

# Domači GPON ONT modem

a@4a.si

c|ot 2. 2. 2023



# Namen

- Modem, ki *prevaja* internetni promet med mediji
- Omogoča operaterju, da ima več nadzora nad omrežjem
- Olajša uporabniku povezavo, ker je *ethernet* razširjen in poznan, GPON pa ne
- Poceni strojna oprema

# Model

- Comtrend GRG-4242u
- Cena: ~ 50 €

← → ↻ 🏠 🔒 search.si/janec.eu:7327/?q=comtrend+grg-

comtrend grg-4242u

število zadetkov: 8 | čas poizvedbe:

[GRG-4242u - Comtrend](#) www.comtrend.com > cee > P

Comtrend's residential GPON ONT GRG-4242u designed for advanced triple-play deployment Comtrend's GPON ONTO...

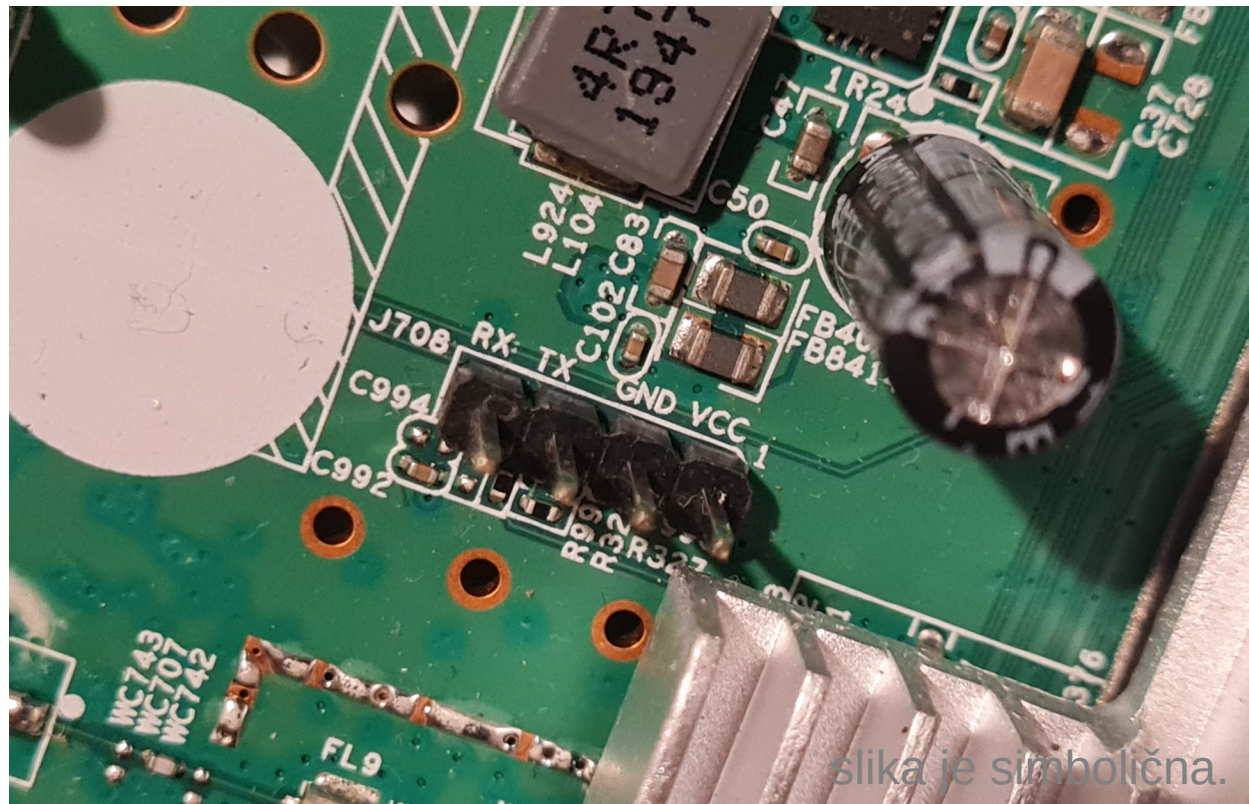


# Specifikacije za operaterje

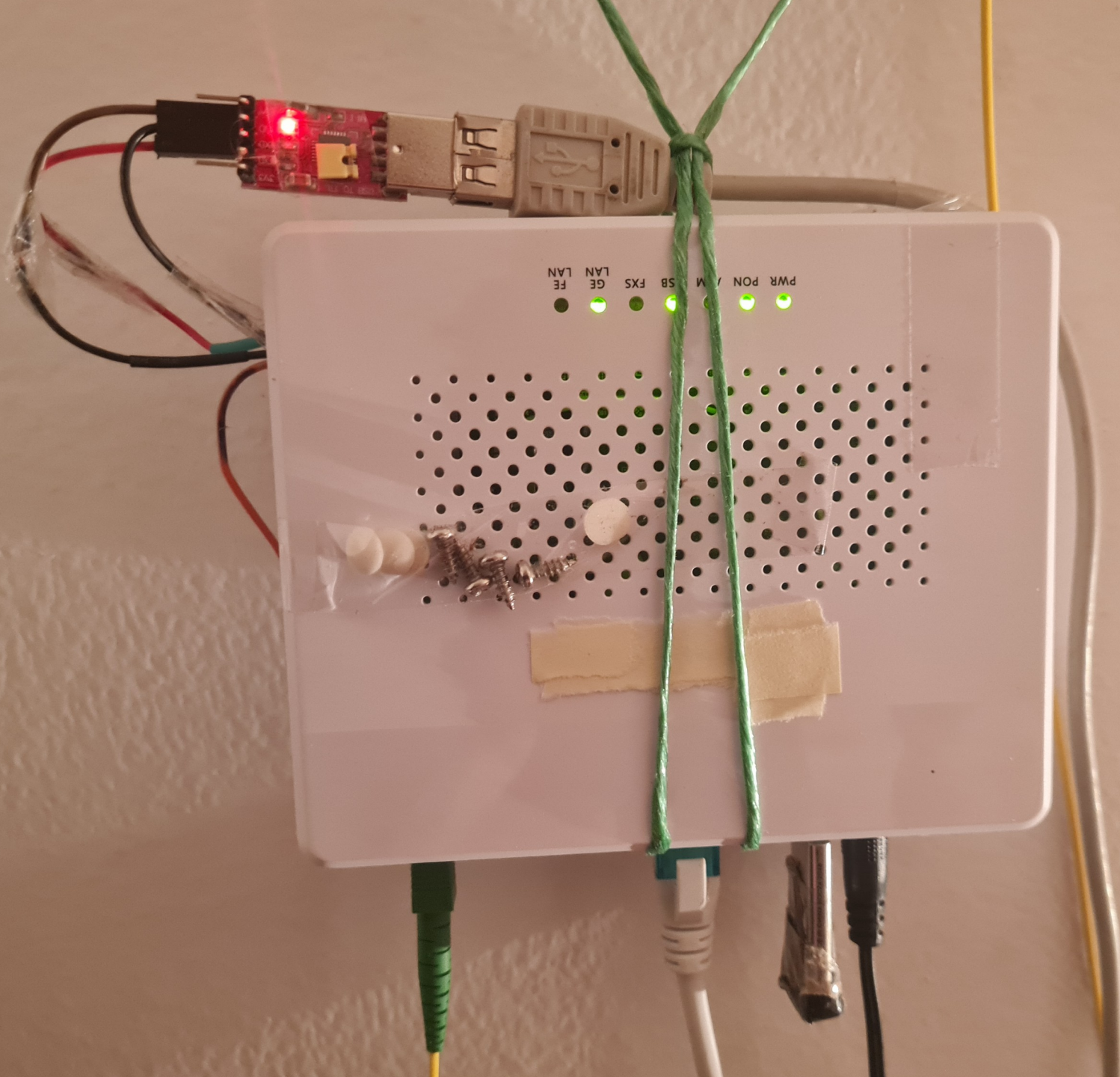
- Trojček preko optike: IGMP TV, analogni telefon, inet
- TR-069 idr., HTTP, SNMP, IPv6
