

Resource Guide

Troubleshooting Common Juniper WX/WXC Issues



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Introduction	3
Troubleshooting.....	3
General Issues:	3
TCP and CIFS Acceleration Issues:	4
CIFS Acceleration Issues:.....	6
Appendix A: SMB Signing	11
Appendix B: Juniper WX/WXC Basic Technology Overview	13
Differences Between WX and WXC Devices	13
Overview of WX/WXC Registration Server	13
Overview of Reduction Subnets and Remote Routes	13
Overview of Juniper MSR and Sequence Caching Compression Technologies ..	14
Reviewing TCP Acceleration and Compression Results Using Built-in Reports	15
Protocol-specific Application Acceleration (CIFS).....	17
Reviewing CIFS Acceleration and Compression Results Using Built-in Reports	18
Data Reporting and Network Visibility	21

Introduction

The purpose of this document is to describe some of the more commonly seen problems and solutions that are encountered with application acceleration devices. We will focus on the WX/WXC WAN optimization and application acceleration platforms, but the same fundamentals can be applied to any application acceleration device.

This document assumes some familiarity with the WX/WXC products. A brief overview of the main product differences and basic technologies of the WX/WXC products is provided in Appendix B:

Troubleshooting

General Issues:

Problem:

No compression; Application Flow Pipelining or CIFS acceleration is occurring.

Solution:

1. Check the WX WebView GUI under Reduction / Endpoints on both devices and make sure the tunnels are up in both directions.
2. Check the GUI under Reduction / Subnets on both devices and make sure the proper subnets are configured and include all devices under test.
3. Check the GUI under Reduction / Advanced / Remote Routes on both devices and make sure the proper subnets are being received from the remote endpoint.

Problem:

The WX/WXC devices do not see each other and are not forming tunnels, although they can ping each other.

Solution:

1. Make sure the registration information is correct on both devices. Remember, the password for the registration server is not the same as the admin password. You can use the same password, but they are independent of each other.
2. Re-enter the registration password on the non-registration server box via the GUI Setup / Registration Server and click on "Submit."
3. Go back to Reduction and see if the tunnel comes up. You may need to check it a couple times; refresh this page by selecting Reduction again.

TCP and CIFS Acceleration Issues:

Problem:

FTP and CIFS file transfers appear to be very slow in both directions or in one direction in particular.

Solution:

This is most likely a duplex mismatch issue somewhere in the setup. Check all the device interfaces to make sure they match. By looking in the logs of the WX/WXC device, you can see if any duplex or CRC errors are indicated on any of the interfaces. You can manually change interface settings on the WX/WXC device in the GUI under Setup / Interfaces.

Problem:

FTP and CIFS file transfers are slow or inconsistent.

Solution:

Make sure there is no loss occurring in the network. If loss is configured on the WAN simulator, configure it for no loss and re-test.

Problem:

FTP and CIFS file transfers appear to be slow or inconsistent.

Solution:

1. Make sure the bandwidth configured on the WAN simulator and the QoS speed on the WX/WXC devices both match. If QoS on the WX/WXC devices is set higher than the available bandwidth, it may overrun the intermediate network. As a test, you can adjust the QoS setting slightly less than the WAN simulator's QoS setting – say one to two percent – and re-test to see if this solves the problem. Use the QoS Wizard to change the bandwidth.
2. Try configuring congestion control so it can automatically adjust for the bandwidth of the network.

Problem:

No Application Flow Pipelining statistics are present and performance is not as expected.

Solution:

The initial TCP handshake may not have been seen. Log out of your FTP session or reboot your PC and reconnect.

Problem:

You see CIFS acceleration and Application Flow Pipelining statistics, but performance is much less than expected.

Solution:

Check the compression results; they should be 95 percent or higher. If you are not seeing that kind of compression, sequence caching may not be enabled (if it's a WXC device), or it may be a WX platform. Go to the GUI under Reduction / Network Sequence Mirroring and make sure Network Sequence Caching (or Network Sequence Mirroring in an old Peribit device) is enabled.

CIFS Acceleration Issues:

Problem:

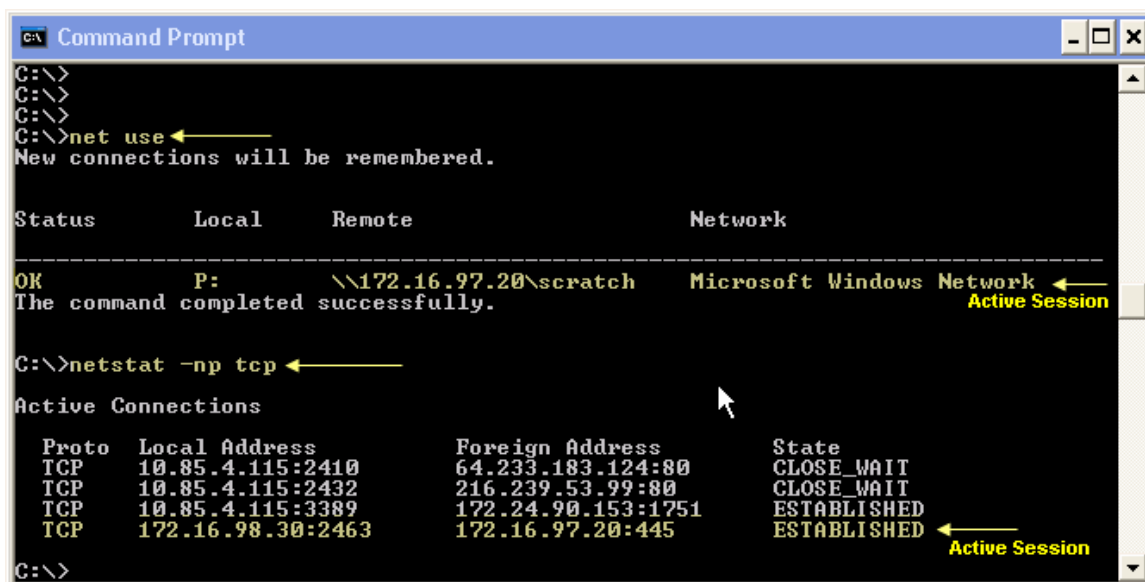
CIFS performance is lower than expected. No CIFS acceleration statistics are present, but compression is good (90+ percent) and TCP acceleration is working correctly.

Solution:

1. The start of the CIFS session may not have been seen. Unmap all drives on the client machine, then remap and retest.
2. Make sure CIFS SMB signing is disabled or that you have configured disabling of SMB signing under CIFS acceleration. Then unmap all drives on the client machine, remap and retest. If this does not work, make sure you verify all the CIFS flows are really gone on the PCs and the WX/WXC devices before re-enabling them.

