WANJet® Appliance Administrator Guide

version 5.0

MAN-0229-02

Product Version

This manual applies to product version 5.0 of the WANJet® appliance.

Publication Date

This manual was published on October 5, 2007.

Legal Notices

Copyright

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

Trademarks

F5, F5 Networks, the F5 logo, BIG-IP, 3-DNS, iControl, Internet Control Architecture, IP Application Switch, iRules, OneConnect, Packet Velocity, SYN Check, Control Your World, ZoneRunner, uRoam, FirePass, TrafficShield, Swan, WANJet, WebAccelerator, Transparent Data Reduction, TDR, and TMOS are registered trademarks or trademarks, and Ask F5 is a service mark, of F5 Networks, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. F5 Networks' trademarks may not be used in connection with any product or service except as permitted in writing by F5.

Patents

This product protected by U.S. Patents 6,327,242 and 7,126,955. Other patents pending.

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

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

2

Installing WANJet Appliances

3

Beginning to Configure WANJet Appliances

4
Using the Configuration Utility

5
Managing WANJet Appliances

6
Managing Administrative Accounts

7
Configuring WANJet Appliance Policies

8
Configuring Advanced Settings

9
Configuring Interfaces, Routes, and System Services

10
Configuring SNMP

11

Saving and Restoring Configuration Data

12

Monitoring the WANJet Appliance

13

Logging WANJet Appliance System Events

14
Working from the Command Line

A
Reviewing WANJet Appliance Messages

B
Configuration Examples

C
WANJet Appliance Private MIB File

D
RMON Tree

E
Console Cable Replacement

Glossary

Index

1

Introducing the WANJet Appliance

- Overview of the WANJet appliance
- Reviewing WANJet appliance features
- About this guide
- Stylistic conventions in this guide
- Finding additional information and technical support

Overview of the WANJet appliance

F5® Networks WANJet® appliance increases distributed application performance by optimizing, thus reducing, the amount of data that is transferred over the WAN. As a result, the WANJet appliance accelerates applications, such as file transfer, email, client-server applications, and data replication, resulting in increased performance for all WAN users.

Various WANJet hardware platforms are available for corporations, data centers, and branch offices. WANJet platforms scale from branch office to data center appliances, and optimize from 2,000 up to 20,000 connections. WANJet appliances feature fault tolerance, and work transparently across all wide-area networks, including dedicated links, frame relays, and satellite connections.

Operating at Layer 5 of the OSI reference model, the WANJet appliance can gather application knowledge, analyze data streams, and determine how to optimize the data most efficiently. The WANJet appliance incorporates technologies including Transparent Data Reduction (TDR), adaptive TCP optimization, Application QoS (traffic shaping), and site-to-site encryption.

TDR technology reduces the amount of bandwidth that repeated data transfers consume across a WAN link, and compresses the data. Adaptive TCP optimization enables the WANJet appliance to adapt to the characteristics of WAN links, and then to accelerate application traffic. Application QoS policies let you assign more bandwidth to critical network traffic. The WANJet appliance uses SSL encryption to protect the traffic moving from site to site.

Reviewing WANJet appliance features

These crucial features of the WANJet appliance are described on the following pages.

- TCP optimization
- Transparent Data Reduction (TDR)
- Application QoS
- Simple Network Management Protocol (SNMP) support
- Connection Intercept
- WANJet appliance bridging
- Fail-to-wire and fail close
- Peer port
- Centralized management using Enterprise Manager

Introducing TCP optimization

The WANJet appliance employs adaptive TCP optimization to speed up traffic by fully using available bandwidth over the WAN. ***TCP optimization*** includes techniques such as session-level application awareness, persistent tunnels, selective acknowledgements, error correction, and optimized TCP windows. These techniques enable the WANJet appliance to adapt, in real time, to the latency, packet loss, and congestion characteristics of WAN links, and accelerate virtually all application traffic.

Understanding optimization: Transparent Data Reduction

F5 Networks' Transparent Data Reduction (TDR) technology dramatically reduces the amount of bandwidth consumed across a WAN link for repeated data transfers. For example, without TDR, a 1 MB file transferred across a WAN link by 100 different users would consume 100 MB of bandwidth. With TDR, the same transfer would consume less than 10 MB 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.

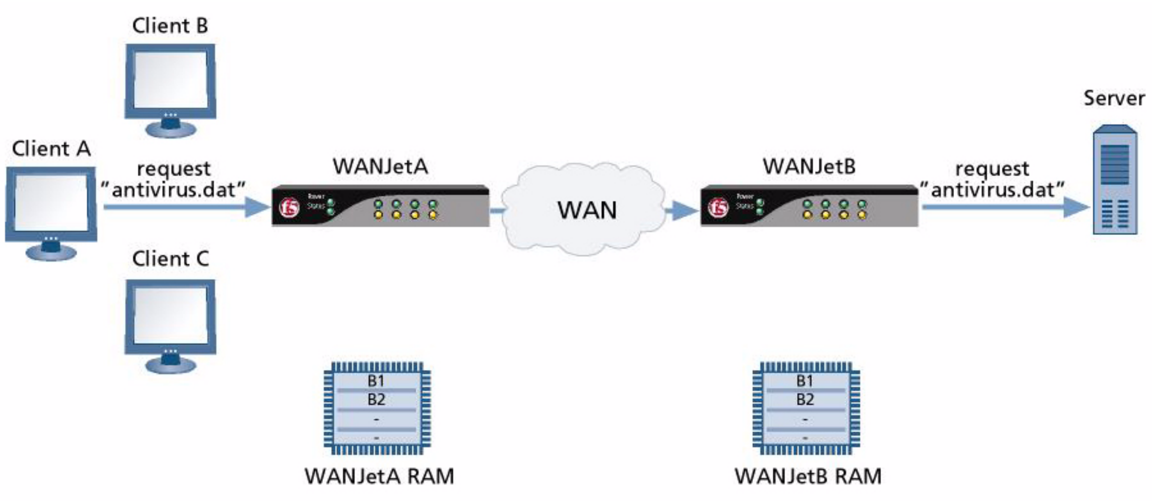
The WANJet appliance implements TDR technology as a two-stage compression process to maximize bandwidth savings while minimizing processing latency. The first step of the process, called ***TDR-2***, examines the transmitted data to determine if any part of it has been previously sent. If so, the WANJet appliance replaces the previously transmitted data with references. The second step, called ***TDR-1***, further compresses the data through the use of dictionary-based compression and advanced encoding schemes.

Using TDR-2: Repeat transfer data reduction

TDR-2 data reduction routines identify and remove all repetitive data patterns on the WAN. As data flows through the two WANJet appliances, each one records the byte patterns and builds a synchronized dictionary. If an identical pattern of bytes traverses the WAN more than once, the WANJet appliance nearest the sender replaces the byte pattern with a reference to it, compressing the data. When the reference reaches the remote WANJet appliance, it replaces the reference with the data, restoring the data to its original format.

Following is an illustrated example of how TDR-2 works.

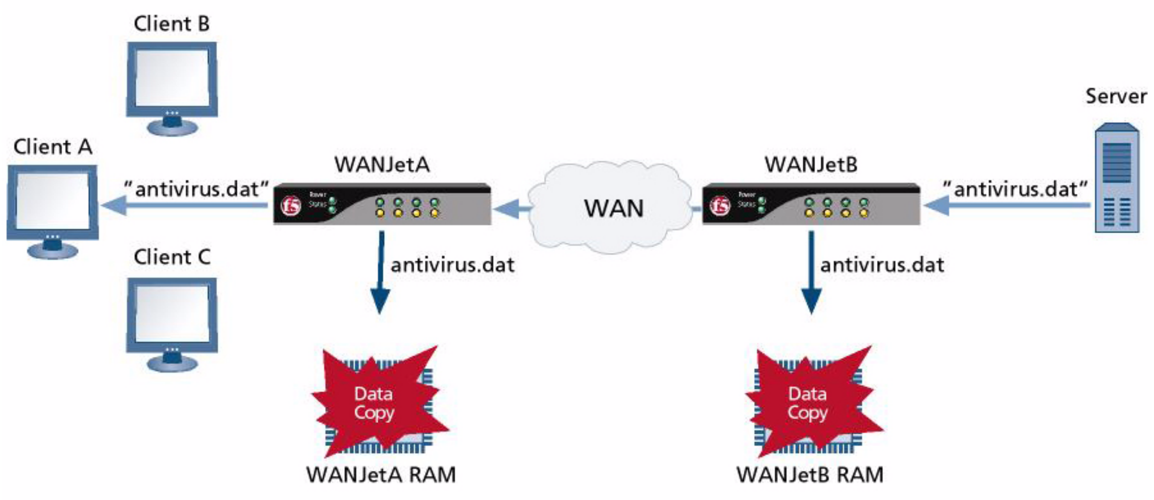
In Figure 1.1, Client A requests a file named **antivirus.dat**.



Note: *Systems with hard disks enabled store data on disk rather than RAM.*

Figure 1.1 *Client requests a file*

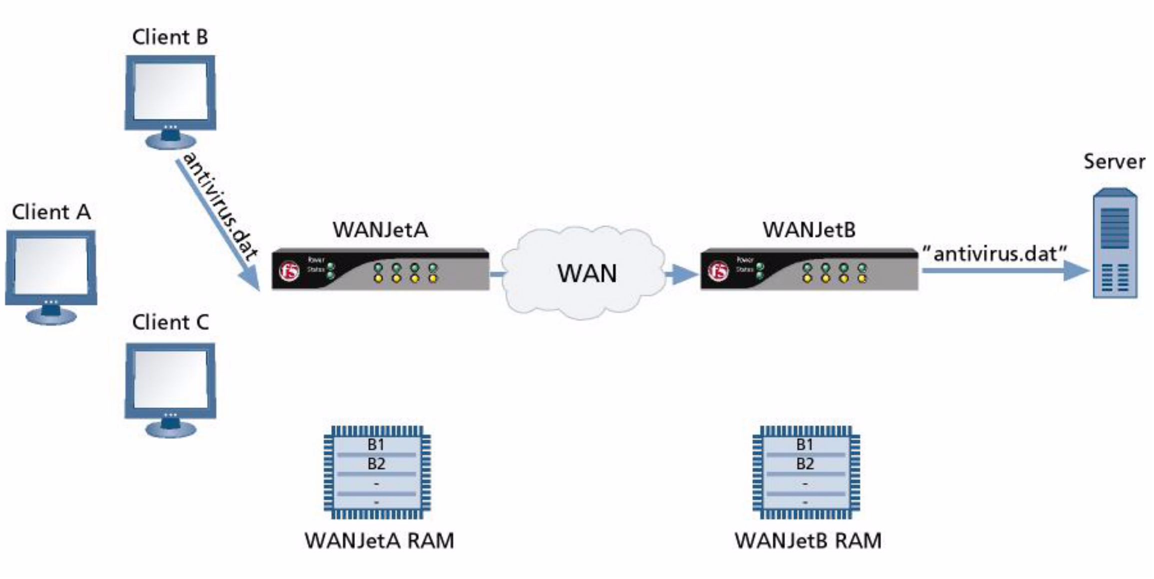
In Figure 1.2, the server on which the file is stored returns the **antivirus.dat** file. WANJetA and WANJetB copy the data to RAM or onto disk, for systems that include hard disk drives.



Note: *Systems with hard disks enabled store data on disk rather than RAM.*

Figure 1.2 *Server returns the file*

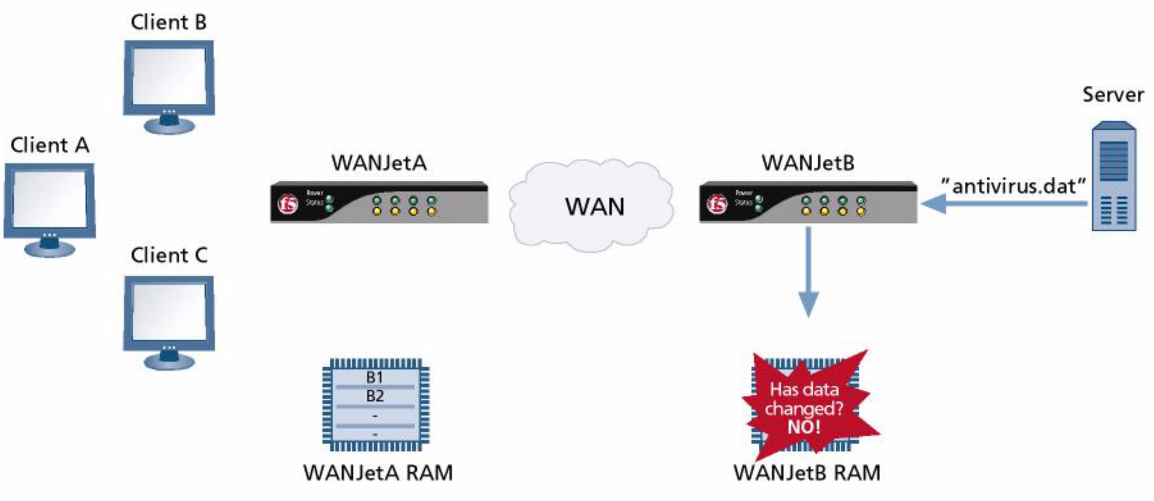
In Figure 1.3, Client B requests the same **antivirus.dat** file.



Note: *Systems with hard disks enabled store data on disk rather than RAM.*

Figure 1.3 *Second client requests the same file*

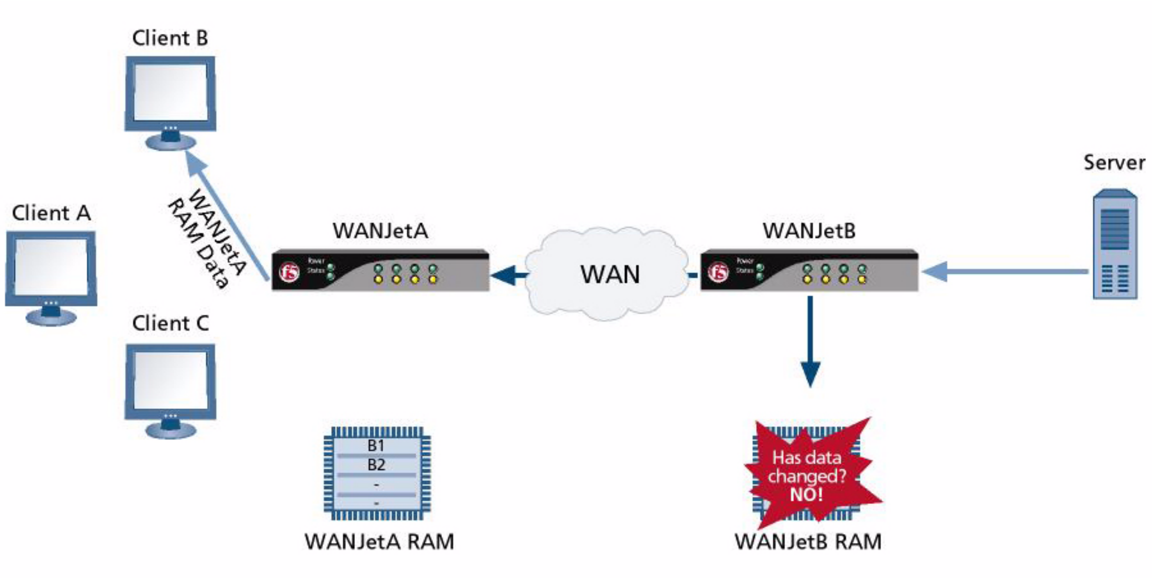
In Figure 1.4, WANJetB compares the **antivirus.dat** file with the data stored on RAM or disk to see if the data has changed, confirming that the data is still current.



Note: *Systems with hard disks enabled store data on disk rather than RAM.*

Figure 1.4 *WANJetB compares the file to the file stored on RAM or disk*

Finally, in Figure 1.5, WANJetB sends a message to WANJetA to use the local data instead of resending the file, because the data has not changed. WANJetA sends Client B the **antivirus.dat** file from its local RAM or disk drive, saving bandwidth over the WAN.



Note: *Systems with hard disks enabled store data on disk rather than RAM.*

Figure 1.5 *WANJetA sends file from RAM or disk*

Using TDR-1: First transfer data reduction and networking adaptivity

After TDR-2 has removed all previously transferred byte patterns, the WANJet appliance applies a second level of data reduction routines called TDR-1. While TDR-2 compression focuses on repeat transfer performance, ***TDR-1*** improves first transfer performance by examining smaller repetitive patterns and, at the same time, by adapting to changing networking conditions and application requirements.

During periods of high congestion, TDR-1 increases compression levels to reduce congestion and networking queuing delay. During periods of low congestion, TDR-1 reduces compression levels to minimize compression-induced latency. The adaptive nature of TDR-1 ensures that the appropriate compression strategy is applied without degrading application performance.

TDR-1 compresses the remaining network data through intelligent network and application-aware routines that encode the remaining data in as few bytes as possible, improving performance for WAN users.

Applying traffic shaping: Application QoS

Application QoS (Quality of Service) is a form of traffic shaping that provides better service for specific data flows by raising the priority of a particular type of traffic and limiting the priority of other traffic. Accordingly, 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.

You can also create a named group of ports, systems, and subnets, called a ***traffic class***. You can then apply an Application QoS policy to that traffic class, treating this type of traffic as one entity.

See *Creating Application QoS policies*, on page 7-9 for information on how to add, edit, or remove Application QoS policies.

Using Simple Network Management Protocol (SNMP)

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). An ***SNMP trap*** provides notification of a significant event (such as a power outage, an error, a fault, or a security violation) that occurred on the network.

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 *WAN optimization messages and codes*, on page A-2 for error codes and descriptions.

The WANJet appliance also stores more detailed SNMP reports that you can access using SNMP-compliant software. For the SNMP-compliant software to access the WANJet appliance, it should authenticate itself using a community string you specify. The machine on which the SNMP-compliant software resides should have access to the SNMP data on the WANJet appliance.

Figure 1.6 illustrates the interaction between the WANJet appliance and the SNMP traps.

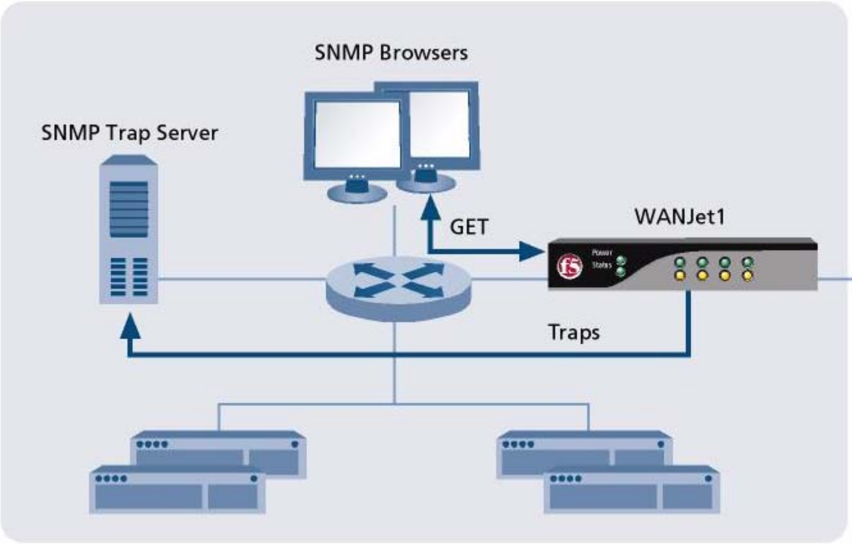


Figure 1.6 WANJet appliance and SNMP data

The Management Information Base (MIB) 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 appliance such as total bandwidth saved for sent data and for received data.

For more information about configuring SNMP settings, see *Enabling RMON2 logs*, on page 12-22.

Including Remote Monitoring support

Remote Monitoring (RMON) is an extension to SNMP that provides comprehensive network monitoring capabilities. It is a network management protocol that monitors different types of data traffic passing through the network. Unlike SNMP, RMON can gather network data from multiple types of MIBs. Thus, RMON 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 is the Remote Network Monitoring MIB that was developed so that network administrators could see the traffic and collect information about remote network segments for troubleshooting and performance monitoring. RMON1 focuses on Layer 1 and Layer 2 of the OSI model.

RMON2 is an extension of RMON1 that includes open, comprehensive network fault diagnosis, planning, and performance-tuning features. In addition, RMON2 includes monitoring of packets on the higher layers of the OSI model, from Layer 3 to Layer 6. Therefore, RMON2 provides data about traffic on network layers for network and application monitoring. Figure 1.7 shows how the WANJet appliance works with RMON2 technology.

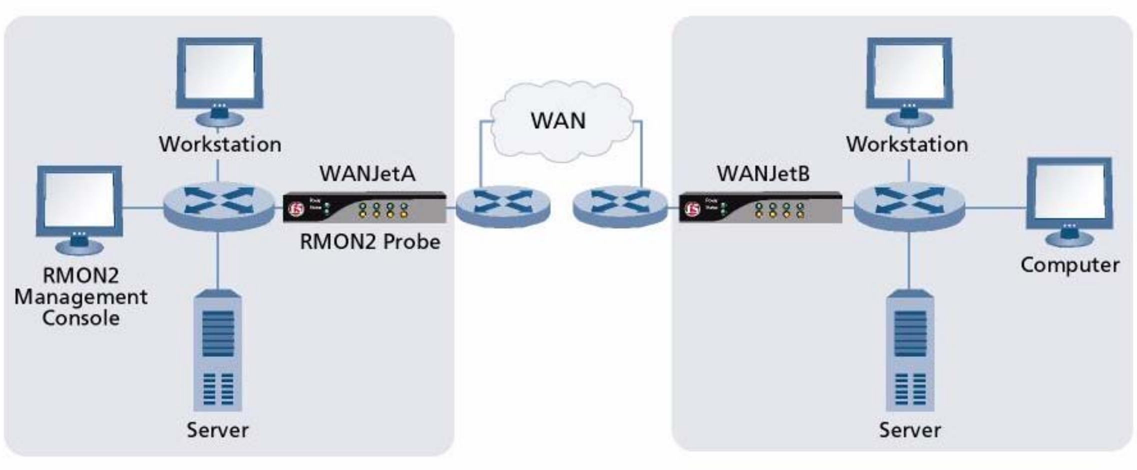


Figure 1.7 *WANJet appliance and RMON2*

The WANJet appliance supports RMON2. RMON2 helps administrators gather and analyze detailed information about network traffic, before or after the WANJet appliance processes it. This information includes:

- Data sent and received between two nodes
- IP addresses of the nodes
- Port used to send and receive data
- Data size before and after the WANJet appliance processes the traffic
- Time stamp
- Number of connections

The WANJet appliance supports the RMON2 groups listed in Table 1.1.

RMON2 group	Description
Protocol Directory	Provides a way for an RMON2 application to determine a list of protocols for which the WANJet appliance monitors and maintains statistics.
Network Layer Matrix	Stores and retrieves network layer (IP layer) statistics for conversations between pairs of network addresses.
Application Layer Matrix	Stores and retrieves application layer statistics for conversations between pairs of network layer addresses.

Table 1.1 *Supported RMON2 groups*

To see where these RMON2 groups fit into the MIB tree, see Appendix D, *RMON Tree*. For more information about configuring RMON2, see *Enabling RMON2 logs*, on page 12-22.

Resetting connections with Connection Intercept

When you start the WANJet appliance, some connections may have already been established. ***Connection Intercept (CI)*** intercepts and resets connections that were initiated before the WANJet appliance became active on the network. If set, the WANJet appliance resets then optimizes existing connections. As usual, the WANJet appliance optimizes new connections starting after the appliance is up and running.

Connection Intercept causes the WANJet appliance to reset connections that were initiated before it started up. You can use Connection Intercept to reset connections for specific ports or services, without having to reboot the relevant servers or restart those services.

The Connection Intercept option impacts system behavior when performing the following tasks:

- 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

You can enable Connection Intercept for specific services or ports when creating optimization policies. The ports on which you implement Connection Intercept require the following settings:

- **Optimized** as the processing mode
- **Connection Intercept** option enabled

For details on how to enable Connection Intercept for an optimization policy, see *Creating optimization policies*, on page 7-2.

Introducing WANJet appliance bridging

When deployed in an inline configuration (LAN and WAN ports connected), the WANJet appliance acts as a Layer 2 bridge for network traffic that is not configured for WAN optimization. Ethernet frames with unoptimized traffic are bridged between the LAN and WAN interfaces.

The ability to act as a bridge for traffic that is not optimized allows the WANJet appliance to be incorporated into redundant network topologies and to support the high-availability features of other network devices. Protocols such as the Address Resolution Protocol (ARP), the Spanning Tree Protocol (STP), the Virtual Router Redundancy Protocol (VRRP) and the Hot Standby Redundancy Protocol (HSRP) function normally in the presence of a WANJet appliance.

Redundancy protocols typically create a shared Virtual IP address (VIP). The VIP is the default gateway for the hosts on the LAN. One router uses the VIP to actively pass traffic, while the other router acts as a standby. The redundancy protocol sends multicast packets between the active and standby routers to indicate that the active router is healthy and continues to pass traffic. These packets are bridged through the active router's WANJet appliance and LAN switches, and bridged back through the peer WANJet appliance to the standby router.

If a failure in a network component (other than the WANJet appliance) prevents the multicast packets from reaching the standby router, the standby router becomes the active router by sending out an ARP packet indicating that it now owns the VIP (this process is often called gratuitous ARP). The gratuitous ARP packet is a Layer 2 broadcast packet, which is bridged by the WANJet appliance to the LAN hosts. LAN hosts then begin using the new router (but with the same IP address, namely the VIP) as their default gateway to send traffic to other networks.

WANJet appliances themselves can use the VIP as their default gateway IP address. If WANJet appliances connect directly from their WAN ports to their routers, both WANJet appliances must use the non-virtual IP address of their connected router's interface.

To use the VIP as the WANJet appliances' default gateway (to achieve redundant default gateways for the WANJet appliances), both of the WANJet appliance WAN ports must connect to switches or other Layer 2 devices that then connect to both routers. Depending on the details of the topology and configuration of your Layer 2 devices and routers, this may introduce Layer 2 loops that require resolution through the Spanning Tree Protocol or other means.

Maintaining network connectivity with the fail-to-wire feature

A core feature of the WANJet appliance is its fail-to-wire feature (set by default). ***Fail-to-wire*** functionality guarantees that a failure of a WANJet appliance does not block data traveling between the LAN and WAN ports when the WANJet appliance is deployed in an inline topology (as opposed to one-armed topology). When a failure in WANJet appliance occurs, the WANJet appliance network interface hardware opens a path that connects the LAN and WAN ports directly.

A WANJet appliance in fail-to-wire state acts effectively as a patch panel connecting two Ethernet cables. In the event of a WANJet appliance failure, data continues to flow between the two connected devices (such as switches, routers, or another WANJet appliance) on either side of the WANJet appliance. By allowing data to pass between connected devices in this manner, WANJet appliance failure does not result in the loss of network connectivity for clients, servers, and other networking devices.

Fail-to-wire occurs regardless of the type of failure in the WANJet appliance, including software bugs, hardware bugs, or hardware failures in components, such as memory chips or hard disks (except physical damage to the WANJet appliance's fail-to-wire hardware components), and loss of power to the WANJet appliance.

The fail-to-wire feature requires that the Ethernet parameters (that is, duplex and speed) of the connected devices' network interfaces are the same, as they would be if cabled directly together.

Setting the correct duplex and speed

You must set the duplex and speed appropriately for the ports on the connected devices. F5 Networks recommends configuring the WANJet appliance interfaces and the interfaces of connected devices to auto-negotiate duplex and speed (**auto** is the default value for interfaces on the WANJet appliance). If you need to change the interface to a value other than **auto**, refer to *Configuring interfaces*, on page 9-1.

After you configure the interfaces to auto-negotiate duplex and speed, F5 Network recommends checking the Diagnostics report (see *Viewing Diagnostic reports*, on page 12-11) to determine whether both the LAN and WAN interfaces have auto-negotiated the same settings. If so, fail-to-wire will work correctly in case of failure. If duplex, speed, or both settings have different values, you need to manually set the parameters on all devices to the same values.

Using the correct cable type

Cabling two network devices together may require use of an Ethernet cable with standard wiring (often called a straight-through cable), or may require an Ethernet cable with pinouts 1, 2, 3, and 6 of one connector wired to pinouts 3, 6, 1, and 2 (respectively) of the connector on the other end (often called a crossover cable). The WANJet appliance Gigabit Ethernet network interfaces can automatically sense which cable type is present (auto-sensing MDI/MDI-X), so during normal operation cable type should not be an issue.

However, in fail-to-wire mode, the effective cable type (that is, the combination of the two cable types) may or may not be appropriate for the two connected devices. As per the Gigabit Ethernet specification, Gigabit Ethernet network interfaces perform auto-sensing of the crossover cable, and configure themselves appropriately. If one or both devices possess Gigabit Ethernet interfaces, you can use any combination of the two cable types for the two cables connected to the WANJet appliance. If neither connected device possesses a Gigabit Ethernet network interface, you must choose the cable type based on the type of devices that effectively connect during fail-to-wire mode.

Rerouting traffic with the fail close feature

An alternative configuration to fail-to-wire exists on the WANJet 400. You can configure the WANJet 400 to ***fail close***, which breaks the connectivity between connected devices. You can implement this option, for example, if you want to create a redundant network architecture in which all traffic is routed to the peer WANJet appliance when a WANJet appliance failure occurs.

When used with the redundancy features of the other network components, fail close can prevent the creation of an unoptimized path through the network. Fail close requires a hardware modification. Refer to *To enable Fail Close on WANJet 400 hardware*, on page 8-5 for instructions.

An alternate setup exists if you cannot use fail close, but requirements do not permit a path in the network that does not have optimization, You can use the router connected to the WAN port to perform policy-based routing of unoptimized traffic, directing it to the active peer WANJet appliance for optimization. Consult the documentation for your routing device, and contact F5 Networks Support for additional information on high-availability configuration of WANJet appliances with policy routing.

Setting up redundant peers

The WANJet appliance supports ***redundant peers***, where two WANJet appliances in the same subnet communicate with each other. Every WANJet appliance model has an Ethernet port labeled **Peer**. You connect the peer ports of two WANJet appliances to set up redundant peers. If connected directly to each other, use a crossover cable; if connected through a switch, use an Ethernet cable.

The peer network provides an alternate path for network traffic that is being optimized by a given WANJet appliance, but due to a failure in the network the normal path to the WANJet appliance is not available. When a failure on the network prevents traffic from reaching a WANJet appliance, redundant paths in a network should permit this traffic to take a path to the peer WANJet appliance.

Instead of passing state information, the WANJet appliance updates the redundant peer when it accepts a connection for optimization. Each WANJet appliance keeps a list of the connections being optimized by its peer. When a WANJet appliance accepts a new connection for optimization, it sends a message to the peer. The peer then adds the connection to its list. After an optimized connection has ended, the WANJet appliance also sends a message to the peer to remove the connection entry from its list.

For more information on connecting WANJet appliances through the Peer port, see *Configuring redundant peers*, on page 8-10.

Managing WANJet appliances using Enterprise Manager

You can deploy and manage multiple WANJet appliances from the Enterprise Manager, a centralized management solution. You need to have purchased and set up Enterprise Manager, which is a separate product from the WANJet appliance. For on setting up and using Enterprise Manager, refer to the Enterprise Manager documentation available on the Ask F5^{SM} Knowledge Base web site, **http://support.f5.com**.

About this guide

This guide describes how to configure 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
- Creating optimization policies
- Creating Application QoS policies and traffic classes
- Performing advanced configuration tasks
- Configuring interfaces, routes, and system services
- Configuring SNMP
- Saving and restoring configuration data
- Monitoring the WANJet appliance’s performance
- Logging WANJet system events
- Working from the command line

Stylistic conventions in this guide

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

Using the solution examples

All examples in this documentation use only private class IP addresses. When you set up the solutions we describe, you must use valid 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.

For example, 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 ***Configuration utility***.

Identifying references to objects, names, and commands

We apply bold formatting 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 log in to the WANJet appliance.

Identifying references to other documents

We use italic text to denote a reference to a specific section, or another document. In references where we provide the name of a book as well as a specific chapter or section in the book, we show the book name in bold, italic text, and the chapter/section name in italic text to help quickly differentiate the two.

For example, see Chapter 6, *Reviewing Hardware Specifications,* in the ***Platform Guide: WANJet® 500*** for details about the WANJet 500 appliance.

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.

For example, the following command traces the route from the WANJet appliance you are working on to the device at IP address **10.1.102.204**:

```
traceroute -v 10.1.102.204
```

Table 1.2 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 1.2 *Command line conventions used in this manual*

Finding additional information and technical support

In addition to this guide, there are other sources of documentation that you can use to work with the WANJet appliance. The information is available in the guides and documents described below.

- ***WANJet® Appliance Quick Start Card***
  The WANJet platform includes a printed ***Quick Start Card*** written for the specific platform that you purchased. It provides basic instructions for a quick setup and initial configuration of the hardware you purchased.

- ***Platform Guide: WANJet® 300***
  This guide describes the WANJet 300 platform, and includes detailed instructions on how to install the WANJet 300.

- ***Platform Guide: WANJet® 500***
  This guide describes the WANJet 500 platform, and includes detailed instructions on how to install the WANJet 500.

- **Online help**
  Context-sensitive online help provides basic information for each screen in the Configuration utility.

In addition to the documentation included with the platform, you can find additional technical documentation by using the following resources.

- **Ask F5^{SM} Customer Support web site**
  The Ask F5 Customer Support web site, **http://support.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
  - Ask F5^{SM} Knowledge Base

◆ **Note**

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

2

Installing WANJet Appliances

- Deploying WANJet appliances
- Reviewing firewall guidelines
- Installing the hardware
- Site information worksheet

Deploying WANJet appliances

This chapter provides conceptual guidelines concerning WANJet appliance installation and configuration. The Quick Start Card included in the shipping box with your WANJet appliance provides the initial hardware installation and setup instructions. You can also find the Quick Start Card on the Ask F5^{SM} Knowledge Base web site, **http://support.f5.com**.

There are two primary ways to deploy a WANJet appliance within a corporate network:

- ◆ Inline deployment, using one of the following configurations:
    - Point-to-point
    - Point-to-multi-point
    - Mesh
- ◆ One-arm deployment, as a transparent proxy

An alternate inline configuration is also possible. The way you choose to deploy the WANJet appliance depends on your current network topology and requirements.

For examples, including illustrations, of basic, mesh, hub and spoke, redundant system, and LAN router configurations, refer to Appendix B, *Configuration Examples*.

Deploying inline

Inline deployment is the most common way to deploy WANJet appliances. In this configuration, you place WANJet appliances directly in the path of traffic, or ***inline***, between a WAN router and LAN switch.

You can scale inline deployment from a simple point-to-point configuration to a more complex point-to-multi-point configuration.

Creating a point-to-point configuration

Point-to-point configuration is a simple one-to-one topology where you place WANJet appliances at each end of the WAN between their respective WAN routers and LAN switches.

Each WANJet appliance is configured to search for traffic that matches specified source and destination subnets, and ports. If the local WANJet appliance detects a match, it processes the traffic and sends it through a tunnel to the remote WANJet appliance, which, in turn, reverses the process and delivers the packets exactly as they originally were. If there is no match, the local WANJet appliance acts as a bridge, and passes the packets unaltered to the WAN.

Figure 2.1 shows inline deployment with two WANJet appliances in a point-to-point configuration, connecting a corporate data center and one remote office.

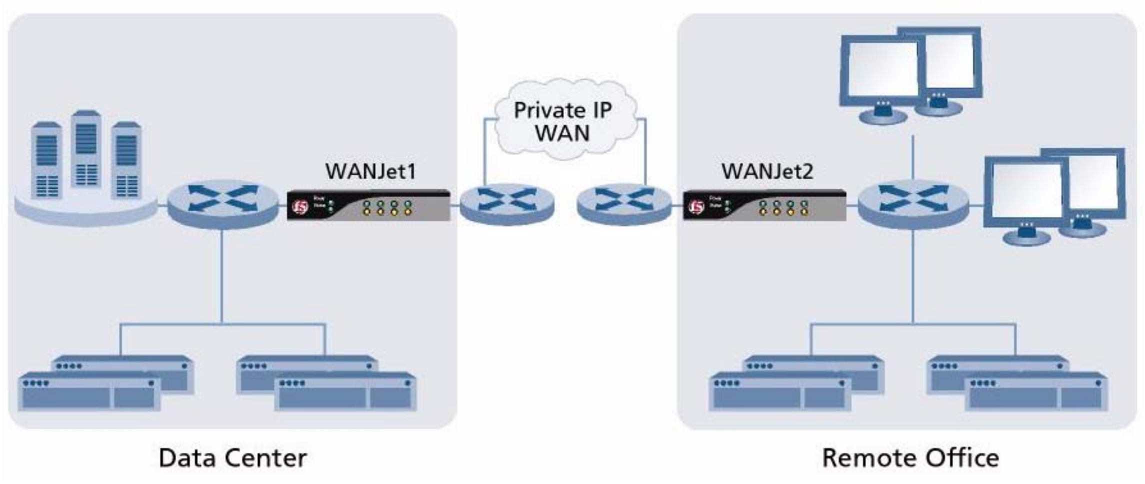


Figure 2.1 Inline deployment in point-to-point configuration

Refer to *Basic point-to-point configuration*, on page B-1, for a more detailed example of this configuration.

Creating a point-to-multipoint configuration

Point-to-multipoint configuration is more complex and involves three or more WANJet appliances. Figure 2.2 illustrates a point-to-multipoint deployment that consists of five appliances that connect 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 ports, and then delivers the traffic across the WAN through a tunnel to the appropriate WANJet appliance.

In this configuration (also called hub and spoke), one appliance is set up as the hub with the four other appliances as remote appliances on the hub. But each of the remote appliances points only to one remote appliance, the hub. If in Figure 2.2 WANJet1 is configured as the hub, WANJet2, WANJet3, WANJet4, and WANJet5 are remote appliances on WANJet1. On WANJet2, WANJet3, WANJet4, and WANJet5, only WANJet1 is configured as a remote appliance.

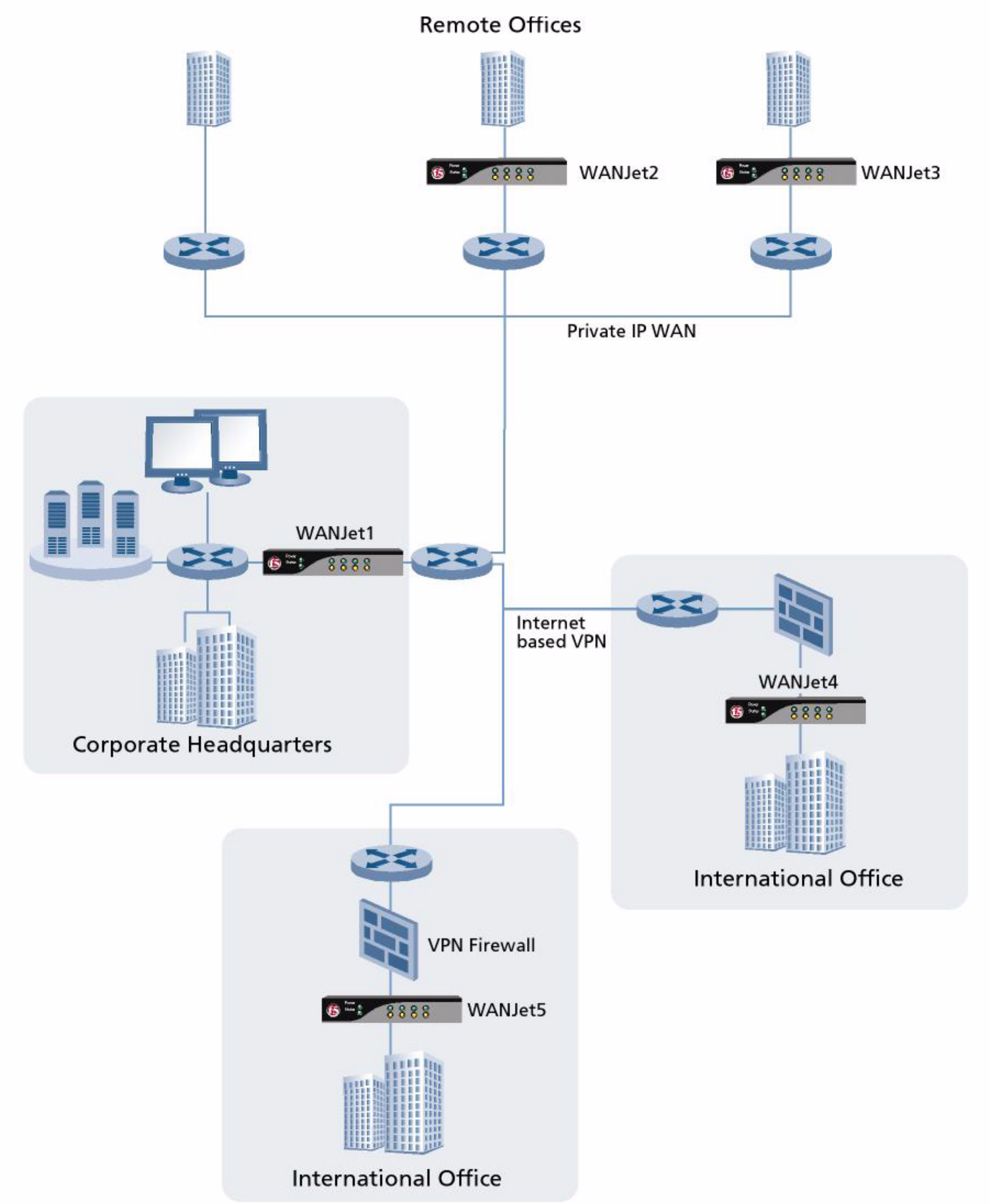


Figure 2.2 *Inline deployment in a point-to-multi-point configuration*

Creating a mesh configuration

Mesh configuration also involves three or more WANJet appliances. In this configuration, you configure all other appliances as remote appliances. If a mesh configuration were shown in Figure 2.2, WANJet1 would have WANJet2, WANJet3, WANJet4, and WANJet5 configured as remote appliances. WANJet2 would have WANJet1, WANJet3, WANJet4, and WANJet5 configured as remote appliances, and so on.

Refer to *Mesh configuration*, on page B-3 for an example of this configuration.

Using an alternate inline configuration

Additionally, there is another way to configure WANJet appliances as redundant peers inline. You can deploy two WANJet appliances in sequence (with the WAN port of one connecting to the LAN port of the second). You configure both to optimize the same network traffic. The WANJet appliance closer to the clients or servers performs the optimizations, while the WANJet appliance behind it bridges all traffic.

If the optimizing WANJet appliance fails in this configuration, the fail-to-wire feature passes unoptimized traffic to the second WANJet appliance, which performs the optimization. A sequential redundant system setup like this one eliminates the potential drawback to the basic inline topology, that a WANJet appliance in the fail-to-wire state can create a network path with no optimization. This type of sequential redundant system setup is attractive when the network topology itself does not contain redundant paths (often the case with a branch office network), but you want redundancy of WANJet appliances.

Deploying in a one-arm configuration

In certain cases, it is not desirable or even possible to deploy the WANJet appliance inline. For example, in the case of a collapsed backbone where the WAN router and LAN switch are in one physical device, you may not be able to deploy the WANJet appliance inline.

If you would prefer not to deploy the WANJet appliance inline, you can use ***one-arm deployment***. In this deployment, the WANJet appliance has a single (hence the term ***one-arm***) connection to the WAN router (or LAN switch) and has all relevant traffic redirected to it by the WAN router (or switch). Figure 2.3 shows a simple one-arm deployment in a corporation that has two networks. Network 1 includes the servers, and network 2 is where the clients are located.

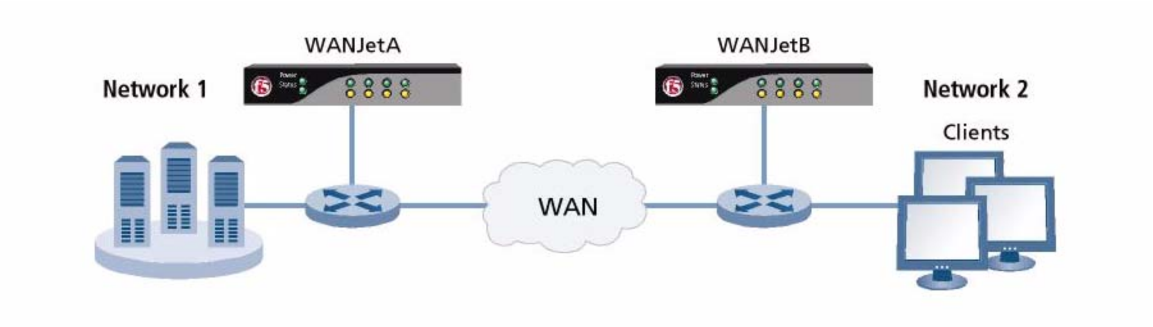


Figure 2.3 *One-arm deployment of WANJet appliance*

Figure 2.4 shows the basic topology and traffic flow for a one-arm deployment.

