613-002108 Rev.E 151211

AT-AR2050V/AT-AR3050S/AT-AR4050S リリースノート

この度は、AT-AR2050V/AT-AR3050S/AT-AR4050S をお買いあげいただき、誠にありがとうございます。このリリースノートは、取扱説明書とコマンドリファレンスの補足や、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 5.4.5-2.1

2 本バージョンで追加・拡張された機能

ファームウェアバージョン **5.4.5-1.1** から 5.4.5-2.1 へのバージョンアップにおいて、以下の機能が追加・拡張されました。

2.1 AT-AR2050V

参照「取扱説明書」

本バージョンより、VPN ルーターの新機種 AT-AR2050V をサポートします。

2.2 PPP アイドルタイマー・オンデマンド接続

参照「コマンドリファレンス」/「PPP」

PPP インターフェースにおいて、アイドルタイマー（無通信時の自動切断）とオンデマンド接続（データ送信要求に応じた自動接続）に対応しました。本機能は新しく追加された ppp timeout idle コマンドで有効化できます。初期設定は無効です。

2.3 PPPoE Unnumbered IP インターフェース

参照「コマンドリファレンス」/「PPP」

PPPoE インターフェースにおいて、複数 IP アドレスを利用可能な LAN 型接続などに必要な Unnumbered IP 設定に対応しました。Unnumbered IP インターフェースは新しく追加された ip unnumbered コマンドで設定します。

2.4 サポートする USB 型データ通信端末の追加

参照「コマンドリファレンス」/「PPP」

下記の USB 型データ通信端末をサポートしました。

○ 富士ソフト FS020U

なお、サポートする USB 型データ通信端末の最新情報は、弊社ホームページでご確認ください。

2.5 フローベース ECMP

参照「コマンドリファレンス」/「IP ルーティング」/「経路制御」

これまで、本製品の ECMP（等コストマルチパスルーティング）は、トラフィックフロー単位で送出インターフェースを振り分けるフローベースではなく、パケット単位で振り分けるラウンドロビン方式で動作していましたが、本バージョンより、同一宛先・同一コストの経路が複数存在する場合にトラフィックフロー単位でパケットを振り分けるフローベース ECMP で動作するよう機能拡張されました。

2.6 clear ip rip route コマンド

参照「コマンドリファレンス」/「IP ルーティング」/「経路制御（RIP）」

clear ip rip route コマンドに invalid-routes パラメーターが追加されました。RIP でスタティック経路を通知している場合、そのスタティック経路を削除した後で他の機器から同一の RIP 経路を受け取ってしまうと、スタティック経路を削除してから 2 分間は経路の更新ができませんが、「clear ip rip route invalid-routes」を実行すれば、即座に経路を切り替えることができます。

2.7 VRRP におけるバーチャルルーター設定数の拡張（AT-AR3050S/AT-AR4050S）

参照「コマンドリファレンス」/「IP ルーティング」/「VRRP」

AT-AR3050S/AT-AR4050S において、バーチャルルーターの設定可能数が下記のとおり拡張されました。

- ○ IPv4 VRRP：32 → 127
- ○ IPv6 VRRP：32 → 255

なお、IPv4 VRRP と IPv6 VRRP を併用する場合は、IPv4、IPv6 それぞれ 127 までとなります。

また、AT-AR2050V では、IPv4 VRRP、IPv6 VRRP ともに、バーチャルルーターの設定可能数は 32 までです。

2.8 ホスト定義における動的割り当てアドレス対応

参照「コマンドリファレンス」/「UTM」/「エンティティー定義」

ホストエンティティーのアドレスを指定する ip address、ipv6 address コマンドにおいて、新しく追加された dynamic interface IFNAME オプションによって、動的に割り当てられる IP/IPv6 アドレスを表せるようになりました。これにより、不定アドレスを持つインターフェースからの通信、同インターフェース宛ての通信を明確に指定できるようになります。

2.9 NAT 方式の拡張

参照「コマンドリファレンス」/「UTM」/「NAT」

UTM 機能で使用可能な NAT 方式が次のとおり拡張されました。

- ○ ダイナミック ENAT（IP マスカレード）において、変換後のグローバル IP アドレスを任意指定できるようになりました。
- ○ ポートフォワーディングにおいて、転送先 TCP/UDP ポートを任意指定できるようになりました（スタティック ENAT）。
- ○ 任意のグローバル IP アドレス・プライベート IP アドレス間を 1 対 1 で変換するスタティック NAT に対応しました。

各 NAT 方式の設定方法はコマンドリファレンスをご覧ください。

2.10 VPN パススルー

参照「コマンドリファレンス」/「UTM」/「NAT」

UTM の NAT 機能において、IPsec、PPTP、L2TP のパススルーに対応しました。これにより、NAT 機能を使用している本製品の配下から外部に対して、これらのプロトコルを利用した VPN 接続が可能になりました。

2.11 ポリシーベースルーティング

参照「コマンドリファレンス」/「トラフィック制御」/「ポリシーベースルーティング」

始点・終点 IPv4/IPv6 アドレス、始点・終点 TCP/UDP ポート、DSCP 値にもとづいてパケットの転送先を制御するポリシーベースルーティングに対応しました。詳細はコマンドリファレンスをご覧ください。

2.12 DNS リレー：ドメインによる DNS サーバー振り分け

参照「コマンドリファレンス」/「IP 付加機能」/「DNS リレー」

DNS リレー機能において、検索対象のドメインごとに異なる DNS サーバーを使う設定が可能になりました。詳細はコマンドリファレンスをご覧ください。

2.13 IPsec 機能拡張

参照「コマンドリファレンス」/「VPN」/「IPsec」

IPsec VPN 関連機能に関して下記の拡張・変更を行いました。

- ○ IKEv1 イニシエーターのサポート
- ○ IKEv1 Aggressive モードのサポート
- ○ IPsec/ISAKMP プロファイル手動設定（カスタムプロファイル）のサポート
- ○ トンネルインターフェースにおけるカスタムセレクターのサポート
- ○ SHA512、AES192 のサポート
- ○ デフォルト ISAKMP プロファイルから Diffi e-Hellman グループ 5 のサポートを削除
- ○ NAT-Traversal のサポート
- ○ ISAKMP INITIAL_CONTACT メッセージのサポート
- ○ DPD パケット送信間隔設定のサポート
- ○ （AT-AR4050S のみ）IPsec トンネルインターフェース数のサポートリミットを 100 から 256 に拡張

詳細はコマンドリファレンスをご覧ください。

2.14 GRE トンネルインターフェースの IPv6 対応

参照「コマンドリファレンス」/「VPN」/「GRE」

GRE トンネルインターフェースのデリバリー（外側）プロトコルとして IPv6 に対応しました。これにともない、IPv6 トンネルインターフェースのサポートは削除されました。

2.15 AMF マスター機能（2 メンバー）の標準対応（AT-AR4050S のみ）

参照「コマンドリファレンス」/「アライドテレシスマネージメントフレームワーク」

本バージョンより、AMF マスター対応機器では、ライセンスなしで AMF マスターとして最大 2 台の AMF メンバーを管理できるようになります。

なお、AMF メンバーを 3 台以上管理したい場合は、これまでどおり AMF マスターライセンスが必要です。

2.16 AT-Vista Manager サポート（AT-AR4050S のみ）

参照「コマンドリファレンス」/「アライドテレシスマネージメントフレームワーク」

AMF ノードマネージメント・ソフトウェア AT-Vista Manager をサポートしました。
AT-Vista Manager との連携には、新しく追加された atmf topology-gui enable コマンド、service http コマンド、log event-host atmf-topology-event コマンドを使います。詳細はコマンドリファレンスおよび AT-Vista Manager のマニュアルをご覧ください。

2.17 AMF における Secure HUB AT-SH510/SH310/SH230/SH210 シリーズと AT-AR2050V のサポート

参照「コマンドリファレンス」/「アライドテレシスマネージメントフレームワーク」

AMF において、Secure HUB AT-SH510/SH310/SH230/SH210 シリーズと AT-AR2050V をサポートしました。

3 本バージョンで仕様変更された機能

ファームウェアバージョン **5.4.5-1.1** から **5.4.5-2.1** へのバージョンアップにおいて、以下の機能が仕様変更されました。

3.1 システム

参照「コマンドリファレンス」/「運用・管理」/「システム」

スタートアップ時にシステム時刻をチェックし、1999 年 23 時 59 分 59 秒以前であった場合は、2000 年 1 月 1 日 0 時 0 分 0 秒にセットするようになりました。
また、上記プロセスにより時刻が変更された場合は以下のようなログが記録されます。

○ user.warning awplus clockcheck: Fixing invalid system time(Thu Jan 1 12:00:26 1970)

3.2 動的に学習した DNS サーバーアドレスの優先順位

参照「コマンドリファレンス」/「運用・管理」/「システム」

これまで、PPP（IPCP）や DHCP で動的に学習した DNS サーバーアドレスは DNS サーバーリストの末尾に追加されていましたが、本バージョンから、動的に学習した DNS サーバーアドレスは手動設定した DNS サーバーアドレスの前に追加され、優先的に使用されるよう仕様変更されました。これにともない、show ip name-server コマンドの表示も、各 DNS サーバーアドレスが動的に学習したものか、手動設定されたものかわかるように仕様変更されています。

3.3 ログ

参照「コマンドリファレンス」/「運用・管理」/「ログ」

○ DDM（Digital Diagnostic Monitoring）対応モジュール挿抜時のログメッセージを変更しました。

[抜いた場合]

変更前
HPI: HOTSWAP Pluggable [IFNAME] hotswapped out: [Module_Name]
変更後
Pluggable[724]: Pluggable [Module_Name] removed from [IFNAME]

[挿した場合]

変更前
HPI: HOTSWAP Pluggable [IFNAME] hotswapped in: [Module_Name]
変更後
Pluggable[738]: Pluggable [Module_Name] inserted into [IFNAME]

○ AMF マスター、または、AMF コントローラーの設定をしている機器において、起動中に以下のログが出るようになりました。

ATMF[1204]: The number of nodes allowed on this ATMF network is 126
ATMF[1204]: The number of ATMF areas allowed to be authenticated is 60

○ サポート上限を超えた AMF ノードがネットワークに参加した場合、2 分おきに Critical ログを出していましたが、一度だけ出力されるように仕様を変更しました。

○ コマンド実行時のログメッセージにおいて、そのコマンドを実行した端末の接続元 IP アドレスもしくはインターフェースが表示されるように仕様を変更しました。

○ PPPoE 未接続時に出力される下記メッセージのログレベルを informational に変更しました。

Unable to complete PPPoE Discovery
Timeout waiting for PADO packets

○ 下記メッセージのログレベルを warning から informational に変更しました。

NSM[1414]: [MLD-DECODE] Socket Read: No MLD-IF for interface

3.4 show atmf node コマンド

参照「コマンドリファレンス」/「アライドテレシスマネージメントフレームワーク」

スタック可能なスイッチはすべて S と表示されていましたが、VCS 機能を no stack enable で無効にした場合、N と表示されるよう仕様変更されました。