How to Check for Active CIFS Sessions on PCs and How to Reset Them

Viewing active CIFS sessions:



```

C:\>
C:\>
C:\>
C:\>net use
New connections will be remembered.

Status          Local          Remote          Network
-----
OK              P:            \\172.16.97.20\scratch  Microsoft Windows Network
The command completed successfully.

C:\>netstat -np tcp
Active Connections

Proto  Local Address          Foreign Address        State
TCP    10.85.4.115:2410       64.233.183.124:80     CLOSE_WAIT
TCP    10.85.4.115:2432       216.239.53.99:80     CLOSE_WAIT
TCP    10.85.4.115:3389       172.24.90.153:1751   ESTABLISHED
TCP    172.16.98.30:2463      172.16.97.20:445     ESTABLISHED
  
```

The above example shows what an active CIFS session should look like when typing the “net use” command; note that it displays active network mappings. You can also delete the session with this command.

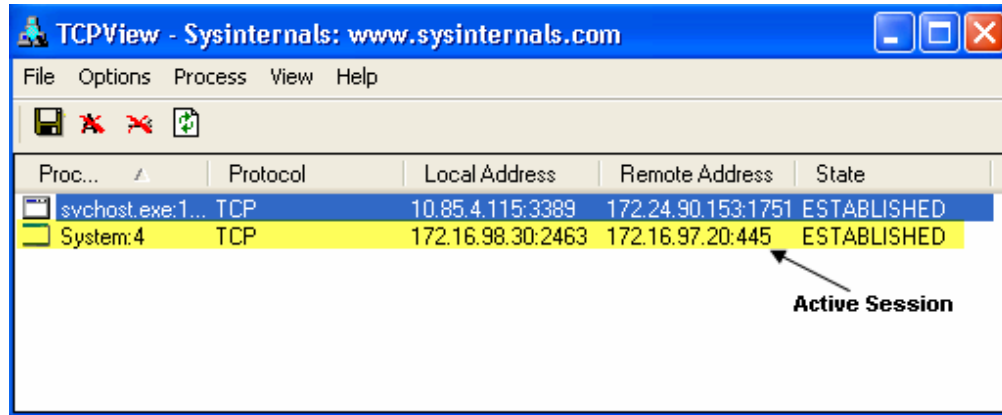
How to reset the CIFS connection with the “net use” command:

To delete the drive mapping in the above case, type “net use p: /delete”

Next, add the drive mapping back with this command: “net use p:
[\\172.16.97.20\scratch](http://172.16.97.20\scratch)”

Alternately, we show what an active CIFS session would look like when typing the “netstat -np tcp” command. In this case, you can see the port number 445 is in use on the connection and it is in an “ESTABLISHED” state.

Viewing active CIFS sessions with TCPview and Resetting them:



TCPView, a free utility available from www.sysinternals.com, allows you to view the active CIFS sessions on the PC in a more graphical way. In the above example, you can see that the highlighted session is using TCP port 445. To close that session down, right-click on that flow and select “Close Connection.”

How do you know the WX/WXC has removed the flow as well?

Once the active session is closed, check the WX/WXC device to make sure that all the flows have been closed.

Viewing active CIFS flows on the WX/WXC platform:

Command Line Interface

Use the field below to enter one or more CLI commands. For help on the use of CLI commands, use the "help" command. For example: "help config app".

show acceleration application cifs status

```
SM-172.16.98.10# show acceleration application cifs status
Active flows: 1
Passive flows: 3
Total flows: 20
Files currently tracked: 1
Accelerated writes: 0
Total writes: 0
Accelerated reads: 0
Total reads: 0
SM-172.16.98.10#
```

To see the active CIFS sessions on the WX/WXC device, you can access the device CLI via the console, via SSH, or through the GUI by going to Admin / Tools / Command Line Interface

Type “show acceleration application cifs status” in the box and press “Submit.”

This will let you know if any active sessions exist and will also indicate whether signed flows were seen. If you see the “Signed Flows” counter listed, then you know signed flows have been seen. These flows cannot be accelerated unless you enable the “Disable SMB signing” checkbox under CIFS Acceleration.

You may also see “Signing disabled flows,” which indicates that signing was optional and was disabled in order to accelerate it.

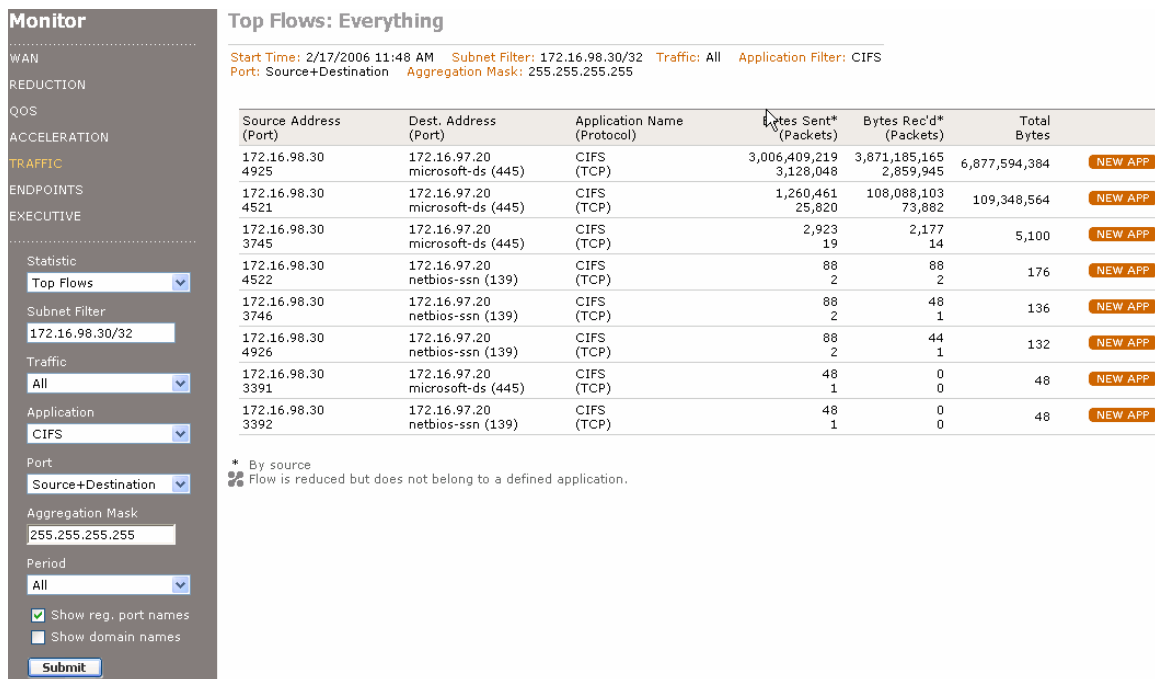
But what if I have mixed counters? I need to look at a specific flow.

