WideBand® CORPORATION

nMU

WideBand Network Management Unit

User Manual
Table of Contents

Introduction

The WideBand Network Management Unit (nMU) is a hardware module that can manage all of the WideBand switches on a network. Such management includes advanced VLAN configuration, watchmen monitoring, and automatic firmware updates. The purpose of the nMU is to improve the management experience of the network manager.

With automatic daily updates, new features are being added continually. WideBand Corporation encourages customers to submit any suggestions and report any 'bugs' they may find. This makes the WideBand nMU a constantly growing and improving product.

Connecting to the nMU

Before the WideBand nMU can be used, it must be configured with a password and correct IP settings. This is done by connecting a keyboard and monitor to the front panel and following the instructions on the screen. Once startup configuration is complete, the management interface can be accessed through a standard browser. By default, DHCP is enabled on the nMU, so it will learn a dynamic IP address if a DHCP server is present on the network. The management interface can be accessed from any standard browser at the URL http://xxx.xxx.xxx.xxx where 'xxx.xxx.xxx.xxx' is the current IP address assigned to the nMU.

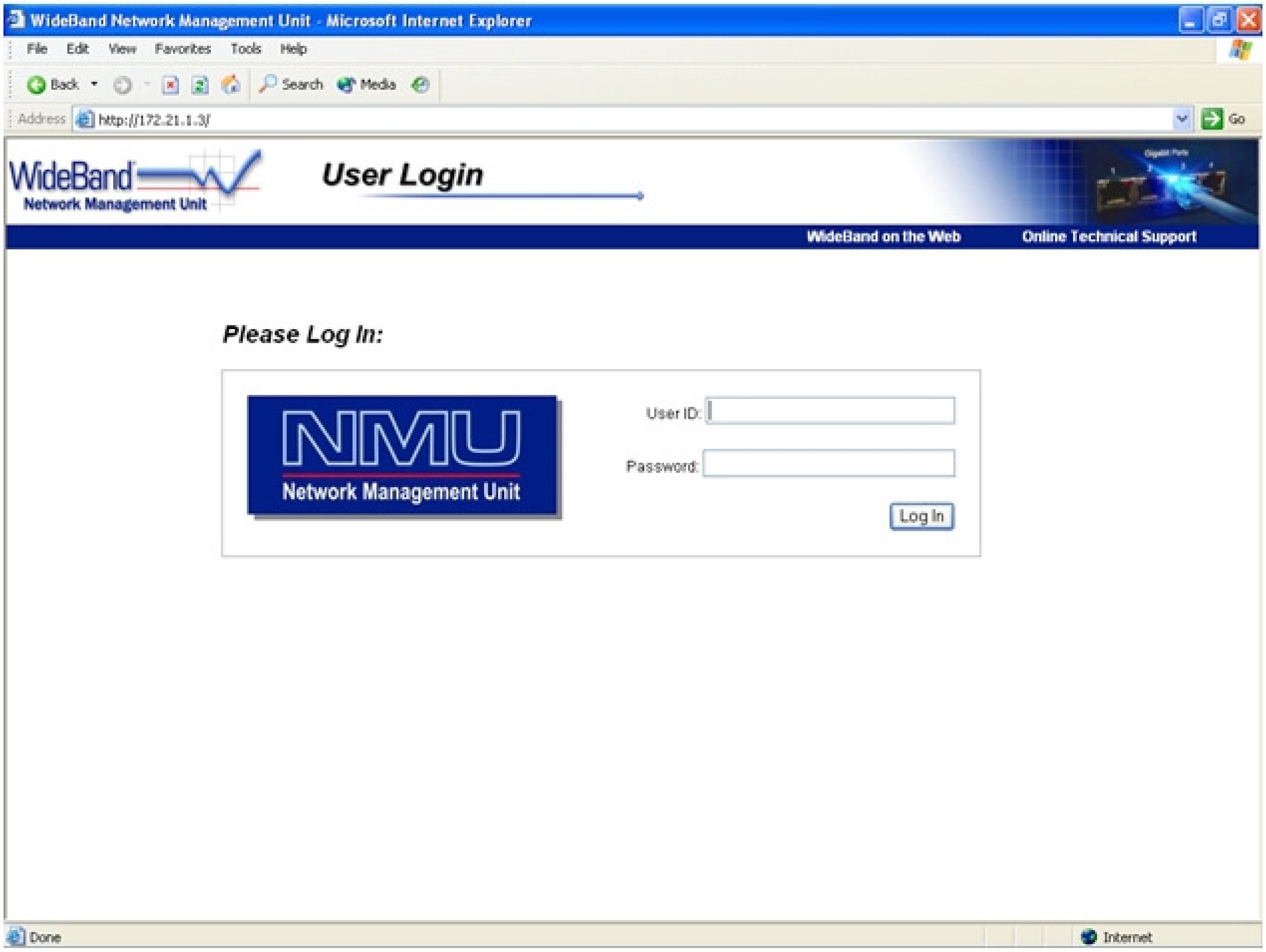

WideBand Network Management Unit - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Media
Address http://172.21.1.3/
Go
WideBand Network Management Unit
User Login
WideBand on the Web
Online Technical Support
Please Log In:
NMU Network Management Unit
User ID:
Password:
Log In
Done
Internet

Figure 1. Users are required to supply a User ID and Password.

Once a user has successfully logged on, a static IP address can also be assigned through the browser interface (See the Network Interface Screen section).

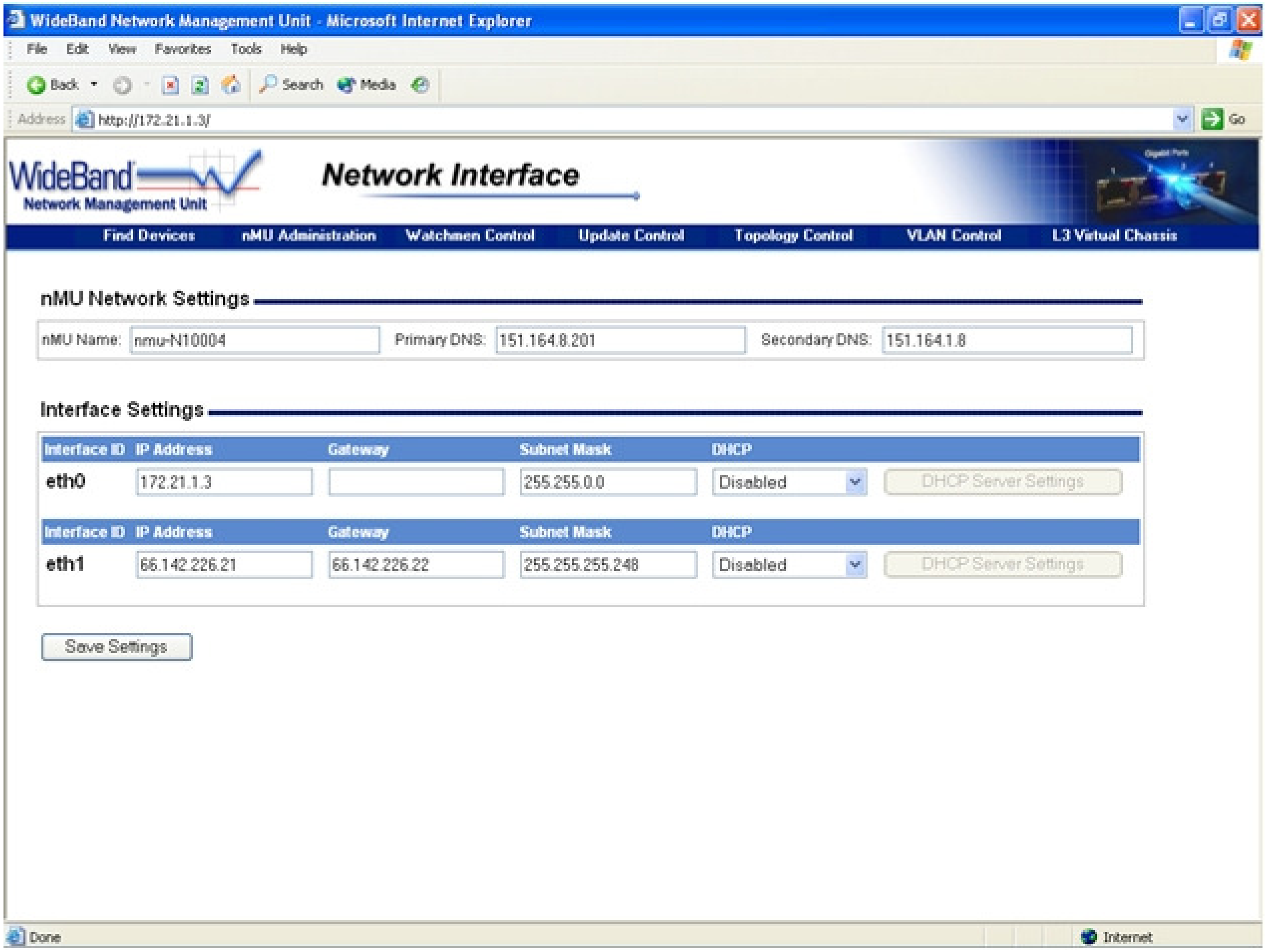
User Login

On the User Login screen you are required to supply a user ID and password (See Figure 1). The WideBand nMU ships with one default user already in place.

The default user is “administrator” with a password that you must set through the startup configuration utility. This user cannot be removed and is needed to add and control normal users.

Network Interface Screen

The Network Interface screen is where the IP settings for each Ethernet Interface on the nMU are configured. You must be logged in as “administrator” to access this screen.



Address: http://172.21.1.3/

nMU Network Settings

nMU Name: nmu-N10004 Primary DNS: 151.164.8.201 Secondary DNS: 151.164.1.8

Interface Settings

Interface ID	IP Address	Gateway	Subnet Mask	DHCP
eth0	172.21.1.3		255.255.0.0	Disabled
eth1	66.142.226.21	66.142.226.22	255.255.255.248	Disabled

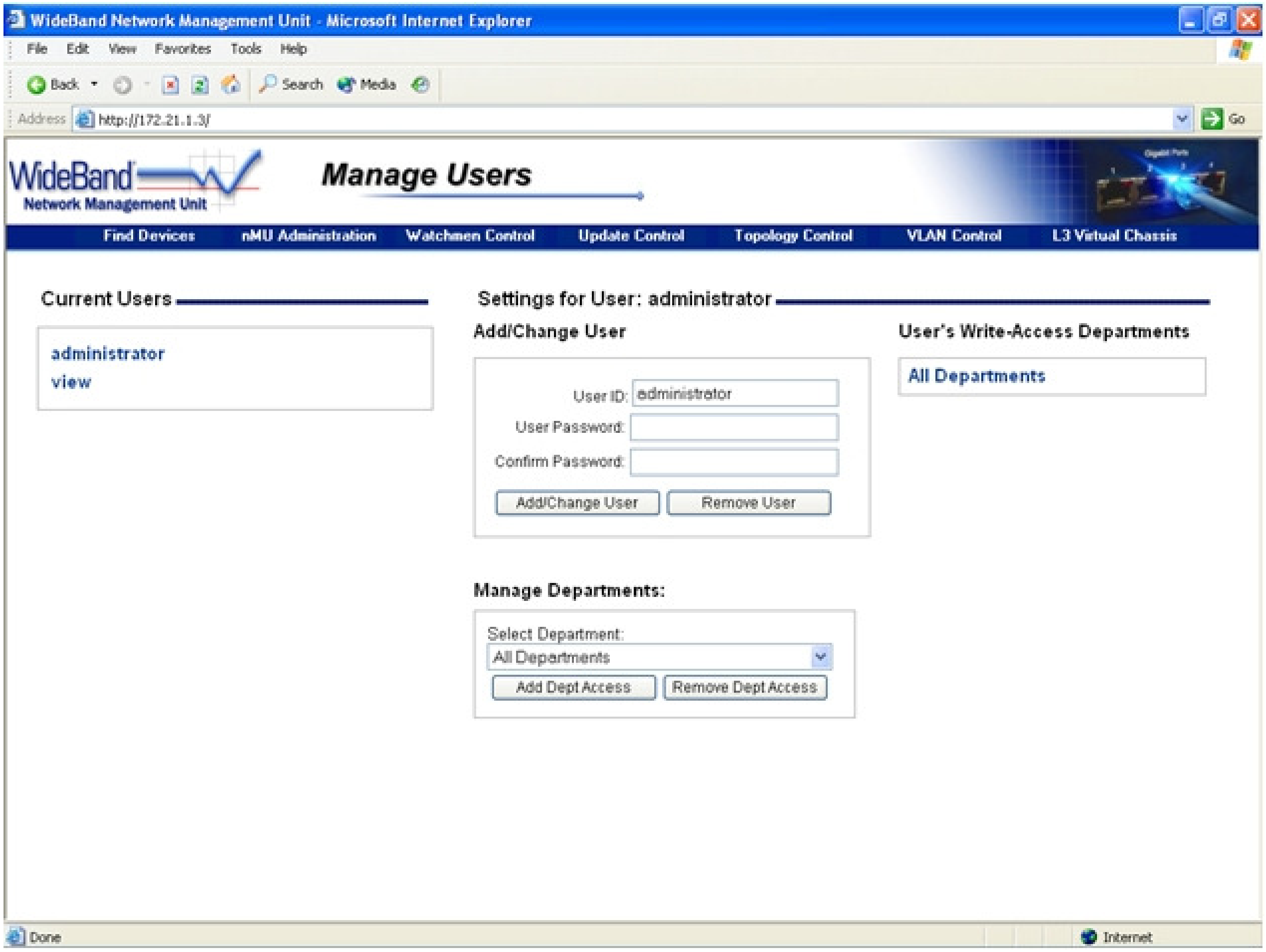
Figure 2. nMU Network Interface settings may only be edited by the administrator user.

It is often desirable to assign a static IP address to the WideBand nMU. It's also important to make sure the nMU has valid IP settings to connect to the Internet. This is needed to send email reports and download the latest updates. The following table describes the IP settings that must be configured correctly:

Field Name	Description
Server Name	Host name that can be used to access the nMU through a browser
Primary DNS	Preferred Domain Name Server the nMU will look for
Secondary DNS	Alternate Domain Name Server the nMU will look for
SMTP Server	An optional SMTP server can be used for outgoing emails reports
IP Address	IP address that must be used to communicate with the nMU
Subnet Mask	Subnet mask of the IP network nMU is running on
Default Gateway	Internet gateway IP address the nMU is using
DHCP Status	DHCP is used to automatically learn an IP address

Manage Users Screen

The Manage Users screen (Figure 3) can only be accessed by the "administrator" user, and is where all nMU users are added and controlled.



WideBand Network Management Unit - Microsoft Internet Explorer

Address: http://172.21.1.3/

Manage Users

Current Users

administrator
view

Settings for User: administrator

Add/Change User

User ID: administrator

User Password:

Confirm Password:

User's Write-Access Departments

All Departments

Manage Departments:

Select Department: All Departments

Figure 3. Use "Manage Users" to add users and their privileges.

Adding Users

To add a user, just enter a new user ID and password in the *User ID* and *User Password* fields. Then click the *Add/Change User* button. A new user will be added only if the user name you specified was not already in the *Current Users* list. If an existing user ID is entered with a new password, its password will be changed.

User Privileges

All nMU users have read access to every device on the network by default. The desired write privileges must be enabled for each user. The WideBand nMU organizes write privileges by department. Each device is added to a department when the nMU takes control of it (See the Making Devices Managed by nMU section).

To give a user write access to a department do the following:

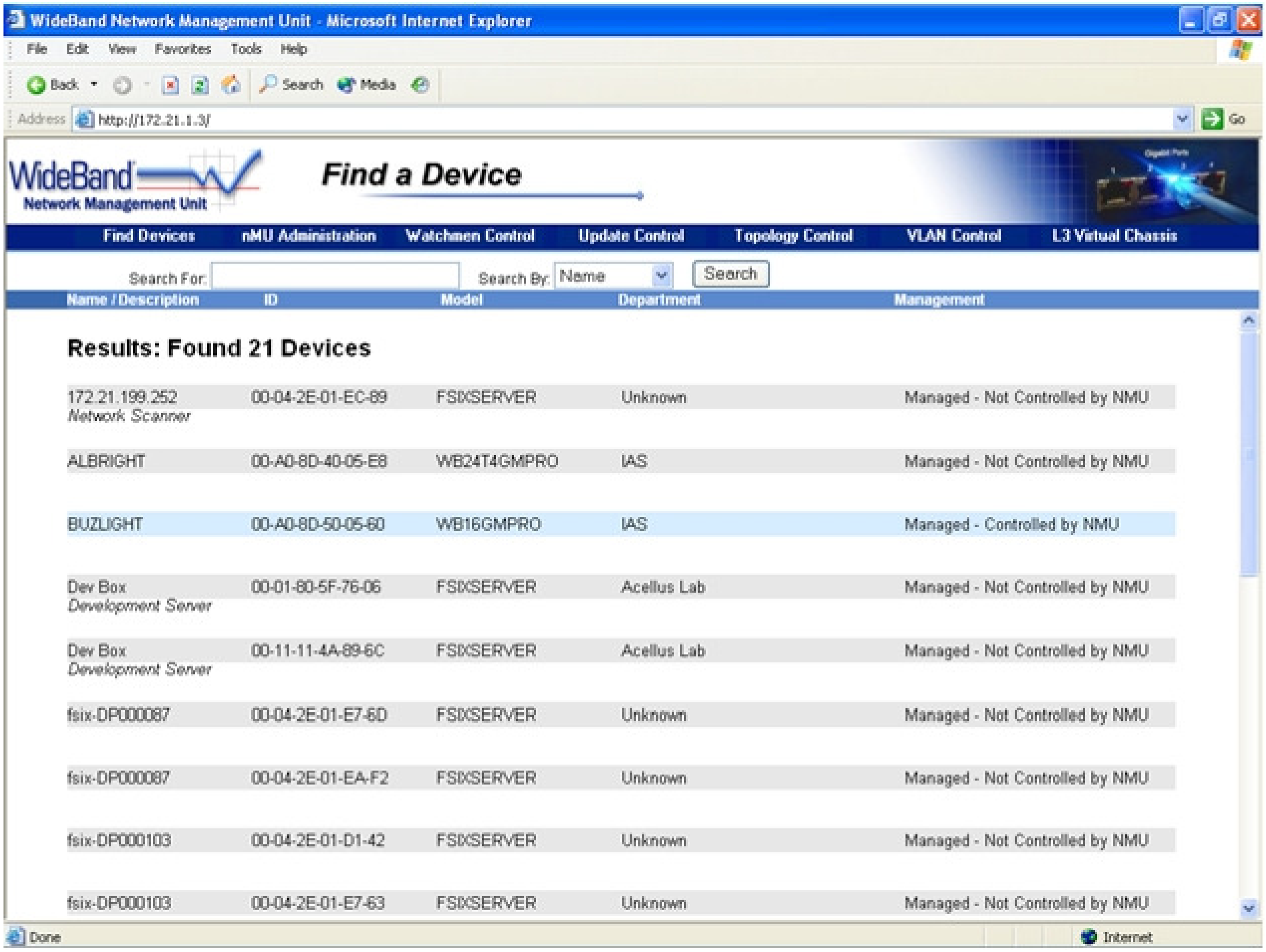
1) Select the user name you wish to modify from the *Current Users* list on the left. The settings for the user ID you selected should show in the *Settings For User* section.
2) In the *Select Department* drop down box, find the department you would like the user to be able to access, and then click on the *Add Dept Access* button. (*Note that if the nMU is not yet managing any devices, no departments will be listed in the* Select Department *drop-down box.*)
3) The newly added department should be added to the *User's Write–Access Departments* list on the right.

You can give a user access to a limited group of departments, or, alternatively, you can give a user access to all departments. Only users with access to all departments can modify VLAN settings or change the department assignment on switches and servers. These privileges are limited in this way because these kinds of changes affect all departments.

Find A Device Screen

When a user logs onto the nMU, the first screen that opens is the *Find A Device* screen (see Figure 4). This screen lists every device that the nMU was able to find on the network. The following color-coding is used in the *Device List*:

- Gray: Denotes devices that are managed, but are not controlled by the nMU.
- Off-White: Denotes devices that are un-managed and are not controlled by the nMU.
- Blue: Denotes devices that are managed and controlled by the nMU.
- Green: Denotes devices that are unmanaged, but still controlled by the nMU.



Search For:

Search By: Name

Results: Found 21 Devices

Name / Description	ID	Model	Department	Management
172.21.199.252 *Network Scanner*	00-04-2E-01-EC-89	FSIXSERVER	Unknown	Managed - Not Controlled by NMU
ALBRIGHT	00-A0-8D-40-05-E8	WB24T4GMPRO	IAS	Managed - Not Controlled by NMU
BUZLIGHT	00-A0-8D-50-05-60	WB16GMPRO	IAS	Managed - Controlled by NMU
Dev Box *Development Server*	00-01-80-5F-76-06	FSIXSERVER	Acellus Lab	Managed - Not Controlled by NMU
Dev Box *Development Server*	00-11-11-4A-89-6C	FSIXSERVER	Acellus Lab	Managed - Not Controlled by NMU
fsix-DP000087	00-04-2E-01-E7-6D	FSIXSERVER	Unknown	Managed - Not Controlled by NMU
fsix-DP000087	00-04-2E-01-EA-F2	FSIXSERVER	Unknown	Managed - Not Controlled by NMU
fsix-DP000103	00-04-2E-01-D1-42	FSIXSERVER	Unknown	Managed - Not Controlled by NMU
fsix-DP000103	00-04-2E-01-E7-63	FSIXSERVER	Unknown	Managed - Not Controlled by NMU

Figure 4. The Find a Device screen displays all devices found, with blue, gray, off-white, and green highlights indicating management and nMU control status.

Searching for Devices

The WideBand nMU has a powerful search engine for finding the device on the network you are looking for. The List of switches can be searched and sorted by any of the following criteria:

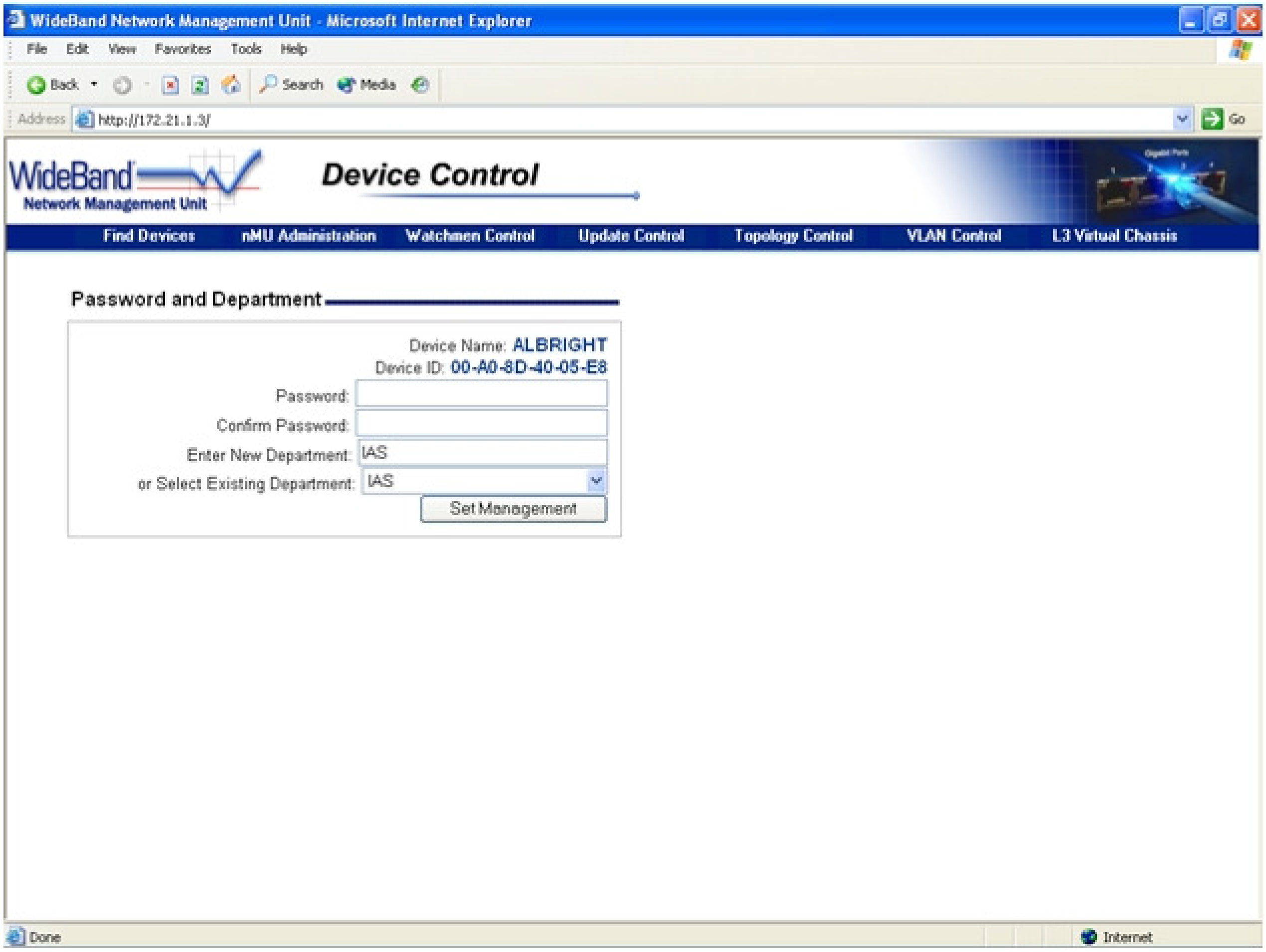
- Name – The name added to the switch for human friendly identification
- Serial No. – Same as the switch MAC address which is unique for every switch
- Model – A short description of the type and number of ports the switch has
- Description – A user defined description of the device
- Department – The department this device is a member of

The Search feature includes built-in wild cards, allowing you to enter partial words, etc and find multiple devices with similar criteria. Entering a blank field as the criteria will return a list of all devices.

Making Devices Managed by nMU

The WideBand nMU can only manage devices that it has learned a password and department for. When a device is selected from the Device List that is not managed by the nMU, a password and department must be supplied before management of that device can continue (See Figure 5).

Once this information has been entered, the nMU will automatically apply all of the department's current settings to the new device (Refer to the Department Topology Settings section for more information on department settings).



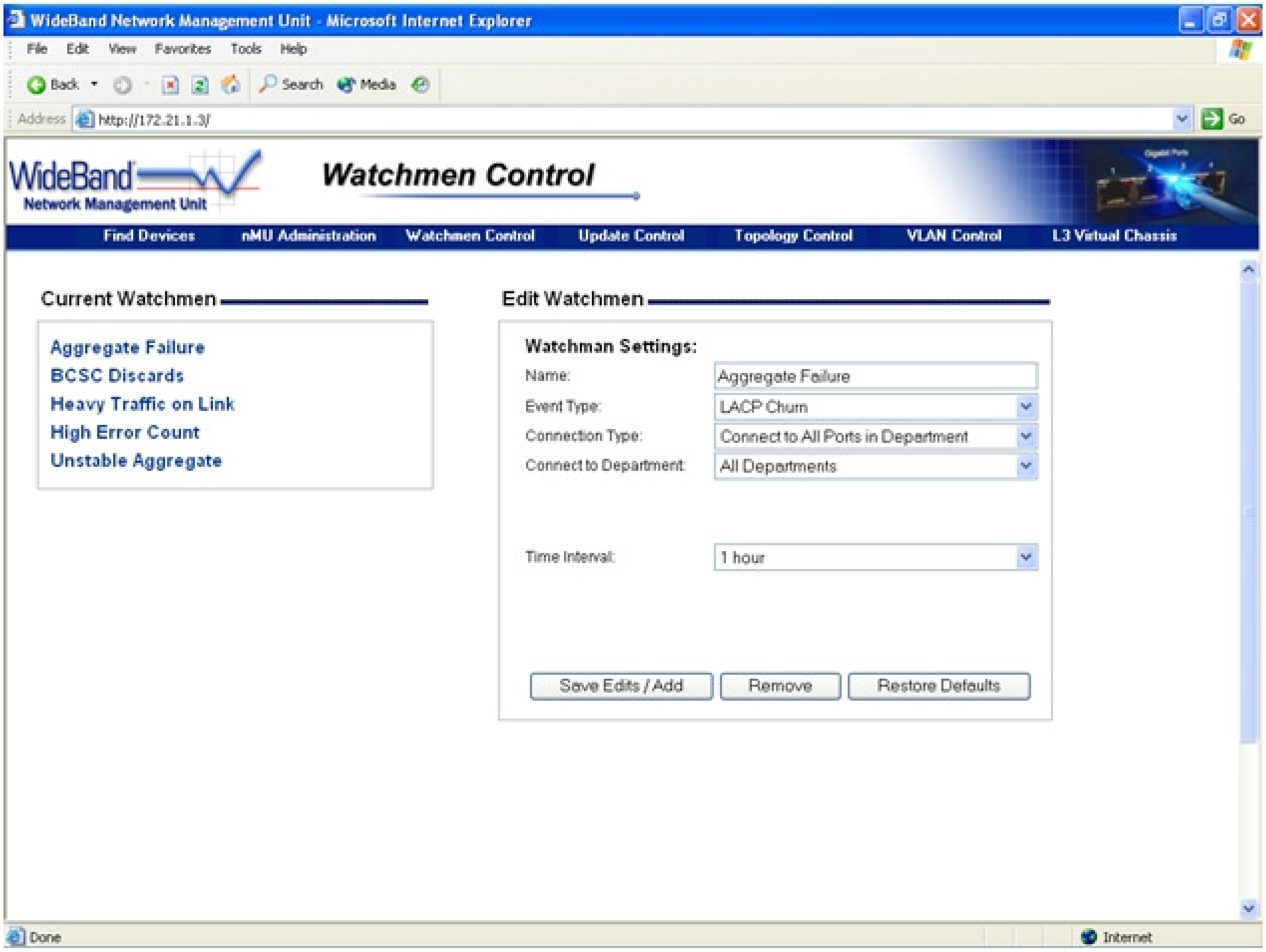
http://172.21.1.3/

Device Name: ALBRIGHT
Device ID: 00-A0-8D-40-05-E8
Password:
Confirm Password:
Enter New Department: IAS
or Select Existing Department: IAS

Figure 5. The nMU requires a password and department before it will manage a device.

