NEXCOM
Committed to Customer Success

White Paper

Bypass All of Your Critical IoT Gateway Issues

I. Problem: IoT gateways are easily affected by service interruptions

An IoT gateway device is crucial in linking together other IoT equipment and devices, sensors, systems, and the cloud. By systematically connecting the field and the cloud, IoT gateway devices offer a localized processing and storage solution, as well as the ability to autonomously control field devices based on sensors' data input.

Generally, IoT gateway devices don't have failover capabilities, so when a gateway is out of service due to reboot, system upgrade, or malfunction, all data to the device is dropped and retransmitted through other network paths. This increases transmission costs and the entire network's latency.

II. Solution: IoT gateway with bypass mechanism

We've solved these issues by introducing the bypass mechanism into IoT gateway devices. During normal system operation, the gateway inspects traffic and the bypass state is normal mode. When the gateway malfunctions or the system is reboot or powered down, the bypass can be set to bypass mode or disconnect mode.

The bypass mechanism is based on a software watchdog. When the system is up and running, it triggers the watchdog, which has been holding the bypass in normal mode. When the system malfunctions, it stops sending triggers and the watchdog switches the bypass relays to bypass mode or disconnect mode.

III. Benefit: the driver provides a rich variety of functions

Because bypass control is closely related to system status, we've developed a Linux driver that's supported from kernel 2.6 to the latest version (kernel 5.x) as well as providing a sysfs control interface. The bypass driver provides information about any installed NEXCOM bypass devices, including the model name, current state, and component NICs. It also supports switching current bypass states and configuring watchdog settings. Moreover, the driver provides power state protection for setting the bypass state while the system powers up or down.

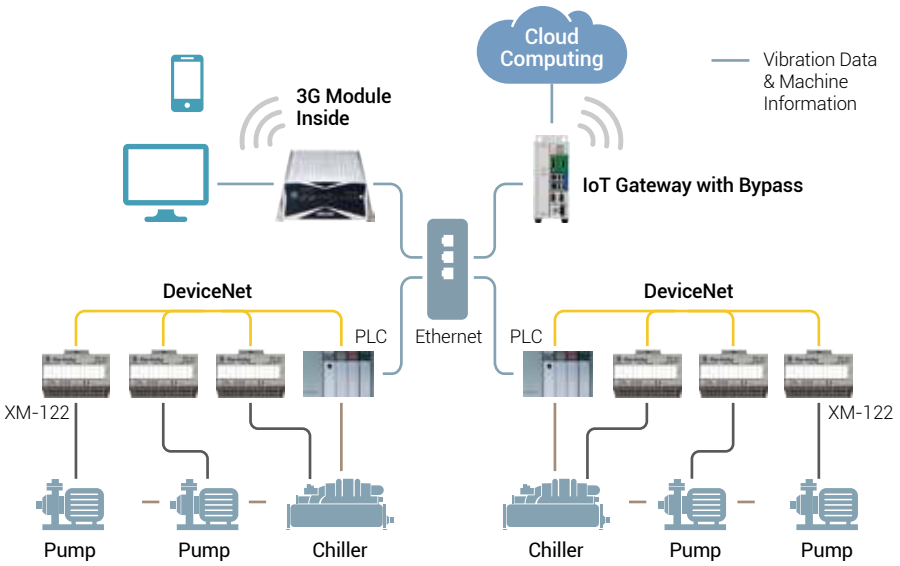

Figure 1. An IoT gateway with bypass mechanism.

