **Management Services** ≫ **Overview**.
   Sous **WebUI (HTTP/HTTPS)** ≫ **Endpoint** sont affichés les nœuds d'extrémité de serveur disponibles pour HTTPS.
2. Sous **Endpoint**, sélectionnez un nœud d'extrémité de serveur HTTPS et modifiez dans la colonne **TCP Port** le port, via lequel les requêtes IU Web sont traitées.
   Conditions :
   – Le nombre 443
   – Un nombre compris entre 1024 et 49151
   – Un nombre compris entre 49500 et 65535

   Par défaut : 443
3. Sous **Endpoint**, sélectionnez un nœud d'extrémité de serveur HTTPS et modifiez dans la colonne **IP Address** l'adresse IP, via laquelle les requêtes IU Web sont traitées.
   Par défaut : 0.0.0.0
   L'adresse IP par défaut autorise les requêtes de clients sur toutes les adresses locales.
4. Validez les modifications.

3.4.4.6 Activation d'un nœud d'extrémité de serveur HTTPS pour la Web UI

Par défaut, le nœud d'extrémité de serveur HTTP pour l'IU Web est activé.

Seuls les utilisateurs possédant le profil utilisateur **Admin** sont habilités à activer un nœud d'extrémité de serveur.

Pour activer un nœud d'extrémité de serveur HTTPS pour l'IU Web, procédez comme suit :

1. Naviguez vers **System** ≫ **Management Services** ≫ **Overview**.
   Sous **WebUI (HTTP/HTTPS)** ≫ **Endpoint** sont affichés les nœuds d'extrémité de serveur disponibles pour HTTPS.
2. Sous **Endpoint**, sélectionnez un nœud d'extrémité de Serveur HTTPS et modifiez le paramètre **Status** en **Enabled**.
3. Validez la modification.

3.4.4.7 Utilisation d'un certificat HTTPS personnalisé.

Le certificat HTTPS atteste l'identité de l'appareil et réglemente les échanges de données cryptées.

Pour pouvoir utiliser un certificat HTTPS personnalisé, il faut que le certificat soit disponible dans le Keystore. Pour plus d'informations, voir "Clés et certificats (Page 138)".

Nous vous recommandons instamment de créer et mettre à disposition vos propres certificats HTTPS. Nous vous conseillons d'utiliser des certificats HTTPS signés soit par des autorités externes fiables, soit par une autorité interne.

Pour utiliser un certificat HTTPS, procédez comme suit :

1. Naviguez vers **System** ≫ **Management Services** ≫ **Transport Security**.
2. Sous **Keystore Reference of TLS Certificate and Key for HTTPS Endpoint** sélectionnez dans **Asymmetric Key** le nom d'une paire de clés.
3. Sous **Certificate** sélectionnez le nom d'un certificat ou d'une chaîne de certificats.
4. Validez la modification.
   Pour pouvoir utiliser le certificat chargé, redémarrez le nœud d'extrémité de serveur HTTPS.
5. Naviguez vers **System** ≫ **Management Services** ≫ **Overview**.
   Sous **WebUI (HTTP/HTTPS)** ≫ **Endpoint** sont affichés les nœuds d'extrémité de serveur disponibles pour HTTPS.
6. Pour activer le certificat, redémarrez l'appareil.
   Pour plus d'informations, voir "Redémarrage de l'appareil (Page 72)".
   Lorsque le redémarrage est terminé, la page d'ouverture de session s'affiche.
7. Connectez-vous.
   Pour plus d'informations, voir "Connexion à un appareil configuré (Page 68)".

Prise en main

4

Ce chapitre décrit les opérations de base à exécuter lors de la première mise en service de l'appareil. Parmi ces tâches, vous aurez à établir une connexion à l'appareil, à accéder à l'interface utilisateur et a configurer un réseau de base.

4.1 Accès à l'IU Web via une connexion réseau

Pour accéder à l'IU Web (Web User Interface), établissez une connexion à distance via le réseau entre un PC client et un appareil.

L'appareil dispose pour de faire d'un serveur HTTP/HTTPS intégré. Si vous accédez à l'appareil au moyen de votre navigateur web, il retourne au PC client des pages HTML en fonction des entrées de l'utilisateur.

Conditions

- L'appareil possède une adresse IP.

  Remarque

  Attribuez à l'appareil une adresse IP via DHCP ou avec SINEC PNI.

- Il existe une connexion réseau entre l'appareil et le PC client.
- Les paramètres de réseau de l'appareil et du PC client concordent.

  Remarque

  Utilisez un ping pour vérifier qu'il existe une connexion et que la communication est possible.

- Sur l'appareil l'accès via HTTP(S) est activé.
- Un navigateur web est disponible sur le PC client.
- JavaScript est activé sur le navigateur web.
- Le navigateur web ne doit pas être paramétré de sorte à devoir charger une nouvelle page du serveur à chaque accès. L'actualité des contenus dynamiques d'une page est assurée par d'autres mécanismes.
- Si vous utilisez un pare-feu, activez les ports voulus.

Protocole	Port TCP
HTTP	80
HTTPS	443

Établir une connexion à un appareil

Pour accéder à l'IU Web, procédez comme suit :

1. Ouvrez un navigateur web.
2. Entrez dans le champ d'adresse du navigateur web l'adresse IP ou l'URL de l'appareil.
3. Appuyez sur la touche **Entrée**.
   Si la connexion à l'appareil est correctement établie, la page d'accueil de l'IU Web s'affiche.
4. Connectez-vous.
   Pour plus d'informations, voir "Connexion (Page 66)".

4.2 Connexion

Ce paragraphe décrit les différentes méthodes de connexion sous SINEC OS.

4.2.1 Profils d'utilisateur et mots de passe prédéfinis

Les profils utilisateur et mots de passe suivants sont configurés par défaut sous SINEC OS :

⚠ **PRUDENCE**
Vulnérabilité - Risque d'intrusion et/ou d'abus Avant la mise en service de l'appareil, modifiez les mots de passe par défaut pour empêcher toute intrusion. Pour plus d'informations, voir "Modification du mot de passe d'un utilisateur (Page 113)".

Profil	Mot de passe
admin	admin

4.2.2 Se connecter à un appareil avec les paramètres par défaut

Pour vous connecter à un appareil avec les paramètres par défaut, procédez comme suit :

1. Établissez une connexion sécurisée à l'appareil et ouvrez l'IU Web.
   La page d'accueil de l'IU Web s'affiche.
   Pour plus d'informations, voir "Accès à l'IU Web via une connexion réseau (Page 65)".
2. Cliquez sur le champ **Username** et saisissez le nom d'utilisateur par défaut.
   Pour plus d'informations, voir "Profils d'utilisateur et mots de passe prédéfinis (Page 66)".
3. Cliquez sur le champ **Password** et saisissez le mot de passe par défaut.

4. Cliquez sur **Sign In** ou appuyez sur la **touche Entrée**.
   L'appareil contrôle les entrées. Comme retour d'information visuel, un symbole de chargement s'affiche à droite des champs.
   - Si les entrées sont correctes, deux autres champs de saisie s'affichent. Il vous est demandé de modifier le mot de passe par défaut.
     Passez à l'étape suivante.
   - Un point d'exclamation rouge s'affiche à droite des champs ainsi qu'un message d'erreur si les entrées ne sont pas correctes. Renouvelez les dernières opérations.
5. Cliquez sur le champ **New Password** et saisissez un nouveau mot de passe.
   Vous pouvez saisir un mot de passe comme suit :
   - Comme mot de passe de hachage
     Si un mot de passe débute par l'une des combinaisons de caractères suivantes, il est considéré comme mot de passe de hachage et est enregistré sous cette forme : 1 (MD5), 5 (SHA-256) ou 6 (SHA-512)
   - Comme mot de passe en clair
     Si un mot de passe débute par une combinaison de caractères autres que 1, 5 ou 6, il est considéré comme un mot de passe en clair et converti par l'appareil à l'aide de l'algorithme de hachage SHA-512.
     Si un mot de passe débute par la combinaison de caractères `$0$`, il est également considéré comme un mot de passe en clair. Utilisez cette combinaison de caractères, si vous voulez configurer un mot de passe qui débute par le caractère `$`.
     Exemple : `$0$$iemens123`

   Conditions :
   - Il doit compter de 6 à 255 caractères
   - Tous les caractères standard ainsi que les caractères spéciaux suivants sont autorisés : # $ % & ( ) * + , - . / : < = > @ [ ] ^ _ { } ~
6. Cliquez sur le champ **Confirm Password** et répétez le nouveau mot de passe.
7. Cliquez sur **Sign In** ou appuyez sur la **touche Entrée**.
   L'appareil contrôle les entrées. Comme retour d'information visuel, un symbole de chargement s'affiche à droite des champs.
   - Une coche verte s'affiche brièvement à côté des champs si les entrées étaient correctes. Pour activer les modifications, la session de l'IU Web est automatiquement rechargée au bout de quelques secondes.
     Connectez-vous avec le nom d'utilisateur et le nouveau mot de passe.
   - Un point d'exclamation rouge s'affiche à droite des champs ainsi qu'un message d'erreur si les entrées ne sont pas correctes. Renouvelez les dernières opérations.

4.2.3 Connexion à un appareil configuré

Pour vous connecter à un appareil configuré, procédez comme suit :

1. Établissez une connexion sécurisée à l'appareil et ouvrez l'IU Web.
   La page d'accueil de l'IU Web s'affiche.
   Pour plus d'informations, voir "Accès à l'IU Web via une connexion réseau (Page 65)".
2. Cliquez sur le champ **Username** et saisissez le nom d'utilisateur.
3. Cliquez sur le champ **Password** et saisissez le mot de passe correspondant.
4. Cliquez sur **Sign In** ou appuyez sur la **touche Entrée**.
   L'appareil contrôle les entrées. Comme retour d'information visuel, un symbole de chargement s'affiche à droite des champs.
   - Une coche verte s'affiche brièvement à côté des champs si les entrées étaient correctes, puis la page d'accueil de l'IU Web s'affiche.
   - Un point d'exclamation rouge s'affiche à droite des champs ainsi qu'un message d'erreur si les entrées ne sont pas correctes. Renouvelez les dernières opérations.

4.3 Déconnexion

Pour vous déconnecter, procédez comme suit :

1. Dans la barre d'état, cliquez sur le bouton du **profil utilisateur**.
2. Cliquez sur le bouton **Logout**.

4.4 Paramètres de base

Ce paragraphe décrit les opérations de la configuration de base qui doivent être exécutées lors de la première mise en service.

4.4.1 Configuration des paramètres de base

Pour configurer les paramètres de base de l'appareil, procédez comme suit :

1. Entrez le nom d'hôte de l'appareil.
   Pour plus d'informations, voir "Modification du nom d'hôte (Page 69)".
2. Saisissez l'emplacement physique de l'appareil.
   Pour plus d'informations, voir "Spécification du lieu d'implantation (Page 69)".
3. Définition d'un interlocuteur responsable de l'appareil
   Pour plus d'informations, voir "Définition d'un interlocuteur responsable de l'appareil (Page 69)".
4. [Facultatif] Définir la passerelle par défaut manuellement.
   Pour plus d'informations, voir "Configuration manuelle de la passerelle par défaut (Page 70)".

4.4.1.1 Modification du nom d'hôte

Le nom d'hôte est un code qui identifie l'appareil au sein du réseau. Le nom d'hôte forme également l'invite de commande de la CLI (par exemple. localhost#).

Le nom d'hôte peut être une désignation de domaine ou un nom de domaine pleinement qualifié (Fully Qualified Domain Name, FQDN).

Remarque

Le nom d'hôte qui précède possède le format : **{ Device Family Name }-{ Serial Number}**.

Procédez comme suit pour modifier le nom d'hôte :

1. Naviguez vers **System** ≫ **Information & State**.
2. Sous **System Information**, entrez le nom d'hôte de l'appareil qui figure sous **Hostname**.
   Conditions :
   - Il doit compter de 1 à 253 caractères.
   - Le nom ne doit pas contenir d'espace.
3. Validez la modification.

4.4.1.2 Spécification du lieu d'implantation

Spécifiez le lieu d'implantation pour que les administrateurs trouvent plus facilement l'emplacement physique de l'appareil.

Pour indiquer où se trouve l'appareil, procédez comme suit :

1. Naviguez vers **System** ≫ **Information & State**.
2. Sous **System Information**, entrez une description de l'emplacement indiqué sous **Location**.
   Condition :
   - Elle doit compter de 1 à 255 caractères.
3. Validez la modification.

4.4.1.3 Définition d'un interlocuteur responsable de l'appareil

Entrez pour d'autres utilisateurs un interlocuteur Il peut s'agir ici du propriétaire de l'appareil ou d'un administrateur système.

Procédez comme suit pour saisir un interlocuteur :

1. Naviguez vers **System** ≫ **Information & State**.
2. Sous **System Information**, saisissez le nom de l'interlocuteur, p. ex. "Pierre Dupont (pdupont@entreprise.com)" sous **Contact**.
   Condition :
   - Il doit compter de 0 à 255 caractères.
3. Validez la modification.

4.4.1.4 Configuration manuelle de la passerelle par défaut

Tous les paquets IP pour lesquels pas d'autres informations de routage n'ont été trouvées sont transmis à la passerelle par défaut. La passerelle par défaut retransmet tous les paquets IP dont l'adresse de destination se trouve dans un autre sous-réseau que l'appareil.

L'adresse IP de la passerelle par défaut peut être configurée manuellement pour l'appareil ou via un protocole de gestion de réseau (p. ex. DHCP).

Aucune passerelle par défaut n'est configurée par défaut pour l'appareil.

Pour configurer manuellement la passerelle par défaut, procédez comme suit :

1. Naviguez vers **Interfaces** ≫ **IP Interfaces**.
2. Sous **IPv4 Default Gateway**, saisissez l'adresse IP de la passerelle par défaut dans le champ **Default Gateway Address (Static)**.
   Condition :
   – L'adresse IPv4 doit se trouver dans un sous-réseau actif.
3. Validez la modification.

4.4.2 Affichage de la passerelle par défaut

L'adresse IP de la passerelle par défaut peut être configurée manuellement pour l'appareil ou via un protocole de gestion de réseau (p. ex. DHCP). Si la passerelle par défaut a été configurée par les deux moyens, l'attribution dynamique via DHCP est prioritaire.

Pour afficher la passerelle par défaut, naviguez vers **Interfaces** ≫ **IP Interfaces**.

Sous **IPv4 Default Gateway**, le champ **Default Gateway Address** affiche l'adresse IP de la passerelle par défaut de l'appareil.

Gestion de l'appareil 5

Ce chapitre décrit comment gérer le matériel, notamment comment redémarrer ou arrêter l'appareil, gérer le firmware ou les fichiers de configuration.

5.1 Redémarrage ou arrêt de l'appareil

Ce chapitre décrit comment redémarrer et arrêter l'appareil.

5.1.1 Ce qu'il faut savoir sur le redémarrage et l'arrêt de l'appareil

Ce paragraphe explique quelles sont les conséquences d'un redémarrage ou d'un arrêt de l'appareil sur les sessions ouvertes, les actions en cours et les modifications de la configuration.

5.1.1.1 Rejet d'une commande

Une commande de redémarrage ou d'arrêt est rejetée par l'appareil si l'appareil est en train de charger un fichier de firmware.

Lorsque l'appareil rejette une commande, un message d'erreur s'affiche et une entrée est inscrite dans le journal d'incidents.

Un utilisateur ne peut pas empêcher le redémarrage ou l'arrêt de l'appareil par un autre utilisateur.

5.1.1.2 Fermeture de sessions

Si la commande est exécutée via une interface utilisateur interactive (CLI/Web UI) et si d'autres sessions sont actives, l'utilisateur exécutant en est informé et il lui est demandé de valider la commande. Si l'utilisateur confirme, toutes les sessions actives sont fermées, hormis sa propre session. La session de l'utilisateur exécutant est fermée conformément aux paramètres de timeout de l'appareil.

En cas d'interfaces utilisateur non interactives (NETCONF) la commande est exécutée sans validation et toutes les sessions sont fermées.

Pour s'assurer que la configuration ne sera pas modifiée après l'exécution de la commande, toute nouvelle session est bloquée.

Exemple

Dans cet exemple, l'appareil est redémarré via la CLI et une autre session est active.

```
localhost# system restart
Are you sure you want to restart the device? [no,yes] yes
```

```
There are 1 other active user session(s) which would be killed. Are
you sure you want to continue? [no,yes] yes
```

5.1.1.3 Prise en compte de la validation des modifications de la configuration

Si un utilisateur a validé des modifications de la configuration (`commit`), cette action est achevée.

Les modifications provisoires (`confirmed commit`) sont annulées.

5.1.2 Redémarrage de l'appareil

Lors du redémarrage, l'appareil est réinitialisé, le firmware interne est rechargé, puis l'appareil exécute un autotest. Les paramètres de la configuration de démarrage sont conservés, l'adresse IP de l'appareil p. ex. Les entrées apprises de la table d'adresses sont effacées. Vous pouvez laisser la fenêtre du navigateur ouverte lors du redémarrage de l'appareil. Après le redémarrage, vous devez vous reconnecter.

Remarque

Si vous redémarrez l'appareil alors qu'il est connecté à un SCALANCE LPE, le SCALANCE LPE est également redémarré.

Pour redémarrer l'appareil, procédez comme suit :

1. Naviguez vers **System** ≫ **Restart** ≫ **Restart**.
2. Sous **Restart System**, cliquez sur **Restart**.
3. Répondez à la demande de confirmation par **Yes**.
   L'appareil redémarre. Lorsque le redémarrage est terminé, la page d'ouverture de session s'affiche.
   Pour abandonner le redémarrage, répondez par **No** à la demande de confirmation.
4. Connectez-vous.
   Pour plus d'informations, voir "Connexion (Page 66)".

5.2 Restauration des paramètres par défaut de l'appareil

IMPORTANT
Risque de connexion - Risque de défaillance des communications Selon la configuration de votre réseau, le rétablissement des paramètres par défaut de votre appareil risque de causer la rotation en boucle de trames et par conséquent la défaillance du trafic de données.

IMPORTANT
Risque de configuration - Risque de perte de données Si un CLP est embroché sur l'appareil, le CLP est également réinitialisé. Les licences enregistrées sur le CLP sont également conservées.

Remarque

Si vous rétablissez les paramètres par défaut de l'appareil, toutes les configurations sont effacées, y compris :

- l'adresse IP
- les utilisateurs créés
- les mots de passe
- les clés et certificats personnalisés

L'appareil n'est ensuite plus accessible que par l'interface série

Si vous affectez à l'appareil une adresse IP via DHCP ou DCP (SINEC PNI par ex.), vous pourrez, avec un profil utilisateur prédéfini, accéder via une connexion réseau à la CLI et à l'IU Web de l'appareil.

Remarque

Si vous restaurez les paramètres par défaut de l'appareil alors qu'il est connecté à un SCALANCE LPE, ceci n'a aucun impact sur la configuration du SCALANCE LPE. Le redémarrage de l'appareil redémarre également le SCALANCE LPE.

Pour rétablir les paramètres par défaut de l'appareil, procédez comme suit :

1. Naviguez vers **System** ≫ **Restart** ≫ **Restore Defaults & Restart**.
2. Sous **Restore Defaults & Restart**, cliquez sur **Restart**.
3. Répondez à la demande de confirmation par **Yes**.
   L'appareil redémarre avec les paramètres par défaut. Lorsque le redémarrage est terminé, la page d'ouverture de session s'affiche.
   Pour abandonner la restauration des paramètres par défaut, répondez par **No** à la demande de confirmation.
4. Connectez-vous.
   Pour plus d'informations, voir "Se connecter à un appareil avec les paramètres par défaut (Page 66)".

5.3 Mise hors service l'appareil

Avant de le mettre hors service, veuillez vous assurer que l'appareil a été intégralement mis hors tension – soit durablement, soir pour la maintenance par des tiers. Ceci comprend également, la suppression de toutes les informations propriétaires sensibles.

Remarque

Si l'appareil est mis hors service pour son élimination, respectez pour son élimination conforme les instructions du manuel de mise en œuvre.

Pour mettre l'appareil hors service, procédez comme suit :

1. Procurez-vous une copie du firmware actuellement installé sur l'appareil.
   Pour plus d'informations, voir "Obtention d'un paquet de firmware (Page 75)".
2. Chargez à nouveau le firmware courant et restaurez les paramètres de configuration par défaut. Ceci doit être exécuté deux fois pour être sûr que toutes les informations propriétaires ont été supprimées des deux partitions.
   Pour plus d'informations sur le chargement du firmware et la restauration des paramètres de configuration, voir "Rétrograder le firmware (Page 78)".
3. Arrêtez l'appareil.
   Pour plus d'informations, voir le **Manuel de configuration SINEC OS CLI**.

5.4 Firmware

Ce chapitre décrit comment modifier la version de firmware installée sur l'appareil.

Remarque

Si vous voulez passer d'une version de firmware de SINEC OS à une autre version, tenez toujours compte de la documentation de la version actuellement installée sur l'appareil. Les instructions se rapportant à différentes versions peuvent varier.

Les descriptions ci-après ne s'appliquent que pour la version de SINEC OS pour laquelle elles ont été rédigées. Pour les indications sur la version de SINEC OS, voir la page de titre et les lignes de bas de page du document.

Remarque

Conformez-vous toujours aux spécifications et restrictions publiées à propos d'une version de firmware. Vous trouverez également une liste des publications de firmware de SINEC OS sur SIOS.

5.4.1 Ce qu'il faut savoir sur la gestion du firmware

Les versions de firmware sont gérées via deux partitions. Une partition est toujours activée (firmware actif), tandis que l'autre est toujours désactivée (firmware de sauvegarde). Deux versions de firmware sont donc toujours enregistrées sur l'appareil.

Les modifications du firmware sont par conséquent toujours apportées à la partition inactive. La partition active est donc bloquée pour les modifications par le système et reste donc active après une modification du firmware. Ceci permet de s'assurer que le système reste opérationnel et que l'on évite des interruptions au cas où p. ex. le chargement du firmware aurait échoué.

La partition mise à jour n'est activée qu'après un redémarrage. La partition utilisée jusque-là est désactivée et reste disponible comme sauvegarde.

Si vous démarrez l'appareil après un changement de firmware, le firmware actif jusque-là est enregistré en même temps que la base de données de configuration. Lorsque vous activez un firmware de sauvegarde, vous restaurez en même temps la base de données de configuration.

5.4.2 Affichage de la version de firmware courante

Pour afficher la version de firmware courante sur l'appareil, naviguez jusqu'à la page d'accueil.

Sous **Information Dashboard**, l'écran affiche les informations suivantes :

Paramètres	Description
Running Firmware	Version de firmware installée sur l'appareil et active
Backup Firmware	Version de firmware installée sur l'appareil et inactive

Vous pouvez également naviguer vers **System** ≫ **Load & Save** ≫ **Firmware**. Sous **Firmware Information**, l'écran affiche les informations complémentaires suivantes :

Paramètres	Description
Running Firmware After Restart	Version de firmware installée qui sera activée au prochain démarrage de l'appareil
Bootloader	Version installée du chargeur-amorce qui est exécutée sur l'appareil

5.4.3 Obtention d'un paquet de firmware

Des paquets de firmware valides sont téléchargeables par défaut sur le Siemens Industry Online Support (SIOS (https://support.industry.siemens.com/cs/de/en/ps/15296/dl)). Vous pouvez également vous procurer des paquets de firmware auprès du service après-vente Siemens.

Pour obtenir un paquet de firmware via SIOS, procédez comme suit :

1. Téléchargez un paquet de firmware comme décrit sur SIOS. Le paquet de firmware est mis à disposition sous forme de fichier ZIP et contient :
   - un fichier de firmware
     le nom du fichier de firmware indique son numéro de version (par exemple. V02.00.00.00). l numéro de version est composé comme suit :
     <Lettre de code><Version fonctionnelle>.<Version>.<Service Pack>.<Hotfix>
   - Conditions de licence correspondantes
2. Enregistrez le fichier de firmware localement sur votre PC ou sur un serveur.
   Selon l'interface utilisateur via laquelle vous chargez le firmware, vous disposez de plusieurs possibilités.

3. Décompressez le contenu du fichier comprissé et vérifiez que le contenu n'a pas été modifié.
4. Selon la version de firmware, effectuez une mise à niveau ou rétrogradez le firmware.
   Pour la suite des opérations, voir "Mise à niveau du firmware (Page 76)" ou "Rétrograder le firmware (Page 78)".

5.4.4 Mise à niveau du firmware

Vous pouvez charger un fichier de firmware à partir d'un PC client local ou d'un serveur distant.

5.4.4.1 Chargement d'un fichier de firmware à jour à partir d'un PC client local

IMPORTANT
Danger électrique - risque de défaut de l'appareil en cas de perte de l'alimentation électrique Si l'alimentation de l'appareil est coupée pendant le chargement du fichier de firmware, il peut en résulter un état d'erreur. Ne coupez pas l'alimentation de l'appareil pendant le chargement du fichier de firmware.

Remarque

Les options suivantes sont disponibles pour interrompre ou annuler un changement de firmware :

- Si vous n'avez pas encore redémarré l'appareil, vous pouvez rejeter le fichier de firmware chargé.
  Pour plus d'informations, voir "Rejet d'un fichier de firmware chargé (Page 80)".
- Si vous avez redémarré l'appareil, vous pouvez activer le firmware de sauvegarde.
  Pour plus d'informations, voir "Activation du firmware de sauvegarde (Page 81)".

Pour charger un fichier de firmware sur l'appareil à partir d'un PC client local, procédez comme suit :

1. Naviguez vers **System** ≫ **Load & Save** ≫ **Firmware**.
2. Sous **Load Firmware from Local PC**, ouvrez à l'aide du bouton **Firmware File** une boîte de dialogue pour sélectionner un fichier.
3. Sélectionnez le fichier de firmware voulu dans la boîte de dialogue puis cliquez sur **Ouvrir**.
4. Pour charger le fichier de firmware, cliquez sur **Load**.
   Sous **Firmware Load Progress**, vous pouvez suivre la progression du chargement.
   - Une icône de chargement s'affiche pendant le chargement du firmware.
   - Si le firmware a été chargé avec succès, une coche verte s'affiche à droite du champ.
   - Si une erreur s'est produite lors du chargement du firmware, un point d'exclamation rouge s'affiche à droite du champ et un message d'erreur s'affiche.

   Pendant le chargement du fichier de firmware, vous pouvez interrompre le processus de chargement en cliquant sur le bouton **Abort**.

5. Pour activer le firmware mis à jour, redémarrez l'appareil.
   Pour plus d'informations, voir "Redémarrage de l'appareil (Page 72)".
   L'appareil redémarre avec la version de firmware à jour. Lorsque le redémarrage est terminé, la page d'ouverture de session s'affiche.
6. Connectez-vous.
   Pour plus d'informations, voir "Connexion à un appareil configuré (Page 68)".
7. [facultatif] Contrôlez la version de firmware.
   Pour plus d'informations, voir "Affichage de la version de firmware courante (Page 75)".

5.4.4.2 Chargement d'un fichier de firmware à jour à partir d'un serveur distant

Vous pouvez charger un fichier de firmware à partir d'un serveur distant.

Conditions

- Vous avez configuré un serveur de manière adéquate.
- Le fichier de firmware (.sfw) se trouve sur le serveur.
- Il existe une connexion entre l'appareil et le serveur.
- Selon votre configuration, le nom d'utilisateur et le mot de passe doivent être connus.

Chargement d'un fichier de firmware sur l'appareil

IMPORTANT
Danger électrique - risque de défaut de l'appareil en cas de perte de l'alimentation électrique Si l'alimentation de l'appareil est coupée pendant le chargement du fichier de firmware, il peut en résulter un état d'erreur. Ne coupez pas l'alimentation de l'appareil pendant le chargement du fichier de firmware.

Remarque

Les options suivantes sont disponibles pour interrompre ou annuler un changement de firmware :

- Si vous n'avez pas encore redémarré l'appareil, vous pouvez rejeter le fichier de firmware chargé.
  Pour plus d'informations, voir "Rejet d'un fichier de firmware chargé (Page 80)".
- Si vous avez redémarré l'appareil, vous pouvez activer le firmware de sauvegarde.
  Pour plus d'informations, voir "Activation du firmware de sauvegarde (Page 81)".

Pour charger un fichier de firmware sur l'appareil via un serveur distant, procédez comme suit :

1. Naviguez vers **System** ≫ **Load & Save** ≫ **Firmware**.
2. Sous **Load Firmware from Remote Server**, configurez les paramètres du serveur distant.
   Pour plus d'informations sur le chargement de fichiers, via un serveur distant, voir "Chargement et enregistrement de fichiers via un serveur distant. (Page 47)".

3. Pour charger le fichier de firmware, cliquez sur **Load**.
   - Une icône de chargement s'affiche pendant le chargement du firmware.
   - Si le firmware a été chargé avec succès, une coche verte s'affiche à droite du champ.
   - Si une erreur s'est produite lors du chargement du firmware, un point d'exclamation rouge s'affiche à droite du champ et un message d'erreur s'affiche.
4. Pour activer le firmware mis à jour, redémarrez l'appareil.
   Pour plus d'informations, voir "Redémarrage de l'appareil (Page 72)".
   L'appareil redémarre avec la version de firmware à jour. Lorsque le redémarrage est terminé, la page d'ouverture de session s'affiche.
5. Connectez-vous.
   Pour plus d'informations, voir "Connexion à un appareil configuré (Page 68)".
6. [facultatif] Contrôlez la version de firmware.
   Pour plus d'informations, voir "Affichage de la version de firmware courante (Page 75)".

5.4.5 Rétrograder le firmware

Vous pouvez charger un fichier de firmware à partir d'un PC client local ou d'un serveur distant.

5.4.5.1 Chargement d'un ancien fichier de firmware à partir d'un PC client local

IMPORTANT
Danger électrique - risque de défaut de l'appareil en cas de perte de l'alimentation électrique Si l'alimentation de l'appareil est coupée pendant le chargement du fichier de firmware, il peut en résulter un état d'erreur. Ne coupez pas l'alimentation de l'appareil pendant le chargement du fichier de firmware.

Remarque

Les options suivantes sont disponibles pour interrompre ou annuler un changement de firmware :

- Si vous n'avez pas encore redémarré l'appareil, vous pouvez rejeter le fichier de firmware chargé.
  Pour plus d'informations, voir "Rejet d'un fichier de firmware chargé (Page 80)".
- Si vous avez redémarré l'appareil, vous pouvez activer le firmware de sauvegarde.
  Pour plus d'informations, voir "Activation du firmware de sauvegarde (Page 81)".

Pour charger un fichier de firmware sur l'appareil à partir d'un PC client local, procédez comme suit :

1. Naviguez vers **System** ≫ **Load & save** ≫ **Firmware**.
2. Sous **Load Firmware from Local PC**, ouvrez à l'aide du bouton **Firmware File** une boîte de dialogue pour sélectionner un fichier.

3. Sélectionnez le fichier de firmware voulu dans la boîte de dialogue puis cliquez sur **Ouvrir**.
4. Pour charger le fichier de firmware, cliquez sur **Load**.
   Sous **Firmware Load Progress**, vous pouvez suivre la progression du chargement.
   - Une icône de chargement s'affiche pendant le chargement du firmware.
   - Si le firmware a été chargé avec succès, une coche verte s'affiche à droite du champ.
   - Si une erreur s'est produite lors du chargement du firmware, un point d'exclamation rouge s'affiche à droite du champ et un message d'erreur s'affiche.

   Pendant le chargement du fichier de firmware, vous pouvez interrompre le processus de chargement en cliquant sur le bouton **Abort**.
5. Pour activer le firmware mis à jour, restaurez les paramètres par défaut de l'appareil.
   Pour plus d'informations, voir "Restauration des paramètres par défaut de l'appareil (Page 72)".
   L'appareil redémarre avec la version de firmware à jour et les paramètres par défaut. Lorsque le redémarrage est terminé, la page d'ouverture de session s'affiche.
6. Connectez-vous.
   Pour plus d'informations, voir "Se connecter à un appareil avec les paramètres par défaut (Page 66)".
7. [facultatif] Contrôlez la version de firmware.
   Pour plus d'informations, voir "Affichage de la version de firmware courante (Page 75)".

5.4.5.2 Chargement d'un ancien fichier de firmware à partir d'un serveur distant

Vous pouvez charger un fichier de firmware à partir d'un serveur distant.

Conditions

- Vous avez configuré un serveur de manière adéquate.
- Le fichier de firmware (.sfw) se trouve sur le serveur.
- Il existe une connexion entre l'appareil et le serveur.
- Selon votre configuration, le nom d'utilisateur et le mot de passe doivent être connus.

Chargement d'un fichier de firmware sur l'appareil

IMPORTANT
Danger électrique - risque de défaut de l'appareil en cas de perte de l'alimentation électrique Si l'alimentation de l'appareil est coupée pendant le chargement du fichier de firmware, il peut en résulter un état d'erreur. Ne coupez pas l'alimentation de l'appareil pendant le chargement du fichier de firmware.

Remarque

Les options suivantes sont disponibles pour interrompre ou annuler un changement de firmware :

- Si vous n'avez pas encore redémarré l'appareil, vous pouvez rejeter le fichier de firmware chargé.
  Pour plus d'informations, voir "Rejet d'un fichier de firmware chargé (Page 80)".
- Si vous avez redémarré l'appareil, vous pouvez activer le firmware de sauvegarde.
  Pour plus d'informations, voir "Activation du firmware de sauvegarde (Page 81)".

Pour charger un fichier de firmware sur l'appareil via un serveur distant, procédez comme suit :

1. Naviguez vers **System** ≫ **Load & Save** ≫ **Firmware**.
2. Sous **Load Firmware from Remote Server**, vous pouvez configurer les paramètres du serveur distant.
   Pour plus d'informations sur le chargement de fichiers, via un serveur distant, voir "Chargement et enregistrement de fichiers via un serveur distant. (Page 47)".
3. Pour charger le fichier de firmware, cliquez sur **Load**.
   – Une icône de chargement s'affiche pendant le chargement du firmware.
   – Si le firmware a été chargé avec succès, une coche verte s'affiche à droite du champ.
   – Si une erreur s'est produite lors du chargement du firmware, un point d'exclamation rouge s'affiche à droite du champ et un message d'erreur s'affiche.
4. Pour activer le firmware mis à jour, restaurez les paramètres par défaut de l'appareil.
   Pour plus d'informations, voir "Restauration des paramètres par défaut de l'appareil (Page 72)".
   L'appareil redémarre avec la version de firmware à jour et les paramètres par défaut. Lorsque le redémarrage est terminé, la page d'ouverture de session s'affiche.
5. Connectez-vous.
   Pour plus d'informations, voir "Se connecter à un appareil avec les paramètres par défaut (Page 66)".
6. [facultatif] Contrôlez la version de firmware.
   Pour plus d'informations, voir "Affichage de la version de firmware courante (Page 75)".

5.4.6 Rejet d'un fichier de firmware chargé

Si vous rejetez un fichier de firmware chargé, le firmware utilisé jusqu'à présent reste actif après un redémarrage. Le firmware mis à jour reste inactif.

Par défaut, le bouton **Decline** est inactif. Ce bouton n'est actif que si un firmware chargé peut être refusé.

Remarque

Vous ne pouvez rejeter un fichier de firmware que si vous n'avez pas encore redémarré l'appareil après le chargement d'un fichier de firmware.

Pour rejeter un fichier de firmware, procédez comme suit :

1. Naviguez vers **System** ≫ **Load & Save** ≫ **Firmware**.
2. Pour rejeter le firmware chargé, cliquez sous **Firmware Information** sur **Decline**.

Remarque

Pas de demande de confirmation

Le fichier de firmware est directement rejeté. Aucune demande de confirmation ne s'affiche.

5.4.7 Activation du firmware de sauvegarde

Si vous activez le firmware de sauvegarde, le firmware actuellement actif (running firmware) est désactivé.

Dans les cas suivants, vous ne pourrez pas activer le firmware de sauvegarde :

- Si, après le chargement d'un fichier de firmware, vous modifiez la configuration et validez les modifications de la configuration.
- Si vous avez activé un nouveau firmware en restaurant les paramètres par défaut de l'appareil. Après la restauration des paramètres par défaut, attribuez un nouveau mot de passe. Ceci équivaut à une validation de la modification de configuration.
- Si un CLP est embroché sur l'appareil.

Remarque

Vous ne pouvez activer un firmware de sauvegarde que si vous avez redémarré l'appareil après le chargement d'un Fichier de firmware.

Si vous n'avez pas encore redémarré l'appareil, vous pouvez rejeter le fichier de firmware chargé. Pour plus d'informations, voir "Rejet d'un fichier de firmware chargé (Page 80)".

Pour activer le firmware de sauvegarde, procédez comme suit :

1. Naviguez vers **System** ≫ **Load & Save** ≫ **Firmware**.
2. Pour activer le firmware de sauvegarde, cliquez sous **Firmware Information** sur **Rollback**. Lorsque vous activez le firmware de sauvegarde, vous restaurez en même temps la base de données de configuration.

   Remarque

   Pas de demande de confirmation

   Le firmware de sauvegarde chargé est directement activé. Aucune demande de confirmation ne s'affiche.

3. Pour activer le firmware mis à jour, redémarrez l'appareil.
   Pour plus d'informations, voir "Redémarrage de l'appareil (Page 72)".
   L'appareil redémarre avec le firmware de sauvegarde. Lorsque le redémarrage est terminé, la page d'ouverture de session s'affiche.

4. Connectez-vous.
   Pour plus d'informations, voir "Connexion à un appareil configuré (Page 68)".
5. [facultatif] Contrôlez la version de firmware pour vous assurer que la version de firmware inactive jusque-là (Backup Firmware) est à présent active (Running Firmware).
   Pour plus d'informations, voir "Affichage de la version de firmware courante (Page 75)".

5.5 Matériel de l'appareil

Cette section décrit comment déterminer le profil matériel de l'appareil.

5.5.1 Listage des constituants matériels

Pour lister les constituants matériels installés sur votre appareil, naviguez vers **System** ≫ **Hardware** ≫ **Hardware Information**.

Les informations suivantes sont affichées sous **Hardware Information** :

Paramètres	Description
Component Name	Un nom unique du constituant
Class	Le type du constituant
Description	Une description du constituant
Parent	Le constituant parent
Hardware Revision	La version matérielle
Serial Number	Le numéro de série du matériel
Operational State	L'état de fonctionnement du constituant. Options disponibles : • **enabled** - Le constituant est opérationnel. • **disabled** - Le constituant a été désactivé.
Status	Informations complémentaires sur l'état actuel du constituant Options disponibles : • **OFF** - Le constituant est hors tension. • **ON** - Le constituant est sous tension. • **OPEN** - Le constituant est ouvert. S'applique à tous les constituants de relais (contact de signalisation). • **CLOSE** - Le constituant est fermé. S'applique à tous les constituants de relais (contact de signalisation). • **{ Couleur }** - Couleur du constituant. S'applique aux LED.
Article Number	Le numéro d'article (référence)

5.6 Fichier de configuration

Les paramètres de configuration SINEC OS peuvent être enregistrés et chargés.

Vous pouvez enregistrer la configuration de votre appareil et la stocker comme copie de sauvegarde.

Vous pouvez charger à nouveau ces copies sur le même appareil pour restaurer une configuration antérieure. Une copie de sauvegarde permet en outre, en cas de besoin ou de panne, d'échanger facilement et rapidement un appareil sans être obligé de configurer l'appareil de rechange.

La condition requise pour pouvoir transférer la configuration sur un appareil de rechange est que le fichier de configuration ait été enregistré par un type d'appareil compatible (même numéro d'article).

Si vous chargez la configuration d'un constituant de réseau défaillant sur un appareil de rechange compatible, l'appareil de rechange adopte immédiatement la configuration. Tenez compte des points suivants :

- Si la configuration IP est obtenue via DHCP, vous devez reconfigurer le serveur DHCP en conséquence.
- Si la configuration comprend des fonctions reposant sur des adresses MAC, adaptez-les en conséquence.

5.6.1 Enregistrement le la configuration courante sous forme de fichier sur un PC client local

Remarque

Si vous modifiez un fichier de configuration enregistré et le chargez à nouveau sur un appareil, il peut en résulter un comportement imprévisible ou la défaillance des communications.

Les fichiers de configuration enregistrés ne doivent être modifiés que par des utilisateurs expérimentés.

Pour enregistrer la configuration courante sous forme de fichier sur PC local, procédez comme suit :

1. Vérifiez que l'IU Web ne se trouve pas en mode configuration exclusive
   Pour plus d'informations, voir chapitre "Barre d'état (Page 38)"
2. Veuillez vous assurer qu'aucun autre utilisateur n'a activé la configuration exclusive.
   Pour plus d'informations, voir chapitre "Affichage d'utilisateurs actifs (Page 114)"
3. Naviguez vers **System** ≫ **Load & Save** ≫ **Configuration**.

4. [Facultatif] Sous **Save Configuration to Local PC** vous pouvez enregistrer le fichier en mode protégé avec **File Protection**.
   Options disponibles :

Option	Description
Disabled	**Par défaut** Le configuration est enregistrée sans autres options.
Enabled	La configuration est enregistrée en mode protégé. En mode protégé, le fichier est enregistré avec une somme de contrôle. La somme de contrôle permet de s'assurer que le fichier enregistré est resté inchangé lors du chargement sur un appareil. Lorsque le fichier enregistré est chargé, l'appareil vérifie la somme de contrôle. Si le fichier a été modifié, les sommes de contrôle ne concordent plus et le fichier n'est pas chargé.

5. [Facultatif] Si vous avez sélectionné sous **File Protection** l'option **Enabled**, attribuez sous **File Password** un mot de passe.
   Condition :
   - Elle doit compter de 1 à 255 caractères.
   - Tous les caractères standard ainsi que les caractères spéciaux suivants sont autorisés : # $ % & ( ) * + , - . / : < = > @ [ ] ^ _ { } ~
6. [Facultatif] Si vous avez attribué un mot de passe sous **File Password**, répétez le mot de passe sous **File Password-Confirm**.
7. Cliquez sur **Save**.
   Le fichier sera enregistré directement dans un dossier prédéfini ou bien, selon le paramétrage de votre navigateur web, vous devrez d'abord choisir l'emplacement.

   Remarque

   Attendez que l'enregistrement soit achevé avant d'apporter des modifications à la configuration de l'appareil.

   Pendant que la configuration est enregistrée, une icône de chargement s'affiche à droite du bouton.
   - Si l'enregistrement s'est terminé avec succès, une coche verte s'affiche.
   - Un point d'exclamation rouge et un message d'erreur s'affichent si l'enregistrement a échoué. Renouvelez les dernières opérations.

   La configuration est enregistrée au format XML.

5.6.2 Enregistrement le la configuration courante sous forme de fichier sur un serveur distant

Vous pouvez enregistrer la configuration courante de l'appareil sur un serveur distant.

Conditions

- Vous avez configuré un serveur de manière adéquate.
- Il existe une connexion entre l'appareil et le serveur.
- Selon votre configuration, le nom d'utilisateur et le mot de passe doivent être connus.

Enregistrement de la configuration

Remarque

Si vous modifiez un fichier de configuration enregistré et le chargez à nouveau sur un appareil, il peut en résulter un comportement imprévisible ou la défaillance des communications.

Les fichiers de configuration enregistrés ne doivent être modifiés que par des utilisateurs expérimentés.

Pour enregistrer la configuration courante sous forme de fichier sur un serveur distant, procédez comme suit :

1. Vérifiez que l'IU Web ne se trouve pas en mode configuration exclusive
   Pour plus d'informations, voir chapitre "Barre d'état (Page 38)"
2. Veuillez vous assurer qu'aucun autre utilisateur n'a activé la configuration exclusive.
   Pour plus d'informations, voir chapitre "Affichage d'utilisateurs actifs (Page 114)"
3. Naviguez vers **System** ≫ **Load & Save** ≫ **Configuration**.
4. Sous **Load/Save Configuration from/to Remote Server** sélectionnez pour le paramètre **Action** l'option **Save**.
5. Configurez les paramètres du serveur distant.
   Pour plus d'informations sur l'enregistrement de fichiers, via un serveur distant, voir "Chargement et enregistrement de fichiers via un serveur distant. (Page 47)".
6. Cliquez sur **Save**.

   Remarque

   Attendez que l'enregistrement soit achevé avant d'apporter des modifications à la configuration de l'appareil.

   Pendant que la configuration est enregistrée, une icône de chargement s'affiche à droite du bouton.

   – Si l'enregistrement s'est terminé avec succès, une coche verte s'affiche.

   – Un point d'exclamation rouge et un message d'erreur s'affichent si l'enregistrement a échoué. Renouvelez les dernières opérations.

   La configuration est enregistrée au format XML.

5.6.3 Chargement d'un ancien fichier de configuration à partir d'un PC client local

Vous pouvez charger un fichier de configuration à partir d'un PC client local.

Conditions

- Le fichier de configuration a été enregistré par un appareil SINEC OS.
- Le fichier de configuration a été enregistré par un type d'appareil compatible (numéros d'article identiques).
- Sur l'appareil qui a enregistré le fichier de configuration, la version de firmware SINEC OS installée était au moins 2.0.

Les configurations non valides sont rejetées avec un message d'erreur le signalant.

Chargement d'un fichier de configuration

IMPORTANT
Risque de configuration - Risque de défaillance des communications Si vous chargez sur un appareil un fichier de configuration, il peut en résulter un comportement imprévisible ou la défaillance des communications. Pour éviter un comportement imprévisible, restaurez les paramètres par défaut de l'appareil. Après la restauration, l'appareil n'est plus accessible que par l'interface série. Si vous affectez à l'appareil une adresse IP via DHCP ou DCP (SINEC PNI par ex.), vous pourrez, avec un profil d'utilisateur prédéfini, accéder via une connexion réseau à la CLI et à l'IU Web de l'appareil. Pour plus d'informations sur la réinitialisation de l'appareil, voir "Restauration des paramètres par défaut de l'appareil (Page 72)".

Remarque

Si vous modifiez un fichier de configuration enregistré et le chargez à nouveau sur un appareil, il peut en résulter un comportement imprévisible ou la défaillance des communications.

Les fichiers de configuration enregistrés ne doivent être modifiés que par des utilisateurs expérimentés.

Pour charger un fichier de configuration sur l'appareil à partir d'un PC local, procédez comme suit :

1. Vérifiez que l'IU Web ne se trouve pas en mode configuration exclusive
   Pour plus d'informations, voir chapitre "Barre d'état (Page 38)"
2. Veuillez vous assurer qu'aucun autre utilisateur n'a activé la configuration exclusive.
   Pour plus d'informations, voir chapitre "Affichage d'utilisateurs actifs (Page 114)"
3. Naviguez vers **System** ≫ **Load & Save** ≫ **Configuration**.

4. Sous **Load Configuration from Local PC**, sélectionnez le comportement de chargement avec **Mode**.
   Options disponibles :

Option	Description
Replace	**Par défaut** Les paramètres de la configuration en cours d'exécution qui sont contenus dans le fichier de configuration sont supprimés par ce paramètre et remplacés par le contenu du fichier de configuration. Les paramètres de la configuration en cours d'exécution ne sont remplacés que si ces paramètres sont également contenus dans le fichier de configuration.
Merge	Ce paramètre fusionne le contenu du fichier de configuration avec la configuration en cours d'exécution. Les paramètres de la configuration en cours d'exécution ne sont fusionnés que si ces paramètres sont également contenus dans le fichier de configuration.

5. [Facultatif] Si la configuration a été enregistrée en mode protégé, sélectionnez sous **File Protection** l'option **Enabled**.
6. [Facultatif] Si la configuration a été enregistrée en mode protégé, un mot de passe a été attribué. Vous avez besoin de ce mot de passe pour charger la configuration.
   Saisissez le mot de passe sous **File Password**.
7. Sous **Configuration File**, ouvrez à l'aide du bouton une boîte de dialogue pour sélectionner un fichier.
8. Sélectionnez le fichier voulu dans la boîte de dialogue puis cliquez sur **Open**.
9. Pour charger le fichier de configuration, cliquez sur **Load**.

   Remarque

   Attendez que le chargement soit achevé avant d'apporter des modifications à la configuration de l'appareil.

   Pendant que la configuration est chargée, une icône de chargement s'affiche à droite du bouton.

   – Si le chargement s'est bien déroulé, une coche verte s'affiche.
   – Un point d'exclamation rouge et un message d'erreur s'affichent si le chargement a échoué. Renouvelez les dernières opérations.

5.6.4 Chargement d'un fichier de configuration à partir d'un serveur distant

Vous pouvez charger un fichier de configuration à partir d'un serveur distant.

Conditions

- Vous avez configuré un serveur de manière adéquate.
- Le fichier de configuration (.xml) se trouve sur le serveur.
- Il existe une connexion entre l'appareil et le serveur.
- Selon votre configuration, le nom d'utilisateur et le mot de passe doivent être connus.

- Le fichier de configuration a été enregistré par un appareil SINEC OS.
- Le fichier de configuration a été enregistré par un type d'appareil compatible (numéros d'article identiques).
- Sur l'appareil qui a enregistré le fichier de configuration, la version de firmware SINEC OS installée était au moins 2.0.

Les configurations non valides sont rejetées avec un message d'erreur le signalant.

Chargement d'un fichier de configuration

IMPORTANT
Risque de configuration - Risque de défaillance des communications Si vous chargez sur un appareil un fichier de configuration, il peut en résulter un comportement imprévisible ou la défaillance des communications. Pour éviter un comportement imprévisible, restaurez les paramètres par défaut de l'appareil. Après la restauration, l'appareil n'est plus accessible que par l'interface série. Si vous affectez à l'appareil une adresse IP via DHCP ou DCP (SINEC PNI par ex.), vous pourrez, avec un profil d'utilisateur prédéfini, accéder via une connexion réseau à la CLI et à l'IU Web de l'appareil. Pour plus d'informations sur la réinitialisation de l'appareil, voir "Restauration des paramètres par défaut de l'appareil (Page 72)".

Remarque

Si vous modifiez un fichier de configuration enregistré et le chargez à nouveau sur un appareil, il peut en résulter un comportement imprévisible ou la défaillance des communications.

Les fichiers de configuration enregistrés ne doivent être modifiés que par des utilisateurs expérimentés.

Pour charger un fichier de configuration sur l'appareil à partir d'un serveur distant, procédez comme suit :

1. Vérifiez que l'IU Web ne se trouve pas en mode configuration exclusive
   Pour plus d'informations, voir chapitre "Barre d'état (Page 38)"
2. Veuillez vous assurer qu'aucun autre utilisateur n'a activé la configuration exclusive.
   Pour plus d'informations, voir chapitre "Affichage d'utilisateurs actifs (Page 114)"
3. Naviguez vers **System** ≫ **Load & Save** ≫ **Configuration**.
4. Sous **Load/Save Configuration from/to Remote Server** sélectionnez pour le paramètre **Action** l'option **Load**.

5. Sous **Mode**, sélectionnez le comportement de chargement.
   Options disponibles :

Option	Description
Replace	**Par défaut** Les paramètres de la configuration en cours d'exécution qui sont contenus dans le fichier de configuration sont supprimés par ce paramètre et remplacés par le contenu du fichier de configuration. Les paramètres de la configuration en cours d'exécution ne sont remplacés que si ces paramètres sont également contenus dans le fichier de configuration.
Merge	Ce paramètre fusionne le contenu du fichier de configuration avec la configuration en cours d'exécution. Les paramètres de la configuration en cours d'exécution ne sont fusionnés que si ces paramètres sont également contenus dans le fichier de configuration.

6. Configurez les paramètres du serveur distant.
   Pour plus d'informations sur le chargement de fichiers, via un serveur distant, voir "Chargement et enregistrement de fichiers via un serveur distant. (Page 47)".
7. [Facultatif] Si la configuration a été enregistrée en mode protégé, sélectionnez sous **File Protection** l'option **Enabled**.
8. [Facultatif] Si la configuration a été enregistrée en mode protégé, un mot de passe a été attribué. Vous avez besoin de ce mot de passe pour charger la configuration.
   Saisissez le mot de passe sous **File Password**.
9. Cliquez sur **Load**.

Remarque

Attendez que le chargement soit achevé avant d'apporter des modifications à la configuration de l'appareil.

Pendant que la configuration est chargée, une icône de chargement s'affiche à droite du bouton.

- Si le chargement s'est bien déroulé, une coche verte s'affiche.
- Un point d'exclamation rouge et un message d'erreur s'affichent si le chargement a échoué. Renouvelez les dernières opérations.

5.6.5 Affichage des informations d'entête d'un fichier de configuration

Pour afficher les informations d'entête d'un fichier de configuration, procédez comme suit :

1. Vérifiez que l'IU Web ne se trouve pas en mode configuration exclusive
   Pour plus d'informations, voir chapitre "Barre d'état (Page 38)"
2. Naviguez vers **System** ≫ **Load & Save** ≫ **Configuration**.
3. Sous **Load/Save Configuration from/to Remote Server** sélectionnez pour le paramètre **Action** l'option **Load**.
4. Configurez les paramètres du serveur distant.
   Pour plus d'informations sur le chargement de fichiers, via un serveur distant, voir "Chargement et enregistrement de fichiers via un serveur distant. (Page 47)".

5. [Facultatif] Si la configuration a été enregistrée en mode protégé, sélectionnez sous **File Protection** l'option **Enabled**.
6. [Facultatif] Si la configuration a été enregistrée en mode protégé, un mot de passe a été attribué. Vous avez besoin de ce mot de passe pour charger la configuration.
   Saisissez le mot de passe sous **File Password**.
7. Cliquez sur **View Info**.
   Pendant que les informations d'entête sont chargées, une icône de chargement s'affiche à droite du bouton.
   - Si l'opération s'achève avec succès, les informations d'entête du fichier de configuration s'affichent sous le bouton.
   - Un point d'exclamation rouge et un message d'erreur s'affichent si l'opération a échoué. Renouvelez les dernières opérations.

Description

Les informations suivantes s'affichent :

Paramètres	Description
Backup Time	Date et heure d'enregistrement du fichier de configuration
Backup By	Utilisateur qui a enregistré le fichier de configuration
Device Type	Nom d'appareil
Serial Number	Numéro de série du matériel
Article Number	Numéro d'article (référence)
Hardware Revision	Version matérielle
Firmware Version	Version du firmware actif sur l'appareil
Hostname	Nom d'hôte configuré
Checksum	Somme de contrôle du fichier de configuration

5.7 Informations sur les logiciels Open Source

Les informations sur les logiciels Open Source (OSS) sont enregistrées sous forme de fichier PDF. Le fichier contient des notes relatives au copyright des logiciels tiers, notamment des logiciels Open Source, contenus dans le présent produit ainsi que les conditions de licence applicables à ces logiciels tiers

Lisez attentivement les informations sur les logiciels Open Source avant d'utiliser le produit.

Les informations OSS sont enregistrées sur l'appareil et sur le support de données fourni.

5.7.1 Enregistrement d'informations OSS sur un PC client local

Pour enregistrer les informations OSS sur un PC client local, procédez comme suit :

1. Naviguez vers **System** ≫ **Load & Save** ≫ **OSS Information**.
2. Sous **Save Open Source Software (OSS) Information to Local PC**, cliquez sur **Save**.
   Le fichier sera enregistré directement dans un dossier prédéfini ou bien, selon le paramétrage de votre navigateur web, vous devrez d'abord choisir l'emplacement.
   Un symbole de chargement s'affiche comme retour d'information visuel, à droite du bouton.
   - Si l'enregistrement s'est terminé avec succès, une coche verte s'affiche.
   - Un point d'exclamation rouge et un message d'erreur s'affichent si l'enregistrement a échoué. Renouvelez les dernières opérations.

5.7.2 Enregistrement d'informations OSS sur un serveur distant

Vous pouvez enregistrer les informations OSS sur un serveur distant.

Conditions

- Vous avez configuré un serveur de manière adéquate.
- Il existe une connexion entre l'appareil et le serveur.
- Selon votre configuration, le nom d'utilisateur et le mot de passe doivent être connus.

Enregistrement des informations OSS

Pour enregistrer les informations OSS sur un serveur distant, procédez comme suit :

1. Naviguez vers **System** ≫ **Load & Save** ≫ **OSS Information**.
2. Sous **Save Open Source Software (OSS) Information to Remote Server**, configurez les paramètres du serveur distant.
   Pour plus d'informations sur le chargement et l'enregistrement de fichiers via un serveur distant, voir "Chargement et enregistrement de fichiers via un serveur distant. (Page 47)".
3. Cliquez sur **Save**.
   Un symbole de chargement s'affiche comme retour d'information visuel, à droite du bouton.
   - Si l'enregistrement s'est terminé avec succès, une coche verte s'affiche.
   - Un point d'exclamation rouge et un message d'erreur s'affichent si l'enregistrement a échoué. Renouvelez les dernières opérations.

5.8 Pupitre opérateur

Selon le lieu d'implantation, vous n'aurez pas toujours un accès direct à l'appareil. L'IU Web propose par conséquent une simulation du pupitre opérateur.

La page d'accueil de l'IU Web affiche **Device Panel** une vue de l'appareil avec le pupitre opérateur.

5.8.1 Ce qu'il faut savoir sur le pupitre opérateur

Le pupitre opérateur de l'appareil comprend les LED et le bouton-poussoir.

5.8.1.1 LED

Chaque appareil possède des LED qui renseignent sur l'état de fonctionnement de l'appareil. Si vous n'avez pas d'accès direct à l'appareil, vous pouvez, grâce aux LED simulées de l'IU Web, surveiller l'état actuel de l'appareil.

L'affichage est mis à jour toutes les 5 secondes.

Les différentes LED sont décrites ci-dessous.

5.8.1.2 LED "A"

La LED "A" (LED d'alarme) visualise l'état de défaut de l'appareil.

Signification durant le démarrage de l'appareil

Couleur de la LED	Etat de la LED	Signification durant le démarrage de l'appareil
-	Eteinte	Le démarrage s'est terminé sans erreur.
Rouge	Allumée	Le démarrage n'est pas encore terminé.

Signification en cours de fonctionnement

Couleur de la LED	Etat de la LED	Signification en cours de fonctionnement
-	Eteinte	L'appareil fonctionne parfaitement.
Rouge	Allumée	L'appareil à détecté une erreur.

5.8.1.3 LED "DM1" et "DM2"

Les LED "DM1" et "DM2" indiquent le mode d'affichage sélectionné.

Il existe 4 modes d'affichage (A, B, C et D). Le mode d'affichage A est le mode par défaut.

Couleur de la LED	Etat de la LED		Signification
	LED DM1	LED DM2	
-	Eteinte		Mode affichage A
Vert	Allumée	Eteinte	Mode affichage B
Vert	Eteinte	Allumée	Mode d'affichage C
Vert	Allumée		Mode d'affichage D

5.8.1.4 LED "L1" et "L2"

Les LED "L1" et "L2" indiquent l'état de l'alimentation aux bornes L1 et L2.

La signification des LED "L1" et "L2" dépend du mode d'affichage sélectionné, voir chapitre "LED "DM1" et "DM2" (Page 92)".

Signification dans les modes d'affichage A, B et C

Dans les modes d'affichage A, B et C, les LED "L1" et "L2" indiquent si la tension d'alimentation est connectée.

LED L1/L2		Connexion L1/L2
Couleur de la LED	**Etat de la LED**	
-	Eteinte	Pas d'alimentation connectée
Vert	Allumée	Alimentation connectée en L1/L2

Signification en mode d'affichage D

Dans la version actuelle, le mode d'affichage D ne fournit pas d'informations.

5.8.1.5 LEDs "P"

Les LED de port "P1", "P2", etc. renseignent sur les ports correspondants.

La signification des LED de port dépend du mode d'affichage sélectionné, voir chapitre "LED "DM1" et "DM2" (Page 92)".

Signification en mode d'affichage A

En mode d'affichage A, les LED de port signalent la présence ou non d'une liaison valide.

Couleur de la LED	Etat de la LED	Signification
-	Eteinte	Pas de lien valide au port (le partenaire de communication est hors tension ou le câble n'est pas connecté par ex.) ou la liaison existe, mais le par est désactivé par le gestionnaire. Dans cet état, aucune donnée n'est émise ou reçue par le port.
Vert	Allumée	Liaison établie et port à l'état normal. Le port est, dans cet état, en mesure d'émettre et de recevoir des données.
	Clignote 1 x fois par période*	Liaison établie et port à l'état "Blocking". Dans cet état, le port n'émet et ne reçoit que des données de gestion (pas de données utiles).
	Clignote 4 x fois par période*	Liaison établie et à l'état "Monitor Port". Dans cet état, le trafic de données d'un autre port est recopié sur ce port.
Jaune	Clignote / allumée	Réception de données sur le port

* 1 période ≙ 2,5 secondes

Signification en mode d'affichage B

En mode d'affichage B, les ports de LED signalent la vitesse de transmission.

Couleur de la LED	État de la LED	Signification
-	Éteinte	Le port fonctionne à 10 Mbit/s
Vert	Allumée	Le port fonctionne à 100 Mbit/s
	Clignote 1 x fois par période*	Le port fonctionne à 10 Gbit/s
Jaune	Allumée	Le port fonctionne à 1 Gbit/s
	Clignote 2 x fois par période*	Le port fonctionne à 2,5 Gbit/s
	Clignote 5 x fois par période*	Le port fonctionne à 5 Gbit/s

* 1 période ≙ 2,5 secondes

Si les paramètres de transmission ne sont pas modifiables (autonégociation désactivée) et si un défaut de connexion survient, la LED de port continue à indiquer la vitesse de transmission paramétrée. Si l'autonégociation est activée, la LED de port s'éteint en présence d'un défaut de connexion.

Signification en mode d'affichage C

En mode d'affichage C, les ports de LED signalent le mode de fonctionnement.

Couleur de la LED	État de la LED	Signification
-	Éteinte	Le port fonctionne en half duplex
Vert	Allumée	Le port fonctionne en full duplex

Signification en mode d'affichage D

Dans la version actuelle, le mode d'affichage D ne fournit pas d'informations.

5.8.1.6 Bouton-poussoir

Chaque appareil possède un bouton-poussoir. Si vous n'avez pas d'accès direct à l'appareil, vous pouvez actionner le bouton-poussoir avec la souris du pupitre opérateur de l'IU Web.

Remarque

Le bouton-poussoir simulé de l'IU Web ne permet pas d'utiliser toutes les fonctions du bouton-poussoir. Vous ne pouvez régler dans l'IU Web que le mode d'affichage.

Sur le pupitre opérateur, le bouton-poussoir est orange.

Pour plus d'informations sur les fonctions du bouton-poussoir, voir "Fonction de bouton-poussoir (Page 96)".

5.8.2 Surveillance de l'état de fonctionnement de l'appareil

Pour surveiller l'état de fonctionnement de l'appareil sur le pupitre opérateur, procédez comme suit :

1. [Facultatif] Paramétrez la mode d'affichage.
   Pour plus d'informations, voir "Réglage du mode d'affichage (Page 95)".
2. Contrôlez à l'aide des LED l'état ou les paramétrages voulus.
   Les LED indiquent le mode d'affichage momentané, l'état des ports et de l'alimentation ou des alimentations ainsi que les défauts.
   Pour plus d'informations, voir "LED (Page 92)".

5.8.3 Réglage du mode d'affichage

Appuyez sur le bouton-poussoir comme suit pour sélectionner le mode d'affichage.

Actionnez le bouton-poussoir en partant du mode d'affichage A	**Etat de la LED**		**Mode affichage**
	DM1	**DM2**	
-	Eteinte		Mode affichage A
appuyer 1 x	Allumée	Eteinte	Mode affichage B
appuyer 2 x	Eteinte	Allumée	Mode d'affichage C
appuyer 3 x	Allumée		Mode d'affichage D

Les informations fournies par les LED "L1", "L2" et les LED de port varient selon le mode d'affichage sélectionné.

