

White paper

The Evolution of LAN Bypass Technology:
Lanner's Generation One to Generation
Three Bypass.

Lanner



Table of Contents

- 1 Introducing LAN Bypass
- 1 Earlier Bypass Generations
- 2 Generation Three Bypass
- 5 Proof of Improvement
- 6 Conclusion
- 7 Comparison Chart for the Three Generations of Bypass

Introducing LAN Bypass

Software stability is a major issue on any platform, but especially network appliances since it could affect the availability of a network. Anyone who uses software has most likely experienced problems that hang and/or force a reset of a computer or program. Such problems also occur in network appliances, and there may be times when there are no administrators around to get the appliance up and running again when things go wrong. The interruption of network connectivity could cause a tremendous loss in business even if it only lasts for a short period of time. Therefore, a method for out-of-band communication (i.e., communications that occur outside of a previously established communication channel) should be considered as a backup solution. Such out-of-band communications are most frequently enabled through a solution known as "LAN bypass."

Bypass Principles

LAN bypass is a fault-tolerance feature that protects your essential business communications in the event of power outage and/or system failure. In a system with LAN bypass, LAN ports are bridged together in pairs through mechanical relays. If the network appliance loses power, data traffic between the paired LAN ports can still continue and your network uptime is unaffected. The following graphic shows the difference between bypass and non-bypass status.

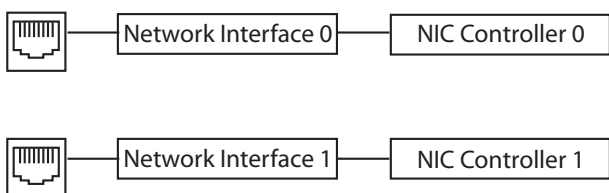


Figure 1: Non-bypass status. NIC controller is functioning normally.

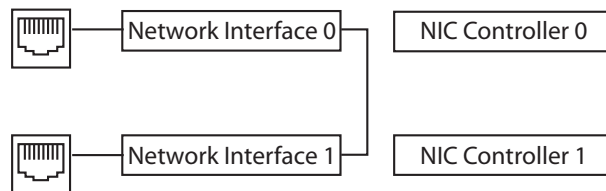


Figure 2: Bypass status. Ethernet network ports are disconnected from the system interfaces. A crossed connection loop-back between the Ethernet ports is established.

Earlier Bypass Generations

Lanner Electronics has for many years released products that offer LAN bypass features. Throughout these years, we have engineered increasingly advanced LAN bypass functions with the help of more intelligent microcontrollers and more powerful and flexible software implementations. We refer to the advances in LAN bypass technology as Generation One, Generation Two and Generation Three.

Generation One

In Generation One bypass, availability of the bypass function was controlled by a hardware jumper on the main board. When the jumper connected the two pins on the jumper block, bypass would be enabled when the system was powered off. If a system shut down, communication could still carry on. This is referred to as a system-off bypass. If the system was powered on, and the jumper was set to enable bypass, software could be used to switch bypass on or off as required.

But using a hardware jumper to enable this setting meant that bypass was always enabled when the system was turned off, even if software had been used to disable bypass. Changing this bypass setting required that the system was turned off and the chassis opened to remove the jumper. A more convenient solution for controlling the bypass status was needed. This led to the creation of Generation Two bypass.

Generation Two

In Generation Two, the hardware jumper was no longer necessary as a new design using a combination of latch relays and a program

that could alter the system BIOS was added. In this program, the system administrator could set the bypass to be enabled or disabled if the system shut down, and the relays would link the ports of bypass pairs. With no hardware jumpers required, these settings could also be changed remotely.

Another benefit in Generation Two was that the settings could be different for different bypass pairs. So one pair could have bypass enabled when the system shut down and another pair could have bypass disabled. In Generation One, every pair was forced to use the same settings.

For both the first and the second generation of bypass, it was possible to use a watchdog timer to enable bypass if the system had a glitch and hung.

