

サザンクロスルータシステム「AR415S」
ファームウェアリリースノート
Version 2.9.2-01

Ver.2.9.2-01

以下のとおり機能追加、機能改善が行われました。

1. 本バージョンで追加された機能

(1) Suppress ARP Flush 機能

通常動作時は、IPインターフェースがリンクアップする際、ARP テーブルのエントリを消去しますが、この機能によって、指定したPPPインターフェースがリンクアップする際にARPテーブルのエントリを消去しないようにすることができます。

本機能の有効/無効の設定は、ADD IP INTERFACE コマンドのFLUSHARPパラメーターで行います。

コマンド

```
ADD IP INTERFACE=interface IPADDRESS={ipadd|DHCP} [FLUSHARP={ON|OFF}]  
SET IP INTERFACE=interface IPADDRESS={ipadd|DHCP} [FLUSHARP={ON|OFF}]
```

パラメーター

FLUSHARP: ARPエントリの消去を行うかどうか。ON(行う)、OFF(行わない)から選択する。OFFにした場合、IP インターフェースがリンクアップしてもARPエントリは消去されない。デフォルトはON。

備考・注意事項

本機能が有効なのはPPPインターフェースのみです。EthernetインターフェースやVLANインターフェースなどではエラーとなります。また、PPPoEインターフェースでは本機能は動作しません。

本機能の設定状態は、SHOW IP INTERFACE コマンドで確認できます。

(2) Dynamic DNS 定期アップデート機能

ダイナミックDNSサービス (<http://www.dyndns.com/>) で使用しているアカウント情報の定期更新(定期アップデート)が可能になりました。

- ① SET DDNS コマンドにPERIODICUPDATE パラメーターが追加されました。

コマンド

```
SET DDNS [SERVER=server] [PORT=port] [USER=userid]  
[PASSWORD=password] [DYNAMICHOST=hostnames]  
[PRIMARYINTERFACE=ipinterface] [SECONDARYINTERFACE=ipinterface]  
[WILDCARD={YES|NO|ON|OFF}]
```

[OFFLINE={YES|NO|ON|OFF}]

[PERIODICUPDATE={1..60|ON|OFF}]

パラメーター

PERIODICUPDATE: 定期更新の周期を1日単位で任意に指定する。OFFにした場合、定期更新を行わない。デフォルトはON(28日周期で定期更新を行う)。

②SHOW DDNS コマンドの表示内容に、Periodic Update とElapsed days の項目が追加されました。

Periodic Update: 設定されている定期更新の周期(単位: 日)。

Elapsed days: 最後に更新が行われてからの経過日数。

2. 本バージョンで変更された機能

(1) EthernetインターフェースへVLANタグの付与

Eth0、またはEth1インターフェースにVLANタグを付与できるようになりました。

コマンド

ADD IP INTERFACE=interface IPADDRESS={ipadd|dhcp}

VLANTAG= {1..4094|none} [VLANPRIORITY={0..7|none}]

SET IP INTERFACE=interface VLANTAG={1..4094|none}

[VLANPRIORITY={0..7|none}]

パラメーター

VLANTAG: VLAN ID (VID)。

VLANPRIORITY: 802.1pユーザープライオリティー(0~7)値。デフォルトは0。

備考・注意事項

- ・VLANTAGパラメーターでタグが付与された場合、VLANPRIORITYパラメーターのデフォルトは0です。
- ・ブリッジングとの併用はできません。
- ・1つのIPインターフェースに設定できるタグは1つです。

(2) VLANインターフェース上でのPPPoEクライアント設定

VLANインターフェースでPPPoEクライアントの設定ができるようになりました。

コマンド

ADD PPP=ppp-interface OVER=physical-interface

CREATE PPP=ppp-interface OVER=physical-interface

SET PPP=ppp-interface OVER=physical-interface

パラメーター

OVER: 物理インターフェース名。ISDN-callname (ISDN コール)、TNL-callname (L2TP コール)、TDM-groupname (TDMグループ)、ETH-servicename (Ethernetインターフェース)、VLAN-servicename (VLANインターフェース)のいずれかを指定する。

servicenameにはPPPoEサービス名を18文字以内で指定する。(ダブルクォーテーション)は使用できない。大文字小文字を区別する。どのサービスでもよいときは、servicenameにANY を指定する。

備考・注意事項

タグVLANとの併用も可能です。

(3)L2TP LNS 代理認証の有効/ 無効

ルーターがL2TP LNS として動作する際、LACから提供される認証情報を元にPPPの代理認証を行うかどうか設定できるようになりました。

コマンド

```
ADD L2TP IP={ipadd|ipadd-ipadd} PPPTEMPLATE=0..31  
[PROXYAUTH={OFF|ON}]
```