Watchmen Control

The WideBand Watchmen are periodic checks that run on the nMU to look for specific conditions that might occur. When the condition is met for a watchman, an event is generated and added to the Watchmen Log. This log is then emailed to a list of recipients. WideBand Watchmen are very useful for maintaining an up-to-date understanding of how a network is performing.



Current Watchmen

- Aggregate Failure
- BCSC Discards
- Heavy Traffic on Link
- High Error Count
- Unstable Aggregate

Edit Watchmen

Watchman Settings:

Name: Aggregate Failure
Event Type: LACP Churn
Connection Type: Connect to All Ports in Department
Connect to Department: All Departments
Time Interval: 1 hour

Figure 6. The WideBand Watchmen can be created and modified on the Watchmen Control screen.

The following table describes the default watchmen on the WideBand nMU:

Watchman Name	Description
Aggregate Failure	Checks every hour for links that are continually trying but failing to aggregate. The IEEE 802.3ad standard calls this phenomenon a LACP Churn. A common cause for LACP Churns is when more than two managed switches are connected through one cheap switch that just forwards the LACP packets. In this situation, aggregation cannot stabilize on the managed switches.

BCSC Discards	Checks every hour for 1000 or more discarded packets due to broadcast storms. Broadcast storms occur when the network is saturated with broadcast traffic. An undesired loop in the network is a common cause for these storms.
Data Not Mirrored	Checks every 2 hours for any mirrored fs[ix] server that has lost connection to its partner.
Heavy Traffic on Link	Checks every 30 minutes for an average of 500 or more Mbps on any Link. If a gigabit link is averaging at 500Mbps, it is almost surely peaking at a much higher bandwidth. In this case, putting in another aggregated link could greatly improve network performance.
High Error Count	Checks every hour for 10000 or more packet errors of any kind on any link. Bad cables, or busy links running in half duplex mode are common causes of high error rates. Errors on one link can potentially slow down the entire LAN.
Network Congestion	Checks every 20 minutes for 10 million or more pause-packets. This would indicate the packet buffers on the switches are full due to network congestion.
Server is Constantly Busy	Checks every hour for fs[ix] servers unable to keep up with client requests. This may occasionally happen when Gold Severs are synchronizing for the first time.
Storage Disk is Full	Checks every 24 hours for fs[ix] servers that have less than 10 gigabytes left on their hard drive.
Unstable Aggregate	Checks every hour for an aggregated link that changes its state 30 or more times. If a link is unstable for any reason, its performance will be greatly derogated.

Adding Watchmen

A new watchman will be created when the *Save Edits / Add* button is pressed, if the name in the *Name* field is not the same as any of the names in the *Current Watchmen* list. If the name is already in the *Current Watchmen* list then that watchman will be modified. There are several different types of watchmen that can be created. The appropriate configuration fields will show and hide on the page, depending on the type of watchman you create. The following table describes the most common fields:

Field Name	**Description**
Name	The name that will be assigned to this watchman.
Event Type	The type of event this watchman will generate. (See the Watchmen Types table, following)
Connect to Department	Specifies the group of devices this watchman will apply to. (Only valid if both the *Connect to Device* and *Connect to Port* fields are empty)
Connect to Device	Specifies a single device this watchman will apply to.
Connect to Port	Specifies a single port this watchman will apply to.
Time Interval	Indicates how often the watchman check will be performed.

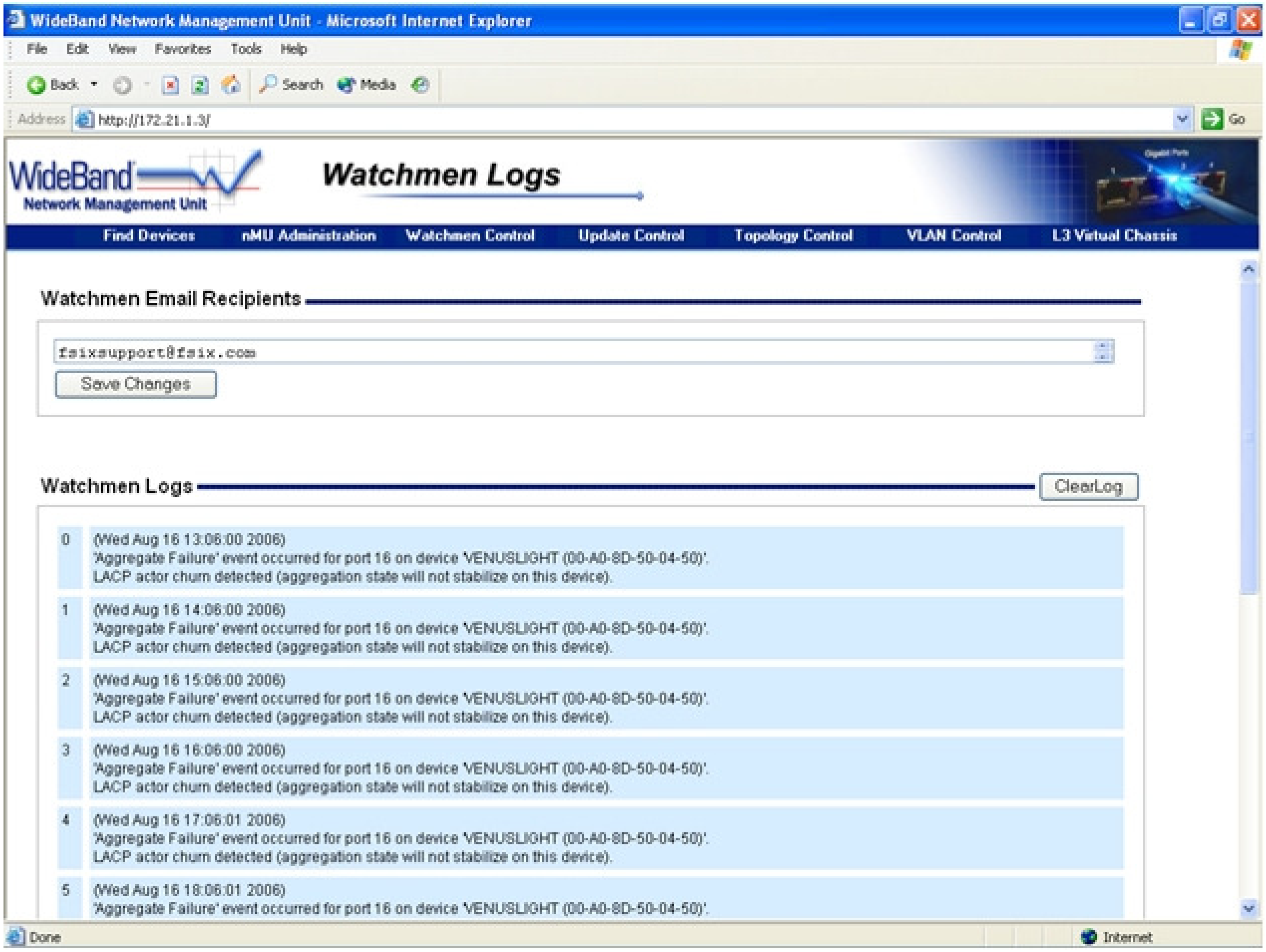
Watchmen Types

The following table describes the different watchman types that are currently defined:

Watchman Type	Description
Error Counter Limit Exceeded	Adds up all of the counter errors for each port and compares that total to the specified *Number of Errors* limit for the time interval.
Specific Counter Limit Exceeded	Looks for an exceeded limit for a specific counter on each port within the specified time interval.
Bandwidth Utilization Limit Exceeded	Checks for links that exceed a defined average bandwidth within the specified time interval.
Aggregate Changed	Looks for links that have changed aggregate status too many times in the defined time interval.
BCSC Discard Exceeded	Checks at the total number of packet discards within the time interval due to broadcast storms on each device.
LACP Churn	Finds any link that is unable to stabilize its aggregation state.
Managed Device Not Responding	Looks for devices that are failing to respond to management requests.
Ping Failed	Makes sure a specified IP address is responding to PING requests.
Error Counter Exceeded (w/o COL)	Adds up all of the counter errors without collisions for each port and compares that total to the specified *Number of Errors* limit for the time interval.
Data Mirroring Failure	A fs[ix] mirroring server is unable to send/receive mirrored data.
Data Disk Full	A fs[ix] server has less than the specified number of gigabytes free on its data disks.
Performance Max Out	A fs[ix] server is unable to keep up with client requests.
Security Vulnerabilities Found	One or more security holes or warnings are found on the scan targets.

Watchmen Log Screen

All of the WideBand Watchmen events are recorded in the Watchmen Log. Every thirty minutes, if there are any new events, the log is emailed to a list of recipients. Clicking the *Clear Log* button will erase all current events in the log.



fsixsupport@fsix.com

```
0  (Wed Aug 16 13:06:00 2006)
   'Aggregate Failure' event occurred for port 16 on device 'VENUSLIGHT (00-A0-8D-50-04-50)'.
   LACP actor churn detected (aggregation state will not stabilize on this device).
1  (Wed Aug 16 14:06:00 2006)
   'Aggregate Failure' event occurred for port 16 on device 'VENUSLIGHT (00-A0-8D-50-04-50)'.
   LACP actor churn detected (aggregation state will not stabilize on this device).
2  (Wed Aug 16 15:06:00 2006)
   'Aggregate Failure' event occurred for port 16 on device 'VENUSLIGHT (00-A0-8D-50-04-50)'.
   LACP actor churn detected (aggregation state will not stabilize on this device).
3  (Wed Aug 16 16:06:00 2006)
   'Aggregate Failure' event occurred for port 16 on device 'VENUSLIGHT (00-A0-8D-50-04-50)'.
   LACP actor churn detected (aggregation state will not stabilize on this device).
4  (Wed Aug 16 17:06:01 2006)
   'Aggregate Failure' event occurred for port 16 on device 'VENUSLIGHT (00-A0-8D-50-04-50)'.
   LACP actor churn detected (aggregation state will not stabilize on this device).
5  (Wed Aug 16 18:06:01 2006)
   'Aggregate Failure' event occurred for port 16 on device 'VENUSLIGHT (00-A0-8D-50-04-50)'.
```

Figure 7. The Watchmen Logs screen maintains a list of every watchman event that has occurred.

Email Recipients

The WideBand nMU will send watchmen event logs to every address specified in the list of recipients. The default address is the following:

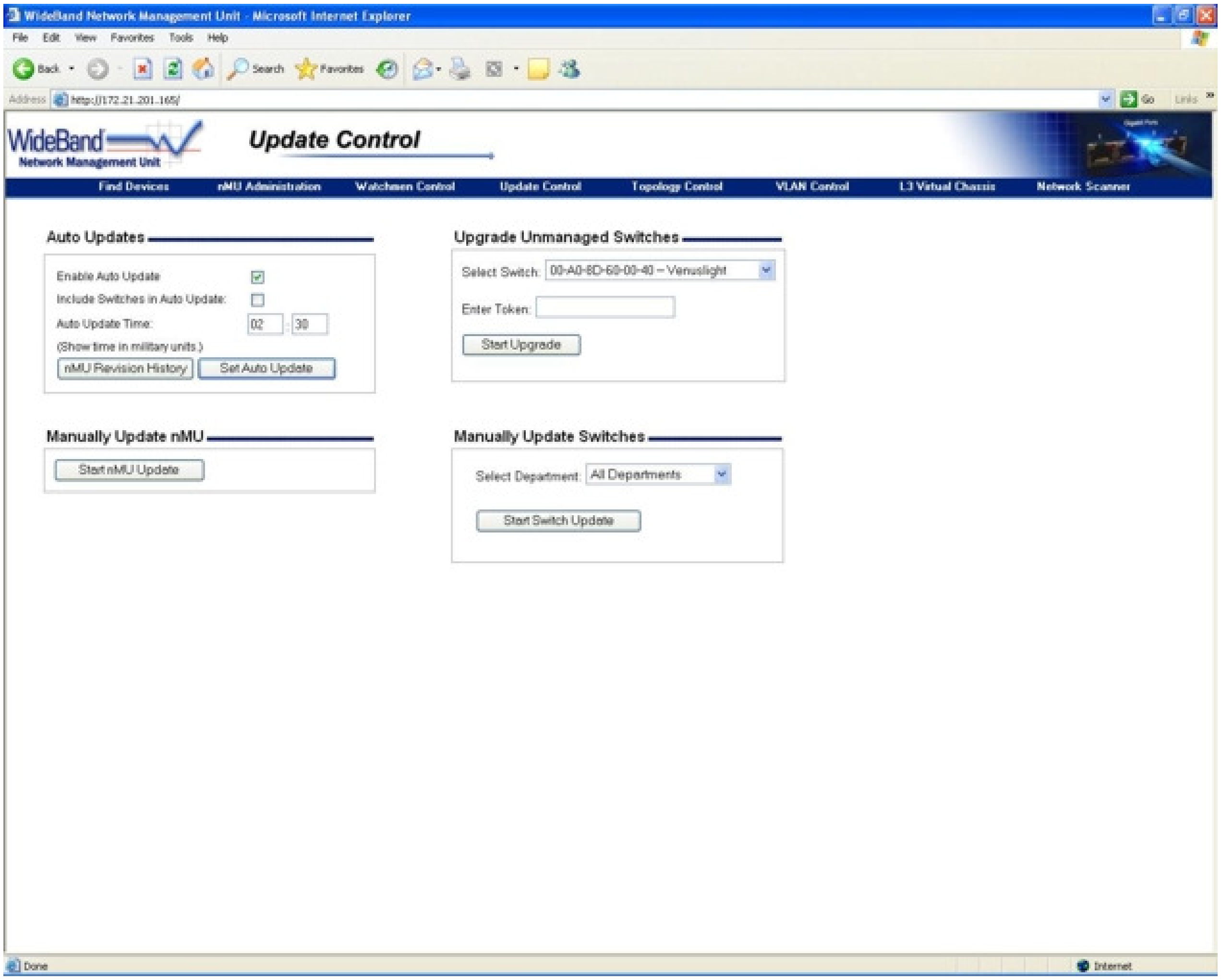
fsixsupport@fsix.com

WideBand Corporation suggests that you leave the default address and just add any other addresses to the list. That way technical support will have a better understanding of any issues that you might encounter.

***Note:** Email addresses should be separated by a comma.*

Update Control Screen

This screen can be accessed through the *Update Control* button on the top banner. All of the manual and automatic updates performed by the nMU are configured here.



Auto Updates

Enable Auto Update ☑

Include Switches in Auto Update: □

Auto Update Time: 02 : 30

(Show time in military units.)

nMU Revision History | Set Auto Update

Upgrade Unmanaged Switches

Select Switch: 00-A0-8D-60-00-40 – Venuslight

Enter Token:

Start Upgrade

Manually Update nMU

Start nMU Update

Manually Update Switches

Select Department: All Departments

Start Switch Update

Figure 8. The Update Control screen is where all of the nMU update settings are configured.

Auto Updates

The WideBand nMU is configured by default to download new updates over the Internet every night. This automatic update is enabled or disabled with the *Enable Auto Update* check box (See Figure 8).

The nMU update optionally includes updating all of the WideBand Professional Switches on the network to the latest firmware. This is normally a good idea, but since the switches will momentarily stop forwarding traffic during an upgrade, this feature is disabled by default. Check the *Include Switches in Auto Update* check box to enable this feature. In order for the update to be successful, the nMU must have access to the Internet (Refer to the nMU IP Configuration section of this manual).

The *Auto Update Time* is shown in military units and describes when the nMU is planning its next automatic update. Remember to save any changes you make to the Auto Update settings by clicking the *Set Auto Update* button.

Upgrade Unmanaged Switches

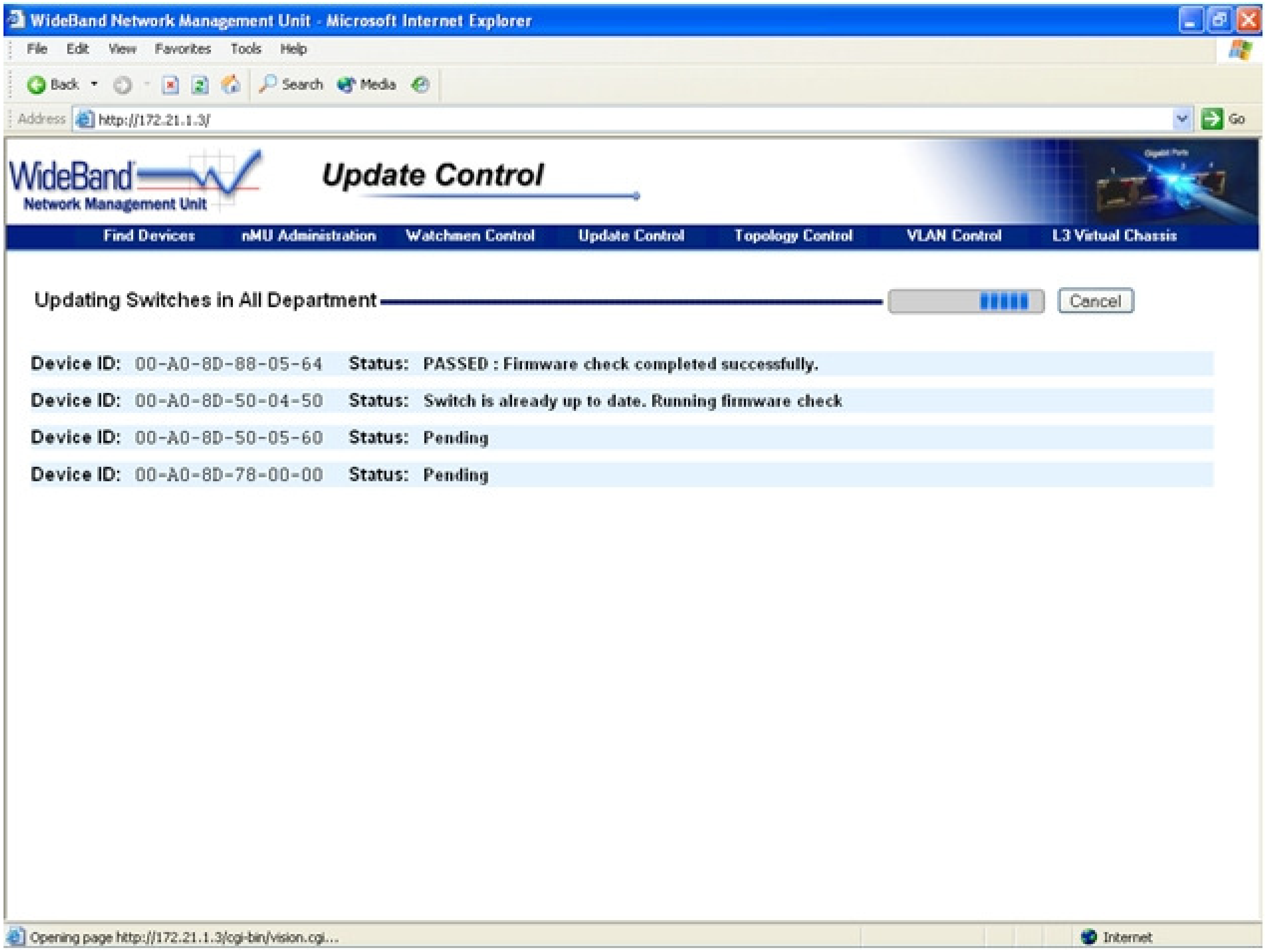
Most WideBand Professional Series Switches that are unmanaged can be upgraded to managed with the purchase of a management Token. Token(s) may be obtained via the web at http://www.wband.com/proswitch, or through your WideBand Reseller. To locate the WideBand Authorized Resellers nearest you, contact the WideBand Sales Office at (888) 663-3050.

Once you have the Token ready to use, select the unmanaged switch to be upgraded from the *Select Switch* list box. Note that the switch must be controlled by the nMU in order to perform an upgrade (See the Making Devices Managed by nMU section). Enter your valid Token in the *Enter Token* field, and click on the *Start Upgrade* button to start the upgrade.

Manually Update Switches

The WideBand nMU will perform switch firmware updates on groups of switches at a time. Each department is a separate group.

To start a group update, choose a department in the *Select Department* list box, and click *Start Switch Update* button (see Figure 8). This will load a screen that reports the update status of every switch in the selected department (see Figure 9). Only a firmware check will be performed on the switches that are already up-to-date.


WideBand Network Management Unit - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Media
Address http://172.21.1.3/ Go
WideBand Network Management Unit
Update Control
Find Devices
nMU Administration
Watchmen Control
Update Control
Topology Control
VLAN Control
L3 Virtual Chassis
Cancel
Opening page http://172.21.1.3/cgi-bin/vision.cgi...
Internet

Updating Switches in All Department

Device ID: 00-A0-8D-88-05-64 Status: PASSED : Firmware check completed successfully.

Device ID: 00-A0-8D-50-04-50 Status: Switch is already up to date. Running firmware check

Device ID: 00-A0-8D-50-05-60 Status: Pending

Device ID: 00-A0-8D-78-00-00 Status: Pending

Figure 9. The firmware update status is reported for each switch in the department.

Manually Update nMU

Manually updating the WideBand nMU does the same thing as the *Auto Update*, but it runs immediately instead of waiting until the middle of the night. Clicking the *Start nMU Update* button initiates a manual nMU update.

A description of the latest downloaded nMU updates can be viewed by clicking the *nMU Revision History* button.

Topology Control

A click on the *Topology Control* link in the top banner opens the Topology Control screen (see Figure 10). This is where we can configure settings that affect the general flow of traffic across the LAN. This screen is divided into two sections; the first section, *Network Spanning Tree Settings*, applies to every switch on the network, while the other section, *Department Topology Set-tings*, applies to individual departments.

Network Spanning Tree

Spanning Tree Protocol (IEEE 802.1D) is used to automatically disable loops in the network. Refer to the Spanning Tree State section for more information on this protocol.

The Spanning Tree protocol works by choosing one switch on the network to be the root, and all the other switches find the shortest path to that root. This being the case, the root switch should be as close as possible to the heart of the network to increase traffic efficiency. The following table describes the settings that control the Spanning Tree Root of the network:

Field Name	Description
Designated Root	ID of the device that is currently acting as root. Note that this field is only valid if the department it was extracted from has Spanning Tree enabled.
Suggest Root	ID of a device the nMU will attempt to make into the root.
Hello Time	Time interval between the generation of Configuration BPDUs if the switch is the Root (In seconds)
Maximum Time	A timeout value to be used by all Bridges in the Bridged LAN if the switch is the Root (in seconds)
Forward Delay	A timeout value to be used by all Bridges in the Bridged LAN if the switch is the Root (in seconds)

Before any new settings can take effect, the *Save Network Settings* button must be pressed which will load a screen that reports the configuration update status of each device. When the nMU suggests a new root to the network, it will often take several seconds for that root to be recognized across the entire LAN.

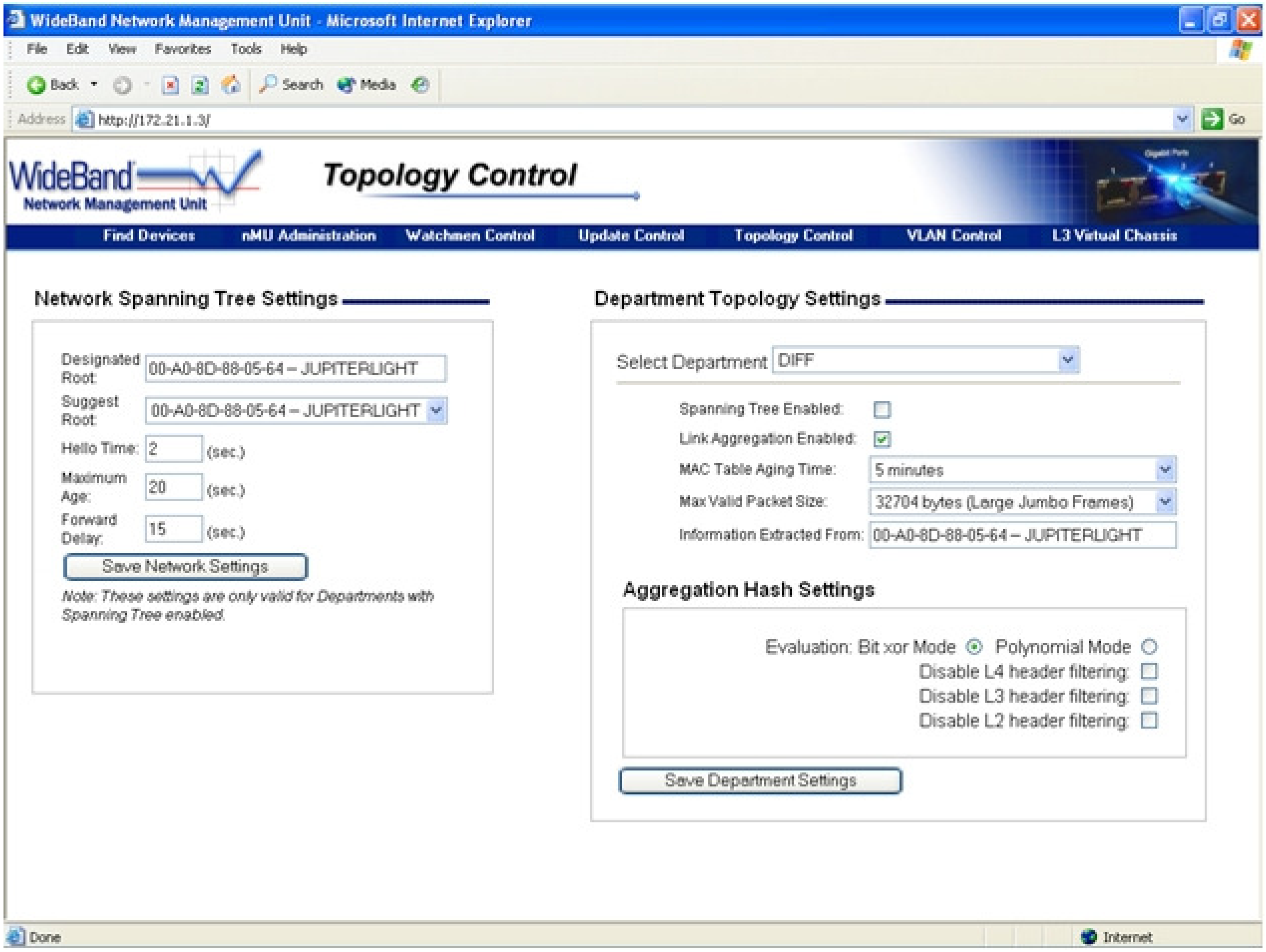
Department Topology Settings

The following table describes the settings that can be configured for each department:

Field Name	Description
Spanning Tree Enabled	Enables Spanning Tree for this department. (Resolves data loops in the network)
Link Aggregation Enabled	Enables Link Aggregation for this department. (Allows multiple

	links to work together as one)
MAC Table Aging Time	The rate at which learned MAC addresses will age out of switches on this department.
Max Valid Packet Size	The largest packet size that switches in this department will forward
Information Extracted From	ID of the device these department settings were extracted from
Evaluation Mode	Select either Bit XOR or Polynomial hashing algorithm (Refer to the LACP Hash Configurations section)
Disable L4 header filtering	Disables use of IP-TCP/UDP Port/Socket in hashing function
Disable L3 header filtering	Disables use of IP/IPX address in hashing function
Disable L2 header filtering	Disables use of MAC address in hashing function

Any changes that are made these fields must be applied to every switch in the department by selecting the *Save Department Settings*.



Network Spanning Tree Settings

Designated Root: 00-A0-8D-88-05-64 – JUPITERLIGHT

Suggest Root: 00-A0-8D-88-05-64 – JUPITERLIGHT

Hello Time: 2 (sec.)

Maximum Age: 20 (sec.)

Forward Delay: 15 (sec.)

Save Network Settings

Note: These settings are only valid for Departments with Spanning Tree enabled.

Department Topology Settings

Select Department DIFF

Spanning Tree Enabled: ☐

Link Aggregation Enabled: ☑

MAC Table Aging Time: 5 minutes

Max Valid Packet Size: 32704 bytes (Large Jumbo Frames)

Information Extracted From: 00-A0-8D-88-05-64 – JUPITERLIGHT

Aggregation Hash Settings

Evaluation: Bit xor Mode ● Polynomial Mode ○

Disable L4 header filtering: ☐

Disable L3 header filtering: ☐

Disable L2 header filtering: ☐

Save Department Settings

Figure 10. The Topology Control screen contains settings that apply to multiple switches on the network.