4　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 **5.4.5-1.1** から **5.4.5-2.1** 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。

4.1 Linux Kernel に関する脆弱性（CVE-2015-1465）への対策を行いました。

4.2 Linux Kernel に関する脆弱性（CVE-2015-5364 および CVE-2015-5366）への対策を行いました。

4.3 OpenSSL 脆弱性（CVE-2015-1788、CVE-2015-1790 ～ 1793、CVE-2015-4000）への対策を行いました。

4.4 DNS への問い合わせ機能を有効にすると、起動時に snmpd のエラーメッセージが表示され、コンフィグの読み込みに時間がかかることがありましたが、これを修正しました。

4.5 show tech-support コマンドが出力するデバッグ情報ファイルにいくつかの show コマンドが含まれていませんでしたが、これを修正しました。

4.6 特権 EXEC モードへの移行権限を持たないユーザーが enable コマンドを実行する場合の以下の問題を修正しました。

(1) enable password コマンドを CLI から動的に設定した場合、前記ユーザーが enable コマンドを実行してもパスワードの入力を求めるプロンプトが表示されない。

(2) enable password コマンドが設定されていないにもかかわらず、設定を保存して再起動すると、前記ユーザーが enable コマンドを実行したときに特権パスワードの入力を求めるプロンプトが誤って表示される。

4.7 システム起動時に自動実行されるフラッシュメモリー上のファイルシステムチェックにおいて、まれにエラーが出力されることがありましたが、これを修正しました。

4.8 SDHC メモリーカードを装着してすぐに取り外すと、SDHC カードスロットの LED が点灯したままになることがありましたが、これを修正しました。

4.9 ログイン認証に RADIUS サーバーを使用している場合、RADIUS サーバーでユーザーに対する特権レベルを変更しても、Authenticator を再起動しない限り、そのユーザーは変更前の特権レベルでログインしてしまっていましたが、これを修正しました。

4.10 RADIUS サーバーや TACACS+ サーバーでのユーザー認証による CLI ログイン時、ユーザー認証データベースに同一ユーザー名が登録されている場合は、ユーザー認証データベース側の権限レベルを使用していましたが、これを修正しました。

4.11 ローカル RADIUS サーバーから IP アドレス「127.0.0.1」の RADIUS クライアント（NAS）を削除し、再起動してもコンフィグに反映されませんでしたが、これを修正しました。

4.12 NTP クライアント機能使用時、NTP によってシステム時刻が西暦 2000 年よりも前に変更されると、その後 show log コマンドを実行してもログが表示されなくなることがありましたが、これを修正しました。

4.13 長時間通信を続けると次のようなエラーログが出力されることがありましたが、これを修正しました。
truncating integer value > 32 bits

4.14 SNMPv3 のユーザーを削除したときは、設定を保存して再起動する必要がありましたが、これを修正しました。

4.15 SFP モジュールを装着している場合、eth ポートの atPortInfoTranceiverType（1.3.6.1.4.1.207.8.4.4.3.14.1.1.2）が正しくありませんでしたが、これを修正しました。

4.16 dot1dStpPortPriority（.1.3.6.1.2.1.17.2.15.1.2）に「.0」をつけて MIB 情報を取得すると機器が再起動することがありましたが、これを修正しました。

4.17 show interface コマンドの出力におけるスペルを修正しました（pointopoint → point-to-point）。

4.18 システムを再起動した場合、スイッチポートの LED 消灯に時間がかかることがありましたが、これを修正しました。

4.19 パケットストームプロテクション機能の設定コマンド storm-control level において、受信上限値として 0.0 を設定できませんでしたが、これを修正しました。

4.20 VCS 構成のスイッチと LACP で接続している状況において、対向スイッチでマスター切り替えが発生するとエラーログを出力していましたが、これを修正しました。

4.21 LACP を有効にしたポート上で RIP などの予約マルチキャストパケットを受信するとエラーメッセージを出力することがありましたが、これを修正しました。

4.22 デフォルトコンフィグで起動後、show mac address-table コマンドを入力すると内部的に使われるブロードキャスト MAC アドレスが登録されているように表示されていましたが、これを修正しました。

4.23 USB 型データ通信端末「ソフトバンクモバイル 203HW」を LTE 回線のみ使用する設定にしている場合、本製品の USB ポートに 203HW を接続した状態で PPP 関連の設定を変更すると、PPP の自動接続が行われませんでしたが、これを修正しました。

4.24 USB モデムを本製品に接続した状態でインターネット接続設定をすると自動で PPP 接続を開始できませんでしたが、これを修正しました。

4.25 PPP 接続中にシステムを再起動すると、再起動中に例外が発生することがまれにありましたが、これを修正しました。

4.26 802.1Q サブインターフェースに説明文（description）を設定している場合、「no encapsulation dot1q」で該当サブインターフェースの設定を削除しても、ランニングコンフィグ上に該当サブインターフェースの設定が残っていましたが、これを修正しました。

4.27 PPP インターフェース上に設定した IPsec トンネルインターフェースでは RIP を使用できませんでしたが、本バージョンからサポートします。

4.28 distribute-list コマンドでトンネルインターフェースを指定した場合、起動時に該当コマンド行がエラーになっていましたが、これを修正しました。

4.29 新しく作成した PPP インターフェースおよびトンネルインターフェース上に設定した ip ospf mtu コマンドがランニングコンフィグにあらわれませんでしたが、これを修正しました。

4.30 show arp コマンドにおいて、マルチキャスト MAC アドレスを持つ ARP エントリーの「Port」欄に特定のスイッチポートを表示していましたが、これを「flood」（フラッディング）と表示するように修正しました。

4.31 VRRPv3 を使用している環境でディレクティドブロードキャストパケットの転送を有効にすると、転送先のインターフェースだけでなく、受信インターフェースにもディレクティドブロードキャストパケットを複製していましたが、これを修正しました。

4.32 VRRP 稼働中にバーチャルルーター ID で使用してる VLAN から IP アドレスを削除すると異常終了することがありましたが、これを修正しました。

4.33 複数の VRRP セッションを作成し、かつ、VRRP マスター / バックアップと配下の機器との接続をトランクグループで設定している時、一つの VRRP セッション以外がダウンすると、残った VRRP セッション内で VRRP マルチキャストパケットストームが発生していましたが、これを修正しました。

4.34 トンネルインターフェースを削除し再設定すると、IPv6 経路のゲートウェイがトンネルインターフェースから他のインターフェースに変わっていましたが、これを修正しました。

4.35 OSPFv3 と BGP4+ の併用環境において、BGP4+ 経路を OSPFv3 で再通知する場合、AS 外部 LSA のネクストホップアドレスとしてリンクローカルアドレスを設定していましたが、これを修正しました。

4.36 PIM-SM の RP として動作させた場合、Register パケットを受信すると、不正な (S,G) エントリーを経路登録していましたが、これを修正しました。

4.37 ip igmp snooping routermode address コマンドで制御用マルチキャストグループアドレスを設定している場合、IGMP Snooping が正しく機能せず、配送すべきでないポートにもマルチキャストパケットが転送されていましたが、これを修正しました。

4.38 IGMP Snooping が有効でも、IGMP パケットをフラッディングしていましたが、これを修正しました。

4.39 高レートで IPv6 マルチキャストパケットを受信すると再起動することがありましたが、これを修正しました。

4.40 zone、network、host コマンドのエラーメッセージにおいて、エンティティー名にはアットマーク（@）を使用可能と表示されていましたが、実際はアットマークを使用できないため、エラーメッセージを修正しました。

4.41 application コマンドでカスタムアプリケーションを作成するときに 64 文字の名前を指定すると、コンフィグにアプリケーション名が正しく保存されませんでしたが、これを修正しました。

4.42 エンティティー定義において、不定 IP アドレスを持つ WAN 側インターフェースだけを指定する方法がなかったため、ファイアウォールの permit ルールにおいて外部からの DNS リクエストをリレーしてしまう可能性がありましたが、ゾーン・ネットワーク・ホストモードの ip address コマンドに追加された「dynamic interface IFNAME」パラメーターを使用することで、この問題は修正されました。

4.43 Web コントロール（URL フィルタリング）機能有効時、配下の端末から Web ページを開くのに 1 分ほどかかることがありましたが、これを修正しました。

4.44 Web コントロール（URL フィルタリング）機能を長時間使用していると、Web アクセスができなくなることがありましたが、これを修正しました。

4.45 Web コントロール（URL フィルタリング）機能を長時間使用すると、buffered ログの表示、削除が正しく行えなくなることがありましたが、これを修正しました。

4.46 システム起動時、UTM 機能が無効でも下記のログが出力されることがありましたが、これを修正しました。
user.notice awplus UTM[684]: Web_Control: URL Filtering enabled
user.notice awplus UTM[684]: antivuirs: AV Enabled

4.47 QoS 有効時、本体宛て ARP reply が低い優先度のキューで取り扱われる場合がありましたが、これを修正しました。

4.48 セカンダリー IP アドレスを設定したインターフェースで DHCP リレーを有効にした場合、セカンダリー IP アドレスが優先的に使用されていましたが、これを修正しました。

4.49 システム起動時、トンネルインターフェースが最初にアップした後、いったんダウンして再度アップしていましたが、これを修正しました。

4.50 無効化されているトンネルインターフェースを「no shutdown」で有効化すると、最初にアップした後、いったんダウンして再度アップしていましたが、これを修正しました。

4.51 interface コマンドで作成しただけのトンネルインターフェースは、ランニングコンフィグでは確認できず、また「no interface tunnelX」で削除することもできませんでしたが、これを修正しました。

4.52 トンネルインターフェース上でダイナミックルーティングプロトコルを使用している場合、該当トンネルインターフェースを削除し、再度追加した場合、通信ができなくなることがありましたが、これを修正しました。

4.53 PPP インターフェース上に作成したトンネルインターフェースは、PPP インターフェースがアップすると、最初にアップした後、いったんダウンして再度アップしていましたが、これを修正しました。

4.54 トンネルインターフェースの設定を変更した場合、設定を保存して再起動しないと内部の経路情報が不正になることがありましたが、これを修正しました。

4.55 PPP インターフェース上にトンネルインターフェースを作成している場合、PPP インターフェースのアップ時に下記のログメッセージが出力されることがありましたが、これを修正しました。
kern.crit awplus kernel: protocol 0806 is buggy, dev tunnel1

