	SmallNetBuilder Router Functional Test List - Version 4 process	
	name	**description**
1	cdrouter_dos_1	Send 'ping of death' ICMP request to LAN side of the router
2	cdrouter_dos_2	Send 'ping of death' ICMP request to WAN side of the router
3	cdrouter_dos_10	Launch LAND attack against router's management port on the LAN
4	cdrouter_dos_20	Verify that the DUT is not a Smurf reflector (ICMP attack)
5	cdrouter_dos_21	Verify that the DUT is not a Fraggle reflector (UDP attack)
6	cdrouter_dos_30	SYN floods an open port on the DUT from spoofed LAN clients
7	cdrouter_dos_31	SYN floods an open port on the WAN from spoofed Internet addresses
8	cdrouter_dos_32	ARP floods the DUT's LAN interface
9	cdrouter_dos_33	Christmas Tree floods the service ports on the WAN from spoofed Internet addresses
10	cdrouter_dos_34	Floods the WAN interface with anomalous TCP packets
11	cdrouter_scale_1	Verify all DHCP clients are operational
12	cdrouter_scale_2	Verify all DHCP clients with multiple TCP connections
13	cdrouter_scale_3	Verify all DHCP clients with single UDP connection
14	cdrouter_scale_10	Verify no duplicate IP addresses are assigned when DHCP address pool is exhausted
15	cdrouter_scale_15	Verify all DHCP clients can create an IPSEC tunnel
16	cdrouter_scale_20	Verify all DHCP clients can create a PPTP tunnel
17	cdrouter_scale_30	Verify all DHCP clients can create a L2TP/IPSEC tunnel
18	cdrouter_scale_40	Verify all DHCP clients can create a L2TP/IPSEC tunnel with NAT-T
19	cdrouter_ssl_100	Verify DUT's LAN HTTPS server refuses connections with deprecated SSL protocols
20	cdrouter_ssl_200	Verify DUT's LAN HTTPS server refuses connections with deprecated SSL ciphers
21	cdrouter_heartbleed_100	Verify DUT's LAN HTTPS server is protected against heartbleed exploit
22	cdrouter_heartbleed_200	Verify DUT's WAN HTTPS server is protected against heartbleed exploit
23	cdrouter_dhcp_server_1	Verify DHCP server returns same IP address when client renews
24	cdrouter_dhcp_server_2	Verify DHCP server rejects DHCPREQUESTS with non-offered IP address
25	cdrouter_dhcp_server_100	Verify DHCP server accepts DHCP client packets with IPv4 length less than 576
26	cdrouter_dhcp_server_200	Verify DHCP server rejects DHCPREQUESTS with IP address of other clients
27	cdrouter_dhcp_server_300	Verify DHCP server ignores site-specific DHCP options
28	cdrouter_dhcp_server_301	Verify DHCP server handles client option with length 0
29	cdrouter_dhcp_server_401	Verify DHCP server ignores DHCP packets with an invalid UDP checksum
30	cdrouter_dhcp_server_501	Verify DHCP server allows multiple DHCP clients with same name (DHCP option 12)
31	cdrouter_dhcp_server_520	Verify DHCP server uses IPv4 broadcast when DHCP client sets broadcast flag
32	cdrouter_dhcp_server_540	Verify DHCP server probes IPv4 client address before assigning
33	cdrouter_dhcp_server_710	Verify DHCP server handles clients using V-I Vendor-Specific Information option
34	cdrouter_dhcp_server_720	Verify DHCP server handles clients using V-I Vendor Class option
35	cdrouter_http_100	Verify HTTP/1.0 GET connections
36	cdrouter_http_101	Verify HTTP/1.0 POST connections
37	cdrouter_http_102	Verify HTTP/1.0 HEAD connections
38	cdrouter_http_200	Verify HTTP/1.1 GET connections
39	cdrouter_http_201	Verify HTTP/1.1 POST connections
40	cdrouter_http_202	Verify HTTP/1.1 HEAD connections
41	cdrouter_http_203	Verify HTTP/1.1 PUT connections
42	cdrouter_http_204	Verify HTTP/1.1 OPTIONS connections
43	cdrouter_http_205	Verify HTTP/1.1 DELETE connections
44	cdrouter_http_250	Verify HTTP/1.1 GET connections with chunked encoding
45	cdrouter_http_260	Verify HTTP/1.1 proxy idle timeout
46	cdrouter_http_270	Verify HTTP/1.1 pipelining
47	cdrouter_http_280	Verify HTTP/1.1 streaming using chunked encoding
48	cdrouter_https_100	Verify HTTPS/1.0 GET connections
49	cdrouter_https_101	Verify HTTPS/1.0 POST connections
50	cdrouter_https_102	Verify HTTPS/1.0 HEAD connections
51	cdrouter_https_200	Verify HTTPS/1.1 GET connections
52	cdrouter_https_201	Verify HTTPS/1.1 POST connections
53	cdrouter_https_202	Verify HTTPS/1.1 HEAD connections
54	cdrouter_https_203	Verify HTTPS/1.1 PUT connections
55	cdrouter_https_204	Verify HTTPS/1.1 OPTIONS connections
56	cdrouter_https_205	Verify HTTPS/1.1 DELETE connections
57	cdrouter_https_250	Verify HTTPS/1.1 GET connections with chunked encoding
58	cdrouter_nat_1	Outbound TCP connections use NAPT
59	cdrouter_nat_2	Outbound UDP connections use NAPT
