中小企業向けシスコ製品の特徴について

Nov 14, 2008

【LANスイッチ編】

Cisco Catalyst 2960
vs
Allied Centre Com

※本資料は、シスコ製品を販売する営業担当者向けの参考資料として作成したものです。
※本資料の内容は、公開されている情報および弊社が実施した検証テストの結果に基づく、弊社独自の見解を示しています。

合同会社ティー・エヌ・シー・ブレインズ

目次

- 世界中で鍛えられた運用性！
  - よくあるトラブル事例－1 （サーバーへの不正侵入者を探す）
  - よくあるトラブル事例－2 （不正なDHCPサーバー）
    - 補足：DHCP Snoopingについて
  - よくあるトラブル事例－3 （LANケーブルのルーズコンタクト）
  - よくあるトラブル事例－4 （管理外のネットワーク拡張）
  - よくあるトラブル事例－5 （ウィルス感染）
  - よくあるトラブル事例－6 （サーバーのNIC故障）
    - 補足：Runtsパケットとは
  - よくあるトラブル事例－7 （ブロードキャストストーム）
    - 補足：ブロードキャストストームとその対策
- Cisco Catalyst 2960の優位点：まとめ
- Cisco Catalyst 2960 vs Allied CentreCOM 8424XL（スペック比較）

世界中で鍛えられた運用性！

よくあるトラブル事例－1（サーバーへの不正侵入者を探す）

社内サーバーから警告メッセージが通知された。何者かが不正アクセスを試みている模様。ボット型のスパイウェアが仕込まれている可能性もある

通常のLANスイッチの場合

解決まで1～5時間

① サーバーのログに残ったIPアドレスとDHCPサーバーのアドレステーブルを照合し、アクセスしたPCのMACアドレスが判明
② 資産管理台帳と照合したが該当するMACアドレスが記録されていないので、何者かが個人PCを接続したものと想定
③ MACアドレスを手がかりに犯人を捜すが、なかなか見つからない

Catalyst2960の場合

解決まで10分

① Catalyst2960のDHCP Snooping機能により、スイッチの各インタフェースに接続されている端末のIPアドレスとMACアドレスを確認できるので、該当PCが接続されているスイッチとインタフェース番号が判明
② LANケーブル配線図と照合して物理的な位置を確認。端末の利用者と直接会話して事情を聞く

世界中で鍛えられた運用性！

よくあるトラブル事例－2（不正なDHCPサーバー）

ある従業員が、雑誌の付録についていたLinuxのCDを興味本位で起動したところ、DHCPサーバーが稼動してしまった。

通常のLANスイッチの場合

復旧まで
1～5時間

① 複数の従業員から「ネットワークが利用できない」とのクレームが来る
② スニファでパケットをキャプチャし調査したところ、DHCPサーバーが不正なIPアドレスを配布していることが判明
③ DHCPサーバーのMACアドレスから、管理外のサーバーであることが判明
④ MACアドレスを手がかりに、不正サーバーを探そうとするが、なかなか見つからない

Catalyst2960の場合

トラブル無し

① DHCPスヌーピング機能により不正なDHCPパケットは破棄され、管理外のサーバーが接続されているインタフェース番号が警告メッセージとして通知される

補足：DHCP Snoopingについて

- DHCP Snooping機能とは
  - DHCPサーバーがパソコン等の端末へIPアドレスを配布する際の通信をトラッキングし、スイッチの各ポートに接続されているMACアドレスおよび配布されたIPアドレスのリストを自動的に作成します
  - また、正規のDHCPサーバーと接続されているポート以外からの、DHCPオファー（IPアドレスの配布）を破棄します
- Allied Centre COMのDHCP Snooping機能
  - Centre COMにもDHCP Snooping機能がありますが、シスコのIP Source Guard相当機能も含まれているため、DHCPでアドレスを取得していない端末のトラフィックを止めてしまうので注意が必要です
  - 固定IP機器を接続する場合にはポート毎に設定を変更する必要があり、端末移設の際にも設定作業が生じてしまうため、専任のIT管理者のいる企業でなければ運用が困難です（次頁参照）
- DHCPのバインディング情報
  - DHCPバインディング情報は、外部サーバーへテキストファイル形式で自動的に保存することも可能ですので、IPアドレスやMACアドレスの検索が容易です

