WANJet™ User Guide

version 4.0

MAN-0221-00

Product Version

This manual applies to product version 4.0 of the WANJet™ appliance.

Publication Date

This manual was published on May 4, 2006.

Legal Notices

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Acknowledgments

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by Bob Withers.

This product includes software developed by Jean-Loup Gaily and Mark Adler.

This product includes software developed by Markus FXJ Oberhumer.

This product includes software developed by Gullaume Fihon.

Table of Contents

1
Introducing the WANJet Appliance

Introducing the WANJet appliance 1-1
About this guide 1-1
Additional information 1-2
Stylistic conventions in this guide 1-2
Using the solution examples 1-2
Identifying new terms 1-2
Identifying references to objects, names, and commands 1-2
Identifying references to other documents 1-3
Identifying command syntax 1-3
Finding help and technical support resources 1-4

2
Overview

About the WANJet appliance 2-1
Adaptive Control and Management at Layer 5 2-1
Transparent Data Reduction 2-2
Application QoS 2-4
Type of Service 2-4
Simple Network Management Protocol Support 2-5
Remote Monitoring support 2-6
System Log protocol support 2-7
Connection Interception 2-8
When to use CI 2-8
Example CI implementation 2-8

3
Installation

WANJet appliance deployment 3-1
In-line deployment 3-1
One-arm deployment 3-2
Firewall guidelines 3-4
Hardware installation 3-4
Site information worksheet 3-5

4
Initial Configuration

Accessing the Web UI 4-1
Using the Web UI 4-2
WANJet Dashboard 4-3
Basic WANJet appliance configuration 4-4
Configuring the first WANJet appliance 4-4
Configuring multiple subnets 4-5
Defining the second WANJet appliance as a remote WANJet appliance 4-6
Configuring the second WANJet appliance 4-7
Defining the first WANJet appliance as a remote WANJet appliance 4-8
Testing connectivity 4-9
Troubleshooting 4-10

5
Monitoring Performance

Introducing reports 5-1
Status report 5-2
Real Time Traffic report 5-3
Comparative Throughput reports 5-4
Diagnostics report 5-10
Monitoring 5-10
Connectivity 5-18
General 5-21
Administration Tools 5-22
Diagnostic Log 5-25
Third-party reporting systems 5-26
Syslog reports 5-26
SNMP reports 5-26
RMON2 Reports 5-27

6
Managing the WANJet Appliance

WANJet appliance authentication settings 6-1
Changing the Web UI password 6-1
Configuring remote authentication 6-2
Changing the WANJet LCD PIN code 6-3
Granting Web UI access 6-4
Time settings 6-5
Setting the time zone 6-5
Synchronizing time automatically 6-6
Setting the time manually 6-6
Shutting down and restarting the WANJet appliance 6-7
Booting from an alternative image 6-9
Backup and recovery 6-9
Upgrading the WANJet appliance software 6-10

7
Advanced Configuration

Optimization Policies 7-1
Subnets 7-1
Port Settings 7-3
Operational mode setting 7-7
Tuning settings 7-9
Updating a configuration 7-10
Modifying a local WANJet appliance network configuration 7-10
Replicating configuration changes on remote WANJet appliances 7-11
Virtual LANs 7-12
Managing VLANs on a WANJet appliance 7-12
Remote WANJet appliances 7-14
Redundant peers 7-16
Changing the interface speed 7-17
Managing static routes 7-17
Configuring Syslog and SNMP settings 7-18
Email alerts 7-19

8
Service Policy Configuration

IT service policies 8-1
Adding, editing, or removing an IT service policy 8-1
Application QoS Policy 8-3
Adding, editing, or removing an Application QoS Policy 8-3
WAN Links 8-5
Adding, editing, or removing WAN Links 8-5
Adding a subnet to a WAN Link 8-6

9
Configuration Examples

Basic configuration 9-1
Mesh configuration 9-3
Hub and spoke configuration 9-5
Redundant configuration 9-7
LAN router configuration 9-9

A
WANJet Appliance Errors

WANJet appliance error messages and codes A-1

B
WANJet Appliance Private MIB

System information B-1
Ethernet card information B-2
MIB file B-3

1

Introducing the WANJet Appliance

- Introducing the WANJet appliance
- Stylistic conventions in this guide
- Finding help and technical support resources

Introducing the WANJet appliance

F5® Networks WANJet™ appliance is an appliance-based solution that delivers LAN-like application performance over the WAN. The WANJet appliance accelerates applications including file transfer, email, client-server applications, data replication, and others, resulting in predictable, fast performance for all WAN users.

For data centers, the WANJet 400 appliance features fault tolerance and scalability for up to 10,000 optimized connections. For branch offices, the WANJet 200 appliance combines fault tolerant features, silent operation and performance for up to 2,000 optimized connections. The WANJet appliance solutions work seamlessly across all wide-area networks including dedicated links, IP VPNs, frame relay, and even satellite connections.

The WANJet appliance delivers unrivaled application performance and reduced IT expenses. At the heart of the WANJet appliance is the F5 Session Matrix™, which is a networking technology that is essential to application performance on the WAN. Operating at Layer 5 of the OSI reference model, the Session Matrix gives the WANJet appliance full application knowledge and network awareness. It integrates key performance technologies, including Transparent Data Reduction™, adaptive TCP optimization, encryption, and quality of service that are applied to application streams.

About this guide

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

This guide provides information about:

- Installing and configuring the WANJet appliance
- Administering and managing the WANJet appliance
- Monitoring the WANJet appliance's performance
- Performing advanced configuration tasks involving subnets, hubs, static routes, and VLANs
- Configuring remote WANJet appliances
- Managing IT service policies and application QoS policies
- Troubleshooting issues

Additional information

In addition to this guide, there are other sources of documentation that you can use in order to work with the WANJet appliance. The following documentation is available in PDF format at **http://tech.f5.com**:

- ***WANJet 200 Quick Start Card***
- ***WANJet 400 Quick Start Card***

Stylistic conventions in this guide

To help you easily identify and understand certain types of information, this documentation uses the following stylistic conventions.

Using the solution examples

All examples in this documentation use only private IP addresses. When you set up the solutions we describe, you must use IP addresses suitable to your own network in place of our sample IP addresses.

Identifying new terms

When we first define a new term, the term is shown in bold italic text.

After you have completed the hardware configuration, using either the LCD panel or a console connected to the F5 appliance's serial port, you can configure the WANJet appliance using the browser-based utility, called the ***Web UI***.

Identifying references to objects, names, and commands

We apply bold text to a variety of items to help you easily pick them out of a block of text. These items include web addresses, IP addresses, utility names, most controls in the Web UI, and portions of commands, such as variables and keywords.

For example, if the IP address of the appliance is **192.168.168.102**, type **https://192.168.168.102:10000** in the web browser to login to the WANJet appliance.

Identifying references to other documents

We use italic text to denote a reference to another document.

For example, see the ***Quick Start Card*** for the F5 WANJet 200 or WANJet 400 appliance for information about installing F5 appliances.

Identifying command syntax

We show actual, complete commands in bold Courier text. Note that we do not include the corresponding screen prompt, unless the command is shown in a figure that depicts an entire command line screen. Table 1.1 explains additional special conventions used in command line syntax.

Item in text	Description
\	Continue to the next line without typing a line break.
< >	You enter text for the enclosed item. For example, if the command has **<your name>**, type in your name.
|	Separates parts of a command.
[ ]	Syntax inside the brackets is optional.
...	Indicates that you can type a series of items.

Table 1.1 *Command line conventions used in this manual*

Finding help and technical support resources

You can find additional technical documentation and product information using the following resource:

F5 Networks Technical Support web site
The F5 Networks Technical Support web site, **http://tech.f5.com**, provides the latest documentation for the product, including:

- Release notes for the WANJet appliance, current and past
- Updates for guides (in PDF form)
- Technical notes
- Answers to frequently asked questions
- The Ask F5 natural language question and answer engine

To access this site, you need to register at **http://tech.f5.com**.

2

Overview

- About the WANJet appliance
- Adaptive Control and Management at Layer 5
- Transparent Data Reduction
- Application QoS
- Type of Service
- Simple Network Management Protocol Support
- System Log protocol support
- Connection Interception

About the WANJet appliance

The WANJet appliance is designed to improve the performance of your networks, reducing the bandwidth consumed when transmitting data. In order for the WANJet appliance to reduce the bandwidth consumed in data transmission, it processes data at one side and reverses this process at the other. The WANJet appliance 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). The WANJet appliance 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. This process requires that at least two WANJet appliances are installed, one to process data at one side and another to reverse data processing at the other side.

Adaptive Control and Management at Layer 5

Adaptive Control and Management at Layer 5 (ACM5) operates at the session layer of the OSI model. This technology enables the WANJet appliance 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 appliance 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 data streams that are not merged, 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, the WANJet appliance's ACM5 technology examines all applications and compresses all traffic types.

Transparent Data Reduction

F5 Networks' Transparent Data Reduction (TDR) technology provides a dramatic reduction in the amount of bandwidth consumed across a WAN link for repeated data transfers. For example, without TDR, a 1MB file transferred across a WAN link by 100 different users would consume 100MB of bandwidth. With TDR, the same transfer would consume less than 10MB of bandwidth. This is a reduction of more than 90% in WAN traffic volume.

With TDR, files are not stored or cached, so data is never out of date and it does not 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, requests are never served from a local WANJet appliance 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.

Following is an illustrated example of how TDR works.

Client A requests a file named **antivirus.dat**.

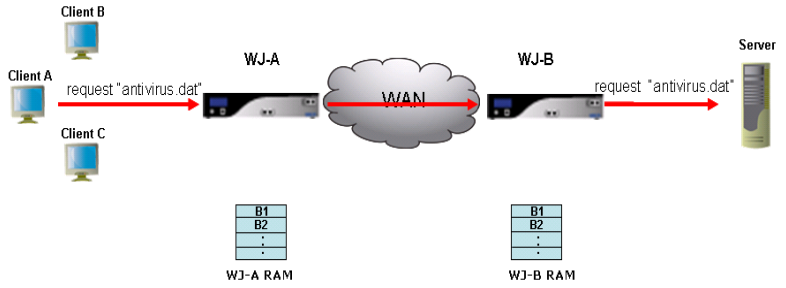

Figure 2.1 *Client requests file*

The Server, on which the file is stored, returns the **antivirus.dat** file. WJ-A and WJ-B copy the data to RAM.

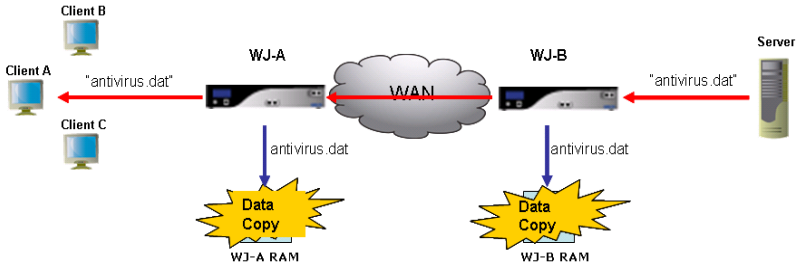

Figure 2.2 *Server returns file*

Client B requests the same **antivirus.dat** file.

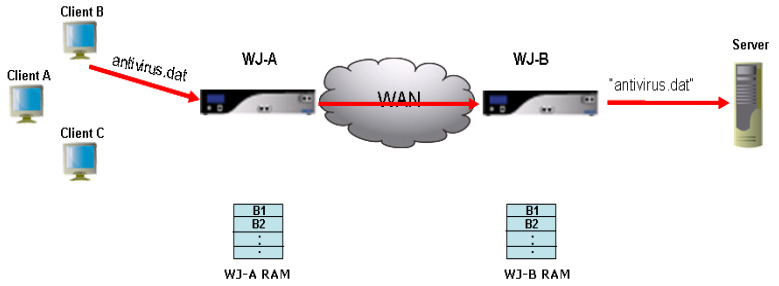

Figure 2.3 *A second client request the same file*

WJ-B compares the **antivirus.dat** file with the data it has in RAM to see if the data has changed, confirming that the data in its RAM is still current.

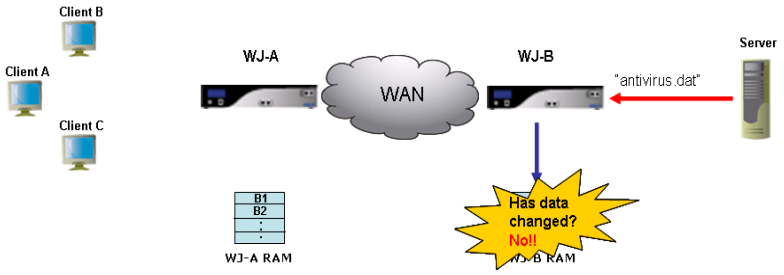

Figure 2.4 *The WANJet appliance compares the file to the file in its RAM*

WJ-B sends a message to WJ-A to use the local data, because the data has not changed. WJ-A sends Client B the data corresponding to **antivirus.dat** file from its local RAM, saving bandwidth.

Application QoS

The WANJet Application QoS provides better service for specific data flows by raising the priority of a specific traffic and limiting the priority for other traffic. Accordingly, the 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 Application QoS policies enables you to downsize the bandwidth consumed over less important network activities and, at the same time, prioritize important and critical data transfer. This way, your bandwidth is used optimally for the transfer of the data that is most important to you.

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

Note

*See **Application QoS Policy**, on page 8-3 for more information.*

Type of Service

The Type of Service feature helps to provide the highest quality of data delivery by prioritizing the delivery of one data stream over another. The WANJet appliance deploys the Type of Service methodologies, giving you control over your data streams. You decide which data stream will get to the receiver first by using the Type of Service feature to assign a priority to data traffic using a specific port. You can assign priorities from 0 to 7, where 0 is the lowest priority, and 7 is the highest. 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 also assign the same priority, such as priority 7, to multiple protocols.

Simple Network Management Protocol Support

Simple Network Management Protocol (SNMP) 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 appliance sends SNMP traps to the SNMP server you specify. The traps you view on the SNMP server are errors for troubleshooting purposes. See *WANJet appliance error messages and codes*, on page A-1 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 Web UI access*, on page 6-4.

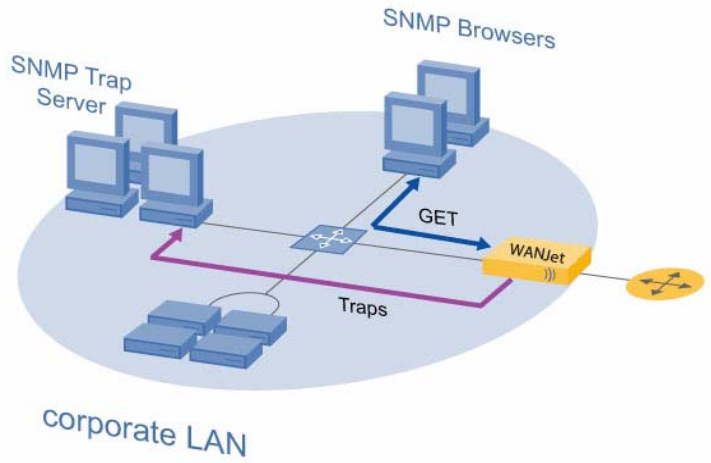

Figure 2.5 *The WANJet appliance and SNMP data*

The Management Information Base that stores the SNMP data contains 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 7-18.

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 was 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.

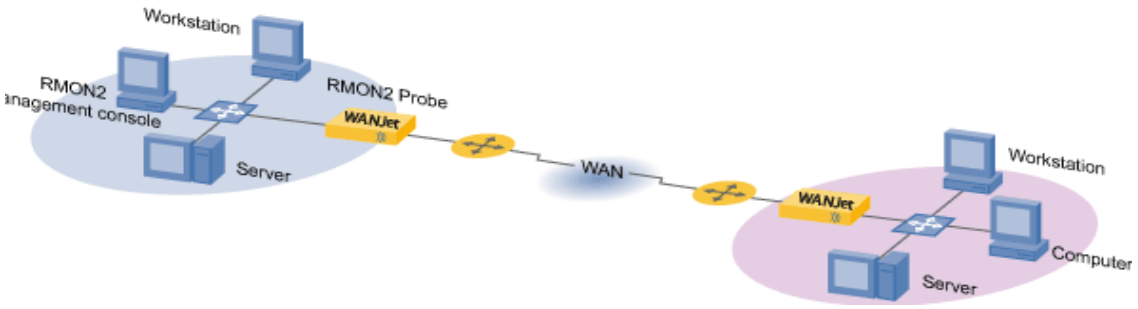

Figure 2.6 *The WANJet appliance and ROMON2*

The WANJet appliance 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 appliance supports the following RMON2 groups.

RMON2 group	Description
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.
Protocol Directory	Contains the protocols for which the agent monitors and maintains statistics.

Table 2.1 *Supported RMON2 groups*

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 7-18.

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 appliance sends system event messages to the Syslog server you specify. The data log sent by the WANJet appliance includes the sent data, and the received data. In addition, the WANJet appliance 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 7-18.

Connection Interception

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

When to use CI

With CI, you can reset connections on a range of different ports, without having to reboot the relevant servers or restart a whole range of services. You can use the CI option when you are performing any of the following processes:

- Installing the WANJet appliance on your network
- Upgrading the WANJet appliance
- Changing the WANJet appliance's mode from inactive to active
- Restarting the WANJet appliance

Before you perform any of the proceeding procedures, verify that the ports for all connections that you are going to reset been assigned the following:

- The ACM5 processing mode
- The Connection Intercept option

Example CI implementation

In this 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:

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

◆ Note

You can use the following process to optimize any port. The best usage for CI is when you want to reset connections on a range of ports, without having to either reboot the relevant servers or restart a whole range of services. The WANJet appliance allows you to reset connections automatically, without having to restart the server or manually reset the connections.

For this example, you need to optimize FTP data by performing the following steps. The WANJet appliance allows you to use this procedure to automatically reset FTP connections, without having to restart the FTP server or restart the connections manually.

To automatically reset FTP connections

1. In the navigation pane, expand **Optimization** and click **Optimization Polic**y.
   The WANJet Optimization Policy screen displays.
2. From the Service Name column, click the service you want to modify. In this example they are the FTP ports (typically ports **20** and **21**, or ports **989** and **990** for a secure connection).
   The Edit Port/Service Name screen displays in a separate window.
3. From the **Processing Mode** list, select ACM5.
4. Check the **Connection Interception** box.
5. Click the **OK** button.
   The Edit Port/Service Name screen closes and the WANJet Optimization Policy screen displays.
6. Verify that the WANJet appliance operational mode is set to active.
7. Restart the WANJet appliance.
   This forces Connection Interception on all configured ports (the FTP ports, in this example). The data using these ports is then optimized once the WANJet appliance restarted.

