



WANJet User Guide

version 3.1

MAN-0205-00

Service and Support Information

Product Version

This manual applies to product version 3.1 of the WANJet™.

Legal Notices

Copyright

Copyright 2005, F5 Networks, Inc. All rights reserved.

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable iControl user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

F5, F5 Networks, the F5 logo, BIG-IP, 3-DNS, iControl, GLOBAL-SITE, SEE-IT, EDGE-FX, FireGuard, Internet Control Architecture, IP Application Switch, iRules, OneConnect, Packet Velocity, SYN Check, Control Your World, ZoneRunner, uRoam, FirePass, TrafficShield, WANJet and WebAccelerator are registered trademarks or trademarks of F5 Networks, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. F5 Networks' trademarks may not be used in connection with any product or service except as permitted in writing by F5.

Patents

This product protected by U.S. Patent 6,327,242. Other patents pending.

Preface

F5 WANJet™ is a network appliance solution that combines leading-edge WAN optimization technology with high-performance application acceleration techniques. It delivers complete bandwidth utilization, high data and transaction throughput.

This guide describes how to install and use the WANJet. Its intended audience consists of the network administrators, information system engineers, and network managers responsible for the configuration and ongoing management of the F5 WANJet system.

This guide provides information on:

- installing and configuring the WANJet
- using performance reports to monitor WANJet performance
- administration and management of your WANJet system
- advanced configuration involving subnets, hubs, static routes, and VLANs
- configuration of remote WANJets
- managing IT service policies and application QoS policies
- troubleshooting

Conventions Used in this Book

This section explains the conventions used in this book.

`Monospaced font` – This font is used for examples, text that appears on the screen, command line utility names, and filenames.

`<bracketed text>` or *italic text* represents elements in a path or example that are intended to be replaced with information specific to your installation or procedural requirements.

Text of this style is used for elements in the user interface, such as the names of buttons, dialog boxes, and so on.

[Text of this color](#) indicates a link in PDF or HTML that you can click on to navigate to a related section.

Note: Notes mark important information. Make sure you read this information before continuing with the task.

Technical Support Information

Phone	(+1) 206-272-6888
Fax	(+1) 206-272-6802
Web	http://tech.f5.com
FTP	ftp.f5.com
Email	support@f5.com

Contents

Chapter 1 Introduction	1
Overview	2
ACM5	2
Transparent Data Reduction	3
How it works	3
Application QoS	4
Type of Service	5
SNMP Support	5
Remote Monitoring Support	6
System Log Protocol Support	8
Connection Interception	8
When to use Connection Interception	8
How to use Connection Interception	8
Example	9
Chapter 2 Installation	11
WANJet Deployment	12
In-Line Deployment	12
Point-to-Point	12
Point-to-Multi-Point	12
One-Arm Deployment	13
Firewall Guidelines	14
Site Information Worksheet	15
Hardware Installation	16
Chapter 3 Initial Configuration	17
Accessing the WANJet Web UI	18
WANJet Dashboard	20
Basic WANJet Configuration	21
Testing Connectivity	26
Troubleshooting	27
Chapter 4 Monitoring Performance	29
Real Time Traffic report	30
Connection Activity report	31

Throughput reports	32
Performance Increase	33
Actual Bandwidth Expansion	34
Optimized Data	35
Overall Data	36
Link Utilization	37
Customizing reports	38
Passthrough Traffic report	39
Diagnostics	40
Connectivity	41
IP diagnostics	41
Bridge diagnostics	42
Ethernet diagnostics	42
Remote WANJet diagnostics	44
RADIUS status	45
Bridge Forwarding Database	46
Diagnostic Log	47
Administration tools	48
Ping	49
Traceroute	50
Packet capture with tcpdump	51
System Information reports	52
QoS	54
VLANs	55
WANJet Links	56
TCP Statistics	56
Connection States	56
Packet retransmissions	57
Receive queue packets pruned	58
TDR Stats	58
Optimized Sessions	59
Passthrough Sessions	60
Optimize Eligible Connections report	61
Remote Status report	61
Third-party reporting systems	62
Syslog reports	62
SNMP reports	62
RMON2 Reports	63
Chapter 5 Managing the WANJet	65
WANJet authentication	66
Changing the WANJet Web UI password	66
Changing the WANJet LCD PIN code	67
Configuring remote authentication	67

WANJet time settings	69
Setting the timezone	69
Synchronizing WANJet time automatically	70
Setting the time manually	70
Shutting down and restarting a WANJet appliance	71
WANJet boot settings	72
Backup and recovery	72
Autorecovery	73
Upgrading the WANJet software	74
Chapter 6 Advanced Configuration	75
Optimization Policies	76
Adding local subnets	76
Adding remote subnets	78
Configuring Port Settings	78
Configuring Specific Ports	79
Configuring All Other Ports	81
Operational Mode	82
One-arm topology	83
WCCP-based discovery	83
Configuring Tuning Settings	85
Updating the Local WANJet Configuration	86
Adding a Subnet	88
Managing Virtual LANs	88
Managing Remote WANJets	90
Adding a Remote WANJet	91
Redundant Peers	93
Updating the NIC Configuration	94
Managing Static Routes	94
Granting Access to WANJet Web UI	95
Configuring Syslog and SNMP Settings	96
Email alerts	98
Chapter 7 Service Policy Configuration	101
IT Service Policies	102
Adding an IT Service Policy	102
Application QoS Policies	103
Adding an Application QoS Policy to a Remote WANJet	103
Editing and deleting application QoS policies	105
Managing WAN Links	106
Adding a WAN Link	106
Editing and deleting WAN links	107
Adding a Subnet to a WAN Link	107
Editing and deleting subnets	108

Chapter 8 Configuration Examples	109
Basic Configuration	110
Mesh Configuration	111
Hub and Spoke Configuration	113
Redundant Configuration	114
LAN Router Configuration	116
 Appendix A RMON2 Tree	119
MIB Tree	120
Protocol Directory Tree	120
Network Layer Matrix	121
Application Data Matrix	121
Configuration Group	122
 Appendix B WANJet Errors	123
WANJet Error Messages and Codes	124
 Appendix C WANJet Private MIB	127
System Information	128
Ethernet Cards Information	128
MIB File	129

Chapter 1

Introduction

[Overview](#) ◀
[ACM5](#) ◀
[Application QoS](#) ◀
[Type of Service](#) ◀
[SNMP Support](#) ◀
[System Log Protocol Support](#) ◀

F5 WANJet uses adaptive TCP acceleration to address the effects of distance and packet loss.

All application clients and servers are acknowledged locally by the F5 appliance on which the WANJet software resides. The software transparently selects TCP window sizes that achieve the highest possible throughput based on link characteristics, and that minimize retransmission in case of packet loss. The result is 100% utilization of WAN links, even over extreme distances, for both compressed and uncompressed data. The WANJet also “stripes” TCP sessions through multiple parallel, persistent tunnels to reduce TCP overhead and increase effective throughput, or uses a single persistent tunnel if that produces the best results.

Without requiring changes to end points or to the network infrastructure, the WANJet allows enterprises to optimize WAN links both for cost and throughput. Using link load-balancing, the technology can multiplex application traffic across many links, based on traffic level or negotiated rate.

Overview

When you purchase an F5 appliance, you specify what software you want pre-installed on the machine. The F5 appliance can come pre-installed with either the WANJet or the WebAccelerator. The WANJet is designed to improve the performance of your networks, reducing the bandwidth consumed when transmitting data. The WebAccelerator is designed specifically to accelerate your web applications by intelligent caching. For more information on the Web Accelerator, see the *F5 WebAccelerator Getting Started* guide.

In order for the WANJet to reduce the bandwidth consumed in data transmission, it processes data at one side and reverses this process at the other. The WANJet works by identifying redundancy patterns in input data and replacing those redundant patterns with symbols (encoding). When data arrives at its destination, symbols are replaced with the original patterns (decoding). This requires at least two F5 appliances installed, one to process data at one side and another to reverse data processing at the other side. WANJet stores a list of all identified redundancy patterns and their equivalent symbols, enabling it to handle both sent and received data at the same time.

ACM5

Adaptive Control and Management at Layer 5 (ACM5) operates at the session layer of the OSI model. This technology enables the WANJet to recognize the redundancies in data traffic. In order to understand why deploying ACM5 technology is more efficient in data compression than other compression techniques, you have to understand the differences between the WANJet utilizing ACM5 and other compression techniques.

Some applications operate at layer 3 of the OSI model. They wait until individual application data streams merge before searching for redundancies. Merged data streams yield fewer redundancies than unmerged streams, so the layer-3 approach is less than optimal.

Some other bandwidth expansion products operate at layer 7 of the OSI model, the application layer. These products do a great job for specific applications, but other traffic crosses the WAN uncompressed, so overall bandwidth savings are limited.

Operating at Layer 5 is more efficient than operating at any other layer in the OSI model, because unlike data compression based on layer 3, the WANJet compresses data streams before data merge, so it finds and removes more redundancies than layer-3 methods.

Unlike layer-7 techniques, WANJet ACM5 technology examines all applications and compresses all traffic types.

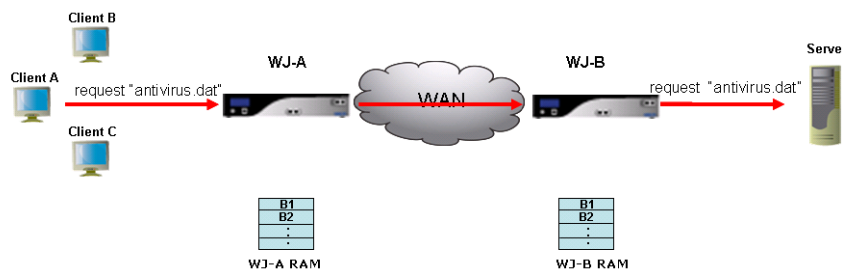
Transparent Data Reduction

F5's TDR (Transparent Data Reduction) technology is a new feature in WANJet 3.1. TDR provides a dramatic reduction in the amount of bandwidth consumed across a WAN link for repeated data transfers. For example, if the same 1MB file is transferred across a WAN link by 100 different users it would consume 100MB of bandwidth without TDR. With TDR the amount of bandwidth consumed would be less than 10MB – a greater than 90% reduction in WAN traffic volume.

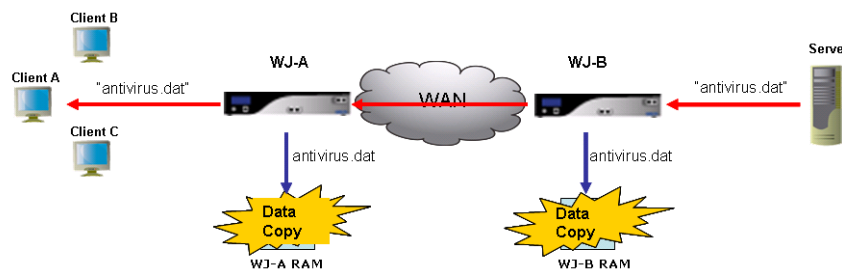
With TDR no files are stored or cached, so data does not go out of date or need to be refreshed. Every request for a piece of data is sent to the server that actually has that data (even across the WAN link). In other words, unlike traditional caching algorithms, no request will ever be served from a local WANJet without the file actually being sent by the server that has the data. As a result, a user can change the name of a file and still experience the same dramatic reduction with TDR.

How it works

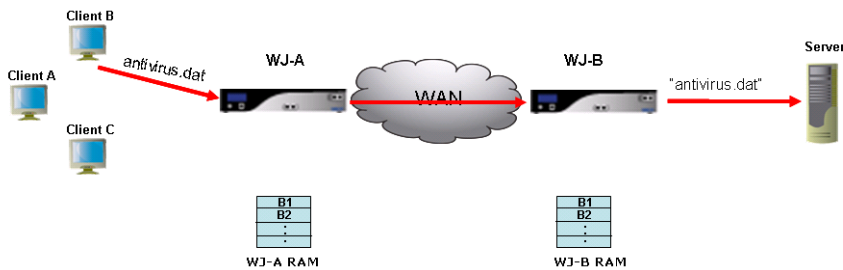
1. Client A requests a file (e.g. `antivirus.dat`):



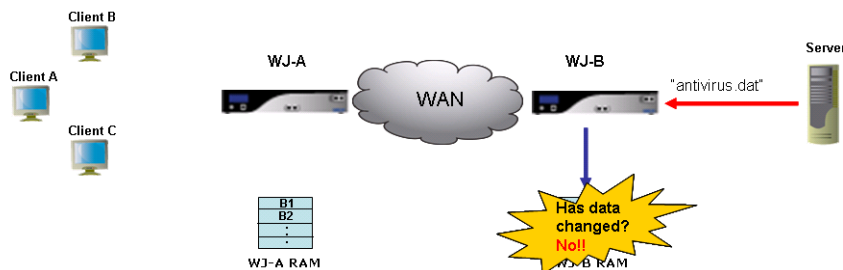
2. Server sends back `antivirus.dat`. WJ-A & WJ-B copy data to RAM:



3. Now Client B requests `antivirus.dat` from server:



4. WJ-B compares file with data in RAM. The data has not changed.



5. WJ-B sends message to WJ-A to use local data because it hasn't changed.
 6. WJ-A sends Client B the data corresponding to `antivirus.dat` from its local RAM. WAN bandwidth is saved!

Application QoS

WANJet Application QoS provides better service for specific data flows by raising the priority of a specific traffic and limiting the priority of other traffics. Accordingly, WANJet Application QoS provides complex networks with a guaranteed level of performance for different applications and traffic types. Your network's data transmission is optimized, providing more control over network resources, and ensuring the delivery of mission-critical data.

Utilizing WANJet Application QoS policies enables you to downsize the bandwidth consumed over low-importance network activities, and at the same time prioritize important and critical data transfer. This way, you are confident that your bandwidth is optimally used for the transfer of the data that is most important to you.

In addition, the WANJet provides high quality of service with applications that are sensitive to delays by supporting the Voice over Internet Protocol (VoIP).

See [Application QoS Policies](#) on page 103 for more details.

Type of Service

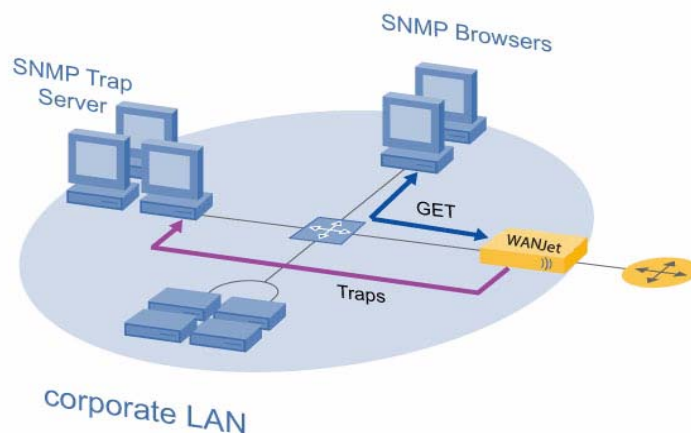
The Type of Service feature aims at providing the highest quality of data delivery through prioritizing the delivery of one data stream over another. The WANJet deploys the Type of Service methodologies, giving you control over your data streams. You decide which data stream should get to the receiver first by using the Type of Service feature to assign a priority to data traffic using a specific port. This means that the data using a specific port is transferred according to its priority. For example, you can decide to give the HTTP traffic the lowest priority while giving the FTP traffic the highest priority. You can assign priorities from 0 to 7, where 0 is the lowest priority, and 7 is the highest. You can assign the same priority, such as priority 7, to multiple protocols.

SNMP Support

SNMP (Simple Network Management Protocol) governs the management and monitoring of network devices. SNMP sends messages to SNMP-compliant servers, where users can retrieve these messages using SNMP compliant-software. SNMP data is stored in a data structure called a Management Information Base (MIB).

The WANJet sends SNMP traps to the SNMP server you specify. The traps you view on the SNMP server are errors for troubleshooting purposes. See [Appendix B, WANJet Error Messages and Codes](#) for error codes and descriptions.

The WANJet also stores more detailed SNMP reports that you can access using SNMP-compliant software. For the SNMP-compliant software to access the WANJet, it should authenticate itself using the community string you specify. The machine on which the SNMP-compliant software resides should have access to the SNMP data in the WANJet Web UI. See [Granting Access to WANJet Web UI](#) on page 95.

Figure 1 WANJet SNMP Data

The Management Information Base that stores the SNMP data contains rich details about the network cards like the network card type, physical address, the card speed, the packets sent and received through each card, the bytes sent and received through each card, and the errors of each card.

In addition, the SNMP reports include detailed information about the WANJet such as total bandwidth saved for sent data and for received data.

For more information about configuring SNMP settings, see [Configuring Syslog and SNMP Settings](#) on page 96.

Remote Monitoring Support

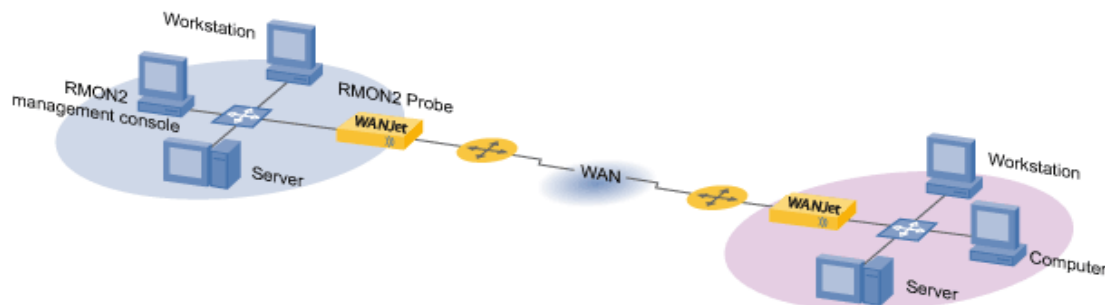
Remote Monitoring (RMON) is an extension to SNMP that provides more comprehensive network monitoring capabilities. It is a network management protocol that monitors different types of data traffic passing through the network. Unlike SNMP, RMON gathers network data from a multiple types of MIB. This provides much richer data about network usage. For RMON to work, network devices, such as hubs and switches, must be designed to support it.

RMON1 MIB standards effort started in 1990 to enable network Administrators to collect information from remote network segments for the purposes of troubleshooting and performance monitoring. RMON1 focused on layer 1 and layer 2

of the OSI model. Due to the high market demand and increasing customer interest, RMON1-compliant software were rapidly developed and brought to market.

RMON2 is an enhanced version of the earlier RMON1 protocol. It differs from RMON1 because it includes more open, comprehensive network fault diagnosis, planning and performance tuning features. In addition RMON2 focuses on the higher layers of the OSI model, layer 3 to layer 6.

Figure 2 WANJet RMON2



The WANJet supports RMON2 to help the user gather, and analyze detailed information about the network traffic either before or after the WANJet processes it, such as:

- data sent and received between two nodes
- IP addresses of these nodes
- port used to send and receive data
- data size before and after the WANJet processes the traffic
- time stamp
- number of connections

The WANJet supports the following RMON2 groups:

Protocol Directory	Contains the protocols for which the agent monitors and maintains statistics.
Network Layer Matrix	Contains the traffic statistics for pairs of network layer addresses.
Application Layer Matrix	Contains the traffic statistics by application layer protocol for pairs of network layer addresses.
Configuration Group	Contains agent capabilities and configurations.

For more information about RMON2 groups, see [Appendix A, RMON2 Tree](#). For more information about configuring RMON2, see [Configuring Syslog and SNMP Settings](#) on page 96.

System Log Protocol Support

The System Log (Syslog) protocol is a mechanism for sending event messages to a Syslog-compliant server. Events can be sent at the start or end of a process or to transmit the current status of a process. The WANJet sends system event messages to the Syslog server you specify. The data log sent by the WANJet includes the sent data, and the received data. In addition, the WANJet sends warning logs to the Syslog server when necessary.

For more information on how to configure the Syslog settings, see [Configuring Syslog and SNMP Settings](#) on page 96.

Connection Interception

CI (Connection Interception) enables WANJet to intercept and reset an existing network connection, to ensure that it is optimized.

When to use Connection Interception

You might use the CI option in any of the following cases:

- Installing WANJet on your network
- Upgrading WANJet
- Changing WANJet mode from Inactive to Active
- Restarting WANJet

How to use Connection Interception

Before carrying out any of the above procedures, make sure that both of the following are true:

- The ports of any connections to be reset have been assigned the ACM5 optimization mode
- The ports have been assigned the “Connection Intercept” option

To assign these options, click on **Operational Settings > Optimization Policy**, and add a new optimization policy for the appropriate port numbers, with **ACM5** and **Connection Intercept** selected.

Refer to [Configuring Specific Ports](#) on page 79 for a more detailed explanation, with screenshots.

Example

You have a backup operation running on the FTP server, and the connection on the FTP port is not optimized for one of the following reasons:

- WANJet is introduced to the network after the FTP connection is opened. So, even if the port of this connection has an optimization policy assigned to it, the traffic of this port will be handled as passthrough.
- WANJet is inactive.
- You are currently upgrading WANJet.

Now you need the FTP data optimized. WANJet allows you to reset FTP connections automatically, without having to either restart the FTP server, or reset FTP connections manually.

To do this:

1. Assign the ACM5 optimization policy to the port(s) of any connections that you need to reset. In this example those would be the FTP ports (normally ports 20 and 21, or ports 989 and 990 for a secure connection).
2. Assign the CI option to the same port number(s).
3. Switch the WANJet operational mode to Active (if it is not already).
4. Restart WANJet. This will force Connection Interception on all configured ports (the FTP ports, in this example). The data using these ports will then be optimized once WANJet has started up again.

Please note that this example is applicable on any port. The best use of Connection Interception is when you want to reset connections on a range of different ports, without having to either reboot the relevant servers or restart a whole range of services.

Chapter 2

Installation

- [WANJet Deployment ◀](#)
- [Firewall Guidelines ◀](#)
- [Site Information Worksheet ◀](#)
- [Hardware Installation ◀](#)

This chapter helps you configure a F5 appliance – with WANJet software installed – on your network. The WANJet appliance is totally transparent to your network, which makes installation and initial configuration easy.

It is important to read this chapter because it provides key information about WANJet installation and configuration guidelines.

WANJet Deployment

There are several ways to deployment WANJet on your network. You can deploy WANJet in-line, in either a point-to-point or a point-to-multi-point configuration. Instead, you might want to deploy WANJet in a one-arm configuration. The way you choose to deploy WANJet depends on your current network topology and requirements.

In-Line Deployment

In-line deployment is the most basic way to deploy WANJet. You can scale it from a simple point-to-point configuration to a point-to-multi-point configuration.

Point-to-Point

This is the simple one-to-one topology. F5 appliances are placed at both ends of the WAN between their respective WAN Router and LAN Switch. Each WANJet is configured to search for traffic matching specified source and destination subnets. If the local WANJet detects a match then traffic is processed and sent down a WANJet tunnel to the remote WANJet that reverses the process and delivers the packets exactly as they were. If there is no match, the local WANJet acts as a bridge and passes the packets unaltered to the WAN.

Figure 3 Point-to-Point Deployment

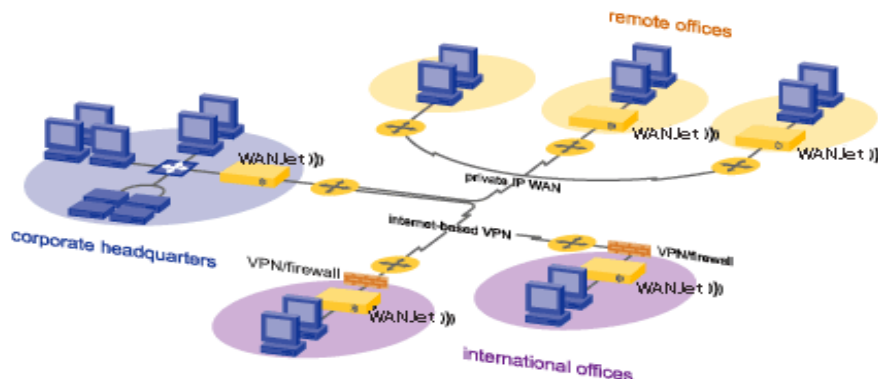


Point-to-Multi-Point

This configuration involves 3 or more F5 appliances. The following figure shows such a deployment involving 5 F5 appliances connecting to each other across intranets and the internet.

As in the case of the point-to-point topology, WANJet processes traffic that matches user-specified source and destination subnets, and then delivers it through a tunnel to the appropriate WANJet across the WAN.

Figure 4 Point-to-Multi-Point Deployment



One-Arm Deployment

A one-arm configuration is more complicated. To decide on the optimal configuration for your system, it helps to understand these three types of one-arm deployment:

- using static routing

WANJet is connected to the LAN switch, and the LAN switch is in turn connected to all the clients on the Network and to the router.

Each and every client on the LAN is configured so that WANJet is its default gateway. All clients' traffic is routed to WANJet.

According to F5 WANJet configuration, it optimizes specific traffic, applies different services on specific traffic, and leaves other traffic untouched. WANJet sends all this traffic back to the router.

- using transparent proxy statically

WANJet is connected to the router directly, so it is transparent to the rest of the LAN clients.

A routing rule is added to the router so that it directs to WANJet only the traffic that WANJet is configured to process (optimize, or apply specific services to). The router is configured so that the passthrough traffic is not sent to WANJet. If you

do not configure the router in this way, the passthrough traffic sent to WANJet is dropped.

According to F5 WANJet configuration, it optimizes specific traffic, and then sends all the traffic back to the router.

- using transparent proxy with the WCCP v2 protocol

WANJet is connected to the router directly and is totally transparent to the LAN clients. All the LAN traffic is routed to WANJet. This part is identical to static transparent proxy.

The difference here is that WANJet communicates with the router using the WCCP v2 protocol. According to its configuration, WANJet decides which traffic to optimize, and which traffic to apply services to. The rest of the traffic is sent back to the router for proper handling.

