MICROSENS
fiber optic solutions

Industrial Ring Networks

Function and configuration

Version: 0.91

Author: Hannes Bauer

Date: 17. Oct. 2005

MICROSENS confidential

Index

Industrial Ring Networks

Summary

This paper describes the basic functionality and the configuration of MICROSENS redundant ring networks and redundant link segments in practical steps. The reader should be familiar with basic networking and the MICROSENS Device Manager software. A section with typical questions and answers helps for planning and troubleshooting of reliable networks.

1. Introduction

Ring structures are widely deployed in WAN infrastructure for a long time.

Compared to star-based networks known from the LAN area, they offer several advantages:

Reduced equipment

All nodes work in an add/drop way, no central office and equipment is required.

Optimized cabling

Especially in large area applications star based cabling requires the massive parallel deployment of cabling from the central office. A ring topology reduces the cabling requirements dramatically, as only adjacent nodes need to be interconnected.

High Reliability

A ring network is distributed over all nodes, there is no single point of failure.

The ring structure ensures that even in the case of a failure of a connection or a full node all nodes remain interconnected. A redundancy protocol redirects the data traffic so all nodes can communicate with each other.

1.1 Ethernet Implementation

As Ethernet is a classical LAN protocol, it is based on a point-to-point star cabling topology.

Physically cabling a standard Ethernet network in a ring structure results in an immediate breakdown of the network as data packets would travel around the ring infinitely and multiply themselves when travelling along.

Protocols like Spanning Tree can detect redundant paths in the network, but they react slowly and are not optimized to handle ring structures.

To build a fast, robust and reliable ring network based on Ethernet technology, special functionality to handle the failure recovery process must be added.

2. Redundant Ring

As Ethernet does not support the operation of physical rings, additional intelligence must be added to the network to do so. To prevent network-loops when physically closing an Ethernet segment to a ring, logically the segment must remain open. This behaviour is controlled by one device in the ring, the so-called ring-master.

2.1 Redundant Ring - normal operation

Under normal operating conditions, the ring-master logically separates the ring on its ports to prevent any uncontrolled cycling of packets in the physical ring. So the ring works as a normal Ethernet network with all switches daisy-chained starting and ending with the ring-master. Only one ring-master per ring is allowed as otherwise the ring would be separated into isolated segments. All other devices in the ring must be working as ring-slaves.

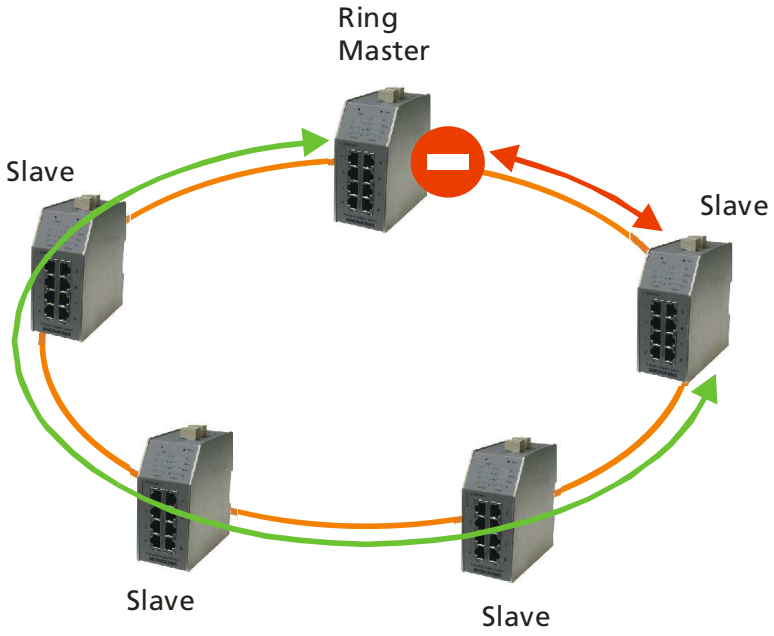

Figure 1: Redundant ring - normal operation

As the normal operating state is stable, no additional traffic for control packets or signalisation is generated, so the full bandwidth is available for user traffic.

2.2 Redundant Ring - failure operation

In case of failure of a link-segment or of a full device in the ring, this failure is detected by the adjacent devices on the absence of the link signal. These devices now start signalling this failure condition by sending special alarm packets to the master. Upon the reception of such a packet by the ring-master, the master closes the internal logical separation between its ring ports, re-establishing the interconnection of all remaining working devices in the ring. As long as the error condition in the ring exists, the adjacent devices periodically send alarm packets to the ring-master. When the ring is re-established, the devices automatically stop sending the alarm packets. When the master notices this by a timeout, it falls back into the normal operation condition and logically separates the ring again.

