AX シリーズ
ネットワークパーティション ソリューションガイド
[応用編]

初 版

はじめに

AX シリーズ ネットワークパーティション ソリューションガイド[応用編]は、AX6700S、AX6600S、AX6300S の各シリーズでサポートしているネットワークパーティションを利用したシステム構築のための応用技術情報をシステムエンジニアの方へ提供し、システムの提案から構築およびその安定稼動のための一助を目的として書かれています。

関連資料

・AX シリーズ ネットワークパーティション ソリューションガイド［基本編］
・AX シリーズ ネットワークパーティション ソリューションガイド［認証編］
・AXシリーズ製品マニュアル（ http://www.alaxala.com/jp/techinfo/manual/index.html ）

本資料使用上の注意事項

本資料に記載の内容は、弊社が特定の環境において基本動作を確認したものであり、機能・性能・信頼性についてあらゆる環境条件すべてにおいて保証するものではありません。弊社製品を用いたシステム構築の一助としていただくためのものとご理解いただけますようお願いいたします。

本資料作成時の OS ソフトウェアバージョンは特記の無い限り以下となっております。

AX6700S , AX6600S , AX6300S	Ver11.1	(OP-NPAR ライセンス有)
AX3600S , AX2400S	Ver11.1.A	

本資料の内容は、改良のため予告なく変更する場合があります。

輸出時の注意

本資料を輸出される場合には、外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。

商標一覧

・アラクサラの名称およびロゴマークは、アラクサラネットワークス株式会社の商標および商標登録です。
・Ethernetは、米国Xerox Corp.の商品名称です。
・イーサネットは、富士ゼロックス(株)の商品名称です。
・そのほかの記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

目次

1. ネットワークパーティションの適用シーン

1.1 ネットワークパーティションの導入契機

これまで「**AX シリーズ ネットワークパーティション ソリューションガイド[基本編]、[認証編]**」で紹介の通り、ネットワークパーティションとは、最小限の物理構成で論理的に独立した複数のネットワークを収容できるシステムソリューションです。その特長や利点から、アラクサラではネットワークパーティションを実際のシステムとしてお勧めできるシーンとして大きく 3 通りのケースを想定しています。

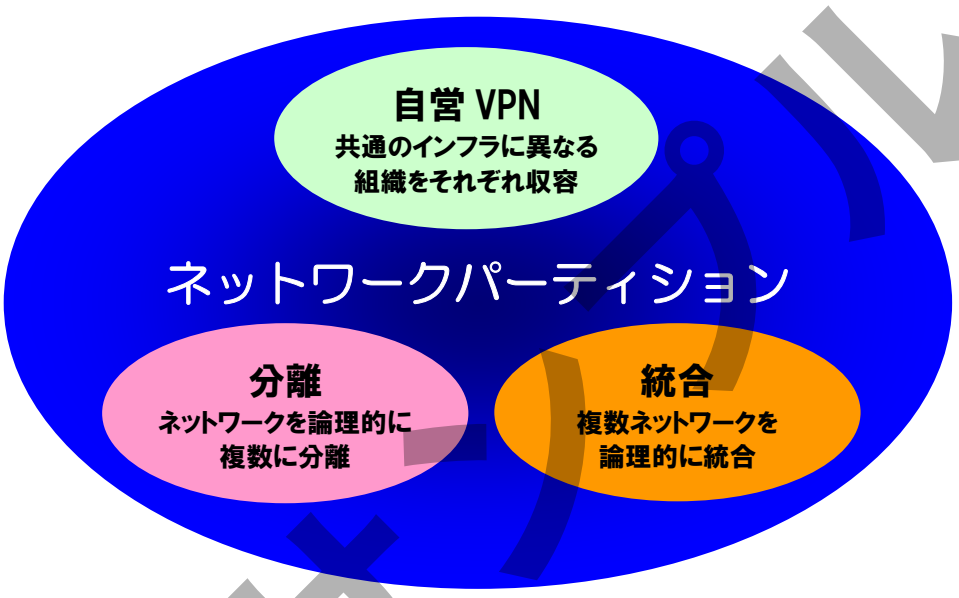


図 1.1-1 ネットワークパーティションをお勧めする 3 つのシーン

●自営 VPN

インフラとしてはひとつとしたいが、その利用ユーザーが独立した個別組織である場合など、接続対象それぞれを VPN ライクに収容するようなシステムを構成したい場合です。