DHCP Snooping関連機能の比較

機能	Cisco	Allied
DHCPバインディングテーブルの作成	DHCP Snooping	DHCP Snooping
不正DHCPパケットの破棄		
固定IP端末のトラフィック停止	IP Source Guard	
不正ARPの破棄	Dynamic ARP Inspection	ARP Security option

- Alliedの実装では、DHCP Snooping機能をEnableにすると、全ての固定IP端末のトラフィックを止めてしまう（CiscoのIP Source Guard相当機能が含まれている）
- ポート毎の設定で固定IPを許可することも可能だが、管理、メンテナンスが非常に煩雑になる
- 本来IP Source Guardは、ブロードバンドサービスを行う通信事業者がDHCPで配布したIPアドレス以外での通信を規制するため等に利用する機能であり、一般企業での使用は管理者の負担が大きい

世界中で鍛えられた運用性！

よくあるトラブル事例－3（LANケーブルのルーズコンタクト）

LANスイッチとサーバー間を接続するケーブルにおいてルーズコンタクト（接触不良）があり、断続的なパケット欠損が起こっていた。

通常のLANスイッチの場合 復旧まで数時間～	① 複数の従業員から「サーバーが遅い」とのクレームが来る ② サーバーやネットワーク機器のCPU使用率を確認したが、特に負荷の高い機器はなかった ③ 関連する機器のステータス情報を調査したが、原因不明でお蔵入りになる ④ 後日、別の作業のため作業員が該当LANケーブルに触れたところ、リンクダウンの警報が発生。ケーブルのルーズコンタクトが判明する
Catalyst2960の場合 復旧まで10分	① 従業員からクレームが来る ② Catalystには、TDR（Time Domain Reflector）と呼ばれる簡易ケーブルテスター機能が搭載されているため、これにより不良ケーブルを発見 ③ ケーブル交換にて復旧

世界中で鍛えられた運用性！

よくあるトラブル事例－4（管理外のネットワーク拡張）

ある従業員が個人で購入した無線APをLANスイッチに接続した。他の従業員も無線LANが利用できるようになり感謝していた。

通常のLANスイッチの場合 復旧まで1～5時間	① 同じフロアに入っている別の企業のIT担当者から、「おたくの会社の共有フォルダが丸見えになっている。何かトラブルがあると嫌なので、無線LANのセキュリティをちゃんとしてほしい」とクレームが来る ② 無線スニファでパケットをキャプチャし、SSIDやMACアドレスから管理外APの存在が判明 ③ 緊急事態なので、近隣のLANスイッチのケーブルを1本づつ抜き差ししながら、APが接続されているポートを特定した。
Catalyst2960の場合 トラブル無し	① Port Security機能を使い、アクセスポートには1端末しか接続できないよう設定していた ② 不正APを経由して2台以上のパソコンを接続した瞬間にポートがシャットダウンされ、管理者に通知される

世界中で鍛えられた運用性！

よくあるトラブル事例－5（ウィルス感染）

IDS（セキュリティ機器）が自己増殖型のウィルスを撒き散らしているPCを発見した。

通常のLANスイッチの場合

解決まで1～5時間

① ウィルス送信元のIPアドレスと、DHCPサーバーのアドレステーブルを照合し、感染PCと思われるMACアドレスが判明
② 資産管理台帳と照合したが該当するMACアドレスが記録されていないので、何者かが個人PCを接続したものと想定
③ MACアドレスを手がかりに犯人を捜すが、なかなか見つからない

Catalyst2960の場合

解決まで5分

① シスコ製のセキュリティ機器（IDS/IPS、CS-MARS）を使用していれば、自動的に感染PCの接続インタフェースが管理画面に表示され、そのままシャットダウンすることも可能

