613-001293 Rev.E 101028

CentreCOM® 9048XL リリースノート

この度は、CentreCOM 9048XL（以下、特に記載がないかぎり「本製品」と表記します）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　2.1.0

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 2.0.5 から 2.1.0 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　動作時温度 45℃対応

参照「取扱説明書」128 ページ
参照「コマンドリファレンス」/「運用・管理」/「システム」

動作時温度の上限値が 40℃から 45℃に変更されました。ファームウェアバージョン 2.1.0 以降で動作させる場合、本製品の動作時温度は 0 ～ 45℃となります。
ただし、以下の条件下では、2.1.0 以降も動作時温度は 0 ～ 40℃です。

○　垂直方向設置時

○　以下の SFP モジュール使用時

- AT-MG8T
- AT-SPLX40
- AT-SPZX80

これにともない、SET SYSTEM SFP-TEMPTHRESHOLDコマンドが追加され、SFPモジュール装着時には、内部温度の監視しきい値を環境条件にあわせて変更できるようになりました。
本コマンドのデフォルトは「40（上限 40℃環境用）」で、SFP モジュールを装着した時点でしきい値は「40」に設定されます。
水平方向設置時で、かつ上限 45℃環境で使用可能な SFP モジュールを装着したときは、設定を「45（上限 45℃環境用）」に変更してください。

本コマンドは、SFP モジュール装着時に限り有効です。SFP モジュールが何も装着されていないときは、本コマンドの設定に関係なく、しきい値は「45」になります。

内部温度がしきい値をまたいだときに SNMP トラップ、ログメッセージが出力されます。

2.2　CPU 使用率の表示

参照「コマンドリファレンス」/「運用・管理」/「システム」

SHOW CPU コマンドで CPU の使用率を表示できるようになりました。
過去 1 秒間、1 分間、5 分間、15 分間の CPU 平均使用率をパーセンテージ（%）で表します。
なお、CPU 使用率は SNMP 経由でも取得可能です。

2.3 SNMP：NEWADDRESS トラップ

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

プライベート MIB のうち、MAC アドレスの登録に関する MIB オブジェクトとトラップをサポートしました。学習機能により FDB に MAC アドレスが登録されたときにトラップが送出されるよう設定できます。
CREATE SNMP COMMUNITY コマンドによる SNMP コミュニティー作成時に TRAP パラメーターで NEWADDRESS を指定します。該当コミュニティーでトラップの生成を有効にするには、ENABLE SNMP COMMUNITY TRAP コマンドを使用します。

2.4 100BASE-FX(LC) SFP モジュール AT-SPFX/2、AT-SPFX/15

参照「コマンドリファレンス」/「スイッチング」

100BASE-FX(LC) SFP モジュール AT-SPFX/2（最長 2km）と AT-SPFX/15（最長 15km）をサポートしました。

2.5 ループガード：受信レート検出のフレーム種別設定

参照「コマンドリファレンス」/「スイッチング」

受信レート検出の対象フレームに、ブロードキャストまたはマルチキャストを個別に指定できるようになりました。
SET SWITCH STORMDETECTION コマンドの FRAMETYPE パラメーターでブロードキャストかマルチキャストかを選択し、FRAMESIZE パラメーターで対象フレームの平均フレームサイズを指定します。

2.6 DHCP Snooping

参照「コマンドリファレンス」/「スイッチング」/「DHCP Snooping」

DHCP サーバー・クライアント間でやりとりされる DHCP メッセージを監視して動的な IP ソースフィルタリングを行う DHCP Snooping をサポートしました。
本機能を利用すれば、DHCP サーバーを用いたネットワーク環境において、正当な DHCP クライアントにだけ IP 通信を許可することができます。
詳細はコマンドリファレンス「DHCP Snooping」を参照してください。

2.7 ハードウェアパケットフィルター

参照「コマンドリファレンス」/「ハードウェアパケットフィルター」
参照「コマンドリファレンス」/「クラシファイア」

ハードウェアレベルで入力パケットをフィルタリング（許可・拒否）するハードウェアパケットフィルター（アクセスコントロールリスト）をサポートしました。
フィルタリング条件は、汎用のパケットフィルターであるクラシファイアによって定義します。
詳細はコマンドリファレンス「ハードウェアパケットフィルター」および「クラシファイア」を参照してください。

