船内 LAN システムにて
使用される技術解説

船内 LAN にて使用される基本的な技術を解説いたします。

株式会社 東北電技工業

1. VLAN (Virtual LAN)

VLAN の目的とは？

VLAN の使用目的は、「ネットワークを任意に分割する」ことです。

一般的なスイッチ／ハブでは、全体が1つのネットワークとなるため、例えば 64 ポートのスイッチ１台で構成されていた部門内ネットワークを2つのサブネットに分割しようとすると、64 ポートのスイッチを撤去して 32 ポートのスイッチ 2 台に置き換えることになりますが、運用上の変更が生じた場合、LAN ケーブル配線のやり直しになり柔軟な運用ができません。

VLAN は、スイッチの分割をスイッチ内部で仮想的に実現することで、ネットワーク分割の作業と物理的な接続状況とを分離することで、ネットワーク構成に柔軟性をもたらすことができます。 ネットワーク分割のメリットは、ネットワーク混雑の回避にとどまらず、ネットワーク利用法やセキュリティレベルの違いなどに応じて、また、ネットワーク特定の部分ににみ特定の運用ポリシーを適用する、といった場合にも、ネットワーク分割が必要となります。

分割したネットワーク間は、標準的なルーティング機構を用いて相互接続できるので、ネットワーク管理の観点からも特別な要素が増えるわけではありません。

VLAN のネットワーク分離の機能は、

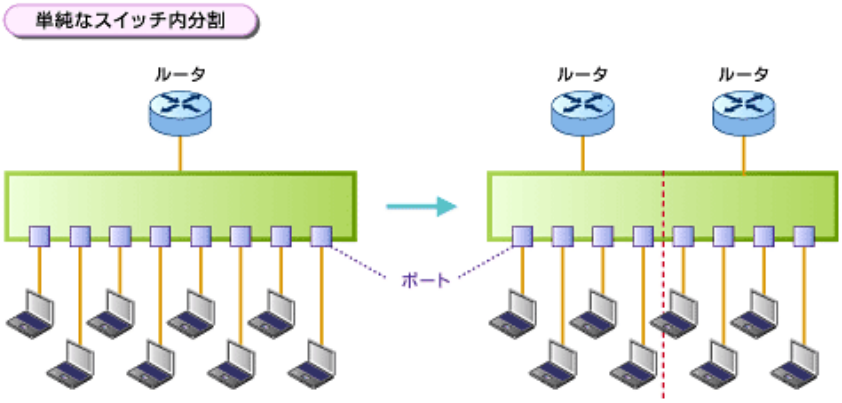
- ･VoIP サービスのためにネットワークに QoS に基づく優先度のレベル分けを導入する。
- ･セキュリティを向上させパケット盗聴の可能性を大幅に低減する。
- ･ユーザーが接続する場所を移動しても常に同じ環境にアクセスできるようにする。

といった最近需要がたかまりつつある、さまざまな用途を実現するための基礎技術として利用されております。

VLAN の実装技術

VLAN の本質が、スイッチ内部でのネットワーク分離であると考えるのであれば、最も単純な実装方法は、スイッチの内部に「仕切り」を入れてやることになります。

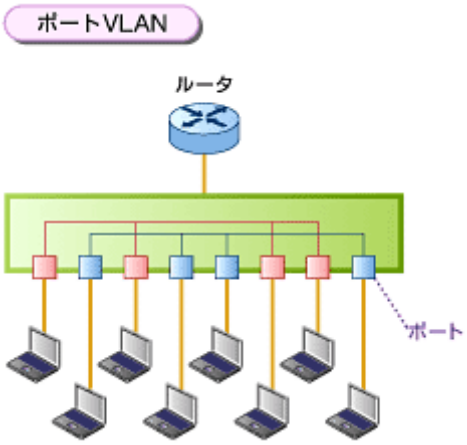
単純に、１台のスイッチを複数台のスイッチに分割するだけでも、ネットワーク分割の目的は達成できることになります。