Si vous n'actionnez pas le bouton-poussoir pendant plus de 1 minute, l'appareil passe automatiquement en mode d'affichage A.

5.9 Contact de signalisation

5.9.1 Contact de signalisation

Le contact de signalisation est un relais d'alarme commandé par évènement ou manuellement. Certaines alarmes peuvent être configurées de sorte que le relais déclenche lorsque l'évènement correspondant se produit. Le relais peut en ouvre être fixé à l'état ouvert ou fermé.

La commande manuelle du relais est utile pour :

- vérifier que le relais de sécurité a été correctement connecté après l'installation de l'appareil
- vérifier que l'état ouvert/fermé est causé par l'appareil même ou par un autre matériel
- laisser le relais à l'état ouvert/fermé durant la recherche de défauts en cas de problème de réseau

5.9.2 Paramétrage du mode du contact de signalisation

Pour paramétrer le mode du contact de signalisation, procédez comme suit :

1. Naviguez vers **System** ≫ **Events** ≫ **Signaling Contact**.
2. Sous **Signaling Contact Mode**, sélectionnez un mode dans **Signaling Contact Mode** Options disponibles :

Option	Description
Event Driven	**Par défaut** Le contact de signalisation est commandé par des alarmes qui sont configurées de sorte qu'elles ouvrent et ferment le relais lorsqu'un évènement défini survient.
Open	Le contact de signalisation est toujours ouvert.
Closed	Le contact de signalisation est toujours fermé.

3. Validez la modification.

5.10 Fonction de bouton-poussoir

L'appareil possède un bouton-poussoir avec les fonctions suivantes :

- **Rétablir les paramètres par défaut de l'appareil**
  Veuillez noter que la fonction du bouton-poussoir n'est pas la même durant la phase de démarrage et en cours de fonctionnement.
  Pour plus d'informations, voir "Rétablir les paramètres par défaut de l'appareil avec le bouton-poussoir (en phase de démarrage) (Page 97)" et "Rétablir les paramètres par défaut de l'appareil avec le bouton-poussoir (en cours de fonctionnement) (Page 98)".
- **Charger un fichier de firmware via TFTP**
  Pour plus d'informations, voir "Charger un fichier de firmware via TFTP (Page 99)".
- **Réglage du mode d'affichage**
  Le mode d'affichage permet de diagnostic l'appareil. Selon le mode d'affichage sélectionné, les LED de l'appareil fournissent différentes informations et renseignent sur l'état de l'appareil.
  Pour plus d'informations, voir "Réglage du mode d'affichage (Page 95)".
  Pour plus d'informations sur les modes d'affichage, voir "LED "DM1" et "DM2" (Page 92)".

5.10.1 Ce qu'il faut savoir sur les fonctions du bouton-poussoir

Ce paragraphe décrit en détail les fonctions du bouton-poussoir.

5.10.1.1 Rétablir les paramètres par défaut de l'appareil avec le bouton-poussoir (en phase de démarrage)

IMPORTANT
Risque de connexion - Risque de défaillance des communications Selon la configuration de votre réseau, le rétablissement des paramètres par défaut de votre appareil risque de causer la rotation en boucle de trames et par conséquent la défaillance du trafic de données.

IMPORTANT
Risque de configuration - Risque de perte de données Si un CLP est embroché sur l'appareil, le CLP est également réinitialisé.

Remarque

Si vous rétablissez les paramètres par défaut de l'appareil, toutes les configurations sont effacées, y compris :

- l'adresse IP
- les utilisateurs créés
- les mots de passe
- les clés et certificats personnalisés

L'appareil n’est ensuite plus accessible que par l'interface série

Si vous affectez à l'appareil une adresse IP via DHCP ou DCP (SINEC PNI par ex.), vous pourrez, avec un profil utilisateur prédéfini, accéder via une connexion réseau au CLI et au Web UI de l'appareil.

Pour rétablir les paramètres par défaut de l'appareil pendant la phase de démarrage, procédez comme suit :

1. Mettez l'appareil hors tension.
2. Appuyez sur le bouton-poussoir puis remettez l'appareil sous tension en maintenant le bouton-poussoir enfoncé.
3. Maintenez le bouton enfoncé jusqu'à ce que la LED d'alarme rouge **A** s'arrête de clignoter et reste allumée en permanence.
4. Relâchez alors le bouton et attendez que la LED d'alarme **A** s'éteigne.
   L'appareil démarre automatiquement avec les paramètres par défaut.

5.10.1.2 Rétablir les paramètres par défaut de l'appareil avec le bouton-poussoir (en cours de fonctionnement)

IMPORTANT
Risque de connexion - Risque de défaillance des communications Selon la configuration de votre réseau, le rétablissement des paramètres par défaut de votre appareil risque de causer la rotation en boucle de trames et par conséquent la défaillance du trafic de données.

IMPORTANT
Risque de configuration - Risque de perte de données Si un CLP est embroché sur l'appareil, le CLP est également réinitialisé.

Remarque

Si vous rétablissez les paramètres par défaut de l'appareil, toutes les configurations sont effacées, y compris :

- l'adresse IP
- les utilisateurs créés
- les mots de passe
- les clés et certificats personnalisés

L'appareil n’est ensuite plus accessible que par l'interface série

Si vous affectez à l'appareil une adresse IP via DHCP ou DCP (SINEC PNI par ex.), vous pourrez, avec un profil utilisateur prédéfini, accéder via une connexion réseau au CLI et au Web UI de l'appareil.

Conditions

- L'appareil est en service.
- La fonction du bouton-poussoir **Rétablir les paramètres par défaut** est activée.
  Vous pouvez activer ou désactiver cette fonction du bouton-poussoir. Pour plus d'informations, voir "Activation de la fonction de bouton-poussoir 'Restauration des paramètres par défaut'. (Page 100)".

Rétablir les paramètres par défaut de l'appareil

Pour rétablir les paramètres par défaut de l'appareil en cours de fonctionnement, procédez comme suit :

1. Sélectionnez le mode d'affichage **A**.
   Le mode d'affichage **A** est activé lorsque les LED **DM1** et **DM2** sont éteintes.
   Si les LED **DM1** et **DM2** sont allumées ou si elles clignotent, appuyez plusieurs fois brièvement sur le bouton-poussoir, jusqu'à ce que les LED s'éteignent.
   Si vous n'actionnez pas le bouton-poussoir pendant plus de 1 minute, l'appareil passe automatiquement en mode d'affichage **A**.
2. Appuyez pendant 12 secondes sur le bouton-poussoir.

   Remarque

   Si vous relâchez le bouton avant l'écoulement des 12 secondes, l'opération est abandonnée.

3. Relâchez le bouton-poussoir au bout de 12 secondes.
   L'appareil redémarre avec les paramètres par défaut.

5.10.1.3 Charger un fichier de firmware via TFTP

Vous pouvez utiliser le bouton-poussoir pour passer en mode de mise à jour pendant le démarrage. Dans ce mode, l'appareil initialise la connexion réseau, démarre le client DHCP et le serveur TFTP et peut recevoir des fichiers, des fichiers de firmware par ex.

Si l'appareil n'est pas joignable via CLI et Web UI, vous pouvez redémarrer l'appareil et charger, en mode de mise à jour, un fichier de firmware sur l'appareil via TFTP.

Remarque

Ce chapitre décrit, à titre d'exemple, la marche à suivre sous Microsoft Windows.

Pour charger un fichier de firmware sur l'appareil via TFTP, procédez comme suit :

1. Mettez l'appareil hors tension.
2. Appuyez sur le bouton-poussoir puis remettez l'appareil sous tension en maintenant le bouton-poussoir enfoncé.
3. Maintenez le bouton-poussoir enfoncé jusqu'à ce que la LED d'alarme rouge **A** commence à clignoter.
4. Relâchez le bouton-poussoir pendant que la LED d'alarme rouge **A** clignote encore.

   Remarque

   Le clignotement ne dure que quelques secondes.

   Le chargeur d'amorçage de l'appareil attend dans cet état le fichier de firmware que vous pouvez charger via TFTP.
5. Connectez un PC client avec un câble Ethernet à un port de l'appareil.
6. Attribuez à l'appareil une adresse IP via DHCP ou avec SINEC PNI.
7. Ouvrez, sur le PC client une invite de commande Windows :

8. Dans l'invite de commande Windows, passez dans le répertoire dans lequel se trouve le fichier de firmware puis exécutez la commande suivante :
   `tftp -i < adresse IP > put < Fichier de firmware : >`

   Remarque

   Vous activez TFTP sous Microsoft Windows comme suit :

   Panneau de configuration ≫ Programmes et fonctionnalités ≫ Activer ou désactiver des fonctionnalités Windows ≫ Client TFTP

9. Lorsque le fichier de firmware a été complètement chargé sur l'appareil et validé, l'appareil redémarre.automatiquement. Cette procédure peut durer quelques minutes.

5.10.2 Activation de la fonction de bouton-poussoir 'Restauration des paramètres par défaut'.

Vous pouvez restaurer les paramètres par défaut de l'appareil avec le bouton-poussoir.

La fonction du bouton-poussoir **Restauration des paramètres par défaut** est activée par défaut.

IMPORTANT
Vulnérabilité - Danger d'intrusion et/ou d'utilisation abusive
Veuillez noter que la configuration ne se rapporte qu'à la fonction en cours de fonctionnement.
Si vous avez désactivé la fonction de bouton-poussoir **Restauration des paramètres par défaut**, la fonction du bouton-poussoir n'est désactivée qu'en cours de fonctionnement. La fonction du bouton-poussoir reste active en phase de démarrage. La fonction n'est désactiver qu'après le chargement de la configuration.
Des utilisateurs malveillants peuvent profiter de cette situation pour perturber le réseau et accéder à l'appareil.

Pour activer la fonction de bouton-poussoir **Restauration des paramètres par défaut**, procédez comme suit :

1. Naviguez vers **System ≫ Hardware ≫ SELECT / SET Button**.
2. Sous **SELECT / SET Button**, modifiez le paramètre **Restore Factory Defaults** en **Enabled**.
3. Validez la modification.

5.11 Configuration License PLUG

Le Configuration and License PLUG (CLP) est une clé USB permettant de sauvegarder et d'échanger des données et des licences.

Le CLP possède une interface USB de type C et peut être utilisé avec les appareils suivants qui possèdent la même interface.

- Produits Siemens
- Ordinateurs personnels (PC), ordinateurs de bureau, tablettes, portables ou smartphones

5.11.1 Ce qu'il faut savoir sur le CLP

Le CLP est utilisé pour la sauvegarde automatique des données de configuration. Il permet, en cas de besoin ou de panne, d'échanger facilement et rapidement un appareil sans être obligé de configurer l'appareil de rechange.

5.11.1.1 Échange d'appareils

Conditions requises pour le transfert de la configuration sur un appareil de rechange :

- Le CLP a été enregistré par un type d'appareil compatible (numéro d'article identique).
- La version du firmware de l'appareil de rechange est identique ou plus récente que celle de l'appareil qui a dernièrement enregistré le CLP.
  Pour s'en assurer, il est possible d'enregistrer le firmware avec la configuration sur le CLP. Pour plus d'informations, voir "Firmware sur CLP (Page 102)".

Si vous embrochez le CLP d'un constituant de réseau défaillant sur un appareil de rechange compatible, l'appareil de rechange démarre automatiquement avec la même configuration que l'appareil défaillant. Tenez compte des points suivants :

- Si la configuration IP est obtenue via DHCP, vous devez reconfigurer le serveur DHCP en conséquence.
- Si la configuration comprend des fonctions reposant sur des adresses MAC, adaptez-les en conséquence.

5.11.1.2 Modes d'exploitation

Les appareils possédant un emplacement de CLP prennent en charge les modes d'exploitation suivants :

- **sans CLP**
  L'appareil enregistre les données de configuration dans la mémoire interne. Ce mode est actif si le CLP n'est pas embroché.
- **avec CLP**
  Pendant la phase de démarrage :
  - Si un CLP **vierge** (paramétrage par défaut) est embroché sur un appareil, l'appareil sauvegarde automatiquement en phase de démarrage ses données de configuration sur le CLP. Il se comporte ainsi comme un CLP sur lequel des données sont enregistrées.
  - Si un CLP **enregistré** est embroché sur un appareil, l'appareil adopte automatiquement en phase de démarrage la configuration du CLP.

  Pendant le fonctionnement :
  - En cours de fonctionnement, les modifications de la configuration sont sauvegardées sur le CLP et en mémoire interne.
  - Les données de configuration sont enregistrées dans une zone de mémoire sécurisée du CLP. Cette zone de mémoire sécurisée est uniquement accessible via l'authentification de l'appareil Siemens.
  - L'appareil vérifie toutes les secondes la présence d'un CLP. Si l'appareil constate que le CLP a été retiré, il redémarre automatiquement.

IMPORTANT
Risque de fausse manœuvre - Risque de perte de données Ne débrochez et n'embrochez le CLP que si l'appareil est hors tension.

  - L'appareil signale des divergences par rapport au fonctionnement normal du CLP (des données incompatibles, erreurs de manipulation ou dysfonctionnements par ex.) à l'aide des mécanismes de diagnostic disponibles (LED ou interfaces utilisateur par ex.).

5.11.1.3 Firmware sur CLP

Outre la compatibilité du type d'appareil, la version de firmware est également importante pour le succès d'un échange d'appareils à l'aide du CLP.

Le transfert de la configuration sur un appareil de rechange ne fonctionne que si la version de firmware sur l'appareil de rechange est identique ou plus récente que celle du firmware sur l'appareil défaillant. Un appareil possédant un firmware plus ancien n'accepte pas le CLP et démarre avec la configuration qui se trouve dans sa mémoire interne.

Un appareil peut donc enregistrer non seulement sa configuration, mais aussi son firmware sur le CLP. Vous pouvez spécifier dans la configuration l'enregistrement ou non du firmware sur le CLP :

- Si la fonction est activée, l'appareil enregistre le firmware courant sur le CLP.
  Si le fichier de firmware est mis à jour sur ll'appareil, la version mise à jour est enregistrée sur le CLP.
- Si la fonction est désactivée, le firmware est supprimé du CLP.
- Si le paramétrage est modifié, l'appareil réagit directement et enregistre ou supprime le firmware du CLP.

En phase de démarrage, l'appareil ne vérifie pas si la fonction est activée ou désactivée. Si les données du CLP embroché sont compatibles et si le CLP contient un firmware valide, mais différent, le firmware du CLP est transféré sur l'appareil.

5.11.1.4 Zones de mémoire

Le CLP possède des zones de mémoire pour différents types de fichier :

- **Zone de mémoire ouverte**
  N'importe quel appareil peut accéder à la zone de mémoire publique.
  Un appareil connecté peut modifier le système de fichiers, mais aussi accéder en lecture et en écriture aux fichiers de la zone de mémoire.
- **Zone de mémoire sécurisée**
  Seuls des appareils Siemens peuvent accéder à la zone de mémoire sécurisée après avoir été authentifiés.
  Pour empêcher toute intrusion, les données de configuration sont enregistrées dans la zone de mémoire sécurisée.
- **Zone de mémoire pour licences**
  Zone de mémoire sécurisée distincte pour licences. Seuls des appareils Siemens peuvent accéder à cette zone après une authentification réussie.

5.11.1.5 Évènements associés

Les évènements suivants qui concernent le CLP, sont directement enregistrés sur le Syslog.

Évènement	Gravité	Message Syslog
EventNoCPlugFound	Info	No CLP found. Internal flash memory used.
EventEmptyCPlugFound	Info	Empty CLP found.
EventCPlugAutoFormat	Info	CLP auto format request.
EventCPlugAccepted	Info	CLP accepted.
EventErrorCPlugFound	Critical	CLP defective.
EventCPlugPluggedOff	Critical	CLP removed at runtime.
EventCPlugDiffType	Critical	CLP has different device type.
EventCPlugCrcError	Critical	CLP has CRC Error.
StateCPlugNotAccepted	Critical	CLP not accepted.
StateCPlugUnmounted	Info	CLP interface unmounted – restart required.

5.11.2 Enregistrement d'un firmware sur le CLP

Vous pouvez spécifier dans la configuration l'enregistrement ou non du firmware sur le CLP et sa synchronisation ou non. Si vous modifiez le paramètre, l'appareil réagit immédiatement.

- Si sous activez la fonction, l'appareil enregistre le firmware courant sur le CLP.
- Si sous désactivez la fonction, l'appareil supprime le firmware courant du CLP.

La fonction est activée par défaut.

Pour désactiver la fonction, procédez comme suit :

1. Naviguez vers **System** ≫ **CLP**.
2. Sous **Configuration & License Plug (CLP)**, modifiez le paramètre **Firmware on CLP** en **Enabled**.
3. Validez la modification.

5.11.3 Enregistrement de la configuration de l'appareil sur le CLP

Vous pouvez supprimer les données enregistrées sur le CLP et les remplacer par la configuration courante de l'appareil.

Pour formater le CLP et enregistrer la configuration courante, procédez comme suit :

1. Naviguez vers **System** ≫ **CLP**.
2. Sous **Configuration & License Plug (CLP)**, cliquez sur **Format & Write**.
3. Répondez à la demande de confirmation par **Yes**.
   L'appareil supprime toutes les données enregistrées sur le CLP et enregistre la configuration courante de l'appareil.
   Pour abandonner l'opération, répondez par **No** à la demande de confirmation.

5.11.4 Réinitialisation du CLP

Vous pouvez supprimer toutes les données enregistrées sur le CLP, y compris les licences et rétablir les données par défaut du CLP.

Remarque

Pour supprimer toutes les données sauf les licences enregistrées, restaurez les paramètres par défaut de l'appareil. Pour plus d'informations, voir "Restauration des paramètres par défaut de l'appareil (Page 72)".

Pour rétablir les paramètres par défaut du CLP, procédez comme suit :

1. Naviguez vers **System** ≫ **CLP**.
2. Sous **Configuration & License Plug (CLP)**, cliquez sur **Restore**.
3. Répondez à la demande de confirmation par **Yes**.
   L'appareil supprime toutes les données enregistrées sur le CLP et restaure les paramétrages par défaut.
   Pour abandonner l'opération, répondez par **No** à la demande de confirmation.

5.11.5 Affichage de l'état du CLP

Pour afficher l'état du CLP, naviguez vers **System** ≫ **CLP**.

Sous **Configuration & License Plug (CLP)** , l'écran affiche les informations suivantes :

Paramètres	Description
CLP Configuration State	Affiche l'état du CLP. Options disponibles : • **CLP not present** - Aucun CLP n'est embroché sur l'appareil. • **Accepted** - Un CLP avec une configuration valide et appropriée est embroché sur l'appareil. • **Not accepted** - Un CLP est embroché sur l'appareil. La CLP contient une configuration non valide ou incompatible. • **Factory** - Un CLP est embroché sur l'appareil. La CLP ne contient pas de configuration. Cet état est également affiché lorsque le CLP a été formaté en cours de fonctionnement.
Device Group	Indique sur quelle ligne de produits le CLP a été précédemment utilisé.
Device Type	Indique sur quel type d'appareil le CLP a été précédemment utilisé.
Filesystem	Affiche le type de système de fichiers existant sur le CLP.
Filesystem Size MB	Affiche la capacité de mémoire maximale du système de fichiers existant sur le CLP.
Filesystem Usage MB	Affiche le volume de mémoire utilisé du système de fichiers du CLP.
Info String	Affiche des informations complémentaires sur l'appareil sur lequel le CLP a été précédemment utilisé, p. ex. le numéro d'article, la désignation de type ainsi que les versions de matériel et de logiciel. La version de logiciel affichée est celle ayant servi lors de la dernière modification de la configuration. À l'état **Not accepted** des informations supplémentaires sur les causes du problème sont affichées.
Firmware on CLP	Si la fonction est activée (**Enabled**), le firmware est enregistré sur le CLP.
Firmware on CLP State	Indique si un firmware est enregistré sur le CLP (**Firmware present**) ou non (**Firmware not present**).

Administration système 6

Ce chapitre décrit comment exécuter diverses activités administratives telles que définir des utilisateurs, configurer des alarmes et gérer des fichiers système.

6.1 Stratégie de mot de passe

SINEC OS utilise une stratégie de mot de passe à l'échelle du système pour l'authentification des utilisateurs. La stratégie de mot de passe est constituée de conditions configurables qui doivent être remplies lors de la configuration de mots de passe.

Un mot de passe doit répondre par défaut aux conditions suivantes :

- Il doit compter de 8 à 255 caractères
- Il doit contenir au moins 1 chiffre

Seuls les utilisateurs possédant le profil utilisateur **Admin** sont habilités à modifier les mots de passe.

Si une condition est désactivée, ces caractères peuvent quand même être contenus dans un mot de passe. Ils ne sont cependant pas obligatoires.

6.1.1 Configuration de la stratégie de mot de passe

Pour modifier la stratégie de mot de passe, procédez comme suit :

1. [Facultatif] Configurez le nombre minimal de caractères qu'un mot de passe doit compter. Pour plus d'informations, voir "Configuration du nombre minimal de caractères (Page 108)".
2. [Facultatif] Configurez le nombre maximal de caractères qu'un mot de passe peut compter. Pour plus d'informations, voir "Configuration du nombre maximal de caractères. (Page 108)".
3. [Facultatif] Configurez qu'un mot de passe doit comporter au moins 1 chiffre. Pour plus d'informations, voir "Configuration de la condition de présence de chiffres (Page 108)".
4. [Facultatif] Configurez qu'un mot de passe doit comporter au moins 1 minuscule. Pour plus d'informations, voir "Configuration de la condition de présence de minuscules (Page 109)".
5. [Facultatif] Configurer qu'un mot de passe doit comporter au moins 1 majuscule. Pour plus d'informations, voir "Configuration de la condition de présence de majuscules (Page 109)".

6. [Facultatif] Configurez qu'un mot de passe doit comporter au moins 1 caractère spécial. Pour plus d'informations, voir "Configuration de la condition de présence de caractères spéciaux (Page 110)".
7. Activez la stratégie de mot de passe.
   Pour plus d'informations, voir "Activation de la stratégie de mot de passe (Page 110)".

6.1.1.1 Configuration du nombre minimal de caractères

Pour configurer le nombre minimal de caractères, procédez comme suit :

1. Naviguez vers **System** ≫ **Security** ≫ **User Management**.
2. Sous **Password Policy**, configurez dans le champ **Minimum Length** le nombre minimal de caractères qu'un mot de passe doit compter.
   Condition :
   – Un nombre compris entre 1 et 255

   Par défaut : 8
3. Validez la modification.

6.1.1.2 Configuration du nombre maximal de caractères.

Pour configurer le nombre maximal de caractères, procédez comme suit :

1. Naviguez vers **System** ≫ **Security** ≫ **User Management**.
2. Sous **Password Policy**, configurez dans le champ **Maximum Length** le nombre maximal de caractères qu'un mot de passe peut compter.
   Condition :
   – Un nombre compris entre 4 et 255

   La plage de valeurs débute par 4 pour éviter des stratégies de mot de passe non valides, si toutes les conditions sont activées :
   – au moins 1 chiffre
   – au moins 1 minuscule
   – au moins 1 majuscule
   – au moins 1 caractère spécial

   Par défaut : 255
3. Validez la modification.

6.1.1.3 Configuration de la condition de présence de chiffres

Un mot de passe doit comporter par défaut au moins 1 chiffre.

Pour configurer qu'un mot de passe doit comporter des chiffres, procédez comme suit :

1. Naviguez vers **System** ≫ **Security** ≫ **User Management**.
2. Sous **Password Policy**, configurez dans le champ **Number** qu'un mot de passe doit comporter des chiffres.
   Options disponibles :

Option	Description
Required	**Par défaut** Un mot de passe doit contenir au moins 1 chiffre.
Not Required	La présence de chiffres dans un mot de passe n'est pas obligatoire.

3. Validez la modification.

6.1.1.4 Configuration de la condition de présence de minuscules

Par défaut, la présence de minuscules dans le mot de passe n'est pas requise.

Pour configurer qu'un mot de passe doit comporter des minuscules, procédez comme suit :

1. Naviguez vers **System** ≫ **Security** ≫ **User Management**.
2. Sous **Password Policy**, configurez dans le champ **Lowercase** qu'un mot de passe doit comporter des minuscules.
   Options disponibles :

Option	Description
Not Required	**Par défaut** La présence de minuscules dans un mot de passe n'est pas obligatoire.
Required	Un mot de passe doit contenir au moins 1 minuscule.

3. Validez la modification.

6.1.1.5 Configuration de la condition de présence de majuscules

Par défaut, la présence de majuscules dans le mot de passe n'est pas requise.

Pour configurer qu'un mot de passe doit comporter des majuscules, procédez comme suit :

1. Naviguez vers **System** ≫ **Security** ≫ **User Management**.
2. Sous **Password Policy**, configurez dans le champ **Uppercase** qu'un mot de passe doit contenir des majuscules.
   Options disponibles :

Option	Description
Not Required	**Par défaut** La présence de majuscules dans un mot de passe n'est pas obligatoire.
Required	Un mot de passe doit contenir au moins 1 majuscule.

3. Validez la modification.

6.1.1.6 Configuration de la condition de présence de caractères spéciaux

Par défaut, la présence de caractères spéciaux dans le mot de passe n'est pas requise.

Les caractères spéciaux suivants sont admis : # $ % & ( ) * + , - . / : < = > @ [ ] ^ _ { } ~

Pour configurer qu'un mot de passe doit comporter des caractères spéciaux, procédez comme suit :

1. Naviguez vers **System** ≫ **Security** ≫ **User Management**.
2. Sous **Password Policy**, configurez dans le champ **Special Character** qu'un mot de passe doit contenir des majuscules.
   Options disponibles :

Option	Description
Not Required	**Par défaut** La présence de caractères spéciaux dans un mot de passe n'est pas obligatoire.
Required	Un mot de passe doit contenir au moins 1 caractère spécial.

3. Validez la modification.

6.1.1.7 Activation de la stratégie de mot de passe

La stratégie de mot de passe est activée par défaut.

Si la stratégie de mot de passe est désactivée, la seule condition requise est que le mot de passe possède au moins 1 caractère.

Pour activer la stratégie de mot de passe, procédez comme suit :

1. Naviguez vers **System** ≫ **Security** ≫ **User Management**.
2. Sous **Password Policy**, modifiez le paramètre **Status** en **Enabled**.
3. Validez la modification.

6.1.2 Affichage de la stratégie de mot passe.

Pour afficher la stratégie de mot de passe active, naviguez vers **System** ≫ **Security** ≫ **User Management**.

Sous **Password Policy**, l'écran affiche les informations suivantes :

Paramètres	Description
Status	Indique si la stratégie de mot de passe est activée ou non. Si la stratégie de mot de passe est désactivée (**Disabled**), la seule condition requise est que le mot de passe possède au moins 1 caractère. Il n'est pas nécessaire que d'autres conditions configurées soient remplies.
Maximum Length	Spécifie le nombre maximal de caractères que peut compter le mot de passe.

Paramètres	Description
Minimum Length	Spécifie le nombre minimal de caractères que doit compter le mot de passe.
Number	Indique si des chiffres doivent être utilisés.
Special Character	Indique si des caractères spéciaux doivent être utilisés.
Lowercase	Indique si des minuscules doivent être utilisées.
Uppercase	Indique si des majuscules doivent être utilisées.

6.2 Gestion des utilisateur

Vous pouvez configurer plusieurs utilisateurs et attribuer à chaque utilisateur un profil d'utilisateur.

Sous SINEC OS vous pouvez configurer les profils d'utilisateur ci-après localement sur l'appareil :

- **Admin**
- **Guest**

À chaque profil sont affectés des droits d'accès différents. Les droits d'accès autorisent l'utilisateur ou lui interdisent de modifier des paramètres ou d'exécuter certaines commandes.

Pour plus d'informations, voir "Droits d’accès (Page 29)".

6.2.1 Majuscules/minuscules dans les noms d'utilisateur

Sous SINEC OS aucune distinction n'est faite entre les majuscules/minuscules dans les noms d'utilisateur (non-respect de la casse).

user1 et **User1** sont deux graphies du même nom utilisateur. Tenez par conséquent compte des points suivants :

- Si un utilisateur a été créé sous le nom **user1**, il n'est plus possible de créer un utilisateur nommé **User1**.
- Si un utilisateur a été créé sous le nom **user1**, il peut se connecter avec les différentes graphies de son nom utilisateur, par exemple **user1**, **User1**, **USER1**. Toutes ces graphies valent pour le profil d'utilisateur et le mot de passe de l'utilisateur créé sous le nom **user1**.

SINEC OS respecte la casse lors de l'enregistrement des noms d'utilisateur. Le nom d'utilisateur est enregistré exactement tel qu'il a été écrit lors de sa création. C'est aussi la graphie utilisée pour les affichages, p. ex. dans la CLI avec la commande `show running-config system authentication user` ou dans la Web UI sous **System** ≫ **Security** ≫ **User Management**.

6.2.2 Configuration d'utilisateurs

Procédez comme suit pour créer un nouvel utilisateur :

1. Créez un nouvel utilisateur et attribuez-lui un mot de passe et un profil d'utilisateur.
   Pour plus d'informations, voir "Configuration d'un nouvel utilisateur (Page 112)".
2. [Facultatif] Modifiez le mot de passe d'un utilisateur.
   Pour plus d'informations, voir "Modification du mot de passe d'un utilisateur (Page 113)".

6.2.2.1 Configuration d'un nouvel utilisateur

Seuls les utilisateurs possédant le profil utilisateur **Admin** sont habilités à configurer un nouvel utilisateur.

Procédez comme suit pour créer un nouvel utilisateur :

1. Naviguez vers **System** ≫ **Security** ≫ **User Management**.
2. Sous **User Management**, cliquez sur **Add**.
   Une nouvelle ligne est insérée dans le tableau.
3. Sous **Username**, saisissez un nom d'utilisateur.
   Vous ne pouvez éditer le nom d'utilisateur qu'immédiatement après l'avoir saisi dans la nouvelle ligne. Dès que le champ n'est plus actif, le nom d'utilisateur passe en lecture seule. Si vous voulez modifier le nom d'utilisateur et le niveau de sécurité, supprimez l'uilisateur et configurez le à nouveau.
   Conditions :
   - Il doit être unique
   - Il doit compter de 1 à 250 caractères
   - Tous les caractères standard ainsi que les caractères spéciaux suivants _ - sont autorisés :
4. Sous **Role**, affectez à l'utilisateur un profil d'utilisateur.
   Une fois que vous avez créé un utilisateur, vous ne pouvez plus en modifier le profil. Si vous voulez modifier le profil d'utilisateur, supprimez l'uilisateur et configurez le à nouveau.
   Options disponibles :

Option	Description
Admin	Les utilisateurs possédant le profil d'utilisateur **Admin** disposent des droits d'accès en écriture et en lecture aux fonctions de l'appareil.
Guest	Les utilisateurs possédant le profil utilisateur **Guest** disposent des droits d'accès en lecture aux fonctions de l'appareil.

5. Attribuez sous **Password** un mot de passe à l'utilisateur.
   Vous pouvez saisir un mot de passe comme suit :

   – Comme mot de passe de hachage
     Si un mot de passe débute par l'une des combinaisons de caractères suivantes, il est considéré comme mot de passe de hachage et est enregistré sous cette forme :

Combinaison de caractères	Algorithme de hachage
1	MD5
5	SHA-256
6	SHA-512

   – Comme mot de passe en clair
     Si un mot de passe débute par une combinaison de caractères autres que 1, 5 ou 6, il est considéré comme un mot de passe en clair et converti par l'appareil à l'aide de l'algorithme de hachage SHA-512.
     Si un mot de passe débute par la combinaison de caractères `$0$`, il est également considéré comme un mot de passe en clair. Utilisez cette combinaison de caractères, si vous voulez configurer un mot de passe qui débute par le caractère `$`.
     Exemple : `$0$$iemens123`

   Conditions :

   – Il doit compter de 8 à 255 caractères

   – Il doit contenir au moins 1 chiffre

   – Tous les caractères standard ainsi que les caractères spéciaux suivants sont autorisés :
     # $ % & ( ) * + , - . / : < = > @ [ ] ^ _ { } ~

   Tenez compte de conditions divergentes découlant de la stratégie de mot de passe configurable. Pour plus d'informations, voir "Affichage de la stratégie de mot passe. (Page 110)".

6. Sous **Password Confirm**, saisissez à nouveau le mot de passe.

7. Validez les modifications.

6.2.2.2 Modification du mot de passe d'un utilisateur

Seuls les utilisateurs possédant le profil utilisateur **Admin** sont habilités à modifier les mots de passe de tous les utilisateurs.

Les utilisateurs possédant le profil d'utilisateur **Guest** peuvent uniquement modifier leur propre mot de passe.

Pour modifier le mot de passe, procédez comme suit :

1. Naviguez vers **System** ≫ **Security** ≫ **User Management**.
2. Sous **User Management**, modifiez le mot de passe de l'utilisateur dans la colonne **Password**. Vous pouvez saisir un mot de passe comme suit :
   - Comme mot de passe de hachage
     Si un mot de passe débute par l'une des combinaisons de caractères suivantes, il est considéré comme mot de passe de hachage et est enregistré sous cette forme :

Combinaison de caractères	Algorithme de hachage
1	MD5
5	SHA-256
6	SHA-512

   - Comme mot de passe en clair
     Si un mot de passe débute par une combinaison de caractères autres que 1, 5 ou 6, il est considéré comme un mot de passe en clair et converti par l'appareil à l'aide de l'algorithme de hachage SHA-512.
     Si un mot de passe débute par la combinaison de caractères `$0$`, il est également considéré comme un mot de passe en clair. Utilisez cette combinaison de caractères, si vous voulez configurer un mot de passe qui débute par le caractère `$`.
     Exemple : `$0$$iemens123`

   Conditions :
   - Il doit compter de 8 à 255 caractères
   - Il doit contenir au moins 1 chiffre
   - Tous les caractères standard ainsi que les caractères spéciaux suivants sont autorisés : # $ % & ( ) * + , - . / : < = > @ [ ] ^ _ { } ~

   Tenez compte de conditions divergentes découlant de la stratégie de mot de passe configurable. Pour plus d'informations, voir "Affichage de la stratégie de mot passe. (Page 110)".
3. Sous **Password Confirm**, saisissez à nouveau le mot de passe.
4. Validez les modifications.

6.2.3 Surveillance de l'utilisateur

Les utilisateurs connectés à l'appareil sont surveillés par SINEC OS et peuvent être affichés. Si vous êtes connecté avec le profil d'utilisateur, `admin` vous pouvez surveiller des utilisateurs, les déconnecter et leur envoyer des messages.

6.2.3.1 Affichage d'utilisateurs actifs

Si vous êtes connecté avec le profil d'utilisateur, **Admin** vous pouvez afficher les utilisateurs qui sont connectés à l'appareil.

Pour afficher les utilisateurs actuellement connectés à l'appareil, naviquez vers **System** ≫ **Security** ≫ **User Management**.

Sous **User Sessions**, l'écran affiche les informations suivantes :

Paramètres	Description
Session	Numéro de la session La propre session est repérée par un *.
User	Nom d'utilisateur
From	Adresse IP avec laquelle l'utilisateur est connecté
Context / Context - Protocol	Interface utilisateur et protocole via lesquels l'utilisateur est connecté
Date	Date et heure auxquelles l'utilisateur s'est connecté
Mode	Mode dans lequel l'utilisateur se trouve momentanément. Valeurs possibles : • **operational** - L'utilisateur se trouve en mode de fonctionnement. • **config-terminal** - L'utilisateur se trouve en mode configuration partagée. • **config-exculsive** - L'utilisateur se trouve en mode configuration exclusive.

6.2.3.2 Affichage de données utilisateur

Pour afficher la configuration de tous les utilisateurs, naviguez vers **System** ≫ **Security** ≫ **User Management**.

Sous **User Management**, l'écran affiche les informations suivantes :

Paramètres	Description
Username	Affiche le nom d'utilisateur.
Role	Affiche le profil d'utilisateur de l'utilisateur.
Password	Le mot de passe est masqué.
Password Confirm	

6.3 Préparation de l'appareil pour un dépannage

Pour effectuer un dépannage, le technicien du SAV Siemens doit avoir provisoirement accès à l'appareil (compte utilisateur Debug) et/ou aux informations de débogage.

Ce chapitre décrit comment préparer l'appareil pour un dépannage de sorte que le technicien du SAV Siemens puisse vous assister au mieux lors du dépannage.

6.3.1 Enregistrement des informations de débogage

Les informations de débogage sont enregistrées dans un fichier ZIP. L'appareil n'enregistre toujours qu'un seul fichier. Lorsque survient un grave défaut, l'appareil crée automatiquement un fichier contenant les informations de débogage correspondantes.

Le fichier ZIP est protégé par un mot de passe. Le mot de passe de l'appareil est spécifique et uniquement connu de votre technicien du SAV Siemens. Enregistrez les informations de débogage et transmettez-les à votre technicien du SAV Siemens.

Vous pouvez enregistrer les informations de débogage sur PC client local ou sur un serveur distant.

6.3.1.1 Enregistrement d'informations de débogage sur un PC client local

Pour enregistrer un fichier ZIP contenant les informations de débogage sur un PC local, procédez comme suit :

1. Naviguez vers **System** ≫ **Load & Save** ≫ **Service Files**.
2. Sous **Save Service File to Local PC** sélectionnez pour le paramètre **File Type** l'option **Debug Information**.
3. Cliquez sur **Save**.
4. Si les informations de débogage ont déjà été enregistrées une fois, une nouvelle demande de confirmation s'affiche.
   Options disponibles :
   - **Yes** - Un nouveau fichier ZIP n'est pas créé. Le fichier ZIP existant est transféré.
   - **No** - Un nouveau fichier ZIP, contenant les informations de débogage momentanées est créé et transféré. Le fichier ZIP existant est écrasé.

   Le fichier sera enregistré directement dans un dossier prédéfini ou bien, selon le paramétrage de votre navigateur web, vous devrez d'abord choisir l'emplacement.
   Un symbole de chargement s'affiche comme retour d'information visuel, à droite du bouton.
   - Si l'enregistrement s'est terminé avec succès, une coche verte s'affiche.
   - Un point d'exclamation rouge et un message d'erreur s'affichent si l'enregistrement a échoué. Renouvelez les dernières opérations.

6.3.1.2 Enregistrement d'informations de débogage sur un serveur distant

Vous pouvez enregistrer les informations de débogage sur un serveur distant.

Conditions

- Vous avez configuré un serveur de manière adéquate.
- Il existe une connexion entre l'appareil et le serveur.
- Selon votre configuration, le nom d'utilisateur et le mot de passe doivent être connus.

Enregistrement des informations de débogage

Pour enregistrer un fichier ZIP contenant les informations de débogage sur un serveur distant, procédez comme suit :

1. Naviguez vers **System** ≫ **Load & Save** ≫ **Service Files**.
2. Sous **Save Service File to Remote Server** sélectionnez pour le paramètre **File Type** l'option **Debug Information**.
3. Configurez les paramètres du serveur distant.
   Pour plus d'informations sur le chargement et l'enregistrement de fichiers via un serveur distant, voir "Chargement et enregistrement de fichiers via un serveur distant. (Page 47)".
4. Cliquez sur **Save**.
5. Si les informations de débogage ont déjà été enregistrées une fois, une nouvelle demande de confirmation s'affiche.
   Options disponibles :
   - **Yes** - Un nouveau fichier ZIP n'est pas créé. Le fichier ZIP existant est transféré.
   - **No** - Un nouveau fichier ZIP, contenant les informations de débogage momentanées est créé et transféré. Le fichier ZIP existant est écrasé.

   Un symbole de chargement s'affiche comme retour d'information visuel, à droite du bouton.
   - Si l'enregistrement s'est terminé avec succès, une coche verte s'affiche.
   - Un point d'exclamation rouge et un message d'erreur s'affichent si l'enregistrement a échoué. Renouvelez les dernières opérations.

6.3.2 Activation du compte utilisateur Debug.

Le compte utilisateur Debug permet à votre technicien du SAV Siemens d'accéder pendant une durée définie à votre appareil. Seuls les utilisateurs possédant le profil utilisateur **Admin** sont habilités à activer le compte utilisateur. Le compte utilisateur Debug est actif jusqu'à ce que le compte soit désactivé ou que l'appareil soit arrêté ou redémarré.

Le compte utilisateur Debug est désactivé par défaut.

Vous ne pouvez activer le compte utilisateur Debug que via CLI.

Pour plus d'informations, voir le **Manuel de configuration SINEC OS CLI**.

Sécurité des données 7

7.1 Sécurité des données

Ce chapitre décrit les fonctions de sécurité des données disponibles. Veuillez vous assurer que l'appareil et le réseau sont suffisamment protégés contre les attaques malveillantes par un contrôle/une mise à jour des paramètres de sécurité des données par défaut.

Remarque

Recommandations générales de sécurisation de l'appareil, voir "Recommandations de sécurité (Page 22)".

7.2 Prévention des attaques par force brute

SINEC OS possède un mécanisme de protection contre les attaques locales et distantes par force brute (BFA) via les interfaces utilisateur CLI, Web UI, SNMP et NETCONF. Le mécanisme surveille le nombre d'échecs de connexion pour chaque nom d'utilisateur unique et chaque adresse IP. Après un nombre d'échecs de tentatives de connexion défini, le nom d'utilisateur ou l'adresse IP est bloqué pendant un certain temps.

7.2.1 Ce qu'il faut savoir sur la prévention des BFA

Lors d'une attaque par force brute, un utilisateur malveillant tente d'accéder à un appareil essayant un grand nombre de noms d'utilisateur, de mots de passe et de noms de communauté SNMP aléatoires jusqu'à ce qu'il obtienne l'accès.

SINEC OS essaye d'empêcher le succès des attaques par force brute en bloquant les noms d'utilisateur uniques et les adresses IP dont les tentatives de connexion échouent de manière répétée.

7.2.1.1 Fonctionnement du mécanisme de prévention

Si la connexion d'un utilisateur ou d'un service échoue, le nom d'utilisateur ou l'adresse IP est inscrit dans une liste. Le mécanisme de prévention commence alors à analyser ce qui suit :

- Le temps écoulé depuis le dernier échec de connexion.
  Ce temps est configurable. Si l'utilisateur/le service tente à nouveau de se connecter pendant cette période et que la tentative échoue à nouveau, le nombre d'échecs de connexion est incrémenté.
- Le nombre d'échecs de connexion
  Ce paramètre est configurable. L'utilisateur/le service est bloqué, lorsque le nombre d'échecs de connexion atteint une valeur limite définie.

Si l'utilisateur ou le service se connecte avec succès avant que le nombre maximal d'échecs de connexion soit atteint, tous les compteurs sont remis à zéro.

Les utilisateurs et services qui ont dépassé le nombre maximal d'échecs de connexion sont bloqués pendant une durée configurable. Si un utilisateur/service bloqué tente à nouveau de se connecter avant que la durée soit écoulée, le blocage est prolongé et la durée remise à zéro.

Le blocage d'un utilisateur est levé, si :

- la durée est écoulée
- le blocage est annulé manuellement par un administrateur via SINEC OS
- l'appareil est redémarré

7.2.1.2 Évènements associés

Les évènements suivants sont déclenchés par le mécanisme de prévention de BFA et enregistrés dans le journal système (Syslog).

Évènement	Gravité	Message Syslog
User blocked	Warning	User "{ Nom d'utilisateur }" account is locked for { Durée } minutes after { Nombre } unsuccessful login attempts.
IP blocked	Warning	IP { Adresse IP } is locked for { Durée } minutes after { Nombre } unsuccessful login attempts

7.2.2 Configuration de la prévention BFA

Pour configurer la prévention BFA, procédez comme suit :

1. [Facultatif] Modifiez le temps de mise à zéro pour commander le temps de blocage des utilisateurs et adresses IP.
   Pour plus d'informations, voir "Modification du délai de remise à zéro automatique (Page 120)".
2. [Facultatif] Modifiez le nombre maximal d'échecs de connexion au bout duquel l'utilisateur et les adresses IP sont bloqués.
   Pour plus d'informations, voir "Modification du nombre maximal d'échecs de connexion (Page 121)".
3. [Facultatif] Modifiez la durée entre échecs de connexion au bout de laquelle les compteurs sont remis à zéro.
   Pour plus d'informations, voir "Modification du délai entre échecs de connexion. (Page 121)".
4. Activez la prévention de BFA.
   Pour plus d'informations, voir "Activation de la prévention de BFA. (Page 122)".

7.2.2.1 Modification du délai de remise à zéro automatique

Le délai de remise à zéro automatique annule le blocage d'utilisateurs et d'adresses IP préalablement bloqués au bout d'une durée définie

Pour définir la durée maximale qui doit s'écouler entre l'instant où un utilisateur ou une adresse IP est bloqué et l'instant où le blocage de l'utilisateur ou de l'adresse IP est levé, procédez comme suit :

1. Naviguez vers **System** ≫ **Security** ≫ **Brute Force Prevention**.
2. Sous **Brute Force Prevention**, configurez **Auto-Reset Timer**.
   Conditions :
   - En format nYnMnDnhnmns, dans lequel n est un nombre personnalisé
   - Minimum 0 seconde
   - Maximum 255 Minutes (15300 secondes)

   Par défaut : 10m
3. Validez la modification.

7.2.2.2 Modification du nombre maximal d'échecs de connexion

Lorsqu'un utilisateur ou une adresse IP tente de se connecter après une précédente tentative infructueuse et que le temps n'est pas encore écoulé, un compteur est incrémenté.

Vous pouvez définir une valeur limite différente pour les utilisateurs et les adresses IP. Si le compteur d'un utilisateur ou d'une adresse IP atteint la valeur limite définie, l'utilisateur ou l'adresse IP est automatiquement bloqué.

Pour modifier le nombre maximal d'échecs de connexion, procédez comme suit :

1. Naviguez vers **System** ≫ **Security** ≫ **Brute Force Prevention**.
2. Sous **Brute Force Prevention**, configurez **User Specific Login Attempts** ou **IP Specific Login Attempts**.
   Condition :
   - Un nombre compris entre 0 et 255

   Par défaut : 10
3. Validez la modification.

7.2.2.3 Modification du délai entre échecs de connexion.

SINEC OS définit une valeur limite du temps maximal qui peut s'écouler entre les échecs de connexion. Le temps est mesuré à compter de l'échec de connexion d'un utilisateur ou d'un service. Si l'utilisateur/le service tente à nouveau de se connecter pendant cette période et que la tentative échoue à nouveau, le nombre d'échecs de connexion de l'utilisateur ou de l'adresse IP est incrémenté.

Pour modifier le délai entre échecs de connexion, procédez comme suit :

1. Naviguez vers **System** ≫ **Security** ≫ **Brute Force Prevention**.
2. Sous **Brute Force Prevention**, configurez **Trigger Interval**.
   Conditions :
   - En format nYnMnDnhnmns, dans lequel n est un nombre personnalisé
   - Minimum 5 Minutes (300 secondes)
   - Maximum 255 Minutes (15300 secondes)

   Par défaut : 5m
3. Validez la modification.

7.2.2.4 Activation de la prévention de BFA.

Pour activer le mécanisme de prévention de BFA, procédez comme suit :

Remarque

La prévention BFA est activée par défaut.

1. Naviguez vers **System** ≫ **Security** ≫ **Brute Force Prevention**.
2. Sous **Brute Force Prevention**, modifiez le paramètre **Brute Force Prevention** en **Enabled**.
3. Validez la modification.

7.2.3 Annulation du blocage d'utilisateurs ou d'adresses IP

Le blocage de noms d'utilisateur et d'adresses IP peut être annulé manuellement.

Pour annuler le blocage d'un nom d'utilisateur ou d'une adresse IP actuellement bloqué, procédez comme suit :

1. Naviguez vers **System** ≫ **Security** ≫ **Brute Force Prevention**.
2. Recherchez sous **Brute Force Prevention - State Information** le nom d'utilisateur ou l'adresse IP bloqué puis cliquez sur **Reset**.

7.2.4 Surveillance de la prévention de BFA

Pour vérifier quels noms d'utilisateur et/ou adresses IP sont momentanément surveillés par le mécanisme de prévention de BFA, naviguez vers .**System** ≫ **Security** ≫ **Brute Force Prevention**.

Des tableaux distincts pour les utilisateurs et les adresses IP fournissent sous **Brute Force Prevention - State Information** les détails suivants :

Paramètres	Description
Username	L'utilisateur ou le Community Name actuellement surveillé. Veuillez noter que des utilisateurs inconnus, à savoir les utilisateurs authentifiés via RADIUS, sont mentionnés comme "Unknown User".
IP Address	Adresse IP qui est momentanément surveillée.
Failed Logins	Nombre momentané d'échecs de connexion
Time Since Last Failed	Le temps (formaté comme nYnMnDnhnmns) écoulé depuis le dernier échec de connexion.
Blocked	Le délai (formaté comme nYnMnDnhnmns), jusqu'au déblocage.

Exemple

Username	Failed Logins	Time Since Last Failed	Blocked
Unknown User	10	4m18s	22s
admin	0	0s	0s

IP Address	Failed Logins	Time Since Last Failed	Blocked
172.30.142.156	1	18s	0s
172.30.142.244	3	2m6s	0s

7.3 Évènements concernant la sécurité des données

Pour répondre aux exigences de la norme de sécurité des données en environnement industriel CEI 62443, il est entre autres nécessaire d'assurer un suivi intégral de toutes les activités des utilisateurs. Un préalable important à cet égard est la génération et la mise à disposition d'évènements adéquats relatifs à la sécurité des données.

7.3.1 Ce qu'il faut savoir sur les évènements relatifs à la sécurité des données

Les évènements relatifs à la sécurité des données de divers constituants (commutateurs IE, PC industriels, serveurs, constituants de réseau et contrôleurs p. ex.) génèrent et contiennent entre autres des informations sur les activités exercées par divers utilisateurs (p. ex. les tentatives de connexion et modifications de la configuration).

Les appareils SINEC OS génèrent des messages d'évènement et les enregistrent localement sous forme de journal système. Les messages d'évènements peuvent par ailleurs être retransmis à une ou plusieurs instances de journalisation centrales. Une instance de journalisation peut être p. ex. un serveur Syslog (p. ex. SINEC INS) ou un Security Information and Event Management (SIEM).

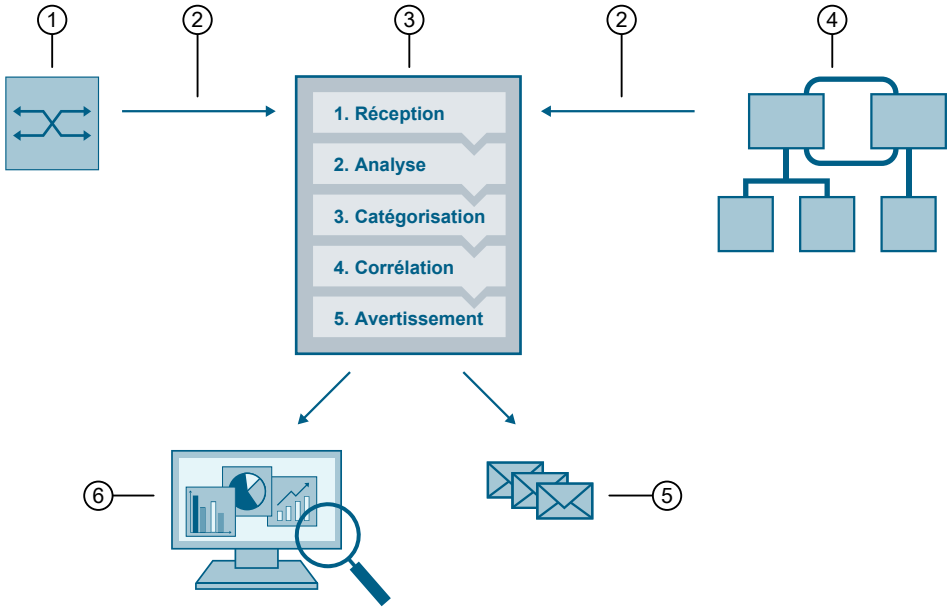
Pour plus d'informations sur le journal système, voir "Journal système (Page 293)".

7.3.1.1 Système SIEM

Un système SIEM permet de collecter des messages d'évènement relatifs à la sécurité des données, de les analyser et de signaler les évènements critiques. Ceci peut être appliqué à des appareils individuels ou à tout un réseau.

Utilisez un système SIEM, pour centraliser les messages d'évènement et détecter une perturbation sur la base d'évènements corrélés.

La figure ci-après représente un système SIEM et les constituants impliqués.



① Commutateur IE/Client Syslog
② Messages d'évènement
③ Système SIEM
④ Réseau
⑤ Notifications
⑥ Interface utilisateur graphique

Figure 7-1 Système SIEM

Le système SIEM traite les messages d'évènement comme suit :

1. **Réception**
   Un serveur Syslog reçoit les messages d'évènement de divers appareils, constituants de réseau, etc.

2. **Analyse**
   Le système SIEM analyse les messages d'évènement et combine chaque message d'évènement avec un évènement spécifique SIEM généralisé.
   Pour qu'un système SIEM puisse traiter les messages d'évènement, leur syntaxe doit être connue et compatible. Pour répondre à ces exigences, les appareils SINEC OS se conforment à la norme CEI 62443.
   Pour plus d'informations sur la syntaxe des messages d'évènement, voir "Variables dans les messages d'évènement (Page 126)".

3. **Catégorisation**
   Les messages d'évènement généralisés sont regroupés en catégories et enregistrés dans la base de données SIEM.
   Ces catégories sont p. ex. les échecs de connexion, modifications de la configuration et autres activités potentiellement malveillantes.
4. **Corrélation**
   Le système SIEM établit des corrélations entre les messages d'évènement. Ceci permet au système SIEM de détecter des anomalies (p. ex. des motifs et tendances inhabituels) qui révèlent la présence d'activités relatives à la sécurité des données.
5. **Avertissement**
   Lorsque des évènements potentiellement liés à la sécurité des données sont identifiés, le système SIEM génère des alertes de sécurité. Celles-ci sont affichées via une interface utilisateur graphique ou émises sous forme de notifications.

7.3.1.2 Structure d'un message d'évènement

Les messages d'évènement relatifs à la sécurité des données sont transmis avec les informations suivantes à une instance de journalisation :

Élément	Description
HEADER	
PRI	Priorité du message d'évènement La priorité est constituée des éléments suivants : • Severity Gravité du message Pour plus d'informations sur la gravité, voir "Niveaux de gravité (Page 298)". • Facility Origine du message L'origine des évènements relatifs à la Sécurité des données est toujours local0.
VERSION	Numéro de version de la spécification Syslog
TIMESTAMP	Horodatage du message d'évènement selon RFC 3339 Exemple : 2010-01-01T02:03:15+02:00
HOSTNAME	Émetteur du message d'évènement avec FQDN, nom d'hôte ou adresse IP Adresse IPv4 selon RFC 1035 : Octets en notation décimale : XXX.XXX.XXX.XXX Les indications manquantes sont remplacées par "-".
STRUCTURED-DATA	

Élément	Description
timeQuality	Informations relatives à la date/heure système Exemple : [timeQuality tzKnown="0" isSynced="0"] Le paramètre **tzKnown** indique si l'émetteur connaît ou non son fuseau horaire. Options disponibles : • Valeur "1" = le fuseau horaire est connu. • Valeur "0" = le fuseau horaire est inconnu. Le paramètre **isSynced** indique si l'émetteur est synchronisé ou non à une horloge fiable, via NTP par ex. Options disponibles : • Valeur "1" = la date/heure système est synchronisée. • Valeur "0" = la date/heure système n'est pas synchronisée.
MSG	
MESSAGE	Message d'évènement sous forme de chaîne de caractères ASCII en anglais

Remarque

Pour plus d'informations sur la structure des messages d'évènement et sur la signification des paramètres, voir RFC 5424 (https://tools.ietf.org/html/rfc5424).

7.3.1.3 Variables dans les messages d'évènement

À chaque message d'évènement, l'élément **{ MESSAGE }** contient des variables qui sont complétées dynamiquement par les données de l'évènement en question. Ces variables sont représentées au chapitre "Surveillance d'évènements relatifs à la sécurité des données (Page 128)", avant les tableaux entre accolades (p. ex. {Journal})

Remarque

La liste des variables n'est pas exhaustive. Seules sont mentionnées les variables qui sont pertinentes pour l'intégration d'un système SIEM.

Les variables suivantes apparaissent dans l'élément **{ MESSAGE }** d'un message d'évènement relatif à la sécurité des données :

Variable	Description	Exemple
IP address	Adresse IP source ou de destination selon RFC1035 ou RFC4291 section 2.2 Format pour IPv4 : %d.%d.%d.%d	192.168.1.105 2001:DB8::8:800:200C:417A
Dest mac	Adresse MAC de destination Format : %02x:%02x:%02x:%02x:%02x:%02x	00:0C:29:2F:09:B3
Src mac	Adresse MAC source Format : %02x:%02x:%02x:%02x:%02x:%02x	00:0C:29:2F:09:B3
Src port	Port source Plage de valeurs : 0 ... 65535 Format : %d	2345

Variable	Description	Exemple
Dest port	Port de destination Plage de valeurs : 0 ... 65535 Format : %d	80
Protocol	Désignation du service qui a généré un évènement, ou du protocole de couche 4 utilisé. Valeurs possibles : WBM | UDP | TCP | SSH | Console | PNIO | NETCONF | 802.1X | RADIUS | DCP | IP | All Format : %d	TCP
User name	Chaîne de caractères sans espaces qui identifie l'utilisateur identifié par son nom. Format : %d	maier
Group	Chaîne de caractères sans espaces qui identifie un groupe par un nom. Format : %d	it-service
Local interface	Nom symbolique d'une interface locale Format : %d	Console
Destination user name	Identifie un utilisateur par son nom. L'utilisateur est combiné à la destination de l'évènement. Format : %d	Peter.Maier
Role	Nom symbolique du rôle de groupe Format : %d	Administrator
Time minute Timeout	Temps en minutes Format : %d	44
Time second	Temps en secondes Format : %d	44
Failed login count	Nombre d'échecs de connexion Format : %d	10
Max sessions	Nombre maximal de sessions Format : %d	10
Version	Indication de version sans espaces Format : %d	V1.0.3SP1
Firewall rule	Chaîne de caractères pour un jeu de règles de pare-feu avec espaces Format : %d	Rule1
Subject	Chaîne de caractères pour l'objet du certificat Est utilisée comme élément de l'authentification par certificat. La chaîne de caractères peut contenir des espaces et des caractères Unicode. Format : (%s) ou (%s %s) Format : (%S) ou (%S %S) ou code UTF8	(Peter Maier)

Variable	Description	Exemple
Config detail	Chaîne de caractères avec espaces pour la configuration Format : %d	VLAN
License key	Chaîne de caractères qui représente une licence ALM ou un numéro d'article d'un CLP Format : %d	SISLSOXTST0100

7.3.2 Surveillance d'évènements relatifs à la sécurité des données

Ce chapitre décrit les messages d'évènement relatifs à la sécurité des données. La catégorisation des messages est basée sur la norme CEI 62443.

7.3.2.1 Identification et authentification d'utilisateurs humains

Les messages d'évènement ci-après renseignent sur les connexions réussies et les échecs de connexion d'utilisateurs.

{Local interface}: User {User name} logged in.

Exemple	Console: User admin logged in.
Signification	Un utilisateur s'est connecté avec succès à l'appareil via une interface locale. Dans l'exemple, l'utilisateur "admin" s'est connecté avec succès via l'interface de console.
Severity	Info
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.1

{Local interface}: Service account logged in.

Exemple	Console: Service account logged in.
Signification	Un utilisateur s'est connecté avec succès à l'aide d'un compte utilisateur Debug à l'appareil SINEC OS via une interface locale. Dans l'exemple, le compte utilisateur Debug s'est connecté avec succès via l'interface de console.
Severity	Info
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.1

{Local interface}: User {User name} failed to log in.

Exemple	Console: User admin failed to log in.
Signification	La tentative de connexion d'un utilisateur via une interface locale de l'appareil SINEC OS a échoué. Dans l'exemple, la tentative de connexion de l'utilisateur "admin" via l'interface de console, a échoué.

Severity	Error
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.1

{Local interface}: Service account failed to log in.

Exemple	Console: Service account failed to log in.
Signification	La tentative de connexion d'un utilisateur avec le compte utilisateur Debug via une interface locale de l'appareil SINEC OS a échoué. Dans l'exemple, la tentative de connexion avec le compte utilisateur Debug via l'interface de console, a échoué.
Severity	Error
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.1

{Protocol}: User {User name} logged in from {IP address}.

Exemple	SSH: User admin logged in from 192.168.0.1.
Signification	Un utilisateur s'est connecté avec succès à l'appareil SINEC OS via une interface de réseau. Dans l'exemple, l'utilisateur "admin" s'est connecté avec succès à partir de l'adresse de réseau "192.168.0.1".
Severity	Info
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.1

{Protocol}: Service account logged in from {IP address}.

Exemple	SSH: Service account logged in from 192.168.0.1.
Signification	Un utilisateur s'est connecté avec succès à l'aide du compte utilisateur Debug à l'appareil SINEC OS via une interface de réseau. Dans l'exemple, le compte utilisateur Debug a été connecté avec succès à partir de l'adresse de réseau "192.168.0.1".
Severity	Info
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.1

{Protocol}: User {User name} failed to log in from {IP address}.

Exemple	SSH: User admin failed to log in from 192.168.0.1.
Signification	La tentative de connexion d'un utilisateur via une interface de réseau à l'appareil SINEC OS a échoué. Dans l'exemple, la tentative de connexion de l'utilisateur "admin" à partir de l'adresse de réseau "192.168.0.1", a échoué.
Severity	Error
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.1

{Protocol}: Service account failed to login from {IP address}.

Exemple	SSH: Service account failed to login from 192.168.0.1.
Signification	La tentative de connexion avec le compte utilisateur Debug via une interface de réseau à l'appareil SINEC OS a échoué. Dans l'exemple, la tentative de connexion du compte utilisateur Debug à partir de l'adresse de réseau "192.168.0.1", a échoué.
Severity	Error
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.1

{Local interface}: User {User name} logged out.

Exemple	Console: User admin logged out.
Signification	Un utilisateur s'est déconnecté avec succès via une interface locale de l'appareil SINEC OS. Dans l'exemple, l'utilisateur "admin" s'est déconnecté manuellement via l'interface de console.
Severity	Info
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.1

{Protocol}: User {User name} logged out from {IP address}.

Exemple	SSH: User admin logged out from 192.168.0.1.
Signification	Un utilisateur s'est déconnecté via une interface de réseau de l'appareil SINEC OS. Dans l'exemple, l'utilisateur "admin" s'est déconnecté manuellement à partir de l'adresse de réseau "192.168.0.1".
Severity	Info
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.1

{Local interface}: Service account logged out.

Exemple	Console: Service account logged out.
Signification	Un utilisateur a déconnecté le compte utilisateur Debug via interface locale de l'appareil SINEC OS. Dans l'exemple, le compte utilisateur Debug a été déconnecté manuellement via l'interface de console.
Severity	Info
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.1

{Protocol}: Service account logged out from {IP address}.

Exemple	SSH: Service account logged out from 192.168.0.1.
Signification	Un utilisateur a déconnecté le compte utilisateur Debug via une interface de réseau de l'appareil SINEC OS. Dans l'exemple, le compte utilisateur Debug a été connecté manuellement à partir de l'adresse de réseau "192.168.0.1".
Severity	Info
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.1

{Local interface}: Default user {User name} logged in.

Exemple	Console: Default user admin logged in.
Signification	Un utilisateur s'est connecté avec succès avec un profil et un mot de passe prédéfinis via une interface locale à l'appareil SINEC OS. Dans l'exemple, l'utilisateur par défaut "admin" s'est connecté avec succès via l'interface de console.
Severity	Info
Facility	local0
Norme	CEI 62443-3-3 référence : n/a (NERC-CIP 007-R5)

{Protocol}: Default user {User name} logged in from {IP address}.

