Mist 設定マニュアル

- Wired Assurance -

スイッチへの DHCP Snooping の設定

ジュニパーネットワークス株式会社
2023年11月 Ver 1.0

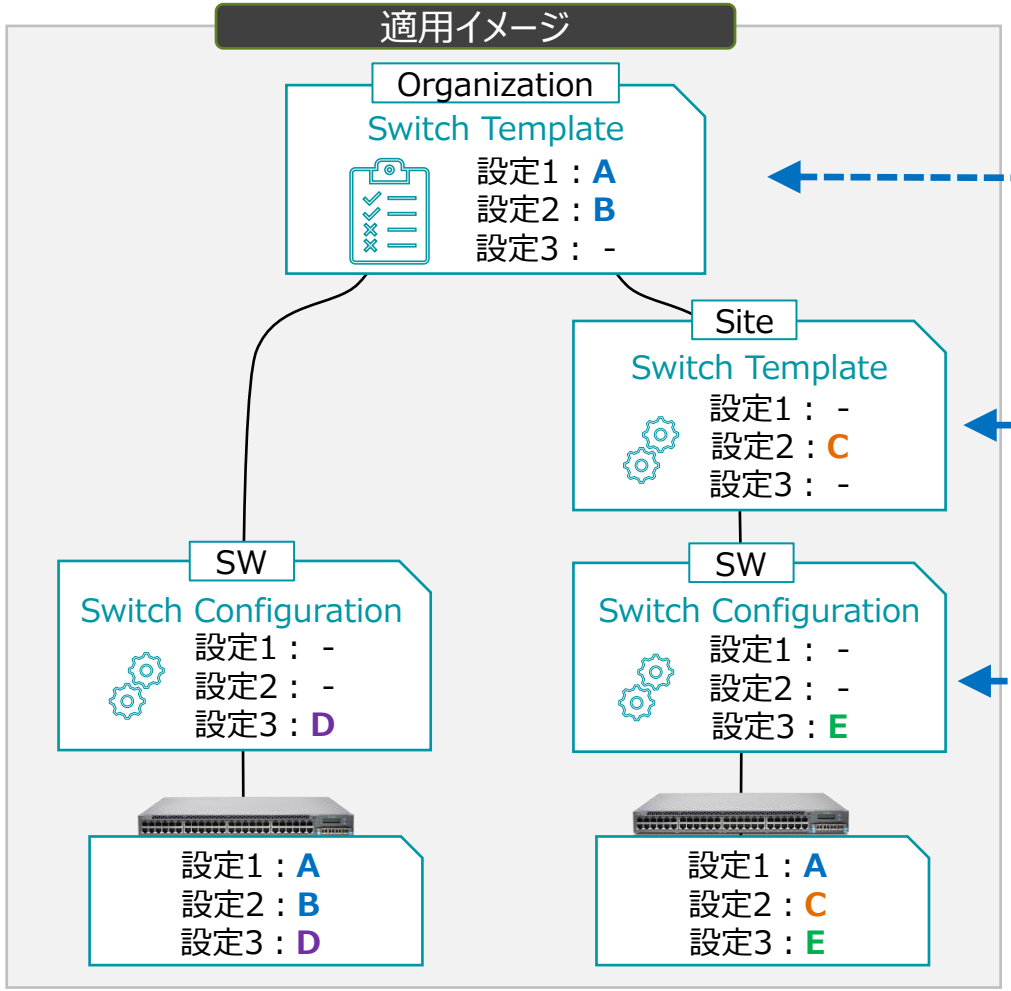
JUNIPer driven by Mist AI

はじめに

- 本マニュアルは、『Wired Assurance におけるスイッチへの DHCP Snooping の設定』について説明します
- 手順内容は 2023年11月 時点の Mist Cloud にて確認を実施しております
  実際の画面と表示が異なる場合は以下のアップデート情報をご確認下さい
  https://www.mist.com/documentation/category/product-updates/
- 設定内容やパラメータは導入する環境や構成によって異なります
  各種設定内容の詳細は下記リンクよりご確認ください
  https://www.mist.com/documentation/
- 他にも多数の Mist 日本語マニュアルを「ソリューション＆テクニカル情報サイト」に掲載しております
  https://www.juniper.net/jp/ja/local/solution-technical-information/mist.html
- **本資料の内容は資料作成時点におけるものであり事前の通告無しに内容を変更する場合があります**
  また本資料に記載された構成や機能を提供することを条件として購入することはできません

テンプレートを使用した設定の概要

Mist の管理画面からスイッチに対し、テンプレートを使用した設定が可能です



Organization レベルの設定

- 選択した複数の Site に紐付くスイッチに対し、Organization 単位で一括設定する場合に使用するテンプレートです

Site レベルの設定

- それぞれの Site に登録されているスイッチに対し、Site 単位で一括設定する場合に使用するテンプレートです
- 同じ設定項目の場合、Organization レベルでの設定は上書きされ、Site レベルの設定が有効になります

各スイッチ単位の設定

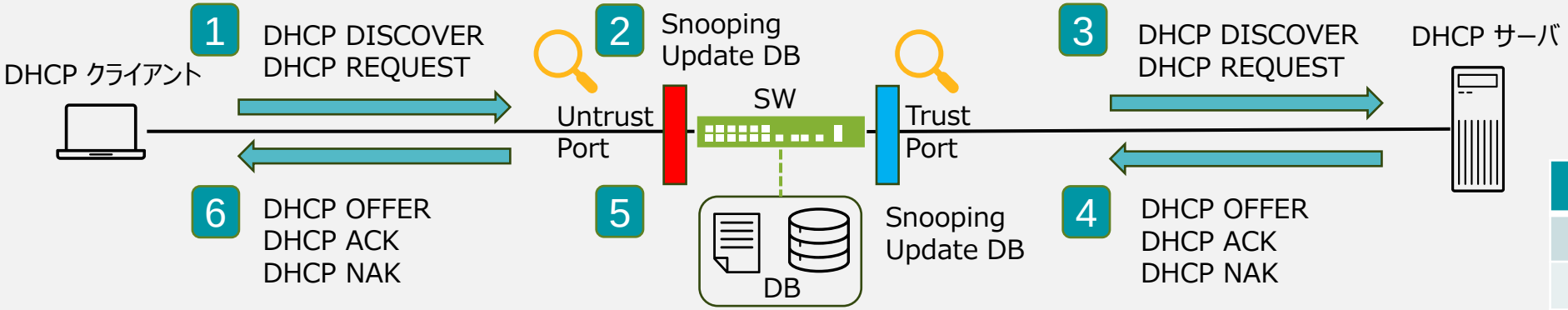
- 各スイッチごとにテンプレートとは異なる設定を行う場合に使用します
- 同じ設定項目の場合、Organization レベルおよび Site レベルでの設定は上書きされ、スイッチ単位の設定が有効になります

ポートセキュリティ

DHCP Snooping

DHCP Snooping

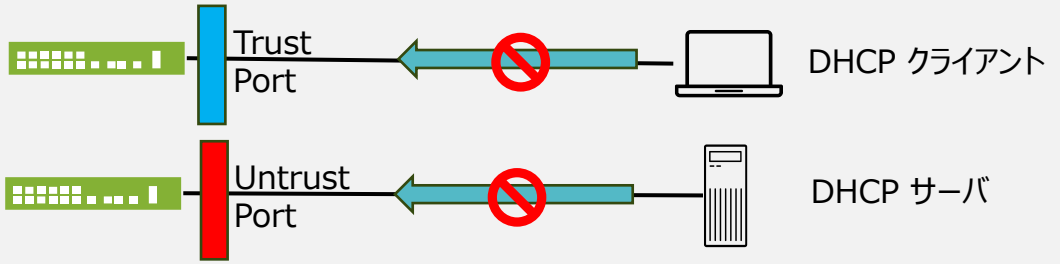
DHCP Snooping とは、スイッチ上で送受信される DHCP サーバと DHCP クライアント間の DHCP パケットを Snooping (のぞき見)して DB を構築することで、 DHCP サーバ/クライアントのなりすまし等を防ぐポートセキュリティ機能の一つです



Mode	default
Trunk	Trusted Port
Access	Untrusted Port

1. DHCP クライアントが DHCP DISCOVER/DHCP REQUEST を送信
2. スイッチは DHCP パケットを Snooping して、Snooping DB を更新
3. スイッチは DHCP DISCOVER/DHCP REQUEST をフォワーディング
4. DHCP サーバは DHCP OFFER/DHCP ACK/DHCP NAK を送信
5. スイッチは DHCP パケットを Snooping して、Snooping DB を更新
6. スイッチは DHCP OFFER/DHCP ACK/DHCP NAK をフォワーディング

Port Type	Description
Trusted Port	DHCP サーバからのトラフィックの受信を許可
Untrusted Port	DHCP クライアントからのトラフィックの受信を許可



ポートセキュリティ

ARP Inspection / IP Source Guard

ARP Inspection

ARP Inspection は、DHCP snooping DB を利用して ARP スプーフィング攻撃をブロックします
DAI(Dynamic ARP Inspection) は、Untrusted Port の ARP パケットを傍受して DHCP Snooping DB で ARP パケットの送信元 MAC アドレスが有効なエントリーと一致するか照合します