The advantage to this method of deploying the WANJet is that it is more tolerant of a failure. If WANJet is down, the router compensates and handles the traffic properly without sending it to WANJet.

Firewall Guidelines

If WANJet is placed behind a firewall, you should open the following ports:

Port Number	Used for
53	A UDP port used for DNS
161	A UDP port used for SNMP
162	An optional UDP port used for SNMP traps
22	A TCP port used for SSH
10000	A TCP port used by the Web UI for managing the WANJet
3701	The default port used by WANJet for managing connections
3702	The default port used by WANJet for TCP data tunnels
3703	The default port used by WANJet for UDP proxying over TCP
N/A	(Allow ICMP packets, to enable the F5 appliance to be pinged)

Site Information Worksheet

The site information sheet is intended to capture all relevant site data. Complete the site information sheet and attach a detailed network diagram for each WANJet site.

Table 1 Site Information Worksheet

Site:	Name:		
	Address:		
	City:		
	State/Province, Country:		
Contact Person:	Name/Title:		
	Email:		
	Work phone:	Cell Phone:	
Link:	Type:		
	Speed in Kb/s:		
	Latency:		
	Utilization %:	Peak	Average
Router Information:	Make:	Model:	
	IP:		
	Routing Protocols Used:		
	Static Routing Table Rules:		
Switch Information:	Make:	Model:	
	IP:		
WANJet Information:	Alias	IP:	
	Subnet Mask:		
	Default Gateway:		
Local Network:	Alias:	IP:	Subnet Mask:
	Alias:	IP:	Subnet Mask:
	Alias:	IP:	Subnet Mask:

Table 1 Site Information Worksheet

Remote Network:	Alias:	IP:	Subnet Mask:
	Alias:	IP:	Subnet Mask:

Hardware Installation

See the *Quick Start* guide for the F5 WANJet 200 or WANJet 400 appliance for information on installing F5 appliances and connecting them to your network.

Chapter 3

Initial Configuration

[Accessing the WANJet Web UI](#) ◀
[Basic WANJet Configuration](#) ◀
[Testing Connectivity](#) ◀
[Troubleshooting](#) ◀

After you have completed all the hardware configuration using either the LCD panel or a console connected to the F5 appliance's serial port, all other configuration is performed using a browser-based utility. You can access this utility, called the **Web UI**, from any machine that can run a web browser and has a network connection.

This chapter describes how to log on to the WANJet Web UI and perform the basic configuration needed for the WANJet to begin processing your traffic. This basic configuration is also covered in the *Quick Start* guide that shipped in the box with your F5 appliance. If the basic configuration steps have already been completed, you do not need to repeat them.

Accessing the WANJet Web UI

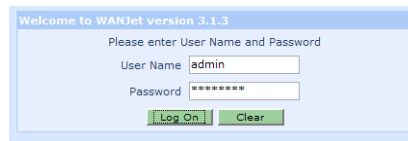
Use the Web UI for all WANJet configuration.

To log on to the Web UI for a particular F5 appliance:

1. Start a web browser and use HTTPS and port 10000 to access the Web UI. For example, if the IP address of the appliance is 192.168.168.102, go to

`https://192.168.168.102:10000`

Tip If your web browser cannot access the Web UI, it is possible that Web UI access has been restricted. You can grant access through the console by specifying the IP address of the machine your browser runs on. Once you have access, you can use the Web UI to change the list. See [Granting Access to WANJet Web UI](#) on page 95.



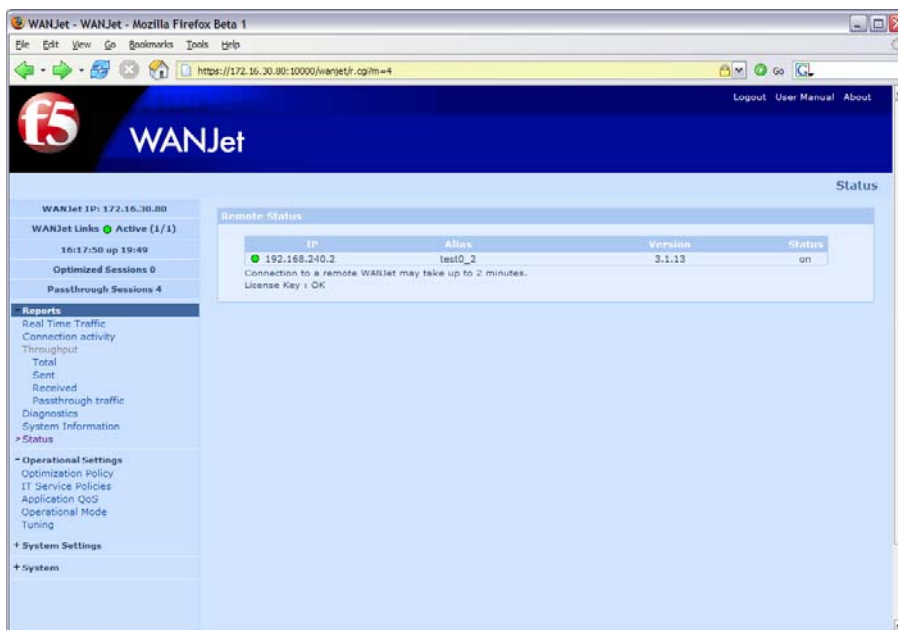
2. When the Welcome to WANJet version 3.1.3 page appears, type `admin` as the username, and enter the default **Password** of `swanlabs` (unless this has been changed by a local administrator).

Note Please change the default password to something more secure at your earliest opportunity. See [Changing the WANJet Web UI password](#) on page 66 for details of how to do this.

3. Click **Log On**. If you like, you can select **Save password** so that you do not have to type in the username and password again. (Only do this if you are the only person who uses your current user account on the computer.)

Tip You will not be able to access WANJet using the Web UI unless you use HTTPS over port 10000 – for example, if you attempt to access the correct IP address using the browser defaults of HTTP over port 80.

The Web UI start page appears. Your F5 WANJet appliance is now online:



When you first log on, the Remote Status page is displayed in the main browser frame. This page displays a quick summary of the status, IP address, alias and software version of connected WANJet appliances. Refer to [Remote Status report](#) on page 61 for more details.

Note When you log into the Web UI for a WANJet appliance, the Web UI treats this appliance as the local WANJet. All other WANJet appliances are treated as remote WANJets. To fully configure each of those WANJets, you must log into the Web UI for each one, using the remote IP address in the URL.

Click on links in the menu bar at the left of the screen to bring up other pages in the Web UI. For example, if a step says to go to the Optimization Policy page, click on **Optimization Policy** under **Operational Settings**. The Remote Status page will then be replaced by the Optimization Policy page in the main browser frame.

Three links always appear at the top right of the Web UI:

- **Logout** logs you out of the Web UI – useful for added security, although your browser session will automatically time out after 30 minutes of inactivity.
- **User Manual** displays the most up-to-date version, in PDF form, of the User Guide (the document you are currently reading).

- **About** displays an informational page, containing:
 - the WANJet version and build number (you should quote these in any support request)
 - a link to your end-user license agreement
 - contact details for your F5 support team.

WANJet Dashboard

For convenience, a variety of status indicators and shortcuts have been placed at the top left of the Web UI, above the **Reports** section of the menu bar. This area is known as the WANJet Dashboard. It is designed so that certain kinds of important information are always available, no matter what part of the Web UI you are working in.

WANJet IP: 172.16.30.80
WANJet Links ● Active (1/1)
22:08:58 up 34 min
Optimized Sessions 0
Passthrough Sessions 1

The Dashboard contains the following sections:

- IP address of the local F5 appliance
- The number of links to remote WANJet appliances, together with the number that are in active mode. A green light is shown if all links are active, a red light if none are active, and a yellow light if only some are active. Click on the word **Active** to display the [Remote Status report](#) (see page 61), which contains more information about each link.
- The current time on the F5 appliance, and the length of time for which the local WANJet has been active (in days, hours and minutes).
- The number of WAN sessions to which ACM5 optimization is currently being applied. This links to the [Optimized Sessions](#) (see page 59).
- The number of WAN sessions for which traffic is being allowed to pass through the F5 appliance, without optimization. This links to the [Passthrough Sessions](#) (see page 60).

Basic WANJet Configuration

Note: If the basic configuration steps detailed in the *Quick Start* guide have already been completed, you can skip the steps in this section.

WANJets must be configured in pairs. Perform these steps for both appliances in your network – that is, both sides of the WAN link. You can perform the configuration functions at each physical appliance, or from a single computer by logging into the Web UI for each appliance.

Assume that there are two appliances, WANJet A and WANJet B, deployed point-to-point (see [Figure 3](#) on page 12 for an illustration):

- a. WANJet A is connected locally and has an IP address of 175.16.2.1
- b. WANJet B is connected at the remote end of the WAN Link and has an IP address of 10.2.0.1

Given this configuration, you would perform the following steps...

Step 1 Log into the Web UI for the first WANJet.

Point your browser to the Web UI for WANJet A. For the example IP address above, you would enter the following URL:

```
https://175.16. 2.1:10000
```

Log in using `admin` as the username and the default password of `swanlabs` (as explained in [Accessing the WANJet Web UI](#) on page 18).

Step 2 Enter the license key and create an alias.

Expand the **System Settings** section of the menu bar, and click on **Local WANJet**.

Local WANJet

WANJet Alias

WANJet IP

WANJet Netmask

WAN Gateway

LAN Router

WANJet Port

License Key - - -

Redundant Peer IP ☐

[VLAN Settings](#)

Note: Click "Save" to apply the changes.
 Changes will not be reflected until the operation is completed.
 In order for WANJet to work properly, you need to replicate the
 Local WANJet changes in the Remote WANJets section of the
 other WANJet(s).

- a. Enter the F5 WANJet license key in the **License Key** field. This key can be found on the Packing List in the box in which the appliance was shipped.

Note: If you are performing a remote upgrade and do not have the new license key, you should click on **Reports > System Information** to obtain the software serial number, and mail this to support@swanlabs.com.

- b. Optionally enter a name for the appliance in the **WANJet Alias** field.
- c. Click **Save** to store this information to WANJet.

Step 3 If your network has multiple subnets, specify the LAN router IP and add subnets.

If your network has multiple subnets, you must set the local router IP address and add local subnets for WANJet. A. Check with your network administrator to find out if you need to specify additional subnets.

- a. On the Local WANJet page, the **LAN Router** field refers to the address of the next-hop router within your LAN. Enter the router's IP address and click **Save**.
- b. Expand the **Operational Settings** section of the menu bar, and click on **Optimization Policy**:

Optimization Policy

Local WANJet: WANJet, 172.16.30.80

Include WANJet Subnet ☒

Local Subnet	Alias
✓ 172.16.30.0/24	

Remote WANJet: test0_2, 192.168.240.2

Remote Subnet	Alias
✓ 192.168.240.0/24	

Protocol	Service	Name Processing	Mode	Compression	Encryption	Connection Intercept	TOS	Priority
TCP	All ports	ACMS	Y	N	N	0 (Low)		
UDP	All ports	Passthrough	N	N/A	N/A	N/A		

Note: Click "Save" to apply the changes.
Changes will not be reflected until the operation is completed.

- c. Ensure that the **Include WANJet Subnet** checkbox is selected. Leave this box checked unless there is a reason not to optimize traffic from the subnet that includes WANJet A.
- d. Click the **Add** button next to the **Local Subnet** section. The Add Subnet page opens in a browser pop-up:

https://172.16.30.80:10000 - Add Subnet - ...

Local Subnet: 175.16.2.0
Netmask: 255.255.255.0
Alias: Subnet A

☒ Enabled ☐ Disabled

OK Cancel

Done 172.16.30.80:10000

- e. Enter the IP address of the subnet in the **Local Subnet** field. The address can use a shorthand format to provide both the subnet address and the subnet mask:

xxx.xxx.xxx.xxx/nn

e.g.

175.16.2.0/24

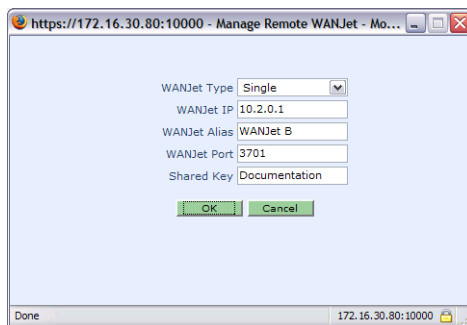
The /24 means that the first 24 bits of the address must match the local subnet address, and the address of any host in the subnet is defined by the last 8 bits of the address. For example, 175.16.2.6 is a valid address for this subnet.

- f. Enter the subnet mask in the **Netmask** field – for example 255.255.255.0. If you entered the subnet address in the /nn format, the corresponding subnet mask is automatically filled in for you.
- g. Enter a string to serve as a name for the subnet in the **Alias** field – for example, Subnet A.
- h. Select the **Enabled** radio button.
- i. Click **OK** to return to the Optimization Policy page. The new subnet is displayed on the list of local subnets. Repeat [Step d](#) through [Step i](#) to add more subnets as needed.
- j. Click **Save** at the bottom of the Optimization Policy page.

Step 4 Define the second WANJet as a remote WANJet

Define WANJet B as a remote WANJet to WANJet A.

- a. Click on **System Settings > Remote WANJets** in the menu bar.
- b. On the Remote WANJets page, click **Add**. The Manage Remote WANJet page is displayed in a new browser window:



- c. Enter the IP address of WANJet B in the **WANJet IP** field – in this example, 10.2.0.1
- d. Enter WANJet B (in this example) in the **WANJet Alias** field.
- e. Enter a **Shared Key** for the WANJet pair. The shared key is a character string that is assigned by your network administrator. The only requirement is that the key must match for any pair of WANJets (that is, you must use the same key when adding WANJet A as a remote WANJet to WANJet B).

- f. Leave all other fields as they are and click **OK**. WANJet B is now listed on the Remote WANJets page. Click **Save** to store the changes to WANJet A.

Step 5 Log out of the first WANJet Web UI

Click **Logoff** on the upper right of the Web UI. Close the browser window.

Step 6 Log in to the Web UI for the second WANJet.

Open a new browser window and enter the URL with the example IP address for WANJet B:

`https://10.2.0.1:10000`

Log in using `admin` as the username and the default password of `swanlabs`.

Step 7 Verify the license key and create an alias.

Expand the **System Settings** section of the menu bar, and click on **Local WANJet**.

- a. Check the F5 WANJet license key in the **License Key** field. The key should match the License Key Certificate found on the Packing List in the box that the WANJet B appliance was shipped in.
- b. Optionally enter a name for the appliance (such as WANJet B) in the **WANJet Alias** field.

Step 8 If your network has multiple subnets, specify the LAN router IP and add subnets.

If you defined a LAN router and added subnets for WANJet A, you probably need to repeat this step for WANJet B (unless it is on a simpler LAN). Refer back to [Step 3](#) for details of how to do this.

Step 9 Define the first WANJet as a remote WANJet

Now define WANJet A as a remote WANJet to WANJet B.

- a. Click on **Remote WANJets** under **System Settings** on the menu.
- b. Click **Add** in the Remote WANJets page to display the Manage Remote WANJet page in a browser pop-up.
- c. Enter the IP address of WANJet A in the **WANJet IP** field – in this example, `175.16.2.1`
- d. Enter the appliance name in the **WANJet Alias** field, in this example, `WANJet A`.
- e. Enter the **Shared Key**. This should be the same key that you entered for WANJet B when you were configuring WANJet A locally (see [Step 4](#)).

- f. Leave all other fields as they are and click **OK**. WANJet A is now listed on the Remote WANJets page.
- g. Click **Save** to store the changes to WANJet B.

Note Once the WAN link between the WANJet pair is configured as above, subnet specifications are automatically exchanged between the appliances. For example, the local subnets specified for WANJet A are copied in as remote subnets for WANJet A in WANJet B's "Remote WANJet" configuration information.

Testing Connectivity

To test the connectivity between the local WANJet and the remote WANJets, perform these checks for each appliance:

Check status

- Click **Reports > Status** in the menu bar to view the status of the remote WANJet(s). A green light displays next to the IP address of any remote WANJets that are enabled and connected.

Check reports

- If you have traffic passing through the network, click any of the throughput reports (**Total**, **Sent**, or **Received**) in the **Reports** section of the menu bar. Optimized Traffic reports should be available.

Check diagnostics

- Click **Reports > Diagnostics** in the menu bar, and then click on **Connectivity > Remote WANJets**. On the Diagnose Remote WANJets page, check the `Tunnel status` for each remote WANJet. The status should be `up`.

Troubleshooting

Some common problems are listed below. If you cannot find your problem here, please contact support@swanlabs.com.

I cannot ping the F5 appliance

Make sure the computer you are pinging from has a valid network connection. Try pinging other known devices. Go to the LCD display and make sure you have the correct IP address for the appliance.

I can ping the F5 appliance, but I cannot ping the WAN gateway

Re-check the cabling as described in the *Quick Start* guide. Make sure the gateway router is connected to the WANJet WAN port with the supplied crossover cable.

I cannot see that the WANJet is optimizing traffic or the optimization is extremely low

Review your configuration of local and remote subnets at both appliances. You might have heavy traffic on a subnet that is not included in WANJet's configuration. Make sure you include all subnets for which traffic should be optimized.

My browser connection times out when I attempt to access the Web UI

Check that you are accessing the correct URL for the Web UI. Entering just `http://` followed by the F5 appliance's IP address will not work: you need to connect to port 10000 using the secure HTTPS protocol, e.g.

`https://123.123.123.123:10000/`

See [Accessing the WANJet Web UI](#) on page 18.

I cannot start the Web UI: I get a Page Not Found error

If the F5 appliance appears to be running, and you are sure you are entering its URL correctly in your web browser, the computer on which you are running your web browser might not have access to the Web UI. The default setting is to grant access to all machines, but that setting can be changed to limit access based on IP address.

You can use the LED panel to add your computer's IP address to the list of machines with access. After that, use the Web UI to change the access settings. See [Granting Access to WANJet Web UI](#) on page 95.

I can access the Login screen for the Web UI, but my browser connection times out when I try to log in

The RADIUS authentication server may not be accessible to WANJet. Try to log in as a local user, using the `admin` username and a default password of `swanlabs` (though this may have been changed by a local administrator). Once you are logged in, click on **System Settings > Remote Authentication**, and check that:

- a. RADIUS authentication is enabled
- b. the Timeout and NRetry variables are set to sensible values (i.e. if both are high, authentication might take a long time to fail).

Refer to [Configuring remote authentication](#) on page 67 for more details.

The Link LED (for the WAN or LAN port) doesn't light up

Verify that your cables are installed properly. Next, verify that the ports on the WAN Router and the LAN Switch connected to the F5 appliance are set to auto-negotiate. If either port is forced to a specific link speed and duplex value, you must set the WANJet port to match this value. To reset the NIC configuration (link speed and duplex value) for a WANJet port, see [Updating the NIC Configuration](#) on page 94.

Note: F5 strongly recommends that if you force the link for one of the WANJet ports, you force the link for both ports. This prevents any link problems in pass-through mode if power to the WANJet device is lost.

Chapter 4

Monitoring Performance

- Real Time Traffic report ◀
- Connection Activity report ◀
- Throughput reports ◀
- Diagnostics ◀
- System Information reports ◀
- Remote Status report ◀
- Syslog reports ◀
- SNMP reports ◀
- RMON2 Reports ◀

The WANJet Web UI includes many different reports that you can use to monitor your F5 appliance's status, connectivity and performance.

Most reports fall into one of three categories: **Throughput**, **Diagnostics** or **System Information**. You can access reports in these categories by clicking on the appropriate link in the **Reports** section of the menu bar, and selecting a detailed report name in the page that is then displayed. Three other reports – **Real Time Traffic**, **Connection Activity** and **Remote Status** – are important enough to have their own links in the menu bar.

Note: To ensure accurate reports, synchronize WANJet time regularly to update your appliances' time settings and ensure that the reports' time settings are adjusted. You can do this using the **System Settings > Time** option (see [WANJet time settings](#) on page 69).

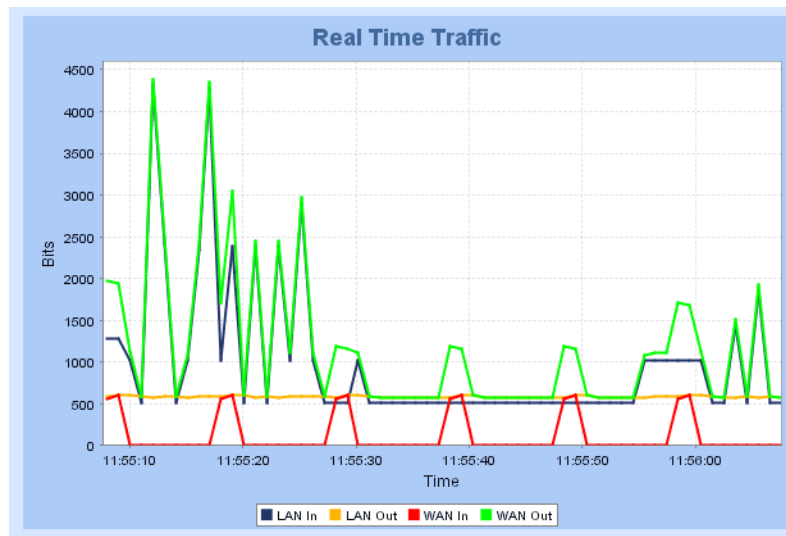
This chapter also covers other ways of obtaining information about WANJet's performance, including network diagnostic tools, operational logs, and integration with third-party reporting tools.

Real Time Traffic report

The Real Time Traffic report shows a graph of total network traffic, in real time, over both the LAN and the WAN. It therefore provides an at-a-glance overview of the network loads passing through your F5 appliance.

To view a graph of network traffic in real time:

- Go to the **Reports** section of the menu bar, and click on **Real Time Traffic**. The Real Time Traffic page is displayed:



In this graph:

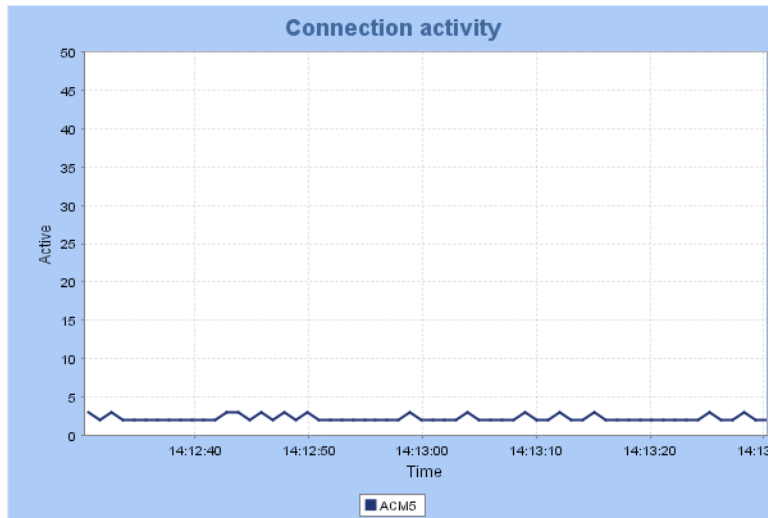
- The vertical axis indicates the amount of network traffic (in bytes per second)
- The horizontal axis indicates the time (24-hour clock, showing hours, minutes and seconds, to the nearest ten seconds)
- The blue line (**LAN In**) represents raw data destined for the WAN passing into the local WANJet from the LAN
- The yellow line (**LAN Out**) represents optimized data passing out of the local WANJet en route to the remote WANJet
- The red line (**WAN In**) represents optimized data passing into the local WANJet from its remote partner
- The green line (**WAN Out**) represents reconstituted data passing out of the local WANJet and into the LAN

Connection Activity report

The Connection Activity report enables you to view, in real time, a graph of the number of active ACM5 connections managed by WANJet – that is, the number of network connections that are currently being optimized.

To view a graph of active connections:

- In the **Reports** section of the menu bar, click on **Connection activity**.



In this graph:

- the vertical axis indicates the number of active connections
- the horizontal axis indicates the time (24-hour clock, showing hours, minutes and seconds, to the nearest ten seconds)
- the blue line represents the change in the number of active ACM5-optimized connections over time

Throughput reports

There are several types of reports you can generate on traffic processed by the WANJet. The Web UI enables you to choose any combination of traffic direction, data type and time period for generating a report. All throughput reports refresh automatically every two minutes.

At the top of the page, there is a summary of the amount of data (in megabytes) handled before and after compression, and the compression ratio achieved (expressed as a percentage). These figures will vary according to the time period selected, and whether you are viewing Total, Sent or Received data. You can also change the type of information that appears here by clicking on **Customize Report** beneath the report graph itself.