Generally speaking, a watchdog timer is a computer hardware or software timer that triggers a system reset or other corrective action, such as enabling bypass. In the case of a system reset, if a crucial program hangs, the watchdog timer can automatically reset the system to bring it back to the normal state. In the case of bypass being the default action, with Generation One and Two bypass, this action precluded an automatic reset. Since the watchdog timer was shared between the bypass and the system, the watchdog could enable a bypass in the event of a hung system, but it could not also activate a reset. This means the watchdog could keep the network connection alive by linking the bypass pairs, but it could not reset the system so its other operations could continue. As a result, a system administrator would have to schedule some network downtime to personally reset the system and get it back up and running.

Generation Two had other shortcomings as well. In some cases, an administrator might want to set up a system to enable bypass when the system is running, but if the system hangs, have the bypass turn off. This was not possible on Generation Two.

There was also an issue with the Genera-

tion Two bypass when non-latch relays were used for connection ports in extremely critical communications networks. In these cases, there could be packet loss. This happened if a bypass pair was connected on a non-powered system. When the system was just turning on, the non-latch relay would make a small jump. This meant the bypass circuit was broken for about 0.3 milliseconds. While this was not long enough to adversely affect most networks, for some networks, the chance of losing any packets of data is unacceptable.

Generation Three Bypass

In the latest Lanner Generation Three bypass, a microcontroller has been added to give more flexibility and more advanced functionality to the bypass function. By using the non-volatile memory in this microcontroller, complex configurations can be stored regardless of the system's operating state.

Generation Three solves several of the issues described above. For one thing, the packet loss experienced with Generation Two when using latch relays to connect bypass pairs is now eliminated. Generation Three bypass delivers 100% lossless communications.

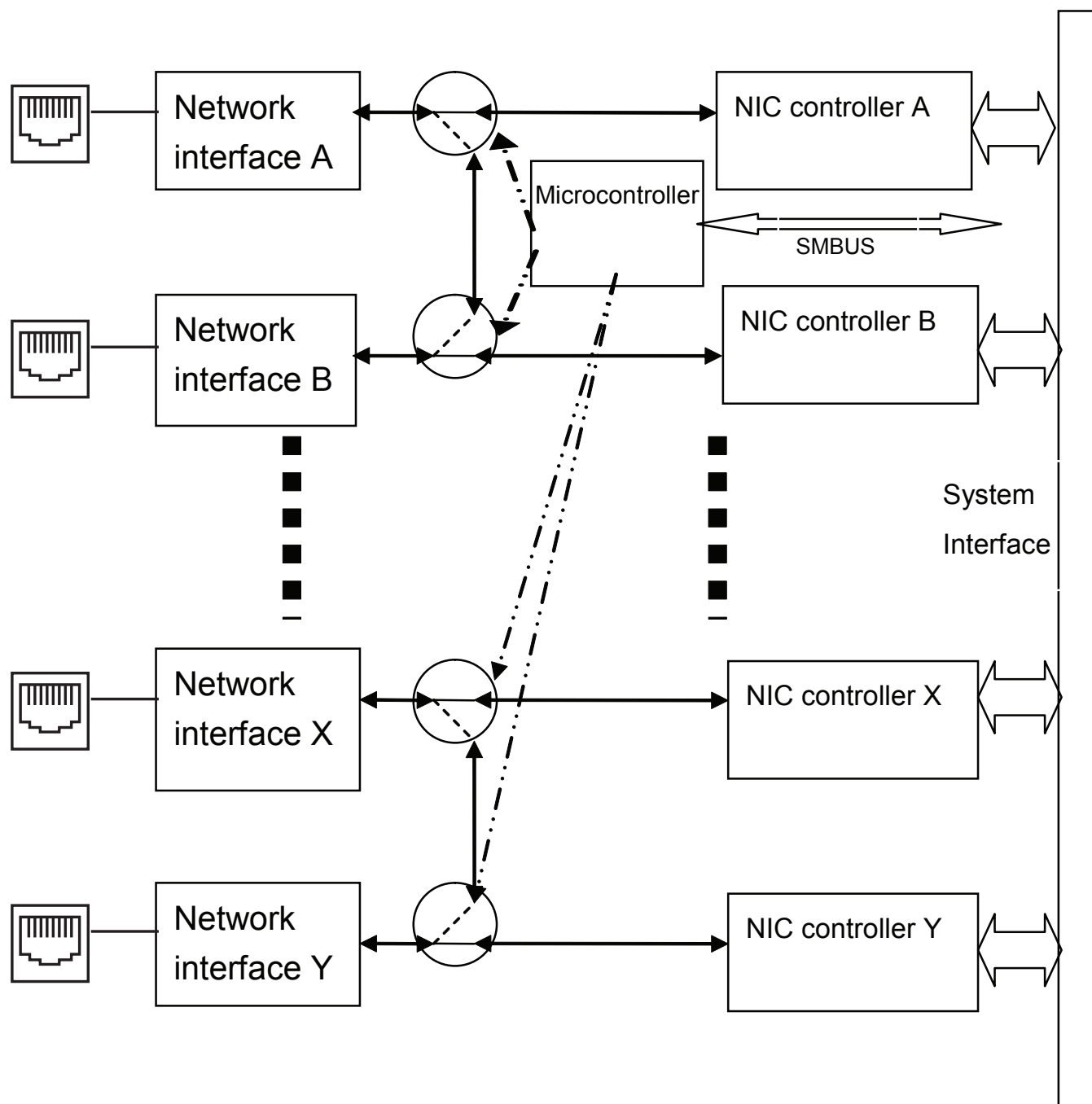
Generation Three also gives each pair of bypass ports their own watchdog timer to use at runtime with a standard setting from 1 to 255 seconds. This frees the system watchdog timer to handle automatic resets or other corrective actions other than bypass. The Generation Three runtime watchdog timers help software to detect abnormal system behavior, which can then be used to trigger the bypass function.