4.56 トンネルインターフェースにおいて、「no mtu」を実行しても MTU を初期値に戻せませんでしたが、これを修正しました。

4.57 トンネルインターフェースを削除した後、再度追加すると、誤ったネクストホップを保持する場合がありましたが、これを修正しました。

4.58 トンネルインターフェースのダウン・アップ後、トンネルインターフェースに設定した MTU 値が再適用されず初期値に戻っていましたが、これを修正しました。

4.59 IPsec トンネルインターフェースにおいて 2700 バイトを超えるパケットを転送できませんでしたが、これを修正しました。

4.60 システム起動後、最初の IPsec 接続では通常よりも時間がかかることがありましたが、これを修正しました。

4.61 対向する両方の装置がほぼ同時に IPsec 接続を開始した場合、IPsec 接続が確立しても、show ipsec sa コマンドで確立した IPsec SA の情報が表示されないことがありましたが、これを修正しました。

4.62 crypto isakmp key コマンドにおいて、対向装置の ISAKMP ID を IPv6 アドレスで指定した場合、自動的に RFC5952（IPv6 アドレスの推奨表記）に準拠する形式でコンフィグに保存するよう修正しました。なお、本修正にともない、ISAKMP ID を IPv6 アドレスで指定した事前共有鍵を「no crypto isakmp key」で削除する場合、RFC5952 に準拠した形式で IPv6 アドレスを指定するよう注意してください。

4.63 IPsec トンネルインターフェースを複数使用している場合、IPsec SA のネゴシエーション時に次のようなログメッセージが表示されていましたが、これを修正しました。
daemon.err XXXX iked: [INTERNAL_ERR]: ike_pfkey.c:218:log_rcpfk_error(): 0:? - ?:(nil):sadb_poll: error at the kernel on DELETE, No such process
daemon.warning XXXX iked: [PROTO_WARN]: ikev2.c:4656:ikev2_process_delete(): 998:yyy.yyy.yyy.yyy[500] - zzz.zzz.zzz.zzz[500]:(nil):can't find sa for proto ESP spi 0x01234567

4.64 IPsec トンネルインターフェースでは、show interface コマンドの送信パケット（output packets）カウンターがカウントされませんでしたが、これを修正しました。

4.65 IPsec 関連プロセスが再起動した場合、IPsec 接続を確立できなくなることがありましたが、これを修正しました。

4.66 本バージョンより、同一装置上で OpenVPN トンネルインターフェースを 2 つ同時に使用できるようになります（Tun モードと Tap モードを 1 つずつ）。なお、2 つ同時に使用する場合は、各トンネルインターフェースで異なる UDP ポート番号を使用するよう設定してください（tunnel openvpn port コマンド）。

4.67 AMF エリアリンクを物理ポートによる接続から、仮想エリアリンクに動的に変更した場合、エリアマスターを再起動するまで仮想エリアリンクが動作しませんでしたが、これを修正しました。

4.68 show atmf detail を実行した際、ドメインの IP 情報が誤って表示されていましたが、これを修正しました。

4.69 AMF 仮想リンクを複数使用してリング構成の AMF 環境を構築する際、デバイスがダウンしたにもかかわらず AMF ノードの情報が更新されないことがありましたが、これを修正しました。

4.70 AMF コントローラーを使用している環境で AMF メンバーのオートリカバリーを実行する場合は、メンバーがローカルマスターより先にコントローラーにバックアップデータを問い合わせていましたが、これを修正しました。

4.71 AMF のローカルマスターとメンバーがオートリカバリーにより復旧した後、ローカルマスターからメンバーへのリモートログインが一時的にできなくなりましたが、これを修正しました。

4.72 AMF メンバーが離脱した際、AMF のメンバーの管理情報が記録されている .configs/atmf-links.conf の中からエントリー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。

4.73 中間階層のドメインコントローラーが AMF ネットワークからはずれた場合、既に存在しないにも関わらずノードリストに表示されていましたが、これを修正しました。

4.74 AMF 仮想リンクを使用している AMF ネットワークで、リブートローリングを実施すると、メンバーノードの ATMFD が再起動することがありましたが、これを修正しました。

4.75 AMF クロスリンクで構成されたリング内の機器で atmf cleanup コマンドを実施すると、リカバリーに失敗していましたが、これを修正しました。

4.76 マスターからのホップ数が 4 以上ある AMF ネットワーク内でトポロジーチェンジが発生すると、エッジの AMF ノードが異常終了してしまう場合がありましたが、これを修正しました。

4.77 AMF を使用している環境で AMF マネージメントサブネットを変更した場合に、変更前の AMF マスターの IP アドレスを NTP サーバーとして保持したままとなっていましたが、これを修正しました。

4.78 AMF マネージメント VLAN 内でパケットストームが発生すると AMF マスターからメンバーが認識できなくなっていましたが、これを修正しました。

4.79 show atmf links コマンドで表示されるリスト上から area-link に所属しているトランクグループが削除できませんでしたが、これを修正しました。

4.80 atmf network-name コマンドが設定されていない状態で「no atmf enable」を実行すると HSL エラーログが表示されていましたが、これを修正しました。

5 本バージョンでの制限事項

ファームウェアバージョン 5.4.5-2.1 には、以下の制限事項があります。

5.1 システム

参照「コマンドリファレンス」/「運用・管理」/「システム」

検索ドメインリスト（ip domain-list）を設定する場合、最初にトップレベルドメインだけのものを設定すると、同一トップレベルドメインを持つ他のエントリーを使用しません。その結果、ホスト名を指定した Ping に失敗することがあります。

5.2 コマンドラインインターフェース

参照「コマンドリファレンス」/「運用・管理」/「コマンドラインインターフェース」

○ edit コマンドを使用すると、コンソールターミナルのサイズが自動で変更されてしまいます。

○ enable コマンド（非特権 EXEC モード）のパスワード入力に連続して失敗した場合、エラーメッセージに続いて表示されるプロンプトの先頭に「enable-local 15」という不要な文字列が表示されます。

○ do コマンド入力時、do の後にコマンド以外の文字や記号を入力しないでください。

5.3 ファイル操作

参照「コマンドリファレンス」/「運用・管理」/「ファイル操作」

○ Apricorn 社の SecureUSB メモリー ASK-256-8GB/16GB/32GB を装着している状態でシステムを再起動した場合、再起動時 SecureUSB メモリーの仕様によりロックがかかるため、再起動後に USB メモリーのセキュリティーを解除するための PIN コードを再度入力してください。

○ edit, mkdir, rmdir, show file, show atmf backup コマンドを使用して Apricorn 社の SecureUSB メモリー ASK-256-8GB/16GB/32GB 上のファイルにアクセスした場合、ASK-256-8GB/16GB /32GB 上のアクセス LED が点滅状態のままになることがあります。その場合は、「dir usb:/」コマンドにて USB メモリーにアクセスする操作を行ってください。

○ ファイル名にはスペースは使用できません。

○ USB メモリーを装着した際、エラーメッセージが表示されることがありますが、これは表示だけの問題であり、動作に影響はありません。

○ フラッシュメモリーから SDHC カードまたは USB メモリーにファイルをコピーする時、途中で SDHC カードや USB メモリーを抜くと、実際はコピーに失敗しているにもかかわらず、（Fail を表すメッセージではなく、）「successful」というメッセージが表示されます。

○ フラッシュメモリーから SDHC カードまたは USB メモリーにファイルをコピーする時、実際にコピーが完了しても、すぐにコピー完了のメッセージが表示されないことがあります。

○ 起動用ファームウェアに設定されているフラッシュメモリー上のファイルと同名のファイルが外部メディア（USB メモリー、SDHC カード）に存在している場合、外部メディア上の該当ファイルを delete コマンドで削除できません。その場合は delete コマンドに force オプションを指定して削除してください。

○ move コマンドでファイルを移動する時、移動先に同じ名前のサブディレクトリーが存在する場合、移動に成功したというメッセージが表示されますが、実際には成功していません。その場合は、ファイル名を変更してから移動してください。

○ ECMP 経路を経由して行う TFTP でのファイル転送は未サポートです。

○ 機器に装着している USB メモリーまたは SD カードを抜き、再度機器に装着した時、以下のログが出ます。

抜いた時
kernel: FAT-fs (sda1): unable to read boot sector to mark fs as dirty

装着した時
kernel: FAT-fs (sda1): Volume was not properly unmounted. Some data may be corrupt. Please run fsck.

また、機器に装着している USB メモリーまたは SD カードを抜き、PC に装着すると、PC 上で「スキャンして修復しますか？」というメッセージが出ますが、ログのみの問題で、ファイルの破損はありません。

5.4 ユーザー認証

参照「コマンドリファレンス」/「運用・管理」/「ユーザー認証」

○ TACACS+ サーバーを利用したコマンドアカウンティング（aaa accounting commands）有効時、end コマンドのログは TACACS+ サーバーに送信されません。

○ TACACS+ サーバーを利用した CLI ログインのアカウンティングにおいて、SSH 経由でログインしたユーザーのログアウト時に Stop メッセージを送信しません。

○ スクリプトで実行されたコマンドは TACACS+ サーバーへは送信されません。

5.5 RADIUS サーバー

参照「コマンドリファレンス」/「運用・管理」/「RADIUS サーバー」

○ server auth-port コマンドによりローカル RADIUS サーバーの認証用 UDP ポート番号を 63998 以上に設定しようとすると、関連プロセスが再起動するログが出力されます。また、上記の UDP ポート番号を使用してポート認証を行うことができません。

○ ローカル RADIUS サーバーに登録するユーザー名の長さは 63 文字までにしてください。

5.6 ログ

参照「コマンドリファレンス」/「運用・管理」/「ログ」

○ no log buffered コマンドを入力してランタイムメモリー（RAM）へのログ出力を一度無効にした後、default log buffered コマンドを実行しても、ログ出力が再開しません。その場合は「log buffered」を実行することにより再開できます。

○ permanent ログにメッセージフィルターを追加した後、default log コマンドを実行してログ出力設定を初期値に戻しても、追加したメッセージフィルターが削除されません。メッセージフィルターを削除するには、log(filter) コマンドを no 形式で実行してください。

○ VLAN インターフェースで IPv6 マルチキャストパケットを受信した場合、以下の誤った MLD エラーログを出力しますが、通信に影響はありません。
kern.warning xxx kernel: Post MLD packet failed
kern.warning xxx kernel: Last message 'Post MLD packet fai' repeated 302 times, suppressed by syslog-ng on xxx

5.7 スクリプト

参照「コマンドリファレンス」/「運用・管理」/「スクリプト」

○ スクリプト機能を使って OSPF、BGP のルーティングプロセスを再起動することはできません。再起動が必要な場合はコマンドから直接実行してください。

○ 間違ったコマンドを入力したスクリプトファイルを実行した場合、本来ならば、コンソール上に "% Invalid input detected at '^' marker." のエラーメッセージが出力されるべきですが、エラーメッセージが出力されないため、スクリプトファイルが正常に終了したかのように見えてしまいますが、通信には影響はありません。