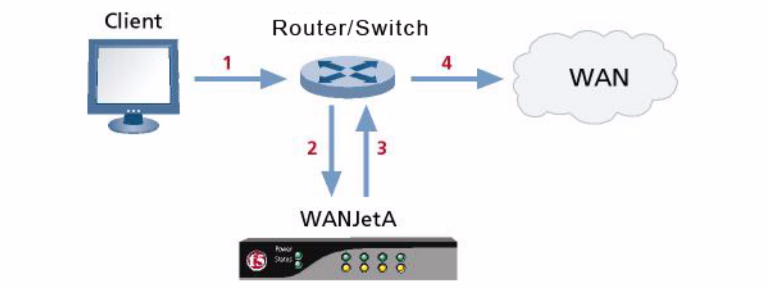


Figure 2.4 One-arm topology and traffic flow

The traffic flow sequence shown in Figure 2.4 is as follows.

- **Step 1:** The client initiates a session.
- **Step 2:** A WAN router redirects traffic to the WANJet appliance.
- **Step 3:** The WANJet appliance processes traffic and sends it back to the WAN router.
- **Step 4:** The WAN router forwards traffic across the WAN.

On the WANJet appliance, you set up one-arm deployment on the Operational Mode screen by selecting **One-arm** as the **Topology** setting. For more information on how to configure one-arm deployment, refer to *Configuring one-arm topology*, on page 8-11.

You deploy the WANJet appliance using a one-arm configuration as a transparent proxy. As the name implies, the transparent method is totally transparent on the network, and requires no modification to any client settings (such as the default gateway). However, you must reconfigure the WAN router.

When the WANJet appliance is deployed as a transparent proxy, it does not change the source IP address of traffic flowing through it. You need to configure nearby routers in your network to redirect traffic to the WANJet appliance by means of static routing.

You can also use policy-based routing to direct traffic to the WANJet appliances in a one-arm deployment. The devices performing policy-based routing may provide health-checking mechanisms to verify the routing through the WANJet appliances. For further information on policy-based routing scenarios, consult the documentation for your routing device, and contact F5 Networks support for additional information on configuration of WANJet appliances with policy routing.

Reviewing firewall guidelines

If the WANJet appliance is placed behind a firewall, you must open certain ports for the WANJet appliance to operate properly. Table 2.1 lists the ports that you must open to allow the traffic to pass through the firewall.

Port Number	Used for
22	A TCP port used for SSH.
53	A UDP port used for DNS.
161	A UDP port used for SNMP.
162	An optional UDP port used for SNMP traps.
443	A TCP or UDP port used for http protocol over TLS/SSL.
520	A TCP port used for the Extended File Name Server,
1026	A port used for Calendar Access Protocol.
3701	The default port that the WANJet appliance uses for managing connections.
3702	The default port that the WANJet appliance uses for TCP data tunnels.
4353	The port used for iQuery protocol.

Table 2.1 *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 you can ping the WANJet appliance.

Installing the hardware

See the Quick Start Card included in the shipping box for instructions on installing WANJet appliances and connecting them to your network. If you have a WANJet 500 or 300, refer also to the appropriate platform guide for additional details concerning hardware installation.

Site information worksheet

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

WANJet Appliance Site Information Worksheet

Site:	Name:		
	Address:		
	City:		
	State/Province, Country:		
Contact Person:	Name/Title:		
	Email:		
	Work phone:	Cell phone:	
Link:	Type:		
	Speed in Mb/s or Kb/s:		
	Latency:		
	Utilization %: Peak	Average	
Router:	Make:	Model:	
	IP address:		
	Routing protocols used:		
	Static routing table rules:		
Switch:	Make:	Model:	
	IP address:		
WANJet Appliance:	Alias:	IP address:	
	Subnet mask:	Management IP address:	
	Default gateway:		
Remote WANJet Appliance:	Alias:	IP address:	
	Subnet mask:	Management IP address:	
	Default gateway:		
Local Networks:	Alias:	IP address:	Subnet:
	Alias:	IP address:	Subnet:
	Alias:	IP address:	Subnet:
Remote Networks:	Alias:	IP address:	Subnet:
	Alias:	IP address:	Subnet:
	Alias:	IP address:	Subnet:
Additional Notes:			

Table 2.2 *Site information worksheet for the WANJet appliance*

3

Beginning to Configure WANJet Appliances

Overview of WANJet appliance configuration

You must set up 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 on to the Configuration utility remotely.

You can alternatively deploy and manage multiple WANJet appliances from the Enterprise Manager, a centralized management solution. You need to have purchased and set up Enterprise Manager, which is a separate product from the WANJet appliance.

WANJet appliances work in pairs to optimize the traffic that flows between them. A pair of WANJet appliances consists of a local WANJet appliance and a remote WANJet appliance, one on either side of a WAN link. A typical configuration might include one WANJet appliance in a data center where company servers reside, and a second WANJet appliance on the other side of the WAN in an office where employees work.

Figure 3.1 shows two WANJet appliances that are deployed in a point-to-point configuration.

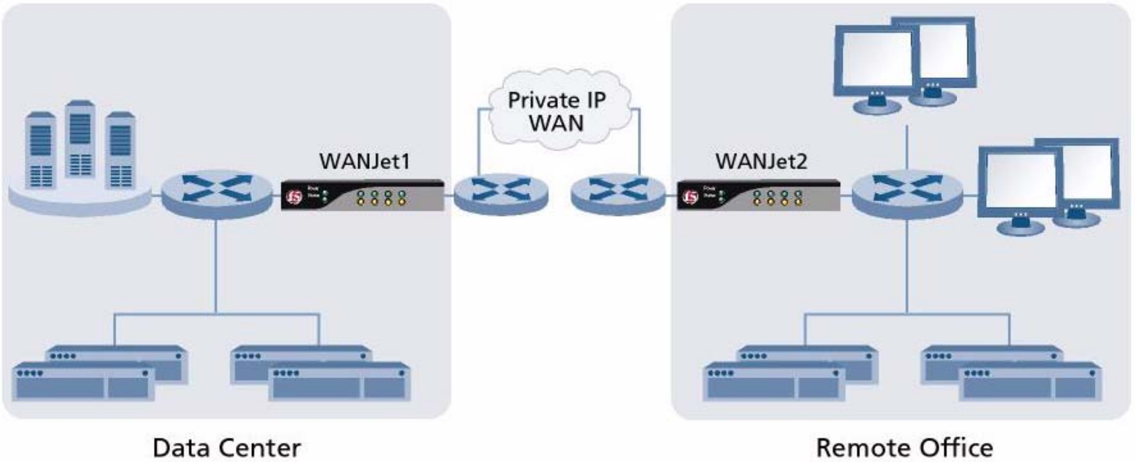


Figure 3.1 *Inline deployment in point-to-point configuration*

The WANJet appliances in this example are connected as follows:

- WANJet1 is in the data center and connects with local IP address **172.16.2.1**.
- WANJet2 is in a remote office and connects to the remote end of the private IP WAN link with IP address **10.2.0.1**.

For this example, basic WANJet appliance configuration includes the following steps:

- Logging on to the first WANJet appliance and running the Setup utility

- Defining the second WANJet appliance as a remote WANJet appliance on the first WANJet appliance
- Logging on to the second WANJet appliance and running the Setup utility
- Defining the first WANJet appliance as a remote WANJet appliance on the second WANJet appliance

It is this basic point-to-point configuration that is described in the remainder of this chapter. Refer to *Creating a point-to-point configuration*, on page 2-1, for more information on this configuration.

Before you configure

Before you can begin with initial configuration, you need to complete the following tasks:

- Install the WANJet appliance hardware
- Connect the cables to the network
- Configure the Management port IP address or bridge IP address

You use the Liquid Crystal Display (LCD) panel, a computer connected to the WANJet appliance's serial port, or a secure shell (SSH) to configure the Management port IP address, netmask and gateway or the WANJet IP (bridge IP) address, netmask, and gateway.

Basic installation is covered in the ***Quick Start Card*** that ships 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.

Configuring the first WANJet appliance

After you complete the initial hardware configuration, you can log on to the WANJet appliance using either the Management IP address or the WANJet IP (bridge IP) address. If you configured the Management port, you should use the Management port IP address to log on.

You can then set up the WANJet appliance using the browser-based interface, called the ***Configuration utility***. If using out-of-band management and the Management port, you can access the Configuration utility from any computer that is connected to the management network, and can run a web browser. If using the WANJet IP (bridge IP) address to log on, you can use any computer that can access the WANJet appliance and run a web browser.

The rest of this chapter describes how to log on to the system using the Configuration utility and perform the basic configuration required for the WANJet appliance to start processing traffic.

Logging on to the system

After you finish installing the WANJet appliance, you can log on and use the Configuration utility to administer the appliance and perform additional configuration. Refer to Chapter 4, *Using the Configuration Utility* for a description of the web-based interface.

You need to log on to the Configuration utility of each WANJet appliance to fully configure it (unless you are using Enterprise Manager for administration).

To log on to the Configuration utility

1. In a web browser, type:

   ```
   https://<Mgmt_IP_address>
   ```

   For example, if the Management IP address of the appliance is **192.168.168.102**, type **https://192.168.168.102** in the web browser. (If you do not have a management network, use the **WANJet IP** (bridge IP) address instead.)
   The Authentication Required screen opens where you can log on.

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).

3. Click **OK**.
   The first time you log on, the Setup Utility Welcome screen opens. If you have already completed the setup using the Setup utility, the Welcome screen opens.

Setting up the WANJet appliance

The first time you log on to the WANJet appliance, the Setup utility opens on the screen. This is where you need to configure basic settings.

To run the Setup utility the first time

1. When you log on to the system for the first time, a message tells you that you must complete the Setup utility. Click **Next**.
   The Setup Utility License screen opens.

2. To begin the licensing process, click **Activate**.
   Follow the onscreen prompts to license the system. For additional details, see *Activating the license*, on page 3-10.

3. Click **Next**.
   The Setup Utility Platform screen opens. This is where you specify base configuration information for managing the system.

4. Proceed based on what you configured.

    - If you configured the Management IP address, netmask, and gateway from the LCD, the **Management Port** settings are already filled in with the values you specified. Skip to the next step.

    - If you configured only the **WANJet IP** (bridge IP) address from the LCD, the **Management Port** settings are blank. However, you must still type an IP address and netmask (use fictitious ones) to proceed with the setup:

        a) **IP Address**: Specify a fictitious IP address for the Management port, for example, **1.1.1.1**.

        b) **Network Mask**: Specify a fictitious netmask for the Management port, for example, **255.255.255.255**.

        c) **Management Route**: Leave this setting blank.

    Note: *If you assign a fictitious IP address and netmask to the Management port, be certain that these addresses do not conflict with others in your network topology.*

5. For the **Host Name** setting, type a fully qualified domain name for the WANJet appliance. An example of a host name is **mywanjet.wanopt.net**.

6. For the **Host IP Address** setting, select one of the following settings:

    - **Use Management Port IP Address** to assign the Management port IP address to the host name. This is the default value, and is the correct value to use if you have configured the Management port.

    - **Custom Host IP Address** to assign a different IP address to the host name. A box opens where you can type the IP address. If you are not using the Management port, select this option and type the WANJet appliance IP address.

7. In the User Administration section, for the **Root Account** and **Admin Account**, type and confirm the passwords. By default, the **root** password is **default**, and the **admin** password is **admin**. We recommend that you change them.

8. Click **Next**.
    The Local WANJet appliance screen opens.

    Note: *If you configured the Bridge IP address, netmask, and WAN gateway from the LCD, values you specified are shown on the screen.*

9. In the **WANJet Alias** box, type a name for the WANJet appliance.

10. If you have not already configured the **WANJet IP**, **WANJet Netmask**, and **WAN Gateway**, you must configure them now. These values are required even if you configure the Management port.

11. In the **Lan Router** box, type the IP address of the LAN router (if your network configuration includes one) that resides between the WANJet appliance and the LAN. The LAN router must be in the same subnet as the WANJet appliance. This setting is optional.
12. Click **Save**.
    The WANJet appliance saves the settings, closes the Setup utility, and opens the Welcome screen. You can now continue with basic configuration.
13. In the navigation pane, expand **WAN Optimization** and click **Operational Mode**.
14. Make sure that **Mode** is set to **Active**.
15. If you activated the license for the first time, you need to reboot the WANJet appliance. Refer to *Shutting down and restarting the WANJet appliance*, on page 5-16.

Configuring multiple subnets

If your local area network has multiple subnets connected through a router, you need to configure the local router IP address and add the local subnets that you want to optimize on the WANJet appliance. If your network configuration uses a LAN router, you need to add subnets behind that router for which you want the WANJet appliance to optimize traffic.

Once the WAN link between the WANJet appliance pair is up, subnet specifications are automatically exchanged between the appliances. So, for example, the local subnets you configure on WANJet1 appear as remote subnets on WANJet2, and local subnets on WANJet2 appear as remote subnets on WANJet1. You can view a list of remote subnets on the Remote WANJets screen.

Before performing the following steps, verify whether you need to configure the WANJet appliance so that it can optimize traffic from additional subnets, and determine whether you are using a LAN router between the WANJet appliance and the LAN.

To configure multiple subnets

1. Log on to the WANJet appliance as described in *Logging on to the system*, on page 3-3.
2. In the navigation pane, expand **WAN Optimization** and click **Local WANJet**.
   The Local WANJet screen opens.
3. Click **Local Subnets**.
   The Local Subnets screen opens. By default, **Include WANJet Subnet** is selected, and the local subnet in which the WANJet appliance resides automatically appears in the list of local subnets.
4. Click the **Add** button.
   The Add Local Subnet screen opens in a separate browser window.

5. 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:

   ```
   172.16.2.0/24
   ```

   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, **172.16.2.6** is a valid address for the subnet defined in this configuration example.

6. 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 system automatically populates the corresponding subnet mask box.*

7. In the **Alias** box, type a string to serve as a name for the subnet.
   For example:

   ```
   Subnet A
   ```

8. For **Operational Status**, click the **Enabled** button.

9. Click **OK**.
   The Local Subnets screen opens with the new subnet in the list of local subnets.

10. Click the **Save** button.

11. Repeat steps 3 through 9 to add as many subnets as required.

Defining the second WANJet appliance as a remote WANJet appliance

After you finish adding subnets to the first WANJet appliance, define the second appliance as a remote WANJet appliance of the first one.

To define the second WANJet appliance as a remote WANJet appliance

1. In the navigation pane, expand **WAN Optimization** and click **Remote WANJets**.
   The Remote WANJets screen opens.

2. Click the **Add** button.
   The Manage Remote WANJet popup screen opens.

3. Leave the **WANJet Type** set to **Single**.

   ***Note**: For information about configuring WANJet appliances as redundant peers, refer to **Configuring redundant peers**, on page 8-10.*

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

   `10.2.0.1`

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

   `WANJet2`

6. Leave the settings as they are for **WANJet Port** (the default value is **3701**) and **MTU** (this setting is only available if you specified a LAN Router).
7. In the **Shared Key** box, type the shared key. The only requirement for the key is that it matches the key added for its partner in the pair. For this example, you must use the same key when adding WANJet1 as a remote WANJet appliance on WANJet2.
8. Click **OK**.
   The popup screen closes.
9. On the Remote WANJet screen, click the **Save** button.
   The new remote WANJet appliance appears in the Remote WANJet appliance list.

Configuring the second WANJet appliance

After you finish configuring the first WANJet appliance, you can configure the second WANJet appliance in the pair. The second WANJet appliance must already be installed as described in the ***Quick Start Card*** included in the shipping box.

Configure the second WANJet appliance as you did the first one, as described in the following topics.

If you have more than two WANJet appliances to configure, continue to set them up in the same way. For point-to-multipoint configuration, set up one WANJet appliance as the hub and the other WANJet appliances as remote appliances on the hub. On each of the remote appliances, set up the hub only as a remote appliance. For a mesh configuration, on each appliance, set up all other WANJet appliances as remote appliances.

Logging on to the second WANJet appliance

Log on to the second WANJet appliance as described in *Logging on to the system*, on page 3-3. The first time you log on, you must run the Setup utility.

Setting up the second WANJet appliance

Run the Setup utility on the second WANJet appliance, as described in *Setting up the WANJet appliance*, on page 3-3.

Configuring multiple subnets on the second WANJet appliance

If you have added subnets on WANJet1, you must do the same for WANJet2, unless WANJet2 is on a simpler local area network. Refer to *Configuring multiple subnets*, on page 3-5, for instructions.

Defining the first WANJet appliance as a remote WANJet appliance

After you finish adding subnets to 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 **WAN Optimization** and click **Remote WANJets**.
   The Remote WANJets screen opens.
2. Click **Add**.
   The Manage Remote WANJet popup screen opens.
3. In the **WANJet IP** box, type the IP address of the remote WANJet appliance. For example:

   ```
   172.16.2.1
   ```
4. In the **WANJet Alias** box, type a name for the remote WANJet appliance. For example:

   ```
   WANJet1
   ```
5. In the **Shared Key** box, type the shared key.
   The only requirement for the key is that it matches the key added for its partner in the pair. For this example, you must use the same key when adding WANJet2 as a remote WANJet appliance to WANJet1.
6. Leave the settings as they are for **WANJet Type**, **WANJet Port**, and **MTU** (this setting is available only if you specified a LAN Router).
7. Click **OK**.
   The popup screen closes. The new remote WANJet appliance appears in the Remote WANJet appliance list.
8. On the Remote WANJet screen, click the **Save** button.

Testing connectivity

When the WAN link is established between the pair of WANJet appliances, the two systems automatically exchange subnet specifications. For example, the local subnets that you specify for WANJetA become remote subnets for WANJetA in WANJetB's Remote WANJet appliance configuration information.

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

- Status of the WAN link(s)
- Status of remote WANJet appliance(s)
- Diagnostics reports

For additional information about WANJet appliance reports, such as those described in the following procedures, see Chapter 12, *Monitoring the WANJet Appliance*.

To check the status of the WAN link on each system

1. Above the navigation pane, check the dashboard to see whether the **WANJet Links** and **Operational Mode** are **Active**.
   If the dashboard shows both the links and mode as **Active** and the indicators are green, the two appliances are up and running, and they are communicating.
2. If the **WANJet Links** or **Operational Mode** are not **Active**, in the navigation pane, expand **WAN Optimization** and click **Operational Mode**.
3. Make sure that **Mode** is set to **Active**.

To view the status of the remote WANJet appliance

In the navigation pane, expand **WAN Optimization** and click **Remote WANJets**.

The Remote WANJets screen opens and displays a list of remote WANJet appliances. A green light displays in the Status column for remote WANJet appliances that are enabled and connected.

To view diagnostics

1. In the navigation pane, expand **WAN Optimization** and click **Diagnostics**.
   The Diagnostics screen opens.
2. From the Connectivity menu, choose Remote WANJets.
   The Diagnose Remote WANJet report opens.
3. Review details about each remote WANJet appliance, including its IP address, whether a ping from the local WANJet appliance was successful, and whether the connection between the two appliances is operational.

Additional configuration tasks

The initial configuration steps described in this chapter are only the minimal steps you need to take to establish a WAN link between two WANJet appliances and start optimizing traffic between the two.

When you have completed the initial configuration steps, we recommend that you perform additional administrative tasks, such as the following:

- Configure optimization and passthrough policies
  Refer to *Creating optimization policies*, on page 7-2.
- Configure traffic-shaping policies
  Refer to *Creating Application QoS policies*, on page 7-9
- Create local or remote accounts
  Refer to Chapter 6, *Managing Administrative Accounts*.
- Set up email alerts
  Refer to *Configuring email alerts*, on page 8-3.
- Synchronize the time automatically
  Refer to *Configuring NTP time servers*, on page 5-14
- Specify the level of log messages to save
  Setting log levels, on page 13-6.

Refer to the other chapters in this document for additional configuration that you can do to fine-tune the WANJet appliance for your environment. For example, refer to *Configuring redundant peers*, on page 8-10, if you want to deploy WANJet appliances in redundant pairs. In general, Chapter 5, *Managing WANJet Appliances*, describes how to change the configuration that you completed while running the Setup utility. Chapter 8, *Configuring Advanced Settings*, explains some more advanced configuration tasks.

Activating the license

You typically activate the license associated with your WANJet appliance during the setup process. The WANJet appliance cannot optimize traffic until the license is activated. If you have run the Setup utility, you may have already activated the license. (To see if the license is already activated, in the navigation pane, expand **System**, then click **License** to see the license status.) This section provides additional details on the license activation process if you need them.

You can activate the license automatically or by using the manual procedure. You only need to activate the license once. If you update the WANJet appliance in the future, the license information is retained.

The license purchased for the WANJet appliance is associated with the bandwidth of the WAN link. To change the bandwidth of that link, you need to contact F5 to obtain a new license, then activate it.

Automatic activation is the easiest method because the WANJet appliance directly connects to the F5 license server and handles the activation. **Automatic** is the default setting if the system locates a route to the license server. However, in certain cases, you may need to manually activate the license. For example, follow the manual procedure if the WANJet appliance does not have a direct connection to the Internet, or if it resides behind a firewall that does not allow for a direct Internet connection. If the system does not find a route to the license server, only the **Manual** setting is available.

To manually activate the license, you need an administrative workstation with a connection to the WANJet appliance and the Internet.

To activate the license automatically

1. Display the License General Properties screen in one of two ways:
    - Run the Setup utility and on the License screen, click **Activate** or **Re-activate**.
    - In the navigation pane, expand **System**, click **License**, then click **Activate** or **Re-activate**.
2. For **Base Registration Key**, you should see your registration key (filled in at the factory).
3. Next to **Activation Method**, click **Automatic**.
4. From the **Outbound Interface** list, your selection depends on your configuration:
    - Select **mgmt** if you configured the Management Port.
    - Select **wan** if you are using the WANJet IP address to log on to the system.
5. Click **Next**.
   The EULA (End User License Agreement) screen opens.
6. Read the EULA, and then click **Accept** if you agree to the conditions.
   The WANJet appliance automatically activates the license.
7. If you activated the license for the first time, you need to reboot the WANJet appliance. Refer to *Shutting down and restarting the WANJet appliance*, on page 5-16.

◆ **Note**

If automatic license activation is not available, you can use manual activation instead, described in the next section.

To activate the license manually

1. Display the License General Properties screen in one of two ways:
    - Run the Setup utility and on the License screen, click **Activate** or **Re-activate**.
    - In the navigation pane, expand **System**, click **License**, then click **Activate** or **Re-activate**.

2. For **Base Registration Key**, you should see your registration key (filled in at the factory).
3. Next to **Activation Method**, click **Manual**.
4. From the **Outbound Interface** list, your selection depends on your configuration:
   - Select **mgmt** if you configured the Management Port.
   - Select **wan** if you are using the WANJet IP address to log on to the system.
5. Click **Next**.
   The Manual Activation screen opens.
6. Select and copy the entire contents of the Dossier box (Ctrl + A, Ctrl + C).
7. Click the link, **Click here to access F5 Licensing Server**, located below the dossier.
   In a separate browser, the Activate F5 License screen opens.
8. On the Activate F5 License screen, paste the dossier that you copied, and click **Next**.
   The Activate F5 Product displays, still in a separate browser.
9. Read the license, then select the option, **I have read and agree to the terms of this license**, and click **Next**.
   The license information is displayed on the Activate F5 Product screen.
10. Select the entire license (Ctrl + A, Ctrl + C), and paste it into the Manual Activation screen after **Step 3: License**.
11. Click **Next**.
    The WANJet appliance activates the license.
12. If you activated the license for the first time, you need to reboot the WANJet appliance. Refer to *Shutting down and restarting the WANJet appliance*, on page 5-16.

To view license information

In the navigation pane, expand **System**, click **License**. The License Properties screen opens and displays the license type, the date the WANJet appliance was licensed, the date the license expires, and active and optional modules.

Troubleshooting

One of the first steps we recommend for troubleshooting the WANJet appliance is to create a system snapshot immediately. It provides detailed information about the WANJet appliance, including:

- Date and time of the snapshot
- WANJet appliance version and build number
- Connection counts
- System and network status
- Recent errors
- Status and configuration settings of the interfaces

Refer to *Creating system snapshots*, on page 12-20 for information on taking a system snapshot. You can provide the system snapshot to the F5 Networks Technical Support team to help resolve technical issues.

Some common problems are listed in Table 3.1. 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 actions
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 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 log on to the WANJet appliance.	Check to see that you are accessing the correct URL for the Configuration utility. If you enter just **http://** followed by the IP address, it will not work. You must use the secure HTTPS protocol. For example: **https://123.123.123.123/** See *Logging on to the system*, on page 3-3.
When I attempt to access the Configuration utility, 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 Configuration utility. Although the default setting grants access to all machines, that setting can be changed to limit access based on IP address. Log on from a computer that is within the network. After that, use the Configuration utility to change the access settings. For instructions, see *Configuring local user accounts*, on page 6-6.

Table 3.1 *Troubleshooting suggestions*

4

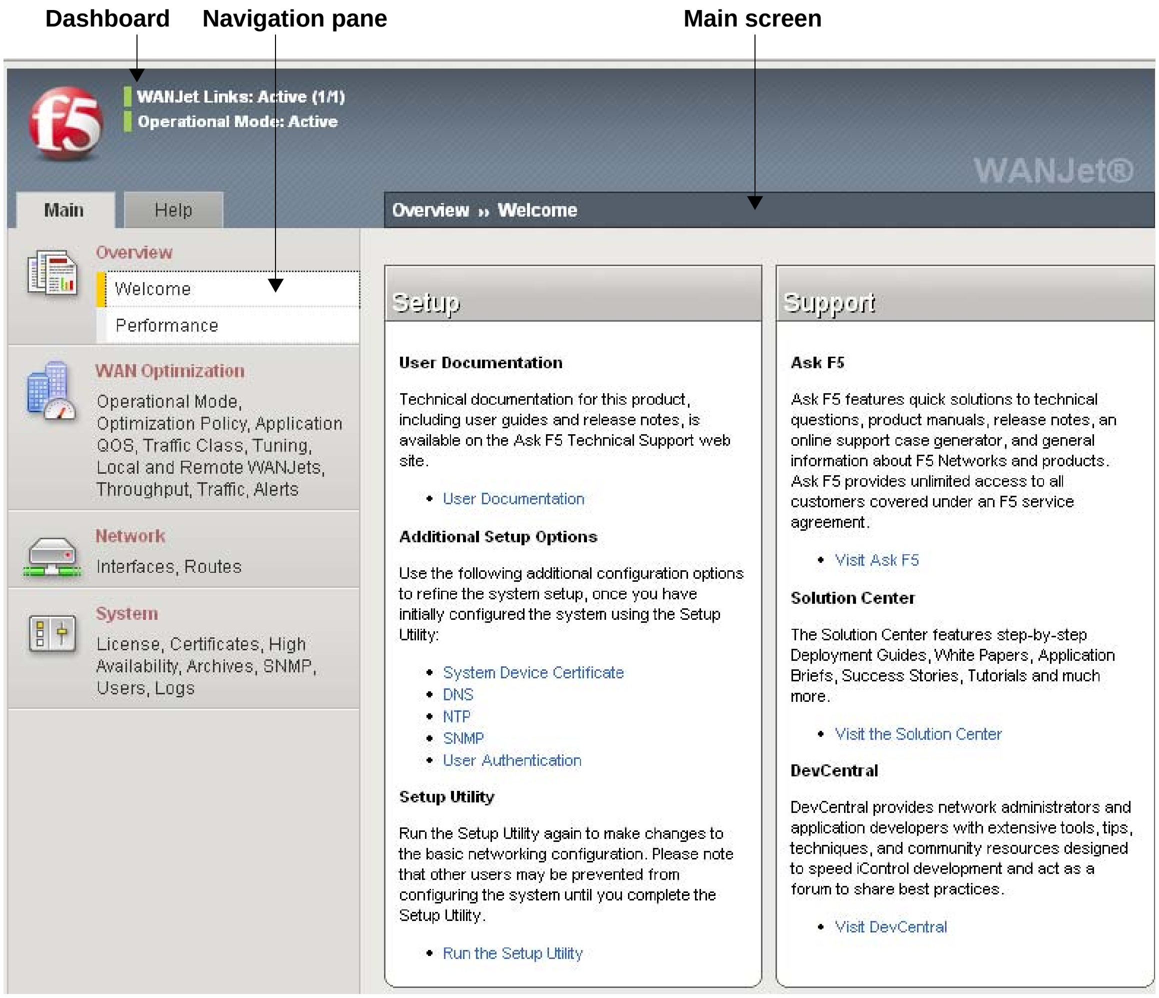
Using the Configuration Utility

- Introducing the Configuration utility
- Using the dashboard
- Learning about the navigation pane
- Troubleshooting access to the Configuration utility

Introducing the Configuration utility

The browser-based interface of the WANJet appliance is called the ***Configuration utility***. The first screen that you see when you log on to the Configuration utility (once you have run the Setup utility) is the Welcome screen, which displays in the main browser frame. This screen provides links to documentation, setup options, support resources, and additional downloads.

Figure 4.1 uses the Welcome screen to show the parts of the Configuration utility.


Dashboard
Navigation pane
Main screen
WANJet Links: Active (1/1)
Operational Mode: Active
WANJet®
Main
Help
Overview » Welcome
Overview
Welcome
Performance
WAN Optimization
Operational Mode, Optimization Policy, Application QOS, Traffic Class, Tuning, Local and Remote WANJets, Throughput, Traffic, Alerts
Network
Interfaces, Routes
System
License, Certificates, High Availability, Archives, SNMP, Users, Logs
Setup
Support

User Documentation

Technical documentation for this product, including user guides and release notes, is available on the Ask F5 Technical Support web site.

- User Documentation

Additional Setup Options

Use the following additional configuration options to refine the system setup, once you have initially configured the system using the Setup Utility:

- System Device Certificate
- DNS
- NTP
- SNMP
- User Authentication

Setup Utility

Run the Setup Utility again to make changes to the basic networking configuration. Please note that other users may be prevented from configuring the system until you complete the Setup Utility.

- Run the Setup Utility

Ask F5

Ask F5 features quick solutions to technical questions, product manuals, release notes, an online support case generator, and general information about F5 Networks and products. Ask F5 provides unlimited access to all customers covered under an F5 service agreement.

- Visit Ask F5

Solution Center

The Solution Center features step-by-step Deployment Guides, White Papers, Application Briefs, Success Stories, Tutorials and much more.

- Visit the Solution Center

DevCentral

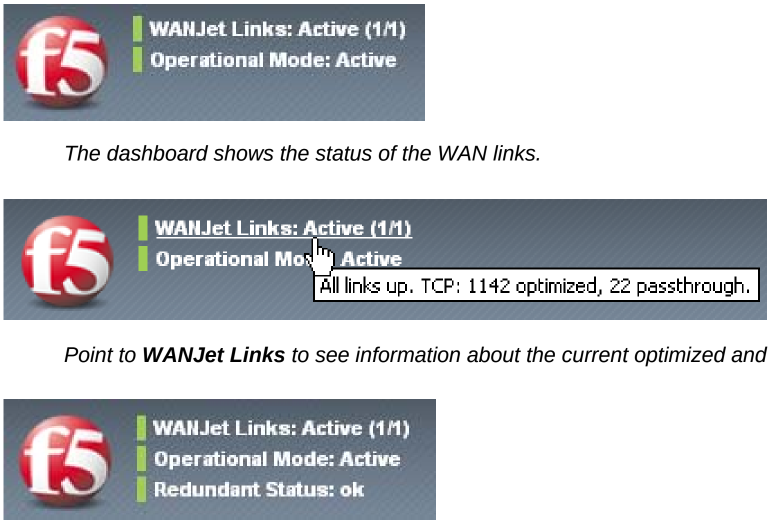
DevCentral provides network administrators and application developers with extensive tools, tips, techniques, and community resources designed to speed iControl development and act as a forum to share best practices.

- Visit DevCentral

Figure 4.1 *Parts of the WANJet appliance Configuration utility*

Using the dashboard

The ***dashboard*** in the upper left corner of the screen displays status indicators. This area is always visible, regardless of where you are in the Configuration utility. Figure 4.2 shows the dashboard in various states.



WANJet Links: Active (1/1)
Operational Mode: Active

The dashboard shows the status of the WAN links.

WANJet Links: Active (1/1)
Operational Mode: Active
All links up. TCP: 1142 optimized, 22 passthrough.

*Point to **WANJet Links** to see information about the current optimized and passthrough sessions.*

WANJet Links: Active (1/1)
Operational Mode: Active
Redundant Status: ok

The dashboard shows the status of the redundant peer, if configured.

Figure 4.2 *Displaying dashboard status*

The dashboard displays the following information:

- **WANJet Links**
  Shows the number of links to remote WANJet appliances, and a colored bar showing the status of remote WANJet appliances:
  - Green indicates that all links are active.
  - Red means that no links are active (or links are not configured).
  - Yellow indicates that this system has links to more than one remote WANJet appliance and only some links are active.

  For more information about link status, click **WANJet Links** to display the WANJet Links report. For more information, see *WANJet Links diagnostics*, on page 12-11.

  For information about status and the number of optimized and passthrough sessions, point to the dashboard. A message shows the status of the links, and if active, the number of TCP sessions that the WANJet appliance is currently optimizing (including all established sessions plus those in the process of being optimized) and the number of passthrough sessions.

- **Operational Mode**
  Shows the state of the WANJet appliance, whether it is **Active** or **Inactive**.
- **Redundant Status**
  Displays the status of the redundant peer, if one is configured on the WANJet appliance.

The dashboard refreshes every10 seconds, providing a snapshot of system activity at the current time. You may see different numbers on the dashboard and the reporting screens (described in Chapter 12, *Monitoring the WANJet Appliance*) because connections are established and terminated very frequently.

Learning about the navigation pane

The ***navigation pane*** is the area on the Main tab at the left of the screen. It includes four sections that you can expand:

- **Overview**
  Provides links for you to view the Welcome page and performance reports.
- **WAN Optimization**
  Provides links to screens where you can configure optimization policies, Application QoS policies, and optimization settings, and view diagnostic reports.
- **Network**
  Provides links to screens that allow you to configure interfaces, add routes, and view network statistics.
- **System**
  Provides links to screens for you to view or modify the system and platform configuration.

Navigating the WANJet appliance

To view other Configuration utility screens, expand a section in the navigation pane on the left side of the screen, and click an option. Information displays in the main area of the screen. For example, to view optimization policies, in the navigation pane, expand **WAN Optimization** and click **Optimization Policy**. The WANJet Protocol Optimization Policy screen opens in the main screen.

Using the main screen

The main screen is the area of the Configuration utility that contains reports showing information about WANJet appliance operations, or fields where you can configure how the WANJet appliance works.

Viewing online help

You display online help by clicking the Help tab at the top of the navigation pane. The Help tab displays information about the current screen, including details on each of the settings, tables, buttons, and other screen elements.

Troubleshooting access to the Configuration utility

If you are having trouble with the Configuration utility of the WANJet appliance, try refreshing the browser using the browser Refresh button.

If your web browser cannot access the Configuration utility, it may be because Configuration utility access is restricted to a limited range of IP addresses. See *Configuring access to the web interface*, on page 6-11**.** You may have to log on from a different location from which access is allowed.

You may be using the incorrect IP address. If you configured a Management IP address, you should use that IP address to log on. You can check the configuration of the WANJet appliance from the LCD. For details on configuring the WANJet appliance from the LCD, refer to the ***Quick Start Guide*** for your platform.

Trying pinging the IP address you are using to log on to the WANJet appliance. Also try accessing the WANJet appliance from the command line to be sure it is operational. Refer to Chapter 14, *Working from the Command Line*.

If you have considered other options and are still having problems with the WANJet appliance (such as logging on to the Configuration utility), you can reboot the appliance. Refer to *Shutting down and restarting the WANJet appliance*, on page 5-16.

5

Managing WANJet Appliances

- Modifying the local WANJet appliance network configuration
- Configuring the Management port, host name, host IP address, and time zone
- Configuring remote WANJet appliances
- Viewing or configuring general properties
- Shutting down and restarting the WANJet appliance

Modifying the local WANJet appliance network configuration

When you initially configure the local WANJet appliance (as described in Chapter 3, *Beginning to Configure WANJet Appliances*), 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, such as the changing the IP address, netmask, or WAN gateway for the local WANJet appliance, defining a redundant peer, and adding subnets. Any values displayed on the Local WANJet appliance screen are likely the ones that you specified during initial configuration using the LCD or the Setup utility.

The subnet in which the WANJet appliance resides is automatically added to the list of local subnets (unless you clear the **Include WANJet Subnet** option on the Local Subnets screen). Refer to *Configuring multiple subnets*, on page 3-5, for details on adding local subnets.

◆ **Important**

You must replicate any changes that you make to the WANJet appliance's IP address, port, or subnet address on each remote WANJet appliance to which the local WANJet appliance is connected. See ***Replicating configuration changes to remote WANJet appliances****, on page 5-3.*

Viewing or changing the local WANJet appliance network configuration

If you need to view or modify the local WANJet appliance configuration, perform the following steps.

To view or modify the local WANJet appliance network configuration

1. In the navigation pane, expand **WAN Optimization** and click **Local WANJet**.
   The Local WANJet appliance screen opens.
2. Modify the values as required.
   Table 5.1 lists and describes the local WANJet appliance settings that you can view or configure.
3. Click the **Save** button.

Setting	Description	Default Value
WANJet Alias	Specifies a name for the WANJet appliance.	No default value
WANJet IP	Specifies the IP address of the local WANJet appliance. If you change this value, you must change it on each remote WANJet appliance that accesses this one.	No default value
WANJet Netmask	Specifies the subnet mask assigned to the WANJet appliance on your network.	No default value
WAN Gateway	Specifies the IP address of the gateway that the WANJet appliance uses to reach the WAN.	No default value
LAN Router	Specifies the IP address of the LAN router (if your network configuration includes one) that resides between the WANJet appliance and the LAN. If you specify a LAN router for your local WANJet appliance, all configured local subnets use it to identify the destinations of packets.	No default value
WANJet Port	Specifies the main port number that the local WANJet appliance uses to communicate with remote WANJet appliances. If you change this value, you must change it on each remote WANJet appliance that accesses this one.	3701
Enable Redundant Peer	Enables or disables a redundant peer. When enabled, this WANJet appliance connects to another WANJet appliance through the peer ports on each.	Enabled (checked)
Self Peer IP	Specifies the IP address of the peer port on the local WANJet appliance. It must be in the same subnet as the redundant peer IP address.	No default value

Table 5.1 *Local WANJet appliance settings*

Setting	Description	Default Value
Redundant Peer IP	Specifies the IP address of the peer port on the duplicate WANJet appliance. It must be in the same subnet as the self peer IP address.	No default value
Peer Netmask	Specifies the netmask of the peer and remote peer subnet. You create a subnet of the IP addresses of the peer ports on the WANJet appliance and the redundant peer.	No default value
Settings for Delayed Connection Acceptance	Links to a screen where you can configure whether to postpone acceptance of LAN requests from certain ports until the server connection is verified.	Link to Delayed Connection Acceptance screen
Local Subnets	Links to a screen where you can add local subnets from which you want the WANJet appliance to accept traffic. By default, the WANJet appliance only recognizes the subnet it is in. Refer to *Configuring multiple subnets*, on page 3-5 for details on adding local subnets.	Link to Local Subnets screen

Table 5.1 *Local WANJet appliance settings (Continued)*

Replicating configuration changes to 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 remote WANJet appliances.

For example, if you have four connected WANJet appliances named B1, B2, B3, and B4, and you log on to B1, the Configuration utility shows B1 as the local WANJet appliance and B2, B3, and B4 as its remote WANJet appliances. Therefore, if you change the IP address for B1, you must also change the IP address for B1 on the remote WANJet appliances (B2, B3, and B4) so that they match.

To update the remote WANJet appliance settings

1. Log on to the local WANJet appliance and modify the settings as needed on the Local WANJets screen.
2. In the navigation pane, expand **WAN Optimization** and click **Remote WANJets**.
   The Remote WANJets screen opens and lists all of the remote WANJet appliances that need to be updated.
3. Log on to each of the remote WANJet appliances listed on the Remote WANJets screen in step 2 and follow these steps:
   a) In the navigation pane, expand **WAN Optimization** and click **Remote WANJets**.
   The Remote WANJets screen opens.
   b) In the IP column of the remote WANJet appliance whose settings you changed, click the IP address.
   The Manage Remote WANJet screen opens.

c) Edit the settings as required and click **OK**.

d) Click **Save** on the Remote WANJets screen.

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

Configuring delayed connection acceptance

The WANJet appliance generally accepts incoming connections from the LAN, then attempts to connect with the server on the remote LAN. If the server is unreachable, the WANJet appliance closes the original client-side LAN connection. A delayed connection acceptance feature, enabled by default, postpones acceptance of LAN requests coming from ports **139** and **445** (ports used for CIFS optimization) until the server connection is verified.

You can configure the ports that will delay accepting requests. If you do not want to use this feature, clear the ports listed in the **Ports** box.

To configure delayed connection acceptance settings

1. In the navigation pane, expand **WAN Optimization** and click **Local WANJet**.
   The Local WANJet screen opens.
2. Click **Settings for Delayed Connection Acceptance**.
   The WANJet Settings for Delayed Connection Acceptance screen opens.
3. In the **Ports** box, type the numbers of any ports for which you want to delay the acceptance of a connection until verifying that the server is reachable. Separate multiple ports with colons (for example, **139:445**).
4. Click **Save** to make the changes.

Running the Setup utility after the system is set up

You can run the Setup utility at any time, even after the system is already configured. From the Welcome screen, click **Run the Setup Utility**. The screens you configure when running the Setup utility are also accessible on the WANJet appliance, as shown in Table 5.2.

Setup utility screen	Configuration utility screen
License	In the navigation pane, expand **System** and click **License**.
Platform	In the navigation pane, expand **System** and click **Platform**.
Local WANJet	In the navigation pane, expand **WAN Optimization** and click **Local WANJet**.

Table 5.2 *Finding Setup utility screens in the Configuration utility*

Whenever you are logged on to the Configuration utility, you can make changes to the settings configured using the Setup utility.

Configuring the Management port, host name, host IP address, and time zone

From the Platform Configuration screen, you can configure these properties for the WANJet appliance:

- Management port IP address, netmask, and gateway
- Host name of the WANJet appliance
- Host IP address of the WANJet appliance
- Time zone in which the WANJet appliance operates

◆ **Note**

You can also configure many of these properties and settings from the Setup utility.

You can also configure user administration settings from the Platform Configuration screen. Refer to *Managing local user accounts*, on page 6-3, for details on how to change passwords for the **root** and **admin** accounts, set up the Support account, and configure SSH access and HTTPD access to the WANJet appliance.

The following procedure provides the basic steps for configuring platform-related properties. Following this procedure are detailed descriptions on how to configure each of the platform properties.

To configure platform properties

1. In the navigation pane, expand **System**, and click **Platform**.
   The Configuration screen opens.
2. Configure the platform property settings as needed.
   For more information, see the rest of this chapter, as well as the online help.
3. At the bottom of the screen, click **Update**.

Configuring the Management port

Every WANJet appliance has a port called the Management port that you can use for out-of-band management. ***Out-of-band management*** provides a dedicated management channel (separate from the data channel) that is used for administration only. The ***Management port*** is an interface that the WANJet appliance uses to receive or send certain types of administrative traffic.

◆ **Tip**

You typically configure the Management port using the LCD on the WANJet appliance hardware, or when you run the Setup utility during initial installation. You need to reconfigure the Management port only if the Management port IP address, netmask, or route has changed, or if you decide to configure the Management port at a later time.

The IP address that you assign to the Management port is typically on the management network. The Management route specifies the default management gateway. Use of the Management port is optional. If you use the Management port, you need to log on to the Configuration utility using its IP address rather than the WANJet IP address (although it is possible to use either).

