

iSCSI ストレージにおける VPN 複数経路アクセス時の性能と TCP パラメータ解析

千島 望[†] 山口 実靖^{††} 小口 正人[†]

[†]お茶の水女子大学 〒112-8610 東京都文京区大塚 2-1-1

^{††}工学院大学 〒163-8677 東京都新宿区西新宿 1-24-2

E-mail: [†]nozomi@ogl.is.ocha.ac.jp, ^{††}sane@cc.kogakuin.ac.jp, ^{†††}oguchi@computer.org

あらまし 近年, ストレージの管理コスト低減などの目的で SAN の導入が進んでおり, IP ネットワークを利用した IP-SAN として iSCSI が期待されている. しかし現状では SAN は主にサイト内のローカル環境のみで用いられている. そこで本稿では VPN を利用することにより, iSCSI を広域ネットワークに適用することを検討した. さらに, より信頼性の高い通信を実現するため VPN 広域ネットワーク内を複数経路で接続し, 高遅延環境での性能と TCP 輻輳ウィンドウの振舞いを評価, 解析した.

キーワード iSCSI, VPN, 輻輳ウィンドウ, スループット, 複数経路

Analysis of Performance and TCP Parameter in the case of Multi-routing VPN Access on iSCSI Storage

Nozomi CHISHIMA[†], Saneyasu YAMAGUCHI^{††}, and Masato OGUCHI[†]

[†] Ochanomizu University Otsuka 2-1-1, Bunkyo-ku, Tokyo, 112-8610 Japan

^{††} Kogakuin University 1-24-2 Nishi-shinjuku, Shinjuku-ku, Tokyo, 163-8677, Japan

E-mail: [†]nozomi@ogl.is.ocha.ac.jp, ^{††}sane@cc.kogakuin.ac.jp, ^{†††}oguchi@computer.org

Abstract The introduction of SAN is advanced for the purpose of the storage management cost reduction, and iSCSI is expected as IP-SAN that uses IP network. However, SAN is mostly used only in the server site currently.

Thus we have claimed iSCSI used in a local environment can be applied to the WAN using VPN. We have examined a realization method and performance for it. Furthermore, we have evaluated performance and behavior of the congestion window, which is one of the TCP parameters, when multi-routing is performed using a multi-routing function of a VPN router.

Key words iSCSI, VPN, Congestion Window, Throughput, multi-routing

1. はじめに

近年, インターネット技術の進展などにより, ユーザが蓄積し利用するデータ容量が爆発的に増加している. これに伴いストレージの増設, 管理コストの増大が問題となっている. そこで SAN(Storage Area Network) が登場し, 広く用いられるようになった. SAN とは, サーバとストレージを物理的に切り離し, 各ストレージとサーバ間を相互接続してネットワーク化したもので, これにより各サーバにばらばらに分散していたデータの集中管理が実現された.

一般に SAN としてはファイバチャネルを用いる FC-SAN(Fibre Channel - SAN) が利用されている. しかし, FC-SAN はファイバチャネルを用いているため高価となり, また距離に制約がある. 一方, SAN に IP ネットワークを利用した IP-SAN として

iSCSI が期待されている [1][2]. iSCSI は, これまで DAS(Direct Attached Storage) で使われてきた SCSI コマンドを TCP/IP パケット内にカプセル化することにより, サーバ(Initiator) とストレージ(Target) 間でデータの転送を行う. 今後インターネットの発展により, ギガビットクラスの回線実現が期待され, iSCSI の有効性もさらに高まると考えられる.

現状において, SAN は主にサーバサイト内のみでしか使用されていない. しかし遠隔バックアップ等を目的として, 離れたサイトのサーバとストレージを SAN で接続することが望まれている. そこで本研究では, VPN(Virtual Private Network) を利用することにより, ローカル環境で使用されている iSCSI を用いて広域ネットワーク上でリモートアクセスを行うことを検討した. さらに, より信頼性の高い通信を実現するため VPN 広域ネットワーク内に複数経路を構築した. iSCSI は複雑な階

層構成のプロトコルスタックで処理されており、パース的なデータ転送も多いことから、通常のソケット通信と比較して、特に高遅延環境においては性能の劣化が著しい [3]。また、下位基盤の TCP/IP 層が提供できる限界性能を超えることはできず、最大限の性能が発揮できるよう TCP パラメータなどを制御することが求められる。本研究では、高遅延環境において VPN 複数経路を用いて iSCSI アクセスを行う際の性能と TCP 輻輳ウィンドウの振舞などを解析する。

本稿の構成は以下の通りである。2 章で研究背景を述べ、3 章で VPN のマルチルーティング機能を利用した本実験システムの概要を述べる。4 章で複数経路 iSCSI アクセスについての性能評価結果を示し、最後に 5 章でまとめる。

