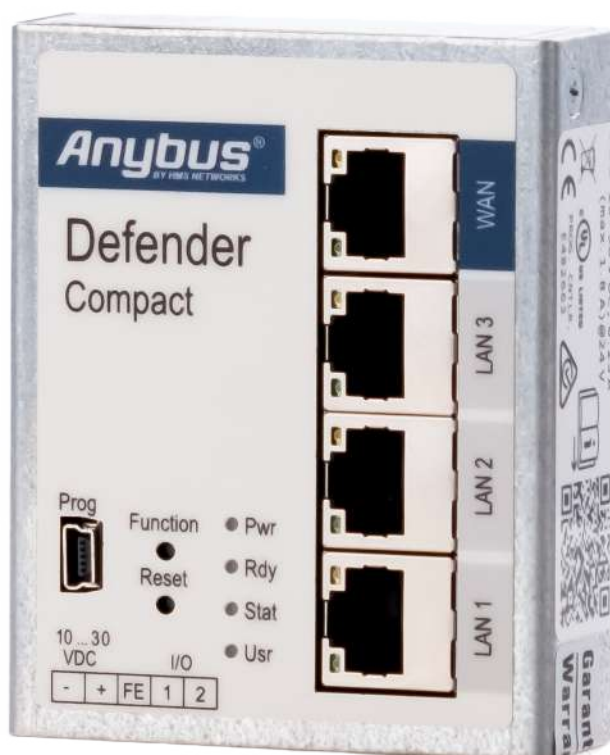


Anybus® Defender Compact Technical Clish Manual

ABD1004-NATFW

Version: 1.2

Publication date 2026-03-25



1.1 General Information

Our products contain, amongst others, so-called open-source software that is provided by third parties and has been published for free public use. The open-source software is subject to special open-source software licenses and the copyright of third parties.

Basically, each customer can use the open-source software freely in compliance with the licensing terms of the respective producers. The rights of the customer to use the open-source software beyond the purpose of our products are regulated in detail by the respective concerned open-source software licenses. The customer use the open-source software freely, as provided in the respective effective license, beyond the purpose that the open-source software gets in our products. In case there is a contradiction between the licensing terms for one of our products and the respective open-source software license, the respective relevant open-source software license takes priority over our licensing terms, as far as the respective open-source software is concerned by this.

The use of the used open-source software is possible free of charge. We do not demand usage fees or any comparable fees for the use of the open-source software contained in our products. The use of the open-source software in our products by the customer is not part of the earnings we achieve with the contractual compensation.

For software that is published under the GPLv2 License, the following applies:

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 2 of the License, or (at your option) any later version. This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details. You should have received a copy of the GNU General Public License along with this program.

If not, see <<https://www.gnu.org/licenses/>>.

All open-source software programs contained in our products can be taken from the available list. The most important open-source software licenses are listed in the Licenses section at the end of this publication. As far as programs contained in our products are subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), the Berkeley Software Distribution (BSD), the Massachusetts Institute of Technology (MIT) or another open-source software license, which regulates that the source code must be made available, and if this software is not already delivered in source code on a data carrier with our product, we will send you this at any time upon request. If it is required to send this on a data carrier, the sending will be made against payment of a cost compensation of Euro 35,00.

Our offer to send the source code upon request ceases automatically 3 years after delivery of our product to the customer. Requests must be directed to the following address, if possible, under specification of the serial number:

HMS Networks

Box 4126

300 04 Halmstad, Sweden

E-Mail: info@hms.se

1.1.1 Version History

Version	Date	Comment
V 0.9	Nov 2nd, 2023	Engineering Draft
V 1.0	July 22 nd , 2025	Anybus Defender Compact Edition
V 1.1	Jan 20 th , 2026	Minor corrections
V 1.2	Mar 25 th , 2026	Minor corrections

