中小企業向けシスコ製品の特徴について

Dec 15, 2008

【ルーター編】

Cisco 1812J
vs
Yamaha RTX1100

※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

Cisco 1812Jは実環境で強い！

ケース1 （期待はずれのWAN増速）

- ある企業では、これまでIP-VPNサービスのアクセス速度を50Mbpsで契約していたが、従業員の増加などによってトラフィックが急増しており、「最近、WAN超えの通信が遅い」とのクレームが出始めていた。
- そこで、アクセス速度を100Mbpsの契約に変更したが、利用者の間では「効果が全く実感できない」との意見が大勢を占めた。
- 念のため、ファイルダウンロードにて通信速度を測定してみると、確かに100Mbps近くの速度が出ており、なぜWAN回線のスピードアップが体感できないのか不明であった。

想定される原因：ルーターの性能不足

- ✓ ネットワーク機器メーカーが公表する最大スループットは、イーサネットの最大パケット長（1518Byte）で計測されている場合がほとんどです。これは、ルーターが効率よくパフォーマンスを発揮するために、大きなパケットを使用したほうが有利なためです。
- ✓ ファイルダウンロードでは最大長のパケットが使用されるため、公表されている性能に近い値が計測されます。
- ✓ しかし、WEBやメールなど実際のトラフィックには小さなパケットも含まれるため、メーカーの公表値よりも低い性能しか発揮できず、ルーターがボトルネックになる場合があります。

参考：IP転送スループット測定結果

- 実環境でのユーザーの体感速度を測るため、インターネット上を流れるトラフィックの平均パケット長（354Byte）を用いたスループット計測を行ったところ、**Cisco1812Jの性能は180Mbps**（片方向90Mbps）であり、これは**100MbpsのWANアクセス回線を使用した場合に必要十分な性能**であることを表しています（ユーザーが利用可能な帯域は回線の物理速度よりも少なくなるため200Mbpsにはなりません）。
- Yamaha RTX1100の最大スループットは120Mbps（片方向60Mbps）であり、100MbpsのWAN回線帯域を使い切ることができませんでした
- また、RTX1100のスループットはQoSを利用した場合に90Mbps（片方向45Mbps）まで低下したのに対して、Cisco1812Jはスループットの低下がありませんでした。

	RTX1100	1812J
公称値	200Mbps	非公開
IP転送スループット測定値 （パケット長：354Byte）	120Mbps （片方向60Mbps）	180Mbps （片方向90Mbps）
QoS利用時スループット	90Mbps （片方向45Mbps）	180Mbps （片方向90Mbps）

Cisco 1812Jは実環境で強い！

ケース2（使い切れない帯域）

- IT部門のAさんが、ファイルダウンロードを行ってWANの通信速度を測定したところ、何度実験しても契約帯域の80%程度の速度しか計測されなかった。
- また、VoIPで通話をしながらファイルダウンロードを行うと、雑音が発生することが解った。

