Dépannage des flaps/boucles MAC sur les commutateurs Cisco Catalyst

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Qu'est-ce que le battement MAC ?
- Directives générales de dépannage
- Étude de cas 1
  - Description du problème
  - Topologie
  - Étapes de dépannage
  - Cause première
  - Résolution
- Étude de cas 2
  - Description du problème
  - Topologie
  - Étapes de dépannage
  - Cause première
  - Résolution
- Prévention

Introduction

Ce document décrit comment dépanner les volets/boucles MAC sur les commutateurs Cisco Catalyst.

Conditions préalables

Exigences

Cisco recommande que vous ayez une connaissance fondamentale des concepts de commutation de base et une compréhension du protocole STP (Spanning Tree Protocol) et de ses fonctionnalités sur les commutateurs Cisco Catalyst.

Composants utilisés

Les informations contenues dans ce document sont basées sur les commutateurs Cisco Catalyst avec toutes les versions (ce document n'est pas limité à des versions logicielles ou matérielles spécifiques).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Ce document sert de guide qui présente une approche systématique pour le dépannage des problèmes de flaps ou de boucles MAC sur les commutateurs Cisco Catalyst. Les flaps/boucles MAC sont des interruptions dans un réseau causées par des incohérences dans les tables d’adresses MAC des commutateurs. Ce document fournit non seulement des étapes pour identifier et résoudre ces problèmes, mais inclut également des exemples pratiques pour une meilleure compréhension.

Qu'est-ce que le battement MAC ?

Un battement d’adresse MAC se produit lorsqu’un commutateur reçoit une trame avec la même adresse MAC source, mais à partir d’une interface différente de celle d’où il l’a initialement apprise. Le commutateur bascule ainsi entre les ports, mettant à jour sa table d’adresses MAC avec la nouvelle interface. Cette situation peut provoquer une instabilité du réseau et entraîner des problèmes de performances.

Dans un commutateur Cisco, l'oscillation MAC est généralement consignée sous la forme d'un message similaire à celui-ci :

```
"%SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan x is flapping between port (1) and port (2)"
```

Dans cet exemple, l'adresse MAC xxxx.xxxx.xxxx a d'abord été apprise sur le port d'interface (1), puis vue sur le port d'interface (2), ce qui a provoqué un battement MAC.

La cause la plus fréquente de l'oscillation MAC est une boucle de couche 2 dans le réseau, souvent en raison d'une mauvaise configuration du protocole STP ou de problèmes avec des liaisons redondantes. D'autres causes peuvent inclure du matériel défectueux, des bogues logiciels ou même des problèmes de sécurité tels que l'usurpation MAC.

Le dépannage des failles MAC implique souvent l'identification et la résolution des boucles sur le réseau, la vérification des configurations des périphériques ou la mise à jour du micrologiciel/logiciel des périphériques.

Directives générales de dépannage

- Identifiez le battement MAC : Recherchez dans votre commutateur des journaux indiquant un battement MAC. Par exemple, dans un commutateur Cisco, le message du journal ressemble à ceci :

```
%SW_MATM-4-MACFLAP_NOTIF: Host [mac_address] in vlan [vlan_id] is flapping between port [port_id_
```