スイッチの内部に仕切りをいれてやるもっとも単純なネットワーク分割

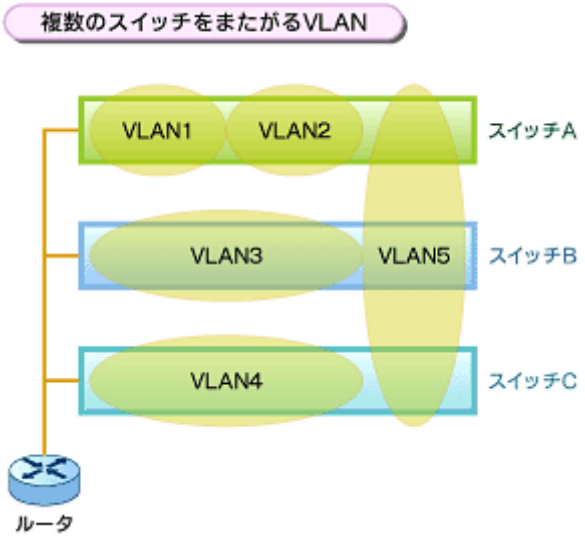
この場合、考え方としては個別に独立した複数のスイッチ、という考え方になるので、分割されたそれぞれの部分を個別にルータにて接続して相互に連結しないと、通信を維持した分割ではなく、単に分断になってしまいます。

次に、ポート VLAN という方式を説明します。
これはスイッチのポート毎に「どの VLAN に所属するか」を設定できるもので、構成の自由度が大幅に向上します。 更に、この方式は、IEEE802.1Q で標準化された VLAN タグの技術と組み合わせることで、スイッチをまたぐような柔軟な VLAN 設定を行うことが可能となり、現在の VLAN の主流ともいえる方式です。



ポートごとに VLAN 設定が行える

ポートごとに VLAN 設定を行えることで、ケーブリングを一切変更せず、ネットワーク分割のやり方だけを変更する、といった使い方が実現できます。
例えば、船内に複数の部門が存在し、その部門の担当箇所が船内中の任意の複数箇所に存在するような場合、ユーザーの PC が接続されているポートの VLAN 設定を変更するだけで、場所にとらわれないグルーピンクを実現できます。
IEEE 802.1Q では、VLAN の実装を標準化し、複数のスイッチにまたがる VLAN の実現を可能とするための VLAN タグの標準が決まりました。
VLAN タグは Ethernet フレームのヘッダに追加され、フレームがどの VLAN に属するかを識別するための ID 情報を含んでいます。
この ID を手がかりに、各スイッチはフレームを適当なポートに送ることができます。
VLAN がスイッチ内部で完結せず、複数のスイッチをまたぐ場合でも、複数のスイッチ間で共通の ID が使われていれば、どの VLAN に所属するフレームなのかという情報が伝達されることになるので、VLAN はスイッチの境界を越えて任意に拡大できます。
ベンダー各社は IEEE802.1Q をサポートしているため、現在では異なるベンダー製のスイッチを混在させても、相互にまたがる VLAN を構築することができるようになっています。



VLAN タグにより複数のスイッチをまたぐ VLAN が構築できるようになった

VLAN を活用する

VLAN は、機能としては「ネットワークを分割する」という比較的単純なものであり、技術的には特に難しいところはないといえます。

分割された VLAN は、それぞれ適切なネットワークアドレスが設定されている限り、標準的なルーティング機構を用いて相互接続できます。

VLAN のネットワーク分割の機能は、

・VoIP サービスのためにネットワークに QoS に基づく優先度のレベル分けを導入する。

・セキュリティを向上させ、パケット盗聴の可能性を大幅に低減する。

・ユーザーが接続する場所を移動しても常に同じ環境にアクセスできるようにする。

といった最近需要が高まりつつあるさまざまな用途を実現するための基礎技術として利用されつつあり、用途と組み合わせた応用形態が重要となります。

2. L2 スイッチ

スイッチは通信したい相手がどのポートに繋がっているかを記憶してパケットを転送します。 L2 スイッチの場合、どのポートにどの PC が繋がっているかは MAC アドレスによって管理されています。