There is also a programmable timer switch that handles the bypass during the first few seconds when a system is turned on. From the moment a system turns on until it is fully booted, you can enable or disable bypass. In Generation Three it is possible to create a timer that decides during the first second of the start-up process whether the bypass should be disabled or enabled. (The setting

can be between 5 to 1275 seconds.) And it is all done conveniently from Lanner software. This is a useful function for systems where an automatic reset by a watchdog timer has occurred and bypass status needs to be controlled at all times.

System Diagram

The following diagram depicts the role and function of the microcontrollers in Generation Three bypass. Unlike Generation Two bypass, which communicates to the host system through a GPIO (General Purpose Input/Output), the Generation Three microcontroller communicates to the host system through the SMBus (System Management Bus)/I2C . Not using a GPIO offers a couple of advantages. First, the bypass implementation can be platform independent, so the same software works for all Intel® processors and platform controller hubs. Second, it saves a GPIO pin for other uses, such as a system status LED or digital input/output functions. The microcontroller can control up to four pairs of bypass.



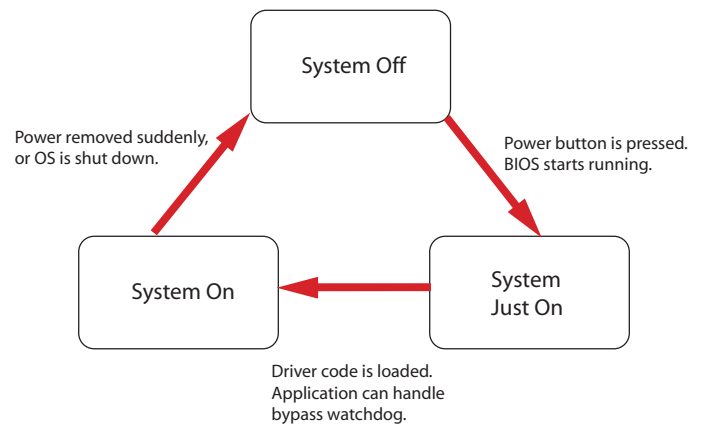
Better Control with Watchdog Timers

The Generation Three bypass solution includes a software development kit that enables system designers to efficiently design systems that support bypass functionality.

Lanner Generation Three bypass with watchdog control has the following features:

- Communication through SMBus (I2C).
- Independent bypass status control for each pair of ports, up to a total of four pairs.
- Ability to bypass Ethernet ports on a host system in response to three instances:
 1. System off
 2. Just-on (just-on is the brief moment when the internal power supply turns on and booting process is in progress)
 3. System on (software request during runtime).
- Reset of system during runtime if system hangs without packet loss.
- Software programmable bypass or normal status.
- Software programmable timer interval for just-on moment.