- データベース内の IP-MAC エントリーが ARP パケット内の情報に対応しない場合、ARP パケットを破棄します
- パケット内の IP アドレスが無効な場合、ARP パケットを破棄します

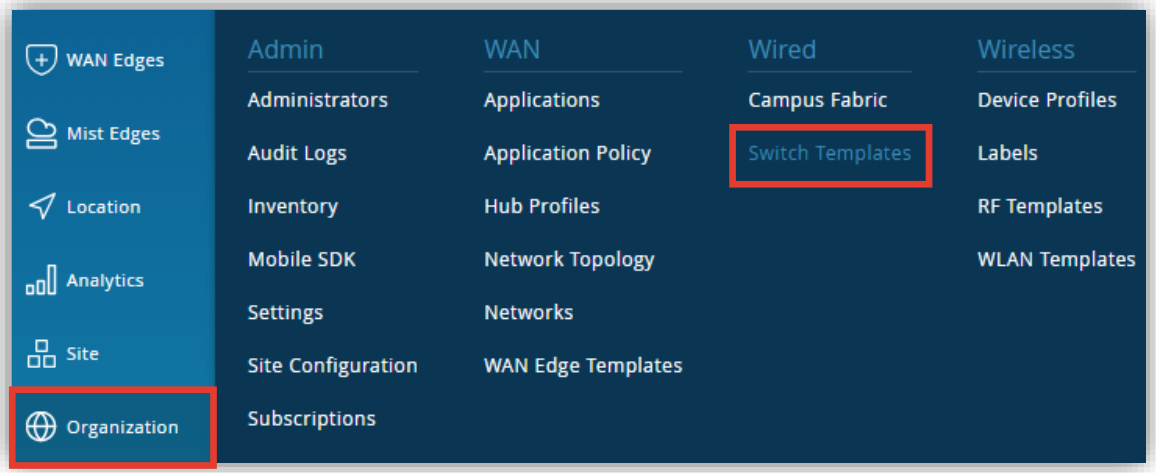
IP Source Guard

IP Source Guard は、スイッチ上の Untrusted Port に接続されたホストから送信された各パケットを検査し、DHCP Snooping DB に格納されているエントリーと照合します
パケットヘッダー(IP アドレス/MAC アドレス)が有効なエントリーと一致しない場合、スイッチはパケットを転送せず破棄します

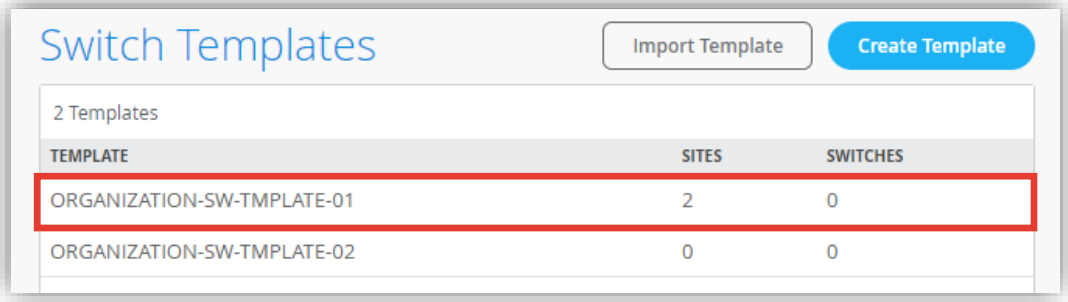
Organization レベルの DHCP Snooping の設定

テンプレートを使用し全てのスイッチに一括で設定を変更する場合

1. [Organization] から [Switch Templates] を選択します



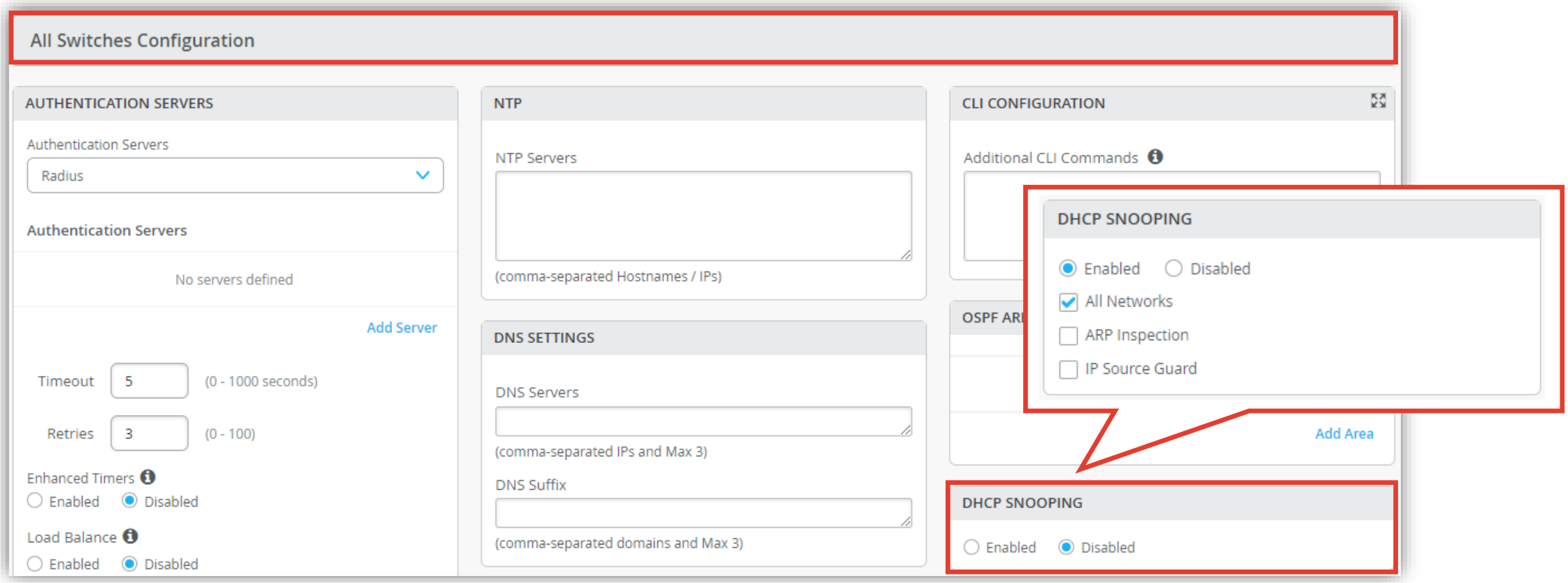
2. 編集対象の [Switch Template] を選択します



Organization レベルの DHCP Snooping の設定

テンプレートを使用し全てのスイッチに一括で設定を変更する場合

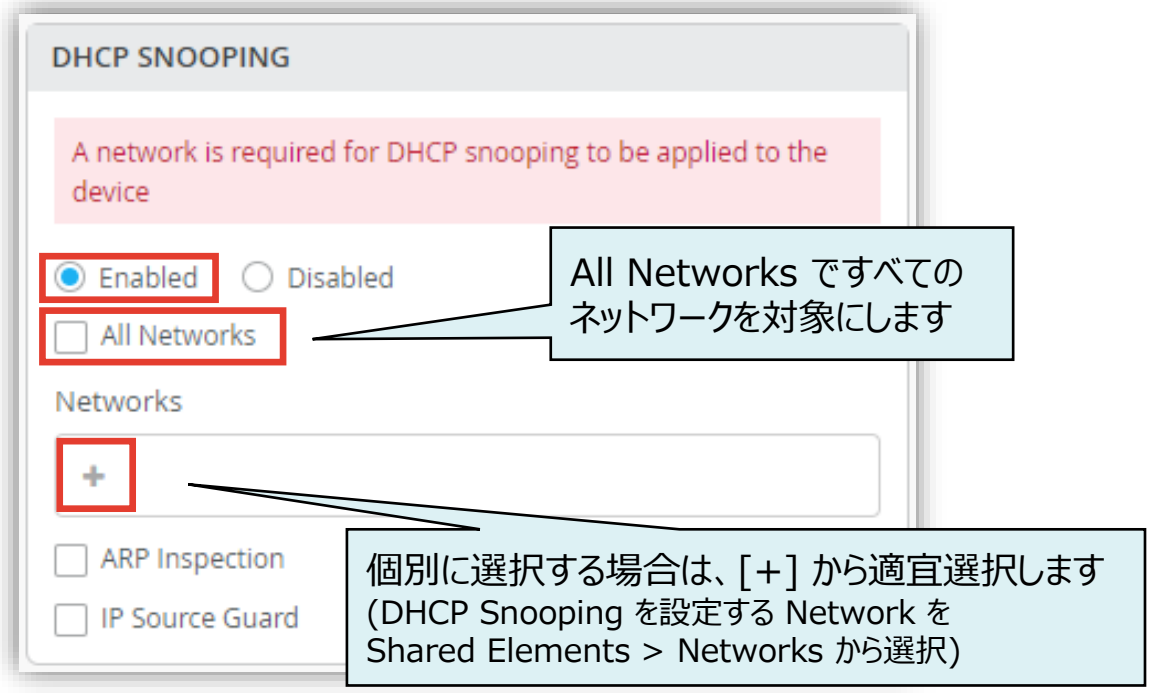
3. [All Switches Configuration] 内の「DHCP SNOOPING」の項目にて設定、[Shared Elements] の [PORT PROFILES] で、[Untrusted Port]、もしくは、[Trusted Port] のいずれかを選択します