Table of Contents

1.1	GENERAL INFORMATION.....	2
1.1.1	Version History.....	2
2	CLISH COMMANDS.....	4
2.1	THE 'COMMIT' – COMMAND	4
2.2	CONFIGURATION MENU	5
2.2.1	User authentication	6
2.2.2	Time settings.....	7
2.2.3	NTP.....	7
2.2.4	Configuration Access Level.....	7
2.2.5	Device information.....	9
2.2.6	Extra settings	9
2.2.7	Packet filter.....	10
2.2.8	Interface configuration	11
2.2.9	Gateway and Nameserver	13
2.2.10	Static routes	13
2.2.11	Operation mode.....	14
2.2.12	DNAT (Port Forwarding).....	14
2.2.13	Network-NAT	15
2.2.14	Simple NAT.....	15
2.2.15	SNAT.....	16
2.2.16	Netlearn	16
2.2.17	Syslog.....	17
2.2.18	Firmware-Update.....	18
3	LAN SEGMENTATION	19
3.1	LAN PORT – LAN INTERFACE – LAN SEGMENT.....	19
3.2	MULTIPLE LAN SEGMENTS	20
3.3	LAN A, LAN B, LAN C	20
4	CONFIGURATION EXAMPLES.....	21
4.1	CREATE THREE SEPARATE LAN SEGMENTS.....	21
4.2	PROVIDE CONFIGURATION ACCESS FOR USER 'OPERATOR' ON THE LAN INTERFACE	22
4.3	ACTIVATE SNAT ON WAN AND LAN A	23
4.4	ENTER A PACKET FILTER RULE	23
4.5	DISABLE A SPECIFIC LAN PORT.....	23

2 Clish Commands

In this chapter all clish commands will be described. To get a better understanding of the functionality of the Anybus Defender Compact we recommend to also read the documentation of the Anybus Defender Compact Manager (see <https://www.hms-networks.com/downloads>). Although the Anybus Defender Compact Manager is not needed to configure the Anybus Defender Compact, its documentation is very helpful and does not only cover the functionality of the Anybus Defender Compact Manager software but also the functionality of the Anybus Defender Compact device.

NOTE: The complete set of the following commands is only visible to user ‘admin’. If you log into the clish with user ‘operator’, ‘viewer’ or ‘factoryreset’ only a subset will be available.

NOTE: The current settings are stored in the so-called ‘running-config’. This config can be shown with this command:

show running-config <cr>

After logging into the clish you will enter the main menu and the following commands will be available.

```
ABDC4#
config  general system settings
exit    exit and logout
reboot  halt and perform a cold restart
show    shows system values
update  firmware update
write   saves all current changes into the flash
```

config <cr>	Enter the configuration menu.
reboot <cr>	Reboot your Anybus Defender Compact device
update <cr>	update the firmware of the device See config <cr> update-src ...
write <cr>	Save all current changes into the flash, i.e. no changes will be lost after a reboot.
show [option] <cr>	Show system values. See options in Picture ... Example: show running-config <cr> lists all configuration settings.
exit <cr>	Leave the clish.

```
ABDC# show
cpu          description  diag      ebttables  info
interfaces  ip          iptables  macs       messages
name         netlearn-list running-config startup-config users
```

2.1 The ‘commit’ – command

Some of the settings that are described on the next pages need to be activated by entering a 'commit' - command after configuration. This is important, because without executing 'commit' these settings will be shown in the running-config although they are NOT activated yet.

2.2 Configuration menu

The configuration menu is the most comprehensive menu where you can edit most system settings.

```
ABDC(config)#
auth                user login settings
clock               time settings
configlevel-bridge configlevel-bridge
configlevel-lan     configlevel-lan
configlevel-usb     configlevel-usb
configlevel-wan     configlevel-wan
description         description
exit                exit from config mode
extra-sets          extra settings
filter-lanwan       filter-lanwan-settings
filter-wanlan       filter-wanlan-settings
interface           select an interface to configure
ip                  set default-gateway or name-server
ip-route            ip route settings
mode                operating mode
name                system name
nat-dnat-lanwan     dnat lan/wan settings
nat-dnat-wanlan     dnat wan/lan settings
nat-net             nat net settings
nat-simple          simple nat settings
nat-snat            snat settings
netlearn            Netlearn settings
no                  negate a command or set its defaults
ntp                 ntp service
syslog              enable syslog
update-src          update parameter
```

config <cr>	Enter configuration menu
--------------------------	--------------------------

2.2.1 User authentication

```
ABDC(config-auth-admin)#
  active      enable or disable user to login
  chpasswd    change password for user authentication
  exit        exit from auth configuration mode
  key         publickey for user authentication
  method      authentication method
  no          negate a command or set its defaults
```