Exemple	SSH: Default user admin logged in from 192.168.0.1.
Signification	Un utilisateur s'est connecté avec succès avec un profil et un mot de passe prédéfinis via une interface de réseau à l'appareil SINEC OS. Dans l'exemple, l'utilisateur "admin" s'est connecté avec succès à partir de l'adresse de réseau "192.168.0.1".
Severity	Info
Facility	local0
Norme	CEI 62443-3-3 référence : n/a (NERC-CIP 007-R5)

{Protocol}: No response from the RADIUS server {IP address}.

Exemple	RADIUS: No response from the RADIUS server 192.168.1.105.
Signification	Pas d'accès à un serveur RADIUS ou bien le serveur RADIUS ne répond pas. Dans l'exemple, le serveur RADIUS à adresse IP "192.168.1.105" ne répond pas.
Severity	Error
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.1

7.3.2.2 Identification et authentification d'appareils

Les messages d'évènement ci-après renseignent sur les connexions réussies et les échecs de connexion à l'appareil.

{Protocol}: Device {Src mac} access granted.

Exemple	WBM: Device 00:0C:29:2F:09:B3 access granted.
Signification	Accès de l'appareil autorisé après authentification réussie du port. Dans l'exemple, l'accès de l'appareil à adresse MAC source "00:0C:29:2F:09:B3" est autorisé.
Severity	Info
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.2

{Protocol}: Device {Src mac} access denied.

Exemple	WBM: Device 00:0C:29:2F:09:B3 access denied.
Signification	Accès de l'appareil refusé sur échec d'authentification de port. Dans l'exemple, l'accès de l'appareil à adresse MAC source "00:0C:29:2F:09:B3" est refusé.
Severity	Error
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.2

{Protocol}: Connection from device {IP address} subject {Subject} successfully established.

Exemple	WBM: Connection from device 192.168.1.105 subject (Peter Maier) successfully established.
Signification	L'appareil a été authentifié avec succès. Dans l'exemple, une connexion a été établie avec succès entre l'appareil à adresse IP "192.168.1.105" et l'appareil OS SINEC.
Severity	Info
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.2

{Protocol}: Connection from device {IP address} subject {Subject} failed.

Exemple	WBM: Connection from device 192.168.1.105 subject (Peter Maier) failed.
Signification	L'authentification de l'appareil a échoué. Dans l'exemple, il n'a pas été possible d'établir une connexion entre l'appareil à adresse IP "192.168.1.105" et l'appareil OS SINEC.
Severity	Error
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.2

7.3.2.3 Gestion des comptes de réseau

Les messages d'évènement ci-après renseignent sur les activités relatives aux comptes utilisateur. Il s'agit par ex. de la création/suppression de comptes utilisateur, de la modification de mots de passe, de l'activation du compte utilisateur Debug.

{Protocol}: User {User name} has changed the password.

Exemple	WBM: User admin has changed the password.
Signification	Un utilisateur a modifié son propre mot de passe. Dans l'exemple, l'utilisateur "admin" a modifié son propre mot de passe.
Severity	Notice
Facility	local0
Norme	CEI 62443-3-3 Reference: SR 1.3

{Protocol}: User {User name} has changed the password of user {Destination user name}.

Exemple	WBM: User admin has changed the password of user user1.
Signification	Un utilisateur a modifié le mot de passe d'un autre utilisateur. Dans l'exemple, l'utilisateur "admin" a modifié le mot de passe de l'utilisateur "user1".
Severity	Notice
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.3

{Protocol}: User {User name} created user-account {Destination user name} with role {Role}.

Exemple	WBM: User admin created user-account admin2 with role Administrator.
Signification	Un utilisateur a créé un compte utilisateur et lui a affecté un profil d'utilisateur. Dans l'exemple, l'utilisateur "admin" a créé le compte utilisateur "admin2" et affecté au compte le profil d'utilisateur "Administrator".
Severity	Notice
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.3

{Protocol}: User {User name} deleted user-account {Destination user name}.

Exemple	WBM: User admin deleted user-account admin2.
Signification	Un utilisateur a supprimé un compte utilisateur existant. Dans l'exemple, l'utilisateur "admin" a supprimé le compte utilisateur "admin2".
Severity	Notice
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.3

{Protocol}: User {User name} enabled the service account.

Exemple	SSH: User admin enabled the service account.
Signification	Un utilisateur a activé le compte utilisateur Debug. Dans l'exemple, l'utilisateur "admin" a supprimé le compte utilisateur Debug.
Severity	Notice
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.3

{Protocol}: User {User name} disabled the service account.

Exemple	SSH: User admin disabled the service account.
Signification	Un utilisateur a désactivé le compte utilisateur Debug. Dans l'exemple, l'utilisateur "admin" a désactivé le compte utilisateur Debug.
Severity	Notice
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.3

7.3.2.4 Échecs de connexion

Les messages d'évènement ci-après renseignent sur les échecs de connexion et les blocages qui en découlent pour empêcher des attaques par force brute (BFA).

{Protocol}: User {User name} account is locked for {Time minute} minutes after {Failed login count} unsuccessful login attempts.

Exemple	All: User admin account is locked for 10 minutes after 11 unsuccessful login attempts.
Signification	La prévention d'attaques par force brute a bloqué un utilisateur pour un temps défini à la suite d'un nombre excessif d'échecs de connexion. Dans l'exemple, la prévention d'attaques par force brute a bloqué l'utilisateur "admin" pour 10 minutes après 11 échecs de connexion.
Severity	Warning
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.11

{Protocol}: {IP address} is temporarily blocked for {Time second} seconds after {Failed login count} unsuccessful login attempts.

Exemple	All: 192.168.1.105 is temporarily blocked for 600 seconds after 11 unsuccessful login attempts.
Signification	La prévention d'attaques par force brute a bloqué une adresse IP pour un temps défini à la suite d'un nombre excessif d'échecs de connexion. Dans l'exemple, la prévention d'attaques par force brute a bloqué l'adresse IP "192.168.1.105" pour 600 secondes après 11 échecs de connexion.
Severity	Warning
Facility	local0
Norme	CEI 62443-3-3 référence : SR 1.11

7.3.2.5 Blocage de session

Les messages d'évènement ci-après renseignent sur la fermeture de sessions en raison de leur inactivité.

{Protocol}: The session of user {User name} was closed after {Time second} seconds of inactivity.

Exemple	SSH: The session of user admin was closed after 60 seconds of inactivity.
Signification	Une session a été fermée en raison de son inactivité. Dans l'exemple, la session de l'utilisateur "admin" a été fermée au bout de 60 secondes d'inactivité.
Severity	Warning
Facility	local0
Norme	CEI 62443-3-3 référence : SR 2.5

7.3.2.6 Limitation du nombre de sessions simultanées

Les messages d'évènement ci-après renseignent sur la limitation de sessions simultanées possibles par interface.

{Protocol}: The maximum number of {Max sessions} concurrent login session exceeded.

Exemple	SSH: The maximum number of 8 concurrent login sessions exceeded.
Signification	Le nombre maximal de sessions simultanées a été dépassé. Dans l'exemple le nombre maximal de 8 sessions simultanées via SSH a été dépassé.
Severity	Warning
Facility	local0
Norme	CEI 62443-3-3 référence : SR 2.7

7.3.2.7 Modifications de la configuration

Les messages d'évènement ci-après informent de modifications de la configuration par un utilisateur ou un protocole.

{Protocol}: User {User name} has changed the configuration.

Exemple	SSH: User admin has changed the configuration.
Signification	Un utilisateur a modifié la configuration. Dans l'exemple, l'utilisateur "admin" a modifié la configuration.
Severity	Info
Facility	local0
Norme	CEI 62443-3-3 référence : SR 2.12

{Protocol}: User {User name} has changed {Config detail} configuration.

Exemple	SSH: User admin has changed VLAN configuration.
Signification	Un utilisateur a modifié certaines valeurs de la configuration. Dans l'exemple, l'utilisateur "admin" a modifié la configuration du VLAN.
Severity	Info
Facility	local0
Norme	CEI 62443-3-3 référence : SR 2.12

{Protocol}: User {User name} has initiated a reset to factory defaults.

Exemple	SSH: User admin has initiated a reset to factory defaults.
Signification	Un utilisateur a initialisé un rétablissement des paramètres d'usine. Dans l'exemple, l'utilisateur "admin" a initialisé un rétablissement des paramètres d'usine.
Severity	Info
Facility	local0
Norme	CEI 62443-3-3 référence : SR 2.12

{Protocol}: A reset to factory defaults was initiated.

Exemple	DCP: A reset to factory defaults was initiated.
Signification	Un utilisateur a initialisé un rétablissement des paramètres par défaut. Dans l'exemple, DCP a initialisé un rétablissement des paramètres par défaut.
Severity	Info
Facility	local0
Norme	CEI 62443-3-3 référence : SR 2.12

7.3.2.8 Intégrité des communications

Les messages d'évènement ci-après informent sur un échec de justification d'intégrité.

{Protocol}: Integrity verification failed.

Exemple	Console: Integrity verification failed.
Signification	Le contrôle d'intégrité de la communication- d'un message a détecté un défaut d'intégrité. Seule une communication basée sur certificat est possible.
Severity	Error
Facility	local0
Norme	CEI 62443-3-3 référence : SR 3.1

7.3.2.9 Intégrité du logiciel et des informations

Les messages d'évènement ci-après informent sur un échec de justification d'intégrité lors du chargement du firmware.

Firmware integrity verification failed. Backup firmware started.

Exemple	Firmware integrity verification failed. Backup firmware started.
Signification	Le contrôle d'intégrité du firmware a révélé un défaut d'intégrité. Le firmware sauvegardé a été chargé.
Severity	Error
Facility	local0
Norme	CEI 62443-3-3 référence : SR 3.4

7.3.2.10 Intégrité de session

Les messages d'évènement ci-après informent sur un échec de justification d'intégrité lors d'une session.

{Protocol}: Session ID verification failed.

Exemple	WBM: Session ID verification failed.
Signification	L'ID de session n'est pas valide.
Severity	Error
Facility	local0
Norme	CEI 62443-3-3 référence : SR 3.8

7.3.2.11 Protection contre les attaques par déni de service (DoS)

Les messages d'évènement ci-après informent sur l'apparition d'une attaque par déni de service.

{Protocol}: Denial-of-Service (DoS) attack detected.

Exemple	Console: Denial-of-Service (DoS) attack detected.
Signification	Une attaque de déni de service (DoS) a été détectée.
Severity	Alert
Facility	local0
Norme	CEI 62443-3-3 référence : SR 3.8

7.3.2.12 Protection des informations de contrôle

Les messages d'évènement ci-après informent sur la suppression du journal d'incidents local.

{Protocol}: User {User name} has cleared the logging buffer.

Exemple	SSH: User admin has cleared the logging buffer.
Signification	Un utilisateur a supprimé le journal d'incidents local. Dans l'exemple, l'utilisateur "admin" a supprimé le journal d'incidents local.
Severity	Notice
Facility	local0
Norme	CEI 62443-3-3 référence : SR 3.9

7.3.2.13 Restauration de l'automate programmable

Les messages d'évènement ci-après informent sur le succès ou l'échec de l'activation du firmware.

{Protocol}: User {User name} activated the firmware {Version}.

Exemple	WBM: User admin activated the firmware v2.0.
Signification	Un utilisateur a activé avec succès une version de firmware. Dans l'exemple, l'utilisateur "admin" a activé avec succès la version de firmware "v2.0".
Severity	Notice
Facility	local0
Norme	CEI 62443-3-3 référence : SR 7.4

{Protocol}: Firmware {Version} was activated.

Exemple	WBM: Firmware v2.0 was activated.
Signification	Un version de firmware a été activée avec succès. Dans l'exemple, la version de firmware "v2.0" a été activée avec succès.
Severity	Notice
Facility	local0
Norme	CEI 62443-3-3 référence : SR 7.4

{Protocol}: User {User name} failed to activate firmware {Version}.

Exemple	WBM: User admin failed to activate firmware v2.0.
Signification	L'activation d'une version de firmware par un utilisateur a échoué. Dans cet exemple, l'activation de la version de firmware "v2.0" par l'utilisateur "admin" a échoué.
Severity	Error
Facility	local0
Norme	CEI 62443-3-3 référence : SR 7.4

{Protocol}: Firmware activation failed.

Exemple	WBM: Firmware activation failed.
Signification	L'activation du firmware a échoué.
Severity	Error
Facility	local0
Norme	CEI 62443-3-3 référence : SR 7.4

7.4 Clés et certificats

Ce paragraphe décrit comment configurer et gérer les clés et certificats.

7.4.1 Ce qu'il faut savoir sur les clés et certificats

L'utilisation de clés et de certificats permet de crypter la communication et de confirmer l'identité des partenaires de communication :

- **Confidentialité**
  Les données sont secrètes et illisibles pour les personnes non autorisées à les écouter.
- **Intégrité**
  Le message reçu par le destinataire est inchangé et identique à celui que l'expéditeur a envoyé. Le message n'a pas été modifié pendant le transfert.
- **Authentification du nœud d'extrémité**
  Le partenaire de communication qu'est le nœud d'extrémité est exactement celui qu'il prétend être et qu'il faut atteindre. L'identité du partenaire est vérifiée.

SINEC OS utilise pour ce faire les composants suivants :

- Il s'agit d'une procédure de chiffrement symétrique avec des clés publiques et privées
- Certificats
- Signatures

7.4.1.1 Procédures de chiffrement

Procédures de chiffrement symétriques.

Lors de procédures de chiffrement symétriques, les partenaires de communication utilisent la même clé pour le chiffrement et le déchiffrement des informations.

La sécurité de la procédure n'est assurée que si la clé est uniquement connue des deux partenaires de communication. La clé doit par conséquent être échangée via une voie sécurisée, c.-à-d. à l'abri d'écoutes et de manipulations.

Procédures de chiffrement asymétriques.

La procédure de chiffrement asymétrique utilise une paire de clés, constituée d'une clé publique et d'une clé privée. Celles-ci sont uniques et sont corrélées par un algorithme mathématique.

- **Clé publique**
  La clé publique est mise à la disposition du public, c.-à-d. à chaque partenaire de communication potentiel. Toute personne possédant la clé publique peut chiffrer des messages adressés au titulaire.
  Les clés publiques doivent être affectées de manière univoque à un titulaire. Pour s'en assurer, les clés publiques possèdent un certificat numérique qui contient des informations sur le titulaire.
- **Clé privée**
  La clé privée doit être uniquement connue du titulaire. La clé privée permet au titulaire de décrypter les messages qui lui sont adressés.
  La clé privée est en outre utilisée pour signer des certificats.

La clé publique n'étant pas secrète, il n'est pas nécessaire d'utiliser, pour la procédure de chiffrement asymétrique, une voie de communication à l'abri des écoutes.

L'inconvénient du chiffrement asymétrique sont les moyens importants nécessaires au chiffrement et déchiffrement ce qui a un impacte sur la vitesse de calcul.

Diffie-Hellman

La procédure Diffie-Hellman est une procédure de chiffrement asymétrique utilisée pour l'échange des clés et l'accord de clés.

L'échange de clés diffie-Hellman permet à deux partenaires de communication de se mettre d'accord sur une clé partagée secrète (clé de session) via une ligne publique. La clé de session peut ensuite être utilisée pour une procédure de chiffrement symétrique.

L'accord de clé DiffieHellman constitue la base du protocole de chiffrement pour la transmission sécurisée de données (p ex. Transport Layer Security, TLS). Lors de la communication, les avantages du chiffrement symétrique (vitesse de calcul plus élevée) peuvent être mis à profit tandis que le chiffrement asymétrique protège la clé de l'accès d'un agresseur.

7.4.1.2 Paires de clés par défaut

Les appareils SINEC OS sont munis de paires de clés définies par le constructeur pour HTTPS et SSH.

Pour que l'utilisateur puisse accéder à la CLI p. ex. lors de la première mise en service, le serveur SSH a besoin d'une paire de clés appropriée.

Les points suivants s'appliquent aux paires de clés par défaut :

- Les clés sont uniques pour chaque appareil.
- Si vous restaurez les paramètres par défaut de l'appareil, les clés et les certificats définis par le constructeur sont conservés.
- Si une paire de clés par défaut est renouvelée, une entrée appropriée est effectuée dans le journal système. Le renouvellement est nécessaire lorsque des données existantes sont corrompues ou parce qu'une mise à jour du firmware spécifie des exigences plus sévères pour les clés.

Les paires de clés et certificats définis par le constructeur sont utilisables pour HTTPS.

7.4.1.3 Certificats

Les certificats numériques sont utilisés pour confirmer des identités et éviter ainsi des attaques de l'homme du milieu. Une identité peut être une personne, un ordinateur ou une machine.

Un certificat selon la norme X.509 contient essentiellement les éléments suivants :

- une clé publique
- des informations sur le titulaire du certificat (c.-à-d. le détenteur de la clé)
- des attributs tels que
  - numéro de série
  - durée de validité
  - attributs : keyEncipherment
    Une clé symétrique cryptée avec la clé contenue dans le certificat est utilisée pour le chiffrement des données.
  - attributs : digitalSignature
    Une signature numérique (authentification) de l'autorité de certification qui a émis le certificat.

Les certificats sont émis par des autorités officielles de certification (Certificate Authority, CA) ou par le titulaire du certificat.

7.4.1.4 Certificats d'une autorité de certification officielle

Pour obtenir un certificat d'une autorité de certification officielle, il faut effectuer les démarches suivantes :

1. Les personnes qui souhaitent obtenir un certificat doivent déposer une demande de certificat par l'intermédiaire d'une autorité d'enregistrement affiliée à l'autorité de certification.
2. L'autorité de certification évalue la demande et le demandeur en fonction de critères définis.
3. Si l'identité du demandeur peut être clairement établie, l'autorité de certification certifie cette identité en délivrant un certificat signé. Le demandeur est ainsi devenu le titulaire du certificat.

7.4.1.5 Certificats autosignés

Les certificats autosignés sont des certificats dont la signature provient du titulaire du certificat et non d'une autorité de certification indépendante.

Exemples :

- Vous pouvez créer un certificat et le signer vous-même, par exemple pour crypter des messages destinés à un partenaire de communication.
  Un titulaire de certificat pourrait signer lui-même son certificat avec sa clé privée. Le partenaire de communication peut vérifier à l'aide de la clé publique que la signature et la clé publique concordent. Pour la communication interne cryptée entre appareils, cela suffit. En revanche, les certificats autosignés ne conviennent pas pour signer d'autres certificats.
- Un certificat racine est, par exemple, un certificat autosigné par l'autorité de certification (émetteur) qui contient la clé publique de l'autorité de certification.

7.4.1.6 Chaîne de certificats

Un certificat numérique lie une identité contenant les données d'un titulaire de certificat à la clé publique de l'identité. Le certificat numérique lui-même est protégé par une signature numérique dont l'authenticité peut être vérifiée à l'aide de la clé publique de l'émetteur du certificat. Pour vérifier l'identité de la clé de l'émetteur, il faut à nouveau un certificat numérique. De cette manière, une chaîne de certificats numériques est créée, chacun confirmant l'authenticité de la clé publique qui permet de vérifier le certificat précédent. Une telle séquence de certificats est appelée chaîne de certificats.

Les certificats sont organisés à cet effet de manière hiérarchique :

- **Certificats racines**
  Au sommet de la hiérarchie se trouvent les certificats racines, root certificate en anglais. Ce sont des certificats qui ne doivent pas être authentifiés par une autre instance. Ils sont émis par une autorité de certification fiable (Certificate Authority). Le titulaire du certificat et l'émetteur de certificats racines sont identiques. Les certificats racines jouissent d'une confiance absolue, ils sont "l'ancre" de la confiance et doivent donc être connus du destinataire comme des certificats dignes de confiance. Les partenaires de communication doivent pouvoir se fier à l'authenticité de ce certificat sans devoir recourir à un autre certificat.
- **Certificats intermédiaires**
  Les certificats racines sont utilisés pour signer des certificats d'autorités de certification subordonnées, appelés certificats intermédiaires. La confiance est ainsi transférée du certificat racine au certificat intermédiaire. Un certificat intermédiaire peut tout aussi bien signer un certificat qu'un certificat racine, c'est pourquoi les deux sont également appelés "certificats CA".
- **Certificats utilisateurs**
  Cette hiérarchie se poursuit en passant par plusieurs certificats intermédiaires jusqu'au certificat utilisateur, également appelé certificat d'entité finale. Le certificat utilisateur est le certificat de l'identité qui doit être identifiée.

La chaîne des certificats intermédiaires jusqu'au certificat racine doit être présente dans le bon ordre dans chaque appareil qui doit valider le certificat utilisateur d'un partenaire de communication.

7.4.1.7 Signatures

Création

L'émetteur d'un certificat génère une valeur de hachage (empreinte numérique) à partir des données du certificat à l'aide d'un algorithme de hachage spécifique (p. ex. SHA-2, Secure Hash Algorithm). Il crée ensuite une signature numérique à partir de la valeur de hachage et de sa clé privée. La procédure de signature RSA est souvent utilisée à cet effet. La signature numérique est enregistrée dans le certificat. Le certificat est ainsi signé.

Vérification

Le vérificateur d'un certificat se procure le certificat de l'émetteur et donc la clé publique. En utilisant le même algorithme de hachage que celui utilisé lors de la signature (par exemple SHA-2), il génère à nouveau une valeur de hachage à partir des données du certificat. Il compare cette valeur de hachage à la valeur de hachage déterminée à l'aide de la clé publique de l'émetteur du certificat et de l'algorithme de signature pour vérifier la signature.

Si la vérification de la signature donne un résultat positif, que les valeurs de hachage concordent, l'identité du titulaire du certificat ainsi que l'intégrité, c'est-à-dire l'authenticité et l'absence de falsification du contenu du certificat, sont prouvées. Toute personne en possession de la clé publique, c'est-à-dire du certificat de l'autorité de certification, peut vérifier la signature et voir ainsi que le certificat a effectivement été signé par l'autorité de certification.

7.4.1.8 Emplacements de mémoire

SINEC OS définit les emplacements de mémoire suivants pour les clés et les certificats :

- **Keystore**
  SINEC OS utilise les paires de clés enregistrées dans le Keystore comme suit :
  - pour la mise à disposition d'un service de serveur (HTTPS p. ex.)
  - pour l'authentification comme client (pour établir p. ex. une connexion sécurisée pour la transmission de données)

  Un ou plusieurs certificats peuvent être enregistrés avec une paire de clés afin de signer la clé publique.
- **Truststore**
  Le Truststore sert à enregistrer des certificats utilisés par SINEC OS pour authentifier d'autres appareils.
  Une entrée peut contenir plusieurs certificats. Il est ainsi possible d'enregistrer tous les certificats d'une autorité de certification fiable dans une même entrée.
  L'emploi d'une autorité de certification fiable permet de réduire les efforts de configuration.
  Un Truststore peut, avec un seul certificat, authentifier plusieurs serveurs distants.

Le Keystore et le Truststore sont des emplacements de mémoire centraux sous SINEC OS. D'autres fonctions peuvent utiliser les paires de clés ou clés et certificats pulblics fiables, contenus dans le Keystore et le Truststore.

7.4.1.9 Règles d'accès

Les règles suivantes s'appliquent à l'accès aux clés et aux certificats :

- Les utilisateurs ne peuvent ni modifier ni supprimer les paires de clés et les certificats définis par le constructeur.
- Les utilisateurs ne peuvent pas ajouter de certificats personnalisés pour les paires de clés définies par le constructeur.
- Les utilisateurs ne peuvent pas lire les clés privées et les paires de clés, selon qu'elles sont définies par le constructeur ou par l'utilisateur.
- Les utilisateurs disposant de droits d'administrateur ont un accès complet aux paires de clés et aux certificats définis par l'utilisateur.
- Lorsque vous enregistrez la configuration, des paires de clés définies par le constructeur sont enregistrées avec une étiquette spéciale.
- Lorsque vous chargez une configuration (sous forme de fichier ou à partir d'un CLP), les paires de clés et les certificats définis par le constructeur ne doivent pas être modifiés. L'appareil restaure ses propres paires de clés et certificats définis par le constructeur.

7.4.1.10 Évènements associés

Les évènements suivants sont déclenchés pour des clés et certificats et enregistrés directement dans le Syslog.

Évènement	Gravité	Message Syslog
Generation of a new SSH host key due to invalid key in the EE-PROM.	Info	An invalid SSH server key has been detected. As such, a new key has been generated.

7.4.2 Gestion du Keystore

Pour configurer le Keystore, procédez comme suit :

1. [Facultatif] Ajoutez des paires de clés au Keystore.
   Pour plus d'informations, voir "Importation d'une paire de clés à partir d'un PC client (Page 144)" et "Importation d'une paire de clés à partir d'un serveur distant (Page 146)".
1. [Facultatif] Ajoutez des certificats au Keystore pour signer la clé publique.
   Pour plus d'informations, voir le **Manuel de configuration SINEC OS CLI**.

7.4.2.1 Importation d'une paire de clés à partir d'un PC client

Vous pouvez charger un fichier depuis un serveur de fichiers et importer ainsi une paire de clés qu'il contient dans le Keystore.

En plus de la clé privée, le fichier peut contenir un certificat utilisateur autosigné ou une chaîne de certificats pour signer la clé publique. Il n'est pas nécessaire de crypter les clés privées. Cela vaut également pour les clés privées au format PKCS#12.

SINEC OS prend en charge les formats suivants :

- Clés codées PEM
  - Public-Key Cryptography Standards (PKCS#1, PKCS#8)
  - Elliptic Curve Cryptography (nach RFC 5915)
- Certificats X.509 codés PEM
- PKCS#12

Remarque

Si le fichier contient plus d'un certificat, l'ordre des certificats doit correspondre à l'ordre de la chaîne de certificats. Le premier certificat du fichier doit être le certificat utilisateur, le dernier un certificat racine. Entre les deux, il peut y avoir des certificats intermédiaires.

Pour importer un certificat dans le Keystore à partir d'un PC client local, procédez comme suit :

1. Naviguez vers **System** ≫ **Load & Save** ≫ **Keys & Certificates**.
2. Sous **Load Certificate to Keystore from Local PC**, saisissez un nom pour la paire de clés dans **Key Name**.
   Condition :
   - Elle doit compter de 1 à 32 caractères
3. Sous **Certificate Name**, entrez le nom du certificat utilisateur qui doit être créé ou être écrasé.
   Condition :
   - Il doit compter de 1 à 64 caractères
4. Sous **Format**, sélectionnez le format du certificat.
   Options disponibles :

Option	Description
PEM	Le fichier est disponible au format PEM.
PKCS12	Le fichier est disponible au format PKCS#12.

5. [Facultatif] Si vous avez sélectionné sous **Format** l'option **PKCS12** et que le fichier PKCS#12 est crypté, entrez sous **Password (if applicable)** le mot de passe du fichier.
   Condition :
   - Il doit compter de 1 à 255 caractères.
6. [Facultatif] Si un fichier PKCS#12 contient un certificat CA et si ce dernier doit être enregistré dans le Truststore, entrez sous **Certificate Bag** le nom du portefeuille de certificats et sous **Certificate Entry Name** le nom du certificat.
   Condition pour le nom du portefeuille de certificats
   - Elle doit compter de 1 à 32 caractères

   Condition pour le nom du certificat :
   - Il doit compter de 1 à 64 caractères
7. Sous **Certificate File** ouvrez à l'aide du bouton une boîte de dialogue pour sélectionner un fichier.
8. Sélectionnez le fichier voulu dans la boîte de dialogue puis cliquez sur **Open**.
9. Pour charger le certificat, cliquez sur **Load**.
   Pendant que le certificat est chargé, une icône de chargement s'affiche à droite du bouton.
   - Si le chargement s'est bien déroulé, une coche verte s'affiche.
   - Un point d'exclamation rouge et un message d'erreur s'affichent si le chargement a échoué. Renouvelez les dernières opérations.
10. Validez la modification.
11. Pour activer le certificat, redémarrez l'appareil.
    Pour plus d'informations, voir "Redémarrage de l'appareil (Page 72)".
    Lorsque le redémarrage est terminé, la page d'ouverture de session s'affiche.
12. Connectez-vous.
    Pour plus d'informations, voir "Connexion à un appareil configuré (Page 68)".

7.4.2.2 Importation d'une paire de clés à partir d'un serveur distant

Vous pouvez charger un fichier depuis un serveur de fichiers et importer ainsi une paire de clés qu'il contient dans le Keystore.

Conditions

- Vous avez configuré un serveur de manière adéquate.
- Le fichier se trouve sur le serveur.
- Il existe une connexion entre l'appareil et le serveur.
- Selon votre configuration, le nom d'utilisateur et le mot de passe doivent être connus.

Chargement d'un fichier sur l'appareil

En plus de la clé privée, le fichier peut contenir un certificat utilisateur autosigné ou une chaîne de certificats pour signer la clé publique. Il n'est pas nécessaire de crypter les clés privées. Cela vaut également pour les clés privées au format PKCS#12.

SINEC OS prend en charge les formats suivants :

- Clés codées PEM
  - Public-Key Cryptography Standards (PKCS#1, PKCS#8)
  - Elliptic Curve Cryptography (nach RFC 5915)
- Certificats X.509 codés PEM
- PKCS#12

Remarque

Si le fichier contient plus d'un certificat, l'ordre des certificats doit correspondre à l'ordre de la chaîne de certificats. Le premier certificat du fichier doit être le certificat utilisateur, le dernier un certificat racine. Entre les deux, il peut y avoir des certificats intermédiaires.

Pour importer un certificat dans le Keystore à partir d'un serveur distant, procédez comme suit :

1. Naviguez vers **System** ≫ **Load & Save** ≫ **Keys & Certificates**.
2. Sous **Load Certificate to Keystore from Remote Server**, saisissez un nom pour la paire de clés dans **Key Name**.
   Condition :
   - Elle doit compter de 1 à 32 caractères
3. Sous **Certificate Name**, entrez le nom du certificat utilisateur qui doit être créé ou être écrasé.
   Condition :
   - Il doit compter de 1 à 64 caractères
4. Sous **Format**, sélectionnez le format du certificat.
   Options disponibles :

Option	Description
PEM	Le fichier est disponible au format PEM.
PKCS12	Le fichier est disponible au format PKCS#12.

5. [Facultatif] Si vous avez sélectionné sous **Format** l'option **PKCS12** et que le fichier PKCS#12 est crypté, entrez sous **Password (if applicable)** le mot de passe du fichier.
   Condition :
   - Il doit compter de 1 à 255 caractères.
6. [Facultatif] Si un fichier PKCS#12 contient un certificat CA et si ce dernier doit être enregistré dans le Truststore, entrez sous **Certificate Bag** le nom du portefeuille de certificats et sous **Certificate Entry Name** le nom du certificat.
   Condition pour le nom du portefeuille de certificats
   - Elle doit compter de 1 à 32 caractères

   Condition pour le nom du certificat :
   - Il doit compter de 1 à 64 caractères
7. Configurez les paramètres du serveur distant.
   Pour plus d'informations sur le chargement de fichiers, via un serveur distant, voir "Chargement et enregistrement de fichiers via un serveur distant. (Page 47)".
8. Pour charger le certificat, cliquez sur **Load**.
   Pendant que le certificat est chargé, une icône de chargement s'affiche à droite du bouton.
   - Si le chargement s'est bien déroulé, une coche verte s'affiche.
   - Un point d'exclamation rouge et un message d'erreur s'affichent si le chargement a échoué. Renouvelez les dernières opérations.
9. Validez la modification.
10. Pour activer le certificat, redémarrez l'appareil.
    Pour plus d'informations, voir "Redémarrage de l'appareil (Page 72)".
    Lorsque le redémarrage est terminé, la page d'ouverture de session s'affiche.
11. Connectez-vous.
    Pour plus d'informations, voir "Connexion à un appareil configuré (Page 68)".

7.4.3 Gestion du Truststore

Pour configurer le Truststore, procédez comme suit :

1. [Facultatif] Créez un portefeuille de certificats dans le Truststore et ajoutez-y des certificats.
   Un portefeuille de certificats permet de regrouper des certificats. Si vous créez un portefeuille de certificats, vous devez y ajouter directement au moins un certificat.
   Pour plus d'informations, voir "Importation d'un certificat à partir d'un PC client local (Page 148)" et "Importation d'une certificat à partir d'un serveur distant (Page 149)".
2. [Facultatif] Créez un trousseau de clés dans le Truststore et ajoutez-y des Known Hosts. Un trousseau de clés permet de regrouper des Known Hosts. Si vous créez un trousseau de clés, vous devez y ajouter directement au moins un Known Host.
   Pour plus d'informations, voir le **Manuel de configuration SINEC OS CLI**.
   Une demande de confirmation est émise lors de la première connexion à un serveur SFTP. Si vous la validez, l'appareil crée automatiquement un trousseau de clés et enregistre les données du Known Host.
   Pour plus d'informations, voir "Chargement et enregistrement de fichiers via un serveur distant. (Page 47)".

7.4.3.1 Importation d'un certificat à partir d'un PC client local

Vous pouvez charger un certificat à partir d'un PC client local.

SINEC OS prend en charge les formats suivants :

- Certificats X.509 codés PEM
- Certificats codés PEM au format PKCS#7

Remarque

Si le fichier contient plus d'un certificat, l'ordre des certificats doit correspondre à l'ordre de la chaîne de certificats. Le premier certificat du fichier doit être le certificat utilisateur, le dernier un certificat racine. Entre les deux, il peut y avoir des certificats intermédiaires.

Pour importer un certificat dans le Tustsore à partir d'un PC client local, procédez comme suit :

1. Naviguez vers **System** ≫ **Load & Save** ≫ **Keys & Certificates**.
2. Sous **Load Certificate to Truststore from Local PC** saisissez dans **Certificate Bag** le nom du portefeuille de certificats auquel vous voulez ajouter le certificat.
   Si vous voulez créer un nouveau portefeuille de certificats, attribuez un nom au portefeuille de certificats.
   Condition :
   – Elle doit compter de 1 à 32 caractères
3. Sous **Certificate Name**, entrez un nom pour le certificat ou la chaîne de certificats.
   Condition :
   – Il doit compter de 1 à 64 caractères
4. Sous **Format**, sélectionnez le format du certificat.
   Options disponibles :

Option	Description
PEM	Le fichier est disponible au format PEM.
PKCS7	Le fichier est disponible au format PKCS#7.

5. Sous **Certificate File**, ouvrez à l'aide du bouton une boîte de dialogue pour sélectionner un fichier.
6. Sélectionnez le fichier voulu dans la boîte de dialogue puis cliquez sur **Open**.
7. Pour charger le certificat, cliquez sur **Load**.
   Pendant que le certificat est chargé, une icône de chargement s'affiche à droite du bouton.
   – Si le chargement s'est bien déroulé, une coche verte s'affiche.
   – Un point d'exclamation rouge et un message d'erreur s'affichent si le chargement a échoué. Renouvelez les dernières opérations.
8. Validez la modification.

9. Pour activer le certificat, redémarrez l'appareil.
   Pour plus d'informations, voir "Redémarrage de l'appareil (Page 72)".
   Lorsque le redémarrage est terminé, la page d'ouverture de session s'affiche.
10. Connectez-vous.
    Pour plus d'informations, voir "Connexion à un appareil configuré (Page 68)".

7.4.3.2 Importation d'une certificat à partir d'un serveur distant

Vous pouvez charger un certificat à partir d'un serveur distant dans le Truststore.

SINEC OS prend en charge les formats suivants :

- Certificats X.509 codés PEM
- Certificats codés PEM au format PKCS#7

Remarque

Si le fichier contient plus d'un certificat, l'ordre des certificats doit correspondre à l'ordre de la chaîne de certificats. Le premier certificat du fichier doit être le certificat utilisateur, le dernier un certificat racine. Entre les deux, il peut y avoir des certificats intermédiaires.

Conditions

- Vous avez configuré un serveur de manière adéquate.
- Le fichier se trouve sur le serveur.
- Il existe une connexion entre l'appareil et le serveur.
- Selon votre configuration, le nom d'utilisateur et le mot de passe doivent être connus.

Chargement d'un certificat

Pour importer un certificat dans le Truststore à partir d'un serveur distant, procédez comme suit :

1. Naviguez vers **System** ≫ **Load & Save** ≫ **Keys & Certificates**.
2. Sous **Load Certificate to Truststore from Remote Server** saisissez dans **Certificate Bag** le nom du portefeuille de certificats auquel vous voulez ajouter le certificat.
   Si vous voulez créer un nouveau portefeuille de certificats, attribuez un nom au portefeuille de certificats.
   Condition :
   – Elle doit compter de 1 à 32 caractères
3. Sous **Certificate Name**, entrez un nom pour le certificat ou la chaîne de certificats.
   Condition :
   – Il doit compter de 1 à 64 caractères

4. Sous **Format**, sélectionnez le format du certificat.
   Options disponibles :

Option	Description
PEM	Le fichier est disponible au format PEM.
PKCS7	Le fichier est disponible au format PKCS#7.

5. Configurez les paramètres du serveur distant.
   Pour plus d'informations sur le chargement de fichiers, via un serveur distant, voir "Chargement et enregistrement de fichiers via un serveur distant. (Page 47)".
6. Pour charger le certificat, cliquez sur **Load**.
   Pendant que le certificat est chargé, une icône de chargement s'affiche à droite du bouton.
   – Si le chargement s'est bien déroulé, une coche verte s'affiche.
   – Un point d'exclamation rouge et un message d'erreur s'affichent si le chargement a échoué. Renouvelez les dernières opérations.
7. Validez la modification.
8. Pour activer le certificat, redémarrez l'appareil.
   Pour plus d'informations, voir "Redémarrage de l'appareil (Page 72)".
   Lorsque le redémarrage est terminé, la page d'ouverture de session s'affiche.
9. Connectez-vous.
   Pour plus d'informations, voir "Connexion à un appareil configuré (Page 68)".

7.4.4 Surveillance de certificats

Ce paragraphe décrit comment surveiller des clés et certificats et se faire afficher des informations détaillées.

7.4.4.1 Affichage de clés dans le Keystore

Pour afficher des clés dans le Keystore, naviguez vers **System** ≫ **Security** ≫ **Keys & Certificates**.

Sous **Keystore - Key Pairs**, l'écran affiche les informations suivantes :

Paramètres	Description
Key Name	Affiche le nom de la paires de clés.
Public Key Format	Affiche le format de la clé publique. Options disponibles : • **ssh-public-key-format** - Format de clé SSH • **subject-public-key-info-format** - Format de clé TLS
Public Key	Affiche la clé publique

Paramètres	Description
Algorithm	Affiche l'algorithme de hachage avec lequel l'empreinte numérique a été créée. Valeurs possibles : • **md5** - Longueur en bits 128 • **sha1** - Longueur en bits 160 • **sha256** - Longueur en bits 256
Fingerprint	Affiche l'empreinte numérique.

7.4.4.2 Affichage de certificats dans le Keystore

Pour des certificats dans le Keystore, naviguez vers **System** ≫ **Security** ≫ **Keys & Certificates**.

Sous **Keystore - Certificates**, l'écran affiche les informations suivantes :

Paramètres	Description
Key Name	Affiche le nom de la paires de clés.
Certificate Name	Affiche le nom du certificat ou de la chaîne de certificats.
Certificate	Affiche le certificat.
Algorithm	Affiche l'algorithme de hachage avec lequel l'empreinte numérique a été créée. Valeurs possibles : • **md5** - Longueur en bits 128 • **sha1** - Longueur en bits 160 • **sha256** - Longueur en bits 256
Fingerprint	Affiche l'empreinte numérique.

7.4.4.3 Affichage de certificats dans le Truststore

Pour afficher des certificats dans le Truststore, naviguez vers **System** ≫ **Security** ≫ **Keys & Certificates**.

Sous **Truststore - Trusted Certificates**, l'écran affiche les informations suivantes :

Paramètres	Description
Certificate Bag	Affiche le nom du portefeuille de certificats an.
Certificate Entry Name	Affiche le nom du certificat ou de la chaîne de certificats.
Certificate	Affiche le certificat.
Algorithm	Affiche l'algorithme de hachage avec lequel l'empreinte numérique a été créée. Valeurs possibles : • **md5** - Longueur en bits 128 • **sha1** - Longueur en bits 160 • **sha256** - Longueur en bits 256
Fingerprint	Affiche l'empreinte numérique.

7.4.4.4 Affichage de Known Hosts

Pour afficher des Known Hosts dans le Truststore, naviguez vers **System** ≫ **Security** ≫ **Keys & Certificates**.

Sous **Truststore - Known Hosts**, l'écran affiche les informations suivantes :

Paramètres	Description
Public Key Bag	Affiche le nom du trousseau de clés.
Public Key Name	Affiche le nom du Known Host.
Public Key Format	Affiche le format de la clé publique. Options disponibles : • **ssh-public-key-format** - Format de clé SSH • **subject-public-key-info-format** - Format de clé TLS
Public Key	Affiche la clé publique
Algorithm	Affiche l'algorithme de hachage avec lequel l'empreinte numérique a été créée. Valeurs possibles : • **md5** - Longueur en bits 128 • **sha1** - Longueur en bits 160 • **sha256** - Longueur en bits 256
Fingerprint	Affiche l'empreinte numérique.

7.5 Authentification de l'utilisateur

SINEC OS propose diverses options pour l'authentification d'utilisateurs qui souhaitent accéder à l'appareil.

7.5.1 Ce qu'il faut savoir sur l'authentification d'utilisateurs

Tout utilisateur qui tente d'accéder à l'appareil via SSH, HTTPS, etc. doit entrer des identifiants valides. Sinon l'accès lui est refusé. Les utilisateurs peuvent être authentifiés à l'aide d'identifiants enregistrés localement sur l'appareil ou via un service distant.

7.5.1.1 Mode d'authentification

Les options d'authentification sont combinables afin de disposer d'une option de secours en cas de défaillance d'une option (p. ex. lorsque les identifiants locaux sont introuvables, le service distant n'est pas joignable, etc.). La liste complète des modes d'authentification comprend :

- **seulement localement**
  Les utilisateurs sont uniquement authentifiés localement.
- **Seulement via RADIUS**
  Les utilisateurs sont uniquement authentifiés via un serveur RADIUS externe.

- **Localement et RADIUS**authentification
  Les utilisateurs sont d'abord authentifiés localement. Si l'utilisateur est inconnu, les identifiants sont retransmis à un serveur RADIUS externe.
- **RADIUS puis localement**
  Les utilisateurs sont d'abord authentifiés via un serveur RADIUS externe. Si le serveur n'est pas joignable, les utilisateurs sont ensuite authentifiés localement.

Pour plus d'informations sur le paramétrage du mode d'authentification, voir "Sélection du mode d'authentification d'utilisateur (Page 156)".

7.5.1.2 Authentification RADIUS

Le Remote Authentification Dial-In User Service (RADIUS) est un protocole basé UDP qui propose l'authentification, l'autorisation et la gestion des utilisateurs (Authentification, Authorization & Accounting – AAA) pour l'accès d'utilisateurs à un appareil. L'appareil comprend un client RADIUS qui retransmet les identifiants à un serveur RADIUS distant.

Si un utilisateur tente d'accéder à un appareil via SSH, HTTPS, etc., le client RADIUS retransmet les identifiants de l'utilisateur (c.-à-d. le nom d'utilisateur et le mot de passe) à un serveur RADIUS distant. Le serveur compare les identifiants de l'utilisateur à une base de données (ou à une autre source) et autorise l'accès si l'utilisateur a pu être identifié.

Remarque

Pour plus d'informations sur le protocole RADIUS, voir la RFC 2865 (https://tools.ietf.org/html/rfc2865).

Serveur RADIUS

Le client RADIUS communique avec un serveur RADIUS via des requêtes d'authentification. La requête par défaut contient les informations suivantes :

- le nom d'utilisateur et le mot de passe de l'utilisateur
- l'adresse IPv4 de l'appareil de destination/le nom de domaine et le numéro de port du serveur auquel la requête est envoyée.
- une clé secrète partagée pour l'authentification de l'appareil auprès du serveur
- des informations spécifiques du fournisseur

À des fins de redondance, il est possible de définir un serveur RADIUS primaire et un secondaire. Si le serveur primaire ne répond pas, la requête d'authentification est retransmise au serveur secondaire. Si les deux serveurs ne répondent pas à la requête, l'accès est refusé.

Port de destination

Le client RADIUS utilise un port de destination UDP spécifique. UDP- 1812 est utilisé par défaut, cette affectation peut toutefois être modifiée par l'utilisateur.

Évènements associés

Les évènements suivants à propos de RADIUS sont directement enregistrés dans le journal système (Syslog).

Évènement	Gravité	Message Syslog	Condition
EXT_AUTH_UNREACHABLE	Erreur	{ Protocole }:{ Utilisateur } external authentication failed: Servers are unreachable	Le serveur RADIUS externe nécessaire à l'authentification n'est pas joignable.
EXT_AUTH_FAIL	Erreur	{ Protocole }:{ Utilisateur } external authentication failed: Invalid username or password	Le serveur RADIUS externe nécessaire à l'authentification est joignable, mais le nom d'utilisateur et/ou le mot de passe ne sont pas corrects.
EXT_AUTH_SUCCESS	Info	{ Protocole }:{ Utilisateur } external authentication successded via { Adresse IP } - logged in	Le serveur RADIUS externe nécessaire à l'authentification est joignable et le nom d'utilisateur et le mot de passe ont été acceptés.

7.5.2 Configuration de l'authentification d'utilisateurs

Pour configurer l'authentification d'utilisateurs, procédez comme suit :

1. Si une authentification RADIUS s'impose, configurez le client RADIUS.
   Pour plus d'informations, voir "Configuration de l'authentification RADIUS (Page 154)".
2. Paramétrez le mode d'authentification d'utilisateurs.
   Pour plus d'informations, voir "Sélection du mode d'authentification d'utilisateur (Page 156)".

7.5.3 Configuration de l'authentification RADIUS

Pour configurer l'authentification RADIUS, procédez comme suit :

1. Configurez un profil de serveur pour un serveur RADIUS.
   Le profil de serveur définit la connexion au serveur externe. Vous pouvez configurer un serveur primaire et un serveur secondaire comme serveur de secours.
   Pour plus d'informations, voir "Configuration d'un profil de serveur RADIUS (Page 154)".
2. Contrôlez la connexion au(x) serveur(s) RADIUS.
   Pour plus d'informations, voir "Contrôle d'une connexion à un serveur RADIUS (Page 156)".

7.5.3.1 Configuration d'un profil de serveur RADIUS

Un profil de serveur RADIUS définit l'adresse IP et autres identifiants nécessaires à l'accès à un serveur RADIUS externe.

Il faut avoir défini au moins un profil de serveur. Il s'agit du serveur RADIUS primaire. Un profil secondaire peut également être défini comme option de secours pour le cas où le serveur primaire ne serait pas joignable.

Pour configurer un profil de serveur RADIUS, procédez comme suit :

1. Naviguez vers **System** ≫ **Security** ≫ **RADIUS Client**.
2. Sous **Remote Authentication Dial-In User Service (RADIUS) Client**, cliquez sur **Add**. Une nouvelle ligne est insérée dans le tableau.

   Remarque

   Server Type est défini automatiquement.

3. Entrez le nom du profil de serveur sous **Name**.
   Condition :
   – Il doit compter de 1 à 253 caractères.
4. Sous **Shared Secret**, indiquez la clé d'authentification requise par le serveur.
   Conditions :
   – Il doit compter de 1 à 128 caractères.
   – Les caractères ASCII autorisés sont 0x21 à 0x7E.

   Après avoir été confirmée, la clé est cryptée avec AES.
5. Sous **Shared Secret Confirm**, entrez à nouveau la clé d'authentification.
   Conditions :
   – Elle doit compter de 1 à 128 caractères.
   – Les caractères ASCII autorisés sont 0x21 à 0x7E.

   Après avoir été confirmée, la clé est cryptée avec AES.
6. Sous **Server Address | FQDN**, indiquez si l'accès au serveur d'effectue via l'adresse IP ou avec un nom de domaine.
   Condition :
   – Il doit compter de 1 à 253 caractères.
7. [Facultatif] Spécifiez sous **Primary** que ce serveur est le serveur primaire.
   Si vous n'avez pas spécifié qu'un profil de serveur est primaire, le premier profil qui a été défini devient automatiquement le profil primaire.
   Le serveur ne peut pas être défini comme serveur primaire si l'autre profil de serveur est déjà défini comme profil primaire.
8. [Facultatif] Sous **UDP Port** spécifiez le port UDP de destination qui doit être utilisé pour la communication avec le serveur.
   Condition :
   – Un nombre compris entre 1 et 65535

   Par défaut : 1812
9. [Facultatif] Définissez sous **Attempts**, le nombre de tentatives que le client RADIUS doit exécuter pour se connecter au serveur.
   Condition :
   – Un nombre compris entre 1 et 5

   Par défaut : 3

10. [Facultatif] Définissez sous **Timeout** le temps en secondes (s) que le client RADIUS attend une réponse du serveur après une tentative de connexion.
    Conditions :
    - En format nYnMnDnhnmns, dans lequel `n` est un nombre personnalisé
    - 1 seconde min. (1s)
    - 255 secondes max. (255s)

    Par défaut : 5s (5 secondes)
11. Validez les modifications.

7.5.3.2 Contrôle d'une connexion à un serveur RADIUS

Après avoir configuré (ou modifié) un profil de serveur RADIUS et avant d'activer l'authentification RADIUS, il est important de vérifier la connexion au serveur RADIUS défini comme destination. La disponibilité d'un serveur peut également être vérifiée ultérieurement dans le cadre d'une recherche d'erreur.

Pour vérifier la disponibilité d'un serveur RADIUS, procédez comme suit :

1. Naviguez vers **System** ≫ **Security** ≫ **RADIUS Client**.
2. Dans le profil de serveur RADIUS voulu, cliquez sur **Test Credentials**.

- Si le serveur RADIUS répond, le caractère ✓ s'affiche temporairement à côté du bouton.
- Si le serveur RADIUS ne répond pas, le caractère ! s'affiche temporairement à côté du bouton.

7.5.4 Sélection du mode d'authentification d'utilisateur

Le mode d'authentification d'utilisateur définit la manière d'authentifier les utilisateurs : localement, par un serveur externe (RADIUS p. ex.) ou par une combinaison des deux méthodes.

Pour sélectionner le mode d'authentification, procédez comme suit :

Remarque

Activez l'authentification RADIUS seulement après avoir vérifié qu'un serveur RADIUS externe est joignable.

1. Naviguez vers **System** ≫ **Security** ≫ **User Management**.
2. Sous **Login Authentication Type & Order**, paramétrez le mode d'authentification d'utilisateurs dans **Type & Order**.
   Options disponibles :

Option	Description
Local	**Par défaut** Les utilisateurs sont authentifiés localement.
RADIUS	Les utilisateurs sont authentifiés via un serveur RADIUS externe.
Local and RADIUS	Les utilisateurs sont d'abord authentifiés localement. Si l'utilisateur est inconnu, les identifiants sont retransmis à un serveur RADIUS externe.
RADIUS and fallback local	Les utilisateurs sont d'abord authentifiés via un serveur RADIUS externe. Si le serveur n'est pas joignable, les utilisateurs sont ensuite authentifiés localement.

3. Validez la modification.

7.5.5 Surveillance de l'authentification d'utilisateurs

Ce paragraphe décrit comment surveiller les aspects de l'authentification d'utilisateurs.

7.5.5.1 Affichage des statistiques RADIUS

Pour afficher les statistiques d'un serveur RADIUS, naviguez vers **System** ≫ **Security** ≫ **RADIUS Client**.

Remarque

Toutes les statistiques RADIUS sont automatiquement supprimées lorsque l'appareil est réinitialisé.

Les informations suivantes sont affichées pour chaque serveur RADIUS défini :

Statistiques	Description
Name	Le nom affecté au serveur RADIUS.
Accepted	Nombre de requêtes d'authentification RADIUS acceptées par le serveur.
Rejected	Nombre de requêtes d'authentification RADIUS refusées par le serveur.
Lost	Nombre de requêtes d'authentification RADIUS perdues parce que le serveur n'était pas joignable.

Administration d'interfaces

8

Ce chapitre décrit comment configurer et gérer des interfaces sur l'appareil.

8.1 Interfaces

Chaque port physique et chaque VLAN est représenté par une interface. Chaque interface offre diverses options de trafic de données entrant ou sortant.

Ce paragraphe décrit les types d'interfaces et leurs paramètres configurables.

IMPORTANT
Vulnérabilité - Risque d'intrusion et/ou d'abus. Tous les ports de pont sont activés par défaut. En outre, tous les ports de pont qui ont été désactivés lors de la restauration des paramètres par défaut de l'appareil (paramètres d'usine) sont de nouveau activés. **Seuls les ports de pont qui sont utilisés devraient être activés.** Un port de pont qui n'est pas utilisé et n'est pas configuré correctement constitue un point d'accès potentiel au réseau auquel l'appareil est connecté.

8.1.1 Ce qu'il faut savoir sur les interfaces

SINEC OS prend en charge les types d'interfaces suivants :

Type	Description
Ports de pont	Ports Ethernet fixes ou SFP (Small Formfactor Pluggable).
Interfaces VLAN	Interfaces logiques pour VLAN. Il est possible de leur affecter des adresses IP et d'autoriser un VLAN de participer à des activités de couche 3.
Function Extender Interfaces (FEI)	Ports représentant des connecteurs physiques sur un moteur de traitement local (LPE) externe.

Chaque port possède des options configurables de vitesse de port, de mode duplex, d'autonégociation et autres.

8.1.1.1 Conventions de dénomination d'interfaces

Les interfaces sont désignées en fonction des conventions suivantes :

Conventions de dénomination	Exemples	Description
ethernet{ Emplacement }/{ Port }	ethernet0/1, ethernet3/2	Les ports de pont sont nommés en fonction de l'emplacement physique où le port se trouve et du numéro de port. Si l'appareil ne prend pas en charge d'emplacement de module comme c'est le cas de la plupart des appareils à petit facteur de forme, le numéro d'emplacement est (0).
vlan{ ID }	vlan1, vlan2	Les interfaces für de VLAN sont nommées en fonction de l'ID de VLAN.
extender{ Emplacement }/{ Port }	extender0/1, extender0/2	Les ports de la Function Extender Interface (FEI) sont nommés **extender**, suivi du numéro d'emplacement et du numéro de port correspondant. Si l'appareil ne prend pas en charge d'emplacement de module comme c'est le cas de la plupart des appareils à petit facteur de forme, le numéro d'emplacement est (0).

8.1.1.2 Autonégociation

SINEC OS prend en charge l'autonégociation pour ports de pont 1000 Mbit/s (ou plus), tels que définis dans IEEE 802.3.

Grâce à l'autonégociation, deux ports de pont peuvent, lors de la détection de la connexion, négocier le plus grand dénominateur commun de leurs paramètres de transmission communs (à savoir la vitesse, le contrôle de flux et le mode duplex). Ceci permet une configuration Zero-Touch (c.-à-d. les ports se configurent automatiquement). Ceci permet aussi une assistance flexible des partenaires de liaison qui ne possèdent pas les mêmes propriétés que votre appareil.

8.1.1.3 Communication en duplex

La communication en duplex permet aux partenaires de liaison de communiquer dans les deux sens. SINEC OS prend en charge les types de voies de communication suivants suivants :

- **Duplex intégral**
  En mode duplex intégral, les deux partenaires de liaison peuvent émettre et recevoir dans les deux sens. La communication via protocole Voice Over Internet (VOIP) est une excellente application pour ce mode de communication. Les locuteurs des deux côtés d'une conversation peuvent parler et s'écouter mutuellement en même temps, car les extrémités de leurs canaux peuvent envoyer et recevoir simultanément des signaux.

Figure 8-1 Communication en duplex intégral

- **Semi-duplex**
  En mode semi-duplex, les deux partenaires de liaison peuvent émettre et recevoir dans les deux sens, mais uniquement chacun à son tour. Le talkie-walkie est un bon exemple de canal de communication semi-duplex. Si vous appuyez sur le bouton pour parler, vous ne pouvez pas entendre la personne à l'autre bout, mais cette personne peut vous entendre.

Figure 8-2 Communication en semi-duplex

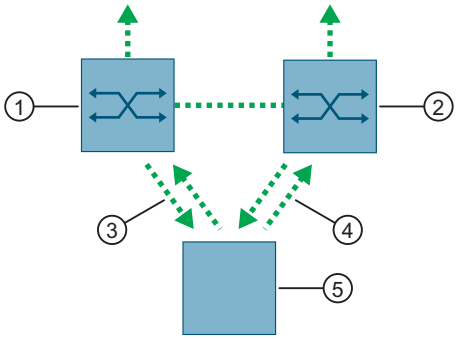
IMPORTANT
Risque de configuration - Risque de fortes pertes de trames Les commutateurs aux deux extrémités de la liaison doivent être configurés pour le même mode de duplex. Si le commutateur A est en mode duplex intégral et si le commutateur B est en mode semi-duplex, de fortes pertes de trames se produisent dans le réseau en cas de trafic de données important.

8.1.1.4 Protection de l'automate par Link Fault Indication (LFI)

Les commandes industrielles modernes possèdent souvent des interfaces de réserve auxquelles on a recours en cas de défaillance d'un lien. Lorsque ces interfaces de supports de données fonctionnent avec des voies d'émission et de réception séparées, elles sont vulnérables aux erreurs qui n'affectent qu'une seule des deux voies.

Scénario

Les deux commutateurs S1 et S2 sont connectés à un automate. S1 est connecté au port principal de l'automate. S2 est connecté au port de réserve qui est désactivé administrativement par l'automate pendant que la liaison à S1 est actifve. S2 doit transmettre des trames à l'automate via S1.



① S1
② S2
③ Voie de transmission principale
④ Voie de transmission de réserve
⑤ Automate

Figure 8-3 Scénario

En cas de défaillance de la voie de transmission de l'automate vers S1, S1 génère quand même un signal de liaison à l'adresse de l'automate par la voie de réception. L'automate détecte cependant le lien à S1 et ne se connecte pas au port de réserve.

Cette situation illustre la nécessité de disposer d'une possibilité d'informer un partenaire de liaison que le signal d'intégrité de la liaison a été bloqué. Une telle possibilité existe sur certains supports de liaison, mais pas sur tous.

Mécanismes de notification natifs

Supports de transmission	Mécanisme de notification natif pour partenaires de liaison
100Base-TX 1000Base-T 1000Base-X	Intègre une fonction d'autonégociation (c.-à-d. que le signal d'autonégociation comprend un mémento spécial qui signale la présence d'un défaut distant).
100Base-FX	Peut comprendre une Far-End-Fault-Indication (FEFI) telle que définie dans l'IEEE 802.3. Cette fonction comprend : • **La transmission de FEFI** Un signal d'intégrité de liaison modifié est transmis lorsqu'une défaillance de la liaison est détectée (c.-à-d. que le partenaire de liaison ne recevra pas de signal de liaison). • **La détection de FEFI** Une perte de liaison est affichée lorsque le partenaire de liaison reçoit un signal FEFI. FEFI est une fonction en option de la norme IEEE 802.3. Cette méthode n'est pas prise en charge par tous les partenaires de liaison.
10Base-FL	Non pris en charge

Link Fault Indication (LFI) (indication de défaut de liaison, LFI)

Les deux commutateurs S1 et S2 sont connectés à un automate. S1 est connecté au port principal de l'automate. S2 est connecté au port de réserve qui est désactivé administrativement

par l'automate pendant que la liaison à S1 est active. S2 doit transmettre des trames à l'automate via S1.

Remarque

LFI peut uniquement être activé pour des ports de fibres optiques en verre.

Dans le scénario décrit plus haut, S1 ne génère plus de signal d'intégrité de liaison, s'il ne reçoit plus de signal de liaison de l'automate. L'automate détecte la défaillance de la liaison et le basculement sur l'interface de réserve.

SINEC OS peut également être configuré de manière à ce que l'adresse MAC soit flushées pour le port de l'automate. Les trames destinées à l'automate inondent S2 d'où elles sont retransmises à l'automate. (une fois que l'automate a transféré sa première trame).

IMPORTANT
Risque de configuration - Risque de défaillance des communications Si LFI est pris en charge par les deux partenaires de liaison, activez LFI uniquement sur l'un des partenaires de liaison. Si LFI est activé sur les deux partenaires, il n'est plus possible d'établir une liaison, car les deux extrémités attendent que l'autre extrémité transmette un signal d'intégrité de liaison.

8.1.1.5 Contrôle de flux

Le contrôle de flux est une fonction optionnelle qui permet à un port de pont compatible Gigabit d'entendre une trame PAUSE émise par son partenaire de liaison. Cette trame est envoyée lorsque le partenaire de liaison a été inondé de plus de trames qu'il ne peut en traiter efficacement. Il a besoin de temps pour réduire sa file d'attente avant de pouvoir recevoir plus de trames.

La trame PAUSE contient une temporisation. Si l'expéditeur ne reçoit pas d'autre trame PAUSE avant l'expiration du délai, il peut poursuivre l'échange de données.

SINEC OS prend en charge la procédure de trame PAUSE, mais il se peut que d'autres appareils ne le fassent pas. Il faut par conséquent que le contrôle de flux soit négocié.

8.1.1.6 Ports de Function Extender Interface (FEI)

Les ports de la Function Extender Interface (FEI) sont les connecteurs physiques entre l'appareil et un Local Processing Engine externe (moteur de traitement local externe, LPE), un appareil de la famille SCALANCE LPE-9000, p. ex. Un LPE peut être utilisé pour diverses applications, pour la réplication du trafic de données p. ex. ou comme appareil de l'Internet des objets (IoT).

Les ports FEI sont toujours visibles dans l'interface utilisateur SINEC OS, même lorsqu'aucun LPE n'est connecté. Ils sont représentés dans l'interface utilisateur comme extender0/*N* (p. ex. extender0/1extender0/2, extender0/3) et figurent toujours en fin d'une liste d'interfaces.

Remarque

Restrictions

- Le mode duplex, la vitesse, l'autonégociation et les paramètres de rétrogradation sont en lecture seule.
- Les ports FEI ne sont pas visibles via PROFINET
- Il n'est pas possible d'effectuer des tests de câbles sur des ports FEI.

Configuration de port FEI

Il s'agit de paramètres définis pour ports FEI :

Port FEI	Autonégociation	Vitesse	Mode duplex	Rétrogradation
extender0/1	Disabled	1 Gbps	Full Duplex	Disabled
extender0/2	Disabled	1 Gbps	Full Duplex	Enabled
extender0/3	Disabled	10 Gbps	Full Duplex	Enabled

8.1.1.7 Ports de convertisseur de médias embrochable

Les appareils à emplacements de convertisseur de médias embrochables peuvent être équipés à volonté de convertisseurs de médias embrochables (Small Form factor Pluggable, SFP).

Les SFP sont des modules standardisés pour établir des connexions réseau qui offrent une multitude de propriétés diverses (vitesse de transmission, longueur de câble, support de transmission).

SINEC OS prend en charge de nombreux convertisseurs de médias embrochables qui permettent d'étendre la portée et les fonctions d'un réseau.

Remarque

Utilisez uniquement des convertisseurs de médias agréés.

Si vous utilisez des convertisseurs de médias qui n'ont pas été validés par Siemens, le fonctionnement de l'appareil conformément aux spécifications n'est pas assuré.

Si vous utilisez des convertisseurs de médias non agréés, les problèmes ci-après peuvent survenir :

- endommagement de l'appareil
- perte des homologations
- violation des dispositions de CEM

Vous trouverez une liste des convertisseurs de médias embrochables agréés dans les manuels des appareils respectifs.