5.8 トリガー

参照「コマンドリファレンス」/「運用・管理」/「トリガー」

○ トリガー設定時、script コマンドで指定したスクリプトファイルが存在しない場合、コンソールに出力されるメッセージ内のスクリプトファイルのパスが誤っています。

誤：% Script /flash/script-3.scp does not exist. Please ensure it is created before
正：% Script flash:/script-3.scp does not exist. Please ensure it is created before

また、スクリプトファイルが存在しないにもかかわらず上記コマンドは入力できてしまうため、コンフィグに反映され、show trigger コマンドのスクリプト情報にもこのスクリプトファイルが表示されます。

○ 定時トリガー（type time）を連続で使用する場合は 1 分以上の間隔をあけてください。連続で実行すると show trigger counter で表示される Trigger activations のカウンターが正しくカウントされません。

○ 複数のトリガーが同時に起動されると、「show trigger counter」で表示されるカウンターが正しい値を表示しなくなります。

5.9 SNMP

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

○ IP-MIB は未サポートです。

○ VLAN 名を SNMP の dot1qVlanStaticName から設定する場合は、31 文字以内で設定してください。

○ snmp-server enable trap コマンドにおいて、snmp-server の文字列を省略し、sn enable trap と入力すると、入力したコマンドがホスト名欄に表示され、コマンドは認識されません。コマンドは tab 補完などを利用し省略せずに入力してください。

○ SNMP マネージャーから MIB 取得要求を連続的に受信すると、"ioctl 35123 returned -1" のようなログが出力されることがありますが、通信には影響ありません。

5.10 NTP

参照「コマンドリファレンス」/「運用・管理」/「NTP」

○ 初期設定時など、NTP を設定していない状態で show ntp status コマンドを入力すると、NTP サーバーと同期していることを示す以下のようなメッセージが表示されます。
Clock is synchronized, stratum 0, actual frequency is 0.000PPM, presicion is 2

○ NTPv4 を使用している場合、ntp master コマンドによる NTP 階層レベル（Stratum）の設定と NTP サーバーによる時刻の取得を併用すると、NTP サーバーによって自動決定される階層レベルが優先されます。

○ NTP による時刻の同期を設定している場合、時刻の手動変更は未サポートとなります。

○ ntp master コマンドで <1-15> パラメーターを省略した場合、NTP 階層レベル（Stratum）は 6 になるべきですが、実際は 12 になります。この問題を回避するため、同コマンドでは NTP 階層レベルを明示的に指定してください。

5.11 仮想端末（vty）

参照「コマンドリファレンス」/「運用・管理」/「端末設定」

仮想端末ポート（Telnet/SSH クライアントが接続する仮想的な通信ポート）がすべて使用されているとき、write memory など一部のコマンドが実行できなくなります。

5.12 Telnet

参照「コマンドリファレンス」/「運用・管理」/「Telnet」

○ 本製品から他の機器に Telnet で接続しているとき、次のようなメッセージが表示されます。

No entry for terminal type "network";
using vt100 terminal settings.

○ 非特権モードでホスト名を使用して、Telnet 経由でリモートデバイスにログインする場合は、ドメイン名まで指定してください。

5.13 Secure Shell

参照「コマンドリファレンス」/「運用・管理」/「Secure Shell」

○ SSH サーバーにおけるセッションタイムアウト（アイドル時タイムアウト）は、ssh server session-timeout コマンドで設定した値の 2 倍で動作します。

○ 本製品の SSH サーバーに対して、次に示すような非対話式 SSH 接続（コマンド実行）をしないでください。
※ 本製品の IP アドレスを 192.168.10.1 と仮定しています。

```
clientHost> ssh manager@192.168.10.1 "show system"
```

○ SSH ログイン時、ログアウトするときに以下のログが表示されますが、動作に影響はありません。
sshd[2592]: error: Received disconnect from xxx.xxx.xxx.xxx: disconnected by server request

○ manager 以外のユーザー名でログインする際、SSH 接続に RSA 公開鍵を使用した場合であってもパスワードが要求されますので、ユーザー名に紐付くパスワードを入力してください。

○ AlliedWare 製品から AlliedWare Plus 製品への SSH 接続は未サポートです。

5.14 インターフェース

参照「コマンドリファレンス」/「インターフェース」

○ IPv6 アドレスを持つインターフェースに show interface コマンドを入力した際の結果に、実際のホップリミットの値が表示されません。

○ LACP チャンネルグループがリンクダウンしているとき、show interface コマンドでは該当グループのパケットカウンターがすべて 0 と表示されます。

5.15 スイッチポート

参照「コマンドリファレンス」/「インターフェース」/「スイッチポート」

○ show flowcontrol interface コマンドの RxPause カウンターが正しく表示されません。

○ 複数ポートにインターフェースモードのコマンドを発行するときは、interface コマンドで対象ポートを指定するときに、通常ポートとして使用できないミラーポートを含めないようにしてください。ミラーポートを含めた場合、一部のポートに設定が反映されなかったり、エラーメッセージが重複して表示されたりすることがあります。

○ ミラーポートとして設定されたポートは、どの VLAN にも属していない状態となりますが、mirror interface none で、ポートのミラー設定を解除し VLAN に所属させても dot1qVlanStaticTable（1.3.6.1.2.1.17.7.1.4.3 ） にポート情報が当該 VLAN に表示されません。ポートに mirror interface コマンドでソースポートのインターフェースとトラフィックの向きを設定した後、設定を外すとポート情報が正しく表示されるようになります。

5.16 リンクアグリゲーション

参照「コマンドリファレンス」/「インターフェース」/「リンクアグリゲーション」

○ スタティックチャンネルグループ（手動設定のトランクグループ）において、shutdown コマンドによって無効にしていたポートに対して no shutdown コマンドを入力しても、ポートが有効にならないことがあります。
この場合は、再度 shutdown コマンド、no shutdown コマンドを入力してください。

○ スタティックチャンネルグループのインターフェースを shutdown コマンドにより無効に設定した後、リンクアップしているポートをそのスタティックチャンネルグループに追加すると、該当するインターフェースが再び有効になります。

○ show interface コマンドで表示される poX インターフェース（LACP チャンネルグループ）の input packets 欄と output packets 欄の値には、リンクダウンしているメンバーポートの値が含まれません。
LACP チャンネルグループ全体の正確な値を確認するには、poX インターフェースではなく各メンバーポートのカウンターを参照してください。

○ トランクグループ（saX、poX）を無効化（shutdown）した状態でメンバーポートを削除しないでください。

○ トランクグループ（saX、poX）のステータスを無効から有効に変更するときは、必ず saX、poX インターフェースに対して「no shutdown」を実行してください。メンバーポートに対して「no shutdown」を実行すると、該当ポートの所属するトランクグループに設定された機能が動作しなくなることがあります。誤ってメンバーポートに「no shutdown」を実行してしまった場合は、ケーブルを抜き差しすることで復旧します。

○ リンクアグリゲーション（LACP およびスタティックチャンネルグループ）使用時に show mac address-table コマンドを実行すると、チャンネルグループ番号ではなく実際に使用されているポート番号が表示されますが、これは表示だけの問題であり動作には影響ありません。

5.17 バーチャル LAN

参照「コマンドリファレンス」/「L2 スイッチング」/「バーチャル LAN」

switchport trunk allowed vlan コマンドの except パラメーターに、該当ポートのネイティブ VLAN として設定されている VLAN を指定しないでください。except パラメーターでネイティブ VLAN を指定した場合、設定内容が正しくランニングコンフィグに反映されず、実際の VLAN 設定状態との間に不一致が発生します。

5.18 スパニングツリープロトコル

参照「コマンドリファレンス」/「L2 スイッチング」/「スパニングツリープロトコル」

スパニングツリープロトコルにおいて、ポートの役割（Role）が Rootport または Alternate から Designated に変更されると、ハロータイム ×3 秒後に下記のログが出力され、トポロジーの再構築が行われます。これによるトラフィックへの影響はありません。

BPDU Skew detected on port port1.0.1, beginning role reselection

5.19 ブリッジング

参照「コマンドリファレンス」/「ブリッジング」

○ 実インターフェースとその上に作成した 802.1Q サブインターフェースの Up/Down 状態が異なる場合、サブインターフェースに IP アドレスを設定することができません。サブインターフェースに IP アドレスを設定するときは、実インターフォースとサブインターフェースの Up/Down 状態を合わせてください。

○ 複数の 802.1Q サブインターフェースに対して、同一の IPv4 アドレスや IPv6 アドレスを設定してもエラーになりませんのでご注意ください。

○ L3 トンネルインターフェース（IPsec、GRE、IPv6）は 802.1Q サブインターフェースをサポートしません。これらのインターフェース上に encapsulation dot1q コマンドで 802.1Q サブインターフェースを作成してもエラーになりませんが、動作しないため設定しないでください。

○ bridge-group コマンドでトンネルインターフェースをソフトウェアブリッジに割り当てるとき、次のようなメッセージが表示される場合がありますが、動作に影響はありません。

Warning: Interface tunnel0 is not fully configure yet

5.20 mtu コマンド

参照「コマンドリファレンス」/「IP ルーティング」/「IP インターフェース」

VLAN インターフェース（vlanX）に対して mtu コマンドを実行すると、ランニングコンフィグ上では該当 VLAN のメンバーポートに対しても mtu コマンドを適用した状態になります。そのため、その状態で設定を保存すると、再起動時スイッチポートに対して mtu コマンドを実行できないためエラーメッセージが出力されますが、動作には影響ありません。

5.21 経路制御

参照「コマンドリファレンス」/「IP ルーティング」/「経路制御」

○ デフォルト経路を登録しているにもかかわらず、show ip route database コマンドで「Gateway of last resort is not set」と表示される場合がありますが、表示だけの問題で通信には影響ありません。

○ IP 経路が 20 エントリー以上登録されていると、デフォルト経路を登録しているにもかかわらず、show ip route コマンドで「Gateway of last resort is not set」と表示される場合がありますが、表示だけの問題で通信には影響ありません。

○ ネクストホップが直結サブネット上にないスタティック経路は未サポートです。

○ show ip route コマンドで、デフォルトルート（0.0.0.0/0）にマッチするアドレスを指定した場合、経路が正しく表示されませんが、これは表示上の問題で実際の通信には問題ありません。

○ 本製品が送出する ISAKMP メッセージはフローベース ECMP ではなく、パケットベース ECMP で送出されます。VPN 接続には影響ありません。

5.22 RIP

参照「コマンドリファレンス」/「IP ルーティング」/「経路制御（RIP）」

○ RIP 認証機能において、複数のパスワード（キーチェーン）を設定した時、送信される RIP パケットの中に含まれるパスワードは、1 番目に設定したパスワードのみになります。