In the user authentication menu, you can edit login settings for the users: admin, operator, viewer and factoryreset.

config <cr> auth [username] <cr>	Enter authentication menu for user [username]
active on <cr>	Enable user [username] to login.
active off <cr>	Disable user [username] to login
chpassword <cr>	Change password for user [username]. Follow the instructions on screen. You have to enter the new password twice.
exit <cr>	Leave this menu.
key <cr>	Enter a public SSH key the user can authenticate with.
method pw <cr>	Set the user authentication method to password.
method key <cr>	Set the user authentication method the SSH key.
no key <cr>	Remove public key for user authentication. Method will be set to password automatically.
no pw-hash <cr>	Remove password hash for user authentication. Password will be set to factory setting.

2.2.2 Time settings

```
ABDC4(config-clock)#
default-time default-time
exit          exit from time configuration mode
timezone      timezone
```

config <cr> clock <cr>	Enter time settings menu.
default-time <cr>	under development
no default-time <cr>	under development
timezone [timezone] <cr>	Set time zone [timezone], e.g. 'Europe/Paris'.
exit <cr>	Leave clock menu.

2.2.3 NTP

config <cr>	To run the commands below you have to be in the config menu.
ntp peer [server] [interval] [retries] [mode] <cr>	Assign a NTP server for synchronizing the time. For the details on the parameters see Anybus Defender Compact-Manager documentation.

2.2.4 Configuration Access Level

Here you can regulate the access authorization for the device configuration via the different interfaces. You can set the access level for the interfaces bridge, wan, lan and usb.

NOTE: You have to take the operation mode into consideration: Setting the access level of the bridge interface, for example, only makes sense if Anybus Defender Compact runs in bridge mode.

NOTE: To get access via a specific interface you also have to enable the respective user you want to login with (see [#1.1.1.User authentication](#))

config <cr>	To run the commands below you have to be in the config menu.
configlevel-[interface_name] [access_level] <cr>	<p>Set the access level for given interface. [interface_name] has to be one of</p> <ul style="list-style-type: none"> • usb • wan • lan • lan-b • lan-c • bridge <p>lan stands for LAN segment A. lan-b stands for LAN segment B. lan-c stands for LAN segment C. => If you have more than one LAN segment, you are able to enable/disable configuration access on the respective LAN interface separately.</p> <p>[access_level] has to be one of</p> <ul style="list-style-type: none"> • admin <ul style="list-style-type: none"> ◦ Enable user viewer, operator and admin to login through this interface. • operator <ul style="list-style-type: none"> ◦ Enable user viewer and operator to login through this interface. • viewer <ul style="list-style-type: none"> ◦ Enable user viewer to login through this interface. • factoryreset <ul style="list-style-type: none"> ◦ Enable users factoryreset, viewer, operator and admin to login through this interface. • off <ul style="list-style-type: none"> ◦ Disable the possibility for users to login via this interface.

2.2.5 Device information

config <cr>	To run the command(s) below you have to be in the config menu.
description [system-description] <cr>	Enter a description for your system. This description will be shown with command 'show description'
name [system-name] <cr>	Enter a name for your system.

```
ABDC(config-extra-sets)#
  configured      is device configured
  debug           debug mode
  debug-level     debug level
  exit            exit from extra settings
  serviceaccess   service access
```

2.2.6 Extra settings

config <cr> extra-sets <cr>	Enter the extra-settings menu.
configured yes <cr>	Turns off the 'Usr'-LED on the device, i.e. the device has been configured. NOTE: When configuring the device via Anybus Defender Compact Manager, this LED will be turned off implicitly.
configured no <cr>	Turns on the 'Usr'-LED on the device, i.e. the device has not been configured, yet. NOTE: When configuring the device via Anybus Defender Compact Manager, this LED will be turned off implicitly.
debug yes <cr>	Under development
debug no <cr>	Under development
debug-level [level] <cr>	Under development
exit <cr>	Leave this menu
serviceaccess yes <cr>	Enable service access to the Anybus Defender Compact for the manufacturer.
serviceaccess no <cr>	Disable service access to the Anybus Defender Compact for the manufacturer.