Link Aggregation

Link Aggregation, also known as Port Trunking, is the ability to set up network ports on a device to work together as one higher-bandwidth link.

The WideBand Professional Series Switches use the IEEE 802.3ad Link Aggregation Control Protocol (LACP) to automatically configure the ports in this manner. This feature is enabled by default on the Professional Series Switches, and up to 16 ports can be connected in one aggregate. Refer to the Department Topology Settings section of this manual for information on controlling Link Aggregation.

Here are some important requirements that you must keep in mind while connecting multiple links for any aggregate:

- Every link must be running at the same speed
- Full Duplex is required on every link in the aggregate
- Link Aggregation must be enabled on both ends of the aggregate

If any of these requirements is not met, the links will not aggregate together, which could create a network loop. You may want Spanning Tree enabled just in case that ever happens.

LACP Hash Configurations

For multiple port aggregates, a hash is used to determine the port on which each packet is to be sent. Normally, the default hash configuration will work fine, but the WideBand Professional Series Switches allow extensive hash management control. In some cases, changes to the hash can more evenly distribute the traffic load on the aggregated links, greatly improving performance. Changing the hash settings is done for each department individually. Refer to the Department Topology Settings of this manual for more information on changing the hash settings.

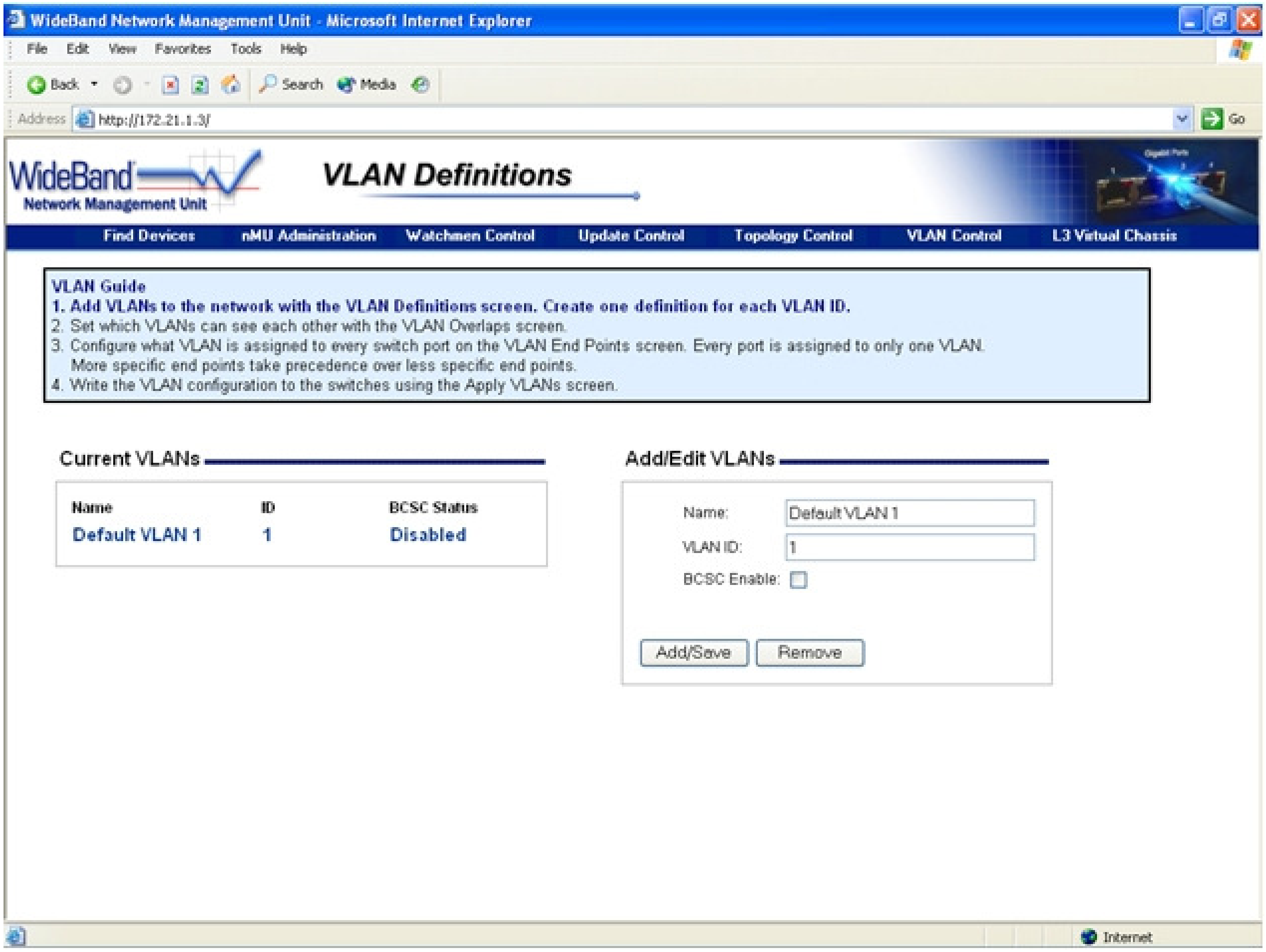
VLAN Management Screens

Switches do not inherently support broadcast domains, which can lead to broadcast storms in large networks that handle a lot of traffic, such as NetBuei or IPX. In conventional networks with routers, broadcast traffic is split up into separate domains to confine this traffic to the originating group and provide a much cleaner network environment. Instead of using physically separate subnets that are linked by traditionally slow routers, the WideBand Professional Series Switch can create segregated broadcast domains based on easily configurable VLANs, and then link these VLANs as required with wire-speed routing.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. The WideBand nMU is designed to automatically configure the VLAN settings across the network based on the settings entered on the VLAN management screens. The VLAN screens menu can be accessed through the *VLAN Control* button on the top banner.

VLAN Definitions

This screen is where every VLAN on the network is defined. To create a new VLAN definition, modify the *Name*, *VLAN ID*, and *VLAN Index* fields. Then click the *Save Edits* button (See Figure 11). A new entry will be added to the *Current VLANs* list as long as the *VLAN ID* is not already defined. The following table describes the VLAN definition settings:


WideBand Network Management Unit - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Media
Address http://172.21.1.3/
Go
WideBand Network Management Unit
VLAN Definitions
Find Devices
nMU Administration
Watchmen Control
Update Control
Topology Control
VLAN Control
L3 Virtual Chassis
Internet

VLAN Guide
1. Add VLANs to the network with the VLAN Definitions screen. Create one definition for each VLAN ID.
2. Set which VLANs can see each other with the VLAN Overlaps screen.
3. Configure what VLAN is assigned to every switch port on the VLAN End Points screen. Every port is assigned to only one VLAN. More specific end points take precedence over less specific end points.
4. Write the VLAN configuration to the switches using the Apply VLANs screen.

Current VLANs

Name	ID	BCSC Status
Default VLAN 1	1	Disabled

Add/Edit VLANs

Name: Default VLAN 1
VLAN ID: 1
BCSC Enable: □

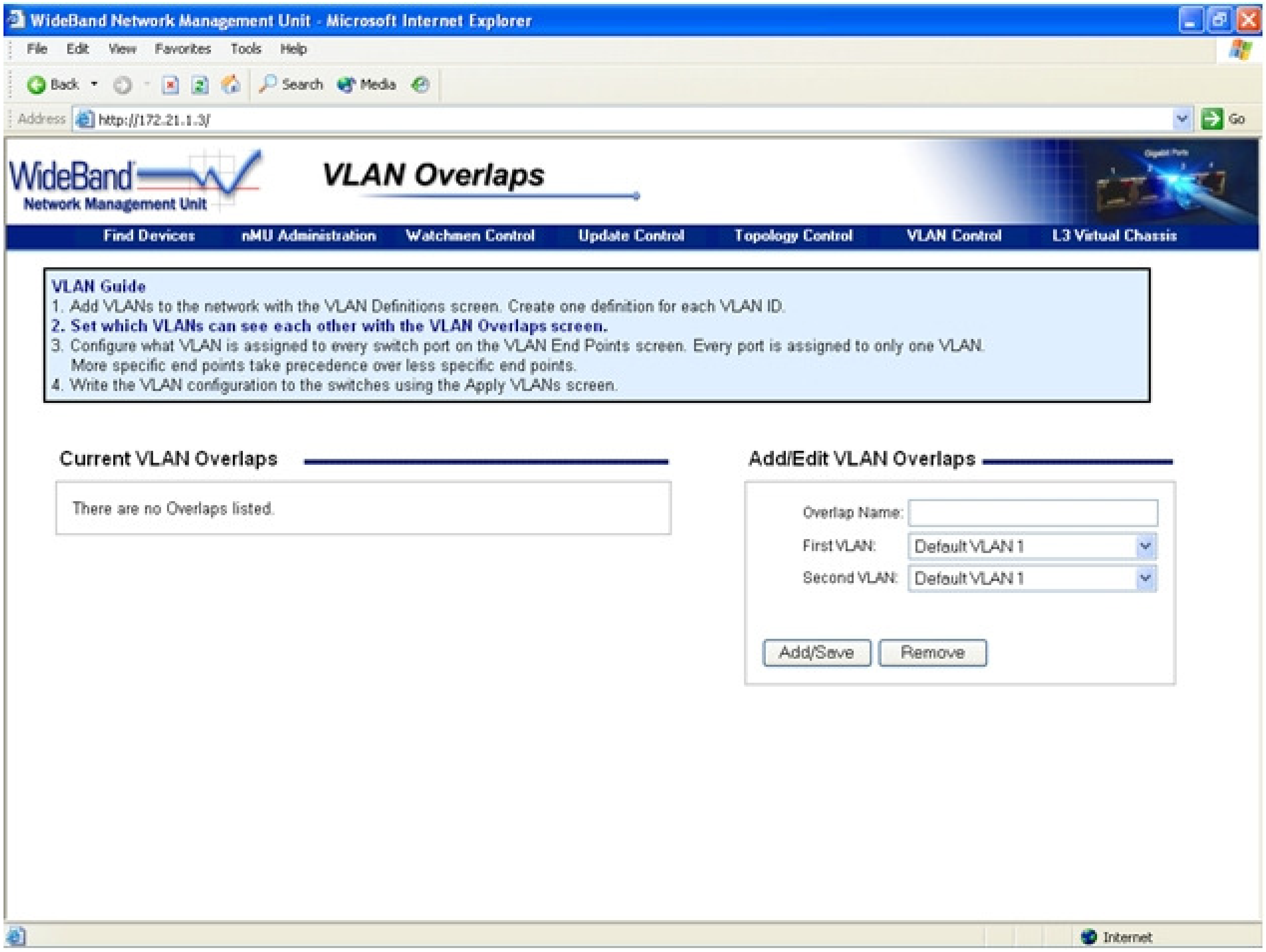
Figure 11. The VLAN Definitions screen contains a list of every VLAN on the network.

Field Name	Description
Name	A logical name assigned to this VLAN
VLAN ID	The VLAN ID this definition defines (1-4094 are valid possibilities)
BCSC Enabled	Check this box to enable broadcast storm control for this VLAN

VLAN Overlaps

VLAN overlaps are one way to let VLANs see each other. One common example of a situation where overlaps are useful is when departments that are separated from each other need to use the same Internet gateway. In this example, the department VLANs should overlap the Internet VLAN but not each other.

VLANs that overlap each other share the same L2 broadcast domain. So using VLANs with overlaps will not lower the broadcast traffic across the overlap. A Layer 3 switch is required to route between two VLANs to completely separate the broadcast traffic.



VLAN Guide

1. Add VLANs to the network with the VLAN Definitions screen. Create one definition for each VLAN ID.
2. **Set which VLANs can see each other with the VLAN Overlaps screen.**
3. Configure what VLAN is assigned to every switch port on the VLAN End Points screen. Every port is assigned to only one VLAN. More specific end points take precedence over less specific end points.
4. Write the VLAN configuration to the switches using the Apply VLANs screen.

Current VLAN Overlaps

There are no Overlaps listed.

Add/Edit VLAN Overlaps

Overlap Name:

First VLAN: Default VLAN 1

Second VLAN: Default VLAN 1

Figure 12. VLAN Overlaps

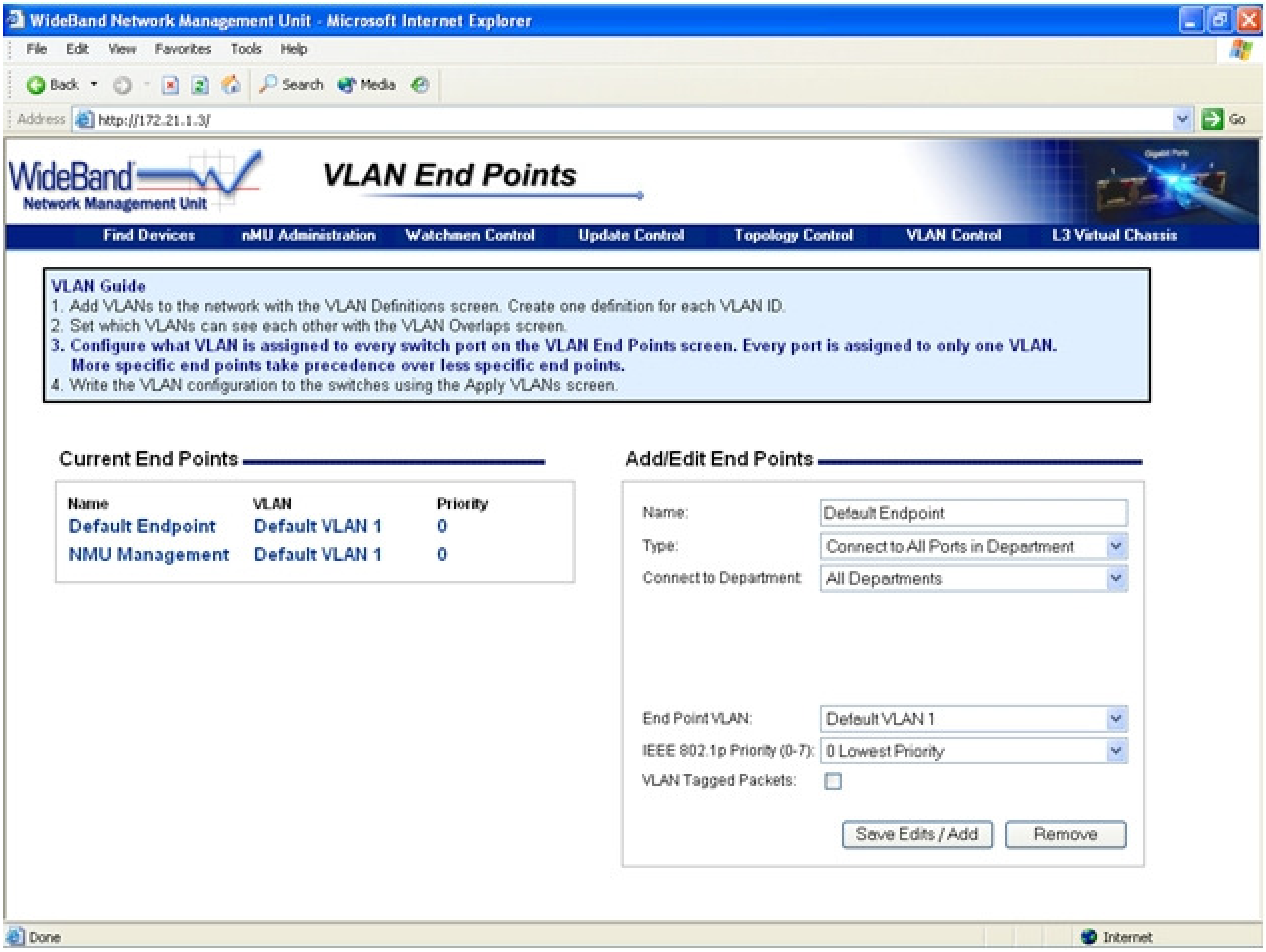
VLAN End Points

End points define what VLAN is assigned to each port (see Figure 13). Every endpoint can apply to a single port, or to a group of ports. It is often very useful to assign the same VLAN to several ports all as one group. The WideBand nMU will automatically connect all endpoints with the same VLAN ID using IEEE 802.1Q explicit VLAN tagging.

When more than one endpoint connect to the same port, the endpoint with the more specific connection type takes precedence. For example, an endpoint connected to a specific port takes precedence over an endpoint that connects to every port on that device. If two endpoints with the same connection type, but different VLAN IDs, apply to the same port, they will cause a conflict, and one of them will not be used.

The following table describes the configuration options for each endpoint:

Field Name	Description
Name	The name that will be assigned to this endpoint.
Type	The type of port grouping this end point is using
Connect to Department	Specifies the department this endpoint will apply to. (Only valid if the *Connect to Device*, *Connect to Port*, and *Connect to MAC Address* fields are empty)
Connect to Device	Specifies one device this endpoint will apply to. (Only valid if the *Connect to MAC Address* field is empty)
Connect to Port	Specifies a single port, or a range of ports, this endpoint will apply to. (Only valid if the *Connect to MAC Address* field is empty)
Connect to MAC Address	Specifies a single MAC address this endpoint will apply to. When the VLANs are applied, the nMU will search the network for the specified MAC address, and assign the endpoint to the port with that MAC address connected.
End Point VLAN	The VLAN this endpoint will assign to every port in its group.
IEEE 802.1p Priority	The VLAN priority that this endpoint will assign to incoming packets
VLAN Tagged Packets	Checked if the endpoint will transmit packets VLAN tagged


WideBand Network Management Unit - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Media
Address http://172.21.1.3/
Go
WideBand Network Management Unit
VLAN End Points
Find Devices
nMU Administration
Watchmen Control
Update Control
Topology Control
VLAN Control
L3 Virtual Chassis
Done
Internet

VLAN Guide
1. Add VLANs to the network with the VLAN Definitions screen. Create one definition for each VLAN ID.
2. Set which VLANs can see each other with the VLAN Overlaps screen.
3. **Configure what VLAN is assigned to every switch port on the VLAN End Points screen. Every port is assigned to only one VLAN. More specific end points take precedence over less specific end points.**
4. Write the VLAN configuration to the switches using the Apply VLANs screen.

Current End Points

Name	VLAN	Priority
Default Endpoint	Default VLAN 1	0
NMU Management	Default VLAN 1	0

Add/Edit End Points

Name: Default Endpoint

Type: Connect to All Ports in Department

Connect to Department: All Departments

End Point VLAN: Default VLAN 1

IEEE 802.1p Priority (0-7): 0 Lowest Priority

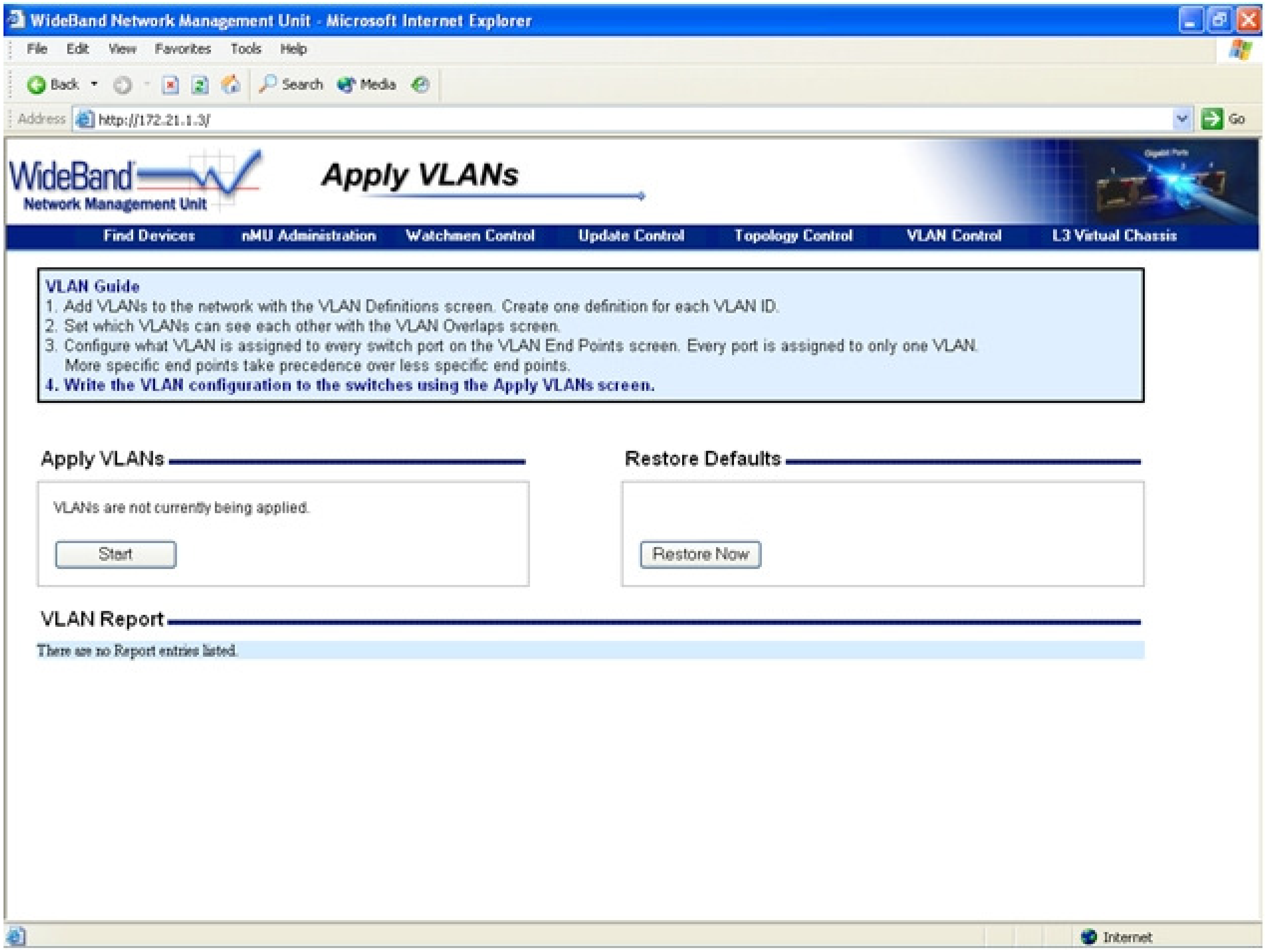
VLAN Tagged Packets: □

Save Edits / Add   Remove

Figure 13. The endpoints define how the VLANs on the network will be applied to each switch.

Warning: When managing the VLAN endpoints, make sure that your workstation will still be on the same VLAN as the nMU. Otherwise, when the new VLAN settings are applied, your PC will lose connection with the nMU.

Apply VLANs



VLAN Guide
1. Add VLANs to the network with the VLAN Definitions screen. Create one definition for each VLAN ID.
2. Set which VLANs can see each other with the VLAN Overlaps screen.
3. Configure what VLAN is assigned to every switch port on the VLAN End Points screen. Every port is assigned to only one VLAN. More specific end points take precedence over less specific end points.
4. **Write the VLAN configuration to the switches using the Apply VLANs screen.**

VLANs are not currently being applied.

There are no Report entries listed.

Figure 14. The nMU can apply VLAN settings in the background while you continue to use the management interface.

After all of the other VLAN screens have been configured, go to the *Apply VLANs* screen to write the new configurations to the network (See Figure 14). To begin applying the new VLAN settings, click the *Start* button. While the VLANs are configured in the background, you may continue to work on the nMU. The VLAN Report will show the status of the configuration as it runs. The report will also show details of where the endpoints connected, and what switches needed VLAN configuration changes.

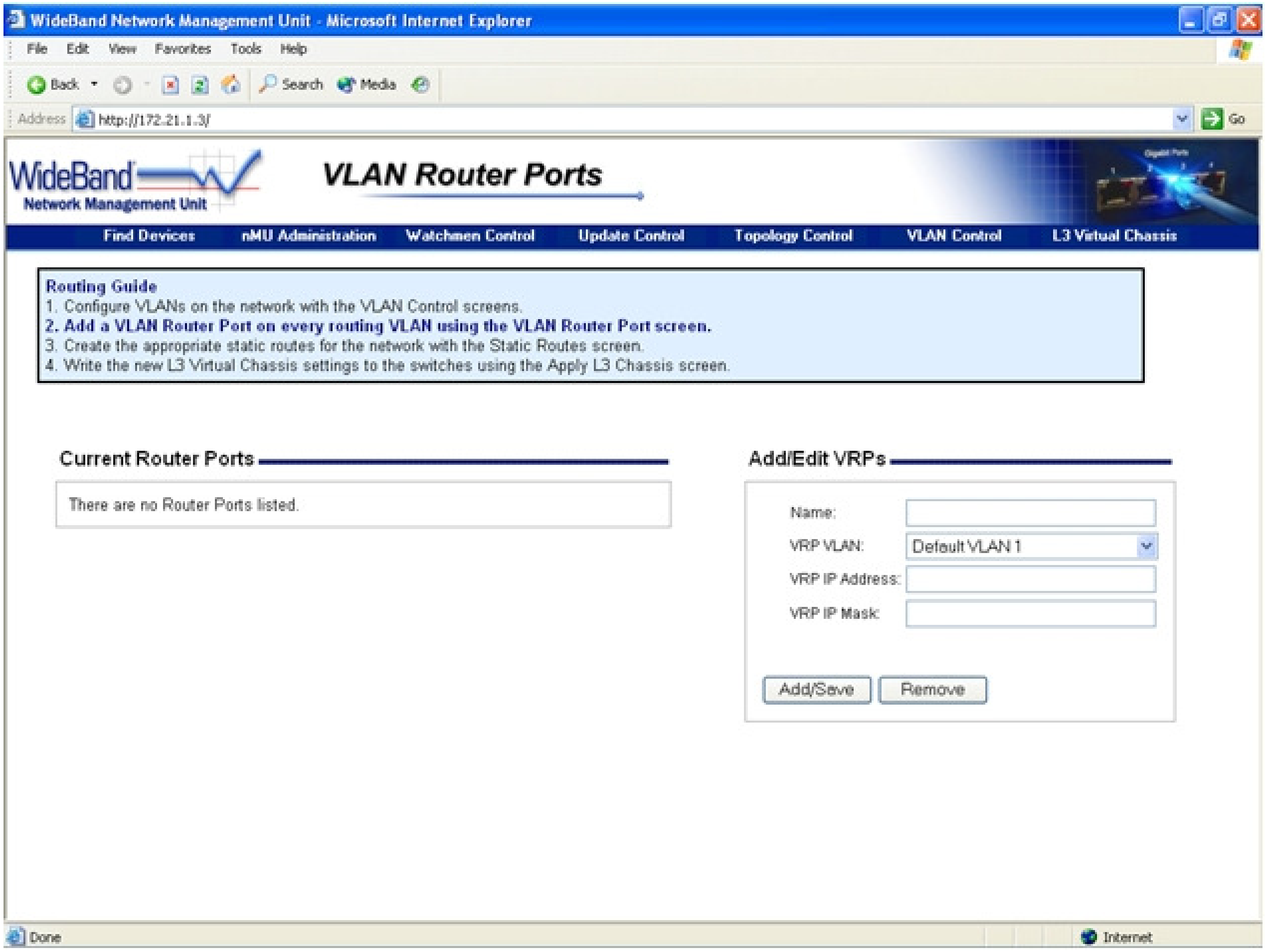
Layer 3 Virtual Chassis

The nMU can configure a group of WideBand Layer 3 switches to work together as one, more powerful L3 switch. This group of switches is known as a L3 Virtual Chassis. When a packet is routed through a Virtual Chassis the TTL is decremented only once (only one router hop). The L3 Virtual Chassis can be very useful for simplifying management of an Ethernet network with multiple L3 switches.

All L3 switches within the L3 Virtual Chassis must be connected to each other ether directly, or through another switch that is part of the Chassis. For example, the L3 switches cannot be connected together with a L2 switch in the middle of the chassis.

VLAN Router Ports

Instead of having physical router ports like conventional routers, the L3 Virtual Chassis has VLAN router ports each of which connects to a VLAN through every switch in the chassis. This powerful architecture makes it possible to easily add redundancy to a L3 network using the Spanning Tree protocol. Since the VLAN router ports connect to VLANs, they don't have to depend on any one L3 switch. If one L3 switch goes down, another L3 switch that is redundantly connected on the same VLAN can automatically take over.



Routing Guide
1. Configure VLANs on the network with the VLAN Control screens.
2. **Add a VLAN Router Port on every routing VLAN using the VLAN Router Port screen.**
3. Create the appropriate static routes for the network with the Static Routes screen.
4. Write the new L3 Virtual Chassis settings to the switches using the Apply L3 Chassis screen.

Current Router Ports

There are no Router Ports listed.

Add/Edit VRPs

Name:
VRP VLAN: Default VLAN 1
VRP IP Address:
VRP IP Mask:

Figure 15. There is up to one VLAN Router Port for each VLAN.

