

Korenix JetNet Industrial Managed Switch 4000 and 4500 SOFTWARE VERSION 2.12 RELEASE NOTES

Before Upgrade

Before you use the Switch firmware, please ensure that you know the product number and use the correct firmware version. By reading the file, you can know the new feature and changes, the fixed bugs and the restrictions. You can find the latest firmware in the Korenix web site, <http://www.korenix.com> or get the help from Korenix Customer Support, Korecare@korenix.com.

About This Software Version

Release Date: Nov. 22, 2007

This firmware V2.12 provides support for the following products:

- JetNet Industrial Managed Ethernet Switch 4508
- JetNet Industrial Managed Ethernet Switch 4508f
- JetNet Industrial Web-Managed Ethernet Switch 4008
- JetNet Industrial Web-Managed Ethernet Switch 4008f
- JetNet Industrial Web-Managed Ethernet Switch 4005
- JetNet Industrial Web-Managed Ethernet Switch 4005f

The software is available in below versions:

- 4508_v212.bin — The firmware V2.12 for JetNet 4508
- 4508f_v212.bin — The firmware V2.12 for JetNet 4508f
- 4008_v212.bin — The firmware V2.12 for JetNet 4008
- 4008f_v212.bin — The firmware V2.12 for JetNet 4008f
- 4005_v212.bin — The firmware V2.12 for JetNet 4008
- 4005f_v212.bin — The firmware V2.12 for JetNet 4008f

CAUTION: *You can only update the correct firmware to the JetNet switches. Ensure the product model number before you start updating.*

The release notes include the below items:

- New Change and Improvement
- Fixes for Known Faults
- Known Restrictions or Limitations
- Updating the Switch Software
- Release History

New Changes and Improvement:

The following changes apply to the version V2.10 (Nov. 22, 2007):

To filter the non-(224.0.0.0-239.255.255.255) multicast stream. Ex: 1.1.1.1, 2.x.x.x... multicast stream will be filtered.

The following changes apply to the version V2.08(4508)/V2.09(4508f) (Nov. 16, 2006):

Add the Power Alarm in our private MIB.

The following changes apply to the version V2.04 (Jul. 4, 2006):

Private MIB enhancement: Add IGMP multicast table display and Couple Ring / Dual Homing setting in private MIB.

The following changes apply to the version V2.01 (Apr.1, 2006):

Start to support the JetNet Commander. JetNet Commander is a tool for supporting devices discovery, group firmware update, backup and restore... You must update the firmware to V2.01 then you can manage the devices by JetNet Commander.

For fixing the Rate Control can't work with QoS restriction. The new Rate Control design removed 16M, 32M and 64M settings. The rate can only support 128K, 256K, 512k, 1M, 2M, 4M, 8M.

Change the default RSTP mode to "Enable".

Change the default Rate Control mode to "Broadcast Only" with "8M" rate.

Change the display of the SysLog Client mode. The latest log appears in the top of the message field.

Add CPU protection mechanism. When the broadcast storm exceeds the threshold, the CPU protection mechanism will filter them.

Remove the System Name/Location/Description setting from the SNMP configuration page. Combine the settings to the Switch Settings page. In the new 4500 Switch Setting page, it provides "System Description/ System Name/ System Location and System".

When change it, the related OIDs will also be changed.

In the new 4000 Switch Setting page, it also provides "System Description/ System Name/ System Location and System" settings, but they can only be activated for local.

Improve dual homing in 4500 series. Set my homing port forwarding when remote homing port has no response.

Correct the fonts in QoS and Rate Control web pages.

Fixes for Known Faults

The following fixes apply to the version V2.12 (4508/4508f/4008/4008f/4005/4005f) (May. 20, 2008):

Fixed Fault LED sometimes incorrectly turns on when switch startup issue.

The following fixes apply to the version V2.08(4508)/V2.09(4508f) (Nov. 16, 2006):

Std MIB: Can't change value in dot1dStpPort.

Std MIB: Can't display Root Bridge well in Standard MIB issue.

Add the Power Alarm in our private MIB.

Fixed the Power Alarm trap display error issue.

The following fixes apply to version 2.06. (Sep. 9, 2006)

Fixed the firefox (Web browser) display issue.