2. 研究背景

2.1 iSCSI

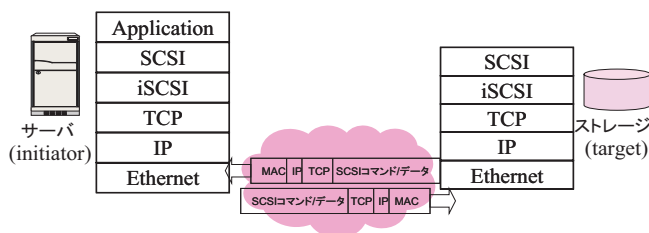


図 1 iSCSI

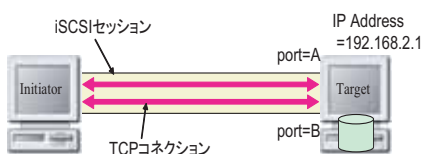


図 2 iSCSI 複数コネクション

IP-SAN の代表的なプロトコルに iSCSI がある。iSCSI は SCSI コマンドを TCP/IP パケットでカプセル化する規格で、iSCSI により SAN を IP 機器だけで構築することが可能となる。一方で図 1 のように複雑な階層構成をとることになり、下位のプロトコルの限界性能を超えることはできない。また、iSCSI アクセスは長距離アクセスであることが多く、ギガビットの太い回線を用いることから遅延帯域積の問題も挙げられている。そこで下位基盤の TCP/IP 層の適切な制御が求められている。

iSCSI は様々なチューニングを行うことができる。本実験で用いたニューハンブシャー大学が提供する UNH-iSCSI の実装では、1 つの iSCSI セッション内に複数の TCP コネクションを確立するように設定することができる。さらにこのコネクションをポート番号と対応付けることができ、1 つの iSCSI セッションをポート番号が異なる複数のコネクションに分けることができる。つまり、図 2 に示すようにターゲットの 1 つの IP アドレス、1 つの iSCSI ドライブにポート番号の異なる複数のコネクションを接続可能である。

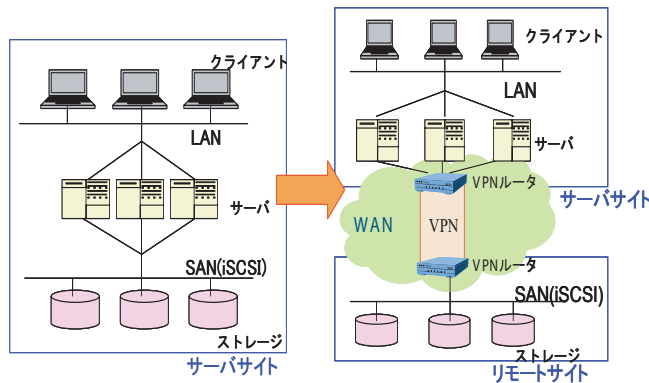


図 3 VPN 利用モデル

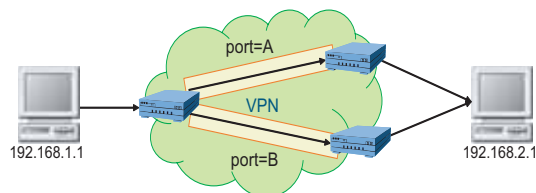


図 4 VPN マルチルーティング機能

2.2 VPN

VPN は、インターネットや通信事業者が持つ公衆ネットワークを使って、拠点間を仮想的に閉じたネットワークで接続する技術である。安価であるという公衆網のメリットを活かしつつ、機密性の低さを暗号化等の別の方法で補うことにより、「実質的な専用網」を実現できるということが VPN の利点である。一方、専用網と異なりネットワークの品質は保証されない場合が多い。

本研究では iSCSI を用いて遠隔バックアップなどを行うために、図 3 に示すように VPN ルータで接続したりリモート環境にネットワークストレージを設置し、広域ネットワーク内の VPN 越しにアクセスを行うことを考えた。この場合、VPN ルータを通ることによってネットワークの帯域幅が制限され、スループットが著しく低下することが起こり得る [4]。さらに広域ネットワーク内は不安定な通信路であることが想定される。そこで本稿では、VPN 広域ネットワーク内を複数経路で接続することを考えた。これにより、データ転送の信頼性やネットワークの耐障害性なども向上すると考えられる。

本実験で用いた VPN ルータ Fujitsu Si-R570 はマルチルーティング機能を有している。マルチルーティング機能を使用すると、ポート番号などの情報を利用して同じ IP アドレスを持つネットワークへ複数の経路を用いて送信することが可能となる。それぞれの通信内容に通信経路を分離することが出来るので、片方の回線をバックアップ用に用いることや、音声データは専用線を用いてそのほかの通信は公衆網を用いるなどと設定することができる。本稿ではこの機能を利用し、iSCSI 複数コネクションと対応付けることにより、コネクションごとに異なる経路を構築することを可能にした。