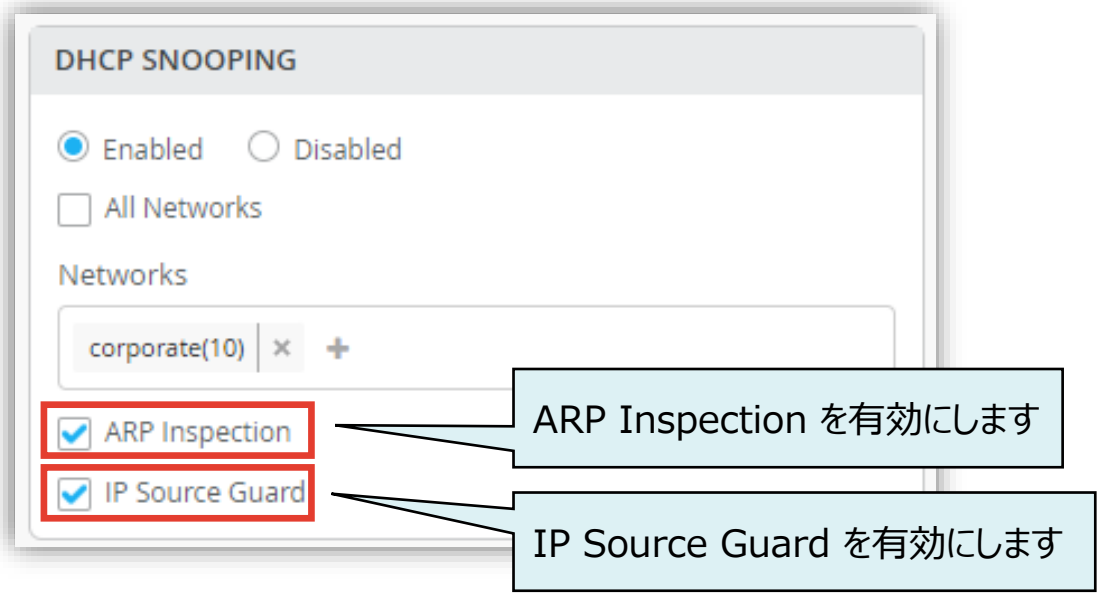
Organization レベルの DHCP Snooping の設定

テンプレートを使用し全てのスイッチに一括で設定を変更する場合

4. [Enabled] をクリックして、DHCP SNOOPING を で有効化し、対象となるネットワークを指定します



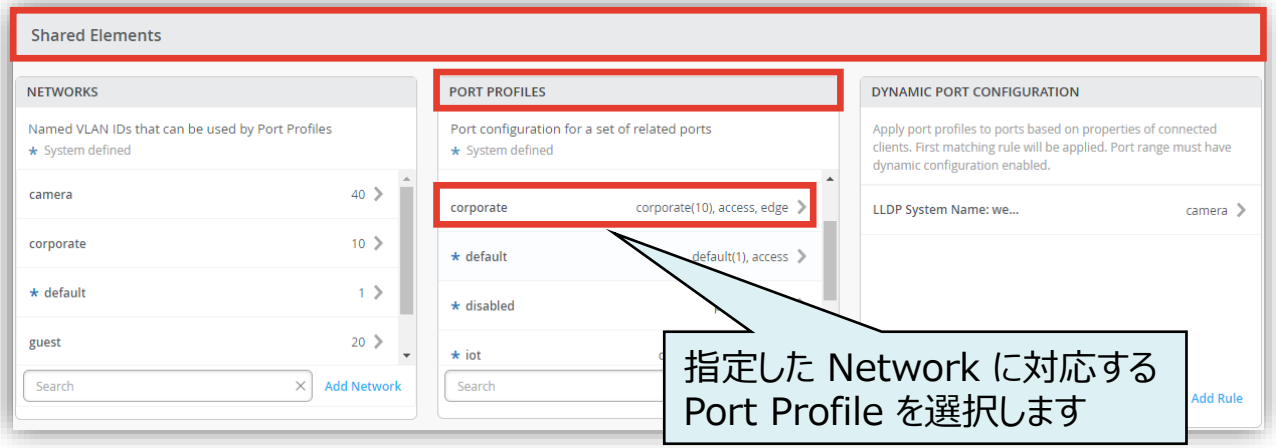
5. [ARP Inspection]、[IP Source Guard] を有効にする場合はそれぞれチェックを入れます

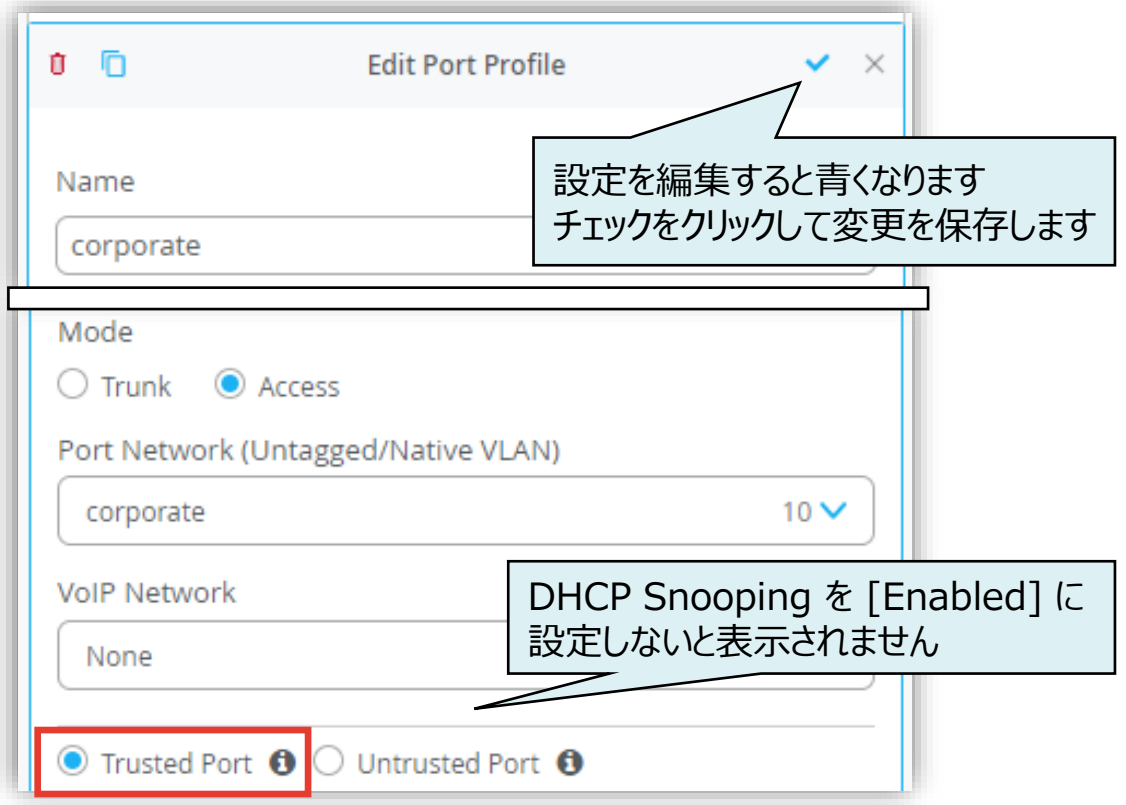


Organization レベルの DHCP Snooping の設定

テンプレートを使用し全てのスイッチに一括で設定を変更する場合

6. 指定した Networks に対応する [Shared Elements] の [PORT PROFILES] で [Trusted Port]、[Untrusted Port] のいずれかを選択します





