AlaxalA

The Guaranteed Network
いちばん近くで、もっと先へ。

AX シリーズ

ホワイトリスト機能 活用ガイド
《運用編》

初版

資料 No. NTS-16-R-002

アラクサラネットワークス株式会社

はじめに

本資料は、アラクサラのホワイトリスト機能の運用に役立てるものとして 運用・保守の操作方法などについて理解を深めてもらうことを目的としています。ホワイトリスト機能を利用される機器の運用および保守する際に、製品マニュアルを補足する技術資料として、ご活用ください。

関連資料

- AX シリーズ製品マニュアル
  （http://www.alaxala.com/jp/techinfo/manual/index.html）
  AX2500S シリーズ
  《ソフトウェアマニュアル》
  ・コンフィグレーションガイド Vol.2
  ・コンフィグレーションコマンドレファレンス
  ・運用コマンドレファレンス
  AX260A シリーズ
  《ソフトウェアマニュアル》
  ・コンフィグレーションガイド Vol.2
  ・コンフィグレーションコマンドレファレンス
  ・運用コマンドレファレンス

- AX シリーズ ホワイトリスト機能活用ガイド [導入編]
  (http://www.alaxala.com/jp/techinfo/guide/index.html#13)

本資料使用上の注意事項

本資料に記載の内容は、弊社が特定の環境において基本動作を確認したものであり、機能・性能・信頼性についてあらゆる環境条件すべてにおいて保証するものではありません。また製品マニュアルの補助資料としてご利用いただけますようお願いいたします。

なお本資料作成時の OS ソフトウェアバージョンは特記の無い限り以下となっております。

AX2500S	Ver. 4.4
AX260A	Ver. 4.4

本資料の内容は、改良のため予告なく変更する場合があります。

輸出時の注意

本製品を輸出される場合には、外国為替及び外国貿易法の規制並びに米国輸出管理規制など外国の輸出関連法規をご確認の上、必要な手続きをおとりください。

なお、不明な場合は、弊社担当営業にお問い合わせ下さい。

商標一覧

- アラクサラの名称およびロゴマークは、アラクサラネットワークス株式会社の商標および登録商標です。
- Ethernet は、富士ゼロックス株式会社の登録商標です。
- イーサネットは、富士ゼロックス株式会社の登録商標です。
- そのほかの記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

目次

1. ホワイトリスト機能の運用について 4

1.1 ホワイトリストの運用コマンド 4
1.2 運用で使うコンフィグレーション 6
1.3 ホワイトリストの追加 7
1.4 ホワイトリストの削除 9
1.5 コンフィグレーションの保存 10
1.6 コンフィグレーションのバックアップとリストア 10
1.7 運用における設定のポイント 12
1.8 未学習パケット情報を検知した場合の対処 13

2. ホワイトリスト機能の保守について 14

2.1 ホワイトリストスイッチの交換 14
2.2 端末の交換 17
2.3 端末の追加 18

1. ホワイトリスト機能の運用について

1.1 ホワイトリストの運用コマンド

ホワイトリスト機能に関する運用コマンドは以下に示すコマンドです。これらのコマンドはホワイトリスト機能の運用に必要となるコマンドです。

表 1-1 運用コマンド一覧

コマンド種別	コマンド	説明
表示コマンド	show white-list address [{port | channel-group-number}]	アドレスリスト情報を表示します。また統計情報を表示します。 登録したアドレスリストを確認する際に使用します。
	show white-list packet [{port | channel-group-number}]	パケットリスト情報を表示します。また統計情報を表示します。 登録したパケットリストを確認する際に使用します。
	show white-list miss-hit	ホワイトリストの運用状態で受信した未学習パケット情報を表示します。
クリア/削除コマンド	clear white-list statistics	show white-list address コマンド, show white-list packet コマンドで表示する統計情報をクリアします
	clear white-list miss-hit	ホワイトリストの運用状態で受信した未学習パケット情報をクリアします。
	erase white-list [{address|packet}] {all | port | channel-group-number}	ホワイトリストを全リスト/ポート単位/チャネル単位で選択し削除します。 オプションでリスト種類の指定ができます。
エントリタイマ機能	set white-list packet entry-timer source <ip address> expire <seconds>	パケットリストのエントリタイマ機能で 一時的に無効化するエントリを設定します。
	show white-list packet entry-timer	ホワイトパケットリストのエントリタイマ機能の設定状態を表示します。

以下に表示コマンドの表示例を示します。

◆ アドレスリスト情報 の表示例

```
# show white-list address

Date 20XX/08/06 20:56:18 UTC
White-list status : Applying
Total learning count : 4
Port change count : 0
Invalid mac address : 7536
Address list overflow : 0
Total inspected packets : 217027

Total entry / Max entry : 9 / 2000
Port     VLAN   MAC address
0/1      4000   0012.e2aa.0000
0/3      4000   0012.e2cc.0000
0/5      4000   0012.e2dd.0000
0/7      2048   0012.e2aa.0001
0/7      2048   0012.e2aa.0002
ChGr:64     1   0012.e202.0251
ChGr:64     1   0012.e202.0252
ChGr:64  4000   0012.e211.0000
ChGr:64  4000   0012.e222.0000

Total miss-hit packets : 304623
```

アドレスリストの統計情報 (全ポート合計)