The following diagram illustrates the three states of the system's operation.



FW-8865 Network Appliance Based on the Intel® Xeon® Processor E3

Using the Intel® Xeon® processor E3 (formerly codenamed "Sandy Bridge"), the FW-8865 is a 1U high-end network security platform with low power consumption.

FW-8865 has room for two Ethernet modules that provide flexible configuration of frontside ports. This lets users upgrade the appliance over time to meet changing requirements.

Modules are available with 2, 4 or 8 ports, and are offered with both copper and fiber. And for applications where bypass is required, there are several modules with bypass.

One of these bypass modules, the NCM-IGM425A, was used in the test described in this whitepaper. It comes with two Generation Three bypass pairs and uses the Intel® 82576EB Gigabit Ethernet Controller. NCM-IGM804A uses the same controller, but offers four pairs of bypass. Lastly, there is the NCM-IGM426A for those who prefer the Intel® Ethernet Controller i350.



NCM-IGM425A

Proof of Improvement

Lanner developed a test to validate one major improvement made in Generation Three over Generation Two bypass: lossless packet transfers at the start of the system just-on state.

Streaming technologies, voice over IP, on-line gaming and videoconferencing demand timely delivery of sequential packets. Lost or dropped packets can result in highly noticeable performance issues. Furthermore, in the transmission of text files, a single packet loss could result in file corruption.

The following table specifies the Lanner products used in the test, the bypass configuration and the test equipment.

Lanner Model	FW-7560	FW-8865
Ethernet Module	N/A (Built in)	NCM-IGM425A
Network Controller	Intel® 82574L Gigabit Ethernet	Intel® 82580DB Gigabit Ethernet
Lanner Bypass Solution	Generation Two	Generation Three
Bypass Configuration	Bypass enabled when system off. Bypass enabled when system on.	
Software and Test Tool	SmartFlow 4.10.031.1 on SmartBit 6000B Forwarding network modules: SmartMetrics 10/100/1000Base-T Ethernet (LAN-3300A)	

Test Setup

Spirent SmartBits was used as a packet generator to provide a bi-directional stream of data that could go through the bypassed ports that were to be tested. The number of packets transmitted and received were recorded by software on the packet generator so that any packet loss would be obvious.

The test starts with the system turned off. The first step is to start the packet generating program which transmits packets through the bypassed ports. Next, the system with the bypassed ports is turned on to simulate a just-on event.

After the just-on event is complete, the system runs for a few more seconds and the packet generating program stops.

The entire program runs for 30 seconds, and at the end, the number of packets received and transmitted from both sides are calculated and compared.



FW-8865 Network Appliance Based on the Intel® Celeron® M Processor

The FW-7560 makes deploying network applications simple and cost-effective. An Intel® Celeron® M processor at 600MHz delivers power-efficient processing while the Intel® 910GMLE Express Chipset with 82801FBM I/O Controller Hub 6 Mobile (ICH6-M) provides PCI-E bus network bandwidth.

FW-7560 includes four integrated Ethernet ports with up to two pairs supporting Generation Two abnormal state packet bypass.

Test Results

The test results on the Generation Two bypass are shown below. The percentage of frame loss in Generation Two was 3.29% on the first pair of ports, and 2.07% on the second pair of ports.

Name	Time	FrameSize	ILoad	TxFrames	RxFrames	LostFrames	Lost (%)
Total	08/29/11 10:15:59	64	100.00000	89,285,712	86,885,125	2,400,587	2.68866
A Group	08/29/11 10:15:59	64	100.00000	89,285,712	86,885,125	2,400,587	2.68866
A 3B1->3B2	08/29/11 10:15:59	64	100.00000	44,642,856	43,170,680	1,472,176	3.29767
A 3B2->3B1	08/29/11 10:15:59	64	100.00000	44,642,856	43,714,445	928,411	2.07964

When the same test was repeated on the FW-8865 with Generation Three bypass, the number of lost frames is reduced to 0, proving that no packet loss takes place during the just-on event.