Note

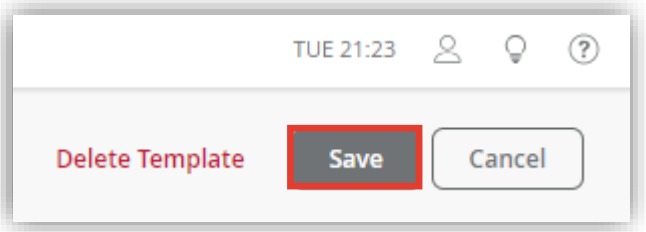
デフォルト設定のままで問題ない場合、この手順はスキップできます

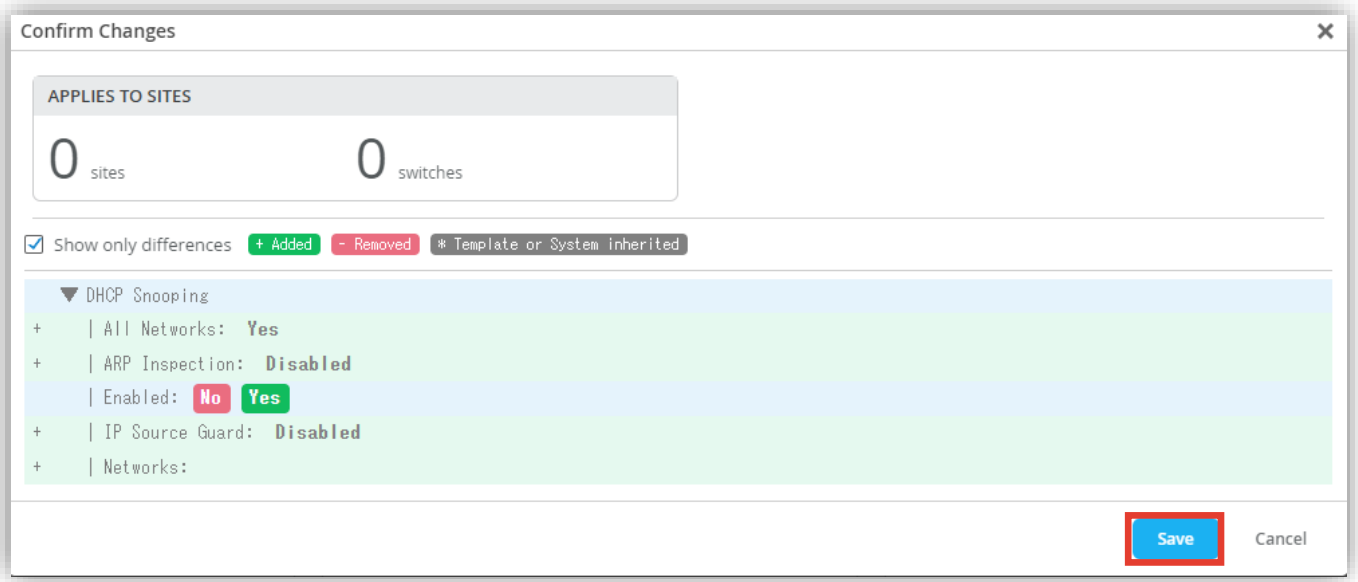
Mode	default
Trunk	Trusted Port
Access	Untrusted Port