Échangeables en cours de fonctionnement

Tous les convertisseurs de médias embrochables sont échangeables en cours de fonctionnement. Vous pouvez débrocher et embrocher des convertisseurs de médias embrochables sans interrompre le fonctionnement de l'appareil. Si un convertisseur de médias embrochable est débroché, cela affecte uniquement la connexion préalablement établie à l'interface du convertisseur de médias embrochable.

Détection automatique

SINEC OS surveille activement chaque convertisseur de médias embrochable, afin de savoir si le convertisseur de médias embrochable a été débroché ou embroché. Tout évènement déclenche une alarme qui est enregistrée dans Syslog.

Smart SFP

Smart SFP est activé par défaut sur chaque convertisseur de médias embrochable.

Smart SFP permet à SINEC OS de configurer automatiquement les paramètres de vitesse, de mode duplex et d'autonégociation d'une interface de manière appropriée pour convertisseur de médias embroché. Ces paramètres reposent sur les propriétés des convertisseurs de médias embrochables.

Les paramètres de l'interface sont conservés lorsqu'un convertisseur de médias embrochable est débroché ou que l'appareil est redémarré. Un convertisseur de médias embrochable peut ainsi être rapidement et facilement remplacé par un convertisseur de médias embrochable du même type, c.-à-d. possédant le même numéro d'article. L'appareil détecte un autre type de convertisseur de médias embrochable, avec d'autres propriétés, sa configuration est automatiquement écrasée par les valeurs du convertisseur de médias embrochable actuel.

Si les propriétés d'un convertisseur de médias embrochable ne sont pas exploitables, vous pouvez désactiver la configuration automatique. Ceci permet d'éviter que SINEC OS configure des paramètres erronés pour l'interface.

Remarque

Les convertisseurs de médias embrochables, validés par Siemens, prennent en charge Smart SFP. Les convertisseurs de médias embrochables qui ne prennent pas en charge Smart SFP peuvent être désactivés et être repérés par **Unidentified**. Désactivez Smart SFP dans ce cas et configurez l'interface manuellement.

Si, alors que Smart SFP est activé, un convertisseur de médias embrochable 1000Base-X qui prend en charge 100Base-X et 1000Base-X, est embroché, l'interface est automatiquement configurée pour 1000Base-X.

Évènements associés

Les évènements suivants sont déclenchés par des convertisseurs de médias embrochables et sont enregistrés directement dans le Syslog.

Évènement	Gravité	Message Syslog
Module-presence	Warning	Module { Nom/Type du convertisseur de médias embrochable } [Inserted | Removed]
Module-state	Warning	Unknown SFP module on interface { Interface de convertisseur de médias embrochable } (vendor: { Constructeur })
		Rejected SFP module on interface { Interface de convertisseur de médias embrochable }
		Unsupported SFP module on interface { Interface de convertisseur de médias embrochable }

8.1.2 Configuration des ports de pont

Les ports de pont sont tous administrativement activés par défaut et configurés pour l'autonégociation. La connexion physique des ports associés à un partenaire de liaison est typiquement la seule chose nécessaire. Éventuellement vous serez cependant obligé d'effectuer des paramétrages complémentaires.

Remarque

Les fonctions de port de pont suivantes sont uniquement configurables via CLI :

- Activation de Link Fault Indication (LFI)
- Désactivation automatique d'un port de pont en cas d'évènement Link down

Pour plus d'informations sur cette fonction, voir le **Manuel de configuration SINEC OS CLI**.

Pour configurer un port de pont, procédez comme suit :

1. [Facultatif] Complétez ou modifiez la description du port de pont.
   Pour plus d'informations, voir "Ajout d'une description pour un port de pont (Page 167)".
2. [Facultatif] Activez l'autonégociation.
   Cette fonction permet à des partenaires de liaison de négocier les paramètres en fonction de leurs capacités et de les configurer automatiquement. L'autonégociation est activée par défaut pour tous les ports de pont.
   Pour plus d'informations, voir "Activation de l'autonégociation (Page 168)".
3. [Facultatif] Choisissez la vitesse à laquelle le port de pont transmet les trames.
   La vitesse est typiquement négociée automatiquement avec le partenaire de liaison, mais doit cependant être paramétrée explicitement pour les ports de pont non compatibles Gigabit.
   Pour plus d'informations, voir "Paramétrage de la vitesse des ports de pont (Page 168)".
4. [Facultatif] Sélectionnez le mode duplex.
   Cette fonction détermine comment les partenaires de liaison communiquent entre eux. La vitesse est typiquement négociée automatiquement avec le partenaire de liaison, mais doit cependant être paramétrée explicitement pour les ports de pont non compatibles Gigabit.
   Pour plus d'informations, voir "Paramétrage du mode duplex (Page 169)".

5. [Facultatif] Activez la rétrogradation.
   Cette fonction permet à deux ports de pont 1000Base-T de négocier une vitesse de transmission inférieure pour pouvoir utiliser un câble à paires torsadées en cuivre, qui est uniquement conçu pour des liaisons 100Base-TX.
   Pour plus d'informations, voir "Activation de la rétrogradation pour les interfaces Gigabit (Page 170)".
6. [Facultatif] Activez le déclenchement d'une alarme en cas d'évènements Link down/Link up.
   Pour plus d'informations, voir "Activation de notifications Link up/Link down (Page 171)".
7. [Facultatif] Attribuez au port de pont une adresse IPv4 statique.
   Pour plus d'informations, voir "Configuration d'une adresse IPv4 statique (Page 185)".
8. [Facultatif] Activez Smart SFP (uniquement pour les ports SFP).
   Pour plus d'informations, voir "Activez Smart SFP (uniquement pour les ports SFP). (Page 171)".
9. Veillez à ce que le port de pont soit activé.
   Pour plus d'informations, voir "Activation d'un port de pont (Page 172)".

8.1.2.1 Ajout d'une description pour un port de pont

Une description peut être ajoutée à chaque port de pont pour faciliter l'identification de l'interface. La description peut contenir p. ex. le nom du constructeur, la désignation du produit, la version du matériel/firmware et/ou l'identification univoque de l'interface.

Pour ajouter une description à un port de pont, procédez comme suit :

1. Naviguez vers **Interfaces** ≫ **Ethernet Interfaces** ≫ **Interfaces**.
2. Sous **Ethernet Interfaces**, entrez dans **Description** une description du port de pont sélectionné.
   Condition :
   – Elle doit compter de 0 à 64 caractères
3. Validez la modification.

8.1.2.2 Activation de l'autonégociation

Pour activer l'autonégociation d'un port de pont, procédez comme suit :

IMPORTANT

Restrictions

- L'autonégociation est uniquement disponible pour les ports de pont de catégorie 1 Gigabit Ethernet (ou supérieurs).
  Pour savoir si un port de pont défini est compatible avec l'autonégociation, voir le **Manuel de configuration SINEC OS CLI**.
- L'autonégociation doit être activée sur les ports Ethernet 1 Gigabit cuivre, si la vitesse paramétrée est de 1000 Mbit/s.
- L'autonégociation doit être activée sur tous les ports Ethernet 10 Gigabits cuivre.
- L'autonégociation doit être désactivée sur tous les ports Ethernet 10 Gigabits à fibre de verre.

Remarque

L'autonégociation est désactivée par défaut pour tous les ports 100BASE-FX, 1000BASE-X et 10GBASE-X.

L'autonégociation est activée par défaut pour tous les autres ports qui prennent en charge cette fonction.

L'autonégociation ne peut être désactivée pour un port de pont, si des valeurs définies sont affectées à la vitesse et au mode duplex (c.-à-d. pas `auto`).

1. Naviguez vers **Interfaces** ≫ **Ethernet Interfaces** ≫ **Interfaces**.
2. Sous **Ethernet Interfaces**, modifiez **Auto-Negotiation** en **Enabled** pour le port de pont sélectionné.
3. Validez la modification.

8.1.2.3 Paramétrage de la vitesse des ports de pont

La vitesse à laquelle un port de pont transfère des trames peut être réglée sur une valeur définie. La vitesse peut également être négociée entre un port et son partenaire de liaison si l'autonégociation est activée. Un port Gigabit Ethernet peut p. ex. être paramétré de sorte qu'il transmette des trames à 100 Mbit/s, pour pouvoir se connecter à un port Fast Ethernet.

Pour paramétrer une vitesse à laquelle un port de pont transmet des trames, procédez comme suit :

IMPORTANT
Restrictions • L'autonégociation doit être activée sur les ports Ethernet 1 Gigabit cuivre, si la vitesse paramétrée est de **1 Gb/s**. • La vitesse doit être paramétrée pour tous les ports de pont Ethernet 1 Gigabit fibre de verre à **1 Gb/s**. • La vitesse doit être paramétrée pour tous les ports de pont Ethernet 10 Gigabit fibre de verre à **10 Gb/s**.

1. Naviguez vers **Interfaces** ≫ **Ethernet Interfaces** ≫ **Interfaces**.
2. Sous **Ethernet Interfaces**, sélectionnez pour **Speed** la vitesse du port de pont sélectionné. Options disponibles :

Option	Description
Auto	Les trames sont transmises à la vitesse déterminée par l'autonégociation.
10 Mb/s	Les trames sont transmises à 10 Mbit/s.
100 Mb/s	Les trames sont transmises à 100 Mbit/s.
1 Gb/s	Les trames sont transmises à 1 Gbit/s.
2.5 Gb/s	Les trames sont transmises à 2,5 Gbit/s.
5 Gb/s	Les trames sont transmises à 5 Gbit/s.
10 Gb/s	Les trames sont transmises à 10 Gbit/s.

   Si l'autonégociation est activée, l'interface signale l'option de vitesse choisie au partenaire de liaison.
   Si l'autonégociation est désactivée, l'interface est exploitée à la vitesse dont elle est capable.
   Par défaut : **Auto**
3. Validez la modification.

8.1.2.4 Paramétrage du mode duplex

La communication en duplex permet aux partenaires de liaison de communiquer dans les deux sens. Selon le mode choisi, les trames peuvent être transmises dans les deux directions soit simultanément, soit en alternance. Le mode duplex peut également être négocié entre les partenaires de liaison pour déterminer la meilleure option en fonction des capacités des deux interfaces.

Pour sélectionner le mode duplex pour un port de pont, procédez comme suit :

IMPORTANT
Risque de configuration - Risque de fortes pertes de trames Les commutateurs aux deux extrémités de la liaison doivent être configurés pour le même mode de duplex. Si un commutateur est en mode duplex intégral et si l'autre commutateur est en mode semi-duplex, de fortes pertes de trames se produisent dans le réseau en cas de trafic de données important.

IMPORTANT
Restriction • Sur tous les ports Ethernet 1 Gigabit (ou plus) en technologie cuivre ou fibre optique, modifiez le paramètre duplex en **duplex intégral**.

1. Naviguez vers **Interfaces** ≫ **Ethernet Interfaces** ≫ **Interfaces**.
2. Sous **Ethernet Interfaces** sélectionnez dans **Duplex Mode** le mode duplex pour l'interface sélectionnée.
   Options disponibles :

Option	Description
Auto	**Par défaut** Le mode duplex est déterminé par autonégociation.
Half-duplex	La communication entre l'interface et son partenaire de liaison intervient dans les deux directions, mais dans une seule direction à la fois. Cette option n'est pas sélectionnable si la valeur paramétrée est de 1 Gbit/s.
Full-duplex	La communication entre l'interface et son partenaire de liaison peut se dérouler simultanément dans les deux directions transmission bidirectionnelle).

3. Validez la modification.

8.1.2.5 Activation de la rétrogradation pour les interfaces Gigabit

La rétrogradation permet d'utiliser un câble à paires torsadées en cuivre entre deux ports Ethernet 1000Base-T. Si vous utilisez un câble à paires torsadées en cuivre et que la rétrogradation est activée, les interfaces réduisent automatiquement à chaque extrémité de la liaison la vitesse de transmission à 10 ou 100 Mbit/s.

Remarque

La rétrogradation est activée par défaut pour tous les ports de pont compatibles Gigabit.

Si la rétrogradation est désactivée, les deux ports tentent d'établir une liaison à 1000 Mbit/s, ce qui n'est pas pris en charge par le câble.

Pour activer la rétrogradation d'un port de pont, procédez comme suit :

1. Naviguez vers **Interfaces** ≫ **Ethernet Interfaces** ≫ **Interfaces**.
2. Sous **Ethernet Interfaces**, modifiez **Downshift** en **Enabled** pour le port de pont sélectionné.
3. Validez la modification.

8.1.2.6 Activation de notifications Link up/Link down

Des notifications SNMP d'évènements Link up et Link down peuvent être activées ou désactivées pour des ports de pont spécifiques. Si elles sont désactivées, les alarmes liées à ces évènements ne sont jamais déclenchées pour ces interfaces.

Remarque

Les notifications de Link up et de Link down sont déactivées par défaut sur tous les ports de pont.

Pour activer les notifications SNMP Link up et Link down sur un port de pont, procédez comme suit :

1. Naviguez vers **Interfaces** ≫ **Ethernet Interfaces** ≫ **Interfaces**.
2. Sous **Ethernet Interfaces**, modifiez **Link Up/Down Traps** en **Enabled** pour le port de pont sélectionné.
3. Validez la modification.

8.1.2.7 Activez Smart SFP (uniquement pour les ports SFP).

Dès qu'un convertisseur de médias est embroché, le port du convertisseur de médias embrochable est activé par défaut administrativement et Smart SFP est activé. SINEC OS configure alors automatiquement les paramètres de l'interface (vitesse, mode duplex et autonégociation) de manière appropriée pour les convertisseurs de médias embrochés.

Pour tous les ports non SFP, la fonction est remplacée par "-".

Pour activer Smart SFP, procédez comme suit :

1. Naviguez vers **Interfaces** ≫ **Ethernet Interfaces** ≫ **Interfaces**.
2. Sous **Ethernet Interfaces**, modifiez le paramètre **SFP Auto Config** du port de convertisseur de médias embrochable en **Enabled**.
3. Validez la modification.

8.1.2.8 Activation d'un port de pont

Pour activer un port de pont, procédez comme suit :

IMPORTANT
Vulnérabilité - Risque d'intrusion et/ou d'abus Tous les ports de pont sont activés par défaut. En outre, tous les ports de pont qui ont été désactivés lors de la restauration des paramètres par défaut de l'appareil (paramètres d'usine) sont de nouveau activés. **Seuls les ports de pont qui sont utilisés devraient être activés.** Une interface qui n'est pas utilisée et n'est pas configurée correctement constitue un point d'accès potentiel au réseau auquel l'appareil est connecté.

1. Naviguez vers **Interfaces** ≫ **Ethernet Interfaces** ≫ **Interfaces**.
2. Sous **Ethernet Interfaces**, modifiez **Interface State** en **Enabled** pour le port de pont sélectionné.
3. Validez la modification.

8.1.3 Configuration d'interfaces VLAN

Il faut qu'au moins une interface VLAN soit définie pour pouvoir accéder à distance via un protocole IP (z.B. HTTP, SNMP, NETCONF, SSH, etc.) à l'appareil. Sinon il est uniquement possible d'accéder à l'appareil via une connexion série directe.

Pour configurer une interface VLAN, procédez comme suit :

1. Définissez une interface VLAN.
   Pour plus d'informations, voir "Ajout d'une interface VLAN (Page 173)".
2. [Facultatif] Ajoutez une description de l'interface.
   Pour plus d'informations, voir "Ajout d'une description à une interface de VLAN (Page 173)".
3. [Facultatif] Configurez la taille de la MTU.
   Pour plus d'informations, voir "Configuration de la taille de la MTU (Page 173)".
4. [Facultatif] Activez le déclenchement d'une alarme en cas d'évènements Link down/Link up.
   Pour plus d'informations, voir "Activation de notifications Link up/Link down (Page 173)".
5. [Facultatif] Attribuez à l'interface une adresse IPv4 statique ou activez DHCP.
   Pour plus d'informations, voir "Attribution d'adresses IP (Page 185)".
6. Activez l'interface VLAN.
   Pour plus d'informations, voir "Activation d'une interface de VLAN (Page 174)".

8.1.3.1 Ajout d'une interface VLAN

Pour ajouter une interface VLAN, procédez comme suit :

1. Vérifiez qu'il existe une interface VLAN statique à laquelle vous pouvez affecter la nouvelle interface.
   Pour plus d'informations sur l'ajout de VLAN statiques, voir "Ajout ou édition d'un VLAN statique (Page 254)".
2. Naviguez vers **Interfaces** ≫ **IP Interfaces**.
3. Sous **IP Interfaces**, cliquez sur **Add**. Une nouvelle ligne est insérée dans le tableau.
4. Sous **Interface**, sélectionnez un VLAN existant.
5. Validez la modification.

8.1.3.2 Ajout d'une description à une interface de VLAN

Il est possible d'ajouter une description à une interface de VLAN pour la distinguer des autres descriptions telles que "Interface du réseau de production" ou "Interface du réseau de gestion".

Pour ajouter une interface de VLAN, procédez comme suit :

1. Naviguez vers **Interfaces** ≫ **IP Interfaces**.
2. Sous **IP Interfaces**, , entrez dans **Description** une description pour l'interface sélectionnée. Condition :
   - Elle doit compter de 0 à 64 caractères
3. Validez la modification.

8.1.3.3 Configuration de la taille de la MTU

L'unité de transmission maximale (Maximum Transmission Unit, MTU) est la taille maximale d'une trame retranmissible par l'interface de VLAN. Les trames qui dépassent cette valeur limite, sont divisées en fragments plus petits, ce qui peut prolonger l'opération de transmission. Il est important de choisir une taille de MTU contribuant à l'optimisation des performances du réseau.

Pour paramétrer la taille de la MTU pour une interface de VLAN, procédez comme suit :

1. Naviguez vers **Interfaces** ≫ **IP Interfaces**.
2. Sous **IP Interfaces**, définissez dans **MTU Size** la taille de MTU pour l'interface sélectionnée. Condition :
   - Un nombre compris entre 68 et 1500

   Par défaut : 1500
3. Validez la modification.

8.1.3.4 Activation de notifications Link up/Link down

Des notifications SNMP d'évènements Link up et Link down peuvent être activées ou désactivées pour des interfaces de VLAN spécifiques. Si elles sont désactivées, les alarmes liées à ces évènements ne sont jamais déclenchées pour ces interfaces.

Les notifications de Link up et de Link down sont désactivées par défaut sur toutes les interfaces de VLAN.

Pour activer les notifications SNMP Link up et Link down sur une interface de VLAN, procédez comme suit :

1. Naviguez vers **Interfaces** ≫ **IP Interfaces**.
2. Sous **IP Interfaces**, modifiez **Link Up/Down Trap** en **Enable** pour l'l'interface sélectionnée.
3. Validez la modification.

8.1.3.5 Activation d'une interface de VLAN

Pour activer une interface de VLAN, procédez comme suit :

Remarque

Les interfaces de VLAN sont toutes activées par défaut.

1. Naviguez vers **Interfaces** ≫ **IP Interfaces**.
2. Sous **IP Interfaces**, modifiez **Interface State** en **Enable** pour l'l'interface sélectionnée.
3. Validez la modification.

8.1.4 Surveillance d'interfaces

Ce paragraphe décrit les diverses options de consultation des informations sur les interfaces disponibles.

8.1.4.1 Affichage de ports de pont

Pour afficher les configurations de ports de pont disponibles, naviguez vers **Interfaces** ≫ **Ethernet Interfaces** ≫ **Interfaces**.

Les informations suivantes sont affichées pour chaque port de pont :

Paramètres	Description
Interface	Le nom du port de pont au format : "{ Type }{ Emplacement }/{ Port : }". Exemple : • ethernet0/1 • extender0/1
Description	Description personnalisée facultative de l'interface
Link Up/Down Trap	Si activé (**enabled**), les évènements Link up ou Link down déclenchent des notifications SNMP.
Interface State	État administratif (ou configuré) de l'interface. Si activé (**enabled**), l'interface peut recevoir et retransmettre des données.

Paramètres	Description
Operational Status	État de fonctionnement de l'interface. Valeurs possibles : • **dormant** - L'interface est en attente d'actions externes • **down** - L'interface est hors service (down). • **lower-layer-down** - L'interface est, du fait de l'état de l'interface, niveau inférieur, hors service (down). • **not-present** – Un constituant fait défaut (un matériel p. ex.). • **testing** - L'interface est en cours de test. • **unknown** - Impossible de déterminer l'état courant. • **up** - L'interface est opérationnelle (up).
Auto-Negotiation	État de l'autonégociation du port de pont.
Speed	Vitesse paramétrée pour le port de pont.
Negotiated Speed	Vitesse maximale négociée entre le port de pont et son partenaire de liaison.
Duplex Mode	Mode duplex paramétré pour le port de pont.
Negotiation Duplex Mode	Mode duplex négocié entre le port de pont et son partenaire de liaison.
Downshift	État downshift paramétré pour le port de pont.

8.1.4.2 Affichage d'interfaces VLAN

Pour afficher les interfaces VLAN disponibles, naviguez vers **Interfaces** ≫ **IP Interfaces**.

Les informations suivantes peuvent être affichées pour chaque interface :

Paramètres	Description
Name	Le nom de l'interface au format "vlan{ VLAN-ID }". La valeur est en lecture seule.
Description	Description personnalisée facultative de l'interface La chaîne de caractères est limitée à 64 caractères.
Link Up/Down Trap	Si activé (**enable**), les évènements Link up ou Link down déclenchent des notifications SNMP.
MTU	Taille maximale de l'unité de transmission (MTU) de l'interface.
Interface State	État administratif (ou configuré) de l'interface. Si activé (**enable**), l'interface peut recevoir et retransmettre des données. La valeur est en lecture seule.

8.1.4.3 Affichage des statistiques d'émission/réception de toutes les interfaces

Pour afficher les statistiques de toutes les interfaces (p. ex. des ports de pont, VLAN, etc.), naviguez vers **Interfaces** ≫ **Interface Statistics**.

Les tableaux suivants s'affichent :

- **Interface Statistics (In)**
- **Interface Statistics (Out)**

Les informations suivantes peuvent être affichées pour chaque interface :

Statistiques	Description
Interface	Le nom de l'interface.
In Octets	Le nombre total d'octets de toutes les trames valides reçues par l'interface.
In Unicast (pkts)	Le nombre de trames unicast reçues avec succès par l'interface.
In Broadcast (pkts)	Le nombre de trames broadcast reçues avec succès par l'interface.
In Multicast (pkts)	Le nombre de trames multicast reçues avec succès par l'interface.
In Discards (pkts)	Le nombre de trames reçues par l'interface, mais rejetées en raison d'une surcharge de la file d'attente d'entrée.
In Errors (pkts)	Le nombre de trames non valides reçues par l'interface.
Out Octets	Le nombre total d'octets de toutes les trames valides retransmises par l'interface.
Out Octets (pkts)	Le nombre de trames unicast retransmises avec succès par l'interface.
Out Broadcast (pkts)	Le nombre de trames broadcast retransmises avec succès par l'interface.
Out Multicast (pkts)	Le nombre de trames multicast retransmises avec succès par l'interface.
Out Discards (pkts)	Le nombre de trames rejetées par l'interface en raison d'une surcharge de la file d'attente de sortie.
Out Errors (pkts)	Le nombre de trames non valides retransmises par l'interface.

8.1.4.4 Affichage des statistiques d'émission/réception des ports de pont uniquement

Pour afficher uniquement les statistiques collectées pour les ports de pont, naviguez vers **Interfaces** ≫ **Ethernet Interfaces** ≫ **Statistics**.

Les tableaux suivants s'affichent :

- **Interface Statistics (In)**
- **Interface Statistics (Out)**
- **Packet Size**

Les informations suivantes peuvent être affichées pour chaque interface :

Statistiques	Description
In Broadcast Frames	Le nombre de trames broadcast reçues avec succès par le port de pont.
In Error FCS Frames	Le nombre de trames reçues par le port de pont et dont la longueur est valide, mais qui n'ont pas passé le contrôle FCS (Frame Check Sequence).
In Error Oversize Frames	Le nombre de trames reçues par le port de pont qui sont plus grandes que la valeur maximale admissible (telle que spécifiée par **max-frame-length**).
In Error Undersize Frames	Le nombre de trames reçues par le port de pont, dont la longueur est inférieure à 64 octets.
In Errors	Le nombre de trames non valides reçues par le port de pont.
In Frames	Le nombre total des trames reçues avec succès par le port de pont.
In Multicast Frames	Le nombre de trames multicast reçues avec succès par le port de pont.
In Total Frames	Le nombre total des trames reçues avec succès par le port de pont (y compris les trames erronées).
In Total Octets	Le nombre total d'octets de données reçus avec succès par le port de pont (y compris les octets erronés).
In Unicast Frames	Le nombre de trames unicast reçues avec succès par le port de pont.
Out Broadcast Frames	Le nombre de trames broadcast émises avec succès par le port de pont.
Out Frames	Le nombre total des trames émises avec succès par le port de pont.
Out Multicast Frames	Le nombre de trames multicast émises avec succès par le port de pont.
Out Octets	Le nombre d'octets de données émis avec succès par le port de pont.
Out Unicast Frames	Le nombre de trames unicast émises avec succès par le port de pont.
64 Octets	Le nombre de paquets de 64 octets reçus et transmis, y compris les paquets perdus.
65 to 127 Octets	Le nombre de paquets de 65 à 127 octets reçus et transmis, y compris les paquets perdus.
128 to 255 Octets	Le nombre de paquets de 128 à 255 octets reçus et transmis, y compris les paquets perdus.
256 to 511 Octets	Le nombre de paquets de 256 à 511 octets reçus et transmis, y compris les paquets perdus.
512 to 1023 Octets	Le nombre de paquets de 512 à 1023 octets reçus et transmis, y compris les paquets perdus.
1024 to 1536 Octets	Le nombre de paquets de 1024 à 1536 octets reçus et transmis, y compris les paquets perdus.

8.1.4.5 Surveillance de convertisseurs de médias embrochables

Pour afficher l'état du CLP, naviguez vers **Interfaces** ≫ **Ethernet Interfaces** ≫ **SFP Diagnostics**.

Sous , l'écran affiche les informations suivantes :

Paramètres	Description
Model	Affiche le nom/type du convertisseur de médias embrochable.
Description	Affiche une description du convertisseur de médias embrochable.
Vendor (Name)	Affiche le constructeur du convertisseur de médias embrochable.
Article Number	Affiche le numéro d'article du convertisseur de médias embrochable.
Part Revision	Affiche la version matérielle du convertisseur de médias embrochable.
Speed	Affiche la vitesse de transmission à laquelle le port du convertisseur de médias embrochable envoie les trames. Valeurs possibles : • **Auto** – Les trames sont transmises à la vitesse déterminée par l'autonégociation. • **10 Mb/s** - Les trames sont transmises à 10 Mbit/s. • **100 Mb/s** - Les trames sont transmises à 100 Mbit/s. • **1 Gb/s** - Les trames sont transmises à 1 Gbit/s. • **2,5 Gb/s** - Les trames sont transmises à 2,5 Gbit/s. • **5 Gb/s** - Les trames sont transmises à 5 Gbit/s. • **10 Gb/s** - Les trames sont transmises à 10 Gbit/s.
Serial Number	Affiche le numéro de série du convertisseur de médias embrochable.
9um Max Link Length	Affiche la longueur de câble maximale en mètres (m) pour un diamètre du noyau de la fibre de 9 µm.
50um Max Link Length	Affiche la longueur de câble maximale en mètres (m) pour un diamètre du noyau de la fibre de 50 µm.
62um Max Link Length	Affiche la longueur de câble maximale en mètres (m) pour un diamètre du noyau de la fibre de 62,5 µm.
Temperatur (°C)	Affiche la température actuelle du convertisseur de médias embrochable en degrés Celsius (°C).
Rx-Power (dBm)	Affiche la valeur actuelle de la puissance de réception en décibels milliwatt (dBm).
Min Rx-Power (dBm)	Affiche la valeur minimale de la puissance de réception du convertisseur de médias embrochable en décibels milliwatt (dBm).
Max Rx-Power (dBm)	Affiche la valeur maximale de la puissance de réception du convertisseur de médias embrochable en décibels milliwatt (dBm).
Tx-Power (dBm)	Affiche la valeur actuelle de la puissance d'émission en décibels milliwatt (dBm).

Paramètres	Description
Min Tx-Power (dBm)	Affiche la valeur minimale de la puissance d'émission du convertisseur de médias embrochable en décibels milliwatt (dBm).
Max Tx-Power (dBm)	Affiche la valeur maximale de la puissance d'émission du convertisseur de médias embrochable en décibels milliwatt (dBm).

8.2 Table d'adresses MAC

SINEC OS gère une table d'adresses MAC, afin d'affecter efficacement les trames entrantes à leur destination.

8.2.1 Ce qu'il faut savoir sur la gestion de la table d'adresses MAC

La table d'adresses MAC (Media Access Control) est une liste interne d'adresses MAC des appareils du réseau. Elle permet à l'appareil de retransmettre efficacement les trames adressées à une adresse MAC spécifique, à l'interface voulue.

La table est constituée d'adresses MAC statiques (définies par l'utilisateur) et d'adresses apprises dynamiquement (que l'appareil a définies lui-même).

8.2.1.1 Entrées MAC dynamiques

Les entrées MAC dynamiques sont celles que l'appareil a apprises automatiquement pendant la réception des trames issues d'appareils hôtes du réseau et qu'il retransmet.

Vieillissement

Les entrées MAC dynamiques sont sujettes au vieillissement et sont automatiquement supprimées au bout d'un certain temps si l'hôte associé ne reçoit pas de trame avant écoulement de ce délai. Ceci permet de maintenir la table à jour.

Apprentissage de nouvelles entrées

Après un redémarrage, toutes les entrées dynamiques sont effacées et l'appareil attend la réception de trames. Lors de la réception et de la retransmission de trames, la table est reconstituée avec les adresses MAC des partenaires de liaison.

À titre d'illustration, imaginez la topologie suivante, dans laquelle les deux hôtes (A et B) retransmettent des données entre eux via le commutateur (SW).

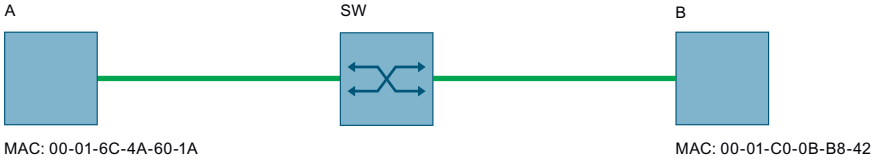


Figure 8-4 Apprentissage d'adresses MAC de deux hôtes

Le commutateur vient d'être redémarré

VIDS	MAC ADDRESS	TRAFFIC CLASS	ENTRY TYPE	FORWARDING PORT
%No entries found%				

Lorsque l'hôte A envoie une trame à l'hôte B, le commutateur apprend l'adresse MAC de l'hôte A et l'ajoute à sa liste.

VIDS	ADDRESS	TRAFFIC CLASS	ENTRY TYPE	FORWARDING PORT
1	00-01-6C-4A-60-1A	unprioritized	dynamic	ethernet0/1

Lorsque l'hôte B répond avec sa propre trame, le commutateur apprend également l'adresse MAC de cet hôte. En peu de temps, tous les appareils qui communiquent sur ce réseau sont ainsi ajoutés à la table d'adresses MAC du commutateur.

VIDS	ADDRESS	TRAFFIC CLASS	ENTRY TYPE	PORT REF
1	00-01-6C-4A-60-1A	unprioritized	dynamic	ethernet0/1
1	00-01-C0-0B-B8-42	unprioritized	dynamic	ethernet0/1

8.2.1.2 Entrées MAC statiques

Les entrées de filtre MAC statiques représentent des adresses MAC définies par l'utilisateur. Ces entrées représentent une affectation définie d'une adresse MAC à un VLAN. Les entrées statiques ne vieillissent pas et peuvent être supprimées individuellement par l'utilisateur.

8.2.2 Configuration de la table d'adresses MAC

Pour configurer comment et quand des adresses MAC sont effacées de la table d'adresses MAC, procédez comme suit :

1. [Facultatif] Définissez le délai de vieillissement.
   Le délai de vieillissement est la durée maximale de maintien d'une entrée dans la table d'adresses MAC jusqu'à son effacement automatique. Si une trame est reçue pour l'adresse MAC avant que la temporisation soit écoulée, la temporisation est remise à 0.
   Pour plus d'informations, voir "Configuration du délai de vieillissement pour adresses MAC (Page 180)".
2. [Facultatif] Activez sur l'appareil, la suppression automatique d'entrées (périmées), lorsqu'une défaillance de la liaison est détectée.
   Pour plus d'informations, voir "Activation du vieillissement d'adresse MAC en cas de défaillance de la liaison (Page 181)".

8.2.2.1 Configuration du délai de vieillissement pour adresses MAC

Les adresses MAC dynamiques apprises sont sujettes au vieillissement au bout d'un délai configurable. Dès que le délai configuré est écoulé, elles sont automatiquement supprimées de la table d'adresses MAC, à condition qu'aucune trame destinée à cette adresse MAC ne soit reçue avant l'écoulement du délai.

Pour configurer le délai de vieillissement des entrées d'adresse MAC, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **MAC Address Table** ≫ **MAC Address Table**.
2. Sous **Media Access Control (MAC) Address Table**, modifiez le paramètre **Aging Time** en temps que les adresses MAC apprises dynamiquement restent enregistrées dans la table d'adresses MAC.
   Conditions :
   - En format nYnMnDnhnmns, dans lequel n est un nombre personnalisé
   - 15 secondes min. (15s)
   - 13 Minutes max. (13m) soit 800 secondes (800s)

   Par défaut : 5m (5 minutes)
3. Validez la modification.

8.2.2.2 Activation du vieillissement d'adresse MAC en cas de défaillance de la liaison

Les adresses MAC dynamiques apprises peuvent être supprimées automatiquement en cas de défaillance de la liaison (vieillissement). On évite ainsi que le trafic de données d'un commutateur ne soit retransmis à un partenaire de liaison qui ne peut pas le recevoir.

Remarque

Le vieillissement des adresses MAC est activé par défaut, mais peut toutefois être désactivé dans certaines applications.

Pour configurer SINEC OS de sorte que les adresses MAC dynamiques apprises soient supprimées automatiquement lors de la détection d'une défaillance de la liaison, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **MAC Address Table** ≫ **MAC Address Table**.
2. Sous **Media Access Control (MAC) Address Table**, modifiez le paramètre **Age Out Upon Link Loss** en **Enabled**.
3. Validez la modification.

8.2.3 Configuration d'entrées de filtre MAC statiques

Pour configurer une entrée de filtre MAC statique, procédez comme suit :

1. Définissez une entrée de filtre MAC statique.
   Pour plus d'informations, voir "Ajout d'une entrée de filtre MAC statique (Page 182)".
2. [Facultatif] Affectez à l'entrée la file d'attente d'une classe de trafic.
   Tous les paramétrages de classe de trafic sont ainsi ignorés et toutes les trames destinées à l'adresse MAC deviennent prioritaires et sont retransmises à la file d'attente indiquée.
   Pour plus d'informations, voir "Affectation de la file d'attente à une classe de trafic. (Page 182)".

8.2.3.1 Ajout d'une entrée de filtre MAC statique

Par la configuration d'une entrée de filtre MAC statique, une adresse MAC est ajoutée à la table d'adresses MAC. Les adresses MAC statiques ajoutées ne sont pas sujettes au vieillissement. Elles ne peuvent être supprimées de la table que par une action explicite de l'utilisateur.

Ajoutez, pour les adresses MAC importantes des entrées de filtre MAC statiques qui doivent y rester, à la table des adresses MAC.

Remarque

Vous pouvez ajouter à la table d'adresses MAC au maximum 256 entrées de filtre MAC statiques.

Remarque

Les adresses MAC suivantes ne sont pas admissibles :

- Adresses MAC nulles
- Adresse MAC broadcast
- Adresses MAC réservées
- Adresses MAC de routeurs virtuels
- La propre adresse MAC de l'appareil

Pour ajouter une entrée de filtre MAC statique, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **MAC Address Table** ≫ **Static**.
2. Sous **Media Access Control (MAC) Address Table (Static Entries)**, cliquez sur **Add**. Une nouvelle ligne est insérée dans le tableau.
3. Sous **VLAN ID**, sélectionnez un VLAN existant pour l'affecter à l'adresse MAC.
4. Saisissez l'adresse MAC sous **MAC Address**.
5. Sous **Forwarding Port**, sélectionnez un port de pont. Cette entrée permet de retransmettre des trames concordantes à ce port de pont.
6. Validez les modifications.

Exemple

On ajoute ci-après une entrée et **ethernet0/1** est sélectionné comme port de retransmission.

VLAN ID	MAC Address	Traffic Class	Forwarding Port
10	3A:34:52:C4:69:B8 b8:e6:45:c6:87:9b	Unprioritized	ethernet0/1

8.2.3.2 Affectation de la file d'attente à une classe de trafic.

Si une entrée de filtre MAC statique est affectée à une classe de trafic, les paramètres de la classe de trafic pour l'interface de retransmission sont tous écrasés. Chaque trame adressée à l'adresse MAC devient automatiquement prioritaire et est retransmise à la file d'attente de la classe de trafic indiquée.

Pour affecter à une entrée de filtre MAC la file d'attente d'une classe de trafic, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **MAC Address Table** ≫ **Static**.
2. Sous **Media Access Control (MAC) Address Table (Static Entries)**, sélectionnez dans **Traffic Class** la file d'attente d'une classe de trafic pou l'entrée de filtre MAC statique sélectionnée.
   Options disponibles :
   - **0 - 7** - File d'attente d'une classe de trafic.
   - **Unprioritized** - Pas de file d'attente affectée à une classe de trafic.

   Par défaut : **Unprioritized**
3. Validez la modification.

Exemple

Dans ce qui suit, on affecte la file d'attente 7 à une entrée statique.

VLAN ID	MAC Address	Traffic Class	Forwarding Port
10	b8:e6:45:c6:87:9b	7	ethernet0/4

8.2.4 Surveillance de la table d'adresses MAC

Ce paragraphe décrit les différentes manières d'afficher et de gérer la table d'adresses MAC.

8.2.4.1 Affichage de la table d'adresses MAC

Pour afficher la table d'adresses MAC, naviguez vers **Layer 2** ≫ **MAC Address Table** ≫ **MAC Address Table**.

Exemple

VLAN ID	MAC Address	Traffic Class	Forwarding Port	Entry Type
1	00:01:6C:4A:60:1A	Unprioritized	ethernet0/1	Dynamic
10	3A:34:52:C4:69:B8	7	ethernet0/1	Static
2	00:01:C0:0B:B8:42	Unprioritized	ethernet0/1	Dynamic

Description

Sous **Media Access Control (MAC) Address Table**, les informations suivantes sont affichées pour chaque entrée :

Paramètres	Description
VLAN ID	VID de VLAN affecté à l'adresse MAC
MAC Address	L'adresse MAC

Paramètres	Description
Traffic Class	La file d'attente d'une classe de trafic affectée à l'adresse MAC. Valeurs possibles : • **0 – 7** - Fle d'attente d'une classe de trafic • **Unprioritized** - Pas de file d'attente affectée à une classe de trafic.
Forwarding Port	Le port de sortie de retransmission affecté à l'adresse MAC. Les trames concordant à l'entrée de l'adresse MAC sont retransmises par cette interface.
Entry Type	Type d'entrée. Valeurs possibles : • **Static** – L'adresse MAC statique a été ajoutée par un utilisateur. • **Dynamic** – L'adresse MAC a été apprise dynamiquement.

8.2.4.2 Suppression d'adresses MAC dynamiques

Si nécessaire, vous pouvez effacer de la table d'adresse MAC toutes les adresses apprises dynamiquement. La table est immédiatement reconstituée lorsque l'appareil recommence à recevoir des trames.

Pour supprimer toutes les adresses MAC apprises dynamiquement de la table d'adresses MAC, exécutez la commande suivante :

1. Naviguez vers **Layer 2** ≫ **MAC Address Table** ≫ **MAC Address Table**.
2. Sous **Purge Dynamic Entries**, cliquez sur **Purge**.

Attribution d'adresses IP

9

Ce chapitre décrit des fonctions liées à l'attribution d'adresses IP, telles que DHCP et DNS.

9.1 Attribution d'adresses IP statiques

Les adresses IP peuvent être attribuées statiquement (manuellement) à une interface IP. Ceci est utile pour les interfaces IP qui doivent toujours être joignables à la même adresse IP.

Pour configurer une adresse IPv4 statique, procédez comme suit :

1. Vérifiez qu'une interface IP a été configurée.
   Pour plus d'informations, voir "VLAN (Page 245)".
2. Configurez une adresse IPv4 statique.
   Pour plus d'informations, voir "Configuration d'une adresse IPv4 statique (Page 185)".

9.1.1 Configuration d'une adresse IPv4 statique

Pour configurer une adresse IPv4 statique, procédez comme suit :

1. Naviguez vers **Interfaces** ≫ **IP Interfaces**.
2. Vérifiez que l'interface IP à laquelle vous voulez attribuer une adresse IPv4 statique a été configurée comme suit :
   - Sous **IP Interfaces** sélectionnez pour le paramètre **DHCP** l'option **Disabled**.
3. Sous **IPv4 Static Addresses**, cliquez sur **Add**.
   Une nouvelle ligne est insérée dans le tableau.
4. Sous **Interface**, sélectionnez une interface IP.
   Vous ne pouvez éditer l'interface IP qu'immédiatement après avoir ajouté une nouvelle ligne. Dès que le champ n'est plus actif, l'interface IP passe en lecture seule. Si vous voulez modifier l'interface IP, supprimez l'entrée et configurez-la à nouveau.
5. Sous **IP Address**, saisissez une adresse IPv4.
   Vous ne pouvez éditer l'adresse IP qu'immédiatement après avoir ajouté une nouvelle ligne. Dès que le champ n'est plus actif, l'adresse IP passe en lecture seule. Si vous voulez modifier l'adresse IP, supprimez l'entrée et configurez-la à nouveau.
6. Sous **Prefix Length**, entrez le préfixe.
7. Validez les modifications.

9.1.2 Affichage de la configuration d'adresses IPv4

Pour afficher la table d'adresses IPv4, naviguez vers **Interfaces** ≫ **IP Interfaces**.

Sous **IPv4 Static Addresses**, l'écran affiche les informations suivantes :

Paramètres	Description
Interface	ID de VLAN de l'interface IP
IP Address	Adresse IP de l'interface IP
Prefix Length	Sous-réseau représenté comme longueur de préfixe

9.2 DNS statique

Ce paragraphe décrit comment configurer un appareil pour qu'avec des configurations sélectionnées il soit possible d'indiquer le nom de l'hôte ou du domaine au lieu de l'adresse IP (p. ex. pour Ping et Traceroute).

9.2.1 Ce qu'il faut savoir sur DNS

Domain Name System (DNS) est un système de bases de données distribuées dans lequel il est possible d'attribuer un nom de domaine à une adresse IP. Le service DNS convertit un nom de domaine en une adresse IP et inversement. Dans le DNS statique, une adresse IP est affectée durablement à un nom de domaine. Si l'adresse IP change, il n'est plus possible d'établir une connexion avec le nom de domaine et la destination n'est plus joignable.

DNS utilise pour le transfert UDP et TCP sur le port 53.

9.2.1.1 Terminologie de base de DNS

Le tableau suivant explique la terminologie de base de DNS.

Terme	Signification
Nom de domaine	Le nom de domaine possède une structure hiérarchique et se compose de plusieurs niveaux. Les différents niveaux représentent les éléments du nom et sont reliés par des points. Un nom de domaine se lit de droite à gauche. Un nom de domaine complet est désigné par le terme de Fully Qualified Domain Name (FQDN). Il décrit une position exacte dans la hiérarchie du DNS, en indiquant tous les niveaux, ou pour le moins le second niveau (second level) et le premier niveau (top level). Exemple : www.industry.siemens.com Dans cet exemple, "com" correspond au niveau supérieur "siemens" au second niveau. "industry"Constitue un domaine de sous-niveau tandis que "www" est le nom d'hôte.
Domaine	Un domaine désigne une zone contiguë du DNS. Un domaine comprend tous les hôtes regroupés sous un nom de domaine commun. Un domaine situé en dessous d'un autre dans la hiérarchie est appelé un sous-domaine. Les sous-domaines sont utilisés pour le regroupement logique et peuvent être gérés par différents serveurs DNS.

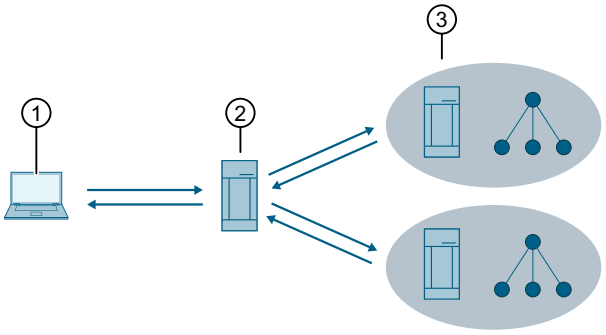
Terme	Signification
Zone	Une zone est une partie du DNS qui est gérée par un serveur DNS. Une zone peut comprendre un domaine entier avec des sous-domaines, mais aussi des sous-domaines distincts.
Serveur DNS	Un serveur DNS ou serveur de noms dispose d'informations qui permettent de résoudre un nom de domaine en une adresse IP. Un serveur DNS peut fournir les informations d'une ou de plusieurs zones DNS : • Un serveur DNS autoritatif fournit lui-même des données d'une ou plusieurs zones. • Un serveur DNS récursif obtient ses informations d'autres serveurs DNS.
Serveur racine	Les serveurs racines ou serveurs de noms racines constituent le niveau supérieur du DNS et donc le point de départ de la structure hiérarchique. Les serveurs racines répondent aux requêtes concernant les serveurs DNS du domaine de premier niveau (TLD, Top-Level-Domain).
Résolveur DNS	Un résolveur DNS est un programme qui fait office d'interface entre les clients DNS et les serveurs DNS. Il résout une requête client en rassemblant les informations recherchées sur les serveurs DNS et en les transmettant au client. Pour que le résolveur DNS puisse fonctionner, il a besoin de l'adresse IP d'au moins un serveur DNS.
Domaine de recherche	Un domaine de recherche est utilisé pour éviter de devoir saisir manuellement l'adresse des domaines fréquemment utilisés. Les domaines de recherche que vous configurez sont automatiquement ajoutés aux noms que vous saisissez. Les résolveurs DNS utilisent des domaines de recherche pour créer un FQDN à partir des noms de domaine relatifs saisis.
Client DNS	On appelle client DNS l'interface d'application du DNS. Le client DNS envoie ses requêtes DNS à un résolveur DNS. Lorsque vous configurez un serveur DNS pour un client DNS, il s'agit d'un résolveur DNS.

9.2.1.2 Communication DNS

Un client DNS qui veut résoudre un nom de domaine en une adresse IP envoie une requête à un résolveur DNS. Le résolveur DNS soit transmet la demande à un autre résolveur DNS qu'il connaît, soit résout la demande en interrogeant les différents niveaux de la hiérarchie DNS.

Par exemple, si le nom de domaine www.industry.siemens.com doit être résolu, le résolveur DNS demande à un serveur racine le serveur DNS du domaine de premier niveau com. Au serveur DNS du domaine de premier niveau, le résolveur DNS demande à son tour le serveur DNS du niveau hiérarchique suivant siemens.com. Selon ce principe, le résolveur DNS interroge tous les niveaux du nom de domaine jusqu'à ce que la requête soit résolue ou qu'une erreur se produise, par exemple parce qu'un domaine de sous-niveau ne peut pas être résolu ou que le serveur DNS responsable ne répond pas.

Si un nom de domaine ne peut pas être résolu, aucune connexion ne peut être établie avec l'hôte concerné.



① Client DNS
② Résolveur DNS
③ Serveurs DNS autoritatifs

Figure 9-1 Communication DNS

9.2.2 Configuration d'un DNS

Pour configurer un DNS, procédez comme suit :

1. Configurez au moins un serveur DNS.
   Pour plus d'informations, voir "Configuration d'un serveur DNS (Page 188)".
2. [Facultatif] Configurez un domaine de recherche.
   Pour plus d'informations, voir "Configuration d'un domaine de recherche (Page 189)".

9.2.2.1 Configuration d'un serveur DNS

Plusieurs serveurs DNS peuvent être enregistrés sur l'appareil. Un indice est attribué aux serveurs DNS dans l'ordre dans lequel ils sont créés. En présence de plusieurs serveurs DNS, l'indice détermine dans quel ordre les serveurs sont interrogés. Le serveur possédant le plus petit indice est interrogé en premier. Les serveurs DNS configurés manuellement sont préconisés.

Pour configurer un Serveur DNS, procédez comme suit :

1. Naviguez vers **System** ≫ **DNS Client**.
2. Sous **DNS Servers (Static)**, cliquez sur **Add**.
   Une nouvelle ligne est insérée dans le tableau.
3. Sous **Name**, entrez le nom du serveur DNS.
   Vous ne pouvez éditer le nom qu'immédiatement après l'avoir saisi dans la nouvelle ligne. Dès que le champ n'est plus actif, le nom passe en lecture seule. Si vous voulez modifier le nom, supprimez le serveur DNS et configurez-le à nouveau.
4. Sous **Server Address**, entrez l'adresse IP du serveur DNS.
5. Validez les modifications.

9.2.2.2 Configuration d'un domaine de recherche

Plusieurs domaines de recherche peuvent être enregistrés sur l'appareil. Ces domaines font l'objet d'une recherche lors de la résolution d'un nom de domaine. Un indice est attribué aux domaines de recherche dans l'ordre dans lequel ils ont été créés ou appris. En présence de plusieurs domaines de recherche, l'indice définit l'ordre dans lequel ils sont consultés. Le domaine de recherche possédant le plus petit indice est interrogé en premier.

Si des domaines de recherche sont enregistrés, vous avez la possibilité d'entrer dans certains champs d'adresse IP le nom de domaine.

Pour créer un domaine de recherche, procédez comme suit :

1. Naviguez vers **System** ≫ **DNS Client**.
2. Sous **Domain Search List (Static)**, cliquez sur **Add**.
   Une nouvelle ligne est insérée dans le tableau.
3. Sous **Domain Name**, entrez le nom du domaine de recherche.
   Condition :
   – Il doit compter de 1 à 251 caractères.
4. Validez les modifications.

9.2.3 Affichage de la configuration DNS

Pour afficher la configuration DNS, naviguez vers **System** ≫ **DNS Client**.

Sous **Domain Name System (DNS) Information**, l'écran affiche les informations suivantes :

Paramètres	Description
Origin	Indique comment le serveur DNS a été ajouté. Options disponibles : • **static** - Le serveur DNS a été ajouté manuellement. • **dynamic** - Le serveur DNS a été appris dynamiquement.

Sous **DNS Servers**, l'écran affiche les informations suivantes :

Paramètres	Description
Server Address	Affiche l'adresse IP du serveur DNS configuré.

Sous **Domain Search List**, l'écran affiche les informations suivantes :

Paramètres	Description
Domain Name	Affiche les domaines de recherche configurés.

9.3 DHCP

Cette section décrit comment configurer un appareil pour qu'il obtienne sa configuration IP d'un serveur DHCP.

9.3.1 Configuration de l'appareil comme client DHCP.

IMPORTANT
Risque de configuration - Risque de défaillance des communications Chaque fois que vous modifiez un paramètre de configuration du client DHCP, le client DHCP est redémarré. Pendant le redémarrage, la communication IP avec l'interface de gestion de l'appareil est brièvement interrompue, car l'appareil obtient à nouveau son adresse IP. Cela peut entraîner de brèves pannes de communication sur le réseau.

Pour configurer l'appareil comme client DHCP, procédez comme suit :

1. Activez l'interface de client DHCP.
   Pour plus d'informations, voir "Activation d'une interface de client DHCP (Page 190)".
2. [Facultatif] Paramétrez une durée de validité.
   Pour plus d'informations, voir "Demande d'une durée de validité (Page 190)".
3. [Facultatif] Modifiez l'ID de client d'une interface de client DHCP.
   Pour plus d'informations, voir "Modification de l'ID de client d'une interface (Page 191)".
4. [Facultatif] Activez l'utilisation du nom d'hôte.
   Pour plus d'informations, voir "Utilisation du nom d'hôte dans les notifications DHCP. (Page 192)".

9.3.1.1 Activation d'une interface de client DHCP

Par défaut, toutes les interfaces de client DHCP sont désactivées. Exception : Pour le VLAN 1, le DHCP est activé par défaut.

Pour activer une interface de client DHCP, procédez comme suit :

1. Naviguez vers **Interfaces** ≫ **IP Interfaces**.
2. Sous **IP Interfaces**, modifiez le paramètre **DHCP** en **Enabled**.
3. Validez la modification.

9.3.1.2 Demande d'une durée de validité

La durée de validité indique combien de temps l'adresse IP attribuée par le serveur DHCP reste valable. La durée de validité demandée par le client peut être acceptée ou ignorée par le serveur.

Par défaut, le client DHCP ne demande pas de durée de validité.

Pour paramétrer une durée de validité, procédez comme suit :

1. Naviguez vers **Interfaces** ≫ **IP Interfaces**.
2. Sous **Dynamic Host Configuration Protocol (DHCPv4) Client** , définissez dans la colonne **Lease Time Requested [s]** la durée de validité qu'une interface de client DHCP demande au serveur DHCP.
   Conditions :
   - En format nYnMnDnhnmns, dans lequel n est un nombre personnalisé
   - 2 minutes minimum (2m)
   - Max. 136 ans 2 mois 9 jours 10 heures 28 minutes 15 secondes (136Y2M9D10h28m15s)
3. Validez la modification.

9.3.1.3 Modification de l'ID de client d'une interface

Pour modifier l'ID de client d'une interface DHCP, procédez comme suit :

1. Naviguez vers **Interfaces** ≫ **IP Interfaces**.
2. Sous **Dynamic Host Configuration Protocol (DHCPv4) Client**, modifiez dans la colonne **Client ID** l'ID de client d'une interface de client DHCP.
   Options disponibles :

Option	Description
MAC Address	**Par défaut** Le client DHCP s'identifie avec son adresse MAC auprès du serveur DHCP.
Hostname	Le client DHCP s'identifie avec son nom d'hôte auprès du serveur DHCP. Pour plus d'informations, voir "Modification du nom d'hôte (Page 69)".
Name of Station	Le client DHCP s'identifie avec son nom d'appareil PROFINET auprès du serveur DHCP.
Select or add new...	Le client DHCP s'identifie avec un ID personnalisé. Cliquez sur le champ **Client ID** et saisissez un ID personnalisé. Conditions : • Il doit compter de 1 à 152 caractères. • Tous les caractères standard ainsi que les caractères spéciaux suivants sont autorisés : _ - . : < = > @ ( )

3. Validez la modification.

9.3.1.4 Utilisation du nom d'hôte dans les notifications DHCP.

Si vous activez cette option, le nom d'hôte du client DHCP sera utilisé dans la communication avec le serveur DHCP. Le serveur DHCP enregistre le nom d'hôte ainsi que l'adresse IP attribuée et peut utiliser ces informations de la manière suivante :

- pour identifier le client DHCP
- pour retransmettre l'affectation à un serveur DNS

Par défaut, le nom d'hôte n'est pas indiqué dans les notifications DHCP.

Pour utiliser le nom d'hôte du client DHCP dans les notifications DHCP, procédez comme suit :

1. Naviguez vers **Interfaces** ≫ **IP Interfaces**.
2. Sous **Dynamic Host Configuration Protocol (DHCPv4) Client**, modifiez le paramètre **Send Hostname** en **Enabled**.
3. Validez la modification.

9.3.2 Affichage de données de configuration d'interfaces de client DHCP

Pour afficher les données de configuration d'interface de client DHCP, naviguez vers **Interfaces** ≫ **IP Interfaces**.

Sous **IP Interfaces**, l'écran affiche les informations suivantes :

Paramètres	Description
Interface	ID de VLAN de l'interface de client DHCP
DHCP	Indique si le client DHCP est activé pour l'interface précitée.

Sous **Dynamic Host Configuration Protocol (DHCP4) Client**, l'écran affiche les informations suivantes de l'interface active du client DHCP :

Paramètres	Description
Interface	ID de VLAN de l'interface de client DHCP
IP Address Granted	Adresse IPv4 de l'interface
Prefix Length	Sous-réseau représenté comme longueur de préfixe
Lease Time Granted [s]	Durée de validité en Format nYnMnDnhnmns, que le serveur DHCP a attribuée.
Lease Time Requested [s]	Durée de validité en Format nYnMnDnhnmns, que le client DHCP a demandée au serveur DHCP.
Client ID	ID du client DHCP avec lequel il se connecte au serveur DHCP
Hostname	Si vous activez cette option, le nom d'hôte du client DHCP sera utilisé dans la communication avec le serveur DHCP.

Redondance de réseaux 10

Ce chapitre décrit les fonctions de redondance de réseau disponibles. La redondance de réseau constitue un mécanisme de protection du réseau évitant les interruptions de service pouvant résulter d'une défaillance ponctuelle.

10.1 Spanning Tree Protocol (STP)

SINEC OS prend en charge la norme IEEE 802.1Q:2014 qui inclut le protocole Rapid Spanning Tree (RSTP) et le protocole Multiple Rapid Spanning Tree (RSTP). Tous deux sont des protocoles de redondance de réseau supprimant des chemins redondants afin d'éviter la formation de boucles dans le réseau.

La configuration de STP s'effectue via la CLI. Pour plus d'informations, voir le **Manuel de configuration SINEC OS CLI**.

10.2 Détection de boucles de réseau

Ce paragraphe décrit comment utiliser et configurer la fonction de détection et de résolution de boucles de réseau (Loop Detection).

10.2.1 Ce qu'il faut savoir sur la détection de boucles de réseau

La détection de boucles de réseau (Loop Detection) est un protocole propriétaire. L'utilisation principale de cette fonction est de détecter les boucles de réseau et de limiter leurs effets.

Les boucles de réseau sont des erreurs de conception d'un réseau. Elles se produisent lorsque deux ports de pont du même appareil sont interconnectés ou lorsqu'il existe au moins deux connexions actives entre deux appareils qui ne sont pas gérées par un protocole (Spanning Tree p. ex.). Un câblage défectueux peut en être la cause, par exemple lors de la mise en service et de l'entretien d'une installation.

Dans le cas d'une boucle de réseau, des trames qui tournent en boucle se forment et sont dupliquées à l'infini, inondant ainsi le réseau. En raison des boucles, les trames de diffusion peuvent donner lieu à une tempête de broadcast en quelques secondes. L'augmentation du nombre de trames entraîne une surcharge du réseau et donc une interruption du trafic de données. En raison de la charge élevée du réseau, un diagnostic est également fortement limité.

Pour détecter les boucles de réseau, les ports de pont configurés de manière appropriée envoient de manière cyclique des Protocol Data Units (PDU) à une adresse multicast prédéfinie. Si le même appareil reçoit à nouveau une PDU envoyée, il existe une boucle.

Vous pouvez configurer la manière dont la détection de boucle réagit à une boucle de réseau détectée et comment elle est signalée. Par défaut, la fonction désactive le port de pont qui envoie les PDU et signale la boucle comme suit :

- L'évènement est enregistré dans le journal système.
- Le contact de signalisation est déclenché.
- La LED d'alarme s'allume.

Si une boucle de réseau se produit, le réseau doit être contrôlé par un administrateur réseau. Les boucles de réseau peuvent être résolues, par exemple, en modifiant la topologie, en adaptant le câblage ou en désactivant les ports de pont.

10.2.1.1 Modes de port

Lorsque la détection de boucle est activée, vous pouvez configurer les modes suivants pour les ports de pont :

- **Mode sending**
  Le port de pont envoie des PDU et retransmet des PDU.
  Pour détecter une boucle de réseau, un appareil doit lui-même envoyer des PDU. Configurez donc pour au moins un port de pont de l'appareil le paramètre **sending**.
  Notez que les PDU qui détectent les boucles de réseau génèrent une charge de réseau supplémentaire. Sélectionnez soigneusement les ports de pont qui envoient des PDU, par exemple aux embranchements d'un anneau (P1 dans l'exemple ci-dessous).
- **Mode forwarding**
  Le port de pont retransmet uniquement des PDU.
  Les boucles ne peuvent être détectées qu'entre les ports de pont qui retransmettent au moins les PDU. Configurez par conséquent pour d'autres ports de pont le paramètre **forwarding** (P 2 dans l'exemple ci-après).
- **Mode blocking**
  Le port de pont n'envoie pas de PDU et ne retransmet pas de PDU.
  Si les PDU interfèrent avec le trafic de données, configurez pour les ports de pont concernés le paramètre **blocking**. Par exemple :
  - Pour les segments de réseau adjacents dans lesquels la détection de boucle n'est pas activée (P3 dans l'exemple ci-dessous)
  - Pour les terminaux connectés (P4 dans l'exemple ci-dessous)

L'exemple suivant montre un commutateur et les différents modes de port de la détection de boucle :

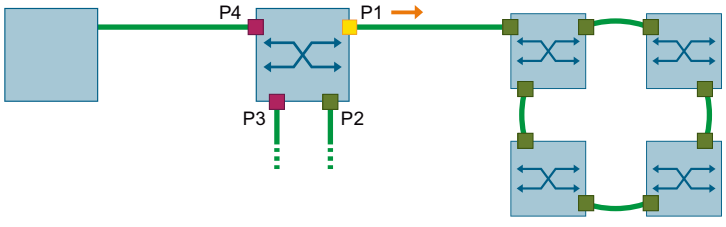


Figure 10-1 Modes de port de la détection de boucle

10.2.1.2 Types de boucles de réseau

La détection de boucles distingue les types de boucles suivants :

- **Boucle de réseau locale**
  Si un appareil reçoit à nouveau une PDU envoyée sur un autre port de pont, il existe une boucle locale.

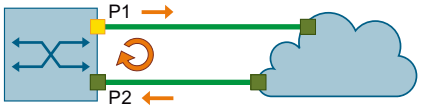


Figure 10-2 Boucle de réseau locale

La détection de boucle peut interrompre une boucle locale en désactivant le port de pont qui a envoyé la PDU.

- **Boucle de réseau distante**
  Si un appareil reçoit à nouveau une PDU envoyée sur le même port de pont, il existe une boucle à distance.

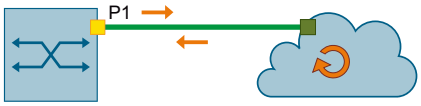


Figure 10-3 Boucle de réseau distante

La détection de boucle ne peut pas interrompre une boucle distante, mais peut limiter ses effets négatifs. En désactivant le port de pont de l'appareil, cette fonction empêche les segments de réseau connectés d'être inondés par les trames tournant en boucle.

10.2.1.3 Mode VLAN

Lors de la détection de boucles de réseau, seul le niveau physique est considéré par défaut. Dans un réseau avec une configuration de VLAN, il peut arriver que la détection de boucle détecte des boucles physiques qui ne mettent cependant pas en danger le trafic de données. Les ports de pont concernés peuvent être séparés logiquement par une configuration VLAN.

Lorsque le mode VLAN est activé, la fonction prend en compte la configuration VLAN des ports de pont lors du traitement des PDU. Pour un appareil qui reçoit à nouveau une PDU envoyée, la fonction ne détecte une boucle que si la PDU a été envoyée et reçue sur le même VLAN.

10.2.1.4 Évènements associés

Les évènements suivants sont déclenchés par la détection de boucles et sont enregistrés directement dans Syslog.

Évènement	Niveau de gravité	Message Syslog
Local loop detected	Error	"Loop Detection" has detected a local loop.
Remote loop detected	Error	"Loop Detection" has detected a remote loop.

10.2.2 Configuration de la détection de boucles de réseau

Remarque

Utilisez cette fonction en particulier dans les segments de réseau dans lesquels aucun Spanning Tree n'est configuré et dans lesquels les abonnés du réseau ne transmettent pas les PDU de pont Spanning Tree.