2.8 ポート認証の機能拡張

参照「コマンドリファレンス」/「ポート認証」

ポート認証機能を以下のとおり拡張しました。

○ IEEE 802.1X-2004 準拠モードに対応し、802.1X 認証で使用する EAPOL のバージョンを選択できるようになりました。
SET PORTAUTH PORT コマンドの EAPOLVERSION パラメーターで 1 を指定すると 802.1X-2001 準拠モード、2 を指定すると 802.1X-2004 準拠モードになります。デフォルトは 1 です。

○ Supplicant の認証成功時、認証失敗時、ログオフ時にログメッセージを出力する認証ログ機能をサポートしました。どの認証方式でどのログメッセージを出力するかを任意に指定できます。
ENABLE/DISABLE PORTAUTH PORT LOGTYPE コマンドで機能の有効・無効を設定します。デフォルトは有効です。

○ RADIUS Access-Request パケット、Accounting-Request パケットに含まれる Calling-Station-Id/Called-Station-Id 属性の MAC アドレスの形式を変更できるようになりました。
SET PORTAUTH CSIDFORMAT コマンドで、MAC アドレスにハイフン、コロン、ピリオドのいずれかを含めるかどうか、含める場合の挿入間隔、MAC アドレス中の 16 進数 a ～ f を大文字・小文字のどちらで表すかを設定できます。デフォルトは「00-00-F4-11-22-33」の形式（2 個おきにハイフン、a ～ f は大文字）です。

○ MAC ベース認証において RADIUS サーバーに認証を要求するときのユーザー名・パスワードの形式を変更できるようになりました。
SET PORTAUTH USERIDFORMAT コマンドで、MAC アドレスにハイフン、コロン、ピリオドのいずれかを含めるかどうか、含める場合の挿入間隔、MAC アドレス中の 16 進数 a ～ f を大文字・小文字のどちらで表すかを設定できます。デフォルトは「00-00-f4-11-22-33」の形式（2 個おきにハイフン、a ～ f は小文字）です。

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 2.0.5 から 2.1.0 へのバージョンアップにおいて、以下の仕様変更が行われました。

3.1 ループガード：タグ付きポートへの LDF 検出有効設定

参照 「コマンドリファレンス」/「スイッチング」

ENABLE SWITCH LOOPDETECTION コマンドで、タグ付きポートに対して LDF 検出機能を有効に設定できるようになりました。ただし、LDF の送出と検出はタグなしパケットで行われますので、タグ付きポートで LDF 検出機能を有効にする場合は、タグなしポートとしても VLAN に所属させるようにしてください。

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 2.0.5 から 2.1.0 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 日付と時刻の設定時にリアルタイムクロックへのアクセスに失敗すると、本製品がリブートすることがありましたが、これを修正しました。

4.2 SHOW LOG コマンドに DATE、TIME、SEVERITY パラメーターを指定して、繰り返しコマンドを実行していると、メモリーが枯渇し、SNMP のアクセスに対して応答できなくなることがありましたが、これを修正しました。

4.3 RADIUS アカウンティング機能において、コンソール（user-1）と Telnet（user-2）のような 2 ユーザーのログイン認証が行われたときに、Accounting-Interim-Update パケットが、後から認証された 1 ユーザー分しか送出されませんでしたが、これを修正しました。

4.4 RADIUS アカウンティング機能において、Accounting-Interim-Update パケットの送信が有効に設定されていても、1 ～ 3 パケット送信後に送信が停止していましたが、これを修正しました。
また、Accounting-Interim-Update パケットの送信後に本製品からログアウトをすると、Stop 属性の Accounting-Request パケットが送信されない場合がありましたが、これを修正しました。

4.5 CREATE SWITCH TRUNK コマンドの PORT パラメーターで、FDB にダイナミックエントリーが登録されている状態のポートを指定してトランクグループを作成すると、該当ポートのエントリーが消去されませんでしたが、これを修正しました。

4.6 ポートトランキングと IGMP Snooping 併用時、複数のトランクグループがあると、DVMRP パケット受信時に最初に作成したトランクグループ以外のグループでポートトランキングが機能せず、グループ内のすべてのポートに DVMRP パケットがフラッディングされていましたが、これを修正しました。

4.7 SET SWITCH PORT コマンドの SECURITYMODE パラメーターでポートセキュリティーを SECURED に設定する際に、対象ポートとして、INTRUSIONACTION が DISABLE に設定されているポートと、INTRUSIONACTION が DISABLE 以外に設定されているポートが混在していると、INTRUSIONACTION=DISABLE の設定が動作しませんでしたが、これを修正しました。