2.2.7 Packet filter

```
ABDC(config-filter-wanlan)#
commit          activate settings
decline-mode    decline mode
exit            exit from filter configuration mode
mode            netfilter operation mode
no              negate a command or set its defaults
rule            Packetfilter rule
```

Configure packet filters for direction WAN -> LAN and/or LAN → WAN.

config <cr> filter-wanlan <cr>	Enter the configuration menu for the packet filter direction WAN → LAN
config <cr> filter-lanwan <cr>	Enter the configuration menu for the packet filter direction LAN → WAN
mode white <cr>	Run the filter in white mode, i.e. decline everything except filter rules (recommended). Also see decline-mode drop/reject
mode black <cr>	Run the filter in black mode, i.e. the filter accepts everything except packets that match filter rules.
mode off <cr>	Disable the filter, i.e. allow everything.
decline-mode drop <cr>	Set the filter decline-mode to 'drop'. If the filter runs in decline-mode (also called white mode, i.e. it declines everything, except filter rules), it drops the packets and the sender will NOT be informed.
decline-mode reject <cr>	Set the filter decline-mode to 'reject'. If the filter runs in decline-mode (also called white mode, i.e. it declines everything, except filter rules), it rejects the packets and the sender will be informed via the ICMP protocol.
rule [number] [source-mac] [source-ip] [source-port] [destination-mac] [destination-ip] [destination-port] [protocol] [firewall action] [comment] [mode] [rule-condition] <cr>	Create a filter rule. For the details on the parameters see Anybus Defender Compact-Manager documentation.
commit <cr>	Activate your settings. Execute this command whenever you have changed the packet filter settings and want them to be activated.
no rule all <cr>	Delete all filter rules.

no rule [number] <cr>	Delete filter rule with rule number [number].
exit <cr>	Leave the menu.

2.2.8 Interface configuration

```

ABDC(config-if-interface0)#
access-level  set the access level of the interface
description   description of the interface
disable       disable the selected interface
enable        enable the selected interface
exit          exit from interface configuration mode
hw-interface  adopted hardware interface
ip            interface internet protocol config commands
no            negate a command or set its defaults

```

Configure the interfaces WAN, LAN, Bridge, USB and the LAN ports

config <cr> interface bridge 0 <cr>	Enter configuration menu for bridge interface. NOTE: bridge interface comprises WAN and LAN ports if Anybus Defender Compact is running in bridge-mode.
config <cr> interface usb 0 <cr>	Enter configuration menu for USB interface.
config <cr> interface ethernet 0 <cr>	Enter configuration menu for WAN interface. NOTE: Only relevant if Anybus Defender Compact runs in gateway-mode.
config <cr> interface ethernet [1 2 3] <cr>	Enter configuration menu for LAN interface 1,2 or 3. NOTE: Only relevant if Anybus Defender Compact runs in gateway-mode.
config <cr> no interface ethernet [num] <cr>	Disable interface ethernet [num]
To execute the following commands, you have to be in one of the config-if menus (e.g. config <cr> interface bridge 0 <cr>):	
access-level <cr>	under development
description [interface-description] <cr>	Enter a description of the interface.
enable <cr>	Enable the interface.
disable <cr>	Disable the interface.

hw-interface [0 1 2 3] <cr>	<p>Assign one or more hardware interfaces to the interface that you are configuring. Hardware interfaces are the actual ethernet ports of the Anybus Defender Compact.</p> <p>hw-interface 0: WAN-Port hw-interface 1: LAN1-Port hw-interface 2: LAN2-Port hw-interface 3: LAN3-Port</p>
	<p>Example: If you are configuring the bridge interface and you enter the following command then the WAN-port and all three LAN-Ports are assigned to the bridge interface: hw-interface 0 1 2 3 <cr></p> <p>NOTE: To be able to assign a hw-interface that has already been assigned to another interface you first have to remove the hw-interface. (see command 'no hw-interface')</p>
ip address [address] [mask] <cr>	<p>Assign ip-address [address] and netmask [mask] to the interface.</p> <p>Example: ip address 192.168.0.1 255.255.255.0 <cr></p>
ip address dhcp <cr>	<p>Starts a dhcp client for that interface, i.e. it tries to obtain an ip address from a dhcp server.</p> <p>NOTE: You need to make sure that there's a dhcp server running in the same network as the respective interface.</p>
no hw-interface <cr>	Remove all assigned hw-interfaces from that interface.
no ip address <cr>	Remove assigned ip address from that interface.
exit <cr>	Leave interface configuration menu.