対策：ルーターのQoS機能

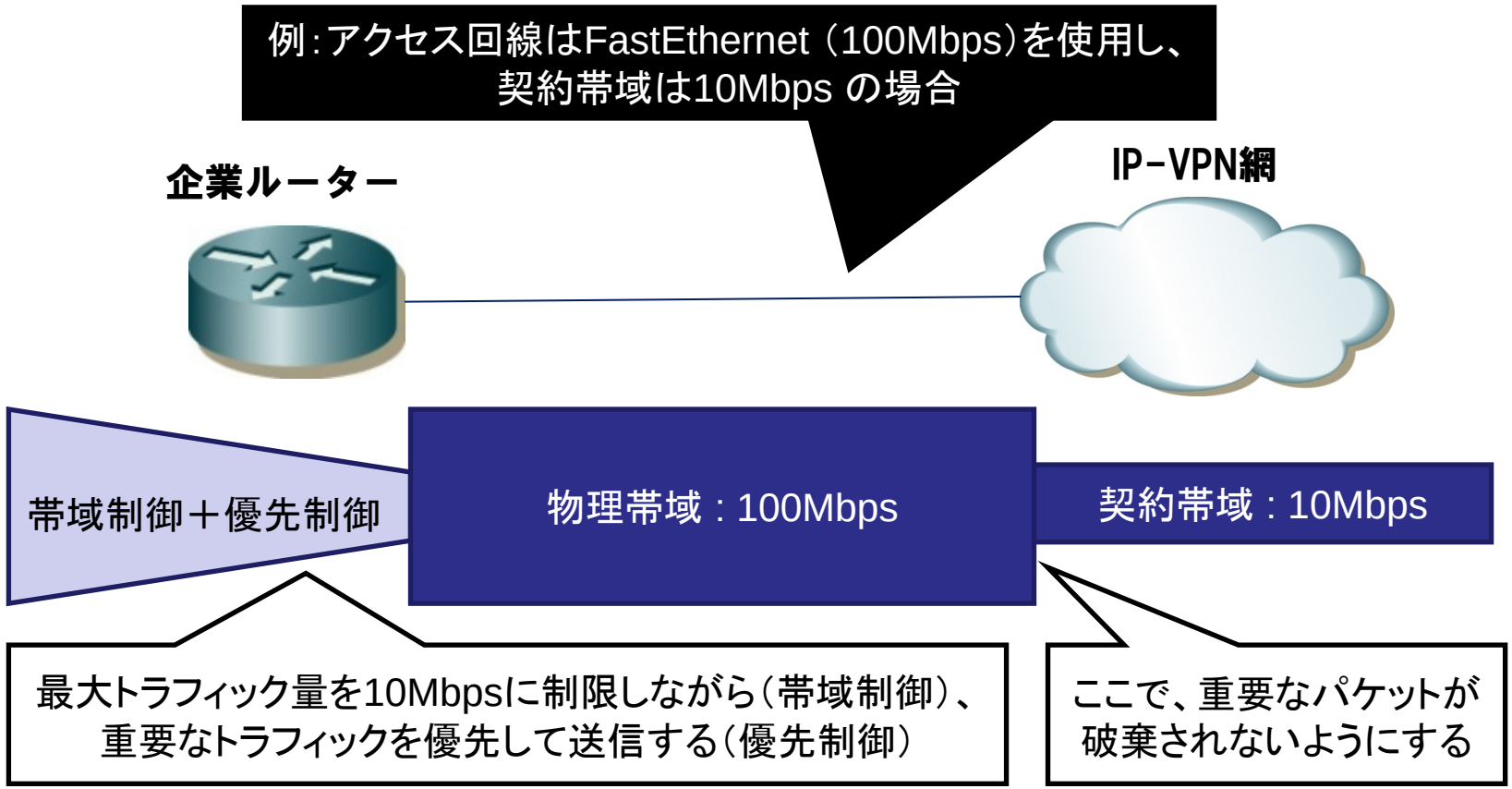
- ✓ この事例の場合には、WANのアクセス回線として100BASE-TX（100Mbps）を使用していましたが、通信事業者との契約で実際に利用できる帯域が10Mbpsに制限されていました。
- ✓ このような場合、ルーターからは最大100Mbpsの速度でトラフィックを送出できますが、WANを透過できるのは10Mbpsだけなので、結果としてWindowsやLinuxなどのOSに搭載されているトラフィック制御機構（TCP輻輳制御）が有効に働かず、回線帯域を十分に利用できない場合があります。
- ✓ また、10Mbpsを超えるトラフィックがWANに流入すると、パケット損失が発生し通信品質が低下します。
- ✓ ルーターに高度なQoS機能が搭載されていれば、このような問題は回避できます。
- ✓ 高度なQoS機能は、トラフィックの特性に合わせた優先制御や帯域制御を行うことで、WANの帯域を最大限に活用しながら、輻輳した場合でも優先されるべきトラフィックを保護します。