If you need to look at a single flow to pin down an issue, or if you are just curious, the following CLI command will show you all the details about a single flow:

```
show flow-details src-ip <IP address> src-port <number> dst-ip <IP address>
dst-port <number> [proto <string>]
```

Here is an example of how you might use this.

1. In the GUI, go to Monitor / Traffic Statistic “Top Flows”



Monitor

WAN
REDUCTION
QOS
ACCELERATION
TRAFFIC
ENDPOINTS
EXECUTIVE

Statistic
Top Flows

Subnet Filter
172.16.98.30/32

Traffic
All

Application
CIFS

Port
Source+Destination

Aggregation Mask
255.255.255.255

Period
All

Show reg. port names
 Show domain names

Submit

Top Flows: Everything

Start Time: 2/17/2006 11:48 AM Subnet Filter: 172.16.98.30/32 Traffic: All Application Filter: CIFS
Port: Source+Destination Aggregation Mask: 255.255.255.255

Source Address (Port)	Dest. Address (Port)	Application Name (Protocol)	Bytes Sent* (Packets)	Bytes Rec'd* (Packets)	Total Bytes	
172.16.98.30 4925	172.16.97.20 microsoft-ds (445)	CIFS (TCP)	3,006,409,219 3,128,048	3,871,185,165 2,859,945	6,877,594,384	NEW APP
172.16.98.30 4521	172.16.97.20 microsoft-ds (445)	CIFS (TCP)	1,260,461 25,820	108,088,103 73,882	109,348,564	NEW APP
172.16.98.30 3745	172.16.97.20 microsoft-ds (445)	CIFS (TCP)	2,923 19	2,177 14	5,100	NEW APP
172.16.98.30 4522	172.16.97.20 netbios-ssn (139)	CIFS (TCP)	88 2	88 2	176	NEW APP
172.16.98.30 3746	172.16.97.20 netbios-ssn (139)	CIFS (TCP)	88 2	48 1	136	NEW APP
172.16.98.30 4926	172.16.97.20 netbios-ssn (139)	CIFS (TCP)	88 2	44 1	132	NEW APP
172.16.98.30 3391	172.16.97.20 microsoft-ds (445)	CIFS (TCP)	48 1	0 0	48	NEW APP
172.16.98.30 3392	172.16.97.20 netbios-ssn (139)	CIFS (TCP)	48 1	0 0	48	NEW APP

* By source
Flow is reduced but does not belong to a defined application.

2. In Subnet Filter, type in the IP address of the device you are interested in with a 32-bit subnet mask. Example: 172.16.98.30/32
3. Set Application to “CIFS”
4. Set Period to “All”

5. Press "Submit"
6. At this point, you should see all the basic flow details
7. Write down the information on the flow you want to look at: source address, source port, destination address, destination port and protocol.
8. In the GUI, go to **Admin / Tools / Command Line Interface**
9. Type in the **show flow-details** command using the information you collected in Step 7 and press "Submit"

Command Line Interface

Use the field below to enter one or more CLI commands. For help on the use of CLI commands, use the "help" command. For example: "help config app".

```
show flow-details src-ip 172.16.98.30 src-port 4925 dst-ip 172.16.97.20 dst-port 445 proto tcp
```

Submit

```
SM-172.16.98.10# show flow-details src-ip 172.16.98.30 src-port 4925 dst-ip 172.16.97.20 dst-port 445 proto tcp

Retrieved flow details with the following parameters:
src-ip = 172.16.98.30, src-port = 4925, dst-ip = 172.16.97.20, dst-port = 445, proto = 6

Flow Details:::

Bytes Sent: -886728238
Packets Sent: 3559925
Bytes Received: 41094231
Packets Received: 3251163
Application Name: CIFS
Application Type: CIFS
Fast Connection configuration: off
Active Flow Pipelining configuration: on
Global Network Sequence Mirroring (NSM) mode: on
NSM application filter: on
Application Acceleration Configurations:
  Global CIFS acceleration mode: on
Traffic Type: Reduced, defined application
Fast Connection (FC) on this flow: Not applied because it is not enabled for FC
Active Flow Pipelining (AFP) on this flow: Applied
Application acceleration on this flow: Applied
SM-172.16.98.10#
```

10. This will show all the flow details, what is enabled, if it is reduced, if AFP and application acceleration are enabled, etc.

Problem:

CIFS performance is lower than expected. No CIFS acceleration statistics are present, but compression is good (90+ percent) and TCP acceleration is working correctly.

Solution:

1. In the GUI, go to Admin / Tools / Command Line Interface. Type the following in the open box: "show acceleration application cifs status"

This will indicate whether you have an active CIFS flow. If not, you should see some indications of why the flow is not active. If you see no active or passive flows and no error flows, you may be looking at the server-side device, not the client-side device. Check the other side.

2. If you see error flows, they will indicate the reason for failure.
 - a. SMB signed flows: This indicates that signing is enabled, and we do not accelerate signed flows. You can disable signing on the machines themselves, or you can set the option for the WX/WXC devices to disable SMB signing when it is optional (see Appendix A: SMB Signing for more details).
 - b. Unsupported Server or Client: As of this writing, the supported CIFS platforms are Windows 2000, 2003 and XP. If you are using Samba or Windows NT, 95, etc., that is probably the issue. We will be adding more server and client support in the future. Contact your sales engineer for more details.

Appendix A: SMB Signing

Basic SMB Requirements for WX/WXC Products

SMB signing must be off for Juniper to accelerate CIFS flows.

In order for SMB signing to be turned off:

- Two talking clients must have the “Digitally Sign Packets (required)” key disabled (this is only on by default in 2000/2003 Domain Controllers)
- If the two talking clients have “Digitally Sign Packets (if possible)” enabled (the default value), then
 - The “Disable SMB Signing” option must be checked on the Juniper WX/WXC (WXOS 5.1.2 or greater) platform

Or...

- Disable the (always) and (if possible) keys on all clients and servers via the group policy

Disabling SMB Signing via Group Policy

Verify that SMB signing is disabled on Windows 2000 and Windows 2003 Domain controllers that are also file servers.