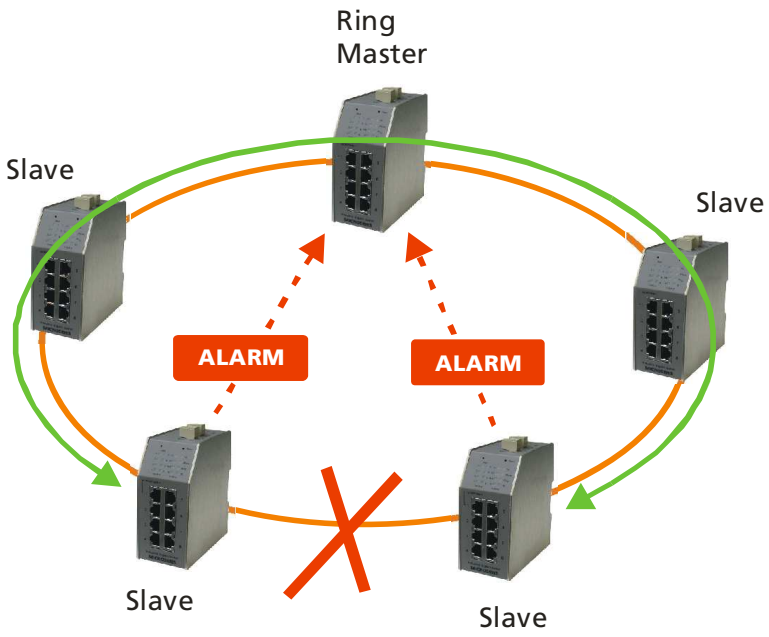

Figure 2: Redundant ring - failure operation

This automatic behaviour is absolutely stable and requires no manual intervention once a ring is configured.

The alarm notification packets sent out in case of a failure have the minimum Ethernet packet size and are repeated every 10 ms. In total the additional load generated by this traffic is below 0.1% of the total capacity.

2.3 Configuration of redundant rings

All new ring switches shipped have the ring functionality disabled, they behave as normal Ethernet switches. When installing these devices in a ring before they are configured correctly, care must be taken not to close the physically to prevent uncontrolled behaviour of the network.

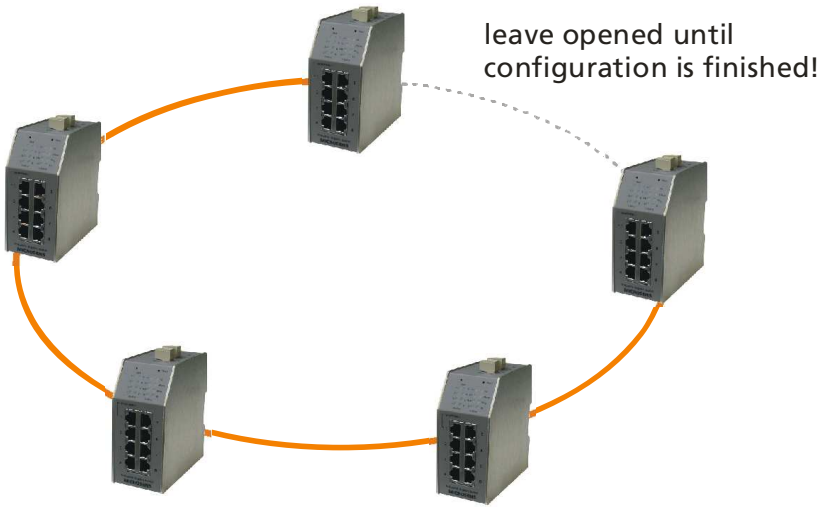

Figure 3: Ring cabling for configuration

Best practice is to install the devices in their original position and to open the cabling in one position (Figure 3).

For further configuration a PC with the latest version of the MICROSENS Device Manager Software running is required.

The ring is configured in 4 basic steps:

1. Assigning an initial IP Address to each ring switch
2. Configuring all switches as rings-slaves
3. Configuring one switch as ring-master
4. Physically close the ring

In the following, these four steps are outlined in detail:

2.3.1. Assigning an initial IP-address to each ring switch

As the devices are not configured, the IP-stack is disabled. To access the devices from the Device Manager, an individual IP-address must be assigned to each device first. To do this, the reset button of each device must be pressed for approx. 10 seconds. When doing this, a PC with the Device Manager software running must be connected to the device or to the network segment the device is connected to. When releasing the reset button, the device sends an IP-configuration-request message to the Device Manager, where a configuration window opens up. Now the basic IP settings can be done. By pressing the send button, the new settings are permanently stored in the device.

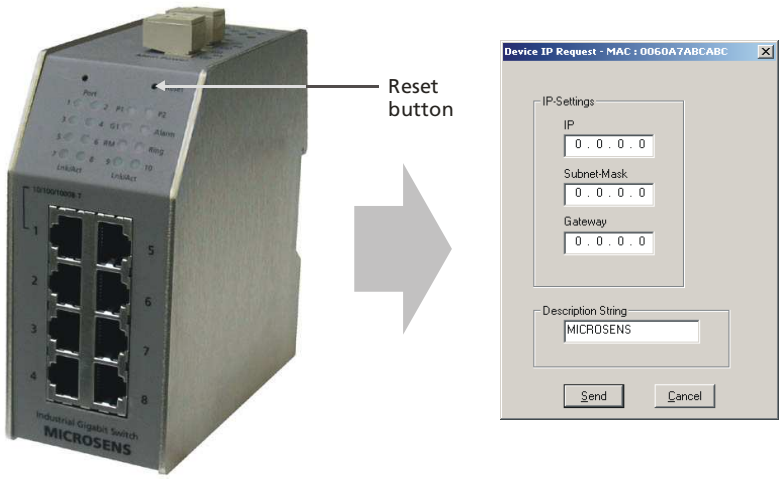

Figure 4: reset button for IP-configuration-request

Once this procedure is finished for each device, all further configurations can be done from the Device Manager Software without the need for a physical access to the device.