Cisco 1812Jは実環境で強い！

ケース2（使い切れない帯域）

対策：ルーターのQoS機能（補足説明）

✓ 高度なQoS機能を持ったルータを使用し、契約帯域にあわせた帯域制御と、優先制御を同時に実行することで、重要なトラフィックを保護することが出来ます。



参考：アプリケーションの速度と品質（テスト結果）

- IP-VPNサービスのサブレート回線を想定した実環境テストにおいて、HTTPの通信速度を測定した結果、Cisco1812Jを使った場合はアプリケーション速度が回線帯域の95.3%に達しましたが、Yamaha RTX1100では同じ条件において82.9%にとどまりました。
  これは**Cisco1812Jの高度なQoS機能が回線の利用可能帯域を最大限に活用し、ネットワーク利用者の体感速度を高めている**ことを示しています。
- 同様の環境において優先パケットの損失率を比較したところ、RTX1100ではトラフィックの輻輳状態に応じてパケット損失が発生しましたが、**Cisco1812Jはパケット損失が全くありません**でした。
  パケットの損失が発生すると、VoIPを利用している場合には音質が劣化し、ミッションクリティカルなアプリケーションでは信頼性の低下が生じます。

	RTX1100	1812J
HTTPダウンロード	回線帯域の82.9%の速度	回線帯域の95.3%の速度
優先パケットの損失	あり	なし

Cisco 1812Jは実環境で強い！

ケース3（インターネットVPNで音声通話）

- B社では、従来IP-VPNサービスを利用していたが、WAN通信コスト削減のため、インターネットVPNへの置き換えを検討していた。
- 同時に、VoIPを利用した内線電話システムの構築を考えているが、インターネットには品質の保証がないため、音声通話の品質が維持できるかどうかが最大の懸案になっている。

結論：インターネット上の通話品質は保証できない

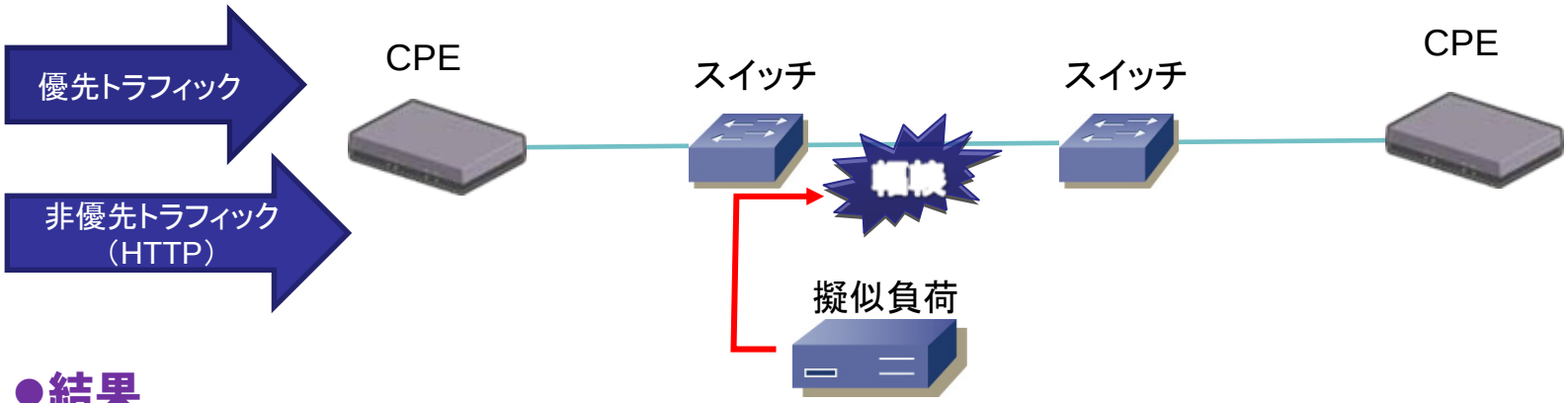
- ✓ 品質保証のないインターネットをWAN回線として利用する場合、どのような方法を使っても、通信品質の確実な維持は原理的に不可能です。
- ✓ 仮に試験運用で問題が出なかったとしても、将来も問題が出ないことを誰かが保障してくれる訳ではありません。実際にインターネットの品質は時々刻々と変化し続けています。
- ✓ VoIPや重要な業務アプリケーションの通信を確実に維持したいのであれば、通信事業者が品質を保障するWANサービスと、ルーターなどネットワーク機器のQoS機能を組み合わせて利用する必要があります。
- ✓ また、ADSLなどアクセス回線の帯域幅がボトルネックになる場合には、Cisco 1812Jが搭載するダイナミックマルチポイントVPN（DMVPN）を利用して、特定の拠点にトラフィックが集中しないようデザインすることが有効な対策となります。