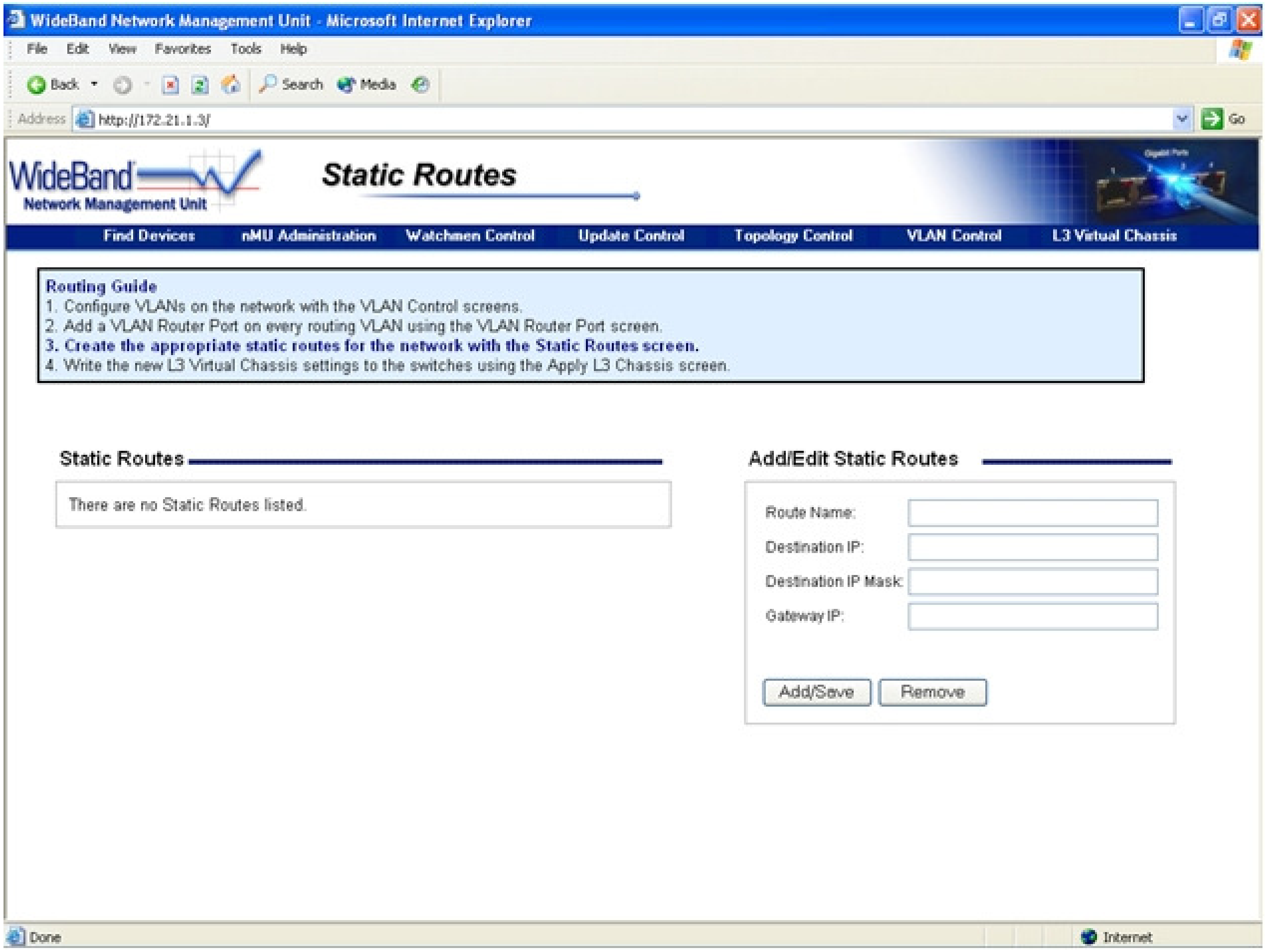
The following table describes what fields can be configured for each VLAN on the network:

Field Name	Description
Name	The name that will be assigned to this VLAN Router Port
VRP VLAN	The VLAN that this VLAN Router Port connects to
VRP IP Address	The IP address this VRP will use for routing
VRP IP Mask	The IP mask for the network this VRP is routing to

Static Routes

Static routes are needed for the L3 Virtual Chassis to communicate with other routers on the network. One common example of another router is an Internet gateway. The following table lists the fields that must be set for each static route:

Field Name	Description
Route Name	The name that you will used to identify this static route
Destination IP	The destination IP network address for this static route
Destination IP Mask	The IP mask of the destination IP network for this static route
Gateway IP	IP address of the next-hop gateway for this route



Routing Guide

1. Configure VLANs on the network with the VLAN Control screens.
2. Add a VLAN Router Port on every routing VLAN using the VLAN Router Port screen.
3. **Create the appropriate static routes for the network with the Static Routes screen.**
4. Write the new L3 Virtual Chassis settings to the switches using the Apply L3 Chassis screen.

Static Routes

There are no Static Routes listed.

Add/Edit Static Routes

Route Name:

Destination IP:

Destination IP Mask:

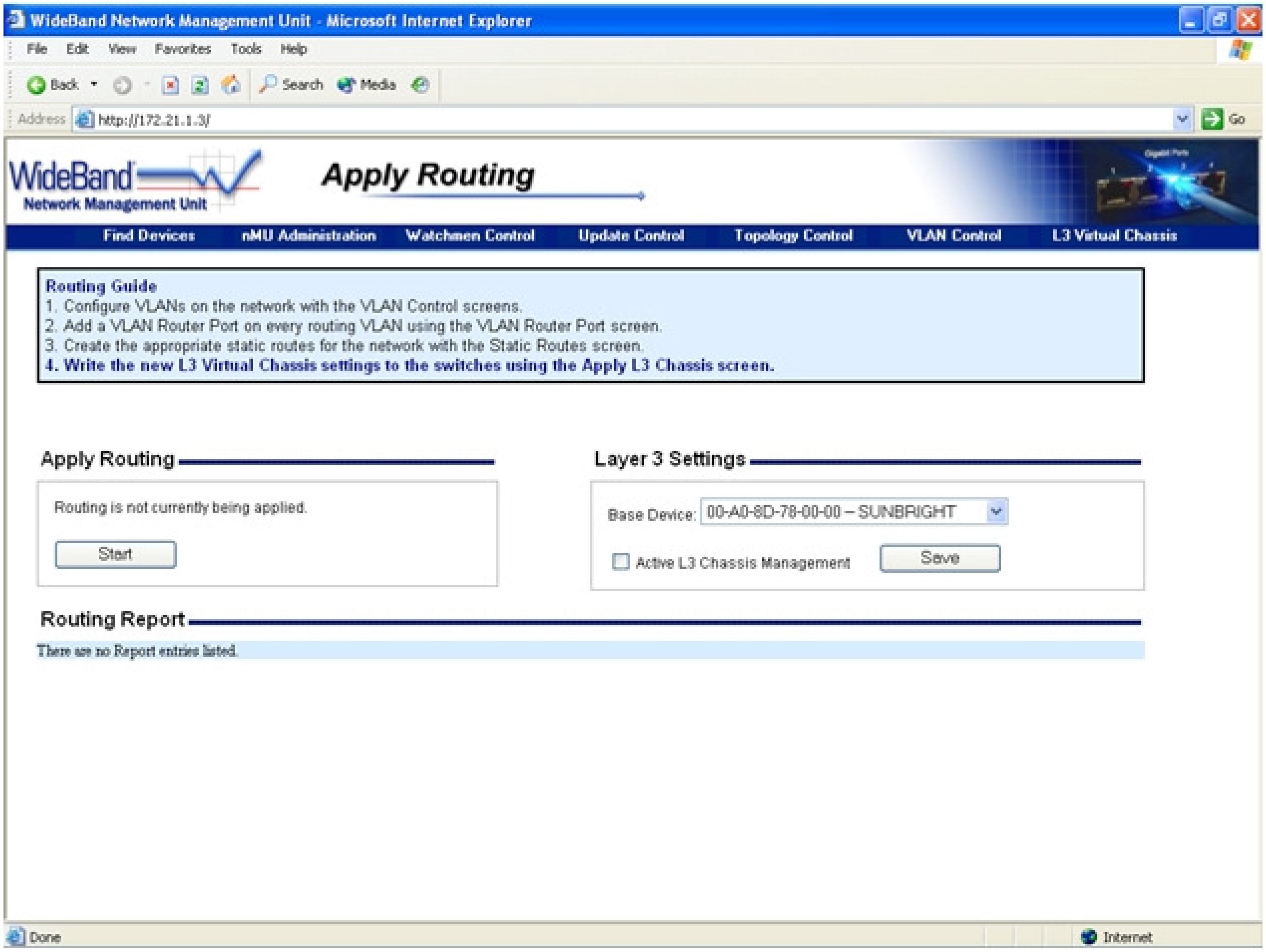
Gateway IP:

Figure 16. Static Routes

Apply Routing

After the L3 Virtual Chassis screens have been configured, the settings must be applied to the switches on the network. Press the *Start* button to begin applying the settings. When the nMU has finished writing the settings be sure to review the *Routing Report* to make sure there were no errors or warnings.

You may also want to select a *Base Device* for your L3 Virtual Chassis. The base device is the L3 switch that every switch in the chassis must be connected to, ether directly, or through another WideBand L3 switch. Also, you can enable *Active L3 Chassis Management*. When this is enabled the nMU will periodically apply the routing settings to make sure nothing needs to change. This is only useful if the network is being physically reconfigured often.


WideBand Network Management Unit - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Media
Address http://172.21.1.3/
Go
WideBand Network Management Unit
Apply Routing
Find Devices
nMU Administration
Watchmen Control
Update Control
Topology Control
VLAN Control
L3 Virtual Chassis

Routing Guide
1. Configure VLANs on the network with the VLAN Control screens.
2. Add a VLAN Router Port on every routing VLAN using the VLAN Router Port screen.
3. Create the appropriate static routes for the network with the Static Routes screen.
4. Write the new L3 Virtual Chassis settings to the switches using the Apply L3 Chassis screen.

Apply Routing

Routing is not currently being applied.

Start

Layer 3 Settings

Base Device: 00-A0-8D-78-00-00 – SUNBRIGHT

☐ Active L3 Chassis Management

Save

Routing Report

There are no Report entries listed.

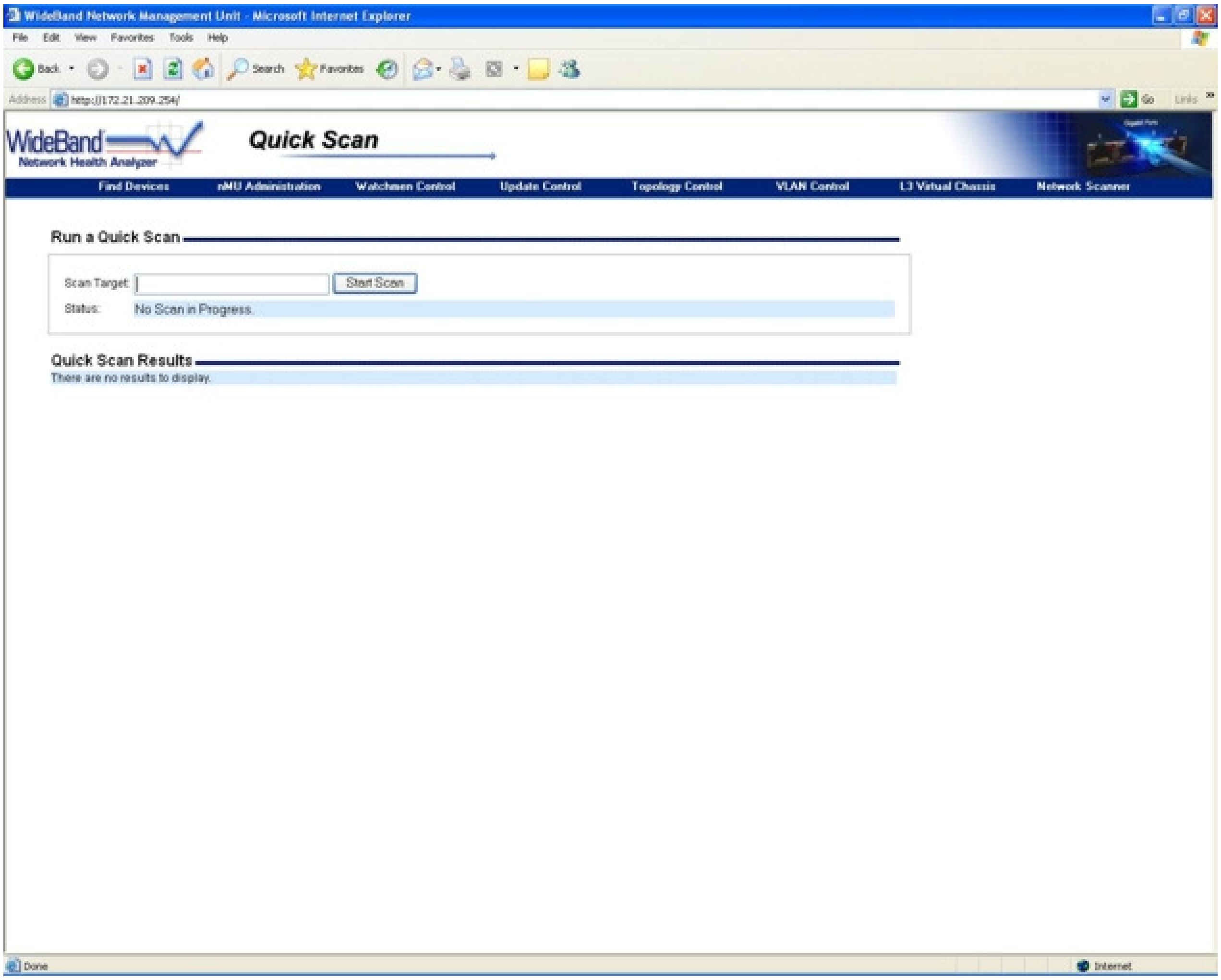
Figure 17. Apply Routing

nMU Network Scanner

The Network Scanner is a quick and comprehensive method of scanning your network for security vulnerabilities. There are two main components to the Network Scanner: the Quick Scan, and the Security Scan.

The Quick Scanner

The Quick Scanner is an easy way of discovering which IP addresses are currently being used on your network. The report it generates gives as much information as the scanner was able to retrieve. This may include not only the IP address, but also the target's hostname, MAC address, and the registered name for that MAC address (i.e. the motherboard manufacturer).



Run a Quick Scan

Scan Target:

Status: No Scan in Progress.

Quick Scan Results

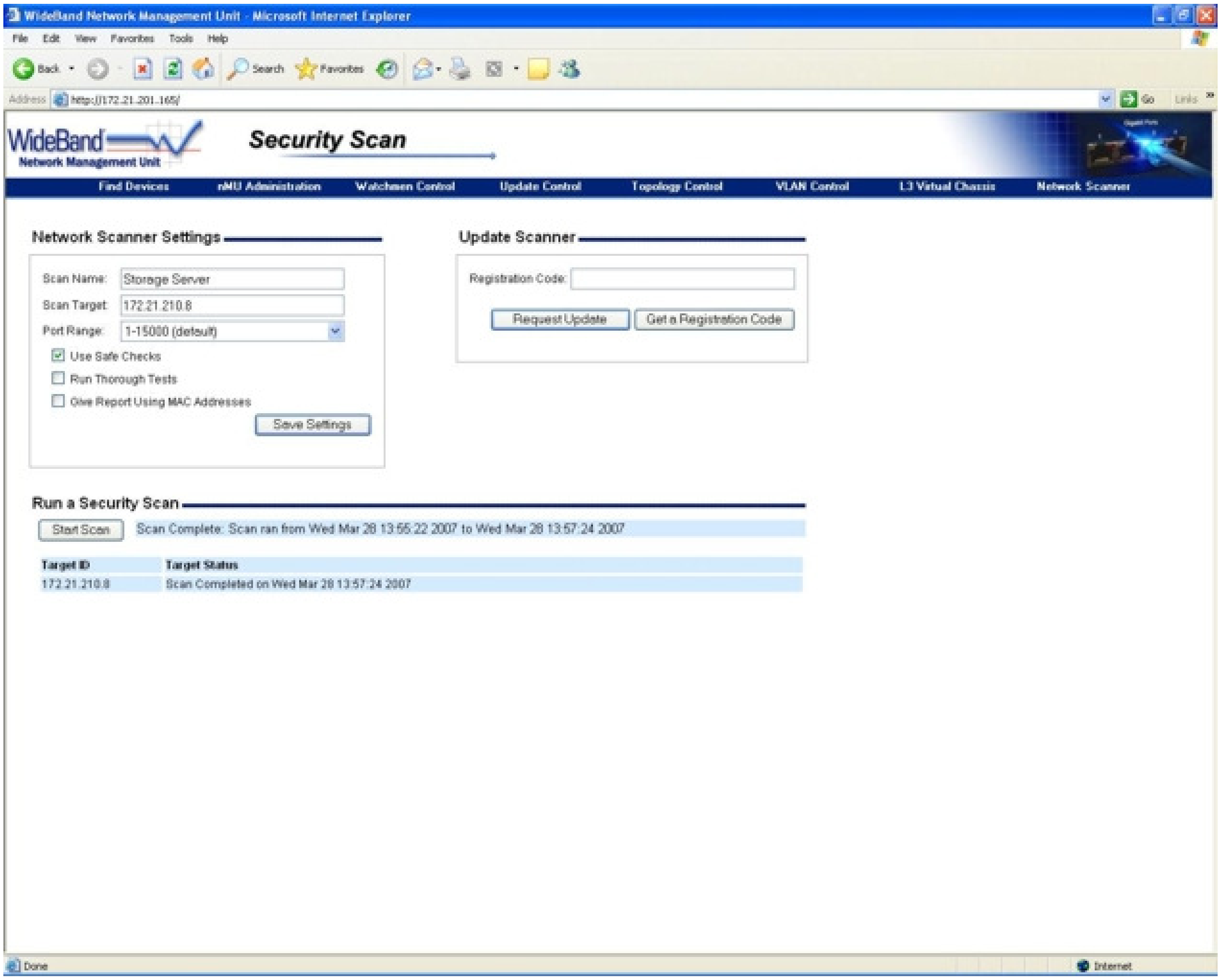
There are no results to display.

Figure 18. Quick Scan

Running a Security Scan

The Security Scan can be used to search for security vulnerabilities on the network. All the options and configurations available for the Network Scanner are located on the Security Scan screen. Here you will find six scanning options:

Option Name	Description
Scan Name	The name can be used to help identify this report on the Scan Reports screen.
Scan Target	The IP address(es) that you wish to scan for security vulnerabilities
Port Range	The range of TCP and UDP ports to include in the port scan
Safe Checks	Only run the safe vulnerability checks during Network Scans
Thorough Tests	Run more extensive and even slower tests during Network Scans
Use MAC Addresses	Identify all targets by their MAC ID instead of their IP address in the Network Scanner reports



Scan Name: Storage Server

Scan Target: 172.21.210.8

Port Range: 1-15000 (default)

☑ Use Safe Checks

□ Run Thorough Tests

□ Give Report Using MAC Addresses

Registration Code:

Scan Complete: Scan ran from Wed Mar 28 13:55:22 2007 to Wed Mar 28 13:57:24 2007

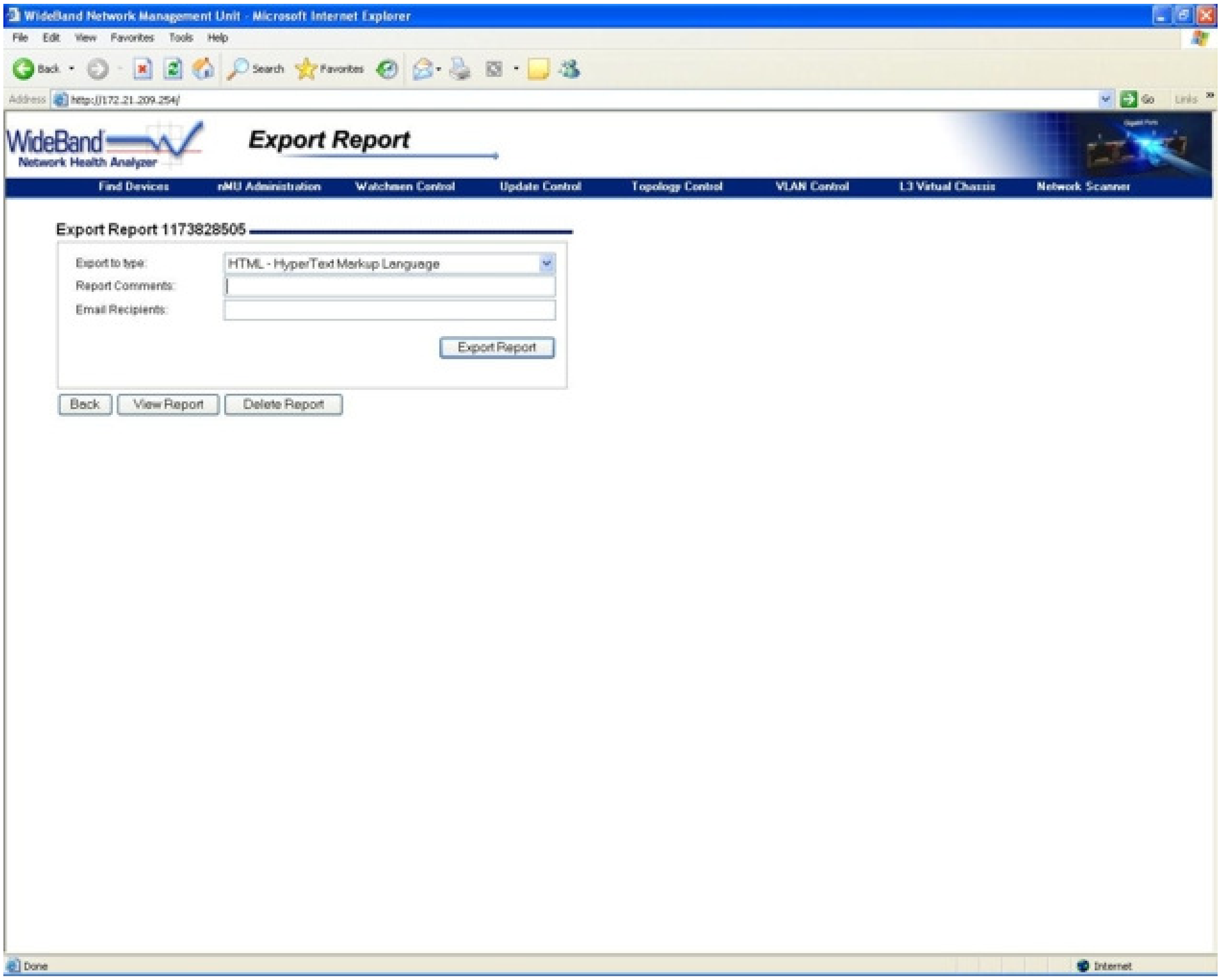
Target ID	Target Status
172.21.210.8	Scan Completed on Wed Mar 28 13:57:24 2007

Figure 19. Security Scan

Exporting a Report

Every Network Scan generates a vulnerability report and is given a unique Report ID. On the Scan Reports screen, you may click on any report and view, delete, or export it. This screen also allows you to search existing reports by the Report ID, the Targets specified, or by the number of holes, warnings, or notes found during the scanning process.

Reports can be exported to any of the following formats: html, xml, nsr, or nbe. The exported file is then sent to any email addresses specified.



http://172.21.209.254/

Export Report 1173828505

Export to type: HTML - HyperText Markup Language

Report Comments:

Email Recipients:

Figure 20. Export Report

Updating your Network Scanner

In order to update your Network Scanner, you will need to register. There is a button on the Security Scan page that will take you to a page with information about the different kinds of updates you can receive.

Once you have registered, enter your registration code into the appropriate field on the Security Scan page. This will run an update on your Network Scanner, and updates will run automatically from then on.

WideBand Switch Management

Device Control

When a switch that is controlled by the nMU is selected from the Device List, the Device Control screen for that switch is loaded (See Figure 21).

Device Identification

Every switch can be assigned a Name, Contact, Location, and Description. Modifications to these fields are saved when the *Save Changes* button below them is pressed. The Department field is displayed here, but can only be modified by using the *Password/Department* button, also found on this screen (See the *Change Password and Department* section).

IP Management Settings

Every managed WideBand switch can be assigned a management IP address. This address can optionally be used for SNMP management.

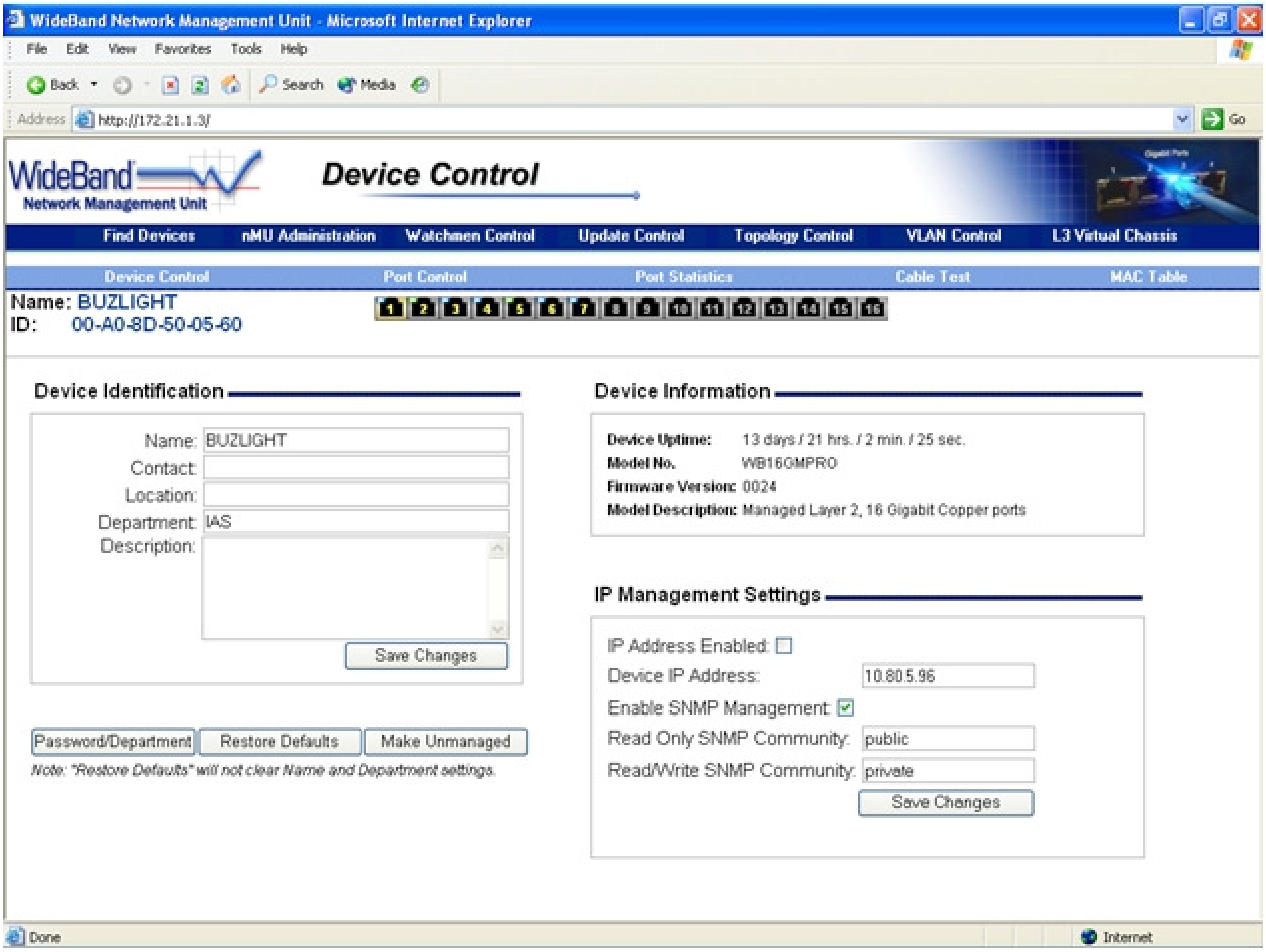
SNMP Communities

SNMP communities are like passwords to authenticate any management entity. The management entity must know the community name in order to have access to any of the SNMP management features. The WideBand Professional Series Switches support the two following communities:

- Read-only Community
- Read-write Community

This separation can be useful to allow public read access to the switch, but limit write access to authorized users only. It is strongly recommended that you change the *Read-write* community immediately. Otherwise, any unauthorized user will be capable of reconfiguring the switch. Always be sure to follow any changes by pressing the *Save Changes* button.

> ***Note:*** *The WideBand Professional Series Switches are not as secure with SNMP enabled regardless of what value is set to the community names. If you are not planning to use SNMP in the near future, we recommend that you keep it disabled by unselecting the Enable SNMP Management check box.*



Name: BUZLIGHT
ID: 00-A0-8D-50-05-60

Device Identification

Name: BUZLIGHT
Contact:
Location:
Department: IAS
Description:

Note: "Restore Defaults" will not clear Name and Department settings.

Device Information

Device Uptime: 13 days / 21 hrs. / 2 min. / 25 sec.
Model No. WB16GMPRO
Firmware Version: 0024
Model Description: Managed Layer 2, 16 Gigabit Copper ports

IP Management Settings

IP Address Enabled: □
Device IP Address: 10.80.5.96
Enable SNMP Management: ☑
Read Only SNMP Community: public
Read/Write SNMP Community: private

Figure 21. The Device Control screen is the central for managing individual devices on the network.