○ RIP で通知するネットワークの範囲を指定するとき 32 ビットマスクで指定しないでください。

○ cisco-metric-behavior コマンドは未サポートです。

○ RIP パケットを送受信する RIP インターフェースの数は 250 までとしてください。

5.23 OSPF

参照「コマンドリファレンス」/「IP ルーティング」/「経路制御（OSPF）」

○ OSPF において、代表ルーター（DR）として動作している時に clear ip ospf process コマンドを入力すると、隣接ルーターが DR に変更されます。

○ OSPF の経路フィルタリングにおいて、match metric コマンドを使った特定経路の破棄ができません。

○ OSPF で完全スタブエリア（area stub no-summary）に指定すると、本来そのエリア内にはデフォルトルートのみを通知するべきですが、各エリアへのルート情報（タイプ 3LSA）が通知されてしまいます。

○ 異なる OSPF プロセス間の OSPF 再通知は未サポートになります。

○ overflow database コマンドを no 形式で実行した場合、設定を有効にするには再起動が必要となります。

○ OSPF 環境でルートマップを使用して IP 経路表へ特定のネットワークのみの経路を登録させる場合、受信した LSU パケット内部の経路エントリーの最初から 255 個までしかルートマップの動作対象になりません。対向機器から受信するルート数は 255 以内におさまるようにしてください。

○ OSPF モードおよび OSPFv3 モードの passive-interface コマンドで、インターフェースを指定せずに実行してすべてのインターフェースで有効にした後、no 形式で一部のインターフェースのみを無効にする操作は行わないでください。

○ PPP インターフェース上に設定した IPsec トンネルインターフェースで OSPF を使用する場合は、該当 IPsec トンネルインターフェースに対して mtu コマンドを実行し、同インターフェースを通るパケットのサイズが 1300 バイト以下になるよう調整してください。

○ OSPF を使用している環境でセカンダリー IP アドレスの設定を動的に行った場合、セカンダリー IP アドレスと同一サブネットのアドレス宛てに本製品の ssh コマンドや ping コマンドなどを実行した場合、始点アドレスとしてプライマリー IP アドレスをセットしたパケットを送信してしまいます。通信先でマネージメント ACL などのアクセス元制限を行っている場合は、本製品のプライマリー IP アドレスからのアクセスも許可するよう設定してください。

5.24 BGP

参照「コマンドリファレンス」/「IP ルーティング」/「経路制御（BGP）」

○ BGP 経路の自動集約機能を有効に設定している場合、デフォルト経路（0.0.0.0/0）のサブネットマスク長が 8 に変換されてしまいます。BGP の経路情報にデフォルト経路が含まれている場合は、自動集約機能を無効にしてください。

○ IPv6 の BGP 機能において、redistribute コマンドで static を指定するとデフォルトルートを BGP 経路表に追加してしまいます。

○ iBGP セッションにおいて、ORIGINATOR_ID 属性値を「0.0.0.0」として通知してしまいます。

○ IPv4/IPv6 BGP ピアとの接続状態が Established から Idle に変わった場合、show ip bgp summary、show bgp ipv6 summary コマンドの表示項目 Up/Down にはセッション切断後の経過時間が表示されるべきですが、Never と表示されます。

○ IPv6 BGP で bgp nexthop-trigger enable コマンドを使用している場合、最適経路更新による通信復旧に時間かかかる場合があります。復旧時間を短縮したい場合は bgp scan-time コマンドで更新間隔を短くすることにより可能です。ただし、間隔を縮めすぎると CPU 使用率が高騰しやすくなるため、あらかじめご検証の上ご使用ください。

○ show ip bgp コマンドで iBGP から学習した経路エントリーを指定して詳細情報を表示した場合、Router-ID は 0.0.0.0 と表示され、正しい値を確認することができません。

○ IPv6 BGP において、リカーシブルックアップを利用して BGP 接続をする場合、IPv6 デフォルトルート経由での接続に失敗するため、IPv6 デフォルトルートを使用せずに宛先 IPv6 アドレスを指定してルートを設定してください。

○ ルートマップ上にある OSPF ルートは BGP 側に再配布されません。

○ neighbor allowas-in コマンドを入力すると、BGP セッションが再起動され、通信が一瞬途切れることがあります。

○ show ip bgp コマンドに「A.B.C.D/M」の形式でエントリーを指定して実行した時、iBGP ピアからプレフィックスの通知を受信しているにもかかわらず、ピアのルーター ID が 0.0.0.0 と表示されてしまいます。

○ BGP の MD5 ダイジェスト認証使用時にパスワードを変更すると、Hold Time が満了するまでセッションを維持するため、新しいパスワードでセッションを張ることができません。

○ IP 経路表に登録されているインターフェース経路は network synchronization コマンドを有効にしても BGP 経路表に追加されません。インターフェース経路を BGP 経路表に追加する場合は redistribute コマンドを使用してください。

○ ルートリフレクターを設定している場合、ルートマップモードの set ip next-hop コマンドが正常に動作せず、ルートマップエントリーにマッチした経路エントリーのネクストホップアドレスを指定値に書き換えることができません。

○ IPv6 BGP ピアの設定をする場合、固定 IPv6 アドレスを設定した VLAN インターフェースを指定してください。リンクローカルアドレスを使った場合は、Update メッセージに含まれる Nexthop に設定されたリンクローカルアドレスの値が正しく通知されません。

○ IPv6 BGP において、neighbor default-originate コマンド（BGP IPv6 アドレスファミリーモード）でデフォルト経路を通知するよう設定している場合は、IPv6 BGP ピアとの通信にループバックインターフェースのアドレスを使うよう設定してください（本製品側では neighbor update-source コマンドで lo インターフェースを指定してください。また対向 BGP ピア側では本製品のループバックインターフェースのアドレスを接続先に指定してください）。

○ IPv4 BGP において、neighbor default-originate コマンド（BGP モード）でデフォルト経路を通知するよう設定している場合は、ソフトリセットを実行しないでください。

5.25 ARP

参照「コマンドリファレンス」/「IP ルーティング」/「ARP」

○ VRRP とプロキシー ARP の両方を有効にしている VLAN インターフェースにおいて、バーチャル IP アドレスがマスタールーターの実アドレスではない場合、接続機器からの ARP Request に対して、バーチャル MAC アドレスではなく受信インターフェースの実 MAC アドレスで応答することがあります。

○ マルチキャスト MAC アドレスをもつスタティック ARP エントリーを作成した後、それを削除してから arp-mac-disparity コマンドを有効にして、同一のエントリーをダイナミックに再学習させる場合は、設定後にコンフィグを保存して再起動してください。

○ 本製品の ARP Request に対して、ブロードキャストアドレス宛ての ARP Reply が返ってきた場合、その情報は本製品の ARP キャッシュに登録されません。

5.26 VRRP

参照「コマンドリファレンス」/「IP ルーティング」/「VRRP」

○ VRRP を使用していない装置では VRRP トラップを有効にしないでください。VRRP トラップの有効化・無効化は、snmp-server enable trap コマンドの vrrp オプションで行います。初期設定は無効です。

○ VRRP のプリエンプトモードを有効にする場合は、バーチャルルーターの優先度が重複しないように設定してください。

○ VLAN に IP アドレスを設定していない状態で VRRP の設定はしないでください。

○ VRRPv3 を使用しているインターフェースの IPv6 グローバルユニキャストアドレスを変更する場合は、最初に当該インターフェース上のバーチャルルーターの設定を削除した後、IPv6 アドレスを変更し、その後バーチャルルーターの設定をしてください。

○ ha associate コマンドを設定した状態でバーチャルルーターの設定を削除すると、HA LED が点灯したままになることがあります。バーチャルルーターの設定を削除する場合は、あらかじめ「no ha association」で HA モードの設定を削除した後、バーチャルルーターを削除してください。

○ VRRP のステータス変更時に下記のログメッセージが出力されますが、VRRP の動作に影響はありません。

VRRPD[1255]: VRRP Event: Transition to MASTER state for 2/1/vlan[vid]
HSL[1225]: HSL: ERROR: Insufficient space in Field Processor to add VRRP trap ARP entry

○ IPv6 VRRP 機能を有効にしたインターフェースがダウンしても、show vrrp コマンドで表示される Multicast membership on IPv6 interface IFNAME のステータスが JOINED と表示されますが、表示上の問題だけであり VRRP の動作に影響はありません。

○ VRRP マスタールーターから自身の所有する IP アドレスでないバーチャル IPv6 アドレス宛てに Ping を実行できません。

○ VRRPv3 とローカルプロキシー ARP を併用時、実 IP を用いたマスタールーターではローカルプロキシー ARP は使用できますが、仮想 IP を用いたバックアップルーターではローカルプロキシー ARP が動作しません。

5.27 IPv6 ルーティング

参照「コマンドリファレンス」/「IPv6 ルーティング」

○ 自身の IPv6 アドレス宛に ping を実行するとエラーメッセージが表示されます。

○ IPv6 において、VLAN が削除されたとき、リンクローカルアドレスが IPv6 転送表から消えません。

○ フラグメントされた IPv6 Echo Request は利用できません。利用した場合 Duplicate パケットは正しく再構築されませんのでご注意ください。

○ VLAN インターフェースに IPv6 アドレスを設定する場合、装置全体で 250 インターフェースを超えないようにしてください。

○ 「no ipv6 forwarding」で IPv6 パケット転送機能を無効化した場合、下記の警告メッセージが表示されますが、実際には再起動は不要です。

% Warning: IPV6 forwarding will not be disabled until the switch reboots.

○ IPv6 パケットに対しては ECMP が動作せず、1 つの経路だけを使用します。

○ IPv6 アドレスに対して ping コマンドを実行してからすぐに Ctrl/C キーでキャンセルすると、コンソールがロックされる場合があります。IPv6 アドレスへの ping をキャンセルする場合は、ping 実行から 1 秒以上経過してからキャンセルしてください。なお、コンソールがロックされてしまった場合は、コンソールタイムアウト後に復旧します。

5.28 IPv6 インターフェース

参照「コマンドリファレンス」/「IPv6 ルーティング」/「IPv6 インターフェース」

○ 受信したルーター通知（RA）パケットにより IPv6 インターフェースのアドレスを自動設定する場合、RA パケットに MTU オプションが設定されていてもその値を採用しません。

○ DHCPv6 クライアント機能を使用した場合、DECLINE カウンターが動作しません。

○ IPv4 アドレスと IPv6 アドレスの両方を設定している VLAN インターフェースで IPv4 の VRRP だけを有効にした場合、IPv6 Router Advertisement が送信されなくなります。

5.29 RIPng

参照「コマンドリファレンス」/「IPv6 ルーティング」/「経路制御（RIPng）」

cisco-metric-behavior コマンドは未サポートです。

5.30 OSPFv3

参照「コマンドリファレンス」/「IPv6 ルーティング」/「経路制御（OSPFv3）」

○ OSPFv3 使用時、passive-interface コマンドで指定するパッシブインターフェースには、実在するインターフェースのみを指定してください。

○ OSPFv3 の OSPF ネイバー暗号化方式を設定すると、次の不要なログが出力されます。これは表示だけの問題であり、動作には影響ありません。

Authentication/Encryption algorithm error, or SA key is wrong.