参考：Yamaha適応型QoS（帯域検出機能）について

Yamahaの主張	現実のネットワーク
ベストエフォート回線に対して一定の帯域で送信するとパケット破損が発生する。帯域検出機能により、帯域変動に合わせてパケット送出速度を調整するため、問題を解決できる。	帯域検出機能が有効に機能するのは、アクセス回線の上り帯域がボトルネックになっている場合だけです。 しかし、ベストエフォート型のWANサービスでボトルネックになっているのは、多くの場合、通信事業者内のネットワーク機器であり、送出する帯域を減らしても、その分を他のユーザーに使われるだけで、ボトルネックが解消されることはありません。 つまり、世界中のルーターがYamahaにならない限り、この機能を使うと損です。

A社が帯域を減らせば、その分をB社が使う

参考：Yamaha適応型QoS（帯域検出機能）
複数のユーザーが帯域を共有する箇所で輻輳が発生している場合の実験結果



●結果

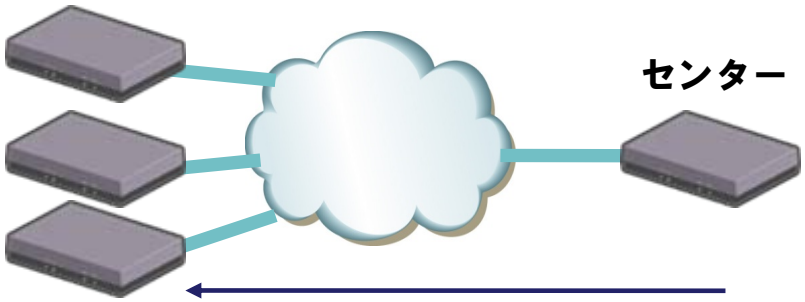
	QoSなし	帯域検出＋優先制御
優先トラフィックのパケット損失率	5.2%	5.4% （悪化）
HTTPの実効スループット	5.1M	3.9M （悪化）

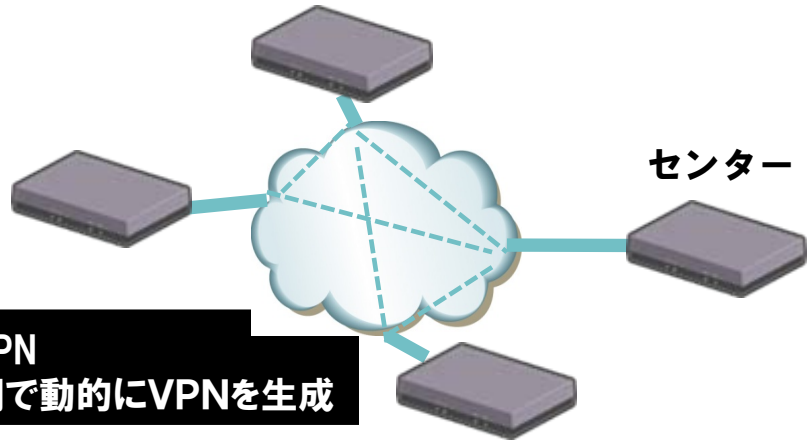
1. 優先制御は輻輳箇所で行わないと効果が出ないため、優先トラフィックも破棄
2. 帯域検出機能によってトラフィック送出量が制限されるので、実効スループットが下がった
3. **QoSを一切使用しない状態のほうが、品質／スループットともに優れていた**

以上の結果により、帯域検出機能は、CPEと直接接続されており他のユーザーと共有していない区間（すなわちアクセス回線の上り帯域）が輻輳している場合にしか効果がないと言える