パラメーター

PROXYAUTH: LNSとして動作する際、PPPの代理認証を行うかどうか。ON(行う)、OFF(行わない)から選択する。デフォルトはON。

3. 本バージョンで修正された項目

- (1)TCP 脆弱性(JVNVU#943657)への対策を行いました。
- (2)本製品が、内部のシステムチェック処理によりリポートした際、ハングアップすることがありましたが、これを修正しました。
- (3)CREATE CONFIG コマンドを実行した時、作成されるコンフィグファイルのサイズによってはエラーが発生する場合がありますが、これを修正しました。
- (4)ごくまれにSNMPのメモリーリークが発生することがありましたが、これを修正しました。
- (5)PPPネゴシエーションにて、対向よりLCP Configure-Reject パケットを受信した時に再送するLCP Configure-Requestパケットを規定回数分送っていませんでしたが、これを修正しました。

- (6) BGPのルートマップ機能を設定している場合、ルート更新時にメモリーリークが発生することがありましたが、これを修正しました。
- (7) BGP使用時、以下のBGPパケットを受信すると、不正なパケットを送出することがありましたが、これを修正しました。
- ・パス属性の拡張Length長が1
 - ・Length フィールドが2バイト
 - ・Length 値が255以下
- (8) ファイアウォールおよびポリシーベースルーティングが設定されている場合に、ポリシーベースルーティングの対象通信であるにもかかわらず、TCPのRST/ACK パケットがポリシーと異なるインターフェースへ送出されてしまうことがありましたが、これを修正しました。
- (9) ファイアウォール機能において、TCP SYN アタック、DoS アタックを継続して受けた場合、例外発生ログを残さずにリポートする場合がありますでしたが、これを修正しました。
- (10) ファイアウォールポリシーからアクセスリストを削除するDELETE FIREWALL POLICY LIST コマンドを実行した際、そのアクセスリストを適用しているファイアウォールルールが削除されませんでした。削除されるように修正しました。
- (11) DHCPレンジ内のIPアドレスをあるMACアドレスに静的に割り当てようとした際、そのMACアドレスが他のIPアドレスに既に静的に割り当てられている場合、そのIPアドレスをエラーメッセージ内に表示するように変更しました。
- (12) ISAKMPフェーズ1で使用するIKE交換モードをAGGRESSIVEモードに設定し、ピアのアドレスをFQDNで設定すると、そのFQDNからISAKMPパケットを受信しても応答しませんでした。これを修正しました。
- (13) インターフェース以外のセレクター情報が重複したIPsecポリシーが存在する際、ISAKMPハートビート機能やDPD機能で対向機器がリンクダウンしていると判定された場合に、ISAKMP SAのみが削除され、関連するIPsec SAが削除されないことがありましたが、これを修正しました。

4. 本バージョンでの留意事項

(1) 認証サーバーについて

RADIUSサーバーを複数登録している場合、最初に登録したRADIUSサーバーに対してのみ、SET RADIUSコマンドのRETRANSMITCOUNTパラメーターが正しく動作しません。最初のRADIUSサーバーへの再送回数のみ、RETRANSMITCOUNTの指定値よりも1回少なくなります。本現象は802.1X認証を使用した場合のみ発生します。

(2) ポート認証について

- ①DISABLE PORTAUTH コマンドで、PORTAUTH パラメーターに8021xを指定すると、EAP Success/パケットを送信してしまいます。
- ②RESET ETH コマンドによってEthernetインターフェースを初期化しても、認証状態は初期化されません。
- ③802.1x認証済みのクライアントがログオフした場合、ログオフしたクライアントのMACアドレスがフォワーディングデータベース(FDB)に保持されたままになります。
- ④ENABLE/SET PORTAUTH PORT コマンドのSERVERTIMEOUT パラメーターが正しく動作しません。これは、SET RADIUSコマンドのTIMEOUTパラメーターとRETRANSMITCOUNTパラメーターの設定が優先されているためです。
SET RADIUSコマンドでTIMEOUT × (RETRANSMITCOUNT + 1)の値をSERVERTIMEOUTより大きく設定した場合は、SERVERTIMEOUTの設定が正しく機能します。

(3) ブリッジングについて

ポート1がタグ付きパケットのブリッジングの対象となるVLANに所属し、そのVLANにIPアドレスが設定されている場合、ポート1からVLANのIPアドレス宛の通信をしようとすると、ルーターがARPIに応答せず、通信ができません。これはポート1でのみ発生し、他のポートでは発生しません。