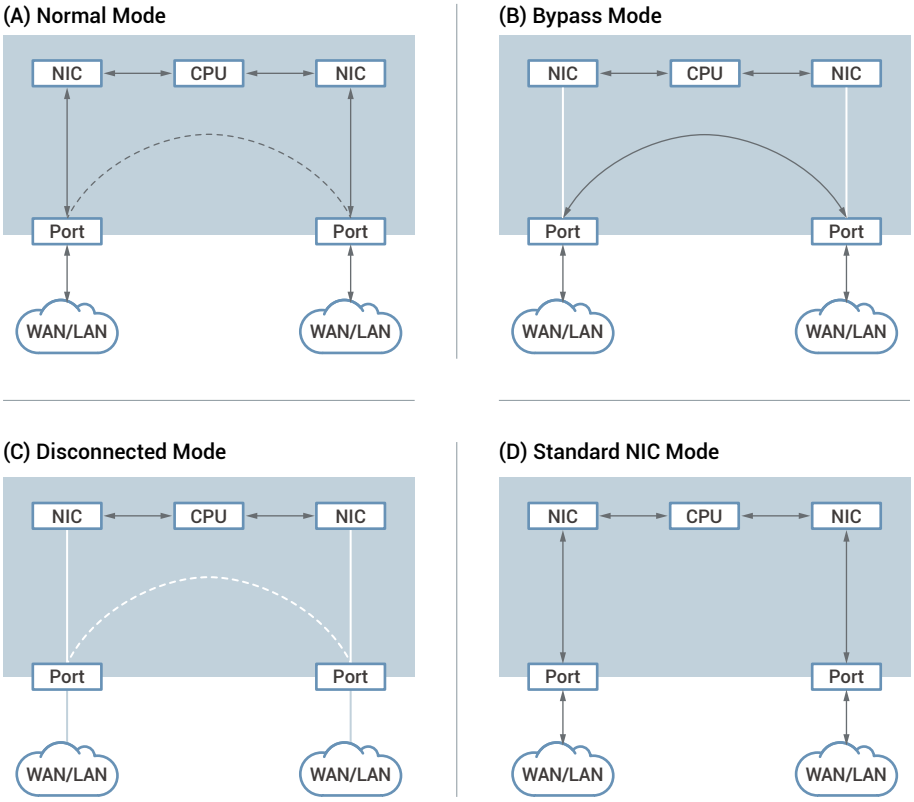

Figure 2. NEXCOM bypass' four modes.

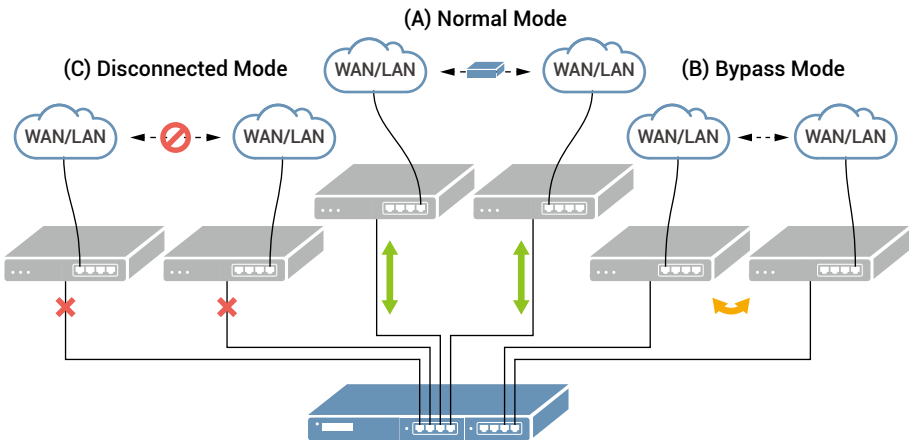

Figure 3. NEXCOM bypass use cases.

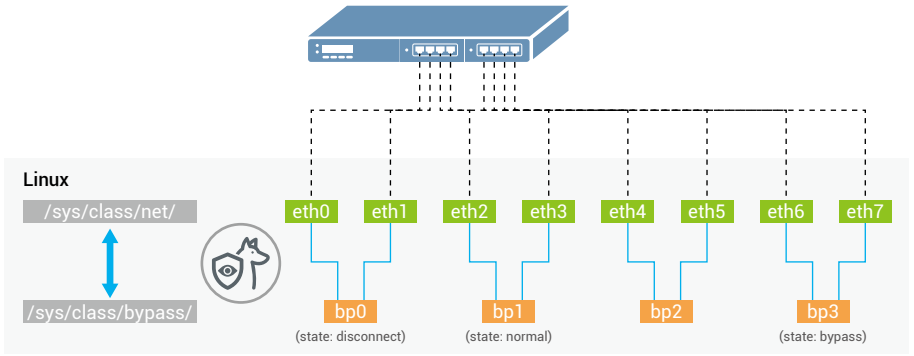

Figure 4. NEXCOM bypass' features.

NEXCOM's bypass system is specially devised to ensure that all components are effectively and efficiently integrated. The NEXCOM bypass driver issues commands to the bypass controller, which then controls the applicable relays in switching among various bypass modes. Through extensive research and development, NEXCOM has additionally developed a unique circuit design that allows the bypass controller to protects the power state in critical cases of sudden power loss.