iSCSI は通常ギガビットクラス以上の太いネットワーク上で用いられるが、途中で VPN ルータの暗号化処理速度などにより

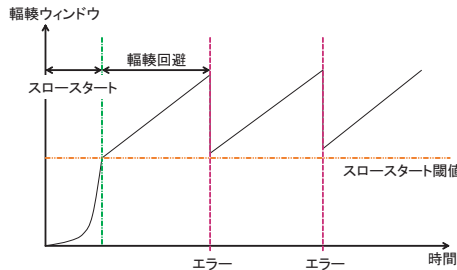


図5 輻輳ウィンドウの変化

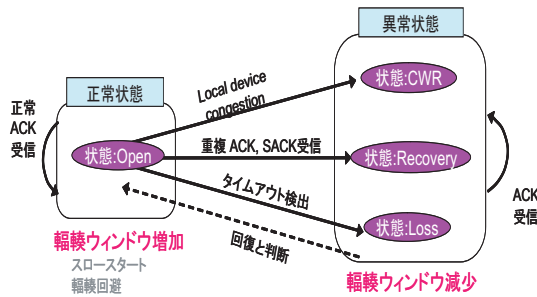


図6 LinuxTCP の状態遷移

スループットが決まる細かい回線が挟まることにより、トラフィックとして大いに性質の異なるものになる [5]。従って iSCSI が最大限の性能が発揮できるように TCP パラメータなどを制御することが求められる。

2.3 TCP 輻輳ウィンドウ

TCP では、通信能力の制御にウィンドウサイズという概念を用いている。ウィンドウサイズとは、ホストが確認応答パケット (Acknowledgement:ACK) なしに一度に送信できるデータの量である。また、データの送信側では輻輳ウィンドウ、受信側では広告ウィンドウという値が決定され、このどちらか小さい方がウィンドウサイズとして用いられる。広告ウィンドウは現在の受信バッファの空き容量を示しており、ACK のヘッダにその情報が含まれて送信側に送られる。一方、輻輳ウィンドウは送信側の制御パラメータで、ネットワークの混雑を回避するため送信側が自主的に制限する値である。

輻輳制御ではこの輻輳ウィンドウが利用されている。輻輳制御はネットワークの混雑解消の方法として TCP が行う機能である。通信開始時にはスロースタートと呼ばれるアルゴリズムに従って指数関数的に輻輳ウィンドウが大きくなる。これによりトラフィックが急激に増加するので、ネットワークが輻輳状態になる可能性がある。これを防ぐため、スロースタート閾値という値を用意し、輻輳ウィンドウがその大きさを超えると輻輳回避と呼ばれるフェーズに入り、一次関数的な増え方となる。そしてエラーが検出されると輻輳ウィンドウは急激に低下し、通常これらを繰り返すことで鋸型のグラフとなる。この様子を図5に示す。

本実験で用いた LinuxOS における TCP の状態遷移を図6に示す。LinuxTCP においては、通信時の状態が正常であれば ACK の受信ごとに輻輳ウィンドウは増加するが、エラーが検出されると異常と判断され、輻輳ウィンドウは低下する。輻輳ウィンドウが低下する原因としては、送信側デバイスドライバのバッ

ファが溢れることによる Local Congestion エラーを検出した場合 (CWR)、重複 ACK 又は SACK を受信した場合 (Recovery)、タイムアウトを検出した場合 (Loss) の3つが挙げられる。さらに Linux の TCP 実装では、通信中に一度設定された輻輳ウィンドウは、そのウィンドウ値を超えるデータ量が送られない限りは変化しないという特徴を持ち、この時スループットはほぼ一定の値で安定することが確認されている。

2.4 既存研究

我々は、これまでに iSCSI を用いたアプリケーション実行性能と TCP パラメータの相関関係の評価を行った [6]。その結果、広告ウィンドウの値を制限することで、輻輳ウィンドウの値も制限でき、それによって実行性能にも影響が出ることが確認された。また、VPN 利用時のネットワークや、iSCSI ストレージアクセスによる性能測定と TCP 輻輳ウィンドウの振舞いを観察した [4][5]。

iSCSI ストレージアクセスにおいて TCP 輻輳ウィンドウを制御する研究としては、輻輳ウィンドウ値を動的にコントロールする手法がある [7]。この手法は、まず Target の OS のカーネルに輻輳ウィンドウモニタ関数を挿入し、これによりモニタした輻輳ウィンドウの変化を観察して、Initiator にその値を通知する。通知を受けた Initiator は輻輳ウィンドウの値に基づきブロックサイズを再指定して、シーケンシャルリードアクセスを行うというものである。この手法を適用し輻輳ウィンドウを限界値で一定に保った場合には、高遅延環境において最大 28% のスループットの向上が確認されている。

さらに iSCSI 複数コネクションに関する研究として、広域 IP 網を介した長距離アクセス向けに iSCSI および関連プロトコルレイヤのプロトコルチューニングの検討が行われ、その有効性が確認されている [8]。

そこで本稿では、iSCSI 複数コネクションを VPN 複数経路に乗せてアクセスすることを検討した。これらを組み合わせることにより、性能の向上だけでなく信頼性の向上も期待できる。そしてこの時のストレージアクセス性能と TCP 輻輳ウィンドウの振舞などを解析した。