●分離

現在あるネットワークを複数の小さなネットワークに分割する場合や、一部分を独立した別のセグメントとして切り出したい場合などです。

●統合

物理的に独立している複数のネットワークを共通のインフラ上に統合して構成する場合です。

以下、各シーン別に解説していきます。

1.2 自営 VPN としてのネットワークパーティション

新規に構築するネットワークシステムの要件として、複数ある組織ごとにネットワークを持つ必要がある、もしくは持たせたいが、それらを共通のインフラの上に構築したい、それぞれのネットワーク全てについて管理する必要がある、などといった場合、ネットワークパーティションによるシステム構成をお勧めできます。

このような要件に対し従来からある技術として MPLS-VPN などによる方式もありますが、高価な専用の機器が必要であったり、設定が複雑などという点で、ネットワークパーティションの方が導入に対するしきいも低く訴求力のある方式と考えます。

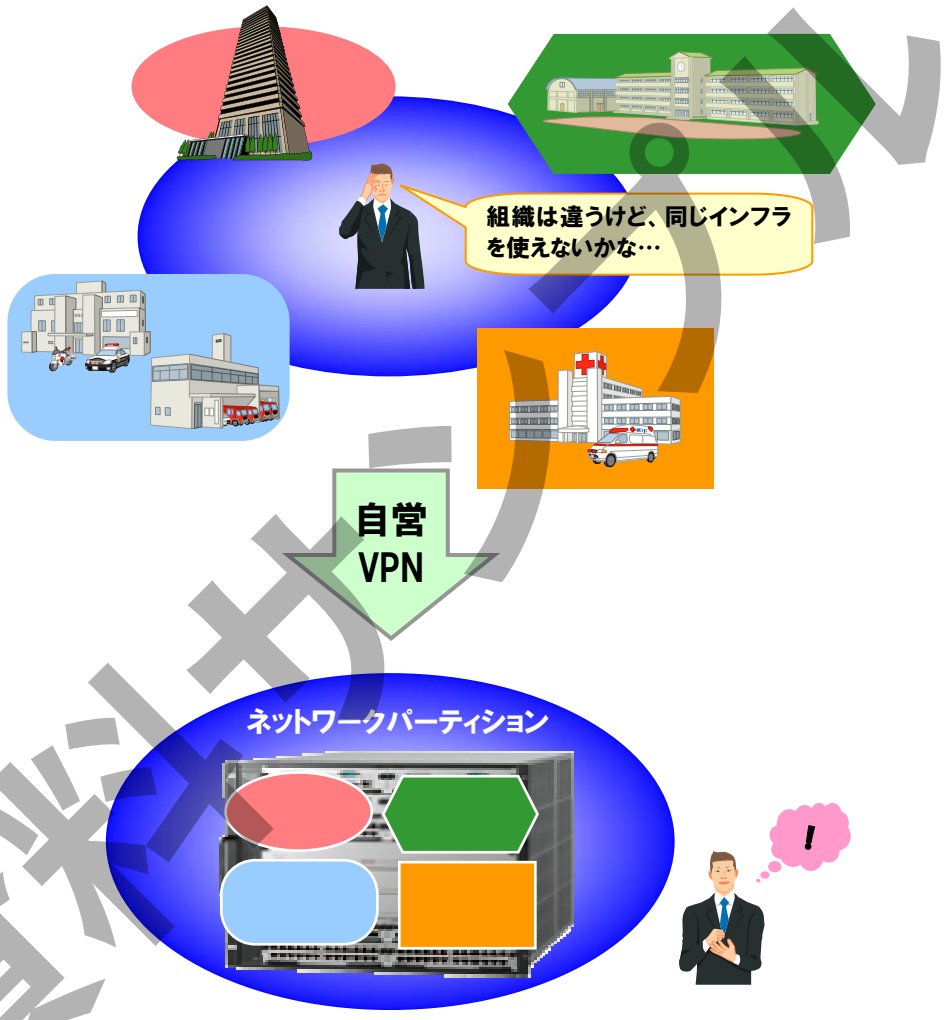


図 1.2-1 自営 VPN としての利用イメージ

このようなシステムを構成するケースでは、新規の導入を前提としてシステムを考えることが多いため、事前にシステムや装置の収容条件を考慮したシステム設計ができ大きな問題などは発生しにくいと思われますが、ポイントとしては運用や管理責任の境界点を明確にすることでしょう。システム全体を取りまとめる組織と各ネットワーク利用組織の間において決定する境界点によって、運用/管理の範囲も決まります。

1.3 ネットワークの分離

組織の拡大などに伴う管理単位の変更や組織間のセキュリティ強化を考える場合、既存のネットワークシステムから一部分を分離したいとか、複数のグループに分割したいといった要求があると思います。そういった際にネットワークパーティションの持つ論理ネットワークによるシステム構成はお勧めです。