4.8 ループガードの受信レート検出（STORMDETECTION）有効時、検出時のアクションとしてポートのリンクダウンが頻繁に発生している状態で、ポートの通信モードを変更すると、通信不可になることがありましたが、これを修正しました。

4.9 トランクポートに対して DISABLE SWITCH PORT AUTOMDI コマンドを実行すると、不正なエラーメッセージが表示されていましたが、正しいエラーメッセージが表示されるよう修正しました。

4.10 ポート認証のマルチプルダイナミック VLAN（VLANASSIGNMENTTYPE=USER 設定）で認証が行われたあと、ポート認証の機能を無効に設定しても、アサインされた VLAN に登録されている本体 MAC アドレスを持つエントリーが FDB から削除されませんでしたが、これを修正しました。

4.11 ポート認証有効時に、Telnet 経由で SHOW DEBUG コマンドを実行すると、まれに本製品がリブートすることがありましたが、これを修正しました。

4.12 ポート認証の 802.1X Authenticator ポートにおいて、所属 VLAN がダイナミック VLAN によってアサインされている状態で Supplicant の再認証を行うと、認証に成功しても Authenticator ポートの状態が待機中（Held）になることがありましたが、これを修正しました。

4.13 ポート認証において、Supplicant の認証に成功したポートに対して、認証方式を変更するなど認証が解除される操作を行っても、Stop 属性の Accounting-Request パケットが送信されませんでしたが、これを修正しました。

4.14 ポート認証において、複数の Supplicant の認証を実施しているポートに対して、SET PORTAUTH PORT コマンドの TYPE パラメーターに NONE を指定して、ポート認証を無効にしても、Stop 属性の Accounting-Request パケットが 1 つの Supplicant 分しか送信されませんでしたが、これを修正しました。

4.15 RSTP において、6 台以上のスイッチによるリング構成時に、スイッチ間のリンクダウンから通信復旧まで約 30 秒の時間がかかっていましたが、これを修正しました。

4.16 Web GUI の Multiple STP において、1 つの MST インスタンスに対して多数の VLAN を関連付ける設定を行うと、CIST/MSTP インスタンス一覧画面で一部の VID が正しく表示されないことがありましたが、これを修正しました。

4.17 Web GUIで、すでに存在するVLAN IDを別のVLAN名で追加する操作を行うと、エラーメッセージが表示されるにもかかわらず、該当 VLAN が削除されていましたが、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 2.1.0 には、以下の制限事項があります。

5.1 SNMP

参照 「コマンドリファレンス」/「運用・管理」/「SNMP」

SNMP マネージャーのタイムアウトによって、同時に 5 個以上の SNMP マネージャーから ifEntry を Get できない場合があります。SNMP マネージャーのタイムアウト値を長く設定するようにしてください。

5.2 RADIUS サーバー

参照 「コマンドリファレンス」/「運用・管理」/「認証サーバー」

○ 802.1X 認証有効時、SET RADIUS コマンドの DEAD-ACTION パラメーターで PERMIT を設定しても、RADIUS サーバーからの応答がないときに、通信ができなくなる場合があります。

○ RADIUS アカウンティング機能有効時に、RADIUS サーバーから Access-Reject パケットを受信すると、本製品から Failed 属性が付加された Accounting-Request パケットが送信されます。

5.3 IP

参照 「コマンドリファレンス」/「IP」

ICMP エコー要求（Ping）パケットを受信したとき、応答に 20 ミリ秒程度かかる場合がありますが、これは正常動作です。

5.4 スイッチング

参照 「コマンドリファレンス」/「スイッチング」

○ スイッチポートの通信速度を変更するとリンクダウン・リンクアップが発生しますが、複数のポートを指定して、AUTONEGOTIATE、10MHAUTO、10MFAUTO、100MHAUTO、100MFAUTO、10-100MAUTO のいずれかに設定を変更した場合、link-down、link-up メッセージが表示されないポートがあります。

○ 100Mbps 光ポート（SFP ポート）では、Jumbo フレームのフレーム長は 9000Byte 以下のサポートとなります。

○ AUTONEGOTIATE でリンクしている 1000Mbps 光ポート（SFP ポート）に対して、通信モードを 1000MFULL に変更すると、リンクダウンするのが正しい動作ですが、いったんリンクダウンしたあと再度リンクアップすることがあります。

○ 100Mbps 光ポート（SFP ポート）において、ミッシングリンク機能がない（または無効に設定されている）メディアコンバーターを経由して通信を行ったあと、本製品を再起動すると起動時にエラーが発生し、通信不可の状態になります。

