

WALL IE – Industrial Bridge and Firewall (700-860-WAL01)

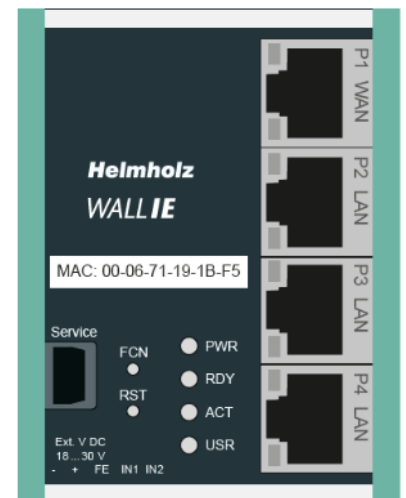
Version: 29.09.2015 - Preliminary

WALL IE is an Industrial Ethernet Bridge and Firewall.

It is used to integrate automation cells into superior production networks while restricting the access between those networks.

For separation of the automation cell without using two separate networks the bridge mode is offered.

It enables packet filtering while acting as a normal Layer 2 switch.



Features

- Easy integration of automation cells into factory networks
- restricting access between networks
- Router and Bridge operating modes
- NAT: Basic NAT, NATPT, Port forwarding
- Packet filtering
- fast and easy configuration using web browser with responsive design
- HTTPS web access (*in preparation*)
- 100 Mbit ethernet
- 1 port WAN
- 3-Port Switch for LAN
- 2 digital inputs for extended functionality, e.g. access control by hardware switch/key (*in prep.*)
- Small form factor



Router Mode

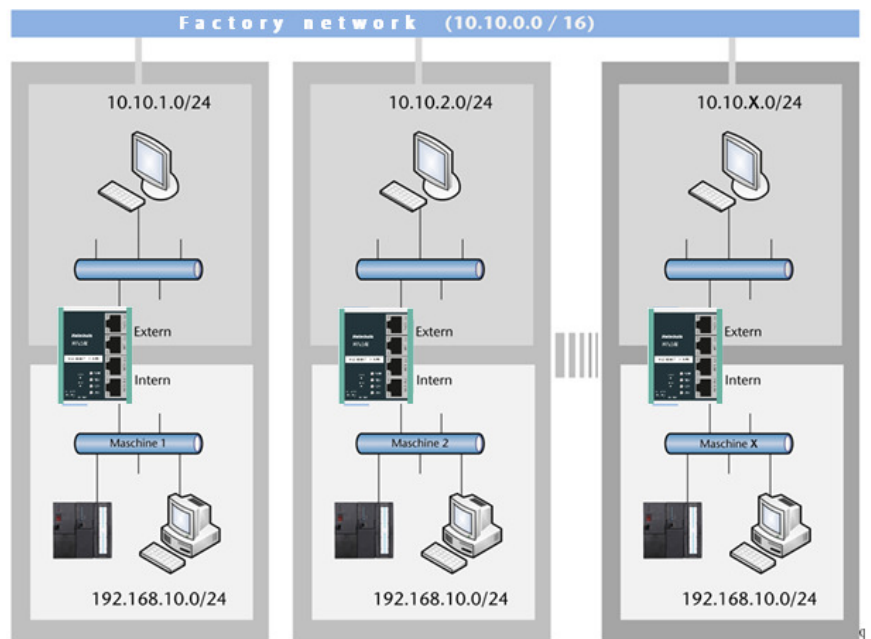
In router mode the device routes traffic between two different IPv4 networks (layer 3). Additionally to this "normal routing" the NAT and packet filter functionality is available.

Static IPv4 routes can be configured for communication from one automation cell to another cell. The network of the remote cell as well as the next hop to that network must be set.

NAT functionality

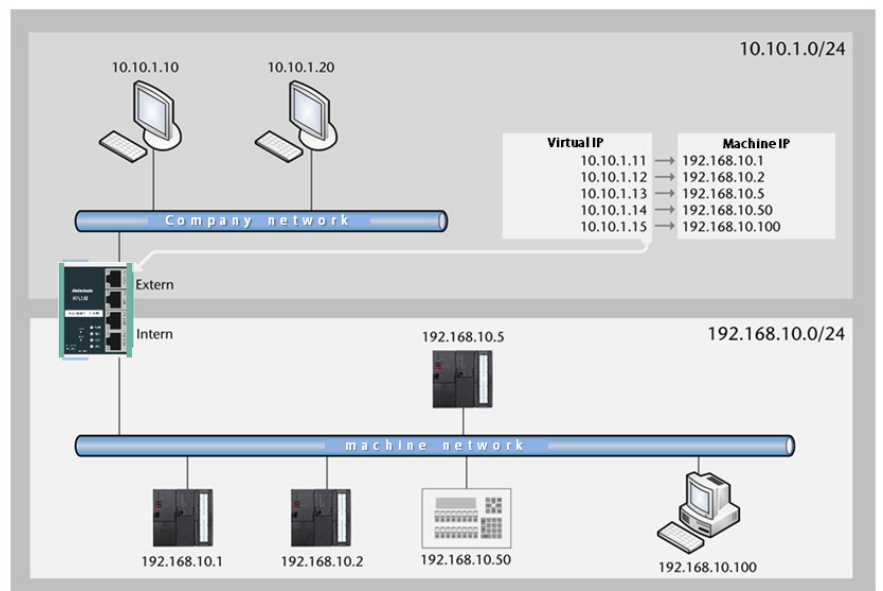
When multiple automation cells with the same IPv4 network are integrated in a superior network there are collisions because the addresses are not unique.