装置の追加、拡張といった物理的リソースへの影響を最小限にとどめながら、論理的に分離されたネットワークシステムの構築ができることはもちろん、設定によって論理ネットワークの追加等が容易におこなえるため、段階を踏んでのシステム移行にも柔軟に対応できます。

図 1.3-1 ネットワークの分離イメージ

ネットワーク分離でのポイントは、ひとつは分離前後でユーザーの環境を維持できるかです。例えば使用しているサーバや端末に設定してあるアドレスの設定を変えないで済むかなど、理想的にはユーザーにシステムの変更が見えないことです。

もうひとつは分離したそれぞれのネットワークの独立性がきちんと保たれることです。ネットワークを分離してもユーザー側で互いのネットワークが筒抜けになってしまっては意味がありません。場合によってはネットワーク認証を組み合わせるなど、エンドユーザーまで含めて使用できる範囲をしっかり分離することです。

そしてさらにシステムの移行がスムーズにおこなえるか、です。ネットワークの分離に関しては、稼働中の大きなネットワークを段階的に分離対象のネットワーク単位に一部ずつ切り出していくケースが現実的と思われますが、この際に極端なサービスの低下(長期に渡るシステムダウンが無い等)無しに、システムの移行ができることが重要です。

1.4 ネットワークの統合

導入するハードウエア、運用、管理などのコストの低減を図る技術として注目されるシステムの仮想化ですが、その基本となるのはシステムの統合と言えるでしょう。ネットワークシステムについても考え方は同様であり、組織間で全く独立しているネットワークシステムのネットワークパーティションの導入による統合は運用、管理の負荷やコストを抑えるのに適したソリューションといえます。このようなシステムの統合は、例えば複数の組織が同じ建屋やフロアに入る場合などが想定されます。