The advantage of using the Management port is that it provides a way to separate the WANJet appliance management data from the data that is being optimized. You connect the Management port to a separate subnet dedicated to a management network, for example, which is a different network from the one where the WANJet appliance IP address is located, and where only administrators have access. You cannot use the Management port for normal traffic that is being optimized. Instead, the WANJet appliance always uses the TMM switch interfaces for that type of traffic. ***TMM switch interfaces*** are those interfaces controlled by the Traffic Management Microkernel (TMM) service. Refer to *TMM service*, on page 9-14, for more details about this service.

We recommend configuring and using the Management port. If you do not have a management network, you still need to specify fictitious values for the Management port settings during setup. Then you log in using the **WANJet IP address** (also called the ***bridge IP***). However, if you want to use Enterprise Manager to manage WANJet appliances, you must use the Management port for communication, not the **WANJet IP address**.

◆ **Note**

The IP address for the Management port must be in IPv4 format.

The following procedure describes how to set up the Management port from the Configuration utility if you did not configure it when you initially installed the WANJet appliance.

To configure the Management port

1. In the navigation pane, expand **System**, and click **Platform**.
   The Configuration screen opens.
2. For the **Management port** settings:
   - In the **IP Address** box, type the IP address of the WANJet appliance on the management network.
   - In the **Network Mask** box, type the netmask for the Management port.
   - In the **Management Route** box, type the IP address of the default management gateway.
3. At the bottom of the screen, click **Update**.

For procedural information on configuring the Management port using the LCD, see the ***Quick Start Guide*** for the WANJet appliance platform. For information on the way that the TMM service affects the Management port, see the description in *TMM service*, on page 9-14.

Changing the host name and host IP address

Every WANJet appliance must have a host name and a host IP address. The IP address can be the same as the address that you used for the Management port, or you can assign a unique address.

You typically configure the host name and IP address for the WANJet appliance when you run the Setup utility during initial configuration. You need to modify the host name and IP address only if it has changed since you set it up.

To specify a host name and IP address

1. In the navigation pane, expand **System**, and click **Platform**.
   The Configuration screen opens.
2. For the **Host Name** setting, type a fully qualified domain name for the WANJet appliance. An example of a host name is **mywanjet.wanopt.net**.
3. For the **Host IP Address** setting, select one of the following settings:
   - **Use Management Port IP Address** to assign the Management port IP address to the host name. This is the default value.
   - **Custom Host IP Address** to assign a different IP address to the host name. A box opens where you can type the IP address. If you are not using the Management port, select this option and type the WANJet appliance IP address.
4. At the bottom of the screen, click **Update**.

Specifying a time zone

The WANJet appliance should be set up for the correct time zone so the logs and system information reflect the correct time. You can set the time using the **date** command on the command line (refer to the Linux man page for details). Note that it is a good idea to configure a time server to synchronize the time on all WANJet appliances (see *Configuring NTP time servers*, on page 5-14).

You typically set the time zone for the WANJet appliance when you run the Setup utility during initial configuration. You need to change it only if you move the appliance to a different time zone.

To change the time zone

1. In the navigation pane, expand **System**, and click **Platform**.
   The Configuration screen opens.
2. For the **Time Zone** setting, select the time zone that most closely represents the location of the WANJet appliance you are configuring.
3. At the bottom of the screen, click **Update**.

Configuring remote WANJet appliances

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

When you initially configure the local WANJet appliance (as described in *Testing connectivity*, on page 3-9) you have set up two WANJet appliances, each as a remote appliance to the other. You need to add remote WANJet appliances only if your configuration includes additional WANJet appliances, such as if you are using a hub and spoke configuration.

To add a remote WANJet appliance

1. In the navigation pane, expand **WAN Optimization** and click **Remote WANJets**.
   The Remote WANJets screen opens.

2. Click **Add**.
   The Manage Remote WANJet appliance screen opens.

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 *Configuring redundant peers*, on page 8-10, for an explanation of redundant peers.)

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

5. If you selected **Redundant** in Step 3, in the **Redundant Peer** box type the IP address for the peer WANJet appliance. Otherwise, the field is not available, and you can skip to Step 6.

   ***Note**: The **Redundant Peer** box can be edited only if you select **Redundant** from the WANJet appliance type list.*

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 number of the main port 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 appliance port number, you must change the port number for this appliance on all remote WANJet appliances.*

8. In the **Shared Key** box, type the shared key that authenticates between the local and remote WANJet appliances. You can set a unique shared key for every pair of WANJet appliances.

9. If you specified an IP address in the **LAN Router** field on the Local WANJet screen, you can select an MTU (Maximum Transmission Unit) type. The MTU is the maximum packet size in bytes that can be transmitted across a link. For **MTU**, select one of the following MTU types:

    - **Direct**
      The value for this type is 1500 bytes, and is the most common MTU type used for the IP protocol. This is the default MTU value.

    - **VPN**
      The default MTU for this option is 1400 bytes.

    - **Other**
      You can specify the MTU value required by your network.

10. Click **OK**.
    The Manage Remote WANJet screen closes.

11. Click **Save**.

To edit or remove a remote WANJet appliance

1. In the navigation pane, expand **WAN Optimization** and click **Remote WANJets**.
   The Remote WANJets screen opens.

2. Click the IP address for the WANJet appliance that you want to edit or remove.
   The Manage Remote WANJet appliance screen opens.

3. Edit the information or click the **Remove** button to remove the remote WANJet appliance.

   ***Note**: If you edit a port number, you must change that port number on all connected WANJet appliances. If you remove a WANJet appliance, you remove all associated subnets.*

4. Click **OK**.
   The Manage Remote WANJet appliance screen closes.

5. Click **Save**.

◆ **Important**

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

Viewing or configuring general properties

The WANJet appliance general properties that you can view are:

- Host name
- Software version number
- Number of CPUs available
- Number of CPUs that are active
- Current CPU mode (uniprocessor or multiprocessor)

The WANJet appliance system properties that you can change are:

- Network boot
- Quiet boot

The following procedure provides the basic steps for configuring system properties.

To view or configure general properties

1. In the navigation pane, expand **System**, and click **Configuration**. The General Configuration screen opens.
2. View any settings. For detailed information on these settings, see the online help and Table 5.3.
3. If you configured any settings, click **Update**.

Table 5.3 describes the general properties.

Property	Description	Default Value
Host Name	Displays the host name of the WANJet appliance. This is the same host name that you can view and modify on the Platform Configuration screen, as described in *Changing the host name and host IP address*, on page 5-8.	No default value
Version	Displays the version number of the WANJet appliance software that is running on the system. The system provides the software version information, and it is changed only when you upgrade or reinstall the software. See *Determining the software version*, on page 5-13.	No default value
CPU Count	Displays the total number of CPUs that the WANJet appliance contains. The system checks the hardware for the number of CPUs.	No default value
Active CPUs	Displays the total number of CPUs that are currently active on the WANJet appliance. The system checks the hardware for the number of active CPUs.	No default value

Table 5.3 *General configuration properties of a WANJet appliance*

Property	Description	Default Value
CPU Mode	Displays the current processor mode of the system, either uniprocessor or multiprocessor. The system checks the hardware to determine the CPU mode.	No default value
Network Boot	Enables or disables the network boot feature. When enabled, the system boots from the network rather than the WANJet appliance. For details, see *Changing the way the system boots*, following.	Disabled (unchecked)
Quiet Boot	Enables or disables the quiet boot feature. If you enable this feature, the system suppresses informational text on the console during the boot cycle. For details, see *Changing the way the system boots*, following.	Enabled (checked)

Table 5.3 *General configuration properties of a WANJet appliance (Continued)*

Determining the software version

The General Configuration screen displays the version of the software that is running on the WANJet appliance. In the navigation pane, expand **System**, and click **Configuration**. The **Version** setting shows the software version.

Changing the way the system boots

You can change the following system boot features:

- Boot from the network
- Display informational text while the system boots

If you enable **Network Boot** and then reboot the system, the system boots from an ISO image on the network, rather than from the WANJet appliance. Use this option only when you want to install software on the system, for example, for an upgrade or a reinstallation. Note that this setting reverts to disabled (cleared) after you reboot the system a second time.

If you enable **Quiet Boot**, the system does not display informational messages on the console when it reboots.

To change the way the system boots

1. In the navigation pane, expand **System**, and click **Configuration**. The General Configuration screen opens.
2. If you want to boot the system from the network, check the box for the **Network Boot** setting.

3. For the **Quiet Boot** setting, specify whether you want to display informational messages when the system boots:
    - Clear the **Enabled** box if you want to view informational messages when the system boots.
    - Check the **Enabled** box if you do not want to display the information.
4. Click **Update**.

Configuring NTP time servers

Network Time Protocol (NTP) is a protocol that synchronizes the clocks on a network. You can specify a list of IP addresses of the servers that you want the WANJet appliance to use when updating the time on network systems. You can also edit or delete the entries in the server list.

To configure a list of NTP time servers

1. In the navigation pane, expand **System**, and click **Configuration**.
   The General Configuration screen opens.
2. From the menu bar, choose NTP.
   The NTP Configuration screen opens.
3. For the **Time Server List** setting, add, edit, or remove an IP address:
    - To add an IP address to the list:

      a) In the **Address** box, type a time server's IP address or host name.

      b) Click **Add**.
    - To edit an IP address in the list:

      a) In the **Time Server List** area, select an IP address.
      The IP address appears in the **Address** box.

      b) In the **Address** box, change the IP address.

      c) Click **Edit**.
    - To remove an IP address from the list:

      a) In the **Time Server List** area, select an IP address.
      The IP address appears in the **Address** box.

      b) Click **Delete**.
4. Click **Update**.

Configuring DNS directory services

Domain Name System (DNS) is an industry-standard distributed internet directory service that resolves domain names to IP addresses. If you plan to use DNS in your network, you need to configure DNS on the WANJet appliance.

When you configure DNS, you create a DNS lookup server list. The ***DNS lookup server list*** allows WANJet appliance users to use IP addresses, host names, or fully qualified domain names to access virtual servers, nodes, or other network objects.

In addition to adding servers to the DNS lookup server list, you can also edit or delete the entries in these lists.

To configure DNS for the WANJet appliance

1. In the navigation pane, expand **System**, and click **Configuration**.
   The General Configuration screen opens.
2. From the menu bar, choose DNS.
   The DNS Configuration screen opens.
3. In the **DNS Lookup Server List** area, you can add, edit, or remove a server IP address:
   - To add a server to the list:

     a) In the **Address** box, type the IP address of a properly configured name server.

     b) Click **Add**.

     c) To add backup DNS servers to the list, repeat steps a and b.
   - To edit an IP address in the list:

     a) In the **DNS Lookup Server List** area, select an IP address.
     The IP address appears in the **Address** box.

     b) In the **Address** box, change the IP address.

     c) Click **Edit**.
   - To remove an IP address from the list:

     a) In the **DNS Lookup Server List** area, select an IP address.
     The IP address appears in the **Address** box

     b) Click **Delete**.
4. Click **Update**.

Shutting down and restarting the WANJet appliance

Shutting down WANJet appliance stops all data processing and brings the system down in a secure way. You typically shut down the system from the command line. You can also shut down the WANJet appliance from the LCD. After the operating system halts, you can then power off the system.

You may need to restart, or reboot, the system instead of shutting it down completely. For example, after licensing the system for the first time, you need to reboot the WANJet appliance.

To shut down the WANJet appliance from the command line

1. Log on to the command line as **root**.
2. Type **shutdown**.
   The operating system shuts down.
3. Turn off the WANJet appliance completely by pressing the On/Off button.

To restart the WANJet appliance from the command line

1. Log on to the command line as **root**.
2. Type **reboot**.
   The operating system halts and restarts.

6

Managing Administrative Accounts

- Introducing user accounts
- Managing local user accounts
- Managing remote user accounts

Introducing user accounts

By creating user accounts for system administrators, you provide additional layers of security. User accounts ensure that the system:

- Verifies the identity of users logging on to the system (authentication)
- Controls user access to system resources (authorization)

To enable user authentication and authorization, you assign passwords and user roles to your user accounts. ***Passwords*** allow you to authenticate users when they attempt to log on to the WANJet appliance. ***User roles*** allow you to control user access to WANJet appliance resources.

You can create and store WANJet administrative accounts either locally on the WANJet appliance, or remotely on a separate authentication server. If you want user accounts to reside locally, you create those user accounts on the WANJet appliance. For information on local user accounts, see *Managing local user accounts*, on page 6-3.

If you want user accounts to reside remotely on a separate authentication server, you do not create the accounts on the WANJet appliance. Instead, you create them using the authentication server, and use the WANJet appliance strictly to assign user roles to those remote accounts.

You can remotely store WANJet appliance user accounts on the following authentication servers:

- Active Directory servers
- Lightweight Directory Access Protocol (LDAP) servers
- Remote Authentication Dial-in User Service (RADIUS) servers

For information on remote user accounts, see *Managing remote user accounts*, on page 6-12.

Understanding accounts

The WANJet appliance comes with the following local accounts:

- **root**
- **support**
- **admin**

The **root** and **support** accounts have full access to WANJet appliance resources. By default, the **admin** account has full access to the Configuration utility but no access to the command line. For more information on the **admin** account, see *Configuring the admin account*, on page 6-3. The **support** account is an account that F5 Technical Support personnel can use to log on to the system. For more information on the **support** account, see *Configuring the support account*, on page 6-8.

◆ **Note**

*You are not required to have any accounts other than the **root**, **support,** and the **admin** accounts, but we recommend that you do so if you have multiple administrators configuring the system.*

Standard user accounts are user accounts that you can optionally create for other WANJet appliance administrators to use. Standard user accounts can reside either locally on the WANJet appliance, or remotely on a remote authentication server. You create and maintain these accounts using the browser-based Configuration utility.

Understanding user roles

User roles are a means of controlling user access to WANJet appliance resources. You assign a user role to each administrative user, and in so doing, you grant the user a set of permissions for accessing WANJet appliance resources.

Table 6.1 lists and describes the various user roles that you can assign to a user account.

User Role	Description
Administrator	This role grants the user complete access to all objects on the system.
Guest	This role grants users permission to view all objects on the system and change their own passwords.
No Access	This role prevents the user from accessing the system.

Table 6.1 *User roles for accounts*

Understanding default user roles

The WANJet appliance automatically assigns a user role to an account when you create that account. The user role that the system assigns to a user account by default depends on the type of account:

- **root and admin accounts**
  The WANJet appliance automatically assigns the **Administrator** user role to the **root** account and the **admin** account. You cannot change this user-role assignment.

- **Other user accounts**
  The WANJet appliance automatically assigns the **No Access** user role to all standard user accounts other than the **admin** account. If the account you are using has the **Administrator** role assigned to it, you can change another account's user role from the default **No Access** role to any other user role, including **Administrator**.

Managing local user accounts

You can create, view, modify, and delete user accounts on the WANJet appliance using the browser-based Configuration utility.

The Configuration utility stores local user accounts (including user names, passwords, and user roles) in a local user account database. When a user logs on using a local account, the WANJet appliance checks the account to determine the user role assigned to that user account.

◆ **Important**

Only users with the role of ***Administrator*** *can create and manage local user accounts. However, users with any role can change their own passwords.*

Configuring the admin account

A user account called **admin** resides on every WANJet appliance. Although the WANJet appliance creates this account automatically, you must still assign a password to the account before you can use it. You initially set the password for the **admin** account by running the Setup utility. You can change the password later from the Platform screen or the Users screen.

The **admin** account resides in the local user account database on the WANJet appliance. By default, the WANJet appliance assigns the **admin** account the **Administrator** user role, which gives the user of this account full access to all WANJet appliance resources. You cannot change the user role for this account. For details on user roles, see *Understanding user roles*, on page 6-2.

Changing admin or root account passwords

When you run the Setup utility on the WANJet appliance, you set up some administrative accounts. Specifically, you provide passwords for the **root** and **admin** accounts, and you may enable the **support** account. The **root** and **admin** accounts are for WANJet appliance administrators, while the **support** account is for F5 Networks support personnel who require access to the customer's system for troubleshooting purposes.

Users logging on to the **root** account have console-only access to the WANJet appliance, by default. Users logging on to the **admin** account have browser-only access to the WANJet appliance, by default.

You can use the User Administration section of the Platform Configuration screen to change the passwords for **root** and **admin** accounts on a regular basis. You can also change the **admin** password from the Users screen. (The **root** account is not listed on the Users screen.)

To change admin or root account passwords

1. In the navigation pane, expand **System**, and click **Platform**.
   The Configuration screen opens.
2. In the User Administration section, locate **Root Account** or **Admin Account**.
3. In the **Password** box, type a new password. In the **Confirm** box, retype the same password.
4. At the bottom of the screen, click **Update**.

To change the admin password from the Users screen

1. In the navigation pane, expand **System**, and click **Users**.
   The User List screen opens, displaying a list of user accounts.
2. In the account list, click the **admin** account name.
   The Account Properties screen for the **admin** account opens.
3. For the **Password** settings, in the **New** box, type a new password. In the **Confirm** box, retype the same password.
4. At the bottom of the screen, click **Update**.

Configuring a secure password policy

You can enforce a secure password policy on user accounts having the **guest** role.

◆ **Important**

You must have the user role of ***Administrator*** *assigned to your account to configure this feature.*

Table 6.2 shows the password policy settings that you can configure.

Setting	Description	Default Value
Secure Password Enforcement	Enables or disables character restrictions, that is, a policy for minimum password length and required characters. When you enable this setting, the Configuration utility displays the **Minimum Length** and **Required Characters** settings.	**Disabled**
Minimum Length	Specifies the minimum number of characters required for a password, and the allowed range of values is **6** to **255**. This setting appears only when you enable the **Secure Password Enforcement** setting. ***Important:*** *When enabled, the WANJet appliance enforces this setting on user accounts with the* ***Guest*** *role assigned to them; any user account with the* ***Administrator*** *role assigned to it (including the* **root**, **support**, and **admin** *accounts) is not subject to the restrictions imposed by this setting.*	**6**
Required Characters	Specifies the number of numeric, uppercase, lowercase, and other characters required for a password. The allowed range of values is **0** to **127**. This setting appears only when you enable the **Secure Password Enforcement** setting. ***Important:*** *When enabled, the WANJet appliance enforces this setting on user accounts with the* ***Guest*** *role assigned to them. Any user account with the* ***Administrator*** *role assigned to it (including the* ***root****,* ***support****, and* ***admin*** *accounts) is not subject to the restrictions imposed by this setting.*	**0**
Password Memory	Specifies, for each user account, the number of former passwords that the WANJet appliance retains to prevent the user from reusing a recent password. The range of allowed values is **0** to **127**. This setting applies to all user accounts.	**0**
Minimum Duration	Specifies the minimum number of days before a user can change a password. The range of allowed values is **6** to **255**. This setting applies to all user accounts.	**6**
Maximum Duration	Specifies the maximum number of days that a user's password can be valid. The range of allowed values is **1** to **99999**. This setting applies to all user accounts.	**99999**
Expiration Warning	Specifies the number of days prior to password expiration that the system sends a warning message to a user. The range of allowed values is **1** to **255**. This setting applies to all user accounts.	**7**

Table 6.2 *Configuration settings for a secure password policy*

To enable secure password enforcement

1. In the navigation pane, expand **System**, and click **Users.**
   The Users screen opens.
2. On the menu bar, click **Authentication**.
   This displays the screen for implementing a password policy.

3. Under Password Policy, locate the **Secure Password Enforcement** setting and set it to meet your needs:
   - If you want to enable character restrictions for the **Guest** account, locate the **Secure Password Enforcement** setting and select **Enabled.**
     This displays the **Minimum Length** and **Restrictions** settings on the screen. Retain or change the values for these settings.
   - If you do not want to enable character restrictions for the **Guest** account, leave the **Secure Password Enforcement** setting set to **Disabled**.
4. Retain the default values for all other settings, or change them to suit your needs.
   These settings represent the secure password policy restrictions, which apply to all user accounts, regardless of user role.
5. Click **Finished**.

◆ **Note**

Whenever you change the secure password policy, the new configuration values, such as password expiration, do not apply to passwords that were created prior to the policy change. However, the new policy takes effect the next time that the user changes his or her password.

Configuring local user accounts

A local user account stored on the WANJet appliance has several properties. Table 6.3 lists and describes these properties, along with their default values.

Property	Description	Default Value
User Name	Specifies the name of the user account.	No default value
Password	Specifies a password that the user will use to log on to the WANJet appliance.	No default value

Table 6.3 *Properties of a local WANJet appliance user account*

Property	Description	Default Value
Role	Specifies the user role that you want to assign to the user account. Allowed values are: **Administrator**, **Guest**, and **No Access**. For more information on these user roles, see Table 6.1, on page 6-2.	**No Access**
Terminal Access	Allows or prevents access to the WANJet appliance command line interface. When you enable this setting: Users with the **Administrator** role assigned to their accounts have permission to use all WANJet appliance command line utilities, as well as any operating system commands that do not require **root** privilege. Users with a **Guest** role assigned to their accounts, when accessing the WANJet appliance through the console, can use **bigpipe** shell commands only.	Unchecked

Table 6.3 *Properties of a local WANJet appliance user account (Continued)*

Depending on the user role assigned to your account (other than the **No Access** role), you can either create, view, modify, or delete local user accounts. Users with the **Administrator** user role assigned to their own accounts can perform all of these tasks with respect to user account objects.

Creating local user accounts

You can optionally create local user accounts for administrators who can configure settings on the WANJet appliance, and for other users who need only to view the information on the WANJet appliance.

◆ **Note**

*Only users with the **Administrator** role can create user accounts.*

To create a local user account

1. In the navigation pane, expand **System**, and click **Users**.
The User List screen opens, displaying a list of all local accounts.
2. In the upper right corner of the screen, click **Create**.
The New User screen opens.

   ***Note:** If the **Create** button is unavailable, you do not have permission to create a local user account. You must have the **Administrator** role assigned to your user account.*
3. In the **User Name** box, type a name for the user account.
4. For the **Password** setting, type and confirm a password for the account.
5. To grant an access level other than **No Access**, use the **Role** setting and select a user role.

6. If you want to allow user access to the command line interface, then from the **Terminal Access** list, select **Enabled**.

   Note: *Selecting* ***Enabled*** *for users with a role of* ***Guest*** *grants access to the* ***bigpipe*** *shell only. Conversely, users with the* ***Administrator*** *role can access all commands and utilities on the system.*

7. Click **Finished**.

Configuring the support account

The **support** account is an optional account that you can enable on the WANJet appliance. When you enable this account, authorized F5 Networks support personnel can access the WANJet appliance to perform troubleshooting.

To enable or disable the support account

1. In the navigation pane, expand **System**, and click **Platform**.
   The Configuration screen opens.

2. For the **Support Account** setting, select **Enabled** box to allow access to the account, or Disabled to prevent access to the account.

3. At the bottom of the screen, click **Update**.

Viewing local user accounts

You can display a list of existing local user accounts and view the properties of an individual account. Only users who have been granted the **Administrator** role can view the settings of other user accounts.

The **admin** account and any other administrative accounts that you have created are shown on the User List screen. The **root** and **support** accounts are not listed on the User List; you can modify them from the Platform screen. See *Changing admin or root account passwords*, on page 6-3.

To display a list of local user accounts

1. In the navigation pane, expand **System**, and click **Users**.
   The User List screen opens, displaying a list of all standard user accounts.

2. View the list of user accounts.

To view the properties of a local user account

1. In the navigation pane, expand **System**, and click **Users**.
   The User List screen opens, displaying a list of all standard user accounts.

2. In the user account list, find the user account you want to view and click the account name.
   This displays the properties of that user account.

Modifying local user accounts

You use the Configuration utility to modify the properties of any existing local user account, other than the **root** account. Only users who have been granted the **Administrator** role can modify user accounts other than their own.

When you modify user account properties, you can:

- Change the password
- Change the user role
- Enable or disable terminal access

Users with a role of **Guest** can change the password for their account, but cannot modify any other properties of their accounts.

To modify properties of a local user account

1. In the navigation pane, expand **System**, and click **Users**.
   The User List screen opens, displaying a list of all standard user accounts.
2. In the user account list, click a user account name.
   This displays the properties of that account.
3. Change one or more of these settings:
   - **Password**
   - **Role**
   - **Terminal Access**
4. Click **Update**.

Changing admin or root account passwords

When you run the Setup utility on the WANJet appliance, you set up some administrative accounts. Specifically, you provided passwords for the **root** and **admin** accounts, and you may have enabled the **support** account. The **root** and **admin** accounts are for WANJet appliance administrators, while the **support** account is for F5 Networks support personnel who require access to the customer's system for troubleshooting purposes.

Users logging on to the **root** account have console-only access to the WANJet appliance, by default. Users logging on to the **admin** account have browser-only access to the WANJet appliance, by default.

You can use the User Administration section of the Platform Configuration screen to change the passwords for **root** and **admin** accounts on a regular basis. You can also change the **admin** password from the Users screen. (The **root** and **support** accounts are not listed on the Users screen, however.)

To change admin or root account passwords

1. In the navigation pane, expand **System**, and click **Platform**.
   The Configuration screen opens.
2. In the User Administration section, locate **Root Account** or **Admin Account**.
3. In the **Password** box, type a new password. In the **Confirm** box, retype the same password.
4. At the bottom of the screen, click **Update**.

To change the admin password from the Users screen

1. In the navigation pane, expand **System**, and click **Users**.
   The User List screen opens, displaying a list of user accounts.
2. In the account list, click the **admin** account name.
   The Account Properties screen for the **admin** account opens.
3. For the **Password** settings, in the **New** box, type a new password. In the **Confirm** box, retype the same password.
4. At the bottom of the screen, click **Update**.

Deleting local user accounts

If the account you are using has an **Administrator** user role, you can delete other local user accounts. When you delete a local user account, you remove it permanently from the local user account database on the WANJet appliance.

◆ **Note**

*You cannot delete the **admin** user account, nor can you delete the user account with which you are logged in.*

To delete a local user account

1. In the navigation pane, expand **System**, and click **Users**.
   This opens the User List screen, displaying a list of all standard user accounts.
2. In the user account list, locate the name of the account you want to delete and click the Select box to the left of the account name.
3. Click the **Delete** button.
   A confirmation box appears.

4. Click **Delete** again.

Configuring SSH access to the WANJet appliance

When you configure SSH access, you enable or disable user access to the WANJet appliance through a Secure Shell (SSH) program, such as PuTTY or OpenSSH. You can also restrict the IP addresses that are allowed access to the system using SSH, or allow SSH access from all addresses.

The **SSH Access** setting controls all user access to the command line using SSH. You can also control terminal access for each specific user account, allowing or preventing a user from logging on at the command line. For details, see *Configuring local user accounts*, on page 6-6.

To configure SSH access

1. In the navigation pane, expand **System**, and click **Platform**.
   The Configuration screen opens.
2. For the **SSH Access** setting, check the **Enabled** box to allow access to the account, or clear the check box to prevent access to the account.
   This setting turns the SSH daemon on (when checked) and off (when cleared).
3. If you enabled SSH Access, for the **SSH IP Allow** setting, select select either * **All Addresses** or **Specify Range**, which allows you to specify a range of addresses.
4. At the bottom of the screen, click **Update**.

Configuring access to the web interface

When you configure HTTPD access, you can restrict the IP addresses that are allowed access to the web interface using https. For example, you may want to specify the subnet where the administrators reside so that only authorized users working on that subnet can log on to the WANJet appliance web interface.

To configure HTTPD access to the web interface

1. In the navigation pane, expand **System**, and click **Platform**.
   The Configuration screen opens.
2. For the **HTTPD IP Allow** setting, select either * **All Addresses** or **Specify Range**, which allows you to specify a range of addresses.
3. At the bottom of the screen, click **Update**.

Managing remote user accounts

Rather than store user accounts locally on the WANJet appliance, you can store them on a remote authentication server. In this case, you create all of your standard user accounts (including user names and passwords) on that remote server, using the mechanism supplied by that server's vendor.

Authentication for remote user accounts is based on standard HTTP authentication, that is, user name and password. The exception to this is when the remote server is specifically configured to perform SSL authentication. In this case, authentication is based on SSL certificates.

Once you have created each user account on the remote server, you can then use the WANJet appliance to assign a user role to that account, for the purpose of controlling user access to WANJet appliance resources.

◆ **Note**

The Configuration utility refers to remote user accounts as external users. An ***external user*** *is any user account that is stored on a remote authentication server.*

You assign a user role to a remote account using the Configuration utility. First, you specify the type of remote authentication server (database) that stores the remote user accounts. Then, you configure each user account to assign a user role to that account. For those remote accounts to which you do not assign a user role, the WANJet appliance assigns a default user role that you define when you identify the remote server type.

The Configuration utility stores all local and remote user-role information in the WANJet appliance's local user account database. When a user whose account information is stored remotely logs into the WANJet appliance and is granted authentication, the WANJet appliance then checks its local database to determine the user role that you assigned to that user.

◆ **Important**

Only users with the role of ***Administrator*** *can manage user roles for remote user accounts.*

Specifying a remote user account server

One of the tasks you perform with the Configuration utility is to specify the type of remote user account server that currently stores your remote user accounts. The available server types that you can specify are:

- Lightweight Directory Access Protocol (LDAP)
- Remote Authentication Dial-In User Service (RADIUS)

When you specify the type of remote server, you can also configure some server settings. For example, you can specify the user role you would like the WANJet appliance to assign to a remote account if you do not explicitly assign one.

Once you have configured the remote server, if you want any of the remote accounts to have a non-default user role, you can explicitly assign a user role to those accounts. For more information on user roles, see *Understanding user roles*, on page 6-2.

If the remote authentication server is an Active Directory or LDAP server and is set up to authenticate SSL traffic, there is an additional feature that you can enable. You can configure the WANJet appliance to perform the server-side SSL handshake that the remote server would normally perform when authenticating client traffic. In this case, you must take some preliminary steps to prepare for remote authentication using SSL.

To prepare for SSL-based remote authentication

1. Convert the Certificate Authority (CA) or self-signed certificates to PEM format.
2. On the WANJet appliance, import the certificates:
    a) In the navigation pane, expand **System**, and click **Device Certificates**.
    The Device Certificate screen opens.

    b) Click **Import**.
    The SSL Certificate/Key Source screen opens.

    c) From the **Import Type** list, select **Certificate**.

    d) In the Certificate Source area, specify whether you want to **Upload File** (type the name of the file containing the certificate or browse to it) or **Paste Text** (paste the text of the certificate in the text box).

    e) Click **Import**.
    You can store the certificates in any location on the WANJet appliance.

Once you have performed these preliminary SSL tasks, you can enable SSL as described in *To configure remote Active Directory or LDAP authentication for WANJet appliance administrative users*, following.

If the remote server is a RADIUS server, see *To configure remote RADIUS authentication for WANJet appliance administrative users*, on page 6-15.

◆ **Note**

Configuring remote authentication using the following procedures creates a user account on the WANJet appliance named ***Other External Users****. For more information on this account, see* ***Understanding default remote-account authorization****, on page 6-17.*

To configure remote Active Directory or LDAP authentication for WANJet appliance administrative users

1. In the navigation pane, expand **System**, and click **Users**.
   The Users screen opens.
2. On the menu bar, click **Authentication**.
   The Authentication screen opens.
3. Click **Change**.
4. From the **User Directory** list, select **Remote - Active Directory** or **Remote - LDAP**.
5. In the **Host** box, type the IP address of the remote server.
6. For the **Port** setting, retain the default port number (**389**) or type a new port number in the box.
   This setting represents the port number that the WANJet appliance uses to access the remote server.
7. In the **Remote Directory Tree** box, type the file location (tree) of the user authentication database on the Active Directory or LDAP server. At minimum, you must specify a domain component (that is, **dc=<value>**).
8. For the **Scope** setting, retain the default value (**Sub**) or select a new value.
   This setting specifies the level of the remote server database that the WANJet appliance should search for user authentication. For more information on this setting, see the online help.
9. For the **Bind** setting, specify a user ID login for the remote server:
   a) In the **DN** box, type the distinguished name for the remote user ID.
   b) In the **Password** box, type the password for the remote user ID.
   c) In the **Confirm** box, retype the password that you typed in the **Password** box.
10. In the **User Template** box, type the distinguished name of the user logging on to the system.
    You specify the template as a variable that the system replaces with user-specific information during the login attempt. For example, you can specify a user template such as **%s@siterequest.com** or **uid=%s,ou=people,dc=siterequest,dc=com**.

11. If you want to enable SSL-based authentication, click the **SSL** box and if necessary, configure the following settings.

    Important: *Be sure to specify the full path name of the storage location on the WANJet appliance. For example, if the certificate is stored in the directory* ***/config/wjconfig/ssl.crt****, type the value* ***/config/wjconfig/ssl.crt****.*

    a) In the **SSL CA Certificate box**, type the name of a chain certificate, that is, the third-party CA or self-signed certificate that normally resides on the remote authentication server.

    b) In the **SSL Client Key** box, type the name of the client SSL key. Use this setting only in the case where the remote server requires that the client present a certificate. If a client certificate is not required, you do not need to configure this setting.

    c) In the **SSL Client Certificate** box, type the name of the client SSL certificate.
    Use this setting only in the case where the remote server requires that the client present a certificate. If a client certificate is not required, you do not need to configure this setting.

12. From the **Role** list, select a user role that you want the WANJet appliance to assign as the default role for remote user accounts.
    The WANJet appliance assigns this user role to any remote user account to which you do not explicitly assign a role. For more information, see *Understanding default remote-account authorization*, on page 6-17.

13. If you want to enable terminal access for the remote user accounts, use the **Terminal Access** list to select **Enabled**.
    If you select **Enabled**, the WANJet appliance grants terminal access to remote user accounts by default.

14. Click **Finished**.

To configure remote RADIUS authentication for WANJet appliance administrative users

1. In the navigation pane, expand **System**, and click **Users**.
   The Users screen opens.

2. On the menu bar, click **Authentication**.
   The Authentication screen opens.

3. Click **Change**.

4. From the **User Directory** list, select **Remote - RADIUS**.

5. From the **Server Configuration** box:

   - If you are planning to use one RADIUS server only, select **Primary Only**.
   - If you want to use a secondary RADIUS server in the event that the primary server becomes unavailable, select **Primary & Secondary**.
     This causes the **Secondary** setting to appear.

6. For the **Primary** setting, configure these settings for the primary RADIUS server:

   a) In the **Host** box, type the IP address of the remote server.

   b) In the **Port** box, retain the default port number (**1812**) or type a new port number in the box.
   This setting represents the port number that the WANJet appliance uses to access the remote server.

   c) In the **Secret** box, type the RADIUS secret.

   d) In the **Confirm** box, retype the secret that you typed in the **Secret** box.
   Note that the values of the **Secret** and **Confirm** settings must match.

7. If you selected **Primary & Secondary** from the **Server Configuration** box, configure the **Host**, **Port**, **Secret**, and **Confirm** settings for the secondary server, using the instructions in the previous step.

8. From the **Role** box, select a user role that you want the WANJet appliance to assign as the default role for remote user accounts.
   The WANJet appliance assigns this user role to any remote user account to which you do not explicitly assign a role. Once you have used this screen to set up the RADIUS server, the WANJet appliance assigns this user role to any remote user account to which you do not explicitly assign a role. For more information, see *Understanding default remote-account authorization*, on page 6-17.

9. If you want to enable terminal access for the remote RADIUS user accounts, use the **Terminal Access** box to select **Enabled**.
   If you select **Enabled**, the WANJet appliance grants terminal access to remote user accounts by default.

10. Click **Finished**.

Configuring authorization for remote accounts

You create WANJet appliance user accounts on your remote server using the mechanism provided by the vendor of your remote server. Then, as described in *Specifying a remote user account server*, on page 6-12, you then use the Configuration utility to specify the remote authentication server that stores WANJet appliance user accounts.

Part of specifying the remote authentication server is configuring certain authorization properties for remote accounts. Specifically, you specify a default user role and terminal access for all user accounts to which you have not individually assigned authorization properties. For more information, see *Understanding default remote-account authorization*, following.

Once you have specified the remote server, including the default authorization properties, you can do the following:

- Change the default remote-account authorization. For more information, see *Understanding default remote-account authorization*, following.
- Assign authorization properties to an individual remote account. For more information, see *Assigning authorization to an individual user account*, on page 6-18.
- Change the authorization properties of an individual remote accounts. For more information, see *Changing authorization for an individual user account*, on page 6-19.

For descriptions of the user roles that you can assign to accounts, see *Understanding user roles*, on page 6-2.

Understanding default remote-account authorization

Sometimes, you might have remote user accounts to which you have not explicitly assigned a user role or terminal access. Such accounts appear in the list of user accounts on the User List screen as **Other External Users**.

To ensure that these accounts have a user role and terminal access assigned to them, the WANJet appliance automatically assigns default values for these properties, to ensure valid user authorization. By default, the authorization values that the WANJet appliance assigns to remote accounts are the authorization properties that you configured as part of specifying the remote authentication server. Table 6.4 lists these properties and their default values.

Remote user account property	Default value
Role	No Access
Terminal access	Disabled

Table 6.4 *Default authorization properties for remote user accounts*

You can change the values that the WANJet appliance uses as the default **Role** and **Terminal Access** values. (See *To change the default remote-account authorization*, following.) Then, whenever you create a user account on the remote server and you do not explicitly assign a user role and terminal access to that account, the WANJet appliance automatically assigns the specified default values to the account.

To change the default remote-account authorization properties, you configure the **Role** and **Terminal Access** settings on the Authentication screen that you use to specify the type of remote authentication server you are using.

To change the default remote-account authorization

1. In the navigation pane, expand **System**, and click **Users**.
   This opens the User List screen, displaying a list of all standard user accounts.
2. On the menu bar, click **Authentication**.
   This displays the Authentication screen.
3. Click **Change**.
4. From the **User Directory** list, select **Remote - Active Directory**, **Remote - LDAP**, or **Remote - RADIUS**.
5. From the **Role** list, select a default user role.
   The WANJet appliance assigns this user role to any remote account to which you have not explicitly assigned a user role.
6. From the **Terminal Access** list, select **Enabled** or **Disabled**.
7. Click **Update**.

Assigning authorization to an individual user account

As stated in the previous section, you do not use the Configuration utility to create remote user accounts for the WANJet appliance. However, if you have the **Administrator** role assigned to your own user account, you can use the Configuration utility to explicitly assign authorization properties (such as a user role) to existing remote accounts.

Note that the WANJet appliance automatically assigns a default user role to a remote account if you do not explicitly do so. For information on configuring the default user role, see *To change the default remote-account authorization*, preceding.

Use the following procedure to configure the authorization properties of an existing remote user account, if you have not already done so. (If you have already configured authorization properties of an individual account and want to change them again, see *Changing authorization for an individual user account*, preceding.)

In this procedure, instead of selecting the account name from a list of user accounts and then modifying its properties, you simulate the creation of a new account, configuring the **User Name** property with the precise name of the existing account. You then configure the other properties on the Create screen as well. In this way, you actually modify the properties of the existing remote account.

To assign authorization for an individual user account

1. In the navigation pane, expand **System**, and click **Users**.
   The User List screen opens.

   Note: *You do not see the user account in the list of user accounts.*

2. In the upper-right corner of the screen, click **Create**.
   This displays the New User screen.

3. In the **User Name** box, type the name of the remote user to which you want to assign a user role.

   Important*: This user name must precisely match the user name assigned to the remote user account.*

4. For the **Role** setting, select a user role.

5. From the **Terminal Access** box, select **Enabled** or **Disabled**, to allow or prevent access to the WANJet appliance through the command line interface.

6. Click **Finished**.

Changing authorization for an individual user account

Sometimes you might want to change the user role and terminal access that you previously assigned to a remote account. To do so, you must change the properties of that account by clicking the account name on the User List screen. Only those remote user accounts to which you have explicitly assigned a user role appear in the list of user accounts. For the procedure on changing the authorization properties for this type of account, see *To change authorization for an individual user account*, following.

Remote user accounts that simply inherit the default user role (configured when you specified the remote authentication server) appear in the list of remote user accounts under the name **Other External Users**. Consequently, you cannot change the authorization properties for any individual account of this type, that is, any account that has inherited the default authorization properties. For more information on assigning default authorization properties, see *Understanding default remote-account authorization*, on page 6-17.

To change authorization for an individual user account

1. In the navigation pane, expand **System**, and click **Users**.
   This opens the User List screen, displaying a list of user accounts to which you explicitly assigned user roles.

2. In the User Name column, click a user name.
   This displays the properties for that user account.

3. From the **Role** list, select a user role.

4. From the **Terminal Access** list, select **Enabled** or **Disabled**.

5. Click **Update**.

Viewing remote user accounts

Using the Configuration utility, you can display a list of those remote user accounts to which you explicitly assigned a non-default user role. If a remote user account has the default role assigned to it, you cannot see that account in the list of remote user accounts.

To display a list of remote user accounts with non-default user roles

1. In the navigation pane, expand **System**, and click **Users**.
   The User List screen opens, displaying a list of all standard user accounts.
2. On the menu bar, click **Authentication**.
   The Authentication screen opens.
3. Verify that the **User Directory** setting specifies a remote authentication server type (Active Directory, LDAP, or RADIUS).
4. On the menu bar, click **User List**.
5. View the list of user accounts.
   Remote user accounts that are assigned the default user role appear in the list as **Other External Users**.

To view the properties of a remote user account

1. Using the previous procedure, display a list of remote user accounts.
2. In the user account list, find the user account you want to view and click the account name.
   This displays the properties of that user account.

   Note: *The only properties displayed for a remote user account are the account name, the user role assigned to the account, and the account's terminal access.*

Deleting authorization for an individual user account

When you delete a remote user account on the WANJet appliance, you are not actually deleting the account from the remote server. Instead, you are changing the values of the user's authorization properties back to the default values. For more information on default authorization values, see *Understanding default remote-account authorization*, on page 6-17.

To delete authorization for an individual user account

1. In the navigation pane, expand **System**, and click **Users**.
   This opens the User List screen, displaying a list of all standard user accounts.
2. Locate an account name in the list and click the corresponding Select box.

3. Click **Delete**.
   A confirmation page appears.
4. Click **Delete**.

◆ **Note**

To delete a remote user account altogether, follow the instructions provided by the server vendor.

7

Configuring WANJet Appliance Policies

- Introducing WANJet appliance policies
- Creating optimization policies
- Creating Application QoS policies
- Defining traffic classes
- Managing policies with Enterprise Manager

Introducing WANJet appliance policies

You create policies on the WANJet appliance so that it handles traffic according to your needs. The WANJet appliance has two types of policies:

- **Optimization policies**
  You create optimization policies to specify which traffic you want to optimize (move faster through the network), and which traffic you want to pass through the WANJet appliance without being changed.
- **Application QoS policies**
  You create Application QoS policies to dedicate a percentage of bandwidth to certain applications to ensure predictable application performance.

This chapter describes how to create, edit, and delete optimization policies that apply to links with all remote WANJet appliances. It also explains how to create exceptions to optimization policies called passthrough destinations. The chapter also describes how to create, edit, and delete Application QoS policies, and how to add, edit, or delete WAN links. You can create ***traffic classes*** to gather together specific types of applications with the idea of applying one Application QoS policy on them as a group.

If you are using Enterprise Manager to manage multiple WANJet appliances, you can create optimization policies and Application QoS policies on one WANJet appliance, and use the changeset feature to apply these policies to multiple WANJet appliances. For more information, see the ***Enterprise Manager Administrator Guide***.