Remarque

La détection des boucles réseau ne remplace pas d'autres fonctions telles que le Spanning Tree ou les protocoles de redondance.

Remarque

La fonction est basée sur l'interface et peut être configurée pour des ports de pont individuels ou groupés.

Pour configurer la détection de boucles de réseau, procédez comme suit :

1. Configurer la manière dont un port de pont traite les PDU pour détecter les boucles de réseau.
   Pour plus d'informations, voir "Configuration de ports de pont pour la détection de boucles de réseau (Page 197)".
2. [Facultatif] Configurer l'intervalle auquel un port de pont envoie des PDU.
   Pour plus d'informations, voir "Configuration de l'intervalle d'émission (Page 197)".
3. [Facultatif] Définissez au bout de combien de PDU reçues la fonction détecte une boucle de réseau local.
   Pour plus d'informations, voir "Définition de la valeur limite de détection d'une boucle de réseau locale (Page 198)".
4. [Facultatif] Configurez l'impact sur un port de pont lorsqu'une boucle de réseau local est détectée.
   Pour plus d'informations, voir "Configuration de la réaction à une boucle de réseau locale (Page 198)".
5. [Facultatif] Configurez l'impact sur un port de pont lorsqu'une boucle de réseau distante est détectée.
   Pour plus d'informations, voir "Configuration de la réaction à une boucle de réseau distante (Page 199)".
6. [Facultatif] Définissez la durée en secondes pendant laquelle un port de pont est désactivé lorsqu'une boucle est détectée sur le réseau.
   Pour plus d'informations, voir "Configuration de la durée de désactivation d'un port de pont (Page 200)".
7. Activez la prise en compte de la configuration VLAN d'un port de pont.
   Pour plus d'informations, voir "Activation du mode VLAN (Page 201)".

8. Activez la détection de boucles de réseau.
   Pour plus d'informations, voir "Activation de la détection de boucles de réseau (Page 201)".
9. [Facultatif] Réinitialiser manuellement un port de pont après avoir supprimé une boucle sur le réseau.
   Pour plus d'informations, voir "Réinitialisation manuelle d'un port de pont après détection d'une boucle de réseau (Page 202)".

10.2.2.1 Configuration de ports de pont pour la détection de boucles de réseau

Tenez compte lors de la configuration des ports de pont de la structure du réseau. Pour plus d'informations, voir "Modes de port (Page 194)".

Pour configurer la manière dont un port de pont traite les PDU pour détecter les boucles de réseau, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Loop Detection**.
2. Sous **Loop Detection**, configurez le paramètre **Transmission State** pour un port de pont. Options disponibles :

Option	Description
Forwarding	**Par défaut** Le port de pont retransmet uniquement des PDU.
Sending	Le port de pont envoie des PDU et retransmet des PDU.
Blocking	Le port de pont n'envoie pas de PDU et ne retransmet pas de PDU.

3. Validez la modification.

10.2.2.2 Configuration de l'intervalle d'émission

L'intervalle d'émission définit le délai qui s'écoule entre la transmission de PDU successives pour la détection de boucles de réseau.

L'intervalle n'est appliqué que lorsque l'envoi et la retransmission de PDU ont été configurés pour un port de pont (paramètre Sending). Pour plus d'informations, voir "Configuration de ports de pont pour la détection de boucles de réseau (Page 197)".

Pour configurer l'intervalle d'émission de PDU, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Loop Detection**.
2. Sous **Loop Detection**, configurez le paramètre **Transmission Interval** pour un port de pont. Conditions :
   - Formaté nYnMnDnhnmns, dans lequel n est un nombre personnalisé
   - Min. 0,5 seconde (0.5s)
   - Max. 5 secondes (5s)

   Par défaut : 1s (1 seconde)
3. Validez la modification.

10.2.2.3 Définition de la valeur limite de détection d'une boucle de réseau locale

Pour détecter une boucle de réseau, un port de pont doit recevoir un nombre défini de PDU consécutives qu'il a lui-même envoyées.

Pour les boucles de réseau locales, vous pouvez configurer cette valeur limite. Une boucle de réseau distante est détectée dès qu'un port de pont reçoit la première PDU qu'il a lui-même envoyée.

Il est conseillé de faire varier la valeur limite pour les appareils d'un même réseau. Dans le cas d'une topologie arborescente, il est préférable d'attribuer aux appareils de haut en bas une valeur limite décroissante. Avec cette configuration, les appareils locaux (③ dans le graphique) réagissent en premier et désactivent de manière ciblée un port de pont avant que les appareils superposés (② ou ①) ne déconnectent une cellule entière.

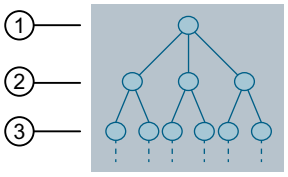


Figure 10-4 Topologie arborescente

Pour définir la valeur limite de détection d'une boucle de réseau, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Loop Detection**.
2. Sous **Loop Detection**, configurez le paramètre **Threshold** pour un port de pont.
   Condition :
   – Un nombre compris entre 1 et 500

   Par défaut : 2
3. Validez la modification.

10.2.2.4 Configuration de la réaction à une boucle de réseau locale

Une boucle de réseau locale est détectée lorsque le nombre de PDU reçues sur un port de pont dépasse la valeur limite.

Pour configurer les réactions à une boucle de réseau locale sur un port de pont, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Loop Detection**.
2. Sous **Loop Detection**, configurez le paramètre **Local Reaction** pour un port de pont. Options disponibles :

Option	Description
Disable Interface	**Par défaut** - Dès que la fonction détecte une boucle de réseau locale, elle désactive le port de pont. La boucle de réseau est interrompue. Les options suivantes permettent de réactiver le port de pont : • Réinitialisez manuellement le port de pont. Pour plus d'informations, voir "Réinitialisation manuelle d'un port de pont après détection d'une boucle de réseau (Page 202)". • Si un évènement de Link down se produit sur un port de pont désactivé, la fonction réinitialise le port de pont dans l'état dans lequel il se trouvait avant la boucle de réseau. • La temporisation de la désactivation d'un port de pont est écoulée. Pour plus d'informations, voir "Configuration de la durée de désactivation d'un port de pont (Page 200)".
No Reaction	Une boucle de réseau n'a pas d'effet sur le port de pont.

3. Validez la modification.

10.2.2.5 Configuration de la réaction à une boucle de réseau distante

Une boucle de réseau distante est détectée dès qu'un port de pont reçoit la première PDU qu'il a lui-même envoyée.

Pour configurer les réactions à une boucle de réseau distante, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Loop Detection**.
2. Sous **Loop Detection**, configurez le paramètre **Remote Reaction** pour un port de pont. Options disponibles :

Option	Description
Disable Interface	**Par défaut** Dès que la fonction détecte une boucle de réseau distante, elle désactive le port de pont. La boucle de réseau n'est pas interrompue pour autant, mais les segments de réseau connectés ne sont pas inondés par les trames qui tournent en boucle. Les options suivantes permettent de réactiver le port de pont : • Réinitialisez manuellement le port de pont. Pour plus d'informations, voir "Réinitialisation manuelle d'un port de pont après détection d'une boucle de réseau (Page 202)". • Si un évènement de Link down se produit sur un port de pont désactivé, la fonction réinitialise le port de pont dans l'état dans lequel il se trouvait avant la boucle de réseau. • La temporisation de la désactivation d'un port de pont est écoulée. Pour plus d'informations, voir "Configuration de la durée de désactivation d'un port de pont (Page 200)".
No Reaction	Une boucle de réseau distante n'a pas d'effet sur le port de pont.

3. Validez la modification.

10.2.2.6 Configuration de la durée de désactivation d'un port de pont

Des boucles de réseau temporaires peuvent survenir, notamment lors de la mise en service ou de la maintenance d'une installation. Si la fonction désactive un port de pont dès qu'une boucle est détectée, vous pouvez utiliser ce paramètre pour définir la durée pendant laquelle le port de pont reste désactivé. La détection de boucle attend la durée configurée et remet le port du pont dans l'état où il se trouvait avant la désactivation.

Si la boucle de réseau persiste, le réseau doit être vérifié par un administrateur réseau.

Vous ne pouvez configurer le timeout que si un port de pont est configuré pour être désactivé à la fois en cas de boucle de réseau locale et de boucle distante.

Pour configurer la durée de désactivation d'un port de pont, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Loop Detection**.
2. Vérifiez que le port de pont pour lequel vous voulez configurer le timeout, a été configuré comme suit :
   - Sous **Loop Detection**, sélectionnez pour le paramètre **Local Reaction** l'option **Disable Interface**.
     Le port de pont est désactivé en cas de boucle de réseau locale.
     Pour plus d'informations, voir "Configuration de la réaction à une boucle de réseau locale (Page 198)".
   - Sous **Loop Detection**, sélectionnez pour le paramètre **Remote Reaction** l'option **Disable Interface**.
     Le port de pont est désactivé en cas de boucle de réseau distante.
     Pour plus d'informations, voir "Configuration de la réaction à une boucle de réseau distante (Page 199)".
3. Sous **Loop Detection** , configurez le paramètre **Reaction Timeout** pour le port de pont voulu.
   Une fois la temporisation écoulée, le port de pont est réactivé.
   Si la valeur configurée est **0s**, le port de pont n'est pas réactivé automatiquement. Contrôlez le réseau et réactivez le port de pont manuellement. Pour plus d'informations, voir "Réinitialisation manuelle d'un port de pont après détection d'une boucle de réseau (Page 202)".
   Conditions :
   - Formaté nYnMnDnhnmns, dans lequel n est un nombre personnalisé
   - Min. 0 seconde (0s)
   - Max. 86400 secondes (86400s)

   Par défaut : 0 seconde (0s)
4. Validez la modification.

10.2.2.7 Activation du mode VLAN

Activez le mode VLAN pour prendre en compte la configuration VLAN du port de pont lors du traitement des PDU. Si le mode VLAN est activé, une seule boucle est détectée lorsque l'appareil reçoit sa propre PDU, envoyée et reçue sur le même VLAN.

Par défaut, le mode VLAN est désactivé.

Pour activer le mode VLAN pour tous les ports de pont de la détection de boucles, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Loop Detection**.
2. Sous **Loop Detection** , modifiez le paramètre **VLAN Loop Detection** en **Enabled**.
3. Validez la modification.

10.2.2.8 Activation de la détection de boucles de réseau

Par défaut, la détection des boucles réseau est désactivée pour tous les ports de pont.

Pour activer la détection de boucles de réseau pour tous les ports de pont, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Loop Detection**.
2. Sous **Loop Detection** , modifiez le paramètre **Loop Detection** en **Enabled**.
3. Validez la modification.

10.2.2.9 Réinitialisation manuelle d'un port de pont après détection d'une boucle de réseau

Si l'appareil ne réinitialise pas automatiquement un port de pont après la détection d'une boucle de réseau, vous pouvez le réinitialiser manuellement à l'état où il se trouvait avant la boucle de réseau.

Pour réinitialiser un port de pont manuellement, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Loop Detection**.
2. Cliquez dans la dernière colonne sur **Reset** pour réinitialiser un port de pont manuellement.

10.2.3 Affichage de l'état de la détection de boucles

Pour afficher l'état de la détection de boucles, naviguez vers **Layer 2** ≫ **Loop Detection**.

Sous **Loop Detection**, l'écran affiche les informations suivantes :

Paramètres	Description
Operational State	Affiche l'état de fonctionnement de la détection de boucles. Options disponibles : • **disabled** - Cet état de fonctionnement signifie : – La détection de boucles est activée et le port de pont n'émet pas de PDU. – La détection de boucles est activée, mais le port de pont est à l'état Link down. • **active** - La détection de boucles est activée. Des PDU sont émises ou retransmises sur ce port de pont. • **detected-local-loop** - La détection de boucles a détecté une boucle de réseau locale. • **detected-remote-loop** - La détection de boucles a détecté une boucle de réseau distante.
Ingress Interface	Le port de pont qui a reçu une propre PDU En cas de boucle de réseau distante, ce paramètre n'est pas affiché. L'appareil reçoit sa propre PDU sur le port du pont pour lequel l'état est affiché.
Ingress VLAN ID	L'ID de VLAN du port de pont sur lequel la propre PDU a été reçue Ce paramètre est uniquement affiché si le mode VLAN est activé.

10.3 Device Level Ring

Device Level Ring (DLR) est une procédure redondante de couche 2 pour EtherNet/IP. Elle permet de réaliser des topologies en anneau avec EtherNet/IP. En cas d'interruption de la chaîne de communication, la communication est maintenue via un chemin redondant.

DLR offre les avantages suivants :

- Redondance de supports
- Une erreur isolée dans la chaîne de communication n'entraîne pas une restriction de l'accessibilité de certains abonnés.
- Détection rapide des erreurs et reconfiguration après l'apparition d'une seule erreur

Remarque

Le présent document ne fournit pas une description exhaustive de DLR. Pour plus d'informations sur DLR, voir le site Internet Open DeviceNet Vendor Association (ODVA) (https://www.odva.org/).

10.3.1 Ce qu'il faut savoir sur DLR

Dans un réseau DLR, chaque nœud de réseau possède l'un des rôles suivants :

- Superviseur de l'anneau
- Nœud d'anneau

Chaque nœud de réseau est intégré dans le réseau via 2 ports Ethernet. Il en résulte une topologie en anneau dans laquelle chaque nœud est connecté à 2 nœuds voisins distincts. Pour éviter les boucles de réseau, un nœud de réseau (le superviseur d'anneau actif) bloque l'un de ses ports DLR.

10.3.1.1 Superviseur de l'anneau

DLR fait la distinction entre les superviseurs actifs et les superviseurs d'anneau de secours :

- **Superviseur d'anneau actif**
  Un superviseur d'anneau actif assure les fonctions suivantes :
  - il gère le réseau DLR
  - il émet régulièrement des trames de balises et d'annonces
    un superviseur d'anneau doit être capable d'émettre et de traiter des trames de balise à un intervalle d'émission par défaut de 400 µs.
  - il surveille en permanence l'état du réseau DLR
  - il détecte les erreurs sur le réseau DLR
  - il collecte les informations de diagnostic sur le réseau DLR
- **Superviseur d'anneau de secours**
  En cas de défaillance du superviseur d'anneau actif, le superviseur d'anneau de secours se charge de la gestion du réseau DLR.
  En tant que superviseur d'anneau de secours, l'appareil se comporte comme un nœud d'anneau basé sur des balises.

Dans un réseau DLR, il doit y avoir un superviseur d'anneau actif. Les superviseurs d'anneau de secours sont recommandés, mais pas nécessaires.

Une priorité est configurée pour chaque superviseur d'anneau. Le superviseur d'anneau avec la valeur de priorité la plus élevée agit comme superviseur d'anneau actif. Si 2 superviseurs d'anneau ont la même valeur de priorité, le superviseur d'anneau avec l'adresse MAC numériquement la plus élevée devient le superviseur d'anneau actif. Tous les autres superviseurs d'anneau deviennent alors des superviseurs d'anneau de secours.

10.3.1.2 Nœud d'anneau

Les nœuds de réseau sans propriétés de superviseur sont classés comme suit :

- **Nœuds d'anneau basés sur des balises**
  Un nœud d'anneau basé sur des balises assure les fonctions suivantes :
  - Il traite les trames de balises pour suivre l'état du réseau DLR
  - Il doit être assisté par un matériel approprié pour qu'il ne soit pas nécessaire de traiter les trames de balises dans la CPU.
  - Il retransmet les trames d'annonces.
  - Il apprend, en cas d'erreur, la nouvelle topologie de réseau
  - Il informe le superviseur de l'anneau des erreurs sur le DLR
- **Nœuds d'anneau basés sur des annonces**
  Un nœud d'anneau basé sur des annonces assure les fonctions suivantes :
  - Il retransmet les trames de balises.
  - Il traite les trames d'annonces pour suivre l'état du réseau DLR
  - Il apprend, en cas d'erreur, la nouvelle topologie de réseau
  - Il informe le superviseur de l'anneau des erreurs sur le DLR

Remarque

Les appareils SINEC OS peuvent uniquement être utilisés comme nœuds d'anneau basés sur des annonces.

10.3.1.3 Trames DLR

Les trames de balises et d'annonces sont toutes deux utilisées pour informer les nœuds d'anneau de l'état actuel du réseau DLR.

Les deux types de trames se distinguent comme suit :

- **Trames de balises**
  - Par défaut, le superviseur d'anneau envoie des trames de balise avec un intervalle d'émission de 400 µs.
  - Le superviseur d'anneau envoie des trames de balise via les deux ports DLR.
  - Les trames de balises contiennent la valeur de priorité du superviseur d'anneau qui a envoyé la trame.
  - La perte de trames de balises permet au superviseur d'anneau de détecter les erreurs dans le réseau DLR.
- **Trames d'annonces**
  - Le superviseur d'anneau envoie des trames d'annonces par défaut avec un intervalle d'envoi de 1 s ou immédiatement lorsqu'une erreur est détectée.
  - Le superviseur d'anneau envoie des trames d'annonces uniquement via un de ses ports DLR.

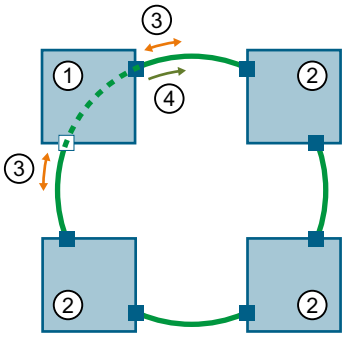
Remarque

En raison des intervalles d'émission différents, les réseaux DLR avec des nœuds d'anneau basés sur les annonces ont des temps de rétablissement plus longs que ceux avec des nœuds d'anneau basés sur les balises.

10.3.1.4 Réseau DLR

DLR distingue les états suivants :

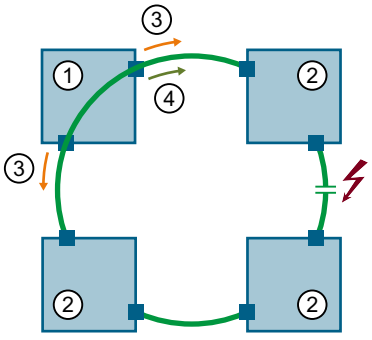
- **État normal**
  Le réseau DLR est à l'état normal lorsque le superviseur d'anneau actif a bloqué un de ses ports DLR. Dans cet état, le superviseur d'anneau actif envoie des trames de balises et d'annonces (également via le port DLR bloqué) afin de surveiller l'état du réseau DLR. Tous les autres nœuds d'anneau traitent les trames en fonction de leurs capacités.
  Tant que le superviseur d'anneau actif reçoit à nouveau ses trames de balises envoyées, tous les chemins de communication du réseau DLR sont intacts.



① Superviseur d'anneau actif
② Nœud d'anneau
③ Trames de balises
④ Trames d'annonces

Figure 10-5 Réseau DLR à l'état normal

- **Défaut**
  Si la chaîne de communication est interrompue à un endroit, par exemple en raison d'une coupure de la ligne ou de la défaillance d'un abonné, les trames de balises n'arrivent plus au superviseur d'anneau actif. Le superviseur d'anneau active son port DLR bloqué et donc le chemin de communication alternatif. Il informe les nœuds de l'erreur. Les nœuds d'anneau apprennent le nouveau chemin de communication. Le réseau DLR est à l'état d'erreur.
  Dès que la reconfiguration est terminée, la communication entre tous les nœuds du réseau est à nouveau possible.



① Superviseur d'anneau actif
② Nœud d'anneau
③ Trames de balises
④ Trames d'annonces

Figure 10-6 Réseau DLR à l'état d'erreur

10.3.2 Configuration du DLR

Pour configurer le DLR, procédez comme suit :

1. Activez EtherNet/IP.
   Pour plus d'informations, voir "Activation d'EtherNet/IP (Page 230)".
2. Ajoutez un VLAN statique pour DLR.
   Pour plus d'informations, voir "Ajout ou édition d'un VLAN statique (Page 254)".
3. Configurez les ports que vous voulez utiliser comme ports de DLR comme ports de jonction.
   Pour plus d'informations, voir "Sélection du type d'affiliation du port (Page 256)".
4. [Facultatif] Assurez-vous que les ports que vous souhaitez utiliser comme ports DLR sont des membres balisés du VLAN DLR.
   Cette configuration n'est nécessaire que si le VLAN DLR correspond au VLAN natif des ports d'anneau DLR.
   Pour plus d'informations, voir "Activation du balisage PVID pour le trafic de données sortant (Page 257)".
5. Désactivez STP sur les ports que vous souhaitez utiliser comme ports DLR.
   Pour plus d'informations, voir "Spanning Tree Protocol (STP) (Page 193)".
6. Sélectionnez le VLAN DLR.
   Pour plus d'informations, voir "Sélection du VLAN DLR (Page 208)".
7. Sélectionnez les ports DLR.
   Pour plus d'informations, voir "Sélection des ports DLR (Page 209)".
8. Activez le DLR.
   Pour plus d'informations, voir "Activation de DLR (Page 209)".

10.3.2.1 Sélection du VLAN DLR

Pour sélectionner le VLAN sur lequel des trames DLR sont émises, procédez comme suit :

1. Veuillez vous assurer que le VLAN voulu a été configuré pour DLR.
   Pour plus d'informations sur l'ajout d'un VLAN statique, voir "Ajout ou édition d'un VLAN statique (Page 254)".
2. Naviguez vers **System** ≫ **EtherNet/IP & DLR**.
3. Sous **EtherNet/IP**, sélectionnez dans **DLR VLAN ID** le VLAN pour le DLR.
4. Validez la modification.

10.3.2.2 Sélection des ports DLR

Pour sélectionner les ports DLR, procédez comme suit :

1. Assurez-vous que les deux ports que vous souhaitez utiliser comme ports DLR sont configurés comme ports de jonction.
   Pour plus d'informations sur le type d'affiliation des ports, voir "Sélection du type d'affiliation du port (Page 256)".
2. [Facultatif] Assurez-vous que les ports que vous souhaitez utiliser comme ports DLR sont des membres balisés du VLAN DLR.
   Cette configuration n'est nécessaire que si le VLAN DLR correspond au VLAN natif des ports d'anneau DLR.
   Pour plus d'informations sur le type d'affiliation des ports, voir "Activation du balisage PVID pour le trafic de données sortant (Page 257)".
3. Veuillez vous assurer que STP est désactivé sur les ports que vous souhaitez utiliser comme ports DLR.
   Pour plus d'informations sur la configuration de STP pour un port de pont, voir "Spanning Tree Protocol (STP) (Page 193)".
4. Naviguez vers **System** ≫ **EtherNet/IP & DLR**.
5. Sous **EtherNet/IP**, sélectionnez dans **DLR Port 1** le premier port DLR.
6. Dans **DLR Port 2**, sélectionnez le deuxième port DLR.
7. Validez les modifications.

10.3.2.3 Activation de DLR

DLR est désactivé par défaut.

Pour activer DLR, procédez comme suit :

1. Naviguez vers **System** ≫ **EtherNet/IP & DLR**.
2. Sous **EtherNet/IP**, modifiez le paramètre **DLR** en **Enabled**.
3. Validez la modification.

10.3.3 Surveillance de DLR

Naviguez vers **System** ≫ **EtherNet/IP & DLR** pour surveiller un réseau DLR.

Sous **Device Level Ring** , l'écran affiche les informations suivantes :

Paramètres	Description
Supervisor IP Address	Affiche l'adresse IP du superviseur d'anneau actif.
Supervisor MAC Address	Affiche l'adresse MAC du superviseur d'anneau actif.

Paramètres	Description
Ring Topology	Affiche la topologie courante du réseau DLR. Valeurs possibles : • **linear** - La topologie **linear** signifie qu'un nœud de l'anneau n'est pas connecté au superviseur d'anneau actif et ne reçoit pas de trames du superviseur. L'appareil se trouve encore ou à nouveau à l'état (Node State) **idle**. • **ring** - La topologie **ring** signifie qu'un nœud de l'anneau se trouve à l'état (Node State) **normal** ou **fault**, c.-à-d. qu'il reçoit des trames du superviseur. L'appareil a au moins une connexion au superviseur d'anneau actif.
Ring State	Signale que l'anneau est ouvert ou fermé. Valeurs possibles : • **normal** - Le superviseur d'anneau actif a bloqué l'un de ses ports DLR. La communication au sein du réseau fonctionne dans une topologie linéaire. • **fault** - Le superviseur d'anneau actif a activé son port bloqué. La communication au sein du réseau est reconfigurée vers un autre chemin de communication.
Node State	Indique l'état interne d'un nœud d'anneau basé sur les annonces (appareil SINEC OS). Valeurs possibles : • **idle** - État initial de l'appareil. L'appareil passe à l'état **idle** lorsqu'il ne reçoit pas de trames d'annonces. • **fault** - L'appareil est à l'état **fault** lorsqu'une erreur est détectée dans le réseau. • **normal** - L'appareil est à l'état **normal** lorsqu'une communication sur le réseau est possible avec tous les nœuds du réseau.
Network Status	Affiche l'état courant du réseau DLR. Valeurs possibles : • **normal** - La communication entre tous les nœuds du réseau est possible. • **ring fault** - Une erreur a été détectée sur le réseau.
Ring Port 1 Status	Affiche l'état courant du port DLR 1. Valeurs possibles : • **up** - L'interface est activée. • **down** - L'interface est désactivée.
Ring Port 2 Status	Affiche l'état courant du port DLR 2. Valeurs possibles : • **up** - L'interface est activée. • **down** - L'interface est désactivée.

10.3.4 Exemples de configuration

Vous trouverez ci-après des exemples de mise en œuvre du DLR.

10.3.4.1 Utilisation du DLR dans le VLAN 0

Comme les trames balisées avec un ID de VLAN 0 sont traitées séparément, il est possible de faire fonctionner un anneau au-delà des limites du VLAN. Les abonnés de l'anneau peuvent être membres de différents VLAN.

Pour configurer un appareil SINEC OS de manière à ce qu'il puisse participer à un DLR dans le VLAN 0, procédez comme suit :

1. [Facultatif] Assurez-vous que les ports que vous souhaitez utiliser comme ports de DLR sont configurés comme ports d'accès.
   Pour plus d'informations, voir "Sélection du type d'affiliation du port (Page 256)".
2. Désactivez STP sur les ports que vous souhaitez utiliser comme ports DLR.
   Pour plus d'informations, voir "Spanning Tree Protocol (STP) (Page 193)".
3. Configurez EtherNet/IP.
   Pour plus d'informations, voir "Configuration d'EtherNet/IP (Page 230)".
4. Sélectionnez les ports DLR.
   Pour plus d'informations, voir "Sélection des ports DLR (Page 209)".
5. Configurez le même VLAN natif pour les deux ports de DLR.
   Pour plus d'informations, voir "Configuration de l'ID de VLAN du port (Page 256)".
6. Activer le mode tunnel VLAN-0 pour le VLAN natif des ports de DLR.
   Pour plus d'informations, voir "Activation du mode de tunnel VLAN 0 (Page 255)".
7. Activez le DLR.
   Pour plus d'informations, voir "Activation de DLR (Page 209)".
8. Vérifiez qu'**aucun** VLAN DLR n'est configuré.
   Pour plus d'informations, voir "Sélection du VLAN DLR (Page 208)".

Découverte et gestion de réseau 11

Ce chapitre décrit les différentes fonctions disponibles pour la détection et la gestion du réseau. Ces fonctions permettent d'assurer la détection automatique des appareils sur le réseau ainsi que la surveillance du réseau et la gestion automatique des appareils.

11.1 LLDP

Le protocole Link Layer Discovery Protocol (LLDP) permet de saisir la topologie de réseaux locaux. Les informations sur la topologie et les connexions physiques entre les constituants du réseau sont la condition préalable à la gestion des réseaux locaux.

11.1.1 Configuration de l'émission et de la réception de LLDPDU pour un port de pont

Pour configurer la manière dont un port de pont traite les PDU pour détecter les boucles de réseau, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Network Discovery** ≫ **LLDP**.
2. Sous **LLDP Interfaces**, configurez le paramètre **Local Settings** pour un port de pont. Options disponibles :

Option	Description
Receive and Transmit	**Par défaut** Des LLDPDU sont émises et reçues sur le port de pont.
Disabled	Aucune LLDPDU n'est émise ni reçue sur le port de pont.
Receive	Des LLDPDU sont reçues, mais pas émises sur le port de pont.
Transmit	Des LLDPDU sont émises, mais pas reçues sur le port de pont.

3. Validez la modification.

11.1.2 Surveillance des informations LLDP des appareils voisins

Pour afficher les informations LLDP des appareils voisins, naviguez vers **Layer 2** ≫ **Network Discovery** ≫ **LLDP**.

Si des appareils voisins prenant en charge LLDP sont connectés, les informations suivantes s'affichent sous **Link Layer Discovery Protocol (LLDP) Neighbors** :

Paramètres	Description
Local Interface	Port sur lequel les informations de l'appareil connecté ont été reçues
Remote System Name	Nom de système de l'appareil connecté
Remote Device ID	Identificateur de l'appareil connecté L'ID correspond au nom d'appareil attribué sous SINEC PNI (STEP 7). Si aucun nom d'appareil n'a été attribué, c'est l'adresse MAC de l'appareil qui est affichée.
Remote Hold Time	Durée formatée nYnMnDnhnmns, pendant laquelle les informations LLDP de l'appareil connecté sont enregistrées avant d'être effacées par l'appareil
Remote Capability	Propriétés qui sont activées sur l'appareil connecté
Remote Port ID	Port de l'appareil connecté

11.2 DCP

SINEC OS prend en charge le protocole Discovery and basic Configuration Protocol (DCP) pour la découverte d'appareils et la configuration de paramètres de réseau de base.

11.2.1 Ce qu'il faut savoir sur DCP

DCP est utilisé dans l'environnement PROFINET pour attribuer des paramètres de base aux appareils, p. ex. l'adresse IP ou le nom d'appareil PROFINET. DCP est utilisé typiquement par les contrôleurs PROFINET ou les outils d'ingénierie (p. ex. SINEC PNI, STEP 7) pour trouver et configurer les appareils. DCP ne peut pas être routé et est limité au réseau local de couche 2.

11.2.2 Configuration de DCP

Pour configurer DCP, procédez comme suit :

1. Configurez les droits d'accès de DCP.
   Pour plus d'informations, voir "Configuration des droits d'accès de DCP (Page 215)".
2. Configurer si les trames DCP peuvent être envoyées depuis un port de pont.
   Pour plus d'informations, voir "Configuration de l'envoi de trames DCP pour un port de pont (Page 216)".

11.2.2.1 Configuration des droits d'accès de DCP

IMPORTANT

Vulnérabilité - risque d'intrusion et/ou d'utilisation abusive

Par définition, lDCP n'est pas sûr. Les droits d'accès de DCP dépendent de l'état de l'appareil.

- DCP est activé à la livraison et après la restauration des paramètres par défaut. Les paramètres d'appareil peuvent être lus et édités. Les droits d'accès de DCP correspondent à l'option **Read-Write**.
  Le paramétrage **Read-Write** peut être potentiellement utilisé pour modifier les fonctions de l'appareil et provoquer ainsi une défaillance du trafic de données. Des utilisateurs malveillants, se trouvant dans le même segment de réseau local, peuvent modifier sans authentification les paramètres IP et/ou le nom d'appareil PROFINET.
- Après la première connexion avec le profil d'utilisateur **admin** prédéfini et l'attribution d'un nouveau mot de passe, l'appareil passe à l'état de fonctionnement sécurisé. À l'état de fonctionnement sécurisé, les droits d'accès de DCP sont automatiquement modifiés en accès en lecture seule. Les paramètres de l'appareil sont alors uniquement accessibles en lecture seule, mais ne peuvent pas être édités. Les droits d'accès de DCP correspondent à partir de cet instant à l'option **Read-Only**.

Pour éviter tout accès non autorisé et/ou abus, configurez pour DCP des droits d'accès en lecture seule (**Read-Only**).

IMPORTANT

Risque de configuration - Risque de coupure de liaison

Si vous utilisez l'appareil en mode PROFINET avec l'option DCP `read-only`, vous risquez de perdre des connexions.

Comme un contrôleur PROFINET ne définit par défaut l'adresse IP que temporairement, l'appareil peut perdre son adresse IP en cas de perte de tension (démarrage à froid) ou de redémarrage (démarrage à chaud). Sans adresse IP, l'appareil n'est accessible que par une connexion série.

Pour définir l'adresse IP de manière rémanente, afin qu'elle soit conservée après un démarrage à froid ou à chaud, vous avez les possibilités suivantes :

- Attribuez l'adresse IP manuellement.
- Configurez pour l'appareil, avec un outil d'ingénierie (STEP 7 ou TIA Portal) le mode **Démarrage priorisé**.

Pour configurer les droits d'accès de DCP, procédez comme suit :

1. Naviguez vers **System** ≫ **PROFINET** ≫ **DCP**.
2. Configurez sous **Discovery and basic Configuration Protocol (DCP)**, dans le champ **DCP Mode**, les droits d'accès de DCP.
   Options disponibles :

Option	Description
Read-Write	**Par défaut** DCP est activé. Les paramètres d'appareil peuvent être lus et édités. Les paramètres IP et/ou le nom d'appareil PROFINET peuvent être édités ou réinitialisés. Veuillez noter que les droits d'accès de DCP changent après la première connexion avec le profil utilisateur prédéfini **admin** et l'attribution d'un nouveau mot de passe et deviennent un accès en lecture seule (**Read-Only**).
Read-Only	DCP est activé. Les paramètres d'appareil peuvent être lus, mais pas édités. L'appareil ne réagit pas aux commandes DCP en écriture. Ainsi, il n'est pas possible d'attribuer de nouveaux paramètres via un outil d'ingénierie, p. ex. L'appareil proprement dit est visible. Si vous avez configuré cette option et que vous souhaitez utiliser l'appareil comme appareil PROFINET, les paramétrages suivants doivent correspondre à ceux du contrôleur : • Adresse IP • Masque de sous-réseau • Adresse de passerelle • Nom d'appareil PROFINET Si les paramètres concordent, l'affectation de DCP n'est pas nécessaire. La communication via PROFINET est possible.
Off	DCP est désactivé. Les paramètres d'appareil ne peuvent être ni lus ni édités. Avec ce réglage, l'appareil ne peut pas être utilisé comme appareil PROFINET.

3. Validez la modification.

11.2.2.2 Configuration de l'envoi de trames DCP pour un port de pont

Il n'est pas possible de désactiver la réception de trames DCP. Vous pouvez configurer l'envoi de trames DCP par le port de pont.

Par défaut, tous les ports du pont envoient et reçoivent des trames DCP.

Pour configurer l'envoi ou non de trames DCP pour un port de pont, procédez comme suit :

1. Naviguez vers **System** ≫ **PROFINET** ≫ **DCP**.
2. Configurez sous **DCP Forwarding** dans la colonne **Forwarding Mode** l'envoi ou non de trames DCP pour un port de pont.
   Options disponibles :

Option	Description
Receive and Transmit	**Par défaut** Ce port envoie et reçoit des trames DCP.
Receive	Ce port reçoit des trames DCP mais n'en envoie pas.

3. Validez la modification.

11.3 PROFINET

PROFINET (Process Field Network) est un standard Ethernet ouvert pour l'automatisation industrielle. PROFINET utilise les normes informatiques existantes et permet une communication continue du niveau terrain au niveau conduite ainsi qu'une ingénierie à l'échelle de l'installation.

PROFINET est mis en œuvre comme suit :

- La communication entre les appareils de terrain est mise en œuvre avec PROFINET IO.
- La technique d'installation et les constituants de réseau sont disponibles en tant que produits SIMATIC NET.
- Les protocoles et procédures de la norme Ethernet sont utilisés pour la maintenance à distance et le diagnostic du réseau (p. ex. SNMP pour le paramétrage et le diagnostic du réseau).

Avec PROFINET, le commutateur IE peut être configuré par un contrôleur PROFINET et échanger des données de diagnostic.

Remarque

Le présent document ne fournit pas une description exhaustive de PROFINET. Vous trouverez de plus amples informations sur PROFINET comme suit :

- Vous trouverez une compilation des exemples d'application PROFINET les plus importants, des FAQ et d'autres contributions dans Industry Online Support dans ces FAQ (https://support.industry.siemens.com/cs/ww/fr/view/108165711).
- Sur le site Internet (http://www.profibus.com) de l'association des utilisateurs de PROFIBUS "PROFIBUS & PROFINET International" également compétente pour PROFINET.
- Pour plus d'informations, voir le Site web Siemens (http://www.siemens.com/profinet).

11.3.1 Ce qu'il faut savoir sur PROFINET

PROFINET, en tant que norme d'automatisation basée sur Ethernet de PROFIBUS International, définit un modèle de communication, d'automatisation et d'ingénierie interconstructeur.

PROFINET est particulièrement adapté aux systèmes d'automatisation industriels et aux réseaux de conduite des processus dans lesquels le contrôle des mouvements et la commande précise des appareils et des équipements de test sont importants.

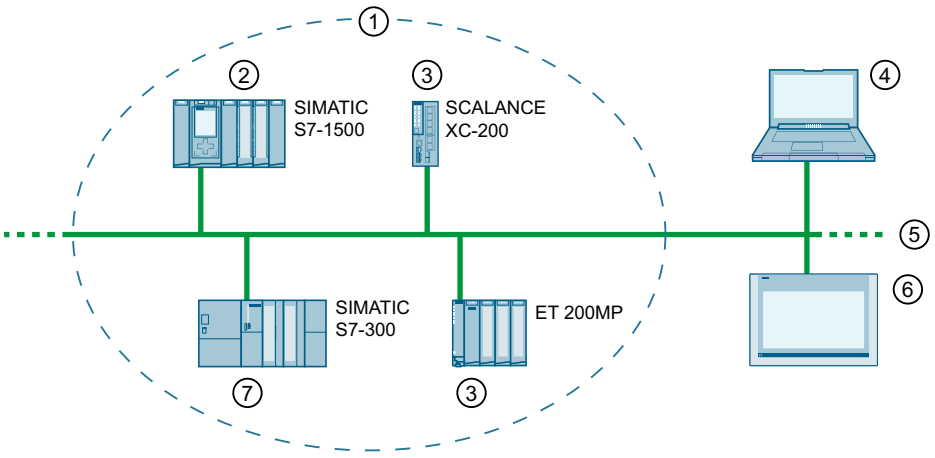
Propriétés de PROFINET

- Norme Ethernet ouverte basée sur Industrial Ethernet (CEI 61918 et aussi CEI 61158/61784)
- Compatibilité entre constituants Industrial Ethernet et Ethernet standard
- Communication continue du niveau terrain jusqu'au niveau conduite ainsi qu'une ingénierie à l'échelle de l'installation
- Grande robustesse grâce à des appareils Industrial Ethernet adaptés à l'environnement industriel (température, immunité aux interférences, etc.)
- Utilisation de TCP/IP et de normes des NTIC
- Compatibilité temps réel
- Intégration sans faille d'autres systèmes de bus de terrain
- Satisfait à des exigences élevées en matière de sécurité, de fiabilité et de disponibilité

11.3.1.1 Constituants PROFINET

Un appareil PROFINET possède toujours une interface PROFINET (électrique, optique, sans fil).

La figure ci-après donne un aperçu des principaux constituants PROFINET :



	Constituants PROFINET	Description
①	Système PROFINET IO	-
②	Contrôleur PROFINET	Appareil qui permet d'adresser des appareils PROFINET connectés. Cela signifie : Le contrôleur PROFINET échange des signaux d'entrée et de sortie avec des appareils de terrain. Le contrôleur PROFINET est l'automate sur lequel le programme d'automatisation est exécuté.
③	Appareil PROFINET	Appareil de terrain décentralisé affecté à un contrôleur PROFINET, p. ex. Distributed IO, terminaux de distributeurs, convertisseurs de fréquence, commutateurs avec fonctionnalité PROFINET IO intégrée
④	PG/PC (Superviseur PROFINET IO)	PG/PC/appareil IHM pour la mise en service et le diagnostic
⑤	PROFINET/Industrial Ethernet	Infrastructure de réseau
⑥	IHM (interface homme-machine)	Appareil de conduite et supervision
⑦	Appareil intelligent	Appareil IO intelligent

Figure 11-1 Constituants PROFINET

11.3.1.2 Adressage d'appareil

Chaque appareil PROFINET est clairement identifiable dans le réseau par son interface PROFINET. Pour cela, chaque interface PROFINET possède :

- **Une adresse MAC** (paramètre par défaut)
  - Chaque abonné Ethernet en possède une et elle est unique dans le monde entier.
  - Est utilisée sous PROFINET comme adresse source/cible pour l'échange cyclique de données.
  - Elle est peu pratique pour la désignation de l'appareil, car elle n'est pas modifiable.
- **Une adresse IP**
  - Est attribuée librement par le configurateur et sert à l'échange acyclique de données. Il s'agit notamment du transfert de projet vers la CPU, de la configuration de l'appareil par la CPU, de la lecture d'informations sur l'appareil (p. ex. la version du firmware) ou de la lecture d'informations de diagnostic.
  - Pour ces services, PROFINET utilise le protocole User Datagramm (UDP). Celui-ci travaille sur la couche 4 et a donc besoin d'une adresse IP comme base.
  - Elle est inscrite dans les appareils par la CPU lors du démarrage du système.
- **Un nom d'appareil PROFINET**
  - Nécessaire lors du démarrage du système. La CPU recherche les appareils à l'aide du nom dl'appareil PROFINET.
  - Offre un grand confort, car il est facilement modifiable.
  - Permet le remplacement d'un appareil sans nouvelle configuration du matériel. En comparaison, il faudrait adapter l'adresse MAC dans la configuration du matériel.
  - Peut être attribué manuellement ou automatiquement (baptême).

11.3.1.3 Communication PROFINET

La communication PROFINET se fait via Industrial Ethernet. Elle prend en charge les modes de transfert suivants :

- Transmission acyclique de données d'ingénierie et de diagnostic ainsi que d'alarmes
- Transmission cyclique des données utiles

Les communications industrielles, notamment dans l'automatisation de la production et des process, exigent une transmission de données en temps voulu (temps réel) et déterministe. Le temps réel signifie qu'un système traite des évènements externes dans un temps donné. Si la réaction est prévisible (déterministe), on parle de système déterministe.

PROFINET IO n'utilise donc pas TCP/IP pour l'échange cyclique de données utiles IO à temps critique, mais la communication en temps réel (RT) ou la communication isochrone en temps réel (IRT) pour l'échange synchronisé de données à des intervalles de temps réservés.

Les télégrammes PROFINET IO sont prioritaires par rapport aux télégrammes standard, conformément à la norme IEEE802.1Q. Le déterminisme requis est ainsi assuré. Avec cette méthode, les données sont transmises via des télégrammes Ethernet prioritaires.

Real-Time (RT)

Avec la communication RT, les données cycliques sont transmises entre le contrôleur PROFINET et l'appareil PROFINET, mais ne sont pas synchronisées.

PROFINET avec RT convient pour :

- Les applications à temps critique dans l'automatisation de la production.
  La transmission des données critiques en termes de temps a lieu à des intervalles de temps garantis.
- La transmission d'alarmes et de données cycliques
- La réalisation de grandes capacités fonctionnelles dans les installations de procédés industriels

Isochronous Real-Time (IRT)

L'IRT est une méthode de transmission synchronisée. La communication via Ethernet est divisée en cycles individuels. Chaque cycle se compose de deux phases, un canal IRT réservé aux données hautement critiques en termes de temps et un "canal ouvert" au sein duquel les télégrammes RT et non critiques en termes de temps sont transmis. Ainsi, les données critiques et non critiques peuvent être transmises via la même connexion. Le canal IRT réservé garantit que les données IRT peuvent être transmises à intervalles réservés et synchronisés dans le temps, sans être influencées par d'autres charges de réseau élevées (par ex. communication TCP/IP ou communication en temps réel supplémentaire).

PROFINET avec IRT convient pour :

- un déterminisme de grande précision, même en cas de fort trafic sur le réseau dû à la communication standard
- l'échange cyclique de données IRT entre les appareils PROFINET
- Transmission parallèle de données productives et de données TCP/IP sur une seule ligne, même en cas de volume de données élevé, avec garantie de la retransmission des données productives par réservation de la bande passante de transmission.

Non Real-Time (NRT)

La communication NRT est une communication non critique en termes de temps et correspond à la communication Industrial Ethernet avec la famille de protocoles TCP/IP. Tout ce qui est transmis via Industrial Ethernet peut également être transmis via PROFINET, p. ex. HTTP, TCP, UDP, SNMP, ARP.

11.3.1.4 Relations PROFINET

Une relation d'application (Application Relation/AR) est établie entre un contrôleur PROFINET et un appareil PROFINET. Ces AR permettent de définir des relations de communication (Communication Relation/CR) avec différentes propriétés :

- **Record Data CR** pour le transfert acyclique de paramètres
- **IO Data CR** pour l'échange cyclique de données de process
- **Alarm CR** pour la signalisation d'alarmes en temps réel

11.3.1.5 Données I&M

Les données d'identification et de maintenance (I&M) sont des informations stockées dans un appareil qui vous aident dans les tâches suivantes :

- la vérification de la configuration de l'installation,
- la recherche de modifications matérielles d'une installation,

Les données I&M sont définies dans la norme PROFINET.

Les données d'identification (données I) sont des informations relatives à l'appareil, telles que le numéro d'article et le numéro de série, dont certaines sont également imprimées sur le boîtier de l'appareil. Les données I sont des informations du fabricant sur l'appareil et ne peuvent être que lues.

Les données de maintenance (données M) sont des informations dépendantes de l'installation, telles que le repère d'emplacement et la date d'installation. Les données M sont créées pendant l'ingénierie du projet. Vous pouvez configurer les données M avec SINEC PNI, p. ex. Avec SINEC OS, les données M peuvent également être lues uniquement.

Les données I&M permettent d'identifier clairement les appareils en ligne.

11.3.1.6 Fichier GSD

Un fichier GSD contient les caractéristiques spécifiques d'un appareil. Les fichiers GSD sont mis à disposition en langage basé XML, à savoir GSDML (General Station Description Markup Language).

Pour pouvoir configurer un appareil avec un outil d'ingénierie (par ex. STEP 7/TIA Portal), l'appareil doit être disponible dans le catalogue de matériel. Si l'appareil que vous utilisez n'est pas listé dans le catalogue de matériel, vous pouvez installer le fichier GSD de l'appareil et le rendre ainsi disponible dans le catalogue de matériel.

11.3.2 Configuration de PROFINET

Pour configurer PROFINET, procédez comme suit :

1. [Facultatif] Configurez l'interface TIA.
   Pour plus d'informations, voir chapitre "Configuration de l'interface TIA (Page 222)"
2. Activez PROFINET.
   Pour plus d'informations, voir chapitre "Configuration du mode exécutif PROFINET (Page 223)"
3. [Facultatif] Enregistrez le fichier GSD.
   Pour plus d'informations, voir le chapitre "Enregistrement du fichier GSD sur un PC client local (Page 224)" ou "Enregistrement du fichier GSD sur un serveur distant (Page 224)".

11.3.2.1 Configuration de l'interface TIA

L'interface TIA donne accès à toutes les fonctions PROFINET de l'appareil.

Les conditions suivantes s'appliquent à l'interface TIA :

- Il faut toujours qu'une interface TIA soit configurée.
- Une seule interface IP peut être configurée comme interface TIA.
- L'interface IP configurée comme interface TIA ne peut pas être supprimée.

L'interface TIA que vous configurez ne sera active qu'après le prochain redémarrage de l'appareil.

Le mode exécutif PROFINET que vous configurez ne sera actif qu'après le prochain redémarrage de l'appareil.

Pour configurer l'interface TIA, procédez comme suit :

1. Naviguez vers **System** ≫ **PROFINET** ≫ **PROFINET Mode**.
2. Sélectionnez sous **PROFINET**, dans le champ **TIA Interface after Restart** une interface IP.
3. Validez la modification.
4. Pour activer la nouvelle interface TIA, redémarrez l'appareil.
   Pour plus d'informations, voir "Redémarrage de l'appareil (Page 72)".
   L'appareil redémarre. Lorsque le redémarrage est terminé, la page d'ouverture de session s'affiche.
5. Connectez-vous.
   Pour plus d'informations, voir "Connexion à un appareil configuré (Page 68)".

11.3.2.2 Configuration du mode exécutif PROFINET

Le mode exécutif PROFINET que vous configurez ne sera actif qu'après le prochain redémarrage de l'appareil.

Pour configurer le mode exécutif PROFINET, procédez comme suit :

1. Naviguez vers **System** ≫ **PROFINET** ≫ **PROFINET Mode**.
2. Sélectionnez sous **PROFINET**, dans le champ **Runtime Mode after Restart** le mode exécutif PROFINET.
   Options disponibles :

Option	Description
On	**Par défaut** PROFINET est activé.
Off	Seuls DCP et LLDP sont activés.

3. Validez la modification.
4. Pour activer le mode exécutif PROFINET, redémarrez l'appareil.
   Pour plus d'informations, voir "Redémarrage de l'appareil (Page 72)".
   L'appareil redémarre. Lorsque le redémarrage est terminé, la page d'ouverture de session s'affiche.
5. Connectez-vous.
   Pour plus d'informations, voir "Connexion à un appareil configuré (Page 68)".

11.3.2.3 Enregistrement du fichier GSD sur un PC client local

Le fichier GSD au format ".xml" est enregistré dans un fichier ZIP avec des images de produits au format ".bmp".

Pour enregistrer le fichier GSD de l'appareil sur un PC local, procédez comme suit :

1. Naviguez vers **System** ≫ **Load & Save** ≫ **Data Models**.
2. Sous **Save Data Model to Local PC** sélectionnez pour le paramètre **File Type** l'option **GSDML**.
3. Cliquez sur **Save**.
   Le fichier sera enregistré directement dans un dossier prédéfini ou bien, selon le paramétrage de votre navigateur Web, vous devrez d'abord choisir l'emplacement.
   Un symbole de chargement s'affiche comme retour d'information visuel, à droite du bouton.
   – Si l'enregistrement s'est terminé avec succès, une coche verte s'affiche.
   – Un point d'exclamation rouge et un message d'erreur s'affichent si l'enregistrement a échoué. Renouvelez les dernières opérations.

11.3.2.4 Enregistrement du fichier GSD sur un serveur distant

Le fichier GSD au format ".xml" est enregistré dans un fichier ZIP avec des images de produits au format ".bmp".

Vous pouvez enregistrer le fichier GSD sur un serveur distant.

Conditions

- Vous avez configuré un serveur de manière adéquate.
- Il existe une connexion entre l'appareil et le serveur.
- Selon votre configuration, le nom d'utilisateur et le mot de passe doivent être connus.

Enregistrement du fichier GSD

Pour enregistrer le fichier GSD de l'appareil sur un serveur distant, procédez comme suit :

1. Naviguez vers **System** ≫ **Load & Save** ≫ **Data Models**.
2. Sous **Save Data Model to Remote Server** sélectionnez pour le paramètre **File Type** l'option **GSDML**.
3. Configurez les paramètres du serveur distant.
   Pour plus d'informations sur le chargement et l'enregistrement de fichiers, via un serveur distant, voir "Chargement et enregistrement de fichiers via un serveur distant. (Page 47)".
4. Cliquez sur **Save**.
   Un symbole de chargement s'affiche comme retour d'information visuel, à droite du bouton.
   – Si l'enregistrement s'est terminé avec succès, une coche verte s'affiche.
   – Un point d'exclamation rouge et un message d'erreur s'affichent si l'enregistrement a échoué. Renouvelez les dernières opérations.

11.3.3 Surveillance de PROFINET

Ce paragraphe décrit les différentes possibilités de surveiller PROFINET.

11.3.3.1 Affichage du mode exécutif PROFINET courant

Pour afficher la configuration PROFINET, naviguez vers **System** ≫ **PROFINET** ≫ **PROFINET Mode**.

Sous **PROFINET** , l'écran affiche les informations suivantes :

Paramètres	Description
Current Runtime Mode	Affiche le mode exécutif PROFINET. Options disponibles : • **off** - Seuls DCP et LLDP sont activés. • **on** - PROFINET est activé.

11.3.3.2 Surveillance de la connexion à un contrôleur PROFINET

Pour afficher la configuration PROFINET, naviguez vers **System** ≫ **PROFINET** ≫ **PROFINET Mode**.

Sous **PROFINET** , l'écran affiche les informations suivantes :

Paramètres	Description
State of Controller Connection	Indique s'il existe une connexion à un contrôleur PROFINET. Options disponibles : • **offline** - Il n'existe pas de connexion à un contrôleur PROFINET. • **online** - Une connexion à un contrôleur PROFINET est établie.

11.3.3.3 Surveillance de l'interface TIA

Notez qu'une modification de l'interface TIA n'est active qu'après un redémarrage. Une distinction est faite entre l'interface TIA active et l'interface TIA configurée.

Naviguez vers **System** ≫ **PROFINET** ≫ **PROFINET Mode** pour surveiller l'interface TIA.

Sous **PROFINET** , l'écran affiche les informations suivantes :

Paramètres	Description
TIA Interface after Restart	Affiche l'Interface TIA configurée. Cette interface TIA sera activée au prochain redémarrage.
Current TIA Interface	Affiche l'interface TIA courante.

11.3.3.4 Affichage des données I&M

Seules les données I&M de l'appareil sont affichées. Les données I&M des constituants subordonnés ayant leurs propres numéros d'article ne sont pas affichées (p. ex. les convertisseurs de médias embrochables).

Pour afficher les données I&M de l'appareil, naviguez vers **System** ≫ **PROFINET** ≫ **I & M**.

Sous **Identification & Maintenance (I & M)** , l'écran affiche les informations suivantes :

Paramètres	Description
Manufacturer ID	Affiche le code constructeur.
Order ID	Affiche le numéro de référence de l'appareil.
Serial Number	Affiche le numéro de série de l'appareil.
Hardware Revision	Affiche la version matérielle de l'appareil.
Software Revision	Affiche la version de logiciel utilisée sur l'appareil.
Revision Counter	Le Revision Counter compte le nombre de mises à jour logicielles effectuées. Indépendamment d'un changement de version, ce champ affiche toujours la valeur "0".
Revision Date	Affiche la date et l'heure de la dernière modification du repère d'emplacement et du repère de subdivision essentielle.
Function Tag	Affiche l'identificateur de fonction (repère de subdivision essentielle) de l'appareil. Le repère de subdivision essentielle permet d'identifier clairement un appareil au sein d'une installation. Vous pouvez configurer le repère de subdivision essentielle avec SINEC PNI, p. ex.
Location Tag	Affiche le repère d'emplacement de l'appareil. Le repère d'emplacement indique clairement où se trouve l'appareil. Vous pouvez configurer le repère d'emplacement avec SINEC PNI, p. ex.
Date	Affiche la date d'installation ou de la première mise en service de l'appareil. Vous pouvez configurer la date avec SINEC PNI, p. ex.
Descriptor	Affiche des informations complémentaires sur l'appareil. Vous pouvez configurer ces informations complémentaires avec SINEC PNI, p. ex.

11.3.3.5 Affichage du nom d'appareil PROFINET

Pour afficher la configuration PROFINET, naviguez vers **System** ≫ **PROFINET** ≫ **PROFINET Mode**.

Sous **PROFINET** , l'écran affiche les informations suivantes :

Paramètres	Description
Name of Station	Affiche le nom d'appareil PROFINET. Configurez le nom d'appareil PROFINET avec SINIC PNI, par ex. Si vous configurez le nom d'appareil PROFINET avec SINEC PNI et qu'il ne correspond pas aux règles de la norme CEI 61158-6-10, il sera converti en conséquence. Ce champ affiche le nom converti.

Naviguez jusqu'à la page d'accueil. Le nom d'appareil PROFINET est également affiché sous **Information Dashboard** ≫ **PROFINET Name of Station**.

11.4 EtherNet/IP

Ethernet Industrial Protocol (EtherNet/IP, EIP) est une norme industrielle ouverte pour Industrial Ethernet temps réel, basée sur TCP/IP et UDP/IP.

Remarque

Le présent document ne fournit pas une description exhaustive du protocole EtherNet/IP. Pour plus d'informations sur EtherNet/IP, voir le site Internet Open DeviceNet Vendor Association (ODVA) (https://www.odva.org/).

11.4.1 Ce qu'il faut savoir sur EtherNet/IP

EtherNet/IP complète Ethernet par le Common Industrial Protocol (CIP) sur la couche application. Sous EtherNet/IP, les fonctions transmission, liaison, réseau et transport des couches inférieures du modèle OSI sont assurées par Ethernet .

11.4.1.1 Common Industrial Protocol

Common Industrial Protocol (CIP) est un protocole d'application de l'automatisation qui prend en charge la transition des bus de terrain vers Industrial Ethernet et les réseaux IP.

EtherNet/IP utilise CIP dans la couche application comme interface entre le monde déterministe du bus de terrain et les applications d'automatisation (automates, IHM, OPC, etc.). CIP se situe au-dessus de la couche transport et complète les services de transport proprement dits par des services de communication destinés à la technique d'automatisation. Cela comprend des services pour le trafic de données cyclique, à temps critique et sur évènement.

11.4.1.2 Types de messages

CIP fait la distinction entre les types de messages suivants :

- **Messages implicites**
  Ce type de message est utilisé pour l'échange de données IO critiques en termes de temps.
- **Messages explicites**
  Ce type de message est utilisé pour l'accès aux paramètres (écriture, lecture).

Sur les appareils SINEC OS, un serveur de messages explicite, implémenté pour EtherNet/IP, répond à la communication contrôlée par requête/réponse des clients de messages explicites.

11.4.1.3 Relation producteur-consommateur

Dans le cadre du CIP, la transmission des messages est basée sur des relations producteur-consommateur.

Contrairement au schéma d'adressage traditionnel, les messages ne contiennent pas d'adresse de destination, mais un identifiant unique.

Un émetteur (Producer) envoie un message qui peut être reçu par un ou plusieurs destinataires (Consumer). Les destinataires déterminent si les données sont pertinentes ou non pour eux en fonction de l'identifiant contenu dans le message. Les données correspondantes ne doivent ainsi pas être transmises plusieurs fois d'une source à plusieurs destinations.

Une relation producteur-consommateur est utilisée lorsqu'un échange rapide de données sans données administratives est requis. Dans les relations producteur-consommateur, le trafic réseau est moins important et la vitesse de transmission plus élevée.

11.4.1.4 Modèle d'objet

CIP utilise un modèle d'objet pour décrire les appareils :

- Les objets d'application définissent la manière dont les informations sur les appareils sont représentées et rendues accessibles d'une manière générale.
- Les objets spécifiques au réseau définissent la configuration des paramètres (par exemple l'adresse IP).
- Les objets et services de communication permettent d'établir des relations de communication et d'accéder aux informations sur les appareils via le réseau.

Chaque objet CIP possède des attributs (données), des services (commandes), des connexions et des comportements (relations entre les valeurs d'attributs et les services). Le CIP comprend une vaste bibliothèque d'objets pour prendre en charge la communication réseau générale, les services réseau tels que le transfert de fichiers et les fonctions d'automatisation typiques.

11.4.1.5 Objets pris en charge

Les objets CIP suivants sont pris en charge :

Classe d'objets	Code	Description
Identity Object	01h	L'objet **Identity** permet d'identifier les périphériques EtherNet/IP et fournit des informations générales sur le périphérique. Le Vendor ID de Siemens est 1251. Le Device Type est 2Ch (Managed Ethernet Switch).
Message Router Object	02h	L'objet **Message Router** retransmet des messages explicites aux objets voulus.
Ethernet Link Object	F6h	L'objet **Ethernet Link** stocke des compteurs spécifiques de la liaison et des informations d'état pour une interface de communication IEEE 802.3.
TCP/IP Interface Object	F5h	L'objet **TCP/IP Interface** propose un mécanisme de configuration de l'interface de réseau TCP/IP d'un appareil EtherNet/IP. Les éléments configurables comprennent notamment l'adresse IP, le masque de réseau, l'adresse de la passerelle et le nom d'hôte de l'appareil.
Connection Manager Object	06h	L'objet **Connection Manager** gère les ressources internes nécessaires aux messages implicites et explicites.
Assembly Object	04h	L'objet **Assembly** permet d'affecter les attributs de différents objets EtherNet/IP à une structure de données qui peut être transmise en lecture ou en écriture. L'objet **Assembly** permet typiquement de rassembler des données de processus.
Base Switch Object	51h	L'objet **Base Switch** représente l'interface de la couche d'application CIP avec les informations d'état de base d'un appareil de type Managed Ethernet Switch.

11.4.1.6 Electronic Data Sheet

Une Electronic Data Sheet (EDS) est une fiche technique électronique qui sert de base commune de configuration. Les caractéristiques d'un périphérique EtherNet/IP sont décrites dans une EDS. Elle contient toutes les informations nécessaires à l'intégration des appareils dans un système EtherNet/IP.

Une EDS contient des informations telles que :

- Symbole du produit
- Constructeur et désignations de l'appareil
- Les données cycliques disponibles

11.4.2 Configuration d'EtherNet/IP

Pour configurer EtherNet/IP, procédez comme suit :

1. [Facultatif] Configurez l'interface de gestion.
   Pour plus d'informations, voir chapitre "Configuration de l'interface de gestion (Page 230)"
2. Activez EtherNet/IP.
   Pour plus d'informations, voir chapitre "Activation d'EtherNet/IP (Page 230)"
3. [Facultatif] Enregistrez le fichier EDS.
   Pour plus d'informations, voir chapitre "Enregistrement du fichier EDS sur un PC client local (Page 230)" ou "Enregistrement du fichier EDS sur un serveur distant (Page 231)".
4. [Facultatif] Configurez DLR.
   Pour plus d'informations, voir chapitre "Device Level Ring (Page 203)"

11.4.2.1 Configuration de l'interface de gestion

L'interface de gestion donne accès à toutes les fonctions EtherNet/IP de l'appareil.

L'interface IP **vlan1** est configurée par défaut.

Les conditions suivantes s'appliquent à l'interface de gestion :

- Il faut toujours qu'une interface de gestion soit configurée.
- Une seule interface IP peut être configurée comme interface de gestion.
- L'interface IP configurée comme interface de gestion ne peut pas être supprimée.

Pour configurer l'interface de gestion, procédez comme suit :

1. Naviguez vers **System** ≫ **EtherNet/IP & DLR**.
2. Sélectionnez sous **EtherNet/IP**, dans le champ **Management Interface** une interface IP.
3. Validez la modification.

11.4.2.2 Activation d'EtherNet/IP

EtherNet/IP est désactivé par défaut.

Pour activer EtherNet/IP, procédez comme suit :

1. Naviguez vers **System** ≫ **EtherNet/IP & DLR**.
2. Sous **EtherNet/IP**, modifiez le paramètre **EtherNet/IP** en **Enabled**.
3. Validez la modification.

11.4.2.3 Enregistrement du fichier EDS sur un PC client local

Le fichier EDS au format ".eds" est enregistré sous forme de fichier ZIP.

Pour enregistrer le fichier EDS de l'appareil sur un PC local, procédez comme suit :

1. Naviguez vers **System** ≫ **Load & Save** ≫ **Data Models**.
2. Sous **Save Data Model to Local PC** sélectionnez pour le paramètre **File Type** l'option **EDS**.
3. Cliquez sur **Save**.
   Le fichier sera enregistré directement dans un dossier prédéfini ou bien, selon le paramétrage de votre navigateur Web, vous devrez d'abord choisir l'emplacement.
   Un symbole de chargement s'affiche comme retour d'information visuel, à droite du bouton.
   – Si l'enregistrement s'est terminé avec succès, une coche verte s'affiche.
   – Un point d'exclamation rouge et un message d'erreur s'affichent si l'enregistrement a échoué. Renouvelez les dernières opérations.

11.4.2.4 Enregistrement du fichier EDS sur un serveur distant

Le fichier EDS au format ".eds" est enregistré sous forme de fichier ZIP.