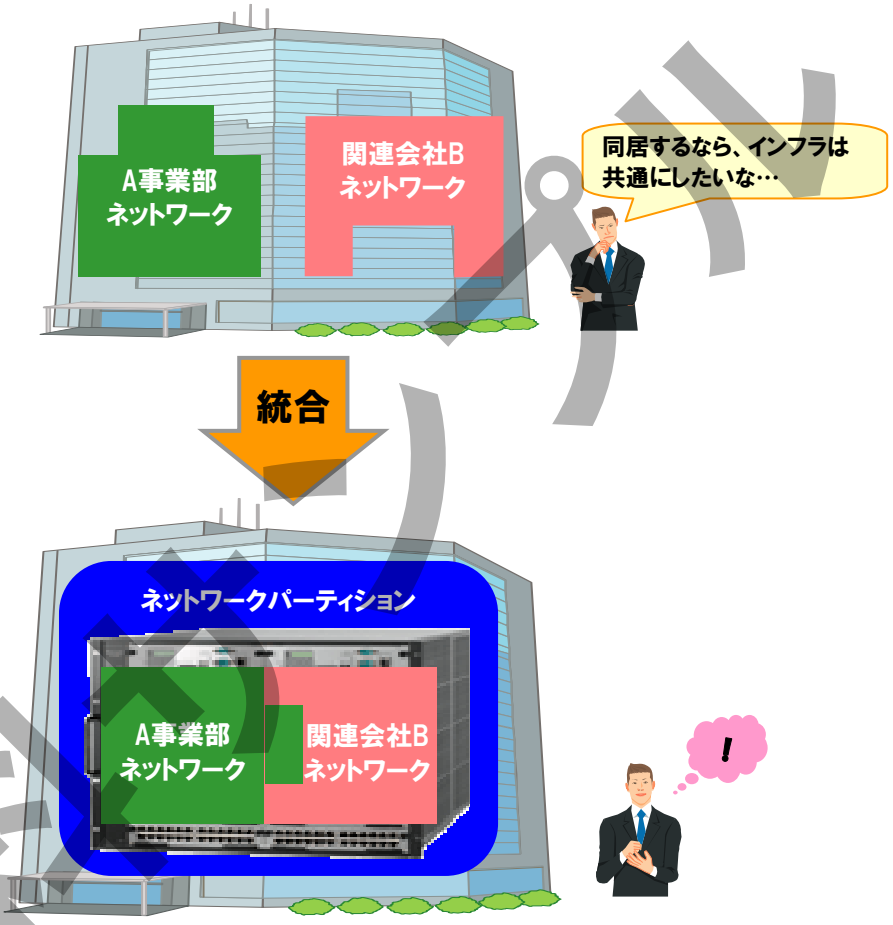


図 1.4-1 ネットワークの統合イメージ

ネットワークの統合でも、統合前後でユーザーの環境を維持できるかはポイントのひとつです。システムの変更による影響がエンドユーザーに及ばないことが理想となります。また、ネットワークを統合するということは、要求される転送能力や収容条件などシステムに必要なネットワークリソースも増えるということになります。ネットワークパーティションによってシステム統合を考える場合は、要求されるネットワークリソースも満足しているかを事前によく検討しておくことです。

2. ネットワークパーティション導入のキーポイント

ここでは、ネットワークパーティションによるネットワークシステムの構築において、一般のネットワークシステムと異なる点など、システム設計にあたり押さえておくべきポイントを解説します。

2.1 VLAN の扱い

ネットワークパーティションは VRF 機能によるレイヤ 3 の論理分割と、VLAN によるレイヤ 2 の論理分割を主体として論理ネットワークを構成します。ですが VLAN に関しては指定可能な VLAN 数が論理ネットワーク数分増える訳ではありません。

このため VLAN を扱うことのできる L2 スイッチであれば、装置としてはネットワークパーティションによる論理ネットワークを意識せずにシステム内で利用できますが、システム設計においてはこのことを十分に理解の上、論理ネットワークとそこで使用される VLAN の対応づけを十分に把握しておく必要があります。

