613-000275 Rev.G 081217

Allied Telesis

CentreCOM® AR570Sリリースノート

この度は、CentreCOM AR570S をお買いあげいただき、誠にありがとうございました。
このリリースノートは、取扱説明書（613-000451 Rev.B）とコマンドリファレンス（613-000273 Rev.C）の補足や、ご使用の前にご理解いただきたい注意点など、お客様に最新の情報をお知らせするものです。
最初にこのリリースノートをよくお読みになり、本製品を正しくご使用ください。

1　ファームウェアバージョン　2.9.1-17

2　本バージョンで追加された機能

ファームウェアバージョン 2.9.1-11 から 2.9.1-17 へのバージョンアップにおいて、以下の機能が追加されました。

2.1　SNMP のエンコード方式の設定

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

SNMP マネージャーからの Get 要求に対し、返信する値（カウンター値）が特定の範囲にある場合の動作を設定できます。以前のバージョンのファームウェアでは、カウンター値の先頭 1Byte が省略されるため、SNMP マネージャーによっては正しい値が表示されないことがありました。本設定（デフォルトで ON）により、省略しない値を出力できます。設定は、追加された SET SNMP ASNBERPADDING コマンドで行います。

コマンド

```
SET SNMP ASNBERPADDING={ON|YES|TRUE|OFF|NO|FALSE}
```

パラメーター

ASNBERPADDING: SNMP マネージャーからの Get 要求に対し、返信する値（カウンター値）が特定の範囲にある場合、カウンター値の先頭 1Byte を省略するかどうかを示す。（特定の範囲とは、2 進数で表記した場合に先頭 9bit がすべて 1 となる数値。32bit カウンターの場合は 4286578688 ～ 4294967295。）ON（デフォルト）の場合、カウンター値の先頭 1Byte を省略しない。OFF を指定すると、カウンター値の先頭 1Byte を省略する。ON、YES、TRUE および OFF、NO、FALSE はそれぞれ同じ意味。

2.2　SNMP トラップ送信遅延時間の設定

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

起動時におけるすべての SNMP トラップを送信するタイミングを任意に遅らせることができるようになりました。設定は、新しく追加された SET SNMP TRAPDELAY コマンドで行います。

コマンド

```
SET SNMP TRAPDELAY=10..600
```

パラメーター

TRAPDELAY: すべての SNMP トラップを送信するタイミングを遅らせる時間（秒）。デフォルトは 10 秒。

2.3 SNMP リンクトラップ送信遅延時間の設定

参照「コマンドリファレンス」/「インターフェース」

SNMP リンクアップ / リンクダウントラップを送信するタイミングを任意に遅らせることができるようになりました。設定は、新しく追加された SET INTERFACE TRAPDELAY コマンドで行います。

コマンド

```
SET INTERFACE={ifIndex|interface} TRAPDELAY=0..60
```

パラメーター

INTERFACE: インターフェースの ifIndex またはインターフェース名。
TRAPDELAY: SNMP リンクアップ / リンクダウントラップを送信するタイミングを遅らせる時間（秒）。デフォルトは 0 秒。

2.4 ファイアウォールにおけるフラグメント化パケット透過の最大数設定

参照「コマンドリファレンス」/「ファイアウォール」

ファイアウォールによってフラグメント化パケットを透過させる場合、「ENABLE FIREWALL POLICY FRAGMENT=UDP」コマンドによって設定可能ですが、このコマンドを実行した場合、透過させることができるフラグメント化パケットの個数は 20 個までとなっていました。本バージョンより、透過できるフラグメント化パケットの個数の上限を変更できるようになりました。設定は、新しく追加された SET FIREWALL MAXFRAGMENTS コマンドで行います。

コマンド

```
SET FIREWALL MAXFRAGMENTS=8..50
```

パラメーター

MAXFRAGMENTS: 透過させるフラグメント化パケットの最大数。

3 本バージョンで修正された項目

ファームウェアバージョン 2.9.1-11 から 2.9.1-17 へのバージョンアップにおいて、以下の項目が修正されました。

3.1 ファイアウォールにおいて、フラグメントされた TCP 再送パケットの取り扱いに問題があり、メモリーリークが発生する場合がありましたが、これを修正しました。

3.2 トンネルインターフェースのダウン時にリブートが発生する場合がありましたが、これを修正しました。

3.3 PPPoE サーバー（Access Concentrator）使用時、PPPoE クライアントから送信された認証が失敗するとメモリーリークが発生する場合がありましたが、これを修正しました。

3.4 ごくまれに RENAME コマンドによりフラッシュメモリー上のファイルが削除される場合がありましたが、これを修正しました。

3.5 atrqos.mib ファイルの末尾に改行が入っていませんでしたが、これを修正しました。

3.6 PPP の Magic Number オプションを使用しない設定の機器からの LCP Echo Request に応答できませんでしたが、これを修正しました。

3.7 PPPoE AC として動作する際、自身が保持していないセッション ID の PPP パケットを受信すると、Ether Type が 0x8864 の PADT パケットを送信していましたが、Ether Type が 0x8863 の PADT パケットを送信するように修正しました。