参考：Yamaha適応型QoS（負荷通知機能）について

Yamahaの主張	現実のネットワーク
拠点からのトラフィックの合計がセンター側機器の処理能力を上回る場合がある。 センターからリモート拠点へ負荷通知を行い、拠点側の送信を抑制することで、確実な受信を可能とする。	そもそも、センター側機器の処理能力が不足するのは、ネットワークデザインおよび機種選定のミスです。 センター側機器にアクセス回線の帯域を上回る性能の機種を選択すれば、この種の問題は発生しません。 アクセス回線の下り帯域がボトルネックになる場合は、センター側にトラフィックが集中しないようDMVPNの使用を推奨します。





Cisco 1812Jは実環境で強い！

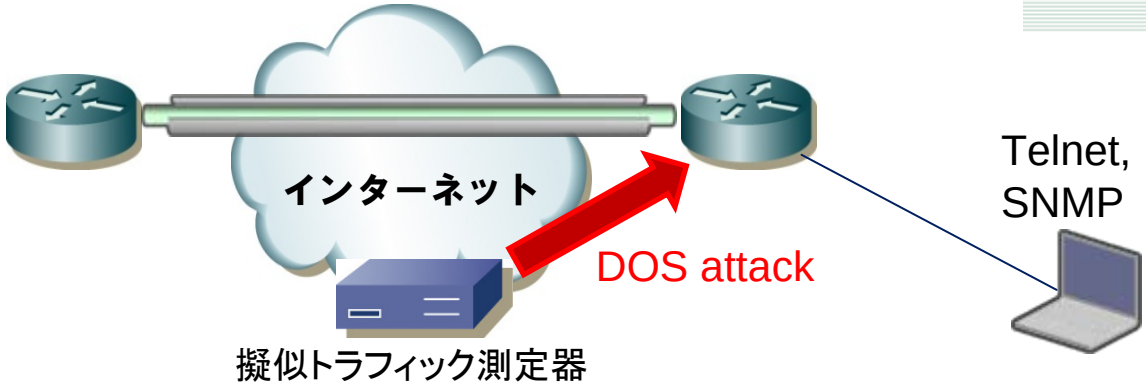
ケース4（ルーターが管理不能に！）

- IT部門のCさんは、リモート拠点の従業員から「本社側のサーバーへのアクセスが非常に遅くて使い物にならない」とのクレームを受けた。
- サーバーの負荷を調査したが問題なかったので、拠点と接続しているルーターの負荷を確認しようとしたところ、ルーターへのアクセスが不能であり、どのような問題が発生しているのか把握することが出来なかった。

原因：ネットワーク機器の過負荷状態

- ✓ ネットワーク機器は、輻輳状態やDOSアタックの状態においても、TelnetアクセスやSNMP監視機能を維持し、管理者によるトラブルシューティングを可能とする事が求められます。
- ✓ 実機を用いたテストにおいて、Cisco1812Jは輻輳時でもルーティングプロトコルが安定しており、DOS攻撃状態でも管理機能を維持できることが証明されました。
- ✓ Yamaha RTX1100では、インターネットからのDOS攻撃を想定したテストにおいて、アクセスリストを設定した場合でもルータの負荷が過度に上昇し、TelnetアクセスやSNMP監視が不能になりました。

参考：DOSアタック耐性テスト



●結果

	Telnetアクセス	CPU	SNMP監視	データ転送への影響
RTX1100（アクセスリスト無し）	アクセス可能だが、かなり重い状態	100%	受信エラー発生（監視不能）	なし
RTX1100（アクセスリスト有り）	アクセス可能だが、かなり重い状態	100%	受信エラー発生（監視不能）	あり 逆方向のトラフィックも大きくロスト
Cisco1812J（アクセスリスト無し）	アクセス不可	測定不能	受信エラー発生（監視不能）	あり 逆方向のトラフィックも大きくロスト
Cisco1812J（アクセスリスト有り）	支障なし	99%	問題なし	影響なし


tnc
T.N.C.Brains
TRAINING & CONSULTING