Vous pouvez enregistrer le fichier EDS sur un serveur distant.

Conditions

- Vous avez configuré un serveur de manière adéquate.
- Il existe une connexion entre l'appareil et le serveur.
- Selon votre configuration, le nom d'utilisateur et le mot de passe doivent être connus.

Enregistrement du fichier EDS

Pour enregistrer le fichier EDS de l'appareil sur un serveur distant, procédez comme suit :

1. Naviguez vers **System** ≫ **Load & Save** ≫ **Data Models**.
2. Sous **Save Data Model to Remote Server** sélectionnez pour le paramètre **File Type** l'option **EDS**.
3. Configurez les paramètres du serveur distant.
   Pour plus d'informations sur le chargement et l'enregistrement de fichiers, via un serveur distant, voir "Chargement et enregistrement de fichiers via un serveur distant. (Page 47)".
4. Cliquez sur **Save**.
   Un symbole de chargement s'affiche comme retour d'information visuel, à droite du bouton.
   – Si l'enregistrement s'est terminé avec succès, une coche verte s'affiche.
   – Un point d'exclamation rouge et un message d'erreur s'affichent si l'enregistrement a échoué. Renouvelez les dernières opérations.

11.5 ARP

SINEC OS prend en charge différents tableaux ARP (Address Resolution Protocol) pour les ports de pont afin de résoudre les adresses IP.

11.5.1 Ce qu'il faut savoir sur ARP

Un tableau ARP ou un cache gère l'attribution interne des adresses IP aux adresses MAC physiques. Lorsque la passerelle tente de définir la route d'une trame entrante, ARP fournit l'adresse physique de chaque hôte figurant dans le tableau avec une adresse IP concordante. Si aucun hôte n'est trouvé, ARP transmet un message ARP à tous les hôtes du réseau afin de trouver l'hôte dont l'adresse IP concorde. Si l'hôte approprié existe, ARP l'ajoute dynamiquement au tableau pour les futures requêtes et fournit l'adresse physique à la passerelle.

Un tableau ARP distinct est géré pour chaque interface VLAN interne.

L'appareil prend en charge jusqu'à 1024 entrées. Lorsque le tableau atteint 512 entrées, le service attend cinq secondes avant de supprimer automatiquement les entrées les plus anciennes, non permanentes et les moins utilisées, afin de faire de la place pour les nouvelles entrées.

Remarque

Seules les adresses IPv4 sont prises en charge.

11.5.2 Affichage de l'aperçu des tableaux ARP

Pour afficher l'aperçu des tableaux ARP pour toutes les interfaces VLAN, naviguez vers **System** ≫ **ARP Table**.

Les informations suivantes sont affichées pour chaque interface VLAN sous **Address Resolution Protocol (ARP) Table** :

Paramètres	Description
Interface	Nom de l'interface VLAN.
IP Address	Adresse IP du nœud voisin.
MAC Address	Adresse de la couche de liaison ou adresse MAC (Media Access Control) du nœud voisin.
Origin	Méthode ayant servi à l'ajout de l'entrée. Valeurs possibles : • **dynamic** – L'affectation a été résolue dynamiquement par ARP.
Age	Temps écoulé depuis la dernière mise à jour de l'entrée voisine. Le temps est indiqué au format nYnMnDnhnmns. Pour plus d'information sur la notation du temps, voir "Indication d'une Durée (Page 49)".

Paramètres	Description
Type	Méthode d'encapsulation utilisée pour le message ARP. Valeurs possibles : • **arpa** – Signifie Advanced Research Projects Agency. Indique que l'interface est connectée à un réseau selon IEEE 802.3.
State	État de l'entrée voisine. Valeurs possibles : • **reachable** - Le voisin est considéré comme joignable. ARP interroge les voisins trouvés à des intervalles aléatoires qui peuvent varier de 15 à 45 secondes. L'accessibilité peut également être confirmée par un protocole de niveau supérieur qui communique avec le voisin. • **stale** - Le voisin est considéré comme non joignable. L'accessibilité est réévaluée la prochaine fois que du trafic est envoyé au voisin. • **delay** - ARP se prépare à déterminer si le voisin est joignable. Au bout de 5 secondes l'état passe à **probe**. • **probe** - Des requêtes Unicast-Neighbor-Solicitation ont été envoyées au voisin. Jusqu'à trois requêtes unicast sont envoyées. Si aucune réponse n'est reçue, jusqu'à trois requêtes multicast sont envoyées. Si le voisin ne répond à aucune des requêtes, l'entrée ARP est considérée comme non valide et est supprimée du tableau. Si une réponse est reçue, l'état passe à **reachable**.

11.6 SNMP

Le Simple Network Management Protocol (SNMP) permet une gestion centralisée des constituants de réseau tels que les commutateurs, les contrôleurs, les modules de communication, les routeurs et les ordinateurs.

Le SNMP permet de surveiller et de contrôler les constituants du réseau à partir d'une station de gestion distante.

L'interface utilisateur Web de SINEC OS Web propose des possibilités de configuration restreintes et une vue d'ensemble limités de SNMP. Vous trouverez des informations sur la configuration complète de SNMP ainsi que sur les concepts et marches à suivre, dans le **manuel de configuration CLI SINEC OS**.

11.6.1 Configuration de l'agent SNMP

Pour configurer l'agent SNMP, procédez comme suit :

1. [Facultatif] Configurez quelle(s) version(s) SNMP l'agent SNMP prend en charge.
   Pour plus d'informations, voir "Configuration des versions de SNMP que l'agent SNMP prend en charge (Page 234)".
2. [Facultatif] Configurez un nœud d'extrémité de serveur pour SNMP.
   Pour plus d'informations, voir "Configuration d'un nœud d'extrémité de serveur pour SNMP (Page 234)".
3. Activez un nœud d'extrémité de serveur pour SNMP.
   Pour plus d'informations, voir "Activation d'un nœud d'extrémité de serveur pour SNMP (Page 235)".
4. Veillez à ce que l'agent SNMP soit activé.
   Pour plus d'informations, voir "Activation de l'agent SNMP (Page 236)".

11.6.1.1 Configuration des versions de SNMP que l'agent SNMP prend en charge

Par défaut, l'agent SNMP prend en charge toutes les versions de SNMP.

Pour activer toutes les versions SNMP pour l'agent SNMP, procédez comme suit :

1. Naviguez vers **System** ≫ **Management Services** ≫ **Overview**.
2. Sous **SNMP**, modifiez le paramètre **SNMPv1** en **Enabled**.
3. Sous **SNMP**, modifiez le paramètre **SNMPv2c** en **Enabled**.
4. Sous **SNMP**, modifiez le paramètre **SNMPv3** en **Enabled**.
5. Validez les modifications.

11.6.1.2 Configuration d'un nœud d'extrémité de serveur pour SNMP

Configurez l'adresse IP locale et le port, via lesquels un nœud d'extrémité de serveur traite des requêtes SNMP.

IMPORTANT
Risque de configuration - Risque de coupure de la liaison Si l'appareil obtient son IP dynamiquement par DHCP, tenez compte de ce qui suit : Si l'adresse IP que l'appareil obtient par DHCP ne concorde pas avec l'adresse IP que vous configurez pour le nœud d'extrémité de serveur NETCONF, l'appareil n'est pas accessible via le nœud d'extrémité de serveur NETCONF. Pour éviter une coupure de la liaison, vous disposez des possibilités suivantes : • Autorisez les requêtes de clients sur toutes les adresses locales (adresse IP par défaut : 0.0.0.0). • Attribuez à l'appareil une adresse IP statique. • Veuillez vous assurer que DHCP attribue toujours la même adresse IP.

Les nœuds d'extrémité de serveur suivants sont définis par défaut :

Nœud d'extrémité	Par défaut
Nom	default
Nœud d'extrémité activé	Oui
Adresse IP	0.0.0.0
Port	161

Seuls les utilisateurs possédant le profil utilisateur **Admin** sont habilités à configurer un nœud d'extrémité de serveur.

Pour configurer un nœud d'extrémité de serveur, procédez comme suit :

1. Naviguez vers **System** ≫ **Management Services** ≫ **Overview**.
   Sous **SNMP** ≫ **Endpoint** sont affichés les nœuds d'extrémité de serveur disponibles pour SNMP.
2. Sous **Endpoint**, sélectionnez un nœud d'extrémité et modifiez dans la colonne **UDP Port** le port, via lequel les requêtes SNMP sont traitées.
   Conditions :
   - Le nombre 161
   - Un nombre compris entre 1024 et 49151
   - Un nombre compris entre 49500 et 65535

   Par défaut : 161
3. Sous **Endpoint** sélectionnez un nœud d'extrémité et modifiez dans la colonne **IP Address** l'adresse IP, via laquelle les requêtes SNMP sont traitées.
   Par défaut : 0.0.0.0
   L'adresse IP par défaut autorise les requêtes de clients sur toutes les adresses locales.
4. Validez les modifications.

11.6.1.3 Activation d'un nœud d'extrémité de serveur pour SNMP

Par défaut, le nœud d'extrémité de serveur pour SNMP est activé.

Seuls les utilisateurs possédant le profil utilisateur **Admin** sont habilités à activer un nœud d'extrémité de serveur.

Pour activer un nœud d'extrémité de serveur pour SNMP, procédez comme suit :

1. Naviguez vers **System** ≫ **Management Services** ≫ **Overview**.
   Sous **SNMP** ≫ **Endpoint** sont affichés les nœuds d'extrémité de serveur disponibles pour SNMP.
2. Sous **Endpoint**, sélectionnez un nœud d'extrémité et modifiez le paramètre **Status** en **Enabled**.
3. Validez la modification.

11.6.1.4 Activation de l'agent SNMP

Par défaut, l'agent SNMP est désactivé. SNMP est alors désactivé pour l'appareil et le port SNMP est fermé. Si vous n'utilisez pas SNMP et afin d'éviter tout accès non autorisé à l'appareil, laissez l'agent SNMP à l'état désactivé.

Remarque

Dans STEP7 classic, il existe un éditeur de topologie qui permet de comparer la topologie hors ligne avec les connexions réelles de l'appareil (topologie en ligne). Si SNMP est désactivé, cette fonction n'est pas disponible dans STEP7 classic. Activez SNMP pour pouvoir utiliser cette fonction.

Pour activer l'agent SNMP, procédez comme suit :

1. Naviguez vers **System** ≫ **Management Services** ≫ **Overview**.
2. Sous **SNMP**, modifiez le paramètre **Status** en **Enabled**.
3. Validez la modification.

11.6.2 Modification du nom d'une SNMP Community

Le Community Name correspond au Community String qu'un utilisateur indique lors d'une requête SNMP via SNMPv1 et v2c.

Pour modifier le nom d'une SNMP Community, procédez comme suit :

1. Naviguez vers **System** ≫ **Management Services** ≫ **SNMP**.
   Sous **SNMPv1/v2c Community Strings** ≫ **Index** sont affichés les SNMP Communities disponibles.
2. Modifiiez le nom d'une SNMP Community sous **SNMPv1/v2c Community Strings** .
   Options disponibles :

Option	Description
Text Name	Le nom de la Community sous forme de chaîne de caractères.
Binary Name	Le Community Name en notation hexadécimale avec des deux-points comme caractères de séparation. Utilisez cette option si Community Name contient des caractères non affichables. Exemple : La valeur "0x123456ABCD" est configurée/présentée comme suit : 12:34:56:AB:CD.

   Condition :

   – Il doit compter de 1 à 256 caractères.
3. Validez la modification.

11.6.3 Modification de l'adresse IP d'une SNMP Target.

Pour modifier l'adresse IP d'une SNMP Target, procédez comme suit :

1. Naviguez vers **System** ≫ **Management Services** ≫ **SNMP**.
   Sous **SNMPv1 Trap Receiver** ≫ **Name** sont affichés les SNMP Targets disponibles.
2. Sous **SNMPv1 Trap Receiver**, modifiez le paramètre **IP Address** d'une SNMP Target.
3. Validez la modification.

11.6.4 Modification du port d'une SNMP Target.

Pour modifier le port d'une SNMP Target, procédez comme suit :

1. Naviguez vers **System** ≫ **Management Services** ≫ **SNMP**.
   Sous **SNMPv1 Trap Receiver** ≫ **Name** sont affichées les SNMP Targets disponibles.
2. Sous **SNMPv1 Trap Receiver**, modifiez le paramètre **UDP Port** d'une SNMP Target.
   Condition :
   – Un nombre compris entre 1 et 65535

   Par défaut : 162
3. Validez la modification.

11.6.5 Affichage de l'ID de moteur

Pour afficher l'Engine ID de l'appareil, naviguez vers **System** ≫ **Management Services** ≫ **SNMP**.

Sous **SNMP Engine ID**, l'écran affiche les informations suivantes :

Paramètres	Description
SNMP Engine ID	Affiche le SNMP-Engine ID de l'appareil.

Contrôle et classification du trafic de données 12

Ce chapitre décrit les fonctions disponibles pour le contrôle et la classification du trafic de données. Utilisez ces sous-systèmes pour contrôler le trafic vers les fonctions de réseau connectées. De plus, des outils d'analyse et de caractérisation du trafic sont disponibles.

12.1 Limitation de la vitesse de transmission

SINEC OS prend en charge la limitation de vitesse de transmission sur certaines interfaces réseau. La limitation de la vitesse de transmission consiste à contrôler la vitesse à laquelle une interface envoie et/ou reçoit le trafic de données.

12.1.1 Ce qu'il faut savoir sur la limitation de la vitesse de transmission

La limitation de la vitesse de transmission consiste à restreindre la bande passante pour une interface spécifique. La restriction peut s'appliquer au trafic entrant (ingress) et/ou sortant (egress) et à un type de trafic spécifique (par exemple, unicast, multicast, broadcast, etc.). Pour certaines applications, il peut être nécessaire de limiter la bande passante afin de préserver la qualité du service.

La limitation de la vitesse de transmission offre en outre une couche de protection contre les attaques de type Denial of Service (DoS) et Distributed Denial of Service (DDos). Ces attaques surchargent les ressources du réseau en inondant un appareil de requêtes.

Remarque

Les valeurs limites sont basées sur les capacités des supports de ports des différentes interfaces Ethernet. Avant de limiter la vitesse de transmission sur une interface, vérifiez les capacités du port physique via SINEC OS.

Pour plus d'informations, voir "Détermination des capacités de l'interface (Page 240)".

Remarque

SINEC OS compte tous les bits de la couche 1 dans chaque trame entrante et sortante, y compris le préambule et l'intervalle nter-trame. Pour une trame de 64 octets de couche 2, on compterait p. ex. 80 octets : 8 octets de préambule + 12 octets d'intervalle inter-trame + 64-octets de trame de couche 2.

12.1.2 Configuration de la limitation de la vitesse de transmission

Pour limiter la vitesse de transmission d'un port de pont pour le trafic sortant ou entrant, procédez comme suit pour le port de pont sélectionné et la direction du trafic de données :

1. [Facultatif] Déterminez si le port de pont sélectionné prend en charge la limitation de la vitesse de transmission pour la direction choisie. Selon le type de média, certains ports de pont peuvent ne pas prendre en charge toutes les options.
   Pour plus d'informations, voir "Détermination des capacités de l'interface (Page 240)".
2. Sélectionnez le type de trames à limiter.
   Pour plus d'informations, voir "Sélection du type de trames à limiter (Page 242)".
3. Sélectionnez la vitesse de transmission à contrôler.
   Pour plus d'informations, voir "Sélection de la vitesse de transmission (Page 243)".
4. Activer la limitation de la vitesse de transmission.
   Pour plus d'informations, voir "Activation de la limitation de vitesse de transmission (Page 244)".

12.1.2.1 Détermination des capacités de l'interface

Les capacités des ports de pont sont limitées en fonction de leurs supports physiques. En ce qui concerne la limitation de la vitesse de transmission, les capacités suivantes sont importantes :

- La vitesse maximale configurable (en kbit/s)
- La vitesse minimale configurable (en kbit/s)
- Le trafic de données admissible

Ces capacités déterminent le paramètre de limitation de la vitesse de transmission du trafic entrant et sortant sur le port du pont.

Remarque

Souvent, les capacités diffèrent selon qu'il s'agit de trafic entrant ou sortant. Un port de pont p. ex. peut contrôler les trames entrantes en fonction du type de trafic de données (p. ex. broadcast, multicast, unicast, etc.), mais pas le trafic de données sortant.

Pour déterminer les différentes capacités de limitation de la vitesse de transmission du trafic entrant et sortant, naviguez vers **Interfaces** ≫ **Ethernet Interfaces** ≫ **Rate Control** :

Les capacités sont indiquées sous **Ethernet Rate Control Capabilities** pour chaque port de pont.

Paramètres	Description
Interface	Le nom de l'interface.
Supported Ingress Traffic Types	Le trafic de données entrant pris en charge par le port de pont Valeurs possibles : • **all** – Tous les types de trafic de données sont pris en charge • **broadcast** – Seul le trafic de données broadcast est pris en charge • **multicast** – Seul le trafic de données multicast est pris en charge • **unknown-unicast** – Seul le trafic de données uniticast inconnu est pris en charge • **mcast-and-unknown-ucast** – Seuls les trafics de données multicast et unicast inconnu sont pris en charge • **bcast-and-unknown-ucast** – Seuls les trafics de données broadcast et unicast inconnu sont pris en charge • **bcast-and-mcast** – Seuls les trafic de données broadcast et multicast sont pris en charge • **bcast-and-mcast-and-unknown-ucast** – Seuls les trafics de données broadcast, multicast et unicast inconnu sont pris en charge
Supported Ingress Rate Types	La vitesse de transfert des données lorsque la vitesse de transmission est limitée pour le trafic entrant. Par défaut : **kbps**
Ingress Rate Min	La vitesse de transmission minimale pour le trafic entrant en kilobits par seconde (kbit/s).
Ingress Rate Max	La vitesse de transmission maximale pour le trafic entrant en kilobits par seconde (kbit/s).

Paramètres	Description
Supported Egress Traffic Types	Le trafic de données sortant pris en charge par le port de pont Valeurs possibles : • **all** – Tous les types de trafic de données sont pris en charge • **broadcast** – Seul le trafic de données broadcast est pris en charge • **multicast** – Seul le trafic de données multicast est pris en charge • **unknown-unicast** – Seul le trafic de données uniticast inconnu est pris en charge • **mcast-and-unknown-ucast** – Seuls les trafics de données multicast et unicast inconnu sont pris en charge • **bcast-and-unknown-ucast** – Seuls les trafics de données broadcast et unicast inconnu sont pris en charge • **bcast-and-mcast** – Seuls les trafic de données broadcast et multicast sont pris en charge • **bcast-and-mcast-and-unknown-ucast** – Seuls les trafics de données broadcast, multicast et unicast inconnu sont pris en charge
Supported Egress Rate Types	La vitesse de transfert des données lorsque la vitesse de transmission est limitée pour le trafic sortant. Par défaut : **kbps**
Egress Rate Min	La vitesse de transmission minimale pour le trafic sortant en kilobits par seconde (kbit/s).
Egress Rate Max	La vitesse de transmission maximale pour le trafic sortant en kilobits par seconde (kbit/s).

12.1.2.2 Sélection du type de trames à limiter

Pour limiter un seul type de trafic spécifique (entrant ou sortant) sur un port de pont, procédez comme suit :

1. [Facultatif] Vérifiez les capacités de l'interface sélectionnée afin de déterminer si elle peut limiter le type de trame que vous souhaitez contrôler dans la direction choisie (c'est-à-dire entrante ou sortante).
   Exemple : Si une interface a la capacité **all** pour le trafic sortant (egress), la vitesse de transmission du trafic sortant ne peut pas être limitée en fonction du type de trafic.
   Pour plus d'informations, voir "Détermination des capacités de l'interface (Page 240)".
2. Naviguez vers **Interfaces** ≫ **Ethernet Interfaces** ≫ **Rate Control**.

3. Configurez sous **Ethernet Rate Control** le **Ingress Traffic Type** et/ou **Egress Traffic Type** pour le port de pont sélectionné.
   Options disponibles :

Option	Description
all	**Par défaut** La limitation de la vitesse de transmission s'applique à l'ensemble du trafic de données.
broadcast	La limitation de la vitesse de transmission ne s'applique qu'au trafic de données broadcast.
unknown-unicast	La limitation de la vitesse de transmission ne s'applique qu'au trafic de données unicast inconnu.

   Notez que les options suivantes sont également disponibles, mais ne sont pas prises en charge dans cette version :

Option	Description
bcast-and-mcast	La limitation de la vitesse de transmission s'applique au trafic de données broadcast et multicast.
bcast-and-mcast-and-unknown-ucast	La limitation de la vitesse de transmission s'applique au trafic de données broadcast, multicast et unicast inconnu.
bcast-and-unknown-ucast	La limitation de la vitesse de transmission s'applique au trafic de données broadcast unicast inconnu.
mcast-and-unknown-ucast	La limitation de la vitesse de transmission s'applique au trafic de données multicast et unicast inconnu.
multicast	La limitation de la vitesse de transmission s'applique au trafic de données multicast et multiicast inconnu.
unicast	La limitation de la vitesse de transmission s'applique au trafic de données unicast et unicast inconnu.
unknown-multicast	La limitation de la vitesse de transmission ne s'applique qu'au trafic de données multicast inconnu.

4. Validez la modification.

12.1.2.3 Sélection de la vitesse de transmission

Pour sélectionner la limite de vitesse de transmission appliquée par le port de pont au trafic sortant ou entrant, procédez comme suit :

1. [Facultatif] Vérifiez les capacités du port de pont sélectionné afin de déterminer s'il peut limiter le type de trame que vous souhaitez contrôler dans la direction choisie (c'est-à-dire entrante ou sortante).
   Exemple : Si un port de pont dispose de la capacité **all** pour le trafic sortant (egress), la vitesse de transmission du trafic sortant ne peut pas être limitée en fonction du type de trafic.
   Pour plus d'informations, voir "Détermination des capacités de l'interface (Page 240)".
2. Naviguez vers **Interfaces** ≫ **Ethernet Interfaces** ≫ **Rate Control**.

3. Sous **Ethernet Rate Control** sélectionnez un port de pont puis saisissez la valeur pour **Ingress Rate** et/ou **Egress Rate**. La vitesse de transmission est définie en kilobits par seconde (kbit/s).
   Par défaut : 0
4. Validez la modification.

12.1.2.4 Activation de la limitation de vitesse de transmission

Par défaut, la limitation de la vitesse de transmission dans les deux sens du trafic est désactivée pour tous les ports de pont.

Pour activer la limitation de la vitesse de transmission pour un port de pont défini, procédez comme suit :

Remarque

La limitation de la vitesse de transmission est activée séparément pour le trafic de données entrant et sortant.

1. Naviguez vers **Interfaces** ≫ **Ethernet Interfaces** ≫ **Rate Control**.
2. Sous **Ethernet Rate Control** sélectionnez un port de pont puis modifiez **Ingress Rate Control State** et/ou **Egress Rate Control State** en **Enabled**.
3. Validez la modification.

12.1.3 Exemples de configuration

Vous trouverez ci-dessous des exemples de la manière dont vous pouvez appliquer la limitation de la vitesse de transmission.

12.1.3.1 Limitation de la vitesse de transmission

Dans cet exemple, l'appareil retransmet le trafic de données sur l'interface ethernet0/1 (un port FX 1000Base) à un serveur qui n'accepte les données qu'à 100 kbit/s. Si cette valeur limite est dépassée, des trames sont perdues.

Figure 12-1 Limitation du trafic de données vers un serveur

Pour limiter la vitesse de transmission du trafic de données vers un serveur, procédez comme suit :

1. Définissez une vitesse de transmission de 100 kbit/s pour le trafic sortant vers ethernet0/1. Pour plus d'informations, voir "Sélection de la vitesse de transmission (Page 243)".
2. Activez la limitation de la vitesse de transmission pour le trafic sortant sur ethernet0/1. Pour plus d'informations, voir "Activation de la limitation de vitesse de transmission (Page 244)".

12.2 VLAN

Ce paragraphe décrit la configuration et le déploiement réussi des VLAN dans les réseaux de couche 2 pour la connexion virtuelle de différents segments de réseau local.

Remarque

L'interface utilisateur Web n'affiche que les VLAN configurés statiquement et permet de les configurer. Les VLAN qui ont été appris dynamiquement via le GARP VLAN Registration Protocol (GVRP) sont uniquement affichés via la CLI.

12.2.1 Ce qu'il faut savoir sur les VLAN

Les réseaux locaux virtuels (VLAN) sont une fonction de la couche 2 définie par la norme IEEE 802.1Q. Ils servent à regrouper logiquement le trafic de données par fonction ou par organisation, ou bien ils contiennent du trafic broadcast, inconnu et multicast (Broadcast, Unknown, Multicast BUM).

Dans une implémentation sans VLAN, le trafic BUM serait acheminé vers tous les nœuds du réseau local et permettrait un trafic any-to-any unicast. En revanche, avec des VLAN, tout le trafic de données reste dans le VLAN, ce qui réduit l'utilisation du réseau local.

Les VLAN appartiennent généralement à des sous-réseaux IP dans lesquels chaque utilisateur final d'un sous-réseau IP spécifique est membre du même VLAN. Le trafic entre les VLAN est donc généralement rendu possible sur IP par l'utilisation de routeurs IP.

Comme les VLAN définissent des connexions logiques et non des connexions physiques, ils réduisent considérablement la complexité de la mise en place ainsi que les besoins en travail et en ressources d'un LAN traditionnel. En même temps, ils améliorent la sécurité et la gestion du trafic.

Le trafic est regroupé en ajoutant aux trames des balises provenant de nœuds du même domaine de broadcast.

Chaque appareil peut définir un ou plusieurs VLAN (domaines de broadcast), jusqu'à un nombre maximal de 4094.

Remarque

Comme les VLAN se partagent la bande passante sur le même lien physique, il est recommandé de configurer des classes de trafic afin d'améliorer l'efficacité du routage. Pour plus d'informations sur les classes de trafic, voir "Classes de trafic (Page 259)".

Les paragraphes suivants expliquent comment le trafic de données de différents segments LAN peut être regroupé logiquement dans des VLAN.

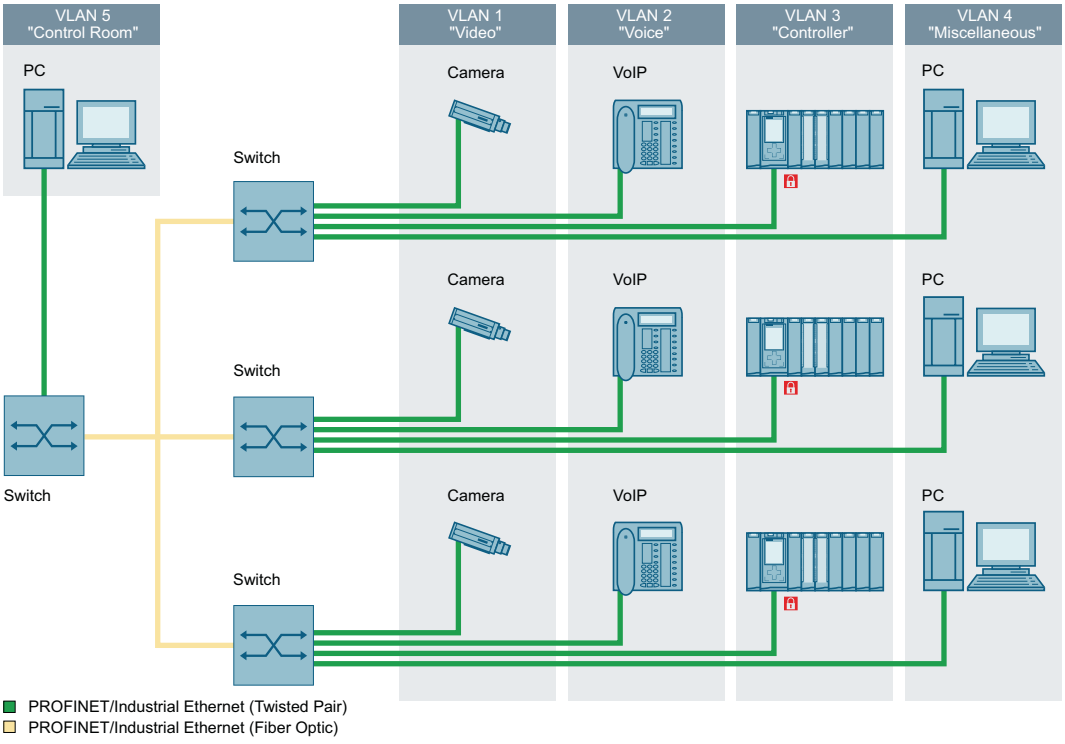


Figure 12-2 Séparation du trafic de données par plusieurs VLAN

12.2.1.1 Création de VLAN

La création de VLAN est soit statique soit dynamique :

- **Statique**
  Les VLAN statiques peuvent être définis directement sous SINEC OS.
- **Dynamique**
  Les VLAN peuvent être appris à l'aide du protocole GARP VLAN.

12.2.1.2 Modes de fonctionnement "compatible VLAN" et "non compatible VLAN"

Les appareils conformes à la norme IEEE 802.1Q sont classés comme **compatibles VLAN** et fonctionnent à tout moment en mode compatible VLAN. Ces appareils reconnaissent les balises VLAN sur les trames entrantes (ingress) et utilisent la balise ainsi que l'adresse MAC ou IP de la cible pour transmettre la trame sur le segment de réseau local virtuel correct.

En revanche, les appareils qui ne sont pas conformes à IEEE 802.1Q sont considérés comme **non compatibles VLAN**. Ces appareils ignorent les balises VLAN et transmettent les trames telles quelles à leur adresse MAC ou IP de destination. Les balises VLAN ne sont pas supprimées de l'en-tête de la trame.

SINEC OS est compatible VLAN et répond ainsi aux règles définies par la norme IEEE 802.1Q :

- Les identifiants VLAN (VID) valides doivent se situer dans la plage de 1 à 4094. Les VID avec une valeur de 0 ou 4095 sont réservés.
- Toute trame (ingress) entrante doit disposer d'un VID valide.
- Toute trame sortante (egress) doit posséder une balise VID valide ou être envoyée sans balise. Les trames avec balise VID non valide ne sont pas retransmises par un appareil compatible VLAN.

SINEC OS accepte également les trames balisées avec un ID de VLAN de 0. Cependant, un **mode tunnel VLAN-0** spécial doit être activé pour ces trames afin qu'elles soient correctement acheminées. Pour plus d'informations sur le mode tunnel VLAN-0, voir "Mode tunnel VLAN 0 (Page 252)".

12.2.1.3 Trames balisées et non balisées

Balises de VLAN (ou balises IEEE 802.1Q) dans l'en-tête IP d'un identifiant de trame comme élément d'un réseau VLAN. Lorsqu'un commutateur de réseau reçoit une trame avec une balise VLAN, l'identifiant VLAN (VID) est extrait de l'en-tête et la trame est transmise à sa destination dans le même VLAN.

Si une trame ne contient pas de balise VLAN ou si elle contient une balise IEEE 802.1p (priorisation) qui ne contient que des informations de priorisation et un VID de 0, elle est considérée comme une trame non balisée.

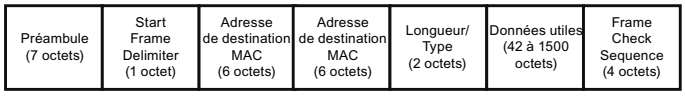


Figure 12-3 En-tête d'une trame non balisée

Figure 12-4 En-tête d'une trame balisée

Tag Protocol Identifier (TPI)

Le champ Tag Protocol Identifier (TPI) identifie la trame comme étant une trame balisée. Il se compose d'un champ de 16 bits, pour lequel 0x8100 est défini.

Tag Control Information (TCI)

La champ Tag Control Information (TCI) définit :

- **Priority Code Point (PCP)**
  Un sous-champ de 3 bits qui indique la classe de service (CoS) IEEE 802.1p associée à la trame. La valeur de ce champ est affectée à un niveau de priorité spécifique comme suit :

PCP	Priorité	Type	Description
111	7	Contrôle du réseau	Trafic de données qui prend en charge la configuration et la maintenance de la structure du réseau.
110	6	Contrôle Inter Réseau	Trafic de données qui prend en charge l'infrastructure de réseau qui doit être délimitée par le domaine administratif.
101	5	Langue	Trafic de données avec une temporisation de moins de 10 millisecondes et une gigue maximale.
100	4	Vidéo	Trafic de données avec une temporisation de 100 millisecondes ou autres applications à faible latence, telles que les communications vidéo interactives.
011	3	Applications critiques	Trafic de données nécessitant une bande passante minimale garantie, mais soumis à une forme de contrôle d'accès afin d'éviter qu'une application ne consomme de la bande passante au détriment des autres applications.
010	2	Excellent Effort	Trafic de données qu'une organisation de services d'information peut prioriser pour des clients sélectionnés. Il s'agit d'un service de type Best Effort.
001	1	Arrière-plan	Trafic de données qui prend en charge l'exécution d'opérations non critiques en arrière-plan (telles que les transferts de masse) pour ne pas affecter l'utilisation du réseau par les autres utilisateurs et applications.
000	0	Best Effort	Trafic de données pour applications non prioritaires. Le traitement équilibré est basé sur la stratégie de redimenionnement dynamique des fenêtres et de retransmission définis par le protocole TCP (Transmission Control Protocol) du service. Il s'agit d'un service Best Effort associé au trafic de données LAN traditionnel.

- **Drop Eligible Indicator (DEI)**
  Un sous-champ de 1 bit qui indique si la trame peut être rejetée pendant les phases de congestion du trafic de données. La valeur peut être utilisée séparément ou avec la valeur PCP.

Valeur	Description
0	Le format de l'adresse MAC est canonique. Dans la représentation canonique, le bit de poids faible de l'adresse est transmis en premier.
1	Le format de l'adresse MAC n'est pas canonique.

- **VLAN ID (VID)**
  Un sous-champ de 12 bits qui indique le VLAN auquel la trame appartient.

Valeur	Description
0	Pas d'ID de VLAN. La trame ne contient que des informations de priorité (trame balisée avec une priorité).
1 – 4094	Les ID de VLAN dans cette plage sont valides.
4095	Cet ID de VLAN est réservé.

12.2.1.4 Ports d'accès et ports de jonction

Chaque port de pont peut être transformé en port **d'accès** ou port **de jonction**.

- **Ports d'accès et ports de jonction**
  Un port d'accès transmet typiquement le trafic de données dans son VLAN natif à un seul terminal (par exemple un PC ou un Intelligent Electronic Device).
- **Ports de jonction**
  Un port de jonction peut acheminer le trafic d'un ou de plusieurs VLAN simultanément sur le même lien. Il est destiné aux applications entre les commutateurs.
  Pour garantir que le trafic appartenant à différents VLAN reste séparé dans l'interface de jonction, chaque trame est encapsulée avec une balise IEEE 802.1Q qui identifie le VLAN auquel la trame appartient.
  Les trames liées au VLAN natif d'un port de jonction peuvent être transmises en tant que trames non balisées.
  Par défaut, chaque port de jonction est un membre de tout VLAN disponible, y compris les VLAN appris dynamiquement au moyen de GVRP. L'adhésion peut être limitée en définissant une liste de VLAN interdits pour le port concerné.

Remarque

Le même identifiant VLAN natif doit être configuré pour les deux extrémités d'une connexion d'interface de jonction.

Par défaut, chaque port d'accès ou de jonction reçoit le PVID avec la valeur 1. Pour les ports de jonction, il représente le VLAN natif du port. Pour le PVID, chaque VLAN défini de manière statique peut être réglé entre 1 et 4094.

Pour plus d'informations sur la configuration d'un port de pont comme port d'accès ou port de jonction, voir "Sélection du type d'affiliation du port (Page 256)".

12.2.1.5 VLAN natif et VLAN par défaut

Le **VLAN par défaut** est appelé VLAN 1. Tous les ports de pont sont affectés par défaut à ce VLAN, jusqu'à ce qu'ils soient affectés explicitement à un autre VLAN.

Le **VLAN natif** est le plus souvent utilisé pour des ports d'accès. Il s'agit du VLAN affecté au port via son identifiant VLAN de port (PVID). Chaque trame non balisée ou balisée avec priorité reçue par le port est retransmise sur le VLAN natif. L'ID par défaut du VLAN natif (ou PVID) est 1, mais il peut être spécifié sur tout VLAN défini statiquement entre 1 et 4094.

Pour plus d'informations sur le paramétrage du VLAN natif pour un port de pont, voir "Configuration de l'ID de VLAN du port (Page 256)".

12.2.1.6 Filtre d'entrée (ingress)

Le filtre d'entrée est une fonction qui peut être activée par port. Elle évalue chaque trame (ingress) entrante avant qu'elle n'entre dans le réseau afin de s'assurer qu'elle provient de la source attendue.

Lorsque le filtre Ingress est activé, l'appareil contrôle toutes les trames balisées qui arrivent sur le port de pont. Si le port du pont n'est pas membre du VLAN auquel la trame est affectée, la trame est rejetée.

Si le filtre ingress est désactivé, les trames sont acceptées par tous les VLAN configurés sur l'appareil.

Remarque

Activez le filtre ingress si vous utilisez des listes de VLAN interdits. Les listes de VLAN interdits empêchent simplement une interface de rejoindre certains VLAN. Elles n'empêchent pas qu'une trame d'un VLAN figurant dans la liste des VLAN interdits soit transmise à une autre interface qui est membre de ce VLAN.

Pour plus d'informations sur l'activation du filtre ingress, voir "Activation du filtre ingress (Page 257)".

12.2.1.7 Règles ingress et egress

Lors du traitement des trames entrantes (ingress) et sortantes (egress), les règles suivantes sont appliquées.

Règles pour le trafic de données entrant (Ingress)

- Un port de pont qui n'applique pas de filtre ingress ou qui n'accepte qu'un type de trame spécifique retransmet toutes les trames dans le VLAN affecté aux trames.
- Si le filtre ingress est activé pour un port de pont, les règles suivantes s'appliquent :
  - Le port n'accepte que les trames dont le VID correspond au VLAN auquel l'interface est affectée.
  - les trames sont rejetées si leur VID ne correspond pas au VLAN affecté au port de réception
- Si une interface physique est configurée pour n'accepter qu'un seul type de trame, les règles suivantes s'appliquent :
  - Si le port n'accepte que les trames non balisées et les trames balisées avec une priorité, les trames balisées sont rejetées.
  - Si le port n'accepte que les trames balisées, les trames non balisées avec une priorité et les trames balisées avec une priorité sont rejetées.
- Les trames non taguées ou les trames taguées avec une priorité sont affectées au PVID de l'interface ingress.

Règles pour le trafic de données sortant (egress)

- Les trames retransmises à une interface d'accès sont rejetées si elles sont affectées à un VLAN autre que le VLAN natif de l'interface egress.
- Les trames qui sont transmises à une interface de jonction sont balisées avec leur VID (et non le VLAN natif de l'interface egress) si elles sont associées à un VLAN dont l'interface egress est membre.
- Si le balisage PVID est activé, les trames sortantes sont balisées indépendamment du type d'adhésion de l'interface egress (accès ou jonction), à condition qu'elles soient affectées au VLAN natif de l'interface egress.
- Si une liste de VLAN interdits est définie pour une interface egress, les trames sont rejetées si elles sont affectées à un VLAN de la liste.

12.2.1.8 GARP VLAN Registration Protocol (GVRP)

Le protocole GARP VLAN Registration (GVRP) est un protocole standard basé sur le protocole GARP (Generic Attribute Registration Protocol) pour la distribution automatique des informations de configuration VLAN dans un réseau. Sur chaque commutateur d'un réseau, seuls les VLAN qui sont requis localement doivent être configurés. Les VLAN configurés sur les appareils voisins sont appris via GVRP. Un utilisateur final compatible GVRP (c'est-à-dire un PC ou un Intelligent Electronic Device) configuré pour un VID spécifique peut être connecté à un commutateur compatible GVRP via une interface de jonction et devenir automatiquement membre du VLAN sélectionné.

Remarque

GVRP est uniquement configurable via la CLI : Pour plus d'informations, voir le **Manuel de configuration SINEC OS CLI**.

12.2.1.9 VLAN interdits

Par défaut, chaque port de jonction est automatiquement un membre de chaque VLAN défini. Il peut toutefois être nécessaire de restreindre le trafic VLAN spécifique sur certains ports de pont. Cela peut être fait en définissant une liste de VLAN interdits. Une telle liste est définie pour des interfaces individuelles et elle régit les VLAN dont le port peut devenir membre. Lorsque le filtre ingress est activé, le trafic entrant appartenant à l'un des VLAN interdits de la liste est automatiquement rejeté.

Une liste des VLAN interdits empêche également l'ajout automatique des ports de pont aux VLAN appris dynamiquement par GVRP. Les VLAN figurant sur la liste des VLAN interdits d'un port de pont ne sont pas non plus communiqués à ce port par GVRP.

Remarque

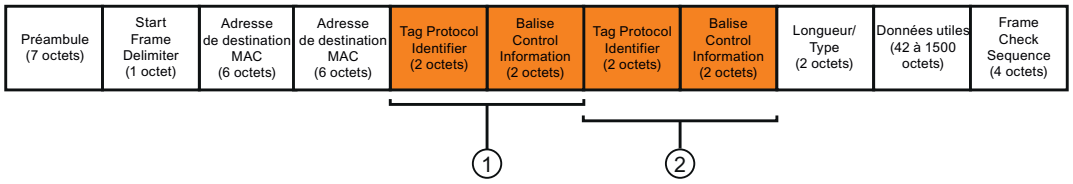
Activez le filtre ingress si vous utilisez des listes de VLAN interdits. Les listes de VLAN interdits empêchent simplement un port de pont de rejoindre des VLAN spécifiques. Elles n'empêchent pas qu'une trame d'un VLAN figurant dans la liste des VLAN interdits soit transmise à un autre port de pont qui est membre de ce VLAN.

12.2.1.10 Mode tunnel VLAN 0

Certaines fonctions, comme PROFINET, transmettent des trames prioritaires balisées avec un ID de VLAN 0. Ces trames doivent en fait être transmises telles quelles avec leur priorité indiquée. Cependant, selon la norme IEEE 802.1Q, chaque trame avec valeur de priorité transmise via un port de pont se voit en principe attribuer le PVID du port au lieu de son ID de VLAN d'origine.

Pour passer outre ce comportement, il est possible d'activer le mode tunnel VLAN 0 pour un VLAN. Les ports de pont qui sont membres de VLAN avec le mode de tunnel VLAN 0 activé traitent alors séparément les trames prioritaires qui sont balisées avec un ID de VLAN de 0.

- À la réception, de telles trames sont classées dans une file d'attente en fonction de leurs valeurs de priorité, et non de la priorité du port de pont.
- En sortie, si le port de pont est un membre **balisé** du VLAN, la trame est doublement balisée avec le VID du port de sortie à l'extérieur ① et la valeur de priorité conservée de la trame à l'intérieur ②. En revanche, si le port de pont est un **membre non balisé** du VLAN, la trame est uniquement transmise avec la valeur de priorité non modifiée.



① Balises extérieures (PVID)

② Balises intérieures (valeur de priorité)

Figure 12-5 Trame à double balise

Remarque

Les trames balisées avec VLAN 0 sont traitées comme des trames normales lorsqu'elles arrivent sur un port de pont dont le VLAN natif est un VLAN **sans** mode tunnel VLAN 0 activé.

Remarque

Le mode tunnel VLAN 0 n'affecte pas le traitement des autres trames non balisées ou balisées.

Le mode tunnel VLAN 0 peut être activé pour chaque VLAN actif et est alors actif pour tous les ports de pont appartenant à ces VLAN.

12.2.1.11 Avantages et inconvénients de l'utilisation de VLAN

Certains des principaux avantages et inconvénients des VLAN sont examinés ci-dessous.

Avantages

- **Séparation du trafic de données en domaines**
  Les VLAN sont le plus souvent utilisés pour leur capacité à restreindre les flux de trafic entre les groupes de périphériques. Le trafic de broadcast inutile peut être limité au VLAN qui en a besoin. Les tempêtes de broadcast dans un VLAN n'affectent pas nécessairement les utilisateurs des autres VLAN.
  Les hôtes d'un VLAN peuvent être empêchés de prendre, intentionnellement ou non, l'adresse IP d'un hôte d'un autre VLAN.
  L'utilisation du Creative Bridge Filtering et de plusieurs VLAN peut diviser des sous-réseaux IP apparemment unifiés en plusieurs zones soumises à différentes stratégies de sécurité/ d'accès.
  Les hôtes multi-VLAN peuvent affecter différents types de trafic à différents VLAN.
- **Administration pratique**
  Les VLAN simplifient le changement d'emplacement des appareils lorsque cela est nécessaire. Lorsqu'un commutateur est installé à un autre endroit, il est fréquent que son point de connexion soit également modifié. Mais dans le cas des VLAN, restaurer l'appartenance à un VLAN d'un commutateur est aussi simple que de copier l'appartenance vers un nouveau port.
- **Moins de matériel**
  Sans les VLAN, la séparation du trafic dans les domaines implique l'utilisation de ponts séparés pour des réseaux distincts. Les VLAN rendent superflus des ponts distincts.
  Le nombre d'hôtes de réseau peut souvent être réduit. Souvent, un serveur est affecté à la fourniture de services à des réseaux indépendants. Ces hôtes peuvent être remplacés par un seul Multihomed-Host qui prend en charge chaque réseau dans son propre VLAN. Cet hôte peut effectuer le routage entre les VLAN.
  Les hôtes multi-VLAN peuvent affecter différents types de trafic à différents VLAN.

Inconvénients

- **Nombre limité de VLAN**
  Chaque réseau est limité à 4094 VLAN, les VID 0 et 4095 étant réservés. Bien que le nombre de 4094 VLAN puisse être suffisant pour la plupart des réseaux, cette valeur peut s'avérer être une limite à l'avenir.
- **Sécurité des données**
  Si le réseau s'étend sur plusieurs régions géographiques, le trafic VLAN peut éventuellement être exposé à des attaques par reniflage ou de l'homme du milieu. Celles-ci peuvent être difficiles à maîtriser si des fonctions de sécurité de couche 3 (p. ex. pare-feu, IPsec, etc.) ne sont pas également mises en œuvre.
- **Investissement**
  Les implémentations qui utilisent principalement des VLAN statiques (c'est-à-dire des VLAN basés sur les ports et les MAC) peuvent être difficiles à maintenir lorsque le réseau se développe au fil du temps. La surveillance et la mise à jour des adhésions au VLAN peuvent prendre beaucoup de temps.

12.2.2 Configuration de VLAN

Pour configurer et affecter un VLAN, procédez comme suit :

1. Ajoutez des VLAN statiques et/ou activez GVRP.
   GVRP est uniquement activable ou désactivable via la CLI : Pour plus d'informations, voir le **Manuel de configuration SINEC OS CLI**.
   Pour plus d'informations sur l'ajout de VLAN statiques, voir "Ajout ou édition d'un VLAN statique (Page 254)".

   Remarque

   Une interface est automatiquement créée pour chaque nouveau VLAN statique.

2. [Facultatif] Configurez l'interface VLAN créée pour le VLAN statique.
   Pour plus d'informations, voir "Configuration d'interfaces VLAN (Page 172)".
3. [Facultatif] Activez le mode tunnel VLAN 0.
   Pour plus d'informations, voir "Activation du mode de tunnel VLAN 0 (Page 255)".
4. Configurez les paramètres VLAN pour un ou plusieurs ports de pont.
   Pour plus d'informations, voir "Configuration de paramètres VLAN pour des ports de pont (Page 255)".

12.2.2.1 Ajout ou édition d'un VLAN statique

Pour ajouter ou éditer un VLAN statique, procédez comme suit :

Remarque

Affectez une adresse IP à l'interface VLAN correspondante pour en faire une interface de gestion. Vous pourrez alors, à l'aide de SSH, accéder à la CLI via le port de gestion.

Pour plus d'informations sur l'affectation d'une adresse IP à une interface de VLAN, voir "Attribution d'adresses IP statiques (Page 185)".

1. Naviguez vers **Layer 2** ≫ **VLANs**.
2. Sous **Static Virtual Local Area Networks (VLANs)**, sélectionnez un VLAN existant ou cliquez sur **Add** pour ajouter un nouveau VLAN.
3. Saisissez l'ID du VLAN sous **VLAN ID**.
   Condition :
   – Un nombre compris entre 1 et 4094
4. [Facultatif] Saisissez un nom pour le VLAN sous **VLAN Name**.
   Condition :
   – Il doit compter de 0 à 32 caractères

   Si aucun nom n'est défini, un nom est affecté au VLAN dans la base de données des VLAN. Le nom possède le format VLAN{numéro}, ce {numéro} étant un nombre à quatre chiffres constitué du VID précédés de zéros.
   Exemple : VLAN0010 est le nom de VLAN par défaut du VLAN 10.
5. Validez la modification.

12.2.2.2 Activation du mode de tunnel VLAN 0

En mode tunnel VLAN 0, tous les ports de pont appartenant à un VLAN donné peuvent transmettre sans modification les trames priorisées balisées avec un ID de VLAN de 0. Cela peut être nécessaire pour certaines fonctions, comme PROFINET, afin de garantir que la valeur de priorité d'une trame ne soit pas modifiée lors de son acheminement vers sa destination. Si le mode de tunnel VLAN 0 n'est pas activé, selon la norme IEEE 802.1Q, chaque trame transmise par un port de pont avec une valeur de priorité se voit attribuer le PVID du port au lieu de son ID de VLAN d'origine.

Pour plus d'informations, voir "Mode tunnel VLAN 0 (Page 252)".

Remarque

Le mode tunnel VLAN 0 peut être activé pour tous les VLAN actifs. Il est désactivé par défaut.

Pour activer le mode tunnel VLAN 0 pour un VLAN, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **VLANs**.
2. Sous **Static Virtual Local Area Networks (VLANs)**, modifiez le paramètre **VLAN-0-Tunnel** du VLAN sélectionné en **Enabled**.
3. Validez la modification.

12.2.3 Configuration de paramètres VLAN pour des ports de pont

Pour configurer les paramètres VLAN pour un port de pont, procédez comme suit :

1. Définissez le port du pont comme interface d'accès ou interface de jonction.
   Pour plus d'informations, voir "Sélection du type d'affiliation du port (Page 256)".
2. [Facultatif] Modifiez l'ID de VLAN du port de pont. Par défaut, l'ID de VLAN défini du port est 1.
   Pour plus d'informations, voir "Configuration de l'ID de VLAN du port (Page 256)".
3. [Facultatif] Si GVRP est activé, paramétrez le mode GVRP pour le port de pont.
   Le mode GVRP est uniquement paramétrable via la CLI : Pour plus d'informations, voir le **Manuel de configuration SINEC OS CLI**.
4. [Facultatif] Activez le balisage PVID pour le trafic de données sortant du port de pont.
   Pour plus d'informations, voir "Activation du balisage PVID pour le trafic de données sortant (Page 257)".
5. [Facultatif] Spécifiez les trames que le port de pont accepte.
   - Pour filtrer les trames en fonction de leur type (c'est-à-dire balisé, non balisé ou les deux), définissez le type de trame accepté.
     Pour plus d'informations, voir "Sélection des types de trames acceptés (Page 257)".
   - Pour filtrer les trames en fonction de leur VID, activez le filtre ingress.
     Pour plus d'informations, voir "Activation du filtre ingress (Page 257)".
6. [Facultatif] Définissez uniquement pour les ports de pont de type port de jonction, la liste des VLAN interdits.
   Pour plus d'informations, voir "Limitation de l'appartenance à un VLAN (Page 258)".

12.2.3.1 Sélection du type d'affiliation du port

Pour sélectionner le type d'affiliation du port, procédez comme suit :

1. Si vous modifiez le type d'affiliation du port de trunk en access, veuillez vous assurer que le mode GVRP est désactivé pour le port de pont sélectionné et que la liste des VLAN interdits a été supprimée. Ces fonctions ne sont pas prises en charge par les ports access.
   Le mode GVRP est uniquement configurable via la CLI. Pour plus d'informations, voir le **Manuel de configuration SINEC OS CLI**.
   Pour plus d'information sur les VLAN interdits, voir "Limitation de l'appartenance à un VLAN (Page 258)".
2. Naviguez vers **Layer 2** ≫ **VLANs**.
3. Sous **Port Based VLANs** sélectionnez un port de pont puis configurez l'option **Type**.
   Options disponibles :

Option	Description
Access	**Par défaut** Le port de pont transfère le trafic de données uniquement sur le VLAN natif.
Trunk	Le port de pont transfère le trafic de données sur tous les VLAN.

4. Validez la modification.

12.2.3.2 Configuration de l'ID de VLAN du port

Le VLAN natif pour un port de pont est déterminé en définissant l'ID de VLAN du port (PVID). Lorsque le VLAN natif est défini, toutes les trames non balisées ou balisées avec une priorité selon IEEE 802.1p que le port de pont reçoit sont affectées à ce VLAN. Les trames balisées avec un ID de VLAN différent de zéro sont toujours affectées à l'ID de VLAN indiqué dans l'en-tête de la trame.

Remarque

Le même identifiant VLAN natif est généralement configuré pour les deux extrémités d'une connexion d'interface de jonction.

Pour configurer l'ID de VLAN d'un port de pont, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **VLANs**.
2. Sous **Port Based VLANs**, sélectionnez pour **Native VLAN ID** la vitesse du port de pont sélectionné.
   Condition :
   – Un nombre compris entre 1 et 4094
3. Validez la modification.

12.2.3.3 Sélection des types de trames acceptés

Les VLAN affectés à un port de pont acceptent par défaut les trames balisées et non balisées. Si nécessaire, ils peuvent toutefois être configurés par port pour n'accepter que les trames balisées ou non balisées.

Pour sélectionner les types de trames qui sont acceptés par un port de pont, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **VLANs**.
2. Configurez sous **Port Based VLANs** le **Acceptable Frame Type** pour le port de pont sélectionné.
   Options disponibles :

Option	Description
All	**Par défaut** Les trames ingress balisées et non balisées sont acceptées.
Tagged Frames Only	Seules les trames de VLAN ingress non balisées sont acceptées.
Untagged and Priority Tagged Only	Seules les trames ingress non balisées ou les trames avec valeur de priorité sont acceptées.

3. Validez la modification.

12.2.3.4 Activation du balisage PVID pour le trafic de données sortant

Le balisage PVID garantit que toutes les trames sortant sur le VLAN natif d'un port de pont sont balisées. Cette option est désactivée par défaut, ce qui signifie que les trames sont retransmises sans être balisées.

Remarque

L'activation du balisage PVID augmente la consommation de bande passante, car des balises VLAN supplémentaires sont ajoutées à l'en-tête de chaque trame. Plus la trame est petite, plus la consommation est importante.

Pour activer le balisage PVID pour un port de pont, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **VLANs**.
2. Sous **Port Based VLANs**, modifiez **Egress Tag** en **Enabled** pour le port de pont sélectionné.
3. Validez la modification.

12.2.3.5 Activation du filtre ingress

Par défaut, le filtre ingress est désactivé pour tous les ports du pont.

Pour activer le filtre Ingress pour un port de pont, procédez comme suit :

Remarque

Activez le filtre ingress si vous utilisez des listes de VLAN interdits. Les listes de VLAN interdits empêchent simplement un port de pont de rejoindre des VLAN définis. Elles n'empêchent pas qu'une trame d'un VLAN figurant dans la liste des VLAN interdits soit transmise à un autre port de pont qui est membre de ce VLAN.

1. Naviguez vers **Layer 2** ≫ **VLANs**.
2. Sous **Port Based VLANs**, modifiez **Ingress Filter** en **Enabled** pour le port de pont sélectionné.
3. Validez la modification.

12.2.3.6 Limitation de l'appartenance à un VLAN

Pour définir la liste des VLAN interdits pour un port de pont, procédez comme suit :

IMPORTANT
Risque de configuration - Risque de perte de données La liste des VLAN interdits doit être configurée de la même manière aux deux extrémités du lien. Les trames excédentaires risquent sinon d'être rejetées.

Remarque

Le port de pont sélectionné doit être défini comme port de jonction.

Remarque

Activez le filtre ingress si vous utilisez des listes de VLAN interdits. Les listes de VLAN interdits empêchent simplement un port de pont de rejoindre des VLAN définis. Elles n'empêchent pas qu'une trame d'un VLAN figurant dans la liste des VLAN interdits soit transmise à un autre port de pont qui est membre de ce VLAN.

Pour plus d'informations sur l'activation du filtre ingress, voir "Activation du filtre ingress (Page 257)".

1. Naviguez vers **Layer 2** ≫ **VLANs**.
2. Sous **Port Based VLANs**, sélectionnez un port de pont et sélectionnez ensuite un ou plusieurs VLAN de la liste **Forbidden VLANs** .
3. Validez la modification.

12.3 Classes de trafic

La classification du trafic consiste à catégoriser et à contrôler la transmission des trames. Elle sert à améliorer les performances du réseau et offre une qualité de service différente pour sélectionner les types de trafic.

Ce paragraphe décrit comment effectuer la classification du trafic de données à l'aide des classes de trafic.

12.3.1 Ce qu'il faut savoir sur les classes de trafic

Les classes de trafic sont une forme de classification du trafic dans laquelle les trames entrantes sont mises en file d'attente en fonction de leur priorité. Un algorithme est ensuite appliqué à chaque file d'attente afin de déterminer quelle file d'attente est autorisée à transmettre des trames en premier, sur la base d'un schéma de traitement unique par algorithme. Cela permet à l'appareil de donner la priorité à la livraison de données souvent sujettes à des pertes et à des délais critiques par rapport aux informations moins critiques.

La classification du trafic est une fonction automatique qui peut être définie par l'utilisateur pour chaque port. Pour chaque port de pont, il est possible de configurer les éléments suivants :

- Affectez des trames aux files d'attente des classes de trafic.
- Modifier la priorité d'une trame lors du transfert (egress).

Lorsqu'une trame est reçue sur un port de pont, l'interface ingress affecte la trame à une classe de trafic dans les phases suivantes :

1. **Contrôle et priorisation**
   Chaque trame est examinée à la réception et une priorité lui est affectée. En fonction des réglages individuels du port de pont, la priorisation peut être basée sur :
   - la balise Priority Code Point (PCP) de la trame
   - la balise Differentiated Services Code Point (DSCP) de la trame
   - la priorité par défaut du port de pont
2. **Affectation**
   La trame est affectée à une classe de trafic en fonction de la priorité de la file d'attente déterminée lors de la phase précédente. Cette affectation peut être adaptée pour les valeurs PCP et DSCP.
   Pour plus d'informations sur l'affectation par défaut de la priorité à la file d'attente, voir "Affectation par défaut (Page 261)".
3. **Retransmission**
   Dès qu'une trame de la file d'attente a été affectée à une classe de trafic, elle attend d'être retransmise. La transmission s'effectue selon un ordre déterminé par le schéma de traitement. Lorsque les trames d'une file d'attente ont été retransmises, les trames de la file d'attente suivante sont transférées.
   À ce stade, il est possible, si nécessaire, d'attribuer une priorité différente à chaque trame 802.1Q de couche 2 balisée lors de son transfert depuis un port de pont spécifique, ou de conserver la priorité actuelle.

12.3.1.1 Files d'attente de classes de trafic

Le trafic de données peut être affecté au maximum à huit files d'attente de classes de trafic (0 à 7). Sur la base de la norme IEEE 802.1Q, les priorités suivantes doivent être affectées aux files d'attente et elles peuvent être utilisées pour les types de trafic suivants :

Priorité	Type	Description
7	Contrôle du réseau	Trafic de données qui prend en charge la configuration et la maintenance de la structure du réseau.
6	Contrôle Inter Réseau	Trafic de données qui prend en charge l'infrastructure de réseau qui doit être délimitée par le domaine administratif.
5	Langue	Trafic de données avec une temporisation de moins de 10 ms et une gigue maximale.
4	Vidéo	Trafic de données avec une temporisation de 100 ms ou autres applications à faible latence, telles que les communications vidéo interactives.
3	Applications critiques	Trafic de données nécessitant une bande passante minimale garantie, mais soumis à une forme de contrôle d'accès afin d'éviter qu'une application ne consomme de la bande passante au détriment des autres applications.
2	Excellent Effort	Trafic de données qu'une organisation de services d'information peut prioriser pour des clients sélectionnés. Il s'agit d'un service de type Best Effort.
0 (par défaut)	Best Effort	Trafic de données pour applications non prioritaires. Le traitement équitable est basé sur la stratégie de redimensionnement dynamique des fenêtres et de retransmission définis par le protocole TCP (Transmission Control Protocol) du service. Il s'agit d'un service Best Effort associé au trafic de données LAN traditionnel.
1	Arrière-plan	Trafic de données qui prend en charge l'exécution d'opérations non critiques en arrière-plan (telles que les transferts de masse) pour ne pas affecter l'utilisation du réseau par les autres utilisateurs et applications.

12.3.1.2 Schéma de traitement

Les schémas de traitement des trames (ou de répartition de la charge) contrôlent l'ordre dans lequel les files d'attente des classes de trafic retransmettent les trames. Chaque schéma applique ses propres règles/stratégies afin de fournir une qualité de service univoque.

À ce stade, SINEC OS applique le schéma de traitement **Strict**. Strict est un algorithme qui n'autorise la transmission des trames d'une file d'attente qu'après la transmission des trames de toutes les files d'attente de priorité supérieure. Exemple : La file d'attente de la classe de trafic 5 ne peut être traitée qu'une fois que la file d'attente de la classe de trafic 6 a été entièrement traitée.

12.3.1.3 Affectation par défaut

Par défaut, les trames entrantes sont affectées aux files d'attente des classes de trafic en fonction de leur marqueur PCP ou DSCP, comme suit :

DSCP	PCP	File d'attente
0 - 7	1	0
8 - 15	0	1
16 - 23	2	2
24 - 31	3	3
32 - 39	4	4
40 - 47	5	5
48 - 55	6	6
56 - 63	7	7

Cette affectation peut être adaptée pour les valeurs PCP et/ou DSCP. Pour plus d'informations, voir "Affectation d'une classe de trafic à une valeur PCP (Page 264)" et/ou "Affectation d'une valeur DSCP à une classe de trafic (Page 265)".