To display a throughput report:

1. Click **Reports > Throughput** in the menu bar
2. Select the direction of traffic by clicking **Total**, **Sent**, or **Received**:
 - **Total** generates reports about all the traffic that the WANJet processes
 - **Sent** generates reports about only the outgoing (sent) data processed by the WANJet
 - **Received** generates reports about only the incoming (received) data processed by the WANJet
3. Next, select one of the report links to display the type of data you want to see:
 - [Performance Increase](#)
 - [Actual Bandwidth Expansion](#)
 - [Optimized Data](#)
 - [Link Utilization](#)
 - [Overall Data](#)

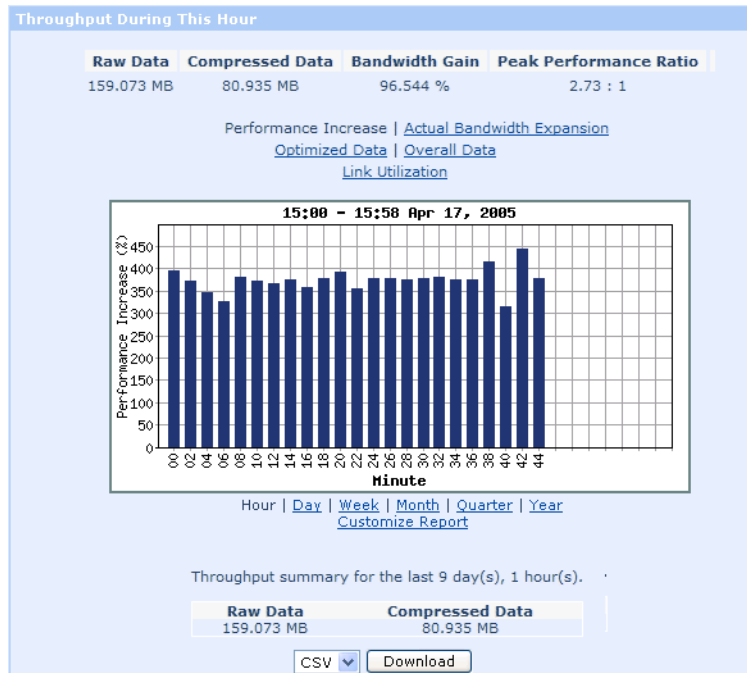
By default, the **Performance Increase** report is displayed.
4. Underneath every chart are links that enable you to select the time period for which data is collected. Click on the appropriate link for the time period over which you wish to view data. A report for the current day is displayed by default.

Note The WANJet saves all the generated reports for the last hour, every hour. If you stopped or restarted the WANJet, or any external termination occurred, you will be able to access the last set of saved reports when you restart the WANJet.

5. At the bottom of the page, select **CSV** and click **Download** to save a copy of the report in CSV (comma-separated) format on your local computer. CSV reports can easily be imported to a database, or analyzed using a spreadsheet package.

Performance Increase

The Performance Increase report enables you to view the percentage increase in bandwidth due to using the WANJet.



In this graph, the vertical axis indicates the percentage increase in bandwidth. This is calculated by comparing the bandwidth freed up by the WANJet to the bandwidth used after optimization:

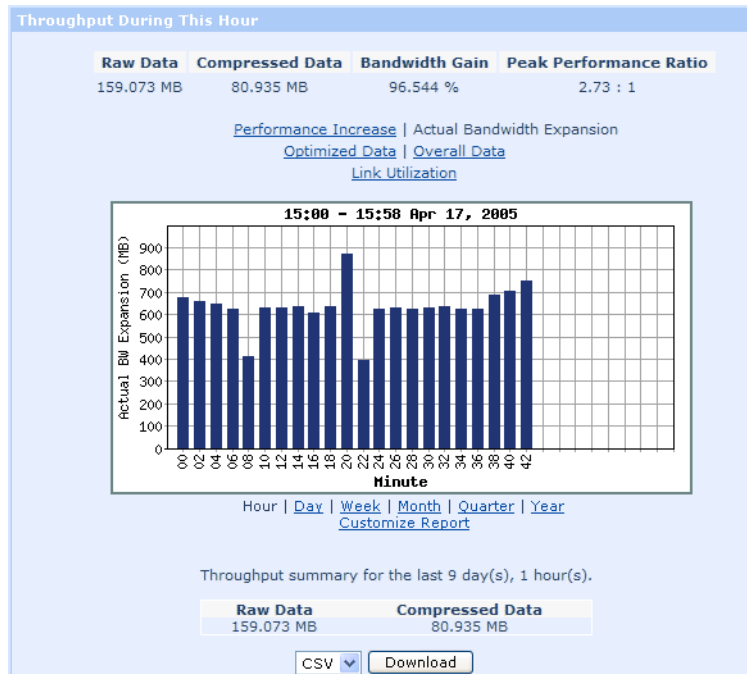
$$(\text{Freed Bandwidth} / \text{Bandwidth after optimization}) * 100 = \text{Percentage Performance Increase}$$

For example, if your bandwidth before the WANJet was 100MB, and the bandwidth used by data after the WANJet is 25MB, then the amount of bandwidth freed up by the WANJet is 75MB. Putting these values into the equation results in:

$$(75\text{MB} / 25\text{MB}) * 100 = 300\% \text{ performance increase}$$

Actual Bandwidth Expansion

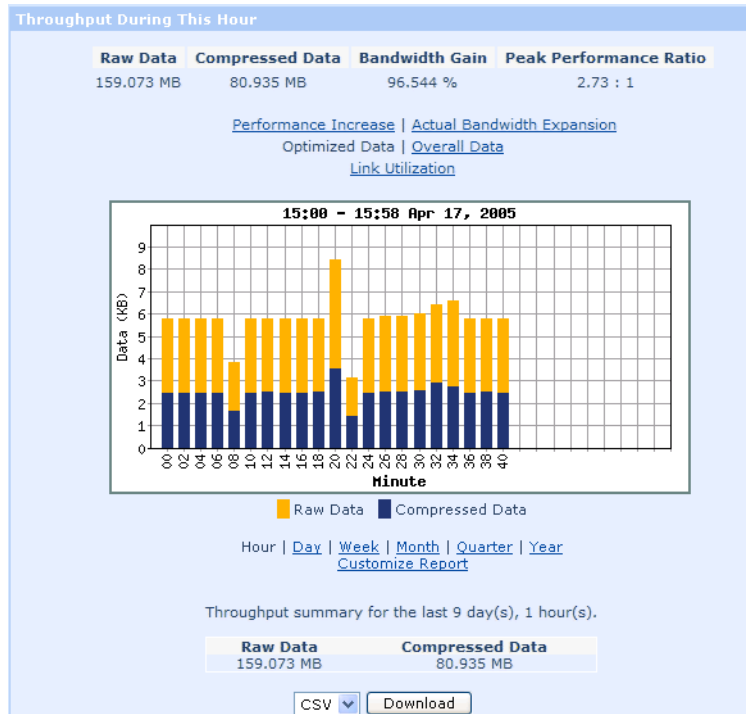
The Actual Bandwidth Expansion report enables you to view the actual bandwidth amount that the WANJet has freed up by optimizing network data.



The vertical axis represents the bandwidth expansion in kilobytes, megabytes, and so on (the unit used changes depending on the extent to which the bandwidth has expanded over the selected time period).

Optimized Data

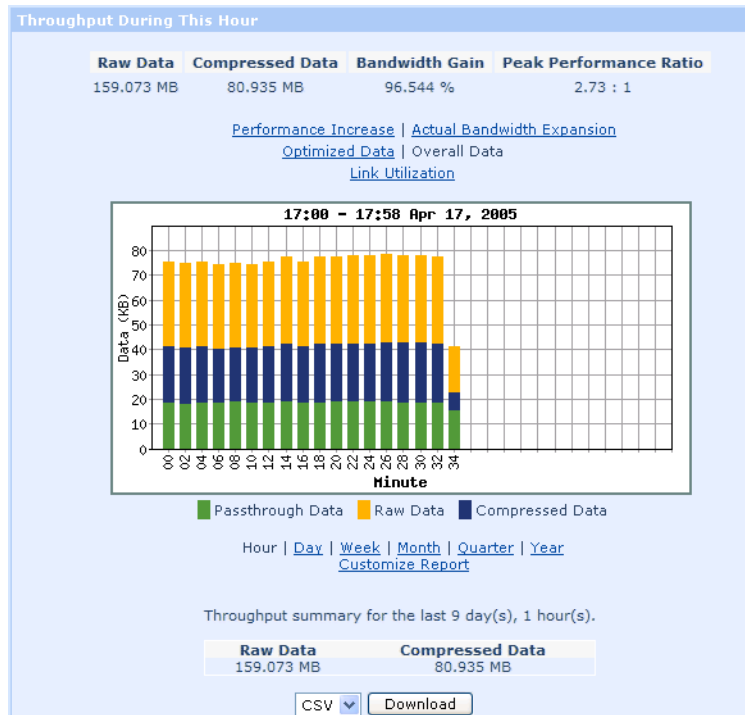
The Optimized Data report allows you to compare the difference in the amounts of network traffic before and after the WANJet processes your data.



The vertical axis indicates the amount of network traffic before and after optimization (in kilobytes, megabytes, etc). The blue bar represents the amount of traffic before optimization, and the yellow bar represents the amount of freed bandwidth.

Overall Data

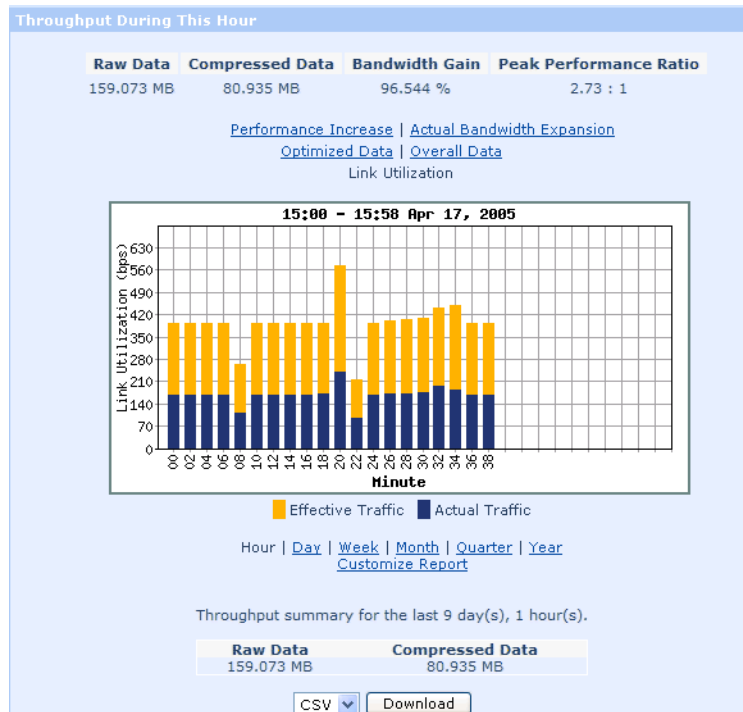
The Overall Data report allows you to compare amounts of passthrough data, raw data, and optimized data.



The vertical axis indicates the amount of data passing through the link (in KB, MB, GB, and so on). The green bars represent the amount of passthrough data, the blue bars represent the amount of compressed (optimized) data, and the yellow bars represent the amount of freed bandwidth. Therefore the bars as a whole represent the total amount of data passing through the F5 appliance.

Link Utilization

The Link Utilization report is similar to the Optimized Data report (see page 35). Instead of showing the total amount of data optimized over a given time period, however, this report shows the average amount of bandwidth used per second, compared to what would have been used if network traffic had not been optimized.



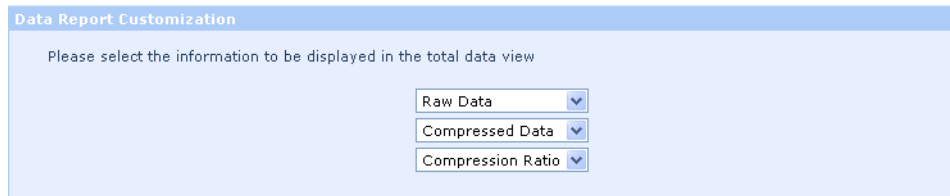
The vertical axis indicates the amount of bandwidth (in kilobits per second, megabits per second, and so on). The blue bars represent the actual bandwidth used. The bars as a whole represent the amount of bandwidth that would have been used if network traffic had not been optimized; therefore, the yellow bars represent the amount of bandwidth saved.

Customizing reports

You can change the appearance of the reports and the way that certain fields are displayed. Reports for each type of traffic (total, sent, and received) can be customized individually.

Under **Reports** on the menu, select **Total**, **Sent**, or **Received**. On the report page, click on the **Customize Report** link.

The Data Report Customization page is displayed:

The image shows a web interface titled "Data Report Customization". Below the title is a light blue box containing the text "Please select the information to be displayed in the total data view". Below this text are three vertically stacked dropdown menus. The first dropdown is labeled "Raw Data", the second is labeled "Compressed Data", and the third is labeled "Compression Ratio". Each dropdown has a small downward arrow on its right side.

Data Report Customization

Please select the information to be displayed in the total data view

Raw Data ▼

Compressed Data ▼

Compression Ratio ▼

Here you can specify the order in which data is displayed at the top of every report for a specific type of traffic. (In other words, you can separately customize the reports for **Total**, **Sent** and **Received** traffic.)

The option you select from the first drop-down list will be the first type of data displayed on the report page, and so on. By default, Raw Data is displayed first, then Compressed Data, and finally the Compression Ratio.

After selecting the order in which to display these fields, click **Save**. You are returned to the report, which should now show the fields in the new order (from left to right). For example, if you set them as shown above, the new report would look like this:

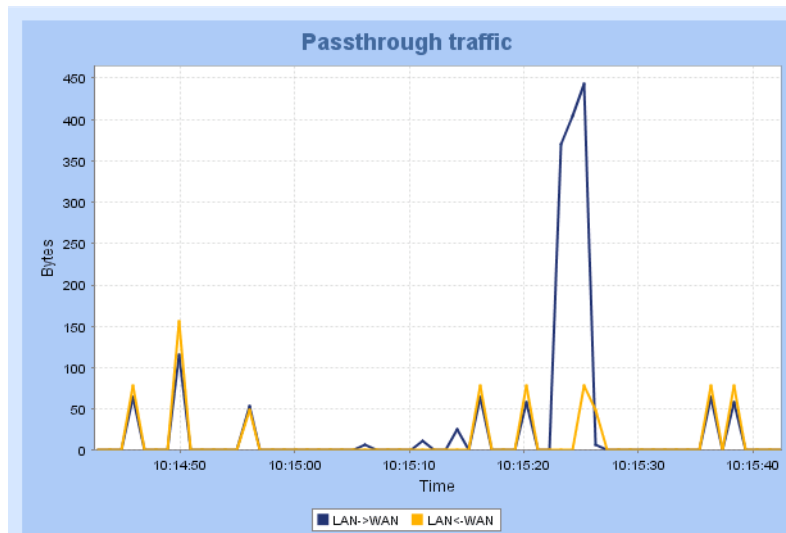
Raw Data	Compressed Data	Compression Ratio
11.271 MB	2.944 MB	282.836 %

Passthrough Traffic report

The Passthrough Traffic report allows you to view, in real time, a graph of passthrough data moving between the WAN and the LAN. Passthrough traffic is network data that is not optimized by WANJet, but allowed to pass through the appliance untouched.

To view a graph of passthrough traffic:

- In the **Reports** section of the menu bar, click on **Throughput > Passthrough traffic**.



In this graph:

- the vertical axis indicates the amount of network traffic (in bytes per second) passing through the F5 appliance without optimization
- the horizontal axis indicates the time (24-hour clock, showing hours, minutes and seconds, to the nearest ten seconds)
- the blue line represents passthrough traffic going from the LAN to the WAN
- The yellow line represents passthrough traffic going from the WAN to the LAN

Diagnostics

The **Diagnostics** section allows you to access a range of useful information, from IP addresses to error log files to the results of popular network analysis tools. Click on **Reports > Diagnostics** in the menu bar to display the initial Diagnostics page:



You can then click on any of the following links:

Connectivity	Displays information about the local WANJet's IP, bridge and Ethernet configuration, and about connectivity to remote WANJets
RADIUS status	Displays details of any RADIUS (remote authentication) servers known to the local WANJet
Bridge Forwarding Database	Lists the MAC addresses (and corresponding IP addresses, if available) of any network devices known to the local WANJet
Diagnostic Log	Allows you to download a log file containing all the errors encountered during the current session
Administration tools	Displays an online interface to the <code>ping</code> , <code>traceroute</code> and <code>tcpdump</code> tools, which are commonly used for diagnosing network problems

Connectivity

Connectivity information is broken up into the categories of **IP**, **Bridge**, **Ethernet** and **Remote WANJets**, which you can view by clicking on the corresponding links beneath the **Connectivity** link on the **Diagnostics** page.

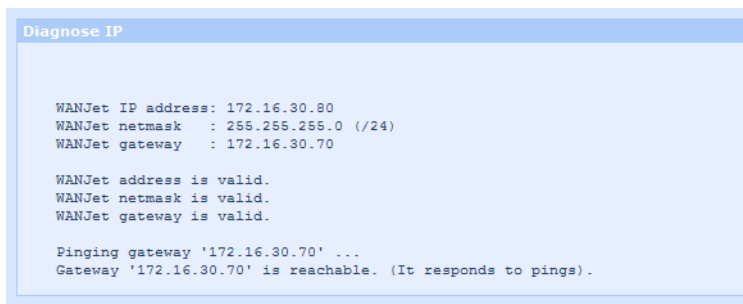
Tip When you click on **Connectivity** itself, all four categories of information are displayed on a single web page – handy for printing out.

IP diagnostics

The Diagnose IP page displays technical details of the local F5 appliance's IP configuration.

To diagnose IP connectivity:

1. Click on **Reports > Diagnostics** in the menu bar.
2. On the Diagnostics page, click on **Connectivity > IP** to display the Diagnose IP page:



The following information is displayed on this page:

- The **IP address** of the local F5 appliance
- The **netmask** of the local subnet, which determines how much of the address identifies the subnetwork on which the WANJet host resides, and how much identifies the host itself
- The IP address of the WAN gateway used by the local F5 appliance

For each of the local IP address, subnet mask and gateway address, this page shows whether the address is valid according to the Internet Protocol standards. To configure these addresses, click on **System Settings > Local WANJet** (see [Updating the Local WANJet Configuration](#) on page 86).

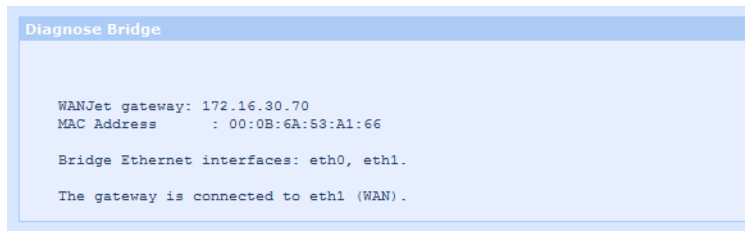
When you display the **Diagnose IP** page, WANJet also pings the local gateway to determine whether it is reachable, and shows the results on this page.

Bridge diagnostics

The Diagnose Bridge page displays details of the internal connectivity – or **bridge** – between the F5 appliance's two Ethernet interfaces.

To diagnose bridge connectivity:

1. Click on **Reports > Diagnostics** in the menu bar.
2. On the Diagnostics page, click on **Connectivity > Bridge** to display the Diagnose Bridge page:



This page shows the IP address and MAC address of the WAN gateway used by the local F5 appliance, together with the Ethernet interfaces that are linked by the bridge.

WANJet QoS does not work unless the Ethernet interfaces are connected properly:

- Interface `eth0` should be connected to the LAN switch or router
- Interface `eth1` should be connected to the WAN gateway

Ethernet diagnostics

The Diagnose Ethernet page displays details about the local F5 appliances's Ethernet interfaces.

To diagnose Ethernet connectivity:

1. Click on **Reports > Diagnostics** in the menu bar.
2. On the Diagnostics page, click on **Connectivity > Ethernet** to display the Diagnose Ethernet page:

```
Diagnose Ethernet

3 Ethernet interfaces found

eth0 (LAN):

Speed: autonegotiated to: 100 Mbits/sec, Full-duplex.
Transmitted: 2,883,316,341 bytes / 6,246,642 packets
Received: 260,543,030 bytes / 3,171,648 packets
Receive errors: 0 (0%)
Collisions: 0 (0%)

There are no collisions.

There are no receive errors.

eth1 (WAN):

Speed: autonegotiated to: 100 Mbits/sec, Full-duplex.
Transmitted: 125,396,191 bytes / 1,708,856 packets
Received: 550,326,265 bytes / 3,524,168 packets
Receive errors: 0 (0%)
Collisions: 0 (0%)

There are no collisions.

There are no receive errors.

eth2 (PEER):

Speed: autonegotiated to: (unrecognized speed setting), (unrecognized duplex setting).
Transmitted: 0 bytes / 0 packets
Received: 0 bytes / 0 packets
Receive errors: 0 (0%)
Collisions: 0 (0%)

LAN and WAN speed/duplex settings are the same.
```

There is one section on this page for each Ethernet interface: LAN, WAN and PEER. For each interface the page displays the maximum speed, duplex setting, amount of data transmitted / received (expressed in both bytes and packets) and the number of receive errors and collisions detected.

WANJet QoS does not work unless the Ethernet interfaces are connected properly:

- eth0 should be connected to the LAN
- eth1 should be connected to the WAN
- eth2 should be connected to the **redundant peer** (if one is present on your LAN; see [Redundant Peers](#) on page 93)

To configure the Ethernet interfaces' speed and duplex settings, click on **System Settings > NIC Configuration** in the menu bar (see [Updating the NIC Configuration](#) on page 94).

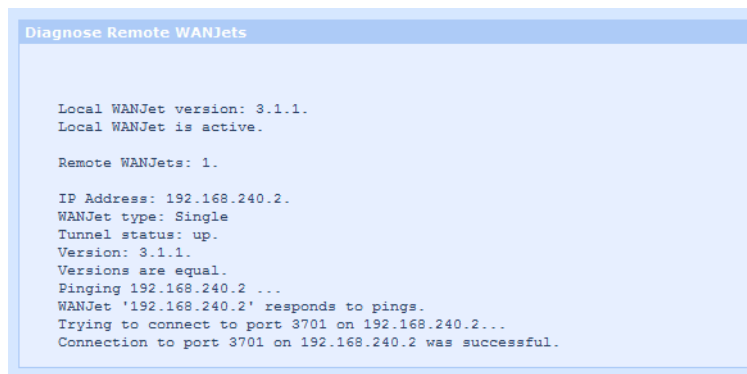
Note For WANJet to work correctly, the speed and duplex setting of the LAN and WAN interfaces should be the same. The **Diagnose Ethernet** page confirms if that is the case, and displays a warning if it is not.

Remote WANJet diagnostics

The **Diagnose Remote WANJets** page displays details about the remote F5 appliances that are connected to the local appliance.

To diagnose remote WANJets:

1. Click on **Reports > Diagnostics** in the menu bar.
2. On the Diagnostics page, click on **Connectivity > Remote WANJets** to display the **Diagnose Remote WANJets** page:



```

Diagnose Remote WANJets

Local WANJet version: 3.1.1.
Local WANJet is active.

Remote WANJets: 1.

IP Address: 192.168.240.2.
WANJet type: Single
Tunnel status: up.
Version: 3.1.1.
Versions are equal.
Pinging 192.168.240.2 ...
WANJet '192.168.240.2' responds to pings.
Trying to connect to port 3701 on 192.168.240.2...
Connection to port 3701 on 192.168.240.2 was successful.
  
```

For each remote F5 appliance, this page shows:

- IP address
- WANJet type – this will be `Single` if there is no redundant peer at the remote end
- tunnel status – `up` if the remote WANJet is currently active
- software version number (this is compared with the local version number)
- whether the remote appliance is responding to pings from the local appliance
- whether the local appliance can connect to the remote appliance on the ports that F5 appliances use to communicate with each other (ports 3701, 3702 and 3703, by default)

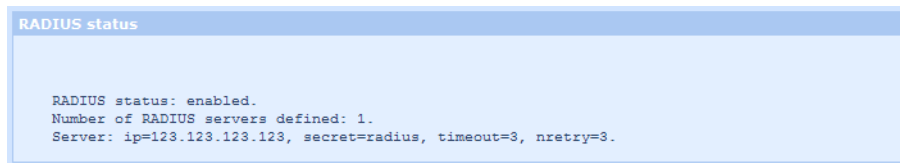
To configure remote WANJets, click on **System Settings > Remote WANJets** in the menu bar (see [Managing Remote WANJets](#) on page 90).

RADIUS status

The RADIUS Status page displays details of any RADIUS authentication servers known to the local F5 appliance. Remote authentication via the RADIUS protocol is an alternative to local authentication via a username and password stored on the F5 appliance.

To diagnose RADIUS status:

1. Click on **Reports > Diagnostics** in the menu bar.
2. On the Diagnostics page, click on **RADIUS status**:



For each RADIUS server, the following information is shown:

- IP address
- Secret (a key which is used to authenticate RADIUS transactions between client and server)
- Timeout period (in seconds)
- Number of times to retry a connection

Note A warning message is displayed if the timeout and number of retries for a RADIUS server are both high, as in that case it could take a long time to determine that the server is not responding to a login attempt.

To configure WANJet to use RADIUS authentication, click on **System Settings > Remote Authentication** (see [Configuring remote authentication](#) on page 67). Refer to <http://www.ietf.org/rfc/rfc2865.txt> for technical details of the RADIUS protocol.

Bridge Forwarding Database

The Bridge Forwarding Database - MAC Addresses page lists all the network devices which have sent traffic through the local WANJet bridge.

To examine the Bridge Forwarding Database:

1. Click on **Reports > Diagnostics** in the menu bar.
2. In the Diagnostics page, click on **Bridge Forwarding Database**:

MAC Address	IP Address	Interface	Local
00:08:0D:22:8A:D9	172.16.30.141	eth0(LAN)	No
00:09:0F:50:15:70	N/A	eth0(LAN)	No
00:0B:6A:53:52:15	N/A	eth0(LAN)	No
00:0B:6A:53:A1:66	N/A	eth1(WAN)	No
00:0D:60:8E:83:C3	N/A	eth0(LAN)	No
00:0D:60:FE:8D:BC	N/A	eth0(LAN)	No
00:0E:35:D3:64:BD	N/A	eth0(LAN)	No
00:0F:66:A3:4F:88	172.16.30.11	eth0(LAN)	No
00:11:43:5C:17:73	172.16.30.143	eth0(LAN)	No
00:11:43:5C:19:BD	N/A	eth0(LAN)	No
00:11:43:69:E3:04	N/A	eth0(LAN)	No
00:11:43:6A:91:7F	N/A	eth0(LAN)	No
00:11:85:FF:6A:80	N/A	eth0(LAN)	No
00:11:85:FF:6A:AE	N/A	eth0(LAN)	No
00:12:F0:0D:39:9E	N/A	eth0(LAN)	No
00:30:6E:D4:A5:97	N/A	eth0(LAN)	No
00:40:63:DA:9F:0D	172.16.30.254	eth0(LAN)	No
00:90:FB:00:EB:1C	N/A	eth0(LAN)	Yes
00:90:FB:00:EB:1D	N/A	eth1(WAN)	Yes
00:C0:4F:61:24:CC	N/A	eth0(LAN)	No
00:D0:B7:2E:A7:A0	N/A	eth0(LAN)	No

For each listed network device, the following information is shown:

- **MAC (Media Access Control) Address** – a unique identifier attached to most forms of networking equipment, and used by many network protocols
- **IP Address** – this is only available if the device has communicated directly with the WANJet
- **Interface** – eth0 if the device is connected to the local WANJet via the LAN; eth1 if it is connected via the WAN
- **Local** – this column reads **Yes** for the F5 appliance's own internal network devices: that is, its two Ethernet interfaces.