2.2.9 Gateway and Nameserver

config <cr>	To run the command(s) below you have to be in the config menu.
ip default-gateway [addr] <cr>	Set the ip address [addr] of the default gateway.
ip name-server [addr]/[mask] <cr>	Set the ip address [addr] and the netmask [mask] (optional) in slash notation of a name-server.
no ip default-gateway <cr>	Remove default gateway.
no ip name-server <cr>	Remove all nameserver entries.
no ip name-sever [addr]/([mask]) <cr>	Remove nameserver with ip address [addr] (and mask [mask] – optional).

2.2.10 Static routes

```
ABDC(config-ip-route)#
  commit    activate settings
  exit      exit from ip route configuration mode
  no        negate a command or set its defaults
  route     ip route
```

config <cr>	To run the command(s) below you have to be in the config menu.
route [number] [network] [netmask] [gateway] [comment] [mode] <cr>	Enter a static route. For the details on the parameters see Anybus Defender Compact-Manager documentation. Example: route 0 10.0.0.0 255.255.255.0 192.168.3.1 ad active With this route you are able to reach the network 10.0.0.0/24 via the gateway 192.168.3.1
commit <cr>	Activate settings.
exit <cr>	Leave ip-route menu.
no route all <cr>	Delete all routes.
no route [num] <cr>	Delete route with route number [num]

2.2.11 Operation mode

config <cr>	To run the command(s) below you have to be in the config menu.
mode bridge <cr>	Run Anybus Defender Compact in bridge mode.
mode gateway <cr>	Run Anybus Defender Compact in gateway mode.

2.2.12 DNAT (Port Forwarding)

```
ABDC(config-dnat-wanlan)#  
commit activate settings  
exit exit from dnat wanlan configuration mode  
no negate a command or set its defaults  
rule Destination NAT WAN>LAN rule
```

config <cr> nat-dnat-wanlan <cr>	Enter DNAT-configuration menu for direction WAN → LAN
config <cr> nat-dnat-lanwan <cr>	Enter DNAT-configuration menu for direction LAN → WAN
rule [num] [source-ip] [source-port] [destination-port] [protocol] [nat-ip] [nat-port] [comment] [mode] [rule-condition] <cr>	Create a DNAT rule. For the details on the parameters see Anybus Defender Compact-Manager documentation.
commit <cr>	Activate settings.
no rule all <cr>	Delete all DNAT rules.
no rule [num] <cr>	Delete DNAT rule with rule number [num].
exit <cr>	Leave DNAT configuration menu.

2.2.13 Network-NAT

```
ABDC(config-nat-net)#  
  commit  activate settings  
  exit    exit from net-nat configuration mode  
  no      negate a command or set its defaults  
  rule    netnat rule
```

config <cr> nat-net <cr>	Enter NETWORK-NAT-configuration menu.
rule [num] [virtual-net] [comment] [mode] ([physical-net]) <cr>	Create a NETWORK-NAT rule. [num]: Rule number [virtual-net]: Enter a free network address as a virtual IP network. [comment]: Add a comment [mode]: active/inactive ([physical-net]): Optional parameter. Can be lana, lan-b or lan-c. Only relevant if you configured more than one LAN segment.
commit <cr>	Activate settings.
no rule all <cr>	Delete all NETWORK-NAT rules.
no rule [num] <cr>	Delete NETWORK-NAT rule with rule number [num].
exit <cr>	Leave NETWORK-NAT configuration menu.

2.2.14 Simple NAT

```
ABDC(config-simple)#  
  commit  activate settings  
  exit    exit from simple nat configuration mode  
  no      negate a command or set its defaults  
  rule    simple nat rule
```

config <cr> nat-simple <cr>	Enter Simple-NAT-configuration menu.
rule [num] [ip-wan] [ip-lan] [comment] [rule-condition] <cr>	Create a Simple-NAT rule. For the details on the parameters see Anybus Defender Compact-Manager documentation.
commit <cr>	Activate settings.
no rule all <cr>	Delete all Simple-NAT rules.
no rule [num] <cr>	Delete Simple-NAT rule with rule number [num].
exit <cr>	Leave Simple-NAT configuration menu.

