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





- ◆ 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 <u>https://www.mist.com/documentation/</u>
- ◆ 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 <u>https://www.juniper.net/jp/ja/local/solution-technical-information/mist.html</u>
- ☆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



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



- DHCP クライアントが DHCP DISCOVER/DHCP REQUEST を送信
 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



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

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

| + WAN Edges | Admin | WAN | Wired | Wireless |
|--------------------------|--------------------|--------------------|------------------|-----------------|
| | Administrators | Applications | Campus Fabric | Device Profiles |
| Mist Edges | Audit Logs | Application Policy | Switch Templates | Labels |
| 🗸 Location | Inventory | Hub Profiles | | RF Templates |
| | Mobile SDK | Network Topology | WLAN Templates | |
| | Settings | Networks | | |
| G Site | Site Configuration | WAN Edge Templates | | |
| \bigoplus Organization | Subscriptions | | | |

2. 編集対象の [Switch Template] を選択します

| Switch Templates | Import Template | Create Template |
|----------------------------|-----------------|-----------------|
| 2 Templates | | |
| TEMPLATE | SITES | SWITCHES |
| ORGANIZATION-SW-TMPLATE-01 | 2 | 0 |
| ORGANIZATION-SW-TMPLATE-02 | 0 | 0 |
| | | |

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

| AUTHENTICATION SERVERS | NTP | CLI CONFIGURATION | |
|---|-------------------------------------|---------------------------|--|
| Authentication Servers | NTP Servers | Additional CLI Commands 🚯 | |
| Authentication Servers | | DHCP SNOOPING | |
| No servers defined | (comma-separated Hostnames / IPs) | Enabled Oisabled | |
| Add Server | DNS SETTINGS | OSPF ARI | |
| Timeout 5 (0 - 1000 seconds) | DNS Servers | IP Source Guard | |
| Retries 3 (0 - 100) | (comma-separated IPs and Max 3) | Add Area | |
| Enhanced Timers 🚺 🔵 Enabled 💿 Disabled | DNS Suffix | DHCP SNOOPING | |
| Load Balance 🕄 | (comma-separated domains and Max 3) | C Enabled O Disabled | |

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

| DHCP SNOOPING | | | | | |
|--|--|--|--|--|--|
| A network is required for DHCP snooping to be applied to the device | | | | | |
| Enabled O Disabled All Networks ですべての ネットワークを対象にします | | | | | |
| Networks | | | | | |
| + | | | | | |
| ARP Inspection IP Source Guard IP Source Guard CDHCP Snooping を設定する Network を Shared Elements > Networks から選択) | | | | | |

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

| DHCP SNOOPING | |
|--------------------|-------------------------|
| Enabled O Disabled | |
| All Networks | |
| Networks | |
| corporate(10) × + | |
| ARP Inspection | ARP Inspection を有効にします |
| IP Source Guard | IP Source Guard を有効にします |

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

| Shared Elements | | | | - 11 | |
|---|---|---|-------------------------------------|---|--|
| NETWORKS | PORT PROFILES | DYNAMIC PORT CONFIGURATION | | Edit Port Pi | rofile × × |
| Named VLAN IDs that can be used by Port Profiles * System defined camera 40 > | Port configuration for a set of related ports * System defined | Apply port profiles to ports based on properties of connected clients. First matching rule will be applied. Port range must have dynamic configuration enabled. | Name | | 設定を編集すると青くなります |
| corporate 10 > | torpurate torpurate(10), access, euge * default | LLUP System Name: we camera > | corpor | ate | チェックをクリックして変更を保存します |
| * default 1 > guest 20 > Search × Add Network | * disabled * iot Search Port Pro | Network に対応する file を選択します | Mode O Truni Port Ne corpo | k Access twork (Untagged/Native VI rate | AN) |
| 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 | VoIP Ne | twork | DHCP Snooping を [Enabled] に 設定しないと表示されません |
| | Mode default | | | | |
| | Trunk Trusted Por | t | Trust | ted Port 🟮 🔿 Untrusted P | ort 🚯 |
| | Access Untrusted Pc | rt | | | |