MAC アドレスは、OSI 参照モデルの第 2 層(物理層)で扱われるので、レイヤー2 スイッチ(L2 スイッチ)と呼ばれます。

スイッチに LAN ケーブルを接続すると、接続先の PC 等の MAC アドレスと接続されたポート番号を関連付けて記憶します。

L2 スイッチは VLAN をサポートしているものもありますが、ルーティングはできません。

3. L3 スイッチ

L3 スイッチは、L2 スイッチの機能に加えて IP アドレスを用いたルーティングができます。

IP アドレスは、OSI 参照モデルの第 3 層で扱われるので、レイヤー3 スイッチ(L3 スイッチ)と呼ばれます。

例えば、VLAN にてネットワーク分割を行った場合、相互に通信するにはルーティングが必要になってきます。

L3 スイッチは、VLAN 間のルーティングに広く用いられています。

4. ルーター

ルーターは「異なるネットワークを接続する機能」を持っています。

しかし L3 スイッチもルーティングができます。

結局、L3 スイッチとルーターはルーティングという点では同じといっていいと思います。

しかし、細かな部分で違いがあります。

■L3 スイッチ

・イーサネットのポートの数が多い。

・ルーティングをハードウェアで処理する。

・高速に処理できる。

■ルーター

・イーサネット以外の様々な回線に対応しているものが多い。

・ルーティングをソフトウェアで処理している。

・柔軟性があり、様々なプロトコルに対応できる。

ルーターと L3 スイッチは、ルーティングの機能を持っているという点で、それほど違いはありません。 しかし光回線や専用線と接続するなど、様々なアクセス回線と接続する場合は、L3 スイッチでは難しく、L3 スイッチの上位にルーターを接続し外との接続を任せることになります。

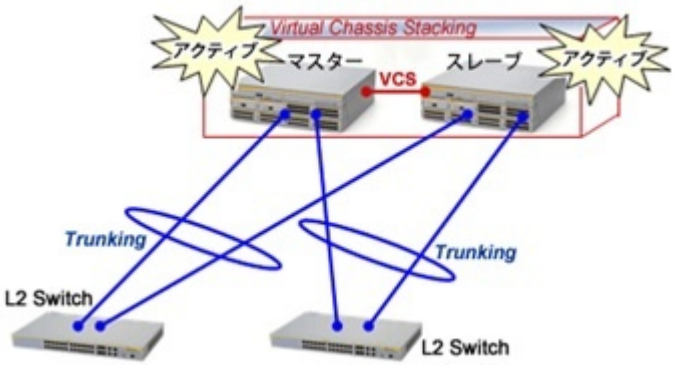
5. 冗長化

長期航海を想定し信頼性の高い機器を選定いたしますが、万が一の故障の際にも引き続き運用が続行できるように、様々な冗長化が採用されております。

(1) L3 スイッチの冗長化

ネットワークの根幹である L3 スイッチが機能しなくなると、船内の全てのネットワークが通信不可となり船内 LAN が使えない状況となります。

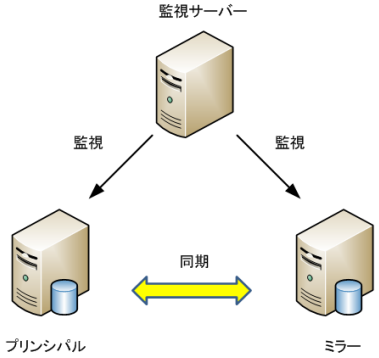
よって、L3 スイッチは信頼性のある機器を選択するとともに、万が一の故障に対応できるよう機器２台による冗長構成としており、１台が故障した場合でももう１台が全機能を維持することを可能とし、使用者には影響を与えないシステムとなっております。