2.2.15 SNAT

```
ABDC(config-snat)#
commit    activate settings
exit      exit from auth configuration mode
lan       snat on lan side (SNAT everything coming out of LAN)
wan       snat on wan side (SNAT everything coming out of WAN)
```

config <cr> nat-snat <cr>	Enter SNAT-configuration menu.
wan active <cr> wan inactive <cr>	Activate SNAT on WAN interface. Deactivate SNAT on WAN interface.
lan active <cr>	Activate SNAT on all existing LAN interfaces.
lan active lan-a lan-b lan-c <cr>	Activate SNAT on specified LAN interfaces. Choose 1 - 3 lan interfaces (lan-a, lan-b, lan-c) you want to activate SNAT on.
lan inactive <cr>	Deactivate SNAT on all existing LAN interfaces.
commit <cr>	Activate settings.
exit <cr>	Leave SNAT configuration menu.

2.2.16 Netlearn

```
ABDC(config-netlearn)#
active      netlearn mode
exit        exit from netlearn configuration mode
level       netlearn level
listlimit   netlearn listlimit
```

config <cr> netlearn <cr>	Enter netlearn configuration menu.
active on <cr>	Activate netlearn mode.
active off <cr>	Deactivate netlearn mode.
level [num] <cr>	Set the capture level (capture mode) from 0-9 This is under development.
listlimit [num] <cr>	Set the max. Number of detected network participants to be listed
exit <cr>	Leave the netlearn configuration menu.

2.2.17 Syslog

```
ABDC(config-syslog)#
active external syslog server mode
exit exit from syslog server configuration mode
level output level for syslog
no negate a command or set its defaults
server external syslog server settings
```

config <cr> syslog <cr>	Enter syslog configuration menu.
activate on <cr>	Enable external Syslog server
active off <cr>	Disable external Syslog server
server [addr] ([port]) ([proto]) <cr>	Set server ip address [addr] and optional port [port] and protocol [proto].
level [num] <cr>	Set the notification level [num]. 0 Emergency 1 Alert 2 Critical 3 Error 4 Warning 5 Notice 6 Informational 7 Debug NOTE: Dependent on the selection, all higher priority levels are also automatically logged.
no server <cr>	Delete Syslog settings.
exit <cr>	Leave Syslog menu.

2.2.18 Firmware-Update

config <cr>	To run the command(s) below you have to be in the config menu.
update-src [type] [source] [release] [filename] <cr>	<p>Define the source of the firmware-update file.</p> <p>For example: update-src swu tftp://169.254.0.4/1-4-1-fwabdc.swu</p> <p>NOTE: To start a firmware update type update <cr> in the main menu.</p>

3 Lan Segmentation

From firmware version 1.4.0 onwards it is possible to separate the LAN interface into multiple segments (up to three).

NOTE: In this mode the Anybus Defender Compact will do routing and firewall filtering, but NAT use-cases are not supported. If SNAT-LAN is enabled, this is applied only to the LAN1 interface. It is not possible to enable SNAT-LAN for LAN2 and/or LAN3.

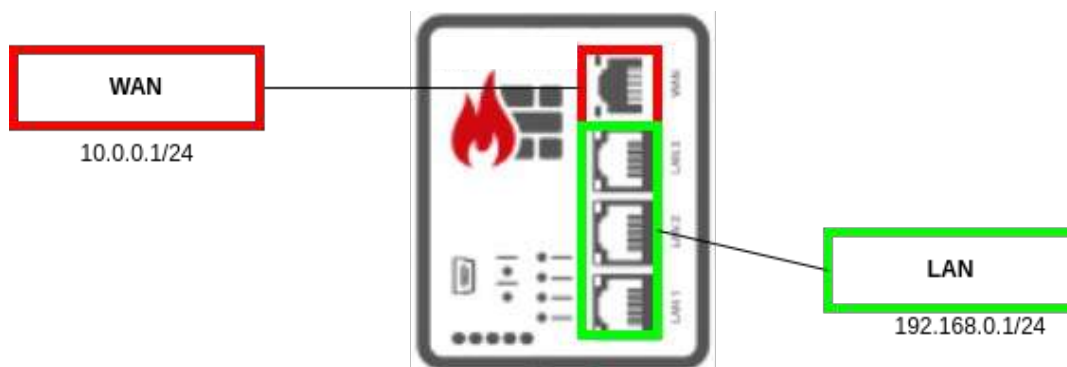
NOTE 2: After configuring multiple segments in CLI the Anybus Defender Compact Manager GUI will show warnings and should not be used to configure the device further.