- NTP, DDNS, DHCP, NAT, UPnP starševski nadzor (user:user)
- 1 Gb DDR3, 1 Gb flash
- GE + FE RJ45, USB 2.0, RJ11 s pripadajočim modemom
- odtočno 1,2 Gb/s @ 1310 nm **SC/APC**  
pritočno 2,4 Gb/s @ 1490 nm 20 km

# Specifikacije za hekerje

- BMIPS4350, ~100 MiB RAM, 318 MiB flasha
- FOSS: Linux 3.4.11-rt19 (2012), BusyBox v1.17.2, radvd 1.8 (CVE-2011-3601 CVSS 7.5), ...
- UART



slika je simbolična.



PWR PON M NO SB FXS GE LAN LAN FE



Base: 4.16\_04  
CFE version 1.0.38-116.228-20 for BCM96848 (32bit,SP,BE)  
Build Date: Wed May 16 14:42:10 CST 2018 (antony@localhost.localdomain)  
Copyright (C) 2000-2013 Broadcom Corporation.

Boot Strap Register: 0xffc2  
Chip ID: BCM5848, MIPS: 600MHz, DDR: 533MHz, Bus: 300MHz  
RDP: 428MHz  
Main Thread: TP0  
Total Memory: 134217728 bytes (128MB)  
Boot Address: 0xb8000000