○ OSPFv3 の AS 境界ルーターで集約された経路エントリーが LSDB に登録されるときメトリックが 1 増加します。

○ 経路集約により作成された null スタティック経路は IPv6 転送表（FIB）に表示されませんので、show ipv6 route database コマンドで表示される IPv6 経路表（RIB）で確認してください。

○ OSPFv3 の認証機能は未サポートです。

○ OSPFv3 で仮想リンクを使用している場合、グレースフルリスタートは未サポートです。

○ IPv6 トンネルインターフェース上で OSPFv3 を使用しルート情報を交換した場合、対向のトンネルインターフェース上に割り当てられた IPv6 アドレスのみ 128 ビットマスクで登録されますが、通信に影響はありません。

○ OSPFv3 において、自装置のトンネルインターフェースの経路情報を通知するとき、メトリックを 0 として通知します。

○ エリア間経路として通知していたインターフェース経路を AS 外部経路に変更する場合は、最初に「no redistribute connected」を実行してから、「redistribute connected」を入力してください。

5.31 近隣探索

参照「コマンドリファレンス」/「IPv6 ルーティング」/「近隣探索」

○ イベントログ上に「Neighbor discovery has timed out on link eth1->5」のログメッセージが不要に表示されることがあります。これは表示上の問題であり通信には影響はありません。

○ ipv6 nd reachable-time コマンドを使用することができません。Reachable Time フィールドは初期値のまま使用してください。

○ （AT-AR4050S のみ）ipv6 neighbor コマンドは未サポートです。

○ （AT-AR2050V、AT-AR3050S のみ）ipv6 neighbor コマンドでは Ethernet インターフェース（eth1 ～ eth2）上に Neighbor を登録できません。

5.32 PIM

参照「コマンドリファレンス」/「IP マルチキャスト」/「PIM」

○ ip igmp static-group コマンドで登録したスイッチポートをタグなし、またはタグつきポートに変更すると、IGMP のエントリーは残っているにもかかわらず、PIM の（*,G）エントリーが削除された状態になります。

○ PIM Prune メッセージを受信してもテーブル上から当該グループが完全に削除されないことがあります。ただし、マルチキャストパケットが転送され続けることはありません。(PIM-SMv4、PIM-SMv6 共通)

5.33 IGMP

参照「コマンドリファレンス」/「IP マルチキャスト」/「IGMP」

○ show ip igmp groups コマンドの表示結果に、IGMP を有効に設定していない VLAN が表示されることがあります。これは show ip igmp groups コマンドの表示だけの問題であり、動作に影響はありません。

○ IGMP プロキシーにおいて、下流インターフェースに指定している VLAN を無効にしても、上流インターフェースにグループ情報が残り続けます。

○ ip igmp proxy-service コマンドの設定を取り消す場合は、いったん対象 VLAN インターフェースを「shutdown」してから、「no ip igmp proxy-service」を実行し、その後 VLAN インターフェースを「no shutdown」してください。

○ マルチキャストグループをスタティックに登録している状態で、同じマルチキャストグループをダイナミックに学習すると、その後スタティック登録したグループを削除しても、show ip igmp groups コマンドと show ip igmp snooping statistics interface コマンドの表示からは該当グループが削除されません。これは表示だけの問題で動作には影響ありません。

○ clear ip mroute コマンドでマルチキャスト経路エントリーを削除すると、ip igmp static-group コマンドで設定した IGMP のスタティックエントリーも削除されてしまいます。clear ip mroute コマンド実行後は、ip igmp static-group コマンドを再実行してください。

○ IGMP が有効化されている VLAN の所属ポートで受信した IGMP Leave メッセージは、同一 VLAN 内にフラッディングされます。

○ IGMP プロキシー機能は、送信元指定付きの IGMPv3 パケットをサポートしていません。IGMP プロキシー使用時は、送信元を指定する機能のない IGMPv1、IGMPv2 か、送信元指定なしの IGMPv3 を使用してください。

○ スイッチポートで受信した IGMP Query を他のスイッチポートに転送する時、IGMP クエリーを複製し 2 つ送信しますが、動作に影響はありません。

5.34 IGMP Snooping

参照「コマンドリファレンス」/「IP マルチキャスト」/「IGMP Snooping」

○ IGMP Snooping が有効な状態で、一旦無効にし、再度有効にした場合、その後に受信する IGMP Report を全ポートにフラッディングします。IGMP Snooping を再度有効にした後、clear ip igmp group コマンドを実行して全てのエントリーを消去することで回避できます。

○ Include リスト（送信元指定）付きのグループレコードが登録されている状態で、あるポートに接続された唯一のメンバーからグループ脱退要求を受信すると、そのポートには該当グループのマルチキャストトラフィックが転送されなくなりますが、他のポートで同じグループへの参加要求を受信すると、脱退要求によって転送のとまっていたポートでもマルチキャストの転送が再開されてしまいます（この転送は、脱退要求を受信したポートの Port Member list タイマーが満了するまで続きます）。

○ ダイナミック登録されたルーターポートを改めてスタティックに設定した場合、ダイナミック登録されてから一定時間が経過すると設定が削除されます。また、一定時間が経過するまでの間、コンフィグ上にはスタティック設定が表示されますが、ip igmp snooping mrouter interface コマンドを no 形式で実行しても、コンフィグから削除することができません。
ルーターポートをスタティックに設定する場合は、該当のポートがダイナミック登録されていないことを確認してください。

○ 未認識の IGMP メッセージタイプを持つ IGMP パケットは破棄されます。

○ 不正な IP チェックサムを持つ IGMP Query を受信しても破棄しません。そのため、当該の IGMP Query を受信したインターフェースはルーターポートとして登録されてしまいます。

○ IGMP Snooping 利用時、IGMP Querier を挟まないネットワーク上にマルチキャストサーバーとホストがいる場合、ホストが離脱した後もタイムアウトするまでパケットが転送され続けます。clear ip igmp コマンドで手動でエントリーを削除してください。

○ IGMP の Querier と IGMP Snooping が有効になっている機器が別に存在する場合、上位の Querier から Query を受け取った際に、レポート抑制機能によって自身がレポートを送信しますが、配下にグループメンバーが存在していない場合でも、Querier にレポートを送信してしまう場合があります。レポート抑制機能を無効化することで本事象は回避できます。

5.35 IPv6 マルチキャスト

参照「コマンドリファレンス」/「IPv6 マルチキャスト」

○ IPv6 環境でマルチキャストルーティングを使用する場合は、上流インターフェースで MLD Snooping を無効にしてください。

○ IPv6 マルチキャスト機能において、OSPFv3 メッセージで使用するマルチキャスト MAC アドレスと同じ MAC アドレスを持つマルチキャストグループを使用している場合、shutdown コマンドで VLAN インターフェースを無効化 / 有効化すると、しばらくの間該当 VLAN に所属するポートでは OSPFv3 メッセージを破棄しますが、一定時間が経過すると自動的に復旧します。

5.36 PIMv6

参照「コマンドリファレンス」/「IPv6 マルチキャスト」/「PIM」

○ PIMv6 使用時、PIMv6 インターフェースが最大まで設定されているとき、それらの VLAN の一つを削除しても、新たに VLAN インターフェースに PIMv6 を設定することができません。VLAN インターフェースから PIMv6 の設定を削除してから、VLAN を削除してください。

○ VRRPv3 と PIM-SMv6 は併用できません。

○ ipv6 pim ext-srcs-directly-connected コマンドは未サポートです。

○ 本バージョンでサポートしている PIM-SMv6 は、ソース指定無しの JOIN (*,G)Join のみサポートで、ソース指定有りの JOIN (S,G)Join は未サポートとなります。

○ 同一インターフェース上で ipv6 pim sparse-mode コマンドを繰り返し実行すると PIM-SMv6 が有効にならなくなる場合があるため、複数回実行しないでください。

○ ipv6 pim spt-threshold コマンドを no 形式で実行しないでください。

5.37 MLD

参照「コマンドリファレンス」/「IPv6 マルチキャスト」/「MLD」

○ MLDv2 において、グループエントリーがスタティック登録されている状態で、同じグループがダイナミックに登録され、待機時間が経過した時、ダイナミック登録されたエントリーとともに、スタティック登録されたエントリーもコンフィグから削除されます。

○ clear ipv6 mld コマンド実行時に「% No such Group-Rec found」というエラーメッセージが表示されることがありますが、コマンドの動作には問題ありません。

○ MLD パケットの Max Query Response Time フィールドの値が、本製品の設定の 1/100 の数値で送出されます。MLD をお使いの際は、ipv6 mld query-max-response-time コマンドでなるべく大きい値（最大値は 240）を設定してください。

○ MLDv2 インターフェースにおいて、終点 IPv6 アドレスがマルチキャストアドレスの MLDv1 Report は受信しますが、終点 IPv6 アドレスが MLDv2 インターフェースのユニキャストアドレスになっている MLDv1 Report は受信せずに破棄します。

○ MLD の Non-Queriers は、レコードタイプが BLOCK_OLD_SOURCES の MLDv2 Report メッセージを受信しても、指定された送信元アドレスを削除しません。

○ MLDv1 と MLDv2 混在環境において、MLDv2 Report で Exclude モードになっている状態で、MLDv1 Report を受信した場合、該当アドレスは Exclude モードのソースリストから削除されているにもかかわらず、その後、該当アドレスからのマルチキャストパケットが転送されません。

○ clear ipv6 mroute コマンドでマルチキャスト経路エントリーを削除すると、ipv6 mld static-group コマンドで設定した MLD のスタティックエントリーも削除されてしまいます。clear ipv6 mroute コマンド実行後は、ipv6 mld static-group コマンドを再実行してください。

○ clear ipv6 mld group * ですべてのグループを削除した場合、ルーターポートのエントリーも削除されてしまいます。
clear ipv6 mld group ff1e::1 のように特定のグループを指定した場合は削除されないため、グループを指定し削除してください。また、削除されてしまった場合も MLD Query を受信すれば再登録されます。

○ スタティック MLD グループを設定した後、clear ipv6 mld コマンドでマルチキャストグループを指定すると、ランニングコンフィグからスタティック MLD グループが削除されます。

○ ipv6 mld static-group コマンドを設定したポートにおいて、そのマルチキャストグループを持つ MLD Join メッセージを受信した状態で、shutdown コマンドによりポートをダウンさせた場合、ランニングコンフィグ上から ipv6 mld static-group コマンドを削除しますので、本コマンドを設定したポート上で shutdown コマンドを実行しないようにしてください。