Creating optimization policies

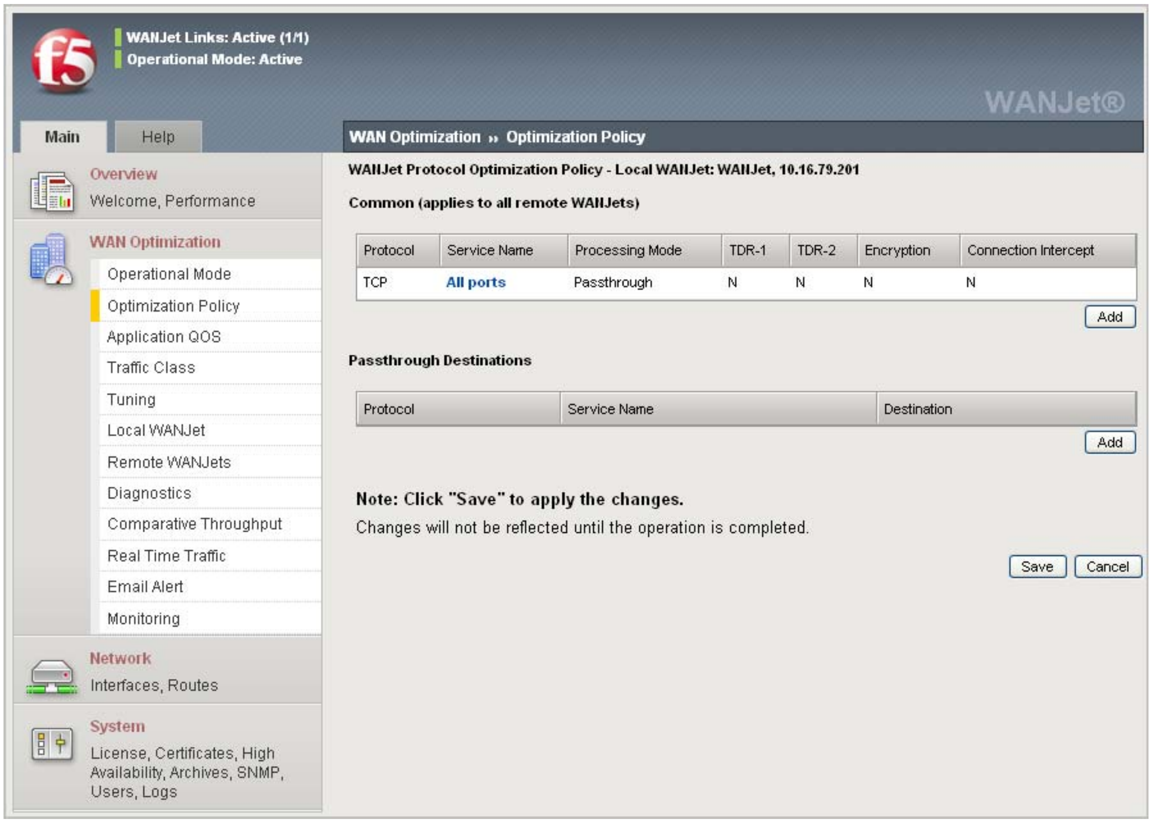
You use optimization policies to specify where and how you want the WANJet appliance to optimize traffic. Optimization policies designate the TCP ports on which the WANJet appliance applies Transparent Data Reduction (TDR) optimization algorithms, and other options including encryption and connection intercept.

The decisions whether to optimize traffic and what options to use are made on the WANJet appliance where the traffic was initiated. Traffic coming from another WANJet appliance on the other side of the WAN is optimized according to the optimization policies on the other WANJet appliance.

To develop your overall optimization plan, you need to complete two tasks:

- Create common optimization policies that you want to apply to connections with all remote WANJet appliances.
  See the next section, *Managing optimization policies*.
- Create exception policies for passthrough traffic.
  See *Managing passthrough destinations*, on page 7-6.

Figure 7.1 shows the Optimization Policy screen.



WANJet Protocol Optimization Policy - Local WANJet: WANJet, 10.16.79.201

Common (applies to all remote WANJets)

Protocol	Service Name	Processing Mode	TDR-1	TDR-2	Encryption	Connection Intercept
TCP	All ports	Passthrough	N	N	N	N

Passthrough Destinations

Protocol	Service Name	Destination

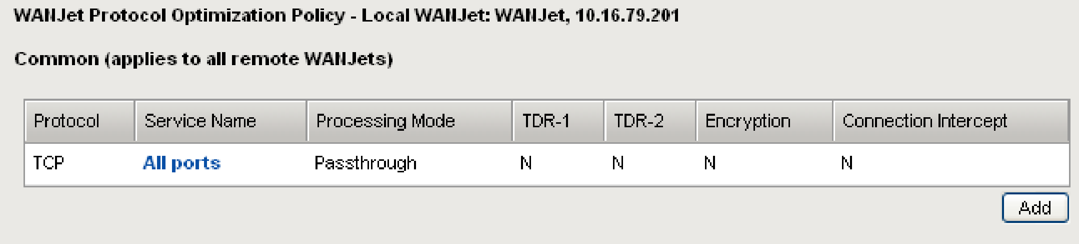
Note: Click "Save" to apply the changes.
Changes will not be reflected until the operation is completed.

Figure 7.1 *Optimization Policy screen*

Before creating optimization policies, you need to have added local subnets from which the WANJet appliance may receive traffic that you want to optimize. Otherwise, traffic from subnets that the WANJet appliance does not recognize is set to passthrough, and it is not optimized. See *Configuring multiple subnets*, on page 3-5, for instructions on how to add local subnets.

Managing optimization policies

Optimization policies apply globally to traffic moving between the local WANJet appliance and remote WANJet appliances. You can create policies for traffic destined for all ports or for specific ports. By default, traffic destined for **All ports** is set to **Passthrough**; it is not optimized for TDR-1 or TDR-2, it is not encrypted, and **Connection Intercept** is not enabled, as shown in Figure 7.2.



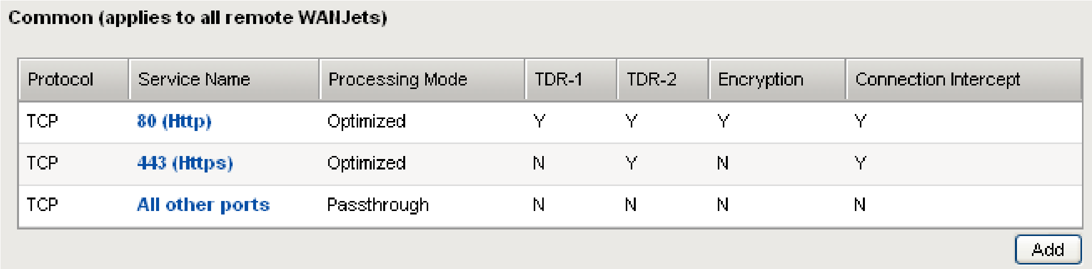
WANJet Protocol Optimization Policy - Local WANJet: WANJet, 10.16.79.201

Common (applies to all remote WANJets)

Protocol	Service Name	Processing Mode	TDR-1	TDR-2	Encryption	Connection Intercept
TCP	All ports	Passthrough	N	N	N	N

Figure 7.2 *Default optimization policy*

You have to edit the default optimization policy or create a new one before you can start optimizing traffic between the local and remote WANJet appliances. When you create new optimization policies, the original optimization policy designated for **All ports** changes to **All other ports**, as shown in Figure 7.3.



Common (applies to all remote WANJets)

Protocol	Service Name	Processing Mode	TDR-1	TDR-2	Encryption	Connection Intercept
TCP	80 (Http)	Optimized	Y	Y	Y	Y
TCP	443 (Https)	Optimized	N	Y	N	Y
TCP	All other ports	Passthrough	N	N	N	N

Figure 7.3 *Optimization policies*

It is typical to have optimization enabled on commonly used ports such as those used for Active FTP, SMTP, HTTP, POP3, IMAP, and HTTPS. You can also consider enabling TDR-1 compression on these ports, except for port **443** (HTTPS).

◆ **Note**

It is difficult to optimize Passive FTP sessions because the server port that Passive FTP uses varies from session to session. However, 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).

You can create new optimization policies, edit existing policies, or delete policies. The optimization policies are of primary importance on the client side WANJet appliance, for example, where users are requesting application data from a data center or hub. You can also add exceptions to the optimization policies as described in *Managing passthrough destinations*, on page 7-6.

To create optimization policies

1. In the navigation pane, expand **WAN Optimization** and click **Optimization Policy**.
   The WANJet Protocol Optimization Policy screen opens.
2. Click the **Add** button located beneath the Common policies table. The Add Port/Service Name popup screen opens.
3. From the **Service Name** list, select the service or application for which you want to customize the optimization policy. The default port used by the service displays in the **From Port** box.

   If you would rather specify the port, 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 the **To** box.

   Note*: Refer to* ***http://www.iana.org/assignments/port-numbers*** *for a list of commonly assigned TCP 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 and do not optimize it.
   - **Optimized**
     Apply WANJet appliance optimization to traffic over this port according to the options specified in the next step.

5. Select one or more WANJet appliance optimization options by checking the check boxes. If you do not select any of the options, traffic is optimized using TCP optimization. TCP optimization adapts the connection to the properties of the WAN link, improving performance and handling congestion control.

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

   - **TDR-1**: Check this box to compress network traffic for the specified port. This is not necessary if the traffic would not benefit from compression, for example if it consists largely of JPEG or ZIP files.
   - **TDR-2**: Check this box to apply the WANJet appliance's TDR-2 intelligent caching algorithm for communications on the specified port.
   - **Encryption**: Check this box if you want to use SSL to encrypt communications for the specified port.
   - **Connection Intercept**: Check this box to reset any connection for the specified port that was initiated before you started the WANJet appliance. For more details, see *Resetting connections with Connection Intercept*, on page 1-9.

6. Click the **OK** button.
   The window closes and the WANJet Protocol Optimization Policy screen displays with a new row in the Common policies table with the details that you entered. You can click the port number (in the Service Name column) to edit these settings.

7. Click the **Save** button at the bottom of the WANJet Protocol Optimization Policy screen to apply the new policy.
   The new policy takes effect immediately for all new connections.

To edit optimization policies

1. In the navigation pane, expand **WAN Optimization** and click **Optimization Policy**.
   The WANJet Optimization Policy screen opens.

2. In the list of optimization policies, click the Service Name link of the policy you want to edit.
   The Edit Port/Service Name popup screen opens.

3. Edit the settings as needed.

4. Click the **OK** button.
   The screen closes.

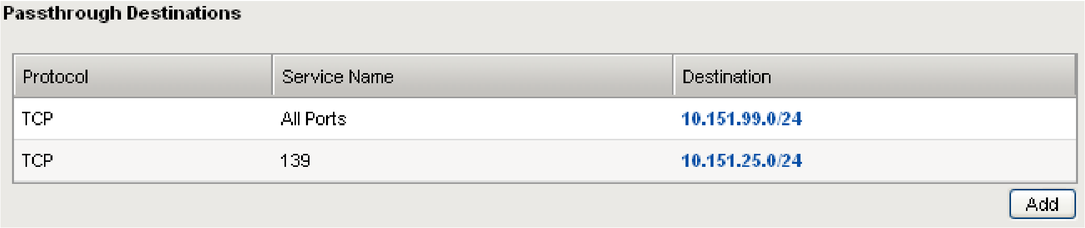
5. Click the **Save** button at the bottom of the WANJet Protocol Optimization Policy screen.
   Changes to optimization policies take effect for all new connections.

To delete optimization policies

1. In the navigation pane, expand **WAN Optimization** and click **Optimization Policy**.
   The WANJet Optimization Policy screen opens.
2. In the list of optimization policies, click the Service Name link of the policy you want to delete.
   The Edit Port/Service Name popup screen opens.
3. Click **Remove**.
   The screen closes and the policy is deleted from the common optimization policies list.
4. Click the **Save** button at the bottom of the WANJet Protocol Optimization Policy screen.

Managing passthrough destinations

You can make exceptions to the optimization policies for specific systems or subnets by creating passthrough destinations. Traffic that flows to ***passthrough destinations*** is not optimized. So, for example, you could optimize traffic to all ports by creating an optimization policy that applies to most traffic, then specify passthrough destinations for any exceptions, as shown in Figure 7.4.



Passthrough Destinations

Protocol	Service Name	Destination
TCP	All Ports	10.151.99.0/24
TCP	139	10.151.25.0/24

Figure 7.4 *Passthrough destinations: exceptions to optimization policies*

Figure 7.4 shows exceptions that were added for two subnets. The WANJet appliance does not optimize traffic destined for **All Ports** on systems in subnet **10.151.99.0/24**. It also does not optimize traffic destined for port **139** on systems in subnet **10.151.25.0/24**. Traffic for these destinations is set to passthrough.

You can create new passthrough destinations, edit existing passthrough destinations, or delete passthrough destinations.

To create passthrough destinations

1. In the navigation pane, expand **WAN Optimization** and click **Optimization Policy**.
   The WANJet Protocol Optimization Policy screen opens.
2. Click the **Add** button located beneath the Passthrough Destinations table.
   The Passthrough Destination popup screen opens.
3. In the **Destination Address** box, type the IP address of the host or subnet where you do not want the traffic to be optimized. For example, specify the subnet **10.8.0.0/24** as:

   ```
   10.8.0.0
   ```
4. In the **Destination Netmask** box, type the netmask of the host or subnet. For example:

   ```
   255.255.255.0
   ```
5. For the **Destination Port** setting, determine which ports to use:
   - Check the **All Ports** box if you want all ports at the destination address to receive passthrough traffic.
   - Clear the **All Ports** box and type the port number of the port at the destination address you want to receive passthrough traffic.
6. Click **OK**.
   The exception is added to the list of passthrough destinations.

To edit passthrough destinations

1. In the navigation pane, expand **WAN Optimization** and click **Optimization Policy**.
   The WANJet Optimization Policy screen opens.
2. In the list of passthrough destinations, click the Destination link of the exception you want to edit.
   The Edit Port/Service Name popup screen opens.
3. Edit the settings as needed.
4. Click **OK**.
   The screen closes.
5. Click the **Save** button at the bottom of the WANJet Protocol Optimization Policy screen.
   Changes to exceptions take effect for all new connections.

To delete passthrough destinations

1. In the navigation pane, expand **WAN Optimization** and click **Optimization Policy**.
   The WANJet Optimization Policy screen opens.
2. In the list of passthrough destinations, click the Destination link of the exception you want to delete.
   The Edit Port/Service Name popup screen opens.

3. Click the **Remove** button.
   The screen closes and the policy is deleted from the common policies list.
4. Click the **Save** button at the bottom of the WANJet Protocol Optimization Policy screen.

Example: CIFS optimization policy with Connection Intercept

Connection Intercept is one of the options that the WANJet appliance provides for optimization policies. This option causes the WANJet appliance to reset connections that were initiated before it started up. One of the uses of Connection Intercept is for client systems that use the CIFS (Common Internet File System) protocol to request file services from server systems over a network.

In this example, the administrators are concerned that they may have existing CIFS connections, already in progress, that are not being optimized after starting or restarting the WANJet appliance. The procedure shows how to create an optimization policy that enables the Connection Intercept option on the CIFS ports (typically ports **139** and **445**). This causes the WANJet appliance to automatically reset connections that are not being optimized, without having to restart each of the connections manually.

To automatically reset CIFS connections

1. In the navigation pane, expand **WAN Optimization** and click **Optimization Policy**.
   The WANJet Optimization Policy screen opens.
2. Under the Common policies table, click **Add**.
   The Add Port/Service Name popup screen opens.

   Note: *If the* ***Netbios-ssn*** *service is already listed, click the Service Name so you can edit the settings.*
3. From the **Service Name** list, select **Netbios-ssn**.
   In the **From Port** box, port **139** is automatically displayed.
4. For the **Processing Mode**, select **Optimized**.
5. Check the **TDR-1** and **TDR-2** boxes.
6. Check the **Connection Intercept** box.
7. Click **OK**.
   The Edit Port/Service Name screen closes, and you see the WANJet Protocol Optimization Policy screen.
8. Repeat steps 2-6 to add **Microsoft-ds** (port **445**).
9. Click the **Save** button to apply the changes.
10. In the navigation pane, expand **WAN Optimization** and click **Operational Mode**.
    The Operational Mode screen opens.
11. Verify that **Mode** is set to **Active**.

12. Click the **Save** button if you changed the mode.
    This implements Connection Intercept on ports **139** and **445**. The next time you restart the WANJet appliance, it resets connections that were already initiated on these ports, and then optimizes the traffic.

Creating Application QoS policies

Application QoS policies help you to obtain better network performance by dedicating bandwidth to specific network traffic that travels between two WANJet appliances or over a WAN link.

When you define an Application QoS policy, you can specify 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. So, for example, you might want to limit the amount of bandwidth that FTP or email (SMTP, POP, or IMAP) traffic can use, and provide more bandwidth for VoIP traffic.

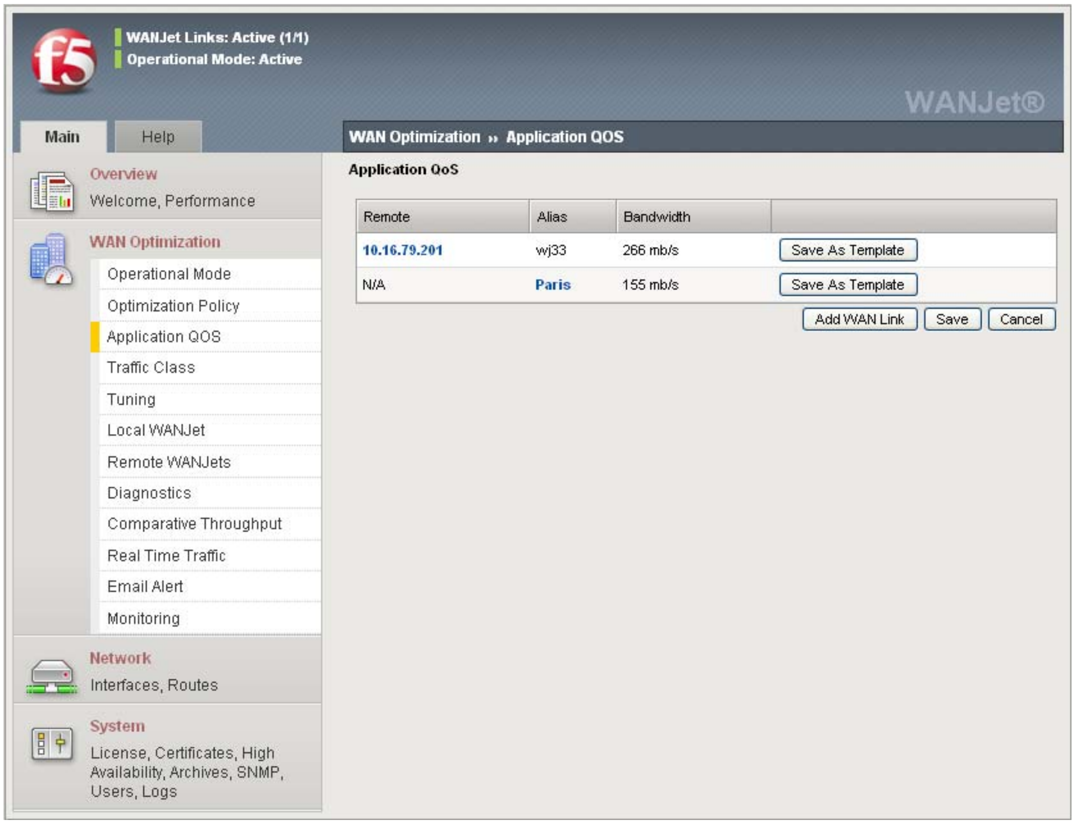
At the same time, you need to ensure that providing sufficient bandwidth to one or more data flows does not handicap the transmission of other data. ***Application QoS*** is a per endpoint setting that you can use to override the tuning page bandwidth setting in a multi-node network.

You can create Application QoS policies for two types of services:

- **Services**
  The basic protocols supported by your network, such as FTP, HTTP, HTTPS, Pop3, and so on.
- **Traffic classes**
  Tailored services that include different types of traffic. If you want to create an Application QoS policy to handle tailored services, you need to have already created or imported the traffic class. See *Defining traffic classes*, on page 7-17.

Most often you create Application QoS policies for traffic moving between two WANJet appliances. Thus, it is important that you have previously configured remote WANJet appliances (and their local subnets). The Application QoS screen, shown in Figure 7.5, lists all of the remote links so that you can create Application QoS policies to shape the traffic between the local and remote WANJet appliances.

If you want to create Application QoS policies for traffic going to an office that does not have a WANJet appliance, follow the procedure described in *Managing Application QoS policies for WAN links*, on page 7-13.



WANJet Links: Active (1/1)
Operational Mode: Active

WAN Optimization » Application QOS

Application QoS

Remote	Alias	Bandwidth	
10.16.79.201	wj33	266 mb/s	Save As Template
N/A	Paris	155 mb/s	Save As Template

Figure 7.5 *Application QoS screen*

In Figure 7.5, you can see one remote WANJet appliance called **wj33** with an IP address of **10.16.79.201** and one WAN link called **Paris** that was added. You can create Application QoS policies for both of these links.

Creating, editing, and deleting Application QoS policies

Before you create Application QoS policies, you need to plan how you want to allocate bandwidth. You need to be familiar both with the major applications that your users work with, and which ones require faster transfer times. You can assign a larger percentage of bandwidth to the highest priority applications.

You can add, edit, or remove Application QoS policies.

To add an Application QoS policy to the link between the local and remote WANJet appliances

1. In the navigation pane, expand **WAN Optimization** and click **Application QoS**.
   The Application QoS screen opens and lists the remote WANJet appliances.

2. In 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 popup screen opens.

3. In the **Link Bandwidth** box, type the bandwidth of the link between the local and the remote WANJet appliances, and from the **Link Bandwidth** list, select a unit (Kb/s or Mb/s).

4. Click the **Add** button.
   The Application QoS Policy popup screen opens.

5. In the **Alias** box, type a name for the policy.

6. In the **Bandwidth** box, type the percentage of bandwidth that you want to guarantee that the policy can use. For example, if you specify 50%, the connections associated with the policy are guaranteed 50% of the available bandwidth if needed.

   Note: *The bandwidth that you allocate to all of the Application QoS policies should not exceed 100%.*

7. In the **Maximum** box, type the maximum percentage that the policy can borrow from unused additional bandwidth. For example, if you specify 90%, the connections associated with the policy can use up to 90% of the additional bandwidth that is available.

8. In the **Services** box, specify the services or traffic classes to use for the Application QoS policy. For each service that you add, specify these settings:

   a) From the **Services** list, select the service or traffic class to add to the Application QoS policy.

   b) From the adjacent service type list, select the associated protocol (TCP or UDP), if applicable.

      Note*: You can configure some ports for both TCP and UDP protocols. To do this, select the service port (for example,* ***FTP****) and then select* ***TCP****. Then on a new line, select service* ***FTP*** *again, and service type* ***UDP****. If you select* ***VoIP****, it uses only the UDP protocol. If you choose a defined traffic class from the menu, the adjacent service type menu disappears.*

   c) Click the **OK** button.
      The Manage the Application QoS Settings of a Remote WANJet appliance popup screen opens.

9. Repeat steps 4-8 to add as many other Application QoS policies as you need.

10. Click the **OK** button.
    The Manage the Application QoS Settings of a Remote WANJet appliance popup screen closes.

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

To edit an Application QoS policy

1. In the navigation pane, expand **WAN Optimization** and click **Application QoS**.
   The Application QoS screen opens and lists the remote WANJet appliances.

2. In the Remote column, click the link to the remote WANJet appliance with the Application QoS policy that you want to edit.
   The Manage the Application QoS Settings of a Remote WANJet appliance popup screen opens listing the subnets.

3. Click the link for the Application QoS policy that you want to edit.

4. Edit the settings to alter the existing Application QoS policy settings.

5. Click the **OK** button.

6. Click the **Save** button.
   The Application QoS screen refreshes.

To disable an Application QoS policy

1. In the navigation pane, expand **WAN Optimization** and click **Application QoS**.
   The Application QoS screen opens.

2. Click the link for the remote WANJet appliance with the Application QoS policy that you want to disable.
   The Manage the Application QoS Settings of a Remote WANJet appliance popup screen opens.

3. In the **Link Bandwidth** box, type **0** for the bandwidth.

4. Click **OK**.

5. Click the **Save** button.
   The Application QoS screen refreshes. The Application QoS policy remains on the WANJet appliance but it is disabled.

To remove an Application QoS policy

1. In the navigation pane, expand **WAN Optimization** and click **Application QoS**.
   The Application QoS screen opens.

2. Click the link for the remote WANJet appliance from which you want to remove an Application QoS policy.
   The Manage the Application QoS Settings of a Remote WANJet appliance popup screen opens.
3. Click the link for the Application QoS policy that you want to remove.
4. Click the **Remove** button to delete the policy.
   The Application QoS policy is removed from the WANJet appliance.
5. Click **OK**.
6. Click the **Save** button.
   The Application QoS screen refreshes.

Managing Application QoS policies for WAN links

When you configure remote WANJet appliances on the local appliance, WAN links are automatically created as connections between the two WANJet appliances. (The section *Creating, editing, and deleting Application QoS policies*, on page 7-10 describes how to create QoS policies for links between two WANJet appliances.) You can add WAN links if you want to create an Application QoS policy for traffic that is going from the local WANJet appliance to a location that does not have a WANJet appliance. You then specify the destination subnets or machines for existing WAN links.

Using WAN links, you can add an Application QoS policy to the traffic passing through the local WANJet appliance and going to a remote network, even if the remote network does not have a 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 whether it is being optimized.

Creating an Application QoS policy for a link between a WANJet appliance and another location that does not have a WANJet appliance involves the following tasks:

- Adding a WAN link
- Specifying the destination subnets for the WAN link
- Creating the Application QoS policy for the WAN link

The tasks are described in the following procedure.

To create an Application QoS policy for a WAN link

1. In the navigation pane, expand **WAN Optimization** and click **Application QoS**.
   The Application QoS screen opens.

2. Add the WAN link between the WANJet appliance and the location that does not have one:

   a) Click the **Add WAN Link** button.
   The Manage the Application QoS Settings of a WAN Link popup screen opens.

   b) In the **WAN Link Alias** box, type a name.

   c) In the **Link Bandwidth** box, type the size of the bandwidth between the local WANJet appliance and the WAN network.

   d) From the **Link Bandwidth** list, select a unit (**kb/s** or **mb/s**).

   e) Click **OK**.
   The Manage the Application QoS Settings of a WAN Link screen closes, and the Application QoS screen refreshes with the new WAN link displayed.

3. Add the destination subnets for the WAN link:

   a) Click the **Add** button beneath the Supported Subnet table.
   The Add Subnet popup screen opens.

   b) In the **Supported Subnet** box, type the IP address of the machine or subnet that the WAN link connects to.

   c) In the **Netmask** box, type the netmask of the new machine or subnet.

   d) In the **Machine(s) Alias** box, type a name for the new machine or subnet.

   e) Click **OK**.
   The Application QoS screen opens, and the new subnet appears in the Support Subnet column.

4. Create Application QoS policies that guarantee a certain percentage of bandwidth to specific services:

   a) Click the **Add** button beneath the Application QoS table.
   The Application QoS Policy popup screen opens.

   b) In the **Alias** box, type a name for the policy.

   c) In the **Bandwidth** box, type the percentage of bandwidth that you want to guarantee that the policy can use. For example, if you specify 50%, the connections associated with the policy are guaranteed 50% of the available bandwidth if needed.

   Note: The bandwidth that you allocate to all of the Application QoS policies should not exceed 100%.

   d) In the **Maximum** box, type the maximum percentage that the policy can borrow from unused additional bandwidth. For example, if you specify 90%, the connections associated with the policy can use up to 90% of the additional bandwidth that is available.

e) In the **Services** box, specify the services or traffic classes to use for the Application QoS policy. For each service that you add:

- From the **Services** list, select the service or traffic class to add to the Application QoS policy.
- From the adjacent service type list, select the associated protocol (TCP or UDP), if applicable.

  Note: You can configure some ports for both TCP and UDP protocols. To do this, select the service port (for example, **FTP**) and then select **TCP**. Then on a new line, select service **FTP** again, and service type **UDP**. If you select **VoIP**, it uses only the UDP protocol. If you choose a defined traffic class from the menu, the adjacent service type menu disappears.
- Click **OK**.
  The Manage the Application QoS Settings of a Remote WANJet appliance popup screen opens.

f) Repeat steps 4-8 to add as many other Application QoS policies as you need.

5. Click the **Save** button to save the changes.

To edit Application QoS policies for a WAN link

1. In the navigation pane, expand **WAN Optimization** and click **Application QoS**.
   The Application QoS screen opens.
2. In the Alias column, click the name of the link that corresponds to the WAN Link that you want to edit.
   The Manage the Application QoS Settings of a WAN Link popup screen opens.
3. Edit the WAN Link settings, add or remove subnets, and modify the Application QoS policies as needed.
4. Click **OK**.
   The Manage the Application QoS Settings of a WAN Link screen closes, and the Application QoS screen refreshes.
5. Click the **Save** button.

To disable an Application QoS policy for a WAN link

1. In the navigation pane, expand **WAN Optimization** and click **Application QoS**.
   The Application QoS screen opens.
2. In the Alias column, click the name of the link that corresponds to the WAN Link that you want to disable.
   The Manage the Application QoS Settings of a WAN Link popup screen opens.
3. In the **Link Bandwidth** box, type **0** for the bandwidth.
4. Click **OK**.

5. Click the **Save** button.
   The Application QoS screen refreshes. The Application QoS policy remains on the WANJet appliance but it is disabled.

To remove a WAN link and associated Application QoS policies

1. In the navigation pane, expand **WAN Optimization** and click **Application QoS**.
   The Application QoS screen opens.
2. In the Alias column, click the name of the link that corresponds to the WAN Link that you want to remove.
   The Manage the Application QoS Settings of a WAN Link popup screen opens.
3. Click **Remove**.
4. Click **OK**.
   The Manage the Application QoS Settings of a WAN Link screen closes, and the Application QoS screen refreshes.
5. Click the **Save** button.

Defining traffic classes

With the traffic class feature, you define services that you can use to achieve specific QoS standards. You can group ports, machines, and subnets under the heading of a traffic class. By assigning both a guaranteed 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 a single type of traffic.

You can use the WANJet appliance to define traffic classes and Application Quality of Service (QoS) policies for your various applications, and apply them to optimally allocate bandwidth. A ***traffic class*** is a named group of ports, machines, and subnets. When creating an Application QoS policy, you can specify the bandwidth for a traffic class (or multiple services grouped together) instead of specifying each specific service.

Adding, editing, or removing a traffic class

You can add, edit, or remove a traffic class.

To add a traffic class

1. In the navigation pane, expand **Optimization** and click **Traffic Class**.
   The WANJet Traffic Classes screen opens.
2. Click the **Add** button.
   The Add Traffic Class popup screen opens.
3. In the **Traffic Class Name** box, type a name for the policy.
4. In the **From** box, type the IP address of the subnet that sends the data, for which you want to specify a traffic class.
5. In the **Netmask** box, type the full netmask of the subnet that sends the data, for which you want to specify a traffic class.
6. In the **To** box, specify the subnet that receives the data, for which you want to specify a traffic class.
7. In the **To Netmask** box, type the full netmask of the subnet that receives the data, for which you want to specify a traffic class.
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 **OK**.
    The Add Traffic Class screen closes, and the WANJet Traffic Classes screen refreshes with the new traffic class displayed.

11. Click the **Save** button to save the changes.

To edit a traffic class

1. In the navigation pane, expand **Optimization** and click **traffic class**.
   The WANJet Traffic Classes screen opens.
2. Click the name of the traffic class that you want to edit or remove.
   The Edit Traffic Class screen displays in a separate browser window.
3. Edit the traffic class settings as needed.
4. Click **OK**.
   The Edit Traffic Class screen closes and the WANJet Traffic Classes screen refreshes.
5. Click the **Save** button to save the changes.

To remove a traffic class

1. In the navigation pane, expand **Optimization** and click **traffic class**.
   The WANJet Traffic Classes screen opens.
2. Click the name of the traffic class that you want to remove.
   The Edit Traffic Class screen displays in a separate browser window.
3. Click the **Remove** button.
   The Edit Traffic Class screen closes and the WANJet Traffic Classes screen refreshes.
4. Click the **Save** button to save the changes.

Managing policies with Enterprise Manager

You can deploy and manage multiple WANJet appliances from the Enterprise Manager, a centralized management solution. You need to have purchased and set up Enterprise Manager, which is a separate product from the WANJet appliance. Refer to the ***Enterprise Manager Administrator Guide*** for information about configuring Enterprise Manager and complete instructions on using the features mentioned in this section.

You can create optimization policies and Application QoS policies on the WANJet appliance, and use Enterprise Manager to push the policy templates to multiple WANJet appliances. The policies that you deploy completely replace any existing policies on those WANJet appliances. This section provides information on how to create the policy templates on the WANJet appliance.

Creating optimization policy templates

To create optimization policy templates that you can apply to multiple WANJet appliances, complete these tasks:

1. Create the optimization policy on one WANJet appliance as described in *Managing optimization policies*, on page 7-3. Saving the policy creates an XML file that includes the policy.

2. From Enterprise Manager, use the **Changesets** feature to apply the optimization policy to multiple WANJet appliances. Follow through the screens specifying required information, and note the following tips:

    - For the **Source**, select **Device** and point to the WANJet appliance where you created the optimization policy.

    - On the Class Selection screen, from the **Available** path list, move **WAN Optimization/Optimization** to the **Selected** list.

3. Deploy the changeset using the **Staged Changesets** feature.
   Note these tips:

    - The changesets completely overwrite any optimization policies on the appliances where you deploy them.

    - You can create a device group that includes all WANJet appliances where you want to deploy the optimization policy. (You can use the same group for deploying both types of policies.)

    - You can save the changeset and use the Staged Changeset feature to deploy the optimization policy template.

Creating Application QoS policy templates

To create Application QoS policy templates that you can apply to multiple WANJet appliances, follow these general steps:

1. Create the Application QoS policy on one WANJet appliance as described in *Creating, editing, and deleting Application QoS policies*, on page 7-10.
2. On the Application QoS screen, on the line where the remote WANJet appliance or WAN link containing the Application QoS policy is listed, click **Save As Template**.
3. In the Alias column, click the name of the link that corresponds to the WAN Link that you want to edit or remove.
4. From Enterprise Manager, use the **Changesets** feature to apply this Application QoS policy to multiple WANJet appliances. Follow through the screens specifying required information, and note the following tips:
    - For the **Source**, select **Device** and point to the WANJet appliance where you created the Application QoS policy.
    - On the Class Selection screen, from the **Available** path list, move **WAN Optimization/Quality of Service** to the **Selected** list.
5. Deploy the changeset using the **Staged Changesets** feature.
   Note these tips:
    - The changesets completely overwrite any Application QoS policies on the appliances where you deploy them.
    - You can create a device group that includes all WANJet appliances where you want to deploy the Application QoS policy. (You can use the same group for deploying both types of policies.)
    - You can save the changeset and use the Staged Changeset feature to deploy the Application QoS policy template.

8

Configuring Advanced Settings

- Introducing advanced configuration
- Adjusting tuning settings
- Configuring email alerts
- Setting operational modes
- Managing device certificates
- Configuring redundant peers
- Configuring one-arm topology
- Restoring factory default values

Introducing advanced configuration

The WANJet appliance includes additional settings that you can configure as needed. It is important that you have a good understanding of your network configuration to perform advanced configuration.

You can configure the following advanced settings:

- **Tuning settings:** Explains ways to control traffic speed. You can specify the link bandwidth and Round Trip Time (RTT) for the WAN link according to bandwidth specified on the WANJet appliance license. A congestion control setting lets you control the amount of traffic the WANJet appliance sends depending on networking conditions. You rarely need to change the tuning settings.
- **Email alerts:** Lets you configure the system to send an email alert in case of system failure. You configure this setting if you want an administrator to receive immediate notice if the system fails.
- **Operational modes:** Allows you to specify whether the system is active or inactive, whether to use disks for data storage (if available on the system), how to handle traffic in case of failure on WANJet 400 platforms, and how to deploy the appliance (inline or one-arm).
- **Device certificates:** Lets you view, import, or export device certificates on the system.
- **Redundant peers:** Describes how to configure a second WANJet appliance as a redundant peer.
- **One-arm topology:** Explains using an alternative deployment method, where the appliance connects to the LAN and has no direct connection to the WAN.
- **Factory default values:** Describes how to return all configuration settings to their factory default values.

Adjusting tuning settings

From the WANJet Tuning screen, you can guarantee maximum throughput by specifying the link bandwidth and the Round Trip Time (RTT) for the WAN link. The maximum bandwidth value is a global setting that relates to the WANJet appliance license that your company purchased. In most cases, F5 Networks does not recommend changing the bandwidth value.

Enabling congestion control causes the WANJet appliance to control the amount of traffic it sends depending on the current networking conditions; it sends less traffic when there is significant packet loss or congestion, but typically causes the network to perform better. When you disable congestion control, the WANJet appliance continues sending packets at full speed regardless of adverse networking conditions.

◆ **Important**

You should modify the tuning settings only when initially setting up the WANJet appliance (after licensing), or if the bandwidth of your WAN link changes. Once they are set, you rarely need to change the tuning settings.

To modify tuning settings

1. In the navigation pane, expand **WAN Optimization** and click **Tuning**.
   The WANJet Tuning screen opens.

2. In the **Bandwidth** box, type a value for your WAN link bandwidth. You can set it to the bandwidth for which the appliance is licensed, or to a lower value. The default bandwidth varies depending on the license purchased and the platform. You can adjust the value lower than the default (but not higher), and 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. You determine the RTT by using the ping utility to send a request to a device on the other side of the WAN link and reviewing the command output. The default RTT is **300** milliseconds.

4. Check the **Congestion Control** box to have the WANJet appliance handle traffic if congestion occurs in the case of packet loss. The **Congestion Control** box is checked by default.

5. Click the **Save** button.
   The WANJet Tuning screen refreshes, and the WANJet appliance saves the changes.

Configuring email alerts

You can configure the WANJet appliance to send an email that includes a system snapshot (containing current system information) to a specific email address in the event of system failure. To successfully send email alerts, the WANJet appliance must be able to access the mail server. For example, if your SMTP server is on a network that is not accessible from your Management port, you need to set up a management route to the SMTP server. See *Adding routes*, on page 9-7.

For information about how to download system snapshots directly, refer to *Diagnostic Log*, on page 12-20.

To configure email alerts

1. In the navigation pane, expand **WAN Optimization** and click **Email Alert**.
   The WANJet Email Alert screen opens.

2. In the **Email address** box, type the email address to which you want the system snapshot sent. If you want the email alert to go directly to F5 Networks, type **WANJetSupport@f5.com**.

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 to pass through spam filters. F5 Networks recommends that you use the alias of the WANJet appliance 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@company.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.

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 enable the email alert, check the **Enabled** box.

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

7. Click the **Test Me** button to confirm that the WANJet appliance 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 appliance does not attempt to resend failed emails.

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

Setting operational modes

You can set operational modes on the WANJet appliance. From the Operational Mode screen, you can:

- Specify the operating mode of the WANJet appliance (whether it is active or inactive).
- Enable or disable TDR-2 disk storage (only available if the appliance has disk storage)
- Determine how you want to handle traffic in case of failure (only available on the WANJet 400 platform).
- Specify how to deploy the WANJet appliance in your network topology (inline or one-arm).

To configure the operational mode settings

1. In the navigation pane, expand **WAN Optimization** and click **Operational Mode**.
   The Operational Mode screen opens.
2. For the **Mode** setting, select one of the following options:
   - **Active**
     Enables optimization.
   - **Inactive**
     Optimization does not occur and the WANJet appliance is completely transparent to network traffic.
3. If your hardware platform includes a hard disk drive, for the **TDR-2 Storage Mode** setting, select one of the following options:
   - **Disk Based Storage**
     If the information being optimized consists of large data sets, this option provides better performance. This is the default value.
   - **Memory Based Storage**
     If the information being optimized consists of smaller data sets, this option provides faster throughput.
4. For the **Failure Mode** setting (WANJet 400 only), select one of the following options:
   - **Fail to Wire** (default)
     If the WANJet appliance fails for any reason, network traffic continues to flow and bypasses the WANJet appliance.

- **Fail Close**
  If the WANJet appliance fails for any reason, the appliance breaks the link and stops traffic from passing through.

*Note: If you select **Fail Close** on a WANJet 400, you must also make a hardware adjustment on the appliance. Refer to **To enable Fail Close on WANJet 400 hardware**, following, for instructions on how to open the unit and change the setting on the NIC.*

5. For the **Topology** setting, specify the way the WANJet appliance is connected to the network by clicking one of the options:
   - **In-Line**
     This is the most common network topology. ***Inline*** means that the WANJet appliance 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 appliance is located on a separate, independent link. Refer to *Configuring one-arm topology*, on page 8-11, for additional instructions.
6. Click the **Save** button.

To enable Fail Close on WANJet 400 hardware

1. Set the **Failure Mode** setting to **Fail Close** as described in the previous procedure, *To configure the operational mode settings*. (Do not forget to click **Save** to save the changed setting.)
2. Shut down the WANJet 400 appliance. See *Shutting down and restarting the WANJet appliance*, on page 5-16.
3. Turn the WANJet appliance upside down. On the bottom of the unit, unscrew the four screws on the left and right edges of the unit.
4. Slide the cover off the top of the WANJet 400 appliance.
5. Facing the front of the WANJet 400 appliance, locate the PXG2BP NIC card on the right near the front of the unit.
6. Tip the WANJet 400 appliance over onto the left side so you can see the buttons on the NIC card better.
7. On the upper right of the NIC card, locate the two switches (labeled **BYPASS MODE**).

   The ENB switch is on the left (towards the front of the card), and is turned off by default. The DIS switch is on the right (towards the back of the card), and is turned on by default.
8. Turn the appliance on. If a warning beep sounds, press the red reset button on the back of the unit next to the power supplies.
9. On the NIC card, press the ENB switch on the left (the one towards the front of the appliance). You hear an audible click.
10. Turn the appliance off and replace the cover.

To re-enable Fail to Wire on the WANJet 400 hardware

1. Set the Failure Mode setting to **Fail to Wire** as described in the procedure, *To configure the operational mode settings*, on page 8-4. (Do not forget to click **Save** to save the changed setting.)
2. Shut down the WANJet 400 appliance.
3. Turn the WANJet appliance upside down. On the bottom of the unit, unscrew the four screws that are on the left and right edges of the unit.
4. Slide the cover off the top of the WANJet 400 appliance.
5. Facing the front of the WANJet 400 appliance, locate the PXG2BP NIC card on the right near the front of the unit.
6. Tip the WANJet 400 appliance over onto the left side so you can see the buttons on the NIC card better.
7. On the upper right of the NIC card, locate the two switches (labeled **BYPASS MODE**).

   The ENB switch is on the left (towards the front of the card), and was previously turned on. The DIS switch is on the right (towards the back of the card), and is off.
8. Turn the appliance on. If a warning beep sounds, press the red reset button on the back of the unit next to the power supplies.
9. On the NIC card, press the DIS switch on the right (the one towards the center of the appliance). This action produces an audible click.
10. Turn the appliance off and replace the cover.

Managing device certificates

Sometimes, multiple WANJet appliances need to communicate securely over a network. For example, multiple WANJet appliances might need to collect performance data over a wide area network, for global traffic management. In this case, these WANJet appliances need to exchange SSL certificates and keys to ensure secure data communication.

You can view information about a device certificate that is currently installed on the WANJet appliance. You can also export a certificate or import a different certificate.

Viewing certificate and key information

You can view information about any SSL certificate and key that you have installed on the WANJet appliance. The specific information you can view about a certificate is:

- Name
- Subject
- Expiration date
- Version
- Serial number (if any)
- Common Name
- Division
- Locality, state or province, and country
- Issuer

To view device certificate and key information

1. In the navigation pane, expand **System**, and click **Device Certificates**.
   This displays the properties of any self-signed certificate.
2. On the menu bar, click **Device Key**.
   This displays the type and size of the key.

Importing, exporting, or renewing a device certificate

You can import, export, or renew two kinds of certificates: a device certificate or a trusted device certificate.

To import a device certificate

1. In the navigation pane, expand **System** and click **Device Certificates**.
   This displays the properties of a self-signed certificate.

2. At the bottom of the screen, click **Import**.
   This displays the screen for importing either a certificate, or a certificate and key.
3. From the **Import Type** list, select an import type, either **Certificate** or **Certificate and Key**.
4. From the **Certificate Source** setting, click either **Upload File** or **Paste Text**:
   - If you click **Upload File**, type a file name or click **Browse** to navigate to the file containing the certificate.
   - If you click **Paste Text**:

     a) Copy the text from another source.

     b) Paste the text into the **Certificate Source** window.
5. Click **Import**.

To export a device certificate

1. In the navigation pane, expand **System**, and click **Device Certificates**.
   This displays the properties of a self-signed certificate.
2. At the bottom of the screen, click **Export**.
   The screen displays the text of the existing certificate.
3. Next to the **Certificate File** setting, click **Download <certificate_name>**.

To renew a device certificate

1. In the navigation pane, expand **System**, and click **Device Certificates**.
   This displays the properties of a self-signed certificate.
2. At the bottom of the screen, click **Renew**.
   This displays the properties of the certificate and its associated key.
3. Change any properties as needed.
   For detailed information, see the online help.
4. Click **Finished**.

Importing and exporting a key

You can import and export device keys.