3. 実験システム

3.1 TCP 輻輳ウィンドウモニタツール

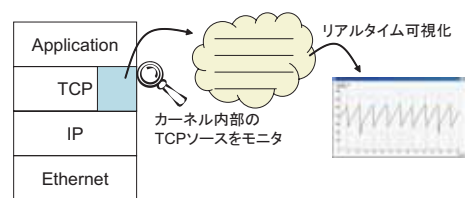


図7 TCP 輻輳ウィンドウモニタツール

本実験では、TCP 輻輳ウィンドウをリアルタイムに可視化するツールを構築した。カーネル内部の TCP ソースにモニタ関数を挿入しカーネルを再コンパイルした。そして図7に示すように、X11 ウィンドウシステムライブラリ関数を用いてモニタした値をリアルタイムに可視化できるようにした。ここで

可視化できるようになったものには、輻輳ウィンドウの値、各種エラーイベントの発生 (Local device congestion, 重複 ACK, SACK 受信, タイムアウト検出) などがある。

3.2 VPN 複数経路アクセス制御システム

本実験では、VPN ルータを用いて複数経路を構築し、高遅延環境における iSCSI ストレージアクセスを実行した時の、TCP パラメータである輻輳ウィンドウと、ストレージアクセス性能を評価するために図 8 に示す実験環境を構築した。

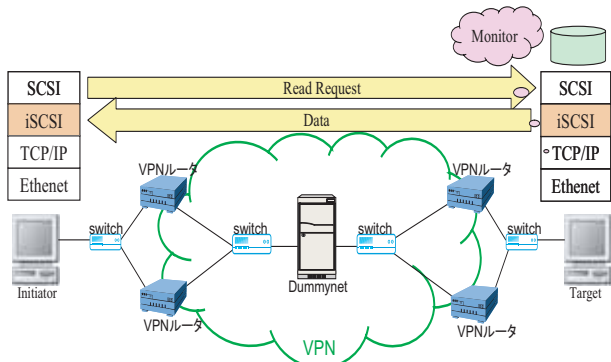


図 8 実験システムの概要

iSCSI ストレージアクセスを行う Initiator とストレージを提供する Target の間に VPN ルータを 4 台を挟み、複数経路アクセスが実行できるように構築した。さらに、遠距離アクセスを想定して、人工的な遅延装置である FreeBSD Dummynet を挿入した [9]。

この実験システムにおいて iSCSI の複数コネクション設定と VPN ルータのマルチルーティング機能を用いて通信制御を行った。まず iSCSI 単数コネクション VPN 単数経路通信の場合は図 9 のような経路を通る。また iSCSI 複数コネクション VPN 単数経路通信の場合は図 10 のように同一経路上を 2 つのコネクションが張れるように iSCSI を設定した。さらに iSCSI 複数コネクション VPN 複数経路通信の場合は図 11, 12 のようにコネクションごとに経路が異なるように VPN ルータの設定を行った。このとき Initiator から送られるパケットは図 11 のように左下の VPN ルータに送るように設定する。そして、VPN ルータのマルチルーティング機能により右の 2 つの VPN ルータ宛にパケットは転送される。このとき、ポート番号の違いによる iSCSI コネクションごとに上下の VPN ルータに分かれるように設定した。Target からのパケット送信も図 12 に示し、先ほどと同様に行われる。

Initiator と Target には、OS は Linux2.4.18-3, CPU は Intel Xeon 2.4GHz, Main Memory は 512MB DDR SDRAM, NIC は Intel Pro/1000XT Server Adapter on PCI-X (64bit,100MHz), iSCSI は UNH IOL reference implementation ver.3 on iSCSI Draft 18 を用いた [10]。そして Dummynet には FreeBSD4.9-RELEASE を用いた。また VPN ルータには Fujitsu Si-R570 を用いた [11]。これは 3DES 暗号化速度最大 500Mbps を実現する。