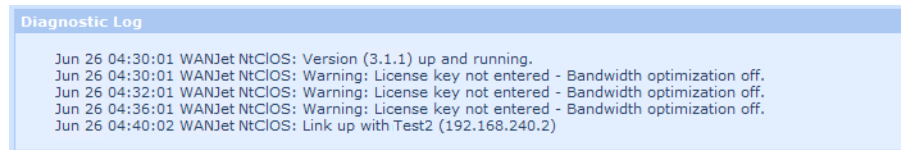
Diagnostic Log

You can view a log containing status information and errors that the WANJet records during a session. This diagnostic log keeps you up to date, and helps you resolve any problems you might face while working with the WANJet. You can also download a system snapshot, which provides information that the F5 Customer Confidence team can use to debug problems.

Using the Web UI, you can display the diagnostic log, and download the system snapshot as a zipped text file to your hard disk. You can also clear all the data in the diagnostic log.

To view the diagnostic log:

1. Click on **Reports > Diagnostics** in the menu bar.
2. On the Diagnostics page, click on **Diagnostic Log**. A few example messages from a log are shown below



At any time, you can clear the diagnostic log in order to delete all the error logs and report data.

To clear the diagnostic log:

1. Click on the **Clear Logs** link at the top right of the Diagnostics page. A warning message appears to let you know that all data saved to the error and report logs will be deleted.
2. Click **OK** if you want to delete the logs. Otherwise, click **Cancel**.

To download a system snapshot:

1. Click on the **System Snapshot** link at the top right of the Diagnostics page. Your browser will open a download window for you to save the snapshot file to your local disk.
2. The system snapshot file is called `snapshot.gz`. This is a compressed plain text file: if you wish to view it, you will first need to extract it using a tool such as `gunzip` (www.gzip.org).
3. Send the compressed `snapshot.gz` file to the F5 Customer Confidence team, preferably after renaming it in the format `snapshot-yourcompanyname-yyyy-mm-dd` (e.g. `snapshot-acme-2005-04-22`).

Administration tools

WANJet provides a browser-based user interface for three popular network diagnostic tools: ping, traceroute, and tcpdump (for packet capture).

To access the diagnostic tools:

1. Click on **Reports > Diagnostics** in the menu bar.
2. On the Diagnostics page, click on **Administration tools**. The Tools page is displayed:

For each tool, there is a text box for specifying command-line parameters, and a button which allows you to run the program via the shell. When you click on a button, the following two sections appear, lower down on the page:

- **Processes:** This shows the full path to the process, along with parameters, as it would appear on the command line. The process number – as allocated by the operating system – is also given. Click on the process number to kill the process (before it has finished running). A confirmation screen like the one below is displayed:

- **Running:** The bottom section displays the process output. This is similar to what you would see in the shell after running the program from the command line. The return code is also displayed: this will be 0 if the program returns successfully.

Ping

The `ping` utility provides a simple test of whether a target host is online and reachable via a TCP/IP network. It works by sending out ICMP request packets to the target and listening for response packets in return. The percentage of packets lost, and the time taken to send and receive them, provide an indication of how well the connection is working.

Parameters

By default, WANJet provides the following parameters for `ping`:

```
-R -c 5 -w 10 <IP address of target host>
```

The default target is the gateway machine for the subnet on which the F5 appliance resides. You can change these parameters using the text box provided, but this is only recommended for experienced users.

Output

The following output is displayed on the page:

- The IP addresses of both the target host and the source host (the server on which `ping` is running)
- A line for each ICMP response packet received back from the target, showing the packet's sequence number, time-to-live, and round-trip time (request time + response time)
- A statistical summary showing:
 - the number of request packets transmitted
 - the number of response packets received back
 - the percentage of packets lost
 - the minimum, average and maximum round-trip times

Further information

If a target host is not reachable via `ping` – that is, the statistical summary shows a 100% packet loss – this does not necessarily mean that there is no working network connection between source and target. For example, a firewall might be blocking ICMP requests from reaching the target host, but allowing some other network traffic through.

For more information about the `ping` tool, see <http://en.wikipedia.org/wiki/Ping>.

Traceroute

The `traceroute` utility is used to plot the route that packets take to a target host. It can thus be helpful in determining the location of any network disruption.

`Traceroute` works by incrementing the TTL (time to live) value of successive packets sent out. TTL values are decremented as packets pass through intermediate hosts (known as hops). When the TTL reaches a value of 1, a `time exceeded` message is sent back to the source host (the host on which `traceroute` is running). By examining the origins of these messages, the path that packets take to the target can be reconstructed.

Parameters

By default, WANJet provides the following parameters for `traceroute`:

```
-v <IP address of target host>
```

As with the `ping` tool, the default target is the gateway for the local subnet. Experienced users can change these parameters using the text box provided.

Output

The page displays the following output:

- The IP address of the target host, the maximum number of hops (that is, the maximum TTL), and the size of the packets sent out
- A list of hosts through which packets are passing, together with the round-trip time taken for each of three packets (packets are sent out in threes, by default) to travel from the source host to the intermediate host and back again.

Further information

`Traceroute` sends out UDP datagram packets by default. If UDP probes are being blocked by a firewall, you can use ICMP echo requests instead (as `ping` does) by specifying the `-I` option. Packets are normally sent to port 33434, which should not be in use: if the target host is listening on this port, you can specify a different port using the `-p` option.

For more information about `traceroute`, see <http://en.wikipedia.org/wiki/Traceroute>.

Packet capture with tcpdump

You can use `tcpdump` to intercept and display the actual contents of TCP/IP packets on the network. This is useful for debugging your network setup, allowing you to isolate the source of a problem by determining whether all routing is working correctly. Data is saved to a PCAP file which can then be viewed using a tool such as Ethereal.

Parameters

By default, WANJet provides the following parameters for `tcpdump`:

```
-c 10 (not port 10000)
```

Packets sent to port 10000 are ignored, since this is the port which the Web UI uses to communicate with the local F5 appliance.

Experienced users can change these parameters using the text box provided.

Output

When `tcpdump` has finished, the Tools page displays a link to the PCAP file that has been produced. You can open this directly if you have an application that can read PCAP files, or save it to disk. The PCAP file is also stored on the server where `tcpdump` is running, at the following path:

```
/usr/local/NetOptimizer/logs/dump.pcap
```

Further information

You will need a specialized application, such as Ethereal (a network protocol analyzer which runs on both Linux and Windows) to read PCAP files produced by `tcpdump`. You can download Ethereal and its documentation for free from <http://www.ethereal.com/>.

System Information reports

The System Information reports enable you to view:

- details of all WANJet network interfaces, including MAC address, error rates, speed and status
- details of passthrough traffic, including both TCP and UDP data
- the WANJet serial number
- detailed information relating to QoS, VLANs, remote WANJet links, TDR statistics, bandwidth, optimized sessions, and passthrough sessions

To view the System Information reports:

- In the **Reports** section of the menu, click on **System Information**. The main System Information page is displayed:

System Information

[QoS](#) | [VLANs](#) | [WANJet Links](#) | [TCP Statistics](#)
[TDR stats](#) | [Optimized Sessions](#) | [Passthrough Sessions](#)

eth0 (LAN)
 MAC 00:90:FB:01:F1:C4
 Speed 1000 Full Duplex
 Status Link ok
 RX: errors:0 dropped:0 overruns:0 frame:0
 TX: errors:0 dropped:0 overruns:0 carrier:0
 collisions:0

eth1 (WAN)
 MAC 00:90:FB:01:F1:C5
 Speed 100 Full Duplex
 Status Link ok
 RX: errors:0 dropped:0 overruns:0 frame:0
 TX: errors:0 dropped:0 overruns:0 carrier:0
 collisions:0

eth2 (Peer)
 MAC 00:90:FB:81:65:84
 Speed N/A
 Status Link error

TCP Passthrough
 LAN->WAN 15421783 Packets/20.601 GB
 WAN->LAN 4770226 Packets/310.410 MB

UDP Passthrough
 LAN->WAN 1583844 Packets/182.628 MB
 WAN->LAN 293 Packets/15.876 KB

Serial Number [REDACTED]

[Reset](#)

Initially, the main **System Information** page displays information about all network cards used by WANJet, together with TCP/UDP passthrough data, and the WANJet serial number. You can view other kinds of information using the links at the top of the page.

Note Click **Reset** at the bottom of the main **System Information** page to reset the counting of all data on this page. If you do not click **Reset**, the data on the page continues to accumulate whenever you refresh the browser.

Network interfaces

Each F5 appliance normally has at least two active network interfaces: one for the connection to the LAN and one for the connection to the WAN. In addition, there is an interface for the connection to a redundant peer WANJet, if one is present on your LAN (see [Redundant Peers](#) on page 93).

For each network interface, the following information is shown:

- The interface's MAC address (a unique identifier attached to most forms of networking equipment)
- The interface's maximum speed (in Mbit/s) and duplex setting (Full Duplex / Half Duplex)
- The interface's current status (Link ok / Link error)
- Any errors raised by the interface; both reception (RX) and transmission (TX) errors are shown:
 - reception errors are further broken down into dropped packets, overruns, and frame errors
 - transmission errors are broken down into dropped packers, overruns, carrier errors, and collisions

Other information

The following information is also shown on the main **System Information** page:

- The numbers of TCP passthrough packets travelling through WANJet from the LAN to the WAN and from the WAN to the LAN (since the appliance started, or since counting was last reset)
- The numbers of UDP passthrough packets travelling through WANJet from the LAN to the WAN and from the WAN to the LAN (since the appliance started, or since counting was last reset)
- Your WANJet serial number, which you may need in order to obtain a F5 WANJet license key

Links to other reports

At the top right of every System Information page, there are links to the individual System Information reports, as follows:

Report	Describes...
QoS	Remote networks that have WANJet QoS policies assigned to them
VLANs	Virtual LANs supported by the local WANJet
WANJet Links	Links to remote F5 appliances
TCP Statistics	Number of TCP segments retransmitted due to timeouts
TDR Stats	Statistics about TDR (Transparent Data Reduction) caching
Optimized Sessions	Number of network sessions undergoing optimization
Passthrough Sessions	Number of network sessions set to pass through the F5 appliance without optimization

QoS

QoS (Quality of Service) policies can help to improve network performance by dedicating bandwidth to specific network traffic. Click on **QoS** at the top of any System Information page to view details of the remote networks that have QoS policies assigned to them:

QoS					
QoS VLANs WANJet Links TCP Packet Retransmissions TDR stats Optimized Sessions Passthrough Sessions					
Remote	Policy	Rate	BytesSent	PacketsSent	Dropped
172.16.1.2	voice	0Kbit	31345436	146474	0
172.16.1.2	Default	1Kbit	115857932	929948	0
Internet	Default	3Kbit	274883807	244997	544912

The following information appears in the QoS report:

Remote	Remote network that has QoS policies assigned to it.
Policy	Name of the QoS policy assigned to the remote network.
Rate	Actual bandwidth assigned to each policy.
Bytes Sent	Number of bytes sent for each policy.
Packets Sent	Number of packets sent successfully for each policy
Dropped	Number of packets dropped for each policy.

For more about QoS, refer to [Application QoS Policies](#) on page 103.

VLANs

A VLAN (Virtual LAN) is a computer network whose boundaries are defined logically, rather than physically. VLANs must be explicitly added to the WANJet Web UI, since they are often implemented by adding tags to Ethernet frames, and these tags must be preserved during optimization.

Click on **VLANs** at the top of any **System Information** page to see the list of virtual LANs supported by the WAN Optimizer.

The following information appears in the VLANs report:

Tag	ID of the virtual LAN
Packets/Bytes	Number of packets and total size in bytes of the network traffic exchanged with the VLAN
Aware	Indicates whether WANJet can identify this virtual LAN

For more information about configuring VLANs to work with WANJet, refer to [Managing Virtual LANs](#) on page 88.

WANJet Links

Click on **WANJet Links** at the top of any **System Information** page to view details of each link to a remote WANJet:

WANJet Links			
QoS VLANs WANJet Links TCP Packet Retransmissions TDR stats Optimized Sessions Passthrough Sessions			
Remote IP	#Retrans	#ACM5	#ACM5 without compression
172.16.1.2	0	1	0

The WANJet Links report contains the following information:

Remote IP	IP address of the remote F5 appliance
Retransmissions	Number of retransmitted packets to the remote WANJet
#ACM5	Number of network connections to the remote WANJet that are being optimized using ACM5
#ACM5 without compression	Number of passthrough network connections that are not being optimized

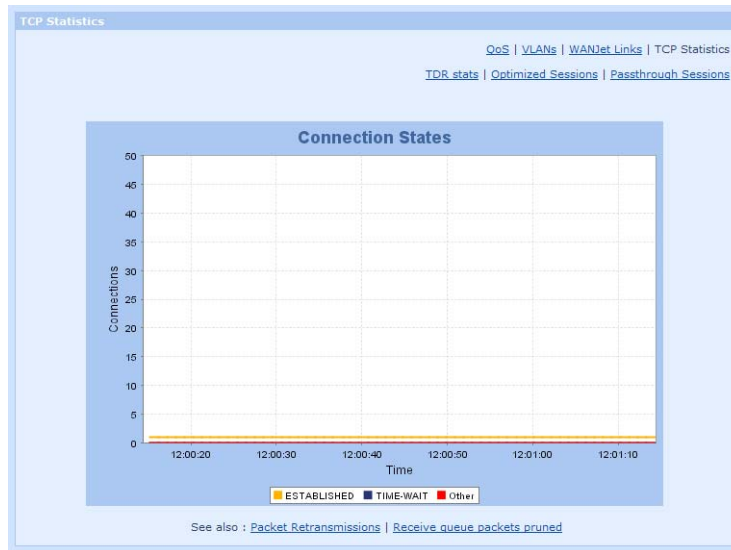
For more about links to remote WANJets, refer to [Managing Remote WANJets](#) on page 90.

TCP Statistics

You can click on **TCP Statistics** at the top of any **System Information** page to view three separate reports into TCP connection activity. The Connection States report is displayed by default. You can view the other reports by clicking on the corresponding link under the graph.

Connection States

This graph displays the current state of each TCP connection visible to the WANJet, for both optimized and passthrough connections.



There are three lines, representing the number of connections in various states:

- ESTABLISHED connections are those that have been successfully opened and are working normally
- Connections in the TIME_WAIT state are waiting for enough time to pass to be sure that the remote TCP received the acknowledgment of a connection termination request, which may take up to four minutes.
- Other possible connection states include LISTEN, SYN-SENT, SYN-RECEIVED, FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, CLOSING, and LAST-ACK. Please refer to IETF RFC #793 (<http://www.ietf.org/rfc/rfc793.txt>) for more details.

Packet retransmissions

TCP segments that time out without being acknowledged by a destination host will be retransmitted by the source host. High levels of these retransmitted segments can indicate network problems. Therefore, the Web UI includes a report which tracks their changing numbers. The blue line in this graph indicates the number of TCP segments (which often correspond to IP packets) that had to be retransmitted, per second.

Receive queue packets pruned

This graph represents the number of segments pruned from the TCP receive queue due to socket overrun. This may happen if the TCP receive buffer is too large on the receiving host. The optimal buffer size is twice the product of the bandwidth and the delay (see <http://www.didc.lbl.gov/TCP-tuning/background.html>).

TDR Stats

TDR (Transparent Data Reduction) is a new feature in the F5 WANJet version 3.1, which further enhances network optimization by caching the contents of frequently accessed files in memory. Click on **TDR stats** at the top of any System Information report page to display statistics for TDR optimization:

WANJetIP	Sent Bytes (TDR)	Sent Bytes (other)	Received Bytes (TDR)	Received Bytes (other)	TDR efficiency %
192.168.240.2	0	0	0	0	0.00
					0.00

The TDR Stats report contains the following information:

WANJet IP	IP address of the remote WANJet
Sent Bytes (TDR)	Amount of sent data (in bytes) to which TDR has been applied, since this WANJet link became active.
Sent Bytes (other)	Amount of sent data (in bytes) to which TDR has not been applied
Received Bytes (TDR)	Amount of received data (in bytes) to which TDR has been applied
Received Bytes (other)	Amount of received data (in bytes) to which TDR has not been applied
TDR efficiency %	Percentage of data sent across the link to which TDR has been applied. The bold number at the bottom of the report gives the average figure across all remote WANJet links.

For more information about how TDR works, please refer to [Transparent Data Reduction](#) on page 3.

Optimized Sessions

Click on **Optimized Sessions** at the top of any System Information page to view all the network connections (at the application layer) currently being optimized by WANJet using the ACM5 process. Use the **Operational Settings > Optimization Policy** link to specify the types of connections that are / are not optimized (see [Optimization Policies](#) on page 76).

Note You can quickly access the Optimized Sessions report from any page in the WANJet Web UI, using the **Optimized Sessions** link near the top of the menu bar (above the **Reports** section). The counter displayed beside this link shows the current number of optimized sessions.

TCP			
LocalIP	Direction	RemoteIP	WANJetIP
172.16.30.146 : 1061	=>	172.16.0.39 : 5222	172.16.1.2
172.16.30.191 : 1097	=>	172.16.0.39 : 5222	172.16.1.2
UDP			
From		To	
10.1.8.90 : 49590		10.10.10.3 : 49590	
10.1.8.90 : 49591		10.10.10.3 : 49591	
10.1.8.90 : 49592		10.10.10.3 : 49592	
10.1.8.90 : 49593		10.10.10.3 : 49593	

The Optimized Sessions report is divided into two sections, for TCP and UDP traffic. The TCP section contains the following information:

Local IP	IP address and port of the local machine
Direction	Direction of optimized data traffic flow. A right arrow (=>) indicates that the direction is from the local machine to the remote machine. A left arrow (<=) indicates that the direction is from the remote machine to the local machine.
Remote IP	IP address and port of the remote machine
WANJet IP	IP address of the remote WANJet appliance handling the optimized session.

The UDP section contains just two columns, giving the IP address and port number for each UDP session's source and destination.

Passthrough Sessions

Click on **Passthrough Sessions** at the top of the System Information page to view a list of all open passthrough sessions.

A passthrough session is a network connection (at the application layer) for which traffic is not optimized by WANJet, but allowed to pass through the appliance untouched. Use the **Operational Settings > Optimization Policy** link to specify the types of connections that are / are not optimized (see [Optimization Policies](#) on page 76).

Note You can quickly access the Passthrough Sessions report from any page in the WANJet Web UI, using the **Passthrough Sessions** link near the top of the menu bar (above the **Reports** section). The counter displayed beside this link shows the current number of passthrough sessions.

TCP	
See also: Optimize Eligible Connections	
From	To
172.16.30.25 : 21 (Ftp)	-> 192.168.241.3 : 32783
172.16.30.25 : 38758	-> 192.168.241.3 : 32784
172.16.30.25 : 40542	-> 192.168.241.3 : 22 (Ssh)
172.16.30.25 : 43438	-> 192.168.241.3 : 32785
172.16.30.80 : 3701	-> 192.168.240.2 : 48437
172.16.30.80 : 54531	-> 192.168.240.2 : 3701
172.16.30.80 : 54568	-> 192.168.240.2 : 3701
172.16.30.80 : 54569	-> 192.168.240.2 : 3701
172.16.30.80 : 54570	-> 192.168.240.2 : 3701
172.16.30.80 : 54571	-> 192.168.240.2 : 3701
172.16.30.140 : 4817	-> 192.168.240.2 : 22 (Ssh)
UDP	
From	To
172.16.30.254 : 53 (Domain)	-> 192.168.240.3 : 44311
172.16.30.254 : 53 (Domain)	-> 192.168.240.3 : 44312
172.16.30.254 : 53 (Domain)	-> 192.168.240.3 : 44313
172.16.30.254 : 53 (Domain)	-> 192.168.240.3 : 44314
172.16.30.254 : 53 (Domain)	-> 192.168.240.3 : 44315
172.16.30.254 : 53 (Domain)	-> 192.168.240.3 : 44316
172.16.30.254 : 53 (Domain)	-> 192.168.240.3 : 44317
172.16.30.254 : 53 (Domain)	-> 192.168.240.3 : 44318
172.16.30.254 : 53 (Domain)	-> 192.168.240.3 : 44319
172.16.30.254 : 53 (Domain)	-> 192.168.240.3 : 44320
172.16.30.254 : 53 (Domain)	-> 192.168.240.3 : 44321
172.16.30.254 : 53 (Domain)	-> 192.168.240.3 : 44322
172.16.30.254 : 53 (Domain)	-> 192.168.240.3 : 44323
172.16.30.254 : 53 (Domain)	-> 192.168.240.3 : 44324
172.16.30.254 : 53 (Domain)	-> 192.168.240.3 : 44325
172.16.30.254 : 53 (Domain)	-> 192.168.240.3 : 44326

The Passthrough Sessions report is split into two lists, one for TCP and one for UDP connections. For each session, the IP address and port for the source and destination host are shown. The application or service that is using the session may also be shown (in brackets).

At the top of the page there is a link to the [Optimize Eligible Connections](#) report (see below).

Optimize Eligible Connections report

When you click on the **Optimize Eligible Connections** link at the top of the Passthrough Sessions report, a report like the one below is displayed. This report shows connections that were set up before the F5 appliance was last activated. If the protocol and software allow it, you can intercept and reset these connections so that from this point on they will be optimized using ACM5. This is most useful for connections that need to be live for a long time so that they can transfer large amounts of data, such as replication processes.

See also: [All Passthrough Sessions](#)

From	To	Reset
10.0.8.61 : 3695	-> 10.55.55.3 : 100	<input type="checkbox"/>
		<input type="checkbox"/> all
		<input type="button" value="Reset"/>

As with the Optimized Sessions and Passthrough Sessions reports, there is a row for each eligible connection, showing the IP address and port for both source and destination. There is also a **Reset** checkbox for each of the connections.

To reset an eligible connection:

1. Select the checkbox for each connection that you wish to reset.
 - Alternatively, select **all** to reset all eligible connections.
2. Click on the **Reset** button at the bottom right of the page. The selected connections will be reset the next time that WANJet is restarted.

For more about the WANJet's connection interception feature, refer to [Connection Interception](#) on page 8.

Remote Status report

The Remote Status report enables you to view the status and details of remote F5 appliances. If the remote WANJet has a redundant peer, the Remote Status report also displays details of the peer appliance (see [Redundant Peers](#) on page 93). The Remote Status report is the first page displayed when you log in to the WANJet Web UI.

To view the Remote Status report:

- Click on **Reports > Status** in the menu bar. The Remote Status report opens and displays the status (*on / off*), IP address, alias, and version of all connected F5 appliances:

Remote Status			
IP	Alias	Version	Status
● 192.168.190.2	Remote-demo-0	3.1.3	on
Connection to a remote WANJet may take up to 2 minutes.			
License Key : OK			

The remote WANJet's license key status (not entered / not valid / expired / OK) is also shown on this page.

Note: To view the status of a remote WANJet directly after changing any of its settings, wait until the local WANJet communicates with the remote WANJet. This can take up to two minutes. Then refresh the **Remote Status** report in your browser.

Third-party reporting systems

WANJet is integrated with several third-party reporting systems, including `syslog`, SNMP and RMON2.

Syslog reports

The WANJet allows you to use an external `syslog` server to view the `syslog` reports that it generates. These reports include data such as the amount of sent and received data processed by WANJet.

Ensure you have entered the IP address of the machine you are using to view `syslog` data in the **Syslog Server IP** field on the Syslog and SNMP page. For more information, see [Configuring Syslog and SNMP Settings](#) on page 96.

SNMP reports

The WANJet allows you to use an external computer as a management station for viewing SNMP (Simple Network Management Protocol) logs that are produced by WANJet on the local appliance. The SNMP data trees are stored in an MIB (Management Information Base). If you need the WANJet private MIB file, see [Appendix C, WANJet Private MIB](#).

Before you can view an SNMP report, configure WANJet to use an SNMP server:

1. On the **Syslog and SNMP** page (under **System Settings** on the menu bar), specify the community string and IP address for an SNMP server. For details of how to do this, see [Configuring Syslog and SNMP Settings](#) on page 96.
2. On the **IP Access Control** page (under **System Settings** on the menu bar) check that the IP address of the SNMP server has access to the Web UI. (The default setting is to grant all machines access, but this might have been changed by an administrator.) For details of how to do this, see [Granting Access to WANJet Web UI](#) on page 95.

After ensuring these tasks are completed, you will be able to view the SNMP reports:

3. Use the community string you specified on the **Syslog and SNMP** frame to authenticate the machine you are using for viewing SNMP data on WANJet.
4. Use SNMP-compliant software to view the SNMP tables. You need to provide the SNMP-compliant software with the IP address of WANJet, in addition to the community string you specified earlier.

The SNMP data on WANJet includes information about the network cards, total bandwidth saved for sent and received data, and amounts of sent and received data processed using ACM5.

To view WANJet SNMP errors, see [Appendix B, WANJet Errors](#).

RMON2 Reports

WANJet also enables you to view RMON2 data trees, which are part of the SNMP data trees that it produces. The RMON2 data is also stored in a MIB.