To import a key

1. In the navigation pane, expand **System**, and click **Device Certificates**.
   This displays the properties of a self-signed certificate.
2. On the menu bar, click **Device Key**
   This displays the properties of the key.
3. Click **Import**.
4. From the **Import Type** list, select an import type, either **Certificate** or **Certificate and Key**.
5. From the **Key Source** setting, click either **Upload File** or **Paste Text**:
   - If you click **Upload File**, type a file name or click **Browse**.
     If you click **Browse**:

     a) Navigate to the relevant Windows folder and click a file name.

     b) On the browser window, click **Open**.
   - If you click **Paste Text**:

     a) Copy the text from another source.

     b) Paste the text into the **Key Source** window.
6. Click **Import**.

To export a key

1. In the navigation pane, expand **System**, and click **Device Certificates**.
   This displays the properties of a self-signed certificate.
2. On the menu bar, click **Device Key**.
   This displays the properties of the key.
3. Click **Export**.
   The screen displays the text of the key.
4. Next to the **Key File** setting, click **Download <key_name>**.

Configuring redundant peers

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

For a conceptual overview of deploying redundant peers, refer to *Setting up redundant peers*, on page 1-12.

Figure 8.1 shows an example of redundant peer configuration.

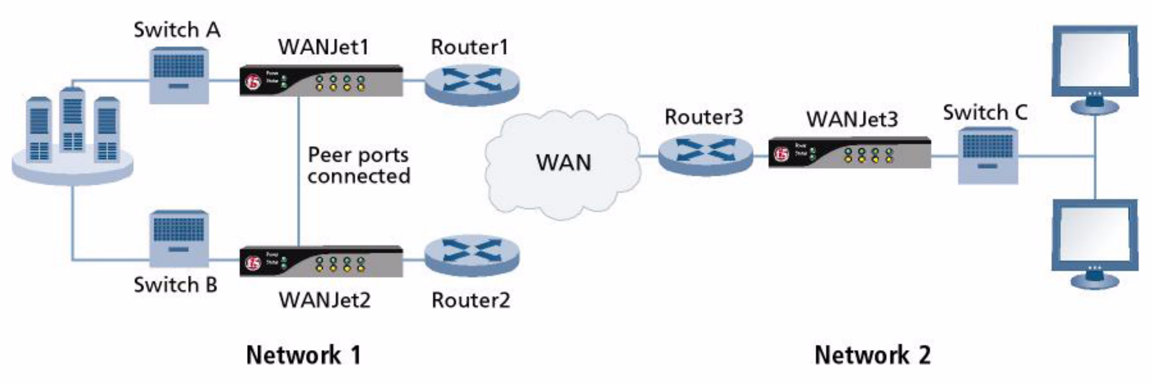


Figure 8.1 *Redundant peer configuration*

To configure the WANJet appliances shown in Figure 8.1, you need to perform the following tasks:

- On WANJet1, set up WANJet2 as a redundant peer, and WANJet3 as a remote WANJet appliance.
- On WANJet2, set up WANJet1 as a redundant peer, and WANJet3 as a remote WANJet appliance.
- On WANJet3, add both WANJet1 and WANJet2 as remote WANJet appliances, set its type as **Redundant**, then specify WANJet2's IP address as the **Redundant Peer**.

For information about how to add remote WANJet appliances, see *Configuring remote WANJet appliances*, on page 5-10.

To set up WANJet appliances as redundant peers

1. Install and set up two WANJet appliances in the same subnet.
2. Connect the two WANJet appliances from the Peer port on one to the Peer port on the other using a crossover cable or a connection through a switch.
3. In the navigation pane of the first WANJet appliance, expand **WAN Optimization** and click **Local WANJet**.
   The Local WANJet screen opens.
4. Check the **Enable Redundant Peer** box.
5. In the **Self Peer IP** box, type the IP address of the Peer port on the local WANJet appliance. It must be in the same subnet as the redundant peer IP address.
6. In the **Redundant Peer IP** box, type the IP address of the WANJet appliance that is the redundant peer of this WANJet appliance.
7. In the **Peer Netmask** box, type the netmask of the peer and remote peer subnet. You create a subnet of the IP addresses of the Peer ports on the WANJet appliance and the redundant peer.
8. Click **Save**.
   The Local WANJet screen refreshes, and the changes are committed to the WANJet appliance.
9. Repeat steps 3-8 on the second WANJet appliance.

Configuring one-arm topology

You can deploy the WANJet appliance out-of-line in a one-arm topology, with one physical connection to the LAN and no direct connection to the WAN.

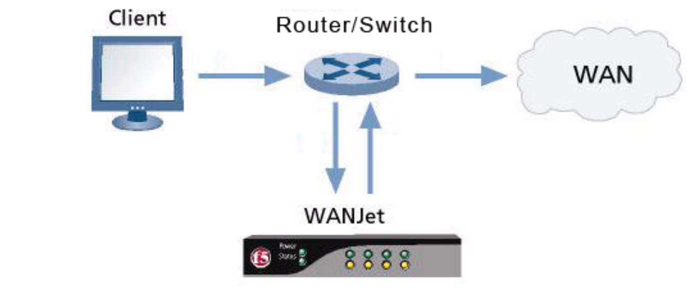


Figure 8.2 *One-arm deployment*

In this deployment, the WANJet appliance has a single (hence the term ***one-arm***) connection to the WAN router (or LAN switch) and has all relevant traffic redirected to it by the WAN router (or switch).

For more information about this configuration, see *Deploying in a one-arm configuration*, on page 2-4.

To configure the WANJet appliance in a one-arm deployment

1. Perform initial configuration of the WANJet appliance as described on the ***Quick Start Card***.
2. Connect the WAN port of the WANJet appliance to the WAN router (or LAN switch) as shown in Figure 8.2.
3. Log on to the WANJet appliance, as described in *Logging on to the system*, on page 3-3.
4. In the navigation pane, expand **WAN Optimization** and click **Operational Mode**.
   The Operational Mode screen opens.
5. For the **Topology** setting, select **One-Arm**.
6. Click **Save**.

Restoring factory default values

You can restore the factory default values on the WANJet appliance. If you do this, the values in all fields on all screens are reset to the default values. You should restore the defaults only in extreme cases, such as when you want to discard all configuration changes that you have made, and start configuration all over again.

Because the WANJet appliance retains the licensing information, you do not have to revalidate the license. However, you do have to reconfigure the rest of the settings and policies.

◆ **Note**

Before restoring factory default values, you should back up the current configuration in case you decide that you want to use the policies and settings that you have already entered. Refer to ***Creating and saving an archive on the WANJet appliance****, on page 11-3, for the procedure on how to save the current settings.*

◆ **Important**

Only experienced system administrators should reset configuration data to the factory default values. We strongly recommend that you modify these settings only under the guidance of F5 Support personnel.

To restore factory default values

1. Connect to the WANJet appliance through the system console (for example, using Telnet).
2. Log on through the console as **root**.
3. Boot the system to single user mode.
4. Type **sys-reset**.
   The system resets the configuration to the factory default values.
5. Reboot the system normally.

9

Configuring Interfaces, Routes, and System Services

- Configuring interfaces
- Configuring routes
- Managing system services

Configuring interfaces

The ***interfaces*** on a WANJet® appliance are the physical ports that you use to connect the WANJet appliance to other devices on the network. Through its interfaces, the WANJet appliance can forward traffic to or from other network devices.

Every WANJet appliance includes the following interfaces:

- **LAN**: Connects to the local area network.
- **WAN**: Connects through the wide area network to other offices.
- **Peer**: Connects to a second WANJet appliance that is part of a redundant WAN router setup.
- **Management**: Connects to a management network to separate administrative traffic from production data.

The LAN, WAN, and Peer interfaces on the WANJet appliance each have unique properties, such as media access control (MAC) address, state, media speed, media type, duplex mode, and flow control settings. On the Network Interfaces screen, you can view all of the properties, and configure the state (**Enabled** or **Disabled**), media type, and flow control of the LAN, WAN, and Peer interfaces.

The Management interface (called the Management port) is not listed on the Network Interfaces or Statistics screens. You typically configure the Management port when initially setting up the WANJet appliance (using the LCD or Setup utility), and can change its configuration on the System Platform screen. After it is configured, you log on to the WANJet appliance using the IP address of the Management port. For more information on the Management port, see *Configuring the Management port, host name, host IP address, and time zone*, on page 5-6.

Viewing interface information

You can display a list of the WANJet appliance data interfaces, showing their current status:

- **UP**: the interface is operational and able to pass data.
- **DOWN**: the interface is not operational; this could happen if the interface is disconnected, if either the LAN or WAN interface is disabled (the other one goes down), or if a hardware failure occurred.
- **DISABLED**: the interface is disabled.

You can also view other information about each interface:

- MAC address of the interface
- Media speed
- VLAN count showing the VLANs to which the interface is assigned

This information is useful when you want to assess the way that a particular interface is forwarding traffic. For example, you can use this information to determine the speed at which an interface is currently operating.

To view a list of interfaces

In the navigation pane, expand **Network**, and click **Interfaces**. This displays a list of the interfaces on the WANJet appliance, along with their status and related information.

To view the properties of an interface

1. In the navigation pane, expand **Network**, and click **Interfaces**.
   The Interface List screen opens and displays the list of interfaces on the WANJet appliance.
2. Click an interface name in the list.
   The Interface Properties screen opens and displays the properties of that interface.

Changing interface properties

You can enable or disable the LAN, WAN, and Peer interfaces, change the interface speed and duplex setting, and change the flow control. The WANJet appliance supports both half-duplex and full-duplex data transmission at various speeds on the interfaces.

To enable or disable interfaces

1. In the navigation pane, expand **Network**, and click **Interfaces**.
   The Interface List screen opens and displays the list of interfaces on the WANJet appliance.
2. Click the Select box to the left of the interface you want to enable or disable.
3. Click **Enable** or **Disable**.

   Note: *If you disable either the **lan** or **wan** interface, the status of the one you disabled changes to **DISABLED**, and the other one changes to **DOWN**.*

To change interface properties

1. In the navigation pane, expand **Network**, and click **Interfaces**.
   The Interface List screen opens and displays the list of interfaces on the WANJet appliance.
2. Click an interface name in the list.
   The Interface Properties screen opens and displays the properties of that interface.
3. In the Configuration area, configure the properties as needed:

- Change the **State** setting to **Enabled** or **Disabled**, as needed. The default value is **Enabled**.
- From the **Requested Media** list, select the interface speed and duplex setting for the interface. The default setting is **auto**, for automatic detection.

  Note: *The speed and duplex settings for the LAN and WAN interfaces must match.*
- From the **Flow Control** list, select the setting that specifies how the interface handles pause frames for flow control.

For additional details on each property, see the following pages.

4. Click **Update**.

Configuring the state of an interface

You can either enable or disable an interface on the WANJet appliance, by configuring the **State** property. By default, each interface is set to **Enabled**, where it can allow incoming or outgoing traffic. When you set the state to **Disabled**, the interface cannot accept any traffic.

Setting the requested media type

You can configure the **Requested Media** property to specify the media type and duplex mode of the LAN, WAN, or Peer interface cards, or you can use the default **auto** value to allow the interface to automatically negotiate the correct setting. The values that you can choose are: **auto**, **10baseT full**, **10baseT half**, **100baseTX full**, **100baseTX half,** and **1000baseT full**, and **1000baseT half**.

For the LAN interface, the interface speed and duplex settings apply to the link between the LAN switch and the WANJet appliance. For the WAN interface, the interface speed and duplex settings apply to the link between the WAN router and the WANJet appliance.

◆ **Note**

The speed and duplex settings for the LAN and WAN interfaces must match.

The default setting for this property is **auto**. If the media type is set to **auto** and the card does not support auto-detection, the default type for that interface is used, for example **1000BaseT half**.

Full duplex mode means that traffic on that interface can travel in both directions simultaneously, while ***half duplex*** mode means that traffic on that interface can only travel in one direction at any given time. Note that if you want the interface to be part of a trunk, the media type must be set to one with full duplex mode.

If the media type of the interface does not allow the duplex mode to be set, this is indicated by an on-screen message. If setting the duplex mode is not supported for the interface, the duplex setting is not saved in the configuration file.

Configuring flow control

You can configure the **Flow Control** property to manage the way that an interface handles pause frames for flow control. ***Pause frames*** are frames that an interface sends to a peer interface as a way to control frame transmission from that peer interface. Pausing a peer's frame transmissions prevents an interface's First-in, First-out (FIFO) queue from filling up and resulting in a loss of data. Possible values for this property are described in Table 9.1

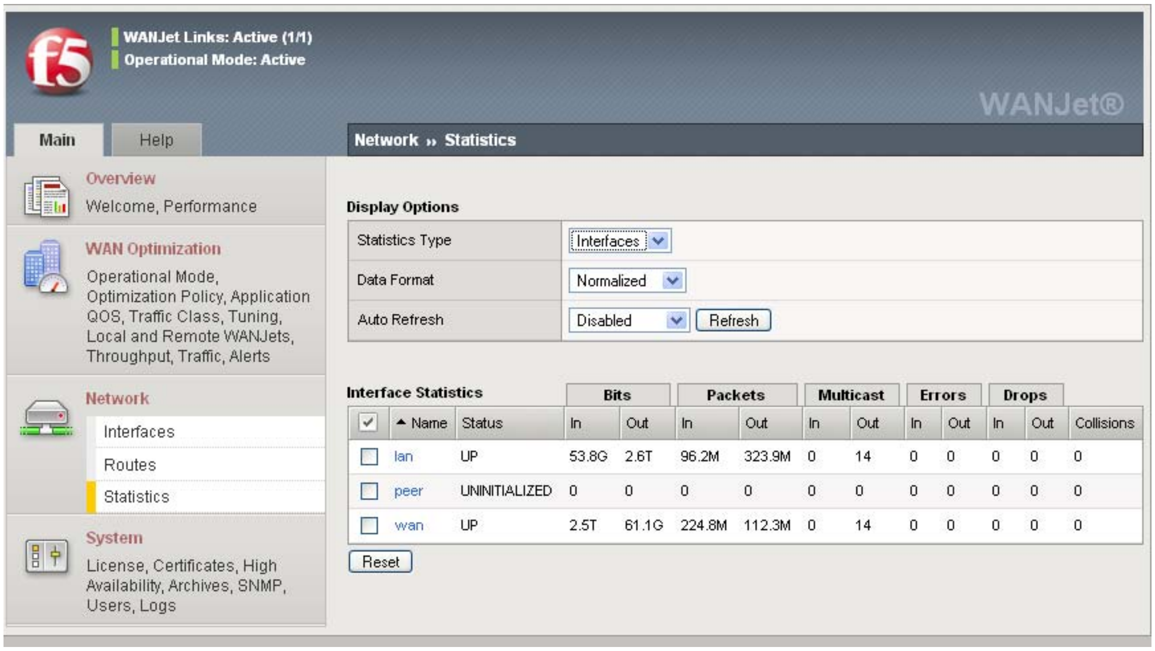
Value	Description
Pause None	Disables flow control.
Pause TX/RX	Specifies that the interface honors pause frames from its peer, and also generates pause frames when necessary. This is the default value.
Pause TX	Specifies that the interface ignores pause frames from its peer, and generates pause frames when necessary.
Pause RX	Specifies that the interface honors pause frames from its peer, but does not generate pause frames.

Table 9.1 *Pause frame values*

Displaying interface statistics

You can display statistics about the data interfaces on the WANJet appliance. Figure 9.1 shows an example of the interface statistics you might see on one WANJet appliance of a pair set up to optimize traffic over a WAN. You can see that the WANJet appliance is not part of a redundant pair because the Peer port is not operating (its status is **UNINITIALIZED**).

.


f5
WANJet Links: Active (1/1)
Operational Mode: Active
WANJet®
Main
Help
Network » Statistics
Overview
Welcome, Performance
WAN Optimization
Operational Mode, Optimization Policy, Application QOS, Traffic Class, Tuning, Local and Remote WANJets, Throughput, Traffic, Alerts
Network
Interfaces
Routes
Statistics
System
License, Certificates, High Availability, Archives, SNMP, Users, Logs
Refresh
Reset

Display Options

Statistics Type	Interfaces
Data Format	Normalized
Auto Refresh	Disabled

Interface Statistics

			Bits		Packets		Multicast		Errors		Drops		
☑	▲ Name	Status	In	Out	In	Out	In	Out	In	Out	In	Out	Collisions
□	lan	UP	53.8G	2.6T	96.2M	323.9M	0	14	0	0	0	0	0
□	peer	UNINITIALIZED	0	0	0	0	0	0	0	0	0	0	0
□	wan	UP	2.5T	61.1G	224.8M	112.3M	0	14	0	0	0	0	0

Figure 9.1 *Sample interface statistics screen*

◆ **Tip**

For descriptions of each screen element, see the online help.

To display interface statistics

1. In the navigation pane, expand **Network**, and click **Statistics**. The interface statistics screen opens and displays statistics for the data interfaces on the WANJet appliance.

2. For the **Data Format** setting, retain the default value (**Normalized**), or select **Unformatted** from the list.

3. For the **Auto Refresh** setting, retain the default value of **Disabled**, or select an automatic refresh interval from the list.

   Note: *Setting the* ***Auto Refresh*** *value to a short interval could impact system performance.*

4. If you want to manually update the statistics, click **Refresh**.

Configuring routes

The WANJet appliance must communicate with other routers, servers, and firewalls in a networked environment. Before you put the WANJet appliance into production, we recommend that you carefully review the router and server configurations in your network. By doing so, you can properly configure routing on the WANJet appliance, and you can adjust the routing configurations on other network devices to include WANJet appliance IP addresses.

Due to the need to process both user application traffic (for optimization) and administrative traffic (or out-of-band management), the WANJet appliance has two routing tables:

- Management routing table
- Data routing table (also called the ***TMM routing table***)

The ***management routing table*** contains information about routes that the WANJet appliance uses to forward traffic (administrative) through the Management port.

The ***data routing table*** is the main TMM routing table, which contains IP routing information about data routes. ***Data routes*** (also called ***TMM switch routes***) are routes that the WANJet appliance uses to forward traffic (data) through the LAN and WAN interfaces.

You can manage the static or management routes defined in the WANJet appliance's routing tables. Specifically, you can:

- View routes
- Add routes
- Modify existing routes
- Delete static routes that no longer apply due to changes in the network

The following sections include procedures for configuring both types of routes.

◆ **Note**

Only users with an ***Administrator*** *user role can create and manage routes on the WANJet appliance.*

Viewing routes

You can view the lists of data or management routes on the WANJet appliance. The lists automatically include the WAN gateway or management route (gateway) that you specified when you initially configured the WANJet appliance. Its destination is shown as Default IPv4.

If your network configuration includes a LAN router and you specify it on the Local WANJet screen, the WANJet appliance automatically creates a static route to it for each remote WANJet appliance that is configured on this system.

To view data routes

In the navigation pane, expand **Network** and click **Routes**. The Route List opens and displays the default gateway, static routes to the LAN router (if you have specified a LAN router) from remote WANJet appliances configured on the system, and any static routes that you added on the system.

To view management routes

1. In the navigation pane, expand **System**, and click **Configuration**. The General Configuration screen opens.
2. On the menu bar, click **Management Routes**. The Management Routes screen opens and displays the default management gateway and any other management routes that you added to the system.

Adding routes

You add a static or management route to ensure that the WANJet appliance can locate subnets that may be inaccessible through the default gateway. You also add routes if you want to override the default network pathway. For example, you may need to add management routes so the WANJet appliance can access an SNMP server for SNMP traps, or an email server to send email alerts.

The default WAN and management gateways are automatically added to the lists. Therefore, you do not need to add them unless they were deleted by mistake.

To add a static route

1. In the navigation pane, expand **Network**, and click **Routes**. The Routes List screen opens.
2. On the upper-right corner of the screen, click **Add**.

   Note: *If the* ***Add*** *button is unavailable, you do not have permission to add a route. You must have the* ***Administrator*** *role assigned to your user account.*
3. From the **Type** list, select **Route**.
4. In the **Destination** box, type a destination IP address.
5. In the **Netmask** box, type the netmask for the IP address you typed in the **Destination** box.

6. For the **Resource** property, select one of the following options:
    - **Use Gateway**, and type the IP address to override the default gateway.
    - **Reject**, if you want to drop all packets sent to a particular IP address.
7. Click **Finished**.
   The new route is added to the route list.

To add a management route

1. In the navigation pane, expand **System**, and click **Configuration**.
   The General Configuration screen opens.
2. On the menu bar, click **Management Routes**.
   The Management Routes screen opens.
3. In the upper-right corner of the screen, click **Add**.

   Note: *If the* ***Add*** *button is unavailable, you do not have permission to add a route. You must have the* ***Administrator*** *role assigned to your user account.*
4. From the **Type** list, select **Route**.
5. In the **Destination** box, type a destination IP address.
6. In the **Netmask** box, type the netmask for the IP address you typed in the **Destination** box.
7. For the **Resource** property, select one of the following options:
    - **Use Gateway**, and type the IP address to override the default gateway.
    - **Reject**, if you want to drop all packets sent to a particular IP address.
8. Click **Finished**.
   The new route is added to the route list.

Modifying routes

You can modify the **Resource** setting of data or management routes in the routes lists. You cannot modify other properties of the route.

To modify the resource for a data route

1. In the navigation pane, expand **Network**, and click **Routes**.
   This displays the current list of static routes.
2. In the Destination column, click a route.
3. For the **Resource** property, select one of the following options:
   - **Use Gateway** and type the IP address.
   - **Reject** if you want to drop all packets sent to a particular IP address or subnet.
4. Click **Update**.

To modify the resource for a management route

1. In the navigation pane, expand **System**, and click **Configuration**.
   The General Configuration screen opens.
2. On the menu bar, click **Management Routes**.
   The Management Routes screen opens.
3. In the Destination column, click the management route you want to change.
   The Properties screen for the management route opens.
4. For the **Resource** property, select one of the following options:
   - **Use Gateway** and type the IP address.
   - **Reject** if you want to drop all packets sent to a particular IP address or subnet.
5. Click **Update**.

Deleting routes

When the routers or destination hosts on your network change for any reason, you may need to delete routes (thereby deleting static entries from the data routing table or management routes from the management routing table). For example, removing a specific host or router from the network might invalidate a destination or gateway address of one of the routes, making the route no longer needed.

To delete a static route

1. In the navigation pane, expand **Network** and click **Routes**.
   A list of the static entries in the routing table appears.
2. Click the Select box to the left of the entry you want to delete.
3. Click **Delete**.
   A Confirm Delete message opens.
4. Click **Delete**.

To delete a management route

1. In the navigation pane, expand **System**, and click **Configuration**.
   The General Configuration screen opens.
2. On the menu bar, click **Management Routes**.
   The Management Routes screen opens.
3. Click the Select box to the left of the entry you want to delete.
4. Click **Delete**.
   A Confirm Delete message opens.
5. Click **Delete**.

Managing system services

The WANJet appliance includes several services that you can start or stop. Also known as daemons, ***services*** perform a variety of functions, such as implementing WAN optimization, handling messaging and configuration data, keeping the time synchronized with an external time server, and handling failure of system services.

Services also log events. Thus, some of the logs display, for each message, the service that reported the event. The logs that show service names are the System log and the Local Traffic log.

You can think of services as belonging to two categories: ***core services***, which start up when you boot the WANJet appliance and run continually, and ***optional services***, which are not essential for basic operation.

◆ **Important**

*You must have an **Administrator** user role assigned to your user account to stop, start, or restart a service.*

Managing core services

The WANJet appliance starts a number of services at boot time, and they remain running as long as the WANJet appliance is operational. Most of these services are essential to the basic operation of the system, and you do not need to monitor them. It is useful to have a basic understanding of the core services listed in Table 9.2.

Service	Description	Impact When Unavailable
CentralManager	Establishes a connection between the local and remote WANJet appliances, handles authentication, exchanging configuration and link up information.	Cannot set up WAN link between local and remote WANJet appliances.
GenericProxy	Optimizes traffic by reducing bandwidth and latency and communicates with remote WANJet appliances.	Cannot optimize traffic.
MCPD	Known as the Master Control Program Daemon, controls messaging and configuration.	Cannot manage traffic; cannot retrieve or update system status; users cannot reconfigure system; disables some of the other services.
SOD	Controls high availability management of system services in case of heartbeat failure.	Cannot automatically handle system services in case of heartbeat failure.
TMM	Known as the Traffic Management Microkernel, manages traffic.	Cannot process user application traffic or any UDP traffic.

Table 9.2 *Core system services*

Starting and stopping core services

You rarely ever need to stop a core service from running. (The TMM service is a possible exception.) For this reason, you cannot use the Configuration utility to start or stop a core service. If you want to explicitly stop or start a core service, you use the **bigstart** command line utility. For information on the **bigstart** utility, see the **bigstart** man page. For information on stopping the TMM service, see *TMM service*, on page 9-14.

Configuring core services for heartbeat failure

System services have heartbeats. A service ***heartbeat*** is a recurring signal that a service generates. The WANJet appliance continually monitors service heartbeats to determine whether the service is still running. For some services, if the system does not detect a heartbeat, the system takes some action with respect to failover. These services are:

- MCPD
- SOD
- TMM
- CentralManager
- Generic Proxy

You can control how the WANJet appliance behaves when it detects a heartbeat failure for a service. For example, you can configure the CentralManager service so that if its heartbeat is undetected, the WANJet appliance automatically restarts the CentralManager.

To configure services for heartbeat failure

1. In the navigation pane, expand **System**, and click **High Availability**.
   The System Services list opens.
2. In the Name column, click the service that you want to configure for heartbeat failure.
3. For the **Heartbeat Failure** setting, select the action that you want the system to take if the heartbeat for this service is not detected:
   - **Restart**: Specifies that the system restarts this system service.
   - **Restart All**: Specifies that the system restarts all system services.
   - **Reboot**: Specifies that the system reboots when this service fails.
   - **No Action**: Specifies that the system takes no action.
4. Click **Finished**.

Introducing selected core services

The core services CentralManager, GenericProxy, MCPD, TMM, and SOD are important because they support key functions of the WANJet appliance. These services run automatically unless you specifically shut them down. They provide essential functions such as authenticating and communicating with remote WANJet appliances, optimizing traffic, maintaining configuration data, and passing traffic through data interfaces.

The CentralManager and GenericProxy support WAN optimization exclusively, whereas the other services MCPD, TMM, and SOD operate on other TMOS™-based systems as well, such as BIG-IP® systems.

CentralManager service

The ***CentralManager*** is a service that handles communication between local and remote WANJet appliances. Specifically, the CentralManager is responsible for these major tasks:

- Communicating with the counterpart CentralManager on each remote WANJet appliances, as follows:
    - The CentralManager service listens for incoming connections from other CentralManagers on the CentralManager listening port, which defaults to port **3701**.
    - The CentralManager service periodically attempts to initiate communication with remote WANJet appliances when they are not already in communication.
    - The CentralManager service authenticates remote WANJet appliances as part of establishing communications.
    - The CentralManager service exchanges configuration information with remote WANJet appliances.
    - The CentralManager service periodically verifies the ability to communicate with remote WANJet appliances on an ongoing basis.
- Communicating using Linux message queues with other services, such as GenericProxy and **udpproxy**, on the same WANJet appliance. This includes notifying other services when the Link Up/Down status of a remote WANJet appliance changes. Link Up and Link Down are defined as follows:

    Link Up: A link to a remote WANJet appliance is considered up for a particular service when communications are established between the CentralManager processes on the two WANJet appliances, configuration information has been exchanged, and the service is up and ready to operate on both WANJet appliances.

    Link Down: A link to a remote WANJet appliance is considered down for a particular service when the service is down at either or both ends, or when the CentralManager considers the communications with the CentralManager at the remote WANJet appliance to be down, or when the service itself has detected a failure that requires the link to go down so that some recovery may take place.

GenericProxy service

The ***GenericProxy*** service optimizes traffic between paired WANJet appliances. It is responsible for these major tasks:

- Optimizing traffic by proxying that traffic over connections, called tunnels, between the GenericProxy services on a pair of WANJet appliances. GenericProxy optimizes traffic by reducing required bandwidth using TDR-1 and TDR-2 technology and reducing latency.
- Achieving these optimizations. The GenericProxy must communicate with the counterpart GenericProxy service on each remote WANJet appliance, as follows:
  - All GenericProxy services listen for incoming connections from other GenericProxy services on the GenericProxy listening port, which is defined as one greater than the CentralManager listening port, which defaults to port **3702** when the CentralManager listening port is port **3701** (the default).
  - The GenericProxy service initiates and establishes communications with GenericProxy services on remote WANJet appliances after receiving Link Up indications from the CentralManager service.
  - As part of the process of initializing and establishing communications, the GenericProxy service manages the recovery and resynchronization of the TDR-2 cache.
  - The GenericProxy service terminates communications with GenericProxy services on remote WANJet appliances after receiving Link Down indications from the CentralManager service, or when it encounters certain errors.

MCPD service

The ***Master Control Program Daemon*** (MCPD) manages the configurations on a WANJet appliance. MCPD performs the following tasks:

- Receives and processes configuration change requests, validates configuration change requests, and updates storage for the target configuration. The service also returns success or failure results to clients.
- Receives and processes statistics and configuration query requests.

TMM service

The Traffic Management Microkernel (TMM) service performs traffic management. As such, the TMM service supports all system and networking components that the WANJet appliance needs to process application and administrative traffic. The TMM service controls the LAN, WAN, and Peer interfaces, but not the Management port.

The TMM service affects the type of interface (TMM switch interface or Management port) that the WANJet appliance uses for network traffic. The effect on the use of interfaces differs depending on the type of traffic. Normally, when the TMM service is running, certain types of network traffic use the Management port, while other types of traffic use the TMM switch interfaces.

- **User application traffic**
  This type of traffic is typically application traffic either destined for or coming to and from a client and a server. User application traffic always uses data interfaces, and never uses the Management port. Therefore, if the TMM service is stopped, the WANJet appliance does not process this type of traffic.
- **Administrative traffic destined for the WANJet appliance**
  This type of traffic is traffic destined for the IP address of the WANJet appliance's Management port. The WANJet appliance then sends its responses to these requests back through the Management port. Because administrative traffic uses the Management port, the WANJet appliance can still process this type of traffic when the TMM service is not running.
- **Administrative traffic coming from the WANJet appliance**
  The WANJet appliance generates this type of administrative traffic, and the source for this type of traffic is the IP address of the Management port. When the TMM service is running, the WANJet appliance sends this type of traffic through a data interface, using the default gateway. If the TMM service becomes unavailable, this type of traffic uses the Management port.

There are certain administrative tasks, however, such as a WANJet software installation, that you should not perform while the TMM service is running. Prior to performing these tasks, you should shut down the TMM service.

When you stop the TMM service and therefore make the data interfaces unavailable, the Management port becomes the only available interface on the WANJet appliance for administrative traffic.

Other administrative tasks that you should perform using the Management port only (because they require you to stop the TMM service) are a PXE installation and boot, and remote management using SSH and HTTPS.

SOD service

The SOD service manages the high availability of system services on the WANJet appliance. If system services fail to send heartbeats, the SOD service implements whatever action is configured for that service (for example, it may restart the service or reboot the system). For details, see *Configuring core services for heartbeat failure*, on page 9-12.

Managing optional services

The WANJet appliance includes a few services that you can start, stop, or restart.

- **ntpd**
  Network time protocol daemon: Sets and maintains the system time of day by connecting to an external time server.
- **snmpd**
  Simple Network Management Protocol (SNMP) daemon: Receives and processes SNMP requests, and sends trap notifications. Note that you must stop this service before updating the SNMP v3 file **/config/net-snmp/snmpd.conf**, which specifies SNMP user names.
- **sshd**
  Secure Shell daemon: Provides secure remote login to the WANJet appliance command line.

Core services, such as the TMM service, must run continually for the WANJet appliance to work properly. For more information on essential services, see *Managing core services*, on page 9-11.

To stop, start, or restart an optional service

1. In the navigation pane, expand **System**, and click **Configuration**.
2. On the menu bar, click **Services**.
   The System Services List opens, and shows the name of each service and its current status.
3. In the Service column, locate the name of the service you want to start, stop, or restart.
4. To the left of the service name, click the Select box.
5. Click **Start**, **Stop**, or **Restart** depending on the action that you want to take.
6. In the History column, review the status of the service.

◆ **Tip**

*You can also start and stop optional services using the **bigstart** utility. For more information, see the **bigstart** man page.*

10

Configuring SNMP

- Introducing SNMP administration
- Configuring the SNMP agent
- Working with SNMP MIB files

Introducing SNMP administration

Simple Network Management Protocol (SNMP) is an industry-standard protocol that gives a standard SNMP management system the ability to remotely manage a device on the network. One of the devices that an SNMP management system can manage is a WANJet® appliance. The SNMP versions that the WANJet appliance supports are: SNMP v1, SNMP v2c, and SNMP v3. The WANJet appliance implementation of SNMP is based on Net-SNMP, which was formerly known as UCD-SNMP.

Reviewing an industry-standard SNMP implementation

A standard SNMP implementation consists of an ***SNMP manager,*** which runs on a management system and makes requests to a device, and an ***SNMP agent,*** which runs on the managed device and fulfills those requests. SNMP device management is based on the standard management information base (MIB) known as MIB-II, as well as object IDs and MIB files.

- The ***MIB*** defines the standard objects that you can manage for a device, presenting those objects in a hierarchical, tree structure.
- Each object defined in the MIB has a unique object ID (OID), written as a series of integers. An ***OID*** indicates the location of the object within the MIB tree.
- A set of MIB files resides on both the SNMP management system and the managed device. ***MIB files*** specify values for the data objects defined in the MIB. This set of MIB files consists of standard SNMP MIB files and enterprise MIB files. ***Enterprise*** MIB files are those MIB files that pertain to a particular company, such as F5 Networks, Inc.
- The WANJet appliance includes a ***private MIB file*** that contains data objects for WAN optimization and other features of the WANJet appliance.

Typical SNMP tasks that an SNMP manager performs include polling for data about a device and receiving notifications from a device about specific events.

Reviewing the WANJet appliance SNMP implementation

To comply with the standard SNMP implementation, the WANJet appliance includes:

- SNMP agent
- Standard SNMP MIB files
- Enterprise MIB files
- Private MIB file

The enterprise MIB files typically reside on both the WANJet appliance and system running the SNMP manager. You can download the enterprise MIB files to your SNMP manager. The WANJet appliance includes a private MIB file that pertains to WAN optimization.

Using the WANJet appliance implementation of SNMP, the SNMP manager can perform these distinct functions:

- Poll for information (such as performance metrics)
- Receive notification of specific events that occur on the WANJet appliance

Summarizing SNMP configuration on the WANJet appliance

Before an SNMP management system can manage a WANJet appliance remotely, you must perform a few configuration tasks on the WANJet appliance. Then you can use standard SNMP commands on the remote manager system to manage the WANJet appliance.

The configuration tasks you perform are:

- **Configuring the SNMP agent**
  You must configure the WANJet appliance so that the SNMP manager can access it. For example, you can allow client access to information that the SNMP agent collects, and you can configure the way the SNMP agent handles SNMP traps.

- **Downloading MIB files**
  You can download MIB files to your remote manager system: the standard SNMP MIB files and the enterprise MIB files, including the private MIB file for the WANJet appliance.

Configuring the SNMP agent

Configuring the SNMP agent involves performing the following tasks:

- **Configuring WANJet appliance information**
  Specify a system contact name, and the location of the WANJet appliance.
- **Configuring client access to the SNMP agent**
  Configure the WANJet appliance to allow access to the SNMP agent from an SNMP management system.
- **Controlling access to SNMP data**
  Assign access levels to SNMP communities or users, to control access to SNMP data.
- **Configuring Traps**
  Enable or disable traps and specify the destination SNMP management system for SNMP traps.

Configuring WANJet appliance information

You can configure the following information:

- **Contact Information**
  The contact information is a MIB-II simple string variable defined by almost all SNMP boxes. The contact name usually contains a user name, as well as an email address.
- **Machine Location**
  The machine location is a MIB-II variable that almost all machines support. It is a simple string that defines the location of the machine.

To configure system information

1. In the navigation pane, expand **System**, and click **SNMP**.
   The SNMP Agent Configuration screen opens.
2. In the Global Setup area, fill in the boxes.
   For more information, see the online help.
3. Click **Update**.

Configuring client access

An SNMP ***client*** refers to any system running the SNMP manager software for the purpose of remotely managing the WANJet appliance. To allow client access to the WANJet appliance, you specify the IP or network addresses (with netmask as required) from which the SNMP agent can accept requests. (By default, SNMP is enabled only for the WANJet appliance loopback interface, **127.0.0.1**.)

To allow client access to the SNMP agent

1. In the navigation pane, expand **System**, and click **SNMP**.
   The SNMP Agent Configuration screen opens.
2. In the SNMP Access section, for the **Type** setting, select **Host** or **Network**, depending on whether the IP address you specify is a host system or a subnet.
3. Type the following information:
   - In the **Address** box, type an IP address or network address from which the SNMP agent can accept requests.
   - If you selected **Network** in step 2, type the netmask in the **Mask** box.
4. Click the **Add** button to add the host or network address to the list of allowed clients.
5. Click **Update**.

Controlling access to SNMP data

To better control access to SNMP data, you can assign an access level to an SNMP v1 or v2c community, or to an SNMP v3 user.

The default access level for communities is read-only. This means that you cannot write to an individual data object that has a read/write access type until you change the default read-only access level of the community or user.

The way to modify this default access level is by using the Configuration utility to grant read/write access to either a community (for SNMP v1 and v2c) or a user (SNMP v3), for a given OID.

When you set the access level of a community or user to read/write, and an individual data object has a read-only access type, access to the object remains read-only. In short, the access level or type that is the most secure takes precedence when there is a conflict. Table 10.1 illustrates this point.

If the access type of an object is...	And you set the access level of a community or user to...	Then access to the object is...
Read-only	Read-only	Read-only
	Read/write	Read-only
Read/write	Read-only	Read-only
	Read/write	Read/write

Table 10.1 *Access control for SNMP data*

To grant community access to SNMP data (v1 or v2c only)

1. In the navigation pane, expand **System**, and click **SNMP**.
   The SNMP Agent Configuration screen opens.
2. On the menu bar, click **Access (v1, v2c)**.
   The SNMP Access (v1, v2) screen opens.
3. In the upper-right corner of the screen, click **Create**.
   The Record Properties screen opens.
4. In the **Community** box, type the name of the SNMP community for which you are assigning an access level (in step 7).
5. In the **Source** box, type the source IP address.
6. In the **OID** box, type the OID for the top-most node of the SNMP tree to which the access applies.
7. For the **Access** setting, select an access level, either **Read Only** or **Read/Write**. (This access level applies to the community name you specified in step 4.)
8. Click **Finished**.

To grant access to SNMP data (v3 only)

1. In the navigation pane, expand **System**, and click **SNMP**.
   The SNMP Agent Configuration screen opens.
2. On the menu bar, click **Access (v3)**.
   The SNMP Access (v3) screen opens.
3. In the upper-right corner of the screen, click **Create**.
   The Record Properties screen opens.
4. In the **User Name** box, type the name of the user to whom you are granting access (in step 8).
5. For the **Authentication** setting, select the type of authentication to use (**MD5**, **SHA**, or **None**), and then type and confirm the user's password.
6. For the **Privacy** setting, select the privacy protocol, and then do one of the following:
   - Type and confirm the user's password.
   - Click the **Use Authentication Password** box.
7. In the **OID** box, type the object identifier (OID) for the top-most node of the SNMP tree to which the access applies.
8. For the **Access** setting, select an access level, either **Read Only** or **Read/Write**. (This access level applies to the user name that you specified in step 4.)
9. Click **Finished**.

Configuring traps

On the WANJet appliance, ***traps*** are definitions of unsolicited notification messages that the WANJet alert system and the SNMP agent send to the SNMP manager when certain events occur on the WANJet appliance. Configuring SNMP traps on a WANJet appliance involves configuring the way that the WANJet appliance handles traps, as well as setting the destination for notifications that the alert system and the SNMP agent send to an SNMP manager.

You use the Configuration utility to configure traps, that is, enable traps and set trap destinations.

Enabling traps for specific events

You can configure the SNMP agent on the WANJet appliance to send, or refrain from sending, notifications when the following events occur:

- The SNMP agent on the WANJet appliance stops or starts. By default, this trap is enabled.
- The WANJet appliance receives an authentication warning, generated when a client system attempts to access the SNMP agent. By default, this trap is disabled.
- The WANJet appliance receives any type of warning. By default, this trap is enabled.

To enable traps for specific events

1. In the navigation pane, expand **System**, and click **SNMP**.
   The SNMP Agent Configuration screen opens.
2. On the menu bar, click **Trap Configuration**.
   The SNMP Trap Configuration screen opens.
3. To send traps when someone starts or stops the SNMP agent, verify that the **Agent Start/Stop** box is checked.
4. To send notifications when authentication warnings occur, click the **Agent Authentication** box.
5. To send notifications when certain warnings occur, verify that the **Device** box is checked.
6. Click **Update**.

Setting the trap destination

In addition to enabling certain traps for certain events, you must specify the destination SNMP manager to which the WANJet appliance should send notifications. For SNMP versions 1 and 2c only, you specify a destination system by providing the community name to which the WANJet appliance belongs, the IP address of the SNMP manager, and the target port number of the SNMP manager.

◆ **Important**

If you are using SNMP v3 and want to configure a trap destination, you do not use the SNMP screens on the WANJet appliance. Instead, you configure the ***snmpd.conf*** *file at the command line. For more information, see the man page for the* ***snmpd.conf*** *file.*

To specify a trap destination

1. In the navigation pane, expand **System**, and click **SNMP**.
   The SNMP Agent Configuration screen opens.
2. On the menu bar, click **Trap Destination**.
   The SNMP Traps (v1, v2c) screen opens.
3. In the upper-right corner of the screen, click **Create**.
   The Record Properties screen opens.
4. For the **Version** setting, select the SNMP version number (**v1** or **v2c**).
5. In the **Community** box, type the community name for the SNMP agent running on the WANJet appliance.
6. In the **Destination** box, type the IP address of the SNMP management system.
7. In the **Port** box, type the port number for the SNMP management system that is to receive the traps.
8. Click **Finished**.

Working with SNMP MIB files

As described earlier, ***MIB files*** define the SNMP data objects contained in the SNMP MIB. The WANJet appliance includes a private MIB file called **WANJet-MIB.txt**. Two additional sets of MIB files reside on the WANJet appliance and the SNMP management system: enterprise MIB files (that is, F5-specific MIB files) and standard SNMP MIB files.

The MIB files are already present on the WANJet appliance. However, you still need to download them to your SNMP management system. You can download these MIB files from the Welcome screen. For more information, see *Downloading SNMP MIB files*, following.

The implementation of the Packet Velocity® ASIC (PVA) feature affects the ability for users to use MIB-II to gather certain kinds of data. For example, with a PVA system, you can use MIB-II to collect statistics on physical system interfaces, but not on logical interfaces (that is, VLANs).

To make MIB-II as clear as possible, we have implemented the SNMP feature so that you use MIB-II for gathering standard operating system data only. You cannot use MIB-II to gather data that is specific to the WANJet appliance and instead must use the F5 enterprise MIB files. OIDS for WANJet appliance data are contained in the F5 enterprise MIB files, including all interface statistics [**1.3.6.1.4.1.3375.2.1.2.4** (**sysNetwork.sysInterfaces**)].

◆ **Note**

All WANJet appliance statistics are defined by 64-bit counters. Thus, because only SNMP v2c supports 64-bit counters, your management system needs to use SNMP v2c to query WANJet appliance statistics data.

Downloading SNMP MIB files

The enterprise MIB files that you can download to the SNMP management system are:

- **WANJet-MIB.txt**
  This MIB file contains information about WAN optimization traps. This is the primary MIB file that relates to the WANJet appliance. To see the available MIB objects in this file, refer to Appendix **C,** ***WANJet Appliance Private MIB File***.

- **F5-BIGIP-COMMON-MIB.txt**
  This MIB file contains common information and TMOS™ notifications (traps). To see the available MIB objects in this file, view the **F5-BIG-IP-COMMON-MIB.txt** file in the **/usr/share/snmp/mibs** directory.

- **F5-BIGIP-LOCAL-MIB.txt**
  This is an enterprise MIB file that contains specific information related to local traffic management. To see the available MIB objects in this file, view the **F5-BIG-IP-LOCAL-MIB.txt** file in the **/usr/share/snmp/mibs** directory.

- **F5-BIGIP-SYSTEM-MIB.txt**.
  The **F5-BIGIP-SYSTEM-MIB.txt** MIB file includes global information on system-specific objects. To see the available MIB objects in this file, view the **F5-BIG-IP-SYSTEM-MIB.txt** file in the **/usr/share/snmp/mibs** directory.