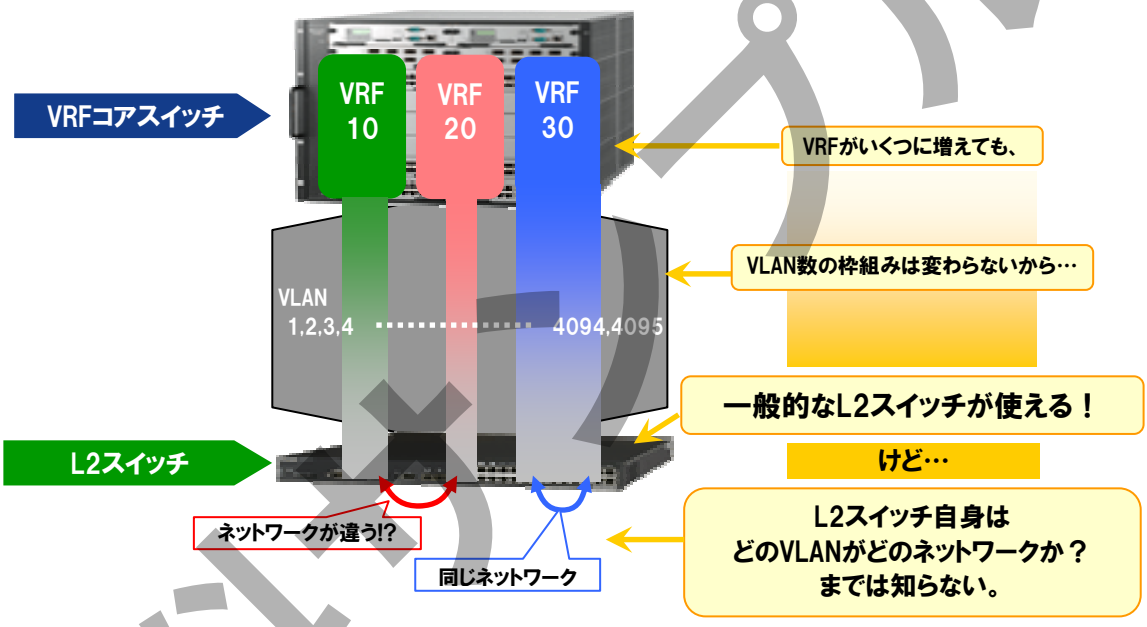


図 2.1-1 ネットワークパーティションでの VLAN

以下にこれらが関連することによる主なポイントを示します。

(1) ディストリビューション、アクセススイッチに VRF 機能なしの L3 スイッチを使う場合

一般のネットワークの場合 VLAN の境界はサブネットの境界でしたが、ネットワークパーティションによるシステムの場合、VLAN の境界がネットワークの境界である場合があります。このため VRF 機能の無い L3 スイッチでディストリビューション/アクセススイッチとして L2 スイッチ的に利用する場合などは VLAN 間の中継やルーティングなどで不要なネットワーク間通信がおこなわれないように注意が必要です。

(2) スイッチ自身が通信をおこなう場合

認証スイッチとして機能する際の RADIUS に関する通信や、syslog, telnet といった装置の運用および管理をおこなう場合などスイッチ自身が通信のエンドポイントになる場合ですが、スイッチ自体はひとつのネットワーク内にあることを前提にしている事が一般的(例えばデフォルトゲートウェイの設定や VLAN への IP アドレス設定など)なため、これらスイッチ内で複数のネットワークを収容するような場合には目的の通信が可能であるか、機能に制限がされないかなどの注意が必要です。