Name	Time	FrameSize	ILoad	TxFrames	RxFrames	LostFrames	Lost (%)
Total	08/29/11 10:18:56	64	100.00000	89,285,712	89,285,712	0	0.00000
A Group	08/29/11 10:18:56	64	100.00000	89,285,712	89,285,712	0	0.00000
A 3B1->3B2	08/29/11 10:18:56	64	100.00000	44,642,856	44,642,856	0	0.00000
A 3B2->3B1	08/29/11 10:18:56	64	100.00000	44,642,856	44,642,856	0	0.00000

Conclusion

Advanced applications may require bypass to be frequently enabled and disabled no matter if the system is on, off, or in the process of restarting. Lanner's Generation Three bypass offers a very high level of LAN bypass control. Even if the system unexpectedly shuts down, Generation Three enables the LAN bypass to be managed with greater accuracy and reliability, maximizing network uptime. In addition, Generation Three adds dedicated watchdogs for different pairs of bypass ports during runtime. This is an important advantage in advanced network appliances that have many applications and serve multiple connections for multiple network sites.

Comparison Chart for the Three Generations of Bypass

	Generation 1	Generation 2	Generation 3
Hardware jumper required to enable bypass	Yes	No	No
Remote Bypass Control	No. It is required to open the chassis to enable the bypass function.	Yes, with the system's remote management method	Yes, with the system's remote management method
Programs to enable/disable bypass pairs dynamically during system run-time	Yes, but hardware jumper must be enabled first. Also, the sample program can only turn on or off all bypass pairs at the same time.	Yes, there are two ways 1. BIOS (requires system reboot). 2. Sample programs (for use during system runtime). User can choose which pairs.	Yes, a comprehensive and complete set of commands for easy management are available.
Configuration that can enable bypass during power-on and disable bypass during power-off	No, impossible	No, impossible	Yes
Multiple watchdogs dedicated for different bypass pairs	No, only one watchdog shared with the host system	No, only one watchdog shared with the host system	Yes
Watchdogs capable of turning both on and off the bypass	No, only a single watchdog that can only turn on all bypass pairs at the same time	No, only a single watchdog that can only turn on all bypass pairs at the same time	Yes, multiple watchdogs can turn on as well as off multiple bypass pairs dynamically and automatically.
Bypass control in 3 distinct states: power-on, just-on and instance	No, it cannot control bypass status in just-on state	No, it cannot control bypass status in just-on state	Yes
Checking of bypass status and watchdog timer values	No	No	Yes, a comprehensive and complete set of commands for easy management is provided.
Using GPIO pins of the host system	Yes	Yes	No, it employs a microcontroller and communicates to the host system through the SMBus
Packet loss when going from an enabled bypass at system on, to an enabled bypass at system on	Yes	Yes	No.
Bypass implementation independent of the Intel® architecture platform of the host system	No	No	Yes, this single bypass solution can run on all of Lanner Intel® processor-based network appliances without any customization.

About Lanner Electronics Inc.

Founded in 1986 and publicly listed (TAIEX 6245) since 2003, Lanner Electronics, Inc. is an ISO 9001 certified designer and manufacturer of network application platforms, network video platforms and applied computing hardware for first-tier companies. Lanner's expertise also extends to include driver and firmware support, enabling customers to optimize hardware and software communication to achieve faster time to market. With headquarters in Taipei, Taiwan and branches in the U.S. and China, Lanner is uniquely positioned to deliver custom technical solutions with localized, value-added service.

Worldwide Offices

Taiwan - Corporate Headquarters

Lanner Electronics Inc.
7F, 173, Section 2, Datong road
Xizhi District, New Taipei City 221
Taiwan
T: +886-2-8692-6060
F: +886-2-8692-6101
E: sales@lannerinc.com

USA

Lanner Electronics (USA) Inc.
41920 Christy Street
Fremont, CA 94538
USA
T: +1-510-979-0688
F: +1-510-979-0689
E: sales_us@lannerinc.com

Canada

LEI Technology Canada Ltd
450 Matheson Blvd E, Unit 40
Mississauga, L4Z 1N8, On
Canada
Toll_free: +1 877-813-2132
T: +1 905-361-0624
E: sales_ca@lannerinc.com

China

First Floor, Xingtianhaiyuan Building,
West First Street Shucun
Agriculture University South Road
Haidian District, Beijing , 100193
P.R.China.
T: +86-10-82795600
F: +86-10-62963250
E: sales_bj@lannerinc.com