Organization レベルの DHCP Snooping の設定

テンプレートを使用し全てのスイッチに一括で設定を変更する場合

7. テンプレートの編集が終了したら、[Save] をクリックします
   変更の差分が表示されるので、確認して再度 [Save] をクリックします

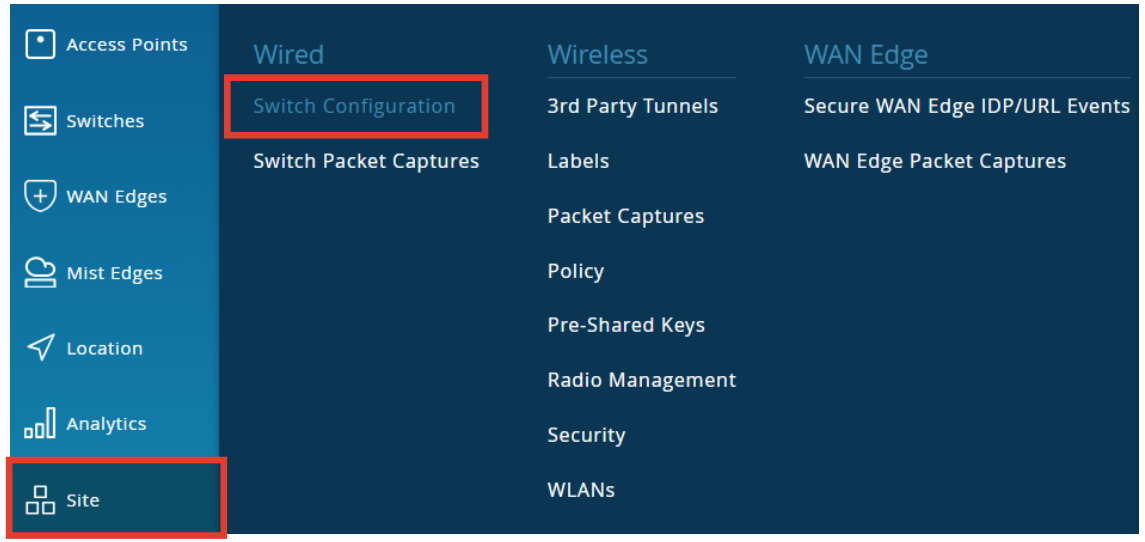




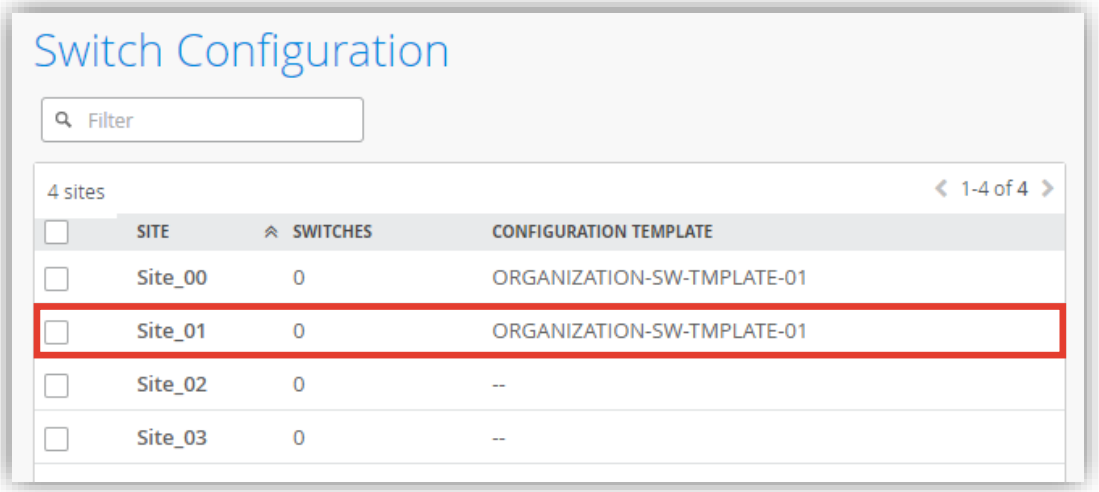
Site レベルの DHCP Snooping の設定

Site ごとに設定を変更する場合

1. [Site] から [Switch Configuration] を選択します



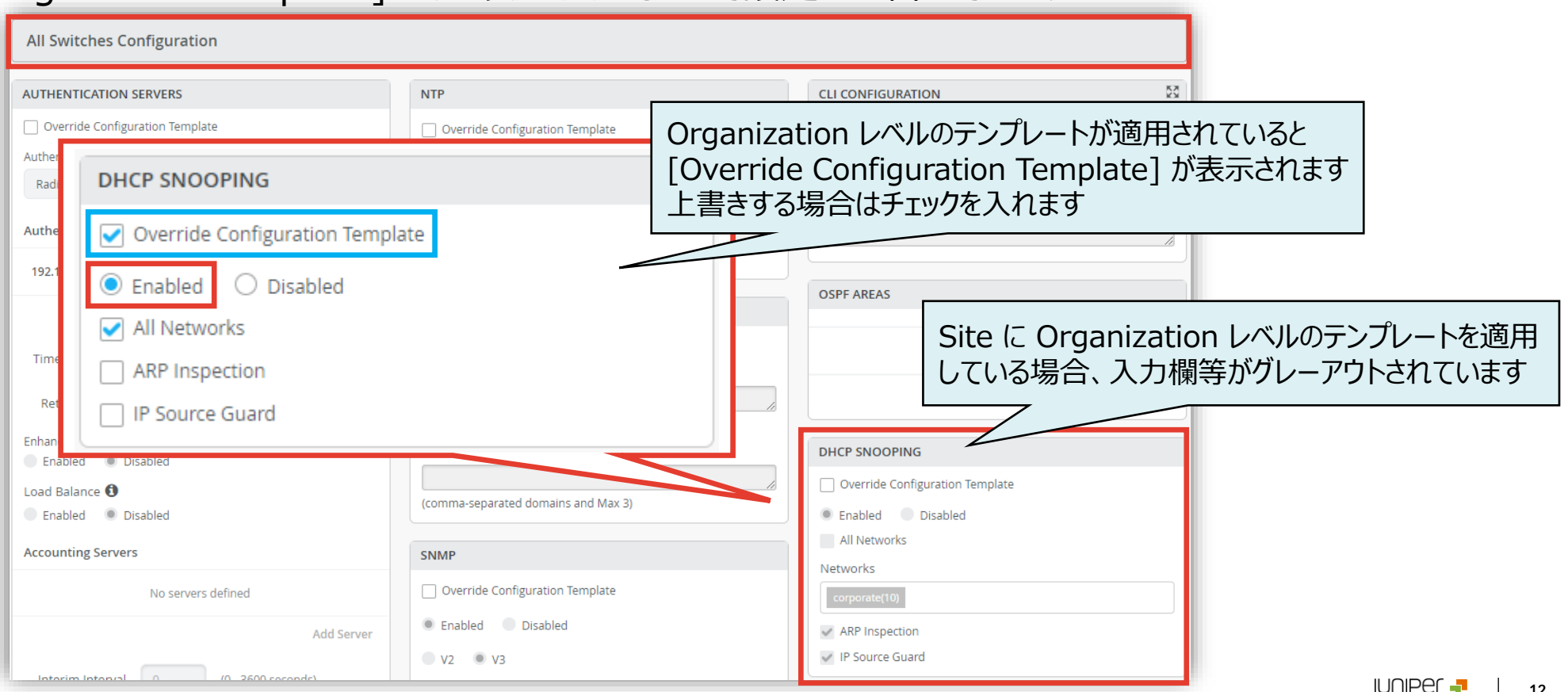
2. 編集対象の [Site] を選択します



Site レベルの DHCP Snooping の設定

Site ごとに設定を変更する場合

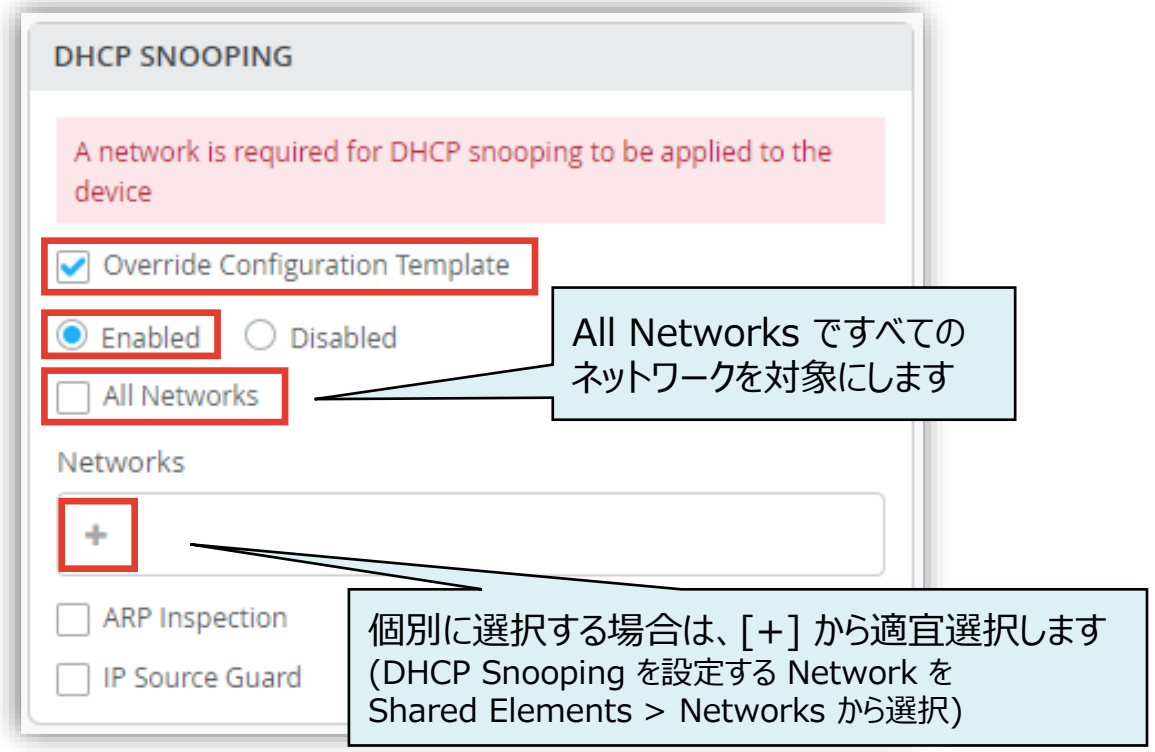
3. [All Switches Configuration] の「DHCP SNOOPING」で [Enabled] をクリックし設定を有効化、[Shared Elements] の [PORT PROFILES] で、[Untrusted Port]、もしくは、[Trusted Port] のいずれかを選択します
   Organization レベルのテンプレート(Organization > Switch Template)を Site に適用している場合、[Override Configuration Template] にチェックを入れることで設定を上書きできます



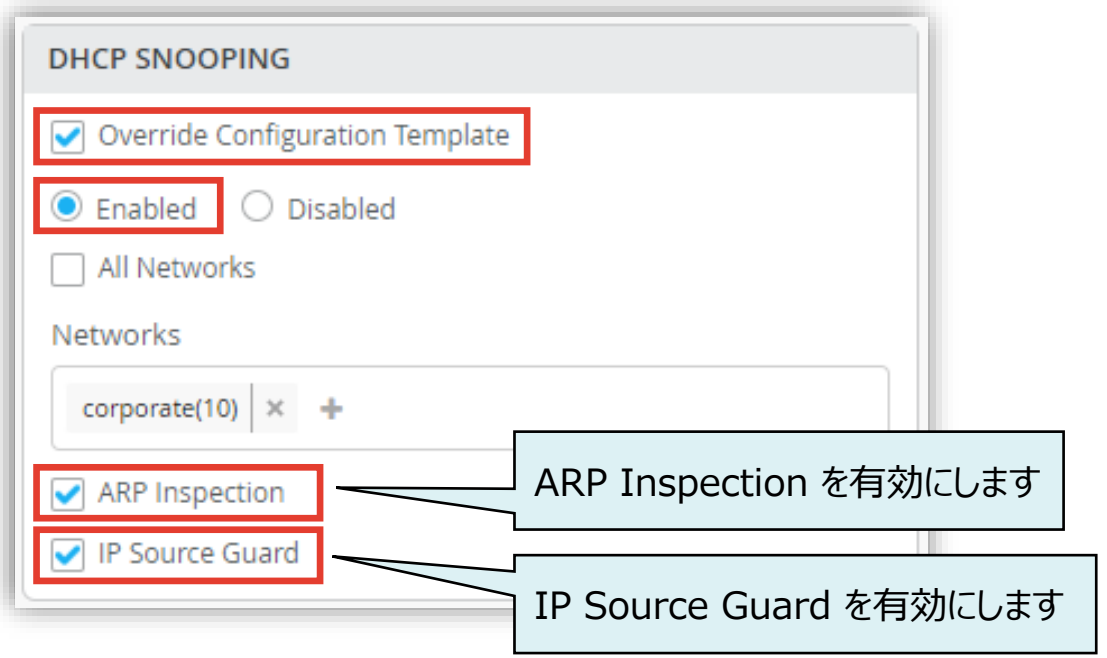
Site レベルの DHCP Snooping の設定

Site ごとに設定を変更する場合

4. [Enabled] をクリックして、DHCP SNOOPING を で有効化し、対象となるネットワークを指定します



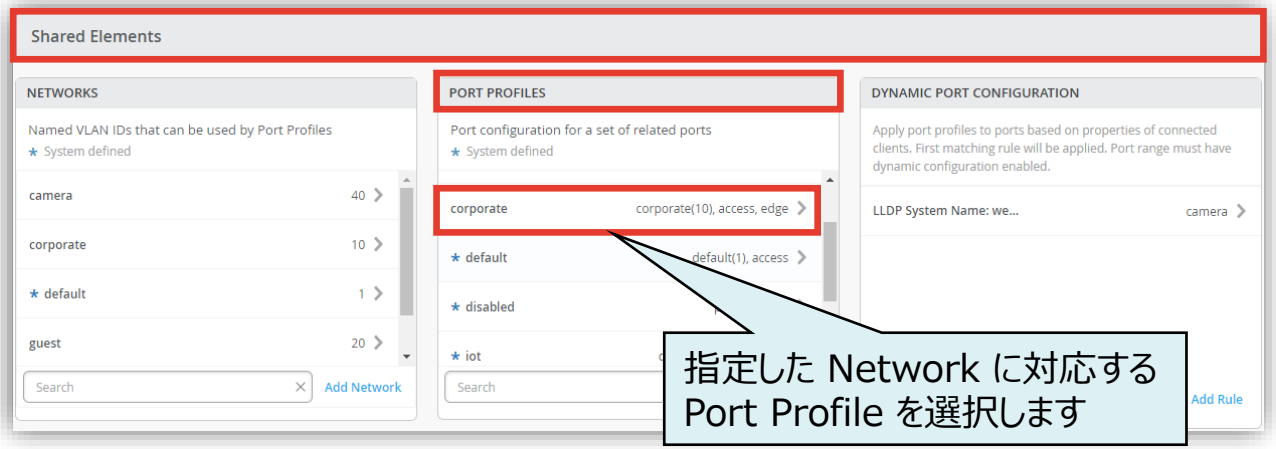
5. [ARP Inspection]、[IP Source Guard] を有効にする場合はそれぞれチェックを入れます