2.2 共用ネットワークと IP アドレス割当ての重複

ネットワークパーティションで構成される論理ネットワーク間では、IP アドレスの設定に関して相互干渉がないため相互で同じ IP アドレスを付与することが可能です。

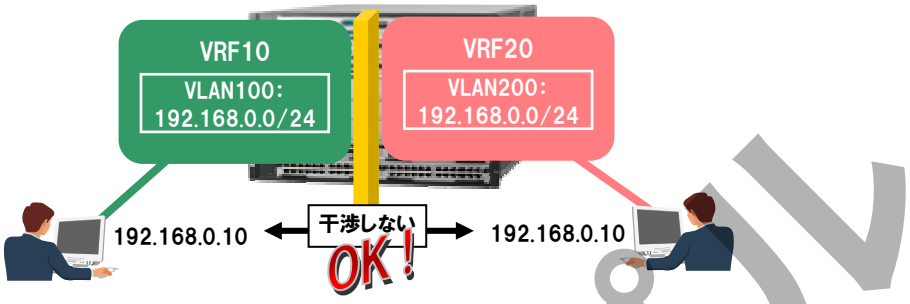


図 2.2-1 IP アドレスの重複 OK！

ただしエクストラネットを利用して VRF 間の通信をおこなう場合、その双方の VRF で同じ IP アドレスがあるとそれぞれを区別する手段がありません。また、共用ネットワークを構成する場合でも共用ネットワークと通信が可能なパーティションのネットワークそれぞれで同じ IP アドレスを使用していると、共用ネットワークからはどちらかのパーティションの IP アドレスしか認識できません。従ってエクストラネットを使用する場合や共用ネットワークを構成する場合はパーティション間で同じ IP アドレスを使用することは禁止となります。

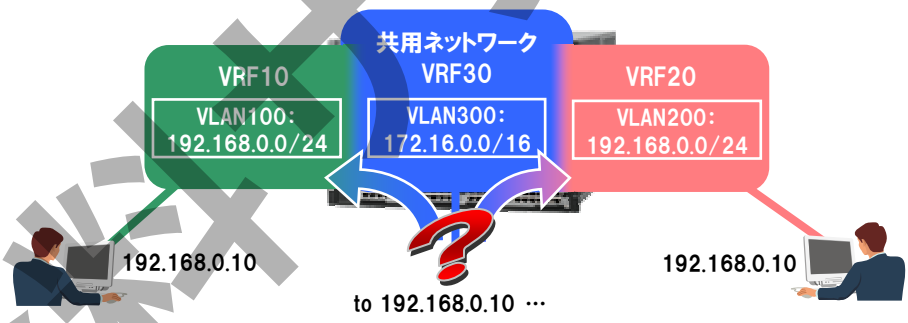


図 2.2-2 共用ネットワーク使用時は IP アドレス重複 NG！

2.3 ネットワーク認証機能の利用

「AX シリーズ ネットワークパーティション ソリューションガイド[認証編]」でもご紹介のとおり、ネットワークパーティションのシステムにおいてもネットワーク認証機能を利用することが可能です。

その認証機能を使ったシステム構成として、認証スイッチをひとつの論理ネットワーク内に収まるように使用する場合は一般的な使用法と同様ですが、一台の認証スイッチで複数のネットワークを扱う(VLAN ごとに所属しているネットワークが異なる)場合は下記のような押さえておくべきポイントがあります。

(1) IP アドレス重複の禁止

認証スイッチ内で使用する VLAN には IP アドレスを付与する必要がありますが、同一のスイッチ内では異なる VLAN に同じ IP アドレスは設定できません。

(2) RADIUS の使用について

同一の認証スイッチで複数ネットワーク分それぞれの RADIUS サーバをそれぞれ参照するということはできません。同一の認証スイッチで複数ネットワークを扱う場合は、参照する RADIUS サーバは複数ネットワーク分の認証情報を統合した構成としてください。

(3) 動的 VLAN 機能の有効利用

AX シリーズの認証スイッチの持つ動的 VLAN 機能をネットワークパーティションと組み合わせることにより、認証前後の環境をネットワーク単位で切替えることができます。またこの際の DHCP についても DHCP サーバを各論理ネットワークごとに独立して扱うことが可能です。