◆ Note

For additional details about how to configure the CI option, refer to ***Configuring specific ports****, on page 7-4.*

3

Installation

- WANJet appliance deployment
- Firewall guidelines
- Hardware installation
- Site information worksheet

WANJet appliance deployment

This chapter provides key information about the WANJet appliance installation and configuration guidelines. There are several ways to deploy a WANJet appliance on your network. The options consist of:

- In-line deployment, in one of the following configurations:
  - Point-to-point
  - Point-to-multi-point
- One-arm deployment

The way you choose to deploy the WANJet appliance depends on your current network topology and requirements.

In-line deployment

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

Point-to-point configuration

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

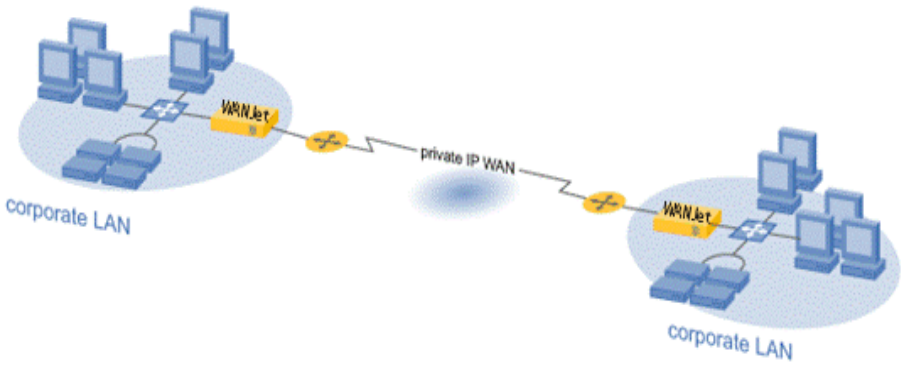

Figure 3.1 *In-line deployment in point-to-point configuration*

Point-to-multi-point configuration

Point-to-multi-point configuration involves three or more F5 appliances. Figure 3.2 illustrates a deployment that consists of five appliances that are connected to each other across intranets and the internet.

As with the point-to-point configuration, the WANJet appliance processes traffic that matches user-specified source and destination subnets, and then delivers it across the WAN through a tunnel to the appropriate WANJet appliance.

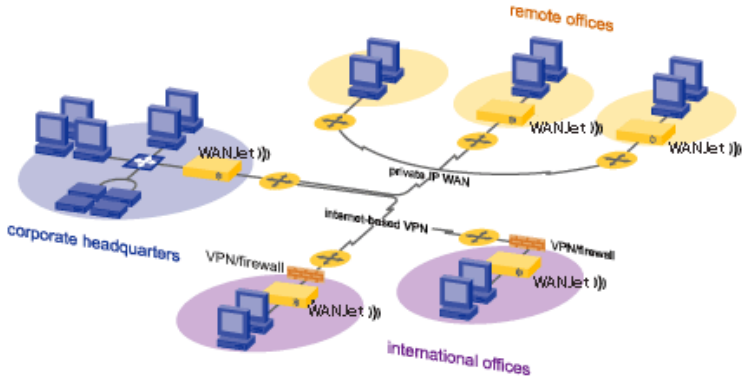

Figure 3.2 *In-line deployment in a point-to-multi-point configuration*

One-arm deployment

A one-arm deployment is more complex than an in-line deployment. To decide on the optimal configuration for your system, it helps to understand the three types of one-arm deployment.

- **Using static routing**
  The WANJet is connected to the LAN switch, and the LAN switch is in turn connected to all of the clients on the network, as well as to the router. Every client on the LAN is configured with the WANJet appliance as its default gateway. All client traffic is routed to the WANJet appliance.

  You can configure the WANJet appliance to optimize specific traffic, apply different services on specific traffic, and leave other traffic untouched. The WANJet appliance sends all this traffic back to the router.
- **Using transparent proxy statically**
  The WANJet appliance is connected to the router directly and is transparent to the rest of the LAN clients.

The router (as per a configured routing rule) directs to the WANJet appliance only traffic that the WANJet appliance is configured to process (optimize or applying specific services). The router is configured so that the passthrough traffic is not sent to the WANJet appliance. If you do not configure the router in this way, the passthrough traffic sent to the WANJet appliance is dropped. In accordance with the WANJet configuration, it optimizes specific traffic, and then sends all the traffic back to the router.

- **Using transparent proxy with the WCCP v2 protocol**
  The WANJet appliance is connected to the router directly and is transparent to the LAN clients. All LAN traffic is routed to the WANJet appliance. This part is identical to static transparent proxy.

  The difference is that the WANJet appliance communicates with the router using the WCCP v2 protocol. In accordance to its configuration, the WANJet appliance determines 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 deployment method is that it is more tolerant of a failure. If the WANJet appliance is down, the router compensates and handles the traffic properly without sending it back to the WANJet appliance.

Firewall guidelines

If the WANJet appliance is placed behind a firewall, you must open certain ports. Table 3.1 lists the ports that you must open to allow the traffic to pass through the firewall.

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 appliance.
10001	The default port used by the WANJet appliance to send real-time chart data.
3701	The default port used by the WANJet appliance for managing connections.
3702	The default port used by the WANJet appliance for TCP data tunnels.
3703	The default port used by the WANJet appliance to proxy UDP over TCP.

Table 3.1 *Ports to open when the WANJet appliance is behind a firewall*

You must also allow the ICMP protocol to pass through the firewall, so that the WANJet appliance can be pinged.

Hardware installation

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

Site information worksheet

Use the following site information sheet to capture all relevant site data. When you complete the site information sheet, attach a detailed network diagram for each WANJet appliance site.

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

4

Initial Configuration

- Accessing the Web UI
- Basic WANJet appliance configuration
- Testing connectivity
- Troubleshooting

Accessing the Web UI

After you have completed the hardware configuration, using either the LCD panel or a console connected to the WANJet appliance's serial port, you can configure the WANJet appliance using the browser-based utility, called the ***Web UI***. You can access the Web UI, from any appliance that is connected to the network and is able to run a web browser.

This chapter describes how to log on to the WANJet Web UI and perform the basic configuration required for the WANJet appliance to start processing traffic. This basic configuration is also covered on the *Quick Start Card* that shipped in the box with the WANJet appliance. If you have already performed the basic configuration steps on the *Quick Start Card*, you do not need to repeat them.

Use the Web UI for all WANJet appliance configuration. To fully configure individual WANJet appliances, you must log into the Web UI for each WANJet appliance, using its remote IP address in the URL.

◆ Note

If your web browser cannot access the Web UI, it may be because the Web UI access is restricted. You can grant access through the console by specifying the IP address of the machine on which your browser runs. Once you have access, you can use the Web UI to change the list. See ***Granting Web UI access, on page 6-4.***

To access the Web UI

1. In a web browser, access the Web UI using HTTPS and port **10000**. For example, if the IP address of the appliance is **192.168.168.102**, type **https://192.168.168.102:10000** in the web browser.
   The welcome screen displays.

   Note*: You must use HTTPS over port* ***10000*** *to access the WANJet appliance using the Web UI. For example, you cannot access the WANJet appliance using the Web UI if you attempt to access the IP address using the browser defaults of HTTP over port* ***80****.*

2. Type the user name and password.
   The default user name is **admin** and the default password is **admin** (unless it was changed by a local administrator).

   Note*: F5 Networks recommends that you change the default password to something more secure at your earliest opportunity. See* ***Changing the Web UI password, on page 6-1*** *for details.*

3. Click the **Log On** button.
   The WANJet appliance is now online.

Using the Web UI

When you log into the Web UI for a WANJet appliance, the Web UI treats the appliance to which you are logged on as the local WANJet appliance. All other WANJet appliances are treated as remote WANJets appliances. When you first log into the Web UI, the WANJet Status screen displays in the main browser frame. This screen displays a brief summary of the status, IP address, alias, and software version for the connected WANJet appliances.

For instruction about obtaining additional remote status information, refer to the *Status report*, on page 5-2.

To view other Web UI screens, expand a section in the navigation pane, on the left side of the screen, and click an option. For example, if a step says to go to the Optimization Policy screen, expand **Optimization** and click **Optimization Policy**. The WANJet Optimization Policy screen replaces the WANJet Status screen in the main browser frame.

The following links always appear at the top right of the Web UI:

- **User Manual**
  Displays the current version of the ***WANJet User Guide*** (PDF format).
- **About**
  Displays an informational screen that contains:
  - The WANJet appliance's version and build number (required when contacting F5 Networks Technical Support)
  - A link to the end-user license agreement
  - Contact details for F5 Networks Technical Support
- **Logout**
  Logs you out of the Web UI. The browser session automatically times out after 30 minutes of inactivity; however, this option is useful for added security.

WANJet Dashboard

The Web UI, below the F5 logo, displays a variety of status indicators and shortcuts. This area is known as the WANJet Dashboard, which is always visible, regardless of where you are in the Web UI.

The WANJet Dashboard displays the following information:

- IP address of the local WANJet appliance.
- The number of links connected to the remote WANJet appliances and the status of the remote WANJet appliances.
  A green light indicates when all links are active, a red light displays if no links are active, and a yellow light if only some links are active. For more information about each link, click the word **Active** on the screen. This displays the Remote Status report. For more information about the Remote Status report, see *Status report*, on page 5-2.
- The current time on the WANJet appliance and the length of time for which the local WANJet appliance has been active (displayed in days, hours and minutes).
- The number of WAN sessions to which ACM5 optimization is currently being applied. This links to the Optimized Sessions. For more information, see *Optimized Sessions diagnostics*, on page 5-11.
- The number of WAN sessions for which traffic is being allowed to pass through the WANJet appliance, without optimization. This links to the Passthrough Sessions. For more information, see *Passthrough Sessions diagnostics*, on page 5-12.

Basic WANJet appliance configuration

You must set up the WANJet appliances in pairs, with one appliance on each side of the WAN link. You can perform the configuration steps for both appliances either on each physical appliance, or from a single computer by logging into the Web UI remotely.

The following configuration example consists of two WANJet appliances that are deployed point-to-point.

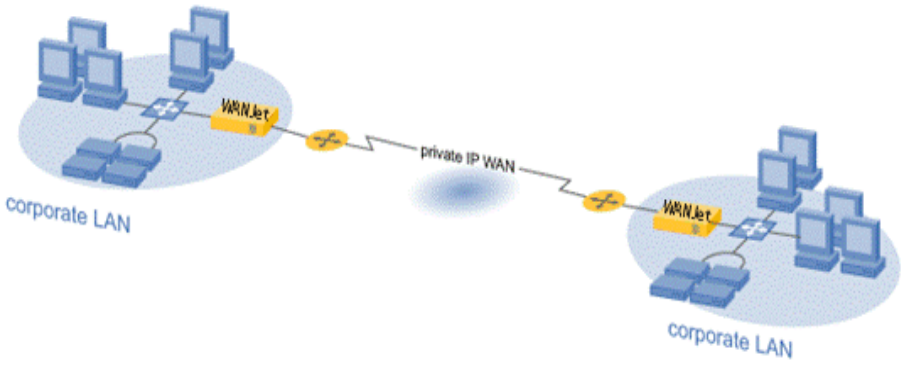

Figure 4.1 *In-line deployment in point-to-point configuration*

The WANJet appliances in this example are connected as follows:

- WANJet A is connected locally with IP address **175.16.2.1**.
- WANJet B is connected at the remote end of the WAN Link with IP address **10.2.0.1**.

Using this example, the basic WANJet appliance configuration consists of the following steps:

- Configuring the local WANJet appliance
- Configuring multiple subnets (if required)
- Defining the second WANJet appliance as a remote WANJet appliance on the first WANJet appliance
- Configuring the remote WANJet appliance
- Defining the first WANJet appliance as a remote WANJet appliance on the second WANJet appliance

Configuring the first WANJet appliance

You configure WANJet appliances in pairs. A pair of WANJet appliances consists of a local WANJet appliance and a remote WANJet appliance, one on either side of a WAN link. You initiate the configuration process by configuring the first WANJet appliance in the pair.

To configure the first WANJet appliance

1. Into a browser, type the address and port for the first WANJet appliance. For this example, you type the following URL in the browser for WANJet A:

   `https://175.16.2.1:10000`

2. Log in to the Web UI.
   The user name is **admin**. The default password is **admin**.

3. In the navigation pane, expand **Configuration** and click **Local WANJet**.
   The Local WANJet screen displays.

4. In the **WANJet Alias** box, you may type a name for the WANJet appliance. For example:

   `WANJet_A`

5. Click the **Save** button.

Configuring multiple subnets

If your network has multiple subnets, you must set the local router IP address and add local subnets for the WANJet appliance.

Once the WAN link between the WANJet appliance pair is up, subnet specifications are automatically exchanged between the appliances.

For example, the local subnets that are specified on WANJet A are copied in as remote subnets for WANJet A in the configuration information on WANJet B.

Before performing the following steps, ask your network administrator if you need to specify additional subnets.

To configure multiple subnets

1. In the navigation pane, expand **Configuration** and click **Local WANJet**.
   The Local WANJet screen displays.

2. In the **LAN Router** box, type the router's IP address.
   This address is the next-hop router in your LAN.

3. Click the **Save** button.

4. In the navigation pane, expand **Optimization** and click **Optimization Policy**.
   The Optimization Policy screen displays.

5. Check the **Include WANJet Subnet** check box.

   ***Note**: If you do not check this box, you must have a specific reason for not optimizing the traffic from the subnet that includes the first WANJet appliance.*

6. Click the **Add** button beneath **Local Subnet**.
   The Add Subnet screen opens in a separate browser window.
7. In the **Local Subnet** box, type the IP address for the subnet.
   You can use the shorthand address format of, **xxx.xxx.xxx.xxx/nn**, to provide both the subnet address and the subnet mask. For example:

   175.16.2.0/24

   Where **/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 the subnet defined in this configuration example.
8. In the **Netmask** box, type the subnet mask. For example:

   255.255.255.0

   ***Note**: If you entered the subnet address in the **/nn** format, as described in the previous step, the corresponding subnet mask box is automatically populated.*
9. In the **Alias** box, type a string to serve as a name for the subnet. For example:

   Subnet A.
10. Click the **Enabled** button.
11. Click the **OK** button.
    The Optimization Policy screen displays with the new subnet in the list of local subnets.
12. Click the **Save** button.
13. Repeat steps 6 through 12 to add additional subnets as required.

Defining the second WANJet appliance as a remote WANJet appliance

Once you have completed the basic configuration for the first WANJet appliance, define the second appliance as a remote WANJet appliance on the first local WANJet appliance.

To define the second WANJet appliance as a remote WANJet appliance

1. In the navigation pane, expand **Configuration** and click **Remote WANJet**.
   The Remote WANJet screen displays.
2. Click the **Add** button.
   The Manage Remote WANJet screen displays in a new browser window.
3. Leave the **WANJet Type** set to **Single**.

***Note**: For information about configuring redundant WANJet appliances, refer to **Redundant peers**, on page 7-16.*

4. In the **WANJet IP** box, type the IP address for the remote WANJet appliance. For example:

   `10.2.0.1`

5. In the **WANJet Alias** box, type a name for the remote WANJet appliance. For example:

   `WANJet_B`

6. Leave the **WANJet Port** setting.

7. In the **Shared Key** box, type the shared key that was assigned by the network administrator. The only requirement for the key is that it matches the key added for its partner on the corresponding system pair. For this example, you must use the same key when adding WANJet_A as a remote WANJet appliance to WANJet_B.

8. Click the **OK** button.
   The browser window closes.

9. In the Remote WANJet screen, click the **Save** button.
   The new remote WANJet appliance displays in the Remote WANJet appliance list.

Configuring the second WANJet appliance

After you have configured the first WANJet appliance, configure the second WANJet appliance in the pair.

To configure the second WANJet appliance

1. Into a browser, type the address and port for the second WANJet appliance. For this example, you would type the following URL in the browser for WANJet B:

   `https://10.2.0.1:10000`

2. Log in to the Web UI.
   The user name is **admin**. The default password is **admin**.

3. In the navigation pane, expand **Configuration** and click **Local WANJet**.
   The Local WANJet screen displays.

4. In the **WANJet Alias** box, you may type a name for the WANJet appliance. For example:

   `WANJet_B.`

5. Click the **Save** button.

If you have defined a LAN router and added subnets for WANJet_A, you must do the same for WANJet_B, unless WANJet_B is on a simpler LAN. Refer to steps 1-11 in *Configuring multiple subnets*, on page 4-5 for instructions. Before performing the steps, ask your network administrator if you need to specify additional subnets.

Defining the first WANJet appliance as a remote WANJet appliance

Once you have completed the basic configuration for the second WANJet appliance, define the first appliance as a remote WANJet appliance on the second WANJet appliance.

To define the first WANJet appliance as a remote WANJet appliance

1. In the navigation pane, expand **Configuration** and click **Remote WANJet**.
   The Remote WANJet screen displays.
2. In the Remote WANJets screen, click **Add**.
   The Manage Remote WANJet screen displays in a new browser window.
3. In the **WANJet IP** box, type the IP address for the remote WANJet appliance. For example:

   ```
   175.16.2.1
   ```

4. In the **WANJet Alias** box, type a name for the remote WANJet appliance.
   For example:

   ```
   WANJet_A
   ```

5. In the **Shared Key** box, type the shared key.
   This key is assigned by the network administrator. The only requirement for the key is that it matches the key added for its partner on the corresponding system pair. For this example, you must use the same key when adding WANJet_B as a remote WANJet appliance to WANJet_A.
6. Leave the settings as they are for **WANJet Type** and **WANJet Port.**
7. Click the **Logoff** button.
8. Close the browser window.

Testing connectivity

When you have completed the configuration steps and the WAN link is established between the WANJet pair, the two WANJet appliances automatically exchange subnet specifications. For example, the local subnets that you specify for WANJet A become remote subnets for WANJet A in WANJet B's Remote WANJet appliance configuration information.

You can test the connectivity between the local and remote WANJet appliances by viewing the following checks on each:

- Status of remote WANJet appliance(s)
- Traffic passing through network
- Diagnostics

For additional information about the following reports, see Chapter 5, *Monitoring Performance*.

To view the status of the remote WANJet appliance(s)

In the navigation pane, expand **Reports** and click **Status**.
A green light displays next to the IP address for remote WANJet appliances that are enabled and connected.