- Notez l'adresse MAC et les interfaces : Le message du journal vous indique l'adresse MAC qui est instable et les interfaces entre lesquelles elle est instable. Prenez note de ceux-ci comme ils aident dans votre enquête.
- Examinez les interfaces affectées : Utilisez l'interface de ligne de commande du commutateur afin d'étudier les interfaces impliquées. Vous pouvez utiliser des commandes comme `show interfaces` ou `show mac address-table` afin de voir quels périphériques sont connectés aux interfaces et où l'adresse MAC est apprise.
- Suivez l'adresse MAC instable : MAC apprend par les ports X et Y. Un port nous conduit à l'endroit où cet MAC est branché et l'autre nous mène à la boucle. Choisissez un port et commencez à utiliser la commande `show mac address-table` sur chaque commutateur de couche 2 dans le chemin.
- Rechercher les boucles physiques : Examinez la topologie de votre réseau afin de voir s'il existe des boucles physiques. Cela peut se produire si plusieurs chemins existent entre les commutateurs. Si une boucle est détectée, vous devez reconfigurer votre réseau afin de supprimer la boucle.
- Vérifier STP : Le protocole STP est conçu pour empêcher les boucles dans votre réseau en bloquant certains chemins. Si le protocole STP est mal configuré, il n'empêche pas les boucles comme il doit l'être. Utilisez des commandes comme `show spanning-tree` pour vérifier la configuration STP. Vérifiez également les notifications de modification de topologie (TCN) à l'aide de la commande `show spanning-tree detail | include ieee|occur|from|is`.
- Rechercher les adresses MAC dupliquées : Si deux périphériques de votre réseau ont la même adresse MAC (généralement vue dans la configuration haute disponibilité (HA) et plusieurs cartes réseau (NIC)), cela peut provoquer un battement MAC. Utilisez la commande `show mac address-table` afin de rechercher des adresses MAC en double sur votre réseau.
- Vérifiez si le matériel ou les câbles sont défectueux : Des câbles réseau ou du matériel défectueux peuvent entraîner l'envoi de trames aux mauvaises interfaces, ce qui entraîne un battement MAC. Vérifiez l'état physique de vos câbles et envisagez de remplacer le matériel afin de voir si le problème persiste. Le battement d'interface peut également entraîner le battement MAC sur les commutateurs.
- Rechercher les bogues logiciels : Parfois, le battement MAC peut être causé par des bogues dans le logiciel de vos périphériques réseau. Vérifiez l'outil de recherche de bogues.

Outil de recherche de bogues : https://bst.cloudapps.cisco.com/bugsearch

Aide sur l'outil de recherche de bogue:
https://www.cisco.com/c/en/us/support/web/tools/bst/bsthelp/index.html#search

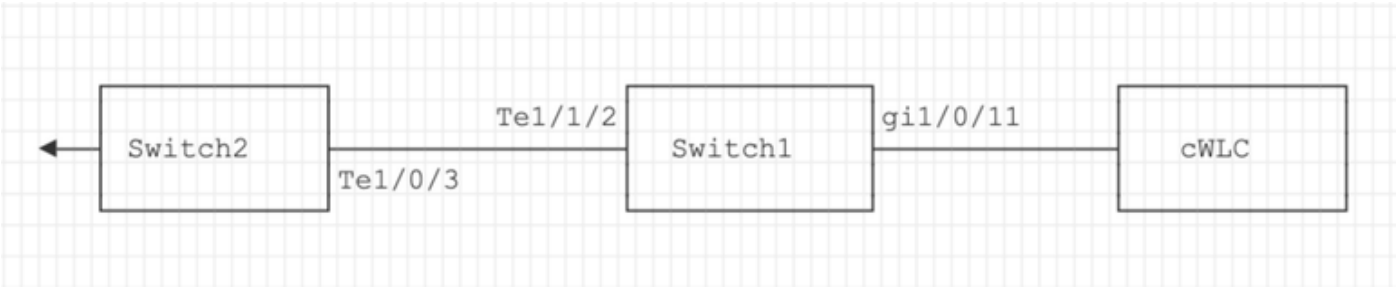
- Contactez l'assistance TAC : Si vous avez tout essayé et que le problème persiste, il peut être temps de contacter l'assistance du TAC Cisco. Ils peuvent fournir une assistance supplémentaire.

Étude de cas 1

Description du problème

Le contrôleur eWLC subit une perte de connectivité à la passerelle, et les pertes de paquets empêchent les AP de rejoindre le contrôleur.

Topologie



Étapes de dépannage

Un battement MAC a été identifié sur le commutateur (Switch1) qui est connecté au WLC électronique.

```
*Aug  5 05:52:50.750: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
*Aug  5 05:53:03.327: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
*Aug  5 05:53:21.466: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
```

Apprentissage MAC :

Entrez la commande show mac address-table address
afin de vérifier l'adresse MAC apprise sur le port.

<#root>

```
Switch1#show mac address-table address 0000.5e00.0101

          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   4    0000.5e00.0101    DYNAMIC     Gi1/0/11
```

```
   4    0000.5e00.0101    DYNAMIC     Te1/1/2
```

Configuration des ports Gi1/0/11 et Te1/1/2 :

Entrez la commande show running-config interface
afin de vérifier la configuration de l'interface.