2.3.2. Configuring all switches as ring-slaves

To see all initialized switches in the Device Manager, the Auto-Discovery process must be started by pressing the corresponding toolbar-button.

Now all switches should appear in the device list window.

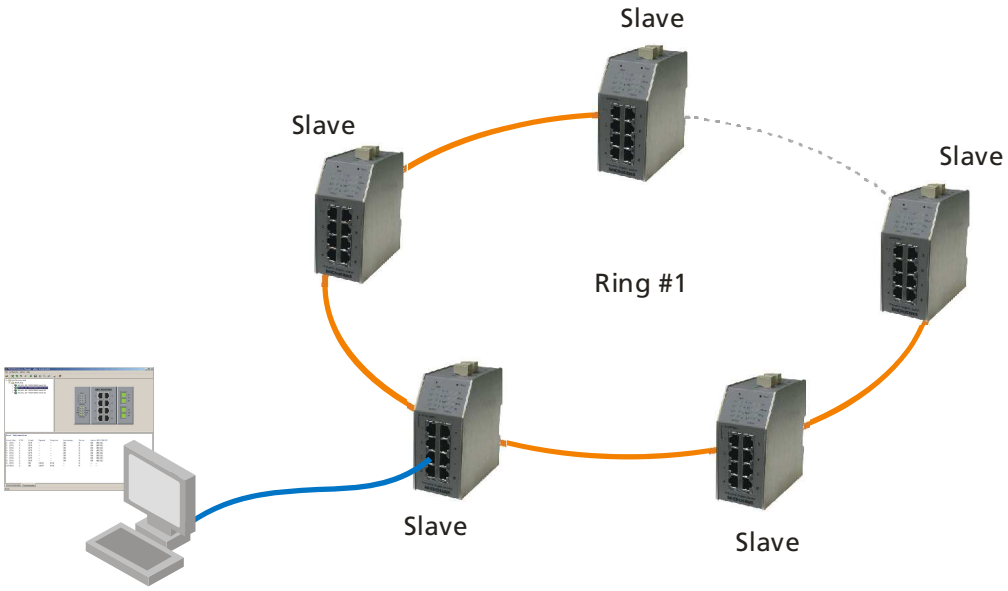

Figure 5: Configuring all switches as slaves

To configure the switches, right click on one switch in the device list and choose ‘Get from current’ from the context menu to load the current configuration from the switch into the Device Manager.

Now choose Configuration/Edit/Hardware Settings from the menu or press the corresponding toolbar-button to open the hardware-configuration window.

Figure 6: Standard configuration for all ring switches

The hardware-configuration-window has a section for the ring-configuration.
Three values can be set:

1. Ring mode enabled/disabled

This field activates the ring mode – select enabled

2. Ring-Master/Ring-Slave

This field configures the ring mode – select Slave

3. Ring-Number

To prevent interference in multi-ring environments, each ring must have a unique ID-number. Enter '1' or any other number.

Once these settings are made, they must be applied to all devices in the ring. Choose 'Apply Configuration' and select 'All devices' .
Now all ring switches are set to ring mode with slave functionality.

2.3.3. Configuring one switch as ring-master

Figure 7: Select 'Master' for ring mode

Reopen the Hardware-configuration-window (Configuration/Edit/Hardware Settings) and select 'Master' in the ring mode field.