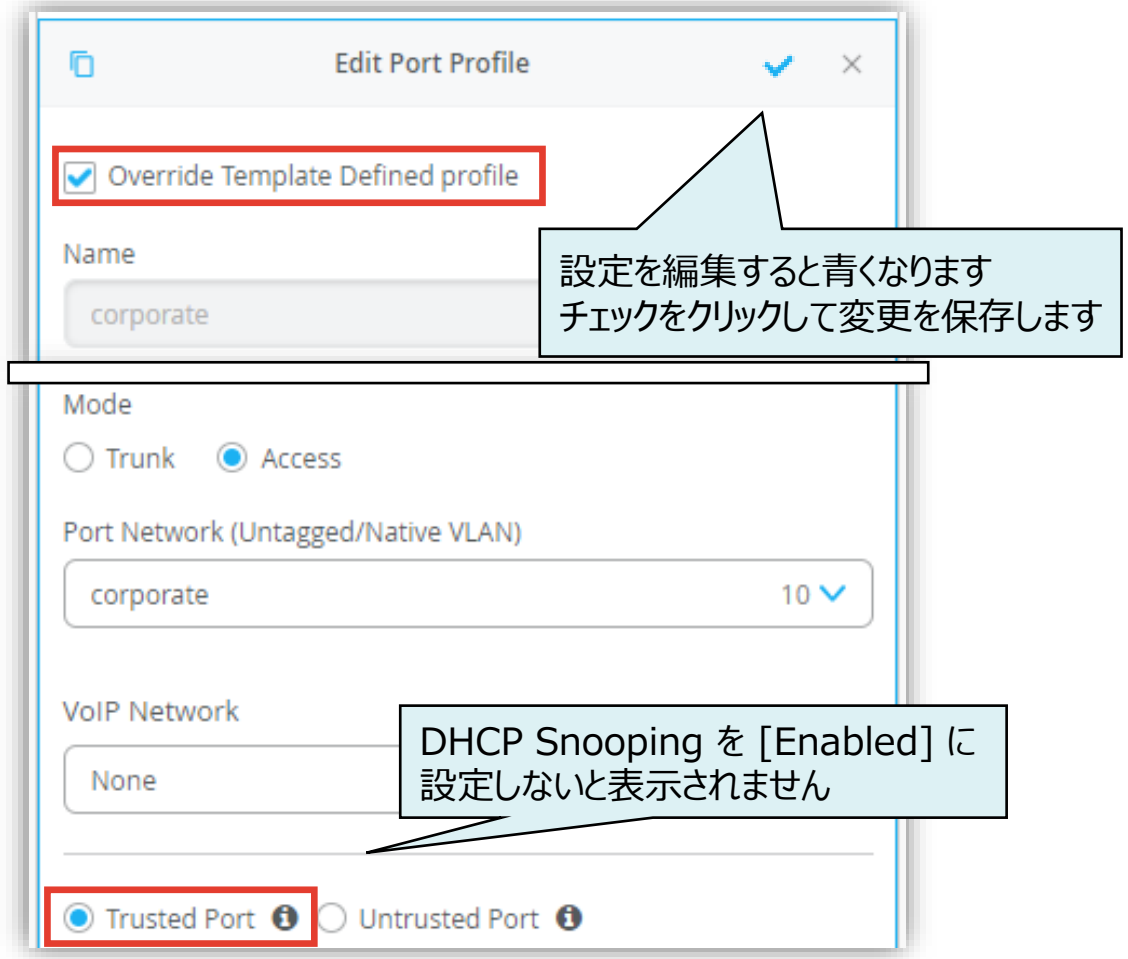


Site レベルの DHCP Snooping の設定

Site ごとに設定を変更する場合

6. 指定した Networks に対応する [Shared Elements] の [PORT PROFILES] で [Trusted Port]、[Untrusted Port] のいずれかを選択します





Note

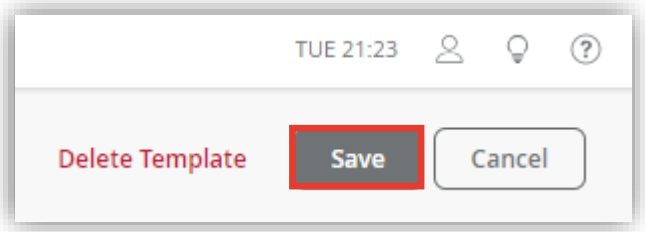
デフォルト設定のままで問題ない場合、この手順はスキップできます

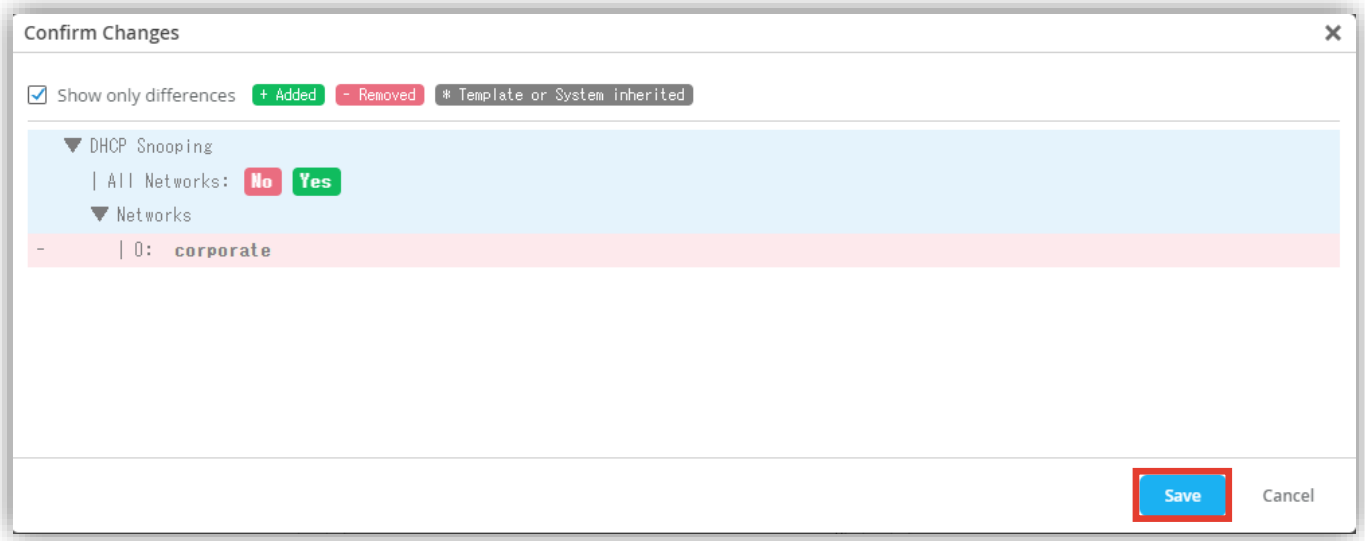
Mode	default
Trunk	Trusted Port
Access	Untrusted Port