<#root>

```
interface GigabitEthernet1/0/11


 switchport trunk native vlan 4
 switchport mode trunk
end


interface TenGigabitEthernet1/1/2


 switchport mode trunk
end
```

Voisins CDP des ports Gi1/0/11 et Te1/1/2 :

Entrez la commande show cdp neighbors
afin de vérifier les détails des périphériques connectés.

<#root>

```
Switch1#show cdp neighbors gi1/0/11


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

eWLC            Gig 1/0/11        130              R T   C9115AXI- Gig 0 < ----- eWLC Controller



Switch1#show cdp neighbors gi1/1/2


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

Switch2
```

```
Ten 1/1/2        163            R S I  C9500-16X Ten 1/0/3 < ----- Uplink Switch
```

Apprentissage MAC sur Switch2 (commutateur de liaison ascendante) :

Entrez la commande show mac address-table address
afin de vérifier l'adresse MAC apprise sur le port.

<#root>

```
Switch2#show mac address-table address 0000.5E00.0101


          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   4    0000.5e00.0101    STATIC

Vl4 < ----- VRRP MAC of Vlan4


   4    0000.5e00.0101    DYNAMIC

Te1/0/13 < ----- Learning from Switch1 (eWLC connected Switch)
```

<#root>

```
Switch2#show vrrp  vlan 4


Vlan4 - Group 1

 - Address-Family IPv4
  State is MASTER
  State duration 5 days 4 hours 22 mins
  Virtual IP address is x.x.x.x

  Virtual MAC address is 0000.5E00.0101 < ------ VRRP MAC of Vlan4


  Advertisement interval is 1000 msec
```

Cause première

Il a été vérifié que l'ID VRRP (Virtual Router Redundancy Protocol) du commutateur 2 et le WLC électronique étaient identiques, ce qui a entraîné la génération du même MAC virtuel par le VRRP.

Résolution

Le problème a été résolu après la modification de l'instance VRRP sur le WLC, ce qui provoquait

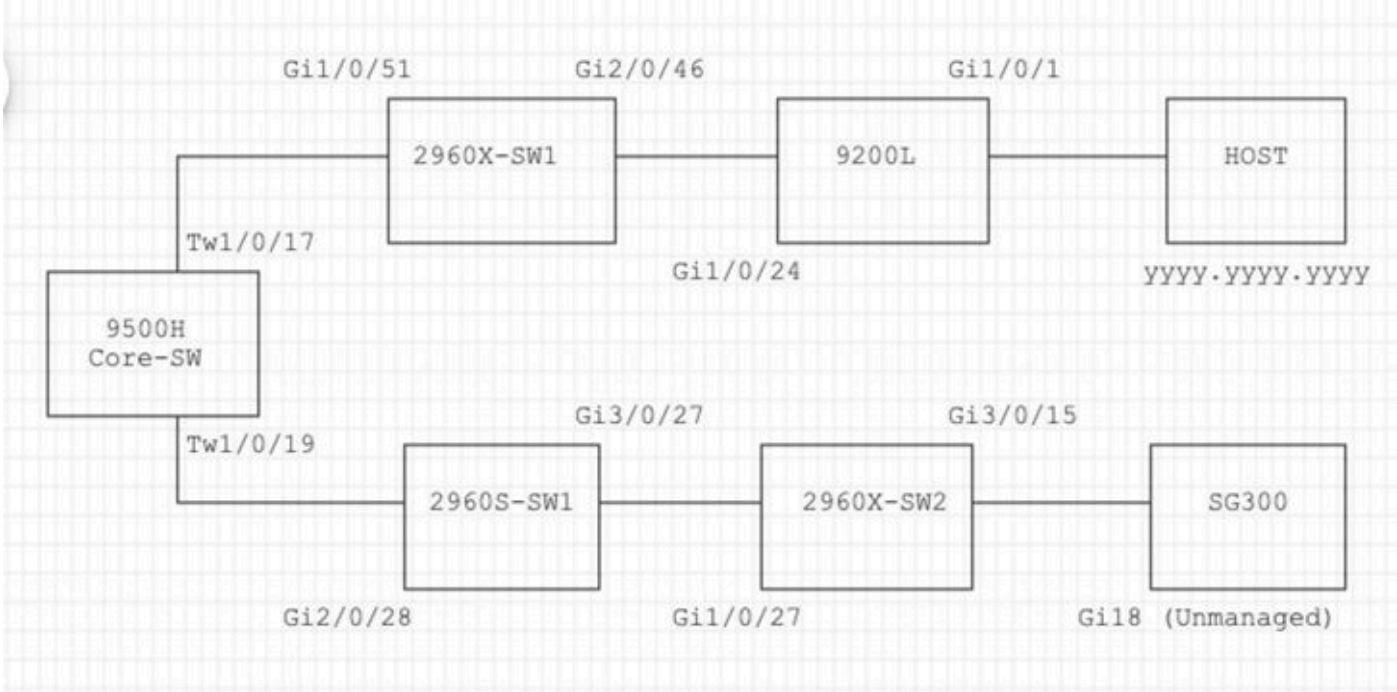
un MAC dupliqué sur le commutateur entraînant une perte de connectivité à la passerelle et des pertes de paquets, ce qui empêchait les AP de rejoindre le contrôleur.