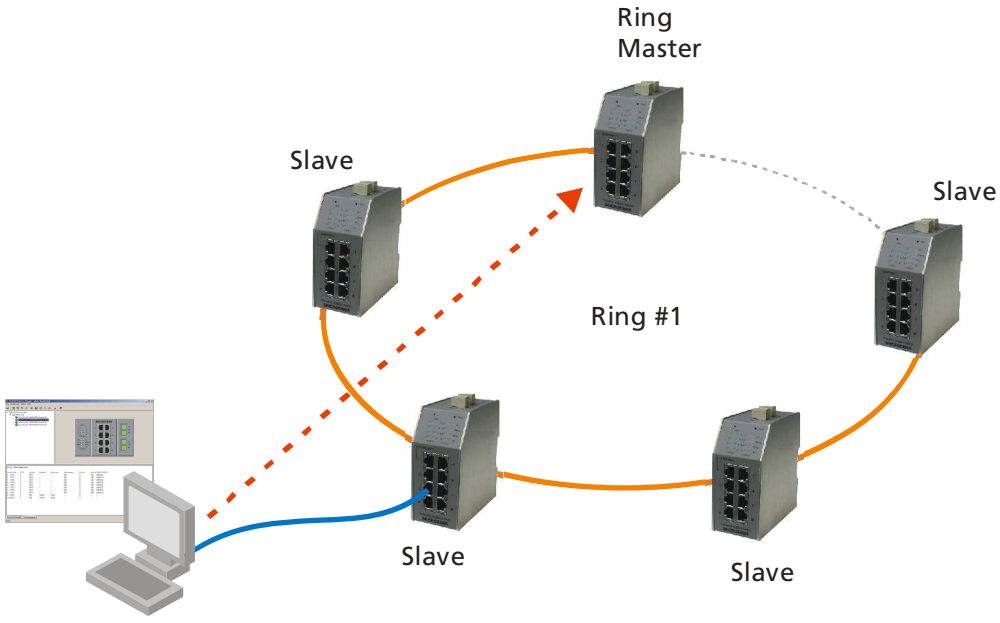

Figure 8: Configuring one switch as ring-master

Right click on the switch you want to be the ring-master device in the device list and chose 'Apply Configuration' and select 'current device' from the selection box.
Now one switch in the ring is configured as master, all others are configured as slaves.
Congratulations - the ring configuration is now completed.

2.3.4. Physically close the ring

As all devices are configured correctly, the ring can be closed physically by connecting the segment left open during the configuration cycle.

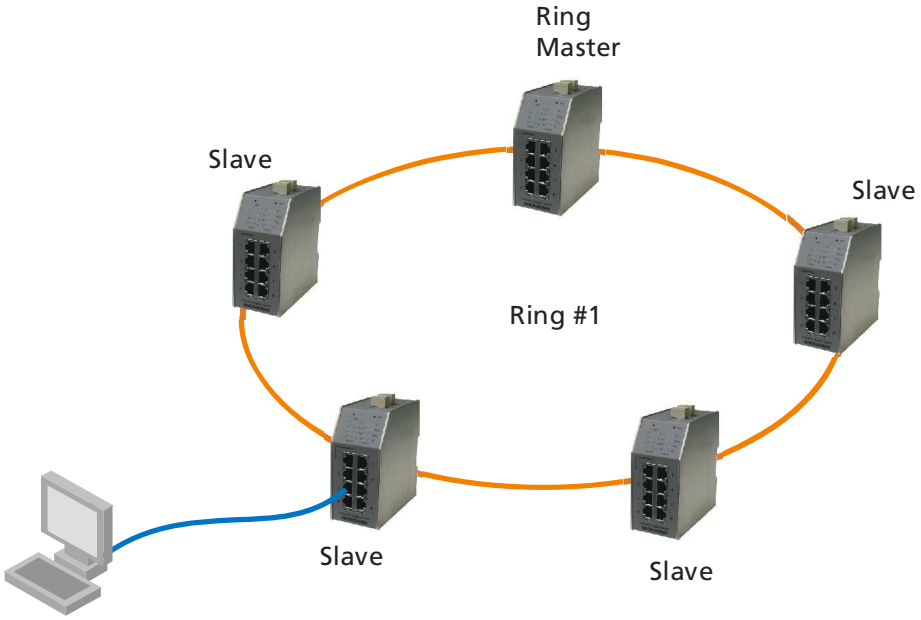

Figure 9: Physically close the ring – configuration completed!

As the ring behaviour works fully automatic, no more interference with the switches during operation is required. Upon a ring failure, the master will reconfigure the ring, when the ring is closed again, the master will automatically fall back into normal operation state.

3. Multi-Ring Networks – Redundant Uplink

3.1 Introduction

For practical reasons it is often desireable to separate the network into several interconnected rings, e.g. to have several sub-rings connected to a main-ring.

Special care must be taken for these interconnections, as they must exhibit the same failure tolerance as the rings themselves.

Connecting two rings just in one location results in a single point of failure. If the interconnecting device fails, the rings themselves remain operating, but their interconnection is lost.