12.3.1.4 Priorisation de paquets de trames entrantes.

Les paragraphes suivants expliquent comment les trames entrantes sont priorisées et retransmises :

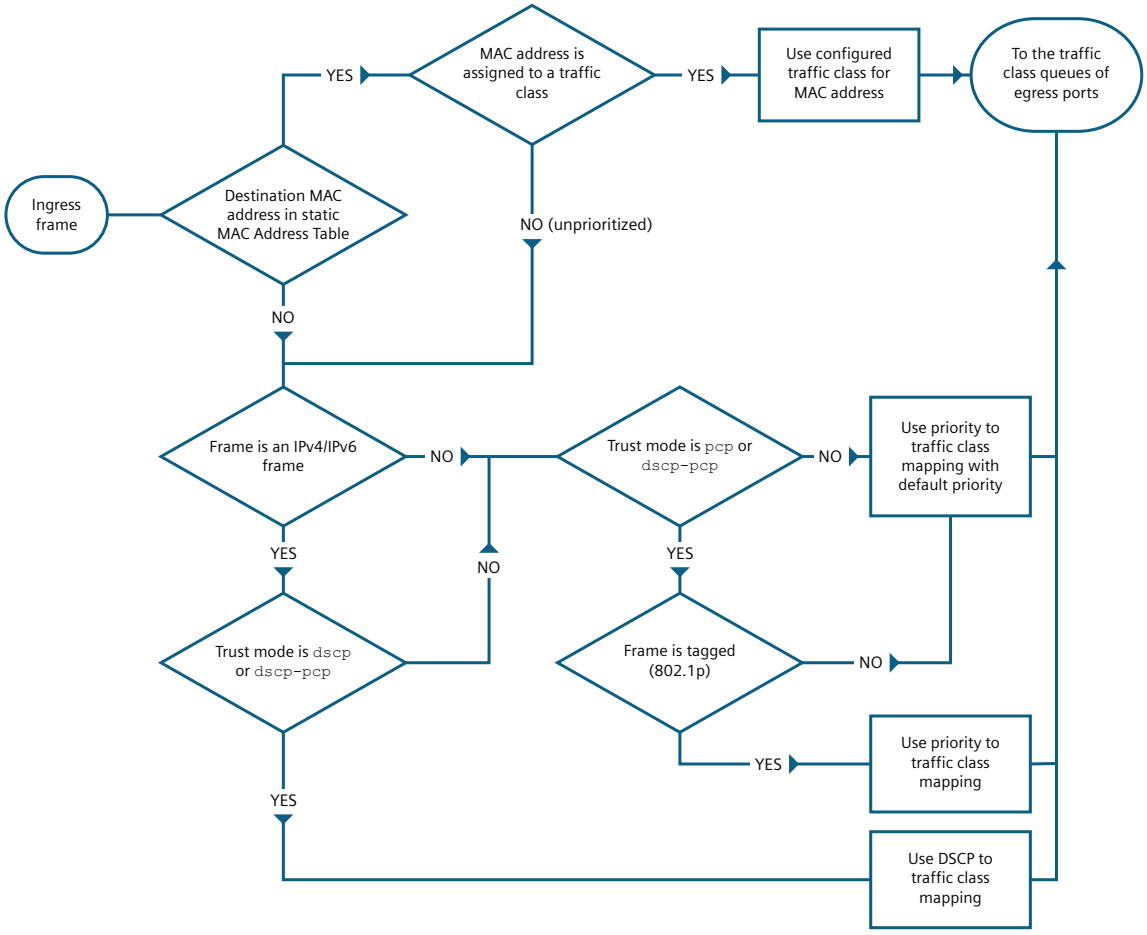


Figure 12-6 Priorisation de trames entrantes

12.3.1.5 Régénération des priorités

Les paragraphes suivants expliquent comment la priorité affectée à une trame entrante est régénérée à la sortie :

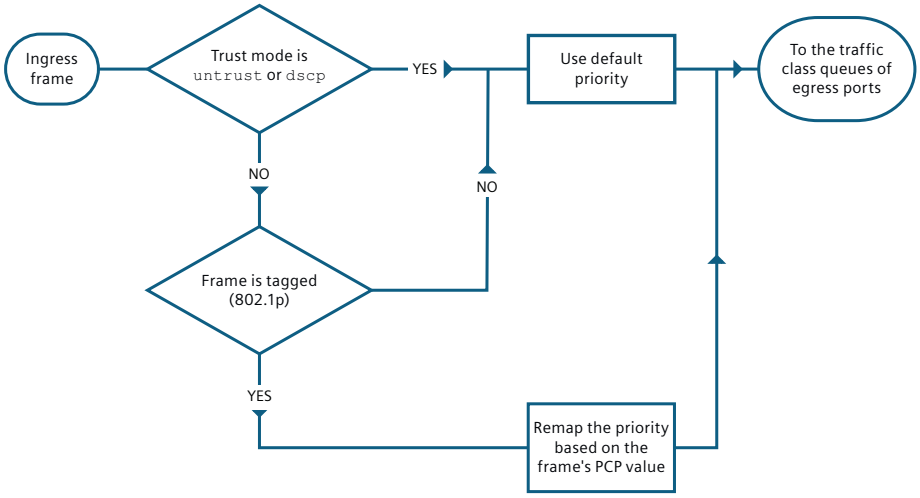


Figure 12-7 Régénération des priorités

12.3.2 Configuration des classes de trafic

Pour configurer des classes de trafic, configurez un ou plusieurs ports de pont pour qu'ils attribuent des classes de trafic aux trames reçues.

Les classes de trafic pour les ports de pont sont configurées en fonction du trafic de données reçu sur chaque port.

- Les trames 802.1Q de couche 2 balisées ont une valeur PCP dans leur en-tête qui permet d'affecter la trame à la file d'attente correspondante de la classe de trafic.
- Les trames de la couche 3 ont une valeur DSCP de 6 bits dans leur en-tête, grâce à laquelle la trame est affectée à une file d'attente de la classe de trafic.

Un port de pont peut recevoir un ou les deux types de trames. Il peut également recevoir des trames qui n'ont aucune des deux valeurs dans l'en-tête.

Pour configurer des classes de trafic pour les ports de pont, procédez comme suit :

1. [Facultatif] Configurez la priorité par défaut du port de pont. Cette priorité est automatiquement affectée à chaque trame qui n'a pas sa propre priorité.
   Pour plus d'informations, voir "Configuration de la priorité par défaut (Page 264)".
2. Définissez la manière dont le port de pont affecte les trames à la file d'attente correspondante de la classe de trafic.
   - Pour les trames 802.1Q de couche 2 balisées, voir "Affectation d'une classe de trafic à une valeur PCP (Page 264)"
   - Pour les trames de couche 3, voir "Affectation d'une valeur DSCP à une classe de trafic (Page 265)"

3. Si le port Bridge est une interface ingress, définissez le mode de confiance.
   Pour plus d'informations, voir "Configuration du mode de confiance (Page 265)".
4. [Facultatif] Pour les trames 802.1Q de couche 2 balisées uniquement, utilisez le changement de priorité pour modifier la valeur PCP lorsque la trame est transmise.
   Pour plus d'informations, voir "Affectation de différentes priorités au trafic de données sortant (egress) (Page 266)".

12.3.2.1 Configuration de la priorité par défaut

Une priorité par défaut doit être affectée à chaque port du pont. Cette priorité est affectée à chaque trame qui n'a pas été priorisée en fonction de son contenu. En particulier si les champs de couche 2/3 pour la priorisation automatique manquent dans l'en-tête. Une priorité par défaut est automatiquement affectée à ces trames à leur arrivée. Les trames sont ensuite affectées à la file d'attente correspondante de la classe de trafic en fonction de la priorité affectée.

La priorité par défaut peut également être utilisée si "**untrust**" est paramétré pour le mode de confiance, même si une valeur PCP ou DSCP est présente.

Pour configurer la priorité par défaut d'un port de pont, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Traffic Classes** ≫ **Queuing Policy & Trust Modes**.
2. Sous **Default Priorities and Trust Modes**, configurez la **Default Priority** du port de pont sélectionné.
   Condition :
   – Un nombre compris entre 0 et 7

   Par défaut : 0
3. Validez la modification.

12.3.2.2 Affectation d'une classe de trafic à une valeur PCP

Certaines trames 802.1Q de couche 2 balisées contiennent une valeur de Priority Code Point (PCP) dans leur en-tête de balise 802.1Q. SINEC OS affecte chaque valeur d'une file d'attente spécifique à une classe de trafic, ce qui peut être paramétré individuellement pour chaque port de pont.

Pour plus d'informations sur l'affectation par défaut de valeurs PCP aux files d'attente de classes de trafic, voir "Affectation par défaut (Page 261)".

Remarque

Jusqu'à huit affectations sont autorisées par port de pont.

Pour configurer un port de pont de manière à ce qu'une valeur PCP spécifique soit affectée à une file d'attente spécifique d'une classe de trafic, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Traffic Classes** ≫ **Priority Mappings**.
2. Sous **Interface Selection**, sélectionnez un port de pont ou sélectionnez **All** pour appliquer vos modifications à tous les ports de pont.

3. Sous **PCP to Interface Queue Mappings**, sélectionnez dans **Queue** une file d'attente d'une classe de trafic pour chaque code de la colonne **PCP Code** .
   Les trames de couche 2 balisées selon 802.1Q avec l'une des valeurs PCP sont affectées à la file d'attente correspondante d'une classe de trafic.
4. Validez la modification.

12.3.2.3 Affectation d'une valeur DSCP à une classe de trafic

Certaines trames de couche 3 contiennent une valeur DSCP (Differentiated Services Code Point) dans leur en-tête IPv4/IPv6. SINEC OS affecte chaque valeur d'une file d'attente spécifique à une classe de trafic, ce qui peut être paramétré individuellement pour chaque port de pont.

Pour plus d'informations sur l'affectation par défaut des valeurs DSCP aux files d'attente des classes de trafic, voir "Affectation par défaut (Page 261)".

Remarque

Jusqu'à 64 affectations sont autorisées par port de pont.

Pour configurer un port de pont de manière à ce qu'une valeur DSCP spécifique soit associée à une file d'attente spécifique d'une classe de trafic, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Traffic Classes** ≫ **Priority Mappings**.
2. Sous **Interface Selection**, sélectionnez un port de pont ou sélectionnez **All** pour appliquer vos modifications à tous les ports de pont.
3. Sous **DSCP to Interface Queue Mappings**, sélectionnez dans **Queue** une file d'attente d'une classe de trafic pour chaque code de la colonne DSCP.
   Les trames de couche 3 balisées avec l'une des valeurs PCP sont affectées à la file d'attente correspondante d'une classe de trafic.
4. Validez la modification.

12.3.2.4 Configuration du mode de confiance

Le mode de confiance détermine si un port de pont utilise la valeur PCP (Priority Code Point) et/ou la valeur DSCP (Differentiated Services Code Point) pour donner la priorité aux trames entrantes, ou s'il doit appliquer sa propre priorité par défaut.

Le mode confiance peut être configuré de plusieurs manières :

- **Ne faire confiance qu'aux valeurs PCP (PCP)**
  Les trames sont uniquement priorisées en fonction de leurs valeurs PCP. Les valeurs DSCP sont ignorées. Si la valeur PCP manque, c'est la priorité par défaut qui est utilisée.
- **Ne faire confiance qu'aux valeurs DSCP (DSCP)**
  Les trames sont uniquement priorisées en fonction de leurs valeurs DSCP. Les valeurs PCP sont ignorées. Si la valeur DSCP manque, c'est la priorité par défaut qui est utilisée.

- **Faire confiance aux valeurs DSCP et PCP (DSCP-PCP)**
  Les trames sont priorisées d'abord en fonction de leurs valeurs DSCP puis en fonction de leurs valeurs PCP. Si les deux valeurs manquent, c'est la priorité par défaut qui est utilisée.
- **Ne pas faire confiance aux valeurs DSCP et PCP (Untrust)**
  Il n'est fait confiance ni aux valeurs DSCP, ni aux valeurs PCP. La priorité par défaut ne s'applique qu'à toutes les trames entrantes.

Pour configurer le mode de confiance (Trust Mode) pour un port de pont ingress, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Traffic Classes** ≫ **Queuing Policy & Trust Modes**.
2. Sous **Default Priorities and Trust Modes**, configurez la **Trust Mode** du port de pont sélectionné.
   Options disponibles :

Option	Description
PCP	**Par défaut** Les trames entrantes sont priorisées en fonction de la valeur PCP. La valeur DSCP (si elle existe) est ignorée. Si la valeur PCP manque, la trames entrante est priorisée en fonction de la priorité par défaut de l'interface.
Untrust	Les trames entrantes sont priorisées en fonction de la priorité par défaut de l'interface. Les valeurs PCP et DSCP (si elles existent) sont ignorées.
DSCP	Les trames entrantes sont priorisées en fonction de leur valeur DSCP. La valeur PCP (si elle existe) est ignorée. Si la valeur DSCP manque, la trame est priorisée en fonction de la priorité par défaut de l'interface.
DSCP-PCP	Les trames entrantes sont d'abord priorisées en fonction de leur valeur DSCP. Si la valeur DSCP manque, la trame est priorisée en fonction de sa valeur PCP (si elle existe). Si la trame ne possède aucune de ces valeurs, c'est la priorité par défaut de l'interface qui est utilisée.

3. Validez la modification.

12.3.2.5 Affectation de différentes priorités au trafic de données sortant (egress)

Par défaut, la valeur PCP de chaque trame entrante et sortante de l'appareil, balisée 802.1Q de couche 2 n'en est pas affectée. Cependant, dans certains cas, il peut être souhaitable d'attribuer une priorité différente à une trame lorsqu'elle est retransmise. P. ex., si une trame est transférée d'un domaine à un autre, il peut être nécessaire de modifier la valeur de priorité de certaines trames pour qu'elle corresponde à l'affectation de la priorité à la classe de trafic de destination.

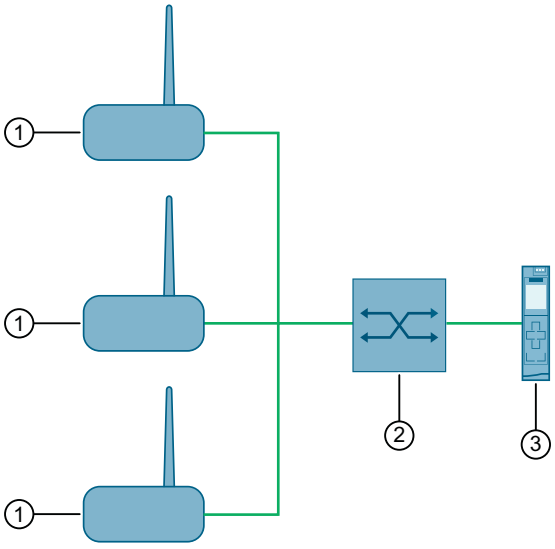
Le changement de priorité s'applique aux trames qui, lorsqu'elles sont reçues (ingress), ont une valeur de priorité spécifique, et attribue une nouvelle valeur à cette priorité lorsqu'elles sont retransmises (egress). Les trames concernées sont affectées à une classe de trafic sur la base de la valeur de priorité initiale de la file d'attente correspondante, mais elles sont retransmises avec une valeur de priorité différente.

Pour configurer un port de pont de manière à ce que le changement de priorité soit appliqué aux trames sélectionnées, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Traffic Classes** ≫ **Priority Mappings**.
2. Sous **Interface Selection**, sélectionnez un port de pont ou sélectionnez **All** pour appliquer vos modifications à tous les ports de pont.
3. Sous **Priority Regeneration**, sélectionnez pour la valeur de priorité ingress voulue (**Ingress Priority**) dans **Egress Priority** une valeur de priorité pour la retransmission.
4. Validez la modification.

12.3.3 Exemples de configuration

Les exemples de configuration suivants montrent différentes procédures pour éviter la perte de trames de haute priorité. Chaque exemple est basé sur un scénario unique dans lequel une série de capteurs sur une ligne de production envoient des messages à une CPU SIMATIC S7 via un commutateur sur lequel SINEC OS est installé.



① Capteur
② Commutateur
③ CPU SIMATIC S7

Figure 12-8 Topologie de classes de trafic de base

12.3.3.1 Priorisation de toutes les trames

Dans cette version du scénario, toutes les trames reçues par le commutateur sont considérées comme importantes, indépendamment de la priorité qui leur est respectivement affectée.

Méthode 1 : Affectation d'une priorité élevée à chaque trame

Dans SINEC OS, la valeur de priorité des trames est ignorée et c'est la priorité par défaut du port de pont récepteur qui est affectée.

1. Définissez une priorité élevée pour la priorité par défaut de chaque port de pont connecté aux capteurs, par exemple 7 (la priorité la plus élevée).
   Pour plus d'informations, voir "Configuration de la priorité par défaut (Page 264)".
2. Paramétrez pour chaque port de pont connecté aux capteurs le mode de confiance **Untrust**.
   Pour plus d'informations, voir "Configuration du mode de confiance (Page 265)".
3. [Facultatif] Envoyez le trafic de données des capteurs et observez les files d'attente du trafic pour vérifier que les trames importantes obtiennent une priorité plus élevée que les autres trames.

Méthode 2 : Priorisation de trames avec une valeur de priorité spécifique

Sous SINEC OS, seules les trames ayant des valeurs PCP ou DSCP ou les deux sont priorisées.

1. Définissez l'une des valeurs suivantes pour chaque port de pont connecté aux capteurs pour le mode de confiance :

Option	Description
PCP	Toutes les trames sont classées dans la file d'attente associée à leur valeur PCP.
DSCP	Toutes les trames sont classées dans la file d'attente associée à leur valeur DSCP.
DSCP-PCP	Toutes les trames sont classées dans la file d'attente associée à leur valeur DSCP ou PCP. Les trames avec une valeur DSCP sont priorisées en premier.

2. [Facultatif] Envoyez le trafic de données des capteurs et observez les files d'attente du trafic pour vérifier que les trames importantes obtiennent une priorité plus élevée que les autres trames.

12.3.3.2 Priorisation de trames sélectionnées

Dans cette version du scénario, la priorité est accordée à des trames spécifiques contenant des messages critiques, comme ceux qui indiquent une interruption de la production. Ces messages doivent être reçus par la CPU SIMATIC S7 avant toutes les autres trames.

Méthode 1 : Configurer les capteurs de manière à ce qu'une priorité élevée soit affectée à chaque trame à la réception

Si les capteurs peuvent contrôler la priorité affectée aux trames à la réception, configurez chaque capteur de manière à attribuer une priorité élevée aux trames contenant des informations

importantes. L'appareil place automatiquement ces trames dans une file d'attente de haute priorité.

1. Attribuez pour, chaque capteur, une priorité élevée aux trames importantes en entrée.
2. Définissez, pour le mode de confiance, l'une des valeurs **PCP** (trafic de données de couche 2 uniquement), **DSCP** (trafic de données de couche 3 uniquement) ou **DSCP-PCP**(trafic de données de couche 3 suivi du trafic de données de couche 2) dans la configuration du commutateur.
   Pour plus d'informations, voir "Configuration du mode de confiance (Page 265)".
3. [Facultatif] Envoyez le trafic des capteurs et vérifiez à la fin la priorité des trames avec un outil de capture de paquets.

Méthode 2 : Affectation aux trames entrantes de la priorité par défaut du port de pont

Sous SINEC OS, une priorité par défaut élevée est affectée au port de pont qui reçoit les trames. Toute trame à laquelle une priorité n'est pas affectée en raison de son contenu est automatiquement transférée vers la file d'attente correspondante dès son arrivée.

1. Indiquez une valeur élevée comme priorité par défaut pour chaque port de pont connecté aux capteurs, par exemple 7 (la priorité la plus élevée).
   Pour plus d'informations, voir "Configuration de la priorité par défaut (Page 264)".
2. Définissez pour le mode de confiance l'une des valeurs **PCP** (trafic de données de couche 2 uniquement) ou **DSCP-PCP**(trafic de données de couche 3, suivi du trafic de données de couche 2).
   Pour plus d'informations, voir "Configuration du mode de confiance (Page 265)".
3. [Facultatif] Envoyez le trafic des capteurs et vérifiez à la fin la priorité des trames avec un outil de capture de paquets.

Méthode 3 : Réaffectation des priorités en sortie

Sous SINEC OS, la priorité affectée aux trames importantes est affectée à une priorité plus élevée.

1. Pour chaque port de pont connecté aux capteurs, indiquez une valeur plus élevée pour la priorité affectée aux trames importantes, par exemple 7 (la priorité la plus élevée).
   Pour plus d'informations, voir "Affectation d'une classe de trafic à une valeur PCP (Page 264)" et/ou "Affectation d'une valeur DSCP à une classe de trafic (Page 265)".
2. Définissez pour le mode de confiance une des valeurs **PCP** (trafic de données de couche 2 uniquement) ou **DSCP-PCP**(trafic de données de couche 3, suivi du trafic de données de couche 2).
   Pour plus d'informations, voir "Configuration du mode de confiance (Page 265)".
3. [Facultatif] Envoyez le trafic des capteurs et vérifiez à la fin la priorité des trames avec un outil de capture de paquets.

Affichage des paramètres de date/heure 13

Ce chapitre décrit comment configurer les services d'horloge pour la saisie des temps et la synchronisation de l'heure. Cela comprend le réglage manuel ou automatique de l'heure et de la date du système à l'aide d'un service tel que NTP.

Il est important de régler correctement la date/heure et de vérifier que l'heure est synchronisée sur tous les appareils pour une bonne gestion et pour le dépannage du réseau. Ils sont nécessaires pour horodater les entrées des journaux système qui aident à suivre les évènements tels que l'utilisation du réseau, les violations de sécurité et les changements de configuration des appareils.

Remarque

Vous ne pouvez activer qu'un seul service d'horloge. Si l'heure est définie automatiquement par un service, comme NTP ou SIMATIC Time, vous ne pouvez pas configurer l'heure du système manuellement. Toute tentative de configuration manuelle de l'heure du système sera refusée.

13.1 Affichage de la date et de l'heure système

Pour afficher des informations sur la date/l'heure sytème, naviguez vers **System** ≫ **System Time**.

Sous **System Time**, l'écran affiche les informations suivantes :

Paramètres	Description
System Clock	Affiche la date et l'heure système réglées
Time Zone	Affiche le fuseau horaire paramétré.

13.2 Configuration de la date et de l'heure système

Pour configurer manuellement la date et l'heure du système, procédez comme suit :

1. Naviguez vers **System** ≫ **System Time**.
2. Sous **System Time**, modifiez le paramètre **System Clock [YYYY-MM-DD HH:MM:SS]**.
   Conditions :
   - **YYYY** indique l'année
   - **MM** indique le mois (01 - 12)
   - **DD** indique le jour (01 - 31)
   - **HH** indique l'heure (00 - 23)
   - **MM** indique les minutes (00 - 59)
   - **SS** indique les secondes (00 - 59)
3. Cliquez sur **Apply**.

13.3 Utilisation de la date et de l'heure système du PC client

Pour utiliser la date et l'heure système du PC client, procédez comme suit :

1. Naviguez vers **System** ≫ **System Time**.
2. Sous **System Time**, cliquez sur **Use PC-Time**.
   L'appareil adopte la date et de l'heure système du PC client. La date et l'heure système sont inscrites dans le champ **System Clock**.

13.4 Configuration du fuseau horaire

Remarque

Les fuseaux horaires ne comprennent pas tous des règles de passage à l'heure d'été/hiver. Vérifiez auparavant si le fuseau horaire voulu comprend ou non des règles de passage à l'heure d'été/hiver.

Pour configurer le fuseau horaire, procédez comme suit :

1. Naviguez vers **System** ≫ **System Time**.
2. Sous **System Time**, modifiez le paramètre **Time Zone**.
   Par défaut : UTC
3. Validez la modification.

13.5 NTP

Ce chapitre décrit la configuration du Network Time Protocol (NTP)

13.5.1 Ce qu'il faut savoir sur Network Time Protocol

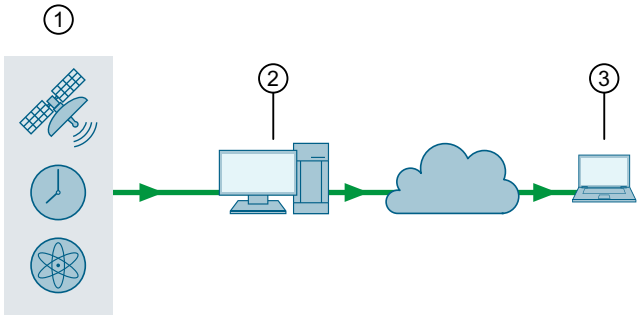
NTP est un protocole de synchronisation horaire hiérarchique entre les serveurs NTP et les clients NTP d'un réseau.

Les implémentations NTP envoient et reçoivent des informations sur l'heure via le User Datagram Protocol (UDP) sur le port 123. Vous pouvez configurer NTP pour que les clients NTP écoutent les trames de broadcast ou de multicast contenant des mises à jour de l'heure.

Le NTP prend en charge les horodatages, que vous pouvez utiliser pour comparer les messages de diagnostic, les évènements, etc. de différents constituants de réseau.

NTP envoie toujours le temps universel coordonné UTC (Universal Time Coordinated). Il correspond à l'heure du fuseau horaire GMT (Greenwich Mean Time).

L'avantage de NTP réside dans la possibilité de synchroniser l'heure au-delà des limites du sous-réseau.

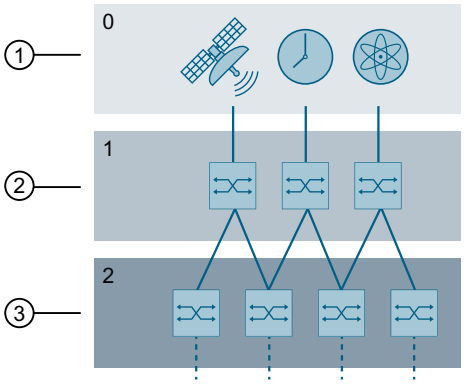


① Source de temps de référence (par exemple, horloge atomique/radioélectrique, récepteur GPS ou service horaire par modem)
② Serveur NTP
③ Client NTP

Figure 13-1 NTP

13.5.1.1 Numéro de strate

Un réseau NTP obtient ses informations horaires à partir d'une source horaire faisant autorité, comme les horloges atomiques/radio, les récepteurs GPS ou les services horaires par modem. Ces informations horaires sont ensuite transmises des serveurs aux clients via NTP. Le nombre de sauts entre un client et la source temporelle déterminante est indiqué par le numéro de strate.



① Niveau de strate 0 (source temporelle déterminante)
② Niveau de strate 1
③ Niveau de strate 2

Figure 13-2 Niveau de strate NTP

Un appareil peut être à la fois le client NTP de la strate supérieure et le serveur de la strate inférieure, s'il en existe une :

- En tant que client NTP, l'appareil récupère l'heure de référence d'un ou de plusieurs serveurs NTP.
- En tant que serveur NTP, l'appareil compare son heure système à d'autres serveurs NTP. Les serveurs NTP se mettent d'accord sur une heure commune à laquelle tous se conforment.

Les serveurs NTP de niveau strate 1 se synchronisent sur une source de temps faisant autorité avec la strate 0 et mettent leur temps à la disposition des clients NTP, appelés strate 2. Un maximum de 16 niveaux de strates est possible.

Les clients NTP utilisent le numéro de strate pour choisir la source de temps la plus fiable. Pour les clients NTP, le numéro de strate est attribué automatiquement, en fonction du nombre de sauts vers la source de temps déterminante.

13.5.1.2 Serveur NTP

Un serveur NTP met son heure à la disposition des clients NTP connectés. Le serveur NTP écoute les requêtes d'heure sur ses interfaces NTP et répond avec son heure de référence.

Le numéro de strate d'un serveur NTP correspond au numéro de strate du serveur de temps en amont + 1.

Le serveur lui-même peut obtenir ses informations sur l'heure à partir de différentes sources :

- Serveur NTP
- NTP Broadcast Server

- NTP Multicast Server
- Horloge logicielle locale

13.5.1.3 Client NTP

Un client NTP envoie des requêtes d'heure à intervalles réguliers et synchronise ainsi activement son heure système. Pour cela, le client NTP compense le retard dû au temps de transmission par des conversions.

Le client peut obtenir ses informations sur l'heure à partir de différentes sources :

- Serveur NTP
- NTP Broadcast Server
- NTP Multicast Server

Si vous configurez plusieurs serveurs, le client interroge tous les serveurs et évalue leurs trames de réponse. Le client choisit le serveur avec la plus grande précision. Cela permet de garantir que le client synchronise son heure système avec une heure exacte. La précision dépend de la qualité du serveur utilisé.

13.5.2 Configuration de NTP

Pour configurer l'appareil comme client NTP, procédez comme suit :

1. Configurez un serveur NTP.
   Pour plus d'informations, voir "Configuration d'un serveur NTP (Page 275)".
2. [Facultatif] Activez un serveur NTP.
   Pour plus d'informations, voir "Activation d'un serveur NTP (Page 276)".
3. [Facultatif] Si une version autre que NTP V4 est requise, définissez la version de NTP.
   Pour plus d'informations, voir "Configuration de la version de NTP (Page 276)".
4. [Facultatif] Configurez les valeurs de l'intervalle d'interrogation.
   Pour plus d'informations, voir "Configuration de l'intervalle d'interrogation NTP (Page 276)".
5. [Facultatif] Pour accélérer la synchronisation lors de la première connexion, activez iBurst.
   Pour plus d'informations, voir "Activation de iBurst (Page 277)".
6. [Facultatif] Pour améliorer la qualité de la synchronisation de l'horloge, activez Burst.
   Pour plus d'informations, voir "Activation de Burst (Page 277)".
7. Activez NTP.
   Pour plus d'informations, voir "Activation de NT (Page 277)".

13.5.2.1 Configuration d'un serveur NTP

Aucun serveur NTP n'est configuré par défaut.

Pour définir un serveur NTPl, procédez comme suit :

1. Naviguez vers **System** ≫ **Time Synchronisation** ≫ **NTP Client**.
2. Sous **NTP Unicast Server**, cliquez sur **Add**.
   Une nouvelle ligne est insérée dans le tableau.
3. Entrez sous **Server Address** l'adresse IP du serveur NTP.
   Vous ne pouvez éditer l'adresse IP du serveur NTP qu'immédiatement après avoir ajouté une nouvelle ligne. Dès que le champ n'est plus actif, l'adresse IP passe en lecture seule. Si vous voulez modifier l'adresse IP, supprimez l'Serveur NTP et configurez-le à nouveau.
   Un serveur NTP nouvellement configuré est par défaut automatiquement activé.
4. Validez les modifications.

13.5.2.2 Activation d'un serveur NTP

Un serveur NTP est activé par défaut.

Pour activer un serveur NTP, procédez comme suit :

1. Naviguez vers **System** ≫ **Time Synchronisation** ≫ **NTP Client**.
2. Sous **NTP Unicast Server**, modifiez le paramètre **Status** en **Enabled**.
3. Validez la modification.

13.5.2.3 Configuration de la version de NTP

Ne modifiez la version de NTP que si une version autre que NTP V4 est requise.

Pour configurer la version de NTP utilisée, procédez comme suit :

1. Naviguez vers **System** ≫ **Time Synchronisation** ≫ **NTP Client**.
2. Sous **NTP Unicast Server**, modifiez dans la colonne **NTP version** la version de NTP.
   Condition :
   – Un nombre compris entre 1 et 4

   Par défaut : 4
3. Validez la modification.

13.5.2.4 Configuration de l'intervalle d'interrogation NTP

Pour configurer l'intervalle d'interrogation d'un serveur NTP, procédez comme suit :

1. Naviguez vers **System** ≫ **Time Synchronisation** ≫ **NTP Client**.
2. Sous **NTP Unicast Server**, définissez dans la colonne **Minpoll [s]** la plus petite valeur en secondes de l'intervalle d'interrogation comme puissance de 2.
   Condition :
   – Un nombre compris entre 4 et 17

   Par défaut : 6
   La valeur 6 correspond à 2^6 (64 secondes).

3. Sous **Maxpoll [s]**, définissez la plus grande valeur de l'intervalle d'interrogation en secondes comme puissance de 2.
   Condition :
   – Un nombre compris entre 4 et 17

   Par défaut : 10
   La valeur 10 correspond à 2^{10} (1024 secondes).
4. Validez les modifications.

13.5.2.5 Activation de iBurst

iBurst (initial Burst) augmente le nombre de trames par intervalle d'interrogation lorsque le serveur NTP n'est pas accessible, en le faisant passer d'une trame à six trames. Cela permet d'accélérer la synchronisation lors de la première connexion.

iBurst est désactivé par défaut. Vous pouvez activer iBurst par serveur configuré.

Pour activer iBurst pour un serveur NTP, procédez comme suit :

1. Naviguez vers **System** ≫ **Time Synchronisation** ≫ **NTP Client**.
2. Sous **NTP Unicast Server**, modifiez le paramètre **iBurst** en **Enabled**.
3. Validez la modification.

13.5.2.6 Activation de Burst

Burst augmente le nombre de trames par intervalle d'interrogation lorsque le serveur NTP est accessible. iBurst, contrairement à Burst, augmente le nombre de trames par intervalle d'interrogation lorsque le serveur NTP n'est pas accessible.

Grâce à Burst, les écarts par rapport à la source de temps sont réduits et la qualité de la synchronisation de l'horloge est améliorée.

Le nombre de trames par Burst est égal à la puissance de 2 de la différence entre la valeur actuelle et la plus petite valeur de l'intervalle d'interrogation. Une trame est envoyée à la plus petite valeur prédéfinie de l'intervalle d'interrogation 6 (64 secondes). Le nombre maximal de huit trames est envoyé à partir d'un intervalle d'interrogation de 9 (512 secondes). Cela permet de garantir que l'intervalle d'interrogation moyen ne dépasse pas le plus petit intervalle d'interrogation.

Burst est désactivé par défaut. Vous pouvez activer Burst par serveur configuré.

Pour activer Burst pour un serveur NTP, procédez comme suit :

1. Naviguez vers **System** ≫ **Time Synchronisation** ≫ **NTP Client**.
2. Sous **NTP Unicast Server**, modifiez le paramètre **Burst** en **Enabled**.
3. Validez la modification.

13.5.2.7 Activation de NT

Par défaut, NTP est désactivé.

Pour activer NTP, procédez comme suit :

1. Naviguez vers **System** ≫ **Time Synchronisation** ≫ **NTP Client**.
2. Sous **Network Time Protocol (NTP) Client**, modifiez le paramètre **NTP Client** en **Enabled**.
3. Validez la modification.

13.5.3 Affichage de la configuration NTP

Pour afficher la configuration NTP, naviguez vers **System** ≫ **Time Synchronisation** ≫ **NTP Client**.

Sous **Network Time Protocol (NTP) Client**, l'écran affiche les informations suivantes :

Paramètres	Description
NTP Client	Indique si NTP est activé.

Sous **NTP Unicast Server**, l'écran affiche les informations suivantes :

Paramètres	Description
Server Address	Affiche l'adresse IP du serveur NTP.
Status	Indique si le serveur NTP est activé.
NTP Version	Affiche la version de NTP utilisée.
Minpoll [s]	Affiche la plus petite valeur de l'intervalle d'interrogation.
Maxpoll [s]	Affiche la plus grande valeur de l'intervalle d'interrogation.
iBurst	Indique si iBurst est activé.
Burst	Indique si Burst est activé.

Filtrage multicast 14

Ce chapitre décrit les fonctions liées au filtrage multicast. Vous utilisez le filtrage multicast pour contrôler le trafic multicast par le biais des appartenances à des groupes multicast.

14.1 Groupes multicast statiques

Ce paragraphe décrit comment définir des entrées statiques pour des groupes multicast connus.

14.1.1 Configuration de groupes multicast statiques

Pour configurer des groupes multicast statiques, procédez comme suit :

1. Ajoutez un ou plusieurs groupes multicast statiques.
   Pour plus d'informations, voir "Ajout d'un groupe multicast statique (Page 279)".
2. Définissez pour chaque groupe multicast statique la classe de trafic.
   Pour plus d'informations, voir "Sélection de classes de trafic pour des groupes multicast statiques (Page 280)".
3. Affectez à chaque groupe multicast statique un port de retransmission.
   Pour plus d'informations, voir "Affectation d'un port de retransmission à des groupes multicast statiques (Page 280)".

Remarque

Tous les groupes multicast statiques sont ajoutés à la base de données des filtres multicast lors de leur création.

Pour plus d'informations, voir "Base de données de filtrage multicast (Page 292)".

14.1.1.1 Ajout d'un groupe multicast statique

Pour ajouter un groupe multicast statique, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Multicast Filtering** ≫ **Static**.
2. Sous **Static Multicast Filtering**, cliquez sur **Add**. Une nouvelle ligne est insérée dans le tableau.
3. Dans la colonne **VLAN ID**, sélectionnez un VLAN statique.
4. Dans la colonne **MAC Address** , saisissez une brève.
5. Validez les modifications.

14.1.1.2 Sélection de classes de trafic pour des groupes multicast statiques

Pour sélectionner la classe de trafic d'un groupe multicast statique, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Multicast Filtering** ≫ **Static**.
2. Sous **Static Multicast Filtering**, sélectionnez dans **Traffic Class** la file d'attente d'une classe de trafic pour le groupe multicast statique sélectionné.
   Options disponibles :
   - **0 - 7** - File d'attente d'une classe de trafic.
   - **Unprioritized** – Pas de file d'attente affectée à une classe de trafic.

   Par défaut : **Unprioritized**
3. Validez la modification.

14.1.1.3 Affectation d'un port de retransmission à des groupes multicast statiques

Chaque groupe multicast statique doit être associé à un port de retransmission par lequel les flux multicast et les messages IGMP peuvent être envoyés.

Pour affecter un port de retransmission à un groupe multicast statique, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Multicast Filtering** ≫ **Static**.
2. Sous **Static Multicast Filtering**, dans la colonne **Forwarding Ports** , sélectionnez une interface pour le groupe multicast statique voulu.
3. Validez la modification.

14.2 GMRP

GARP Multicast Registration Protocol (GMRP) est une forme de filtrage multicast pour le pruning du trafic multicast de couche 2.

14.2.1 Ce qu'il faut savoir sur GMRP

GMRP est une application du Generic Attribute Registration Protocol (GARP). Il offre un mécanisme de gestion des appartenances à des groupes multicast dans un réseau de couche 2 ponté. Il permet aux commutateurs Ethernet et aux stations terminales d'enregistrer dynamiquement les appartenances à des groupes multicast avec des ponts MAC dans le même segment LAN. Ces informations peuvent ensuite être distribuées à tous les ponts du segment LAN qui prennent en charge les services de filtrage avancés.

14.2.1.1 Rejoindre/quitter des groupes multicast avec GMRP

Les paragraphes suivants décrivent comment GMRP gère les adhésions des groupes multicast.

- **Adhérer à un groupe multicast**
  Lorsque des stations terminales souhaitent rejoindre un groupe multicast, elles envoient un message GMRP **Join**. Le commutateur client qui reçoit le message **Join** ajoute le port par lequel le message a été reçu au groupe multicast spécifié dans le message. Il transmet ensuite le message **Join** à tous les hôtes du VLAN dont un doit être la source multicast.
  Lorsqu'un commutateur client envoie des mises à jour GMRP (depuis des ports compatibles GMRP), tous les groupes multicast connus du commutateur (qu'ils soient ajoutés manuellement ou appris dynamiquement via GMRP) sont communiqués au reste du réseau. Tant qu'un hôte du réseau de couche 2 s'est inscrit à un groupe multicast, le trafic est transmis depuis la source multicast correspondante sur le réseau. Le trafic transféré par la source est transféré par les autres commutateurs du réseau uniquement vers les ports dont le commutateur a reçu des messages **Join** pour le groupe multicast.
- **Quitter un groupe multicast**
  Les commutateurs clients envoient régulièrement des requêtes GMRP sous la forme d'un message **Leave-All**. Si un hôte (soit un commutateur, soit une station terminale) souhaite rester dans le groupe multicast, il confirme son appartenance au groupe en répondant par un message **Join** approprié. Dans le cas contraire, l'hôte répondra par un message **Leave** ou tout simplement ne répondra pas.
  Si le commutateur client reçoit un message **Leave** de l'hôte ou n'a pas reçu de réponse après l'expiration d'un délai d'attente, l'hôte est retiré du groupe multicast.

14.2.1.2 Types d'attribus GARP

Comme GMRP est une application de GARP, les transactions se font à l'aide de GARP.

GMRP définit les deux types d'attributs suivants :

- **Groupe**
  Identifie les accès MAC d'un groupe
- **Requête de service**
  Identifie les requêtes de service d'un groupe

Les attributs de requête de service servent à définir l'un des comportements suivants pour le filtrage multicast du port de réception :

- Transférer tout le trafic des groupes multicast sur le VLAN
- Transférer tout le trafic inconnu (groupes multicast) pour lequel aucun membre n'est enregistré dans un VLAN sur l'appareil

Si GMRP est désactivé, les trames GMRP reçues sont acheminées comme tout autre trafic de données. Dans le cas contraire, les trames GMRP sont traitées et ne sont pas transmises.

14.2.2 Configuration de GMRP

Pour configurer GMRP, procédez comme suit :

- Activez GMRP globalement.
  Pour plus d'informations, voir "Activation de GMRP (Page 282)".
- Définissez le mode GMRP pour des ports de pont sélectionnés.
  Le mode GMRP détermine la manière dont les divers ports de pont traitent les messages GMRP.
  Pour plus d'informations, voir "Sélection du mode GMRP par port de pont (Page 282)".
- [Facultatif] Sélectionnez un délai d'attente pour GMRP avant de supprimer un groupe multicast enregistré après une tentative de sortie du groupe.
  Pour plus d'informations, voir "Configuration d'une temporisation avant de quitter un groupe multicast (Page 283)".
- [Facultatif] Activer l'inondation en cas de modification de la topologie.
  Pour plus d'informations, voir "Activation de l'inondation en cas de modification de la topologie (Page 283)".

14.2.2.1 Activation de GMRP

Pour activer GMRP pour toutes les interfaces de port de pont, procédez comme suit :

Remarque

GMRP est désactivé par défaut.

1. Naviguez vers **Layer 2** ≫ **Multicast Filtering** ≫ **GMRP**.
2. Sous **GARP Multicast Registration Protocol (GMRP)**, paramétrez pour **GMRP** l'option **Enabled**.
3. Validez la modification.

14.2.2.2 Sélection du mode GMRP par port de pont

Les ports de pont peuvent être configurés individuellement pour ignorer ou traiter les messages GRMP de type **Join** et **Leave**.

Pour configurer la manière dont une interface de port de pont traite les messages GMRP, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Multicast Filtering** ≫ **GMRP**.
2. Sous **GARP Multicast Registration Protocol (GMRP)**, configurez le **GMRP Mode** du port de pont sélectionné.
   Options disponibles :

Option	Description
Disabled	**Par défaut** GMRP est désactivée sur l'interface.
Declare and Register	Tous les groupes multicast sont communiqués et les nouveaux groupes sont enregistrés dynamiquement.
Declare Only	Tous les groupes multicast (configurés et appris) sont communiqués, mais les nouveaux groupes ne sont pas enregistrés.

3. Validez la modification.

14.2.2.3 Configuration d'une temporisation avant de quitter un groupe multicast

Lorsque SINEC OS reçoit un message **Leave**ou **Leave-All** pour un hôte appartenant à un groupe multicast, l'hôte est retiré du ou des groupes multicast spécifiés. Le délai entre la réception du message et la suppression de l'hôte peut être retardé. Cela donne à l'hôte la possibilité d'envoyer un message **Join** et de rester dans le ou les groupes multicast.

Pour créer une temporisation avant de supprimer un hôte d'un groupe multicast, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Multicast Filtering** ≫ **GMRP**.
2. Sous **GARP Multicast Registration Protocol (GMRP)**, configurez **Leave Timer**.
   Conditions :
   - En format nYnMnDnhnmns, dans lequel n est un nombre personnalisé
   - 0,6 seconde min. (0.6s)
   - 5 Minutes max. (5m) soit 300 secondes (300s)

   Par défaut : 4s (4 secondes)
3. Validez la modification.

14.2.2.4 Activation de l'inondation en cas de modification de la topologie

Si des changements de topologie STP se produisent ou si des changements de liens se produisent sans qu'un TCN ne soit déclenché, SINEC OS inonde temporairement toutes les interfaces contrôlées par GMRP. Si l'inondation en cas de changement de topologie est activée, toutes les interfaces RSTP non edge seront également inondées.

Pour activer l'inondation en cas de modification de la topologie, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Multicast Filtering** ≫ **GMRP**.
2. Sous **GARP Multicast Registration Protocol (GMRP)**, modifiez le paramètre **Topology Change Flooding** en **Enabled**.
3. Validez la modification.

14.2.3 Exemples de configuration

Vous trouverez ci-après des exemples de mise en œuvre de GMRP.

14.2.3.1 Configuration de l'adhésion à des groupes multicast via GMRP

Cet exemple de configuration montre comment un réseau d'hôtes et de commutateurs peut rejoindre dynamiquement deux groupes multicast avec GMRP.

Généralités

Dans ce scénario, l'appareil SINEC OS fait office d'intermédiaire entre deux sources de trafic multicast et deux hôtes qui souhaitent recevoir des flux multicast de l'une des sources.

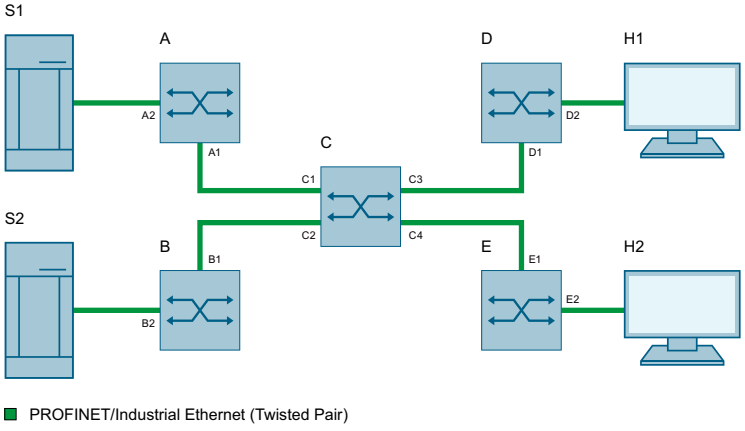


Figure 14-1 Topologie

Les sources de trafic multicast, S1 et S2, transmettent par multicast respectivement vers les groupes multicast 1 et 2.

L'hôte H1 n'est pas compatible GMRP, mais doit recevoir le trafic multicast du groupe multicast 1.

L'hôte H2 n'est pas compatible GMRP et doit recevoir le trafic multicast du groupe multicast 2.

Un réseau de commutateurs avec l'appareil SINEC OS au cœur relie les hôtes aux sources multicast.

Configuration

1. Connectez les appareils comme représentés dans la topologie.
2. Activez GMRP globalement sur tous les commutateurs (c'est-à-dire sur les commutateurs A, B, C, D et E).
3. Configurez des interfaces pour chaque commutateur afin de traiter les messages GMRP (c.-à-d. les interfaces A1, A2, B1, B2, etc.).
4. Ajoutez un groupe multicast statique au commutateur D pour le VLAN 1, avec l'interface D2 comme port de retransmission.
   Cela permet à H1 de recevoir tout le trafic multicast pour le groupe multicast 1.

Résultat

Lorsque tous les appareils sont connectés et configurés, les hôtes H1 et H2 peuvent établir leur appartenance au groupe multicast comme suit :

1. À la place de H1, le commutateur D communique au réseau son appartenance au groupe multicast 1 via l'interface D1. En conséquence, l'interface C3 du commutateur C devient un membre du groupe multicast 1.
2. Le commutateur C propage ensuite le message **Join**, ce qui fait que les interfaces A1, B1, C3 et E1 deviennent également membres du groupe multicast sur leur commutateur respectif.
3. Comme H2 est GMRP-aware, il envoie un message d'adhésion au commutateur E pour communiquer son appartenance au groupe multicast 2. En conséquence, l'interface E2 devient membre du groupe multicast 2.
4. Le commutateur E propage ensuite le message **Join** de H2, ce qui fait que les interfaces A1, B1, C4 et D1 deviennent également membres du groupe multicast 2 sur leur commutateur respectif.

L'enregistrement basé GMRP a maintenant été propagé sur le réseau, de sorte que le trafic multicast de S1 et S2 peut atteindre sa destination comme suit :

1. S1 retransmet le trafic de données multicast sur l'interface A2 au commutateur A.
2. Le commutateur A retransmet le trafic de données à l'interface A1 qui est membre du groupe multicast 1.
3. De A1, le trafic de données multicast est retansmis à l'interface C3 puis à l'hôte H1.
4. S2 retransmet le trafic de données multicast sur l'interface B2 au commutateur B.
5. Le commutateur B retransmet le trafic de données à l'interface B1 qui est membre du groupe multicast 2.
6. De B1, le trafic de données multicast est retansmis à l'interface C4 puis à l'hôte H2.

14.3 IGMP Snooping

L'Internet Group Management Protocol-Snooping (IGMP-Snooping) est une fonction de couche 2 qui permet aux commutateurs Ethernet d'écouter les communications IGMP entre les hôtes IP et les routeurs multicast. Les commutateurs Ethernet peuvent alors acheminer intelligemment les flux multicast uniquement vers les hôtes qui se sont abonnés au groupe multicast.

14.3.1 Ce qu'il faut savoir sur IGMP Snooping

Certains commutateurs retransmettent par défaut des flux multicast non sollicités à toutes les interfaces d'un VLAN, obligeant ainsi certains hôtes du domaine broadcast à traiter un trafic multicast qu'ils n'ont pas demandé. Il en résulte que ces hôtes consomment inutilement beaucoup de ressources nécessaires ailleurs et sont éventuellement exposés à une attaque par déni de service.

L'IGMP snooping garantit que les flux multicast ne sont retransmis qu'aux hôtes qui les demandent. En écoutant et en analysant (snooping) les messages de rapport d'appartenance IGMP d'un routeur multicast et de ses clients, IGMP snooping détermine quelles interfaces sont connectées à des hôtes compatibles IGMP. Le trafic multicast est alors uniquement dirigé vers ces hôtes et n'inonde pas l'ensemble du VLAN.

Remarque

SINEC OS prend en charge les versions 2 et 3 d'IGMP Snooping.

14.3.1.1 Modes IGMP

IGMP Snooping permet aux commutateurs d'assurer l'écoute du fonctionnement des routeurs multicast. Comme les requêtes IGMP générales du routeur sont alors reconnues, les requêtes **Join** et **Leave** peuvent être envoyées au nom des clients et des hôtes. IGMP Snooping peut également raccourcir les flux multicast en conséquence.

IGMP Snooping peut être configuré pour fonctionner dans l'un des modes suivants :

- **Mode passif**
  En mode **passif**, IGMP Snooping écoute les requêtes IGMP générales et envoie des requêtes **Join** et **Leave** au nom des ports Consumer. Il n'est pas possible d'envoyer des requêtes.
  Le mode **passif** doit être activé s'il existe un routeur multicast.
- **Mode actif**
  En mode **actif**, IGMP Snooping peut envoyer des requêtes IGMP générales qu'il recevrait normalement d'un routeur multicast.
  Le mode **actif** doit être activé s'il n'existe pas de routeur multicast distant.

14.3.1.2 Filtrage/réduction du trafic de données multicast

IGMP Snooping filtre le trafic IP multicast vers les hôtes (pruning) et utilise pour cela l'adresse MAC multicast de la destination de chaque trame, qui est déterminée par l'adresse IP multicast du groupe multicast.

Exemple : L'adresse IP multicast W.X.Y.Z correspond à l'adresse MAC 01-00-5E-XX-YY-ZZ. Dans cette adresse XX sont les 7 bits de faible poids de X, et YY et ZZ sont Y et Z en notation hexadécimale.

Remarque

Veuillez noter que des adresses IP multicast telles que 224.1.1.1 et 225.1.1.1 sont toutes deux affectées à la même adresse MAC (p. ex. 01-00-5E-01-01-01). Il s'agit d'un problème connu pour lequel le groupe de travail réseau de l'IETF ne propose actuellement pas de solution. Les utilisateurs sont invités à prendre en compte ce problème et à l'éviter dans la mesure du possible.

14.3.1.3 IGMP Snooping Querier

Sous IGMP, le routeur multicast avec l'adresse IP la plus basse est choisi comme routeur maître ou Querier (requérant). Le requérant est chargé de demander régulièrement aux hôtes des messages de rapport IGMP afin de déterminer quels hôtes souhaitent recevoir du trafic IP multicast. IGMP Snooping utilise ces rapports pour affecter aux hôtes des flux multicast spécifiques.

Toutefois, si aucun routeur multicast n'est disponible sur le VLAN, la surveillance IGMP doit être mise en mode *actif* sur au moins un commutateur du même réseau local. Les commutateurs avec snooping IGMP en mode **actif** participent au processus de sélection comme les routeurs multicast.

14.3.1.4 Règles sous IGMP Snooping

Les règles suivantes s'appliquent sous IGMP Snooping :

- Si IGMP Snooping est en mode **passif**, au moins un commutateur compatible IGMP sur le réseau doit être en mode **actif** pour envoyer des requêtes IGMP générales.
- Par défaut, le trafic multicast reçu d'une source inconnue est retransmis vers tous les ports. Cependant, si le trafic multicast provient d'un groupe multicast connu (c'est-à-dire si au moins un port est membre du même groupe), le trafic est retransmis uniquement aux ports qui sont membres de ce groupe multicast ou qui sont connectés au requérant IGMP sélectionné/configuré (routeur multicast).
- Les trames non-IGMP dont l'adresse IP multicast de la destination est comprise entre 224.0.0.0 et 224.0.0.255 sont toujours retransmises vers tous les ports. Ce comportement est basé sur le fait que de nombreux systèmes n'envoient pas de rapports d'adhésion pour les adresses IP multicast dans cette zone tant qu'ils écoutent encore de telles trames.
- IGMP ne transmet les rapports d'adhésion que sur les ports connectés à des routeurs multicast. L'envoi de rapports aux hôtes n'est pas pris en charge, car cela peut empêcher un hôte de rejoindre un groupe multicast particulier.
- Les routeurs multicast utilisent IGMP pour sélectionner un routeur maître en tant que querier. Le requérant est le routeur avec l'adresse IP la plus basse. Tous les autres routeurs deviennent des non-requérants et ne participent qu'à l'acheminement du trafic multicast. Les appareils compatibles IGMP en mode **actif** participent au processus de sélection du requérant, tout comme les routeurs multicast.

- Lorsque le processus de sélection du requérant est terminé, IGMP retransmet les requêtes reçues du requérant sélectionné.
- Lorsque des trames IGMP sont transmises, le requérant envoie des requêtes IGMP générales et attribue une adresse IP source de 0.0.0.0.

14.3.2 Configuration d'IGMP Snooping

Pour configurer IGMP Snooping, procédez comme suit :

1. Activez IGMP Snooping globalement
   Pour plus d'informations, voir "Activation d'IGMP Snooping (Page 288)".
2. Sélectionnez la version d'IGMP. Celle-ci détermine quels types de messages IGMP l'appareil est en mesure d'émettre et de recevoir.
   Pour plus d'informations, voir "Sélection de la version d'IGMP (Page 289)".
3. Sélectionnez le mode IGMP souhaité :
   Pour plus d'informations, voir "Sélection du mode IGMP (Page 289)".
4. Configurez l'intervalle d'interrogation IGMP.
   Pour plus d'informations, voir "Configuration de l'intervalle d'interrogation IGMP (Page 290)".
5. [Facultatif] Activer l'inondation en cas de modification de la topologie.
   Pour plus d'informations, voir "Activation de l'inondation en cas de modification de la topologie (Page 290)".
6. [Facultatif] Configurez la retransmission des routeurs multicast.
   Pour plus d'informations, voir "Configuration de la retransmission des routeurs multicast (Page 291)".
7. Activez IGMP Snooping pour un ou plusieurs VLAN statiques.
   Pour plus d'informations, voir "Activation d'IGMP Snooping par VLAN (Page 290)".

14.3.2.1 Activation d'IGMP Snooping

Pour activer IGMP Snooping, procédez comme suit :

Remarque

IGMP Snooping est activé par défaut.

1. Naviguez vers **Layer 2** ≫ **Multicast Filtering** ≫ **IGMP Snooping**.
2. Sous **Internet Group Management Protocol (IGMP)**, modifiez **IGMP Snooping** en **Enabled**.
3. Validez la modification.

14.3.2.2 Sélection de la version d'IGMP

La version d'IGMP détermine le type de messages IGMP qui peuvent être envoyés et reçus par le pont.

- Si IGMPv2 est activé, les messages IGMPv3 peuvent uniquement être envoyés, mais pas reçus.
- Si IGMPv3 est activé, tous les messages IGMP peuvent être envoyés et reçus.

Pour sélectionner la version IGMP, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Multicast Filtering** ≫ **IGMP Snooping**.
2. Sous **Internet Group Management Protocol (IGMP)**, configurez **Version**.
   Options disponibles :

Option	Description
2	**Par défaut** Modifie la version d'IGMP en IGMPv2.
3	Modifie la version d'IGMP en IGMPv3.

3. Validez la modification.

14.3.2.3 Sélection du mode IGMP

IGMP Snooping peut être configuré pour fonctionner en mode **actif** ou en mode **passif** en activant ou désactivant le requérant IGMP.

- Si le requérant IGMP est activé, IGMP Snooping se trouve en mode **actif**.
- Si le requérant IGMP est désactivé, IGMP Snooping se trouve en mode **passif**.

Remarque

Le requérant IGMP est désactivé par défaut (mode passif).

Remarque

Si IGMP Snooping est en mode **passif**, au moins un commutateur compatible IGMP sur le réseau doit être en mode **actif** pour envoyer des requêtes IGMP générales.

Pour plus d'informations sur les modes **actif** et **passif**, voir "Modes IGMP (Page 286)".

Pour sélectionner le mode IGMP, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Multicast Filtering** ≫ **IGMP Snooping**.
2. Sous **Internet Group Management Protocol (IGMP)**, modifiez le paramètre **IGMP Querier** en **Enabled** (mode actif) ou **Disabled** (mode passif).
3. Validez la modification.

14.3.2.4 Configuration de l'intervalle d'interrogation IGMP

L'intervalle d'interrogation IGMP détermine la fréquence de transmission des requêtes IGMP. L'intervalle est mesuré en secondes entre deux transmissions successives.

L'intervalle d'interrogation détermine également le moment où les groupes multicast appris dynamiquement deviennent obsolètes. Le délai de vieillissement est de 2 x { intervalle } + 10 secondes.

Pour configurer l'intervalle d'interrogation IGMP, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Multicast Filtering** ≫ **IGMP Snooping**.
2. Sous **Internet Group Management Protocol (IGMP)**, configurez **Query Interval**. Conditions :
   - En format nYnMnDnhnmns, dans lequel n est un nombre personnalisé
   - 10 secondes min. (10s)
   - 60 Minutes max. (60m) soit 3600 secondes (3600s)

   Par défaut : 2m5s (2 minutes, 5 secondes)
3. Validez la modification.

14.3.2.5 Activation de l'inondation en cas de modification de la topologie

Si des changements de topologie STP se produisent ou si des changements de liens se produisent sans qu'un TCN ne soit déclenché, SINEC OS inonde temporairement toutes les interfaces affectées aux VLAN où IGMP Snooping est activé. Si l'inondation en cas de changement de topologie est activée, toutes les interfaces RSTP non edge seront également inondées.

Pour activer l'inondation en cas de modification de la topologie, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Multicast Filtering** ≫ **IGMP Snooping**.
2. Sous **Internet Group Management Protocol (IGMP)**, modifiez le paramètre **Topology Change Flooding** en **Enabled**.
3. Validez la modification.

14.3.2.6 Activation d'IGMP Snooping par VLAN

Pour activer IGMP Snooping sur un VLAN statique, procédez comme suit :

Remarque

IGMP Snooping est désactivé par défaut par rapport à chaque VLAN statique.

1. Naviguez vers **Layer 2** ≫ **Multicast Filtering** ≫ **IGMP Snooping**.
2. Sous **IGMP Snooping VLANs**, modifiez le paramètre **IGMP Snooping** du VLAN sélectionné en **Enabled**.
3. Validez la modification.

14.3.3 Configuration de la retransmission des routeurs multicast

Pour configurer la retransmission des routeurs multicast, procédez comme suit :

1. Activez la retransmission des routeurs multicast.
   Pour plus d'informations, voir "Activation de la retransmission de routeurs multicast (Page 291)".
2. Configurez une ou plusieurs interfaces de routeur multicast.
   Pour plus d'informations, voir "Configuration d'une interface de routeur multicast (Page 291)".

14.3.3.1 Activation de la retransmission de routeurs multicast

Pour activer la retransmission de routeurs multicast, procédez comme suit :

Remarque

La retransmission de routeurs multicast est activée par défaut.

1. Naviguez vers **Layer 2** ≫ **Multicast Filtering** ≫ **IGMP Snooping**.
2. Sous **Internet Group Management Protocol (IGMP)**, modifiez le paramètre **Router Forwarding** en **Enabled**.
3. Validez la modification.

14.3.3.2 Configuration d'une interface de routeur multicast

Les interfaces de routeur multicast établissent une connexion statique à un routeur multicast.

Pour configurer une interface de routeur multicast, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Multicast Filtering** ≫ **IGMP Snooping**.
2. Sous **Internet Group Management Protocol (IGMP)**, sélectionnez une ou plusieurs interfaces de la liste **Multicast Router** .
3. Validez la modification.

14.3.4 Surveillance d'IGMP Snooping

Ce paragraphe décrit les différentes méthodes de surveillance de l'état des groupes multicast appris à l'aide de la fonction IGMP Snooping.

14.3.4.1 Affichage de l'état des groupes multicast appris

Pour afficher l'état des groupes multicast qui ont été appris dynamiquement par IGMP Snooping, naviguez vers **Layer 2** ≫ **Multicast Filtering** ≫ **IGMP Snooping** :

Les informations suivantes s'affichent sous **IGMP Snooping Status** :

Paramètres	Description
Interface	le port de pont sur lequel le groupe multicast a été appris.
VLAN ID	l'ID du VLAN sur lequel le groupe multicast travaille.
Address	L'adresse IPv4 de destination du groupe multicast.
Last Reporter	L'adresse IPv4 de l'hôte qui a envoyé en dernier le rapport d'adhésion au groupe multicast.
MAC Address	Adresse MAC de destination du trafic de données qui est retransmis pour le groupe multicast.
Up Time	Le temps écoulé en secondes (s) depuis l'apprentissage d'un groupe multicast.
Joined Ports	Une liste des ports de pont qui ont reçu les messages IGMP Join du groupe multicast.
Multicast Router	Une liste de ports de pont qui retransmettent le trafic multicast aux routeurs multicast.

14.4 Base de données de filtrage multicast

La base de données pour de filtrage multicast enregistre tous les groupes multicast actuels qui ont été configurés de manière statique ou appris de manière dynamique par filtrage multicast.

Pour afficher la base de données de filtrage multicast, naviguez vers **Layer 2** ≫ **Multicast Filtering** ≫ **Filtering Database**.

Sous **Multicast Filtering Database**, les informations suivantes sont affichées pour chaque entrée :

Paramètres	Description
VLAN ID	Le VID du VLAN appartenant au groupe multicast.
MAC Address	L'adresse MAC de destination du groupe multicast.
Traffic Class	La file d'attente d'une classe de trafic affectée à l'adresse MAC. Valeurs possibles : • **0 – 7** - File d'attente d'une classe de trafic • **Unprioritized** – Pas de file d'attente affectée à une classe de trafic.
Forwarding Ports and States	Le (les) port(s) de retransmission sortant(s) affecté(s) à l'adresse MAC et son (leur) état. Les valeurs possibles sont : • **Static** – L'adresse MAC statique a été ajoutée par un utilisateur. • **Dynamic** – L'adresse MAC a été apprise dynamiquement par un protocole de pont. • **Static-Dynamic** – L'adresse MAC a été apprise dynamiquement puis ajoutée statiquement par un utilisateur.

Diagnostic 15

15.1 Diagnostic

Ce chapitre décrit les outils de diagnostic disponibles.

15.2 État du système

Ce paragraphe décrit comment surveiller l'état du système, y compris le temps de fonctionnement, le dernier redémarrage, etc.

15.2.1 Affichage de la date/heure système de démarrage

Pour afficher la date et l'heure auxquelles l'appareil a été redémarré pour la dernière fois, naviguez vers **System** ≫ **Information & State**: L'heure est affichée dans la zone **System State** sous **Boot Date/Time**.

Exemple

2021-01-01 00:08:00

15.2.2 Affichage du temps de fonctionnement du système

Pour afficher le durée totale de fonctionnement de l'appareil depuis le dernier redémarrage, naviguez vers **System** ≫ **Information & State**. La durée totale est affichée dans la zone **System State** sous **Uptime**. La durée totale est affichée en nombre de jours, d'heures, de minutes et de secondes.

Exemple

2D4h37m37s

15.3 Journal système

SINEC OS enregistre toutes les alarmes et les évènements sélectionnés dans un journal système (Syslog). Le journal système est utilisé par les administrateurs réseau pour détecter les évènements qui ont un impact sur les performances et la sécurité.

Le journal du système est enregistré localement, mais tout ou partie du journal peut être transmis à un serveur Syslog distant pour y être stocké et surveillé de manière centralisée.