60	cdrouter_nat_101	NAPT with multiple LAN hosts using the same TCP source port
61	cdrouter_nat_120	NAPT with a TCP and UDP connection using the same source port
62	cdrouter_nat_130	Verify NAPT with outbound TCP connections using high and low source ports
63	cdrouter_nat_150	Verify TCP source port can be reused after a passive close behind NAPT
64	cdrouter_nat_201	NAPT with multiple LAN hosts using the same UDP source port
65	cdrouter_nat_300	Verify NAPT checks source IP address of inbound UDP packets
66	cdrouter_nat_320	UDP headers with a checksum equal to 0 should not be modified
67	cdrouter_nat_330	Outbound TCP connection using IPv4 options
68	cdrouter_nat_340	Outbound UDP connection using IPv4 options
69	cdrouter_nat_350	Verify NAPT uses port parity preservation
70	cdrouter_nat_360	Verify ICMP Destination Unreachable message from WAN does not destroy NAT UDP mapping
71	cdrouter_nat_361	Verify ICMP Destination Unreachable message from WAN does not destroy NAT TCP mapping
72	cdrouter_nat_400	Verify basic MSS Clamping for TCP sessions
73	cdrouter_nat_401	Verify MSS Clamping with TCP options from different clients
74	cdrouter_nat_410	Verify MSS Clamping does not modify smaller MSS values
75	cdrouter_nat_500	NAT uses single binding for TCP session with same source IP and source port
76	cdrouter_nat_501	NAT uses single binding for UDP session with same source IP and source port
77	cdrouter_nat_510	NAT performs hairpin translation for LAN side TCP connections
78	cdrouter_nat_511	NAT performs hairpin translation for LAN side UDP connections
79	cdrouter_nat_530	Verify TCP connections using TCP window scale option through NAT

80	cdrouter_nat_600	Verify TCP Fast Open cookie request through NAT
81	cdrouter_nat_610	Verify TCP connections using TCP Fast Open option through NAT
82	cdrouter_icmp_1	Verify ICMP Echo Requests (ping) work through router
83	cdrouter_icmp_2	Verify ICMP Echo Requests from multiple LAN clients work through router
84	cdrouter_icmp_5	Verify ICMP Echo Requests to router's LAN side IP address from the LAN
85	cdrouter_icmp_6	Verify ICMP Echo Requests to router's WAN side IP address from the LAN
86	cdrouter_icmp_10	Verify ICMP Time Exceeded packet is sent when incoming TTL is 1
87	cdrouter_icmp_11	Verify NAT translates IP address in ICMP Time Exceeded packet
88	cdrouter_icmp_12	Verify NAT translates IP address in ICMP Destination Unreachable with code port unreachable
89	cdrouter_icmp_13	Verify NAT translates IP address in ICMP Destination Unreachable with code fragmentation needed
90	cdrouter_icmp_14	Verify NAT translates IP address in outbound ICMP Destination Unreachable with code port unreachable
91	cdrouter_icmp_20	Verify router supports Path MTU Discovery over WAN interface
92	cdrouter_forward_1	Verify IPv4 TTL is decremented for forwarded packets
93	cdrouter_forward_2	Verify packet is not forwarded when IPv4 TTL is 1
94	cdrouter_forward_3	Verify packet can be forwarded back through incoming LAN interface
95	cdrouter_forward_4	Verify packet is not forwarded if IPv4 checksum is corrupt
96	cdrouter_forward_10	Forward UDP packets with various packet lengths (LAN to WAN)
97	cdrouter_forward_11	Forward UDP packets with various packet lengths (WAN to LAN)
98	cdrouter_forward_20	No packets are forwarded if WAN lease expires
99	cdrouter_firewall_100	Perform TCP port scan test on router's public WAN IP address
100	cdrouter_firewall_101	Perform UDP port scan test on router's public WAN IP address
101	cdrouter_firewall_1	Inbound TCP connections to public side HTTP port are blocked
102	cdrouter_firewall_2	Inbound TCP connections to LAN hosts are blocked
103	cdrouter_firewall_10	DHCP server ignores DHCP client request from the WAN
104	cdrouter_firewall_12	DNS requests from the WAN are ignored by DNS proxy or relay
105	cdrouter_firewall_110	Perform TCP fragmentation port scan test on router's public WAN IP address
106	cdrouter_firewall_301	Verify firewall blocks/accepts piggyback TCP SYN connections from WAN
107	cdrouter_vservice_10	Verify each configured TCP virtual service
108	cdrouter_vservice_20	Verify each configured UDP virtual service
109	cdrouter_vservice_30	Verify TCP virtual services are reachable from the LAN side
110	cdrouter_vservice_40	Verify UDP virtual services are reachable from the LAN side
111	cdrouter_tport_10	Verify basic case for each configured trigger port application
112	cdrouter_tport_30	Verify multiple LAN hosts can use trigger ports after mappings are aged out
