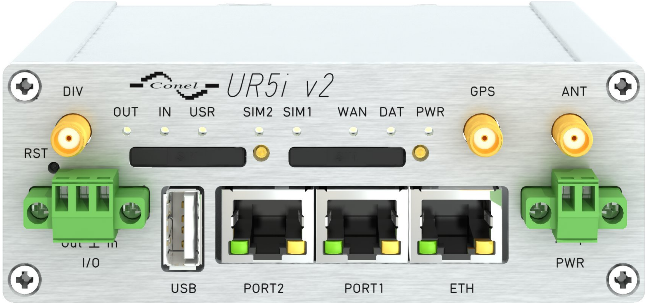
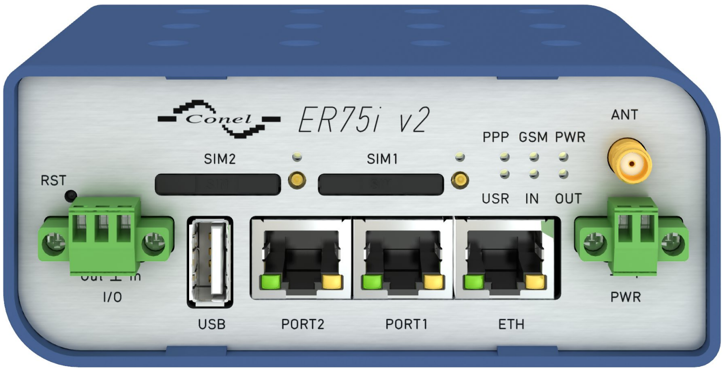
User Module

NMAP

APPLICATION NOTE





ADVANTECH

Used symbols

Danger – Information regarding user safety or potential damage to the router.

Attention – Problems that may arise in specific situations.

Information or notice – Useful tips or information of special interest.

Example – example of function, command or script.

Advantech B+B SmartWorx s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Document No. APP-0043-EN, revised on November 28, 2018. Released in the Czech Republic.

Contents

List of Figures

1. Description of user module

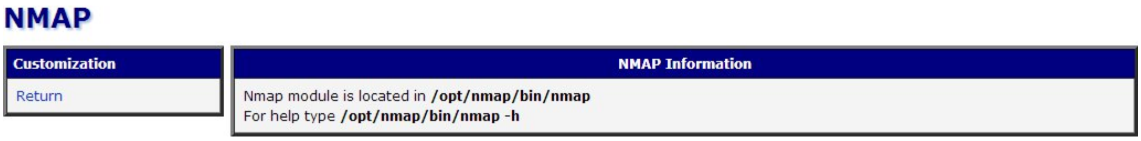
User module *NMAP* is not contained in the standard router firmware. Uploading of this user module is described in the Configuration manual (see [1, 2]).

The user module is v2 and v3 router platforms compatible.

This module allows user to perform TCP and UDP scan. It can also be used for sending pings (i.e. IP datagrams, which are intended to verify the functionality of a connection between two network interfaces).

NMAP module has a web interface which can be invoked by pressing the module name on the *User modules* page of the router web interface. The left part of the web interface (ie. menu) contains only the *Return* item, which switches this web interface to the interface of the router. In the right part are displayed the following information:

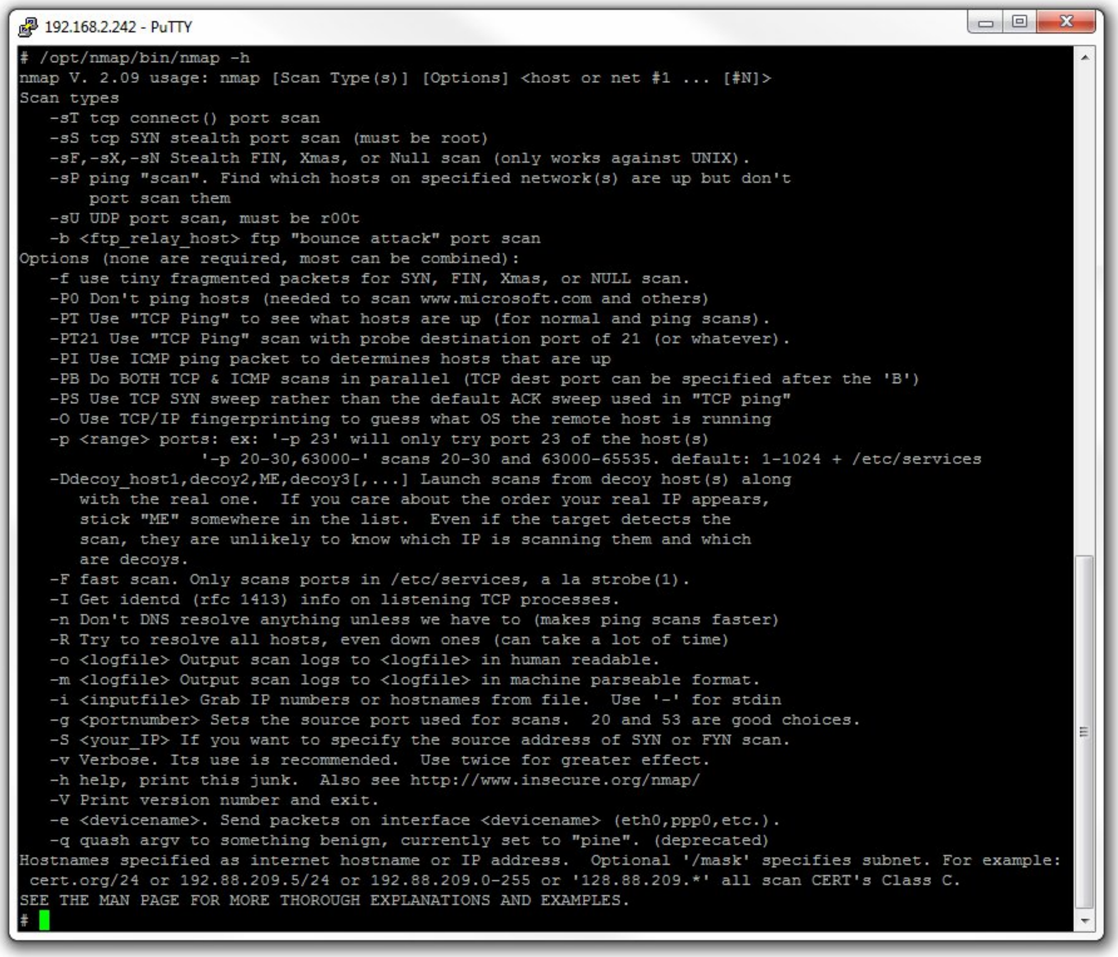
- Nmap module is located in /opt/nmap/bin/nmap
- For help type /opt/nmap/bin/nmap -h