5.5 ポートトランキング

参照「コマンドリファレンス」/「スイッチング」

トランクグループを以下のいずれかの条件で複数作成し、512 個以上の MAC アドレスが使用される通信が発生している状態で、トランクポートの追加と削除を繰り返し実施すると、本製品がリブートすることがあります。

- トランクグループの所属ポートに 512 個以上のスイッチフィルターが登録されている
- トランクポートの通信モードがポート本来の通信モードと異なる設定になっている

5.6 IGMP Snooping

参照「コマンドリファレンス」/「IGMP Snooping」

○ IGMP Snooping 有効時、IGMP パケットの通信中にグループの所属 VLAN を変更すると、IGMP Snooping 用のテーブルから変更前の VLAN 情報が削除されません。

○ IGMP Snooping 有効時、メンバーが存在するポートをミラーポートに設定しても、IGMP Snooping 用のテーブルから該当ポートの情報が削除されません。

○ IGMP Snooping と、EPSR アウェアまたはスパニングツリープロトコル併用時、経路の切り替えが発生したときにマルチキャストグループの登録がクリアされないため、切り替え前に登録されたルーターポートが残ったままになります。
なお、EPSR アウェアについては、CREATE EPSR コマンドの DELETEMCAST オプションで、リングトポロジーチェンジ発生時にマルチキャストグループのエントリーを FDB から削除する設定が可能です。

5.7 IGMP Snooping/MLD Snooping

参照「コマンドリファレンス」/「IGMP Snooping」
参照「コマンドリファレンス」/「MLD Snooping」

ポートトランキングと IGMP Snooping または MLD Snooping の併用時、トランクグループ内で最も番号の小さいポートを DISABLE SWITCH PORT コマンドで無効に設定すると、トランクグループ内のそれ以外のポートでマルチキャストデータが転送されなくなります。
ただし、DISABLE SWITCH PORT コマンド実行時に LINK=DISABLE を指定して、該当ポートを物理的にリンクダウンさせると、本現象は発生しません。

5.8 スパニングツリー

参照「コマンドリファレンス」/「スパニングツリープロトコル」

本製品の実装では、トポロジーチェンジ発生時にエッジポートに設定されたポートの FDB が消去されます。

5.9 Web GUI

参照 「コマンドリファレンス」/「Web GUI」

Web GUI でマルチプル VLAN(Protected Port 版) のポート設定を行う際、グループ番号の設定変更とタグなし / タグ付きの設定変更を同時に行うことができますが、個別に変更するようにしてください。
グループ番号の変更とタグなし→タグ付きの変更を同時に行った場合、該当ポートがタグなしとしてデフォルト VLAN にも追加されます。

6 取扱説明書の補足・誤記訂正

同梱の取扱説明書の誤記訂正です。

6.1 トリガーエントリーの作成

参照 「取扱説明書」85 ページ

取扱説明書の 85 ページ「トリガーエントリーの作成」において、CREATE TRIGGER コマンドの ENDTIME と STARTDATE パラメーターの説明に一部誤りがありましたので、下記のとおり訂正して、お詫びいたします。

○ ENDTIME

誤：
ENDTIME の指定を省略すると、トリガーは起動したまま終了しません（解除をしないかぎりパワーセーブモードが継続します）。

正：
ENDTIME の指定を省略すると、トリガーは起動したまま翌日になるまで終了しません。

○ STARTDATE

誤：
ENDDATE と ENDTIME の指定を省略すると、トリガーは起動したまま終了しません（解除をしないかぎりパワーセーブモードが継続します）。

正：
ENDDATE と ENDTIME の指定を省略すると、トリガーは起動したまま翌日になるまで終了しません。

7 未サポートコマンド（機能）

以下のコマンド（パラメーター）はサポート対象外ですので、あらかじめご了承ください。

SET HTTP SERVER PORT
SET SYSTEM LANG
RESET PORTAUTH PORT
LOAD METHOD=TFTP FILE=filename SERVER=ipadd BOOT
SET IGMPSNOOPING HOSTSTATUS
SET MLDSNOOPING HOSTSTATUS
SHOW DHCPSNOOPING NVS
SHOW DHCPSNOOPING HWFILTER

8　コマンドリファレンスについて

コマンドリファレンス「CentreCOM 9048XL コマンドリファレンス 2.1.0（613-001280 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、あわせてご覧ください。

コマンドリファレンスのパーツナンバー「613-001280 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/