You can access RMON2 data in the same way as SNMP data. You must have already specified a community string and the IP address of an SNMP server and set your RMON2 preferences on the **Syslog and SNMP** page. For details of how to do this, see [Configuring Syslog and SNMP Settings](#) on page 96. Note that the SNMP server must have access to WANJet, as described under [Granting Access to WANJet Web UI](#) on page 95.

To view RMON2 reports:

1. Use the community string you specified on the **Syslog and SNMP** page to authenticate the machine you are using to view the SNMP data on WANJet.
2. Use SNMP-compliant software to view the RMON2 data tree, which is a part of the SNMP data tree. You need to provide the SNMP-compliant software with the IP address of WANJet, in addition to the community string you specified earlier.

The RMON2 data on WANJet includes data sent and received between two nodes, the IP addresses of these nodes, the port used to send and receive data, data size before and after the WANJet processes it, times at which data was sent, and the numbers of connections.

Chapter 5

Managing the WANJet

- WANJet authentication ◀
 - WANJet time settings ◀
 - Shutting down and restarting a WANJet appliance ◀
 - WANJet boot settings ◀
 - Backup and recovery ◀
 - Upgrading the WANJet software ◀
-

The F5 WANJet requires only basic administration. The most frequent management tasks involve synchronizing the time settings and performing regular backups. Other basic tasks include changing your password and PIN settings, shutting down and restarting your F5 appliance, and upgrading your WANJet software version.

WANJet authentication


To keep your WANJet settings secure, the WANJet Web UI is password-protected, whilst the LCD menu on the front of the appliance is PIN-protected. You can change the password and/or PIN code at any time. F5 recommends that you change them regularly – once a month, for example – and that you immediately change them from the default password and PIN.

Changing the WANJet Web UI password

You can change the password for the `admin` user account, which is the only local account that someone can use to access the WANJet Web UI. (Remote accounts may also be used, and their passwords cannot be changed via the page shown below: for more details, refer to [Configuring remote authentication](#) on page 67.)

To modify the password you use to access the WANJet Web UI:

1. Expand the **System Settings** section of the menu bar, and click on **Password**. The Password page is displayed:



2. Enter the old password in the **Old Password** field. Leave this field blank if the default password was left unchanged during initial configuration.
3. Enter the new password in the **New Password** field. As a general rule, passwords should consist of at least 6 characters and include a mixture of lower and upper-case letters, numbers, and punctuation marks. A blank password is not allowed.
4. Enter the new password again for confirmation in the **Confirm Password** field. This must exactly match the string entered in the **New Password** field.
5. Click **Save** to save the new password, or click **Cancel** to keep the old password. Click **Yes** on the confirmation window.

Note: Since there is only one local password for the Web UI, be sure to warn any other users that you are changing the password (unless they are using remote authentication).

Changing the WANJet LCD PIN code

There is no default PIN code for the F5 appliance's LCD (Liquid Crystal Display).

To create or change the PIN code you use to access the LCD:

1. Expand the **System Settings** section of the menu bar, and click on **LCD PIN**. The LCD PIN page is displayed:



2. Enter the old LCD PIN in the **Old PIN** field. Leave this field blank if the PIN has not been set during initial configuration.
3. Enter the new PIN in the **New PIN** field. This must be a 4-digit number.
4. Enter the new PIN again for confirmation in the **Confirm PIN** field. This must exactly match the number entered in the **New PIN** field.
5. Click **Save**.

Configuring remote authentication

You can choose whether to authenticate WANJet users against a RADIUS remote authentication server, or against WANJet's local database. If you are authenticating users with the RADIUS protocol, you must provide certain information, including the server's IP address, secret, timeout period, and number of retries.

To set up WANJet remote authentication:

1. Expand the **System Settings** section of the menu bar, and click on **Remote Authentication**. The Remote Authentication screen is displayed. Initially, this screen contains only a pair of radio buttons.
 - At this point, if you do not wish to use remote authentication, select **No Remote Authentication** and click **Save**. The WANJet will then authenticate users against its local database.
2. Select **RADIUS** to use remote authentication with a RADIUS server. A new section appears on the page allowing you to enter the server details, as below. (If you select the RADIUS option, but do not add any server details, WANJet will continue to authenticate users against its local database.)

Remote Authentication

☐ No Remote Authentication
☒ RADIUS

Server	Secret	Timeout	NRetry	
123.123.123.123	abracadabra	3	3	Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Add

See also : [RADIUS Diagnostics](#)

Save Cancel

3. Under **Server**, type the RADIUS server's IP address.
4. Under **Secret**, type the server's shared secret. This is a key which is used to authenticate RADIUS transactions between the client (your local F5 appliance, in this case) and the server.
5. Under **Timeout**, type the number of seconds that WANJet should wait after sending a RADIUS request, before giving up on a response from the RADIUS server. We recommend using a value of 3 seconds.
6. Under **NRetry**, type the number of times that WANJet should send a RADIUS request to the server before deciding that it is not responding. We recommend using a value of 3.

Note: If you enter a value in the **Timeout** field, you must also enter a value in the **NRetry** field. Ensure that both values are not too high, as in that case it could take a long time to determine that the server is not responding to a login attempt. This problem will be compounded if you are using more than one RADIUS server.

7. Click **Add** to store the server's details to the page. The details are not stored permanently until you click on **Save**.

You can specify multiple RADIUS servers, in which case user authentication will be required from one of them rather than from all of them. Once server details have been added, the only way to edit them is to click on **Delete** and then add new details.

8. Click **Save**. The **Remote Authentication** page refreshes, and the RADIUS server details are saved to WANJet.

When WANJet is set to use remote authentication, you can click on **RADIUS Diagnostics** to view the RADIUS Status diagnostic report. See [RADIUS status](#) on page 45 for details of this report.

Refer to <http://www.ietf.org/rfc/rfc2865.txt> for technical information on the RADIUS protocol.

WANJet time settings

Time management in the WANJet involves setting the time zone and synchronizing all linked F5 appliances. When you click on **System Settings > Time**, the page that appears is divided into three sections:

- **Timezone** allows you to set the time zone and the first day of the week (see below)
- **Time Server** allows you to select a server for automatically synchronizing your F5 appliances (see page 70)
- **Time** allows you to set the current time manually (see page 70)

Setting the timezone

The Timezone section enables you to set the timezone within which your F5 appliance is operating.

To set the WANJet timezone:

1. Expand the **System Settings** section of the menu bar, and click on **Time**.
2. In the Timezone section, select the closest geographical location to your site from the **Current location** list. The default location is *America/New York*.
3. In the **First Day of Week** drop-down list, select the day on which your working week begins. The day you specify here is considered the first day of the week for all the performance reports that the WANJet generates about your traffic.
4. Click on **Change timezone** to save your changes.

Synchronizing WANJet time automatically

You can use a specific time server to synchronize WANJet time automatically. The IP addresses of several commonly used time servers are provided, or you can specify the address of another time server yourself.

For more information about time servers, refer to www.eecis.udel.edu/~mills/ntp/clock2a.html

To use a time server to synchronize your F5 appliances:

1. Expand the **System Settings** section of the menu bar, and click on **Time**.
2. In the Time Server section, select the IP address of a commonly used time server from the **Host/Address** drop-down list.
 - Alternatively, select `User Specified` and enter the IP address of your preferred time server.
3. Click on **Sync time** to save your changes.
4. Repeat this step in the Web UI for every F5 appliance that you are using.

Setting the time manually

You can adjust the time on your F5 appliances manually through the Web UI, instead of synchronizing with a time server.

To set the date and time manually:

1. Expand the **System Settings** section of the menu bar, and click on **Time**.
2. In the Time section, select the current Day, Month, Year, Hour, Minute and Second from the drop-down lists provided.
3. Click on **Set time** to save your changes.
4. Repeat this step in the Web UI for every F5 appliance that you are using.

Shutting down and restarting a WANJet appliance

Shutting down WANJet stops all data processing. You can shut down or restart using either the Web UI or the LCD on the appliance.

Warning! Be sure to notify your users before shutting down or restarting a F5 appliance, as network performance will be affected.

To shut down via the Web UI:

1. Expand the **System** section of the menu bar, and click on **Shutdown**.
2. On the Shutdown page, click on **Shutdown WANJet**.
3. A confirmation dialog appears. Click **OK** if you wish to shut down your F5 appliance. Otherwise, click **Cancel**.

To shut down via the LCD panel:

1. On the F5 appliance's front LCD panel, press the **X (Cancel)** button to activate the main menu.
2. Press the **✓ (Enter)** button to display the **Setup** menu.
3. Select **Shutdown**, and press the **✓** button. A confirmation message is displayed.
4. Press **✓** again to shut down the appliance. Alternatively, press **X** to escape this menu sequence.

Note: To turn off the F5 appliance completely, press the **On/Off** button at the back of the appliance. Before doing that, however, you should first shut down the appliance using one of the methods described above.

To restart via the Web UI

1. Expand the **System** section of the menu bar, and click **Restart**.
2. On the Restart page, click on **Restart WANJet**.
3. A confirmation dialog appears. Click **OK** if you wish to restart WANJet. Otherwise, click **Cancel**.

To restart via the LCD Panel

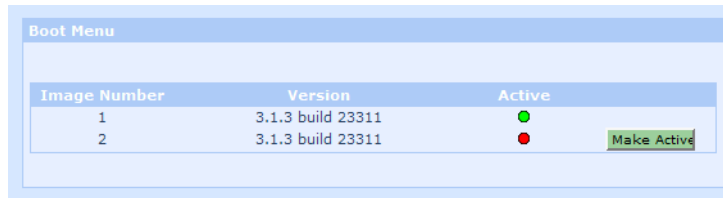
1. Press the **X** button to activate the main menu.
2. Press the **✓** button to display the **Setup** menu.
3. Select **Restart**, and press **✓**. A confirmation message is displayed.
4. Press **✓** to restart WANJet. Alternatively, press **X** to escape this menu sequence.

WANJet boot settings

Up to two WANJet images may be present on the same flash memory card. If something goes wrong with your first installation, you can boot from the other image instead. In that case, you will need to reconfigure all WANJet settings that differ from the defaults.

To boot the F5 appliance from a different WANJet image:

1. Expand the **System** section of the menu bar, and click on **Boot Menu**:



2. The WANJet software version and build number are shown for each image. Click on the **Make Active** button next to the image that you wish to activate.
3. Click **Yes** on the confirmation window.

Warning! WANJet will reboot as soon as you click **Yes**, and will not work normally again until the new image has been fully configured. Therefore you should prepare thoroughly, and notify other network users, before taking this step on a live system.

Backup and recovery

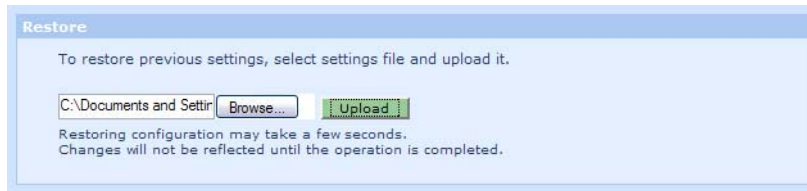
F5 recommends that you make regular backups of your current WANJet settings. You should also perform a backup before making any major changes to the settings. It is then easy to restore the system in the event of a failure.

To create a backup file of the current WANJet settings:

1. Expand the **System** section of the menu bar, and click on **Backup**. The Backup frame opens.
2. Click where it says **here**. Your browser will open a File Download window for you to save the backup file to your local computer. The file is called `Settings-[ServerName].NTCL` – you should probably edit this filename to identify the F5 appliance that was backed up, and the date at which the backup was made.

To restore a saved backup of WAN Optimizer settings:

1. Expand the **System** section of the menu bar, and click on **Restore**:



2. Click **Browse** to open a browser Upload window and locate the backup file you want to upload. WANJet backup files end in the extension .NTCL
3. On the Restore screen, click **Upload**.
4. The Web UI refreshes and you are returned to the home page. The backup settings will now be in effect.

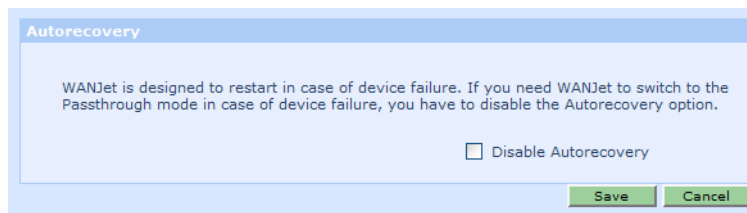
Autorecovery

When there is a device failure on your F5 appliance, the WANJet can attempt to restart or can switch to passthrough mode where traffic flows through your network as if the WANJet device did not exist. Autorecovery, where the WANJet attempts to restart, is the default mode.

You can set an option to disable this restart behavior. If you disable autorecovery, the WANJet switches to passthrough mode in case of device failure.

To disable WANJet autorecovery:

1. Expand the **System** section of the menu bar, and click on **Autorecovery**:



2. Select **Disable Autorecovery** if you want the WANJet to switch to Passthrough mode in case of device failure.
3. Click on **Save** at the bottom of the page.

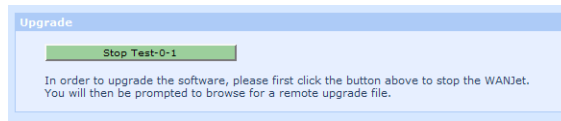
Upgrading the WANJet software

WANJet's Web UI makes it easy for you to upgrade the version of the WANJet software installed on your F5 appliance.

Note You must stop the current WANJet processing session before you can upgrade. Therefore you should notify network users before beginning the process, and do it a time that is minimally disruptive to the network.

To upgrade the WANJet software version:

1. Before beginning the upgrade process, ensure that a disk image of the new version of the WANJet (on CD-ROM, for example) is accessible from the local computer on which you are viewing the Web UI.
2. In the Web UI, expand the **System** section of the menu bar, and click **Upgrade**:



3. On the **Upgrade** page, click **Stop [Server Name]** to stop the current processing session. A confirmation pop-up appears. Click **OK** to continue.
4. On the next page, click **Browse** to launch a browser dialog in which you can locate the upgrade file on your local computer, and upload it to your F5 appliance.
5. Click **Upgrade WANJet**. After the upgrade process is complete, the F5 appliance will restart automatically.

Chapter 6

Advanced Configuration

- Optimization Policies ◀
 - Operational Mode ◀
 - Configuring Tuning Settings ◀
 - Updating the Local WANJet Configuration ◀
 - Managing Remote WANJets ◀
 - Redundant Peers ◀
 - Updating the NIC Configuration ◀
 - Managing Static Routes ◀
 - Granting Access to WANJet Web UI ◀
 - Configuring Syslog and SNMP Settings ◀
 - Email alerts ◀
-

Aside from the initial hardware setup and basic WANJet configuration, which occurred when you installed your F5 appliance in Chapters 2 and 3, and the basic administration tasks described in Chapter 5, WANJet includes a range of advanced settings for fine-tuning your WAN link optimization:

- *Optimization policies* allow you to specify the TCP/UDP ports that WANJet's ACM5 optimization is applied to
- WANJet's *operational mode* controls whether optimization is active, whether TDR is operational, and how the appliance is deployed in your network topology
- The *Tuning* page allows you to set the average bandwidth, round-trip time, buffer size and queue size for your WAN link, to fine-tune WANJet performance
- *Local* and *remote WANJet configuration* involve setting IP addresses and other parameters for the networks in which your WANJets are operating
- Enabling a *redundant peer* avoids having a central point of failure for optimization
- You can update the *NIC configuration* for your WANJet's network interfaces, and manage *static routes* through your subnets
- For added security, control *access* to the WANJet Web UI by client IP address
- Configure *syslog*, *SNMP* and *RMON2 settings* for remote error logging

Optimization Policies

Optimization policies allow you to specify the TCP/UDP ports that WANJet's ACM5 and TDR optimization algorithms are applied to. On the Optimization Policy page, you also make WANJet aware of local and remote subnets.

Optimization Policy

Local WANJet

WANJet, 172.16.30.80

Include WANJet Subnet

☒

Local Subnet	Alias
✓ 172.16.30.0/24	

Add

Remote WANJet

test0_2, 192.168.240.2

Reset

Remote Subnet	Alias
✓ 192.168.240.0/24	

Add

Protocol	Service Name	Processing Mode	TDR-1	TDR-2	Encryption	Connection Intercept
TCP	20 (Active FTP data)	ACM5	Y	N	N	N
TCP	25 (Smtp)	ACM5	Y	N	N	N
TCP	80 (Http)	ACM5	Y	N	N	N
TCP	110 (Pop3)	ACM5	Y	N	N	N
TCP	220 (Imap3)	ACM5	Y	N	N	N
TCP	443 (Https)	ACM5	N	N	N	N
TCP	All other ports	Passthrough	N	N	N	N
UDP	All ports	Passthrough	N	N/A	N/A	N/A

Add

Note: Click "Save" to apply the changes.

Changes will not be reflected until the operation is completed.

Save

Cancel

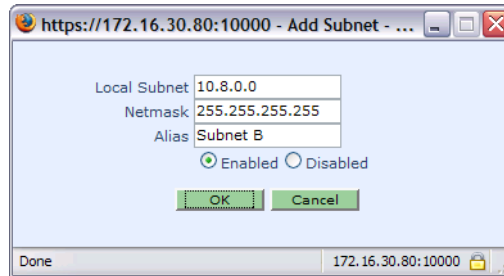
On this page there is a check box labelled **Include WANJet Subnet**. This box is checked by default. If you uncheck this box, the WANJet subnet is removed from the subnet list and the traffic of this subnet is no longer processed. Do this if you wish only traffic from the subnets listed below this checkbox to be processed.

Adding local subnets

You can add a new machine or subnet to the list of machines/subnets whose data is processed by the WANJet, and update or remove machines and subnets whose data is already being processed.

To add a new subnet to the local WANJet

1. Expand the **Operational Settings** section of the menu bar, and click on **Optimization Policy**.
2. Click on the **Add** button below the Local Subnets list. The Add Subnet page opens in a browser pop-up:



3. Enter the IP address of the new local machine/subnet in the **Local Subnet** field, for example 10.8.0.0
4. Enter the netmask of the local machine/subnet in the **Netmask** field, for example 255.255.0.0
5. Enter a name for the new machine/subnet in the **Alias** field, for example Subnet B.
6. Select **Enabled** if you want the WANJet to process the traffic of this machine/subnet at this time. Otherwise, select **Disabled**.
7. Click **OK**. You are returned to the Optimization Policy page and the new machine/subnet is displayed on the local subnets list.
8. Click **Save** at the bottom of the page.

To update or remove a local machine or subnet:

1. Click the link of the machine/subnet in the list of local subnets on the Optimization Policy page. The Edit Subnet page opens in a browser pop-up. This is exactly the same as the Add Subnet page shown above, except that it also has a **Remove** button.
2. Click **Remove** to delete this subnet from the list, or edit the settings and click **OK**.
3. Save your changes by clicking **Save** on the Optimization Policy page.

Note: You cannot update or remove the local F5 appliance's own subnet.

Adding remote subnets

You can add a new machine or subnet to a remote WANJet network, and edit or delete existing machines and subnets. Always add the gateway of any remote WANJet as one of its subnets and ensure that the status of this subnet is disabled.

To add a new subnet to a remote WANJet:

1. Expand the **Operational Settings** section of the menu bar, and click on **Optimization Policy**.
2. In the **Remote WANJet** drop-down list, select the remote WANJet that you want to add subnets to.
3. Click on the **Add** button below the Remote Subnets list. The Add Subnet page opens in a browser pop-up (see page 77 for a screenshot).
4. In the **Supported Subnet** field, enter the IP address of the machine/subnet that you want to make visible to the remote F5 appliance.
5. In the **Netmask** field, enter the netmask of the remote subnet.
6. In the **Machine(s) Alias** field, enter a name for the machine/subnet.
7. The default status for the new subnet is **Enabled**. Select **Disabled** if you do not want the WANJet to process the traffic of this subnet at this time.
8. Click **OK**. You are returned to the Optimization Policy page with the new subnet displayed in the list of remote subnets.
9. Click **Save** at the bottom of the page.

To update or remove a subnet from a remote WANJet:

1. Select the appliance in the **Remote WANJet** drop-down list.
2. In the **Remote Subnet** list, click on the IP address of the subnet you want to modify or remove. The Edit Subnet page opens in a browser pop-up. This is exactly the same as the Add Subnet page (see page 77), except that it also has a **Remove** button.
3. Click **Remove** to permanently delete this subnet, or edit the settings and click **OK** to modify it.
4. Save your changes by clicking **Save** on the Optimization Policy frame.

Configuring Port Settings

For each port on a remote WANJet, you can set the processing mode and the ToS (Type of Service) priority that are assigned to packets. These can be assigned separately for TCP and UDP packets – allowing you, for example, to optimize TCP traffic on a port while allowing UDP traffic to pass through untouched.

By default, some commonly used ports (corresponding to Active FTP, SMTP, HTTP, POP3, IMAP and HTTPS) have ACM5 optimization enabled. All these ports except 443 (HTTPS) also have TDR-1 compression enabled. Settings for these ports can be edited by clicking on the corresponding link. All other ports have optimization disabled by default.

Note: Passive FTP sessions are difficult to optimize specifically, since the server port used by Passive FTP varies from session to session. If optimization of Passive FTP is needed, you should enable optimization on all TCP ports (see page 81) and disable optimization on those ports that do not require it (typically ports used by real-time applications such as VoIP telephony).

Configuring Specific Ports

To set the processing mode for a particular port (or range of ports):

1. Expand the **Operational Settings** section of the menu bar, and click on **Optimization Policy**.
2. Select the IP address of the WANJet to which you are connecting from the **Remote WANJet** drop-down list.
3. Click on the third **Add** button (circled in the screenshot below), underneath the **TOS Priority** column:

Optimization Policy

Local WANJet: WANJet, 172.16.30.80

Include WANJet Subnet ☒

Local Subnet	Alias
✓ 172.16.30.0/24	

Add

Remote WANJet: test0_2, 192.168.240.2

Reset

Remote Subnet	Alias
✓ 192.168.240.0/24	

Add

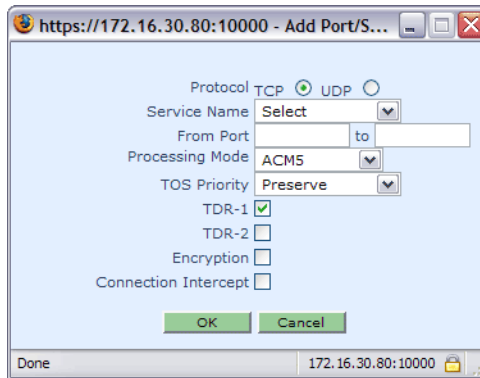
Protocol	Service Name	Processing Mode	TDR-1	TDR-2	Encryption	Connection Intercept
TCP	20 (Active FTP data)	ACMS	Y	N	N	N
TCP	25 (Smtp)	ACMS	Y	N	N	N
TCP	80 (Http)	ACMS	Y	N	N	N
TCP	110 (Pop3)	ACMS	Y	N	N	N
TCP	220 (imap3)	ACMS	Y	N	N	N
TCP	443 (https)	ACMS	N	N	N	N
TCP	All other ports	Passthrough	N	N	N	N
UDP	All ports	Passthrough	N	N/A	N/A	N/A

Add

Note: Click "Save" to apply the changes.
Changes will not be reflected until the operation is completed.

Save Cancel

The Add Port/Service Name form opens in a browser pop-up:



4. You can select a service or application that uses the network from the **Service Name** drop-down list. The default port used by this service will then appear in the **From Port** field.

Alternatively, you can enter the port number directly in the **From Port** field. To specify a range of ports, enter the first port of the range in the **From Port** field and the last port in the **To** field.

Refer to <http://www.iana.org/assignments/port-numbers> for a list of commonly assigned TCP/UDP port numbers and the services and applications that use them – but remember that these may differ on your system.

5. Choose a **Processing Mode** for the specified port(s). Select either:
 - **Passthrough** – to leave traffic over this port in its raw state
 - **ACMS** – to apply WANJet optimization to traffic over this port
- Select the priority you want to assign to this port or ports from the **TOS Priority** list:
 - 7 – for Network Control
 - 6 – for Internet Control
 - 5 – for Critical
 - 4 – for Flash Override
 - 3 – for Flash
 - 2 – for Immediate
 - 1 – for Priority
 - 0 – for Routine

Refer to <http://www.ietf.org/rfc/rfc0791.txt> for more information about ToS priority levels.

6. You can set four different WANJet optimization options using checkboxes (these options are only available if you have selected **ACM5** as the processing mode):
 - Check the **TDR-1** box if you want to compress network traffic on the specified port. This is not necessary if the traffic would not benefit from compression, for instance if it consists largely of JPEG or ZIP files.
 - Check the **TDR-2** box if you want to apply WANJet's TDR-2 intelligent caching algorithm
 - Check the **Encryption** box if network traffic on the specified port is encrypted using SSL
 - Check the **Connection Intercept** box if you want to reset any connection over the specified port that was opened before these settings were applied
7. Click **OK** to return to the Optimization Policy page. A new row will now appear in the third table on the page, containing the details you have just entered. You can click on the port number (in the **Service Name** column) to edit these settings.
8. Click **Save** at the bottom of the Optimization Policy page to apply the new port settings to the selected F5 appliance.

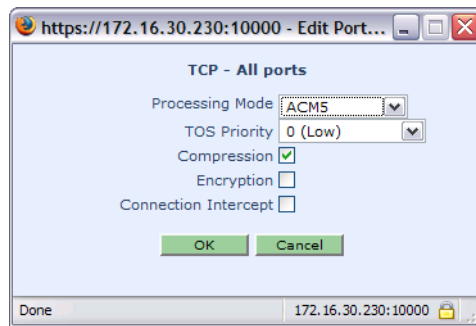
Configuring All Other Ports

In addition to defining optimization policies for specific ports, you can change the default policies that have been set up for all TCP and all UDP ports. (Any policies defined for individual ports will override these default policies.)