Change Password and Department

The *Password/Department* button leads to the *Change Password and Department* screen (See Change Password and Department), which allows you to change the selected switch's department membership. After you have entered a new password and department, the nMU will apply the correct department settings to the switch. Note that only users with write access to all departments can change the password and department of a switch.

Restore Defaults

In some cases it is useful to clear out any management settings on the switch and start over with the factory defaults. This can be accomplished by clicking the *Restore Defaults* button.

> ⚠ **Warning:** Restoring factory defaults will cause all configuration data to be lost. If the current configurations are required for proper communication with the switch, like specific VLAN settings, the switch may become inaccessible over the network.

***Note:** Restoring factory defaults will not clear the Device Identification settings.*

Make Unmanaged by nMU

The nMU will periodically read statistics and status information from every switch it is managing.

The *Make Unmanaged* button can be used to discontinue the nMU management for the selected switch. When the nMU stops managing a device, it simply forgets the device's password, and none of the management settings on the device are changed. Therefore, in order to manage the device over the network again, you will need to manually remember what password was assigned to it (See Making Devices Managed by nMU).

Port Control

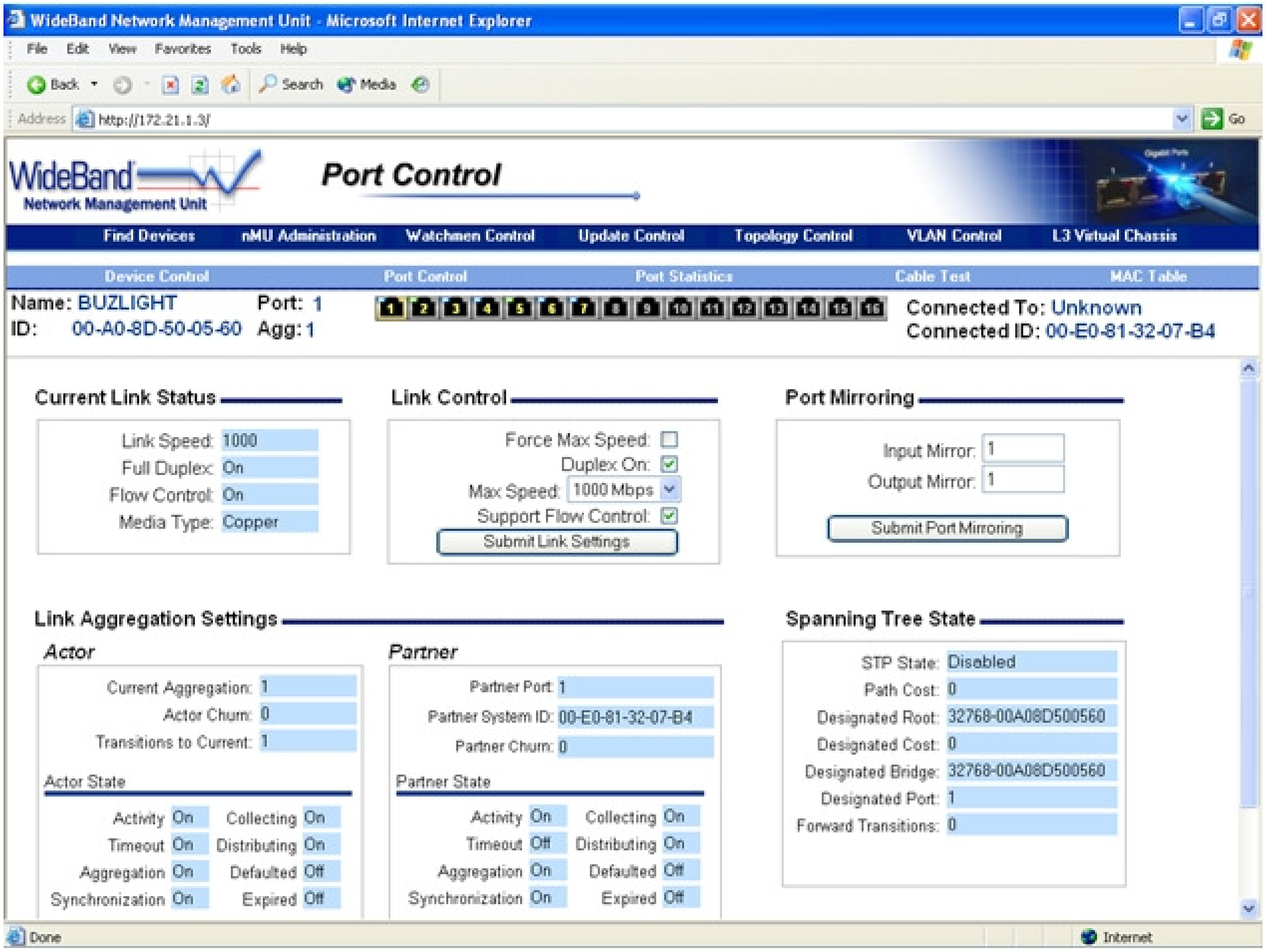
On the Port Control screen you will be able to do the following:

- Get a quick look at the status of every port
- View current link status details for each port
- Configure link status details for each port
- View and configure Port Mirroring status for each port
- View Link Aggregation status for each port
- View the Spanning Tree state of each port

At the top of the Port Control display you will find the name and ID of the device, the number of the port whose information is currently being displayed, and a "Current Status" bar. Also, to the right of the current status bar is information about the device this port is connected to.

You will find the Current Status bar at the top of several management screens. It is used to display the basic status of every port on the currently selected device. Since it updates every time you enter any of the four Device Control screens (*Device Control, Port Control, Port Statistics,* and *MAC Table*), the Current Status bar is a good way to see what ports are linked at any given moment. Click on the menu link to any of these screens, or click on any of the port numbers on the Current Status bar itself to update it immediately. The color representation of each port light relates to the link indicators on the switch as expressed in the following table:

Light	Font Color	Meaning
No light displayed	Grey	Port is not linked
Green light displayed	Yellow	Port is linked and is running at 10/100 Mbps
Blue light displayed	Yellow	Port is linked and is running at 1 Gbps



Name: BUZLIGHT
ID: 00-A0-8D-50-05-60
Port: 1
Agg: 1
Connected To: Unknown
Connected ID: 00-E0-81-32-07-B4

Current Link Status

Link Speed: 1000
Full Duplex: On
Flow Control: On
Media Type: Copper

Link Control

Force Max Speed: □
Duplex On: ☑
Max Speed: 1000 Mbps
Support Flow Control: ☑

Port Mirroring

Input Mirror: 1
Output Mirror: 1

Link Aggregation Settings

Actor

Current Aggregation: 1
Actor Churn: 0
Transitions to Current: 1

Actor State

Activity	On	Collecting	On
Timeout	On	Distributing	On
Aggregation	On	Defaulted	Off
Synchronization	On	Expired	Off

Partner

Partner Port: 1
Partner System ID: 00-E0-81-32-07-B4
Partner Churn: 0

Partner State

Activity	On	Collecting	On
Timeout	Off	Distributing	On
Aggregation	On	Defaulted	Off
Synchronization	On	Expired	Off

Spanning Tree State

STP State: Disabled
Path Cost: 0
Designated Root: 32768-00A08D500560
Designated Cost: 0
Designated Bridge: 32768-00A08D500560
Designated Port: 1
Forward Transitions: 0

Figure 22. The Port Control screen shows the link configuration for a single port on a managed device.

From the Device Control, Port Control, and MAC Table screens, clicking on any port on the Current Status bar will bring up the Port Control screen for that port. From the Port Statistics screen, clicking on a port will bring up the Port Statistics screen for that port.

Current Link Status

Next on the Port Control screen is more detailed information about each port. The *Current Link Status* portion of the screen indicates whether the port is linked and provides details about the current link. Remember that the current link details will be determined by the link information of both the port and the link partner at the other end of the wire. These details are listed and explained in the following table:

Name	Description
Link Speed	Link speed of the port in Megabits per second (0 if not linked)
Media Type	The type of media this port is using (Copper or Fiber)
Full Duplex	Link Duplex status of this port: On indicates *Full Duplex:* Send and receive data simultaneously *(Best Performance)* Off indicates *Half Duplex:* Data moves only one direction at a time

Flow Control	Flow Control status on link: *On:* Flow Control is enabled on both sides of the link *(Best Performance)* *Off:* Flow Control is disabled on one or both sides of the link

Link Control

The *Link Control* portion of the Port Control screen allows the user to set new link information for each of the ports, as described in the following table:

Setting	Options	Description
Force Max Speed	Checked	Force link settings; auto-negation is disabled so all settings must be entered manually
	Unchecked	Port will automatically negotiate with link partner for best link settings *(Recommended)*
Duplex On	Checked	Full Duplex – Send and receive data simultaneously *(Best Performance)*
	Unchecked	Half Duplex – Data moves in only one direction at a time
Max Speed	10	Advertise a max speed of 10Mbps
	100	Advertise a max speed of 100Mbps
	1000	Advertise a max speed of 1000Mbps (only on gigabit ports)
	Disabled	Port is disabled and will not link
Note: Only actually available speeds for this port are shown in the pull-down list.		
Support Flow Control	Checked	Support Flow Control on this side of the link *(Best Performance)*
	Unchecked	Don't support Flow Control

Make sure that any changes you make are saved to the device by clicking the *Submit Link Settings* button before closing the screen or clicking on any other submit buttons on this screen. If any of the new settings would cause the nMU to lose its ability to communicate with the device, the nMU will detect the error, and revert back to the former settings. This is a feature built into the WideBand Management Protocol to protect the user from an accidental management lockout. However, it is possible to disable the port through which your computer is connected to the nMU. In this case, you would have to move your computer's connection to a port that has not been disabled in order to use the same computer to continue managing the network.

Port Mirroring

Port Mirroring is a powerful tool used for monitoring and debugging the network. It works by duplicating all network traffic moving in or out of one port, called the *Monitored Port*, to another port, called the *Mirror Port*. This allows the network administrator to monitor any port's traffic during normal operation.

As shown in Figure 22, each port has an *Input Mirror* and an *Output Mirror* field. So each Monitored Port can have two Mirror Ports. When the Mirrored Port is the same as the Monitored Port the Mirroring function is disabled. In Figure 22, both the Input and the Output Mirror are disabled. Be sure to save all changes before closing the screen by clicking on *Submit Port Mirroring*.

Link Aggregation Settings

Link Aggregation, also known as Port Trunking, is the ability to set up multiple network ports on a device to work together as one higher-bandwidth link. The WideBand Professional Series Switches use the IEEE 802.3ad Link Aggregation Control Protocol (LACP) to automatically configure the ports in this manner. This feature is enabled by default on the Professional Series Switches, and up to 16 ports can be connected in one aggregate.

When managing LACP keep in mind that the switch we are currently managing is referred to as the *Actor*, while the device at the other end of the aggregate is referred to as the *Partner*. This means that if we were to go manage the device on the other end, these names would reverse.

The Port Control screen displays two boxes with different *Link Aggregation* settings. These are the *Actor* and *Partner* boxes. These both relate to a single port on the switch, which can be selected by clicking on the port in the *Current Status* bar at the top of the screen. These boxes are described with more detail in the following tables:

Actor Box Data

Field Name	Description
Current Aggregation	The ID of the aggregate which this port is currently a member of (The aggregate ID is the same as the lowest-numbered port in the aggregate). All ports that are in the same aggregate as the selected port will show up gold on the port status bar at the top of the screen.
Actor Churn	An Actor Churn occurs when the port's aggregation status fails to stabilize
Transitions to Current	The number of valid aggregations this port has had since power up
Actor State	This port's current Aggregation State (described with more detail in the *Aggregation State Bits* table, below)

Partner Box Data

Field Name	Description
Partner port	Port number on the Partner to which we are connected
Partner System ID	Aggregation ID of the Partner (Based on the Partner's MAC address)
Partner Churn	A Partner Churn occurs when the Partner aggregation status fails to stabilize
Partner State	Partner's current Aggregation State (described with more detail in the *Aggregation State Bits* table, below)

Aggregation State Bits

Bit Name	Status	Description
Activity	On Off	Running in Active LACP mode (always sends LACPDUs) Running in Passive LACP mode (only sends LACPDUs when a Partner is detected)
Timeout	On Off	Using Short Timeout (3 seconds) Using Long Timeout (90 seconds)

Aggregation	On Off	This link is considered *Aggregate-able* (ready to trunk) This link is considered *Individual* (will never join a trunk)
Synchronization	On Off	Link is in sync, and is a member of a valid aggregate Link is out of sync (reconfiguring aggregation)
Collecting	On Off	Traffic received on this link will be accepted Traffic from this link will be discarded
Distributing	On Off	This link is ready to send data This link is not yet ready to send data
Defaulted	On Off	No Partner is detected, so default values are in use A valid Partner is running on the other end of the link
Expired	On Off	Partner has not responded for *Timeout* time, and this link is getting ready to go to the default Partner values. A recent response from the Partner has been received

For more information on Link Aggregation, please see Link Aggregation under Department Topology Settings*,* later in this manual.

Spanning Tree State

Ethernet networks are normally susceptible to traffic loops. Such loops occur when a user accidentally connects ports in such a way that data gets stuck in an endless path. The loop will continue to collect traffic until it crashes the entire network with a packet storm. To resolve this potentially serious problem IEEE developed the Spanning Tree Protocol (IEEE 802.1D). This protocol monitors each link, and disables any that create loops. This feature comes at the small cost of a 45-second delay that begins when the port links and continues until it starts passing data. The purpose of this delay is to allow Spanning Tree to check for loops on the link before enabling it. On the WideBand Professional Series Switches, Spanning Tree is disabled by default.

Spanning Tree is also occasionally used for redundancy since multiple paths can be connected between two points. If one path is lost, the other will start working.

The Port Control screen displays several Spanning Tree settings for each port. These settings are described in the following table:

Setting	**Description**
STP State	This port's Spanning Tree State: *Blocking:* To stop a loop, Spanning Tree is preventing this Port from passing data *Listening:* Preparing to participate in frame relay *Learning:* Learning MAC addresses, but data is not forwarding *Forwarding:* Participating in frame relay *(Normal Operation)* *Disabled:* Spanning Tree is disabled on this port, or port is not linked
Path Cost	The Cost that will be added to traffic on this link
Designated Root	The unique Bridge Identifier of the Bridge assumed to be the Root by this port
Designated Cost	The path cost this port offers to the Root
Designated Bridge	The unique Bridge Identifier of the Bridge that this port uses to reach the Root
Designated Port	The port on the Designated Bridge which is this port's path to the Root

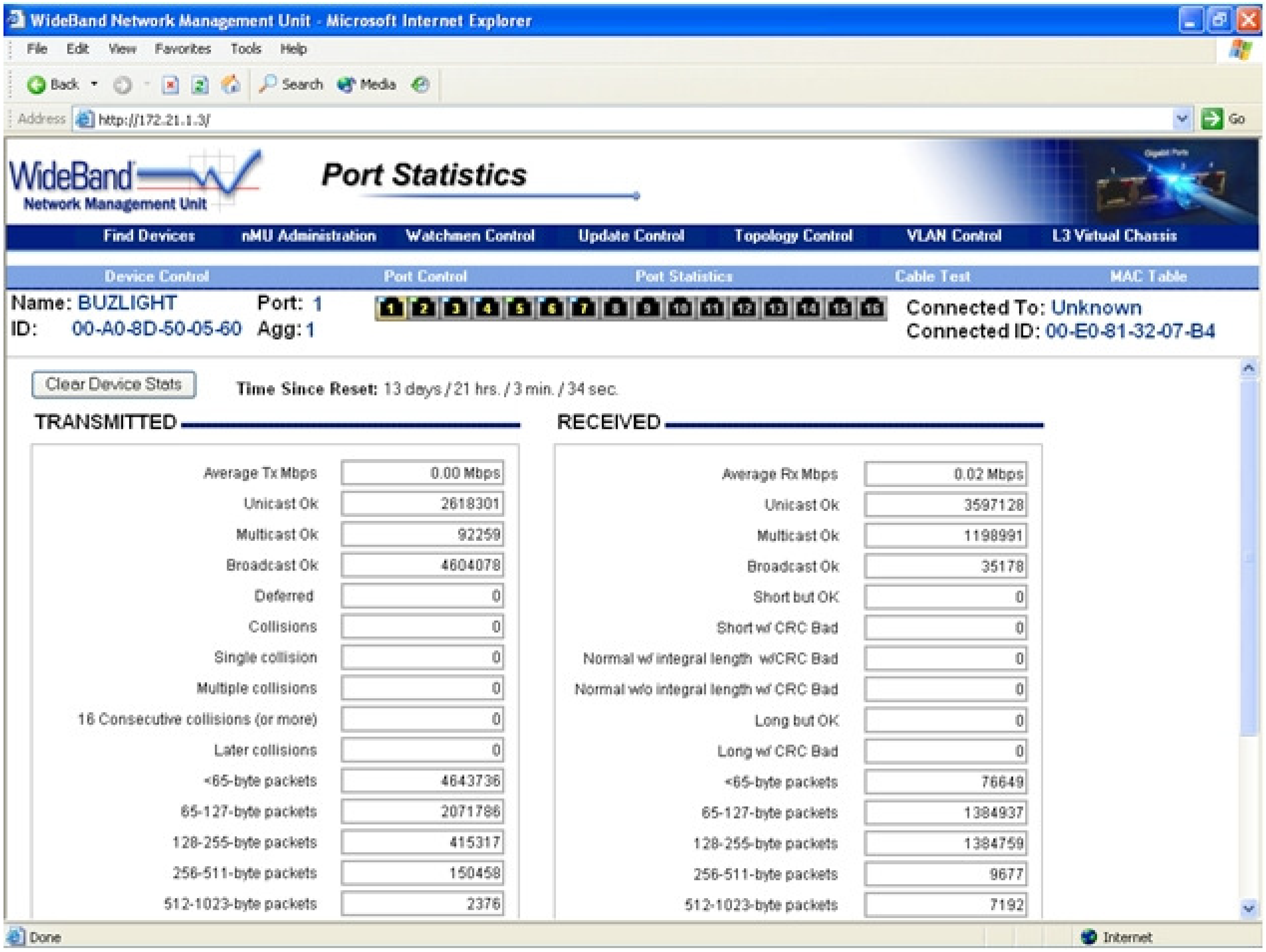
Forward Transitions	A counter of how many times this port has advanced to the Forwarding State

Port Statistics

The *Port Statistics* screen displays the “quick view” Current Status bar (described above), and provides 39 RMON statistics for each port. After clicking on *Port Statistics* on the Menu Bar, to access the statistics for a given port, click on the port number on the Current Status bar. The port’s statistics will appear in the fields below the bar, as shown in Figure 23.

The statistics displayed in the *Port Statistics* screen reflect how efficiently data is being transferred through each port, and provide information to help determine what is causing any delays that might be observed. Move the mouse over the name of any counter to get a more detailed description at the bottom of the screen. A few words of explanation might also be helpful:

- *Unicast Packets* are packets that are addressed to go to a single, specified destination.
- *Multicast Packets* are packets addressed in such a way that anyone who “tunes in” may receive them much like an AM Radio signal is broadcast to that group of people who have AM Radio receivers.
- *Broadcast Packets* are packets addressed to go to every device connected to the network.
- *CRC Errors* refer to errors in the checksum that is done to ensure that an error-free packet has been received.
- According to the Ethernet Standard, when a collision occurs, the Ethernet network will retry as many as 16 times to resend the packet. If the system cannot get the data through in 16 attempts, it will stop trying.



Name: BUZLIGHT Port: 1
ID: 00-A0-8D-50-05-60 Agg: 1

Connected To: Unknown
Connected ID: 00-E0-81-32-07-B4

Time Since Reset: 13 days / 21 hrs. / 3 min. / 34 sec.

TRANSMITTED

Average Tx Mbps	0.00 Mbps
Unicast Ok	2618301
Multicast Ok	92259
Broadcast Ok	4604078
Deferred	0
Collisions	0
Single collision	0
Multiple collisions	0
16 Consecutive collisions (or more)	0
Later collisions	0
<65-byte packets	4643736
65-127-byte packets	2071786
128-255-byte packets	415317
256-511-byte packets	150458
512-1023-byte packets	2376

RECEIVED

Average Rx Mbps	0.02 Mbps
Unicast Ok	3597128
Multicast Ok	1198991
Broadcast Ok	35178
Short but OK	0
Short w/ CRC Bad	0
Normal w/ integral length w/CRC Bad	0
Normal w/o integral length w/ CRC Bad	0
Long but OK	0
Long w/ CRC Bad	0
<65-byte packets	76649
65-127-byte packets	1384937
128-255-byte packets	1384759
256-511-byte packets	9677
512-1023-byte packets	7192

Figure 23. The Port Statistics screen shows 39 counters plus the average transmit and receive bandwidths of one port.

Clearing Statistics

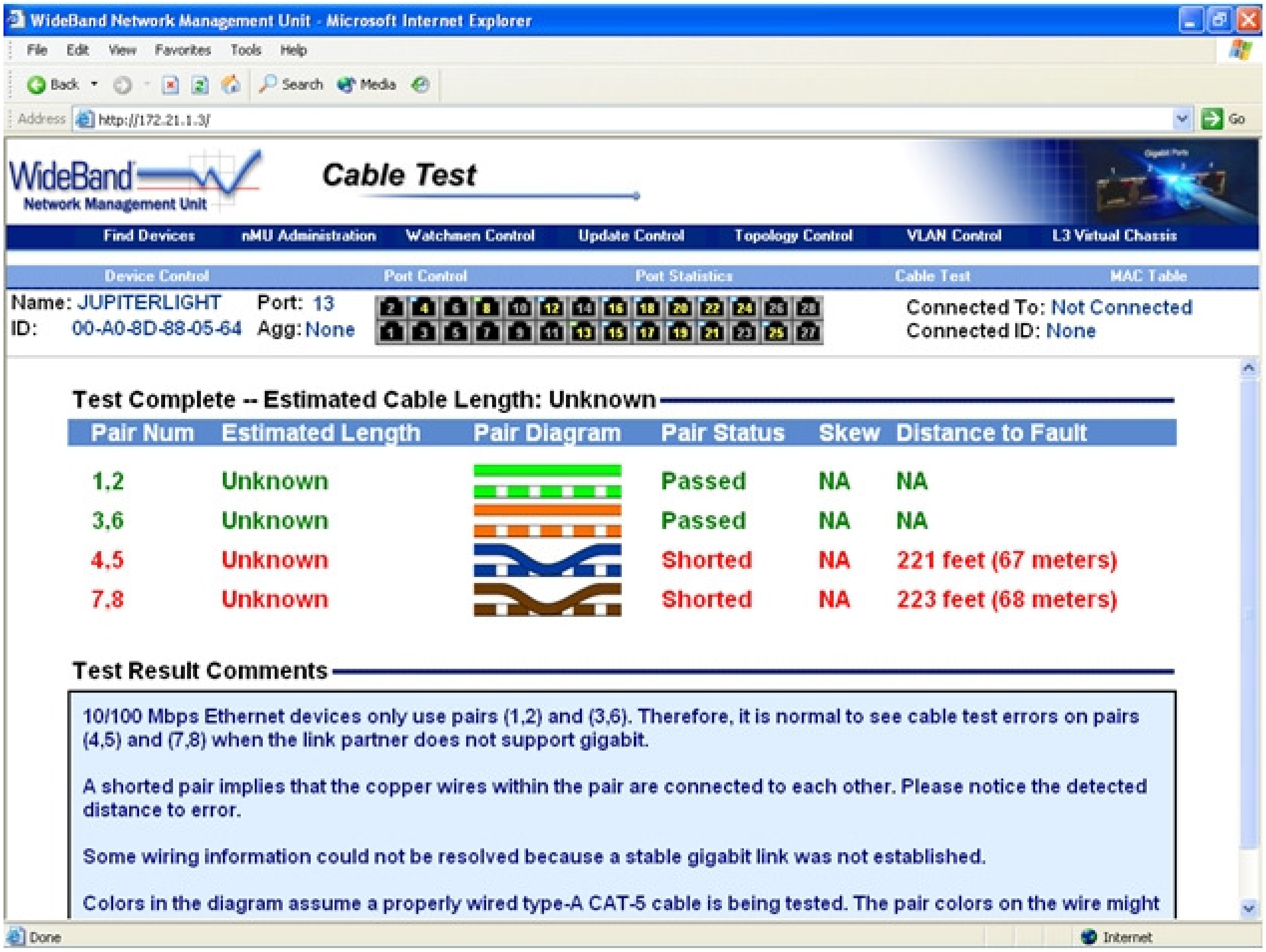
At the top of the screen there is a button for clearing the Statistics: *Clear Device Stats*. Clicking on *Clear Device Stats* will "zero out" all the statistics for all of the ports on the device.

Cable Test Screen

The nMU, in conjunction with the WideBand Professional Series Switches, supports cable testing on all gigabit copper ports. This cable test includes the following features:

- Ability to detect any shorts or cuts in each pair
- Ability to detect any serious impedance mismatch on each pair
- Ability to detect any polarity mismatch on each pair
- Calculates the distance to point of failure on the wire
- Measures skew in nano seconds between the pairs
- Generates cable length estimation

When the Cable Test screen is selected in the menu, the nMU will start testing the cable connected to the currently selected port. Once the test is complete, the Cable Test screen will show the wiring information for that port as shown in Figure 24. Interactive notes are displayed at the bottom of the screen based on the test results. These notes can be very helpful for understanding what the results mean. The following table describes the fields in the pair status diagram:



Name: JUPITERLIGHT Port: 13
ID: 00-A0-8D-88-05-64 Agg: None

Connected To: Not Connected
Connected ID: None

Test Complete -- Estimated Cable Length: Unknown

Pair Num	Estimated Length	Pair Diagram	Pair Status	Skew	Distance to Fault
1,2	Unknown		Passed	NA	NA
3,6	Unknown		Passed	NA	NA
4,5	Unknown		Shorted	NA	221 feet (67 meters)
7,8	Unknown		Shorted	NA	223 feet (68 meters)

Test Result Comments

10/100 Mbps Ethernet devices only use pairs (1,2) and (3,6). Therefore, it is normal to see cable test errors on pairs (4,5) and (7,8) when the link partner does not support gigabit.

A shorted pair implies that the copper wires within the pair are connected to each other. Please notice the detected distance to error.

Some wiring information could not be resolved because a stable gigabit link was not established.

Colors in the diagram assume a properly wired type-A CAT-5 cable is being tested. The pair colors on the wire might

Figure 24. Cable Test Screen

Name	Description
Pair Num	Pin numbers for the wires in this pair
Estimated Length	Estimated length for this pair
Pair Diagram	A graphic that describes this pair’s status
Pair Status	The detected status of this pair
Skew	The timing skew of this pair relative to other pairs
Distance to Fault	Estimated distance to the cable failure, if any

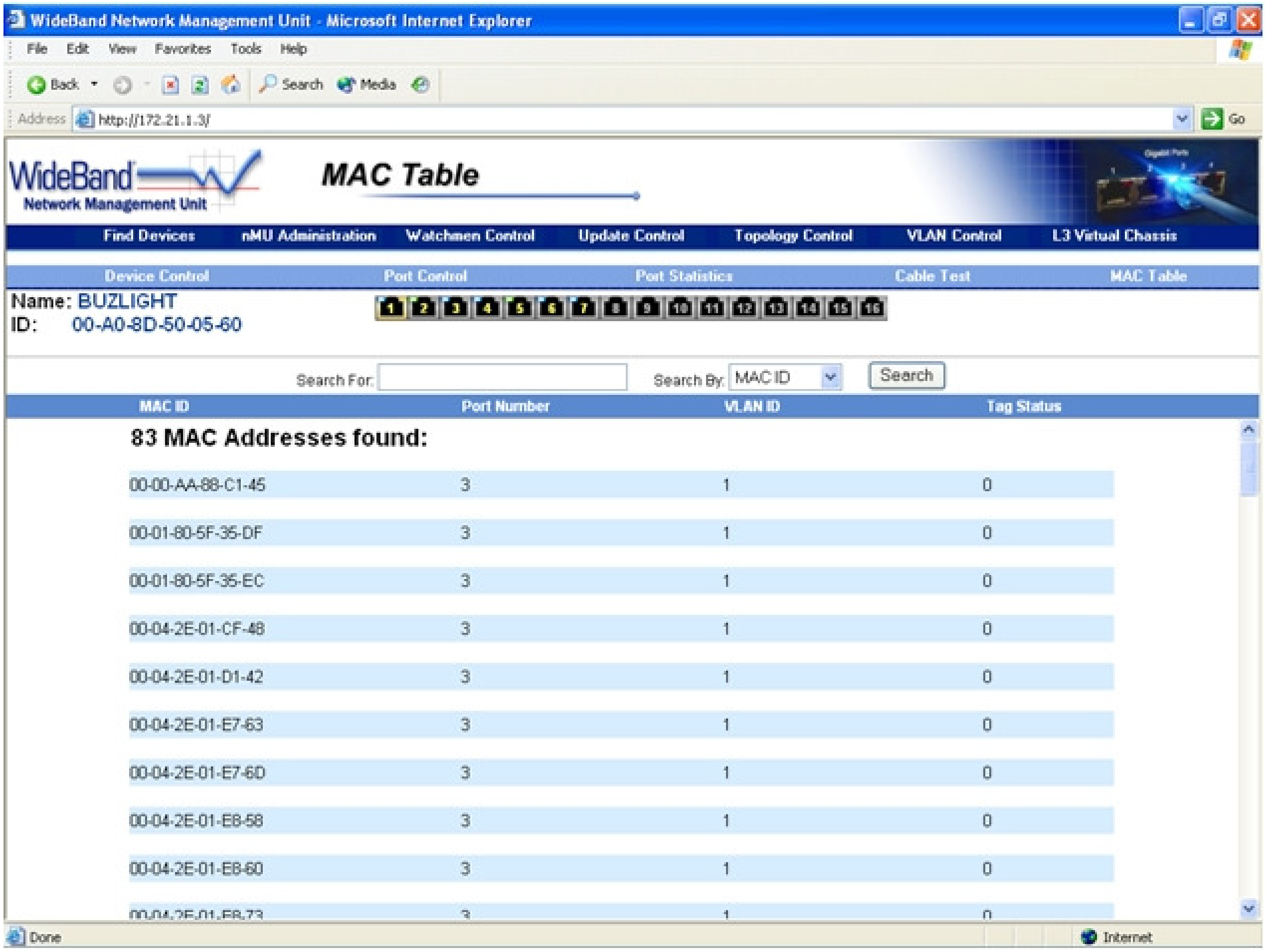
Warning: While a cable is being tested, the link will momentarily stop passing data. Therefore, it is important to verify that temporary loss of service is acceptable on the link before starting the cable test. Remember that this momentary down time is much less than what you would experience if you had to connect a hardware tester.