To view traffic passing through network

1. In the navigation pane, expand **Reports** and click **Comparative Throughput**.
2. Click the **Total Throughput**, **Sent Throughput**, and **Received Throughput** tabs to view the various reports.

To view diagnostics

1. In the navigation pane, expand **Reports** and click **Diagnostics**.
   The Diagnostics screen displays.
2. On the menu bar, click **Remote WANJets** from the connectivity menu.
   The Diagnose Remote WANJet report displays.
3. Review the status for each remote WANJet appliance.
   The status should be **active**.

Troubleshooting

Some common problems are listed in Table 4.1. If you are experiencing an issue that is not included in the following table, contact **http://www.f5.com/customer_support/** for assistance.

Issue	Suggested action(s)
I cannot ping the WANJet appliance	Verify that the computer from which you are pinging has a valid network connection. Try pinging other known devices. Verify that you are using the correct IP address for the appliance, by reading it from the LCD display.
I can ping the WANJet appliance, but I cannot ping the WAN gateway.	Verify that the cabling is connected properly, as described in the *Quick Start Card*. Make sure that you connected the gateway router to the WANJet appliance's WAN port, using the supplied crossover cable.
I cannot see that the WANJet appliance 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 the WANJet appliance's configuration. You must include all subnets for which traffic should be optimized.
My browser connection times out when I attempt to access the Web UI.	Check to see that you are accessing the correct URL for the Web UI. If you enter just **http://** followed by the WANJet appliance's IP address, it will not work. You must connect to port **10000** using the secure HTTPS protocol. For example: **https://123.123.123.123:10000/** See *Accessing the Web UI*, on page 4-1.
When I attempt to access the Web UI, I get a Page Not Found error.	If you are certain that you entered the URL correctly and the WANJet appliance appears to be running, it may indicate that the computer from which you are running your web browser does not have access to the Web UI. Although the default setting grants access to all machines, that setting can be changed to limit access based on IP address. Use the LED panel to add your computer's IP address to the list for access. After that, use the Web UI to change the access settings. For instructions, see *Granting Web UI access*, on page 6-4.

Table 4.1 *Troubleshooting*

Issue	Suggested action(s)
I can access the Login screen for the Web UI, but my browser connection times out when I try to log in.	This issue can occur when the WANJet appliance is not able to access the RADIUS authentication server or when the Timeout and NRetry variables are set too high. See *To configure the WANJet appliance for remote RADIUS authentication*, on page 6-2 Log in as a local user, using the **admin** user name and a default password of **admin** (note that the local administrator may have changed the default password). After you are logged in, click **Security > Remote Authentication**, and verify that RADIUS authentication is enabled. Review the Timeout and NRetry values. F5 Networks recommends a value of **3** for each of these settings. If these settings are too high, authentication might take a long time to fail, causing the connection to time out. For information, see *Configuring remote authentication*, on page 6-2.
The Link LED (for the WAN or LAN port) does not light up.	Verify that the cables are installed properly on the WANJet appliance. Check to see if the ports on the WAN Router and the LAN Switch connected 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. For information about resetting the NIC configuration (link speed and duplex value) for a WANJet port, see *Changing the interface speed*, on page 7-17 F5 Networks strongly recommends that if you force the link for one of the WANJet ports, you force the link for both ports. This prevents link problems in pass-through mode if power to the WANJet device is lost.

Table 4.1 *Troubleshooting (Continued)*

5

Monitoring Performance

- Introducing reports
- Status report
- Real Time Traffic report
- Comparative Throughput reports
- Diagnostics report
- Third-party reporting systems

Introducing reports

There are several different reports in the WANJet appliance's Web UI that you can use to monitor the status, connectivity and performance of your WANJet appliance. Most reports fall into one of the following categories:

- Monitoring
- Connectivity
- General

You can access the following reports by expanding **Reports** in the menu and clicking one of the following report options:

- Status
- Realtime Traffic
- Comparative Throughput
- Diagnostics

Note

To ensure accurate reports, we suggest that you frequently synchronize the time settings on the WANJet appliances and check the time settings for the Reports. For more information, see Time settings, on page 6-5.

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

Status report

The WANJet appliance's Status report provides the status and details for a remote WANJet appliance. If the remote WANJet appliance has a redundant peer, the Remote Status report also displays details about the peer appliance. The Remote Status report is the first screen displayed when you log in to the WANJet appliance Web UI.

To view the Status report

In the navigation pane, expand **Reports** and click **Status**.
The initial WANJet Status screen displays the following information for all connected WANJet appliances:

- Status
- IP address
- Alias
- Version
- License key status (not entered, not valid, expired, or OK)

Note

If you want to view the status of the remote WANJet appliance immediately after changing any of its settings, you must wait until the local WANJet appliance communicates with the remote WANJet appliance. This can take up to two minutes. Once this time has elapsed, refresh your browser.

Real Time Traffic report

The Real Time Traffic report displays a graph of all network traffic, in real time, over both the LAN and the WAN. This provides an at-a-glance overview of the network traffic that is passing through the WANJet appliance.

To view a graph of network traffic in real time

In the navigation pane, expand **Reports** and click **Real Time Traffic**.

The Real Time Traffic screen displays.

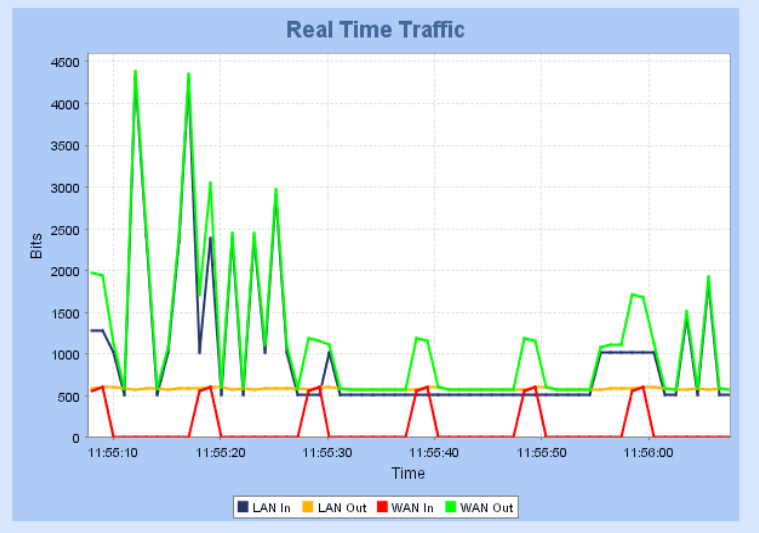

Figure 5.1 *Real Time Traffic report*

In this graph:

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

Comparative Throughput reports

You can generate a Comparative Throughput report based on any combination of traffic direction, data type, and time period.

At the top of each report screen, 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 vary according to the time period selected and the direction of traffic. Comparative Throughput reports refresh automatically every two minutes. You can easily import CSV reports to a database, or spreadsheet package.

To generate a Comparative Throughput report and save it to CSV

1. In the navigation pane, expand **Reports** and click **Comparative Throughput**.
2. On the menu bar, click one of the following to select the direction of traffic and to display the associated report screen:
   - **Total Throughput**
     Reports on all the traffic that the WANJet appliance processes.
   - **Sent Throughput**
     Reports on only the outgoing (sent) data processed by the WANJet appliance.
   - **Received Throughput**
     Reports only the incoming (received) data processed by the WANJet appliance.
3. From the options below the Throughput table, click one of the following to determine how the data is displayed:
   - **Performance Increase report** (default)
   - **Actual Bandwidth Expansion report**
   - **Optimized Data report**
   - **Link Utilization report**
   - **Overall Data report**
4. From beneath the chart, click an option that represents the time period for which you want to view collected data. The default is **current day**.

   ***Note**: The WANJet appliance saves all of the reports generated for the last hour, every hour. If you stopped or restarted the WANJet appliance, or any external termination occurred, you will be able to access the last set of saved reports when you restart the WANJet appliance.*
5. From the Download Report list, choose **CSV**.
6. Click the **Download** button.

Performance Increase report

The Performance Increase report displays the percentage increase in bandwidth, due to using the WANJet appliance.

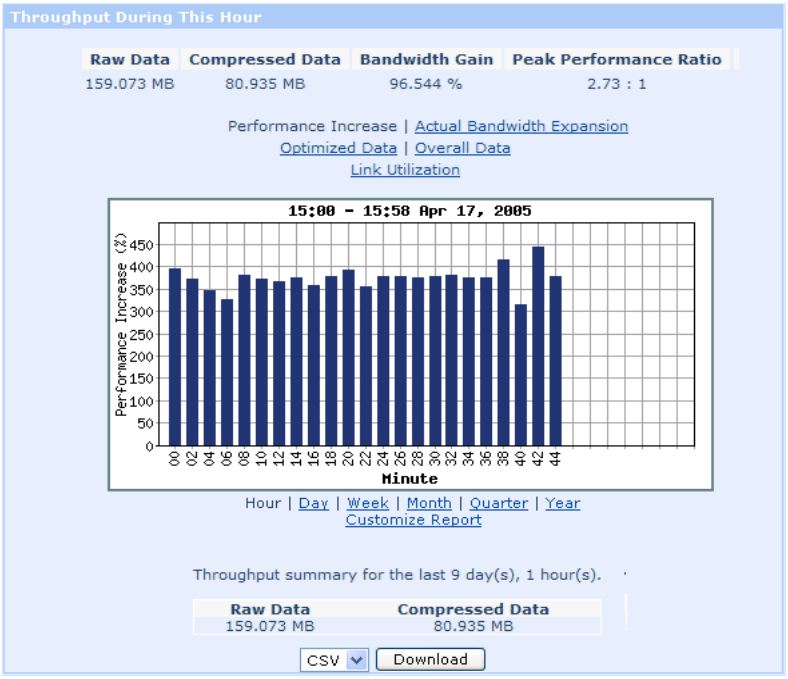

Figure 5.2 *Performance Increase report*

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

(Freed Bandwidth / Bandwidth after optimization) * 100 = 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. With these values, the equation results in the following:

(75MB / 25MB) x 100 = 300% performance increase

Actual Bandwidth Expansion report

The Actual Bandwidth Expansion report displays the actual bandwidth amount that the WANJet appliance has freed, by optimizing network data.

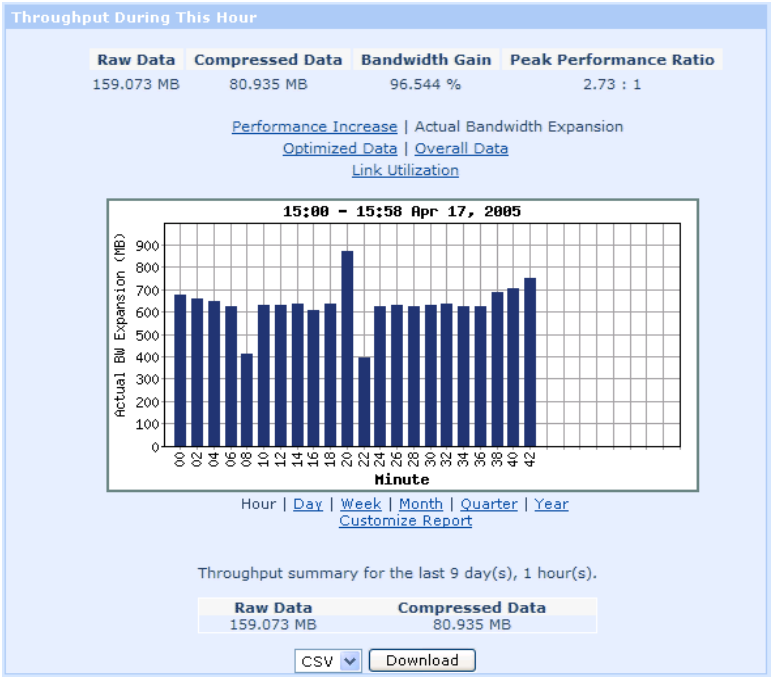

Figure 5.3 *Actual Bandwidth Expansion report*

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

Optimized Data report

The Optimized Data report displays the difference in the amounts of network traffic before and after WANJet appliance processes the data.

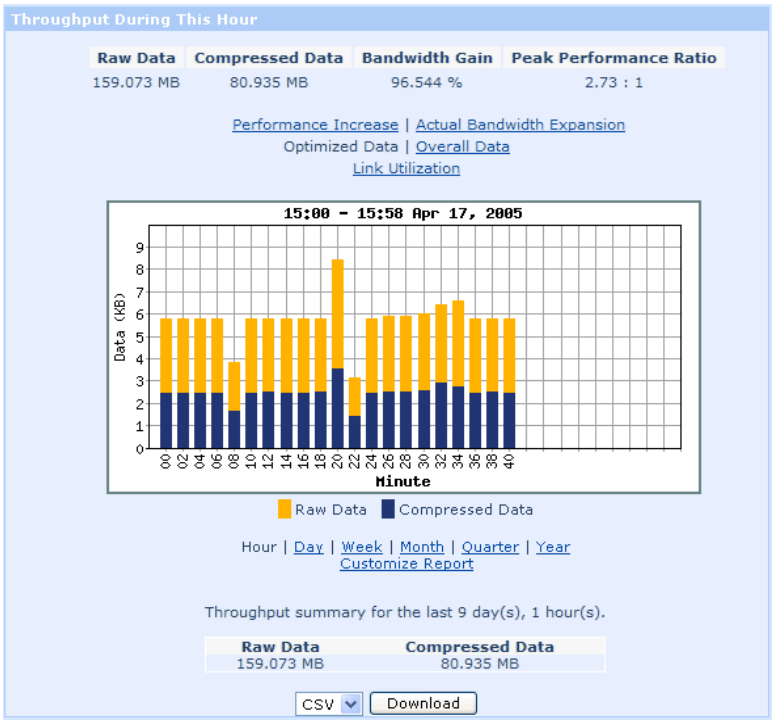

Figure 5.4 *Optimized Data report*

In this graph:

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

Overall Data report

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

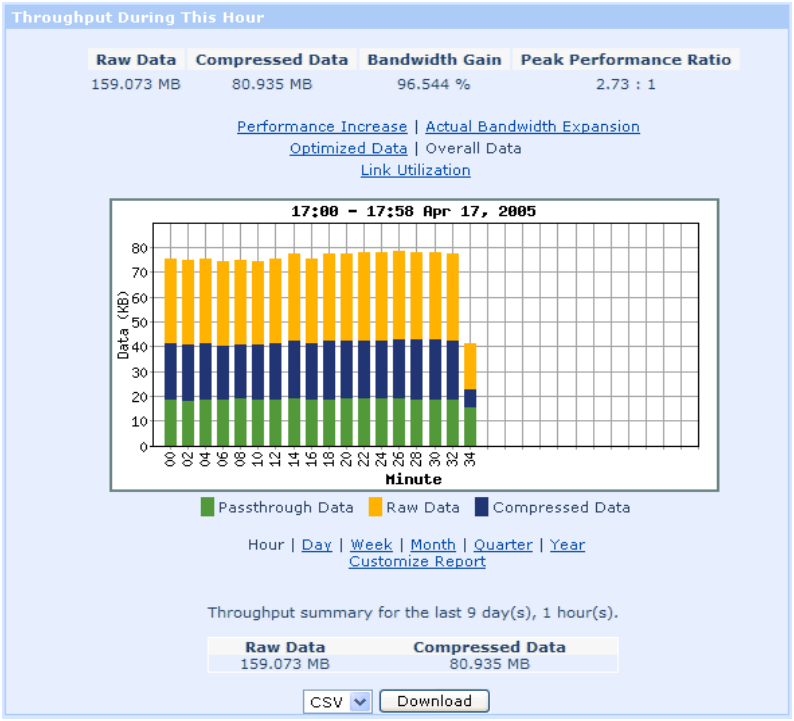

Figure 5.5 *Overall Data report*

In this graph:

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

Link Utilization report

The Link Utilization report is similar to the *Optimized Data report*, on page 5-7. However, instead of showing the total amount of data optimized over a given time period, this Link Utilization report displays the average amount of bandwidth used per second, compared to what would have been used if network traffic had not been optimized.

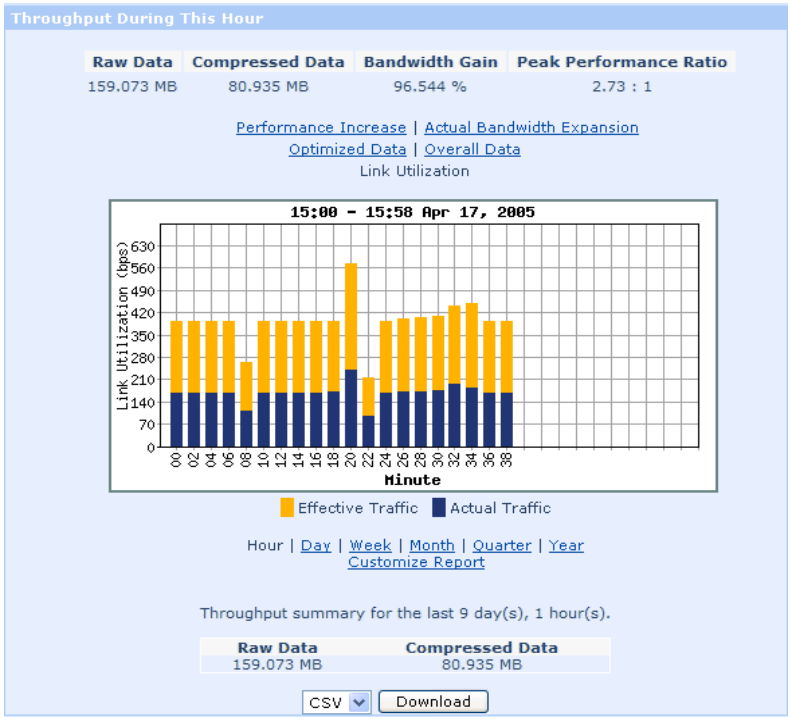

Figure 5.6 *Link Utilization report*

In this graph:

- The vertical axis indicates the amount of bandwidth (in kilobits per second, megabits per second, and so forth).
- 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.

Diagnostics report

The Diagnostics report provides you access to a range of useful information, such as IP addresses, error log files, and the results of popular network analysis tools.