3.1 LAN port – LAN interface – LAN segment

The Anybus Defender Compact has 3 **LAN ports**, i.e. physical ethernet ports you can plug in an ethernet cable. On the housing of the device these ports are labeled “LAN 1”, “LAN 2” and “LAN 3”.

With the default configuration, all three LAN Ports are part of one **LAN interface**. An interface has an ip address and with this ip address the Anybus Defender Compact can be addressed directly.

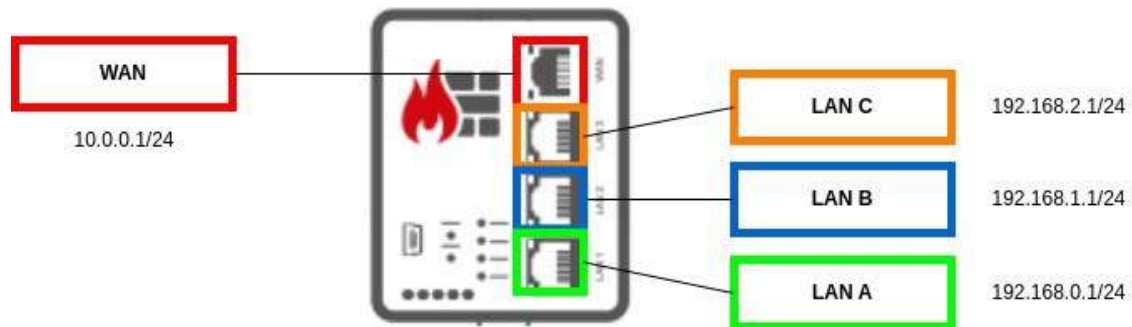
If all LAN Ports are part of the same LAN Interface, there exists only one **LAN segment**, i.e. one network where all members are located within the same ip address range.



3.2 Multiple LAN segments

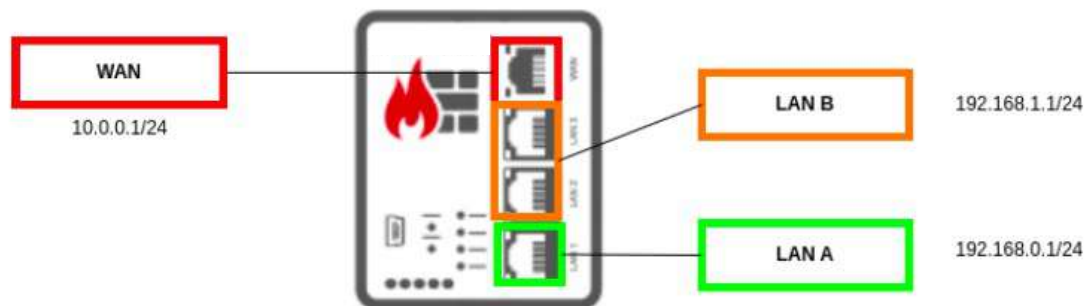
When running in gateway mode the Anybus Defender Compact per default has two interfaces: The **WAN interface** that comprises a single ethernet port (labeled WAN) and the **LAN interface** that comprises three ethernet ports (labeled LAN 1, LAN 2 and LAN 3)

In this example the **WAN interface** has the ip address 10.0.0.1 and the LAN interface has the ip address 192.168.0.1



Every LAN interface has its own ip address and therefore all members connected to one interface are part of the same network or segment.

In the next example there are only two LAN segments: LAN segment LAN A, that comprises **LAN port 1**, and LAN segment LAN B, that comprises **LAN port 2** and **LAN port 3**:



3.3 LAN A, LAN B, LAN C

With some of the commands you can choose between lan-a, lan-b and lan-c (e.g. activate SNAT on a specific LAN interface).

Be aware that it depends on your configuration which LAN ports are affected by this command. I.e. if you assigned LAN port 2 and 3 to LAN B and you activate SNAT on LAN B, it will affect LAN port 2 and 3, of course. But if you assigned LAN port 1, 2 and 3 to LAN A, there doesn't exist a segment LAN B and thus it has no effect if you activate SNAT on LAN-B.