学習済みのアドレスリスト数／最大エントリ数

アドレスリストの未学習パケット受信数

◆ パケットリスト情報 の表示例

```
# show white-list packet

Date 20XX/06/06 20:55:59 UTC
White-list status : Applying
Total learning count : 9
Port change count : 0
Invalid mac address : 7536
Invalid ip packets : 5889
Invalid arp packets : 7810
Unsupported packets : 0
Packet list overflow : 0
Total inspected packets : 205994

Total entry / Max entry : 19 / 32000
 Port   VLAN    Type                                                    Matched packets
 0/1    4000    arp smac=0012.e2aa.0000 sip=192.168.100.100                           0
 0/3    4000    other smac=0012.e2bb.0000 dmac=0000.ffff.0000                         0
 0/5    4000    ipv4 sip=192.168.254.101 dip=192.168.254.254                        156
 0/7    2048    ipv4 sip=192.168.254.102 dip=192.168.254.254                        156
 0/7    2048    ipv4 sip=192.168.254.103 dip=192.168.254.254                        156
ChGr:64    1   other smac=0012.e202.0251 dmac=0180.c200.0002                         0
ChGr:64    1   other smac=0012.e202.0251 dmac=0180.c200.000e                         0
ChGr:64 4000   other smac=0012.e202.0252 dmac=0180.c200.0002                         0
ChGr:64 4000   other smac=0012.e202.0252 dmac=0180.c200.000e                         0
Total miss-hit packets : 281885
```

パケットリストの統計情報 (全ポート合計)

学習済みのパケットリスト数／最大エントリ数

パケットリストに一致したパケット数

パケットリストの未学習パケット受信数

◆ 未学習パケット情報 の表示例

```
# show white-list miss-hit

Date 20XX/06/08 17:25:28 UTC
White-list status : Applying

Total entry / Max entry : 404 / 2000
  Port  VLAN    Last detection time   First detection time          Count
  0/1   2000    20XX/06/08 17:25:28   20XX/06/08 16:57:00           8308
   [a] mac=0012.e278.0007
  0/1   1000    20XX/06/08 17:25:28   20XX/06/08 16:57:03           8274
   [a] mac=0012.e234.0008
   [p] type=arp smac=0012.e234.0008 sip=192.168.254.108
  0/9   2000    20XX/06/08 17:25:28   20XX/06/08 16:57:01           8824
   [a] mac=0012.e278.000a
   [p] type=ipv4 sip=110.110.110.119 dip=120.120.120.129 proto=tcp sp=56806 dp
=61175
  0/10  400     20XX/06/08 17:25:28   20XX/06/08 16:57:00           9679
   [p] type=ipv4 sip=110.110.110.112 dip=120.120.120.122 proto=51 Unsupported
  0/3   1       20XX/06/08 16:15:20   20XX/06/08 16:15:18              3
   [a] mac=00eb.f009.0001
  0/5   1       20XX/06/08 16:15:19   20XX/06/08 16:15:19              1
   [a] mac=0012.e272.12ac
   [p] type=other smac=0012.e272.12ac dmac=0180.c200.0000
```

[a]だけ表示：アドレスリスト未学習パケット情報
[p]だけ表示：パケットリスト未学習パケット情報
[a][p]両方表示：アドレスリスト・パケットリスト両方での未学習パケット情報

1.2 運用で使うコンフィグレーション

ホワイトリスト機能の運用で使用するコンフィグレーションは以下のとおりです。手動で該当するホワイトリストエントリを追加したり削除したりする際に使用します

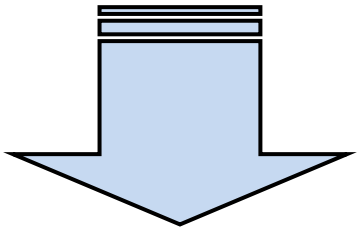
表 1-2 コンフィグレーションコマンド一覧

リスト種類	コマンド
アドレスリスト	white-list data "a <mac> v <vlan id> p <IF#>" white-list data "a <mac> v <vlan id> c <channel group>"
パケットリスト (IPv4)	white-list data "p <IF#> v <vlan id> ip <src ip><dest ip> [<protocol> [s <src port>] [d <dst port>]]" white-list data "c <channel group> v <vlan id> ip <src ip><dest ip> [<protocol>[s <src port>] [d <dst port>]]"
パケットリスト （ARP）	white-list data "p <IF#> v <vlan id> arp <src mac> <src ip>" white-list data "c <channel group> v <vlan id> arp <src mac> <src ip>"
パケットリスト （IPv4/ARP 以外）	white-list data "p <IF#> v <vlan id> <src mac> <dst mac>" white-list data "c <channel group> v <vlan id> <src mac> <dst mac>"

キーワード: a, p, c, v, ip, s, d, arp
設定値 :< >で表示しているパラメータ名

[注意事項]
1. ポート番号またはチャネルグループ番号が異なる場合は、当該エントリが上書きされます。
2. 下線部のシンタックスチェック、補完機能、ヘルプ機能は実施されません。
3. ダブルクォート内の書式は、上記のいずれかの形式で入力されることを前提とします。
4. キーワードや設定値の入力順が不正な場合は、装置に正しく反映されない場合があります。
5. キーワードを含む設定値はすべて小文字で入力してください。
6. キーワードと設定値の間はスペース1文字を入力してください。

気になる続きは…



・アラクサラ　インテグレータ会員

または

・ビジネスパートナー様会員

にご登録いただければ、全てをご覧いただけます！

アラクサラ インテグレータ会員またはビジネスパートナー様会員へ登録することで、アラクサラ製品のご利用にあたり役立つ各種資料(システム構築ガイドなど)を全て閲覧することができます。ぜひこの機会にご登録下さい。

アラクサラネットワークス株式会社

〒212-0058
川崎市幸区鹿島田一丁目１番２号 新川崎三井ビル西棟
http://www.alaxala.com/