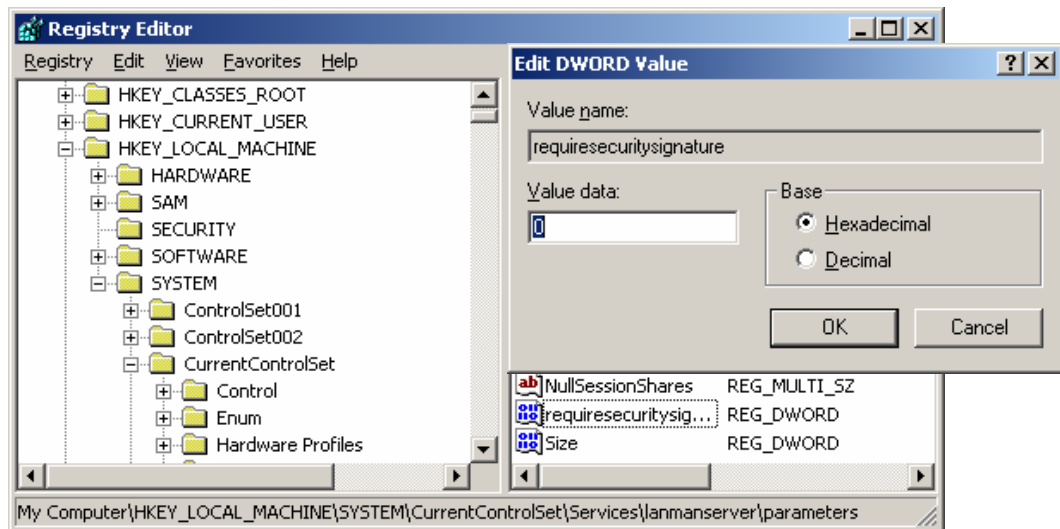
For more information, refer to the Microsoft Web site:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;887429>

1. On a Windows 2000 domain controller:
 - a. Open Active Directory Users and Computers on the domain controller
 - b. Right-click Domain Controllers and select Properties
 - c. Click the Group Policy tab
 - d. Click Default Domain Controllers Policy and select Edit
 - e. Click Default Domain Controllers Policy/Computer Configuration/Windows
2. Settings/Security Settings/Local Policies/Security Options:
 - a. Disable the four signing options:
 - Digitally sign client communication (always)
 - Digitally sign client communication (when possible)
 - Digitally sign server communication (always)
 - Digitally sign server communication (when possible)
3. Reboot all domain controllers, member servers, and clients for which you want to accelerate CIFS traffic

4. To confirm that SMB signing is disabled on Windows 2000 clients:
 - a. Click Start/Settings/Control Panel and select Administrative Tools
 - b. Select Local Security Policy, and then select Local Policies/Security Options
 - c. Disable the four signing options:
 - Digitally sign client communication (always)
 - Digitally sign client communication (when possible)
 - Digitally sign server communication (always)
 - Digitally sign server communication (when possible)

How to Disable SMB Signing via Regedit



- This works only if machines don't log into a domain (otherwise registry edits are over-written by the group security policy)
- On all machines that want to be optimized, set the following DWORD to 0 and reboot
- `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature`
- `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManWorkstation\Parameters\EnableSecuritySignature`

Appendix B: Juniper WX/WXC Basic Techonolgy Overview

Differences Between WX and WXC Devices

The main difference between the WX and WXC devices is the WXC platform includes an onboard hard-drive, enabling it to support Network Sequence Caching in addition to Molecular Sequence Reduction™ (MSR™) compression. (The WX supports MSR only.) This means that, with the WXC platform, you will see maximum compression (95+%) on the second pass of a test file. Also, the WXC platform can compress virtually any type or size of file because it has a much larger dictionary. When troubleshooting WX devices for compression and acceleration, you will need to send a file three times to ensure maximum compression and acceleration results. The examples in this document assume a WXC platform was used for testing, but with the exception of the compression rates all information applies equally.

Overview of WX/WXC Registration Server

When configuring the WX/WXC devices, you will be asked to configure a registration server, which is used to communicate the availability and capabilities of all WX/WXC devices in the network. Any WX/WXC device can be the registration server.

When configuring the registration server, you will be asked to assign a password. You should make a note of the password, because you will need it when configuring the remote WX/WXC device later.

Note: The registration server password is a separate password from the admin password. You can make both of them the same, but each is changed independently of the other. All devices need to use the same registration password to communicate with each other.

The main reason Juniper chose to use this registration model is that it provides a secure method for the devices to authenticate themselves via SSL so that no unauthorized devices can be deployed that may cause network disruptions. This model also provides an automated method for the devices to learn about each other and exchange capabilities. Together, these features provide a secure auto-discovery mechanism that simplifies configuration and setup in complex networks.

Some vendors provide auto-discovery systems that have no authorization process — an approach that could lead to network disruptions due to unexpected traffic patterns. This approach is also much more susceptible to hackers, since no authorization is required. The WX/WXC devices use SSL to authenticate between each other, keeping the whole process secure.

Overview of Reduction Subnets and Remote Routes

The WX/WXC platforms use network subnet mappings to identify traffic that they should reduce. The WX/WXC device matches the destination addresses received on the LAN interface to remote routes received from other WX/WXC devices. If they

match, the WX/WXC platform will apply the appropriate optimization policies to that traffic; if they do not match, the traffic is passed through untouched.

You must make sure that each WX/WXC device has all the local subnets (subnets reachable on this side of the network) configured as Reduction Subnets for which you want the other WX/WXC devices to optimize traffic. You also need to make sure you are receiving the proper remote routes from other WX/WXC devices. Remote routes are the advertised Reduction Subnets from other WX/WXC devices; if you do not have any remote routes in the WX/WXC device, it will not optimize any traffic.

Overview of Juniper MSR and Sequence Caching Compression Technologies

Juniper has two different but complementary technologies for compressing data, Molecular Sequence Reduction (MSR) and Network Sequence Caching. MSR is an algorithm that uses DRAM memory as the repository of the pattern dictionary. It is most useful for applications that use short, chatty transactions — i.e. smaller patterns — but it is also beneficial for medium to larger patterns as well.

Sequence caching uses hard drives as the storage repository for data patterns, making it effective for remembering very large patterns (whole files, bulk file transfers, data base replication).