NAND ECC BCH-4, page size 0x800 bytes, spare size used 64 bytes  
NAND flash device: MXIC MX30LF1G08AA, id 0xc2f1 block 128KB size 131072KB  
MDIO Error: MDIO got failure status on phy 1  
Board IP address : 192.168.1.1:ffffff00  
Host IP address : 192.168.1.100  
Gateway IP address :  
Run from flash/host/tftp (f/h/c) : f  
Default host run file name : vmlinux  
Default host flash file name : bcm963xx\_fs\_kernel  
Boot delay (0-9 seconds) : 1  
Boot image (0=latest, 1=previous) : 0  
Default host ramdisk file name :  
Default ramdisk store address :  
Board Id (0-8) : 684880-1862  
Number of MAC Addresses (1-32) : 32  
Base MAC Address : 1c:64:99: [REDACTED]  
PSI Size (1-128) KBytes : 64  
Enable Backup PSI [0|1] : 1  
System Log Size (0-256) KBytes : 0  
Auxillary File System Size Percent: 0  
Serial Number : [REDACTED]  
WLAN Password : 000000000000000000000000  
PCB ID : 0  
ACS Password : 00000000000000000000000000000000  
Main Thread Number [0|1] : 0  
GPON Serial Number : "CMTJ [REDACTED]"  
GPON Password : "0x202020202020202020202020"  
MC memory allocation (MB) : 4  
TM memory allocation (MB) : 20  
DHD 0 memory allocation (MB) : 0  
DHD 1 memory allocation (MB) : 0  
DHD 2 memory allocation (MB) : 0  
WLAN Feature : 0x00  
Voice Board Configuration (0-3) : SI32181\_LCCB  
Partition 1 Size (MB) : 0M  
Partition 2 Size (MB) : 0M  
Partition 3 Size (MB) : 0M  
Partition 4 Size (MB) (Data) : 4M

\*\*\* Press any key to stop auto run (1 seconds) \*\*\*  
Auto run second count down: 0  
Booting from latest image (address 0xbbd80000, flash offset 0x03d80000) ...  
Decompression LZ4 Image OK!  
Entry at 0x803fcd30  
Starting program at 0x803fcd30  
Linux version 3.4.11-rt19 (lucien@ccesw1) (gcc version 4.6.2 (Buildroot 2011.11) ) #1 SMP PREEMPT Mon Aug 31 17:54:32 CST 2020  
reading nvram into inMemNvramData  
ulPsiSize 0x40  
backupPsi 0x1

```
..  
#  
# gponctl getSnPwd | grep -v Serial\ Number:  
  
===== Serial Number & Password =====  
  
Password : 20-20-20-20-20-20-20-20-20-20  
  
=====  
  
# gponctl getEncryptionKey  
  
===== Encryption Key =====  
  
Encryption key: 00000000000000000000000000000000  
  
=====
```



# c4n 1 h45 r007?

- Login: root  
Password for root: >:-/

```
DYING GASP IRQ Initialized and Enabled
Serial: BCM63XX driver $Revision: 3.00 $
Magic SysRq with Auxilliary trigger char enabled (type ^ h for list of supported commands)
ttyS0 at MMIO 0xb0800640 (irq = 104) is a BCM63XX
ttyS1 at MMIO 0xb0800660 (irq = 105) is a BCM63XX
SysRq : HELP : loglevel(0-9) BRCM: show summary status on all CPUs(A) reBoot Cr
ash terminate-all-tasks(E) memory-full-oom-kill(F) kill-all-tasks(I) thaw-files
ystems(J) show-backtrace-all-active-cpus(L) show-memory-usage(M) nice-all-RT-ta
sks(N) powerOff show-registers(P) show-all-timers(Q) Sync show-task-states(T) U
nmount show-blocked-tasks(W) BRCM: show interrupt counts on all CPUs(Y)
All commands are case insensitive.
[]
consoled:error:587.686:oalMsg_initWithFlags:115:connect to /var/smd_messaging_server_addr failed, rc=-1 errno=2
consoled:error:587.686:main:228:could not connect to CMS smd (ret=9002) == drop to shell for debug

BusyBox v1.17.2 (2020-08-31 18:10:51 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

# cat /etc/passwd
admin:$1$DmTYjrz7$/7yJd4aenG/.iCyB5okvC0:0:0:Administrator://:bin/sh
poweruser:$1$mcMxUW7b$oCiocm5Cqr6DyT/t9hCy01:0:0:Technical Support://:bin/sh
user:$1$mG9dQV0M$eu3HAnbw1J6nD8WmyEiIs1:0:0:Normal User://:bin/sh
nobody:$1$jRUyRgpH$tXtFtD/pxxN7PQZYReXmu0:0:0:nobody for ftp://:bin/sh
# []
```

# Pes čuvaj in obratni inženiring

- `/bin/ct_monitor & + cutter`

```
0x004005a5 libcms_msg.so
0x004005b3 libcms_util.so
0x004005c2 libbcm_crc.so
0x004005d0 libbcm_flashutil.so
0x004005e4 libcms_boardctl.so
0x004005f7 libcrypt.so.0
0x00400605 libdl.so.0
0x00400610 libcms_core.so
0x0040061f libcms_qdm.so
0x0040062d libnanoxml.so
0x0040063b libgponctl.so
0x00400649 libgponif.so
0x00400656 libomci.so
0x00400661 libomcipm_drv.so
0x00400672 libm.so.0
0x0040067c libvlanctl.so
0x0040068a libpwrctl.so
0x00400697 libethswctl.so
0x004006a6 libeponctl.so
0x004006b4 librdpactl.so
0x004006c2 libtmctl.so
0x004006ce libc.so.0
0x004006d8 libqcc_s.so.1
```

```
void devCtl_setWatchDogTime(int32_t param_1)
{
    (*gp0xffff8010)();
    (*gp0xffff8010)();
    fcn.00400920(param_1);
    return;
}
```