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

| | TUE 21:23 | 2 | Ģ | ? |
|-----------------|-----------|---|-------|---|
| Delete Template | Save | C | ancel | |

| | rm Changes | |
|------|---|--|
| AP | PLIES TO SITES | |
| C | | |
| _ | SIKS SWICHES | |
| 🖌 Sh | now only differences 🕂 Added 🗧 Removed 🔹 Template or System inherited | |
| | ▼ DHCP Snooping | |
| + | All Networks: Yes | |
| + | ARP Inspection: Disabled | |
| | Enabled: No Yes | |
| + | IP Source Guard: Disabled | |
| | | |

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

| Wired | Wireless | WAN Edge |
|------------------------|---|---|
| Switch Configuration | 3rd Party Tunnels | Secure WAN Edge IDP/URL Events |
| Switch Packet Captures | Labels | WAN Edge Packet Captures |
| | Packet Captures | |
| | Policy | |
| | Pre-Shared Keys | |
| | Radio Management | |
| | Security | |
| | WLANs | |
| | Wired Switch Configuration Switch Packet Captures | WiredWirelessSwitch Configuration3rd Party TunnelsSwitch Packet CapturesLabelsPacket CapturesPolicyPre-Shared KeysRadio ManagementSecurityWLANs |

| Swit | ch Cor | nfiguration |) | |
|---------|---------|-------------|----------------------------|--------------|
| 4 sites | | | | < 1-4 of 4 > |
| | SITE | | CONFIGURATION TEMPLATE | |
| | Site_00 | 0 | ORGANIZATION-SW-TMPLATE-01 | |
| | Site_01 | 0 | ORGANIZATION-SW-TMPLATE-01 | |
| | Site_02 | 0 | | |
| | Site_03 | 0 | | |
| | | | | |

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

| All Switches Configuration | | |
|---|--|--|
| AUTHENTICATION SERVERS | NTP | CLI CONFIGURATION 53 |
| Override Configuration Template Auther Rad DHCP SNOOPING Author | Override Configuration Template | Organization レベルのテンプレートが適用されていると [Override Configuration Template] が表示されます 上書きする場合はチェックを入れます |
| 192.1 Enabled Disabled All Networks Time ARP Inspection Ret IP Source Guard Enhan IP Source Guard | ale | OSPF AREAS Site に Organization レベルのテンプレートを適用 している場合、入力欄等がグレーアウトされています |
| Enabled Disabled Load Balance Disabled Enabled Disabled | (comma-separated domains and Max 3) | Override Configuration Template Enabled Insabled All Networks |
| No servers defined Add Server | Override Configuration Template Enabled Disabled | Networks Corporate(10) ARP Inspection |
| lataria lataryal 0 (0 2600 seconds) | ● V2 ● V3 | |

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

| DHCP SNOOPING | | | | | | | |
|--|--------------|--|--|--|--|--|--|
| A network is required for DHCP snooping to be applied to the device | | | | | | | |
| Override Configurat | ion Template | | | | | | |
| Enabled Disabled All Networks ですべての ネットワークを対象にします | | | | | | | |
| Networks | | | | | | | |
| + | | | | | | | |
| ARP Inspection IP Source Guard IP | | | | | | | |

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

| DHCP SNOOPING |
|---|
| Override Configuration Template |
| Enabled O Disabled |
| All Networks |
| Networks |
| corporate(10) × + |
| ▲ ARP Inspection を有効にします |
| IP Source Guard IP Source Guard を有効にします |