To set the default processing mode for all TCP/UDP ports:

1. Expand the **Operational Settings** section of the menu bar, and click on **Optimization Policy**.
2. Select the IP address of the WANJet to which you are connecting from the **Remote WANJet** drop-down list.
3. Go to the third table on the Optimization Policy page. In the **Service Name** column, for either the TCP or the UDP protocol, click on the **All Ports** link (this will read **All other ports** if optimization policies have been defined for specific ports).

The Edit Port/Service Name form opens in a browser pop-up:



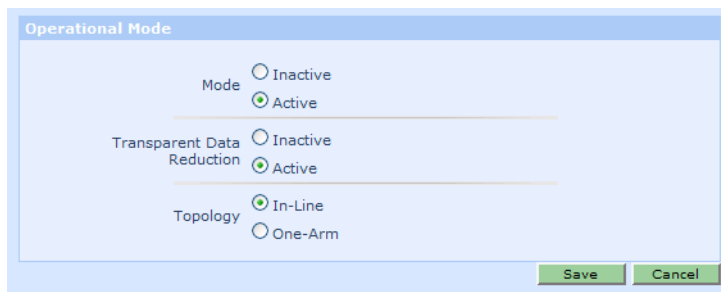
4. Follow the steps listed in the previous section for configuring a specific port, starting at [Step 5](#) on page 80.
5. Once you have clicked **OK** on the pop-up, be sure to click **Save** on the Optimization Policy page, or your changes will be lost.

Operational Mode

The Operational Mode page allows you to control whether WANJet is active or inactive, whether TDR (Transparent Data Reduction) is operational, and how WANJet is deployed in your network topology.

To configure WANJet's operational mode:

1. Expand the **Operational Settings** section in the menu bar, and click on **Operational Mode**. The Operational Mode page is displayed:



2. The **Mode** section allows you to enable and disable WANJet optimization. When set to **Inactive**, optimization does not occur and WANJet becomes completely transparent to network traffic.
3. In the **Transparent Data Reduction** section, you can activate or deactivate WANJet's TDR technology (see [Transparent Data Reduction](#) on page 3).
4. Update the **Topology** section if you change the way in which your F5 appliance is connected to the network. The usual network topology is **In-Line**, which means that the WANJet is located between the LAN (or the LAN switch) and the WAN gateway (or the LAN router). If you select this option, you can skip to [Step 8](#)

If the WANJet is located on a separate independent link, select **One-Arm** instead (see the next section).

Click **Save** to store your changes to WANJet's operational mode, or **Cancel** to abandon them.

One-arm topology

This option allows WANJet to be deployed out-of-line, with one physical connection to the LAN and no direct connection to the WAN (see [One-Arm Deployment](#) on page 13).

If you select **One-Arm** in the **Topology** section of the **Operational Mode** page, a new section entitled **Redirection Method** appears. Choose either:

- **Static Routing** – if each client on your LAN is configured to route network traffic through WANJet
- **Transparent Proxy** – if LAN traffic designated for optimization is directed to WANJet by a router

If you select **Transparent Proxy** in the **Redirection Method** section, a new section entitled **Discovery Method** appears. Choose either:

- **Static** – if passthrough traffic is not routed to WANJet. In this case, only network traffic which is scheduled for ACM5 optimization is routed through the F5 appliance, and this traffic will be lost if WANJet is not running.
- **WCCPv2** – if WANJet communicates with your network router using WCCP (the Web Cache Coordination Protocol). In this case, all network traffic is routed through the F5 appliance, but the router will by-pass the appliance if WANJet is not running.

WCCP-based discovery

WANJet can use the WCCP protocol to advertise itself to a LAN router as a “web cache”. Local routers and web caches together form a service group. Routers redirect traffic to the group-member web caches – i.e., the local WANJet(s) – according to an algorithm defined for the service group.

If you select **WCCPv2** in the **Discovery Method** section, four new controls appear. The **Operational Mode** page now looks like the screenshot overleaf:

Operational Mode

Mode ☐ Inactive ☒ Active

Transparent Data Reduction ☐ Inactive ☒ Active

Topology ☐ In-Line ☒ One-Arm

Redirection Method ☐ Static Routing ☒ Transparent Proxy

Discovery Method ☐ Static ☒ WCCPv2

Service ID (51-100)

Priority (1-255)

Router

Authenticate ☐ Password

Save **Cancel**

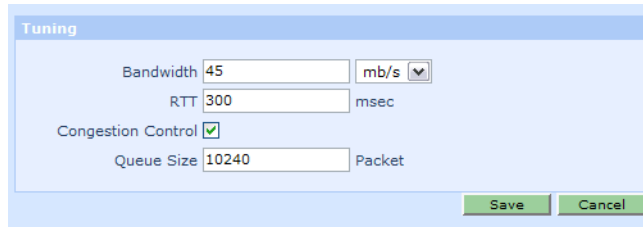
- Enter the service group identifier in the **Service ID** field. This must be a number between 51 and 100. It should match the service ID configured on the LAN router.
- Enter the priority assigned by the router to the service group in the **Priority** field. This must be a number between 0 and 255. It determines the order in which redirection rules are followed, and should also match the priority configured on the router.
- Enter the IP address of the LAN router communicating with WANJet in the **Router** field.
- If WCCP is configured to require authentication between WANJet and the router, check the **Authenticate** box and type in the password.

Link Refer to <http://www.fags.org/rfcs/rfc3040.html> for a detailed specification of the WCCP protocol.

Click **Save** to store your changes to WANJet's operational mode, or **Cancel** to abandon them.

Configuring Tuning Settings

Under **Operational Settings** on the menu, click on **Tuning**. The Tuning page enables you to make the maximum use of WAN link bandwidth, guaranteeing maximum throughput. To configure WANJet tuning settings, you specify the link bandwidth, and the RTT (Round Trip Time).



1. In the **Bandwidth** field, enter your WAN link bandwidth. The default bandwidth is 45 megabits per second. (You can change the unit used in this field to kilobits per second, for lower-bandwidth links).
2. In the **RTT** field, enter the average round trip time for your WAN link. The default round trip time is 300 milliseconds.
3. Select the **Congestion Control** checkbox if you want WANJet to handle the traffic congestion that occurs in the case of packet loss (this is selected by default).
4. In the **Queue Size** field, enter the maximum number of outgoing packets to keep in a queue before they start to be dropped (in case of network problems). The default queue size is 10240 packets.
5. Click **Save** at the bottom of the page. The Tuning page refreshes and your changes are committed to WANJet.

Updating the Local WANJet Configuration

Under **System Settings** on the menu, click on **Local WANJet**. This frame allows you to edit network information for the local WANJet, define redundant peers, add subnets, and define VLANs to the local WANJet. The initial values shown on this frame were specified during initial hardware configuration (using the LCD panel or a serial console) and WANJet software configuration, as described under [Basic WANJet Configuration](#) on page 21.

Changes to WANJet IP address, port, or subnet address must be replicated wherever these settings appear:

- on the Local WANJet page in the Web UI for this WANJet
- on each Remote WANJet page that describes this WANJet in the Web UI of any remote WANJets connected to this one

For example, assume you have four connected F5 appliances, called B1, B2, B3, and B4. When you bring up the Web UI for B1 using its IP address in the URL, the Web UI shows it as the local WANJet and shows B2, B3, and B4 as its remote WANJets. If, for example, you change the IP address for B1 on its Local WANJet frame, you must also log onto the Web UI for B2, go to the Remote WANJets page and click on the link for B1, and change the IP address for B1 to match. You must repeat this step for B3 and B4. This way, the IP address specified for WANJet B1 is correct for all F5 appliances that communicate with it.

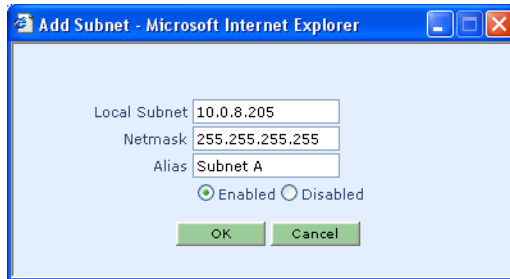
Provide information, such as the alias, that was not part of the initial configuration, or modify current values. Click **Save** when you have finished.

WANJet Alias	Name used for this WANJet appliance. This name is displayed at the upper-left corner of the home page when you log onto the WANJet Web UI.
WANJet IP	IP address assigned to the local F5 appliance on your network. If you change this value, you change this WANJet IP address for each remote WANJet that accesses it. See the Note below.
WANJet Netmask	Subnet mask assigned to the F5 appliance on your network.
WAN Gateway	IP address of your gateway.
LAN Router	IP address of the network router.
WANJet Port	The main port number that the local WANJet uses to communicate with remote WANJet appliances. The default port is 3701. You should only change this port if you also change it for all remote WANJet appliances. See the Note below.
License Key	License key for the local installation of WANJet. If this field is blank or contains an invalid key, WANJet does not process your data.
Redundant Peer IP	IP address of the redundant WANJet peer. Check the box, and the text box for the IP address appears.

Note To update the IP address or port for this WANJet on all the remote WANJets, go to **Remote WANJets** under **System Settings** in the menu. From that frame, you can use the **Login** link for each remote WANJet to log into its Web UI and make the necessary changes from its Remote WANJet frame.

Adding a Subnet

There are several ways to add a subnet to the WANJet. You can use the method described under [Adding local subnets](#) on page 76. Alternatively, from the Local WANJet page, click the **Add** button to bring up the Add Subnet form in a browser pop-up:



1. In the **Local Subnet** field, enter the IP address of the new local subnet.
2. In the **Netmask** field, enter the netmask of the new local subnet.
3. In the **Alias** field, enter a name for the new subnet.
4. Select **Enabled** if you wish the WANJet to optimize network traffic for this subnet. Otherwise, select **Disabled**.
5. Click **OK**. The Local WANJet page is displayed, with the new subnet added to the list of subnets.
6. Click **Save** at the bottom of the page.

Edit the subnet settings at any time by clicking on the corresponding link in the list of subnets.

Note: If you change the subnet IP address, you must change this value (on the Remote WANJets page) in the Web UI for each remote WANJet that is linked to the local one.

Remove a subnet at any time by clicking the corresponding link in the list of subnets, and then clicking **Remove** on the Edit Subnet form.

Managing Virtual LANs

A VLAN (Virtual LAN) is a computer network whose boundaries are defined logically, rather than physically. WANJet must be explicitly made aware, via the Web UI, of any VLANs that are linked to your network. This is because VLANs are often implemented by adding tags to Ethernet frames, and these tags must be preserved during optimization.

To add a VLAN to WANJet via the Web UI:

1. Click on **System Settings > Local WANJet** in the menu bar.
2. On the Local WANJet page, click on **VLAN Settings**. Any VLAN currently defined in the WANJet is shown here:

IP	Netmask	Gateway	Tag
10.0.8.209	255.255.0.0	10.0.8.200	1245

Note: Press "Save" to apply the changes.
Changes will not be reflected until the operation is completed.

Add Save Cancel

3. Click the **Add** button to display the Add VLAN page in a browser pop-up:

https://172.16.30.230:10000 - Add VLAN - ...

WANJet Virtual IP 10.0.8.209
VLAN Netmask 255.255.255.255
VLAN Gateway 10.0.8.200
VLAN Tag 1245

OK Cancel

Done 172.16.30.230:10000

4. In the **WANJet Virtual IP** field, enter the virtual IP address assigned to the local F5 appliance on this VLAN – that is, the IP address which other machines on the VLAN use to communicate with the appliance.
5. In the **VLAN Netmask** field, enter the subnet mask for the VLAN.
6. In the **VLAN Gateway** field, enter the virtual IP address of the gateway machine for the VLAN.
7. In the **VLAN Tag** field, enter the VLAN ID. WANJet uses this information to preserve tagged Ethernet frames that pass to and from the VLAN.
8. Click **OK** to return to the VLAN Settings page, and click **Save** at the bottom of that page.

After making WANJet aware of the VLAN, add the VLAN as one of the subnets of the local WANJet so that the WANJet can optimize the traffic coming from this VLAN. You should also make any remote WANJets that are linked to the local appliance aware of the VLAN, and also add it as one of their subnets. This is necessary if the remote WANJets are to handle optimized data from the VLAN.

To edit or delete a VLAN, click on its IP address in the table on the VLAN Settings page. This will display the Edit VLAN page in a browser pop-up, in which you can change any of the VLAN information or use the **Remove** button to delete it.

When you remove a VLAN from a local WANJet, you must also remove it from the list of subnets supported by that WANJet.

Managing Remote WANJets

In order to optimize data sent over a network link, a pair of F5 appliances – each running the WANJet software – are needed. A remote WANJet reverses the optimization process for data sent from the local WANJet. In order for this to happen, however, the local WANJet must be made aware of the remote WANJet using the Web UI. If you do not specify a remote F5 appliance to receive the processed data, network traffic will pass through the local WANJet without being optimized.

On the **Remote WANJets** page, you can change the settings of each remote WANJet that is linked to the local WANJet. You can also use the **Login** link to bring up the Web UI for a remote WANJet and configure it as if it were a local appliance:

IP	Alias	Version	WANJet Port	Manage
192.168.190.2	Remote-demo-0	3.1.3	3701	Login

Note: Click "Save" to apply the changes.
Changes will not be reflected until the operation is completed.

[Add](#) [Save](#) [Cancel](#)

Note: Always click **Save** after making any changes to remote WANJet configuration, or your changes will be lost.

Adding a Remote WANJet

To link a remote WANJet to the local appliance:

1. Expand the **System Settings** section of the menu bar, and click on **Remote WANJets**.
2. Click on the **Add** button. The Manage Remote WANJet page opens in a browser pop-up:

3. Select the **WANJet Type** as either **Single** or **Redundant**. Select **Redundant** if you have two connected WANJet peers on the same remote LAN. (See [Redundant Peers](#) on page 93 for an explanation of these node types.)
4. In the **WANJet IP** field, enter the IP address of the remote WANJet. If you selected **Redundant** in [Step 3](#), there is also a **Node 2** field for you to enter the peer's IP address.
5. In the **WANJet Alias** field, enter a meaningful name for the remote WANJet (limited to 13 characters).
6. In the **WANJet Port** field, enter the main port number on which the remote WANJet listens for data from the local WANJet. The default port number is 3701. Change this port only if you change it for all connected F5 appliances.
7. In the **Shared Key** field, enter a shared key which authenticates between local and remote WANJets. You can set a unique shared key for every pair of F5 appliances.
8. If the local WANJet has a LAN router specified for it, you can select an **MTU** (Maximum Transmission Unit) for the remote WANJet. The MTU is defined as the size of the largest datagram able to pass across a network connection. Choose one of the following options:

Direct The default MTU for this option is 1500 bytes. It is the most common MTU for the IP protocol.

VPN The default MTU for this option is 1400 bytes.

Other You can specify the MTU of your network according to your needs.

9. Click **OK** on the **Manage Remote WANJet** page to return to the main **Remote WANJets** page.
10. Click **Save** at the bottom of this page.
11. You now need to add the gateway of the remote WANJet as a disabled subnet. For information on how to add a subnet, see [Adding remote subnets](#) on page 78.

Tip: For information on specifying a processing mode for a particular port, see [Configuring Specific Ports](#) on page 79.

To edit the settings of a remote WANJet, click on the appliance's IP address on the **Remote WANJets** page. Make your changes on the **Manage Remote WANJet** page and click **OK** when finished. After returning to the **Remote WANJets** page, be sure to click **Save** to commit your changes.

Remember that if you edit the port number of the remote WANJet, you must change this port for all connected F5 appliances so they can communicate with each other.

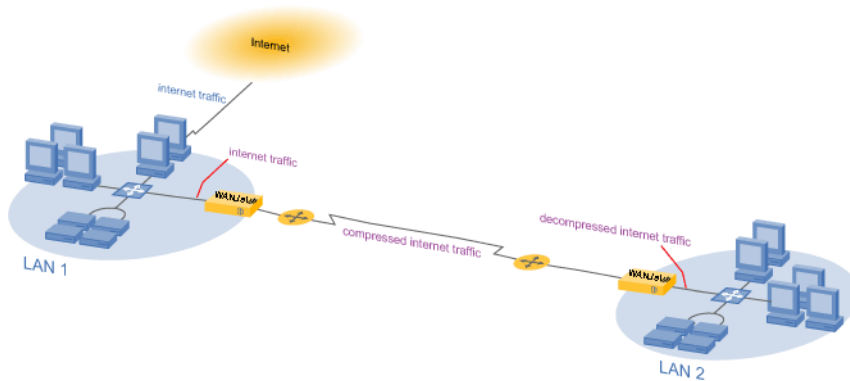
To delete a remote WANJet, click the IP address of the remote WANJet on the **Remote WANJets** page. Click **Remove** on the **Manage Remote WANJet** pop-up. After returning to the **Remote WANJets** page, click **Save** to commit your changes. By removing a remote WANJet and its network, you also remove all associated subnets and ports.

Note: When you remove the network for a remote WANJet, the local WANJet will no longer see the remote appliance, and any data sent to the network of the removed WANJet will pass through without being optimized.

Redundant Peers

Redundancy offers a continuous mode of operation and eliminates having a central point of failure for either LAN switching or routing. WANJet supports redundancy by allowing the use of a second F5 appliance on a LAN, connected to a redundant router. The second appliance is known as a redundant peer. In the case of failure of one of the LAN's routers, the corresponding WANJet appliance detects that the router is down and service continues through the remaining active router and F5 appliance.

Not only does the WANJet offer you a continuous mode of operation, but it also provides load-balancing under normal network conditions by distributing network traffic over two F5 appliances.



You cannot access a redundant peer through the Web UI until you have added both the primary peer and the redundant peer to the **Remote WANJets** table of a F5 appliance that is remote from the peers' LAN. For more information on how to add remote WANJets, see [Adding a Remote WANJet](#) on page 91.

Assume that there is a primary peer called WANJet A and its redundant peer WANJet A-1. A and A-1 are connected to the remote appliances WANJet B and WANJet C. To be able to access A and A-1, you must:

1. Add both A and A-1 to the **Remote WANJets** page in the Web UI for WANJet B.
2. Add both A and A-1 to the **Remote WANJets** page in the Web UI for WANJet C.

Updating the NIC Configuration

You can specify the speed of the network interfaces the WANJet uses to communicate with the LAN and the WAN. The WANJet supports different speeds in both half-duplex and full duplex.

1. Expand the **System Settings** section of the menu bar, and click on **NIC Configuration**.

The screenshot shows a window titled "Nic Configuration". Inside, there are two rows. The first row is for "eth0 (LAN)" with a "Media Type" dropdown menu set to "Auto Negotiate". The second row is for "eth1 (WAN)" with a "Media Type" dropdown menu also set to "Auto Negotiate". At the bottom right of the window, there are two buttons: "Save" and "Cancel".

2. Select the type of network interface that WANJet uses to connect to the LAN and WAN from the **eth0** and **eth1** drop-down lists, and click **Save**.

By default, WANJet will negotiate both interface speeds automatically, so you do not normally need to set these details manually.

Managing Static Routes

Expand the **System Settings** section of the menu bar, and click on **Routing Table**.

The routing table contains information on any gateway (router) you specify as routing the data of a specific network. Data packets sent to this gateway use the relevant static route to identify their destination.

The screenshot shows a window titled "Routing Table". It contains a table with the following data:

Network	Netmask	Next Hop	MTU
10.9.9.0	255.255.255.0	10.55.55.20	1500
10.7.7.0	255.255.255.0	10.55.55.1	1500
10.0.0.0	255.255.0.0	10.55.55.2	1500

Below the table, there is a note: "Note: To delete an entry in the Routing Table, delete the content of the "Network" field of that entry." At the bottom right of the window, there is a "Save" button.

If you specified a LAN router for your local WANJet, all subnets in your local WANJet use this LAN router to identify the destinations of packets. To be able to specify a gateway for each subnet, remove the IP address from the **LAN Router** field on the Local WANJet page (see [Updating the Local WANJet Configuration](#) on page 86).

To add a static route:

1. In the **Network** field, enter the IP address of the subnet that should route its data to a specific gateway.
2. In the **Netmask** field, enter the netmask of the network.
3. In the **Next Hop** field, enter the IP address of the gateway to which the data should be routed. Data packets use this gateway to send them to their destination.
4. In the **MTU** field, enter the MTU – the maximum packet size – of datagrams transferred through this route.
5. Click **Save** at the bottom of the page.

To edit an existing static route, modify any values that need changing and click **Save**.

Note: If you modify the **Network** field, which is the IP address of a network, you must also modify the **Netmask** field.

To remove a static route, simply clear the **Network** field of the route that you wish to delete. Click **Save** and the static route is removed.

Granting Access to WANJet Web UI

Expand the **System Settings** section of the menu bar, and click on **IP Access Control**.

On this screen, you can limit access to the Web UI:

The default setting is **Allow all addresses**, so that any machine on your network can access the Web UI. With this setting, you can restrict access by creating a password for the Web UI and providing this password only to approved personnel. See [Changing the WANJet Web UI password](#) on page 66.

To provide an additional layer of security, you can restrict the machines allowed to access the Web UI, using their IP addresses as identification. Choose one of the following two options and enter the IP addresses of the machines or subnets in the text box:

- **Allow Listed Addresses**

Enables the machines or subnets that you specify in the text box to access the appliance and the SNMP reports residing on it. At a minimum, specify the IP addresses for:

- your SNMP server, to be able to see SNMP and RMON2 reports (refer to [Configuring Syslog and SNMP Settings](#) on page 96)
- your Syslog server, to be able to see Syslog data (refer to page 96)
- the machine from which you are currently accessing the Web UI through a browser
any other machines from which you want to manage WANJet or the WANJet using the Web UI

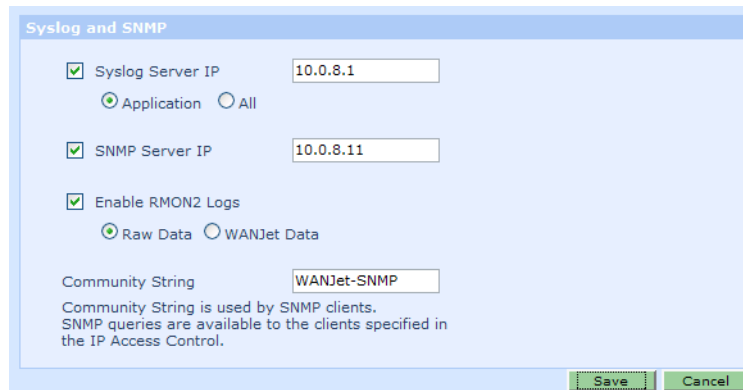
- **Deny Listed Addresses**

Prevents the machines or subnets that you specify in the text box from accessing the appliance or SNMP reports. All other machines on your network are granted access to the appliance and the SNMP reports residing on it.

If a machine that has not been granted access to the Web UI attempts to access it through a browser, the browser returns a 404: Page Not Found error page.

Configuring Syslog and SNMP Settings

Under **System Settings** on the menu, click on **Syslog and SNMP**. You can specify which servers you want to retrieve Syslog, SNMP, and RMON2 reports, whether RMON2 data is gathered before or after the WANJet processes it, and the community string for viewing SNMP reports:



The screenshot shows a configuration window titled "Syslog and SNMP". It contains the following settings:

- ☒ Syslog Server IP: 10.0.8.1
- ☒ Application ☐ All
- ☒ SNMP Server IP: 10.0.8.11
- ☒ Enable RMON2 Logs
- ☒ Raw Data ☐ WANJet Data
- Community String: WANJet-SNMP

Below the Community String field, there is a note: "Community String is used by SNMP clients. SNMP queries are available to the clients specified in the IP Access Control." At the bottom right, there are "Save" and "Cancel" buttons.

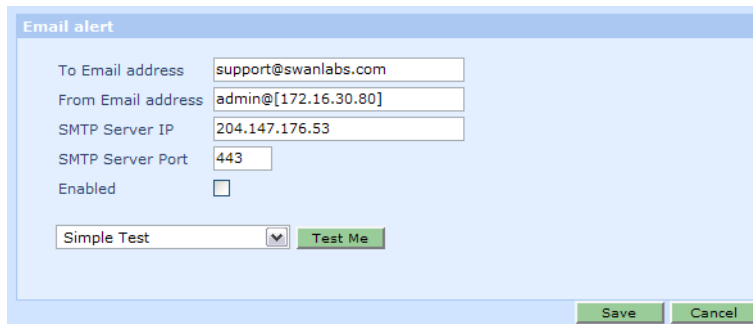
1. Check the **Syslog Server IP** box and enter the IP address of the server that receives WANJet Syslog data.
 - Select **Application** to store only the application error log on this server
 - Select **All** to store all error logs on this server
2. Check the **SNMP Server IP** box and enter the IP address of the SNMP server to which the WANJet sends error messages. For more information on viewing SNMP reports, see [SNMP reports](#) on page 62.
 - Check the **Enable RMON2 Logs** box if you want to view RMON2 data. Choose either:
 - **Raw WANJet** to view RMON2 logs from before the WANJet processes your traffic
 - **WANJet Data** to view RMON2 logs after the WANJet processes your traffic.

For more information on viewing RMON2 reports, refer to [RMON2 Reports](#) on page 63.
3. In the **Community String** field, enter the shared community string needed to access the SNMP reports on WANJet.
4. Click **Save**. The Syslog and SNMP page refreshes and your changes are committed to WANJet.

Email alerts

The Email alert page allows you to receive system snapshots by email. An email containing logged information is automatically sent to a specified email address in the event of system failure. For information on how to download system snapshots directly, refer to [Diagnostic Log](#) on page 47.

To configure email alerts, go to the **System Settings** section of the menu bar and click on **Email alert**.