Note: *Some of the older WideBand switches do not support the full cable test, and cannot be upgraded in the field. Also, cable testing is not supported on switch ports that do not support gigabit. For more information on what your switches support, please contact customer support.*

MAC Table

Every Ethernet switch must build and maintain a MAC address-forwarding table. This table is used to determine what port the incoming traffic should be forwarded to. An entry in the table is created every time a packet with a new source MAC address is received in the switch. Each table entry keeps track of the following information about that packet:

- The source MAC address of the packet (a unique six byte value assigned to the Ethernet MAC which generated the packet)
- What port number the packet was received on
- The VLAN ID that was assigned to the packet
- Whether or not the received packet had a VLAN tag



Address: http://172.21.1.3/

MAC Table

Name: BUZLIGHT
ID: 00-A0-8D-50-05-60

Search For:
Search By: MAC ID

83 MAC Addresses found:

MAC ID	Port Number	VLAN ID	Tag Status
00-00-AA-88-C1-45	3	1	0
00-01-80-5F-35-DF	3	1	0
00-01-80-5F-35-EC	3	1	0
00-04-2E-01-CF-48	3	1	0
00-04-2E-01-D1-42	3	1	0
00-04-2E-01-E7-63	3	1	0
00-04-2E-01-E7-6D	3	1	0
00-04-2E-01-E8-58	3	1	0
00-04-2E-01-E8-60	3	1	0
00-04-2E-01-E8-73	3	1	0

Figure 25. The MAC Table screen shows the MAC addresses that have been learned by a switch.

The switch determines where to send each packet by finding the packet's destination MAC address in the table, and using that entry to know what port leads to the destination MAC. If there is no entry with the same MAC address and VLAN as the packet, then the switch must flood the packet to every port that might lead to the destination MAC (every port which is a member of the packet's VLAN).

WideBand Professional Series Switches can maintain up to 8k MAC address entries in all layer 2 models, and up to 32k in layer 3 models. Entries that are not used for a few minutes age out and are deleted to make room for new entries.

MAC Address Tables in the WideBand Professional Series Switches can be viewed on the *MAC Address Tables* screen shown in Figure 25.

Viewing this table can be useful for debugging and network monitoring. It also provides the ability to see where any Ethernet MAC on the network is in relation to the managed switch.

Searching for Addresses

The WideBand nMU has a powerful search engine for finding the MAC Address you are looking for. The list of addresses can be searched and sorted by any of the following criteria:

- MAC ID – A six-byte MAC address that is assigned to a device on the network.
- Port Number – Port number that the MAC ID was received on.
- VLAN – VLAN number that the MAC ID was received on.
- Tag Status – VLAN tag status for the MAC table entry.

The Search feature includes built-in wild cards, allowing you to enter partial words, etc and find multiple MAC Addresses with similar criteria. Entering a blank field as the criteria will return a list of all the MAC Addresses in the table.

fs[ix] Server Management

Gold Server Initial Configuration

When a Gold Server needs to be configured for the first time, it will not be managed by the nMU and its name will be "fsix-" followed by its serial number. From the Find Devices screen, make it managed by clicking on it.

Note: *The password you assign here will be the administrator password.*

After assigning a password and department, you see the Gold Server configuration screen. Here you must provide your company name, an email address, and three IP addresses (one for the Gold unit, one for the Mirror, and another that will be shared by the servers, which you will use to access these servers). You will also need to supply the subnet mask, gateway, and DNS information. Lastly, you will need to specify the mode you would like your servers to operate in:

- Standard mode will allow you to use your servers as a network fileserver, or a web server.
- In iSCSI mode, your Gold Server will act as a local drive. This is especially useful for applications that will not work using network-mapped drives.

When in iSCSI mode, several of the screens shown in the Server Administration section will not be accessible when managing the server through the nMU, and management via the servers' shared IP address will be completely disabled.

Note: *Once the configuration information has been entered into the Gold Server, the Mirror Server will initialize automatically. It will then sync the mirrored partition. This will take several hours. The Server may be used for storage during this period, but will not operate at full speed.*

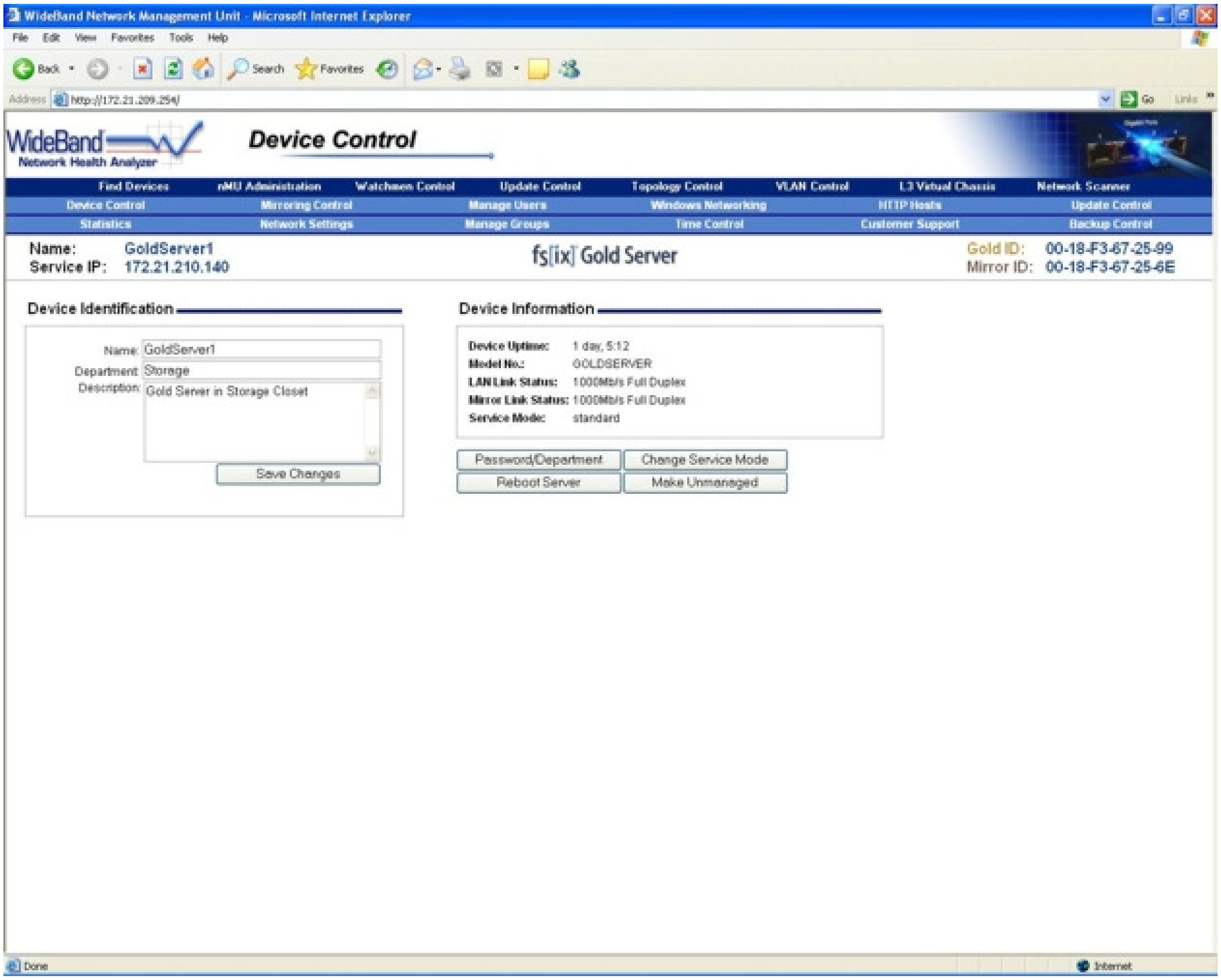
Server Device Control

After your servers have been configured, you will be taken to the Device Control screen (see Figure 26). If your servers are in standard mode, you may also manage your servers directly by typing the shared IP address into your browser's address bar, or by clicking on the blue IP address labeled as the Service IP.

Also shown here is the name assigned to your Gold Server, as well as the department, description, service mode, uptime, and link status. The gold highlighting on the Gold ID (see Figure 26) indicates that the Gold unit is currently primary. Clicking on the ID will take you to that unit's Device Control screen.

Note: *Several management screens are only available on the primary unit of a Gold Server even when it is in standard mode. An attempt to access these screens on the secondary unit will result in an error. In this case just click on the Device ID of the primary unit in the right-hand side of the banner and try again.*

From this screen you may choose to change the server's password and department or service mode. You may also reboot the server or make it no longer managed by the nMU.



Name: GoldServer1
Service IP: 172.21.210.140

Gold ID: 00-18-F3-67-25-99
Mirror ID: 00-18-F3-67-25-6E

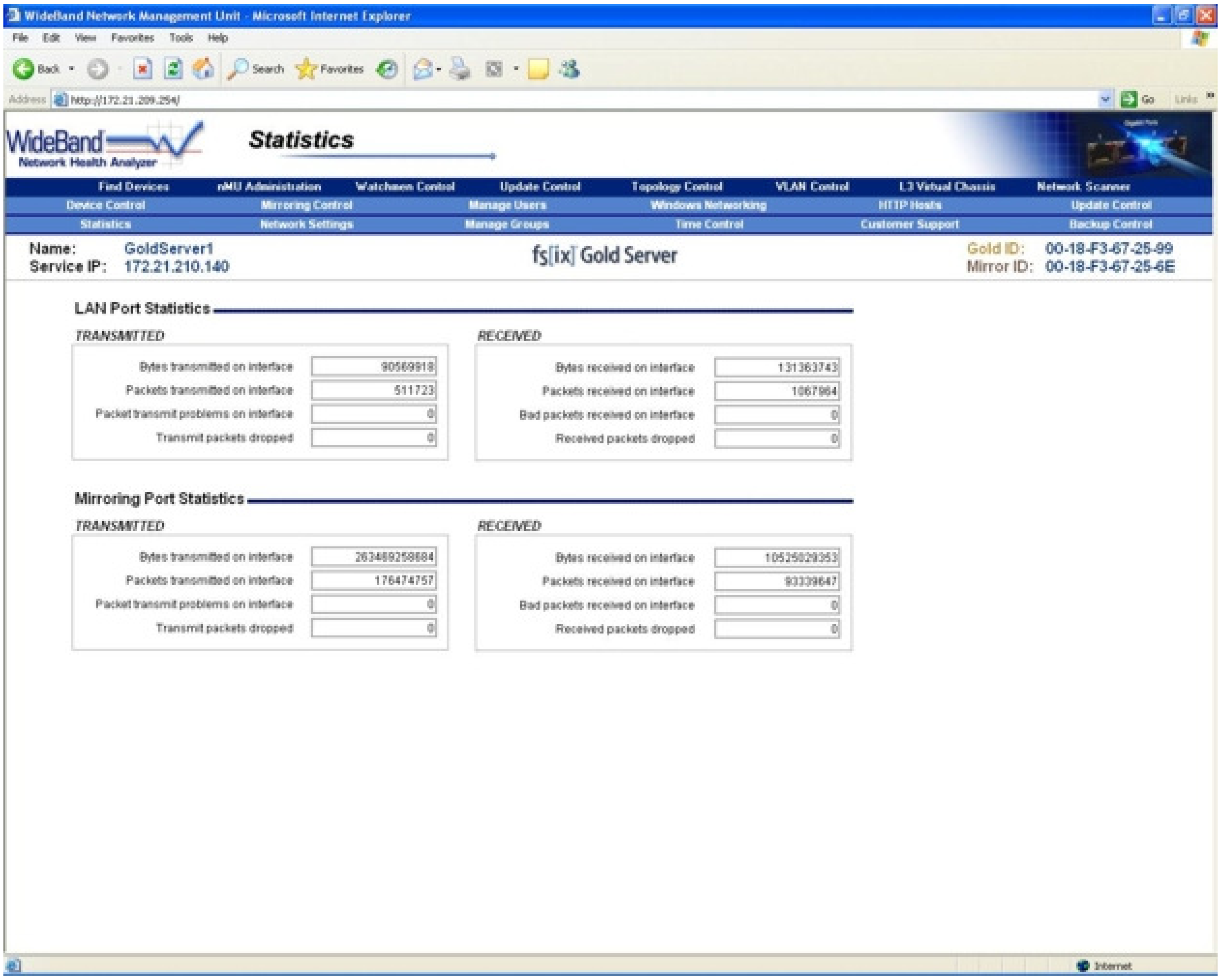
Name: GoldServer1
Department: Storage
Description: Gold Server in Storage Closet

Device Uptime: 1 day, 5:12
Model No.: GOLDSERVER
LAN Link Status: 1000Mb/s Full Duplex
Mirror Link Status: 1000Mb/s Full Duplex
Service Mode: standard

Figure 26. Device Control

Server Statistics

On this screen you will see a count of all the bytes and all the packets that have been sent or received by a Gold Server on either network interface (See Figure 27). This screen also keeps track of errors transmitting packets and the number of dropped packets.



Name: GoldServer1
Service IP: 172.21.210.140

Gold ID: 00-18-F3-67-25-99
Mirror ID: 00-18-F3-67-25-6E

LAN Port Statistics

TRANSMITTED		*RECEIVED*	
Bytes transmitted on interface	90569918	Bytes received on interface	131363743
Packets transmitted on interface	511723	Packets received on interface	1067964
Packet transmit problems on interface	0	Bad packets received on interface	0
Transmit packets dropped	0	Received packets dropped	0

Mirroring Port Statistics

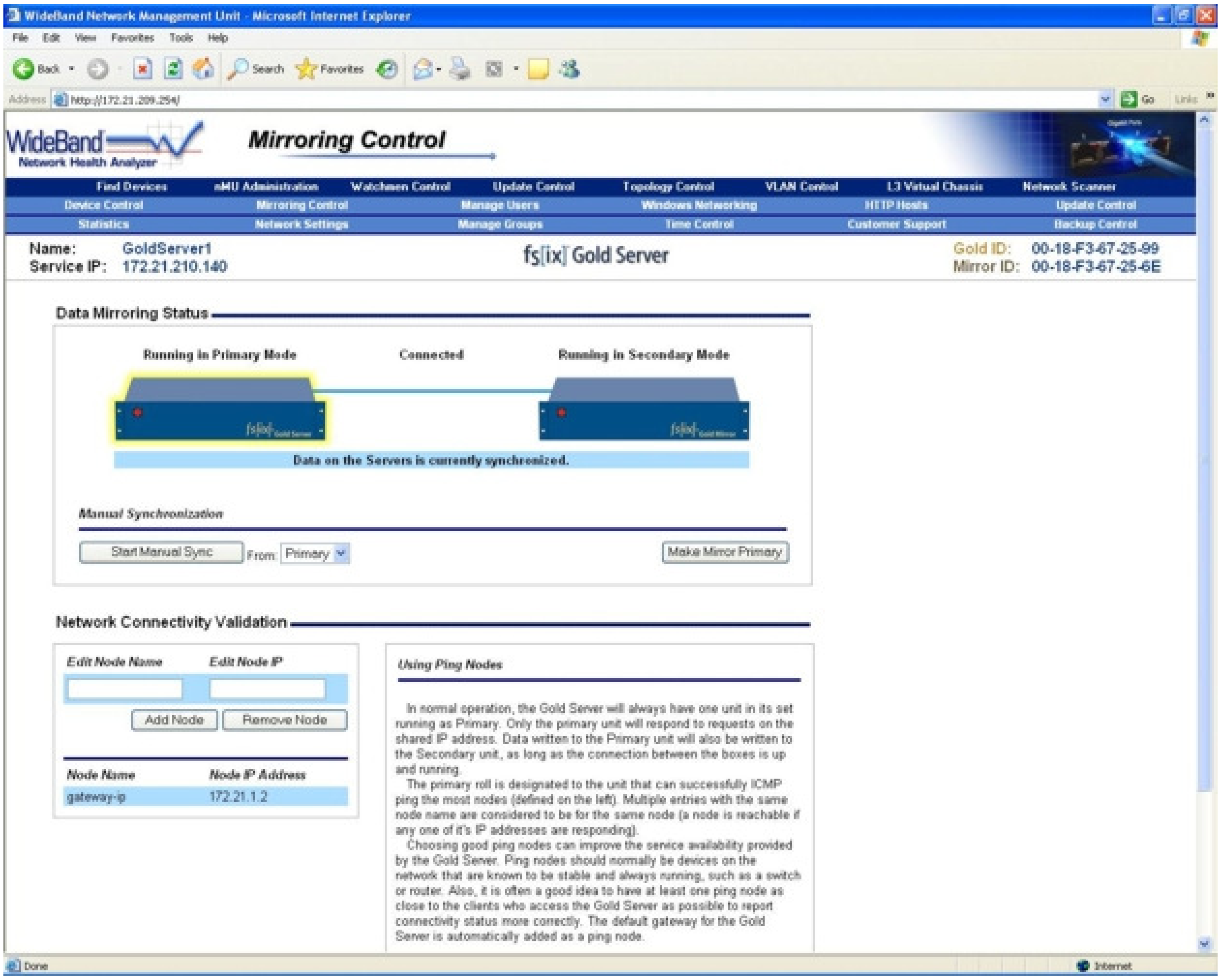
TRANSMITTED		*RECEIVED*	
Bytes transmitted on interface	263469258684	Bytes received on interface	10525029353
Packets transmitted on interface	176474757	Packets received on interface	93339647
Packet transmit problems on interface	0	Bad packets received on interface	0
Transmit packets dropped	0	Received packets dropped	0

Figure 27. Statistics

Server Mirroring Control

The Data Mirroring Status section allows you to monitor the status of both units in the Gold Server set. This section also allows you to change which unit has control over the shared resources, start a manual sync, or attempt a reconnect.

The Network Connectivity Validation section allows you to add or remove IP addresses that your servers will ping to test their network connectivity.



Name: GoldServer1
Service IP: 172.21.210.140

Gold ID: 00-18-F3-67-25-99
Mirror ID: 00-18-F3-67-25-6E

Data on the Servers is currently synchronized.

From: Primary

Node Name	Node IP Address
gateway-ip	172.21.1.2

In normal operation, the Gold Server will always have one unit in its set running as Primary. Only the primary unit will respond to requests on the shared IP address. Data written to the Primary unit will also be written to the Secondary unit, as long as the connection between the boxes is up and running.

The primary roll is designated to the unit that can successfully ICMP ping the most nodes (defined on the left). Multiple entries with the same node name are considered to be for the same node (a node is reachable if any one of it's IP addresses are responding).

Choosing good ping nodes can improve the service availability provided by the Gold Server. Ping nodes should normally be devices on the network that are known to be stable and always running, such as a switch or router. Also, it is often a good idea to have at least one ping node as close to the clients who access the Gold Server as possible to report connectivity status more correctly. The default gateway for the Gold Server is automatically added as a ping node.

Figure 28. Mirroring Control Screen

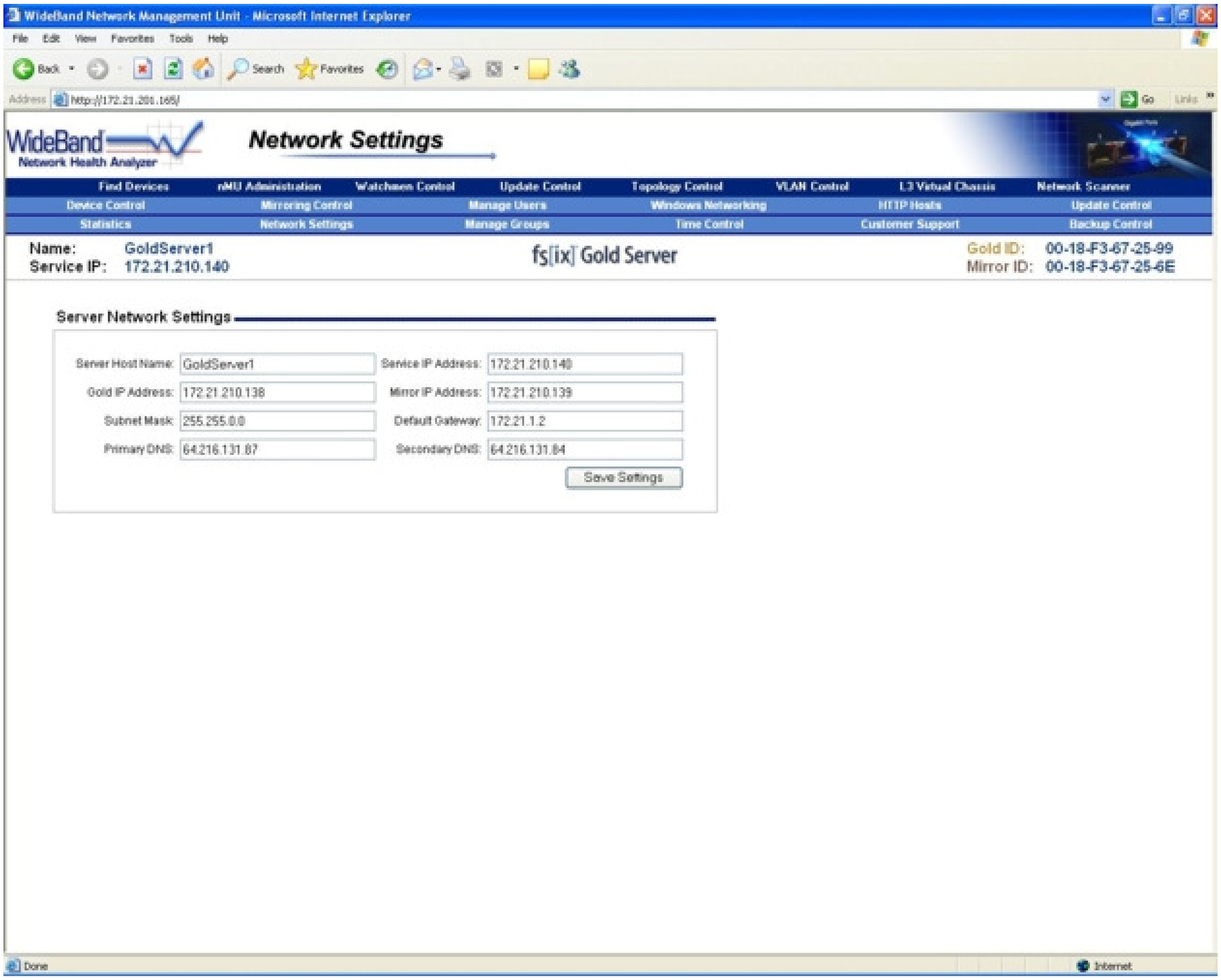
Start Manual Sync – Starts a resynchronization of all of the data from one unit to the other in the Gold Server set. It is not possible to start a sync to the unit running as primary. Also, this synchronization process can take up to several hours, and should only be done if necessary. The shared data will be available during a data sync, but performance will be lower than normal until the sync is complete.

The following buttons only show when they apply:

- Connect Button – Make this unit start attempting to connect to its peer again.
- Make Gold Primary – Force the shared IP address and services over to the Gold unit.
- Make Mirror Primary – Force the shared IP address and services over to the Mirror unit.

Server Network Settings

The Network Settings screen is where the server hostname, IP addresses, subnet mask, gateway, and DNS information may be configured.



Name: GoldServer1
Service IP: 172.21.210.140

Gold ID: 00-18-F3-67-25-99
Mirror ID: 00-18-F3-67-25-6E

Server Network Settings

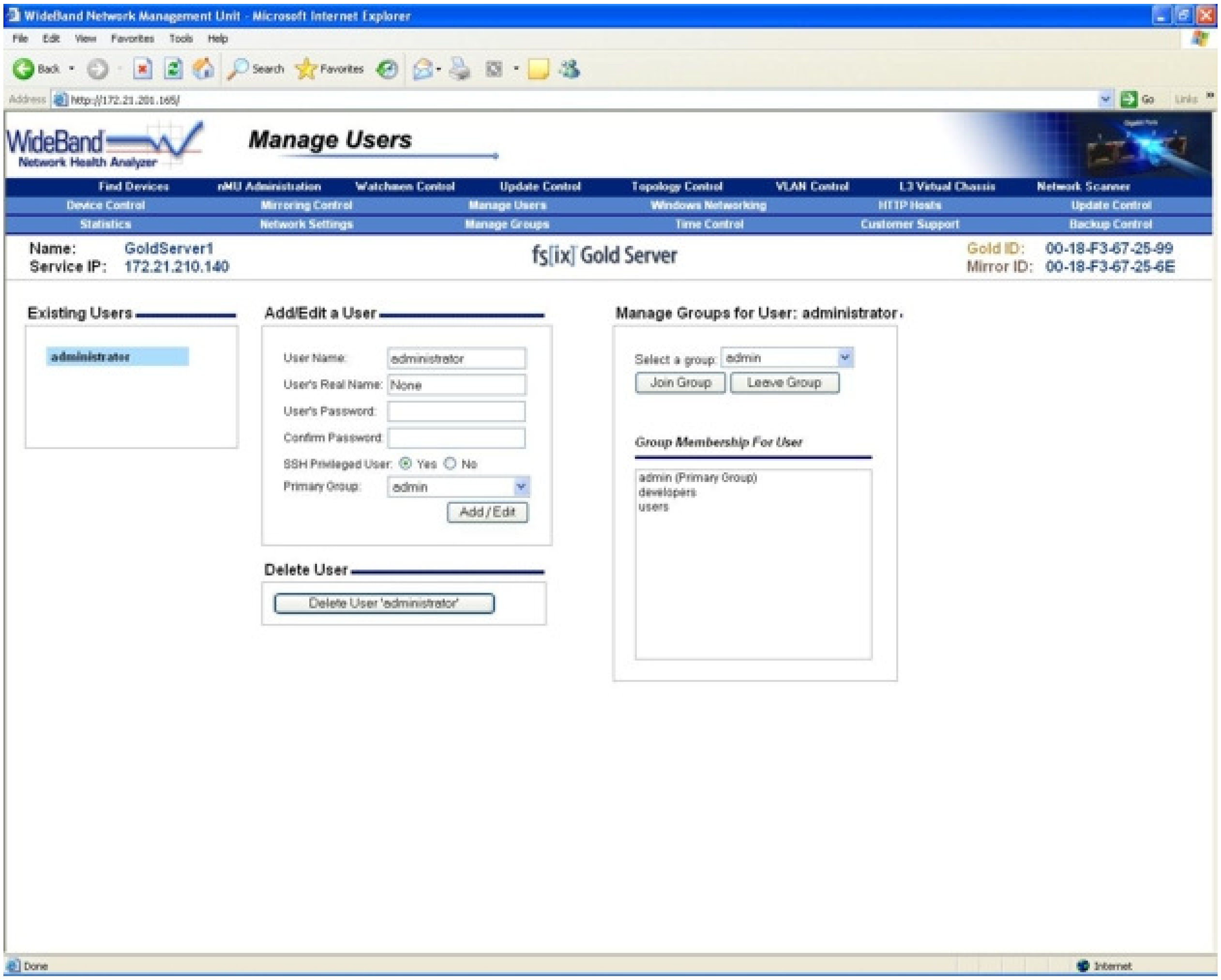
Server Host Name: GoldServer1
Service IP Address: 172.21.210.140
Gold IP Address: 172.21.210.138
Mirror IP Address: 172.21.210.139
Subnet Mask: 255.255.0.0
Default Gateway: 172.21.1.2
Primary DNS: 64.216.131.87
Secondary DNS: 64.216.131.84

Figure 29. Network Settings Screen

Server Name – A unique name that identifies this server on the network.
Service IP Address – A static IP address that is shared between the Gold and Mirror units in the Gold Server set. This is the IP address that should normally be used to communicate with the Gold Server set.
Gold IP Address – A static IP address that is assigned to the Gold unit.
Mirror IP Address – A static IP address that is assigned to the Mirror unit.
Subnet Mask – The IP mask for all three IP addresses used by the Gold Server set.
Default Gateway – The default IP gateway for the Gold Server set.
Primary DNS – IP address of the primary DNS server for the Gold Server set.
Secondary DNS – IP address of the secondary DNS server for the Gold Server set.