この実験環境において、TCP 輻輳ウィンドウモニタツールを起動し、iSCSI シーケンシャルリードアクセス時の性能や TCP パラメータの振舞いを観察した。

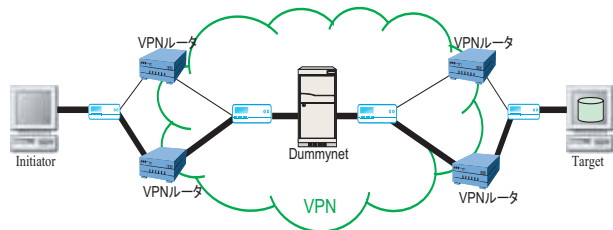


図 9 iSCSI 単数コネクション VPN 単数経路

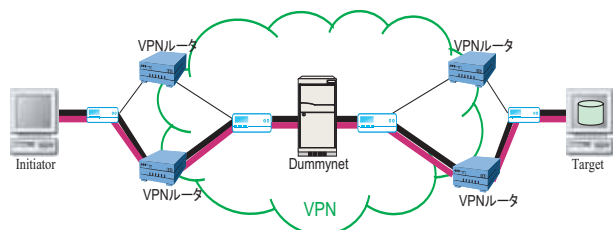


図 10 iSCSI 複数コネクション VPN 単数経路

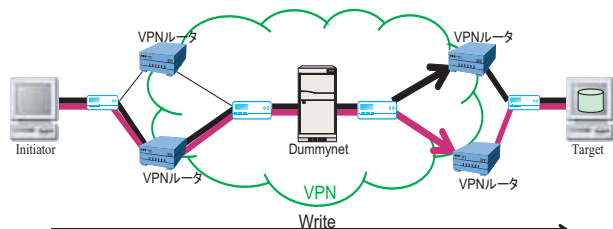


図 11 iSCSI 複数コネクション VPN 複数経路 1

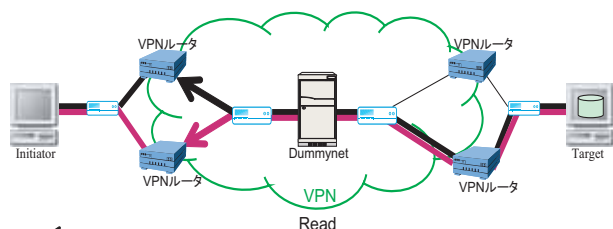


図 12 iSCSI 複数コネクション VPN 複数経路 2

本実験ではストレージアクセスのみの性能を評価するため、Initiator 側では raw デバイスを使用することにより、キャッシュの影響を排除した。また、iSCSI ストレージアクセスにおけるネットワーク性能に焦点を当てて評価を行うため、Target は UNH 実装が提供するメモリモードで動作させ、ディスクアクセスを伴わないようにした。

4. 実行結果

4.1 性能測定結果

4.1.1 ブロックサイズ変更時のスループットの比較

図 13 は iSCSI 単数コネクション VPN 単数経路, iSCSI 複数コネクション VPN 単数経路, iSCSI 複数コネクション VPN 複数経路の、iSCSI ストレージアクセスにおいてブロックサイズを変化させた時のスループット比較のグラフである。この実験において遅延は入れていない。

どの場合でもブロックサイズを増加していくとスループットは増加していくが、ブロックサイズ 512KB を過ぎたところか

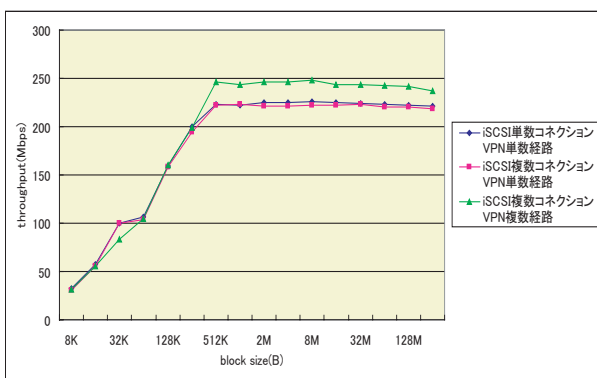


図 13 スループットの比較

らスループットはほぼ一定となる．また，単数コネクション単数経路と複数コネクション単数経路には殆どスループットに変化は見られないものの，複数コネクション複数経路の場合のみスループットが向上している様子が見られる．

複数コネクション複数経路の場合でスループットが向上した結果を考察する．Initiator と Target はギガビットイーサネットで接続しているが，VPN ルータの暗号化速度は最大 500Mbps である．また実際に本実験の VPN 単数経路接続ネットワークのソケット間通信のスループットを測定したところ 330Mbps 程度の性能であった．したがって VPN ルータの暗号化処理が通信のボトルネックとなっており，経路を複数にしたことにより，VPN ルータでの暗号化処理が分散され負荷が軽くなったと考えられる．また 2 つの回線を用いたにも関わらず，2 倍近い性能が得られていないのは，回線が完全に二重化されていないという理由が挙げられる．iSCSI はコネクションへのパケット転送をラウンドロビンによって振り分けているため，複数コネクション複数経路の場合でも 2 つの回線を 1 つずつ交互に使っているだけで，2 つの回線を同時には使っていないためであろう．

4.1.2 片道遅延時間変更時のスループット比較

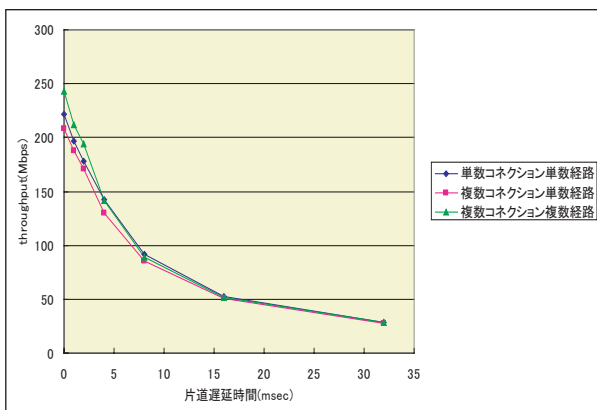


図 14 片道遅延時間とスループット比較

図 14 は iSCSI 単数コネクション VPN 単数経路，iSCSI 複数コネクション VPN 単数経路，iSCSI 複数コネクション VPN 複数経路の，iSCSI ストレージアクセスにおいて片道遅延時間を変化させた時のスループット比較のグラフである．この実験においてブロックサイズは 2MB に設定した．