4 Configuration Examples

4.1 Create three separate LAN segments

With the following commands you create LAN segments LAN A, LAN B and LAN C and assign ip addresses to the LAN interfaces. Before changing the LAN segment configuration, we always recommend starting with deleting the existing LAN segments, i.e. removing the LAN ports from the interfaces, since it is not possible to assign a LAN port to an interface if it has already been assigned to another interface.

Command	Explanation
Step 1: Remove all LAN ports from the interfaces	
config <cr>	Enter the configuration menu
interface ethernet 1 <cr>	Enter the interface 1 configuration menu
no hw-interface <cr>	Remove all LAN ports from interface 1
exit <cr>	Leave interface 1 configuration menu
interface ethernet 2 <cr>	Enter the interface 2 configuration menu
no hw-interface <cr>	Remove all LAN ports from interface 2
exit <cr>	Leave interface 2 configuration menu
interface ethernet 3 <cr>	Enter the interface 3 configuration menu
no hw-interface <cr>	Remove all LAN ports from interface 3
exit <cr>	Leave interface 3 configuration menu
Step 2: Assign LAN ports and ip addresses to the interfaces	
config <cr>	Enter the configuration menu
interface ethernet 1 <cr>	Enter the interface 1 configuration menu
hw-interface 1 <cr>	Assign LAN port 1 to interface 1
ip address 192.168.0.1 255.255.255.0 <cr>	Assign ip address 192.168.0.1/24 to interface 1
exit <cr>	Leave interface 1 configuration menu
interface ethernet 2 <cr>	Enter the interface 2 configuration menu
hw-interface 2 <cr>	Assign LAN port 2 to interface 2
ip address 192.168.1.1 255.255.255.0 <cr>	Assign ip address 192.168.1.1/24 to interface 2
exit <cr>	Leave interface 2 configuration menu
interface ethernet 3 <cr>	Enter the interface 3 configuration menu

hw-interface 3 <cr>	Assign LAN port 3 to interface 3
ip address 192.168.2.1 255.255.255.0 <cr>	Assign ip address 192.168.2.1/24 to interface 1
exit <cr>	Leave interface 3 configuration menu

Now you are running-config should contain these entries:
(type **config** <cr> **show running-config** <cr>)

```
interface ethernet 1
  hw-interface 1
  ip address 192.168.0.1 255.255.255.0
!
interface ethernet 2
  hw-interface 2
  ip address 192.168.1.1 255.255.255.0
!
interface ethernet 3
  hw-interface 3
  ip address 192.168.2.1 255.255.255.0
```

4.2 Provide configuration access for user 'operator' on the LAN interface

Command	Explanation
Step 1: Enable user 'operator' and set authentication password	
config <cr>	Enter the configuration menu
auth operator <cr>	Enter user authentication menu for user 'operator'
active on <cr>	Enable user 'operator'
method pw <cr>	Set authentication method for user 'operator' to password
chpasswd <cr>	Change password for user 'operator'. (Follow instructions on screen)
Step 2: Activate configuration access	
config <cr>	Enter the configuration menu
configlevel-lan operator <cr>	Activate configuration access on LAN interface for user 'operator' (and user 'viewer')

4.3 Activate SNAT on WAN and LAN A

Command	Explanation
config <cr>	Enter the configuration menu
nat-snat <cr>	Enter SNAT configuration menu.
wan active <cr>	Enable SNAT on the WAN interface
lan active lan-a <cr>	Enable SNAT on the LAN A interface.
commit <cr>	Activate settings.

4.4 Enter a packet filter rule

Command	Explanation
config <cr>	Enter the configuration menu
filter-wanlan <cr>	Enter the packet filter configuration menu for direction WAN → LAN
mode white <cr>	Set filter mode to 'white' for direction WAN → LAN
rule 1 any 10.0.0.5 any any any icmp drop my_rule active <cr>	Enter a filter rule that drops all ICMP packets from sender with ip address '10.0.0.5'.
commit <cr>	Activate settings.

4.5 Disable a specific LAN port

If you don't want to use a specific LAN port and want to prevent it from being used, you can disable it completely:

Command	Explanation
config <cr>	Enter the configuration menu
interface lan-port 1 <cr>	Enter configuration menu for LAN port 1.
disable <cr>	Disable LAN port 1.