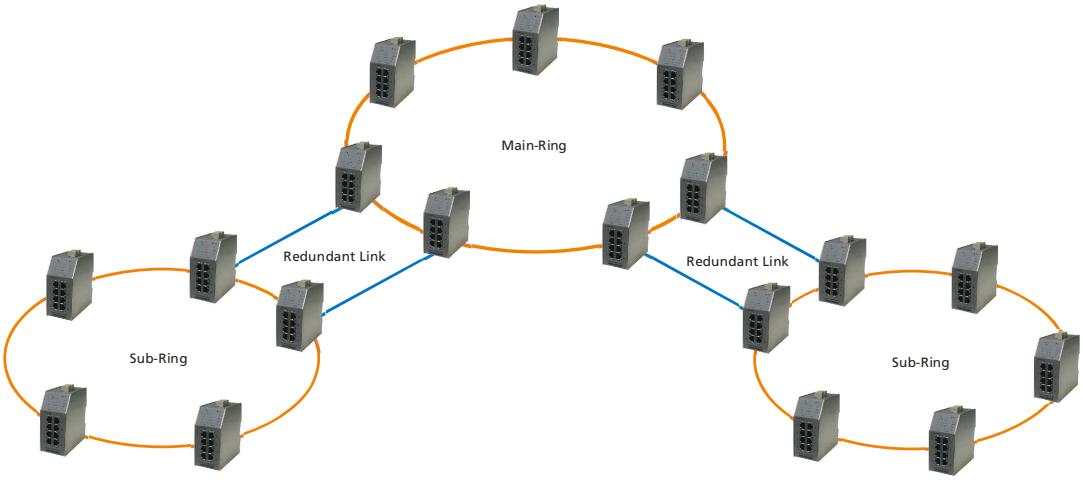

Figure 10: Main-/sub-rings interconnected by redundant links

To prevent such a situation, the rings must be interconnected by two independent connections. To prevent loops in the network, a special redundancy protocol is used to make sure that only one link is active at a time.

If the main-link between the rings fails, the backup-link becomes active automatically, maintaining the interconnection of the rings.

3.2 Redundant link - normal operation

Similar to the ring configuration one interconnection node is configured as main-link controller, as the other node is configured as backup-link controller.

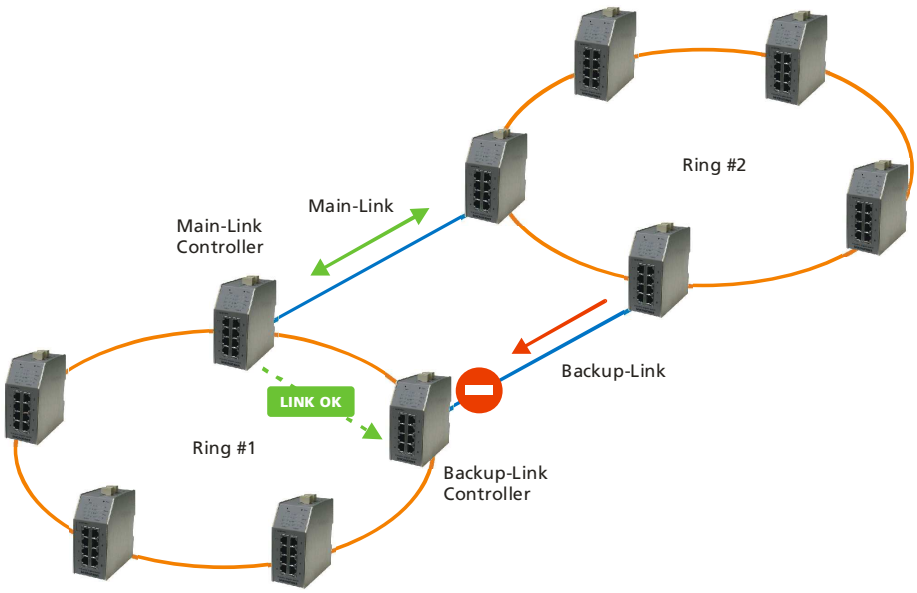

Figure 11: Redundant link – normal operation

Under normal operating conditions the main-link is active whereas the backup-link is logically blocked. All traffic between the rings flows through the main-link controller node. The main-link controller periodically sends a link status message to the backup-link controller indicating whether the main-link is active or not.

3.3 Redundant link - failure operation

If the main-link fails, the main-link controller logically blocks the uplink port and sends a link-fail message to the backup-link controller.

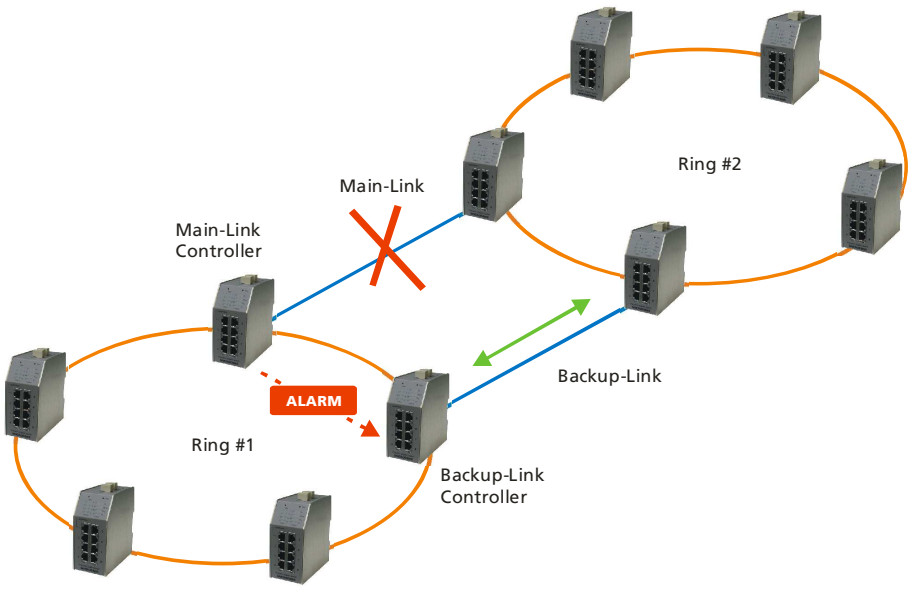

Figure 12: Redundant link – failure operation

Upon the reception of such a message, the backup-link controller logically activates the uplink until it receives a main-link-ok message from the main-link controller again. If the main-link controller should fail completely, the backup-link controller will notice this by a timeout in the reception of link-status messages and activate its uplink accordingly.