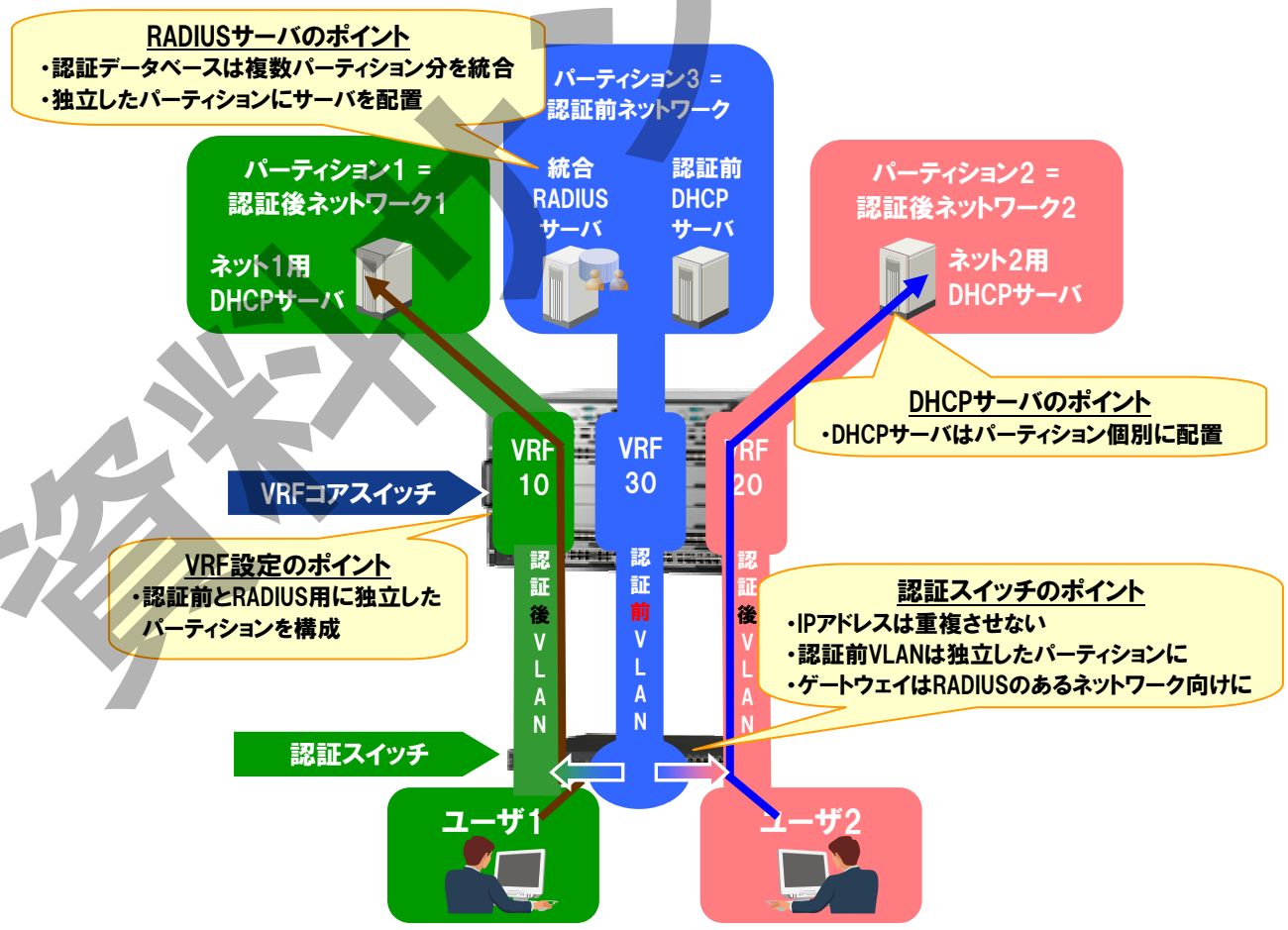


図 2.3-1 複数ネットワークを 1 台の認証スイッチで扱う推奨構成

2.4 運用管理とグローバルネットワーク

ネットワークパーティションにおいて、VRF 機能を使用する装置では運用および管理に利用する主だった機能はグローバルネットワーク上で動作させることを目的としています。(一部の機能はグローバルネットワーク以外の VRF(パーティション)によるネットワーク上でも利用可能です。詳細は下表を参照ください。)