Type flag name or address here

## Functions



Name

- ▶ entry0
- ▶ fcn.00400920
- ▶ fcn.004009dc
- ▶ fcn.00400a70
- ▶ **main**
- ▶ sym.\_fini
- ▶ sym.\_init
- ▶ sym.imp.\_\_uclibc\_main
- ▶ sym.imp.devCtl\_setWatchDogTime
- ▼ sym.imp.signal
  - Offset: 0x00400af0
  - Size: 0x20
  - Import: true
  - Nargs: 0x0
  - Nbbs: 0x1
  - Nlocals: 0x3
  - Call type: n32
  - Edges: 1
  - StackFrame: 32
  - Comment:
- ▶ sym.imp.sleep
- ▶ sym.stop\_ct\_watchdog

```
// WARNING: Unknown calling convention yet parameter storage is locked
// WARNING: [rz-ghidra] Matching calling convention n32 of function main fa

void main(int argc, char **argv)
{
    int32_t iVar1;
    int32_t in_t9;

    // signal(SIGKILL, signal)
    (**(code **)(in_t9 + 0x103f8))(9, *(undefined4 *)(in_t9 + 0x103ec));
    // signal(SIGHUP, signal)
    (**(code **)(in_t9 + 0x103f8))(1, *(undefined4 *)(in_t9 + 0x103ec));
    // signal(SIGTERM, signal)
    (**(code **)(in_t9 + 0x103f8))(0xf, *(undefined4 *)(in_t9 + 0x103ec));
    // signal(SIGQUIT, signal)
    (**(code **)(in_t9 + 0x103f8))(3, *(undefined4 *)(in_t9 + 0x103ec));
    // signal(SIGPIPE, SIG_IGN)
    (**(code **)(in_t9 + 0x103f8))(0xd, 1);
    // signal(SIGINT, SIG_IGN)
    (**(code **)(in_t9 + 0x103f8))(2, 1);
    iVar1 = *(int32_t *)(in_t9 + 0x103e8);
    while (*(int32_t *)(iVar1 + 0xb90) != 0) {
        // devCtl_setWatchDogTime()
        (**(code **)(in_t9 + 0x103fc))(0x3c);
        // sleep(5)
        (**(code **)(in_t9 + 0x10408))(5);
    }
    return;
}
```

```
b:/tmp/gcc83/build/stbgcc-8.3-0.4[0]# grep "#define\sSIG" mips-unknown-linux-gnu/sys-root/usr/include/bits/signal-generic.h
#define SIG_ERR ((__sighandler_t) -1) /* Error return. */
#define SIG_DFL ((__sighandler_t) 0) /* Default action. */
#define SIG_IGN ((__sighandler_t) 1) /* Ignore signal. */
#define SIGINT 2 /* Interactive attention signal. */
#define SIGILL 4 /* Illegal instruction. */
#define SIGABRT 6 /* Abnormal termination. */
#define SIGFPE 8 /* Erroneous arithmetic operation. */
#define SIGSEGV 11 /* Invalid access to storage. */
#define SIGTERM 15 /* Termination request. */
#define SIGHUP 1 /* Hangup. */
#define SIGQUIT 3 /* Quit. */
#define SIGTRAP 5 /* Trace/breakpoint trap. */
#define SIGKILL 9 /* Killed. */
#define SIGBUS 10 /* Bus error. */
#define SIGSYS 12 /* Bad system call. */
#define SIGPIPE 13 /* Broken pipe. */
#define SIGALRM 14 /* Alarm clock. */
#define SIGURG 16 /* Urgent data is available at a socket. */
#define SIGSTOP 17 /* Stop, unblockable. */
#define SIGTSTP 18 /* Keyboard stop. */
#define SIGCONT 19 /* Continue. */
#define SIGCHLD 20 /* Child terminated or stopped. */
#define SIGTTIN 21 /* Background read from control terminal. */
#define SIGTTOU 22 /* Background write to control terminal. */
#define SIGPOLL 23 /* Pollable event occurred (System V). */
#define SIGXCPU 24 /* CPU time limit exceeded. */
#define SIGXFSZ 25 /* File size limit exceeded. */
#define SIGVTALRM 26 /* Virtual timer expired. */
#define SIGPROF 27 /* Profiling timer expired. */
#define SIGUSR1 30 /* User-defined signal 1. */
#define SIGUSR2 31 /* User-defined signal 2. */
#define SIGWINCH 28 /* Window size change (4.3 BSD, Sun). */
#define SIGIO SIGPOLL /* I/O now possible (4.2 BSD). */
#define SIGIOT SIGABRT /* IOT instruction, abort() on a PDP-11. */
#define SIGCLD SIGCHLD /* Old System V name */
b:/tmp/gcc83/build/stbgcc-8.3-0.4[0]# grep "#define\sSIG" mips-unknown-linux-gnu/sys-root/usr/include/bits/signum.h
#define SIGEMT 7 /* Emulator trap. */
#define SIGPWR 19 /* Power failure imminent. */
#define SIGUSR1 16
#define SIGUSR2 17
#define SIGCHLD 18
#define SIGWINCH 20
#define SIGURG 21
#define SIGPOLL 22
#define SIGSTOP 23
#define SIGTSTP 24
#define SIGCONT 25
#define SIGTTIN 26
#define SIGTTOU 27
#define SIGVTALRM 28
#define SIGPROF 29
#define SIGXCPU 30
#define SIGXFSZ 31
b:/tmp/gcc83/build/stbgcc-8.3-0.4[0]#
```

