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 2.9.2-07

Ver.2.9.2-07

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）DISABLE SWITCH PORT コマンドのLINKパラメーターの追加

DISABLE SWITCH PORT コマンドにLINKパラメーターが追加されました。LINKパラメーターにDISABLEを指定することによって、スイッチポートを物理的にリンクダウンさせることが可能になりました。

コマンド

DISABLE SWITCH PORT={port-list|ALL} [LINK={DISABLE|ENABLE}]

SHOW SWITCH PORT

（2）WAN/ETHポートの無効/ 有効設定

新規に追加されたDISABLE ETHコマンドによってWAN側Ethernetポートを無効にすることが可能になりました。本コマンドでLINKパラメーターにDISABLEを指定することによって、ポートを物理的にリンクダウンさせることができます。また、新規に追加されたENABLEETHコマンドによって、無効にしたWAN側Ethernetポートを有効にすることができます。

コマンド

DISABLE ETH=eth-interface [LINK={DISABLE|ENABLE}]

ENABLE ETH=eth-interface

SHOW ETH STATE

（3）SHOW IPSEC ISAKMPコマンドの追加

新規に追加されたSHOW IPSEC ISAKMPコマンドによって、IPsec SAごとに関連するISAKMP SAを一覧表示することが可能になりました。

コマンド

SHOW IPSEC ISAKMP

（4）Responder Rekey Extension機能

Responder Rekey Extension機能が追加されました。Android端末などのISAKMP/IPsecキープアライブ機

能を持たない機器との接続時に、対向機器の死活監視が可能になりました。

CREATE ISAKMP POLICY/SET ISAKMP POLICYコマンドに追加されたREKEYパラメーターで本機能を有効にできます。本機能が有効な場合、ISAKMP SA保持時間満了までIPsecSAの通信の有無を監視し、通信がなくなるまでISAKMPの保持時間を延長し続けます。

ISAKMP SA保持時間満了時にIPsec通信の停止を検知するとISAKMP SAと該当ISAKMP SAに管理されているIPsec SAを削除します。

コマンド

CREATE ISAKMP POLICY=policy PEER=ANY [REKEY={ON|OFF|TRUE|FALSE}]

SET ISAKMP POLICY=policy PEER=ANY [REKEY={ON|OFF|TRUE|FALSE}]

SHOW ISAKMP POLICY

2. 本バージョンで変更された機能

（1）PPPoEサービス名の最大文字数の拡張

以下のコマンドで指定するPPPoEサービス名に設定できる文字数が18 文字から64 文字に拡張されました。

コマンド

ADD PPP=ppp-interface OVER=physical-interface

CREATE PPP=ppp-interface OVER=physical-interface

DELETE PPP=ppp-interface OVER=physical-interface

SET PPP=ppp-interface [OVER=physical-interface]

ADD PPP ACSERVICE=service-name TEMPLATE=template
ACINTERFACE=interface

DELETE PPP ACSERVICE=service-name

SET PPP ACSERVICE=service-name

（2）CREATE PPP/SET PPP コマンドのPADRRETRYパラメーターの追加

CREATE PPP/SET PPP コマンドにPADRRETRYパラメーターが追加されました。

PPPoE ディスカバリーステージで送信したPADR に対してPPPoE AC（AccessConcentrator）からPADSが送信されてこなかった場合に、前バージョンまではディスカバリーステージを3 回実施後に終了しましたが、PADRRETRY パラメーターに0を指定することでディスカバリーステージを繰り返し実施することが可能になりました。

コマンド

ADD PPP=ppp-interface OVER=physical-interface

CREATE PPP=ppp-interface OVER=physical-interface [PADRretry={0|15}]

SET PPP=ppp-interface [PADRretry={0|15}]

SHOW PPP CONFIG

SHOW PPP LIMITS

（3）ICMPチェックサム検証の仕様変更

本体宛てICMPv4/v6 Echo RequestパケットのICMPチェックサムフィールド値が「0xffff 」である場合、前バージョンまでは該当パケットをチェックサムエラーで破棄していましたが、本バージョンからは同フィールドの値が「0x0000」であると見なしてチェックサムを検証するよう仕様変更しました。

（4）SET DDNSコマンドのサポート対象パラメーターの変更

Dynamic Network Services社が提供するダイナミックDNSサービスDynDNS.com（http://www.dyndns.com/）のDynamic DNS Freeサービスで提供されていたワイルドカード機能が有料化されたため、SET DDNSコマンドに含まれるWILDCARDパラメーターを未サポートとさせていただきます。

（5）ISAKMP のIPsec SA管理方法の変更

IPsec通信を行う際、IPsec SAが必ずISAKMP SAに管理されている状態を保つように仕様を拡張しました。本バージョンより、IPsec SAを管理するISAKMP SAが明確になりました。

これによりIPsec SAがISAKMP SAと連動して動作するようになり、ISAKMP SAが削除される際にIPsec SAも同時に削除され、管理されていないIPsec SAが存在することがなくなりました。

コマンド

SHOW IPSEC POLICY [SABUNDLE]

3．本バージョンで修正された項目

（1）本製品がTelnetやBGPなどのTCPコネクションを確立している状態において、TCPの状態がTIMEWAITのときに再送データを受信すると、それ以降再送データを受信しなくても不要なACKを再送していましたが、これを修正しました。

（2）BGPピアへの通知時に経路属性を変更するルートマップ（OUTROUTEMAP）において、プレフィックスに応じて異なる属性値をセットするよう設定しても、意図した属性値がセットされないことがありましたが、これを修正しました。