5.38 MLD Snooping

参照「コマンドリファレンス」/「IPv6 マルチキャスト」/「MLD Snooping」

○ MLD Snooping の Report 抑制機能が有効なとき（初期設定は有効）、ルーターポートで受信した MLDv1 Report または Done メッセージを受信ポートから再送出してしまいます。これを回避するには、「no ipv6 mld snooping report-suppression」で Report 抑制機能を無効化してください。

○ MLD Snooping を無効にしても一部の MLD Snooping の機能が動作し続けます。このため、show コマンド上の MLD エントリーが更新されつづけたり、MLD のパケットを受信した際に MLD が動作していることを示すログが出力されます。

5.39 UTM

参照「コマンドリファレンス」/「UTM」

○ Web コントロールモードの rule コマンドを no 形式で実行するとき（ルールを削除するとき）、存在しないルール番号を指定してもエラーになりません。ルール番号をミスタイプした場合など、削除したつもりのルールが削除されていなくても気付かない可能性があるため、ルール削除時にはご注意ください。

○ ファイアウォールと NAT の最大ルール数は両機能あわせて 500 ですが、ルール数が 500 に近づくにつれてパフォーマンスが低下するため、なるべくルール数は少なく設定してください。

○ 無効な NAT ルールが存在する状態で show nat rule コマンドを実行すると、次のようなログが出力されます。
yyyy mm dd hh:mm:ss user.err awplus firewalld: NAT: Sending iptables -t nat -L PORT_FORWARDING_RULE_10 -v -x 2>&1 ¦ grep DNAT ¦ awk '{print $1}' failed

○ アプリケーションコントロール（DPI）機能を有効にした場合、NAT ルールにおいてアプリケーション「ftp」が正しく動作しなくなります。これを回避するため、アプリケーションコントロール（DPI）機能を使用する場合は、下記のようにして FTP 通信を表すカスタムアプリケーション「ftp」を定義してください。

```
awplus(config)# application ftp
awplus(config-application)# protocol tcp
awplus(config-application)# sport 1024 to 65535
awplus(config-application)# dport 21
```

○ 複数のユーザーが同時にアプリケーション定義やエンティティー定義の設定を行うと、コマンドが競合し、意図しない設定になることがありますので、同時に設定を変更しないようにしてください。

○ Ethernet インターフェース（eth1 ～ eth2）上でスタティック NAT を使用する場合、NAT グローバルアドレスとして該当インターフェースと異なる IP アドレスを使用するときは、同インターフェースでローカルプロキシー ARP（ip local-proxy-arp コマンド）を有効にするか、NAT グローバルアドレスに対応するスタティック ARP エントリーを対向装置に設定してください。

5.40 トラフィックシェーピング

参照「コマンドリファレンス」/「トラフィック制御」/「トラフィックシェーピング」

○ トラフィックシェーピングルールを設定していない状態で仮想帯域を設定し、その後トラフィックシェーピング機能を有効にした場合、show traffic-shaping interface コマンドの結果が正常に表示されません。これを回避するには、最初にトラフィックシェーピング機能を有効にしてください。

○ トラフィックシェーピングルールの設定時に、未定義のアプリケーションを指定するとエラーメッセージが出力されます。トラフィックシェーピングルールを設定するときは、使用するアプリケーションをあらかじめ定義してから、ルールを設定してください。

○ トラフィックシェーピング機能を有効にしているとき、次のようなログメッセージが出力されることがありますが、動作には影響ありません。

kernel: HTB: quantum of class 10001 is big. Consider r2q change

5.41 DNS リレー

参照「コマンドリファレンス」/「IP 付加機能」/「DNS リレー」

DNS リレーと VRRP を併用した場合、VRRP のバーチャル IP アドレス宛てに転送された DNS パケットを DNS サーバーに転送することができません。クライアントには VRRP のバーチャル IP アドレスではなく、VRRP マスタールーターの LAN 側実 IP アドレスをプライマリー DNS サーバーアドレスに、また VRRP バックアップルーターの LAN 側実 IP アドレスをセカンダリー DNS サーバーアドレスとして設定してください。

5.42 DHCP サーバー

参照「コマンドリファレンス」/「IP 付加機能」/「DHCP サーバー」

○ 同じ DHCP クライアントから 2 回目の割り当て要求があった場合、割り当て中の IP アドレスは show ip dhcp binding コマンドの実行結果で表示される IP アドレス割り当て状況に残ったままになります。リースしているアドレスの使用期間が満了すると、当該の IP アドレスは割り当て状況一覧から消去されます。

○ show ip dhcp binding コマンドで DHCP クライアントへの IP アドレス割り当て状況を確認するとき、いくつかの DHCP プールに関する情報が表示されないことがあります。

○ DHCP プールが複数設定された環境で show ip dhcp binding コマンドを使用する際は、DHCP プール名やクライアントの IP を指定した状態で実行してください。

○ 多数の DHCP プールを作成している環境において、ネットワークアドレス部に 10 か 100 の数字を含む IP アドレス（10.1.1.1/24、172.16.100.5/24 など）を払い出した場合、10 の部分が 2 ～ 9 になっている別のアドレス（10.1.1.1 に対して 2.1.1.1 や 9.1.1.1 など）、および、100 の部分が 11 ～ 99 になっている別の IP アドレス（172.16.100.5 に対して 172.16.11.5 や 172.16.99.5 など）のリース情報が消えることがあります。

5.43 DHCP リレー

参照「コマンドリファレンス」/「IP 付加機能」/「DHCP リレー」

○ DHCP リレー機能において転送可能な DHCP メッセージの最大長を設定した場合、その最大長より大きなパケットを受信してもパケットを正しく破棄せず、DHCP オプションの一部を削除して転送してしまうことがあります。

○ show counter dhcp-relay コマンドのカウンターが正しく表示されません。

5.44 DHCPv6 サーバー

参照「コマンドリファレンス」/「IP 付加機能」/「DHCPv6 サーバー」

○ 複数の DHCPv6 プールを設定する際は、アドレス範囲やプレフィックスが異なる DHCPv6 プールに重複しないように設定してください。

○ DHCPv6 サーバー機能において、動的に割り当てるアドレスの最終有効時間が infinite（無期限）の場合、IPv6 アドレスを配布しても、show コマンドに反映されません。

○ DHCPv6 サーバー使用時、DHCPv6 サーバー配下のホストに、DHCP プール内の IPv6 アドレスを固定設定しないでください。

○ DHCPv6 プールのサポートリミットは 200 個です。

5.45 トンネルインターフェース

参照「コマンドリファレンス」/「VPN」/「トンネルインターフェース」

○ 複数のトンネルインターフェースで同じ対向アドレス（tunnel destination）を設定した場合、2 つ目以降のトンネルインターフェースでは対向アドレスの設定削除ができません。2 つ目以降のトンネルインターフェースで対向アドレスを変更したい場合は、tunnel destination コマンドを再実行して上書き設定するか、いったん該当トンネルインターフェースを削除したのち、再作成してください。

○ GRE および IPv6 トンネルインターフェースの TTL を tunnel ttl コマンドで変更した場合は、設定を保存して再起動してください。変更後に再起動しないと、ルーティングが正常に行われなくなることがあります。

○ トンネルインターフェースを削除した場合、下記の不要なログメッセージが出力されますが、動作への影響はありません。

BGP[1293]: Parse error for message Link Down ret=-1
PIM-SMv6[1262]: Parse error for message Link Down ret=-1
PIM-DM[1272]: Parse error for message Link Down ret=-1
PIM-SM[1290]: Parse error for message Link Down ret=-1

○ トンネルインターフェースの下位インターフェース（親インターフェース）に対して「shutdown」/「no shutdown」を繰り返し実行しないでください。繰り返し実行すると、トンネル経由の通信が行えなくなることがあります。

○ トンネルインターフェースの MTU を変更すると次のようなエラーメッセージがログに出力されますが、通信には影響ありません。
user.err XXXX HSL[1253]: HSL: ERROR: Error finding iif L2 interface info 11
user.err XXXX HSL[1253]: HSL: ERROR: Group(xxx.xxx.xxx.xxx) Source

○ tunnel source コマンドでは「lo」から始まる無効なインターフェース名を設定することができますが、動作しないため該当インターフェースを指定しないようにしてください。

5.46 IPsec

参照「コマンドリファレンス」/「VPN」/「IPsec」

○ 多数の IPsec over IPv6 トンネルインターフェースが同時に VPN 接続を開始した場合、不正な ISAKMP メッセージを送信することがありますが、その後正常な ISAKMP メッセージを送信するため、VPN 接続には問題ありません。

○ 対向機器との IPsec 接続が切断されても ISAKMP SA および IPsec SA が削除されないことがありますが、対向機器から新しい IPsec セッションが開始されれば新しい SA を作成します。

5.47 L2TPv3

参照「コマンドリファレンス」/「VPN」/「L2TPv3」

L2TPv3 トンネルインターフェース経由で SSH を使用する場合は、mtu コマンドで L2TPv3 トンネルインターフェースの MTU を 1300 バイト以下に設定してください。

5.48 OpenVPN

参照「コマンドリファレンス」/「VPN」/「OpenVPN」

○ OpenVPN Tun(L3) トンネルインターフェースの設定時、「IP packet with unknown IP version=15 seen」というログメッセージが出力されることがありますが、動作に影響はありません。

○ OpenVPN トンネルインターフェースは同時に 2 つまで使用可能です（Tun モードと Tap モードを 1 つずつ）。なお、2 つ同時に使用する場合は、各トンネルインターフェースで異なる UDP ポート番号を使用するよう設定してください（tunnel openvpn port コマンド）。

5.49 GRE

参照「コマンドリファレンス」/「VPN」/「GRE」

○ IPsec 保護（tunnel protection ipsec）を適用している GRE トンネルインターフェース上にトラフィックが存在する状態で該当インターフェースがダウンした場合、informational レベルの下記ログメッセージが繰り返し出力されます。ただし、本ログメッセージは informational レベルのため、初期設定では buffered ログ、permanent ログには保存されず、show log、show log permanent コマンドでも確認できません。

iked: [INTERNAL_ERR]: ikev2_auth.c:555:ikev2_auth_verify(): 4:xx.xx.xx.xx[500] - yy.yy.yy.yy[500]:(nil):no shared key with peer

○ GRE トンネルインターフェースにおいて、MTU よりサイズの大きいパケットを受信した場合、本来なら ICMPv6 の「Packet Too Big」を返すべきですが、「Destination Host Unreachable」を返します。

○ GRE トンネルインターフェースにおいて、対向装置までの経路 MTU が GRE トンネルインターフェースの MTU よりも小さい場合、本製品は LAN 側から受け取った IPv6 パケットを破棄し、送信元に ICMPv6 Packet Too Big エラーメッセージを返送すべきですが、エラーを返送せずに IPv6 パケットを GRE パケットにカプセル化してトンネル対向に向けて送信します。