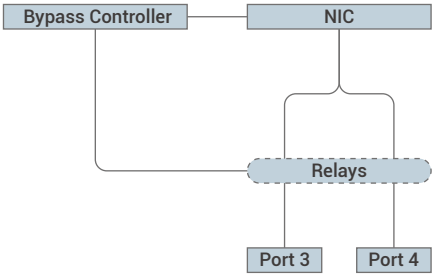

Figure 5. NEXCOM bypass block diagram.

The NEXCOM bypass driver provides user spaces a set of unified control methods. The administrator can use nodes to control the bypass state, while the system code can enable the watchdog and then trigger it regularly to ensure the system is alive. Furthermore, the application is able to control bypass via RESTful API, based on NEXCOM's Atlas OS™ (VNF).

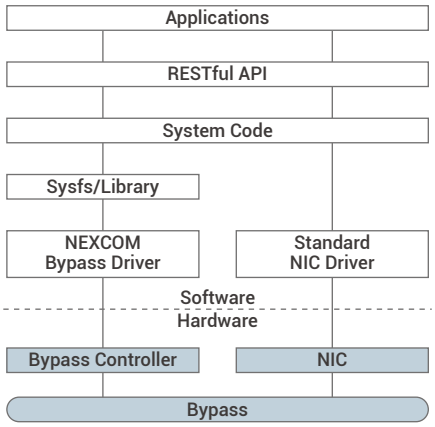

Figure 6. Software stack.

IV. Conclusion

IoT gateway devices typically connect the field and cloud but don't deliver failover capabilities. Utilizing NEXCOM's integrated solution with bypass mechanism reduces network transmission costs and latency.

The adaptive configurations for four different modes fulfills various use case requirements, while the bypass driver provides user spaces easy-to-use interfaces. Both system codes and applications can also easily manage our bypass devices. Moreover, the driver is extendable to a diversity of Ethernet controllers. It's evident that no matter what needs you have, NEXCOM's IoT gateway with bypass mechanism is your best bet.

Appendix A

Function Specifications

Modes	Description
Normal mode	LAN is operating normally
Bypass mode	Redirects traffic to bypass port
Disconnected mode	LAN is physically disconnected
Conventional NIC mode	No bypass feature

Simple Steps to Enable Watchdog Settings

- Step 1. Specify the mode once timeout occurs (default: bypass mode).
- Step 2. Specify the time period needed to feed watchdog (default: 8 seconds).
- Step 3. Enable watchdog and regularly feed before timeout.

Note:

The bypass will switch to the specified mode once the timer expires. Additional information such as number of occurrences and remaining time are also available.

Supported Power Events

The bypass mode will switch to the preset mode with these four events:

- Power on
- Power off
- System reset
- Power loss

Appendix B: Product Information

Module Type	Controller	No. of Bypass Pair	Link Speed	Media Type	I/O Ports	Interface
NI 142CX1	Intel® I350AM4	2	1G	Copper	4 x RJ45	PCIe 3.0
NI 142CX1-OS*	Intel® I350AM4	2	1G	Copper	4 x RJ45	PCIe 3.0
NI 184CX1	Intel® I350AM4	4	1G	Copper	8 x RJ45	PCIe 3.0
NI 184CX1-OS*	Intel® I350AM4	4	1G	Copper	8 x RJ45	PCIe 3.0
NX 142FX1	Intel® XL710-BM1	2	10G	Fiber	4 x SFP+	PCIe 3.0
NQ 221FX1	Intel® XL710-BM2	1	40G	Fiber	2 x QSFP+	PCIe 3.0

*Open Compute Project (OCP) NIC 3.0

Founded in 1992, NEXCOM integrates its capabilities and operates eight global businesses, which are Industrial Mesh, Intelligent Platform @ Smart City, Intelligent Video Security, Mobile Computing Solutions, Medical and Healthcare Informatics, Network and Communication Solutions, Smart Manufacturing, and Open Robotics and Machinery. This strategic deployment enables NEXCOM to offer time-to-market, time-to-solution products and services without compromising cost.

www.nexcom.com

NEXCOM is an Associate member of the Intel® Internet of Things Solutions Alliance. From modular components to market-ready systems, Intel and the 600+ global member companies of the Intel® Internet of Things Solutions Alliance provide scalable, interoperable solutions that accelerate deployment of intelligent devices and end-to-end analytics. Close collaboration with Intel and each other enables Alliance members to innovate with the latest technologies, helping developers deliver first-in-market solutions.

Learn more at: intel.com/iotsolutionsalliance

Intel and Atom are registered trademarks of Intel Corporation in the United States and other countries.