Broadcom / stbgcc-8.3 Public

Notifications Fork 1 Star 0

Code Issues Pull requests Security Insights

master 1 branch 3 tags

Go to file Code

About

GCC 8.3 based releases (stbgcc)

Readme

0 stars

3 watching

1 fork

Releases 3

stbgcc-8.3-0.4 Latest on Sep 14, 2021

+ 2 releases

Packages

No packages published

Ryceancurry Initial commit 8763726 on Jun 2, 2021 1 commit

README.md Initial commit last year

README.md content: stbgcc-8.3 GCC 8.3 based releases (stbgcc)

# stbgcc-8.3-0.4 Latest

alexchu-cpe released this Sep 14, 2021 `stbgcc-8.3-0.4` 8763726

Fix pthread\_rwlock\_timed\*lock() compiler optimization bug  
Build with docker centos-6.9 & gcc-6.3

```
b:/tmp[0]# cat helloworld.c
#include <stdio.h>
int main (void) {
    puts("Pozdravljen, clot!\n");
}
b:/tmp[0]# mips-linux-gcc -static helloworld.c
b:/tmp[0]# █

#
# wget http://10.69.69.2/a.out
Connecting to 10.69.69.2 (10.69.69.2:80)
200 OK, File Get Success
# chmod +x a.out
# ./a.out
Pozdravljen, clot!

# █
```

## Assets 7

<a href="#">stbgcc-8.3-0.4.x86_64.deb</a>	275 MB	Sep 13, 2021
<a href="#">stbgcc-8.3-0.4.x86_64.rpm</a>	488 MB	Sep 14, 2021
<a href="#">stbgcc-8.3-0.4.x86_64.tar.bz2</a>	433 MB	Sep 14, 2021
<a href="#">stbgcc-8.3-0.4.x86_64.tar.bz2.asc</a>	488 Bytes	Sep 14, 2021
<a href="#">stbgcc-8.3-0.4_src.tar.gz</a>	231 MB	Sep 14, 2021
<a href="#">Source code (zip)</a>		Jun 2, 2021

# Statistika uporabe omrežja

#	day	rx		tx		total		avg. rate
1	2023-01-10	286.56 GiB		147.57 GiB		434.13 GiB		43.16 Mbit/s
2	2022-03-22	138.54 GiB		285.15 GiB		423.69 GiB		42.12 Mbit/s
3	2023-01-07	149.34 GiB		185.11 GiB		334.44 GiB		33.25 Mbit/s
4	2022-07-28	140.84 GiB		129.43 GiB		270.27 GiB		26.87 Mbit/s
5	2022-03-23	187.65 GiB		79.54 GiB		267.19 GiB		26.56 Mbit/s