○ GRE over IPv6 トンネルインターフェースの MTU 値をいったん設定した後で他の値に変更したときは、設定を保存してから再起動してください。

5.50 アライドテレシスマネージメントフレームワーク（AMF）

参照「コマンドリファレンス」/「アライドテレシスマネージメントフレームワーク」

○ AMF リンクとして使用しているスタティックチャンネルグループの設定や構成を変更する場合は、次に示す手順 A・B のいずれかにしたがってください。

[手順 A]
1. 該当スタティックチャンネルグループに対して shutdown を実行する。
2. 設定や構成を変更する。
3. 該当スタティックチャンネルグループに対して no shutdown を実行する。

[手順 B]
1. 該当ノード・対向ノードの該当スタティックチャンネルグループに対して no switchport atmf-link を実行する。
2. 設定や構成を変更する。
3. 該当ノード・対向ノードの該当スタティックチャンネルグループに対して switchport atmf-link を実行する。

○ リブートローリング機能でファームウェアバージョンを A から B に更新する場合、すでに対象ノードのフラッシュメモリー上にバージョン B のファームウェアイメージファイルが存在していると、ファームウェアの更新に失敗します。このような場合は、対象ノードから該当するファームウェアイメージファイルを削除してください。

○ AMF ネットワーク内にマスターノードが存在しない場合でも AMF ネットワークが構成できてしまいますが、AMF 機能は利用できません。

○ AMF マスターが AMF メンバーよりも後に AMF ネットワークに参加するとき、AMF マスターのコンフィグにてその他メンバーからのワーキングセット利用やリモートログインに制限がかけてあっても、既存のメンバーに対してこれらの制限が反映されません。再度 AMF マスター上で atmf restricted-login コマンドを実行することで、全ての AMF メンバーに対して制限をかけることができます。

○ AMF マスター上で atmf recover コマンドによってメンバーノードの内蔵フラッシュメモリーの復元を実行した場合、復元が完了しても、マスターノード上で完了を示すメッセージが出力されません。復元の完了は、対象ノードにおけるログ出力によって確認できます。

○ ワーキングセットプロンプトでは do コマンドを使用できません。

○ オートリカバリーが成功したにもかかわらず、リカバリー後に正しく通信できない場合は、代替機の接続先が交換前と同じポートかどうかを確認してください。
誤って交換前とは異なるポートに代替機を接続してしまった場合は、オートリカバリーが動作したとしても、交換前とネットワーク構成が異なるため、正しく通信できない可能性がありますのでご注意ください。

○ atmf cleanup コマンドの実行後、再起動時に HSL のエラーログが表示されますが、通信には影響はありません。

○ AMF ネットワーク名を変更すると、システム再起動を推奨するログの出力と共に、ノードの離脱、再加入が発生しますが、全ノードが再加入できないことがあります。AMF ネットワーク名を変更した後は、必ず再起動を行ってください。再加入できないノードに対しては、Telnet などでログインし、再起動を実施してください。

○ AMF マスターによる自動バックアップの実行時に本製品のバックアップが失敗することがありますが、次のバックアップタイミングでは成功します。

○ バックアップ先 SSH サーバーに接続できない状況では、「show atmf backup server-status」コマンドの応答に 1 分程度の時間がかかります。

○ HA モード VRRP を使用する AMF メンバーと、AMF マスターとの間で AMF 仮想リンクが 1 本のみ設定されている（VRRP マスタールーターとバックアップルーターの共通 IP アドレスを AMF 仮想リンクの終端アドレスとして指定した）構成において、VRRP マスタールーターがダウンした場合、他の AMF メンバーにワーキングセット経由で接続できなくなることがあります。このような構成で AMF 仮想リンクを使用する場合は、VRRP を構成する各 AMF メンバーの LAN 側 IP アドレスを終端アドレスとして、AMF 仮想リンクを複数設定してください。

○ atmf working-set コマンドを no 形式で実行する場合は、グループ名を省略しないでください。

○ AT-Vista Manager を使用時、DomainController/BackupDomainController になっている AMF メンバーの Management IPv6 Address がノード詳細画面に表示されません。

○ 同一デバイス間で複数のエリア仮想リンクを使用している時、一方の設定を削除した場合、リンクステータスは Active のままとなります。この時、もう一方のリンクのリンクステータスに Active と表示されるべきですが何も表示されません。これは表示上だけの問題であり通信に影響はありません。

○ AMF マスターに挿入したローカルメディア（USB メモリー）の空き容量が足りない状態で AMF バックアップを実行した場合に出力するエラーメッセージが正しい宛先を示していませんが動作に影響はありません。

○ LACP と AMF を併用している場合、LACP チャンネルグループのメンバーポートがリンクダウンすると、次のようなエラーログが出力されますが、これはログのみの問題で、AMF や通信には影響ありません。
kern.err XXXX kernel: Unexpected parent vlan4092 found for [IFNAME]
kern.err XXXX kernel: Parent interface vlan4092 found while deleting [IFNAME]

○ HA モード VRRP を使用する AMF メンバーと、AMF マスターとの間で AMF 仮想リンクが 1 本のみ設定されている（VRRP マスタールーターとバックアップルーターの共通 IP アドレスを AMF 仮想リンクの終端アドレスとして指定した）構成において、VRRP マスタールーターがダウンした場合、切り替え後の AMF メンバーで AMF のオートリカバリーができなくなることがあります。このような構成で AMF 仮想リンクを使用する場合は、VRRP を構成する各 AMF メンバーの LAN 側 IP アドレスを終端アドレスとして、AMF 仮想リンクを複数設定してください。

○ shutdown コマンドがいずれかのインターフェースに設定されている AMF マスターをリカバリーすると以下のログが出力されますが、通信に影響はありません。
NSM[1091]: port1.0.31 enabling failed :-45

○ AMF コントローラーとローカルマスターが別筐体で、かつ、同一エリアに存在する場合、ローカルマスターで atmf restricted-login コマンドを実行すると AT-Vista Manager のノードマップにおいて、同エリアの AMF ノードに対し SSH 接続ができません。

○ AMF と EPSR の併用時、AMF マスターと AMF メンバー間のリンクタイプを、AMF クロスリンクから AMF リンクに変更した後は、AMF マスターと AMF メンバーそれぞれでリンクタイプ設定を保存して再起動してください。ただし、AMF 経由で AMF マスターから AMF メンバーのリンクタイプを変更すると、その時点で AMF の接続が切れてしまうため、設定の保存と再起動が AMF マスターから行えません。そのため、本設定の変更を行う場合には、AMF 経由ではできませんので、コンソールや TELNET/SSH で接続して行ってください。

○ atmf backup bandwidth コマンドのオンラインヘルプにおいて、AMF バックアップデータの転送に使用する帯域を 0kbps に制限することができるようなヘルプメッセージが表示されます。実際には、値に 0 を指定した場合、atmf backup bandwidth コマンドを no 形式で実行したときと同様、AMF バックアップデータの転送に使用する帯域の制限が解除されます。

○ no atmf enable で AMF 機能を無効化しても、AMF 自動バックアップ機能が動作しようとします。バックアップファイルは保存されませんが、空のフォルダーが作成され、ログが出力されます。

6 マニュアルの補足

6.1 サポートする USB 型データ通信端末

サポートする USB 型データ通信端末につきましては、弊社ホームページでご確認ください。

6.2 サブスクリプションライセンス

参照「コマンドリファレンス」/「UTM」

サブスクリプションライセンスはファームウェアバージョン **5.4.5-1.1** 以降でのみご使用いただけます。

6.3 サポートする OpenVPN クライアント

参照「コマンドリファレンス」/「VPN」/「OpenVPN」

本バージョンでは、OpenVPN クライアントとして下記 OS/ アプリケーションの組み合わせをサポートします。

OS	アプリケーション
Windows7 (32bit)	OpenVPN GUI v5 (2.3.6)
	OpenVPN GUI v7 (2.3.7)
	OpenVPN GUI v7 (2.3.8)
	vpnux Client (ver.1.3.0.0)
Windows7 (64bit)	OpenVPN GUI v5 (2.3.6)
	OpenVPN GUI v7 (2.3.7)
	OpenVPN GUI v7 (2.3.8)
	vpnux Client (ver.1.3.0.0)
Windows8.1 (64bit)	OpenVPN GUI v5 (2.3.6)
	OpenVPN GUI v7 (2.3.7)
	OpenVPN GUI v7 (2.3.8)
	vpnux Client (ver.1.3.0.0)
Windows10 (64bit)	OpenVPN GUI v7 (2.3.8)
	vpnux Client (ver.1.3.0.0)
MAC OS X	Tunnelblick 3.4.3
	Tunnelblick 3.6 beta10
Android 4.4.x	OpenVPN for Android 0.6.29
	OpenVPN for Android 0.6.35
iOS 8	OpenVPN Connect 1.0.5

7　サポートリミット一覧

	AT-AR2050V	AT-AR3050S	AT-AR4050S
パフォーマンス			
VLAN 登録数	1000	4094	
MAC アドレス（FDB）登録数	1024		
IPv4 ホスト（ARP）登録数	1024		
IPv4 ルート			
IPv4 スタティックルート登録数	1000		
RIPv1/v2 ルート登録数	1500		
OSPFv2 ルート登録数	1000		
BGP4 ルート登録数	10000		
IPv6 ルート			
IPv6 スタティックルート登録数	1000		
RIPng ルート登録数	1500		
OSPFv3 ルート登録数	1000		
BGP4+ ルート登録数	10000		
リンクアグリゲーション			
グループ数（筐体あたり）	2※1		
ポート数（グループあたり）	4※2		
VPN			
IKEv1 同時接続可能セッション数	100※3		256※3
IKEv2 同時接続可能セッション数	100※3		256※3
L2TPv3 同時接続可能セッション数	256※3		
OpenVPN 同時接続可能セッション数	100※4		
PPPoE			
PPPoE 同時接続可能セッション数	20		
ローカル RADIUS サーバー ※5			
ユーザー登録数	5000		
RADIUS クライアント（NAS）登録数	1000		
ファイアウォール			
セッション数	65535		
ルール数	500※6		

※1 スタティックチャンネルグループと LACP チャンネルグループを合わせて 2 グループまでサポートします。
※2 LAN 側スイッチポートのみ使用可能です。
※3 共有するトンネルインターフェースの合計値です。
※4 vpnux Client（Windows 版）は 1 セッション、OpenVPN Connect（iOS 版）は 2 セッションまでをサポートします。
※5 OpenVPN でのみ使用可能です。
※6 ファイアウォールルールと NAT ルールを合わせて 500 ルールをサポートします。

8　最新マニュアルについて

最新の取扱説明書（613-002124 Rev.B）とコマンドリファレンス（613-002107 Rev.F）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、これらの最新マニュアルに対応した内容になっていますので、お手持ちのマニュアルが上記のものでない場合は、弊社ホームページで最新の情報をご覧ください。

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