To view diagnostics information

1. In the navigation pane, expand **Reports** and click **Diagnostics**. The initial Diagnostics screen displays.
2. Click one of the following links for additional information:
   - **Monitoring**
   - **Connectivity**
   - **General**

Monitoring

Monitoring diagnostic information is broken up into the following categories:

- Interfaces
- Optimized Sessions
- Passthrough Sessions
  - All Passthrough Sessions
  - Optimized Eligible Connections
  - Autopass
  - Realtime
- WANJet Links
- RADIUS status
- TCP Statistics
  - Connection States
  - Packet Retransmissions
  - Received queue packets Pruned
- TDR Statistics
- QoS
- VLANs

Interfaces diagnostics

A WANJet appliance typically has at least two active network interfaces: one for the connection to the LAN and one for the connection to the WAN. In addition, if a redundant peer WANJet appliance is present on your LAN, there is an interface for that connection. (For more information, see *Redundant peers*, on page 7-16.)

To view diagnostics for interfaces

1. In the navigation pane, expand **Reports** and click **Diagnostics**. The initial Diagnostics screen displays.
2. On the menu bar, choose Interfaces from the Monitoring menu. The Interfaces screen displays with the following information for each network interface:
   - 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).
   - Reception (RX) errors raised by the interface, including dropped packets, overruns, and frame errors.
   - Transmission (TX) errors raised by the interface, including dropped packers, overruns, carrier errors, and collisions.

Optimized Sessions diagnostics

The Optimized Sessions report displays all of the network connections at the application layer that are currently being optimized by WANJet appliance using the ACM5 process.

To view diagnostics for Optimized Sessions

1. In the navigation pane, expand **Reports** and click **Diagnostics**. The initial Diagnostics screen displays.
2. On the menu bar, choose Optimized Sessions from the Monitoring menu.
   The Optimized Sessions screen displays.

   ***Note**: Optionally, you can view the Optimized Sessions screen by clicking the Optimized Sessions link from the menu from any screen in the Web UI. The counter beside the Optimized Sessions link displays the current number of optimized session.*

   The Optimized Sessions report is divided into two sections: one for TCP and one for UDP traffic.

   The TCP section contains the following information:

   - **Local IP**
     IP address and port for 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 for the remote WANJet appliance.

- **WANJet IP**
  IP address for the remote WANJet appliance handing the optimized session.

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

Note

For information about how to specify connections for optimization, see Optimization Policies, on page 7-1.

Passthrough Sessions diagnostics

A ***passthrough session*** is a network connection (at the application layer) for which traffic is not optimized by WANJet appliance, but allowed to pass through the appliance untouched.

To view diagnostics for Passthrough Sessions

1. In the navigation pane, expand **Reports** and click **Diagnostics**.
   The initial Diagnostics screen displays.
2. On the menu bar, choose Passthrough Sessions from the Monitoring menu.
   The Passthrough Sessions screen displays.

   The Passthrough Sessions report is divided into two sections: one for TCP traffic and one for UDP traffic, with specific information for each session.

   From this screen you can view one of the following reports:

   - **All Passthrough Connections**
     Displays a detailed list of all passthrough connections.
   - **Optimize Eligible Connections**
     Displays connections that were set up before the WANJet 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.
   - **Autopass**
     Displays a list of connections that are passed through automatically when the destination server is refusing connections.
   - **Realtime**
     Displays passthrough traffic throughput in real time.

Note

For information about how to specify connections for optimization, see Optimization Policies, on page 7-1.

WANJet Links diagnostics

To view diagnostics for WANJet Links

1. In the navigation pane, expand **Reports** and click **Diagnostics**. The initial Diagnostics screen displays.
2. On the menu bar, choose WANJet Links from the Monitoring menu. The WANJet Links screen displays the following information:
   - **Remote IP**
     IP address of the remote WANJet appliance.
   - **#Retrans**
     Number of retransmitted packets to the remote WANJet appliance.
   - **#ACM5**
     Number of network connections to the remote WANJet appliance that are being optimized using ACM5.
   - **#ACM5 without compression**
     Number of passthrough network connections that are not being optimized.

Note

For additional information about links to remote WANJet appliances, refer to Remote WANJet appliances, on page 7-14.

RADIUS Status diagnostics

The RADIUS Status screen displays details of any RADIUS authentication servers known to the local WANJet appliance. Remote authentication through the RADIUS protocol is an alternative to local authentication with a user name and password stored on the WANJet appliance.

Note

For information about how to configure WANJet appliance to use RADIUS authentication, see Configuring remote authentication, on page 6-2. For technical details about the RADIUS protocol, refer to ***http://www.ietf.org/rfc/rfc2865.txt****.*

To view diagnostics for RADIUS status

1. In the navigation pane, expand **Reports** and click **Diagnostics**. The initial Diagnostics screen displays.
2. On the menu bar, choose RADIUS from the Monitoring menu. The RADIUS screen displays with the following information for each RADIUS server:
   - **IP address**

- **Secret**
  The key that is used to authenticate RADIUS transactions between client and server.
- **Timeout period, in seconds**
- **Number of times to retry a connection**

Note

The WANJet appliance displays a warning message if the settings for both the timeout and number of retries are too high, because this could cause a delay in determining if the RADIUS server is not responding to a login attempt.

TCP Statistics diagnostics

TCP Statistics provide the following reports for TCP connectivity activity:

- Connection States
- Packet retransmissions
- Receive queued packets pruned

The Connections States report is displayed by default.

To view diagnostics for TCP Statistics

1. In the navigation pane, expand **Reports** and click **Diagnostics**. The initial Diagnostics screen displays.
2. On the menu bar, choose TCP Statistics from the Monitoring menu. The TCP Statistics screen displays with the Connections States report, by default.
3. Click the options above the report to view one of the following reports:
   - Connections States
   - Packet Retransmissions
   - Receive queue packets Pruned

Connection States

The Connection States report displays a graph of current state for each TCP connection that is visible to the WANJet appliance, for both optimized and passthrough connections. In this report, three lines represent the number of connections in the following states:

- **ESTABLISHED**
  Those connections that have been successfully opened and are working normally.
- **TIME-WAIT**
  Connections in the TIME-WAIT status are waiting to see that the remote TCP received the acknowledgment of a connection termination request. This can take up to four minutes.

- **Other**
  Other possible connection states include:
  - LISTEN
  - SYN-SENT
  - SYN-RECEIVED
  - FIN-WAIT-1
  - FIN-WAIT-2
  - CLOSE-WAIT
  - CLOSING
  - LAST-ACK

Note

For more information about these states, see IETF RFC #793 at ***http://www.ietf.org/rfc/rfc793.txt.***

Packet Retransmissions

TCP segments that time out without being acknowledged by a destination host are retransmitted by the source host. A high number of these retransmitted segments can indicate network problems. Therefore, the Web UI includes a report that tracks those numbers and their trends.

The Packet Retransmissions report consists of a graph with a blue line. The blue line indicates the number of TCP segments (which often correspond to IP packets) that had to be retransmitted per second.

Receive queue packets Pruned

The Receive queue packets Pruned report provides a graphic representation of the number of segments pruned from the TCP receive queue due to socket overrun. Pruning can occur 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.

Note

For more information about TCP tuning background, see ***http://www-didc.lbl.gov/TCP-tuning/background.html****.*

TDR Statistics diagnostics

Transparent Data Reduction (TDR) further enhances network optimization by caching the contents of frequently accessed files in memory.

To view diagnostics for TDR Statistics

1. In the navigation pane, expand **Reports** and click **Diagnostics**. The initial Diagnostics screen displays.

2. On the menu bar, choose TDR Statistics from the Monitoring menu. The TDR Statistics screen displays the following information:
   - **WANJetIP**
     IP address of the remote WANJet appliance.
   - **Sent Bytes (TDR)**
     The amount of data sent in bytes, to which TDR has been applied since the WANJet link became active.
   - **Sent Bytes (other)**
     Amount of data in bytes to which TDR has not been applied.
   - **Received Bytes (TDR)**
     Amount of received date in bytes to which TDR has been applied.
   - **Received Bytes (other)**
     Amount of received date 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 is the average for all remote WANJet links.

◆ Note

For more information about TDR, see Transparent Data Reduction, on page 2-2.

QoS diagnostics

Quality of Service (QoS) policies can help to improve network performance by dedicating bandwidth to specific network traffic.

To view diagnostics for QoS policies for remote networks

1. In the navigation pane, expand **Reports** and click **Diagnostics**. The initial Diagnostics screen displays.
2. On the menu bar, choose TDR Statistics from the Monitoring menu. The QoS report screen displays the following information:
   - **Remote**
     The Remote network that has a QoS policy assigned to it.
   - **Policy**
     Name of the QoS policy assigned to the remote network.
   - **Rate**
     Actual bandwidth assigned to each QoS policy.
   - **Bytes Sent**
     Number of bytes sent for each QoS policy.
   - **Packets Sent**
     Number of packets successfully sent for each QoS policy.

- **Dropped**
  Number of packets dropped for each QoS policy.

Note

For additional information about QoS, refer to Application QoS Policy, on page 8-3.

VLANs diagnostics

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

To view VLANs supported by WAN optimizer

1. In the navigation pane, expand **Reports** and click **Diagnostics**. The initial Diagnostics screen displays.
2. On the menu bar, choose VLANs from the Monitoring menu. The VLANs Information screen displays the following information.

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

Table 5.1 *VLAN report*

Note

For information about configuring VLANs to work with the WANJet appliance, refer to Virtual LANs, on page 7-12.

Connectivity

Connectivity diagnostic information is organized in the following categories:

- All
- Ethernet
- IP
- Bridge
- Remote WANJet

Ethernet diagnostics

The Diagnose Ethernet screen displays details about the Ethernet interfaces for the local WANJet appliance. For WANJet appliance to work correctly, the speed and duplex settings for the LAN and WAN interfaces should be the same. The Diagnose Ethernet screen confirms if that is the case, and displays a warning if it is not.

Note

For information about configuring the speed and duplex settings for Ethernet interfaces, see Changing the interface speed, on page 7-17).

To view diagnostics for Ethernet connectivity

1. In the navigation pane, expand **Reports** and click **Diagnostics**. The initial Diagnostics screen displays.
2. On the menu bar, choose Ethernet from the Connectivity menu. The Diagnose Ethernet screen with a section for each of the following Ethernet interfaces:
   - **eth2** (PEER)
   - **eth3** (ETH3)
   - **eth1** (WAN)
   - **eth0** (LAN)

The following information displays for each interface:

- Speed
- Transmitted
- Received
- Receive errors
- Collisions

WANJet appliance QoS does not work unless the Ethernet interfaces are connected as follows:

- The **eth0** interface must be connected to the LAN.

- The **eth1** interface must be connected to the WAN.

Note

***Note**: If a redundant pair is present, the **eth2** interface must be connected to the redundant peer. For more information, see Redundant peers, on page 7-16.*

IP diagnostics

The Diagnose IP screen displays technical details about the local WANJet appliance's IP configuration.

To view diagnostics for IP connectivity

1. In the navigation pane, expand **Reports** and click **Diagnostics**. The initial Diagnostics screen displays.
2. On the menu bar, choose IP from the Connectivity menu. The Diagnose IP screen displays the following information:
   - The IP address of the local WANJet appliance.
   - The netmask of the local subnet. This determines how much of the address identifies the subnetwork on which the WANJet appliance host resides, and how much identifies the host itself.
   - The IP address of the WAN gateway used by the local WANJet appliance.
   - The results of the local gateway ping.

Note

Addresses must adhere to the Internet Protocol standards. For more information about configuring addresses, see Updating a configuration, on page 7-10.

Bridge diagnostics

The Diagnose Bridge screen displays details of the internal connectivity, or ***bridge***, between Ethernet interfaces between the two WANJet appliances.

To view diagnostics for Bridge connectivity

1. In the navigation pane, expand **Reports** and click **Diagnostics**. The initial Diagnostics screen displays.
2. On the menu bar, choose Bridge from the Connectivity menu. The Diagnose Bridge screen displays the following information:
   - The IP address and MAC address of the WAN gateway that the local WANJet appliance uses
   - The Ethernet interfaces that are linked by the bridge

WANJet appliance QoS does not work unless the Ethernet interfaces are connected as follows:

- The **eth0** interface must be connected to the LAN switch or router.
- The **eth1** interface must be connected to the WAN gateway.

Remote WANJet appliance diagnostics

The Diagnose Remote WANJet screen displays details about the remote WANJet appliances that are connected to the local WANJet appliance.

Note

For information about how to configure remote WANJet appliances, see Remote WANJet appliances, on page 7-14.

To view diagnostics for remote WANJet connectivity

1. In the navigation pane, expand **Reports** and click **Diagnostics**. The initial Diagnostics screen displays.
2. On the menu bar, choose Remote WANJets from the Connectivity menu.
   The Diagnose Remote WANJet screen displays the following information for each remote WANJet appliance:
   - The software version number, which is compared to the local version number
   - The status of the local WANJet appliance
   - The number of remote WANJet appliances
   - The IP address for the remote WANJet appliance
   - The WANJet appliance type, which will be Single if there is no redundant peer at the remote end
   - Whether the remote WANJet appliance is responding to pings from the local WANJet appliance
   - Whether the local WANJet appliance can connect to the remote WANJet appliance on the ports that WANJet appliances use to communicate with each other. These ports are **3701**, **3702**, and **3703** by default.

General

General diagnostic information is broken up into the following categories:

- Bridge Forwarding Database
- Administration Tools
- Diagnostic Log

To view general diagnostic information

In the menu bar of the Diagnostic screen from the General menu, choose the item that corresponds to the information that you want to view.

Bridge Forwarding Database diagnostics

The Bridge Forwarding Database Media Access Control (MAC) Addresses screen lists all of the network devices that have sent traffic through the local WANJet appliance bridge.

To view diagnostics for Bridge Forwarding Database

1. In the navigation pane, expand **Reports** and click **Diagnostics**. The initial Diagnostics screen displays.
2. On the menu bar, choose Bridge Forwarding Database from the General menu.
   The Bridge Forwarding Database screen displays the following information for each network device configured:
   - **MAC Address**
     A unique identifier attached to most forms of networking equipment, and used by many network protocols.
   - **IP Address**
     Only available if the device has communicated directly with the WANJet appliance
   - **Interface**
     The interface is defined as **eth0** if the device is connected to the local WANJet appliance through the LAN and as **eth1** if the device is connected through the WAN.
   - **Local**
     This column displays **Yes** for the WANJet appliance's own two internal network devices; that is, its Ethernet interfaces.

Administration Tools

The WANJet appliance provides a browser-based user interface for the following three network administration diagnostic tools:

- Ping
- Traceroute
- Packet Capture

To use the administration tools

1. In the navigation pane, expand **Reports** and click **Diagnostics**.
   The initial Diagnostics screen displays.
2. On the menu bar, choose Administration Tools from the General menu.
   The Administration Tools screen displays. For each tool, there is a box in which you can specify command-line parameters, and a button to initiate the program using the shell.
3. Click the button for the tool that you want to run.
   The lower half of the screen displays the following information:
   - The full path and parameters to the process, as it appears on the command line.
   - The process number, as allocated by the operating system. You can stop a process by clicking the process number before it has finished running.
   - The process output, which is similar to what you would see in the shell after running the program from the command line.
   - The return code, which is **0** if the program returns successfully.

Ping

The ping tool provides a simple test to confirm that a target host is online and reachable through 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, as well as the time taken to send and receive them, provides an indication as to how well the connection is working.

◆ Note

If a ping is unable to reach a target host, that is the statistical summary shows a 100% packet loss, it 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****.*

By default, WANJet appliance 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 WANJet appliance resides. You can change the parameters by typing new parameters in the associated text box.

Important

F5 Networks recommends that only advanced users change parameters.

The WANJet appliance displays the following output for ping:

- 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 lost packets
  - The minimum, average, and maximum round-trip times

Traceroute

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

Traceroute works by incrementing the time to live (TTL) 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, you can reconstruct the path that packets take to the target host.

Note

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 port* ***33434****, you can specify a different port using the* ***-p*** *option.*

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

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

```
-v <IP address of target host>-c 10 (not port 10000)
```

As with the ping tool, the default target is the gateway for the local subnet. You can change the parameters by typing new parameters in the associated text box.

Important

F5 Networks recommends that only advanced users change parameters.

The WANJet appliance displays the following output for traceroute:

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

Packet Capture

You can use the **tcpdump** utility to intercept and display the contents of TCP/IP packets on the network. This is useful for debugging your network configuration, because it allows you to isolate the source of a problem by determining if all routing is working correctly. Data is saved to a PCAP file.

Note

You 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/****.*

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

```
-c 10 (not port 1000)
```

Packets sent to port **10000** are ignored, since this is the port that the Web UI uses to communicate with the local WANJet appliance. You can change the parameters by typing new parameters in the associated text box.

Important

F5 Networks recommends that only advanced users change parameters.

When the **tcpdump** process has finished running, the Tools screen displays a link to the PCAP file that is produced. If you have an application that can read PCAP files, you can open the PCAP file directly, or you can save the file to disk. The PCAP file is also stored on the server where **tcpdump** is running, at the following location:

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

Diagnostic Log

The Diagnostic Log contains status information and errors that the WANJet appliance records during a session. This Diagnostic Log keeps you informed and helps you resolve any problems that you might encounter while working with the WANJet appliance. You can clear the data in the Diagnostic Log at any time. You can also download a system snapshot as a zipped text file to your hard disk. You can provide this zipped text file to the F5 Networks Technical Support team to help resolve technical issues.

To view the Diagnostic Log

1. In the navigation pane, expand **Reports** and click **Diagnostics**. The initial Diagnostics screen displays.
2. On the menu bar, choose Diagnostic Log from the General menu. The Diagnostic Log screen displays.

To clear the Diagnostic Log

1. From the Diagnostic Log screen, click the **Clear Logs** button. A warning message displays to let you know that all data saved to the error and report logs will be deleted.
2. Click **OK** to delete the logs.

To download a system snapshot

1. From the Diagnostic Log screen, click the **System Snapshot** button. The browser opens a download window for you to save the snapshot file to your local disk.
2. Save the snapshot file. The system snapshot file is named **snapshot.txt.gz**. This is a compressed plain text file.

   ***Note**: If you want to view the snapshot file, you will first need to extract it using a tool such as **gunzip**, which is available at **www.gzip.org**.*
3. Rename the compressed file in the following format:

   `snapshot-<yourcompanyname-yyyy-mm-dd>`

   For example:

   `snapshot-acme-2005-04-22`

   You can provide this file to F5 Network Technical Support for assistance in troubleshooting issues.

Third-party reporting systems

The WANJet appliance is integrated with several third-party reporting systems, including Syslog, SNMP, and RMON2.