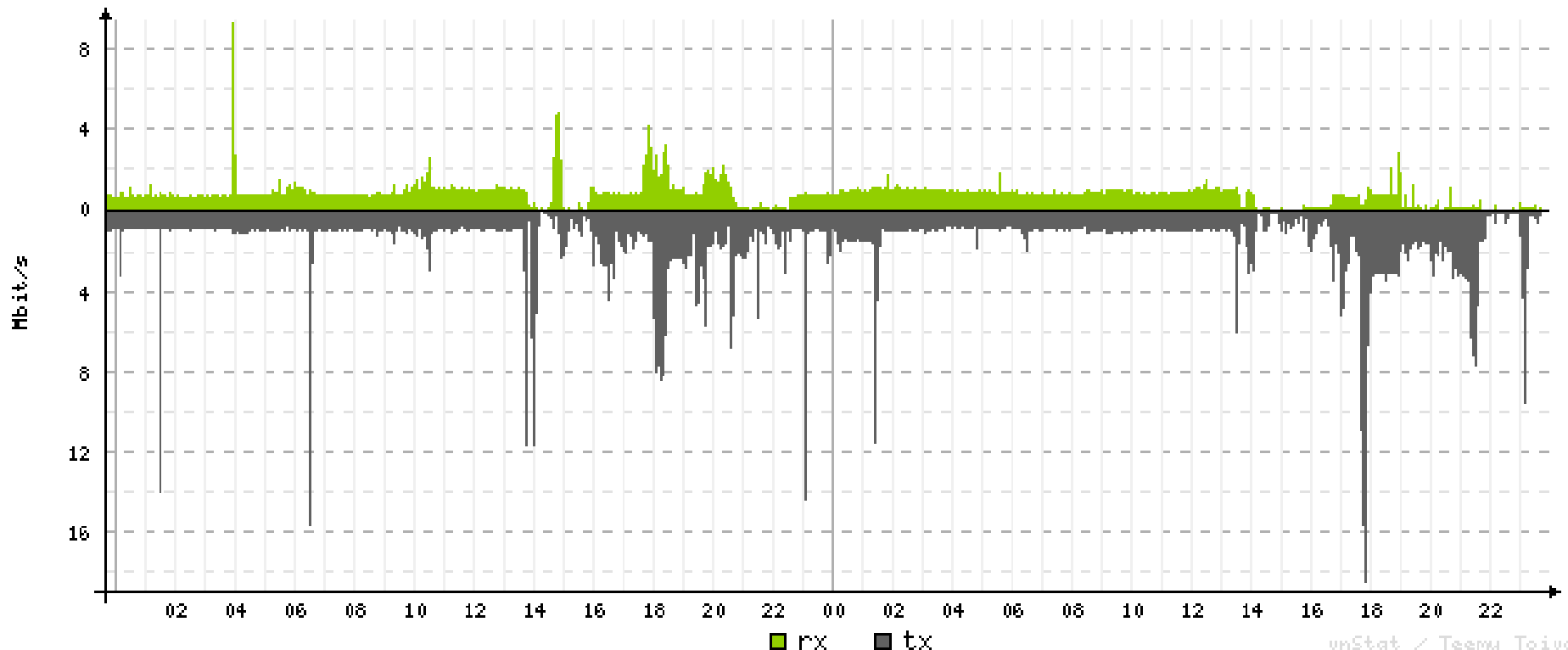
eth1	year	rx		tx		total		avg. rate																
^	2022	27.96 TiB		8.93 TiB		36.89 TiB		10.29 Mbit/s	t															
	2023	2.41 TiB		930.94 GiB		3.32 TiB		10.58 Mbit/s	t															
	estimated	27.54 TiB		10.40 TiB		37.94 TiB			t															
									t															
									t	t														
	t	t							t	t														
	t	t	t	t					t	t	t	t	t	t	t	t	t	t	t	t	t	t	t	
	t	rt	rt	rt	rt	rt	rt	rt	rt	rt	rt	rt	rt	rt	rt	rt	rt	rt	rt	rt	rt	rt	rt	
----->																								
	22	23	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21

# vnStat(i)

- cross-compilation s toolchainom
- libsqlite3, zlib, libpng, libfreetype, libgd in vnstat

<http://4a.si/ont.shtml>

2023-02-01 23:45





# Še nekaj drugih prednosti

```
..
# tcpdump -vvvveni eth1.0 tcp port 1337
tcpdump: WARNING: eth1.0: no IPv4 address assigned
tcpdump: listening on eth1.0, link-type EN10MB (Ethernet), capture size 65535 bytes
23:56:29.415632 88:e6:4b:e3:c1:c6 > 00:1a:92:4b:00:40, ethertype IPv4 (0x0800), length 74: (tos 0x0, ttl 54, id 5140, o
ffset 0, flags [DF], proto TCP (6), length 60)
    83.212.126.242.36418 > 89.212.146.168.1337: Flags [S], cksum 0xfdaa (correct), seq 2843037134, win 64240, options [
mss 1436,sackOK,TS val 351137932 ecr 0,nop,wscale 7], length 0
23:56:29.415908 00:1a:92:4b:00:40 > 88:e6:4b:e3:c1:c6, ethertype IPv4 (0x0800), length 74: (tos 0x0, ttl 64, id 0, offs
et 0, flags [DF], proto TCP (6), length 60)
    89.212.146.168.1337 > 83.212.126.242.36418: Flags [S.], cksum 0x7edd (correct), seq 4293563424, ack 2843037135, win
65160, options [mss 1460,sackOK,TS val 4153470828 ecr 351137932,nop,wscale 10], length 0
23:56:29.451483 88:e6:4b:e3:c1:c6 > 00:1a:92:4b:00:40, ethertype IPv4 (0x0800), length 66: (tos 0x0, ttl 54, id 5141, o
ffset 0, flags [DF], proto TCP (6), length 52)
    83.212.126.242.36418 > 89.212.146.168.1337: Flags [.], cksum 0xaa1b (correct), seq 1, ack 1, win 502, options [nop,
TS val 351137968 ecr 4153470828], length 0
23:56:31.290789 88:e6:4b:e3:c1:c6 > 00:1a:92:4b:00:40, ethertype IPv4 (0x0800), length 69: (tos 0x0, ttl 54, id 5142, o
ffset 0, flags [DF], proto TCP (6), length 55)
    83.212.126.242.36418 > 89.212.146.168.1337: Flags [P.], cksum 0x2977 (correct), seq 1:4, ack 1, win 502, options [nop,
TS val 351139807 ecr 4153470828], length 3
23:56:34.264886 00:1a:92:4b:00:40 > 88:e6:4b:e3:c1:c6, ethertype IPv4 (0x0800), length 66: (tos 0x0, ttl 64, id 35566,
offset 0, flags [DF], proto TCP (6), length 52)
    89.212.146.168.1337 > 83.212.126.242.36418: Flags [F.], cksum 0x91ad (correct), seq 1, ack 4, win 64, options [nop,
TS val 4153475677 ecr 351139807], length 0
23:56:34.300698 88:e6:4b:e3:c1:c6 > 00:1a:92:4b:00:40, ethertype IPv4 (0x0800), length 66: (tos 0x0, ttl 54, id 5143, o
ffset 0, flags [DF], proto TCP (6), length 52)
    83.212.126.242.36418 > 89.212.146.168.1337: Flags [F.], cksum 0x8434 (correct), seq 4, ack 2, win 502, options [nop,
TS val 351142817 ecr 4153475677], length 0
23:56:34.300933 00:1a:92:4b:00:40 > 88:e6:4b:e3:c1:c6, ethertype IPv4 (0x0800), length 66: (tos 0x0, ttl 64, id 35567,
offset 0, flags [DF], proto TCP (6), length 52)
    89.212.146.168.1337 > 83.212.126.242.36418: Flags [.], cksum 0x85c6 (correct), seq 2, ack 5, win 64, options [nop,n
op,TS val 4153475713 ecr 351142817], length 0
^C
7 packets captured
7 packets received by filter
0 packets dropped by kernel
```

```
# █
```