どの場合も片道遅延時間を長くするとスループットは急激に減少した．また，遅延時間が短い時には複数コネクション複数経路が一番性能が良かったが，遅延時間を長くするとどの場合でも性能に変化がなくなってきている．これは，遅延時間が短い時は複数経路にすることで，ルータでの処理が軽減され性能が向上したと考えられるが，高遅延環境にすると，図 11，12 のように遅延を 2 つのコネクションが通る同一経路上に入れているので，経路の方がボトルネックとなり，性能に差がなくなってきたためであると考えられる．

4.2 輻輳ウィンドウの比較

4.2.1 低遅延環境における輻輳ウィンドウの変化

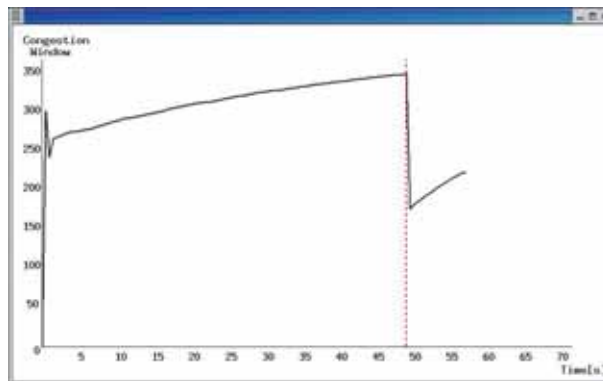


図 15 輻輳ウィンドウ (単数コネクション単数経路)

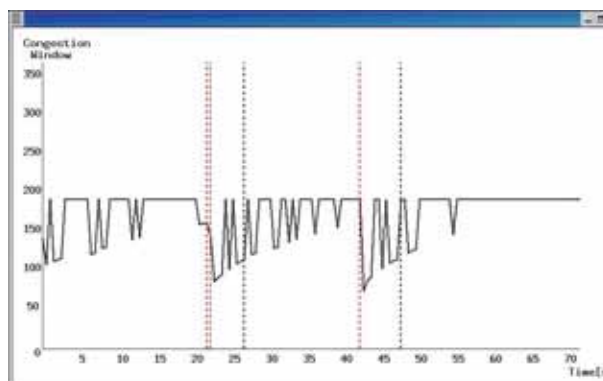


図 16 輻輳ウィンドウ (複数コネクション単数経路)

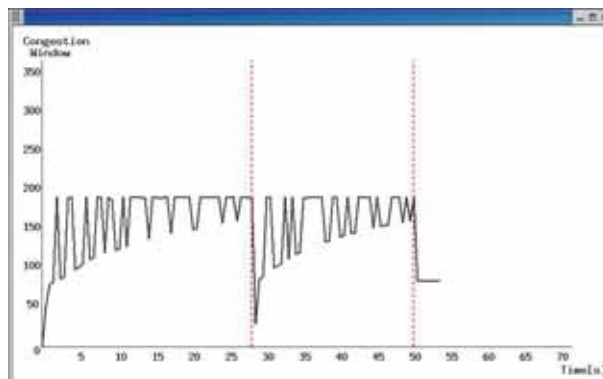


図 17 輻輳ウィンドウ (複数コネクション複数経路)

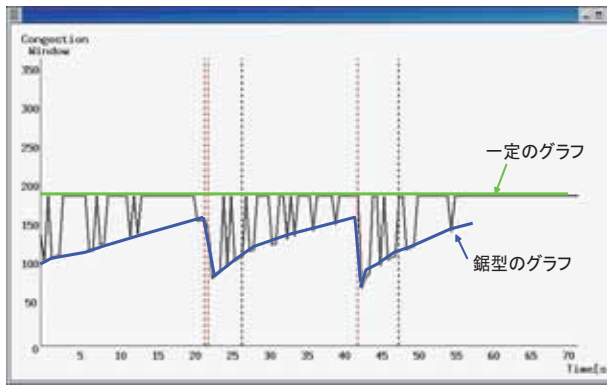


図 18 輻輳ウィンドウ 2 (複数コネクション単数経路)

図 15, 16, 17 は TCP 輻輳ウィンドウをモニタした際の時間変化の様子である。この時のブロックサイズは 4MB, 遅延は入っていない。

図 15 は単数コネクション単数経路の場合に iSCSI シーケンシャルリードアクセス通信を行った時の輻輳ウィンドウをモニタした様子である。また図 15 に示された細かい縦の破線は Local device congestion (CWR エラー) が起こったことを表しており、これは送信側のデバイスドライバのバッファが溢れることによるエラーである。輻輳ウィンドウは約 350 パケットまで増加した後、CWR エラーが検出され急激に減少している。