世界中で鍛えられた運用性！

よくあるトラブル事例－6（サーバーのNIC故障）

サーバーのNICが故障し、断続的なパケット欠損が起こっていた。

通常のLANスイッチの場合

復旧まで数時間～

① 複数の従業員から「サーバーが遅い」とのクレームが来る
② サーバーやネットワーク機器のCPU使用率を確認したが、特に負荷の高い機器はなかった
③ 関連する機器のステータス情報を調査したが、問題はなさそうだった。
④ サーバーへのPingでパケットロスが発生することから、関連するケーブルなどを順次交換したところ、NIC交換によって復旧した。

Catalyst2960の場合

トラブルの未然防止

① 定期的にCatalystのShowコマンドを使ってインタフェースのステータスを確認していたところ(*下記注)、特定のポートでRuntsパケットを受信していることが判明
② 休日にサービスを停止して関連するケーブルなどの交換調査を行ったところ、サーバーのNIC交換によって復旧した

*Cisco Works等のNMSを利用すれば、Runtsなどのエラーパケットが一定の閾値を超えた場合に自動的に管理者へ通知することも可能

補足：Runtsパケットとは

- ケーブルやNICの不良、外部からのノイズ、オートネゴシエーションの失敗などが原因となり、不完全なイーサネットフレームを受信する場合があります
- Catalyst2960では、これをRuntsパケットとしてカウントしており、”show interface”コマンド等で確認できます
- 実機による検証の結果、Allied CentreCOMは、不完全なイーサネットフレームを受信した場合でも、正しいフレームとしてカウントしていることが解りました
- ネットワーク管理者は、Allied CentreCOMでは正しいイーサネットフレームの受信をカウントしているのに、実際には転送されていない（不完全なフレームなので転送できない）という状況に直面し、故障箇所を特定することが出来ません

参考：不完全なイーサネットフレーム受信時のカウンタ表示

測定器から64byte未満のエラーフレームを送出し、スイッチ側でのカウンタ表示を確認

Catalyst2960
Runtsをカウント

```
Cat2960-A#sh int f0/1
FastEthernet0/1 is up, line protocol is up (connected)
 （略）

     0 packets input, 9828 bytes, 0 no buffer
     Received 0 broadcasts (0 multicasts)
     156 runts, 0 giants, 0 throttles
     156 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
```

CentreCOM
正常フレームとして
カウント

```
Manager > sh int=port1
 （略）

Interface Counters

  ifInOctets ..................  14679
  ifInUcastPkts ................  233
  ifInNUcastPkts .................  0
  ifInDiscards ...................  0
  ifInErrors .....................  0
```

世界中で鍛えられた運用性！

よくあるトラブル事例－7（ブロードキャストストーム）

複数のLANスイッチ間でブロードキャストフレームがループし続ける現象（ブロードキャストストーム）が発生した。

通常のLANスイッチの場合

復旧まで数時間～

① 多数のパソコンの処理が一斉に遅くなった
② 調査を開始したところ、パソコンのCPU負荷の異常な上昇と、ネットワークのトラフィックが急増していることが解った
③ ワーム型ウィルスの発生を想定し情報収集を行ったが原因が特定できなかった
④ ケーブルの抜き差しを繰り返して切り分けを行ったところ、LANスイッチの冗長化されたアップリンクポートのうち、片方を切り離すと現象が回復することが解った
⑤ メーカーの技術者による調査で根本原因が判明するまでの間、そのままの状態で運用することにした

Catalyst2960の場合

トラブルの未然防止

① Catalystが搭載する、ループガード、ルートガード、UDLD（短方向リンク検出プロトコル）、ストームコントロール、BPDUガード等のループ防止機構により、ブロードキャストストームの発生を未然に防止し、万一発生した場合でも影響が最小限に限定される