3.4 Configuration of redundant links

As with the redundant uplink functionality, also the redundant link function is disabled on new devices. To prevent network-loops, the redundant link must only be connected after the configuration has been completed.

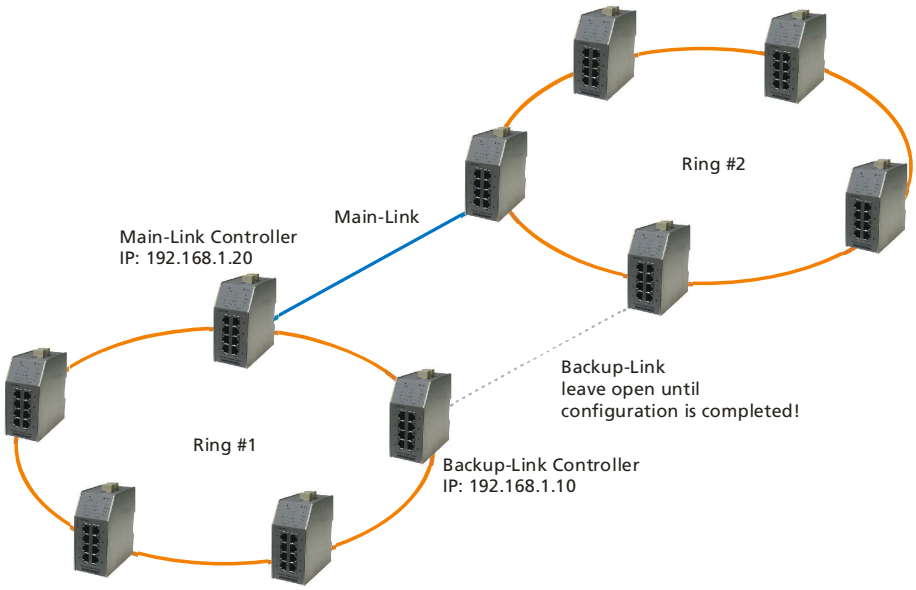

Figure 13: Redundant link configuration

The redundancy feature of the link is controlled from one side of the link, so only two switches have to be configured. The switches on the opposite side of the link react automatically and don't need to be configured.

Assuming that all switches have already been initialized for the ring configuration and are visible in the Device Manager, the link configuration can be done in three steps:

1. Configuring the main-link
2. Configuring the backup-link
3. Physically closing the redundant connection

In the following, these three steps are outlined in detail:

3.4.1. Configuring the main-link

Right click on one switch to be the main-link controller in the device list and choose 'Get from current' from the context menu to load the current configuration from the switch into the Device Manager.

Now choose *Configuration/Edit/Hardware Settings* from the menu or press the corresponding toolbar-button to open the hardware-configuration window.

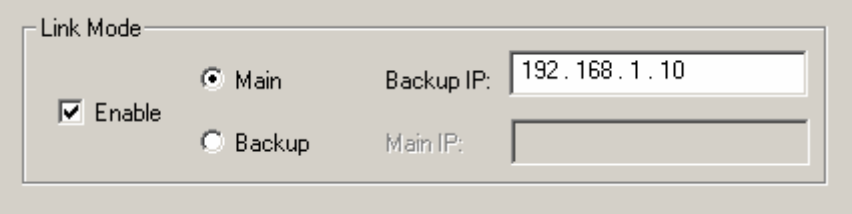

Figure 14: Main-link controller configuration

The hardware-configuration-window has a section for the link-configuration.

Three values can be set:

Link mode enable/disable

This field activates the ring mode – check Enable

Main-/Backup-Link

This field configures the controller mode – select Main

Backup IP Address

For the link status communication, here the IP address of the second link controller must be entered. Enter the IP address of the backup-link controller.

Once these settings are made, they must be applied to the switch. Choose 'Apply Configuration' and select 'Current device' .

Now the switch is configured as main-link controller..

3.4.2. Configuring the backup-link

Right click on one switch to be the backup-link controller in the device list and choose ‘Get from current’ from the context menu to load the current configuration from the switch into the Device Manager.

Now choose *Configuration/Edit/Hardware Settings* from the menu or press the corresponding toolbar-button to open the hardware-configuration window.

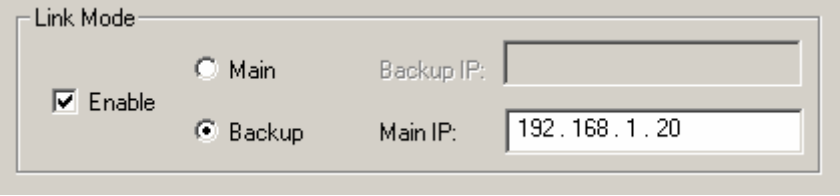

Figure 15: Backup-link controller configuration

The hardware-configuration-window has a section for the link-configuration.