Étude de cas 2

Description du problème

Certains serveurs sont inaccessibles ou connaissent une latence/des pertes importantes.

Topologie



Étapes de dépannage

1. Un battement MAC a été détecté sur le commutateur principal.

```
Nov 14 08:36:34.637: %SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan 1 is flapping between port Tw
Nov 14 08:36:34.838: %SW_MATM-4-MACFLAP_NOTIF: Host yyyy.yyyy.yyyy in vlan 1 is flapping between port Tw
Nov 14 08:36:34.882: %SW_MATM-4-MACFLAP_NOTIF: Host zzzz.zzzz.zzzz in vlan 1 is flapping between port Po
```

2. Choisissez l’adresse MAC yyyy.yyyy.yyyy pour le processus de dépannage.

Apprentissage MAC :

Entrez la commande show mac address-table address
afin de vérifier l'adresse MAC apprise sur le port.

<#root>

```
Core-SW#show mac address-table address yyyy.yyyy.yyyy


          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy    DYNAMIC     Twe1/0/17
```

Voisins CDP des ports Twe 1/0/17 et Twe 1/0/19 :

Entrez la commande show cdp neighbors
afin de vérifier les détails des périphériques connectés.

<#root>

```
Core-SW#show cdp neighbors Twe 1/0/17


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

2960X-SW1

                 Twe 1/0/17        162              S I   WS-C2960X Gig 1/0/51



Core-SW#show cdp neighbors Twe 1/0/19


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

2960S-SW1

                 Twe 1/0/19        120              S I   WS-C2960S Gig 2/0/28
```

Journaux de 2960X-SW1 connectés à Core-SW Twe1/0/17 :

MAC yyyy.yyyy.yyyy oscille entre les ports Gi1/0/51 et Gi2/0/46 (9200L).

<#root>

```
2960X-SW1#show mac address-table address yyyy.yyyy.yyyy
```

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy    DYNAMIC     Gi1/0/51
```

2960X-SW1#show mac address-table address yyyy.yyyy.yyyy

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy DYNAMIC     Gi2/0/46
```

2960X-SW1#show run interface gi 1/0/51

```
Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet1/0/51
switchport mode trunk
end
```

2960X-SW1#show run interface gi 2/0/46

```
Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet2/0/46
switchport mode trunk
end
```

Journaux de 9200L :

(Il semble s'agir du port valide pour cette adresse MAC.)

<#root>

9200L#show mac address-table address yyyy.yyyy.yyyy

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy DYNAMIC     Gi1/0/1
```

9200L#show run interface gi 1/0/1

```
Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet1/0/1
switchport mode access
end
```

2960S-SW1 connecté à Core-SW Twe1/0/19 :

(Il semble s'agir d'un chemin de boucle.) Le port sur le Core-SW a été arrêté afin d'atténuer la boucle.

Cependant, des flaps MAC étaient toujours observés sur le Core-SW.

Journaux de 2960S-SW1 :

<#root>

```
Nov 14 08:36:34.637: %SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan 1 is flapping between port G
Nov 14 08:36:34.838: %SW_MATM-4-MACFLAP_NOTIF: Host yyyy.yyyy.yyyy in vlan 1 is flapping between port G
Nov 14 08:36:34.882: %SW_MATM-4-MACFLAP_NOTIF: Host zzzz.zzzz.zzzz in vlan 1 is flapping between port G
```

2960S-SW1#show run interface gi 3/0/27