図 16 は複数コネクション単数経路の場合の輻輳ウィンドウをモニタした様子である。このとき、単数コネクションの場合のグラフと大きく変化している様子が分かる。ここで現れる細かい縦の破線が CWR エラーで、太い縦の破線は重複 ACK, SACK を受信したことによるパケットロスエラーが起きたことを示している。ここで輻輳ウィンドウモニタツールは、2つのコネクションのうち一方でも輻輳ウィンドウの値が変わったら表示されるようになっている。そして可視化されるグラフには、一定時間ごとの輻輳ウィンドウの値が表示される。それぞれのコネクションとも独立で値が変わるため、ランダムにグラフ表示されることになる。すなわちコネクションごとの輻輳ウィンドウは、図 18 のようにそれぞれ一定のものと鋸型のものとなっていると考えられる。

図 17 は複数コネクション複数経路の場合の輻輳ウィンドウをモニタした様子である。このときの縦の破線は CWR エラーを示しており、輻輳ウィンドウの変化は複数コネクション単数経路の場合とほぼ同じになった。

ここで複数コネクションにした場合、図 18 のように一定のグラフと鋸型のグラフになった結果を考察する。2つのコネクションのうちどちらか片方のコネクションが輻輳ウィンドウを使い切ったら ACK が返るまで次の iSCSI アクセス行われなくなる。iSCSI コネクションへのパケット振り分けはラウンドロビンで実行されているので、片方のアクセスが止まってしまうともう片方のアクセスも止まることになる。したがってもう一方のコネクションには輻輳ウィンドウ分を使い切る量のパケットが送られないので、Linux TCP 輻輳ウィンドウの特徴により片方の輻輳ウィンドウは一定となったと考えられる。

次に単数コネクションと複数コネクションの輻輳ウィンドウの違いを比較する。この2つのグラフを比べると、検出されるエラーの回数が複数コネクションの時のほうが単数コネクションの時より多くなっている。また、複数コネクションの一定のグラフと鋸型のグラフの輻輳ウィンドウを足し合わせると、最大で単数コネクションの時の輻輳ウィンドウの値である 350 パケットに近い値をとっていることが分かる。複数コネクションの場合、一定のグラフと鋸型のグラフになるので、その両方の輻輳ウィンドウ分だけパケットは送信されることになる。したがって Target のデバイスドライバが溢れる頻度が高くなるものと考えられる。

4.2.2 高遅延環境における輻輳ウィンドウの変化

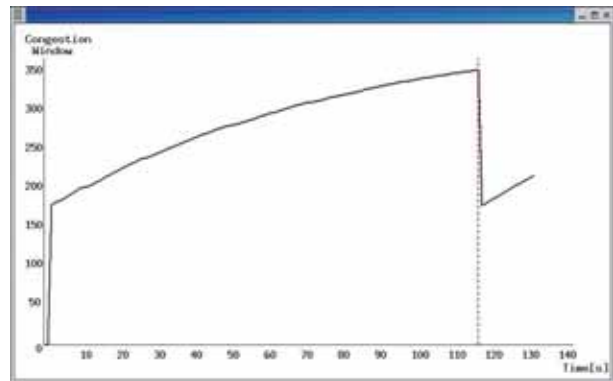


図 19 輻輳ウィンドウ (単数コネクション単数経路)

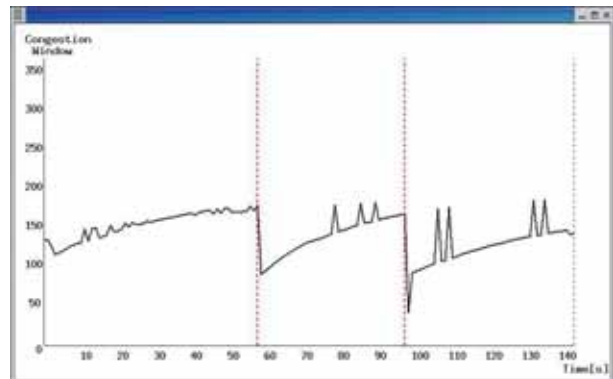


図 20 輻輳ウィンドウ (複数コネクション単数経路)

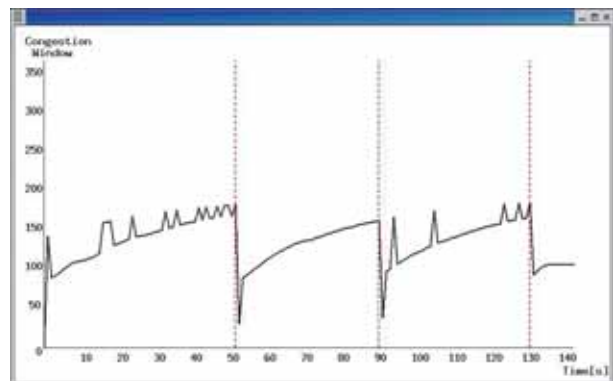


図 21 輻輳ウィンドウ (複数コネクション複数経路)

次に、高遅延環境における輻輳ウィンドウの振舞いを比較した。この時輻輳ウィンドウの振舞がよくわかるように、横軸を 140 秒に拡大した。また、ブロックサイズは 2MB、片道遅延時間は 8msec に設定した。図 19 は単数コネクション単数経路の場合、図 20 は複数コネクション単数経路の場合、図 21 は複数コネクション複数経路の場合の輻輳ウィンドウをモニタした様子である。グラフに現れる細かい縦の破線が CWR エラー、太い縦の破線が重複 ACK、SACK 受信によるエラーである。