3.8 ブリッジフィルター設定時、不要な SET BRIDGE FILTER=1 ENTRY=1 PORT=ALL コマンドが追加されてしまい、ブリッジフィルターが正しく動作していませんでしたが、これを修正しました。

3.9 BGP 脆弱性（JVNVU#929656）への対策を行いました。

3.10 レンジ NAT 使用時に、グローバル側からの TCP パケットを不正に書き換え、通信が行えませんでしたが、これを修正しました。

3.11 DNS に関するキャッシュポイズニング脆弱性（JVNVU#800113）への対策を行いました。

3.12 IPv6 近隣通知（NA）パケットの受信を待っているときに、Target link-layer address オプションの値が 00-00-00-00-00-00 の不正な NA パケットを受信するとリブートしていましたが、これを修正しました。

3.13 PIM-SM 使用時、ルーティング済みのマルチキャストパケットを筐体内に保持し続け、メモリーリークが発生する場合がありましたが、これを修正しました。

3.14 ファイアウォール使用時、TCP オプションヘッダーを正しく認識できず、スループットが低下する場合がありましたが、これを修正しました。

3.15 L2TP とファイアウォールを併用している場合、トンネル確立後、ファイアウォールセッションを削除し L2TP の再送処理が行われるまで通信が行えませんでしたが、これを修正しました。

3.16 UPnP で使用する TCP セッションが保持され続け、本製品との TCP 通信が行えなくなる場合がありましたが、これを修正しました。

3.17 VRRP のバーチャル IP アドレスとして自身のインターフェースの IP アドレスを使用している場合（優先マスタールーターとして設定している場合）、インターフェース監視機能（ADD VRRP MONITOREDINTERFACE コマンドで設定）によってマスタールーターからバックアップルーターに移行した後も、バーチャル IP アドレス宛ての ARP Request に対し、自身の MAC アドレスで応答することがありましたが、これを修正しました。

3.18 ファイアウォールルールに VRRP のバーチャル IP アドレスを指定した場合、バーチャル IP アドレス宛ての ARP に VRRP のバックアップルーターも応答していましたが、これを修正しました。

3.19 DHCP サーバーとマルチホーミングを併用した場合、DHCP クライアントに IP アドレスを割り当てたあと、再度、DHCP クライアントから DHCP DISCOVER パケットが送信されると、すでに割り当てた IP アドレスと異なる IP アドレスを割り当てていましたが、これを修正しました。

3.20 インターフェースダウンなどにより、リモート装置までの経路が確立されていない状態で L2TP の発呼が行われた場合、インターフェースアップ後にトンネルが確立されてもトンネル作成のための SCCRQ パケットが続けて送信される場合がありましたが、これを修正しました。

3.21 SHOW L2TP TUNNEL CALL コマンドを実行するとリブートする場合がありましたが、これを修正しました。

3.22 インターフェースダウン時、L2TP でカプセリングされたパケットを送信する際にリブートする場合がありましたが、これを修正しました。

3.23 L2TP においてリモート側の装置が再起動しトンネルの不整合が発生した場合、新たにトンネルを作成できませんでしたが、これを修正しました。

3.24 リモート側の装置より L2TP 接続の切断が開始される際に、受信したパケットの Result Code によっては、機器がリブートする場合がありましたが、これを修正しました。

3.25 センター経由の拠点間 IPsec 通信において、拠点間通信時にセンター側ルーターから ICMP Redirect が送出されていましたが、これを修正しました。

3.26 IPsec SA 未確立時に受信したパケットを SA が確立するまで保持していましたが、これを修正しました。

3.27 IPsec で処理されるパケットが、random.rnd ファイルを 20 分周期で自動更新する際に、破棄される場合がありましたが、これを修正しました。

3.28 ポリシー名とインターフェース以外の値が同じ IPsec ポリシーを複数設定した場合、先に設定した IPsec ポリシーが常に優先され、設定どおり動作していませんでしたが、これを修正しました。

4 本バージョンでの制限事項・注意事項

ファームウェアバージョン 2.9.1-17 には、以下の制限事項や注意事項があります。

4.1 ADD DHCP6 POLICY コマンド

参照「コマンドリファレンス」/「DHCPv6 サーバー」

「ADD 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。

4.2 ADD DHCP6 KEY コマンド

参照「コマンドリファレンス」/「DHCPv6 サーバー」

DHCPv6 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。

5 取扱説明書とコマンドリファレンスについて

最新の取扱説明書（613-000451 Rev.B）とコマンドリファレンス（613-000273 Rev.C）は弊社ホームページに掲載されています。
本リリースノートは、上記の取扱説明書とコマンドリファレンスに対応した内容になっていますので、お手持ちの取扱説明書、コマンドリファレンスが上記のものでない場合は、弊社 Web ページで最新の情報をご覧ください。

※パーツナンバー「613-000273 Rev.C」は、コマンドリファレンスの全ページ（左下）に入っています。

http://www.allied-telesis.co.jp/