（3）BGPセッションがEstablished状態になる前にピアからUPDATEメッセージを受信した場合、このメッセージを破棄してしまい、メッセージ内の経路情報を学習できないことがありましたが、これを修正しました。

（4）SET SYSTEM NAMEコマンドで完全なドメイン名（FQDN）を設定していても、PINGコマンド、TRACEコマンドでは、短いホスト名を指定した場合にドメイン名の補完が行われませんでしたが、これを修正しました。

（5）IPv6 over IPv4トンネリングインターフェース、および、6to4トンネリングインターフェースを経由した通信において、最初の1パケットを破棄していましたが、これを修正しました。

（6）PIM-SMにおいて、ランデブーポイント（RP）への到達性が一定期間失われると、その後RPへの到達性が復帰してもマルチキャスト経路がすぐに復旧しないことがありましたが、これを修正しました。

（7）ランデブーポイント（RP）への経路が切断された後、PIM ツリーのRPF Neighbourto RPに不正なIPアドレスが表示されていましたが、これを修正しました。

（8）L2TP/IPSecによるリモートアクセス環境で、L2TPの接続要求パケットの再送が行われると、L2TPの接続に失敗する場合がありましたが、これを修正しました。

（9）IPルートテンプレートによって経路情報が自動登録されている場合に、IPsec SA更新時に該当IPsecポリシーを使用した通信が発生していないと、旧IPsec SAを削除する際に当該経路情報も削除してしまっていましたが、これを修正しました。

（10）複数の拠点との間にIPsec SAを確立するセンター側において、DISABLE IPSECコマンドによってすべてのIPsec SAが削除される場合、1 つの拠点にすべてのDeleteペイロードを送信してしまい、結果としてほとんどの拠点側にてDeleteメッセージを受信できませんでしたが、これを修正しました。

（11）1つのNAT機器の配下にある複数のAndroid端末からルーターに対してNAT トラバーサルを使用してVPN接続を行うと、最後に接続してきた端末のみの通信が維持され、それ以外の端末の通信が切断されてしまいましたが、これを修正しました。

（12）ISAKMP機能において、IKEのステータスやエラー情報を通知するNotifyペイロードを送信する際のバッファーの計算に誤りがあり、誤ったメモリーアクセスが発生し、本製品がリブートしていましたが、これを修正しました。

（13）IPsec機能のSAバンドルスペック設定において、IPsec SAの有効期限(EXPIRYSECONDS)を設定し以下の両方の条件に合致した条件で通信した場合に、本製品がリブートしていましたが、これを修正しました。

・本製品がIPsecのレスポンダーである場合。

・IPsecのイニシエーターから通知されるIPsec SAの有効期限が、本製品に設定されたIPsec SAの有効期限より長い場合。

（14）IPSec SA更新時に該当IPsec ポリシーを使用した通信が発生していない状況において、対向機器から古いIPSec SAを削除する Delete メッセージを受信することによりIPSec SAが削除された場合、IPルートテン

プレートによって登録された経路が削除されていましたが、これを修正しました。

（15）Re-KEYにより新旧2つのISAKMP SAが存在する状況で、古いISAKMP SAが削除されるタイミングで新しいIPsec SAも削除してしまう場合がありましたが、これを修正しました。

（16）ISAKMP/IPsecポリシーのPEERにANYまたはDYNAMICを設定した場合、実際は行っていないにも関わらず名前解決に失敗したようなログが表示されてしまうことがありましたが、これを修正しました。

（17）PEER=ANYでVPNが接続されている場合、VPN ピアが接続されているNAT機器のIPアドレスが変わることによって、ISAKMP SA を通じて送信されるInfoメッセージ（IPsec DPD、ISAKMPハートビートなど）は、ARルーターで保持している送信元アドレスと異なるIPアドレスで受信します。このInfoメッセージの破棄処理において、メモリーの解放漏れが発生していましたが、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

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）ETHインターフェース

Ethernetポートでリンクダウンをともなうポート無効に設定後、該当ポートの速度設定を変更すると、SHOW ETH STATEコマンドで表示されるActual speed/duplexの表示がConfigured speed/duplexと同じ表示になります。

（3）ポート認証

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。

（4）ブリッジング

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アドレス宛ての通信をしようとすると、 ルーターがARP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。

（5）ダイナミックDNS

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

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。

（7）IPv6

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。

（8）ファイアウォール

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、Host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。

（9）DHCPv6サーバー

①ADD 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。

②DHCPv6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。

（10）L2TP

①ADD 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。

②L2TP インターフェースでOSPFオンデマンドを使用した場合、L2TPの自動接続を開始しません。

（11）IPsec

①Android OS標準のVPNクライアントではない独自VPN クライアントを実装してIPsec DPDに対応したスマートフォンN-06Cとリモートアクセス VPNを行うと、N-06Cの送信するR-U-THEREメッセージを受信しても本製品はR-U-THEREACKメッセージを返しません。
これを回避するには、PPP LCPエコーの間隔を短くするなどして、通信中は端末側からのIPsec DPDを動作させないようにしてください。

②SET ISAKMP POLICYコマンドでIPsec DPDとISAKMPハートビートを同時に指定すると、DPDの動作モードが正しく反映されません。IPsec DPD とISAKMPハートビートを設定する場合には、同時に指定しないようにしてください。

③SET IPSEC POLICYコマンドを実行した場合、該当するIPsecポリシー上に確立しているIPSec SAが削除されますが、削除されたIPSec SAにIPルートテンプレートが設定されている場合、テンプレートを通じて追加された経路が削除されません。
DELETE IP ROUTEコマンドで該当するIPルート情報を削除することにより、この不整合から復旧させることができます。

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）