The following fixes apply to version 2.03 (Jun 19, 2006).

Intermediate version for changing Model number. Internal use only, not released version.

Note: In V1.x version, the switch didn't check the model number. In V2.x version, the switch can check the model number. So, if some of the customers mis-upgrade the 4008/4508 V1.x to 4008f/4508f V2.x, then they can't recover and may have unexpected problem. The V2.03 is the intermediate version just for changing the firmware from 4008/4508 to 4008f/4508f, or 4008f/4508f to 4008/4508.

The following fixes apply to version 2.02 (May. 22, 2006).

Fix the MAC address was changed when restoring other switches' configuration file. In V2.01, when you restore the configuration file downloaded from device 1 to device 2, the MAC address of the device 1 will replace the MAC address of device 2. Then the 2 devices have the same MAC, it may lead the MAC address conflict problem.

The following fixes apply to version 2.01 (Apr. 1, 2006).

Fix the wrong VID and priority number in VLAN tag replied from the CPU.

Fix the CPU can't be ping under heavy broadcast traffic. Use the CPU Broadcast storm protection mechanism to guarantee the CPU resources.

Fix the device can't be managed after RSTP port failure and recover. Enhance the RSTP Edge port detection state machine which may lead the MAC address table didn't refresh correctly after RSTP port failure/recover.

Fix the wrong port ID in SNMP Link Up/Down Trap issue.

Fix the CPU interface ID to 9 for the SNMP Bridge MIB.

Fix the interoperability issue between the JetNet and IntraVue SNMP browser.

Fix the problem that the "Disable" IGMP snooping can't refresh all the learnt Multicast groups. Multicast stream may not be forwarded when this problem occurs.

Fix the JetNet can't transmit the multicast stream smoothly issue. Correct the learning behavior for the IGMP control packets.

Fix the Dual Homing ports can't work well with upper devices issue. The symptom is the Dual Homing show Link Up/Down periodically (about 2 mins).

Modify the latest help pages.

Known Restrictions or Limitations

The following restrictions or limitations apply to JetNet 4000/4500 series.

Wait until the system go to "System Reboot" page. Since the JetNet only provide one firmware version in the flash, when the firmware transmitting is complete, the system will erase the old firmware then write the new firmware to the flash automatically, reboot or unexpected shut down will lead the switch lost its firmware.

Known Interoperability Issues when implementing Super Ring Dual Homing with 3rd Party RSTP ring. When implement Dual Homing with other 3rd party switches, the link change of the Super Ring may not be aware by the 3rd party switches, the MAC address of their physical ports may not be refreshed soon. The traffic will not recover soon and need to wait until the MAC address table ageing timeout. Before implementing the function, please do the lab test to confirm first. **Note that using Korenix switches in both the RSTP and Super Ring will not have such problem.**

Known Interoperability Issues when implementing Super Ring Dual Homing with Cisco Switch (3500). If you disable the Ring Master (Turn off the R.M. Dip) of the Super Ring, the Super Ring will be a loop environment and flood storm streams in the ring. When Cisco switch detects the storm stream in the Dual Homing ports which attached to the Cisco switch. Cisco will disable the 2 ports and you should manually re-enable the 2 ports in UI even when the storm steam stopped. Since this is Cisco private design, we can't ask the switch ports become enable by sending packets. So, **Note 1** that making sure your enable the R.M. of the Super Ring before connect the Ring in a loop, otherwise you'll encounter such problem when connecting with Cisco switch. **Note 2** that when connecting Dual Homing ports to 3COM device or other device which doesn't support such mechanism, the problem wouldn't occur.

The limit packet type of the Rate Control Egress rule is "All" packets. This is the chipset limitation.

Due to the CPU power limitation, we add CPU protection mechanism to the CPU interface to guarantee the CPU have enough power to perform the switch protocols mechanism and wouldn't be easily effected by the broadcast storm. But, since the ARP packet is also one kind of broadcast in the network, we can't specifically separate the ARP packets from the broadcast traffic. The symptoms include:

1. When the broadcast traffic exceeds the threshold, sometimes the client PC can't ping the switch IP address due to CPU can't receive the ARP packet from clients. In our lab test, the threshold is around 4 MB continuously broadcast storm(DA=FFFFFF FFFFFF, Packet Size = 64 bytes) stream. As long as the PC learnt the ARP, the problem will disappear.
2. Under the same condition (4M broadcast storm), the restriction wouldn't be found

when client PCs ping remote PCs. The CPU power of the PC is faster than switch's CPU power. The threshold is according to the CPU power of the PCs.