WX devices run only MSR, while WXC devices support both MSR and sequence caching. From an operational and testing perspective, WXC devices will see little compression results on the first pass of a file but will see dramatic compression results (95+%) on the second pass. WX devices will see varying compression rates on the first pass, usually somewhat better results on the second pass, and the greatest reduction on the third pass. This does not mean the patterns learned are only good for that specific file; these same patterns will be seen in many other similar files, so as the dictionary increases in size, so does the effectiveness of MSR and sequence caching technologies on a broad range of files and data types.

Overview — What is TCP Acceleration?

One advantage of the TCP protocol is that it ensures the reliable transport of data from sender to receiver. TCP accomplishes this reliable delivery by requiring the receiver to send acknowledgements for all data sent by the sender. If a sender hasn't received an acknowledgement, it will resend that portion of data. The amount of data a TCP sender will send before it requires an acknowledgement back is called the TCP window size, which varies by implementation. For example, the IP stack in Microsoft Windows XP has a window size of 64 KB.

On high-capacity or high-latency WAN links, it's possible for the TCP sender to send an entire TCP window of data before it receives any acknowledgements because the WAN link can hold more data than a single window size can fill. In these cases, the overall throughput of the TCP flow is lower than the WAN link can accommodate since the sender stops sending until it receives an acknowledgement indicating that previously sent data successfully arrived.

Juniper's Active Flow Pipelining (AFP) feature removes this flow limitation by building a reliable tunnel between two Juniper devices and using a different, more reliable transport protocol that is not slowed by link latency or bandwidth restrictions. Juniper's AFP feature provides tremendous application performance improvements in many situations, but AFP alone will not improve application throughput in all instances.

Compression or TCP Acceleration Alone is Not Enough

When AFP is combined with MSR and/or sequence caching, the available bandwidth of the connection will be dramatically increased. For example, a T-1 link with 100ms of latency will see no benefit from AFP alone. Compressing traffic by 90 percent increases available bandwidth by 10 times, but throughput can only be increased by about 3.5 times. A standard 64k TCP window at 100ms can only send about 5 Mbps. Combining AFP and compression, however, can expand the pipe by 10 times and fill it at 15 Mbps, a 300 percent increase in performance over compression alone and 1,000 percent improvement overall.

What Types of Applications do AFP and Sequence Caching Benefit the Most?

The applications that will derive the greatest benefit from these technologies are file transfer applications and applications that access large amounts of data – applications like FTP, HTTP file download, file backup, etc. Applications that deal with smaller amounts of data, like HTTP web browsing, will generally see significant improvement, but results will not be as dramatic. Interactive applications will see little or no benefit from AFP and sequence caching, but they benefit tremendously from MSR compression.

Note: You will usually see at least some reduction in the amount of time it takes for the file to be transferred. If the amount of time is slightly longer than the original file transfer, it could be that the file is either random data or is already highly compressed. In these cases, we will add a slight amount of overhead for the initial transaction. However, the file should be reduced dramatically (95+ percent) in the next transfer since its pattern will be stored in the dictionary.

Understanding AFP Results:

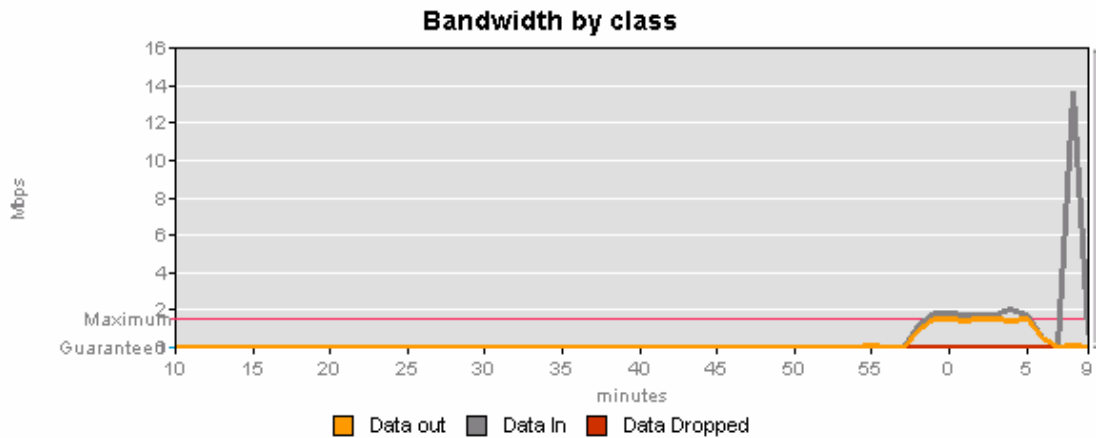
On the first pass of a file you will usually see at least some reduction in the amount of time it takes for the file to be transferred. If the amount of time is slightly longer than the original file transfer, it could be that the file is either random data or is already highly compressed. In these cases, we will add a slight amount of overhead for the initial transaction. However, the file should be reduced dramatically (95+ percent) in the second transfer since its pattern will be stored in the dictionary.

Reviewing TCP Acceleration and Compression Results Using Built-in Reports

Below is an example of a 100 MB zip file being transferred twice. The report is outbound QoS (**Monitor / QoS statistic / Outbound Bandwidth**, below), and the destination is the remote WXC device. The results clearly show that the first time the file was sent, it had little compression and took longer to transfer compared to the second transfer, which had very high compression and transferred much more quickly. The FTP results were 476 seconds for the first time and 11 seconds for the second time – a 98 percent improvement in throughput.

Outbound Bandwidth: Last 60 Minutes

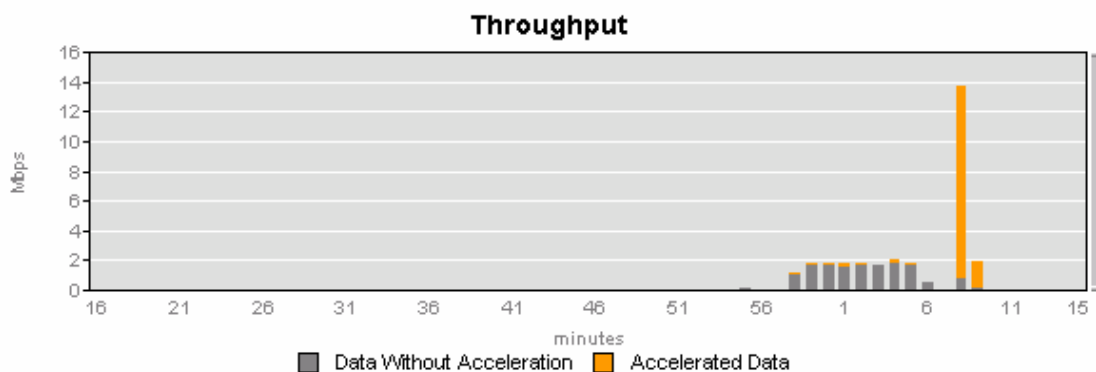
Start Time: 2/12/06 12:10 PM Class: All Destination: 172.16.97.10



The acceleration graph (**Monitor / Acceleration Statistic / Application Flow Pipelining**, below) shows that the first pass of the file saw minimal acceleration, while the second pass shows significant acceleration.