(4) IP/経路制御(BGP-4)について

BGPによる経路制御とルートマップ機能をそれぞれ使用する構成で、BGPのプレフィックスにルートマップが設定されていない場合、ルートマップ機能が正常に動作しません。

- ①MED (MULTI-EXIT DISCRIMINATOR) 属性が設定されたプレフィックスを含む最適な経路が複数追加される場合に、設定とは異なるMED値を通知します。
- ②MED属性が設定されたプレフィックスを含む最適な経路が変更または削除される場合に、設定とは異なるMED値を通知します。

(5) ダイナミックDNSについて

- ①ダイナミックDNSのアップデートで、以下の2つのケースにおいて、アップデートは再送されません。
 - ・本製品からのTCP SYNパケットに対して、ダイナミックDNSサーバーからのSYN ACKパケットが返って来ない場合
 - ・本製品からのTCP SYNパケットに対して、ICMP Host Unreachableメッセージが返される場合

②ダイナミックDNSのアップデート(HTTP GET)に対する応答として、ダイナミックDNS(HTTP)サーバーから特定のエラーコード(404 Not Found)を受信すると、SHOW DDNS コマンドのSuggested actionsの項目にHTMLタグの一部が表示されることがあります。

(6) DNSリレーについて

DNSリレー機能有効時、下記条件のとき、クライアントからの名前解決要求に対してクライアントが指定したアドレスとは異なるアドレスで応答します。

- ①2つ以上のVLANが設定されており、それぞれが異なるIPネットワークに所属している
 - ②DNSクライアントが、DNSサーバーのアドレスとして自身が所属していないVLANのIP アドレスを指定している
- これを回避するには、自身が所属しているVLAN のIPアドレスをDNSサーバーとして設定してください。

(6) IPv6について

- ①RIPng経路を利用してIPv6 マルチキャスト通信を行っている場合、経路が無効(メトリック値が16)になっても、しばらくその経路を利用して通信を行います。
- ②ガーベージコレクションタイマーが動作中のRIPng経路は、新しいメトリック値を持つ経路情報を受信しても、タイマーが満了するまで経路情報を更新しません。

(7) ファイアウォールについて

- ①ファイアウォールにてリモートIP を指定せずにダブルNAT ルールを設定すると、ルーターがすべての Gratuitous ARPに対して応答してしまうため、HostIにてアドレス重複を検出し、通信できないことがあります。
- ②ファイアウォールにて動的にIP アドレスが割り当てられるインターフェースをPublicインターフェースとして設定した際、ルールNATのGBLIP パラメーターに"0.0.0.0"を設定すると、NAT 後のソースアドレスがPublicインターフェースのIPではなく、"0.0.0.0" に変換されるためパケットを送信しません。

(8) DHCPv6サーバーについて

- ①DHCPv6サーバーで認証機能を使用した場合、ADD DHCP6 KEYコマンドのSTRICTパラメーターが動作しません。
- ②ADD DHCP6 POLICYコマンドでDHCPv6 サーバーの設定を変更しても、サーバーからReconfigureメッセージが送信されません。ADD DHCP6 POLICYコマンドの実行後、さらにSET DHCP6 POLICYコマンドを実行してください。これにより、Reconfigureメッセージが送信されます。

(9) L2TPについて

ADD L2TP USER コマンドでACTION/パラメーターにdnslookupを指定し、PREFIX/パラメーターは未設定とした場合、設定を保存し、再起動するとコンフィグエラーになります。これを回避するには、再起動トリガーでADD L2TP USERコマンドを再入力してください。

4. 取扱説明書・コマンドリファレンスの補足事項

(1) A.7 製品仕様/ ハードウェア/ インターフェース/WAN ポート

【誤】10BASE-T/100BASE-TX × 1(オートネゴシエーション、Full Duplex/Half Duplex/10Mbps/100Mbps 手動設定、常にMDI/MDI-X 自動切替)

【正】10BASE-T/100BASE-TX × 1(オートネゴシエーション時MDI/MDI-X 自動切替、Full Duplex/Half Duplex/10Mbps/100Mbps 手動設定時はMDI 固定)

(2) リモートアクセス

ファイアウォール機能が有効なルーターに対して、Telnet 経由でマルチホーミングの設定を行うと、Telnetが切断されます。

(2) UPnP ユニキャスト探索

UPnP 機能有効時、本製品のユニキャストアドレスを宛先MAC アドレスに指定されたSSDPパケットに回答しません。ENABLE IP MACDISPARITYコマンドを実行することで、当該のSSDPパケットに回答できるようになります。