3. In practical term, the problem is hardly to see unless you inject the broadcast storm from the packet generator. There is internal gap time between all the ethernet packets, most of the clients can't generate such continuous and critical packets. The ARP request/reply time from the PC to the CPU is very short around few mini second. As long as CPU learnt the ARP. The problem will disappear. And, if the broadcast traffic is really very heavy in your network, not only the switch will be effected but also the running applications/client PCs will also be effected. The way to avoid this is to find out the source of the broadcast storm and terminate the broadcast storm stream.

The rate of the Rate Control only support 128K, 256K, 512k, 1M, 2M, 4M, 8M. This is the chipset suggestion.

Updating the Switch Software

To update the software on the Switch:

1. Download the firmware for your switch.
2. If you haven't installed the TFTP server in your management station, download the TFTP server applications and install it on the management station.
3. Launch the TFTP server application.
4. Point the Upload/Download default directory on the TFTP server to the directory where the upgrade file is located.
5. Make sure the switch being upgraded has an IP address assigned to it. Default IP is **192.168.10.1**.
6. Access the Web management UI of the switch.
7. Log into the Switch management.
8. The default user name is **admin**, the default password is **admin**.
9. From the top-level menu, select **TFTP Update Firmware** page.
10. Enter the **TFTP Server IP address** of the TFTP server connected to the Switch.
11. Enter the upgrade **Firmware File name**.
12. Click "**Apply**" to start the upgrading process. You can see the firmware file transmitting on the TFTP server application.
13. When the software upgrade is complete, the system will write the new firmware to the flash automatically. **Note that the process will erase the old firmware then write the new firmware, reboot or unexpected shut down will lead the switch lost its firmware.**
14. After writing to flash, the management UI will go to "**System Reboot**" page and ask you to reboot the switch.
15. Please click "**Reboot**" to run the new firmware. **Note that without rebooting the switch, the switch will still run the old firmware and configuration.**

Note 1: When initiating a TFTP upgrade using the Web interface, if an incorrect TFTP server IP address or software upgrade file name is entered, the process will be terminated about 30 seconds. Or you can correct the IP address or file name and press "Apply" to restart the process again.

Note 2: When attempting to upgrade the incorrect software on the unit, it may report the following error:

TFTP server not found or incorrect firmware image file.

If you encounter this error, please find out the correct version for your product, correct file name and apply the command again.

Note 3: Should you forget the Admin username and password, IP address of the device you want update, you can press the "Reset" button to reset the configuration to default. The default IP is 192.168.10.1. Default username is Admin, password is "Admin" as well.

Release History:

4008/4008f		4508	
Version No	Release Date	Version No	Release Date
V2.01	Apr. 1, 2006	V2.01	Apr. 1, 2006
V2.02	May. 22, 2006	V2.02	May. 22, 2006
V2.03	Jun. 19, 2006	V2.03	Jun. 19, 2006
V2.04	Jul. 4, 2006	V2.04	Jul. 4, 2006
V2.06	Sep. 9, 2006	V2.05	Aug. 28, 2006
V2.10	Nov. 22, 2007	V2.06	Sep. 9, 2006
V2.12	May. 20, 2008	V2.08	Nov. 16, 2006
		V2.10	Nov. 22, 2007
		V2.12	May. 20, 2008

4005/4005f		4508f	
V2.01	Apr. 1, 2006	V1.08	Feb. 14
V2.06	Sep. 9, 2006	V91.12	Feb. 21
V2.12	May. 20, 2008	V2.00	not yet
		V2.01	Apr. 1, 2006
		V2.02	May. 22, 2006
		V2.03	Jun. 19, 2006
		V2.04	Jul. 4, 2006
		V2.05	Aug. 28, 2006
		V2.06	Sep. 9, 2006
		V2.09	Nov. 16, 2006
		V2.10	Nov. 22, 2007
		V2.12	May. 20, 2008