Syslog reports

With the WANJet appliance, you can view syslog reports from an external syslog server. These reports include data, such as the amount of sent and received data that is processed by the WANJet appliance.

Note

*You must type the IP address for the machine you are using in the **Syslog Server IP** box of the Syslog and SNMP screen, in order to view syslog data. For more information, Configuring Syslog and SNMP settings, on page 7-18.*

SNMP reports

With the WANJet appliance, you can use an external computer as a management station for viewing Simple Network Management Protocol (SNMP) logs that the WANJet appliance produces on the local appliance. The SNMP data trees are stored in an Management Information Base (MIB).

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

Note

*For the WANJet private MIB file, see Appendix B, **WANJet Appliance Private MIB**.*

To configure the WANJet appliance to use an SNMP server

1. In the navigation pane, expand **Configuration** and click **Monitoring**.
   The initial WANJet Syslog and SNMP screen displays.
2. In the Syslog Server IP box, type the community string and IP address for the SNMP server.
   For detailed instructions, see *Configuring Syslog and SNMP settings*, on page 7-18.
3. Click **IP Access Control**.
   The IP Access Control screen displays.

4. Verify that the Web UI has access to the IP address of the SNMP server. The default setting is to grant access to all, but this may have been changed by an administrator.
   For detailed instructions, see *Granting Web UI access*, on page 6-4.

To view SNMP reports

To view the SNMP tables, use SNMP-compliant software. You need to provide SNMP-compliant software with the IP address for the WANJet appliance and community string that you specified on the Syslog and SNMP screen.

◆ Note

*For a list of WANJet appliance SNMP errors and descriptions, s*ee *Appendix A, **WANJet Appliance Errors**.*

RMON2 Reports

You can use the WANJet appliance to view RMON2 data trees, which are part of the SNMP data trees that the WANJet appliance produces. The RMON2 data is stored in a MIB.

◆ Note

*For the WANJet private MIB file, see Appendix B, **WANJet Appliance Private MIB**.*

The RMON2 data on WANJet appliance 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 appliance processes it, times at which data was sent, and the numbers of connections**.**

To enable RMON2 Logs

1. In the navigation pane, expand **Configuration** and click **Monitoring**.
   The initial WANJet Syslog and SNMP screen displays.
2. Check the **Enable RMON2 Logs** check box.
3. Click the button next to either **Raw Data** or **WANJet Data**.
4. In **Community String** box, type the community string.
   For detailed instructions, see *Configuring Syslog and SNMP settings*, on page 7-18.
5. Click the **Save** button.

You access RMON2 data the same way that you access SNMP data. Before accessing RMON2 data, you must specify a community string and IP address for the SNMP server as discussed in the previous section for SNMP reports. Set the RMON2 preferences on the Syslog and SNMP screen.

For detailed instructions, see *Configuring Syslog and SNMP settings*, on page 7-18. Note that the SNMP server must have access to WANJet appliance, as described under *Granting Web UI access*, on page 6-4.

To view RMON2 reports

To view the RMON2 data tree, use SNMP-compliant software.You need to provide SNMP-compliant software with the IP address for the WANJet appliance and community string that you specified on the Syslog and SNMP screen.

6

Managing the WANJet Appliance

- WANJet appliance authentication settings
- Granting Web UI access
- Shutting down and restarting the WANJet appliance
- Booting from an alternative image
- Backup and recovery
- Upgrading the WANJet appliance software

WANJet appliance authentication settings

To maintain the security of the WANJet appliance settings, the Web UI is password-protected, while 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 Networks recommends that you immediately change the password and PIN code from the defaults and then change them regularly (once a month, for example) thereafter.

Changing the Web UI password

The admin user account password is the only local account that you can use to access the Web UI. You can use remote accounts to access the Web UI; however, you cannot change the passwords for remote accounts from the WANJet Password screen. For more details, refer to *Configuring remote authentication*, following.

Important

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

To change the WANJet Web UI password

1. In the navigation pane, expand **Security** and click **Password**.
   The WANJet Password screen displays.
2. In the **Old Password** box, type the old password.

   ***Note**: If you did not change the default password during the initial configuration, leave this box blank.*
3. In the **New Password** box, type the new password.
   As a general rule, passwords should consist of at least 6 characters and include a mixture of lowercase and uppercase letters, numbers, and punctuation marks. A blank password is not allowed.
4. In the **Confirm Password** box, retype the new password.
   This must match the password that you typed in the **New Password** box.
5. Click the **Save** button to save the new setting.
   A confirmation screen displays.
6. Click **Yes** to confirm the new password.

Configuring remote authentication

You can choose to authenticate WANJet appliance users against the WANJet appliance's local database, or against a RADIUS remote authentication server.

To configure the WANJet appliance for local authentication

1. In the navigation pane, expand **Security** and click **Remote Authentication**.
   The WANJet Remote Authentication screen displays.
2. Click the button next to **No Remote Authentication**.
3. Click the **Save** button.

To configure the WANJet appliance for remote RADIUS authentication

1. In the navigation pane, expand **Security** and click **Remote Authentication**.
   The WANJet Remote Authentication screen displays.
2. Click the button next to **RADIUS**.
3. In the box under **Server**, type the IP address for the RADIUS server.
4. In the box under **Secret**, type the server's shared secret.
   This is the key that authenticates RADIUS transactions between the client (the local WANJet appliance, in this case) and the RADIUS server.
5. In the box under **Timeout**, type the number of seconds that the WANJet appliance should wait after sending a RADIUS request. After this time has expired, WANJet appliance stops waiting for a response. F5 Networks recommends that you use the value of **3**.
6. In the box under **NRetry**, type the number of times that you want the WANJet appliance to send a RADIUS request to the server before giving up. F5 Networks recommends that you use the value of **3**.

   ***Note**: If you type a value in the **Timeout** box, you must also enter a value in the **NRetry** box. If you set the values too high, 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 the **Add** button to store the new information.
8. Repeat Step 2 through 7 for any additional RADIUS servers.

   ***Note**: Once you have added server details, you cannot edit them. You must delete and the information and add it again.*

9. Click the **Save** button.
   The Remote Authentication screen refreshes with the RADIUS server details that you added.

Note

After you configure the WANJet appliance to use remote RADIUS authentication, you can view diagnostic RADIUS reports. For more information, see ***Connectivity****, on page 5-18 for details about this report. For information about RADIUS protocol, refer to* ***http://www.ietf.org/rfc/rfc2865.txt.***

Changing the WANJet LCD PIN code

There is no default PIN code for the Liquid Crystal Display (LCD) on the WANJet appliance.

To create or change the LCD PIN code

1. In the navigation pane, expand **Security** and click **LCD PIN**.
   The LCD PIN screen displays.
2. In the **Old PIN** box, type the old PIN.
   This is a four-digit number.
3. In the **New PIN** box, type the new PIN.
   This must be a four-digit number.
4. In the **Confirm PIN** box, retype the new PIN.
   It must match the PIN that you typed in the **New PIN** box.
5. Click the **Save** button.

Granting Web UI access

You can restrict or allow access to the WANJet appliance's Web UI, and the SNMP reports residing on it, to specific WANJet appliances or subnets as follows:

- **Allow all addresses** (default)
  Provide access to all WANJet appliances or subnets residing on the network.
- **Allow Listed Addresses**
  Provide access to specified WANJet appliances or subnets.
- **Deny Listed Addresses**
  Prevent access for specified WANJet appliances or subnets, while allowing access from all other WANJet appliances or subnets residing on the network.

Once configured, if a restricted WANJet appliance attempts to access the Web UI, the browser returns a 404: Page Not Found error.

Note

To ensure that only specific users access the Web UI, you can create a password for the Web UI and provide this password only to approved personnel. See ***Changing the Web UI password, on page 6-1****.*

To allow specific IP addresses access to the Web UI

1. In the navigation pane, expand **Security** and click **IP Access Control**.
   The WANJet IP Access Control screen displays.
2. Select **Allow Listed Addresses**.
3. In the box, specify IP addresses from which you want to allow access to the Web UI. At a minimum, specify the IP addresses for the following:
   - The SNMP server, so that you can view SNMP and RMON2 reports. (See *Configuring Syslog and SNMP settings*, on page 7-18.)
   - The Syslog server, so that you can view Syslog data. (See *Configuring Syslog and SNMP settings*, on page 7-18.)
   - The WANJet appliance from which you are currently accessing the Web UI through a browser, and any other WANJet appliance from which you want to access the Web UI.
4. Click the **Save** button.

To deny specific IP addresses access to the Web UI

1. In the navigation pane, expand **Security** and click **IP Access Control**.
   The WANJet IP Access Control screen displays.

2. Select **Deny Listed Addresses**.
3. In the box, specify the addresses that you want to deny access to the Web UI.
4. Click the **Save** button.

Time settings

Time management for the WANJet appliance involves setting the time zone and synchronizing all linked WANJet appliances. Synchronizing the time settings is one of the most frequent administrative management tasks that you perform.

The setting options include:

- **Timezone**
  When you initially configure a WANJet appliance, you must set the time zone and the first day of the week.
- **Time Server**
  With this option, you can choose a time server to use for automatic time synchronization for the WANJet appliances.
- **Time**
  With this option, you can set the current time manually for the WANJet appliance.

Setting the time zone

Use the following procedure to set the time zone and the first day of the week for the WANJet appliance.

To set the time zone

1. In the navigation pane, expand **Configuration** and click **Time**. The WANJet Time Settings screen displays.
2. From the **Current location** menu in the Timezone section, choose the closest geographical location to your site.
3. From the **First Day of the Week** menu, choose a day.
4. Click the **Change timezone** button to save the changes.

Repeat these steps for every WANJet appliance in your network.

Synchronizing time automatically

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

Note

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

To use a time server to synchronize time automatically

1. In the navigation pane, expand **Configuration** and click **Time**. The WANJet Time Settings screen displays.
2. From the **Host/Address** menu in the Time Server section, choose the IP address for a commonly used time server. Alternatively, choose **User Specified** and in the box, type the IP address for a preferred time server.
3. Click the **Sync time** button to save the changes.

Repeat these steps for every WANJet appliance in your network.

Setting the time manually

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

To set the date and time manually

1. In the navigation pane, expand **Configuration** and click **Time**. The WANJet Time Settings screen displays.
2. From the current **Day**, **Month**, **Year**, **Hour**, **Minute** and **Second** menus in the Time section, choose the appropriate options.
3. Click the **Set time** button to save the changes.

Repeat these steps for every WANJet appliance in your network.

Shutting down and restarting the WANJet appliance

Shutting down WANJet appliance stops all data processing. You can shut down or restart the WANJet appliance from the Web UI or the LCD panel.

Important

Notify your users before you shut down or restart a WANJet appliance, as network performance will be affected.

To shut down the WANJet appliance using the Web UI

1. In the navigation pane, expand **System** and click **Shutdown & Restart**.
   The WANJet Shutdown & Restart screen displays.
2. Click the **Shutdown WANJet**.
   A confirmation request appears.
3. Click the **OK** button to shut down the WANJet appliance.

To shut down the WANJet appliance using the LCD panel

1. On the front LCD panel of the WANJet appliance, press the X (**Cancel**) button to activate the main menu.
2. Press the ✓ (**Enter**) button to display the **Setup** menu.
3. From the menu, choose **Shutdown**.
4. Press the ✓ (**Enter**) button.
   A confirmation message displays.
5. Press the ✓ (**Enter**) button to shutdown the appliance, or press X to cancel and escape the menu sequence.

Note

You can turn off the WANJet appliance completely by pressing the On/Off button located on the back of the appliance, after you shut it down using the LCD panel.

To restart the WANJet appliance using the Web UI

1. In the navigation pane, expand **System** and click **Shutdown & Restart**.
   The WANJet Shutdown & Restart screen displays.
2. Click the **Restart WANJet** button.
   A confirmation message displays.
3. Click the **OK** button to restart the WANJet appliance.

To restart the WANJet appliance using the LCD Panel

1. On the front LCD panel of the WANJet appliance, press the X (**Cancel**) button to activate the main menu.
2. Press the ✓ (**Enter**) button to display the **Setup** menu.
3. From the menu, choose Restart.
4. Press the ✓ (**Enter**) button.
   A confirmation message displays.
5. Press ✓ to restart the WANJet appliance, or press X to cancel and escape the menu sequence.

Booting from an alternative image

You can have up to two WANJet appliance images on the same flash memory card. If something goes wrong with the first installation, you can boot from the alternative image.

Important

When you reboot from the second image, you must reconfigure all of the default WANJet appliance settings. The WANJet appliance does not work normally until you configured the changes. Therefore, before you complete the following steps, identify the required configuration changes and notify all network users.

To boot the WANJet appliance from the alternative WANJet image

1. In the navigation pane, expand **System** and click **Upgrade & Boot Menu**.
   The WANJet Boot Menu screen displays the WANJet appliance's version and build number for each image. The active versions has a green button next to it and the inactive image has a red button next to it.
2. Click the **Make Active** button next to the image you want to activate.
   A confirmation request displays.
3. Click the **Yes** button.

Backup and recovery

F5 Networks recommends that you create backups of your current WANJet settings on a regular basis. You should also perform a backup before making any major changes to the settings. This makes it easy to restore the system in the event of a failure. Backing up your current content is one of the most frequent administrative management tasks that you perform.

To create a backup file of the current WANJet appliance settings

1. In the navigation pane, expand **System** and click **Backup & Restore**.
   The WANJet Configuration Backup & Restore screen displays.
2. Click the word **here**.
   The browser opens a File Download window for you to save the backup file to your local computer. This default backup file is **Settings-<ServerName>.NTCL.**
3. Save the file to your local hard drive.

4. Rename the backup file to identify the specific WANJet appliance you are backing up, and the current date.

To restore a saved backup of WAN Optimizer settings

1. In the navigation pane, expand **System** and click **Backup & Retstore**.
   The WANJet Configuration Backup & Restore screen displays.
2. From the WANJet Configuration Restore section, click the **Browse** button to locate the backup file that you want to upload. The WANJet appliance's backup files end with the extension **.NTCL**.
3. Click the **Upload** button.
   The Web UI refreshes to the home page, and the backup settings are now in effect.

Upgrading the WANJet appliance software

You can easily upgrade the installed software on the WANJet appliance using the Web UI.

Important

Before you perform an upgrade, you must stop the current WANJet appliance processing session. F5 Networks recommends that you upgrade during a time that will be the least disruptive to network users. Before upgrading, inform all network users that the appliance will be unavailable.

To upgrade the WANJet appliance's software version

1. Verify that a disk image of the new version of the WANJet software is accessible from the local computer on which you are viewing the Web UI (on CD-ROM, for example).
2. In the navigation pane, expand **System** and click **Upgrade & Boot Menu**.
   The WANJet Boot Menu screen displays.
3. Click the **Upgrade** button.
   A confirmation request displays.
4. Click the **OK** button to continue.
5. Click the **Browse** button and locate the upgrade file on your computer.
6. Upload the upgrade file to the WANJet appliance.
7. Click **Upgrade WANJet**.
   The WANJet appliance restarts automatically when the upgrade process is complete.

7

Advanced Configuration

- Optimization Policies
- Tuning settings
- Updating a configuration
- Virtual LANs
- Remote WANJet appliances
- Redundant peers
- Changing the interface speed
- Managing static routes
- Configuring Syslog and SNMP settings
- Email alerts

Optimization Policies

You can use Optimization Policies to specify the TCP/UDP ports to which WANJet's ACM5 and TDR optimization algorithms are applied.

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

Subnets

The procedures to add, remove, or modify subnets are different for the local and remote WANJet appliances.

By default, the **IncludeWANJet Subnet** check box is checked on the Optimization Policies screen. If you clear this check box, the WANJet subnet is removed from the subnet list and the traffic for this subnet is no longer processed. Clear the **IncludeWANJet Subnet** check box if you want to process only traffic from the subnets that are listed below the check box.

Adding, editing, or removing subnets on a local WANJet appliance

To add a new subnet to the local WANJet

1. In the navigation pane, expand **Optimization** and click **Optimization Policy**.
   The WANJet Optimization Policy screen displays.
2. Clear the **Optimize all Subnets** check box.
3. Click the **Add** button located below the Local Subnets list.
   The Add Local Subnet screen displays in a separate window.
4. In the **Local Subnet** box, type the IP address for the new local machine/subnet. For example:

   `10.8.0.0`
5. In the **Netmask** box, type the netmask for the local machine/subnet. For example:

   `255.255.0.0`
6. In the **Alias** box, type a name for the new machine/subnet. For example:

   `Subnet B`
7. Click one of the following buttons:

   - **Enabled**
     To have the WANJet process the traffic for the machine/subnet at this time.

- **Disabled**
  To keep the WANJet from processing the traffic for the machine/subnet at this time.

8. Click the **OK** button.
   The window closes.
9. Click the **Save** button at the bottom of the WANJet Optimization Policy screen.

To update or remove a machine or subnet on the local WANJet

1. In the navigation pane, expand **Optimization** and click **Optimization Policy**.
   The WANJet Optimization Policy screen displays.
2. Clear the **Optimize all Subnets** check box.
3. From the list of local subnets, click the link of the machine/subnet that you want to remove or edit.
   The Edit Local Subnet screen displays.
4. Click **Remove** to remove this subnet from the list, or to edit the settings.
5. Click the **OK** button.
   The window closes.
6. Click the **Save** button at the bottom of the WANJet Optimization Policy screen.

Note

You cannot update or remove the local the WANJet's own subnet.

Adding a subnet for a remote WANJet appliance

Important

Always add the gateway of any remote WANJet as one of its subnets and confirm that the status of this subnet is disabled.

To add a new subnet to a remote WANJet

1. In the navigation pane, expand **Operational Settings** and click **Optimization Policy**.
   The Optimization Policy screen displays.
2. From the **Remote WANJet** list, select the remote WANJet to which you want to add subnets.
3. Click the **Add** button located below the Remote Subnets table.
   The Add Remote Subnet screen displays.

4. In the **Supported Subnet** box, type the IP address of the machine/subnet that you want to make visible to the remote WANJet.
5. In the **Netmask** box, type the netmask of the remote subnet.
6. In the **Machine(s) Alias** box, type a name for the machine/subnet.
7. If you do not want the WANJet to process the traffic for this subnet at this time, click **Disabled**. Otherwise, leave it at the default of **Enabled**.
8. Click the **OK** button.
   The window closes.
9. Click the **Save** button at the bottom of the WANJet Optimization Policy screen.