補足：ブロードキャストストームとその対策

- イーサネットは本来バス型の接続形態のみを前提として設計されており、ループ状に接続するとブロードキャストストームが発生して、ネットワーク全体に対して重大な問題を引き起こします。
- IEEE802.1Dとして標準化されたスパニングツリープロトコル（STP）が開発されたことでループ状の接続が可能になり、ネットワークの信頼性向上のためにLANスイッチやインタフェースを冗長化するデザインが採用されるようになりました。
- しかし、STPの仕組みはLANスイッチの特定のポートを強制的に停止させること（ブロッキングポート）により、ループの無いツリー状のトポロジーを擬似的に構築しているだけであり、ソフトウェアのバグや管理者の設定ミス、不適切な接続を行うことで容易にブロードキャストストームが発生する可能性があり、実際にSTPの導入初期において多くのトラブルを経験しています。
- シスコでは過去のトラブル事例に基づき、ブロードキャストストームを防止するための多数の機能を実装しているため、単一箇所の故障やバグによって致命的な影響を与えることは無くなっています。

Cisco Catalyst2960 の優位点（まとめ）

- **世界中のエンタープライズに鍛えられた運用性**
  - ✓トラブルを起こさせない機能、何が起こっているのかを把握するためのコマンドなど、運用支援の質と量が決定的に違います

- その他の優位点
  - ●グラフィカルユーザーインタフェース（GUI）の**管理ツールが無料**
    - ✓ ネットワークトポロジー表示から、1クリックで装置前面パネルをグラフィカル表示し、各種設定や状態情報の取得が可能です
  - ●標準で1000Base-Tのアップリンクを搭載（WS-C2960-24TT-Lの場合）
    - ✓ Centre COM 8424XLは別途購入が必要
  - ●**ユニファイドコミュニケーションとの親和性**（シスコ製IPフォンとの接続の場合）
    - ✓ IPフォンに電源を供給するPOE機能
    - ✓ IPフォンを検知して適切なQoSを自動で設定（Auto Detect）
    - ✓ 自動的に音声とデータを別のVLANに収容（Voice VLAN, Data VLAN）
    - ✓ IPフォン接続ポートでも802.1x認証機能を使用可能

Cisco Catalyst 2960 vs Allied CentreCOM 8424XL（スペック比較）

機能	Cisco **Catalyst2960-24TT**	Allied Telesis **CentreCOM 8424XL (RoHS)**
ポート数	10/100Mbps 24ポート	10/100Mbps 24ポート
DRAM	64MB	32MB
フラッシュメモリ	32MB	8MB
アップリンクポート	10/100/1000 固定 2ポート	拡張スロット※1
スイッチング・ファブリック	16Gbps	8.8Gbps
スループット （64byteパケットを基本とするフォワーディング速度）	6.5Mpps	6.54Mpps
VLAN登録数	255	256
MACアドレス登録数	最大8000	最大8000
QoS	○	○
ポートセキュリティー (MACアドレスフィルタリング)	○	○
IEEE 802.1X認証機能対応	○	○
VRRP	×	×
ポートトランキング （FEC/GEC）	○	○
環境条件	動作温度：0 ～ 45°C（32 ～ 113°F） 保管温度：–25 ～ 70°C（–13 ～ 158°F） 動作相対湿度：10 ～ 85%（結露しないこと）	動作時温度 ファンモジュール未装着時：0～40℃ ファンモジュール装着時：0～50℃ 動作時湿度 80%以下（結露なきこと） 保管時温度 -20～60℃ 保管時湿度 95%以下（結露なきこと）
最大消費電力	30W	19W（最大28W）
AC入力電圧	100 ～ 240 VAC（オートレンジ）	AC100-240V
AUTO MDIX	○	○
寸法 （高さ×幅×奥行き）	4.4 × 44.5 × 23.6 cm（1.73 × 17.5 × 9.3 インチ）	38(H)×263(W)×179(D) mm
価格	150,000（市場想定価格*）	194,000（定価）

*市場想定価格：シスコ製品には定価の設定がないため、シスコパートナーが提示している定価の一例を示します。


tnc
T.N.C.Brains
TRAINING & CONSULTING