This page contains the following fields:

- | | |
|---------------------------|---|
| To Email Address | The address to which the system snapshot is sent. By default, emails are sent to support@swanlabs.com |
| From Email Address | <p>The address from which the email alert will appear to be sent. This need not be an actual email account, but should look like a valid address in order to pass through spam filters.</p> <p>A good rule of thumb is to use the alias of the WANJet from which the snapshot was taken as the first part of the address (before the @ symbol), and use your company's domain name as the second part of the address, e.g. WJ_NewYork@acme.com</p> |
| SMTP Server IP | The IP address (not the domain name) of an SMTP mail server accessible from the WANJet appliance, that can forward this email |

SMTP Server Port	<p>The port on the mail server to which the SMTP request for the email alert will be sent.</p> <p>Note: The normal port used by SMTP is 25. However, the default port used by the WANJet for email alerts is 443 (normally used by SSL traffic). This is because traffic to port 443 is more likely to be allowed through a firewall. You should ensure that the mail server specified in the SMTP Server IP field is set up to forward traffic on port 443 to port 25.</p>
Enabled	<p>Select this checkbox to enable the automatic emailing of system snapshots.</p>

Email alerts are disabled by default, but it is recommended that you enable them after filling in the details in the fields listed above.

Before enabling email alerts you should use the **Test Me** button to test whether the WANJet can access the mail server and send the email. You can send a simple test message, create a new system snapshot to send, or send all past system snapshots. Sending a test message is advisable because the WANJet will not attempt to resend failed emails.

Service Policy Configuration

[IT Service Policies](#) ◀
[Application QoS Policies](#) ◀
[Managing WAN Links](#) ◀

WANJet enables you to define IT service policies and application Quality of Service (QoS) policies for your various applications, and apply them to optimally allocate bandwidth. An IT service policy specifies a named group of ports, machines, and subnets. When you define an application QoS policy, you can specify an IT service group, in addition to specifying the bandwidth you want to allocate to particular applications, such as:

- mission-critical applications
- video and voice streaming
- interactive video or voice
- data transfers
- web-based applications

These different classes of applications have very different network requirements. The challenge is to align the network services to the application's requirements from a performance perspective.

IT Service Policies

The **IT Service Policies** feature enables you to define services used to achieve specific QoS standards. You can group ports, machines and subnets under the heading of an IT service policy. By assigning a minimum and a maximum amount of bandwidth to this service (in an Application QoS policy), you treat this group of ports, machines and subnets as one entity. This is simpler than creating many different services which each handle a single type of traffic.

Adding an IT Service Policy

To define a new IT service policy:

1. Under **Operational Settings** on the menu, click on **IT Service policies**.
2. Click **Add**. The IT Service Policy page opens in a browser pop-up:

3. Enter the name you choose for this service in the **Policy Name** field.
4. Enter the IP address and the netmask of the subnets for which you want to specify an IT service Policy. To specify the subnet that sends the data, enter the IP address in the **From** field, with the full netmask, in dotted quad format, after the slash (/). To specify the subnet that receives the data, enter the IP address in the **To** field, again with the full netmask after the slash.
5. Specify the port you want. Select a port from the **Ports** drop-down list or enter a range of ports using the **From Port** fields.
6. Select the protocol type of the ports specified earlier from the **Protocol** drop-down list.
7. Click **OK** to return to the IT Service Policies page.
8. Click **Save**. The IT Service Policies page refreshes and your changes are saved.

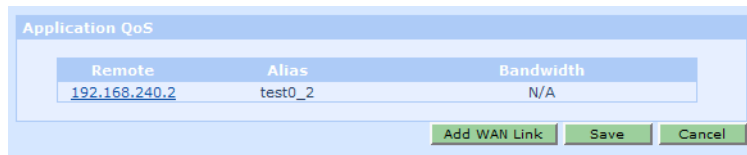
You can also edit or delete an IT service policy. On the IT Service Policies page, click the name of the policy to open the IT Service Policy pop-up and edit the policy. Make your changes and click **OK** to save them, or to delete the policy, click **Remove**.

Application QoS Policies

The **Application QoS** feature helps you obtain better network performance by dedicating bandwidth to specific network traffic. At the same time, you can ensure that providing sufficient bandwidth one or more data flows does not handicap the transmission of other data flows. The Application QoS polices can handle different types of services:

- Fundamental services – the basic protocols supported by your network
- IT service policies – tailored services that include different types of traffic (see page 102)

Under **Operational Settings** on the menu, click on **Application QoS**. The Application QoS page is displayed:



Remote	Alias	Bandwidth
192.168.240.2	test0_2	N/A

[Add WAN Link](#) [Save](#) [Cancel](#)

Adding an Application QoS Policy to a Remote WANJet

To add a policy to a remote WANJet:

1. Go to the Application QoS page shown above.
2. Click on the link of the remote WANJet to which you want to assign an application QoS policy. The Manage the Application QoS Settings of a Remote WANJet page opens in a browser pop-up:

Node Type:

WANJet IP:

WANJet Alias:

Link Bandwidth:

Supported Subnet	Netmask	Alias	Status
192.168.240.0	255.255.255.0		Enabled

Protocol	Service Name	Processing Mode	Compression	Encryption	Connection Intercept	TOS Priority
TCP	All ports	ACMS	Y	N	N	0 (Low)
UDP	All ports	Passthrough	N	N/A	N/A	N/A

Application QoS Policy	Bandwidth	Maximum
Default	100%	100%

Done 172.16.30.80:10000

3. Enter the bandwidth size of the link between the local WANJet and this remote WANJet in the **Link Bandwidth** field, and then select the units, either Kb/s or Mb/s, from the drop-down list.
4. Click the **Add** button next to the Application QoS Policy section. The Application QoS Policy page opens in a browser pop-up:

Alias:

Bandwidth: % Maximum: %

Services:

VoIP	<input type="text" value="UDP"/>
Ftp	<input type="text" value="TCP"/>
Asp	<input type="text" value="TCP"/>
Nfs	<input type="text" value="UDP"/>

Done 172.16.30.80:10000

5. Enter a name for this policy in the **Alias** field.

6. Enter the minimum amount of bandwidth that this policy should use in the **Bandwidth** field.
7. Enter the maximum amount of bandwidth that this policy can use in the **Maximum** field. The maximum amount of bandwidth is used only when there is plenty of link bandwidth to go round.
8. Select the ports or IT service policies to use for this policy from the **Services** drop-down lists, and specify the type of each protocol as either TCP or UDP.

A port can have both protocols (TCP and UDP). First select the port, for example **FTP**, and select **TCP**. Then on a new line, select **FTP** again, and **UDP**. If you select **VoIP**, it only uses the UDP protocol.

If you select an IT service policy from the drop-down list, the adjacent service type list disappears.
9. Click **OK** to return to the Manage the Application QoS Settings of a Remote WANJet page.
10. Click **OK** again to return to the Application QoS page.
11. Click **Save**. The Application QoS page refreshes and your changes are saved.

Editing and deleting application QoS policies

To edit or delete an application QoS policy from a remote WANJet:

1. Go to the Application QoS page shown on page 103.
2. Click on the IP address of the remote WANJet.
3. On the Manage the Application QoS Settings of a Remote WANJet page, click on the link for the application QoS policy that you wish to edit or delete.
4. On the Application QoS Policy page you can edit the settings as described in [Adding an Application QoS Policy to a Remote WANJet](#) on page 103, or click **Remove** to delete the policy.
5. Click **OK** on both the Application QoS Policy page and the Manage the Application QoS Settings of a Remote WANJet page.
6. On the main Application QoS page, remember to click **Save** or your changes will be lost.

Managing WAN Links

The WAN Links feature enables you to add an application QoS policy to the traffic passing through the local WANJet and going to a remote network, whether or not the remote network has WANJet installed. In this way, the WANJet enables you to manage and manipulate the bandwidth size for all the traffic transferred through your local WANJet, regardless of the processing mode of this traffic.

Adding a WAN Link

To add a new WAN link to WANJet:

1. Expand the **Operational Settings** section of the menu bar, and click on **Application QoS**.
2. On the Application QoS page, click on the **Add WAN Link** button. The Manage the Application QoS Settings of a WAN Link page is displayed in a browser pop-up:

https://172.16.30.80:10000 - Manage the Application QoS Settings of a WAN Link - Mozilla Fir...

WAN Link Alias:

Link Bandwidth:

Supported Subnet	Netmask	Alias

Add

Application QoS Policy	Bandwidth	Maximum
Default	100%	100%

Add

OK Cancel

Done 172.16.30.80:10000

Note You can add a link to a network that does not have WANJet installed. In that case, the application QoS policy is applied to the traffic sent to it from your local WANJet.

3. Enter the name you choose for the new WAN link in the **WAN Link Alias** field.
4. Enter the bandwidth size of the link between the local WANJet, and the WAN network in the **Link Bandwidth** field, and then select the units from the adjacent drop-down list.
5. Click **OK** to return to the Application QoS page, where the new WAN link is now displayed.
6. Click **Save**. The Application QoS page refreshes, and your changes are saved.

Editing and deleting WAN links

To edit or delete a WAN link:

1. Click on **Operational Settings > Application QoS** in the menu bar
2. Click on the link (in the Alias column) corresponding to the WAN link that you wish to edit or delete. The **Manage the Application QoS Settings of a WAN Link** page is displayed in a browser pop-up.

This is identical to the page shown on page 106, except that a **Remove** button is also present. On this screen, you can also add a new application QoS policy, which works just like adding a policy for a remote WANJet (as described on page 103).

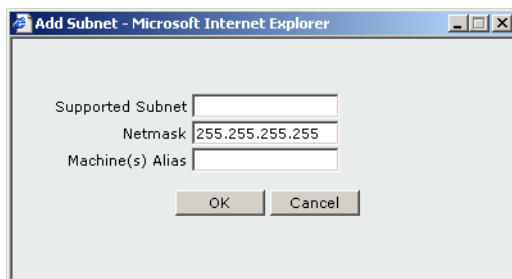
3. Click **Remove** to delete the link, or edit the settings and click **OK** to save your changes.
4. You must click **Save** on the main **Application QoS** page for the new WAN link to be permanently added to the system.

Adding a Subnet to a WAN Link

You can add subnets or machines to any of the WAN links you previously added. This way, you can make use of the application QoS policies with more nodes (computers, subnets, networks).

To add a subnet to a WAN link:

1. Click on **Operational Settings > Application QoS** in the menu bar.
2. In the **Application QoS** page (see page 103), click on the link in the **Alias** column corresponding to the appropriate WAN link. (You can also add a subnet as part of the process of adding the WAN link.)
3. In the **Manage the Application QoS Settings of a WAN Link** page (see page 106), click on the first **Add** button (next to the **Alias** column). The **Add Subnet** page opens in a browser pop-up:



The screenshot shows a browser window titled "Add Subnet - Microsoft Internet Explorer". Inside the window is a form with the following fields:

- Supported Subnet**: An empty text input field.
- Netmask**: A text input field containing the value "255.255.255.255".
- Machine(s) Alias**: An empty text input field.

At the bottom of the form are two buttons: **OK** and **Cancel**.

4. Enter the IP address of the machine or subnet you want to add in the **Supported Subnet** field.

5. Enter the netmask of the machine or subnet in the **Netmask** field.
6. Enter the name you choose for the machine or subnet in the **Machine(s) Alias** field.
7. Click **OK** to return to the Manage the Application QoS Settings of a WAN Link page, where the subnet now appears to the Supported Subnet column.
8. Click **OK** to return to the Application QoS page.
9. Click **Save**. The Application QoS page refreshes and your changes are saved to WANJet.

Editing and deleting subnets

To edit or delete a subnet from a WAN link:

1. Click on **Operational Settings > Application QoS** in the menu bar.
2. On the Application QoS page (see page 103), click on the link in the Alias column corresponding to the appropriate WAN link.
3. On the Manage the Application QoS Settings of a WAN Link page (see page 106), click on the link in the Supported Subnet column corresponding to the subnet that you want to edit or delete.

The Edit Subnet page appears in a browser pop-up. This is identical to the Add Subnet page shown in the previous subsection, except that a **Remove** button is also present.

4. Click **Remove** to delete the subnet, or edit the settings and click **OK** to save your changes.
5. Click **OK** on the Manage the Application QoS Settings of a WAN Link page.
6. On the main Application QoS page, remember to click **Save** to store the changes in WANJet.

Configuration Examples

[Basic Configuration](#) ◀

[Mesh Configuration](#) ◀

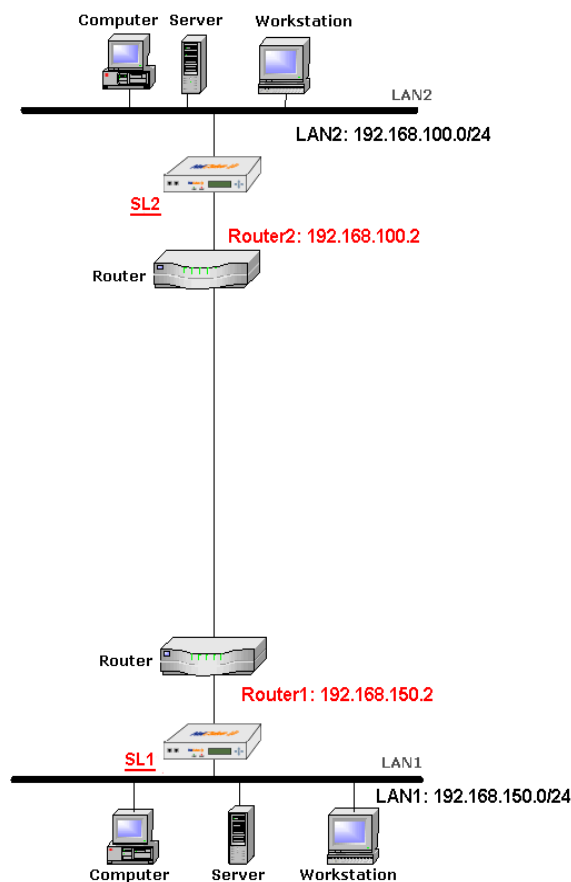
[Hub and Spoke Configuration](#) ◀

[Redundant Configuration](#) ◀

[LAN Router Configuration](#) ◀

The configuration examples aim at taking you step by step through some common WANJet configuration scenarios, in order to give you a clear idea about the configuration details, and provide you with a comprehensive picture for the relation between different configuration options.

Basic Configuration



Configuration Example: Basic Configuration

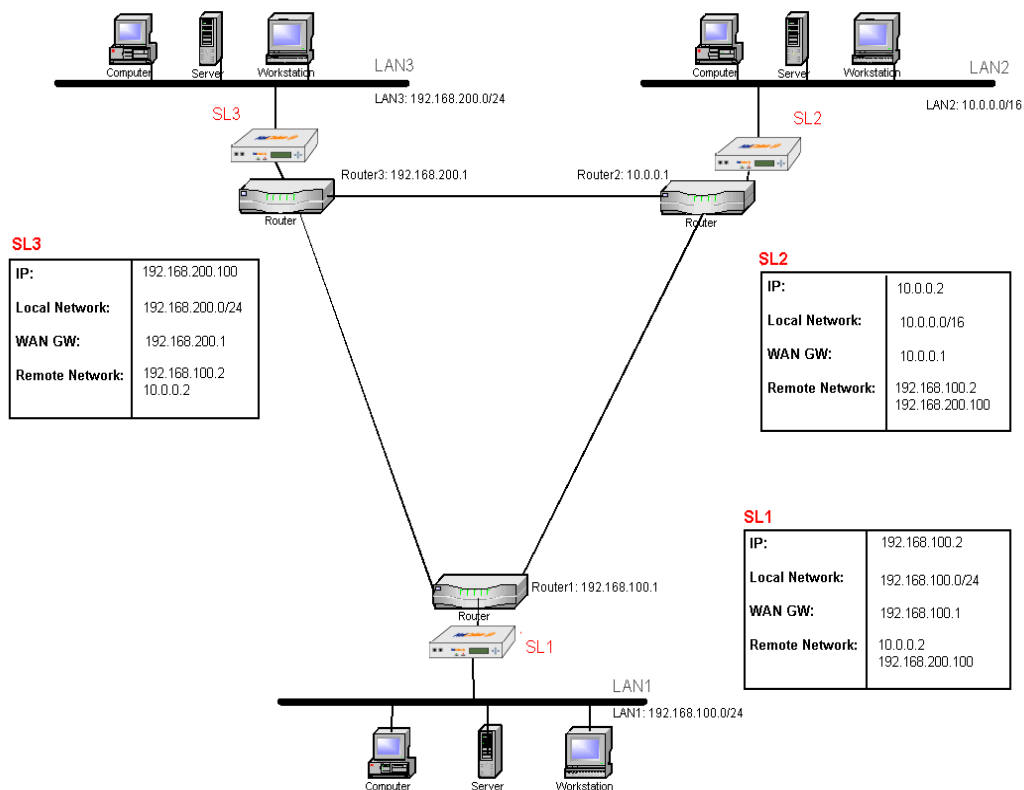
]

	SL1	SL2
IP Address	192.168.150.100	192.168.100.100
Local Network	192.168.150.0/24	192.168.100.0/24
Gateway	192.168.150.2	192.168.100.2
Remote Network	192.168.100.2	192.168.150.2

Configuration Notes:

- This diagram represents a basic configuration, where two LANs are connected, and two F5 appliances are installed. LAN1 has SL1 installed, and LAN2 has SL2 installed.
- LAN2 is a remote network of LAN1, and LAN1 is the remote network of LAN2.
- SL1 sends processed data to SL2 to handle, while SL2 sends processed data to SL1 to handle.

Mesh Configuration



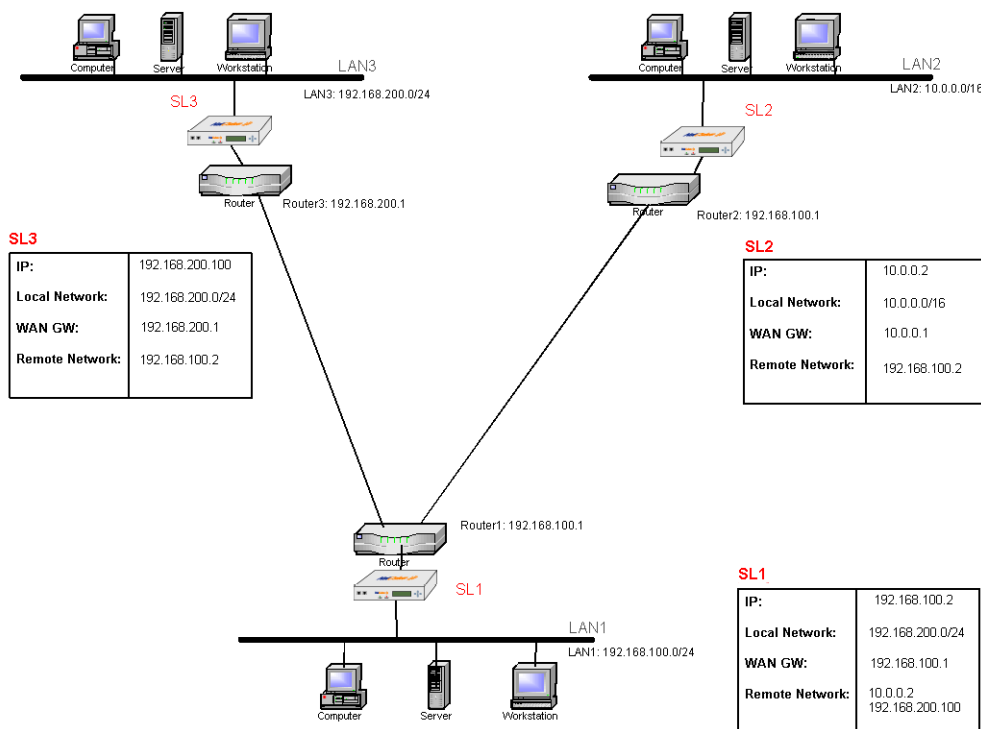
Configuration Example: Mesh

	SL1	SL2	SL3
IP Address	192.168.100.2	10.0.0.2	192.168.200.100
Local Network	192.168.100.0/24	10.0.0.0/16	192.168.200.0/24
Gateway	192.168.100.1	10.0.0.1	192.168.200.1
Remote Network	10.0.0.2	192.168.200.100	192.168.100.2
	192.168.200.100	192.168.100.2	10.0.0.2

Configuration Notes:

- This diagram represents a Mesh configuration, where three LANs are connected, and three F5 appliances are installed. LAN1 has SL1 installed, LAN2 has SL2 installed, and LAN3 has SL3 installed.
- LAN2 and LAN3 are the remote WANJets of LAN1, LAN1, and LAN3 are the remote WANJets of LAN2, and LAN1, and LAN2 are the remote WANJets of LAN3.
- SL1 sends processed data to SL2 and SL3 to handle, SL2 sends processed data to SL1 and SL3 to handle, and SL3 sends processed data to SL1 and SL2 to handle.

Hub and Spoke Configuration



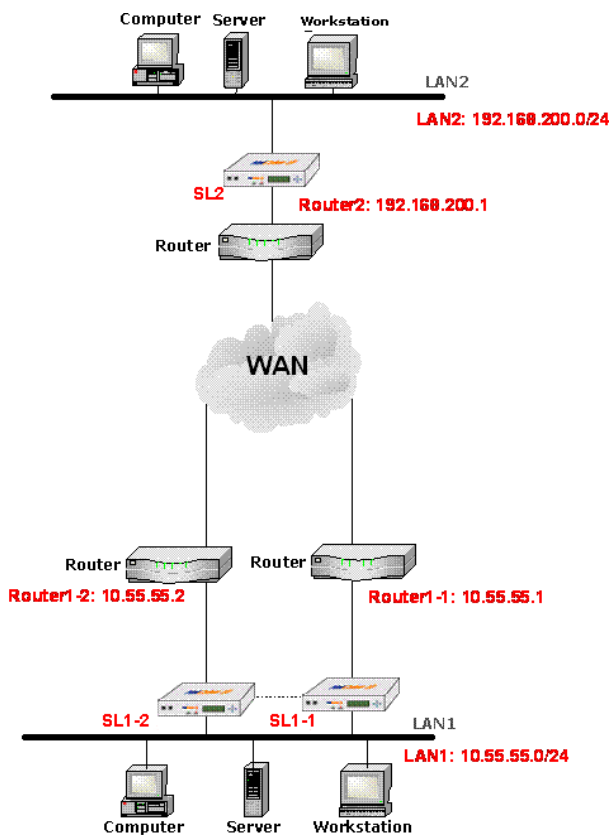
Configuration Example: Hub-and-Spoke

	SL1	SL2	SL3
IP Address	192.168.100.2	10.0.0.2	192.168.200.100
Local Network	192.168.100.0/24	10.0.0.0/16	192.168.200.0/24
Gateway	192.168.100.1	10.0.0.1	192.168.200.1
Remote Network	10.0.0.2 192.168.100.2	192.168.200.100	192.168.100.2

Configuration Notes:

- This diagram represents a HUB-and Spoke configuration, where three LANs are connected, and three F5 appliances are installed. One LAN is connected to the other two LANs, and the other two LANs are connected to this LAN only and not to each other.
- LAN1 has SL1 installed, LAN2 has SL2 installed, and LAN3 has SL3 installed.
- SL1 sends processed data to both SL2 and SL3 to handle, SL2 sends processed data to SL1 only to handle, and SL3 sends processed data to SL1 only to handle.

Redundant Configuration

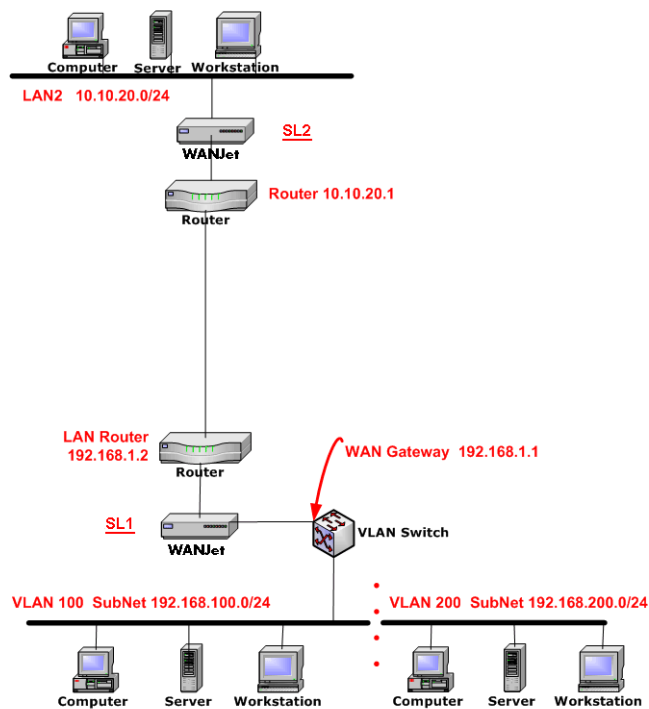


	SL1-1	SL1-2	SL2
IP Address	10.55.55.3	10.55.55.4	192.168.200.100
Local Network	10.55.55.0/24	10.55.55.0/24	192.168.200.0/24
Gateway	10.55.55.1	10.55.55.2	192.168.200.1
Remote Network	192.168.200.100	192.168.200.100	10.55.55.3
Subnet			10.55.55.0/24
Remote Network			10.55.55.4
Subnet			10.55.55.100/32
			10.55.55.110/32

Configuration Notes:

- This diagram represents a redundant configuration example, where two LANs are connected, and one of the LANs has a redundant WANJet installed.
- LAN1 has two WANJet appliances installed, SL1-1 and SL1-2, and LAN2 has SL2 installed. SL1-2 is the redundant peer of SL1-1, in case of failure of any of the routers the other router and its corresponding WANJet resumes to function.
- SL1-1 processes the data of half the subnets of LAN1 (Subnet A), while SL1-2 processes the data of the other half of the subnets of LAN1 (Subnet B).
- SL1-1 sends processed data to SL2 to handle, and SL1-2 sends processed data to SL2 to handle.
- SL2 processes, and sends the data that should be routed to Subnet A to SL1-1 to handle. SL2 processes and sends the data that should be routed to Subnet B to SL1-2 to handle.