Port Settings

You can set the processing mode and the Type of Service (ToS) priority that are assigned to packets for each port on a remote the WANJet appliance. You can assign these separately for TCP and UDP packets so that you can, for example, 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 of these ports, except **443** (HTTPS), also have TDR-1 compression enabled. You can edit the settings for these ports by clicking 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 you need to optimize Passive FTP, enable optimization for all TCP ports and disable optimization for 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 specific port or a range of ports

1. In the navigation pane, expand **Optimization** and click **Optimization Policy**.
   The WANJet Optimization Policy screen displays.
2. Click the **Add** button, located beneath the Protocol Optimization Policies table.
   The Add Port/Service Name screen displays.
3. From the **Service Name** list, select a service or application that uses the network. The corresponding default port used by the service appears in the **From Port** box.

   Alternatively, in the **From Port** box, type the port number. To specify a range of ports, type the first port in the range in the **From Port** box, and the last port in range in the **to** box.

   ***Note**: 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. Keep in mind that these may differ on your system.*
4. From the **Processing Mode** list, select one of the options:
   - **Passthrough**
     Leave traffic over this port in its raw state.
   - **ACM5**
     Apply WANJet optimization to traffic over this port.
5. From the **TOS Priority** list, select a priority for the port(s):

   7 - Network Control
   6 - Internet Control
   5 - Critical
   4 - Flash Overdrive
   3 - Flash
   2 - Immediate
   1 - Priority
   0 - Routine

   ***Note**: Refer to **http://www.ietf.org/rfc/rfc0791.txt** for more information about ToS priority levels.*
6. Select a WANJet optimization option by checking one of the optimization option check boxes.

The following options are available only if you have selected **ACM5** as the processing mode.

Check box	Optimization description
TDR-1	Check this box 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.
TDR-2	Check this box to apply the WANJet's TDR-2 intelligent caching algorithm.
Encryption	Check this box if network traffic on the specified port is encrypted to use SSL.
Connection Intercept	Check this box to reset any connection over the specified port that was opened before the new settings were applied.

7. Click the **OK** button.
   The window closes and the WANJet Optimization Policy screen displays with a new row in the Protocol Optimization Policies table with the details that you entered. You can click on the port number (in the **Service Name** column) to edit these settings.
8. Click the **Save** button at the bottom of the WANJet Optimization Policy screen to apply the new port settings.

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 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. In the navigation pane, expand **Optimization** and click **Optimization Policy**.
   The WANJet Optimization Policy screen displays.
2. From the Remote WANJet menu, choose the remote WANJet to which you are connecting.
3. In the third table in the Service Name column, for TCP or UDP protocol, click **All Ports**. (This reads **All other ports** if optimization polices are defined for specific ports.)
   The Edit Port Service Name screen displays.
4. From the **Service Name** list, select a service or application that uses the network. The corresponding default port used by the service appears in the **From Port** box.

Alternatively, in the **From Port** box, type the port number. To specify a range of ports, type the first port in the range in the **From Port** box and the last port in range in the **to** box.

***Note**: 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. Keep in mind that these may differ on your system.*

5. From the **Processing Mode** list, select one of the options:
   - **Passthrough**
     Leave traffic over this port in its raw state.
   - **ACM5**
     Apply WANJet optimization to traffic over this port.
6. From the **TOS Priority** list, select a priority for the port(s):

   7 - Network Control
   6 - Internet Control
   5 - Critical
   4 - Flash Overdrive
   3 - Flash
   2 - Immediate
   1 - Priority
   0 - Routine

   ***Note**: Refer to **http://www.ietf.org/rfc/rfc0791.txt** for more information about ToS priority levels.*
7. Select a WANJet optimization option by checking one of the optimization option check boxes.

   The following options are only available if you have selected **ACM5** as the processing mode.

Check box	Optimization description
TDR-1	Check this box 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.
TDR-2	Check this box to apply the WANJet's TDR-2 intelligent caching algorithm.
Encryption	Check this box if network traffic on the specified port is encrypted to use SSL.
Connection Intercept	Check this box to reset any connection over the specified port that was opened before the new settings were applied.

8. Click **OK**.
   The Optimization Policy screen displays with a new row in the third table that contains the details that you entered. You can click on the port number (in the **Service Name** column) to edit these settings.
9. Click the **Save** button to apply the new port settings.

Operational mode setting

From the Operational Mode screen, you can:

- Specify the operational mode of the WANJet (active or inactive).
- Specify Transparent Data Reduction (TDR) as operational.
- Specify how the WANJet is deployed in your network topology (in-line or one-arm).

To configure the operational mode settings

1. From the navigation pane, expand **Optimization** and click **Operational Mode**.
   The Operational Mode screen displays.
2. For the Mode setting, select one of the following options:
   - **Active -** WANJet optimization is enabled.
   - **Inactive -** WANJet optimization does not occur and the WANJet is completely transparent to network traffic.
3. For the Topology setting, specify the way the WANJet is connected to the network by clicking one of the options:
   - **In-Line -** This is the most common network topology. ***In-line*** means that the WANJet is located between the LAN (or the LAN switch) and the WAN gateway (or the LAN router).
   - **One-Arm -** Select this option if your WANJet is located on a separate, independent link. If you select this option, see the following section *One-arm topology*, for additional instructions.
4. Click the **Save** button.

One-arm topology

This option allows the WANJet to be deployed out-of-line, with one physical connection to the LAN and no direct connection to the WAN

◆ Note

*For more information about this configuration, see **One-arm deployment**, on page 3-2.*

When you select **One-Arm** topology for the operational mode setting, a new section titled Redirection Method displays.

From the Redirection Method section, select one of the following options:

- **Static Routing**
  Use this option if each client on your LAN is configured to route network traffic through the WANJet.
- **Transparent Proxy**
  Use this option if LAN traffic designated for optimization is directed to the WANJet by a router.
- **Non-Transparent Proxy**
  Use this option if you want the WANJet appliance to act as the default gateway for all clients in the LAN. In this configuration, every client on the LAN must be configured to use the WANJet appliance's IP address as its default gateway.

If you select **Transparent Proxy**, a new section titled Discovery Method displays. From this section, select one of the following options:

- **Static**
  Use this option if passthrough traffic is not routed to the WANJet. In this case, only network traffic that is scheduled for ACM5 optimization is routed through the WANJet. This traffic is lost if the WANJet is not running.
- **WCCPv2**
  Use this option if the WANJet communicates with your network router using the Web Cache Coordination Protocol (WCCP). In this case, all network traffic is routed through the WANJet, but the router by-passes the appliance if WANJet is not running. If you select this option, see the following section, *WCCP-based discovery*, for additional instructions.

WCCP-based discovery

The WANJet appliance 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, for example, the local WANJet appliance(s), in accordance with an algorithm defined for the service group.

◆ Note

For detailed specifications about the WCCP protocol, see ***http://www.faqs.org/rfcs/rfc3040.html****.*

If you select WCCPv2 in the Discovery Method section, four new controls display.

To configure WCCP-based discovery

1. In the **Service ID** box, type the service group identifier. This must be a number between 51 and 100, and must match the service ID configured on the LAN router.

2. In the **Priority** box, type the priority assigned by the router to the service group. This number determines the order in which redirection rules are followed. This must be a number between 0 and 255, and must match the priority configured on the LAN router.
3. In the **Router** box, type the IP address that the LAN router uses to communicate with the WANJet appliance.
4. Check the **Authenticate** check box.
5. If WCCP is configured to require authentication between the WANJet appliance and the LAN router, type a password in the **Password** box.
6. Click the **Save** button.

Tuning settings

From the Tuning screen, you can guarantee maximum output by specifying the link bandwidth and the Round Trip Time (RTT) for the WAN link.

To modify Tuning settings

1. In the navigation pane, expand **Optimization** and click **Tuning**. The WANJet Tuning screen displays.
2. In the **Bandwidth** box, type a value for your WAN link bandwidth. The default bandwidth is 45 megabits per second. You can use the list to change the units to kilobits per second for lower-bandwidth links.
3. In the **RTT** box, type the value for the average round trip time for the WAN link. The default RTT is 300 milliseconds.
4. Check the **Congested Control** check box if you want the WANJet appliance to handle the traffic if congestion occurs in the case of packet loss. The **Congested Control** check box is checked by default.
5. In the **Queue Size** box, type the maximum number of outgoing packets to keep in the queue before dropping (in case of network problems). The default **Queue Size** is 10240 packets.
6. Click the **Save** button.
   The WANJet Tuning screen refreshes, and the changes are committed to the WANJet appliance.

Updating a configuration

When you initially configure the local WANJet appliance (as described in Chapter 4, *Initial Configuration*) you specify the network settings for the WANJet appliance, such as IP address, ports, subnets, redundant peers, and connected remote WANJet appliances.

From the Local WANJet appliance screen, you can edit the network information for the local WANJet, such as defining redundant peers, adding subnets, and defining VLANs to the local WANJet. The initial values displayed on the Local WANJet appliance screen are the ones that you specified during initial configuration.

Important

You must replicate any changes that you make to the WANJet's IP address, port, or subnet address, on each remote WANJet to which the local WANJet appliance is connected. See ***Replicating configuration changes on remote WANJet appliances*** *in the following section.*

Modifying a local WANJet appliance network configuration

To modify the local WANJet appliance configuration, perform the following steps.

To modify the local WANJet appliance network configuration

1. In the navigation pane, expand **Configuration** and click **Local WANJet**.
   The Local WANJet appliance screen displays.
2. Modify the values as required. The values are defined as follows:
   - **WANJet Alias**
     The name that is used for the local WANJet appliance. This name is displayed at the upper-left corner of the home when you log onto the WANJet Web UI.
   - **WANJet IP**
     The IP address that is assigned to the local WANJet on your network. If you change this value, you must change it on each remote WANJet that accesses the local WANJet appliance. See *Replicating configuration changes on remote WANJet appliances* in the following section.
   - **WANJet Netmask**
     Subnet mask assigned to the WANJet on your network.
   - **WAN Gateway**
     The gateway the WANJet appliance uses to reach the WAN.
   - **LAN Router**
     The gateway that the WANJet appliance uses to reach the LAN.

- **WANJet Port**
  The main port number that the local WANJet appliance uses to communicate with remote WANJet. The default port is **3701**. If you change this value, you must change it on each remote WANJet that accesses the local WANJet appliance. See *Replicating configuration changes on remote WANJet appliances* in the following section.
- **License Key**
  For the local installation of the WANJet appliance. If this box is blank or contains an invalid key, the WANJet appliance does not process data.
- **Redundant Peer IP**
  IP address of the redundant WANJet appliance. If you check the **Redundant Peer IP** check box, the **IP address** box displays.

3. Click the **Save** button.

Replicating configuration changes on remote WANJet appliances

If you make any changes to the IP address, port setting, or subnet address on a local WANJet appliance, you must replicate the changes everywhere they appear, including to connected remote WANJet appliances.

For example, if you have four connected WANJet appliances named B1, B2, B3, and B4, and you bring up the Web UI for B1, the Web UI shows B1 as the local WANJet and B2, B3, and B4 as its remote WANJets. Therefore, if you change the IP address for B1, you must also change the IP address for B1 for the remote WANJet appliances (B2, B3, and B4) so that it matches.

To update the remote WANJet appliance settings from the local WANJet appliance

1. Log onto the Web UI of the WANJet appliance.
2. In the navigation pane, expand **Configuration** and click **Remote WANJets**.
   The Local WANJet screen displays.
3. Click the IP address of the remote WANJet appliance that you want to edit.
   The Manage Remote WANJet screen displays in a separate window.
4. Edit the settings as required.
5. Click the **OK** button.
   The Manage Remote WANJet The Remote WANJet screen closes.
6. Click the **Save** button at the bottom of the Remote WANJets screen.
7. Repeat steps 3 through 6 for each remote WANJet appliance that connects to the local WANJet appliance for which you changed settings.

Once complete, the local WANJet appliance should be able to communicate with all connected remote WANJet appliances.

◆ Note

Alternatively, you can change the settings for the connected WANJet appliances by logging into each WANJet appliance's Web UI.

Virtual LANs

A Virtual LAN (VLAN) is a computer network that has logically defined (rather than physically defined) boundaries. You must use the Web UI to make the WANJet explicitly aware of any VLANs that are linked to your network. This is required because VLANs are often implemented by adding tags to Ethernet frames. These tags must be preserved during optimization.

Managing VLANs on a WANJet appliance

You can manage VLANs on a WANJet appliance using the following procedures.

To add a VLAN to a WANJet

1. In the navigation pane, expand **Configuration** and click **Local WANJet**.
   The Local WANJet appliance screen displays
2. Click the **VLAN Settings** link beneath the table.
   The VLAN Setting screen displays with all of the currently defined VLANs.
3. Click the **Add** button.
   The Add VLAN screen displays in a separate window.
4. In the **WANJet Virtual IP** box, type the virtual IP address assigned to the local WANJet on this VLAN. That is, the IP address that other machines on the VLAN use to communicate with the local WANJet appliance.
5. In the **VLAN Netmask** box, type the subnet mask for the VLAN.
6. In the **VLAN Gateway** box, type the virtual IP address of the gateway machine for the VLAN.
7. In the **VLAN Tag** box, type the VLAN ID that the WANJet appliance uses to preserve tagged Ethernet frames that pass to and from the VLAN.
8. Click the **OK** button.
   The Add VLAN screen closes.
9. Click the **Save** button.

After you add the VLAN to the WANJet, you must perform the following tasks:

- Add the VLAN as one of the subnets of the local WANJet so that the WANJet can optimize the traffic coming from this VLAN.
  For instructions, see *Subnets*, on page 7-1.
- Add the VLAN to any remote WANJets that are linked to the local appliance, and also add it as one of their subnets. This is necessary if the remote WANJets are to handle optimized data from the VLAN.
  For instructions, see *Replicating configuration changes on remote WANJet appliances*, on page 7-11 and *Subnets*, on page 7-1.

To edit or remove a WANJet VLAN

1. In the navigation pane, expand **Configuration** and click **Local WANJet**.
   The Local WANJet appliance screen displays
2. Click the **VLAN Settings** link beneath the table.
   The VLAN Setting screen displays with all of the currently defined VLANs.
3. Click the IP address for the VLAN you want to edit or remove.
   The Edit VLAN screen displays in a separate window.
4. Edit the VLAN information or click the **Remove** button to remove it.
5. Click the **OK** button.
   The Edit VLAN screen closes.
6. Click the **Save** button.

Important

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

Remote WANJet appliances

To optimize the data that is sent over a network link, you need a pair of WANJets, each running the WANJet software. A remote WANJet reverses the optimization process for data that is sent from the local WANJet. For this configuration to work, the local WANJet must be aware of the remote WANJet. If you do not specify a remote WANJet to receive the processed data, network traffic passes through the local WANJet without being optimized.

To add a remote WANJet

1. In the navigation pane, expand **Configuration** and click **Remote WANJet**.
   The Remote WANJet screen displays.
2. Click the **Add** button.
   The Manage Remote WANJet appliance screen displays.
3. From the WANJet Type list, select **Single.**
   Or, if you have two connected WANJet appliance peers on the same remote LAN, select **Redundant**. (See *Redundant peers*, on page 7-16 for an explanation about these node types.)
4. In the **WANJet IP** box, type the IP address for the remote WANJet appliance.
5. If you selected **Redundant** in Step 3, type the IP address for the peer WANJet appliance in the **Node 2** box. Otherwise, skip to Step 6.

   ***Note**: The **Node 2** box appears only if you select **Redundant** from the WANJet type menu.*
6. In the **WANJet Alias** box, type a name for the remote WANJet appliance. The name must have fewer than 14 characters.
7. In the **WANJet Port** box, type the main port number on which the remote WANJet appliance listens for data from the local WANJet appliance. The default port number is **3701**.

   ***Note**: If you change the WANJet port number, you must change it for all connected WANJet appliances.*
8. In the **Shared Key** box, type the shared key that authenticates between the local and remote WANJets. You can set a unique shared key for every pair of WANJet.
9. If the local WANJet appliance has a LAN router specified for it, you can select a Maximum Transmission Unit (MTU) for the remote WANJet appliance. The MTU is defined as the size of the largest datagram able to pass across a network connection. Select one of the following options:

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

- **VIP**
  The default MTU for this option is 1400 bytes.
- **Other**
  You can specify the MTU for your network according to your needs.

10. Click the **OK** button.
    The Manage Remote WANJet screen closes.
11. Click the **Save** button.

You now need to add the gateway of the remote WANJet as a disabled subnet. For information about how to add a subnet, see *Subnets*, on page 7-1.

To edit or remove a remote WANJet

1. In the navigation pane, expand **Configuration** and click **Remote WANJet**.
   The Remote WANJet screen displays.
2. Click the IP address for the WANJet appliance that you want to edit or remove.
   The Manage Remote WANJet appliance screen displays.
3. Edit the information or click the **Remote** button to remove the remote WANJet appliance.

   ***Note**: If you edit a port number, you must change the port number on all connected WANJet appliances. If you remove a WANJet appliance, you remove all associated subnets and ports.*
4. Click **OK** button.
   The Remote WANJet appliance screen displays.
5. Click the **Save** button.

Important

If you remove a remote WANJet appliance, the local WANJet no longer sees it, and any data sent to the removed remote WANJet appliance's network passes through without being optimized.

Redundant peers

Redundancy offers a continuous mode of operation and eliminates a central point of failure for LAN switching and routing. The WANJet supports redundancy using a second WANJet on a LAN, connected to a redundant router. The second WANJet is known as a redundant peer. If one of the LAN's routers fail, the corresponding WANJet detects that the router is down and continues service through the remaining active router and WANJet.

Not only does this redundant system offer you a continuous mode of operation, but it also provides load-balancing under normal network conditions by distributing network traffic over two WANJets.

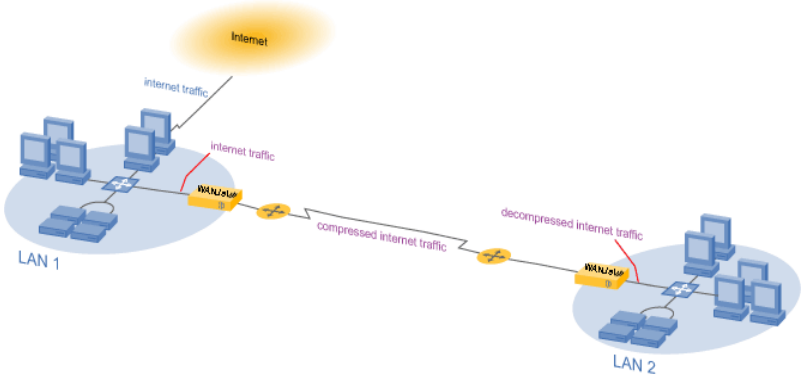

Figure 7.1 *Redundant peer configuration*

To access a redundant peer through the Web UI, you must add both the primary peer and the redundant peer to the Remote WANJet's table of a F5 appliance that is remote from the peers' LAN.