One solution for this is the usage of different IP addresses in every subnetwork. The other one is using Network Address Translation (NAT).



Basic NAT

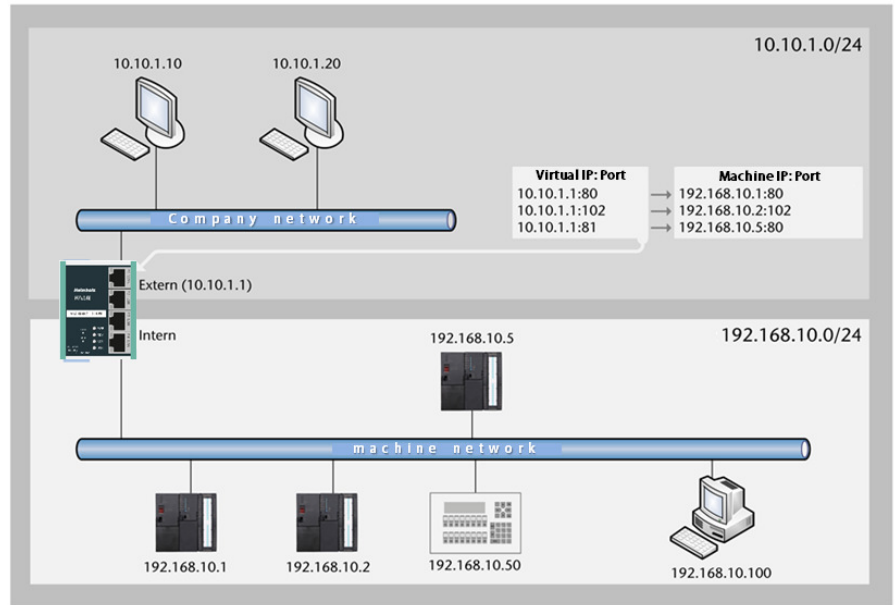
Basic NAT - also called "1:1 NAT" or "Static NAT" - is the translation of single IP addresses or IP address ranges. Only the IPv4 source and destination addresses are manipulated. Therefore all IPv4 traffic is translated ("all ports").



NAPT: Network Address and Port Translation

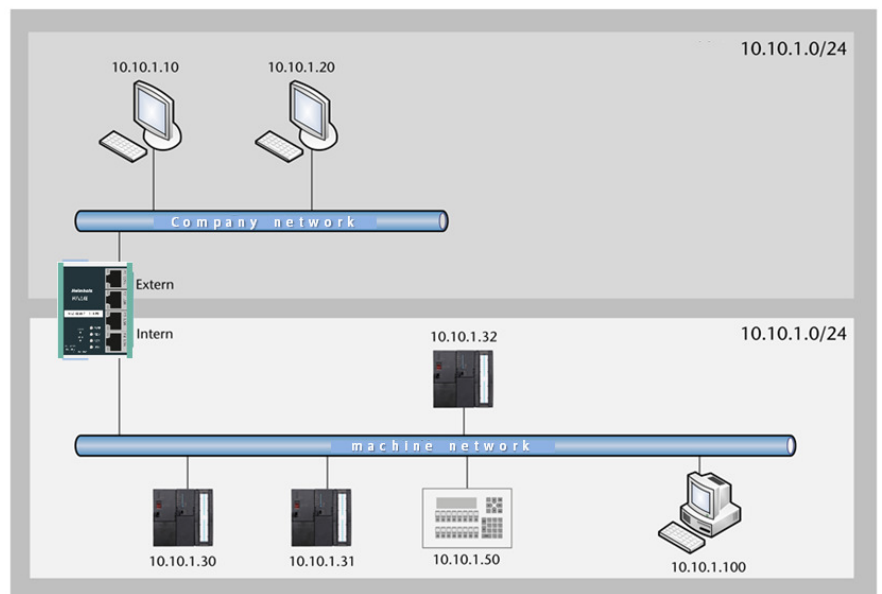
NAPT - also called “1:N NAT” or “masquerading” - is the translation of a whole network using a single IP address. The source address of a packet from automation cell to production network is replaced with the configured IP.

Using port forwarding one can configure that packets sent to specific TCP/UDP ports of the production network address are forwarded to a IP address in the automation cell (e.g. 10.10.1.1:8080 to 192.168.10.2:80).



Bridge Mode

In bridge mode the firewall has no routing and NAT functionality. Instead it acts as a layer 2 switch between LAN and WAN interface. The bridge mode enables packet filtering in flat network hierarchies. This is used to divide the network in two physical areas without using different IP networks.



Packet filter functionality

Filter criteria: IP Addresses, TCP/UDP ports
MAC addresses and Ethertype filtering in preparation.