Active Flow Pipelining: Last 60 Minutes

Start Time: 2/12/06 12:16 PM Application: all Destination: all



The WXC platform features a very rich set of reporting capabilities. You may want to look at some of the other reports as well to get a better idea of the type and granularity of data that can be gathered when performing various tests.

Protocol-specific Application Acceleration (CIFS)

Specific application acceleration techniques are required for protocols that run on top of TCP but maintain their own set of rules and flow control — protocols such as the Common Internet File System (CIFS). For example, while TCP usually has a 64 kilobyte window for sending and receiving data, the window CIFS uses can be much smaller — often 32 kilobytes or less. This smaller window size requires many more round trips to complete a transaction. Additionally, CIFS applications usually require many more transactions to complete a given task due to their complexity. When opening a file, for instance, CIFS makes many requests for file attributes such as who owns the file, when it was created, when it was last accessed, etc. Each of these requests is treated as a separate transaction that requires a response before the next request can be sent.

Protocol-specific application acceleration understands how the upper-layer protocol behaves and uses that information to increase the performance of those protocols. For example, if a file is opened from a file server to a client, the WX/WXC device sees the initial file open request and knows that several other smaller transactions are going to take place immediately after the open request. Normally this would require several transactions between the client and server, but when the client-side WX/WXC sees the open request, it also sends requests for the additional items that it knows the client will request next. That way, when the client requests this additional information, it is immediately available and the client-side WX/WXC device responds directly. This type of pre-fetching greatly accelerates transaction times over the normal request-response process that requires additional round trip times for every action.

What Kind CIFS Results Should I Expect ?

Test results will vary based on file size and how files are accessed. CIFS has much more overhead than FTP, and factors such as operating system version, application (Word, Excel, etc.) and application version can affect your results. In general, when doing any copy-type function (drag-and-drop, copy-paste, Robocopy, etc.), you should see a 90 percent or more increase in performance. When opening or saving a file using applications like Word, Excel, etc., expect to see an 80 to 90 percent increase in performance.

CIFS Acceleration Tips

Always make sure you are getting proper acceleration and compression of a well-known application like FTP if encountering issues with CIFS acceleration. The TCP acceleration features must be working for CIFS acceleration to work.

SMB signing should be disabled on the PCs and/or disabled in the checkbox for CIFS acceleration. (See Appendix A: SMB Signing for more details.)

You need to see the beginning of the CIFS transaction for CIFS acceleration to take place. You should delete all drive mappings on the client PC and then remap them or reboot your PC.

Make sure you are using supported operating systems for clients and servers. These include Windows 2000, 2003 and XP. More systems will be supported in the future; contact your sales engineer for details. If you want to test operating systems that are currently not supported, your sales engineer can help you set up the testing.

Reviewing CIFS Acceleration and Compression Results Using Built-in Reports

If you conducted your tests properly, you should see some distinctive patterns in the reports. For instance, you will see the second pass of a file will yield dramatically higher throughput, compression, etc. results than the first pass. This will be most noticeable if using large files that are highly compressible or random data for your samples.

CIFS acceleration is a bit more involved so, in order to get the complete picture, you need to understand all the pieces involved and where you should be looking in order to verify your results.

CIFS acceleration is composed of three parts: compression, application flow pipelining, and CIFS-specific acceleration. It is important to note where each of these happens so that you know where to look. Compression and Application Flow Pipelining happen on the side that is compressing the file (in other words, the side where the file is coming from – server or client). CIFS acceleration happens on the side that mapped the drive to the remote side. This is typically the client side, but since CIFS allows anyone to map a drive, it could be the server side as well.

In a typical client-server setup, this is where you will see the statistics show up, depending on the type of transaction.

When copying files from the server to the client (file open):

- Application Flow Pipelining statistics will be on the server side
- QoS outbound statistics will be on the server side
- Compression statistics will be on the server side
- CIFS acceleration statistics will be on the client side

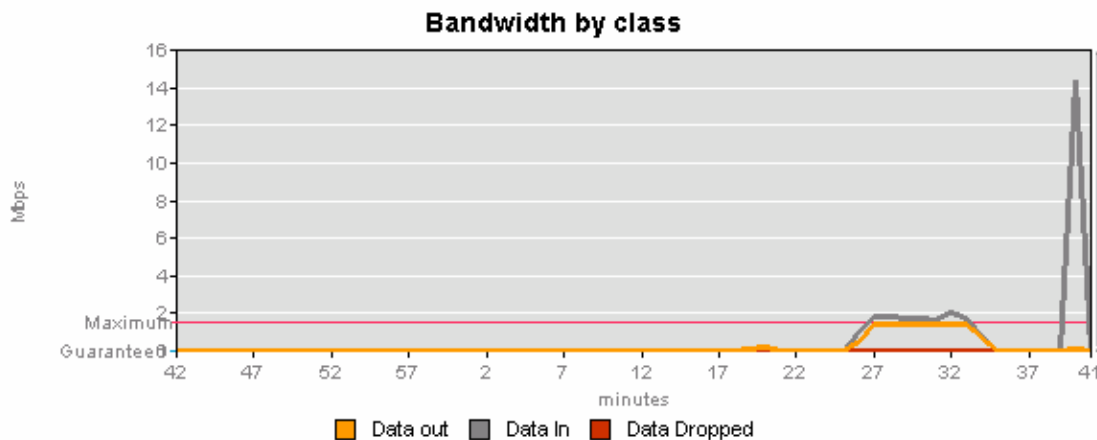
When copying files from the client to the server (file save):

- Application Flow Pipelining statistics will be on the client side
- QoS outbound statistics will be on the client side
- Compression statistics will be on the client side
- CIFS acceleration statistics will be on the client side

Below is an example of a 100 MB zip file being transferred twice via Robocopy from server to client. On the server side, the report is outbound QoS (Monitor / QoS statistic “Outbound Bandwidth”) and the destination is the remote WX/WXC device. You can clearly see that the first time it was sent, there was little compression and the file took longer to transfer compared to the second time, where compression was very high and the transfer time was much faster. The FTP results were 490 seconds for the first transfer and 20 seconds for the second transfer, showing a 96 percent throughput improvement.