```
Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet3/0/27
switchport mode trunk
end
```

2960S-SW1#show cdp neighbor gi 3/0/27

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
```

2960X-SW2

Gig 3/0/27 176 S I WS-C2960X Gig 1/0/27

Journaux de 2960X-SW2 :

<#root>

```
2960X-SW2#show run interface gi 3/0/15


Building configuration...

Current configuration : 39 bytes
!
interface GigabitEthernet3/0/15
end


2960X-SW2#show cdp neighbor gi 3/0/15


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

SG300     Gig 3/0/15        157              S I   SG300-28P gi18




2960X-SW2#config terminal


2960X-SW2(config)#interface gi 3/0/15


2960X-SW2(config-if)#shutdown
```

Cause première

Des failles MAC ont été détectées en raison du commutateur SG300 (non géré) connecté au réseau.

Résolution

Le problème de battement MAC a été résolu en arrêtant le port connecté au commutateur non géré SG300.

Prévention

STP Portfast :

STP PortFast fait passer immédiatement un port LAN de couche 2 à l'état de transmission, en contournant les états d'écoute et d'apprentissage. STP PortFast empêche la génération de TCN STP, qui ne sont pas significatifs à partir des ports qui ne reçoivent pas les BPDU (Bridge Protocol Data Units) STP. Configurez STP PortFast uniquement sur les ports connectés aux périphériques

hôtes finaux qui terminent les VLAN et à partir desquels le port ne doit jamais recevoir de BPDU STP, tels que les stations de travail, les serveurs et les ports sur les routeurs qui ne sont pas configurés pour prendre en charge le pontage.

Protection BPDU :

STP BPDU Guard complète la fonctionnalité de STP PortFast. Sur les ports compatibles STP PortFast, STP BPDU Guard protège les boucles de couche 2 que STP ne peut pas fournir lorsque STP PortFast est activé. STP BPDU Guard arrête les ports qui reçoivent des BPDU.

Root Guard :

Root Guard empêche les ports de devenir des ports racine STP. Utilisez STP Root Guard afin d'empêcher les ports inappropriés de devenir des ports racine STP. Un exemple de port inapproprié est un port qui se connecte à un périphérique qui n'est pas directement contrôlé par l'administrateur réseau.

Protection de boucle :

La protection contre les boucles est une optimisation propriétaire de Cisco pour le protocole STP. Le dispositif de protection contre les boucles protège les réseaux de couche 2 contre les boucles qui se produisent lorsque quelque chose empêche le transfert normal des unités BPDU sur des liaisons point à point (par exemple, un dysfonctionnement de l'interface réseau ou une CPU occupée). La protection contre les boucles complète la protection contre les défaillances de liaison unidirectionnelle fournie par la détection de liaison unidirectionnelle (UDLD). Le dispositif de protection contre les boucles isole les défaillances et permet au protocole STP de converger vers une topologie stable, le composant défaillant étant exclu de la topologie STP.

Filtre BPDU :

Cela désactive le protocole STP. Les BPDU ne sont ni envoyées ni traitées à leur réception. Il est commun aux fournisseurs de services, pas nécessairement aux réseaux d'entreprise.

UDLD agressif :

Le protocole UDLD propriétaire de Cisco surveille la configuration physique des liaisons entre les périphériques et les ports qui prennent en charge UDLD. UDLD détecte l'existence de liaisons unidirectionnelles. UDLD peut fonctionner en mode normal ou agressif. UDLD en mode normal classe une liaison comme unidirectionnelle si les paquets UDLD reçus ne contiennent pas d'informations correctes pour le périphérique voisin. En plus de la fonctionnalité du mode normal UDLD, le mode agressif UDLD met les ports dans l'état err-disabled si la relation entre deux voisins précédemment synchronisés ne peut pas être rétablie.

Contrôle des tempêtes :

Le contrôle des tempêtes de trafic est implémenté dans le matériel et n'affecte pas les performances globales du commutateur. En général, les stations d'extrémité telles que les PC et les serveurs sont la source du trafic de diffusion qui peut être supprimé. Afin d'éviter le traitement inutile du trafic de diffusion excédentaire, activez le contrôle de tempête de trafic pour le trafic de

diffusion sur les ports d'accès qui se connectent aux stations d'extrémité et sur les ports qui se connectent aux noeuds de réseau clés.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.