To download MIB files

1. In the navigation pane, expand **Overview**, and **c**lick **Welcome**.
   The Welcome screen opens.

2. Scroll to the Downloads section, and locate the **SNMP MIBs** section.

3. Click the type of MIB file to download.

4. Follow the instructions on the screen to complete the download.

11

Saving and Restoring Configuration Data

- Introducing archives
- Managing archives

Introducing archives

By using the Setup utility and the Configuration utility to configure the WANJet appliance, you create a set of configuration data. This data consists of system and network definitions such as IP addresses, interface properties, system accounts, and more. Using the Archives feature, you can back up the current configuration data, and if necessary, restore the data at a later time. We recommend that you use this feature to mitigate the potential loss of WANJet appliance configuration data.

What is an archive?

Before you upgrade the WANJet appliance with a newer version, you should always create an ***archive***, which is a backup copy of the configuration data. This archive is in the form of a ***user configuration set***, or UCS. Then, if you need to recover that data later, you can restore the data from the archive that you created.

A UCS contains the following types of WANJet appliance configuration data:

- System-specific configuration files
- Product licenses
- User accounts and password information
- Domain Name Service (DNS) zone files
- Installed SSL keys and certificates

When you back up the configuration data, the WANJet appliance creates a new file with a **.ucs** extension. Each UCS file contains various configuration files needed for the WANJet appliance to operate correctly, as well as the configuration data.

◆ **Important**

To create, delete, upload, or download an archive, you must have the ***Administrator*** *role assigned to your user account.*

Working with archives

Using the Configuration utility, you can save and restore archives that are stored on the WANJet appliance. Furthermore, for added security, you can save archives to and restore archives from a remote system.

Saving archives

By default, the system stores all archives in the directory **/var/local/ucs**. You can specify a different location, but in this case, the Configuration utility does not display the UCS files when you view the list of archives.

After you create an archive on the WANJet appliance, you can download a copy of the UCS file to a remote system. If you later need to restore the data, and are unable to access the directory where you saved the archive, you still have a backup copy of the file. For more information on saving archives, see *Creating and saving an archive on the WANJet appliance*, on page 11-3.

◆ **Important**

UCS files include the host name of the WANJet appliance as part of the data stored in that file. When you later specify this UCS file during the process of restoring configuration data to a WANJet appliance, the host name stored in this UCS file must match the host name of the system on which you are restoring the configuration data. Otherwise, the system does not fully restore the data.

◆ **Important**

If your configuration data includes SSL keys and certificates, be sure to store the archive file in a secure location.

Restoring archives

The **/var/local/ucs** directory is the only location on the WANJet appliance from which you can restore an archive. However, if you previously downloaded an archive to a remote system, and a WANJet appliance event prevents you from accessing the **/var/local/ucs** directory, you can upload the archive from that remote system. For more information on restoring archives, see *Restoring data from a WANJet appliance archive*, on page 11-5.

Managing archives

You can create, store, and access archives, on both the WANJet appliance and a remote system. You can also view any existing archive files and their properties, as well as delete archives that you no longer need. Specifically, you can use the Configuration utility to:

- View a list of existing archives
- Create a new archive and save it on the WANJet appliance
- View the properties of an existing archive
- Restore data from a WANJet appliance archive
- Download a copy of an archive to another system
- Upload a copy of an archive that you previously saved to another system
- Delete an existing archive from the WANJet appliance

◆ **Note**

Only users with the ***Administrator*** *user role can manage archives.*

Viewing a list of existing archives

You can view a list of archives (that is, UCS files) that are currently stored in the **/var/local/ucs** directory on the WANJet appliance. When you view a list of archives, the Configuration utility displays the following information:

- Name of the UCS file
- Date that the UCS file was created or uploaded
- Size of the file, in kilobytes

◆ **Note**

Whenever you last upgraded the WANJet appliance to a new version, you were required to create a UCS file named ***config.ucs****, using the* ***bigpipe config save*** *command. This UCS file appears in the list of UCS files on the Archives screen.*

To view a list of existing archives

In the navigation pane, expand **System**, and click **Archives**. The Archives screen opens, displaying a list of existing UCS files.

Creating and saving an archive on the WANJet appliance

You can create a new archive, which the WANJet appliance automatically stores in a default location, the **/var/local/ucs** directory. You can create as many separate archives as you want, as long as each archive has a unique file name. Also, you can specify that the WANJet appliance store an archive in a directory other than **/var/local/ucs**, although in this case, the Configuration utility does not include the archive name in the list of archives on the Archives screen.

When you create an archive, you configure some settings, such as a setting to encrypt the archive file for security reasons. Table 11.1 lists and describes these settings, and shows their default values.

Setting	Description	Default Value
File Name	Specifies the file name for the archive. You do not need to specify the UCS file name extension. The WANJet appliance appends the UCS extension automatically.	No default value
Encryption	Enables or disables encryption of the archive. If you select **Enabled**, two other settings, **Passphrase** and **Verify Passphrase**, appear on the screen. ***Note:*** *This setting appears only when you have used the Preferences screen to set the* ***Archive Encryption*** *setting to* ***On Request*** *or* ***On****.*	**Disabled**
Passphrase	Specifies a password that a user must use to decrypt an archive.	No default value
Verify Passphrase	Specifies the password that you defined with the **Passphrase** setting.	No default value
Private Keys	Specifies whether to include or exclude private keys in the archive.	**Include**
Version	Displays the version of the WANJet appliance software that is currently running. You cannot configure the **Version** setting.	No default value

Table 11.1 *Settings for creating an archive*

To create an archive

1. In the navigation pane, expand **System**, and click **Archives**.
   The Archives screen opens.

2. In the upper-right corner of the screen, click **Create.**
   The New Archive screen opens.

   Note: *If the* ***Create*** *button is unavailable, you do not have permission to create an archive. You must have the* ***Administrator*** *role assigned to your user account.*

3. In the **File Name** box, type a unique file name for the archive.
   We recommend that the file name match the name of the WANJet appliance. For example, if the name of the WANJet appliance is **wanjet2**, then the name of the archive file should be **wanjet2.ucs**. For more information, see *Working with archives*, on page 11-1.

4. If you want to encrypt the archive, from the **Encryption** list, select **Enabled**.

5. If you want the WANJet appliance to include any private keys, from the **Private Keys** list, select **Include**.
   In this case, be sure to store the archive file in a secure environment.
6. Click **Finished**.

Viewing archive properties

Using the Configuration utility, you can view the properties of an archive that you previously created. Note that you cannot modify the properties of an archive. If you want to modify an archive, you must delete the archive you want to change and then create a new one.

The properties of an archive that you can view are:

- The name of the archive
- The version of the WANJet appliance on which the archive was created
- The encryption state of the archive (encrypted or unencrypted)
- The date that the archive was created
- The size of the archive, in kilobytes

To view the properties of an archive

1. In the navigation pane, expand **System**, and click **Archives**.
   The Archives screen opens.
2. In the Name column, click the name of the archive that you want to view.
   This displays the properties of that archive.

Restoring data from a WANJet appliance archive

In the unlikely event that the WANJet appliance configuration data becomes corrupted, you can restore the data from the archive that is currently stored in the directory **/var/local/ucs**. If no archive exists in that directory, then you cannot restore configuration data.

◆ **Important**

The name of the archive must match the host name of the WANJet appliance you are restoring. For example, if the host name of the WANJet appliance you are restoring is ***WANJet2****, then the name of the archive must be* ***WANJet2.ucs****. If necessary, you can change the host name of the WANJet appliance to match the name of the archive.*

To restore data from a WANJet appliance archive

1. In the navigation pane, expand **System**, and click **Archives**.
   The Archives screen opens.
2. In the File Name column, click the name of the archive that you want to use to restore the configuration data.
   This displays the properties of that archive.
3. Click **Restore.**
   This restores the WANJet appliance configuration data.

Downloading an archive to a remote system

As described in the section *Introducing archives*, on page 11-1, you can download a copy of an existing archive to a remote system, that is, the system from which you ran the Configuration utility to create the archive. This feature protects the configuration data in the unlikely event that the WANJet appliance experiences a system catastrophe.

When you download an existing archive, you first display the properties of the archive you want to download, and then specify the complete path name of the location to which you want to save the archive copy.

To download an archive

1. In the navigation pane, expand **System**, and click **Archives**.
   The Archives screen opens.
2. In the File Name column, click the name of the archive that you want to view.
   This displays the properties of that archive.
3. For the **Archive File** setting, click the **Download: <.ucs filename>** button.
   A confirmation screen appears.
4. Click **Save**.
   The WANJet appliance downloads a copy of the UCS file to the system from which you initiated the download.

Uploading an archive from a remote system

If you previously downloaded a copy of an archive to a remote system (that is, the system from which you initiated the download), you can upload that archive to the WANJet appliance at any time. This is most useful when a WANJet appliance event has occurred that has caused the archive stored on the WANJet appliance to either become unavailable or corrupted for some reason.

Note that when you upload a copy of an archive, you must specify the exact path name for the directory in which the downloaded archive copy is stored.

To upload an archive

1. In the navigation pane, expand **System**, and click **Archives**.
   The Archives screen opens.
2. In the upper-right corner of the screen, click **Upload**.
   This opens the Upload screen.
3. In the **File Name** box, type the complete path and file name of the archive that you want to upload onto the WANJet appliance.
   If you do not recall the path or file name, you can use the **Browse** button to locate and select the file name.
4. For the **Options** setting, check the **Overwrite existing archive file** box if you want the WANJet appliance to overwrite any existing archive file.

   Note: *The WANJet appliance overwrites an existing archive with the uploaded file only when the name of the archive you are uploading matches the name of an archive on the WANJet appliance.*
5. Click **Upload**.
   This uploads the specified archive to the directory **/var/local/ucs** on the WANJet appliance.

Deleting an archive

You can use the Configuration utility to delete any archive on the WANJet appliance that is stored in the directory **/var/local/ucs.**

To delete an archive

1. In the navigation pane, expand **System**, and click **Archives**.
   The Archives screen opens.
2. In the File Name column, locate the name of the archive you want to delete.
3. To the left of the archive name, check the Select box.
4. Click **Delete**.
   A confirmation box appears.
5. Click **Delete** again.
   This deletes the archive from the **/var/local/ucs** directory on the WANJet appliance.

12

Monitoring the WANJet Appliance

- Introducing reports
- Viewing Real Time Traffic reports
- Viewing Comparative Throughput reports
- Viewing Diagnostic reports
- Using third-party reporting systems

Introducing reports

The WANJet appliance provides reports that you can use to monitor WAN traffic, connectivity, and performance. You can display the reports on the WANJet appliance by expanding **WAN Optimization** in the navigation pane and clicking one of the following report options:

- **Diagnostics**
- **Comparative Throughput**
- **Real Time Traffic**
- **Monitoring**

It is easier to view the reports if your Configuration utility browser window is full-screen size.

◆ **Note**

To ensure accurate reports, we suggest that you configure an NTP time server for each WANJet appliance to synchronize the time. For more information, see Configuring NTP time servers, on page 5-14.

This chapter describes how to display the reports and also explains other ways of obtaining information about performance, including using network diagnostic tools, reviewing operational logs, and integrating with third-party reporting tools.

Information about the WANJet link status and the operational mode of the local appliance appears on the dashboard, in the top left corner of the Configuration utility screen. The dashboard provides a snapshot of system activity, and it is updated every 10 seconds. Therefore, you may see different numbers on the dashboard and the reporting screens described in this chapter because connections are established and terminated very frequently. For more information about the dashboard, see *Using the dashboard*, on page 4-2.

Viewing Real Time Traffic reports

The Real Time Traffic report displays a graph, in real time, of the volume of network traffic on both the LAN and the WAN. interfaces of the local WANJet appliance. The graph provides an at-a-glance overview of the network traffic that is traveling through the WANJet appliance.

To view a graph of network traffic in real time

In the navigation pane, expand **WAN Optimization** and click **Real Time Traffic**.
The Real Time Traffic report opens as shown in Figure 12.1. You may need to reply to Security Information questions, and press Enter or spacebar to view the report.

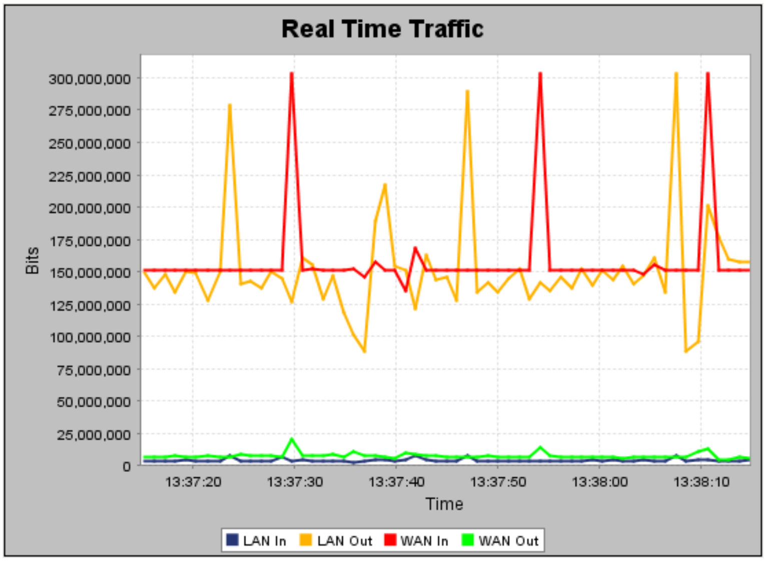


Figure 12.1 *Real Time Traffic report (standard inline configuration)*

In a Real Time Traffic report for a standard inline configuration:

- The vertical axis indicates the amount of network traffic, in bits per second.
- The horizontal axis shows the time (using a 24-hour clock) in hours, minutes, and seconds, in 10-second intervals.
- The blue line (**LAN In**) represents the raw data traveling into the local WANJet appliance on its LAN interface.
- The yellow line (**LAN Out**) represents the data (optimized and non-optimized) traveling out of the local WANJet appliance on its LAN interface.

- The red line (**WAN In**) represents the data (optimized and non-optimized) traveling into the local WANJet on its WAN interface appliance from its remote partner.
- The green line (**WAN Out**) represents the data (reconstituted and passthrough) traveling out of the local WANJet appliance on its WAN interface.

If you run the Real Time Traffic report on a WANJet appliance set up using a one-arm configuration, the report changes. Because there are no LAN and WAN connections in that configuration, you see only two lines showing the **Data In** and **Data Out**, as shown in Figure 12.2.

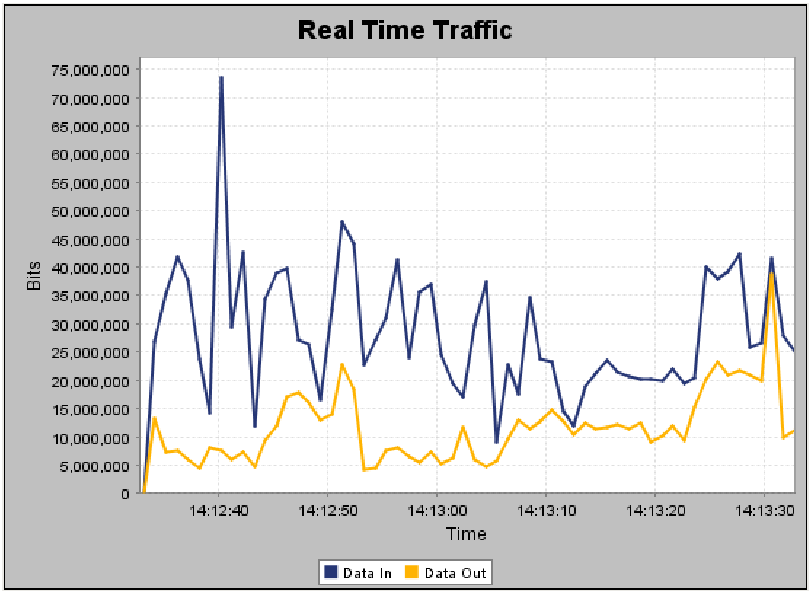


Figure 12.2 *Real Time Traffic report (one-arm configuration)*

In a Real Time Traffic report for a one-arm configuration:

- The vertical axis indicates the amount of network traffic, in bits per second.
- The horizontal axis shows the time (using a 24-hour clock) in hours, minutes, and seconds, in 10-second intervals.
- The blue line (**Data In**) represents the raw data that is traveling into the local WANJet appliance.
- The yellow line (**Data Out**) represents the data traveling out of the local WANJet appliance.

For more information on one-arm configuration, refer to *Deploying in a one-arm configuration*, on page 2-4.

Viewing Comparative Throughput reports

You can generate a Comparative Throughput report based on any combination of traffic direction, data type, and time period. Comparative Throughput reports refresh automatically every two minutes.

At the top of each report, there is a summary of the amount of data handled before and after compression, the bandwidth made available by optimization (expressed as a percentage of the total bandwidth), and the compression ratio achieved. These figures vary according to the selected time period and direction of traffic.

The table below the graph, **Throughput summary for the last <0> days, <0> hours**, summarizes the amount of raw data and the compressed data on the WANJet appliance since its installation.

The default report that is displayed when you open this screen is the total throughput (direction) for optimized data (data type) for the last hour (time period). As you make your selections, the data displayed on the screen changes accordingly.

You can download any of the reports as text files with comma-separated values (CSV). Then, you can import CSV reports into a database or spreadsheet package.

To generate a Comparative Throughput report and save it to a file

1. In the navigation pane, expand **WAN Optimization** and click **Comparative Throughput**.
2. Near the top of the main screen, click one of the following options to select the direction of traffic:
    - **Total Throughput**
      Shows all traffic that the WANJet appliance processes.
    - **Sent Throughput**
      Shows the outgoing (sent) data that was optimized.
    - **Received Throughput**
      Shows the incoming (received) data that was optimized.
3. To determine the portion of data to display and how to display it, click one of the following data type options above the graph:
    - **Performance Increase report**
      Shows the performance increase by comparing the bandwidth before and after optimization. See *Performance Increase report*, on page 12-6.
    - **Actual Bandwidth Expansion report**
      Shows the actual bandwidth amount that the WANJet appliance freed during optimization. See *Actual Bandwidth Expansion report*, on page 12-7.

- **Optimized Data report**
  Shows a comparison of the amount of network traffic before and after the WANJet appliance optimized the data. See *Optimized Data report*, on page 12-8.
- **Overall Data report**
  Shows the amount of passthrough data, raw data, and compressed data. See *Overall Data report**, on page 12-9***.
- **Link Utilization report**
  Displays the average amount of bandwidth used, compared with the amount of bandwidth that would have been used without optimization. See *Link Utilization report*, on page 12-10.

4. Below the graph, click the time period for which you want to display data: **Hour**, **Day**, **Week**, **Month**, **Quarter**, or **Year**. The default value is **Hour**.

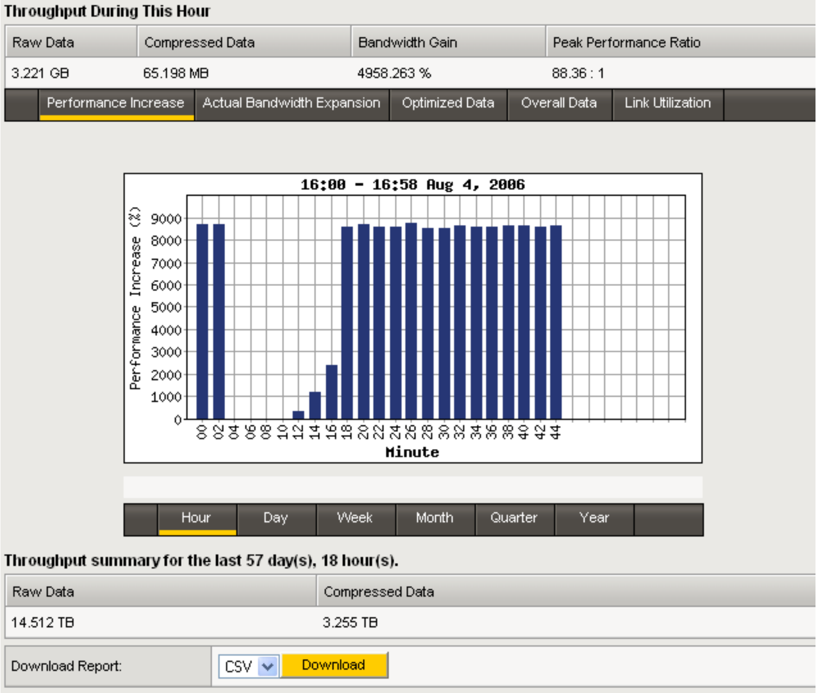
   The time period you select also determines the interval for which the throughput total summaries appear at the top of the report.

   Note*: The WANJet appliance saves all of the reports generated for the last hour, every hour. If you stop or restart the WANJet appliance, or any external termination occurs, you can view the last set of saved reports when you restart the WANJet appliance.*

5. To save the report to a file, in the **Download Report** box, click the **Download** button.
   The displayed report is saved into a text file with a CSV extension.

Performance Increase report

The Performance Increase report displays the percentage increase in bandwidth that results from using the WANJet appliance.



Throughput During This Hour

Raw Data	Compressed Data	Bandwidth Gain	Peak Performance Ratio
3.221 GB	65.198 MB	4958.263 %	88.36 : 1

Throughput summary for the last 57 day(s), 18 hour(s).

Raw Data	Compressed Data
14.512 TB	3.255 TB

Download Report: CSV

__Figure 12.3__ Performance Increase report

In this report, shown in Figure12.3, the vertical axis indicates the percentage increase in bandwidth. The system calculates this percentage by comparing the bandwidth freed up by the WANJet appliance with the bandwidth used after optimization. This is calculated as follows:

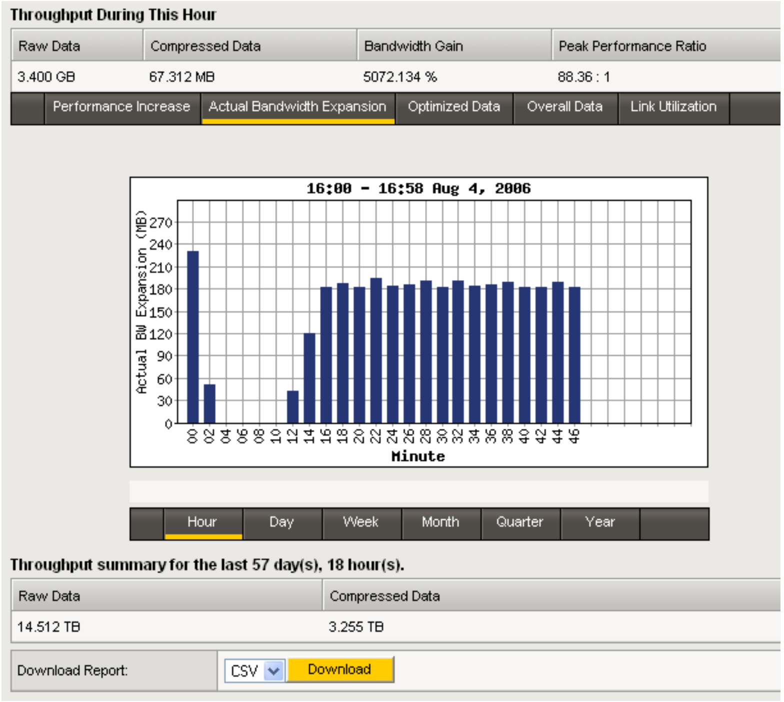
(Freed Bandwidth / Bandwidth after optimization) x 100 = Percentage Performance Increase

For example, if the bandwidth before optimization was 100 MB, and the bandwidth used by data after optimization is 25 MB, the amount of bandwidth freed up by the WANJet appliance is 75 MB. Using these values in the equation results in the following performance increase percentage:

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

Actual Bandwidth Expansion report

The Actual Bandwidth Expansion report, shown in Figure12.4, displays the amount of actual bandwidth that the WANJet appliance has freed by optimizing network data.



Throughput During This Hour

Raw Data	Compressed Data	Bandwidth Gain	Peak Performance Ratio
3.400 GB	67.312 MB	5072.134 %	88.36 : 1

Throughput summary for the last 57 day(s), 18 hour(s).

Raw Data	Compressed Data
14.512 TB	3.255 TB

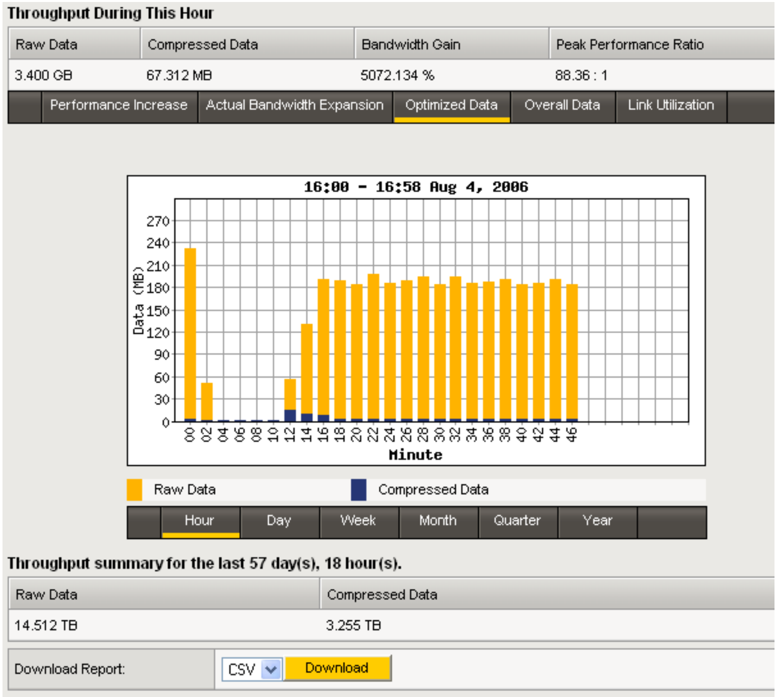
Download Report: CSV Download

Figure 12.4 Actual Bandwidth Expansion report

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

Optimized Data report

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



Throughput During This Hour

Raw Data	Compressed Data	Bandwidth Gain	Peak Performance Ratio
3.400 GB	67.312 MB	5072.134 %	88.36 : 1

Throughput summary for the last 57 day(s), 18 hour(s).

Raw Data	Compressed Data
14.512 TB	3.255 TB

Download Report: CSV Download

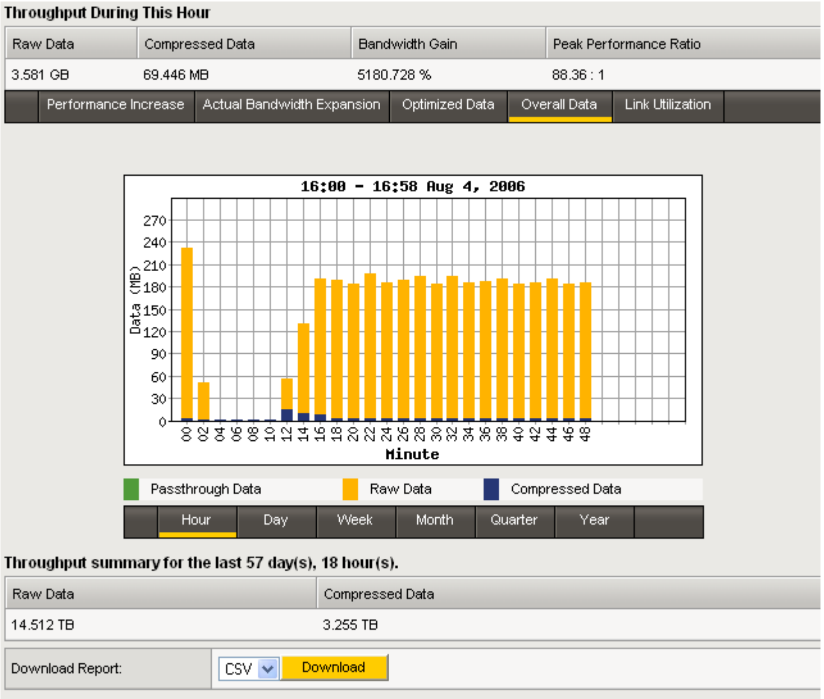
Figure 12.5 *Optimized Data report*

Figure12.5 shows the elements in this report:

- 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 after 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.



Throughput During This Hour

Raw Data	Compressed Data	Bandwidth Gain	Peak Performance Ratio
3.581 GB	69.446 MB	5180.728 %	88.36 : 1

Throughput summary for the last 57 day(s), 18 hour(s).

Raw Data	Compressed Data
14.512 TB	3.255 TB

Download Report: CSV Download

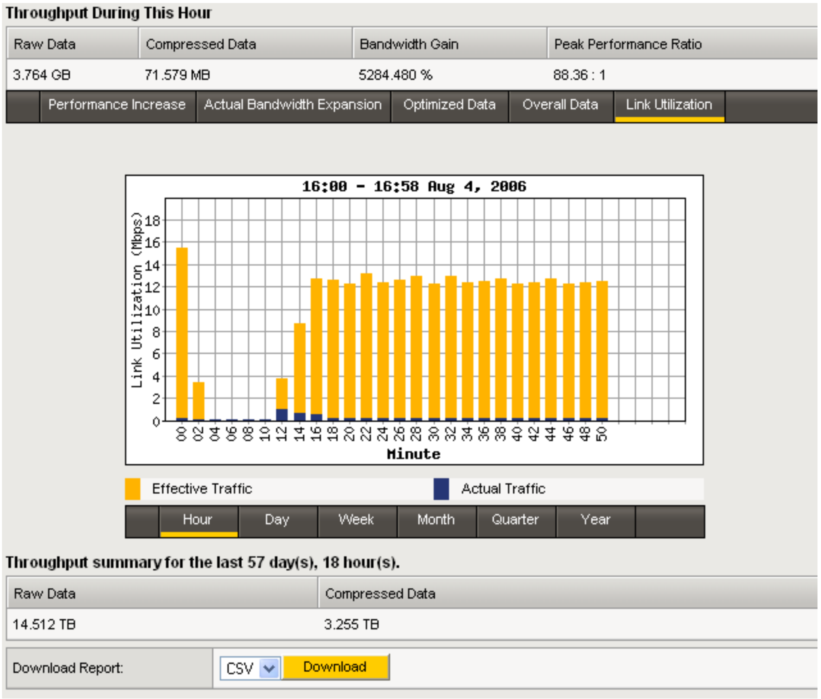
Figure 12.6 Overall Data report

Figure12.6 shows the elements in this report:

- The vertical axis indicates the amount of data traveling through the link (in kilobytes, megabytes, gigabytes, and so forth).
- The green bar represents the amount of passthrough data.
- The blue bar represents the amount of compressed (optimized) data.
- The yellow bar represents the amount of freed bandwidth.
- The bars as a whole represent the total amount of data traveling through the WANJet appliance.

Link Utilization report

The Link Utilization report is similar to the *Optimized Data report*, on page 12-8. However, instead of showing the total amount of data optimized over a given time period, the 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.



Throughput During This Hour

Raw Data	Compressed Data	Bandwidth Gain	Peak Performance Ratio
3.764 GB	71.579 MB	5284.480 %	88.36 : 1

Throughput summary for the last 57 day(s), 18 hour(s).

Raw Data	Compressed Data
14.512 TB	3.255 TB

Download Report: CSV

Figure 12.7 *Link Utilization report*

Figure12.7 shows the elements in this report:

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

Viewing Diagnostic reports

Diagnostic reports provide you with 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 **WAN Optimization** and click **Diagnostics**.
   The initial diagnostics screen opens.
2. On the menu bar, click one of the following options to display detailed reports:
   - **Monitoring**
   - **Connectivity**
   - **General**

   Each menu bar option provides several additional reports.

Monitoring

The following diagnostic reports are available from the Monitoring menu:

- WANJet Links
- Optimized Sessions
- Passthrough Sessions
- TCP Statistics
- TDR Statistics
- QoS

WANJet Links diagnostics

The WANJet Links report displays information about other WANJet appliances that connect to the one you are working on.

To view diagnostics for WANJet Links

1. In the navigation pane, expand **WAN Optimization** and click **Diagnostics**.
   The initial diagnostics screen opens.
2. From the Monitoring menu, choose WANJet Links.
   The WANJet Links report opens and displays the following information:
   - **Remote IP**
     IP address of the remote WANJet appliance.

- **Optimized Packets**
  Number of packets sent to the remote WANJet appliance that have been optimized.
- **Retransmitted Packets**
  Number of packets that the local WANJet appliance retransmitted to the remote WANJet appliance because the first transmission was not acknowledged.
- **Total Passthrough Packets**
  Number of packets sent to the remote WANJet appliance that have not been optimized.

◆ **Note**

For additional information about links to remote WANJet appliances, refer to Configuring routes, on page 9-6.

Optimized Sessions diagnostics

The Optimized Sessions report displays all of the network connections at the application layer that the WANJet appliance is currently optimizing. In contrast to the number of optimized sessions shown on the dashboard, the report shows established sessions only, and does not include those in the process of being set up or torn down. Therefore, the number of optimized sessions shown in the dashboard may not match the number in the Optimized Sessions report.

To view diagnostics for Optimized Sessions

1. In the navigation pane, expand **WAN Optimization** and click **Diagnostics**.
   The initial diagnostics screen opens.
2. From the Monitoring menu, choose Optimized Sessions.
   The Optimized Sessions screen opens.

   The Optimized Sessions report has two sections: one for TCP and another for UDP traffic.

   The TCP section contains the following information:

   - **LocalIP**
     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.
   - **RemoteIP**
     IP address and port for the remote WANJet appliance.
   - **WANJetIP**
     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 (from) and destination (to).

◆ **Note**

For information about how to specify connections for optimization, see Creating optimization policies, on page 7-2.

Passthrough Sessions diagnostics

A ***passthrough session*** is a network connection (at the application layer) for traffic that the WANJet appliance does not optimize, but allows that particular type of traffic to pass through the appliance untouched.

To view diagnostics for Passthrough Sessions

1. In the navigation pane, expand **WAN Optimization** and click **Diagnostics**.
   The initial diagnostics screen opens.
2. From the Monitoring menu, choose Passthrough Sessions.
   The Passthrough Sessions screen opens.

   The Passthrough Sessions report has two sections: one for TCP traffic and another for UDP traffic, with specific information in each section.

   From this screen, you can view the following reports:

   - **All Passthrough Sessions**
     Displays a detailed list of all passthrough sessions.
   - **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. 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.
   - **Realtime**
     Displays the amount of passthrough traffic throughput in real time.

◆ **Note**

For information about how to specify connections for optimization, see Creating optimization policies, on page 7-2.

TCP Statistics diagnostics

The TCP Statistics menu provides options to view information about TCP connections.

To view diagnostics for TCP Statistics

1. In the navigation pane, expand **WAN Optimization** and click **Diagnostics**.
   The initial diagnostics screen opens.
2. From the Monitoring menu, choose TCP Statistics.
   The TCP Statistics screen opens with the Connections States report displayed, by default.
3. Click the options above the report to view the following reports:
   - **Connections States**
   - **Packet Retransmissions**
   - **Receive Queue Packets Pruned**

Connection States

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

- **ESTABLISHED**
  Established connections 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

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

Packet Retransmissions

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

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.

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 on the receiving host is too large. The optimal buffer size is twice the product of the bandwidth and the delay.

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 storing the contents of frequently accessed files in memory. The TDR-2 Statistics report provides information about TDR-2 utilization. For more information about TDR, refer to *Understanding optimization: Transparent Data Reduction*, on page 1-2.

◆ **Note**

The WANJet appliance updates the statistics in the report at the completion of a session. For example, if you transfer a 1 GB file, the updated TDR-2 statistics are available when the file transfer is complete.

To view diagnostics for TDR Statistics

1. In the navigation pane, expand **WAN Optimization** and click **Diagnostics**.
   The initial diagnostics screen opens.
2. From the Monitoring menu, choose TDR Statistics.
   The TDR Statistics report opens and displays the following TDR-2 information:
   - **WANJetIP**
     IP address of the remote WANJet appliance.
   - **Sent Bytes (TDR-2)**
     The amount of sent data, in bytes, to which TDR-2 optimization has been applied since the WANJet link became active.
   - **Sent Bytes (other)**
     Amount of sent data, in bytes, to which TDR-2 optimization has not been applied.

- **Received Bytes (TDR-2)**
  Amount of received data, in bytes, to which TDR-2 optimization has been applied.
- **Received Bytes (other)**
  Amount of received data, in bytes, to which TDR-2 optimization has not been applied.
- **TDR-2 efficiency %**
  Percentage of total data sent and received across the link to which TDR-2 optimization has been applied. This percentage represents the increase in performance due to TDR-2 optimization. The bold number at the bottom of the report is the average TDR-2 effectiveness for all the remote WANJet appliance links to the local WANJet appliance.

QoS diagnostics

Quality of Service (QoS) policies can 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 **WAN Optimization** and click **Diagnostics**.
   The initial diagnostics screen opens.
2. From the Monitoring menu, choose QoS.
   The QoS report opens and displays the following information:
   - **Remote WANJet**
     The IP address of a remote WANJet or the alias of a WAN link that has a QoS policy assigned to it.
   - **Policy**
     Name of the QoS policy assigned to traffic on the link. Each remote WANJet appliance and WAN link has a default policy (shown as **Default**) in addition to any policies that you create.
   - **Rate**
     Minimum bandwidth assigned to the policy when the traffic load rises. For example, if you assigned a bandwidth of 50% to the policy and the link bandwidth is 100 mb/s, the rate would be 50 mb/s.
   - **Ceiling**
     Maximum percentage that the policy can borrow from unused bandwidth.
   - **Bytes Sent**
     Number of bytes sent in accordance with the policy.
   - **Dropped**
     Number of qualified packets that the policy could not handle.

For additional information about QoS, refer to ***Creating Application QoS policies***, on page 7-9.

Connectivity

Connectivity diagnostic information includes the following reports:

- **All**
- **Ethernet**
- **IP**
- **Bridge**
- **Remote WANJets**
- **Connections**

All connectivity diagnostics

The Diagnose Connectivity report displays details about all types of configurations (Ethernet, IP, bridge, and remote WANJet appliances).

To view diagnostics for all connectivity

1. In the navigation pane, expand **WAN Optimization** and click **Diagnostics**.
   The initial diagnostics screen opens.
2. From the Connectivity menu, choose All.
   The Diagnose Connectivity screen opens.

This report includes the information for all the configuration types, each of which also has a separate report. The information is the same in the combined report and the individual reports, as described in the following sections.

Ethernet diagnostics

The Diagnose Ethernet report displays details about the Ethernet interfaces on the local WANJet appliance, including the speed, flow control, transmitted and received bytes, errors, and collisions. For WANJet appliances to work correctly, the speed and duplex settings for the LAN and WAN interfaces should be the same. The Diagnose Ethernet screen confirms these settings.

◆ **Note**

For information about configuring the speed and duplex settings for Ethernet interfaces, see Configuring interfaces, on page 9-1.

To view diagnostics for Ethernet connectivity

1. In the navigation pane, expand **WAN Optimization** and click **Diagnostics**.
   The initial diagnostics screen opens.

2. From the Connectivity menu, choose Ethernet.
   The Diagnose Ethernet report opens and includes a section for each of the Ethernet interfaces on the WANJet appliance:
   - **Management**
   - **LAN**
   - **Peer**
   - **WAN**

   For each interface, the report includes information about the speed and duplex settings, flow control, data transmitted, errors, and collisions.

   Application QoS works only if the Ethernet interfaces are connected as follows:
   - The **LAN** interface must connect to the LAN switch or router.
   - The **WAN** interface must connect to the WAN gateway.

◆ **Note**

If a redundant pair is present, the ***Peer*** *interface must be connected to the redundant peer. For more information, see Configuring redundant peers, on page 8-10.*

IP diagnostics

The Diagnose IP report displays technical details about the configuration of the IP address of the local WANJet appliance.

To view diagnostics for IP connectivity

1. In the navigation pane, expand **WAN Optimization** and click **Diagnostics**.
   The initial diagnostics screen opens.
2. From the Connectivity menu, choose IP.
   The Diagnose IP report opens and 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.

Bridge diagnostics

The Diagnose Bridge report 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 **WAN Optimization** and click **Diagnostics**.
   The initial diagnostics screen opens.

2. From the Connectivity menu, choose Bridge.
   The Diagnose Bridge report opens and 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

The WANJet appliance bridge works only if the Ethernet interfaces are connected as follows:

- The **LAN** interface must connect to the LAN switch or router.
- The **WAN** interface must connect to the WAN gateway.

Remote WANJet appliance diagnostics

The Diagnose Remote WANJet report 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 Configuring remote WANJet appliances, on page 5-10.

To view diagnostics for remote WANJet appliance connectivity

1. In the navigation pane, expand **WAN Optimization** and click **Diagnostics**.
   The initial diagnostics screen opens.

2. From the Connectivity menu, choose Remote WANJets.
   The Diagnose Remote WANJets report opens and displays the following information for each remote WANJet appliance:

   - The software version number, which is compared to the version number of the software on the local WANJet appliance
   - 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 is **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.
- The status of the tunnel between the two WANJet appliances

Connections diagnostics

The Diagnose Connections report displays information about optimized and passthrough connections.

General

General diagnostic information is where you find the Diagnostic log and can create system snapshots.

Diagnostic Log

The Diagnostic Log contains status information and errors that the WANJet appliance records during a session. This log keeps you informed and helps resolve problems that you might encounter while working with the WANJet appliance.

To view the diagnostic log

1. In the navigation pane, expand **WAN Optimization** and click **Diagnostics**.
   The initial diagnostics screen opens.
2. From the General menu, choose Diagnostic Log.
   The Diagnostic log shows information about the WANJet appliance.

Creating system snapshots

You can create a system snapshot and download it 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 create a system snapshot

1. At the top the Diagnostic Log screen, click **System Snapshot** to get the current system status.
   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__: To view the snapshot file, you first need to extract it using a tool such as __gunzip__, which is available at __www.gzip.org__.

3. Rename the compressed file using the following format:

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

   For example:

   `snapshot-acme-2005-04-22`

   You can provide this file to F5 Networks Technical Support for assistance with troubleshooting issues.

Using third-party reporting systems

You can configure the WANJet appliance to work with third-party reporting systems, including NetFlow and RMON2.

Configuring a NetFlow server

If you use NetFlow for network monitoring, you can configure a NetFlow server on the WANJet appliance. If configured, the WANJet appliance transfers traffic data to the NetFlow server for analysis.

To configure a NetFlow server

1. In the navigation pane, expand **WAN Optimization** and click **Monitoring**.
   The WANJet Netflow and SNMP screen opens.
2. Check the **Netflow Server IP** box, and type the IP address of the NetFlow server.
3. Click **Save**.

RMON2 reports

The WANJet appliance provides statistics for network and application performance through Remote Network Monitoring (RMON2). You can configure the WANJet appliance so that you can view RMON2 reports (data trees), which are part of the SNMP data trees that are stored on the WANJet appliance. The RMON2 data is stored in a MIB. For information on the WANJet MIB file, see Appendix **C, *WANJet Appliance Private MIB File***.

The RMON2 data on the 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. You can configure the WANJet appliance to report these statistics as **Raw Data** (prior to being optimized) or **WANJet Data** (optimized).

Enabling RMON2 logs

If you use RMON2 to monitor network traffic, you can configure the WANJet appliance to gather RMON2 data.

To configure RMON2 logs

1. In the navigation pane, expand **WAN Optimization** and click **Monitoring**.
   The WANJet Netflow and SNMP screen opens.
2. To collect RMON2 data, check the **Enable RMON2 Logs** box and select an option:
   - **Raw Data**
     To gather RMON2 logs before the WANJet appliance processes traffic.
   - **WANJet Data**
     To gather RMON2 logs after the WANJet appliance processes traffic.

   Note*: For details on the Raw Data and WANJet Data settings, see RMON2 configuration settings, on page 12-22.*
3. Click **Save**.

For additional instructions, see *RMON2 configuration settings*, on page 12-22. Note that the SNMP server must have access to the WANJet appliance.

To view RMON2 reports

To view the RMON2 data tree, you must use SNMP-compliant software. You need to provide SNMP-compliant software with the IP address of the WANJet appliance.

RMON2 configuration settings

RMON2 provides network and application protocol statistics (bytes transmitted and bytes received) that include both the unoptimized protocol statistics from the LAN side, and the optimized (compressed) protocol statistics from the WAN side. When enabling RMON2 logs as described in the previous section, you can configure the WANJet appliance to report this information as:

- **Raw Data**
- **WANJet Data**

If your network monitoring system recognizes only the standard RMON2 variables, select the option that reports the type of data you prefer to monitor. If you want to monitor the unoptimized data, select the **Raw Data** option. If you want to monitor the optimized data, select the **WANJet Data** option.