Outbound Bandwidth: Last 60 Minutes

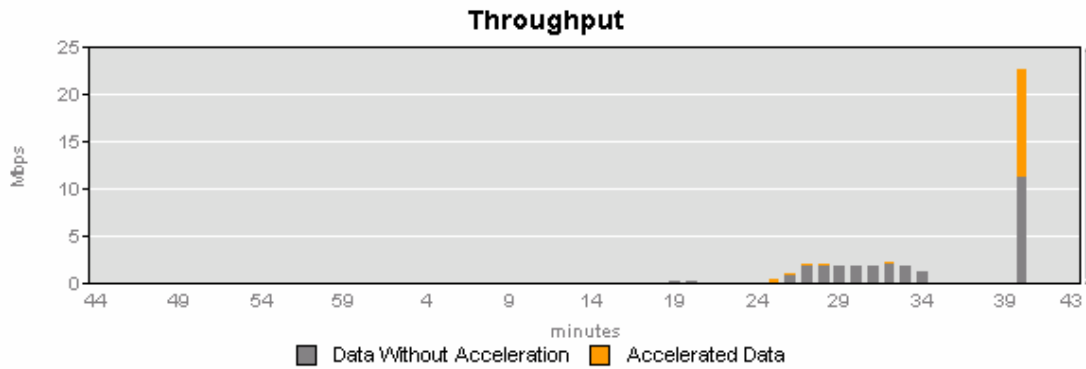
Start Time: 2/12/06 12:42 PM Class: All Destination: 172.16.98.10



Again on the server side, look at the acceleration graph (**Monitor / Acceleration statistic “Application Flow Pipelining”**) and you can see that while the first pass of the file had minimal acceleration, the second pass shows significant acceleration.

Active Flow Pipelining: Last 60 Minutes

Start Time: 2/12/06 12:44 PM Application: all Destination: all



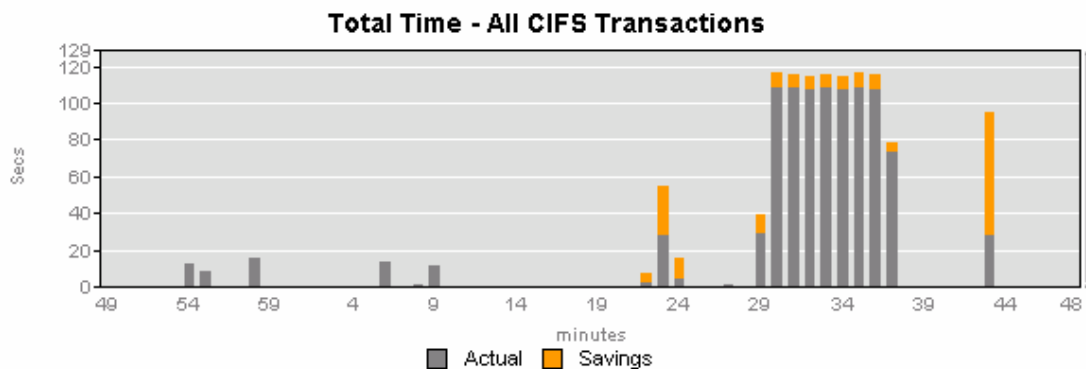
On the client side WX/WXC device, if you look at the CIFS Acceleration report (**Monitor / Acceleration / statistic "CIFS Acceleration"**), it is possible to determine how much transfer time the CIFS acceleration optimizations saved. If you do not see anything on this graph, it could be that the CIFS transaction was not seen by the WX/WXC device or you are looking at the wrong WX/WXC platform. Remember, the CIFS acceleration statistics will only be seen on the client-side WX/WXC device.

CIFS Acceleration: Last 60 Minutes

Start Time: 2/12/06 12:49 PM Application: all Destination: all

Summary

Transaction Type	Total Time (Secs)		Savings	
	Actual	w/o Peribit*	Secs	Percent
All CIFS Transactions	981.37	1,161.09	179.72	15.5%



If you do not see any CIFS acceleration statistics, consult the Troubleshooting section since this typically indicates you are seeing much poorer performance results as well.

The WX/WXC platforms features a very rich set of reporting capabilities. You may want to look at some of the other reports as well to get a better idea of the type and granularity of data that can be gathered when performing various tests.

Data Reporting and Network Visibility

The reports listed above are available via the WebView utility, which ships with the WX/WXC platforms. However, a number of other useful reports and graphs are available through the WX Central Management System™ (WX CMS) software. Working with the WX/WXC products, the WX CMS software provides unprecedented visibility into WAN performance. Examples of some of these reports and graphs are shown below; for a complete list and description of all available reports, see the Monitoring and Reporting section of the WX/WXC Operators Guide.

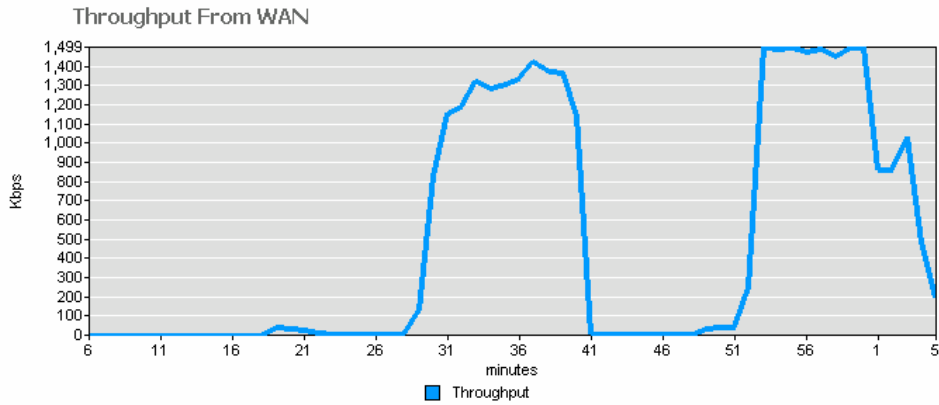
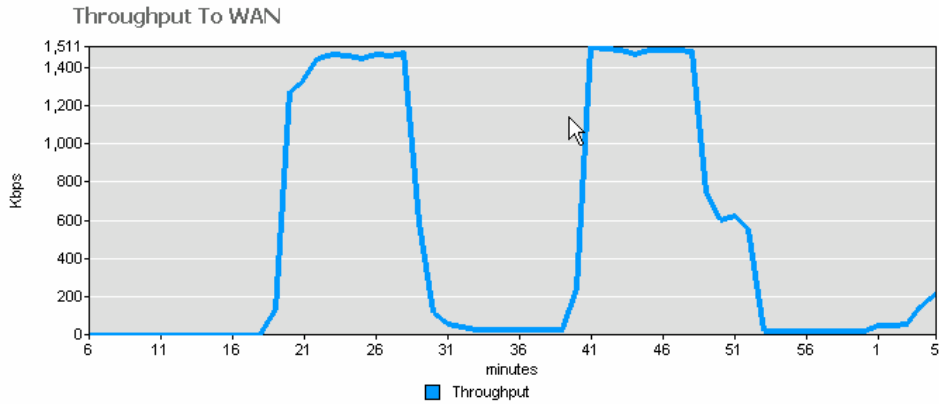
The WX/WXC platforms allow for filtering of all reports as applicable by timeframe, application and destination. The ability to filter traffic by destination is especially powerful as it provides visibility into the network's traffic patterns, not just traffic types and quantity like most devices.