# Še nekaj drugih prednosti

- Večja varnost in zasebnost, ker teče manj procesov
- Lažje diagnosticiramo težave z omrežjem
- Za zahtevnejšega uporabnika je uporaben direkten dostop do dnevniških zapisov:

```
ERR: bdmf_attr_elem_add_as_buf#4215: ip_class: status:Error in parameters. attribute:flow index:0
ERR: ip_flow_key_validate#1112: status:Error in parameters Missing Source port
ERR: bdmf_attr_elem_add_as_buf#4215: ip_class: status:Error in parameters. attribute:flow index:0
ERR: ip_flow_key_validate#1112: status:Error in parameters Missing Source port
ERR: bdmf_attr_elem_add_as_buf#4215: ip_class: status:Error in parameters. attribute:flow index:0
ERR: ip_flow_key_validate#1112: status:Error in parameters Missing Source port
ERR: bdmf_attr_elem_add_as_buf#4215: ip_class: status:Error in parameters. attribute:flow index:0
INFO: rcu_preempt detected stalls on CPUs/tasks: {} (detected by 0, t=60002 jiffies)
INFO: Stall ended before state dump start
ERR: ip_class_attr_flow_add#1185: status:Internal error IP flow creation failed, error=150
ERR: bdmf_attr_elem_add_as_buf#4215: ip_class: status:Internal error. attribute:flow index:0
ERR: ip_class_attr_flow_add#1185: status:Internal error IP flow creation failed, error=150
ERR: bdmf_attr_elem_add_as_buf#4215: ip_class: status:Internal error. attribute:flow index:0
INFO: rcu_preempt detected stalls on CPUs/tasks: {} (detected by 0, t=60002 jiffies)
INFO: Stall ended before state dump start
ERR: ip_class_attr_flow_add#1185: status:Internal error IP flow creation failed, error=150
ERR: bdmf_attr_elem_add_as_buf#4215: ip_class: status:Internal error. attribute:flow index:6835
ERR: ip_class_attr_flow_add#1185: status:Internal error IP flow creation failed, error=150
ERR: bdmf_attr_elem_add_as_buf#4215: ip_class: status:Internal error. attribute:flow index:13744
ERR: ip_class_attr_flow_add#1185: status:Internal error IP flow creation failed, error=150
ERR: bdmf_attr_elem_add_as_buf#4215: ip_class: status:Internal error. attribute:flow index:-2147408548
ERR: ip_class_attr_flow_add#1185: status:Internal error IP flow creation failed, error=150
ERR: bdmf_attr_elem_add_as_buf#4215: ip_class: status:Internal error. attribute:flow index:0
ERR: ip_class_attr_flow_add#1185: status:Internal error IP flow creation failed, error=150
ERR: bdmf_attr_elem_add_as_buf#4215: ip_class: status:Internal error. attribute:flow index:0
ERR: ip_class_attr_flow_add#1185: status:Internal error IP flow creation failed, error=150
ERR: bdmf_attr_elem_add_as_buf#4215: ip_class: status:Internal error. attribute:flow index:0
ERR: ip_class_attr_flow_add#1185: status:Internal error IP flow creation failed, error=150
ERR: bdmf_attr_elem_add_as_buf#4215: ip_class: status:Internal error. attribute:flow index:10492
ERR: ip_class_attr_flow_add#1185: status:Internal error IP flow creation failed, error=150
ERR: bdmf_attr_elem_add_as_buf#4215: ip_class: status:Internal error. attribute:flow index:6992
ERR: ip_class_attr_flow_add#1185: status:Internal error IP flow creation failed, error=150
ERR: bdmf_attr_elem_add_as_buf#4215: ip_class: status:Internal error. attribute:flow index:-2078137336
ERR: ip_class_attr_flow_add#1185: status:Internal error IP flow creation failed, error=150
ERR: bdmf_attr_elem_add_as_buf#4215: ip_class: status:Internal error. attribute:flow index:0
ERR: ip_class_attr_flow_add#1185: status:Internal error IP flow creation failed, error=150
ERR: bdmf_attr_elem_add_as_buf#4215: ip_class: status:Internal error. attribute:flow index:0
ERR: ip_class_attr_flow_add#1185: status:Internal error IP flow creation failed, error=150
ERR: bdmf_attr_elem_add_as_buf#4215: ip_class: status:Internal error. attribute:flow index:0
ERR: ip_class_attr_flow_add#1185: status:Internal error IP flow creation failed, error=150
ERR: bdmf_attr_elem_add_as_buf#4215: ip_class: status:Internal error. attribute:flow index:0
ERR: ip_class_attr_flow_add#1185: status:Internal error IP flow creation failed, error=150
ERR: bdmf_attr_elem_add_as_buf#4215: ip_class: status:Internal error. attribute:flow index:0
ERR: ip_class_attr_flow_add#1185: status:Internal error IP flow creation failed, error=150
ERR: bdmf_attr_elem_add_as_buf#4215: ip_class: status:Internal error. attribute:flow index:0
```