Three values can be set:

Link mode enable/disable

This field activates the ring mode – check Enable

Main-/Backup-Link

This field configures the controller mode – select Backup

Backup IP Address

For the link status communication, here the IP address of the second link controller must be entered. Enter the IP address of the main-link controller.

Once these settings are made, they must be applied to the switch. Choose ‘Apply Configuration’ and select ‘Current device’ .

Now the switch is configured as backup-link controller..

Congratulations - the link configuration is now completed.

3.4.3. Physically closing the redundant connection

As both controllers are configured correctly, the link can be closed physically by connecting the segment left open during the configuration cycle.

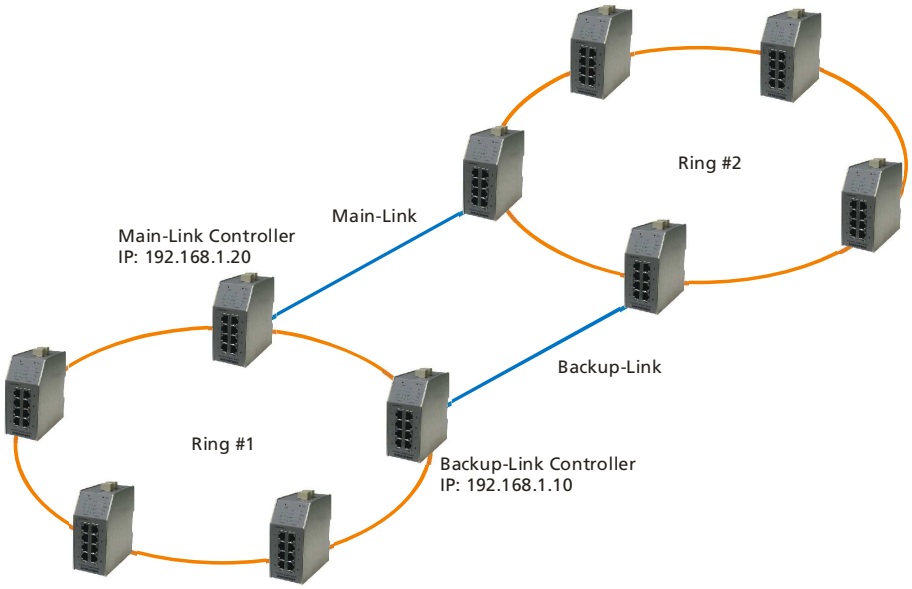

Figure 16: Physically close the redundant link – configuration is completed!

As the link behaviour works fully automatic, no more interference with the switches during operation is required. Upon a main-link failure, the controllers will reconfigure the link, when the main-link is up again, the controllers will automatically fall back into normal operation state.

4. Frequently asked questions

Q: How fast is the ring reconfiguration time in case of a failure?

A: For Gigabit Ethernet (1 Gbps) rings: 20 ms

The reaction time is measured from the moment of link loss of a defective segment up to the moment the master has restored the Ethernet path. The values given are maximum values for a typical ring with 10 nodes and medium loaded traffic. The number of nodes in the ring, the length of the ring segments and the traffic load on the ring can affect the reconfiguration time, as the alarm notification packets from the slaves to the master can be delayed. For details see the next question and answer.

Q: How is the ring reconfiguration time affected by the size of the ring?

A: Each additional switch and each additional fiber adds latency to the transmission of the alarm notification packets from the slave to the master.

1. Delay caused by switch packet forwarding

Each switch in the ring forwards packets in store-and-forward mode. That means each packet entering the switch is first stored in the internal buffer completely before it is sent out again.

Alarm notification packets are mimimum sized Ethernet packets (64 bytes), so their delay is relatively short, but in worst case scenario they have to wait for a number of maximum size packet in the buffer to be transmitted first. The following table shows the typical delays for 100 Mbps and 1 Gbps networks:

Delay type	**Ring Speed Gigabit Ethernet (1 Gbps)**
Switch processing delay	3 µs
Minimum Packet (64 Bytes) (no load)	0.85 µs
Maximum Packet (1500 Bytes) (low load)	12,5 µs
10x Maximum Packet (heavy load)	125 µs

Table 1: Delays caused by switch packet forwarding

Assuming 10 maximum sized packets in the buffer is a worst case scenario occurring only at highly loaded networks.

2. Delay caused by length of fibers

The speed of light in an optical fiber is roughly 2/3 of the vacuum speed of light, resulting in a signal delay of approx. 5 ns per meter of fiber.

The following table shows the resulting signal delay for typical fiber distances:

Fiber Distance	Signal Delay
1 m	5 ns
100 m	0.5 µs
1 km	5 µs
10 km	50 µs
100 km	500 µs

Table 2: Delay caused by length of fibers

These values are independent from the data rate. For large-area application these values can become relevant.

Q: Is the number of switches per ring limited?