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

| NETWORKS | | PORT PROFILES | | DYNAMIC PORT CONFIGURATION | | |
|--|---------------------|--|-------------------------------|---|--|-------------------------------|
| Named VLAN IDs that can be us * System defined | ed by Port Profiles | Port configuration * System defined | for a set of related ports | Apply port profiles to ports based on pr clients. First matching rule will be applie dynamic configuration enabled. | roperties of connected ed. Port range must have | Override Template Defined p |
| amera | 40 > | corporate | corporate(10), access, edge 义 | LLDP System Name: we | camera 📏 | Name |
| orporate | 10 📏 | * default | default(1), access 👌 | | | corporate |
| r default | 1 > | * disabled | | | | corporate |
| guest | 20 🔪 🗸 | * iot | 指定した N | etwork に対応 | する | Mode |
| Search | × Add Network | Search | Port Profi | le を選択します | Add Rule | O Trunk Access |
| | | | | | | |
| | | | | | | Port Network (Untagged/Native |
| Mate | | | | | | corporate |
| 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 📗 | |
| | | Modo | dofault | | | VoIP Network |
| | | mode | derault | | | None IV |
| | | Trunk | Trusted Port | | | |
| | | IT GITIX | in doced i ore | | | |
| | | Access | Untrusted Por | t | | |

| Edit Edit | Port Profile | ~ | • × | | |
|--|---------------------|------------------------|---------------|-------------|-----|
| Override Template Defin | ned profile | | | | |
| Name corporate | 設 つ チェ | ー 官を編集する ックをクリック | ると青くな して変更 | ります 夏を保存 | します |
| Mode Trunk Occess Port Network (Untagged/Na corporate | itive VLAN) | | 10 🗸 | | |
| VoIP Network None | DHCP Snoo 設定しないと | oping を [l 表示されまt | Enabled せん | d] (こ | |
| ● Trusted Port 1 ○ Un | trusted Port 🕚 | | JUU | | 14 |

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

| | TUE 21:23 | 2 | Ŷ | ? |
|-----------------|-----------|---|-------|---|
| Delete Template | Save | C | ancel | |

| Confirm Changes | |
|--|--------|
| 🗹 Show only differences 🕂 Added 🗧 Removed 🗱 Template or System inherited) | |
| V DHCP Snooping | |
| All Networks: No Yes | |
| 🔻 Networks | |
| - D: corporate | |
| | |
| | |
| | |
| | |
| | |
| | |
| Save | Cancel |



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

| Mist | DIVE DEMO | | | | | | | TUE | 22:02 <u>&</u> Ç |
|-----------------|----------------------|----------------------|----------------------|-----------------|--------------------|----------|--------------------|---------------|----------------------|
| Monitor | ¹⁸ Switch | es site Live-De | emo 🔻 List To | pology Location | | 22:00:12 | 2 (updates every 3 | 3 minutes) 🗳 | Inventory |
| ⊞ Marvis™ | | | 16 | 2 | 0 | | 46 W | | |
| Clients | | Adop | ted Switches Discove | red Switches | Wired Clients | Total A | llocated AP Power | | |
| • Access Points | 100% Swi | itch-AP Affinity 93% | PoE Compliance 100% | VLANs 100% | Version Compliance | e > 99% | Switch Uptime | 89% Config | g Success |
| Switches | Q Filter | | | | | | | | |
| + WAN Edges | | Status | ∧ Name ∧ | IP Address | Model | Mist APs | Wireless Clients | Wired Clients | Insights |
| | | 🗲 Connected | ld-cup-idf-c2 | 172.16.84.63 | EX3400-48P | 0 | 0 | | Switch Insights |
| | | S Connected | IPCLOS-DIST2 | 10.2.2.43 | EX9214 | 0 | 0 | | Switch Insights |
| ✓ Location | | 🗲 Connected | IPCLOS-ACC2 | 10.2.2.47 | EX9214 | 0 | 0 | | Switch Insights |
| | | S Connected | ld-cup-idf-d-desktop | 192.168.2.11 | EX2300-C-12P | 0 | 0 | | Switch Insights |
| | | S Connected | ld-cup-idf-d | 10.100.0.125 | EX4100-48MP | 0 | 0 | | Switch Insights |
| G Site | | S Connected | ld-cup-idf-bb | 10.100.0.212 | EX4100-48MP | 0 | 0 | | Switch Insights |
| Organization | | S Connected | ld-cup-idf-a-core | 10.100.1.47 | EX4100-48MP | 0 | 0 | | Switch Insights |
| | | S Connected | ld-cup-idf-c | 10.100.0.121 | EX4100-48MP | 0 | 0 | | Switch Insights |
| | ✓ □ | 😫 Connected | ld-cup-idf-d-VC | 172.16.85.12 | EX2300-48P | 0, 0 | 0 | | Switch Insights |
| | | | | | EX2300-48P | | | | |