表 2.4-1 VRF 装置の運用管理機能の動作対応

運用に関する機能		動作対応		備考
		グローバルネットワーク	グローバルネットワーク以外の VRF	
一般の運用機能	show コマンド	○	○	
	ping	○	○	
	traceroute	○	○	
	telnet コマンド	○	○	
	telnet サーバ	○	ー	
	ssh コマンド	○	ー	
	ssh サーバ	○	ー	
	ftp コマンド	○	ー	
	ftp サーバ	○	ー	
SNMP	エージェント	○	○	
	MIB/Trap	○	○	・取得可能な情報は装置単位 ・VRF 対応プライベート MIB(IP,ARP,経路)
syslog	メッセージ送信	○	ー	

動作対応： ○：動作可能 ー：動作非対応

VRF 装置以外の一般のスイッチに関しては、グローバルネットワーク上でも各論理ネットワーク上でも一般のネットワーク上と同様に運用および管理に関するコマンドや機能を使用できます。

従って、VRF 装置を含めたシステム全体を運用および管理するには、グローバルネットワークを利用しその適用範囲を調整する必要があります。

ネットワークパーティションの各論理ネットワーク毎にそれぞれ運用管理をおこなう場合は、VRF 装置の運用管理機能に制限(SNMP や ping,traceroute といった監視系のみ(上表参照)。)がある以外は一般のネットワーク同様に運用および管理をおこなうことが可能です。

2.5 リソースの分配

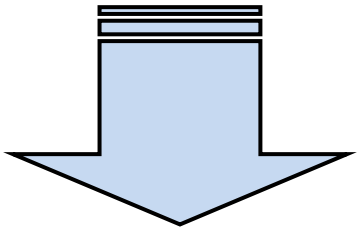
ネットワークパーティションでは論理的に複数のネットワークを収容可能ですが、物理的にはそのコアとなる装置は単体の装置であることは変わりません。従って各論理ネットワークでの通信に必要なリソースはその装置の持つリソースを分け合って使用することとなります。例えば、パケットやフレームの転送能力や CPU の処理能力などは各論理ネットワークで必要に応じて分け合うこととなります。ただし IP 経路や ARP テーブルなどに関してはパーティション毎に使用数の制限などが可能です。(下表参照)

表 2.5-1 論理ネットワーク毎に制限可能なリソースと実行コマンド

制限対象	使用コマンド	制限の単位	備考
MAC アドレステーブル学習数	`mac-address-table limit`	VLAN 毎	
ARP テーブル登録数	`arp-limit`	VRF 毎	
IP 経路数	`maximum routes`	VRF 毎	警告のみも可
IGMP グループ数	`ip igmp group-limit`	VRF 毎	
IGMP 合計ソース数	`ip igmp source-limit`	VRF 毎	
PIM-SM/SSM マルチキャスト中継エントリとネガティブキャッシュエントリの合計数	`ip pim mcache-limit`	VRF 毎	
PIM-SM/SSM マルチキャストルーティングエントリ数	`ip pim mroute-limit`	VRF 毎	

このため、特にネットワークの統合などにおいては、統合後に予想される通信に必要なリソースの使用量(統合前各ネットワークの使用リソースの合計)が、装置あたりの収容条件や収容能力を超えてしまわないよう注意が必要です。

気になる続きは…



・アラクサラ　インテグレータ会員

または

・ビジネスパートナー様会員

にご登録いただければ、全てをご覧いただけます！

アラクサラ インテグレータ会員またはビジネスパートナー様会員へ登録することで、アラクサラ製品のご利用にあたり役立つ各種資料(システム構築ガイドなど)を全て閲覧することができます。ぜひこの機会にご登録下さい。

アラクサラネットワークス株式会社

〒212-0058
川崎市幸区鹿島田一丁目１番２号 新川崎三井ビル西棟
http://www.alaxala.com/