WAN Throughput Graph

The WAN graphs available under **Monitor / WAN** provide throughput data to and from the WAN, Performance Reporting (latency and loss), and Application breakdown.

WAN Throughput: Last 60 Minutes

Start Time: 02/14/06 04:06 PM Application: All Destination: All destinations



Reduction Graphs

The Reduction graphs, available under **Monitor / Reduction**, provide charts showing traffic reduction levels by percentage, byte count, packet count, application breakdown, throughput in vs. throughput out, etc.

Data Reduction: Last 60 Minutes

Show Passthrough Data

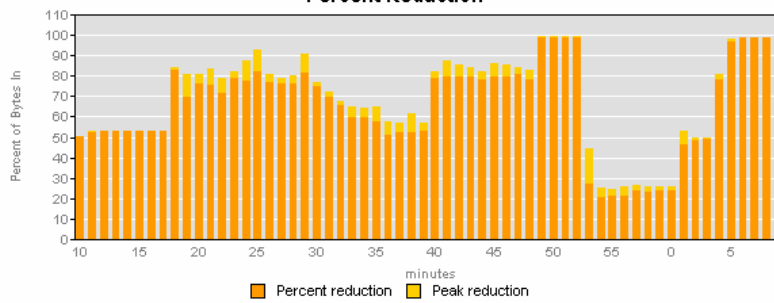
Start Time: 2/14/06 4:10 PM Application: all Destination: all

[Reduction By Endpoint...](#)

Summary

Peak Data Reduction	99.1 %
Total Data Reduction	93.3 %
Effective WAN Capacity	14.83 X
Total Bytes Into Reduction	3.17 GB
Total Bytes Out of Reduction	219.02 MB
Total Bytes Passed Through	0.00 KB

Percent Reduction

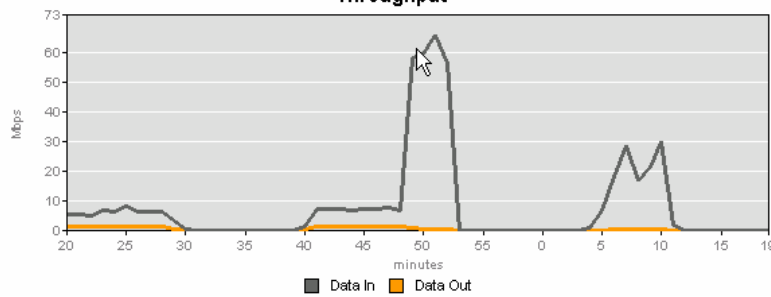


Throughput: Last 60 Minutes

Show Passthrough Data

Start Time: 2/14/06 4:20 PM Application: all Destination: all

Throughput

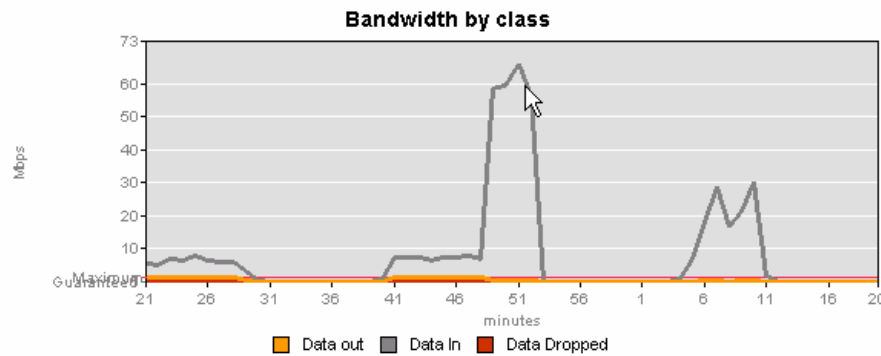


QoS Graphs

The QoS graphs available under **Monitor / QoS** provide charts showing the traffic rate in vs. the traffic rate out, dropped packets, and dropped bytes. The QoS graphs are filterable by traffic class and destination.

Outbound Bandwidth: Last 60 Minutes

Start Time: 2/14/06 4:21 PM Class: All Destination: 172.16.98.10

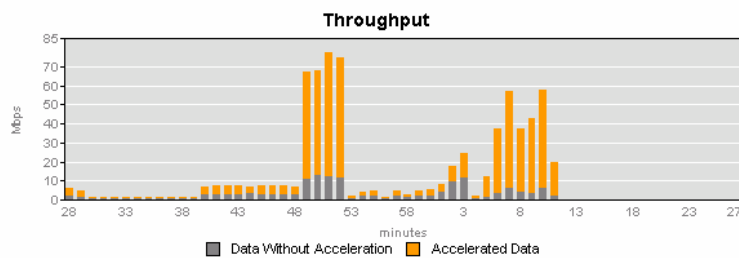


Acceleration Graphs

The Acceleration graphs available under **Monitor / Acceleration** provide charts showing the amount of TCP acceleration, CIFS acceleration, MAPI acceleration, etc.

Active Flow Pipelining: Last 60 Minutes

Start Time: 2/14/06 4:28 PM Application: all Destination: all



Application	Total TCP Sessions (count)	Accelerated Sessions (count)	Traffic (MB)	Average Session Throughput (Mbps)		Acceleration Factor
				Actual	w/o Accel.*	
CIFS	0	0	3114.91	17.72	3.20	5.5 X
AOL	0	0	0.00	0.00	0.00	0.0 X
CVS	0	0	0.00	0.00	0.00	0.0 X