Manage Users On Server

This screen may be used to add, edit, and delete users. You may also manage a user's group membership.



Name: GoldServer1
Service IP: 172.21.210.140
Gold ID: 00-18-F3-67-25-99
Mirror ID: 00-18-F3-67-25-6E

Existing Users

administrator

Add/Edit a User

User Name: administrator
User's Real Name: None
User's Password:
Confirm Password:
SSH Privileged User: ● Yes ○ No
Primary Group: admin

Delete User

Manage Groups for User: administrator

Select a group: admin

Group Membership For User

admin (Primary Group)
developers
users

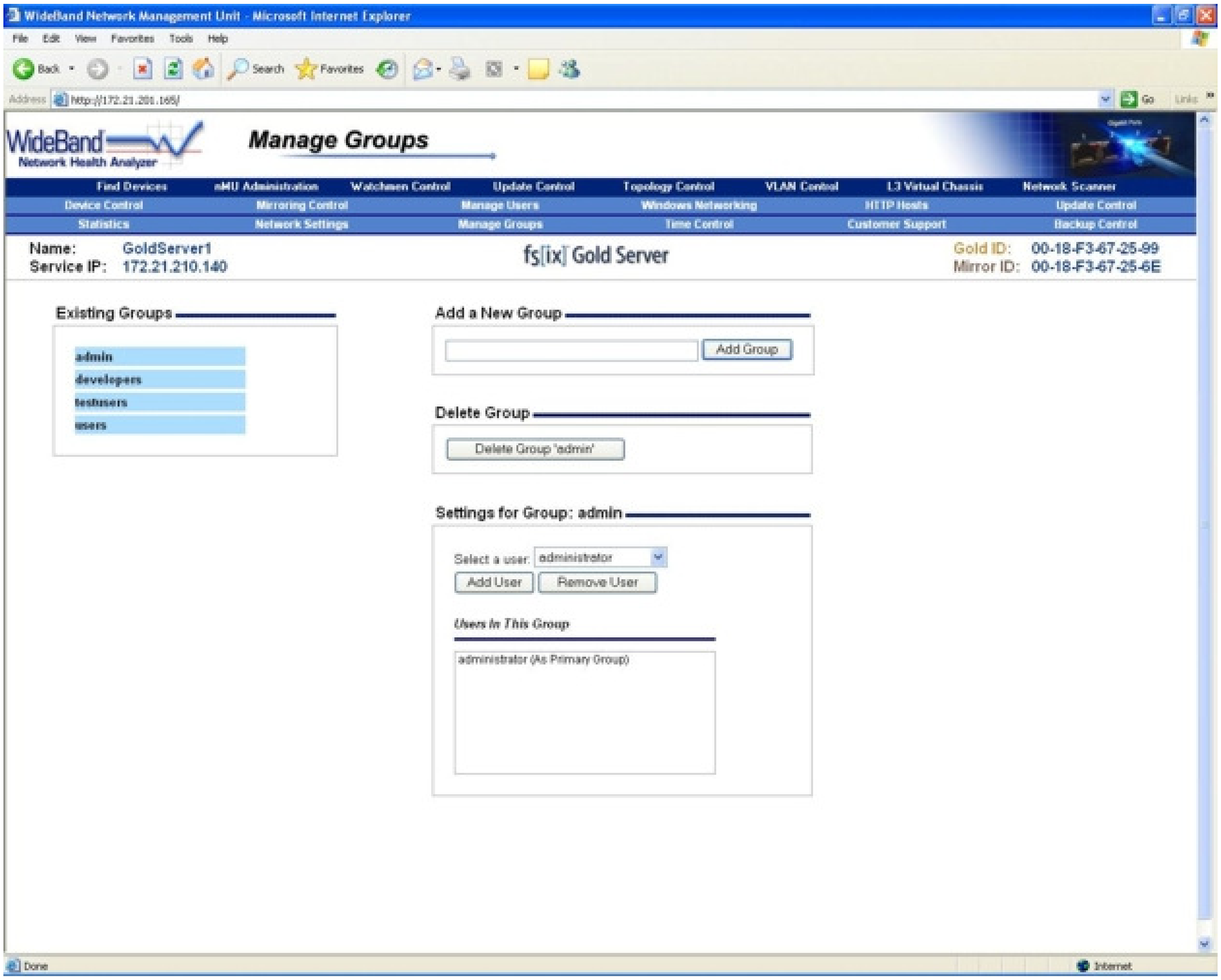
Figure 30. Manage Users Screen

User Name – A unique user name that this user will use to log in.
User's Real Name – The user's full name. This field is optional, and only used for your own future reference.
User's Password – A password this user will need to know in order to prove his/her identity. When making changes to a current user, this field can be left blank, indicating that the password should not change.
Confirm Password – This field must be the same as the User's Password field in order to save a new password.
SSH Privileged User – SSH (or Secure Shell) access allows the user to open a fs[ix] shell connection. To keep your Gold Server secure, only give SSH privileges to users who need it (such as developers and administrators).
Primary Group – The group that will be given ownership (by default) to files/folders that are created by this user through SSH.
Group Membership List – This list shows every group that the selected user is currently a member of on this Gold Server. The group that is marked with '(Primary Group)' is set by the

Primary Group field (in the Add/Edit a User Section, at center), and cannot be modified through this list.

Manage Groups On Server

This screen may be used to add or remove groups. You may also manage group membership.



Name: GoldServer1
Service IP: 172.21.210.140

Gold ID: 00-18-F3-67-25-99
Mirror ID: 00-18-F3-67-25-6E

Existing Groups

- admin
- developers
- testusers
- users

Add a New Group

Delete Group

Settings for Group: admin

Select a user: administrator

Users In This Group

administrator (As Primary Group)

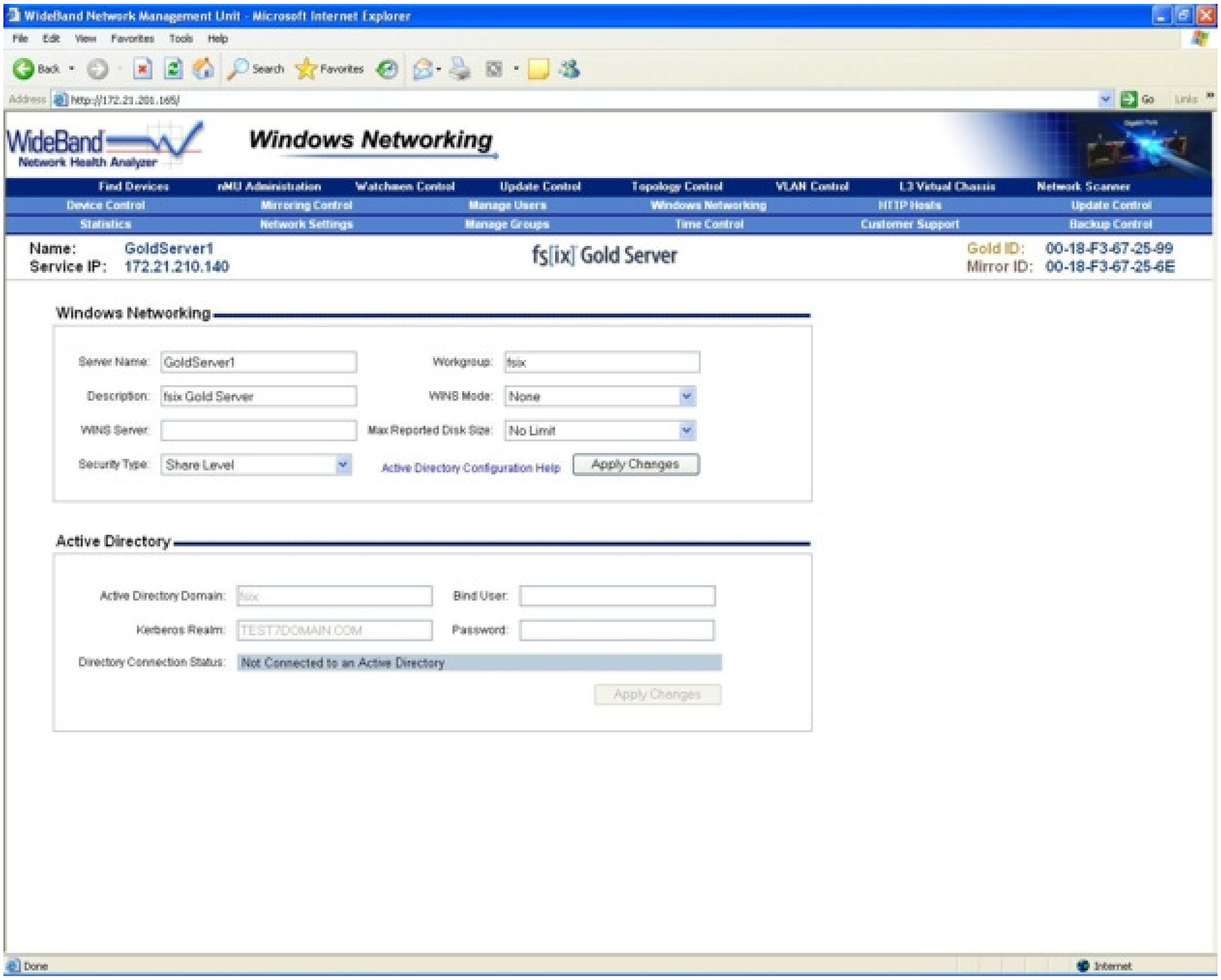
Figure 31. Manage Groups

Users in Group List – This list shows every user that is currently a member of the selected group. The users that are marked with '(As Primary Group)' are set by the Primary Group field for each user (on the Manage Users screen), and cannot be modified by this screen.

Windows Networking On Server

Here you may configure Windows networking options, including the server's identity settings and global share parameters.

Next, to the Apply Changes button there is a link to a help page for Active Directory Configuration. This screen gives six steps to help you join your Gold Server to your Active Directory.



Name: GoldServer1
Service IP: 172.21.210.140
Gold ID: 00-18-F3-67-25-99
Mirror ID: 00-18-F3-67-25-6E

Windows Networking

Server Name: GoldServer1
Workgroup: fsix
Description: fsix Gold Server
WINS Mode: None
WINS Server:
Max Reported Disk Size: No Limit
Security Type: Share Level

Active Directory

Active Directory Domain: fsix
Bind User:
Kerberos Realm: TEST7DOMAIN.COM
Password:
Directory Connection Status: Not Connected to an Active Directory

Figure 32. Windows Networking

Windows Networking Section:

Server Name – A unique name that identifies this server on the network.
Workgroup – The Windows Networking Workgroup this server is a part of.
Description – A description of this server that will be seen by other Windows machines when browsing the network.
WINS (or Windows Internet Naming Service) is used to automatically learn what NetBIOS names belong to what IP addresses on the Windows network. The Gold Server can act in one of three different WINS modes:

- 'None' prevents the Gold Server from participating in WINS communications.
- 'Client' allows the Gold Server to learn WINS information.
- 'Server' lets the Gold Server learn and supply WINS information to other machines.

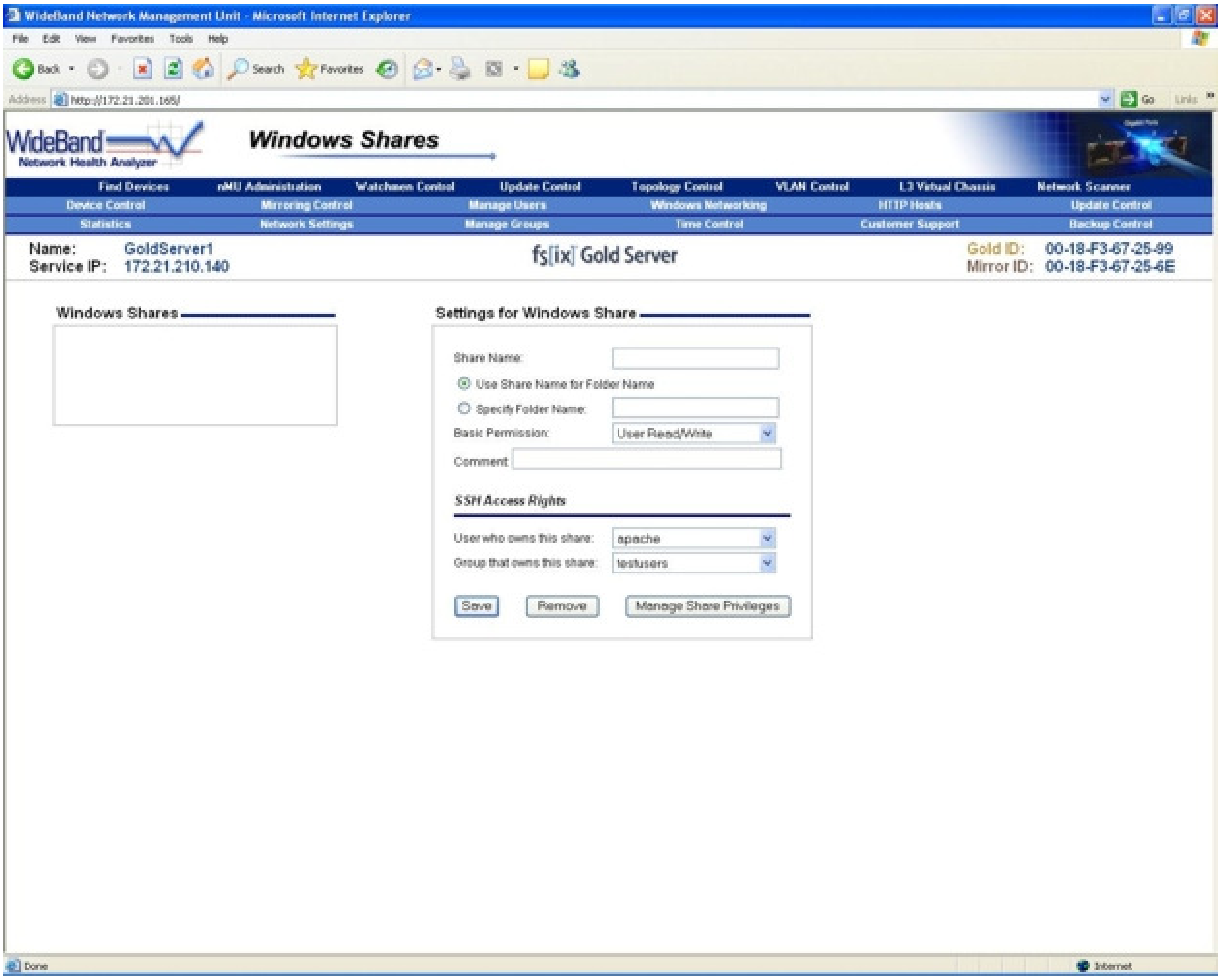
WINS Server – This field specifies a specific WINS Server that should be used.
Max Reported Disk Size – Some older versions of Windows cannot handle shares of large sizes. This field can be used to fool those legacy operating systems into supporting a large share.
Choosing a security type is an important part of configuration. The Gold Server supports three security modes which define how the server will verify its Windows users.
Share Level: When in share level mode the server will allow access to any user who knows a correct password. This is the lowest level of security and is not recommended for most applications.
User Level: When user level security is used, each user must provide a correct username and password in order to access share data. This is the preferred security mode when the Gold Server is not a part of an Active Directory.
Active Directory: When a Microsoft Active Directory is present on the network. The Gold Server can receive all of its user and group information from the directory server. Also, all user authentication will be done with Kerberos, so passwords will not be sent across the network in plain text.

Active Directory Section:

Active Directory Domain – The Microsoft Active Directory Domain the Gold Server should connect to.
Kerberos Realm – The Kerberos realm that should be used for authentication. This is normally the same as the domain, but all upper case. As an example, for the AD domain ‘example.com’ the Kerberos realm would be ‘EXAMPLE.COM’.
Bind User – The Active Directory user to use when binding this server to the domain (normally an administrative user).
Password – The Kerberos password for the Bind User.

Windows Shares On Server

You may create Windows shares and allow users to store and access files on your server over the network.



Address: http://172.21.201.165/

Name: GoldServer1
Service IP: 172.21.210.140

Gold ID: 00-18-F3-67-25-99
Mirror ID: 00-18-F3-67-25-6E

Share Name:
● Use Share Name for Folder Name
○ Specify Folder Name:
Basic Permission: User Read/Write
Comment:

User who owns this share: apache
Group that owns this share: testusers

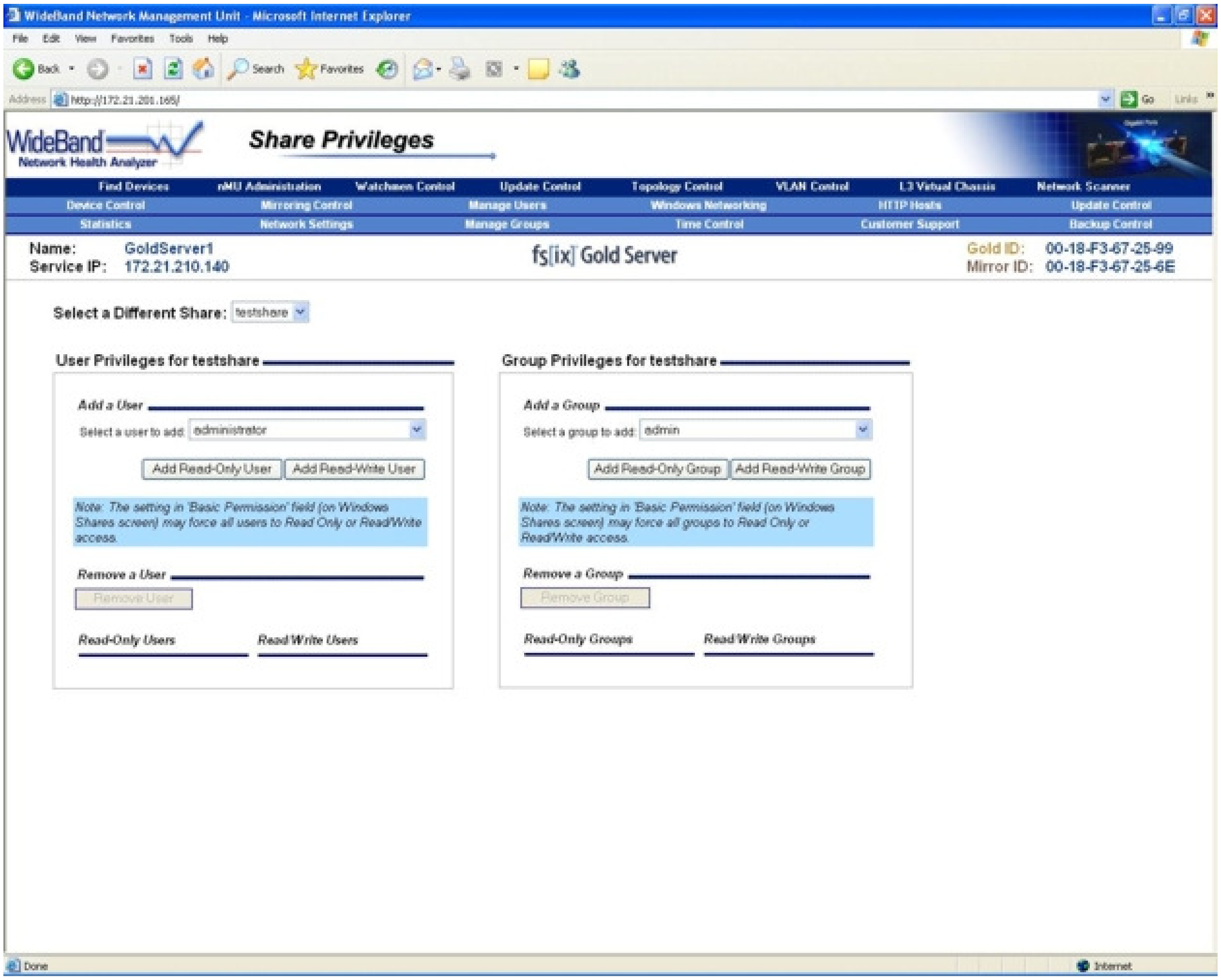
Figure 33. Windows Shares

Share Name – The name that will be used to access this share on the network.
Folder Name – The name of the folder that will contain all of the share data. The folder will be created if it does not already exist.
Basic Permission – Used to control what types of access this share will allow. Allowing guest access opens the share to anyone. The settings on this field can override any settings on the Share Privileges screen.
Comment – A description of the share that Windows machines will see when browsing the network.
User who owns this share – To control data access from SSH users, files/folders created within this share will be owned by this user.
Group that owns this share – To control data access from SSH users, files/folders created within this share will be owned by this group.

Share Privileges On Server

User and Group Privileges sections allow you to select a user or a group and give them read-only or read/write privileges on the selected share.

Note: *When in ‘share level’ security mode (set on the Windows Networking screen) all users within a given share will have the same privileges.*



Share Privileges

Name: GoldServer1
Service IP: 172.21.210.140

Gold ID: 00-18-F3-67-25-99
Mirror ID: 00-18-F3-67-25-6E

Select a Different Share: testshare

User Privileges for testshare

Add a User

Select a user to add: administrator

Note: The setting in 'Basic Permission' field (on Windows Shares screen) may force all users to Read Only or Read/Write access.

Remove a User

Read-Only Users *Read/Write Users*

Group Privileges for testshare

Add a Group

Select a group to add: admin

Note: The setting in 'Basic Permission' field (on Windows Shares screen) may force all groups to Read Only or Read/Write access.

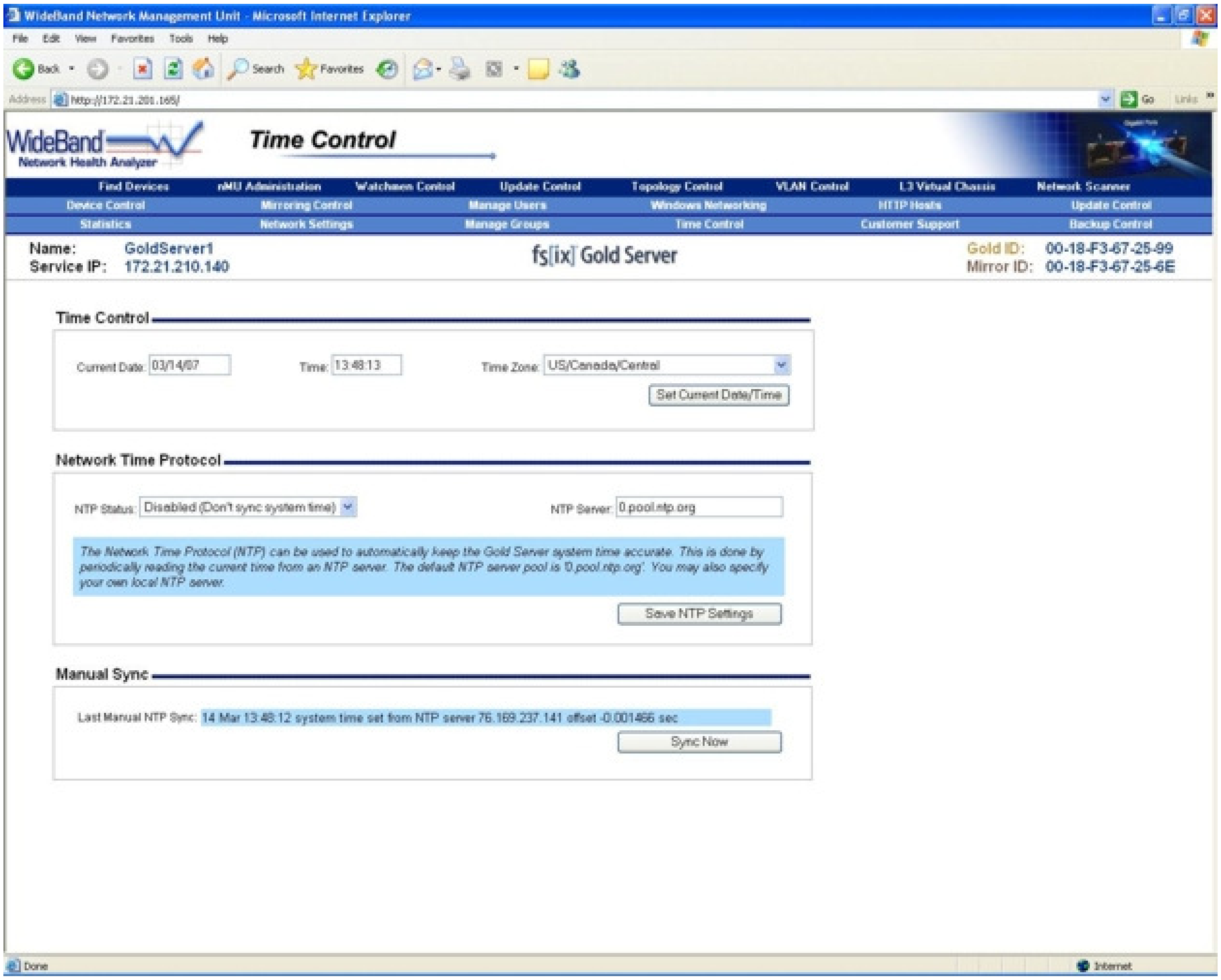
Remove a Group

Read-Only Groups *Read/Write Groups*

Figure 34. You may grant share access by user or by group.

Server Time Control

Here you can set the time, date, and time zone to match your area. You may also run a manual sync or enable NTP to sync the correct time automatically.



Name: GoldServer1
Service IP: 172.21.210.140

Gold ID: 00-18-F3-67-25-99
Mirror ID: 00-18-F3-67-25-6E

Time Control

Current Date: 03/14/07 Time: 13:48:13 Time Zone: US/Canada/Central

Network Time Protocol

NTP Status: Disabled (Don't sync system time) NTP Server: 0.pool.ntp.org

The Network Time Protocol (NTP) can be used to automatically keep the Gold Server system time accurate. This is done by periodically reading the current time from an NTP server. The default NTP server pool is '0.pool.ntp.org'. You may also specify your own local NTP server.

Manual Sync

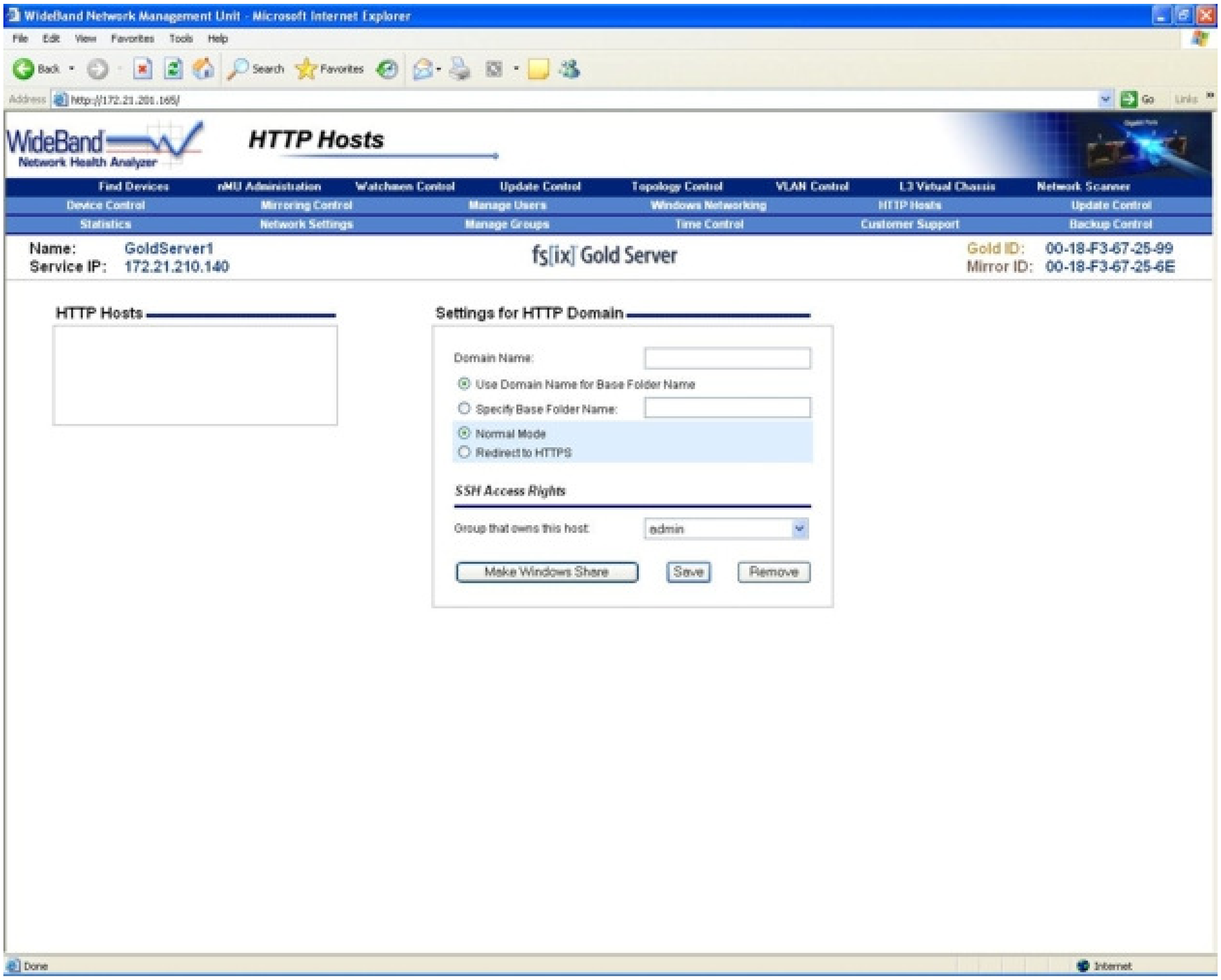
Last Manual NTP Sync: 14 Mar 13:48:12 system time set from NTP server 76.169.237.141 offset -0.001466 sec

Figure 35. Time Control Screen

Current Date – The current date should be entered in the format: mm/dd/yy
Time – The current time should be entered in the format: hh:mm:ss (use military units)
Time Zone – Select the time zone that is closest to your area.
NTP Status – Enable NTP to get periodic synchronization of the system time.
NTP Server – Specify what NTP server shall be used for time synchronizations.
Sync Now – Run a manual NTP time sync with the selected NTP server.