(2) データベースのミラー化

運行中に収集した全てのデータは、データベースサーバーに記録･蓄積されますが、何らかの原因でサーバーが故障した場合、データの参照や記録が不可能となり、データベースにアクセスするアプリケーションは正常動作ができない状態に陥ります。

上記を回避するため、データベースサーバーを２台設置して常時同期を行なう構成とし、万が一どちらかが故障等により停止した場合でも、速やかにもう一方に切り替わり、引き続き通常通りの運用が可能となる仕組みを構築することができます。



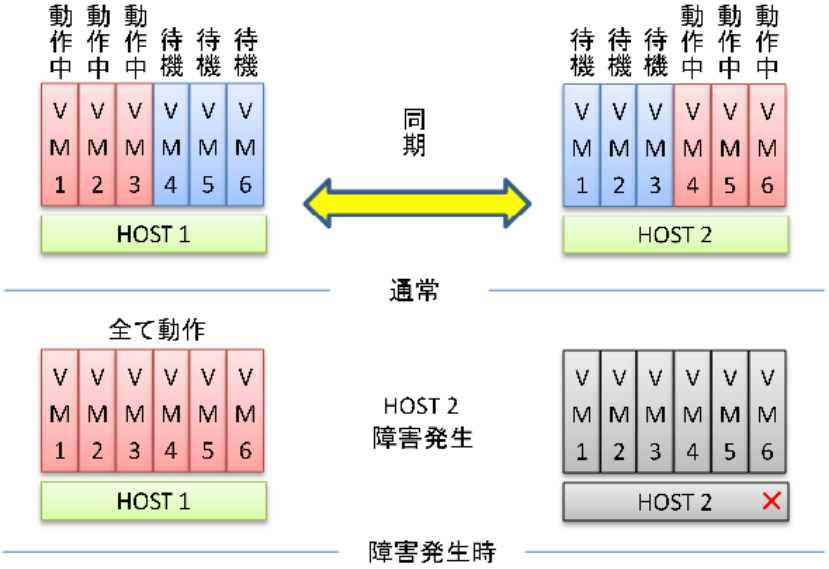
(3) 仮想サーバーの冗長化

データベースサーバー以外のサーバーは、仮想化技術による仮想サーバーにて構築することができます。

仮想サーバーを稼働させる仮想ホスト機を複数設置し、お互いに他方へ仮想サーバーのコピー（レプリカ）を持たせ、このレプリカを定期的に最新の状態に同期を取りながら保管、何時でも起動できる状態で待機させる構成といたします。

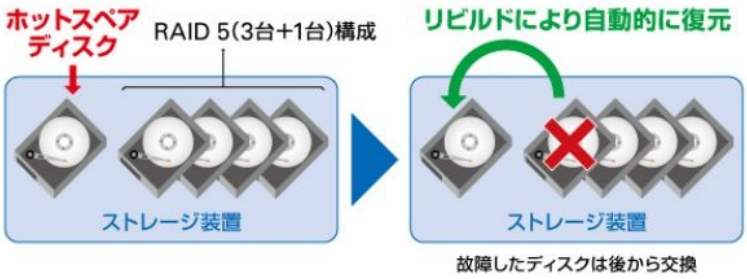
万が一、何れかの仮想サーバーがダウンした場合においても、その仮想サーバーに対するレプリカを起動することにより、迅速な運用再開が可能となります。