If your RMON2-based monitoring software recognizes the F5 Networks-added table entries, the choice of setting may not be significant. Select the setting that allows you to use both types of data in the way best suited to the configuration of your network management software.

The following sections provide further technical details concerning the implications of selecting either option.

Raw data

By selecting the **Raw Data** option on the WANJet NetFLow and SNMP screen, you instruct the WANJet appliance to place unoptimized (LAN-side) protocol statistics into the standard variables reported through RMON2. The F5-specific second set of variables contains the optimized protocol statistics.

For example, performing an SNMP walk of the **protocolDirTable** object (OID 1.3.6.1.2.1.16.11.2 in the RMON2 MIB) might display the following variable names in **protocolDirDescr**:

Standard RMON2 (unoptimized/LAN-side)

```
any.ip
any.ip.udp
any.ip.tcp
any.ip.tcp.22
```

F5 Networks (optimized/WAN-side)

```
any.IPuncompressed
any.IPuncompressed.udp
any.IPuncompressed.tcp
any.IPuncompressed.tcp.22
```

In this example, the first three protocols in both lists are permanent entries. The fourth protocol in both shows a protocol that is added to the tables at runtime. The protocol, **any.ip.tcp.22**, contains statistics for the Secure Shell (SSH) protocol. This is true for both the **Raw Data** and **WANJet Data** options.

WANJet appliance data

By selecting the **WANJet Data** option on the WANJet NetFlow and SNMP screen, you instruct the WANJet appliance to place optimized (WAN-side) protocol statistics into the standard variables reported through RMON2. The F5-specific second set of variables contains the unoptimized protocol statistics.

For example, performing an SNMP walk of the **protocolDirTable** object in this configuration might have the following variable names in **protocolDirDescr**:

Standard RMON2 (optimized/WAN-side)

```
any.ip
any.ip.udp
any.ip.tcp
any.ip.tcp.22
```

F5 Networks (unoptimized/LAN-side)

```
any.IPcompressed
any.IPcompressed.udp
any.IPcompressed.tcp
any.IPcompressed.tcp.22
```

13

Logging WANJet Appliance System Events

- Introducing WANJet appliance logging
- Understanding log types
- Setting log levels
- Configuring encrypted remote logging

Introducing WANJet appliance logging

Viewing and managing log messages is an important part of maintaining a WANJet® appliance. Log messages inform you on a regular basis of the events that are happening on the system. Some of these events pertain to general events happening within the operating system, while other events are specific to the WANJet appliance, such as the stopping and starting of WANJet system services.

The mechanism that the WANJet appliance uses to log events is the utility **syslog-ng**. The ***syslog-ng*** utility is an enhanced version of the standard logging utility **syslog**.

The types of events that the WANJet appliance logs are:

- **System events**
  System event messages are based on operating system events, and are not specific to the WANJet appliance.

- **Local traffic events**
  Local-traffic event messages pertain specifically to the local traffic management system.

- **Audit events**
  Audit event messages are those that the WANJet appliance logs as a result of changes to the WANJet appliance configuration. Logging audit events is optional, and audit logging is disabled, by default.

Summarizing logging features

The logging mechanism on a WANJet appliance includes several features designed to keep you informed of system events in the most effective way possible.

One of the primary features of the logging feature is its ability to log different types of events, ranging from system events to local traffic events. Through the WANJet appliance auditing feature, you can even track and report changes that users make to the WANJet appliance configuration, such as adding a virtual server or designating a device to be part of a redundant system. For more information, see *Reviewing log content*, on page 13-2 and *Understanding log types*, on page 13-4.

When setting up logging on the WANJet appliance, you can customize the logs by designating the minimum severity level, or log level, that you want the WANJet appliance to report when a type of event occurs. The ***minimum log level*** indicates the minimum severity level at which the WANJet appliance logs that type of event.

For example, you can specify that, for any change a user makes to the bigdb database, the minimum severity level for which the WANJet appliance logs messages is **Warning**. This means that the WANJet appliance logs

Warning and more severe messages such as **Error** and **Critical** messages, but not less severe ones such as **Notice**, **Informational**, or **Debug** messages. For more information, see *Setting log levels*, on page 13-6.

You can search for a string within a log event, that is, filter the display of the log messages according to the string you provide. For more information, see *Viewing and filtering log messages*, on page 13-3.

Finally, you can log WANJet appliance events to a remote logging server. You do this by identifying the IP address or host name of the remote logging server, and creating an encrypted network connection, or tunnel, for sending log information to that remote server. For more information, see *Configuring encrypted remote logging*, on page 13-9.

◆ **Tip**

You can also configure the system to send email or activate pager notification based on the priority of the logged event.

Reviewing log content

The logs that the WANJet appliance generates include several types of information. For example, all logs except the audit log show a timestamp, host name, and service for each event. Some logs show a status code, while the audit log shows a user name and a transaction ID corresponding to each configuration change. All logs contain a 1-line description of each event.

Table 13.1 lists the categories of information contained in the logs and the specific logs in which the information is displayed.

Information Type	Explanation	Log Type
Timestamp	The time and date that the system logged the event message.	System Local Traffic
Host name	The host name of the system that logged the event message. Because this is typically the host name of the local machine, the appearance of a remote host name could be of interest.	System Local Traffic
Service	The service that generated the event.	System Local Traffic
Status code	The status code associated with the event. Note that only events logged by WANJet appliance components, and not operating system services, have status codes.	Local Traffic
Description	The description of the event that caused the system to log the message.	System Local Traffic
User Name	The name of the user who made the configuration change.	Audit

Table 13.1 *Log information categories and their descriptions*

Information Type	Explanation	Log Type
Transaction	The identification number of the configuration change.	Audit
Event	A description of the configuration change that caused the system to log the message.	Audit

Table 13.1 *Log information categories and their descriptions (Continued)*

Viewing and filtering log messages

You can view and filter the log files that the WANJet appliance generates.

To view log messages

1. In the navigation pane, expand **System**, and click **Logs**.
   The Logs screen opens.
2. On the menu bar, click **System**, **Local Traffic**, or **Audit**, depending on the type of log messages you want to view.
   This displays the appropriate logs.
3. If you want to display another screen of messages, first locate the page list at the lower-right corner of the screen. You can either:
   - Display the list and select a page number or **Show All**.
   - Click the right arrow to advance to the next page of messages.

To filter log messages based on a search string

1. In the navigation pane, expand **System**, and click **Logs**.
   The Logs screen opens.
2. On the menu bar, click **System**, **Local Traffic**, or **Audit**, depending on the type of log messages you want to view.
   This displays the appropriate logs.
3. In the **Search** box (directly above the Timestamp column), type a string, optionally using the asterisk as a wildcard character.
4. Click **Search**.
   This displays only those messages containing the string you specified.

Understanding log types

The WANJet appliance automatically logs three main event types: system, local traffic, and configuration changes (audit). Each type of event is stored in a separate log file, and the information stored in each log file varies depending on the event type. All log files for these event types are placed in the directory **/var/log**.

Logging system events

Many events that occur on the WANJet appliance are operating system-related events, and do not specifically apply to the WANJet appliance. The WANJet appliance logs the messages for these events in the file **/var/log/messages**.

Table 13.2 shows some sample system log entries.

Timestamp	Host	Service	Event
Mon Jun 25 03:34:45 PDT 2007	wanjet3	syslog-ng[1151]	new configuration initialized
Mon Jun 25 03:35:06 PDT 2007	wanjet3	syslog-ng[1151]	SIGHUP received, restarting syslog-ng
Mon Jun 25 04:38:06 PDT 2007	wanjet3	shutdown	shutting down for system reboot

Table 13.2 *Sample system log entries*

Logging local traffic events

Many of the events that the WANJet appliance logs are related to local area traffic passing through the WANJet appliance. The WANJet appliance logs the messages for these events in the file **/var/log/ltm**.

Table 13.3 shows some sample local-traffic log entries.

Timestamp	Host	Service	Status Code	Event
Mon Jun 25 03:34:45 PDT 2007	wanjet2	logger	011d0004	Disk partition shared has only 19 free
Mon Jun 25 03:35:06 PDT 2007	wanjet2	sod[1439]	01140029	HA daemon_heartbeat genericproxy fails action is restart.
Mon Jun 25 04:38:06 PDT 2007	wanjet2	NtClOS	NA	Link down with wj79 10.16.79.201
Mon Jun 25 04:40:06 PDT 2007	wanjet2	NtClOS	NA	Link up with wj79 10.16.79.201

Table 13.3 *Sample local-traffic log entries*

Some of the specific types of events that the WANJet appliance displays on the Local Traffic logging screen are:

- Address Resolution Protocol (ARP) packet and ARP cache events
- bigdb database events (such as populating and persisting bigdb variables)
- HTTP protocol events
- HTTP compression events
- IP packet discard events due to exceptional circumstances or invalid parameters (such as a bad checksum)
- Layer 4 events (events related to TCP, UDP, and Fast L4 processing)
- MCP/TMM configuration events
- Monitor configuration events
- Network events (Layers 1 and 2)
- Packet Velocity® ASIC (PVA) configuration events
- iRule events related to run-time iRule processing
- SSL traffic processing events
- General TMM events, such as TMM startup and shutdown

◆ **Note**

*For information on setting a minimum log level on each of these event types, see **Setting log levels for local traffic events**, on page 13-6.*

Auditing configuration changes

Audit logging is an optional feature that logs messages whenever a WANJet appliance configuration is changed. You can track auditing changes:

- By user action
- By system action
- By loading configuration data

The WANJet appliance logs the messages for these auditing events in the file **/var/log/audit**.

Table 13.4 shows some sample audit log entries. In this example, the first entry shows that user **admin** enabled the audit logging feature; the second entry shows where user **admin** disabled **Terminal Access** for user **NetworkAdmin**.

Timestamp	User Name	Transaction	Event

Fri Jun 8 16:01:13 PDT 2007	admin	107134-1	DB_VARIABLE modified:
			name="config.auditing"
			value="enable"

Fri Jun 8 16:04:18 PDT 2007	admin	110470-2	USERDB_ENTRY modified:
			name="NetworkAdmin"
			shell="/bin/false"

Table 13.4 *Sample audit log entries*

By default, audit logging is disabled. For information on enabling this feature, see *Setting log levels*, following.

Setting log levels

Using the Configuration utility, you can set log levels on both local traffic and auditing events. For each type of local traffic event, you can set a minimum log level. The ***minimum log level*** indicates the minimum severity level at which the WANJet appliance logs that type of event. For more information, see *Setting log levels for local traffic events*, following.

For auditing events, you can set a log level that indicates the type of event that the system logs, such as the user-initiated loading of WANJet appliance configurations, or system-initiated configuration changes. For more information, see *Setting log levels for auditing events*, on page 13-8.

Setting log levels for local traffic events

For local traffic events, you can set a minimum log level. Thus, for different kinds of local traffic events, such as bigdb configuration events or events related to HTTP compression, you can set different minimum log levels.

The log levels that you can set on certain types of events, ordered from highest severity to lowest severity, are:

- Emergency
- Alert
- Critical
- Error
- Warning

- Notice
- Informational
- Debug

For example, if you set the minimum log level for bigdb events to **Error**, then the system only logs messages that have a severity of **Error** or higher for those events. If you retain the default minimum log level (**Informational**), then the system logs all messages that have a severity of **Informational** or higher (that is, all messages except **Debug** messages).

You can set a minimum log level on many different types of local traffic events. Table 13.5 shows the types of local traffic events and the minimum log levels that you can configure for them. Because not all log levels are available for every local-traffic event type, the table shows the specific log levels you can set on each event type. Following the table is the procedure for setting the minimum log level on a local traffic event type.

Local-Traffic Event Type	Available Minimum Log Levels	Default Value
ARP/NDP	Error, Warning, Notice, Informational, Debug	Warning
BigDB	Critical, Error, Warning, Notice, Informational, Debug	Informational
HTTP	Error, Debug	Error
HTTP Compression	Error, Debug	Error
IP	Warning, Notice	Notice
iRules	Error, Informational, Debug	Informational
Layer 4	Notice, Informational, Debug	Notice
MCP	Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug	Notice
Monitors	Error, Debug	Error
Network	Critical, Error, Warning, Notice, Informational, Debug	Warning
Packet Velocity® ASIC	Informational, Debug	Informational
SSL	Error, Warning	Warning
Traffic Management OS	Emergency, Critical, Error, Notice, Informational	Error

Table 13.5 *Local-traffic event types and their available log levels*

To set a minimum log level for local traffic events

1. In the navigation pane, expand **System**, and click **Logs**.
   This opens the Logs screen.
2. On the menu bar, click **Options**.
   The screen for setting minimum log levels opens.
3. In the Local Traffic Logging area of the screen, locate the event type for which you want to set a minimum log level.
   An example of an event type is HTTP Compression.
4. Select a minimum log level from the list.
5. Click **Update**.

◆ **Note**

*For more information on local traffic event types, see **Logging local traffic events**, on page 13-4.*

Setting log levels for auditing events

An optional type of logging that you can enable is audit logging. Audit logging logs messages that pertain to configuration changes that users or services make to the WANJet appliance configuration. (For more information, see *Auditing configuration changes*, on page 13-5.)

You can choose one of four log levels for audit logging. In this case, the log levels do not affect the severity of the log messages; instead, they affect the initiator of the audit event.

The log levels for audit logging are:

- **Disable**
  This turns audit logging off. This is the default value.
- **Enable**
  This causes the system to log messages for user-initiated configuration changes only.
- **Verbose**
  This causes the system to log messages for user-initiated configuration changes and any loading of configuration data.
- **Debug**
  This causes the system to log messages for all user-initiated and system-initiated configuration changes.

To set a minimum log level for audit events

1. In the navigation pane, expand **System**, and click **Logs**.
   This opens the Logs screen.
2. On the menu bar, click **Options**.
   This displays the screen for setting minimum log levels on local traffic events.
3. In the Audit Logging area of the screen, select a log level from the **Audit** list.
4. Click **Update**.

Configuring encrypted remote logging

You can configure the Syslog utility on the WANJet appliance to send WANJet appliance log information to a remote logging host, using an encrypted network connection. To do this, you create a port-forwarding SSH tunnel to the remote logging host, and configure **syslog-ng** on the WANJet appliance to send log messages through the SSH tunnel.

Before you begin

Before you attempt to configure encrypted remote logging, you must meet the following conditions on the WANJet appliance and your remote logging host:

- **On the WANJet appliance**
  You must have a console with root access to the WANJet appliance.
- **On the remote logging host**
  You must have a console with root access to the remote logging host, the IP address, or the host name of the remote logging host.
- **For both systems**
  You must have both systems connected to the same subnetwork.

◆ **WARNING**

You should attempt this configuration only if you understand the risks associated with making changes to service startup scripts.

Creating the remote encrypted logging configuration

When creating an encrypted remote logging configuration, you must complete the following tasks:

- Review the SSH syntax required to create this configuration.
- Create a unique SSH identity key to identify and authorize the WANJet appliance.
- Edit the **syslog-ng** service startup script to create and destroy the SSH tunnels.
- Edit the remote logging host to accept **syslog-ng** messages through the SSH tunnel.
- Copy the unique SSH identity key to the remote logging host and append it to the authorized key file.
- Verify the logging configuration and restart **syslog-ng**.

Reviewing the SSH syntax required to create this configuration

This configuration requires that the WANJet appliance is able to establish an SSH connection to the remote logging host. On the WANJet appliance, use the **ssh** command to create the tunnel. Figure 13.1 is an example of the syntax required to create an SSH tunnel.

```
$ ssh -L <local tunnel port>:<remote log hostname>:<remote
tunnel port> \
  <remote user>@<remote log hostname> \
  -nNCxf \
  -i <key identity file>
```

Figure 13.1 *Establish an SSH tunnel from the WANJet appliance to the logging host.*

Table 13.6 contains detailed descriptions of the **ssh** syntax elements shown in Figure 13.1.

SSH syntax	Description
<local tunnel port>	The port SSH listens on for connections in order to forward them to **<remote log hostname>:<remote tunnel port>**.
<remote log hostname>	The IP address or FQDN of the remote logging server.
<remote tunnel port>	The port to which you want the SSH daemon on the remote logging server to forward connections.

Table 13.6 *Detailed syntax elements for configuring SSH*

SSH syntax	Description
<remote user>	The user name that **ssh** attempts to authenticate, as on **<remote log hostname>**.
<key identity file>	A file name from which the identity (private key) for authentication is read.

Table 13.6 *Detailed syntax elements for configuring SSH (Continued)*

Creating a unique SSH key to identify and authorize the WANJet appliance

After you have reviewed the **ssh** command syntax, use the **ssh** command to create the encrypted tunnel on the WANJet appliance, you must create a unique key on the WANJet appliance. The unique key is used to identify and authorize the WANJet appliance to the remote logging host.

Use the following command to create the file **syslog_tunnel_ID** and **syslog_tunnel_ID.pub**.

```
$ ssh -b 2048 -f syslog_tunnel_ID -t rsa -N "" -P ""
```

Use the following command to make **syslog_tunnel_ID** readable only by the **root** account:

```
$ chmod 600 syslog_tunnel_ID
```

Use the following command to make the public portion of the unique SSH ID named **syslog_tunnel_ID.pub** readable by all accounts:

```
$ chmod 644 syslog_tunnel_ID.pub
```

Copy **syslog_tunnel_ID** and **syslog_tunnel_ID.pub** into **/var/ssh** with the following command:

```
$ cp syslog_tunnel_ID* /var/ssh
```

Editing the syslog-ng start script to open and close the encrypted tunnel

Next change the **syslog-ng** start script, **/etc/init.d/syslog-ng**, so that the encrypted tunnel is opened when the **syslog-ng** script starts up and is closed when the script is restarted or stopped.

Before you edit the **syslog-ng** start script, save a backup copy to the root directory. Use the following command to save the backup to the root directory:

```
$ cp /etc/init.d/syslog-ng /root/syslog-ng.backup
```

After you save a backup of the **syslog-ng**, edit the startup script **/etc/init.d/syslog-ng** to automatically create a SSH tunnels when **syslog-ng** is started, or closed when **syslog-ng** is restarted or stopped.

The example configuration in this document demonstrates how to create a tunnel to a host using the following IP addresses and ports:

- IP address of **10.0.0.100**
- Local tunnel port of **5140**
- Remote tunnel port of **5140**
- User name **logger** on host **10.0.0.100**.

Type the syntax below the line that reads **start)**. Figure 13.2 is an example of what the section of the **syslog-ng** start script looks like after you specify the syntax. In this example, the syntax you add is shown in bold text.

```
start)
      ssh -L 5140:10.0.0.100:5140 \
      logger@10.0.0.100 -nNCxf \
      -i var/ssh/syslog_tunnel_ID
       echo -n "Starting $INIT_NAME: "
       daemon --check $INIT_PROG "$INIT_PROG $INIT_OPTS"
```

Figure 13.2 *Example syntax to start the syslog-ng script*

Next, add syntax below the line that reads **stop)**. Figure 13.3 shows the syntax you need to add in bold text.

```
stop)
       for sshTunnel in \
          `ps -ewo "%p!%a" | \
           grep ssh | \
           grep syslog_tunnel_ID | \
           grep -v grep | \
           cut -f 1 -d !`; do
           if [ -n "$sshTunnel" -a $sshTunnel -gt 10 ]; then
               echo " -- Shutting down SSH tunnel with process $sshTunnel"
               kill -TERM $sshTunnel
           fi
       done
       echo -n "Stopping $INIT_NAME: "
```

Figure 13.3 *Example syntax to start the syslog-ng script*

Editing syslog-ng to log messages on the remote logging host

After you add the syntax to open and close SSH tunnels, you can edit the **syslog-ng** configuration to log messages to the remote machine. To do this, you need to create source and filter configuration blocks based on the local environment.

Using the example IP addresses and ports used in the example in the previous section, you would edit the **syslog-ng.conf** file to look like the **syslog-ng.conf** in Figure 13.4.

```
# capture all messages
filter f_catchall {
   level(debug...emerg);
};

# send message to localhost through tcp port 5140
destination d_remoteLogTunnel {
   tcp("127.0.0.1" port(5140););
};

# Combine everything to actually perform logging
log {
   source(local);
   filter(f_catchall);
   destination(d_remoteLogTunnel);
};
```

Figure 13.4 *Example **syslog-ng.conf** configuration*

Copying the unique SSH identity to the remote logging host and appending it to the authorized keys file

After you have edited the **syslog-ng.conf** to log messages on the remote logging host, you must copy the unique SSH identity to the remote logging host. To do this, copy the **syslog_tunnel_ID.pub** to the remote syslog server, and append this key to the **authorized_keys** file found in the**.ssh** folder under the home directory of the user that you want to use to capture remote log messages.

```
$ cat syslog_tunnel_ID.pub >> ~logger/.ssh/authorized_keys
```

◆ **Note**

The following instructions are examples. The actual process for setting up the new SSH key to be automatically authorized, and configuring the syslog service may be different on your system.

Verify that the logging facility is configured and ready to receive syslog messages on the **<remote tunnel port>**. If the remote logging host uses **syslog-ng**, you need to add a source configuration block like the one in Figure 13.5.

```
source remote {
   tcp(ip(10.0.0.100) port(5140));
};
```

Figure 13.5 *Remote logging host source identification block.*

In addition to the source identification block, you also need to add filter, destination, and log configuration blocks to use the data from the source **remote** as required by your application.

Verifying the logging configuration and restarting syslog-ng

Finally, verify that the SSH connection is functional and restart the **syslog-ng** service.

To verify the configuration from a command line and restart the syslog-ng service

1. Log in as **root** to the WANJet appliance.
2. Make an SSH connection to the remote logging host using the new identity key you created.

   ```
   # ssh logger@10.0.0.100 -i /var/shh/syslog_tunnel_ID
   ```

   If everything is configured correctly, you should be able to get shell access to the remote logging host without being challenged for a password. (When you add the new identity key to the remote host's **authorized_keys** file, the key is used to authenticate the WANJet appliance.)
3. Exit from the SSH session to the WANJet appliance command line.
4. Restart the **syslog-ng** service by typing the following command:

   ```
   $ /etc/init.d/syslog-ng restart
   ```

   The WANJet appliance now sends log messages to your remote host.

14

Working from the Command Line

- Command line overview
- Attaching a computer to the WANJet appliance
- Getting to the command line
- Using commands

Command line overview

You can use the command line to configure the WANJet appliance and perform commands. While it is not typically necessary to use the command line interface, some administrators may prefer to use the Linux shell. In some cases, such as when rebooting or shutting down the WANJet appliance, it is necessary to execute commands at the command line.

You may find that it is easier to perform initial configuration on the WANJet appliance at the command line than it is using the LCD. You can configure the Management IP address, netmask, and gateway for the WANJet appliance using the **config** command. Then you can complete configuration from the browser-based Setup utility and Configuration utility.

In addition, if you do not have physical access to the WANJet appliance, you can use an SSH program to connect to the command line interface. You can perform initial configuration, as described in *Configuring the WANJet appliance from the command line*, on page 14-6. You can also use SSH for troubleshooting the WANJet appliance.

This chapter explains how to access the command line interface and describes some of the most useful commands. For additional information, refer to the following:

- **Online man pages**
  The WANJet product includes online **man** pages for **bigpipe** commands and many standard Linux commands.

- ***BIG-IP® Command Line Interface Guide***
  This reference document includes details on all of the TMOS™-related commands that are available from the command line of the WANJet appliance.

Attaching a computer to the WANJet appliance

You need to attach a computer to the WANJet appliance to access the command line through a serial console. You can then use a terminal emulator program, such as HyperTerminal, to connect to the WANJet appliance's command line interface.

WANJet platforms require a specific console cable to connect the computer. Refer to Appendix E, *Console Cable Replacement*, for more information about the cable.

To connect a computer to a WANJet appliance

1. On a computer or laptop, plug the console cable into the serial port on the computer and tighten the cable screws.
2. Plug the other end of the cable into the port labeled **Console** on the WANJet appliance. The console port is an RJ-45 port on the front of the WANJet 300, 400, and 500.

Getting to the command line

You can access the command line in the following ways:

- Using a terminal emulator on a serial console (local only)
- Using an SSH program (local or remote)

You can use a terminal emulator program to access the command line if working locally using a serial console connected to the WANJet appliance. If you are using a computer running Microsoft® Windows®, you can use HyperTerminal™ or other terminal emulator program. You can also use any SSH program, such as PuTTY, AlphaCom, or SecureCRT® to get to the command line if working locally or remotely.

The following procedure uses HyperTerminal; other terminal emulators require similar setup steps. The procedure *To use PuTTY to get to the command line*, on page 14-3, describes how to use an SSH client to get to the command line.

To use HyperTerminal to get to the command line

1. On the connected computer, from the Start menu, choose All Programs, then Accessories, then Communications, and then click **HyperTerminal**.
   The Connection Description popup screen opens.
2. In the **Name** box, type a name for the connection, then click **OK**.
   The Connect To popup screen opens.

3. From the **Connect using** list, select the port where the WANJet appliance is connected to the computer.
   The Properties screen for the port opens.
4. From the **Bits per second** list, select **9600**.
5. From the **Data bits** list, select **8**.
6. From the **Parity** list, select **None**.
7. From the **Stop bits** list, select **1**.
8. From the **Flow control** list, select **Xon/Xoff**.
9. Click **OK**.
   The connection session opens, and the login prompt appears in the console window.
10. At the **login** prompt, type **root**.
    You can also log on using any account for which **Terminal Access** is **Enabled**. For details, see *Creating local user accounts*, on page 6-7.
11. At the **Password** prompt, type the **root** password.
    You now have access to the Linux shell.

To use PuTTY to get to the command line

1. From any computer on a network that can connect to the WANJet appliance, start **PuTTY**.
   The PuTTY Configuration popup screen opens.
2. In the **Host Name (or IP address)** box, type the Management IP address of the WANJet appliance.
3. For the **Protocol**, select **SSH**.
4. Click **Open**.
5. When connecting to a WANJet appliance for the first time, a message asking you to check the host key appears. To continue, you must click **Yes** to indicate that you trust the host.
   A console window opens.
6. At the **login as** prompt, type **root**.

   Note: *You can also log on using any account for which* ***Terminal Access*** *is* ***Enabled****. For details, see* ***Creating local user accounts****, on page 6-7.*
7. At the **Password** prompt, type the **root** password.
   You now have access to the Linux shell.

To log off the command line

When you are done working at the command line, you can log off by typing **exit**, **logout,** or by closing the session.

Using commands

After you have logged on to the command line through your terminal emulator, SSH client, or console server, you can execute commands on the command line. The WANJet appliance CLI supports standard Linux commands, **bigpipe** commands, and **bigstart** commands.

Type **bigpipe** at the command line to display a list of the **bigpipe** commands. Online **man** pages are also available for the **bigpipe**, **bigstart**, and available Linux commands. Refer also to the ***BIG-IP® Command Line Interface Guide*** for information about the commands that are available.

Table 14.1 lists commands commonly used when administering a WANJet appliance.

Command	Description
b, bp, or bigpipe	Displays the **bigpipe** utility. **b** and **bp** are abbreviations for **bigpipe**. Displays a list of all **bigpipe** commands. For details, see the online man pages or the ***BIG-IP® Command Line Interface Guide***.
b interface stats	Displays interface statistics for the LAN, WAN, MGMT, and Peer interfaces. In the Configuration utility, you can view interface statistics for the LAN, WAN, and Peer interfaces on the Network >> Interfaces >> Statistics screen.
b load	Reloads all of the configuration files if something goes wrong in the Configuration utility and you are not ready to reboot the system. You can reload configuration files only from the command line.
b mgmt	Displays the IP address and netmask for the Management port. In the Configuration utility, you can configure the Management port on the System >> Platform screen.
bigstart status	Displays the status of important system processes including the central manager, generic proxy, and tmm. You can view the status of system processes only from the command line.
config	Configures minimal network settings for the WANJet appliance including setting the Management IP address, netMask, default route (gateway) for the Management port. In the Configuration utility, you can configure the Management port on the System >> Platform screen.

Table 14.1 *Useful WANJet appliance commands*

Command	Description
date	Sets the system date and time. In the Configuration utility, on the System >> Configuration >> NTP screen, you can configure an NTP time server to set the time.
exit	Logs off the WANJet appliance. In the Configuration utility, you can close the browser window to log off.
halt, reboot, poweroff	Shuts down the WANJet appliance. You can only shut down the WANJet appliance from the command line.
help	Lists available bash shell commands and a brief description of each.
ifconfig bridge	Displays the IP address of the WANJet appliance (also called the bridge IP) plus other statistics. In the Configuration utility, you can configure the IP address of the WANJet appliance on the WAN Optimization >> Local WANJet screen.
logout	Logs off the WANJet appliance. In the Configuration utility, you can close the browser window to log off.
ping <IP address>	Tests whether an IP address is reachable across an IP network. In the Configuration utility, on the Remote WANJets screen, you can click the status field of a remote WANJet appliance to ping that appliance.
reboot	Restarts the WANJet appliance. You can reboot the WANJet appliance only from the command line.
shutdown	Securely shuts down the WANJet, sending a message to all users that the system is going down. You can shut down the WANJet appliance only from the command line.
switchboot	Boots from an alternate slot or partition. You can boot only from an alternate slot at the command line.
sys-reset	Restores factory defaults, removing all configuration that you have done on the WANJet appliance. You can restore factory defaults only from the command line.

Table 14.1 *Useful WANJet appliance commands (Continued)*

The following procedures describe how to use several of the commands after having logged on to the WANJet appliance command line.

Configuring the WANJet appliance from the command line

You can perform initial configuration of the Management port on the WANJet appliance from the command line. On platforms that include a liquid crystal display, or LCD, you can configure the addresses there instead. The Quick Start Card included in the shipping box with your WANJet appliance describes the initial hardware installation and setup instructions using the LCD.

To configure the Management port from the command line

1. In the terminal emulator, type **config**.
   The Configuration utility screen opens.
2. Click **OK** to proceed.
   The Configure IP Address screen opens.
3. In the **IP Address** box, type the IP address of the Management port, and click **OK**.
4. In the **Netmask** box, type the netmask for the Management port, and click **OK**.
   The Management Route screen opens, asking whether you want to create a default route for the Management port.
5. Reply to whether you want to create a default route for the Management port:
   - Click **Yes** if you want to create a default route so that you can connect to the WANJet appliance from another subnet.
   - Click **No** if you do not want to create a default route (Management gateway) for the Management port. In this case, you can only log on from a computer located in the same network as the WANJet appliance.
6. If you replied **Yes** in step 5, in the **Management Route** box, type the IP address for the gateway to the management network, and click **OK**. If you replied **No**, skip to step 7.
   The Confirm Configuration screen opens.
7. Click **Yes** to accept the configuration.

   When you complete this step, the command line prompt returns and the new configuration information is applied to the WANJet appliance immediately. Values that you changed on the command line are also changed in the Configuration utility.

Running ping from the command line

You can use the **ping** command to test whether a destination address is reachable across an IP network. For example, if you are having trouble connecting to a second WANJet appliance, you could ping the gateway IP address or the IP address of the other WANJet appliance.

To use ping from the command line

In the terminal emulator, type **ping <destination>**, where **<destination>** is the IP address or host name of the computer you are trying to reach. **Ping** output shows an overview of the command, followed by a list of responses received. It continues to show responses until you stop the command by typing Ctrl + C.

At the end of the command output, you can see **ping** statistics including the number of packets transmitted and received between the WANJet appliance on which you are working and the destination computer, the percentage of packet loss, the total time it took, and the round trip time between the two computers.

For example, the following command checks to see whether or not the computer at the IP address **192.168.72.254** is responsive. The **-c 5** option specifies the count and stops sending requests after five replies are received (or when the deadline is reached). The **-w 10** option indicates a deadline of 10 seconds.

```
ping -c 5 -w 10 192.168.72.254
```

Type **man ping** to see the complete syntax of the command. Refer to documentation on the Linux **ping** command for details on using all of the options.

Shutting down or restarting the WANJet appliance from the command line

You can shut down the WANJet appliance or restart it from the command line. Shutting down WANJet appliance stops all data processing and brings the system down in secure way.

To shut down the WANJet appliance from the command line

1. Log on to the command line as **root**.
2. Type **shutdown**.
   The operating system shuts down.
3. Turn off the WANJet appliance completely by pressing the On/Off button.

To restart the WANJet appliance from the command line

1. Log on to the command line as **root**.
2. Type **reboot**.
   The operating system halts and restarts.

Booting from an alternate image

You typically have two software images on the flash memory card of the WANJet appliance. One image is active and the other is inactive. If something goes wrong with the first installation, you can boot from the alternate image.

Also, having two images lets you install a newer release on one yet maintain the current installation for cases when you want to test an upgrade without losing the previous version. When you perform an upgrade, the WANJet appliance gives you the option of using the configuration settings from the current installation on the upgraded image.

To boot the WANJet appliance from the alternate WANJet appliance image

1. From the command line, log in as **root**.
2. To list the partitions, type **`switchboot -l`**.
3. To switch partitions, type **`switchboot`**.
4. To start the WANJet appliance from the alternate partition, type **reboot**.
   The WANJet appliance reboots and starts up using the other image.

A

Reviewing WANJet Appliance Messages

Displaying WANJet appliance messages

Using the Configuration utility, you can display messages about events that have occurred on the WANJet appliance. You can view WAN optimization messages only, or TMOS-related messages as well as the WAN optimization messages.

To view WAN optimization messages

1. In the navigation pane, expand **WAN Optimization** and click **Diagnostics**.
2. From the General menu, choose Diagnostic Log.
   The Diagnostic log opens.
   Refer to Table A.1, on page A-2, for general descriptions of the messages.

To view TMOS-related messages

1. In the navigation pane, expand **System** and click **Logs**.
   The System log opens.
2. On the menu bar, click **Local Traffic** or **Audit** to view additional logs.
   Refer to Chapter 13, *Logging WANJet Appliance System Events*, for more details.

WAN optimization messages and codes

When events occur on the WANJet appliance, all messages are logged in the **/var/log/ltm** file. Table A.1 lists information about messages, such as errors, warnings, or diagnostic log messages, that relate specifically to WAN optimization.

If your company uses a centralized message server, you can configure the WANJet appliance to send messages to an associated SNMP server or Syslog server. Refer to Chapter 10, *Configuring SNMP*, for more information.

Code	Message and Description	WANJet Appliance Component
1000 to 1002	Error: Configuration error	Optimization Engine
1003 to 1005	Error: Initialization error	Optimization Engine
1006 to 1007	Error: Internal error Description: Internal errors related to TCP compression.	Optimization Engine
1100 to 1103	Error: Internal error	Packet Processor
1150	Maximum number of optimized connections reached	Packet Processor
1151	Connection reset: Source IP:Port <IP address:port #> Destination IP:Port <IP address:port #> Description: The WANJet appliance reset the connection because Connection Intercept is turned on.	Packet Processor
1200 to 1201	Error: Configuration error	Optimization
1202 to 1203	Error: Initialization error	Optimization
1204 to 1207	Error: Internal error	Optimization
1209	Link down with <Proxy IP address> Description: The local WANJet appliance has no communication with the remote WANJet appliance.	Optimization
1210	Link up with <Proxy IP address> Description: The WANJet appliance resumed communication with the remote WANJet appliance.	Optimization
1211	Authentication failed with <Proxy IP address>	Optimization

Table A.1 *WAN optimization messages*

Code	Message and Description	WANJet Appliance Component
1212	Error: Connection from unauthorized proxy <Proxy IP address>	Optimization
1213	Error: Internal error	Optimization
1214	Error: The version <version #> is incompatible with <Proxy IP address> version <version #>	Optimization
1215	Error: License expired on <date>	Optimization
1216	Error connecting to remote client <Proxy IP> from <Initiator_IP> Description: The remote WANJet appliance was unable to connect to a server from the initiator IP address.	Optimization
1217	Error connecting to local client <Proxy IP> error (<error spec>) Description: where <error spec> is a standard socket error. The local WANJet appliance was unable to connect to a server.	Optimization
1218	Error: Diagnostic log test error Description: For internal use only.	Optimization
1219	Connection (<server IP> <-> <client IP>) not optimized: SMB signing required (code 1219) Description: The connection requires SMB signing so it was not optimized.	Optimization
1221	GP Session Up Description: A diagnostic log message that occurs when the generic proxy session starts.	Optimization
1222	GP Session Down Description: A diagnostic log message that occurs when the generic proxy session fails.	Optimization
1250	Version (<version #>) up and running	Optimization
1251	Error: Internal error	Optimization
1252	Warning: License Limit Exceeded	Optimization
1253	Warning: Invalid license key - Bandwidth optimization off	Optimization

Table A.1 *WAN optimization messages (Continued)*

Code	Message and Description	WANJet Appliance Component
1254	Warning: License key not entered - Bandwidth optimization off or Warning: License expired - Bandwidth optimization off or Warning: License invalid <reason> - Bandwidth optimization off	Optimization
1255	Warning: <#> days remain for evaluation license to expire	Optimization
1256	Warning: WANJet is activated for evaluation for <#> days	Optimization
1257	Warning: Evaluation license key expired	Optimization
1258	License violation: Bandwidth optimization stopped	Optimization
1259	Cannot complete the remote upgrade. Not enough free space.	Optimization
NA	<SSL> certs invalid (error : <error>) - backing up to /tmp/certs_bak and recreating Description: The SSL Certificates are invalid.	Optimization
NA	<NOProxy> has waited too long for GPStart Description: A problem occurred while starting the optimization service; the WANJet appliance was unable to become active.	Optimization
1260	Error: Upgrade failed. Please contact F5 technical support team.	WANJet Management
1300	Error: Logging error Description: The logging facility could not get error messages from the WANJet appliance.	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

Table A.1 *WAN optimization messages (Continued)*

Code	Message and Description	WANJet Appliance Component
1424	WCCP Configuration Error	WCCP
1425	WCCP Runtime Error	WCCP
1426	WCCP is not enabled on the router	WCCP

Table A.1 *WAN optimization messages (Continued)*

B

Configuration Examples

- Basic point-to-point configuration
- Mesh configuration
- Hub and spoke configuration
- Redundant system configuration
- LAN router configuration

Basic point-to-point configuration

Figure B.1 shows an example of a basic point-to-point configuration of WANJet appliances.

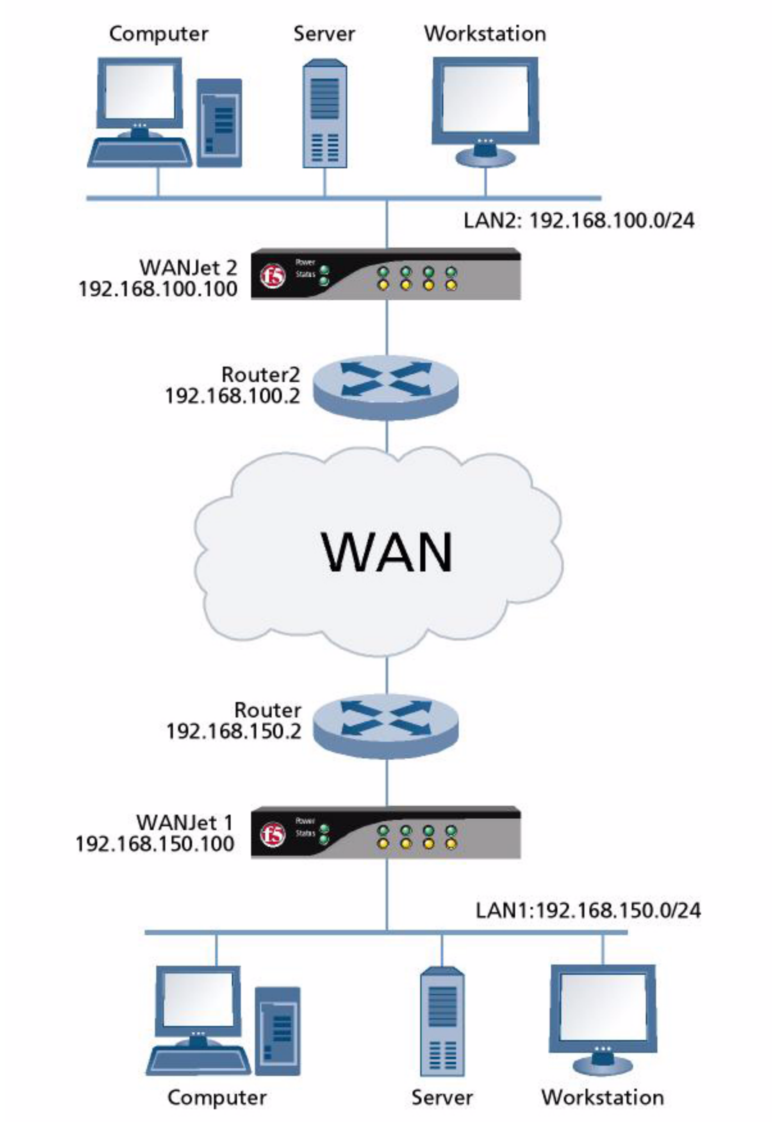


Figure B.1 *Basic WANJet appliance configuration*

In this example:

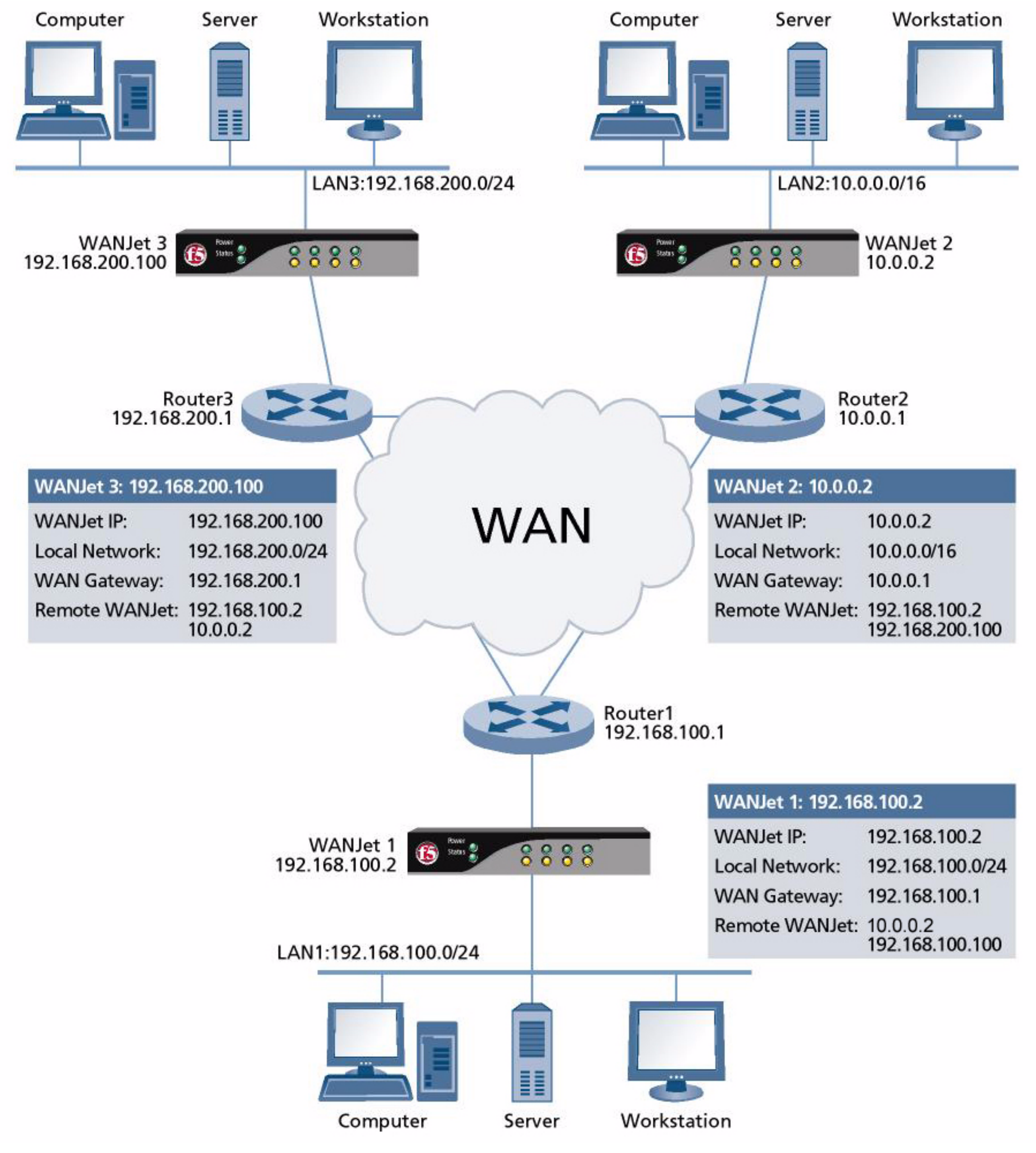
- This configuration includes two WANJet appliances.
- The network includes two LANs (LAN1 and LAN2) that are connected.
- LAN2 is a remote network of LAN1, and LAN1 is the remote network of LAN2.
- LAN1 includes WANJet1, and LAN2 includes WANJet2.
- Configure WANJet2 as a remote WANJet appliance on WANJet1, and configure WANJet1 as a remote WANJet appliance on WANJet2.
- WANJet1 sends optimized data to WANJet2, while WANJet2 sends optimized data to WANJet1.