A: Theoretically not, there is no technical limit for the number of switches in a ring. But there are practical limits that should be considered:

1. The bandwidth of the ring is shared among all switches. The larger the ring, the lower the available bandwidth per switch gets.
2. Each ring works in store-and-forward mode, so each node adds latency to a packet travelling along the ring. For latency critical applications (Voice over IP, real-time control etc.) the maximum allowed latency must be considered.

From our experience we recommend a practical ring size of 20 switches.

Q: What is the minimum number of switches per ring?

A: The smallest possible ring can be build by two switches connected together in parallel on the two ring ports. Functional this would rather be called a redundant connection between the two switches than a ring.

Q: Can ring switches and standard switches be mixed in the same ring?

A: As the ring is an Ethernet network, it is theoretically possible to integrate standard (non-ring) switches into it. We do not recommend this, as you are losing the fast failure recovery functionality.

In case of a ring failure, the data traffic must be rerouted. Ring switches do this by reconfiguring their internal MAC-table in case of a failure event. Normal switches will eventually not notice the change of the network structure and forward data incorrectly. This will last until the internal aging timer has deleted the old MAC-address entries. As the normal aging time is several minutes, the ring will not work correctly during this time period.

Q: What happens if the ring-master fails?

A: Nothing. As the ring-master separates the ring logically under normal operating conditions, this separation is maintained when the master fails. Of course there is no more redundant behaviour, but generally the redundancy can compensate only one failure in the ring, and this is already the case when the master has failed.

Q: What happens if there are two ring-masters in the same ring?

A: There is only one master per ring allowed. A second master would distort the correct function of the ring. As the master logically separates the ring, a second master on the same ring would add a second separation of the ring, resulting in two ring segments that cannot communicate with each other.

Q: Where should the ring-master be located in the ring?

A: Basically any switch in the ring can be configured as ring-master or slave, the only special function of the master is the control of the redundancy behaviour.

When designing a ring network with centralized data traffic, there is often a tendency to put the ring-master in the location of the central uplink or the main server of the ring. This is not always beneficial, as the ring-master is the start and endpoint of the switch-chain build by the ring. In worst case a packet entering the ring at the ring-master must travel the whole ring to reach the switch at the end of the chain.

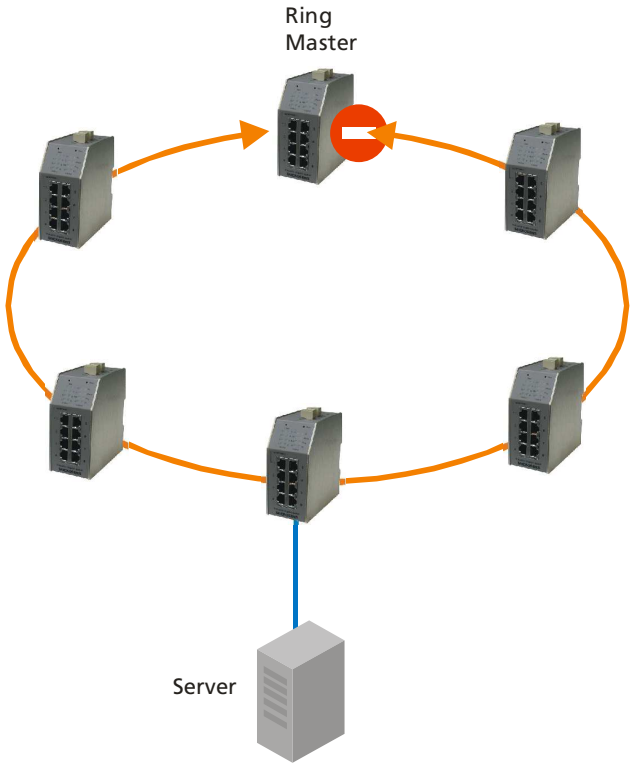

Figure 17: Locating the ring-master opposite the main traffic node.

Putting the central uplink or the main-server in the middle of the chain (on the switch located opposite to the master in the ring) balances the traffic on the ring, as all packets from and to the uplink must only travel half the ring in maximum.

5. Glossary

Aging	MAC-address entries in the MAC-table that are not used for a certain time are automatically deleted. The aging time is typically 3 to 5 minutes.
Ethernet	Transmission protocol family defined in IEEE Std. 802.3 standard.
Fast Ethernet	Ethernet protocol with 100 Mbps transmission speed.
Gbps	Gigabits per second = 1,000,000,000 bits per second.
Gigabit Ethernet	Ethernet protocol with 1 Gbps transmission speed.
IEEE	The Institute of Electrical and Electronics Engineers, Inc. Authority for the definition of international IT-Standards. Website www.ieee.org.
LAN	Local Area Network.
MAC	Media Access Control.
MAC-address	Unique number to address nodes in Ethernet networks.
MAC-table	Internal switch table used for forwarding of incoming packets. It stores the information which MAC-address is located on which port of the switch. It is automatically learned by the switch from the incoming data traffic.
Mbps	Megabits per second = 1,000,000 bits per second.
WAN	Wide Area Network.