For example, if you have a primary peer called WANJet A with a redundant peer called WANJet A-1, both of which are connected to the remote appliances B and C, you will have to perform the following steps to access WANJet A and A-1 from WANJet B and C.

- Add WANJet A and A-1 to WANJet B.
- Add WANJet A and A-1 WANJet C.

◆ Note

For more information about how to add remote WANJets, see **Remote WANJet appliances, on page 7-14**.

Changing the interface speed

The WANJet supports different speeds in both half-duplex and full duplex. By default, the WANJet appliance is set to auto-negotiate and negotiates both interface speeds automatically; however, you can use the following procedure to manually specify the speed of the network interfaces that the WANJet uses to communicate with the LAN and the WAN.

To specify network interface settings

1. In the navigation pane, expand **Configuration** and click **Interfaces**. The NIC Configuration screen displays.
2. From the **eth0** list, select the interface that corresponds with the link between the LAN switch and the WANJet appliance. The speed duplex value between the LAN and the WAN media type must match.
3. From the **eth1** menu, select the interface that corresponds with the link between the WAN router and the WANJet appliance. The speed duplex value between the LAN and the WAN media type must match.
4. Click the **Save** button.

Managing static routes

The Static Routes table contains information about the gateway (router) that you specify to route the data for a specific network. Data packets sent to the defined gateway use the relevant static route to identify their destination.

When you specify a LAN router for your local WANJet, all subnets configured for the local WANJet use it to identify the destinations of packets.

◆ Note

*To specify a gateway for each subnet, remove the IP address from the **LAN Router** box on the Local WANJet appliance page. See **Updating a configuration**, on page 7-10 for specific instructions.*

To add a static route

1. In the navigation pane, expand **Configuration** and click **Routes**. The WANJet Routes screen displays.
2. In the **Network** box, type the subnet's IP address for which you want to route data to a specific gateway.
3. In the **Netmask** box, type the netmask for the network.

4. In the **Next Hop** box, type the IP address for the gateway to which the data should be routed. Data packets use this gateway to send them to their destination.
5. In the **MTU** box, type the maximum packet size of datagrams that you want transferred through this route.
6. Click the **Save** button.

To edit or remove an existing static route

1. In the navigation pane, expand **System Settings** and click **Routes**. The WANJet Routes screen displays.
2. Modify the **Network** and/or **Netmask** settings as required, or clear the **Network** settings for the route that you want to remove.
3. Click the **Save** button.

Configuring Syslog and SNMP settings

You can configure the WANJet appliance to retrieve Syslog, SNMP, and RMON2 reports from specific servers and specify whether RMON2 data is gathered before or after the WANJet processes it. You can also define the community string for viewing SNMP reports.

To configure Syslog and SNMP settings

1. In the navigation pane, expand **Configuration** and click **Monitoring**.
   The **WANJet Syslog and SNMP** screen displays.
2. Check the **Syslog Server IP** check box and type the IP address of the server that receives WANJet Syslog data.
3. Specify which log to store:
   - **Application**
     Stores only the application error log on the server that you specified.
   - **All**
     Stores all error logs on the server that you specified.
4. Check the **SNMP Server IP** check box and type the IP address of the SNMP server to which the WANJet sends error messages. (For more information about viewing SNMP reports, see *SNMP reports*, on page 5-26.)
5. To view RMON2 data, check the **Enable RMON2 Logs** check box and select an option:
   - **Raw WANJet**
     To view RMON2 logs before the WANJet processes traffic.

- **WANJet Data**
  To view RMON2 logs after the WANJet processes traffic.

***Note**: For information about viewing RMON2 reports, refer to **RMON2 Reports**, on page 5-27.*

6. In the **Community String** box, type the shared community string used to access the SNMP reports on WANJet.
7. Click the **Save** button.
   The Syslog and SNMP page refreshes, and the changes are committed to WANJet.

Email alerts

You can configure the WANJet appliance to send an email containing system snapshots (with logged information) to a specified email address in the event of system failure.

◆ Note

*For information about how to download system snapshots directly, refer to **Diagnostic Log**, on page 5-25.*

To configure email alerts

1. In the navigation pane, expand **Configuration** and click **Email Alert**.
   The WANJet Email Alert screen displays.
2. In the **Email address** box, type the email address to which you want the system snapshot sent.
3. In the **From Email address** box, type the email address from which you want the email to appear to be sent.

   This does not need to be a valid email address, but it should look like a valid address in order to pass through spam filters. F5 Networks recommends that you use the alias of the WANJet from which the snapshot was taken as the first part of the address (before the @ symbol), and your company's domain name as the second part of the address. For example, **WJ_NewYork@f5.com**.
4. In the **SMTP Server IP** box, type the IP address (not the domain name) of an SMTP mail server that is accessible from the WANJet appliance from which this email can be forwarded.
5. In the **SMTP Server Port** box, type the port number for the mail server to which the SMTP request for the email alert will be sent.

   ***Note**: Typically, the port for SMTP is **25**; however, the default port that the WANJet appliance uses for email alerts is **443** (which is normally used by SSL traffic). The WANJet appliance uses port **443**,*

*because it is more likely to be allowed through by a firewall. Verify that the mail server specified in the SMTP Server IP box is set up to forward traffic on port **443** to port **25**.*

6. To automatically email system snapshots, check the **Enabled** check box.

   Email alerts are disabled by default, but F5 Networks recommends that you enable them after you configure the settings on the Email Alert screen.

7. Click the **Test Me** button to confirm that the WANJet can access the mail server and send the email. You can use the test feature to send a simple test message, create a new system snapshot to send, or send all past system snapshots. F5 Networks recommends that you send a test message, because the WANJet does not attempt to resend failed emails.

8. After you have confirmed that the email alert that you configured works, click the **Save** button.

8

Service Policy Configuration

- IT service policies
- Application QoS Policy
- WAN Links

IT service policies

You can use the WANJet appliance to define IT service policies and Application Quality of Service (QoS) policies for your various applications, and to 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 as well as 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 individual 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.

The IT Service Policy 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 each of which handles single type of traffic.

Adding, editing, or removing an IT service policy

You can add, edit, or remove an IT service policy from the IT Service Policy screen.

To add an IT service policy

1. In the navigation pane, expand **Optimization** and click **IT Service Policy**.
   The WANJet IT Service Policies screen displays.
2. Click the **Add** button.
   The Add IT Service Policy screen displays in separate browser window.
3. In the **Policy Name** box, type a name for the service.
4. In the **From** box, type the IP address of the subnet that sends the data, for which you want to specify an IT service policy.
5. In the **Netmask** box, type the full netmask (in dotted quad format) of the subnet that sends the data, for which you want to specify an IT service policy.
6. In the **To** box, specify the subnet that receives the data, for which you want to specify an IT service policy.

7. In the **Netmask** box, type the full netmask (in dotted quad format) of the subnet that receives the data, for which you want to specify an IT Service Policy.
8. You can specify a port in one of the following ways:
   - From the **Ports** list, select a port.
   - In the **From Port** and **To** boxes, specify a range of ports.
9. From the **Protocol** list, select a protocol type for the ports that you specified.
10. Click the **OK** button.
    The Add IT Service Policy screen closes and the WANJet IT Service Policies screen refreshes with the new IT Service Policy displayed.
11. Click the **Save** button to save the changes.

To edit or remove an IT service policy

1. In the navigation pane, expand **Optimization** and click **IT Service Policy**.
   The WANJet IT Service Policies screen displays.
2. Click the name of the IT policy that you want to edit or remove. The Edit IT Service Policies screen displays in separate browser window.
3. Edit the policy settings, or click the **Remove** button to delete the policy.
4. The Edit IT Service Policies screen closes and the WANJet IT Service Policies screen refreshes with the new IT Service Policy displayed.
5. Click the **Save** button to save the changes.

Application QoS Policy

The Application QoS Policy 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 to one or more data flows does not handicap the transmission of other data flows. The Application QoS Polices handle two types of services:

- **Fundamental services**
  The basic protocols supported by your network.
- **IT service policies**
  Tailored services that include different types of traffic.
  (See *IT service policies*, on page 8-1.)

Adding, editing, or removing an Application QoS Policy

You can add, edit, or remove an Application QoS Policy from the Manage the Application QoS Settings of a Remote WanJet screen.

To add an Application QoS Policy to a remote WANJet appliance

1. In the navigation pane, expand **Optimization** and click **Application QoS**.
   The Application QoS screen displays.
2. From the table, click the IP address of the remote WANJet appliance to which you want to apply an Application QoS Policy.
   The Manage the Application QoS Settings of a Remote WANJet appliance screen displays in separate browser window.
3. In the **Link Bandwidth** box, type the bandwidth size of the link between the local WANJet appliance and the remote WANJet appliance.
4. From the **Link Bandwidth** list, select a unit (Kb/s or Mb/s).
5. Click the **OK** button.
   The Application QoS Policy screen displays in a separate browser window.
6. In the **Alias** box, type a name for the policy.
7. In the **Bandwidth** box, type the minimum percentage of bandwidth that the policy should use.
8. In the **Maximum** box, type the maximum percentage that the policy can use.The maximum amount of bandwidth is used only when there is plenty of link bandwidth available.
9. From the **Services** menu, select the ports or IT service policies to use for the policy.
10. From the adjacent service type list, select the associated protocol (TCP or UDP).

***Note**: You can configure a port for both TCP and UPD protocols. To do this, select the port, for example FTP, and select TCP. Then on a new line, select FTP again, and UDP. If you select VoIP, it uses only the UDP protocol. If you select an IT Service Policy from the menu, the adjacent service type menu disappears.*

11. Click the **OK** button.
    The Application QoS screen displays.
12. Click the **Save** button.
    The Application QoS screen refreshes.

To edit or remove an Application QoS Policy from a remote WANJet appliance

1. In the navigation pane, expand **Optimization** and click **Application QoS**.
   The Application QoS screen displays.
2. Click the link for the remote WANJet appliance for which you want to edit or remove an Application QoS Policy. The Manage the Application QoS Settings of a Remote WANJet appliance screen displays in separate browser window.
3. Click the link for the Application QoS Policy that you want to edit or remove.
4. Edit the settings or click the **Remove** button to delete the policy.
5. Click the **OK** button.
   The Application QoS screen displays.
6. Click the **Save** button.
   The Application QoS screen refreshes.

WAN Links

With the WAN Links feature, you can add an Application QoS Policy to the traffic passing through the local WANJet appliance and going to a remote network, whether or not the remote network has WANJet appliance installed. In this way, you can manage and manipulate the bandwidth size for all the traffic transferred through the local WANJet appliance, regardless of the traffic's processing mode.

Adding, editing, or removing WAN Links

To add a new WAN link

1. In the navigation pane, expand **Optimization** and click **Application QoS**.
   The Application QoS screen displays.
2. Click the **Add WAN Link** button.
   The Manage the Application QoS Settings of a WAN Link screen displays in a separate browser window.
3. In the **WAN Link Alias** box, type a name.
4. In the **Link Bandwidth** box, type the size of the bandwidth between the local WANJet appliance and the WAN network.
5. From the **Link Bandwidth** list, select a unit (Kb/s or Mb/s).
6. Click the **OK** button.
   The Application QoS screen displays.
7. Click the **Save** button.
   The Manage the Application QoS Settings of a WAN Link screen closes and the Application QoS screen refreshes with the new WAN link displayed.
8. Click the **Save** button to save the changes.

To edit or remove a WAN link

1. In the navigation pane, expand **Optimization** and click **Application QoS**.
   The Application QoS screen displays.
2. From the Alias column, click the name of the link that corresponds to the WAN Link that you want to edit or remove.
   The Manage the Application QoS Settings of a WAN Link screen displays in a separate browser window.
3. Edit the WAN Link settings, or click the **Remove** button to delete the WAN Link.

4. Click the **OK** button.
   The Manage the Application QoS Settings screen closes and the Application QoS screen displays with the new changes.
5. Click the **Save** button.

Adding a subnet to a WAN Link

You can add subnets or machines to any existing WAN Link. In doing so, you can make use of the Application QoS policies with more nodes (computers, subnets, or networks).

◆ Note

In addition to the following procedure, you can also add a subnet when you add a WAN Link.

To add a subnet to a WAN Link

1. In the navigation pane, expand **Optimization** and click **Application QoS**.
   The Application QoS screen displays.
2. From the **Alias** column, click the name of the link that corresponds to the WAN Link to which you want to add a subnet.
   The Manage the Application QoS Settings of a WAN Link screen displays in a separate browser window.
3. Click the **Add** button, beneath the Support Subnet table.
   The Add Subnet screen displays in a separate window.
4. In the **Supported Subnet** box, type the IP address of the machine or subnet that you want to add.
5. In the **Netmask** box, type the netmask of the new machine or subnet.
6. In the **Machine(s) Alias** box, type a name for the new machine or subnet.
7. Click the **OK** button.
   The Application QoS screen displays and the new subnet appears in the Support Subnet column.
8. Click the **OK** button.
   The Manage the Application QoS Settings closes and the Application QoS screen displays with the new changes.
9. Click the **Save** button.

To edit or remove a subnet from a WAN link

1. In the navigation pane, expand **Optimization** and click **Application QoS**.
   The Application QoS screen displays.
2. From the Alias column, click the name of the link that corresponds to the WAN Link from which you want to edit or remove a subnet.
   The Manage the Application QoS Settings of a WAN Link screen displays in a separate browser window.
3. From the Supported Subnet column, click the name that corresponds to the subnet that you want to edit or remove.
   The Edit Subnet screen displays in a separate browser window.
4. Edit the subnet settings, or click the **Remove** button to delete the subnet.
5. Click the **OK** button.
   The Edit Subnet screen closes and the Manage the Application QoS Settings of a WAN Link screen displays.
6. Click the **OK** button.
   The Manage the Application QoS Settings of a WAN Link screen closes and the Application QoS screen displays with the new changes.
7. Click the **Save** button.

9

Configuration Examples

- Basic configuration
- Mesh configuration
- Hub and spoke configuration
- Redundant configuration
- LAN router configuration

Basic configuration

Following is an illustration of a basic configuration example.

In this example:

- Two LANs are connected and two WANJet 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.

	WJ1	WJ2
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

Table 9.1 *Basic configuration specifications*

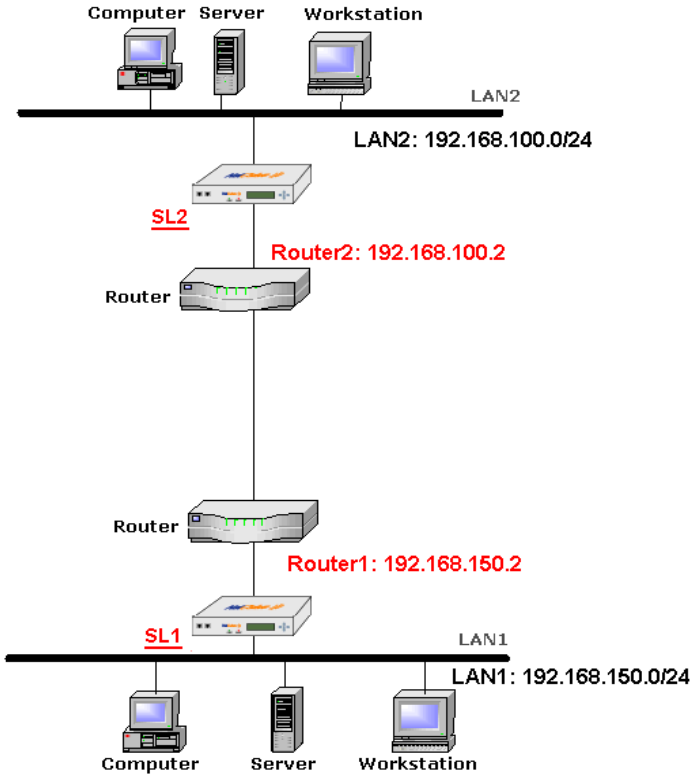

Figure 9.1 *Basic configuration diagram*

Mesh configuration

Following is an illustration of a mesh configuration example.

In this example:

- Three LANS are connected and three WANJet appliances are installed.
- LAN1 has SL1 installed, LAN2 has SL2 installed, and LAN3 has SL3 installed.
- LAN2 and LAN3 are the remote WANJet appliances of LAN1, LAN1, and LAN3 are the remote WANJet appliances of LAN2, and LAN1, and LAN2 are the remote WANJet appliances s 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.

	WJ1	WJ2	WJ3
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 1	10.0.0.2	192.168.200.100	192.168.100.2
Remote Network 2	192.168.200.100	192.168.100.2	10.0.0.2

Table 9.2 *Example mesh configuration specifications*

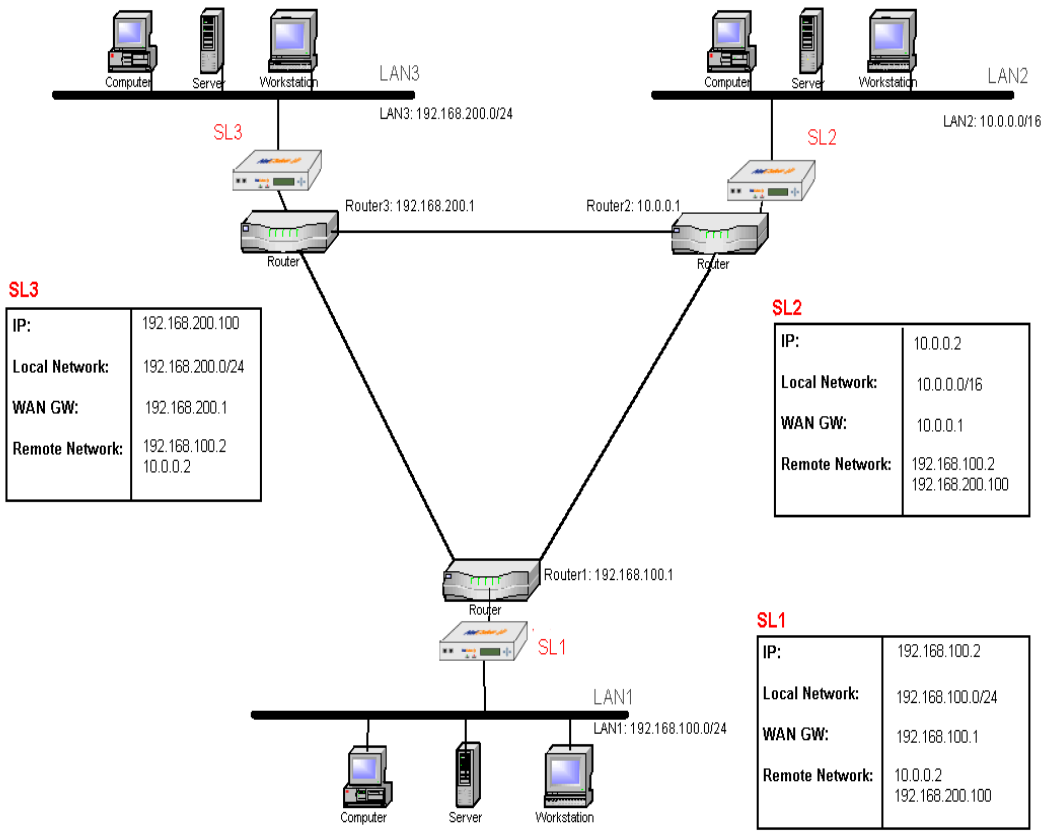

Figure 9.2 *Mesh configuration diagram*

Hub and spoke configuration

Following is an illustration of a hub and spoke configuration example.