Des évènements spécifiques, typiquement ceux qui nécessitent une résolution immédiate, peuvent également être envoyés aux administrateurs du réseau par courrier électronique et/ou par notifications SNMP lorsqu'ils se produisent.

15.3.1 Ce qu'il faut savoir sur la journalisation système

Le journal système (Syslog) enregistre tous les messages d'évènements générés par les différents constituants du système sous SINEC OS.

Le journal système est affiché par un journal d'incidents. Le journal d'incidents affiche les entrées les plus récentes du journal système, 1000 au maximum. Lorsque de nouveaux évènements surviennent, les entrées les plus anciennes sont supprimées. Le journal d'incidents affiche par défaut tous les messages d'évènements, mais peut être filtré selon les besoins.

Les utilisateurs peuvent modifier le format d'horodatage des entrées du journal système.

15.3.1.1 Structure d'une entrée de journal système

Chaque entrée du journal système représente un évènement unique.

Exemple

```
2021-01-03T02:49:15-00:00 localhost   2m55s        dmfd
info          coldStart
```

Cette entrée d'information indique que l'appareil a été redémarré le 2021-01-03T02:49:15-00:00 ou à 2:49 AM le 1er mars 2021, GMT-0 (soit il a été arrêté puis redémarré manuellement, soit l'appareil a été redémarré via SINEC OS).

Description

Chaque entrée du journal système se compose des éléments suivants :

{ Horodatage }	**{ Nom d'hôte }**	**{ Temps de fonctionnement}**	**{ Programme }**	**{ Gravité}**	**{ Message }**
L'horodatage associé à l'évènement.	Le nom d'hôte affecté à l'appareil.	Le temps écoulé entre le dernier redémarrage de l'appareil et le moment de l'évènement. Format : nYnMnDnhnmns	Le programme qui a généré le message.	Gravité du message.	La description de l'évènement.

15.3.1.2 Niveaux de gravité

Chaque message d'évènement du journal système est associé à l'un des niveaux de gravité standard suivants :

Gravité de l'évènement	Valeur	Description
Emergency	0	Indique une erreur grave qui empêche la poursuite du fonctionnement de l'appareil.
Alert	1	Indique une erreur nécessitant une attention immédiate.
Critical	2	Indique une défaillance du système primaire, par exemple une erreur de l'appareil ou un dysfonctionnement du système ou de l'application. Typiquement, ces alarmes ne sont pas restaurables.
Error	3	Signale un état d'erreur.
Warning	4	Indique qu'une erreur peut se produire si l'état associé n'est pas corrigé.
Notice	5	Indique un évènement inhabituel, mais qui n'est pas un état d'erreur.
Info	6	Signale un message d'information normal. Aucune mesure n'est nécessaire.

15.3.1.3 Composants Syslog

Les composants Syslog représentent les processus internes qui génèrent des évènements. En séparant les messages d'évènements par composant, il est possible de les filtrer différemment lorsque les messages sont transmis à des serveurs Syslog distants.

Les composants Syslog suivants sont disponibles :

Composant	Description
kern	Messages liés au noyau
user	Messages au niveau de l'utilisateur
mail	Messages liés à la messagerie
daemon	Messages liés au deamon système
auth	Messages liés à l'authentification et à l'autorisation
syslog	Messages liés au système
authpriv	Messages relatifs à l'autorisation hors système

15.3.1.4 Connexion à distance

Les entrées du journal système peuvent être transmises à un maximum de cinq serveurs Syslog distants pour y être stockées et analysées de manière centralisée. Il est possible de contrôler quelles entrées sont transmises à l'aide de filtres.

Plusieurs filtres peuvent être définis pour chaque serveur Syslog, chacun d'entre eux s'appliquant à un composant spécifique.

15.3.1.5 Filtre d'évènements

Le service de journalisation du système comprend un mécanisme de filtrage.

Filtre du journal d'incidents

Dans le journal d'incidents, les messages d'évènements peuvent être filtrés à l'aide d'une règle de filtrage. Cette règle spécifie un niveau de gravité et indique au système s'il doit afficher uniquement les messages de ce niveau de gravité ou les messages de ce niveau de gravité et plus. Par exemple, si une règle indique que seuls les messages dont le niveau de gravité est "critique" ou supérieur doivent être inclus, seuls les messages répondant à ces critères seront affichés.

Filtre Syslog distant

Pour les serveurs Syslog distants, il est possible de définir une ou plusieurs règles de filtrage par composant Syslog et par niveau de gravité. Les règles sont appliquées individuellement dans l'ordre dans lequel elles sont définies. Seuls les messages couverts par les règles sont transmis.

15.3.2 Configuration de la journalisation système distante

Pour transmettre des évènements du journal système à un serveur Syslog distant, procédez comme suit :

1. Ajoutez un profil pour un serveur Syslog distant. Vous pouvez définir jusqu'à cinq serveurs.
   Pour plus d'informations, voir "Ajout d'un profil pour un serveur Syslog distant. (Page 296)".
2. Ajoutez au moins une règle de filtrage pour chaque serveur Syslog distant afin de contrôler quels messages d'évènement sont transmis.
   Pour plus d'informations, voir le **Manuel de configuration SINEC OS CLI**.

15.3.2.1 Ajout d'un profil pour un serveur Syslog distant.

Vous pouvez définir jusqu'à cinq profils de serveurs Syslog distants. Chaque profil définit :

- Le nom d'hôte ou l'adresse IP du serveur.
- Le port qui est affecté au serveur
- Les journaux qui sont retransmis au serveur (uniquement CLI)
- Certificats TLS et clés (uniquement CLI)

Pour plus d'informations sur les fonctions qui sont uniquement disponibles sous CLI, voir le **Manuel de configuration SINEC OS**.

Pour ajouter un profil pour un serveur Syslog distant, procédez comme suit :

1. Naviguez vers **System** ≫ **Logging** ≫ **Remote Syslog**.
2. Sous **Remote Syslog**, cliquez sur **Add**. Une nouvelle ligne est insérée dans le tableau.
3. Sous **Name**, attribuez un nom à la connexion au serveur.
4. Sous **Server Address/FQDN**, entrez l'adresse IPv4 ou le nom d'hôte du serveur Syslog distant.
5. Sous **UDP Port**, entrez le port qui est affecté au serveur.
   Par défaut : 514
6. Validez les modifications.

15.3.3 Surveillance du journal système

Ce paragraphe décrit comment accéder au journal d'incidents et comment surveiller les connexions au serveur distant.

15.3.3.1 Affichage du journal d'incidents

Pour afficher le journal d'incidents, naviguez vers **System** ≫ **Logging** ≫ **Logbook**.

Les informations suivantes sont affichées pour chaque entrée du journal sous **Logbook** :

Paramètres	Description
Time	Horodatage de l'évènement.
Uptime	Le temps écoulé entre le dernier redémarrage de l'appareil et le moment de l'évènement. Format : nYnMnDnhnmns.
Severity	Gravité du message.
Message	Description du message.

15.3.3.2 Affichage du serveur de journalisation distant

Les entrées du journal système peuvent être transmises à un ou plusieurs serveurs Syslog distants pour y être stockées et analysées de manière centralisée.

Pour afficher des informations sur les serveurs de journalisation distants qui ont été définis, naviguez vers **System** ≫ **Logging** ≫ **Remote Syslog**.

Les informations suivantes sont affichées sous **Remote Syslog** pour chaque serveur :

Paramètres	Description
Name	Le nom affecté au serveur Syslog distant.
Server Address / FQDN	Le nom d'hôte ou l'adresse IP du serveur Syslog distant.
UDP Port	Le port désigné sur le serveur Syslog distant.

15.3.3.3 Suppression du journal d'incidents

Pour effacer des entrées du journal d'incidents, procédez comme suit :

Remarque

L'effacement du journal d'incidents ne supprime pas le journal système.

1. Naviguez vers **System** ≫ **Logging** ≫ **Logbook**.
2. Sous **Clear Logbook**, cliquez sur **Clear**.

15.4 Gestion des évènements

Le système de gestion des évènements surveille activement l'appareil et identifie les évènements spécifiques qui se produisent pendant son fonctionnement. Tous les évènements sont enregistrés dans le journal système (Syslog). Un évènement peut également déclencher une notification SNMP, peut être envoyé par e-mail aux administrateurs et/ou déclencher une alarme.

La configuration d'alarmes individuelles est prise en charge par le système de gestion des évènements.

15.4.1 Ce qu'il faut savoir sur la gestion des évènements

Les paragraphes suivants décrivent le système de gestion des évènements et la manière dont il surveille certains évènements qui se produisent pendant le fonctionnement, les enregistre et en informe les utilisateurs.

15.4.1.1 Niveaux de gravité

Chaque évènement et chaque alarme est associé à l'un des niveaux de gravité suivants :

Gravité de l'évènement/ l'alarme	Valeur	Description
Emergency	0	Signale une erreur critique qui empêche la poursuite du fonctionnement de l'appareil.
Alert	1	Indique une erreur nécessitant une attention immédiate.
Critical	2	Indique une défaillance du système primaire, par exemple une erreur de l'appareil ou un dysfonctionnement du système ou de l'application. Typiquement, ces alarmes ne sont pas restaurables.
Error	3	Signale un état d'erreur.
Warning	4	Indique qu'une erreur peut se produire si l'état associé n'est pas corrigé.
Notice	5	Signale un évènement inhabituel, mais qui n'est pas un état d'erreur.
Info	6	Signale un message d'information normal. Aucune mesure n'est nécessaire.

15.4.1.2 Ressources et évènements

Les évènements suivants sont surveillés par l'appareil pendant son fonctionnement. Chaque évènement est catégorisé par ressource (sous-système) et possède un niveau de gravité associé. La plupart des évènements génèrent une alarme qui peut être activée/désactivée selon les besoins.

Remarque

Certaines fonctions déclenchent leurs propres évènements en dehors du système de gestion des évènements. Ces évènements spécifiques d'un fonction sont directement enregistrés dans Syslog. Celles-ci sont décrites dans les rubriques respectives consacrées à ces fonctions.

Pour plus d'informations sur les niveaux de gravité, voir "Niveaux de gravité (Page 298)".

Évènements PROFINET

Les évènements suivants se rapportent à des activités PROFINET.

Ressource	ID d'évènement	Niveau de gravité standard
PROFINET	Configuration*	Alert
PROFINET	IP-Configuration*	Alert
PROFINET	Connection	Notice
PROFINET	Fault	Alert

* Aucune alarme affectée.

Évènements de la gestion du châssis

Les évènements suivants se rapportent à la configuration matérielle de l'appareil.

Ressource	ID d'évènement	Niveau de gravité standard
chassis-mgmt	Bad-power-supply	Alert
chassis-mgmt	Module-presence*	Warning
chassis-mgmt	Module-state*	Warning

* Aucune alarme affectée.

Évènements de la gestion de l'appareil

Les évènements suivants se rapportent à l'authentification des utlilisateurs, à la température ambiante détectée, etc.

Ressource	ID d'évènement	Niveau de gravité standard
device-mgmt	Authentication-failure	Warning
device-mgmt	Brute-force-prevention	Warning
device-mgmt	System-cold-start*	Info
device-mgmt	System-warm-start*	Info
device-mgmt	User-session-timeout*	Warning
device-mgmt	Vlan-linkDown/linkUp	Info

* Aucune alarme affectée.

Évènements de la gestion des commutateurs

Les évènements suivants se rapportent à des activités des commutateurs, telles que Link Up, Link Down, boucles de réseau, modifications de la topologie, etc.

Ressource	ID d'évènement	Niveau de gravité standard
switch-mgmt	Bouncing-link	Alert
switch-mgmt	Bpdu-guard-activated	Alert
switch-mgmt	Bundle-port-inconsistent-speed	Error
switch-mgmt	Ertm-target-ip-address-unresolved	Alert
switch-mgmt	Fast-link-detection-disabled	Warning
switch-mgmt	Gmrp-cannot-learn-more-addresses	Alert
switch-mgmt	Gvrp-cannot-learn-more-vlans	Alert
switch-mgmt	Igmp-group-membership-table-full	Alert
switch-mgmt	Igmp-mcast-forwarding-table-full	Alert
switch-mgmt	Intermittent-link	Alert
switch-mgmt	Linkdown/linkup	Info
switch-mgmt	Loop-detection	Alert
switch-mgmt	Mac-address-not-learned	Alert
switch-mgmt	Mcast-cpu-filtering-table-full	Alert
switch-mgmt	New-stp-root	Notice
switch-mgmt	Received-looped-back-bpdu	Alert
switch-mgmt	Stp-topology-change	Notice
switch-mgmt	Unresolved-speed	Error

Évènements de journalisation

Les évènements suivants se rapportent aux identifiants de connexion à l'appareil.

Ressource	ID d'évènement	Niveau de gravité standard
logging	Expired-certificate	Error
logging	Invalid-certificate	Error

15.4.1.3 Alarmes

Certains évènements peuvent générer une alarme afin d'informer les utilisateurs lorsque l'évènement se produit. Les alarmes sont affichées dans une liste d'alarmes et/ou dans le journal système.

Types d'alarmes

Il existe deux types d'alarmes

- **Lié à l'état**
  Des alarmes liées à l'état sont générées lorsque des conditions spécifiques sont détectées et ne peuvent être supprimées qu'une fois l'état d'erreur corrigé.
  Un exemple d'alarme liée à l'état est l'alarme **Alimentation électrique défectueuse** (Bad-power-supply). Si le défaut a été supprimé (c'est-à-dire que la puissance d'entrée a été corrigée), l'alarme est prête pour l'effacement automatique dès qu'un utilisateur a acquitté l'évènement.
  L'alarme peut également être acquittée si la situation n'a pas encore été corrigée. Une fois l'état corrigé, l'alarme est automatiquement effacée.
- **Non lié à l'état**
  Les alarmes non liées à l'état sont générées lorsqu'un évènement se produit et restent actives jusqu'à ce qu'elles soient supprimées par un utilisateur.
  Un exemple d'alarme non liée à l'état est l'alarme **Erreur d'authentification** (Authentication-failure). Un utilisateur peut à tout moment acquitter ou supprimer cette alarme. Si l'effacement automatique est réglé pour l'alarme, l'alarme est également annulée par l'acquittement.

Messages d'alarme statiques et dynamiques

Certains évènements ont un message d'alarme statique et un message d'alarme dynamique :

- Les messages d'alarme statiques sont des messages fixes qui s'affichent dans la liste des alarmes. Ces messages sont également inclus dans tous les e-mails envoyés.
- Les messages dynamiques sont plus contextuels et fournissent plus de détails sur l'évènement (p. ex. protocole, utilisateur, adresse IP, etc.). Ils apparaissent dans le journal d'incidents si l'évènement est activé. Ils peuvent également être affichés dans la liste des alarmes si aucun message statique n'est défini pour l'évènement.

Alarmes disponibles

Les alarmes suivantes sont émises lorsque certains évènements se produisent, à condition que ces évènements soient configurés pour déclencher une alarme. Les alarmes sont affichées dans la liste des alarmes.

Pour plus d'informations sur l'affichage des alarmes actives, voir "Listage d'alarmes actives (Page 310)".

Alarmes PROFINET

Évènement associé	Lié à un état	Niveau de gravité	Message d'alarme	Description	Solution recommandée
Configuration	Oui	Remarque	**Message statique** "PROFINET configuration invalid, conflict detected." **Messages dynamiques** "PROFINET configuration invalid, conflict detected: { Message }." "PROFINET configuration on port { Numéro de port } invalid, conflict detected: { Message }."	Une erreur de configuration MRP a été détectée.	Vérifier les détails de la configuration et des journaux système.
IP-Configuration	Oui	Remarque	**Message statique** "IP address collision detected." **Message dynamique** "IP address collision detected. The IP address { Adresse IP } is already used."	L'adresse IP indiquée a déjà été utilisée.	Vérifiez toutes les adresses IP utilisées sur le réseau et trouvez une adresse IP libre.
Connection	Oui	Notice	**Message statique** *Aucun* **Messages dynamiques** "PROFINET connection established."	Une connexion, ou Application Relation (AR), a été établie.	Notification Aucune mesure nécessaire.
Fault	Oui	Alert	**Message statique** *Aucun* **Messages dynamiques** "PROFINET fault - please use STEP 7 for diagnostics."	Une connexion, ou Application Relation (AR), a été établie en mode **evident**.	Établissez une connexion en mode **evident**. Pour plus de détails, voir la documentation utilisateur de STEP 7.

Alarmes de la gestion du châssis

Évènement associé	Lié à un état	Niveau de gravité	Message d'alarme	Description	Solution recommandée
Bad-power-supply	Oui	Alert	**Message statique** *Aucun* **Message dynamique** "Power line #{ Numéro } lost."	La puissance d'entrée vers l'alimentation indiquée est en dehors de la plage de fonctionnement normale ou le câble d'alimentation est déconnecté.	Veuillez vous assurer que la puissance d'entrée est connectée et que la plage de fonctionnement correspond aux spécifications de l'appareil.
Module-presence	Oui	Warning	**Message statique** *Aucun* **Messages dynamiques** "Module ({ Emplacement }) Removed" "Module ({ Emplacement }) Inserted" "LPE Module Connected" "LPE Module Removed"	Un module a été soit débroché de l'emplacement indiqué ou embroché. Pour les modules LPE en particulier, cela signifie que le module a été connecté ou déconnecté.	Installez ou retirez le module. Veuillez noter que les modules LPE peuvent être échangés en cours de fonctionnement. Redémarrez l'appareil après l'installation ou le retrait du module.
Module-state	Oui	Warning	**Message statique** *Aucun* **Messages dynamiques** "Unknown SFP module on interface { Interfaces } (vendor: { Fournisseur })" "Rejected SFP module on interface { interface }" "Unsupported SFP module on interface { interface }" "LPE Module Enabled" "LPE Module Disabled"	Indique l'état des convertisseurs de médias SFP et des modules LPE. Pour les convertisseurs de médias SFP, cela signifie que le module n'a pas été reconnu, qu'il a été rejeté ou qu'il n'est pas pris en charge. Pour un module LPE, l'état du module est indiqué.	N'utilisez que des convertisseurs de médias SFP agréés par Siemens et compatibles avec votre appareil.

Alarmes dans la gestion des appareils

Évènement associé	Lié à l'état	Niveau de gravité	Message d'alarme	Description	Solution recommandée
Authentication-failure	Non	Avertissement	**Message statique** "A user failed to login due to incorrect authentication credentials." **Message(s) dynamique(s)** "{ Protocole }: Service account failed to log in." "{ Protocole }: User { Utilisateur } failed to log in." "{ Protocole }: Service account failed to login from { Adresse IP }." "{ Protocole }: User { Utilisateur } failed to login from { Adresse IP }."	Un utilisateur ou un service a utilisé des données d'authentification incorrectes pour se connecter à l'appareil.	Informez l'utilisateur ou mettez à jour le service afin que les données de connexion correctes soient utilisées. Si le compte ou l'adresse IP associé(e) est bloqué(e) par le mécanisme de protection contre les attaques par force brute, demandez à l'utilisateur/au service d'attendre le délai approprié avant la prochaine tentative.
Brute-force-prevention	Non	Avertissement	**Message statique** "A user account or an IP address is temporarily blocked, after exceeding maximum count of unsuccessful login attempts." **Message(s) dynamique(s)** "All: User { Utilisateurs } account is locked for { Minutes } minutes after { Compteur } unsuccessful login attempts." "IP:{ Adresse IP } is temporarily blocked for { Secondes } seconds after { Compteur } unsuccessful login attempts."	Le compte ou l'adresse IP utilisé par un utilisateur ou un service a été bloqué par le mécanisme de protection contre les attaques par force brute. Cela se produit après une série de tentatives de connexion infructueuses.	Indiquez à l'utilisateur ou au service d'attendre 10 minutes avant la prochaine tentative de connexion avec le même compte ou la même adresse IP. Il est également possible d'utiliser un autre compte ou une autre adresse IP.

Évènement associé	Lié à l'état	Niveau de gravité	Message d'alarme	Description	Solution recommandée
Vlan-linkDown/linkUp	Non	Info	**Message statique** "VLAN interface up/down." **Message(s) dynamique(s)** "vlan{ VID }[Up | / Down]"	Le VLAN indiqué est en service ou défaillant.	Notification Aucune mesure nécessaire.

Alarmes de la gestion de commutateur

Évènement associé	Lié à un état	Niveau de gravité	Message d'alarme	Description	Solution recommandée
Bouncing-link	Non	Alert	**Message statique** "Bouncing link detected or disappeared on a port." **Message dynamique** "Bouncing link [is | was] detected [on port { Numéro de port }]."	La détection de liens sur le port indiqué a été interrompue trop souvent.	Contrôlez les deux extrémités de la connexion par câble. Si le problème persiste, contactez le service après-vente Siemens.
Bpdu-guard-activated	Non	Alert	**Message statique** "BPDU Guard activated on a port." **Message dynamique** "Port { Numéro de port } BPDU Guard activated."	La protection BPDU a été activée et le port de pont spécifié a été désactivé.	Activez à nouveau le port de pont et déterminez pourquoi il a reçu une BPDU.
Bundle-port-inconsistent-speed	Non	Error	**Message statique** "Inconsistent speed detected or disappeared on a port." **Message dynamique** "Inconsistent speed [is | was] detected on port { Numéro de port }."	Une vitesse incohérente est détectée sur un port groupé.	Les paramètres de vitesse doivent être identiques pour tous les ports groupés.

Évènement associé	Lié à un état	Niveau de gravité	Message d'alarme	Description	Solution recommandée
Ertm-target-ip-address-unresolved	Oui	Alert	**Message statique** "Monitoring device with configured IP can't be reached." **Message dynamique** "[Local | Remote] monitoring device with IP: { Adresse IP } can't be reached, verify if the [monitoring device | monitoring device and gateway] is up and running."	L'analyseur/renifleur de paquets (appareil de surveillance vers lequel le trafic répliqué est envoyé) n'est pas accessible.	Si l'analyseur/renifleur de paquets se trouve dans le même sous-réseau (local), veuillez vous assurer que l'appareil est prêt à fonctionner. Si l'analyseur de paquets se trouve dans un autre sous-réseau (distant), vérifiez la configuration de la passerelle et/ou veuillez vous assurer que l'appareil est prêt à fonctionner.
Fast-link-detection-disabled	Non	Warning	**Message statique** "FLD disabled or enabled on a port." **Message dynamique** "Bouncing link [was] detected [on port { Numéro de port }] [, disabling FLD]."	La détection de liens commandée par alarme est désactivée sur le port indiqué.	Veuillez contacter le service après-vente Siemens.
Intermittent-link	Non	Alert	**Message statique** "Intermittent link detected or disappeared on a port." **Message dynamique** "Link [is | was] intermittent on port { Numéro de port }."	Le lien sur le port indiqué est souvent activé et désactivé.	Contrôlez les deux extrémités de la connexion par câble. Si le problème persiste, contactez le service après-vente Siemens.
Linkdown/linkup	Non	Info	**Message statique** "Link status changed on a port." **Message dynamique** "Port { Numéro de port } [is | was] down."	Le port indiqué est désactivé.	Cette alarme est supprimée dès que le port est opérationnel. Si le port n'est pas désactivé, contrôlez les deux extrémités de la connexion par câble. Si le câble est connecté, veuillez vous assurer que le port est activé.

Évènement associé	Lié à un état	Niveau de gravité	Message d'alarme	Description	Solution recommandée
Loop-detection	Oui	Alert	**Message statique** "Loop Detected on a switch port." **Messages dynamiques** "[remote | local] loop detected, Interface: { Numéro de port } disabled [for { secondes } s]." "[remote | local] loop detected, no further actions required for { Numéro de port }."	Une boucle locale ou une boucle distante a été détectée. Le port indiqué a peut-être été bloqué.	Contrôlez votre réseau pour détecter d'éventuelles boucles de réseau et réarmez la détection de boucle du port indiqué.
Mac-address-not-learned	Non	Alert	**Message statique** "MAC address failed to be learned on a VLAN." **Message dynamique** "VLAN { VID }: { Adresse MAC } not learned { Erreur }."	L'adresse MAC indiquée n'a pas été apprise sur le VLAN. Il est possible que la capacité maximale d'adresses MAC apprises ait été atteinte ou qu'une collision de hachage d'adresses MAC se soit produite.	Vous pouvez soit supprimer les entrées statiques, soit attendre que les entrées dont les hôtes n'ont plus besoin soient supprimées de manière dynamique.

Évènement associé	Lié à un état	Niveau de gravité	Message d'alarme	Description	Solution recommandée
Received-looped-back-bpdu	Non	Alert	**Message statique** "Looped back BPDU received on a port." **Message dynamique** "Port { Numéro de port } received looped back BPDU."	Une BPDU a été détectée sur le port de pont qui a lui-même envoyé cette BPDU. Causes possibles : • Un stub loopback est enfiché sur le port de pont • Le port de pont était auparavant le port de pont racine avant que la priorité du pont n'ait été abaissée. Il se peut alors que le port du pont reçoive ses propres informations obsolètes avant que celles-ci n'aient été supprimées en raison de leur vieillissement. • Le câble ou le matériel est défectueux.	Procédez comme suit en fonction des raisons possibles indiquées : • Supprimez le loopback stub. • Attendez que les informations obsolètes aient été supprimées. • Remplacez le câble ou le matériel défectueux.
Unresolved-speed	Non	Error	**Message statique** "Unresolved speed detected or disappeared on a port." **Message dynamique** "[Was] [Unable | unable] to obtain speed information from port { Numéro de port }."	Impossible de déterminer les caractéristiques de vitesse du port indiqué.	Veuillez contacter le service après-vente Siemens.
Gmrp-cannot-learn-more-addresses	Oui	Alert	**Message statique** *Aucun* **Message dynamique** "GMRP cannot learn more addresses."	Le nombre maximal de groupes multicast appris est atteint.	Attendez que les groupes appris dont les hôtes n'ont plus besoin soient supprimés de manière dynamique.

Évènement associé	Lié à un état	Niveau de gravité	Message d'alarme	Description	Solution recommandée
Gvrp-cannot-learn-more-vlans	Oui	Alert	**Message statique** *Aucun* **Message dynamique** "GVRP cannot learn more VLANs."	L'appareil a atteint le nombre maximal de VLAN pris en charge.	Vous pouvez soit supprimer les VLAN statiques, soit attendre que les VLAN soient supprimés de manière dynamique.
Igmp-group-membership-table-full	Oui	Alert	**Message statique** *Aucun* **Message dynamique** "IGMP Group Membership table full."	Le tableau des adhésions aux groupes multicast IGMP de couhe 3 est plein. Les combinaisons uniques adresse MAC/ VLAN/port sont enregistrées dans ce tableau interne.	Attendez que les groupes appris dont les hôtes n'ont plus besoin soient supprimés de manière dynamique.
Igmp-mcast-forwarding-table-full	Oui	Alert	**Message statique** *Aucun* **Message dynamique** "IGMP Mcast Forwarding table full."	Le tableau des adhésions aux groupes multicast IGMP de couhe 2 est plein. Les combinaisons uniques adresse MAC/ VLAN sont enregistrées dans ce tableau interne.	Attendez que les groupes appris dont les hôtes n'ont plus besoin soient supprimés de manière dynamique.
Mcast-cpu-filtering-table-full	Oui	Alert	**Message statique** *Aucun* **Message dynamique** "Can't filter more mcast streams from CPU."	Le nombre maximal de flux Multicast installés dans le système est atteint.	Erreur interne. Aucune mesure nécessaire.
New-stp-root	Non	Notice	**Message statique** *Aucun* **Message dynamique** "New STP Root."	Une nouvelle racine STP a été sélectionnée.	Vérifier si la modification était attendue en raison de changements dans la topologie du réseau (par exemple, configuration du réseau ou pannes non planifiées/planifiées).
Stp-topology-change	Non	Notice	**Message statique** *Aucun* **Message dynamique** "STP topology change."	Un port de pont est passé de l'état Apprentissage à l'état Retransmission, ou de l'état Retransmission à l'état Blocage.	Vérifier si le changement était attendu en raison de modifications de la topologie du réseau (par exemple, configuration du réseau ou pannes non planifiées/planifiées).

Journalisation des alarmes

Évènement associé	Lié à un état	Niveau de gravité	Message d'alarme	Description	Solution recommandée
Expired-certificate	Non	Error	**Message statique** "The TLS certificate is expried." **Message dynamique** "Certificate validation failed; subject='{ Rubrique }', issuer='{ Émetteur }', error='certificate has expired', depth='{ Profondeur }'"	Le certificat d'une session TLS a expiré.	Remplacez le certificat de la session TLS spécifiée.
Invalid-certificate	Non	Error	**Message statique** "The TLS certificate is invalid." **Message dynamique** "Certificate validation failed; subject='{ Rubrique }', issuer='{ Émetteur }', error='{ Détails de l'erreur }', depth='{ Profondeur }'"	Le certificat d'une session TLS n'est pas valide.	Remplacez le certificat de la session TLS spécifiée.

15.4.2 Configuration d'évènements

La configuration d'évènements est uniquement disponible dans la CLI.

Pour plus d'informations, voir le Manuel de configuration SINEC OS CLI.

15.4.3 Surveillance d'alarmes

Ce paragraphe décrit les différentes méthodes de surveillance d'alarmes.

15.4.3.1 Listage d'alarmes actives

Pour lister toutes les alarmes actuellement actives, naviguez vers **System** ≫ **Events** ≫ **Active Alarms**.

Toutes les alarmes actives sont affichées sous forme de tableau.

Les informations suivantes sont affichées pour chaque alarme active :

Paramètres	Description
Date Time	Date et l'heure auxquelles l'évènement est survenu.
Resource	Ressource (ou sous-système) associé à l'évènement.
Event ID	Nom de l'évènement
Message	Le message d'erreur
Event Number	Le nombre d'instances actives de l'alarme déclenchée par le même évènement. Exemple : La valeur 2 indique que le même évènement s'est produit deux fois. Chaque fois qu'une alarme est supprimée, le nombre d'évènements diminue. L'alarme est retirée de la liste dès que le nombre d'évènements est égal à 0.
Severity	Le niveau de gravité associé à l'évènement.
User Action	Action requise de l'utilisateur. Valeurs possibles : • **clear-or-ack** – Une alarme doit être supprimée ou acquittée. • **resolve-or-ack** – Attendez que l'erreur se résolve d'elle-même ou acquittez l'alarme.
Actuators/Status	État des actionneurs tels que le contact de signalisation ou la LED d'alarme. Valeurs possibles : • **none** – Aucun effet sur les actionneurs • **led** – Seule la LED d'alarme est actionnée • **relay** – Seul le contact de signalisation est actionné • **led-relay** – La LED d'alarme et le contact de signalisation sont actionnés • **acked** – L'évènement a été acquitté par un utilisateur et l'actionneur/les actionneurs ont été réinitialisés

15.4.3.2 Suppression et acquittement d'alarmes

Les alarmes actives peuvent être acquittées ou supprimées individuellement ou toutes ensemble.

Acquittement de toutes les alarmes actives

Pour acquitter toutes les alarmes actives, procédez comme suit :

1. Naviguez vers **System** ≫ **Events** ≫ **Active Alarms**.
2. Sous **Active Alarms**, cliquez sur **Acknowledge**.

Acquittement d'alarmes sélectionnées

Pour acquitter une alarme spécifique liée à l'état, procédez comme suit :

1. Naviguez vers **System** ≫ **Events** ≫ **Active Alarms**.
2. Sous **Active Alarms**, cliquez dans le tableau **Acknowledge** sur l'alarme sélectionnée.

Suppression de toutes les alarmes actives

Pour supprimer toutes les alarmes actives, procédez comme suit :

1. Naviguez vers **System** ≫ **Events** ≫ **Active Alarms**.
2. Sous **Active Alarms**, cliquez sur **Clear**.

Suppression d'alarmes sélectionnées

Pour supprimer une alarme spécifique, non liée à l'état, procédez comme suit :

1. Naviguez vers **System** ≫ **Events** ≫ **Active Alarms**.
2. Sous **Active Alarms**, cliquez dans le tableau **Clear** sur l'alarme sélectionnée.

15.5 SMTP

Les évènements peuvent être configurés de manière à envoyer un e-mail à une liste définie de destinataires lorsque l'évènement en question se produit. Cela permet p. ex. d'avertir un certain nombre d'administrateurs lorsqu'un problème est survenu sur l'un de leurs appareils.

Les e-mails sont envoyés via Simple Mail Transfer Protocol (SMTP).

Remarque

Le service SMTP doit être activé globalement et également pour chaque évènement qui envoie une notification par e-mail.

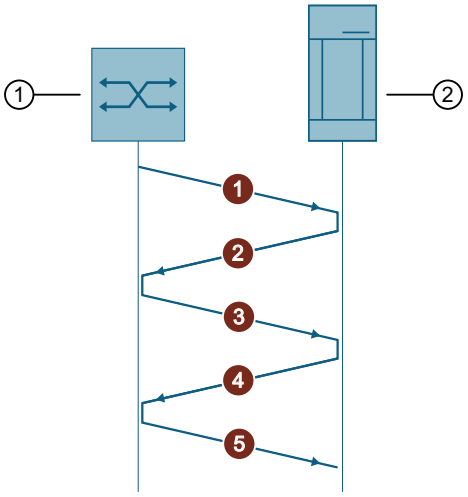
Pour plus d'informations sur la configuration d'évènements, voir le **Manuel de configuration SINEC OS CLI**.

15.5.1 Ce qu'il faut savoir sur SMTP

Le client SMTP communique avec un serveur SMTP distant afin d'envoyer des notifications par e-mail à une liste définie de destinataires. Certains serveurs SMTP peuvent exiger un compte d'utilisateur et une authentification pour que les requêtes par e-mail puissent être traitées par le client.

15.5.1.1 Échange entre client SMTP et serveur SMTP

Lorsqu'un évènement se produit et que l'alarme associée est configurée pour envoyer une notification par e-mail, le client SMTP sur l'appareil initie une connexion TCP avec un serveur SMTP distant. Ensuite, l'échange suivant a lieu entre le client et le serveur SMTP :



① SMTP Client
② SMTP Server

Figure 15-1 Séquence de communication SMTP

Opération	Description
1	Le client SMTP envoie un message HELLO au serveur SMTP. La connexion TCP est établie
2	Le serveur SMTP répond au message HELO.
3	Le client SMTP envoie : • l'adresse e-mail à partir de laquelle le message doit être envoyé • la liste des destinataires
4	Le serveur SMTP accepte l'adresse e-mail et la liste des destinataires.
5	Le client SMTP envoie l'e-mail au serveur SMTP.

15.5.1.2 Format de l'e-mail

Tous les e-mails envoyés par le service SMTP contiennent les informations suivantes :

From:	{ Adresse e-mail SMTP }
To:	{ La liste des destinataires }
Subject:	Received event from device { `Nom d'hôte` } with resource({ `Ressource` }) and ID ({ `ID d'évènement` })

Date:	{ Date }
A new event is raised on device { Nom d'appareil } (located at { Localisation }) with the following details: Resource: { Ressource } Event ID: { ID d'évènement } Severity: { Niveau de gravité } Time: { Date et heure } Serial number: { Numéro de série } Message: { Message d'alarme }	

Exemple

From:	alerts@company.com
To:	emmanuel.goldstein@company.com; winston.smith@company.com
Subject:	Received event from device XCM332 with resource(switch-mgmt) and ID(Linkdown/linkup)
Date:	Fri, 11 Jun 2021 16:24:38 +0000 (2021-06-11 12:24:38 PM)
A new event is raised on device XCM332 (located at facility 7B) with the following details: Resource:switch-mgmt Event ID:Linkdown/linkup Severity:info Fri Jun 11 16:24:38 2021 Serial Number:VPM5001692 Message:Port ethernet0/4 is down	

15.5.2 Configuration de SMTP

Pour configurer SMTP, procédez comme suit :

1. Ajoutez des utilisateurs qui doivent recevoir les e-mails du service SMTP.
   Pour plus d'informations, voir "Ajout des destinataires d'e-mail (Page 314)".
2. Configurez le compte utilisateur SMTP.
   Pour plus d'informations, voir "Configuration du compte SMTP (Page 315)".
3. Configurez les paramètres du serveur SMTP.
   Pour plus d'informations, voir "Configuration d'un serveur SMTP (Page 316)".
4. Testez la connexion au serveur.
   Pour plus d'informations, voir "Tester la connexion au serveur SMTP (Page 315)".
5. Activez SMTP.
   Pour plus d'informations, voir "Activation de SMTP (Page 315)".

15.5.2.1 Ajout des destinataires d'e-mail

Les e-mails du service SMTP peuvent être envoyés à 20 adresses e-mail à la fois.

Pour ajouter une adresse e-mail à la liste des destinataires, procédez comme suit :

1. Naviguez vers **System** ≫ **SMTP Client**.
2. Sous **SMTP Recipients**, cliquez sur **Add**. Une nouvelle ligne est insérée dans le tableau.
3. Sous **Email Address**, entrez l'adresse e-mail du nouveau destinataire.
4. Validez la modification.

15.5.2.2 Tester la connexion au serveur SMTP

Pour tester la connexion au serveur SMTP, procédez comme suit :

1. Naviguez vers **System** ≫ **SMTP Client**.
2. Sous **Simple Mail Transfer Protocol (SMTP) Client**, cliquez sur **Test SMTP**.

15.5.2.3 Activation de SMTP

Pour activer le service SMTP, procédez comme suit :

Remarque

Le service SMTP est désactivé par défaut.

Remarque

Le compte SMTP doit être configuré avant que le service SMTP puisse être activé.

Pour plus d'informations sur la configuration du compte SMTP, voir "Configuration du compte SMTP (Page 315)".

1. Naviguez vers **System** ≫ **SMTP Client**.
2. Sous **Simple Mail Transfer Protocol (SMTP) Client**, modifiez **Status** en **Enabled**.
3. Validez la modification.

15.5.3 Configuration du compte SMTP

Le service SMTP nécessite un compte de messagerie à partir duquel tous les messages d'évènements sont envoyés.

Pour configurer le compte, procédez comme suit :

1. Configurez l'adresse e-mail à partir de laquelle tous les messages d'évènement seront envoyés.
   Pour plus d'informations, voir "Configuration de l'adresse e-mail du compte (Page 316)".
2. [Facultatif] Ajoutez une description de l'adresse.
   Pour plus d'informations, voir "Ajout d'une description du compte (Page 316)".

15.5.3.1 Configuration de l'adresse e-mail du compte

Pour spécifier le compte de messagerie à partir duquel SMTP enverra tous les messages d'évènement, procédez comme suit :

1. Naviguez vers **System** ≫ **SMTP Client**.
2. Sous **SMTP Account**, entrez dans **Email Address**, l'adresse e-mail du compte SMTP.
3. Validez la modification.

15.5.3.2 Ajout d'une description du compte

Pour ajouter une description du compte SMTP, procédez comme suit :

1. Naviguez vers **System** ≫ **SMTP Client**.
2. Sous **SMTP Account**, saisissez dans **Description** une brève description.
   Condition :
   – Elle doit compter de 1 à 128 caractères.
3. Validez la modification.

15.5.4 Configuration d'un serveur SMTP

Pour configurer les paramètres du serveur SMTP, procédez comme suit :

Remarque

Ne définissez pas plus d'un serveur SMTP.

1. Configurez le profil du serveur SMTP pour le serveur qui doit être utilisé pour distribuer les notifications par e-mail.
   Pour plus d'informations, voir "Configuration du profil du serveur SMTP (Page 317)".
2. Définissez le temps maximum que SINEC OS attend une réponse du serveur SMTP.
   Pour plus d'informations, voir "Configuration de la temporisation des réponses SMTP (Page 317)".
3. [Facultatif] Configurez le client SMTP pour qu'il s'authentifie automatiquement auprès du serveur SMTP.
   Pour plus d'informations, voir "Configuration de l'authentification SMTP (Page 317)".

15.5.4.1 Configuration du profil du serveur SMTP

Pour configurer le profil du serveur SMTP utilisé pour distribuer les notifications par e-mail, procédez comme suit :

1. Naviguez vers **System** ≫ **SMTP Client**.
2. Sous **SMTP Server**, saisissez dans la colonne **Server Address/FQDN** le nom d'hôte ou l'adresse IP du serveur SMPT.
   Condition :
   - Le nom ou l'adresse doit compter de 0 à 253 caractères
3. Sous **Port**, spécifiez le port sur lequel le serveur SMTP doit recevoir les messages.
   Par défaut : 25
4. [Facultatif] Sous **Description**, entrez une description du serveur SMTP.
   Condition :
   - Elle doit compter de 1 à 128 caractères.
5. Validez les modifications.

15.5.4.2 Configuration de la temporisation des réponses SMTP

Lorsque le client SMTP souhaite établir une connexion TCP au serveur SMTP, il envoie un message HELLO. Le serveur SMTP dispose d'un délai limité pour répondre avant que le client ne considère le serveur comme inaccessible.

Pour configurer le temps que le client SMTP attend une réponse du serveur SMTP, procédez comme suit :

1. Naviguez vers **System** ≫ **SMTP Client**.
2. Sous **SMTP Server**, saisissez dans la colonne **Timeout** le temps sous **Timeout**.
   Conditions :
   - En format nYnMnDnhnmns, dans lequel n est un nombre personnalisé
   - 1 seconde min. (1s)
   - 255 secondes max. (255s)

   Par défaut : 30s (30 secondes)
3. Validez la modification.

15.5.5 Configuration de l'authentification SMTP

Toutes les communications entre le client SMTP et le serveur peuvent être authentifiées. Un compte d'utilisateur est nécessaire pour ce faire sur le serveur SMTP.

Remarque

Le mot de passe est envoyé en texte clair au serveur SMTP. Veuillez vous assurer que le serveur SMTP est configuré de manière à accepter les mots de passe en texte clair.

Pour configurer le client SMTP pour votre propre authentification, procédez comme suit :

1. Créez un compte sur le serveur SMTP. Notez le nom d'utilisateur et le mot de passe du compte créé.
2. Configurez le client SMTP pour qu'il saisisse ces identifiants lors de l'établissement de la connexion au serveur SMTP.
   Pour plus d'informations, voir "Configuration de l'utilisateur SMTP (Page 318)".
3. Activez l'authentification SMTP.
   Pour plus d'informations, voir "Activation de l'authentification SMTP (Page 318)".

15.5.5.1 Configuration de l'utilisateur SMTP

Pour configurer l'utilisateur SMTP, procédez comme suit :

1. Naviguez vers **System** ≫ **SMTP client**.
2. Sous **SMTP Account**, modifiez **Username** en nom d'utilisateur du compte sur le serveur SMTP.
   Conditions :
   - Elle doit compter de 1 à 128 caractères.
   - Il doit débuter par un trait de soulignement (_) ou par un caractère alphanumérique
   - Le nom d'utilisateur peut contenir des caractères alphanumériques, numériques ou ASCII (0x20 à 0x7E), y compris des traits de soulignement (_), des traits d'union (-), des points (.) et le caractère @.
3. Sous **Password**, entrez le mot de passe correspondant au nom d'utilisateur.
   Conditions :
   - Elle doit compter de 1 à 128 caractères.
   - Il doit débuter par un trait de soulignement (_) ou par un caractère alphanumérique
   - Le nom d'utilisateur peut contenir des caractères alphanumériques, numériques ou ASCII (0x20 à 0x7E), y compris des traits de soulignement (_), des traits d'union (-), des points (.) et le caractère @.
4. Saisissez de nouveau le mot de passe sous **Password Confirm**.
5. Validez les modifications.

15.5.5.2 Activation de l'authentification SMTP

Pour activer l'authentification de l'utilisateur SMTP, procédez comme suit :

Remarque

L'authentification de l'utilisateur SMTP est désactivée par défaut.

1. Naviguez vers **System** ≫ **SMTP client**.
2. Sous **SMTP Account**, dans la colonne **Authentication**, sélectionnez l'option **Enabled**.
3. Validez la modification.

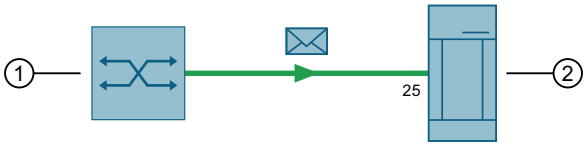
15.5.6 Exemples de configuration

Vous trouverez ci-après des exemples de mise en œuvre de SMTP.

15.5.6.1 Configuration de SMTP pour l'envoi de notifications d'évènements

Cet exemple montre comment configurer l'appareil pour qu'il envoie des notifications par e-mail à un groupe d'administrateurs.

La topologie suivante montre un client SMTP qui envoie des notifications par e-mail à un serveur SMTP distant, ATSNSer6, sur le port 25.



① SMTP Client
② Serveur SMTP (ATSNSer6)

Figure 15-2 Envoi de notifications par e-mail à ATSNSer6

Le client utilise l'authentification SMTP pour s'assurer que la communication est sécurisée. Il est également configuré pour attendre jusqu'à 60 secondes une réponse du serveur.

Pour parvenir à cette configuration, procédez comme suit :

1. Définissez le compte de messagerie à partir duquel toutes les notifications par e-mail seront envoyées.
   Pour plus d'informations, voir "Configuration de l'adresse e-mail du compte (Page 316)".
2. Définissez le serveur SMTP (ATSNSer6) et le numéro de port (25).
   Pour plus d'informations, voir "Configuration du profil du serveur SMTP (Page 317)".
3. Définissez une valeur de 60 secondes pour le délai de réponse du serveur.
   Pour plus d'informations, voir "Configuration de la temporisation des réponses SMTP (Page 317)".
4. Définissez le nom d'utilisateur SMTP pour le serveur SMTP.
   Pour plus d'informations, voir "Configuration de l'utilisateur SMTP (Page 318)".
5. Activez l'authentification SMTP.
   Pour plus d'informations, voir "Activation de l'authentification SMTP (Page 318)".
6. Définissez les destinataires d'e-mail.
   Pour plus d'informations, voir "Ajout des destinataires d'e-mail (Page 314)".
7. Activez le service SMTP.
   Pour plus d'informations, voir "Activation de SMTP (Page 315)".
8. Configurez une ou plusieurs alarmes pour envoyer une notification par e-mail via SMTP.
   Pour plus d'informations, voir "Configuration d'évènements (Page 310)".
9. [Facultatif] Générez une alerte et surveillez le serveur SMTP pour vérifier que la notification par e-mail a bien été transmise.

15.6 Réplication de trafic de données

La réplication de trafic est une fonction de couche 2 qui vous permet de répliquer un ou plusieurs flux de données afin de surveiller et d'analyser le trafic. Le trafic répliqué est retransmis à un analyseur/renifleur de paquets externe. Les administrateurs et les techniciens de réseau analysent le trafic afin de détecter les attaques, d'analyser les données, de rechercher et de corriger les erreurs et de surveiller les performances globales du réseau.

15.6.1 Ce qu'il faut savoir sur la réplication du trafic de données

Le trafic de données reçu et/ou transmis sur n'importe quel port de pont ou VLAN peut être répliqué (copié et retransmis) vers un analyseur de paquets/renifleur. L'analyseur peut être connecté localement à l'appareil sur lequel le trafic répliqué est généré ou à un appareil distant accessible via le réseau.

15.6.1.1 Sessions de réplication du trafic de données

Une session de réplications du trafic définit plusieurs sources de trafic (par exemple des ports de pont ou de VLAN) et une destination vers laquelle le trafic répliqué est acheminé. La destination de toutes les sessions doit être unique.

SINEC OS ne prend actuellement en charge qu'une seule session (session 1), préconfigurée avec un port de destination (ethernet0/1). Il s'agit d'une configuration standard qui peut être modifiée si nécessaire.

IMPORTANT
Risque de configuration - Risque de coupure de la liaison Les ports de pont utilisés pour la gestion de l'appareil ne doivent pas être choisis comme destination du trafic répliqué. Lorsqu'un port de pont est configuré comme destination pour la réplication du trafic, il est automatiquement retiré de tous les VLAN et basculé en mode port de commutateur. Toutes les sessions actives sur ce port sont fermées et il ne sera plus possible d'accéder à l'appareil via ce port.

15.6.1.2 Sources et destinations pour la réplication du trafic de données

Pour la réplication du trafic, il faut définir une ou plusieurs sources de trafic et une destination de la réplication.

Sources du trafic de données

Une source de trafic peut être un port de pont et/ou un VLAN.

Si la source est un port de pont, seul le trafic d'une direction donnée (entrant ou sortant) peut être répliqué ou tout le trafic du port peut l'être.

Si la source est un VLAN, tout le trafic est répliqué sur l'appareil qui appartient au VLAN.

Destinations de la réplication

Une cible de la réplication peut être un port de pont spécifique ou une adresse IP vers laquelle le trafic répliqué est redirigé.

Utilisez un port de pont spécial si l'analyseur/renifleur de paquets est directement connecté à l'appareil ou à un autre appareil du même réseau.

Une autre possibilité consiste à retransmettre le trafic par Encapsulated Remote Traffic Mirroring (ERTM) si l'analyseur/renifleur de paquets est accessible via une adresse IP. ERTM encapsule le trafic répliqué avec des en-têtes MAC, IP et GRE et l'achemine dans un réseau de couche 3 via un tunnel GRE. Le trafic encapsulé est transmis à l'analyseur comme un trafic de couche 3 normal et y est désencapsulé avant l'analyse.

15.6.1.3 Appliquer la réplication de trafic de données

Tenez compte des exigences et des restrictions suivantes avant de répliquer le trafic de données :

- Si le débit en duplex intégral des trames sur le port de pont source dépasse la vitesse de transmission du port de destination, les trames sont rejetées. Comme le trafic reçu et transmis du port de pont source est répliqué sur le port de destination, les trames sont rejetées si le trafic total dépasse la vitesse de retransmission du port de destination. Ce problème est encore accentué lorsque le trafic de données d'un port source en duplex intégral de 100 Mbit/s est répliqué vers un port cible en semi-duplex de 10 Mbit/s.
- Les trames de gestion des commutateurs générées par le périphérique (telles que Telnet, HTTP, SNMP, etc.) ne sont éventuellement pas répliquées.
- Les trames non valides reçues sur le port de surveillance ne sont pas répliquées. Il s'agit notamment des erreurs CRC, des paquets de données trop grands ou trop petits, des fragments, du jabber, des collisions, des collisions tardives et des évènements rejetés.

15.6.2 Configuration de la réplication de trafic de données

Pour configurer la réplication du trafic, procédez comme suit :

1. Définissez une ou plusieurs sources de trafic à surveiller.
   Une source de trafic peut être un port de pont avec une direction de trafic spécifique (c'est-à-dire entrant, sortant ou les deux) ou un VLAN. Chaque source de trafic doit être configurée séparément.
   Pour plus d'informations, voir "Sélectionnez une source de trafic de données (Page 322)".
2. Sélectionnez la destination du trafic de données répliqué.
   La destination peut être un port de pont ou une adresse IP.
   Pour plus d'informations, voir "Définition de la destination de la réplication (Page 323)".
3. Activez la réplication du trafic de données.
   Pour plus d'informations, voir "Activation de la réplication du trafic de données (Page 323)".

15.6.2.1 Sélectionnez une source de trafic de données

Plusieurs sources de trafic peuvent être définies dans une session de réplication de trafic. Les sources peuvent être des flux de trafic reçus et/ou transmis via une interface et/ou appartenant à un VLAN particulier.

Pour sélectionner une source de trafic, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Traffic Mirroring**.
2. Sous **Traffic Mirroring Sources**, sélectionnez une interface ou la source VLAN pour la session voulue.
   Définissez les paramètres ci-après pour une interface :
   - **Ingress Traffic of Ports**
     Sélectionnez une ou plusieurs interfaces. Le trafic de données reçu par les interfaces est répliqué.
   - **Egress Traffic of Ports**
     Sélectionnez une ou plusieurs interfaces. Le trafic de données retransmis par les interfaces est répliqué.

   Configurez ce qui suit pour un VLAN :
   - **Traffic of VLANs**
     Sélectionner un ID de VLAN ou saisissez l'ID. Le trafic de données du VLAN indiqué est répliqué.
3. Validez les modifications.

Exemple

Dans l'exemple suivant, la session 1 est uniquement configurée pour répliquer le trafic de données retransmis à ethernet0/5.

Session	Traffic of VLANs	Ingress Traffic of Ports	Egress Traffic of Ports
1	-	0 items selected.	**ethernet0/5**

Exemple

Dans l'exemple ci-après, la session 1 est uniquement configurée pour répliquer le trafic de données reçu par ethernet0/2, ethernet0/3 et ethernet0/4.

Session	Traffic of VLANs	Ingress Traffic of Ports	Egress Traffic of Ports
1	-	**ethernet0/2, ethernet0/3, ethernet0/4**	**ethernet0/5**

Exemple

Dans l'exemple suivant, la session 1 est également configurée pour répliquer le trafic de données balisé du VLAN 10.

Session	Traffic of VLANs	Ingress Traffic of Ports	Egress Traffic of Ports
1	**10**	**ethernet0/2, ethernet0/3, ethernet0/4**	**ethernet0/5**

15.6.2.2 Définition de la destination de la réplication

Le trafic répliqué peut être retransmis vers une interface ou vers une adresse IP.

IMPORTANT
Risque de configuration - Risque de coupure de liaison Les ports de pont utilisés pour la gestion de l'appareil ne doivent pas être choisis comme destination du trafic répliqué. Lorsqu'un port de pont est configuré comme destination pour la réplication du trafic, il est automatiquement retiré de tous les VLAN et basculé en mode port de commutateur. Toutes les sessions actives sur ce port sont fermées et il ne sera plus possible d'accéder à l'appareil via ce port.

Pour définir la destination du trafic de données répliqué, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Traffic Mirroring**.
2. Sous **Traffic Mirroring Sessions**, sélectionnez dans **Destination Port** un port de pont auquel le trafic de données répliqué doit être retransmis.
3. Sous **Destination Remote IP**, saisissez une adresse IP à laquelle le trafic de données répliqué doit être envoyé.
4. Validez les modifications.

Exemple

Dans l'exemple suivant, la session 1 est configurée pour transmettre le trafic de données répliqué à ethernet0/2.

Session	State	Destination Port	Destination Remote IP
1	Disabled	**ethernet0/2**	

Exemple

Dans l'exemple suivant, la session 1 est configurée pour transmettre le trafic de données répliqué à l'adresse IP 172.30.141.141.

Session	State	Destination Port	Destination Remote IP
1	Disabled	-	172.30.141.141

15.6.2.3 Activation de la réplication du trafic de données

La réplication du trafic de données est désactivée par défaut.

IMPORTANT
Risque de configuration - Risque de coupure de la liaison Lorsque la réplication de trafic de données est activée, le port de destination sélectionné est automatiquement retiré de tous les VLAN et basculé en mode port de commutateur. Toutes les sessions actives sur ce port sont fermées et il ne sera plus possible d'accéder à l'appareil via ce port.

Pour activer la réplication du trafic de données, procédez comme suit :

1. Naviguez vers **Layer 2** ≫ **Traffic Mirroring**.
2. Sous **Traffic Mirroring Sessions**, modifiez le paramètre **State** pour la session sélectionnée en **Enabled**.
3. Validez la modification.

Exemple

Dans l'exemple suivant, la réplication du trafic de données est activée pour la session 1.

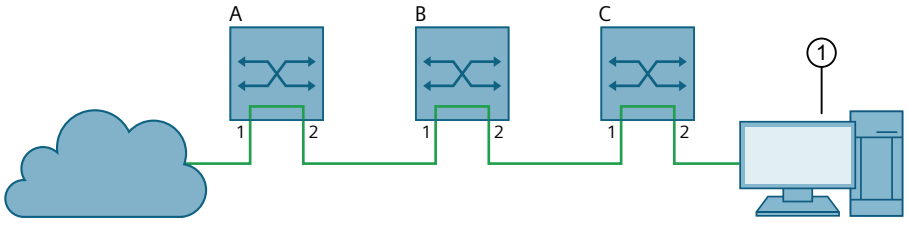
Session	State	Destination Port	Destination Remote IP
1	**Enabled**	ethernet0/1	

15.6.3 Exemples de configuration

Vous trouverez ci-après des exemples de configuration d'une réplication de port.

15.6.3.1 Configuration d'une réplication du trafic de données dans un réseau de couche 2

Dans cet exemple, le trafic reçu sur le port de pont ethernet0/1 du commutateur A est répliqué et transmis au commutateur C, qui est connecté à un analyseur/renifleur de paquets. Le trafic de données répliqué doit être redirigé par le commutateur B.



① Analyseur/renifleur de paquets

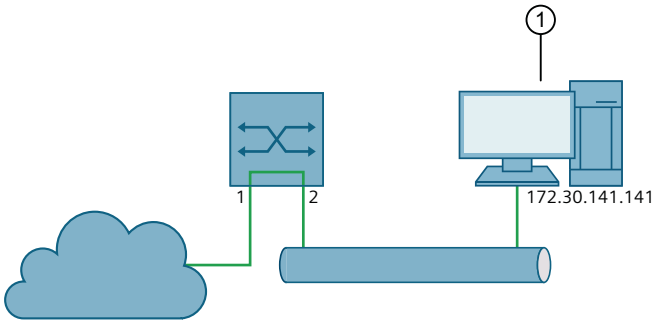
Figure 15-3 Réplication de trafic de données dans un réseau de couche 2

Pour configurer chaque commutateur, procédez comme suit :

1. Paramétrez comme port de pont source ethernet0/1.
   Pour plus d'informations, voir "Sélectionnez une source de trafic de données (Page 322)".
2. Paramétrez comme port de pont de destination ethernet0/2.
   Pour plus d'informations, voir "Définition de la destination de la réplication (Page 323)".
3. Activez la réplication du trafic de données.
   Pour plus d'informations, voir "Activation de la réplication du trafic de données (Page 323)".

15.6.3.2 Configuration de la réplication de trafic distant

Dans cet exemple, le trafic entrant sur ethernet0/1 est répliqué, encapsulé et retransmis via un tunnel GRE vers un ordinateur exécutant un analyseur/renifleur de paquets. L'ordinateur est accessible sous 172.30.141.141.



① Analyseur/renifleur de paquets

Figure 15-4 Encapsulated Remote Traffic Mirroring

Pour configurer l'appareil, procédez comme suit :

1. Paramétrez comme port de pont source ethernet0/1.
   Pour plus d'informations, voir "Sélectionnez une source de trafic de données (Page 322)".
2. Paramétrez comme destination l'adresse IP 172.30.141.141.
   Pour plus d'informations, voir "Définition de la destination de la réplication (Page 323)".
3. Activez la réplication du trafic de données.
   Pour plus d'informations, voir "Activation de la réplication du trafic de données (Page 323)".

15.7 Diagnostic de câbles

Les problèmes de connexion sont parfois dus à des problèmes de câbles Ethernet. Pour détecter des défauts de câbles, des courts-circuits, des câbles ouverts ou des câbles trop longs, SINEC OS dispose d'un utilitaire intégré de diagnostic des câbles.

15.7.1 Exécution d'un test de diagnostic de câble

Pour effectuer un test de diagnostic de câble avec un câble Ethernet, procédez comme suit :

Remarque

Un test de diagnostic de câble sur un seul port de pont prend en moyenne une à deux secondes.

Remarque

Les tests de diagnostic de câbles peuvent être effectués simultanément sur plusieurs ports.

Remarque

Les tests de diagnostic des câbles ne peuvent être effectués que sur des câbles Ethernet en cuivre.

1. Déterminez le port de pont auquel le câble Ethernet à tester est connecté.
2. Veuillez vous assurer que l'autre extrémité de la ligne est connectée à un port de pont présentant les mêmes caractéristiques techniques de réseau.
   Connectez p. ex. un port 100Base-T à un port 100Base-T ou un port 1000Base-T à un port 1000Base-T.
3. Naviguez vers **Interfaces** ≫ **Ethernet interfaces** ≫ **Cable Diagnostics**.
4. Cliquez sur **Démarrer** pour le port de pont sélectionné, pour démarrer le test de diagnostic de câble.
   Les résultats du test sont affichés immédiatement à la fin du test.
   Pour plus d'information sur les résultats du test, voir "Affichage des résultats du diagnostic de câbles (Page 326)".
5. [Facultatif] Réinitialisez le port de pont.
   Pour plus d'informations, voir "Réinitialisation d'un port de pont (Page 326)".

15.7.2 Réinitialisation d'un port de pont

Il peut s'avérer nécessaire, après un test de diagnostic de câbles, de réinitialiser un port de pont afin de rétablir la communication entre celui-ci et son port homologue. La réinitialisation permet de redémarrer certains modes, par exemple l'autonégociation, le mode duplex, etc.

Remarque

Un câble ne peut être réinitialisé que si l'état de diagnostic du port de pont est connu (p. ex. stopped ou started).

Pour réinitialiser un port de pont, procédez comme suit :

1. Naviguez vers **Interfaces** ≫ **Ethernet interfaces** ≫ **Cable Diagnostics**.
2. Cliquez pour le port de pont sélectionné sur **Reset** pour réinitialiser l'interface.

15.7.3 Affichage des résultats du diagnostic de câbles

Les résultats sont disponibles sous **Interfaces** ≫ **Ethernet interfaces** ≫ **Cable Diagnostics** et sont affichés immédiatement après l'exécution du test de diagnostic.

Les informations suivantes sont affichées pour chaque port de pont :

Paramètres	Description
Diagnostic State	État courant du test de diagnostic de câble. Valeurs possibles : • `stopped` - Le test est terminé. • `started` - Le test est encore en cours d'exécution.
Result	Résultat du dernier test de diagnostic des câbles effectué. Valeurs possibles : • `passed` - Le port de pont a passé le dernier test avec succès. • `failed` - Le port du pont n'a pas réussi le dernier test.
Result Pair [*N*]	Résultat du test de câble pour la paire de conducteurs, dans lequel *N* peut prendre les valeurs suivantes : • 12 (paires 1/2) • 36 (paires 3/6) • 45 (paires 4/5) • 78 (paires 7/8) Valeurs possibles : • `good` - Aucun défaut, court-circuit ou désadaptation d'impédance n'a été détecté. • `open` - Un circuit électrique ouvert a été constaté dans le câble (par exemple, pas de contact entre les broches). • `short` - Un court-circuit a été constaté dans le câble. • `impedance` - Une désadaptation d'impédance a été constatée. Pour les ports de pont FastEthernet, un résultat `good` est requis pour `result-pair12` et `result-pair36`. Pour les ports de pont Gigabit Ethernet, un résultat `good` est requis pour toutes les paires de conducteurs.
Distance Pair [*N*]	Le résultat de mesure du test de câble pour la distance au défaut (Distance-to-Fault, DTF), où *N* peut prendre les valeurs suivantes : • 12 (paires 1/2) • 36 (paires 3/6) • 45 (paires 4/5) • 78 (paires 7/8) Le résultat de la mesure indique la distance en mètres (m) entre l'appareil et le défaut sur la ligne.

Dépannage

16

Ce chapitre décrit les erreurs qui peuvent survenir lors du travail avec SINEC OS ou lors du développement d'un réseau, ainsi que l'aide correspondante.

Remarque

Si vous avez besoin d'une assistance supplémentaire, contactez le Service après-vente Siemens.

16.1 L'appareil se trouve dans une boucle de redémarrage

L'appareil effectue sans arrêt des redémarrages et vous ne pouvez plus accéder à l'appareil.

Solution

Si l'appareil effectue sans arrêt des redémarrages, vous disposez des options suivantes :

- Veuillez contacter le service après-vente Siemens.
  Un technicien de service Siemens peut charger les informations de débogage de l'appareil et analyser l'erreur.
  Pour plus d'informations, voir "Service après-vente (Page 18)".
- Restaurez les paramètres par défaut de l'appareil avec le bouton-poussoir.
  Les informations de débogage enregistrées par l'appareil sont alors perdues et l'erreur ne peut pas être examinée.
  Pour plus d'informations, voir "Fonction de bouton-poussoir (Page 96)".