単数コネクション単数経路の場合、輻輳ウィンドウの増え方は遅くなっているが輻輳ウィンドウの振舞いは遅延なしの時とほぼ変わらない。一方で複数コネクションの場合、遅延なしの時には一定のグラフと鋸型のグラフとなっていたが、高遅延環境においては、2つのコネクションごとに別々の動きをしているものの、片方が一定とはなっていない。これは低遅延環境においては、片方の輻輳ウィンドウは使い切れず一定の値となっていたが、高遅延環境になるとパケットを送り出してから ACK が返ってくるまでの時間が長いので、どちらのコネクションにおいても輻輳ウィンドウが使い切られて、その結果値が変化しているものと考えられる。

また、どの場合も遅延なしの時は、CWR エラーや重複 ACK 受信によるエラーが起こり輻輳ウィンドウが減少していたが、高遅延環境ではそれ以外にもタイムアウトによるエラーが頻発した。

5. ま と め

本稿では、iSCSI ストレージアクセスにおいてコネクションを単数、複数に変化させ、VPN 接続も単数経路、複数経路に変化させた時のスループットの違いと輻輳ウィンドウの振舞いを観察し、比較した。

その結果、iSCSI 単数コネクション VPN 単数経路と iSCSI 複数コネクション VPN 単数経路を比較すると、スループットはほとんど変わらないが、輻輳ウィンドウの振舞いが大きく変化している様子がわかった。これは iSCSI コネクションが複数になったため輻輳ウィンドウがコネクションごとに異なる振舞いをしているためであると考えられる。さらに、片方のコネクションにより iSCSI アクセスが止められることにより、もう一方のコネクションでは輻輳ウィンドウを使いきれず一定の値となっている。また、iSCSI 複数コネクション VPN 単数経路と iSCSI 複数コネクション VPN 複数経路を比較すると、スループットは複数コネクション複数経路の方が多少向上するが、輻輳ウィンドウはほとんど変化が見られない。これは VPN ルータでの暗号化処理が複数経路となったため負担が軽減されたものと考えられる。

また、高遅延環境においてはスループットはどの場合もほとんど変化がなくなることがわかった。これは遅延を入れたことで、経路によるボトルネックが問題となったためであると考えられる。この時の輻輳ウィンドウは、きれいに一定のグラフと鋸型のグラフとはなっていないものの、2つのコネクションがそれぞれ違った動きをしていることがわかった。さらに、タイムアウトによるエラーが増加していた。

今後はさらに詳しく解析を進め、VPN 複数経路にした場合に性能が向上するような通信を実現させていきたい。

文 献

- [1] iSCSI Specification, <http://www.ietf.org/rfc/rfc3720.txt?number=3270>
- [2] SCSI Specification, <http://www.danbbs.dk/~dino/SCSI/>
- [3] 山口実靖, 小口正人, 喜連川優: "高遅延広帯域ネットワーク環境下における iSCSI プロトコルを用いたシーケンシャルストレージアクセスの性能評価ならびにその性能向上手法に関する考察", 電子情報通信学会論文誌 Vol. J87-D-I, No.2, pp.216-231, 2004 年 2 月
- [4] 千島 望, 豊田 真智子, 山口 実靖, 小口 正人: "VPN 接続環境における TCP パラメータと通信性能の相関関係評価", FIT2006, L-042, 2006 年 9 月
- [5] 千島 望, 豊田 真智子, 山口 実靖, 小口 正人: "iSCSI アクセス時の VPN 環境における TCP 輻輳ウィンドウ制御手法の検討", DBWS2006, pp.709-712, 2006 年 7 月
- [6] 千島 望, 豊田 真智子, 山口 実靖, 小口 正人: "iSCSI における TCP パラメータとアプリケーション実行性能の相関関係評価" 第 68 回情報処理学会全国大会, pp.131-132, 2006 年 3 月
- [7] 豊田 真智子, 山口 実靖, 小口 正人: "高遅延ネットワーク環境における iSCSI リードアクセス時の TCP 輻輳ウィンドウ制御手法の性能評価", SACSIS 2005, pp.443-450, 2005 年 5 月
- [8] 藤原 啓成, 若宮 直紀, 志賀 賢太: "広域 IP 網を介した iSCSI 通信におけるプロトコルチューニングの一検討", 第 68 回情報処理学会全国大会, pp.155-156, 2006 年 3 月
- [9] L.Rizzo: "dummynet", http://info.iet.unipi.it/~luigi/ip_dummynet/
- [10] InterOperability Lab, Univ. of New Hampshire, <http://www.iol.unh.edu/consortiums/iscsi/>
- [11] 富士通 IP アクセスルータ GeoStream Si-R シリーズ GeoStream Si-R570, <http://fenics.fujitsu.com/products/sir/sir570/index.html>