In this example:

- Three LANS are connected and three WANJet 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.

	WJ1	WJ2	WJ3
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 1	10.0.0.2	192.168.200.100	192.168.100.2
Remote Network 2	192.168.100.2		

Table 9.3 *Example hub and spoke configuration specifications*

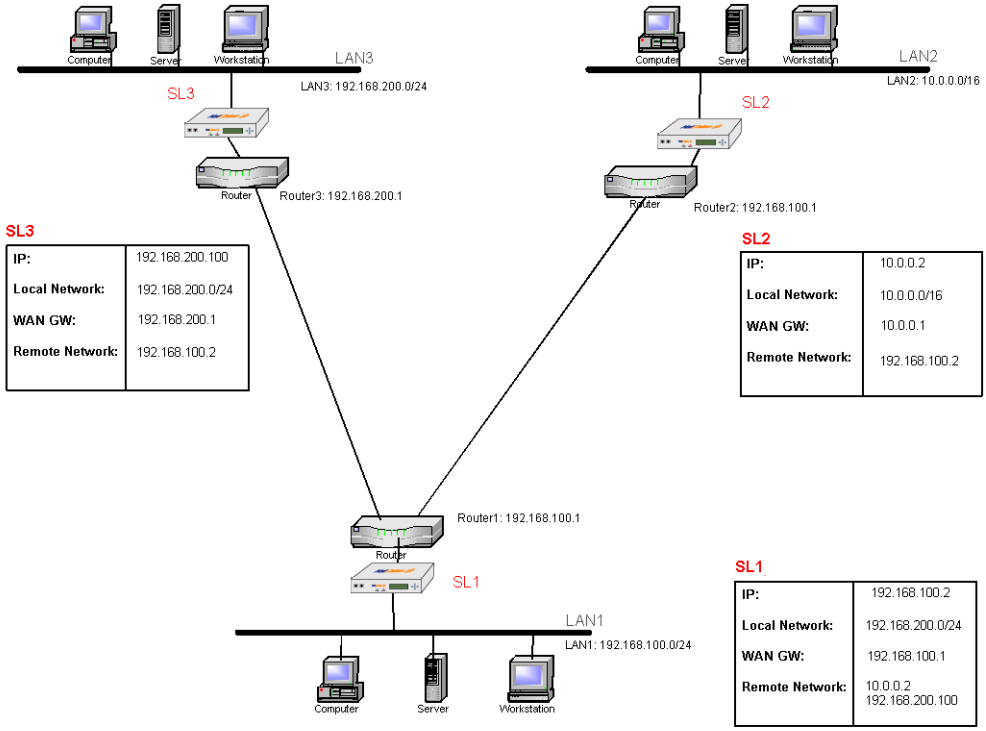

Figure 9.3 *Hub and spoke configuration diagram*

Redundant configuration

Following is an illustration of a redundant configuration example.

In this example:

- Two LANS are connected and one of the LANs has a redundant WANJet appliances 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 appliance resumes 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.

	WJ1-1	WJ1-2	WJ2
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			10.55.55.0/24

Table 9.4 *Example redundant configuration specifications*

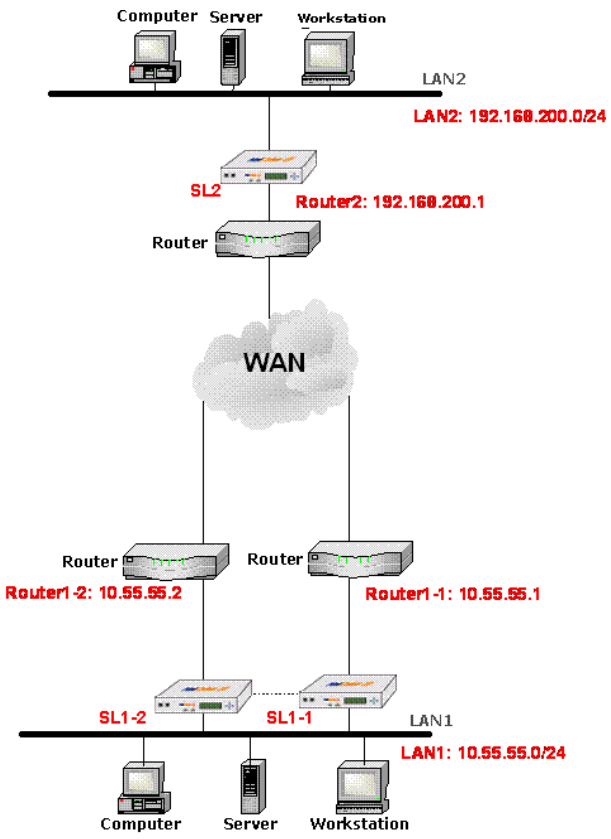

Figure 9.4 *Redundant configuration diagram*

LAN router configuration

Following is an illustration of a LAN configuration example.

In this example:

- A VLAN switch connects two or more virtual networks to a WANJet appliance and the WANJet appliance 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 appliance considers this VLAN switch as its gateway because it connects WANJet appliance (SL1) to its local network (LAN1).
- WANJet appliance sees the local network through the VLAN switch. So, in order for WANJet appliance 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).

	WJ1	WJ2
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

Table 9.5 *LAN router configuration specifications*

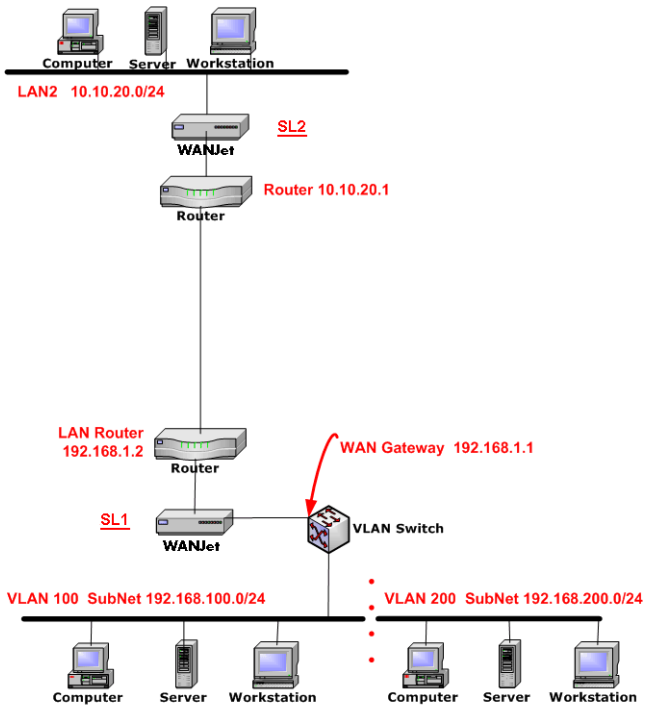

Figure 9.5 *Example LAN router diagram*

A

WANJet Appliance Errors

- WANJet appliance error messages and codes

WANJet appliance error messages and codes

A WANJet appliance may send any of the following error messages to its associated SNMP server and/or Syslog server.

◆ Note

*You can also view this list of errors from the Web UI, by clicking **Diagnostics** in the navigation pane, and then **Diagnostic Log**.*

Error Code	Error Message	WANJet Component
1000 to 1002	Configuration errors	Optimization Engine
1003 to 1005	Initialization error	Optimization Engine
1006 to 1007	Internal errors	Optimization Engine
1100 to 1103	Internal error	Packet Processor
1150	Maximum number or ACM5 connections reached	Packet Processor
1200 to 1201	Configuration errors	ACM5
1202 to 1203	Initialization error	ACM5
1204 to 1207	Internal errors	ACM5
1209	Link down with (Proxy IP)	ACM5
1210	Link up with (Proxy IP)	ACM5
1211	Authentication failed with (Proxy IP)	ACM5
1212	Error: Connection from unauthorized proxy (Proxy IP)	ACM5
1213	Internal error	ACM5
1214	Error: The version (%f) is incompatible with (Proxy IP) version (%f)	ACM5
1215	Error: License expired on 01/01/2004	ACM5
1250	Version (%f) up and running	ACM5
1251	Internal error	ACM5
1252	Warning: License Limit Exceeded	ACM5

***Table A.1** WANJet appliance error messages and codes*

Error Code	Error Message	WANJet Component
1253	Warning: Invalid license key - Bandwidth optimization off.	ACM5
1254	Warning: License key not entered - Bandwidth optimization off.	ACM5
1255	Warning: x (day(s) remain(s) for evaluation for x days	ACM5
1256	Warning: WANJet is activated for evaluation for x days	ACM5
1257	Warning: Evaluation license key expired.	ACM5
1258	License violation: Bandwidth optimization stopped.	ACM5
1259	Cannot complete the remote upgrade. Not enough free space.	ACM5
1300	Logging error	Logs
1420	WCCP ServiceGroup (TCP) is up	WCCP
1421	WCCP ServiceGroup (UDP) is up	WCCP
1422	WCCP ServiceGroup (TCP) is down	WCCP
1423	WCCP ServiceGroup (UDP) is down	WCCP
1424	WCCP Configuration Error	WCCP
1425	WCCP Runtime Error	WCCP
1426	WCCP is not enabled on the router	WCCP

Table A.1 *WANJet appliance error messages and codes (Continued)*

B

WANJet Appliance Private MIB

- System information
- Ethernet card information
- MIB file

System information

The system-related information path is:

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

The system-related information description is:

TotalSentBandwidthSavingPercent

TotalRecvBandwidthSavingPercent

TotalSentBeforeNetCelera

TotalSentAfterNetCelera

TotalRecvBeforeNetCelera

TotalRecvAfterNetCelera

LastSentBandwidthSavingPercent

LastRecvBandwidthSavingPercent

LastSentBeforeNetCeleraRate

LastSentAfterNetCeleraRate

LastRecvBeforeNetCeleraRate

LastRecvAfterNetCeleraRate

Ethernet card information

The Ethernet card-related information path is:

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

The Ethernet card related information description is:

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

Following is the WANJet Private MIB file. You can use this file if you need to compile the MIB file in order to browse the MIB through the standard MIB browser. To use the WANJet Private MIB file, copy the following file into your SNMP-compliant software, and compile it. Refer to the documentation of your SNMP-compliant software for specific instructions.

```
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."
                ::= { ncSnmpTrapList 1102 }

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

```
            ::= { ncSnmpTrapList 1150 }

-- ACM5 Traps

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

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

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

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

       ncTrap1204     OBJECT-TYPE
              SYNTAX  OCTET STRING
              ACCESS  read-only
              STATUS  current
              DESCRIPTION     "Error: Internal error."
              ::= { ncSnmpTrapList 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 exeeded."
           ::= { 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)."
              ::= { ncSnmpTrapList 1400 }

END
```

Index

A

access
- allowing access by IP address 6-4
- granting access to SNMP reports 6-4

ACM5
- assigning to traffic 7-3
- description 2-1

Actual Bandwidth Expansion report 5-6
admin user account
- accessing Web UI 6-1

Application QoS Policy
- adding 8-3
- description 2-4, 8-3, 8-5
- editing 8-4
- removing 8-4

B

backup files
- creating 6-9

bandwidth
- setting size for WAN link 7-9

bandwidth used, report 5-9
basic configuration example 9-1
bridge
- connectivity 5-19
- defined 5-19
- viewing diagnostics for connectivity 5-19

buffer size, application 7-9

C

command syntax, conventions 1-3
Comparative Throughput report 5-4
compression technology 2-1
configuration
- and deployment options 3-1
- testing 4-9

congestion control 7-9
CSV, and reports 5-4

D

data traffic, setting priority 2-4
deployment
- in-line 3-1
- of WANJet appliance 3-1
- one-arm 3-2
- point-to-multi-point 3-1
- point-to-point 3-1

diagnosing problems
- reports 5-10
- using error codes A-1

diagnostics
- downloading 5-25
- monitoring information 5-10

Diagnostics report 5-10

E

error messages and codes A-1
Ethernet cards
- and SNMP information B-2
- viewing diagnostics 5-18

event messages
- and syslog 2-7

F

firewall ports 3-4
freed bandwidth, report 5-5

G

gateway, specifying a static route 7-17
guaranteed performance
- providing for networks 2-4

H

hub and spoke configuration example 9-5

I

initial configuration, verifying connectivity 4-9
in-line deployment, description 3-1
interface diagnostics
- viewing 5-11

IP address
- access to Web UI data 6-4
- and multiple subnets 4-5

IT service
- adding policy 8-1
- defined 8-1

L

LAN router configuration example 9-9
LCD
- setting PIN code 6-3

license
- upgrading 6-10

Link Utilization report 5-9
Liquid Crystal Display. See LCD.
local routers
- and service groups 7-8

logs
- and diagnostics 5-10
- downloading 5-25

M

Management Information Base. See MIB.
mesh configuration example 9-3
MIB 2-5, B-3
modes, processing 7-3
monitoring, diagnostics information 5-10

N

navigation in user interface 4-2

O

one-arm deployment 3-2
operational mode setting 7-7
Optimized Data report 5-7
oS
    described 2-4
outgoing packets
    setting queue size 7-9
Overall Data report 5-8

P

packet retransmissions 5-15
packets
    by VLAN 5-17
    directing through a gateway 7-17
password
    setting for Web UI 6-1
path
    and SNMP system information B-1
    for SNMP Ethernet cards B-2
peers, redundant 7-16
performance
    providing guaranteed level 2-4
Performance Increase report 5-5
PIN code, setting 6-3
point-to-point configuration
    description 3-1
point-to-point deployment 3-1
ports
    and the WANJet appliance 3-4
    assigning for a specific port or range or ports 7-4
    configuring to remote 7-3
    opening when behind a firewall 3-4
power off 6-7
Private MIB file B-3
problems
    diagnosing 4-10
    using diagnostic reports 5-10
    viewing error codes A-1
processing modes 7-3
    assigning for a specific port or range of ports 7-4
proxy, transparent 3-2

Q

queue size
    for outgoing packets 7-9

R

Real Time Traffic report 5-3
redundant configuration example 9-7
redundant peers, description 7-16
remote monitoring. See RMON.
remote user accounts
    accessing Web UI 6-1
remote WANJet appliance
    managing from local WANJet appliance 7-14
reports
    and actual bandwidth expansion 5-6
    and comparative throughput 5-4
    and diagnostic log 5-25
    and link utilization 5-9
    and optimized data 5-7
    and overall data 5-8
    and performance increase 5-5
    and real time traffic 5-3
    and RMON2 5-27
    and SNMP 5-26
    and status 5-2
    and syslog 5-26
    and traffic reduction 5-7
    and VLAN data 5-17
    overview 5-1
    saving to CSV 5-4
restart process 6-7
retransmitted packets 5-15
RMON
    supporting 2-6
RMON1
    description 2-6
    See also RMON2.
RMON2
    configuring reports for 7-18
    description 2-6
    supported groups 2-7
    viewing reports 5-27, 7-18
RMON2 groups
    defined 2-7
round trip time
    specifying for WAN link 7-9

S

security
    setting PIN code for LCD 6-3
    setting Web UI password 6-1
service groups
    and local routers 7-8
    and web caches 7-8
    defined 7-8
service policies
    and Application QoS Policy 2-4
    and IT service 8-1
settings
    creating backup file for 6-9
    restoring from backup 6-10
shut down process 6-7

Simple Network Management Protocol. See SNMP.
size
of application buffer 7-9
of queue for outgoing packets 7-9
snapshot of system 5-10
SNMP
access to reports 6-4
and MIB 2-5
and system information B-1
configuring reports for 7-18
description 2-5
Ethernet cards information B-2
MIB B-3
viewing reports 5-26
SNMP reports
viewing 7-18
static routes, specifying 7-17
Status report 5-2
stylistic conventions 1-2
subnets
adding on a local WANJet appliance 7-1
adding on a remote WANJet appliance 7-2
adding to a WAN link 8-6
editing on a local WANJet appliance 7-1
editing or removing from a WAN link 8-7
removing from a local WANJet appliance 7-1
support
downloading diagnostics
diagnostics
and logs 5-25
synchronizing time 6-6
syslog
and event messages 2-7
and reports 5-26
configuration reports for 7-18
description 2-7
supporting 2-7
viewing reports 7-18
syslog servers 2-7
System Log protocol. See syslog.
system snapshot 5-10, 5-25

T

TCP/UDP ports
setting default processing mode 7-5
time
setting 6-5
setting manually 6-6
time management 6-5
time server, to synchronize 6-6
time zone
setting 6-5
topology
and operational mode setting 7-7
ToS
assigning priorities to data traffic 2-4
traffic
setting priority 2-4
traffic optimized report 5-7
transparent proxy 3-2
troubleshooting
testing connectivity 4-9
tuning
specifying bandwidth and RTT for WAN link 7-9
Type of Service. See ToS.

U

upgrading software 6-10

V

version, upgrading 6-10
VLAN
and report data 5-17
defining to local 7-12

W

WAN
setting bandwidth size 7-9
WAN link
adding 8-5
adding subnets 8-6
editing or removing 8-5
purpose 8-5
setting bandwidth size 7-9
WAN Optimizer
errors A-1
WANJet Dashboard, description 4-3
WANJet Private MIB file B-3
WCCP v2 protocol 3-3
Web 1-2
web caches
and service groups 7-8
Web UI
description 4-1
granting access 6-4
setting password 6-1
using menu 4-2
viewing screens 4-2