	WANJet1	**WANJet2**
IP Address	192.168.150.100	192.168.100.100
Local Network	192.168.150.0/24	192.168.100.0/24
WAN Gateway	192.168.150.2	192.168.100.2
Remote WANJet appliance	192.168.100.100	192.168.150.100

Table B.1 *Basic configuration specifications*

Mesh configuration

Figure B.2 shows an example of a mesh configuration including three WANJet appliances.



WANJet 3: 192.168.200.100	
WANJet IP:	192.168.200.100
Local Network:	192.168.200.0/24
WAN Gateway:	192.168.200.1
Remote WANJet:	192.168.100.2 10.0.0.2

WANJet 2: 10.0.0.2	
WANJet IP:	10.0.0.2
Local Network:	10.0.0.0/16
WAN Gateway:	10.0.0.1
Remote WANJet:	192.168.100.2 192.168.200.100

WANJet 1: 192.168.100.2	
WANJet IP:	192.168.100.2
Local Network:	192.168.100.0/24
WAN Gateway:	192.168.100.1
Remote WANJet:	10.0.0.2 192.168.100.100

__Figure B.2__ Mesh configuration

In this example:

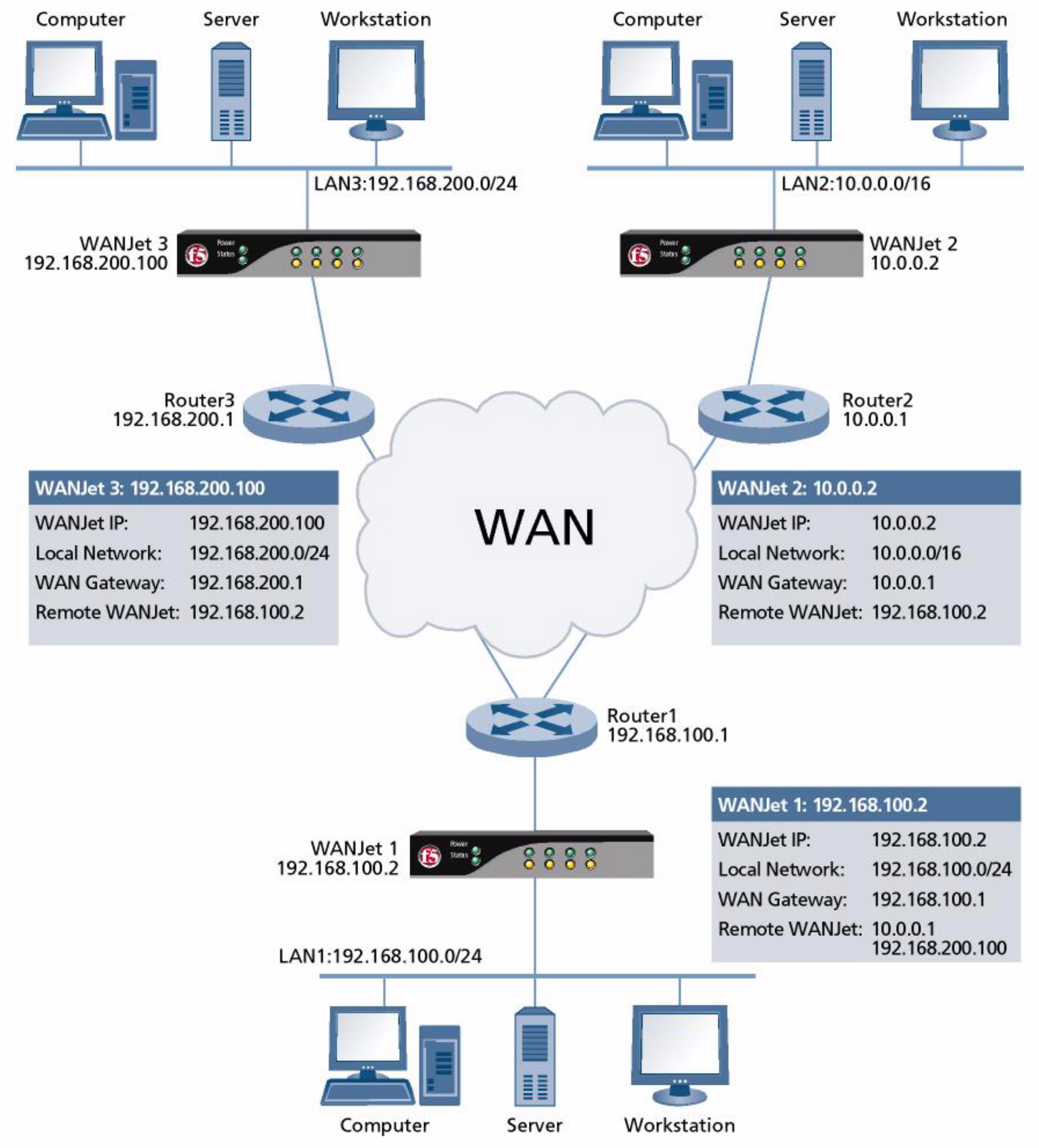
- This configuration includes three WANJet appliances.
- The network includes three LANs (LAN1, LAN2, and LAN3) that are connected.
- LAN1 includes WANJet1, LAN2 includes WANJet2, and LAN3 includes WANJet3.
- Configure WANJet2 and WANJet3 as remote WANJet appliances on WANJet1; configure WANJet1 and WANJet3 as remote WANJet appliances on WANJet2; and configure WANJet1 and WANJet2 as remote WANJet appliances on WANJet3.
- WANJet1 sends optimized data to WANJet2 and WANJet3; WANJet2 sends optimized data to WANJet1 and WANJet3; and WANJet3 sends optimized data to WANJet1 and WANJet2.

	WANJet1	**WANJet2**	**WANJet3**
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
WAN Gateway	192.168.100.1	10.0.0.1	192.168.200.1
Remote WANJet appliance 1	10.0.0.2	192.168.200.100	192.168.100.2
Remote WANJet appliance 2	192.168.200.100	192.168.100.2	10.0.0.2

Table B.2 *Example mesh configuration specifications*

Hub and spoke configuration

Figure B.3 shows an example of a hub and spoke configuration.



WANJet 3: 192.168.200.100	
WANJet IP:	192.168.200.100
Local Network:	192.168.200.0/24
WAN Gateway:	192.168.200.1
Remote WANJet:	192.168.100.2

WANJet 2: 10.0.0.2	
WANJet IP:	10.0.0.2
Local Network:	10.0.0.0/16
WAN Gateway:	10.0.0.1
Remote WANJet:	192.168.100.2

WANJet 1: 192.168.100.2	
WANJet IP:	192.168.100.2
Local Network:	192.168.100.0/24
WAN Gateway:	192.168.100.1
Remote WANJet:	10.0.0.1 192.168.200.100

Figure B.3 *Hub and spoke configuration*

In this example:

- This configuration includes three WANJet appliances.
- The network includes three LANs (LAN1, LAN2, and LAN3) that are connected.
- LAN1 connects to LAN2 and LAN3, and LAN2 and LAN3 connect to LAN1, but LAN2 and LAN3 do not connect to each other.
- Configure WANJet2 and WANJet3 as remote WANJet appliances on WANJet1; configure WANJet1 as a remote WANJet appliance on both WANJet2 and WANJet3.
- LAN1 includes WANJet1, LAN2 includes WANJet2, and LAN3 includes WANJet3.
- WANJet1 sends optimized data to both WANJet2 and WANJet3, WANJet2 sends optimized data to WANJet1 only, and WANJet3 sends optimized data to WANJet1 only.

	WANJet1	**WANJet2**	**WANJet3**
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
WAN Gateway	192.168.100.1	10.0.0.1	192.168.200.1
Remote WANJet appliance 1	10.0.0.2	192.168.100.2	192.168.100.2
Remote WANJet appliance 2	192.168.200.100		

Table B.3 *Example hub and spoke configuration specifications*

Redundant system configuration

Figure B.4 shows an example of a redundant system configuration.

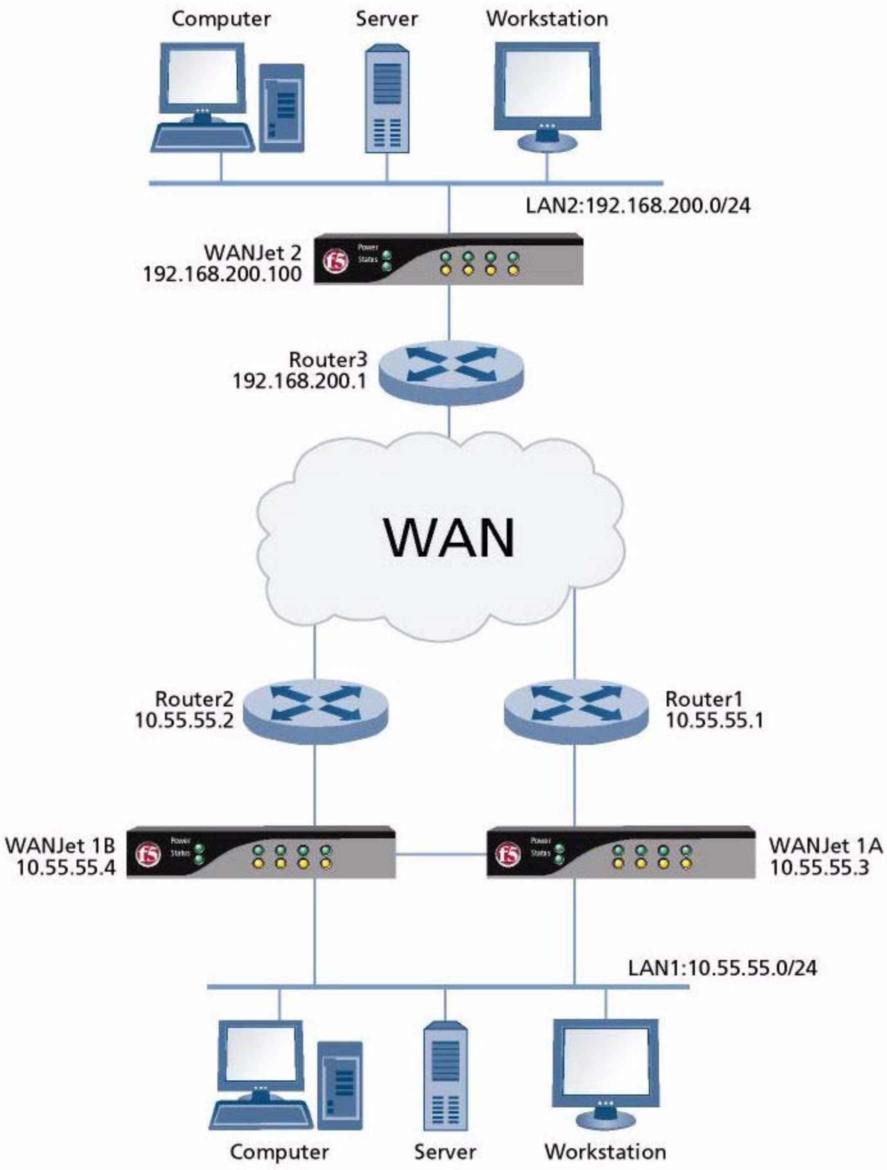


Figure B.4 *Redundant system configuration*

In this example:

- Two LANs are connected, and one of the LANs has WANJet appliances installed in a redundant system configuration.
- LAN1 includes two WANJet appliances, WANJet1A and WANJet1B, and LAN2 includes WANJet2. WANJet1B is the redundant peer of WANJet1A. In case of router or WANJet appliance failure, the other router and its corresponding WANJet appliance resume function.
- WANJet1B processes the half of the data in LAN1, and WANJet1B processes the other half of the data in LAN1 (load balancing).
- WANJet1A sends optimized data to WANJet2, and WANJet1B sends optimized data to WANJet2.

	WANJet1A	**WANJet1B**	**WANJet2**
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 WANJet appliance	192.168.200.100	192.168.200.100	10.55.55.3
Subnet			10.55.55.0/24
Remote WANJet appliance	192.168.200.100	192.168.200.100	10.55.55.4

Table B.4 *Example redundant configuration specifications*

LAN router configuration

Figure B.5 shows an example of a LAN router configuration.

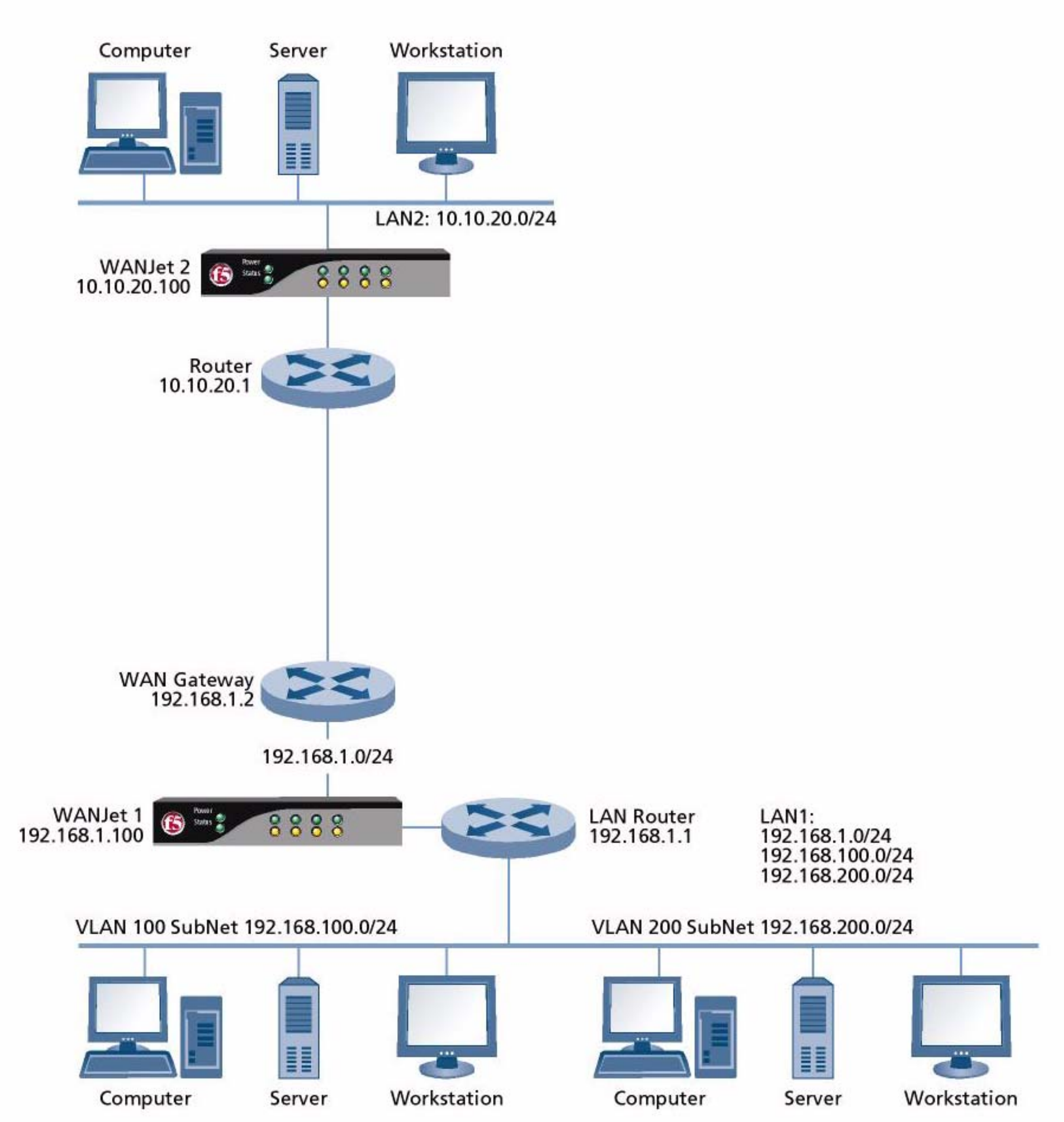


Figure B.5 *LAN router configuration*

In this example:

- A LAN router connects two networks to a WANJet appliance, and the WANJet appliance connects to the outside WAN through another router (WAN gateway).
- LAN1 includes WANJet1, and LAN2 includes WANJet2.
- LAN1 comprises three networks VLAN 100, VLAN 200, and WANJet1's network (**192.168.1.0/24**). The LAN router connects all three networks. You configure the LAN router on WANJet1.
- You configure VLAN 100 and VLAN 200 as local subnets on WANJet1.
- LAN1 and WANJet1 connect to the WAN through the WAN gateway.

	WANJet1	**WANJet2**
IP Address	192.168.1.100	10.10.20.100
Local Network	192.168.1.0/24	10.10.20.0/24
Local Subnets	VLAN 100: 192.168.100.0/24 VLAN 200: 192.168.200.0/24	10.10.20.0/24
LAN Router	192.168.1.1	
WAN Gateway	192.168.1.2	10.10.20.1

Table B.5 *LAN router configuration specifications*

C

WANJet Appliance Private MIB File

- Introducing MIB files
- Ethernet card information

Introducing MIB files

You can use WANJet Private Management Information Base (MIB) file if you need to compile the MIB file to browse the MIB using a standard MIB browser. You can download the MIB file from the WANJet appliance, and use it with your SNMP management software. For additional information about SNMP MIB files and configuring SNMP, refer to Chapter 10, *Configuring SNMP*.

To download the private MIB file for the WANJet appliance

1. In the navigation pane, expand **Overview**, and **c**lick **Welcome**.
   The Welcome screen opens.
2. Scroll to the Downloads section, and locate the **SNMP MIBs** section.
3. Click **Download WANJet Private MIB (WANJet-MIB.txt)**.
   The file contents displays on the screen.
4. Type Ctrl + A to select the text, then paste it into any text editor and save the file.
5. Copy the MIB file into your SNMP management software and compile it.

Refer to the documentation of your SNMP management software for additional instructions.

WANJet appliance MIB file

Following is the WANJet Private Management Information Base (MIB) file.

```
F5NETWORKS-GLOBAL-REG DEFINITIONS ::= BEGIN

IMPORTS

enterprises FROM SNMPv2-SMI;

F5 OBJECT IDENTIFIER

::= { enterprises 3375 }

WANJet OBJECT IDENTIFIER

::= { F5 11 }

Statistics OBJECT IDENTIFIER

::= { WANJet 2 }

SnmpTraps OBJECT IDENTIFIER

::= { WANJet 3 }

-- ********************************************** Statistics

TotalSentBandwidthSavingPercent OBJECT-TYPE

SYNTAX INTEGER

ACCESS read-only

STATUS current
```

```
DESCRIPTION "Percentage of bandwidth saved on the traffic sent
to other WANJet appliances today."
::= { Statistics 1 }
TotalRecvBandwidthSavingPercent OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS current
DESCRIPTION "Percentage of bandwidth saved on the traffic
received from other WANJet appliances today."
::= { Statistics 2 }
TotalSentBeforeWANJet OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS current
DESCRIPTION "Effective traffic sent from this WANJet appliance
to other WANJet appliances
today in MB (before WANJet)."
::= { Statistics 3 }
TotalSentAfterWANJet OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS current
DESCRIPTION "Optimized traffic sent from this WANJet appliance
to other WANJet appliances
today in MB (after WANJet)."
::= { Statistics 4 }
TotalRecvBeforeWANJet OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS current
DESCRIPTION "Effective traffic received
from other WANJet appliances
today in MB (before WANJet)."
::= { Statistics 5 }
TotalRecvAfterWANJet OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS current
DESCRIPTION "Optimized traffic received
from other WANJet appliances
today in MB (after WANJet)."
::= { Statistics 6 }
```

```
LastSentBandwidthSavingPercent OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS current
DESCRIPTION "Percentage of bandwidth saved on the traffic sent
to other WANJet appliances during the last five minutes.
This value may be plotted to create a chart."
::= { Statistics 7 }
LastRecvBandwidthSavingPercent OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS current
DESCRIPTION "Percentage of bandwidth saved on the traffic
received from other WANJet appliances during the last five
minutes.
This value may be plotted to create a chart."
::= { Statistics 8 }
LastSentBeforeWANJetRate OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS current
DESCRIPTION "The rate of effective traffic sent from this WANJet
appliance to other WANJet appliances in Kbps (before WANJet).
This value may be plotted to create a chart."
::= { Statistics 9 }
LastSentAfterWANJetRate OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS current
DESCRIPTION "The rate of optimized traffic sent from this WANJet
appliance to other WANJet appliances in Kbps (after WANJet).
This value may be plotted to create a chart."
::= { Statistics 10 }
LastRecvBeforeWANJetRate OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS current
DESCRIPTION "The rate of effective traffic received
from other WANJet appliances in Kbps
(before WANJet).
This value may be plotted to create a chart."
::= { Statistics 11 }
```

```
LastRecvAfterWANJetRate OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS current
DESCRIPTION "The rate of optimized traffic received
from other WANJet appliances in Kbps
(after WANJet).
This value may be plotted to create a chart."
::= { Statistics 12 }
-- ********************************************** SnmpTraps
SnmpTrapObjs OBJECT IDENTIFIER
::= { SnmpTraps 1 }
SnmpTrapID OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS current
DESCRIPTION "Holds the ID of the SNMP Trap."
::= { SnmpTrapObjs 1 }
SnmpTrapDescription OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Holds the description of the SNMP Trap."
::= { SnmpTrapObjs 2 }
SnmpTrapList OBJECT IDENTIFIER
::= { SnmpTraps 2 }

-- Optimization Engine Traps
Trap1000 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Configuration error."
::= { SnmpTrapList 1000 }
Trap1001 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Configuration error."
::= { SnmpTrapList 1001 }
```

```
Trap1002 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Configuration error."
::= { SnmpTrapList 1002 }
Trap1003 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Initialization error."
::= { SnmpTrapList 1003 }
Trap1004 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Initialization error."
::= { SnmpTrapList 1004 }
Trap1005 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Initialization error."
::= { SnmpTrapList 1005 }
Trap1006 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Internal error."
::= { SnmpTrapList 1006 }
Trap1007 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Internal error."
::= { SnmpTrapList 1007 }
-- Packet Processor Traps
Trap1100 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Internal error."
::= { SnmpTrapList 1100 }
```

```
Trap1101 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Internal error."
::= { SnmpTrapList 1101 }
Trap1102 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Internal error."
::= { SnmpTrapList 1102 }
Trap1103 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Internal error."
::= { SnmpTrapList 1103 }
Trap1150 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Maximum number of optimized connections reached."
::= { SnmpTrapList 1150 }
-- ACM5 Traps
Trap1200 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Configuration error."
::= { SnmpTrapList 1200 }
Trap1201 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Configuration error."
::= { SnmpTrapList 1201 }
Trap1202 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Initialization error."
::= { SnmpTrapList 1202 }
```

```
Trap1203 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Initialization error."
::= { SnmpTrapList 1203 }
Trap1204 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Internal error."
::= { SnmpTrapList 1204 }
Trap1205 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Internal error."
::= { SnmpTrapList 1205 }
Trap1206 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Internal error."
::= { SnmpTrapList 1206 }
Trap1207 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Internal error."
::= { SnmpTrapList 1207 }
Trap1209 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Link down with (Proxy IP)."
::= { SnmpTrapList 1209 }
Trap1210 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Link up with (Proxy IP)."
::= { SnmpTrapList 1210 }
```

```
Trap1211 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Authentication failed with (Proxy IP)."
::= { SnmpTrapList 1211 }
Trap1212 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Connection from unauthorized Proxy (Proxy
IP)."
::= { SnmpTrapList 1212 }
Trap1213 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Internal error."
::= { SnmpTrapList 1213 }
Trap1214 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: This version (%f) is incompatible with
(Proxy IP) version
(%f)."
::= { SnmpTrapList 1214 }
Trap1215 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: License expired on (%f)."
::= { SnmpTrapList 1215 }
Trap1216 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Connecting to remote client (%f)."
::= { SnmpTrapList 1216 }
Trap1217 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Connecting to local client (%f) error (%f)."
::= { SnmpTrapList 1217 }
```

```
Trap1250 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Version (%f) up and running."
::= { SnmpTrapList 1250 }
Trap1251 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Internal error."
::= { SnmpTrapList 1251 }
Trap1252 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Warning: License limit exceeded."
::= { SnmpTrapList 1252 }
Trap1253 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Warning: Invalid license key - Bandwidth
optimization off."
::= { SnmpTrapList 1253 }
Trap1254 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Warning: License key not entered - Bandwidth
optimization off."
::= { SnmpTrapList 1254 }
Trap1255 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Warning: Evaluation license key expires in x days."
::= { SnmpTrapList 1255 }
Trap1256 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Warning: WANJet evaluation license is activated for
x days."
::= { SnmpTrapList 1256 }
```

```
Trap1257 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Warning: Evaluation license key expired."
::= { SnmpTrapList 1257 }
Trap1258 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: License violation - Bandwidth optimization
stopped."
::= { SnmpTrapList 1258 }
Trap1259 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Cannot complete the remote upgrade. Not
enough free space."
::= { SnmpTrapList 1259 }
Trap1260 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Upgrade failed. Please contact F5 technical
support team."
::= { SnmpTrapList 1260 }
-- Logging Traps
Trap1300 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "Error: Logging error."
::= { SnmpTrapList 1300 }
-- WCCP Traps
Trap1420 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "WCCP ServiceGroup TCP is up."
::= { SnmpTrapList 1420 }
```

```
Trap1421 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "WCCP ServiceGroup UDP is up."
::= { SnmpTrapList 1421 }
Trap1422 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "WCCP ServiceGroup TCP is down."
::= { SnmpTrapList 1422 }
Trap1423 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "WCCP ServiceGroup UDP is down."
::= { SnmpTrapList 1423 }
Trap1424 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "WCCP Configuration Error."
::= { SnmpTrapList 1424 }
Trap1425 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "WCCP Runtime Error."
::= { SnmpTrapList 1425 }
Trap1426 OBJECT-TYPE
SYNTAX OCTET STRING
ACCESS read-only
STATUS current
DESCRIPTION "WCCP is not enabled on the router."
::= { SnmpTrapList 1426 }
END
```

Ethernet card information

The WANJet appliance provides Ethernet card information by means of the standard SNMP.

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
```

D

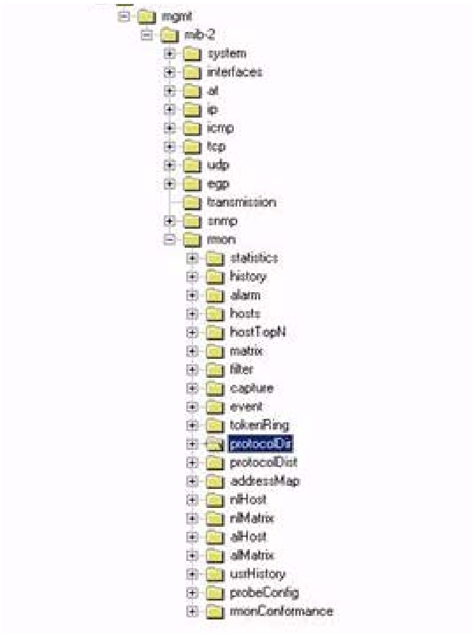
RMON Tree

- RMON tree overview
- MIB tree
- Protocol directory tree
- Network layer matrix
- Application data matrix

RMON tree overview

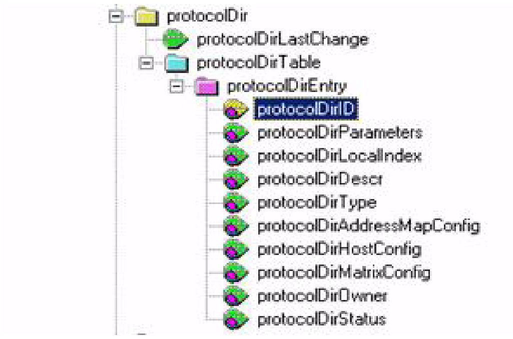
This appendix shows the standard RMON MIB tree and all the groups for RMON1 and RMON2. You can use it to locate the RMON groups that the WANJet appliance supports.

MIB tree



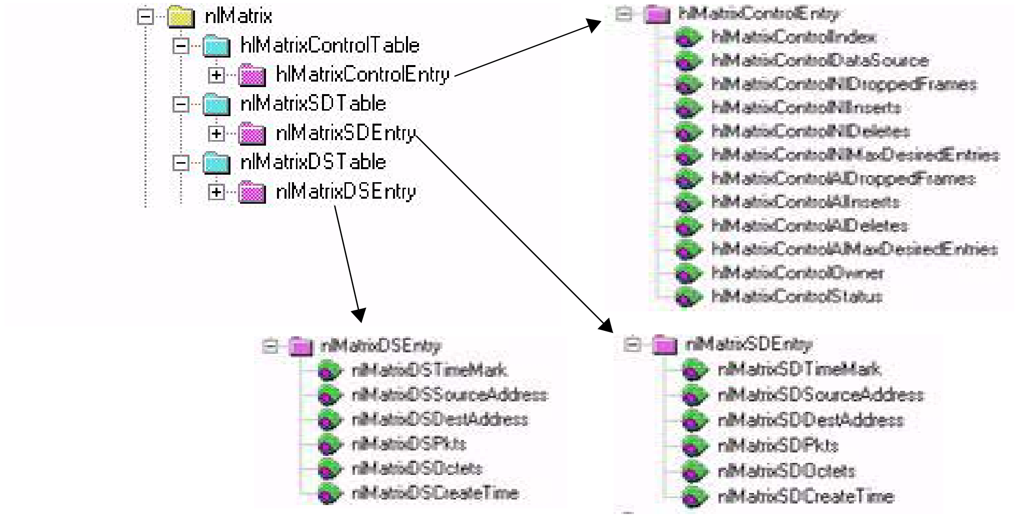
```
mgmt
  mib-2
    system
    interfaces
    at
    ip
    icmp
    tcp
    udp
    egp
    transmission
    snmp
    rmon
      statistics
      history
      alarm
      hosts
      hostTopN
      matrix
      filter
      capture
      event
      tokenRing
      protocolDir
      protocolDist
      addressMap
      nlHost
      nlMatrix
      alHost
      alMatrix
      usrHistory
      probeConfig
      rmonConformance
```

Protocol directory tree



```
protocolDir
  protocolDirLastChange
  protocolDirTable
    protocolDirEntry
      protocolDirID
      protocolDirParameters
      protocolDirLocalIndex
      protocolDirDescr
      protocolDirType
      protocolDirAddressMapConfig
      protocolDirHostConfig
      protocolDirMatrixConfig
      protocolDirOwner
      protocolDirStatus
```

Network layer matrix



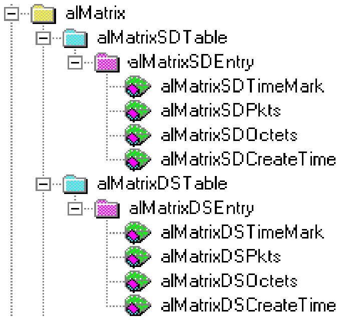
- nlMatrix
  - hlMatrixControlTable
    - hlMatrixControlEntry
  - nlMatrixSDTable
    - nlMatrixSDEntry
  - nlMatrixDSTable
    - nlMatrixDSEntry

- hlMatrixControlEntry
  - hlMatrixControlIndex
  - hlMatrixControlDataSource
  - hlMatrixControlNlDroppedFrames
  - hlMatrixControlNlInserts
  - hlMatrixControlNlDeletes
  - hlMatrixControlNlMaxDesiredEntries
  - hlMatrixControlAlDroppedFrames
  - hlMatrixControlAlInserts
  - hlMatrixControlAlDeletes
  - hlMatrixControlAlMaxDesiredEntries
  - hlMatrixControlOwner
  - hlMatrixControlStatus

- nlMatrixDSEntry
  - nlMatrixDSTimeMark
  - nlMatrixDSSourceAddress
  - nlMatrixDSDestAddress
  - nlMatrixDSPkts
  - nlMatrixDSOctets
  - nlMatrixDSCreateTime

- nlMatrixSDEntry
  - nlMatrixSDTimeMark
  - nlMatrixSDSourceAddress
  - nlMatrixSDDestAddress
  - nlMatrixSDPkts
  - nlMatrixSDOctets
  - nlMatrixSDCreateTime

Application data matrix



- alMatrix
  - alMatrixSDTable
    - alMatrixSDEntry
      - alMatrixSDTimeMark
      - alMatrixSDPkts
      - alMatrixSDOctets
      - alMatrixSDCreateTime
  - alMatrixDSTable
    - alMatrixDSEntry
      - alMatrixDSTimeMark
      - alMatrixDSPkts
      - alMatrixDSOctets
      - alMatrixDSCreateTime

E

Console Cable Replacement

- Replacing the console cable

Replacing the console cable

The WANJet appliance includes a console cable for attaching a console to the appliance. If this cable is lost, or becomes damaged, you may need to create a new cable. This section describes the included cable, which you can use as a model to create or purchase a new cable.

Figure E.1 illustrates the DB9 to RJ-45 cable connector provided on the WANJet 300, 400, and 500 platforms.

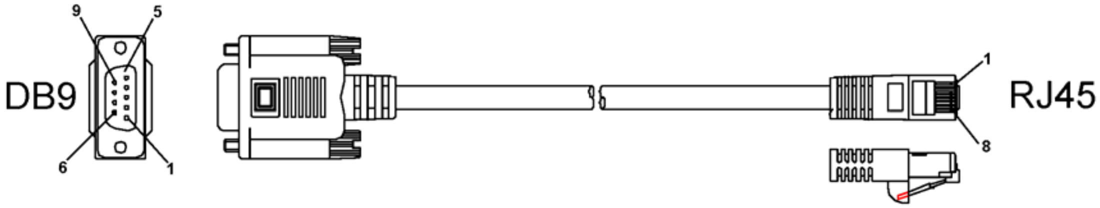


Figure E.1 *DB9 to RJ-45 cable diagram (WANJet 300, 400, and 500)*

The numbers indicated in Figure E.1 correspond to the mappings specified in Table E.1.

DB9 pin	Name	RJ45 pin
1	Carrier Detect (CD)	NC
2	Receive Data (RXD)	3
3	Transmit Data (TXD)	6
4	Data Terminal Ready (DTR)	7
5	GND	5
6	Data Set Ready (DSR)	4
7	Request to Send (RTS)	8
8	Clear to Send (CTS)	2
9	Ring Indicator (RI)	NC

Table E.1 *Pinouts for DB9 to RJ-45 cable (WANJet 300, 400, and 500)*

Glossary

Application QoS

Application QoS is a per-endpoint setting that you can use to configure policies that adjust the bandwidth consumed by specific types of network traffic (also referred to as ***traffic shaping***). See also *Quality of Service (QoS) level*.

archive

An archive is a backup copy of the WANJet appliance system configuration data. This archive is in the form of a user configuration set, or UCS. See also *user configuration set (UCS)*.

authentication

Authentication is the process of verifying a user's identity when the user is attempting to log on to a system.

authorization

Authorization is the process of identifying the level of access that a logged-on user has been granted to system resources.

bandwidth

Bandwidth specifies the amount of data that can be transferred over a network connection in a fixed amount of time. Bandwidth is usually stated in bits per second (bps), kilobits per second (Kbps), or megabits per second (Mbps).

bridge IP

The bridge IP is the IP address of the local WANJet appliance.

certificate

A certificate is an online credential signed by a trusted certificate authority and used for SSL network traffic as a method of authentication.

certificate authority (CA)

A certificate authority is an external, trusted organization that issues a signed digital certificate to a requesting computer system for use as a credential to obtain authentication for SSL network traffic.

Configuration utility

The Configuration utility is the browser-based application that you use to configure the WANJet appliance.

Connection Interception (CI)

Connection Interception (CI) intercepts and resets connections that were initiated before the WANJet appliance became active on the network.

dashboard

The dashboard is the area at the top of the navigation pane in the Configuration utility. It displays status indicators and is always visible in the Configuration utility.

data route

A data route (also called TMM switch route) is a route that the WANJet appliance uses to forward traffic through the LAN and WAN interfaces.

data routing table

The data routing table contains IP routing information about data routes. It is the main TMM routing table. See also *TMM (Traffic Management Microkernel) service*.

default route

A default route is the route that the system uses when no other route specified in the routing table matches the destination address or network of the packet to be routed.

domain name

A domain name is a unique name that is associated with one or more IP addresses. Domain names are used in URLs to identify particular Web pages. For example, in the URL **http://www.siterequest.com/index.html**, the domain name is **siterequest.com**.

Domain Name System (DNS)

Domain Name System (DNS) is an industry-standard distributed internet directory service that resolves domain names to IP addresses.

full duplex mode

Full duplex mode means that traffic on that interface can travel in both directions simultaneously.

GenericProxy service

The GenericProxy service optimizes traffic between paired WANJet appliance.

half duplex mode

Half duplex mode means that traffic on that interface can travel in only one direction at any given time.

inline

Inline is a method of deployment that places the WANJet appliances directly in the path of traffic between a WAN router and a LAN switch. See also *point-to-point configuration*, *point-to-multipoint configuration*, and *one-arm configuration*.

interface

A physical port on a WANJet appliance is called an interface.

Layer 1 through Layer 7

Layers 1 through 7 refer to the seven layers of the Open System Interconnection (OSI) model. Thus, Layer 1 represents the physical layer, Layer 2 represents the data-link layer, Layer 3 represents the IP layer, and Layer 4 represents the transport layer (TCP and UDP). Layer 5 manages connections between applications, and Layer 6 represents the presentation layer. Layer 7 represents the application layer, handling traffic such as HTTP and SSL.

LCD

LCD stands for liquid crystal display. An LCD panel is available on the front of WANJet 300, 400, and 500 platforms. You can use the LCD and its associated keypad to configure the LAN, WAN, and Management ports on the unit and perform basic administration tasks.

LED indicators

The LED indicators on the front of the WANJet appliance are lights that show the status of the system.

Management Information Base (MIB)

A Management Information Base (MIB) is the database that SNMP creates to store the information it collects. The WANJet appliance includes three types of MIB files: standard MIB files, enterprise MIB files pertaining to F5 Networks; and the private MIB file, which contains data objects for WAN optimization and other features of the WANJet appliance.

Management port

The Management port on the WANJet appliance can connect to the management network, if your organization is using out-of-band management.

management route

A management route is a route that forwards traffic through the management (**MGMT**) interface.

management routing table

The management routing table contains information about the routes that the WANJet appliance uses to forward traffic through the Management port.

Master Control Program Daemon (MCPD)

The Master Control Program Daemon (MCPD) manages the configuration data on a WANJet appliance.

navigation pane

The navigation pane is the area on the Main tab on the left of the screen in the WANJet appliance Configuration utility. It includes the following four sections that you can expand to view the various Configuration utility screens: Overview, WAN Optimization, Network, and System.

Network Time Protocol (NTP)

Network Time Protocol (NTP) is a protocol that synchronizes the clocks on a network.

NIC

A network interface card (NIC) is an expansion board used to connect a computer to a network.

one-arm configuration

A one-arm configuration is an alternative to inline deployment in which the WANJet appliance has a single connection to the WAN router or LAN switch, which redirects relevant traffic to the appliance. See also *point-to-point configuration* and *point-to-multipoint configuration.*

OSI model

See *Layer 1 through Layer 7*.

out-of-band management

Out-of-band management is the use of a dedicated management channel (separate from the data channel) for administration only. See also *Management port*.

passthrough destination

A passthrough destination is the IP address of a host or subnet for which you configure the WANJet appliance to not optimize the traffic destined for specified ports.

passthrough session

A passthrough session is a network connection (at the application layer) for traffic that the WANJet appliance does not optimize. Instead, the WANJet appliance allows that particular type of traffic to pass through the appliance untouched.

Peer port

The Peer port on the WANJet appliance is an Ethernet port that can connect using a crossover cable to a second WANJet appliance to form a redundant pair. See also *redundant peer*.

point-to-multipoint configuration

Point-to-multipoint configuration is a complex topology that involves three or more WANJet appliances. It can provide connections across intranets and the Internet. See also *point-to-point configuration* and *one-arm configuration*.

point-to-point configuration

Point-to-point configuration is a simple one-to-one topology where you place WANJet appliances at each end of the WAN between their respective WAN routers and LAN switches. See also *point-to-multipoint configuration* and *one-arm configuration*.

Quality of Service (QoS) level

The Quality of Service (QoS) level is a means by which network equipment can identify and treat traffic differently based on an identifier. Essentially, the QoS level specified in a packet enforces a throughput policy for that packet. See also *Application QoS*.

redundant peer

A redundant peer is a WANJet appliance that is connected to another WANJet appliance in the same subnet and provides an alternate path for network traffic. See also *Peer port*.

Remote Monitoring (RMON)

Remote Monitoring (RMON) is an extension to SNMP that provides comprehensive network monitoring capabilities.

RMON1

RMON1 is the MIB that allows network administrators to see traffic and collect information about remote network segments for troubleshooting and performance monitoring. RMON1 focuses on Layer 1 and Layer 2 of the OSI model.

RMON2

RMON2 is an extension of RMON1 that includes open, comprehensive network fault diagnosis, planning, and performance-tuning features. RMON2 focuses on Layer 3 to Layer 6 of the OSI model.

router

A router is a Layer 3 networking device. If no VLANs are defined on the network, a router defines a broadcast domain.

Setup utility

The Setup utility walks you through the initial system configuration process. You can run the Setup utility from the Configuration utility start page.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is an industry-standard protocol for managing and monitoring network devices. The SNMP agent run on a management system and makes requests to a device. The SNMP agent runs on the managed device and fulfills those requests.

SNMP trap

An SNMP trap provides notification of a significant event that occurred on the network, for example, a power outage, an error, a fault, or a security violation.

SSH

SSH is a protocol for secure remote login and other secure network services over a non-secure network.

SSL (Secure Sockets Layer)

SSL is a network communications protocol that uses public-key technology as a way to transmit data in a secure manner.

system snapshot

The system snapshot is a file that contains current detailed information about the WANJet appliance.

TCP optimization

TCP optimization is a set of techniques that the WANJet appliance employs to accelerate application traffic.

TDR-1

TDR-1 is the second step in the Transparent Data Reduction compression process, which further compresses the data through the use of dictionary-based compression and advanced encoding schemes. See also *Transparent Data Reduction (TDR)* and *TDR-2*.

TDR-2

TDR-2 is the first step in the Transparent Data Reduction compression process, which replaces previously transmitted data with references. See also *Transparent Data Reduction (TDR)* and *TDR-1*.

TMM (Traffic Management Microkernel) service

The TMM service is the process running on the WANJet appliance that performs most traffic management for the product and controls the TMM switch interfaces. See also *data route* and *data routing table*.

TMOS (Traffic Management Operation System)

The Traffic Management Operating System™ (TMOS) is the internal mechanism within the WANJet appliance that is responsible for all traffic-management functions.

traffic class

A traffic class is a named group of ports, systems. and subnets that you create so that you can apply a single Application QoS policy to multiple services.

Transparent Data Reduction (TDR)

Transparent Data Reduction™ (TDR) technology provides a dramatic reduction in the amount of bandwidth consumed by repeated data transfers across a WAN link.

user configuration set (UCS)

A user configuration set is a backup file that you create for the WANJet appliance configuration data. When you create a UCS, the WANJet appliance assigns a **.ucs** extension to the file name. See also *archive.*

user role

A user role is a type and level of access that you assign to a WANJet appliance user account. By assigning user roles, you can control the extent to which WANJet appliance administrators can view or modify the WANJet appliance configuration.

VLAN (Virtual LAN)

VLAN stands for virtual local area network. A VLAN is a logical grouping of network devices. VLANs provide a way to structure a large network for increased security, separating systems with sensitive data, for special projects, or into separate departments.

WAN (wide area network)

A WAN is a computer network that spans a large geographic area, and typically consists of two or more local area networks (LANs). A WAN may also include public or shared user networks. The most well-known example of a WAN is the Internet.

Index