Site レベルの DHCP Snooping の設定

Site ごとに設定を変更する場合

7. テンプレートの編集が終了したら、[Save] をクリックします
   変更の差分が表示されるので、確認して再度 [Save] をクリックします

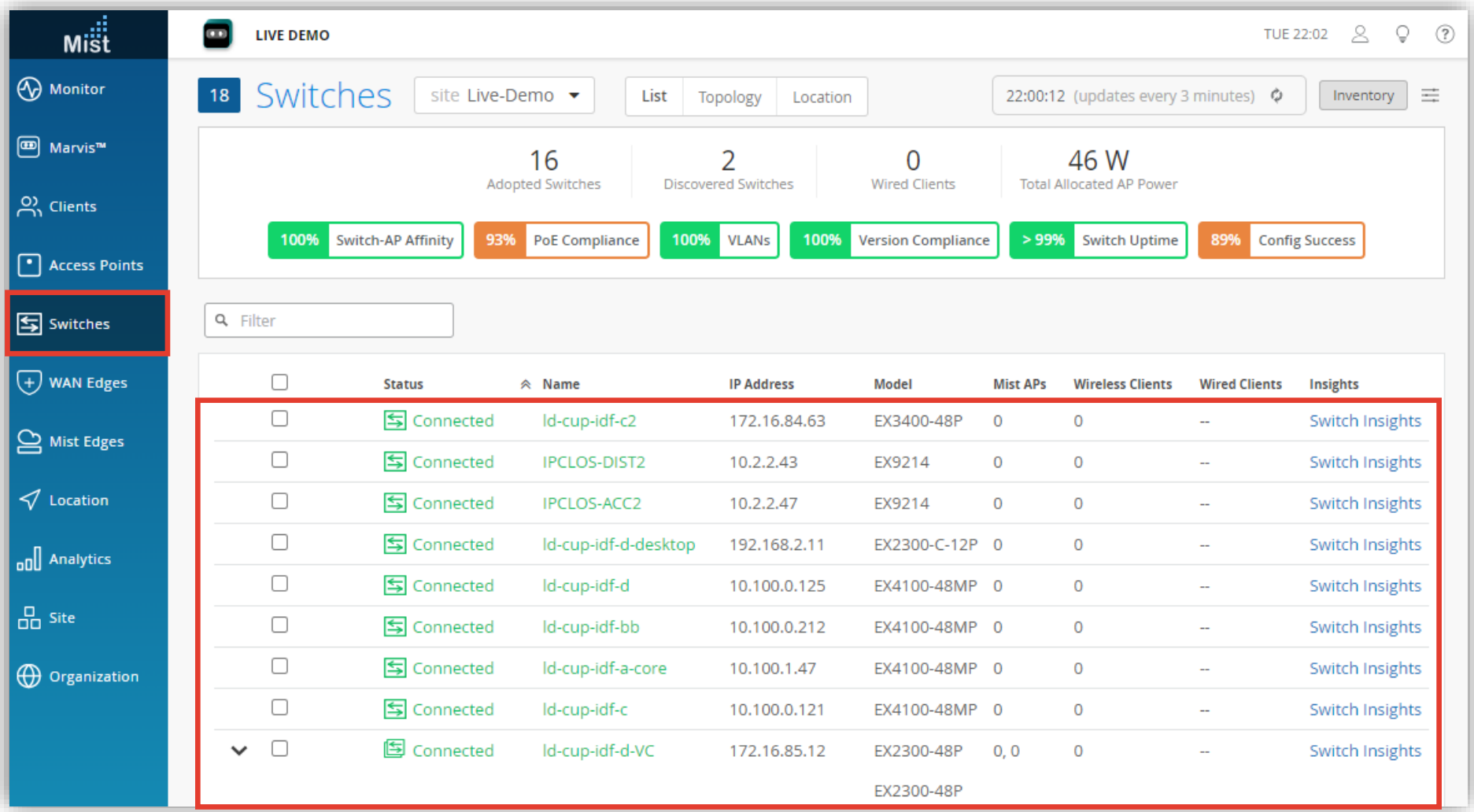




スイッチ単位の DHCP Snooping の設定

スイッチごとに設定を変更する場合

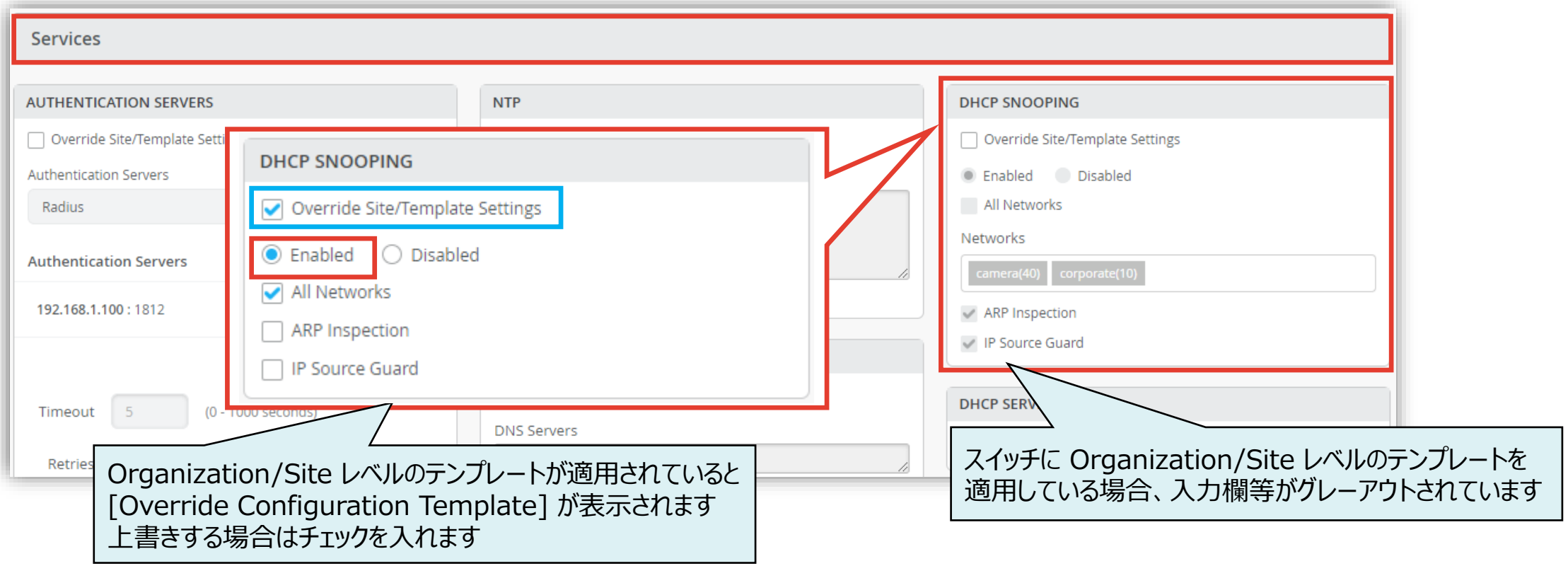
1. 各スイッチごとに設定を変更する場合、[Switches] を選択し、一覧から [EX/QFXスイッチ] をクリックします



スイッチ単位の DHCP Snooping の設定

スイッチごとに設定を変更する場合

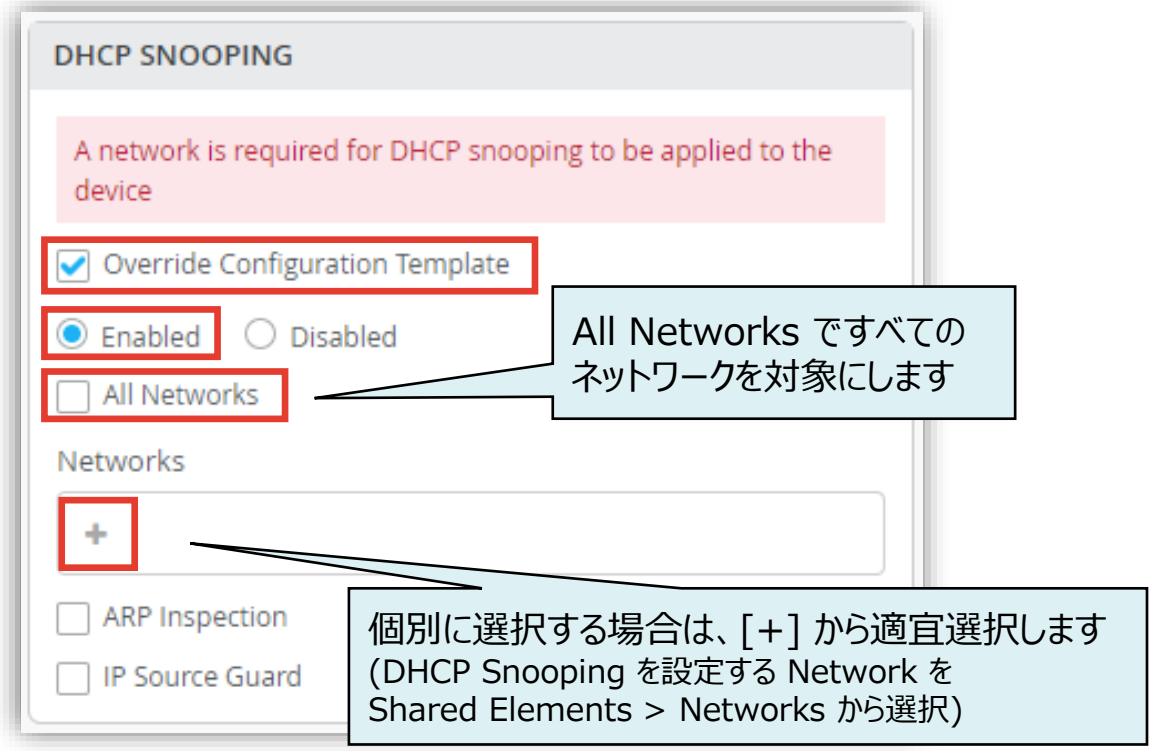
2. [Services] の「DHCP SNOOPING」で [Enabled] をクリックし設定を有効化、[Shared Elements] の [PORT PROFILES] で、[Untrusted Port]、もしくは、[Trusted Port] のいずれかを選択します
   Organization/Site レベルのテンプレート(Organization > Switch Template/Site > Switch Configuration)をスイッチに適用している場合、[Override Configuration Template] にチェックを入れることで設定を上書きできます