また、仮想ホスト機が故障した場合は、もう一方の仮想ホスト機にて全ての仮想サーバーを稼働させることにより、迅速な運用再開が可能となるような構成となります。



(4) ハードディスクの冗長化

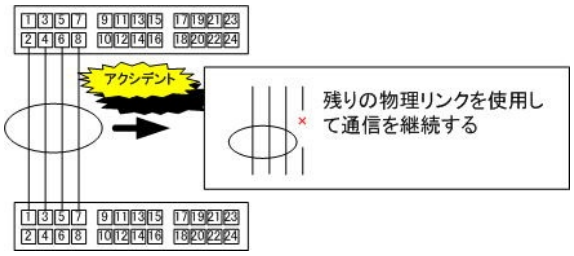
全てのサーバー、及び NAS に関しては、RAID 構成により構築し、それぞれ数個のハードディスクが故障しても、自動的にホットスペアディスクに切り替わり、そのまま運用を続行することが可能な構成となります。



(5) 配線の冗長化

L3スイッチから各フロアへのLANケーブルは、それぞれ複数本の配線を行い、ポートトラッキング構成といたします。

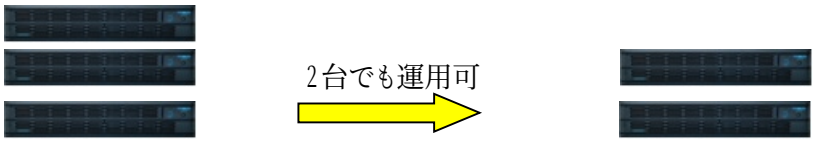
複数本の1本が断線、またはコネクタが外れても、システムの動作は問題なく運用を続行することが可能となります。



(6) 電源部の冗長化

システムの電源は、3台のUPSにより供給し、どれか1台が故障しても通常通りの運用が可能な冗長構成とすることができます。

特にサーバーラック内の根幹機器への電源供給は、2台のUPSにて並列供給とし、どちらか一方が故障等にて突然電源停止となった場合でも、切替時の瞬断無しで運用が続行可能な構成となります。



6. バックアップ

万が一のサーバーダウンに対する冗長化に関して上記にて説明いたしましたが、更に下記のバックアップ機能も構築し、設定したスケジュールにより自動的にバックアップを作成することが可能なシステムを構築することができます。

(1) 仮想サーバーのバックアップ

バックアップ用NASへ定期的に自動バックアップ、若しくは手動バックアップ

(2) 仮想ホスト機のイメージバックアップ

バックアップ用NASへ定期的に自動バックアップ、若しくは手動バックアップ

(3) データベースのバックアップ

バックアップ用NASへ定期的に自動バックアップ、若しくは手動バックアップ

(4) NASのバックアップ

バックアップ用 NAS へ1日1回の同期を取ることにより、一方に不具合が発生しても、もう一方にて引き続き運用を続けることができます。

7. 電源供給とシャットダウン信号の送信

船内中の全ての船内 LAN 機器は、専用 UPS により供給されており、船内電源切り替え等の瞬断にも影響を受けません。

また、ブラックアウトが数分間続いた場合は、コンピュータ機器や NAS 等のハードディスクを装備している機器に対してネットワーク越しにシャットダウン信号を送信し、UPS の電源供給が切れる前に各機器のシャットダウンが完了することができます。

8. システムアラームとメール通知

システムに何らかの異常、またはその兆候が検出された場合は、システムアラームを送信し、操舵室のアラームを鳴動いたします。

またサーバーや各ネットワーク機器等のファームウェアは、正常性を常時監視しており、何らかの異常が発生した場合は、設定した宛先（通常はシステム管理者）へメールを送信する機能を構成することができます。

これにより、冗長化等により自動的に不具合が解消され運用が続行された場合でも、システムの異常状態を把握することが可能となります。

9. 陸上施設

メールシステムは船舶利用を考慮した独自のメールシステムの構築が必須です。

通信プロトコルはネットワーク圧縮機能を利用した独自のプロトコルにて通信を行い、陸上に設置したメールサーバーと同期を取りながら中継され、陸上に設置したメールサーバーからインターネットへ配信される仕組みとなります。

10. リモートメンテナンス

遠隔地からリモート接続で船内あるいは陸上施設の各種サーバーにログインし、メンテナンスを実行可能とする仕組みを構築することが可能です。