16

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

| Services | | |
|---|--|---|
| AUTHENTICATION SERVERS | NTP | DHCP SNOOPING |
| Override Site/Template Sett Authentication Servers Radius Authentication Servers 192.168.1.100 : 1812 Timeout 5 (0 | DHCP SNOOPING Override Site/Template Settings Enabled Disabled All Networks ARP Inspection IP Source Guard | Override Site/Template Settings Enabled Disabled All Networks Carnera(40) corporate(10) ARP Inspection IP Source Guard |
| Retries Organiza [Override 上書きする | tion/Site レベルのテンプレートが適用されていると e Configuration Template] が表示されます 場合はチェックを入れます | スイッチに Organization/Site レベルのテンプレートな 適用している場合、入力欄等がグレーアウトされていま |

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

| DHCP SNOOPING | | | |
|---------------------------------|------------------------------------|--|-----------------------|
| A network is required to device | for DHCP snoop | ing to be applied to the | |
| ✓ Override Configurat | ion Template | | |
| Enabled O Disal | bled | All Networks ですべてな ネットワークを対象にします | D - |
| Networks | | | |
| + | | | |
| ARP Inspection | 個別に選択 (DHCP Snoo Shared Eler | する場合は、[+] から適宜 oping を設定する Network を ments > Networks から選択 | 選択します ^注 |

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

| DHCP SNOOPING |
|---|
| Override Configuration Template |
| Enabled Disabled |
| All Networks |
| Networks |
| corporate(10) × + |
| ARP Inspection ARP Inspection を有効にします |
| IP Source Guard を有効にします |

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

| Networks & Port Profiles | | | Edit Port Pr | ofile 🗸 🗙 |
|---|---|---|---|---|
| NETWORKS Named VLAN IDs that can be used by Port Profiles * Site, Template, Campus Fabric or System Defined | PORT PROFILES Port configuration for a set of related ports * Site, Template, Campus Fabric or System Defined | DYNAMIC PORT CONFIGURATION Apply port profiles to ports based on properties of connected clients. First matching rule will be applied. Port range must have | Override Template Defined pro | ofile |
| * camera 40 > * corporate 10 > | * ap default(1), trunk, edge > * camera camera(40), access > | dynamic configuration enabled. Override Site/Template Settings * LLDP System Name: we camera > | Name | 設定を編集すると青くなります チェックをクリックして変更を保存します |
| search Xet | * default default(1), access Search × Ad 指行 | 定した Network に対応する rt Profile を選択します | Mode Trunk Access Port Network (Untagged/Native VL | AN) |
| Note デフォルト設定のままで へ A | で問題ない場合、この <mark>Mode default</mark> Trunk Trusted Port Access Untrusted Port | 手順はスキップできます t | Corporate VoIP Network None ① Trusted Port ① ○ Untrusted | 10 ▼ CP Snooping を [Enabled] に としないと表示されません |

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

| | TUE 21:23 | 2 | Ģ | ? |
|-----------------|-----------|---|-------|---|
| Delete Template | Save | C | ancel | |

| Confirm Changes | | |
|--|------|-------|
| Show only differences 🕂 Added 💽 Removed 🚺 🛪 Template or System inherited | | |
| ▼ DHCP Snooping | | |
| All Networks: No Yes | | |
| ARP Inspection: Enabled Disabled | | |
| IP Source Guard: Enabled Disabled | | |
| ▼ Networks | | |
| - D: corporate | | |
| - 1: camera | | |
| | | |
| | | |
| | | |
| 9 | Save | Cance |
| - | | |

Thank you