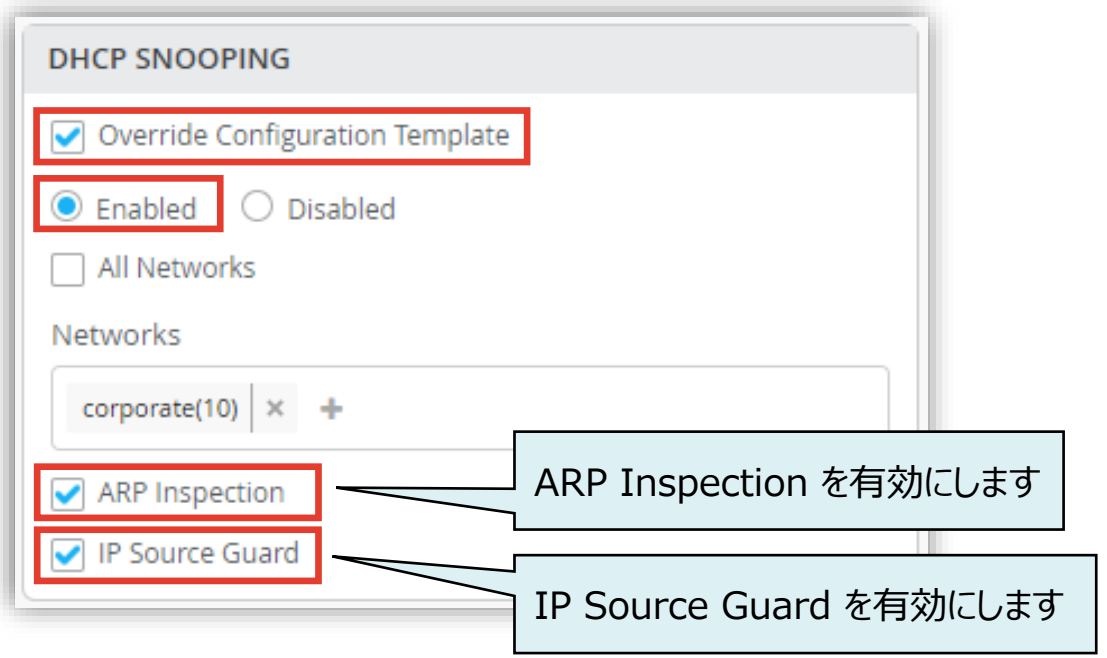
スイッチ単位の DHCP Snooping の設定

スイッチごとに設定を変更する場合

3. [Enabled] をクリックして、DHCP SNOOPING を で有効化し、対象となるネットワークを指定します



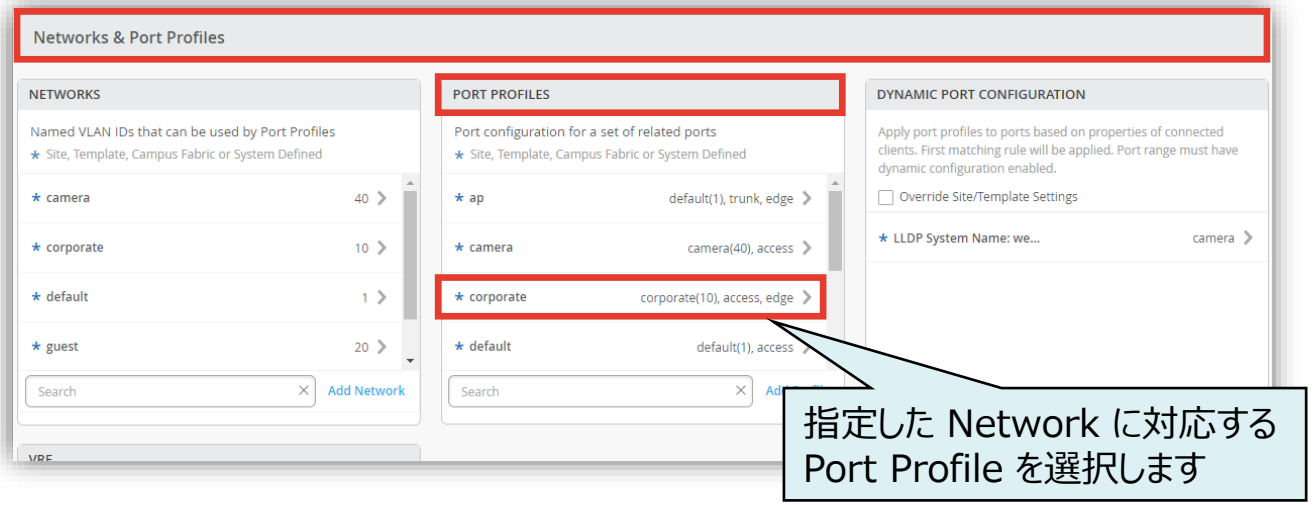
4. [ARP Inspection]、[IP Source Guard] を有効にする場合はそれぞれチェックを入れます

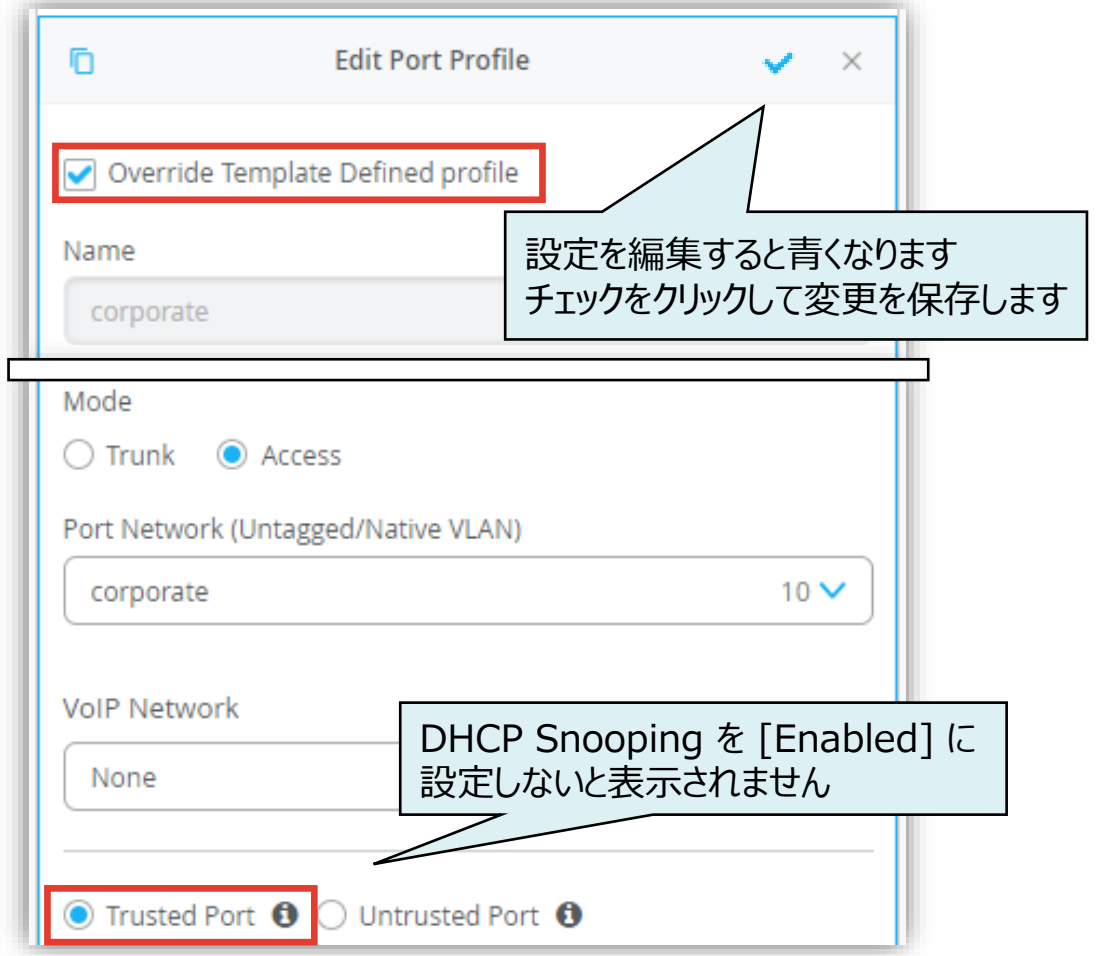


スイッチ単位の DHCP Snooping の設定

スイッチごとに設定を変更する場合

5. 指定した Networks に対応する [Networks & Profiles] の [PORT PROFILES] で [Trusted Port]、[Untrusted Port] のいずれかを選択します





Note

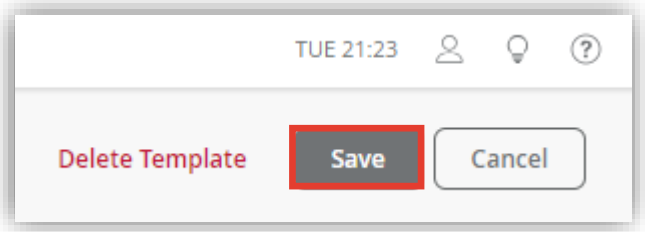
デフォルト設定のままで問題ない場合、この手順はスキップできます

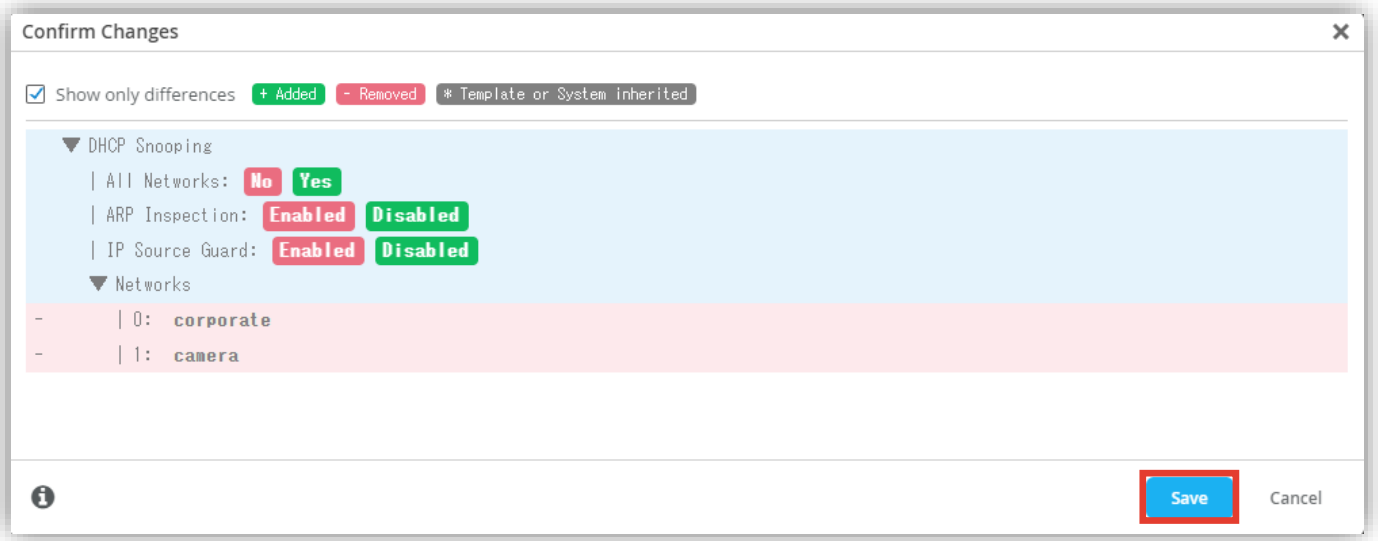
Mode	default
Trunk	Trusted Port
Access	Untrusted Port

スイッチ単位の DHCP Snooping の設定

スイッチごとに設定を変更する場合

6. テンプレートの編集が終了したら、[Save] をクリックします
   変更の差分が表示されるので、確認して再度 [Save] をクリックします





Thank you