Nmap module is located in **/opt/nmap/bin/nmap**
For help type **/opt/nmap/bin/nmap -h**

Figure 1: Web interface

The first line informs about the location of NMAP user module and the second informs about a way to display help for this module. After invoking the help, a list of all parameters which can be used in the context of this module is printed (see figure on next page). Most of them can be combined.



```
# /opt/nmap/bin/nmap -h
nmap V. 2.09 usage: nmap [Scan Type(s)] [Options] <host or net #1 ... [#N]>
Scan types
   -sT tcp connect() port scan
   -sS tcp SYN stealth port scan (must be root)
   -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (only works against UNIX).
   -sP ping "scan". Find which hosts on specified network(s) are up but don't
       port scan them
   -sU UDP port scan, must be r00t
   -b <ftp_relay_host> ftp "bounce attack" port scan
Options (none are required, most can be combined):
   -f use tiny fragmented packets for SYN, FIN, Xmas, or NULL scan.
   -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
   -PT Use "TCP Ping" to see what hosts are up (for normal and ping scans).
   -PT21 Use "TCP Ping" scan with probe destination port of 21 (or whatever).
   -PI Use ICMP ping packet to determines hosts that are up
   -PB Do BOTH TCP & ICMP scans in parallel (TCP dest port can be specified after the 'B')
   -PS Use TCP SYN sweep rather than the default ACK sweep used in "TCP ping"
   -O Use TCP/IP fingerprinting to guess what OS the remote host is running
   -p <range> ports: ex: '-p 23' will only try port 23 of the host(s)
                  '-p 20-30,63000-' scans 20-30 and 63000-65535. default: 1-1024 + /etc/services
   -Ddecoy_host1,decoy2,ME,decoy3[,...] Launch scans from decoy host(s) along
      with the real one.  If you care about the order your real IP appears,
      stick "ME" somewhere in the list.  Even if the target detects the
      scan, they are unlikely to know which IP is scanning them and which
      are decoys.
   -F fast scan. Only scans ports in /etc/services, a la strobe(1).
   -I Get identd (rfc 1413) info on listening TCP processes.
   -n Don't DNS resolve anything unless we have to (makes ping scans faster)
   -R Try to resolve all hosts, even down ones (can take a lot of time)
   -o <logfile> Output scan logs to <logfile> in human readable.
   -m <logfile> Output scan logs to <logfile> in machine parseable format.
   -i <inputfile> Grab IP numbers or hostnames from file.  Use '-' for stdin
   -g <portnumber> Sets the source port used for scans.  20 and 53 are good choices.
   -S <your_IP> If you want to specify the source address of SYN or FYN scan.
   -v Verbose. Its use is recommended.  Use twice for greater effect.
   -h help, print this junk.  Also see http://www.insecure.org/nmap/
   -V Print version number and exit.
   -e <devicename>. Send packets on interface <devicename> (eth0,ppp0,etc.).
   -q quash argv to something benign, currently set to "pine". (deprecated)
Hostnames specified as internet hostname or IP address.  Optional '/mask' specifies subnet. For example:
 cert.org/24 or 192.88.209.5/24 or 192.88.209.0-255 or '128.88.209.*' all scan CERT's Class C.
SEE THE MAN PAGE FOR MORE THOROUGH EXPLANATIONS AND EXAMPLES.
# 
```

Figure 2: NMAP help (Telnet or SSH)

2. Recommended literature

[1] Advantech B+B SmartWorx: **v2 Routers Configuration Manual** (MAN-0021-EN)

[2] Advantech B+B SmartWorx: **SmartFlex Configuration Manual** (MAN-0023-EN)

[3] Advantech B+B SmartWorx: **SmartMotion Configuration Manual** (MAN-0024-EN)

[4] Advantech B+B SmartWorx: **SmartStart Configuration Manual** (MAN-0022-EN)

[5] Advantech B+B SmartWorx: **ICR-3200 Configuration Manual** (MAN-0042-EN)

Product related documents can be obtained on *Engineering Portal* at `https://ep.advantech-bb.cz/` address.