LAN Router Configuration



Configuration Example: WAN Gateway and LAN Router

	SL1	SL2
IP Address	192.168.1.100	10.10.20.100
Local Network	192.168.1.0/24	10.10.20.0/24
Subnets	VLAN 100: 192.168.100.0/24 VLAN 200: 192.168.200.0/24	
WAN Gateway	192.168.1.1	10.10.20.1
LAN Router	192.168.1.2	N/A

Configuration Notes:

- This diagram represents a LAN Router configuration example where a VLAN switch connects two or more virtual networks to WANJet, and WANJet is connected to the outside WAN through another router.
- LAN1 has SL1 installed, LAN2 has SL2 installed.
- LAN1 is divided into two virtual networks VLAN100, and VLAN 200. A VLAN switch is acting as the router between the two LANs and between both of them and SL1. WANJet considers this VLAN switch as its gateway because it connects WANJet (SL1) to its local network (LAN1).
- WANJet sees the local network through the VLAN switch. So, in order for WANJet to see, and process the data of the virtual LANs, you have to add these LANs as subnets to LAN1.
- LAN1 and SL1 is connected to the outside WAN through another router (that is, the LAN Router).

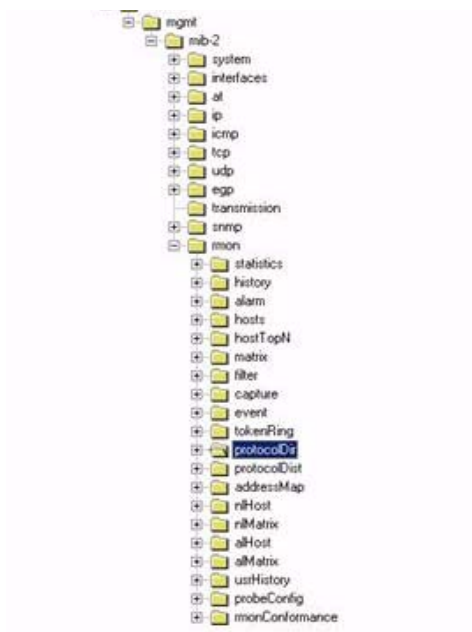
Appendix A

RMON2 Tree

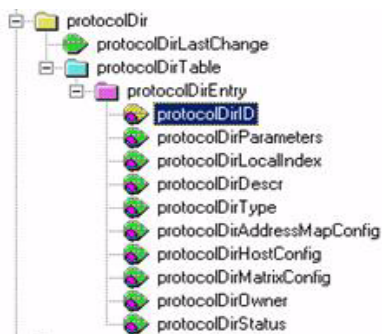
- [MIB Tree ◀](#)
- [Protocol Directory Tree ◀](#)
- [Network Layer Matrix ◀](#)
- [Application Data Matrix ◀](#)
- [Configuration Group ◀](#)

This appendix contains diagrams showing MIB tree with the standard RMON MIB and all the groups for both RMON1 and RMON2.

MIB Tree



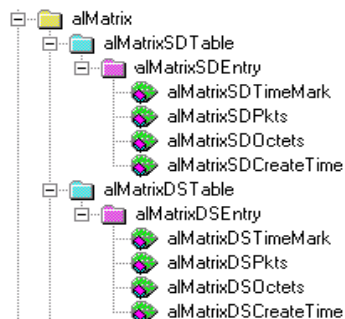
Protocol Directory Tree



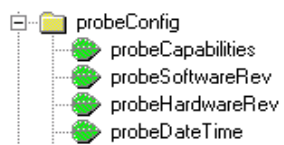
Network Layer Matrix



Application Data Matrix



Configuration Group



Appendix B

WANJet Errors

[WANJet Error Messages and Codes](#) ◀

This appendix includes the list of errors that a WANJet may send to its associated SNMP server and/or Syslog server. In addition, you can view this list of errors through the **Diagnostic Log** option in the Web UI.

WANJet Error Messages and Codes

Error Code	Error Message	WANJet Component
1000 to 1002	Configuration errors	Optimization Engine
1003 to 1005	Initialization error	
1006 to 1007	Internal errors	
1100 to 1103	Internal error	Packet Processor
1150	Maximum number of ACM5 connections reached	
1200 to 1201	Configuration errors	ACM5
1202 to 1203	Initialization error	
1204 to 1207	Internal errors	
1209	Link down with (Proxy IP)	
1210	Link up with (Proxy IP)	
1211	Authentication failed with (Proxy IP)	
1212	Error: Connection from unauthorized proxy (Proxy IP).	
1213	Internal error	
1214	Error: This version (%f) is incompatible with (Proxy IP) version (%f).	
1215	Error: License expired on 01/01/2004.	
1250	Version (%f) up and running	
1251	Internal error	
1252	Warning: License Limit Exceeded	
1253	Warning: Invalid license key - Bandwidth optimization off.	
1254	Warning: License key not entered - Bandwidth optimization off	
1255	Warning: x day(s) remain(s) for the evaluation license key to expire.	
1256	Warning: WANJet is activated for evaluation for x days	

Error Code	Error Message	WANJet Component
1257	Warning: Evaluation license key expired.	ACM5
1258	License violation - Bandwidth optimization stopped.	
1259	Cannot complete the remote upgrade. Not enough free space.	
1300	Logging error	Logs
1420	WCCP ServiceGroup (TCP) is up.	WCCP
1421	WCCP ServiceGroup (UDP) is up	
1422	WCCP ServiceGroup (TCP) is down	
1423	WCCP ServiceGroup (UDP) is down	
1424	WCCP Configuration Error	
1425	WCCP Runtime Error	
1426	WCCP is not enabled on the router	

Appendix C

WANJet Private MIB

[System Information](#) ◀
[Ethernet Cards Information](#) ◀
[MIB File](#) ◀

This appendix contains the WANJet Private MIB file in case you need it. All you have to do is to copy this file to your SNMP-compliant software, and compile it. Refer to the documentation of your SNMP-compliant software for instructions.

System Information

The system-related information path:

`.iso.org.dod.internet.private.enterprises.13993. = .1.3.6.1.4.1.13993.`

The system-related information description:

TotalSentBandwidthSavingPercent
 TotalRecvBandwidthSavingPercent
 TotalSentBeforeNetCelera
 TotalSentAfterNetCelera
 TotalRecvBeforeNetCelera
 TotalRecvAfterNetCelera
 LastSentBandwidthSavingPercent
 LastRecvBandwidthSavingPercent
 LastSentBeforeNetCeleraRate
 LastSentAfterNetCeleraRate
 LastRecvBeforeNetCeleraRate
 LastRecvAfterNetCeleraRate

Ethernet Cards Information

The Ethernet cards related information path:

`.iso.org.dod.internet.mgmt.mib-2.interfaces = .1.3.6.1.2.1.2`

The Ethernet cards related information description:

IfNumber
 ifTable.ifEntry.ifIndex
 ifTable.ifEntry.ifDescr
 ifTable.ifEntry.ifEnter
 ifTable.ifEntry.ifMtu
 ifTable.ifEntry.ifSpeed
 ifTable.ifEntry.ifPhysAddress
 ifTable.ifEntry.ifInOctets
 ifTable.ifEntry.ifInUcastPkts
 ifTable.ifEntry.ifInDiscards
 ifTable.ifEntry.ifInErrors
 ifTable.ifEntry.ifOutOctets
 ifTable.ifEntry.ifOutUcastPkts
 ifTable.ifEntry.ifOutDiscards
 ifTable.ifEntry.ifOutErrors

MIB File

This is the MIB file that might be needed to compile the MIB file for browsing the MIB through a standard MIB browser:

```
SWANLABS-GLOBAL-REG DEFINITIONS ::= BEGIN

    IMPORTS
        enterprises          FROM SNMPv2-SMI;

    SwanLabs          OBJECT IDENTIFIER
        ::= { enterprises 13993 }

    NetCelera          OBJECT IDENTIFIER
        ::= { SwanLabs 1 }

    ncVersion          OBJECT-TYPE
        SYNTAX  OCTET STRING
        ACCESS  read-only
        STATUS  current
        DESCRIPTION
            "The NetCelera software version"
        ::= { NetCelera 1 }

    ncStatistics        OBJECT IDENTIFIER
        ::= { NetCelera 2 }

    ncSnmpTraps          OBJECT IDENTIFIER
        ::= { NetCelera 3 }

-- ***** ncStatistics

    TotalSentBandwidthSavingPercent OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-only
        STATUS  current
        DESCRIPTION
            "Percent bandwidth saving on the traffic sent
             to other NetCelera boxes today."
        ::= { ncStatistics 1 }

    TotalRecvBandwidthSavingPercent OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-only
        STATUS  current
        DESCRIPTION
            "Percent bandwidth saving on the traffic
             received from other NetCelera boxes today."
        ::= { ncStatistics 2 }

    TotalSentBeforeNetCelera          OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-only
        STATUS  current
        DESCRIPTION
            "Effective traffic sent
             from this NetCelera Box to other NetCelera boxes
             today in MB (before NetCelera)."
        ::= { ncStatistics 3 }

    TotalSentAfterNetCelera          OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-only
        STATUS  current
```

```

DESCRIPTION      "Optimized traffic sent
                  from this NetCelera Box to other NetCelera boxes
                  today in MB (after NetCelera)."
```

::= { ncStatistics 4 }

```

TotalRecvBeforeNetCelera      OBJECT-TYPE
SYNTAX  INTEGER
ACCESS  read-only
STATUS  current
DESCRIPTION      "Effective traffic received
                  from other NetCelera boxes
                  today in MB (before NetCelera)."
```

::= { ncStatistics 5 }

```

TotalRecvAfterNetCelera      OBJECT-TYPE
SYNTAX  INTEGER
ACCESS  read-only
STATUS  current
DESCRIPTION      "Optimized traffic received
                  from other NetCelera boxes
                  today in MB (after NetCelera)."
```

::= { ncStatistics 6 }

```

LastSentBandwidthSavingPercent  OBJECT-TYPE
SYNTAX  INTEGER
ACCESS  read-only
STATUS  current
DESCRIPTION      "Percent bandwidth saving on the traffic sent
                  to other NetCelera boxes during the last five minutes.
                  This value may be plotted to create a chart."
```

::= { ncStatistics 7 }

```

LastRecvBandwidthSavingPercent  OBJECT-TYPE
SYNTAX  INTEGER
ACCESS  read-only
STATUS  current
DESCRIPTION      "Percent bandwidth saving on the traffic received
                  from other NetCelera boxes during the last five minutes.
                  This value may be plotted to create a chart."
```

::= { ncStatistics 8 }

```

LastSentBeforeNetCeleraRate      OBJECT-TYPE
SYNTAX  INTEGER
ACCESS  read-only
STATUS  current
DESCRIPTION      "The rate of effective traffic sent
                  from this NetCelera Box to other NetCelera boxes in Kbps
                  (before NetCelera).
                  This value may be plotted to create a chart."
```

::= { ncStatistics 9 }

```

LastSentAfterNetCeleraRate      OBJECT-TYPE
SYNTAX  INTEGER
ACCESS  read-only
STATUS  current
DESCRIPTION      "The rate of real Optimized traffic sent
                  from this NetCelera Box to other NetCelera boxes in Kbps
                  (after NetCelera).
                  This value may be plotted to create a chart."
```

::= { ncStatistics 10 }

```

LastRecvBeforeNetCeleraRate    OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  current
    DESCRIPTION  "The rate of effective traffic received
                  from other NetCelera boxes in Kbps
                  (before NetCelera).
                  This value may be plotted to create a chart."
    ::= { ncStatistics 11 }

LastRecvAfterNetCeleraRate    OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  current
    DESCRIPTION  "The rate of real Optimized traffic received
                  from other NetCelera boxes in Kbps
                  (after NetCelera).
                  This value may be plotted to create a chart."
    ::= { ncStatistics 12 }

-- ***** ncSnmpTraps

ncSnmpTrapObjs OBJECT IDENTIFIER
    ::= { ncSnmpTraps 1 }

ncSnmpTrapID    OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  current
    DESCRIPTION  "Holds the ID of the SNMP Trap."
    ::= { ncSnmpTrapObjs 1 }

ncSnmpTrapDescription OBJECT-TYPE
    SYNTAX  OCTET STRING
    ACCESS  read-only
    STATUS  current
    DESCRIPTION  "Holds the description of the SNMP Trap."
    ::= { ncSnmpTrapObjs 2 }

ncSnmpTrapList OBJECT IDENTIFIER
    ::= { ncSnmpTraps 2 }

-- Optimization Engine Traps

ncTrap1000    OBJECT-TYPE
    SYNTAX  OCTET STRING
    ACCESS  read-only
    STATUS  current
    DESCRIPTION  "Error: Configuration error."
    ::= { ncSnmpTrapList 1000 }

ncTrap1001    OBJECT-TYPE
    SYNTAX  OCTET STRING
    ACCESS  read-only
    STATUS  current
    DESCRIPTION  "Error: Configuration error."
    ::= { ncSnmpTrapList 1001 }

```

```

ncTrap1002      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: Configuration error."
    ::= { ncSnmpTrapList 1002 }

ncTrap1003      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: Initialization error."
    ::= { ncSnmpTrapList 1003 }

ncTrap1004      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: Initialization error."
    ::= { ncSnmpTrapList 1004 }

ncTrap1005      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: Initialization error."
    ::= { ncSnmpTrapList 1005 }

ncTrap1006      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: Internal error."
    ::= { ncSnmpTrapList 1006 }

ncTrap1007      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: Internal error."
    ::= { ncSnmpTrapList 1007 }

-- Packet Processor Traps

ncTrap1100      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: Internal error."
    ::= { ncSnmpTrapList 1100 }

ncTrap1101      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: Internal error."
    ::= { ncSnmpTrapList 1101 }

```

```

ncTrap1102      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: Internal error."
    ::= { ncSnmptTrapList 1102 }

ncTrap1103      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: Internal error."
    ::= { ncSnmptTrapList 1103 }

ncTrap1150      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Maximum number of ACM5 connections reached.
                  (OR)
                  Maximum number of speed array connections for (RemoteIP) reached."
    ::= { ncSnmptTrapList 1150 }

-- ACM5 Traps

ncTrap1200      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: Configuration error."
    ::= { ncSnmptTrapList 1200 }

ncTrap1201      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: Configuration error."
    ::= { ncSnmptTrapList 1201 }

ncTrap1202      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: Initialization error."
    ::= { ncSnmptTrapList 1202 }

ncTrap1203      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: Initialization error."
    ::= { ncSnmptTrapList 1203 }

ncTrap1204      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: Internal error."
    ::= { ncSnmptTrapList 1204 }

```

```

ncTrap1205      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: Internal error."
    ::= { ncSnmpTrapList 1205 }

ncTrap1206      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: Internal error."
    ::= { ncSnmpTrapList 1206 }

ncTrap1207      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: Internal error."
    ::= { ncSnmpTrapList 1207 }

ncTrap1209      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Link down with (Proxy IP)."
    ::= { ncSnmpTrapList 1209 }

ncTrap1210      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Link up with (Proxy IP)."
    ::= { ncSnmpTrapList 1210 }

ncTrap1211      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Authentication failed with (Proxy IP)."
    ::= { ncSnmpTrapList 1211 }

ncTrap1212      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: Connection from unauthorized Proxy (Proxy IP)."
    ::= { ncSnmpTrapList 1212 }

ncTrap1213      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: Internal error."
    ::= { ncSnmpTrapList 1213 }

ncTrap1214      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: This version (%f) is incompatible with (Proxy IP) version
(%f)."
    ::= { ncSnmpTrapList 1214 }

```



```

ncTrap1250      OBJECT-TYPE
                SYNTAX  OCTET STRING
                ACCESS   read-only
                STATUS   current
                DESCRIPTION "Version (%f) up and running."
                ::= { ncSnmpTrapList 1250 }

ncTrap1251      OBJECT-TYPE
                SYNTAX  OCTET STRING
                ACCESS   read-only
                STATUS   current
                DESCRIPTION "Error: Internal error."
                ::= { ncSnmpTrapList 1251 }

ncTrap1252      OBJECT-TYPE
                SYNTAX  OCTET STRING
                ACCESS   read-only
                STATUS   current
                DESCRIPTION "Warning: License limit exceeded."
                ::= { ncSnmpTrapList 1252 }

ncTrap1253      OBJECT-TYPE
                SYNTAX  OCTET STRING
                ACCESS   read-only
                STATUS   current
                DESCRIPTION "Warning: Invalid license key - Bandwidth optimization off."
                ::= { ncSnmpTrapList 1253 }

ncTrap1254      OBJECT-TYPE
                SYNTAX  OCTET STRING
                ACCESS   read-only
                STATUS   current
                DESCRIPTION "Warning: License key not entered - Bandwidth optimization off."
                ::= { ncSnmpTrapList 1254 }

ncTrap1255      OBJECT-TYPE
                SYNTAX  OCTET STRING
                ACCESS   read-only
                STATUS   current
                DESCRIPTION "Warning: x days remain for the evaluation license key to expire."
                ::= { ncSnmpTrapList 1255 }

ncTrap1256      OBJECT-TYPE
                SYNTAX  OCTET STRING
                ACCESS   read-only
                STATUS   current
                DESCRIPTION "Warning: NetCelera is activated for evaluation for x days."
                ::= { ncSnmpTrapList 1256 }

ncTrap1257      OBJECT-TYPE
                SYNTAX  OCTET STRING
                ACCESS   read-only
                STATUS   current
                DESCRIPTION "Warning: Evaluation license key expired."
                ::= { ncSnmpTrapList 1257 }

ncTrap1258      OBJECT-TYPE
                SYNTAX  OCTET STRING
                ACCESS   read-only
                STATUS   current
                DESCRIPTION "Error: License violation - Bandwidth optimization stopped."
                ::= { ncSnmpTrapList 1258 }

```

```
-- Logging Traps

ncTrap1300      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Error: Logging Error."
    ::= { ncSnmpTrapList 1300 }

-- Speed Array Traps

ncTrap1400      OBJECT-TYPE
    SYNTAX      OCTET STRING
    ACCESS      read-only
    STATUS      current
    DESCRIPTION  "Maximum number of remote NetCelera machines reached.
                  Disabling Speed Array service for (Proxy IP)."
```

END

Index

A

access

- allowing access by IP address 95
- granting access to SNMP reports 95
- log into Web UI 18
- setting password, PIN 66

ACM5

- assigning to traffic 78
- description 2

adding

- application QoS policy 103
- IT service policy 102
- remote WANJet 91
- subnet 107
- subnet to local 76, 88
- subnet to remote 78
- VLAN to local 88
- WAN link 106

address

- local WANJet and subnet 86
- network cards 52
- Web UI 18

all other TCP ports 81

application data matrix 121

application QoS

- applying without remote WANJet 106
- description 4
- specifying bandwidth 104

application QoS policy

- adding 103
- defining 103
- deleting 105
- editing 105
- reports 55

assigning

priorities to data traffic 5

traffic processing modes to port 79

autorecovery 73

B

backing up

- uploading backup file 73
- WANJet settings 72

bandwidth

- setting in QoS policy 104
- setting WAN size 85

buffer size, application 85

C

charts, see also reports 32

cluster 102

compression

- specify mode 80

compression technology 2

configuration

- testing 26

configuration group 122

configuration tool 18

congestion control 85

contact information v

conventions used v

Customer Confidence team v

customize reports 38

D

defining resources 102

deleting

- application QoS policy 105
 - IT service policy 102
 - subnet 77, 108
 - WAN link 107
- deploying WANJet 12
- deployment
 - in-line 12
 - one-arm 13
 - point-to-multi-point 12
 - point-to-point 12
 - specify type 82
- diagnosing problems 27
 - error codes 124
 - reports 40
- directing packets through a gateway 94
- dropped packets 55
- duplex mode 94

E

- editing
 - application QoS policy 105
 - IT service policy 102
 - subnet 108
 - subnet specification 77
 - WAN link 107
- error messages and codes 124
- ethernet cards
 - setting speed 94
 - SNMP information 128
- event messages 8

F

- F5 contact information v
- features 2
- figures
 - basic configuration 110
 - hub and spoke configuration 113
 - LAN router configuration 116
 - mesh configuration 111
 - point-to-multi-point deployment 13
 - point-to-point deployment 12
 - redundant peer 93
 - redundant peer details 114

- RMON2 data collection 7
 - SNMP data collection 6
 - Web UI home page 19
- firewall ports 14
- font conventions used v

G

- gateway, specifying a static route 94
- graphs, see also reports 32
- guaranteed performance 4

H

- hub and spoke 113

I

- in-line deployment 12
- IP address
 - access to Web UI data 95
 - SNMP server 96
 - syslog server 96
- IT Service
 - adding policy 102
 - deleting policies 102
 - described 102
 - editing policies 102

L

- LAN
 - speed used 94
- LAN router
 - example 116
 - remote WANJet settings 91
 - specify IP address 87
 - topology setting 83
- legacy IP precedence 80
- license
 - upgrading 74
 - verify 25
- local WANJet
 - adding redundant peer 87
 - setting network information 86

- logging in 18
- logs, diagnostic 40
 - downloading 47

M

- matrix
 - application data 121
 - network layer 121
- mesh configuration 111
- MIB file 129
- MIB tree 120
- modes, processing 78
- monitoring traffic 32
- MTU, specifying 91

N

- navigating in user interface 19
- network card
 - speed 94
- network layer matrix 121
- NIC configuration 94

O

- one-arm deployment 13

P

- packet retransmissions 57
- packets
 - by policy 55
 - by VLAN 55
 - retransmitted 56
- passthrough 78
- password
 - for router 84
 - setting 66
- path
 - MIB tree 120
 - SNMP ethernet cards 128
 - SNMP system information 128
- performance, guaranteed level 4
- PIN code, setting 67

- ping, no response 27
- point-to-multi-point deployment 12
- point-to-point deployment 12
- ports
 - configuring to remote 78
 - identifying specific or range 79
 - open in firewall 14
- power off 71
- priority for data traffic 5
- priority levels 80
- probeConfig 122
- problems
 - browser times out 27
 - cannot ping 27
 - cannot ping WAN gateway 27
 - diagnosing 27
 - diagnostic reports 40
 - error codes 124
 - link LED not lighting 28
 - login timeout 28
 - page not found 27
 - passthrough mode 73
 - traffic not optimized 27
- processing modes 78
- protocol directory tree 120
- proxy, transparent 13

Q

- queue size 85

R

- Real Time Traffic report 30
- recovery 72
 - automated 73
- redundant peer
 - described 93
 - example 114
- remote monitoring support 6
- remote WANJet
 - adding or changing subnet 78
 - application QoS 103
 - application QoS with none 106
 - managing from local 90

- specifying to local 91
- removing
 - subnet 77
- reports
 - bandwidth freed 34
 - bandwidth used 37
 - by traffic type 32
 - customizing 38
 - overall data 36
 - percentage bandwidth freed 33
 - percentage improved 33
 - QoS data 55
 - RMON2 63
 - select time period 32
 - SNMP 62
 - syslog 62
 - system information 52
 - traffic reduction 35
 - VLAN data 55
- restart, autorecovery 73
- restarting 71
- restoring settings 72
- retransmitted packets 56, 57
- RMON2
 - access to reports 95
 - application data matrix 121
 - configuration group 122
 - description of support 6
 - MIB tree 120
 - network layer matrix 121
 - protocol directory tree 120
 - viewing reports 63
- round trip time 85

S

- security
 - PIN code 67
 - router password 84
 - Web UI password 66
- servers
 - SNMP 96
 - syslog 8
- service policies
 - IT 102

- QoS 4
- setting time 69
- shutting down 71
- size
 - application buffer 85
 - queue 85
- snapshots of system 40
- SNMP
 - access to reports 95
 - description of support 5
 - ethernet cards information 128
 - MIB file 129
 - RMON2 6
 - specifying server 96
 - system information 128
 - viewing reports 62
- static routes, specifying 94
- subnet of WAN link
 - deleting 108
 - editing 108
- subnets
 - adding to WAN link 107
 - changing 77
 - defining to local 88
 - defining to WANJet 76
 - specifying to remote 78
- support
 - contacting F5 v
 - downloading diagnostic logs 47
- synchronizing time 70
- syslog
 - description 8
 - IP address of server 96
 - reports 62
 - viewing reports 62
- system information report 52
- system snapshot 47
- system snapshots 40

T

- TDR 82
- time
 - setting 69
 - setting manually 70

- time period for reports 32
- time server, to synchronize 70
- time zone 69
- topology 12
 - LAN or WAN 83
 - set option 82
- ToS
 - described 5
 - specifying 80
- traffic
 - do not process 78
 - setting priority 5
- traffic optimized report 35
- transparent proxy 13
- trees
 - MIB 120
 - protocol directory 120
- tuning 85
- Type of Service, see also ToS 5

U

- upgrading software 74
- uploading a backup 73
- URL for login 18
- user interface, accessing 18

V

- verify initial configuration 26
- version, upgrading 74
- VLAN
 - defining to local 88
 - report data 55
- VLAN ID 89

W

- WAN
 - set bandwidth size 85
 - speed used 94
- WAN link
 - adding 106
 - deleting 107
 - editing 107

- purpose 106
- WAN Optimizer
 - errors 124
 - overview 2
- WANJet
 - adding remote to local 91
 - backing up 72
 - basic configuration diagram 110
 - hub and spoke diagram 113
 - LAN router 91
 - LAN router diagram 116
 - mesh configuration diagram 111
 - network information for local 86
 - PIN 67
 - process subnet traffic 76
 - redundant diagram 114
 - replicating local information to remote 86
 - restart 71
 - restoring settings 73
 - shutdown 71
 - user interface 18
- WCCP v2 protocol 14
- Web UI
 - granting access 95
 - local or remote 19
 - logging in 18
 - page not found 27
 - setting password 66
 - using menu 19
- worksheet, configuration data 15