HTTP Hosts On Server

Here you may configure different virtual hosts. Virtual hosts enable you to have multiple HTTP domains on a single machine.



Name: GoldServer1
Service IP: 172.21.210.140
Gold ID: 00-18-F3-67-25-99
Mirror ID: 00-18-F3-67-25-6E

Domain Name:
● Use Domain Name for Base Folder Name
○ Specify Base Folder Name:
● Normal Mode
○ Redirect to HTTPS

Group that owns this host: admin

Figure 36. HTTP Hosts Screen

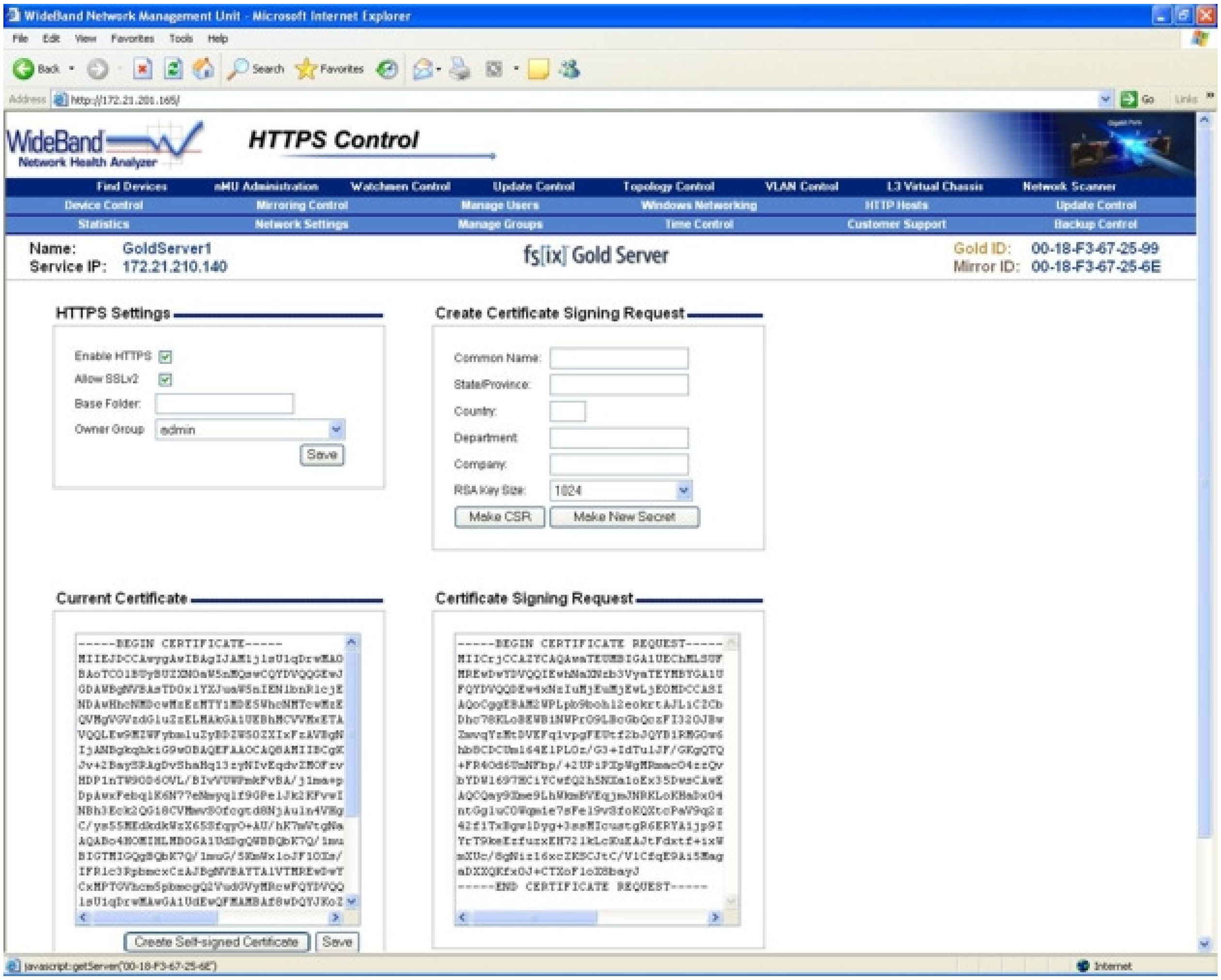
Domain Name - The domain name this virtual host will respond to.
Base Folder - Name of the folder that contains all of the HTML and PX files for this virtual host.
Redirect to HTTPS - All requests to this virtual host's domain will be redirected to the HTTPS host.
Group that owns this host - Group that will have SSH access to the files in this virtual host.
Save - Save and apply changes to this HTTP virtual host.
Remove - Delete this virtual host from the Gold Server.
Make Windows Share - Configure a Windows share to access files within this virtual host. The new share will automatically be created, but the Share Privileges screen must be used to set up its privileges.

Server HTTPS Control

Using HTTPS, you may view data over a secure connection to a server. This screen allows you to configure the Gold Server's HTTPS settings.

The simplest way to secure HTTP communication with the Gold Server is to fill out the Create Certificate Signing Request form and click the Make New Secret button. This will allow HTTPS communication, but browsers may warn the user that the certificate wasn't signed by a trusted authority.

To prevent this, create a Certificate Signing Request, or CSR, and submit it to a commercial Certificate Authority, who may in turn send you a valid certificate to paste into your Current Certificate buffer, and click Save.



Name: GoldServer1
Service IP: 172.21.210.140
Gold ID: 00-18-F3-67-25-99
Mirror ID: 00-18-F3-67-25-6E

HTTPS Settings

Enable HTTPS ☑
Allow SSLv2 ☑
Base Folder:
Owner Group: admin
Save

Create Certificate Signing Request

Common Name:
State/Province:
Country:
Department:
Company:
RSA Key Size: 1024
Make CSR | Make New Secret

Current Certificate

-----BEGIN CERTIFICATE-----
MIIEJDCCAwygAwIBAgIJAMljlsU1qDrwMA0
BAoTCO1BWyBUIXNOaW5nMQswCQYDVQQGEwJ
GDAMBgNVBAsTD0x1YXJuaW5nIEN1bnRlcjE
NDAwMhcNMDcwMzEzMTY1MDE5WhcNMTcwMzE
QVMgVGVzdGluZzELMAkGA1UEBhMCVVMxETA
VQQLEw9MZWFybmluZyBDZW50ZXIxFzAVBgN
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgK
Jv+2BaySRAgDvShaHq1JzyNIvEqdvZMOFzv
HDP1nTW9O04OVL/BIvVUWPmkFvBA/j1ma+p
DpAwxFebqiK6N77eNmyq1f9GPe1Jk2KFvwI
NBh3Eck2QG18CVMmv8Ofcgtd8NjAuln4VMg
C/ys55MEdkdkWzX65SfqyO+AU/hK7wWtgNa
AQABo4HOMIHLMB0GA1UdDgQWBBQbK7Q/1mu
BIGTMIGQgBQbK7Q/1muG/5KmWx1oJF1OIn/
IFRlc3RpbmcxCzAJBgNVBAYTA1VTMREwDwY
CxMPTGVhcm5pbmcgQ2VudGVyMRcwFQYDVQQ
lsU1qDrwMAwGA1UdEwQFMAMBAf8wDQYJKoZ

Create Self-signed Certificate | Save

Certificate Signing Request

-----BEGIN CERTIFICATE REQUEST-----
MIICrjCCAZYCAQAwaTEUMBIGA1UEChMLSUF
MREwDwYDVQQIEwhNaXNzb3VyaTEYMBYGA1U
FQYDVQQDEw4xMzIuMjEuMjEwLjE0MDCCASI
AQoCggEBAM2WPLpb9boh12eokrtAJLiC2Cb
Dho78KLoBEWB1NWPrO9LBoGbQozFI32OJBw
ZmvqYzMtDVEFqivpgFEUtf2bJQYB1RMGOw6
hbBCDCUm164E1PLOz/G3+IdTu1JF/GKgQTQ
+FR4Od6UmNFbp/+2UPiPIgWgMPmmcO4zzQv
bYDW1697HCiYCwfQ2h5NXa1oEx35DwsCAwE
AQCQmy9Xme9LhWkmBVEqjmJNRKLoKHaDx04
ntGg1uC0Wqmie7sFe19v8foKQXtcPaV9q2z
42f1TxBgw1Dyg+3ssMIcustgR6ERYAijp9I
YrT9keEzfuzxEH721kLcKuEAJtFdxtf+ixW
mXUc/8gNiz16xcZKSCJtC/V1CfqE9Ai5Mag
aDXXQKfx0J+CTXoF1oX8bayJ
-----END CERTIFICATE REQUEST-----

javascript:getServer('00-18-F3-67-25-6E')

Figure 37. HTTPS Control Screen

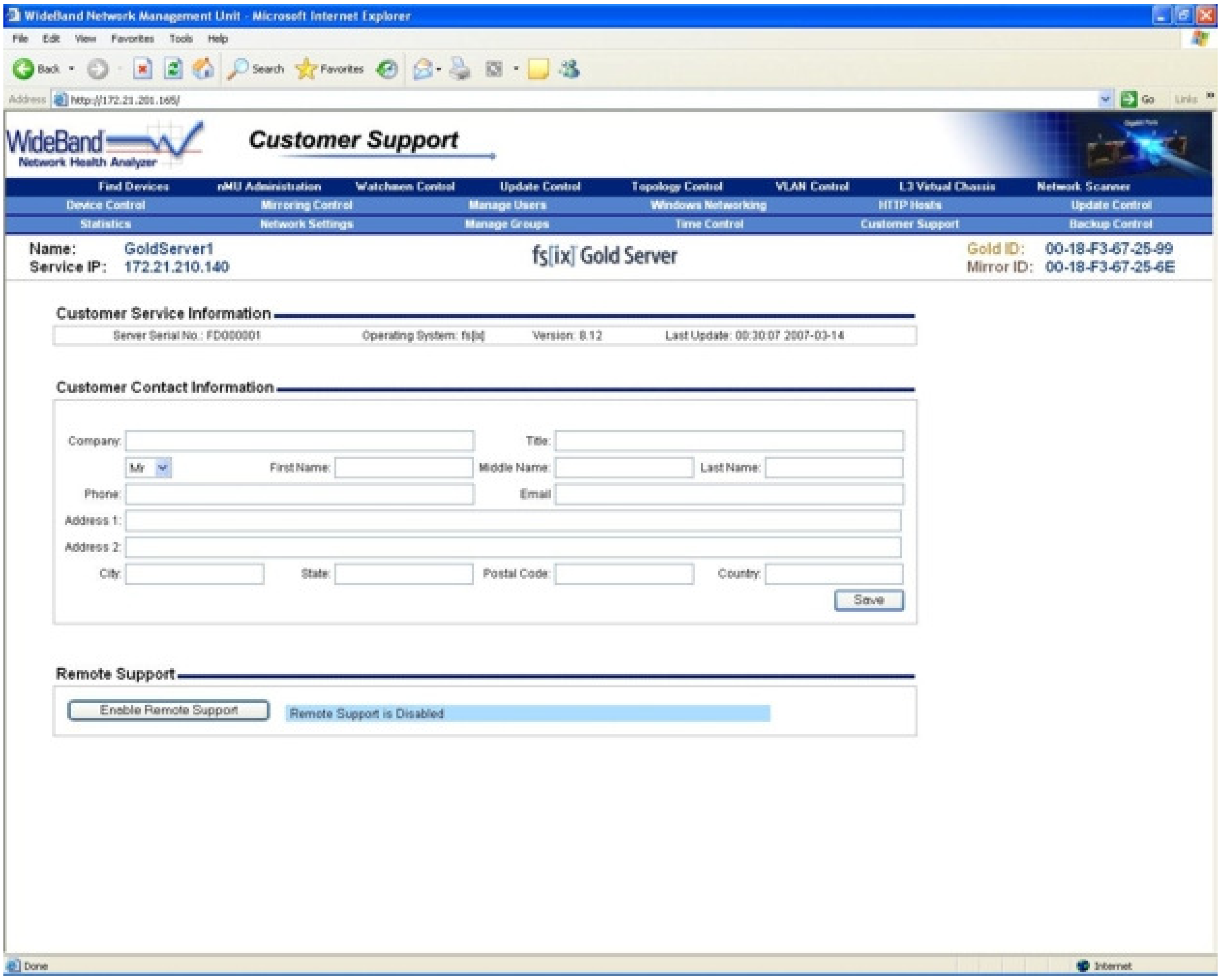
Enable HTTPS - Checked if Secure HTTP will be supported on this Gold Server.
Allow SSLv2 - Checked if less secure, but more common, SSLv2 is allowed for HTTPS communication. Otherwise only TLS is allowed.
Base Folder - Name of the folder that contains all of the HTML and PX files for HTTPS.
Owner Group - Group that will have SSH access to the files in this folder.
Save - Save and apply changes to the HTTPS host.

Common Name - Domain or IP address of this Gold Server. Important: If this doesn't match what the browser is expecting, the browser will warn the user that the certificate is not valid.
State/Province - Full name of your State or Province. Do not abbreviate this name.
Country - Country name shown as a two-letter code.
RSA Key Size - Size of the RSA key that will be used. 2048 bits is more secure, but 1024 bits is more commonly supported by older browsers.
Make CSR - Create a new Certificate Signing Request.
Make New Secret - Generate a new RSA secret. Warning: The old RSA secret will be lost, and any signed certificate for that secret will become worthless.
Certificate Buffer - Certificate that is used by browsers to verify this Gold Server.
CSR Buffer - Certificate Signing Request that can be given to a certificate authority.
Create Self-Signed Certificate - Replace the current certificate with a self-signed certificate. This will be functionally secure, but browsers will warn that this certificate is not signed by a trusted certificate authority.
Save Cert - Save the current certificate buffer text.

Customer Support For Server

Included on the server is a small database of information about your company and the server itself. The purpose of this database is to provide you with important information about the server, and provide personalized customer support.

From this screen you are also able to activate or deactivate remote support. When remote support is enabled, fs[ix] Customer Support representatives are able to log into your servers for advanced troubleshooting if you encounter problems.



Name: GoldServer1
Service IP: 172.21.210.140

Gold ID: 00-18-F3-67-25-99
Mirror ID: 00-18-F3-67-25-6E

Customer Service Information

Server Serial No.: FD000001 Operating System: fs[ix] Version: 8.12 Last Update: 00:30:07 2007-03-14

Customer Contact Information

Company: Title:
Mr First Name: Middle Name: Last Name:
Phone: Email
Address 1:
Address 2:
City: State: Postal Code: Country:

Remote Support

Remote Support is Disabled

Figure 38. Customer Support Screen

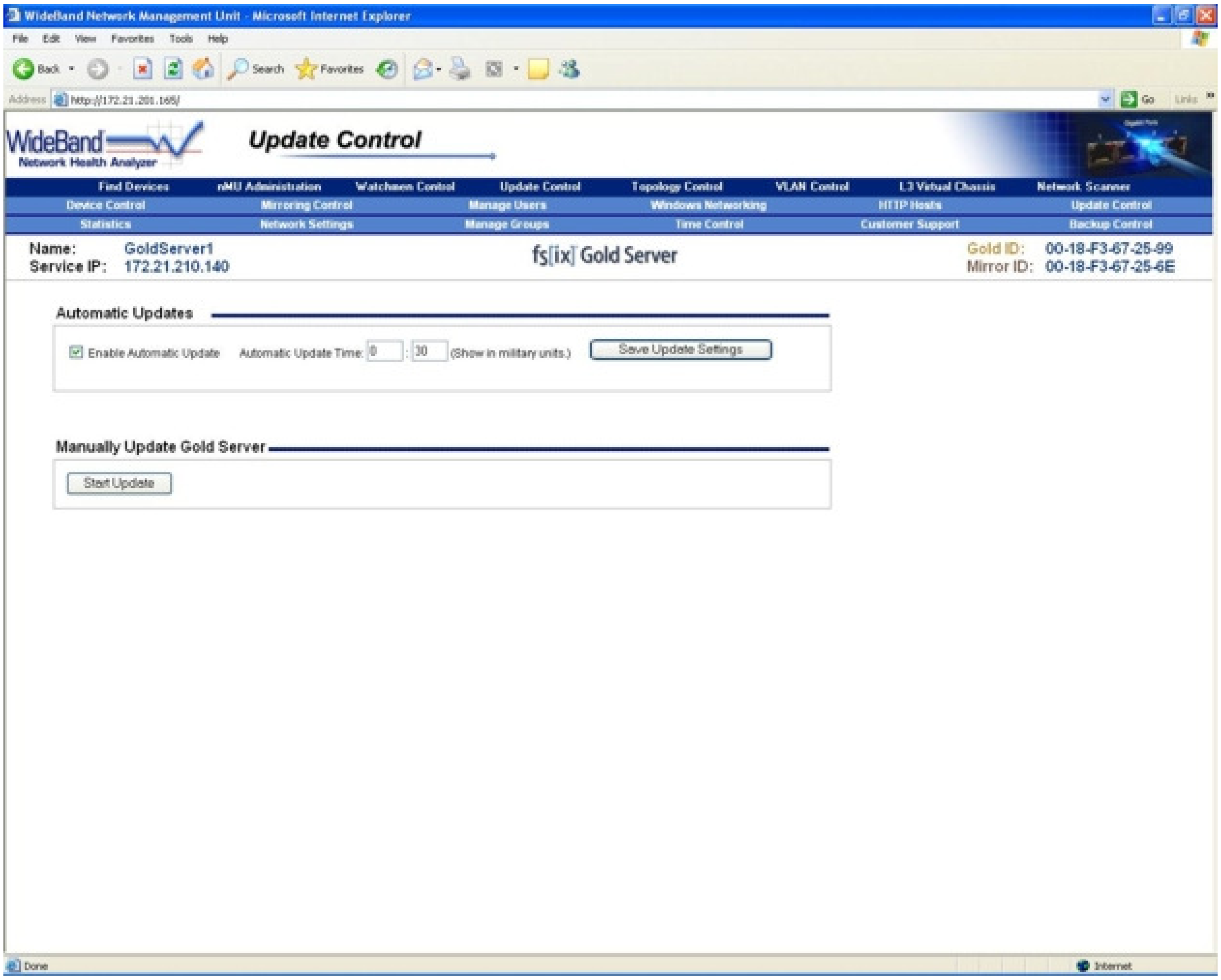
Customer Contact Information – This information is used by fs[ix] support to provide better service to Gold Server customers.

Enable Remote Support – Enabling remote support opens a connection that will allow the fs[ix] technical support team to SSH into your server remotely, and give direct support. For security reasons, only enable remote support when assistance is needed.

Server Update Control

Here you may change your server’s update settings, or start a manual update.

To receive updates, the servers must be provided with correct gateway and DNS information, as well as outbound TCP access to the internet through port 80, 21, 873, 23, 20, 37, or 123. Updates are enabled by default.



Name: GoldServer1
Service IP: 172.21.210.140

Gold ID: 00-18-F3-67-25-99
Mirror ID: 00-18-F3-67-25-6E

Automatic Updates

☑ Enable Automatic Update   Automatic Update Time: 0 : 30 (Show in military units.)

Manually Update Gold Server

Figure 39. Update Control Screen

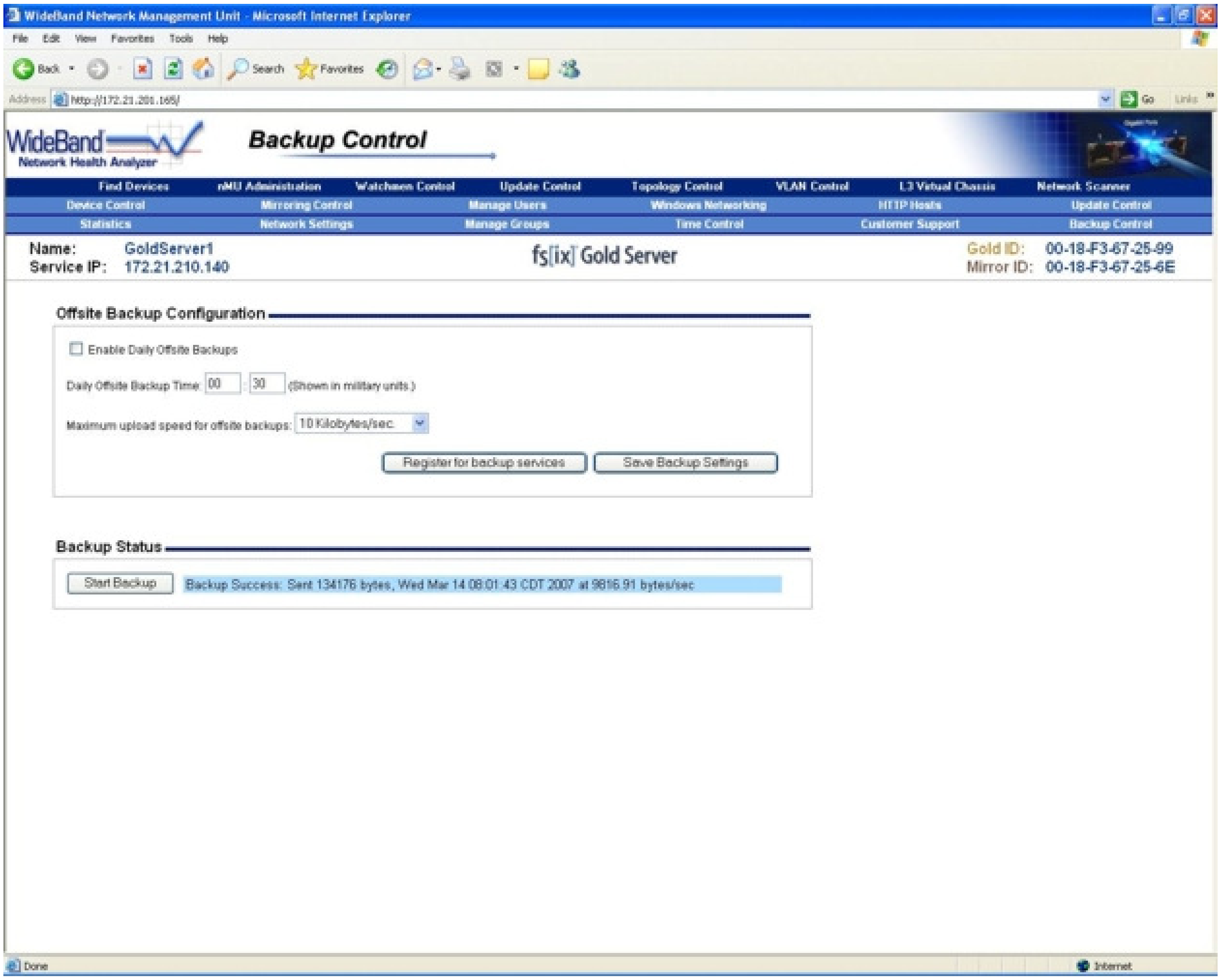
Enable Automatic Update – Select this field to receive daily updates for the Gold Server set.
Automatic Update Time – The time, in military units, that the Gold Server will update at each day.
Start Update – Run a Gold Server update on the primary unit right now.

Server Backup Control

Gold Servers support the optional off-site backup service. The off-site copy of the data is sent 256-bit AES encrypted over the Internet. This provides the user with a greater degree of protection for sensitive data.

The Off-Site Backup Service insures your critical data is protected and readily accessible in the event of theft, fire, or natural disaster. Backup settings such as off-site backup time and speed are configured on the Backup Control Screen.

You may register for the Off-Site Backup Service by clicking on the Register for backup services button, or by going to http://support.wband.com.



Address: http://172.21.201.165/

Name: GoldServer1
Service IP: 172.21.210.140
Gold ID: 00-18-F3-67-25-99
Mirror ID: 00-18-F3-67-25-6E

Offsite Backup Configuration

□ Enable Daily Offsite Backups

Daily Offsite Backup Time: 00 : 30 (Shown in military units.)

Maximum upload speed for offsite backups: 10 Kilobytes/sec.

Backup Status

Backup Success: Sent 134176 bytes, Wed Mar 14 08:01:43 CDT 2007 at 9816.91 bytes/sec

Figure 40. Backup Control Screen

Enable Daily Offsite Backups – Select this field to backup data offsite daily for the Gold Server set.
Daily Offsite Backup Time – The time, in military units, when the Gold Server's daily offsite backup will occur.
Start Backup -- Begin an offsite backup right now.

iSCSI Configuration

The Gold Servers can be configured as a local drive on a Windows machine using iSCSI. The first step is to install the iSCSI Initiator, which may be downloaded at the following URL:

http://www.microsoft.com/downloads/details.aspx?FamilyID=12cb3c1a-15d6-4585-b385-befd1319f825&DisplayLang=en

Next, open the iSCSI Initiator, go to the Discovery tab and click Add. Enter your server's shared address in the window provided.

From the Targets tab, click Log On. From this window, check Automatically restore this connection when the system boots and click the Advanced button.

Next, check CHAP logon information, and fill out the User name and Target secret fields with the iSCSI username and password you entered while configuring your servers.

Go to the Bound Volumes/Devices tab, click Bind All, then click OK.

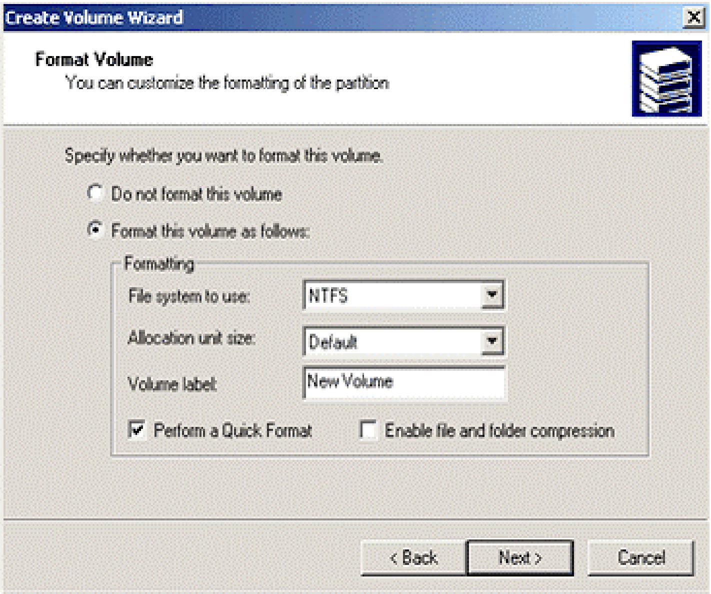
After this has been done, go to Control Panel – Administrative Tools – Computer Management – Storage – Disk Management.

This will bring up the "Write Signature and Upgrade Disk Wizard". Click Next and select the checkbox beside the new disk, then click Next – Next – Finish.

Next, right-click on the new disk and click on Create Volume… From here, most of the defaults are acceptable. However, you may choose to perform a quick format, re-label the drive, or change other configuration settings.

When this is done, you may begin using your servers.

You may refer to your operating system's documentation for more information on formatting and configuring your drives.



Create Volume Wizard

Format Volume
You can customize the formatting of the partition

Specify whether you want to format this volume.

○ Do not format this volume
● Format this volume as follows:

Formatting
File system to use: NTFS
Allocation unit size: Default
Volume label: New Volume
☑ Perform a Quick Format
□ Enable file and folder compression

Figure 41. Creating a Volume

Power Requirements

Model Number	Power Specification
WBNMUPRO	115V/230V~, 50Hz-60Hz, 8A/5A

Installation

The WideBand nMU has no serviceable parts inside.

This equipment must be connected to a controlled power circuit offering short-circuit and Overcurrent protection.

Electromagnetic Compatibility

The WideBand nMU is certified with the following standards:

- FCC/ CISPR Class A
  - Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment 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 will be required to correct the interference at this own expense.
  - Any changes or modifications made by the user, which are not expressly approved by WideBand Corporation for compliance could void the user's authority to operate the equipment.
- CE Mark
  - EN55022: 1998
  - EN55024: 1998
- IEC 60950-1

Customer Service and Support

You may contact Customer Support in any of the following ways:

Phone: (toll free) (888) 220-4020
Email: techsupport@wband.com
USPS WideBand Corporation
401 West Grand
Gallatin, MO 64640-1133

Customer Support Hours: Mon-Thu 7 a.m. to 7 p.m. Central Time
Fri 7 a.m. to 5 p.m. Central Time