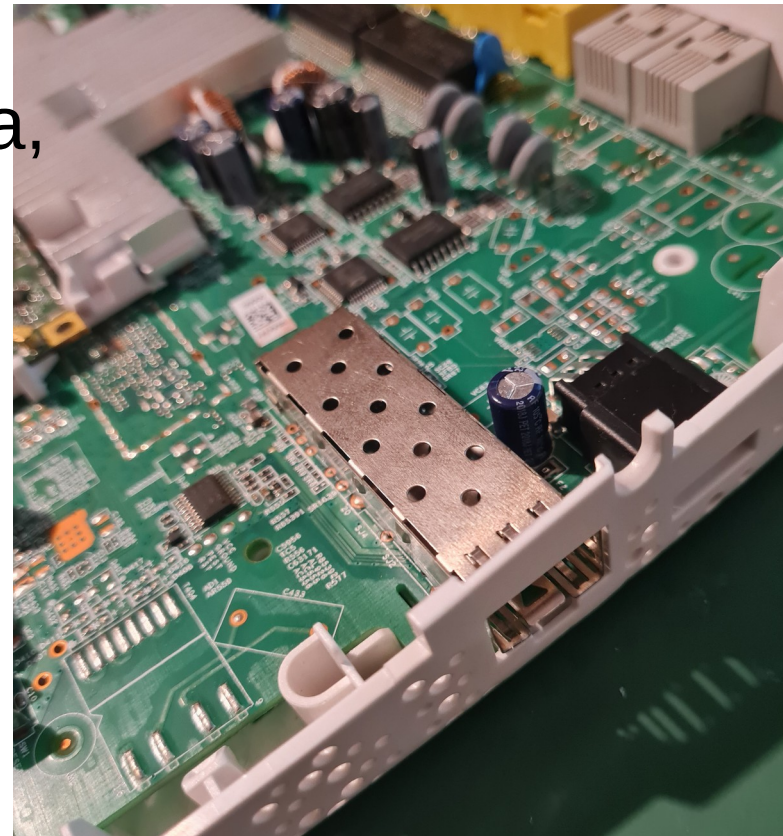
```
00000000@UJU
```

# Težave

- V primeru *hekanja* modema operater *ne bo vesel* porabljenega časa za podporo
- Neha delovati, ko operater hoče spremeniti nastavitve, pa TR-069/SNMP ne deluje (ponavadi je restart za nekaj sekund dovolj za ponovno vzpostavitev)
- Na modem lahko nekdo naloži zlonamerno programsko opremo in ga vrne operaterju

# Beseda o SFP

- *Small form-factor pluggable*
- Na njem teče lastniška koda in OS (Linux)
- ONU
- Standardizirana komunikacija, ki pa ni *ethernet*
- Ponavadi za uporabnika proti plačilu



# Ideje za prihodnost

- Kloniranje modema (oz. S/N)
- Preizkušanje, kaj se zgodi, ko se na priključku pojavi nepričakovan S/N
- Implementacija TR-069 in SNMP strežnika, ki posluša zahteve operaterja
- Prošnja operaterju/proizvajalcu za izvorno kodo GPL orodij

Vprašanja?

# Viri, literatura in dodatno

- <https://hack-gpon.github.io/>
- [https://www.comtrend.com/cee/Product/236\\$prod.html](https://www.comtrend.com/cee/Product/236$prod.html)
- [https://www.comtrend.com/dbase/upload-img/download/DS\\_GRG-4242u\\_R1%203\\_031721.pdf](https://www.comtrend.com/dbase/upload-img/download/DS_GRG-4242u_R1%203_031721.pdf)
- <http://splet.šijanec.eu./ont.shtml>