113	cdrouter_l2tppt_1	Verify L2TP session passes through router
114	cdrouter_l2tppt_2	Verify L2TP over IPSEC session passes through router
115	cdrouter_l2tppt_10	Verify L2TP over IPSEC with NAT-T passes through router
116	cdrouter_pptppt_1	PPTP control session can be established at port 1723
117	cdrouter_pptppt_2	Tunneled PPTP data packets pass through router (PPP over GRE)
118	cdrouter_pptppt_100	Verify the max number of PPTP pass through connections for a single LAN host
119	cdrouter_ipsecpt_1	Verify IKE packets pass through router on UDP port 500
120	cdrouter_ipsecpt_2	Verify tunnel mode IPSEC packets pass through router
121	cdrouter_ipsecpt_3	Fragmented tunnel mode IPSEC packets are forwarded between LAN and WAN
122	cdrouter_ipsecpt_30	Verify unknown IPv4 protocol types using the pass through mechanism
123	cdrouter_ipsecpt_100	Verify the maximum number of IPSEC pass through connections for a single LAN host
124	cdrouter_ipsecpt_120	Verify IKE with multiple LAN clients using same VPN server
125	cdrouter_ipsecpt_200	IPSEC pass through without NAT-T based IPSEC client
126	cdrouter_ipsecpt_210	IPSEC pass through with NAT-T based IPSEC client
127	cdrouter_app_2	Verify router supports the active mode FTP PORT command
128	cdrouter_app_3	Multiple FTP connections using the same source port
129	cdrouter_app_10	Connections opened for FTP PORT command check for correct IPv4 address
130	cdrouter_app_11	Verify FTP PORT command succeeds when TCP segment is retransmitted
131	cdrouter_app_12	Verify FTP PORT translation stays the same when TCP segment is retransmitted
132	cdrouter_app_14	Verify router closes public ports opened with the FTP PORT command
133	cdrouter_app_20	Verify DNS queries to router are forwarded to real DNS server
134	cdrouter_app_21	Verify DNS queries sent to primary DNS server
135	cdrouter_app_22	Verify DNS queries sent to backup DNS server
136	cdrouter_app_25	Verify DNS relay on router fails over to backup DNS server
137	cdrouter_app_26	Verify DNS relay on router fails over to backup DNS server (using same ID for retransmissions)
138	cdrouter_app_100	Verify router supports wrapping of TCP sequence number for FTP transfers
139	cdrouter_app_110	Verify HTTPS session through the router
140	cdrouter_app_120	Verify SMTP session through the router
141	cdrouter_app_122	Verify POP3 session through the router
142	cdrouter_app_124	Verify TFTP session through the router
143	cdrouter_app_126	Verify NTP session through the router
144	cdrouter_app_130	Verify STUN session through the router
145	cdrouter_app_131	Verify authenticated STUN session through the router
146	cdrouter_app_200	Verify router translates outbound H.323/Q.931 SETUP messages
147	cdrouter_app_205	Verify router translates outbound H.245 Open Logical Channel Requests
148	cdrouter_app_207	Verify router translates outbound H.245 Open Logical Channel Ack Response
149	cdrouter_mptcp_1	Verify a Multipath TCP connection can be opened
150	cdrouter_mptcp_2	Verify a Multipath TCP connection with two subflows can be opened
151	cdrouter_renumber_1	Verify WAN client learns new IP address when WAN server renumbers
152	cdrouter_renumber_2	Verify existing TCP connections can be reestablished after WAN renumber
153	cdrouter_renumber_6	Verify WAN side switches to new gateway after renumber
154	cdrouter_ssdp_1	Verify UPnP router responds to SSDP Discovery Requests on LAN
155	cdrouter_ssdp_2	Verify UPnP router does not respond to SSDP Discovery Requests on WAN
156	cdrouter_ssdp_3	Verify UPnP router supports discovery of required IGD devices and services
157	cdrouter_ssdp_5	Verify UPnP router responds to unicast SSDP Discovery Requests on LAN
158	cdrouter_upnp_10	Verify XML description of IGD root device can be parsed
159	cdrouter_upnp_12	Verify XML descriptions can not be loaded from the WAN side of router
160	cdrouter_upnp_20	Verify XML description for WANIPConnection or WANPPPConnection service can be parsed

161	cdrouter_upnp_25	Verify router responds to UPnP Query for ConnectionStatus
162	cdrouter_upnp_30	Verify UPnP GetExternalIPAddress Action returns WAN IP address
163	cdrouter_upnp_31	Verify UPnP GetStatusInfo Action returns correct ConnectionStatus information
164	cdrouter_upnp_32	Verify UPnP GetStatusInfo Action returns increasing Uptime value
165	cdrouter_upnp_35	Add/delete dynamic UPnP TCP port mapping for wildcard IP source address
166	cdrouter_upnp_36	Add/delete dynamic UPnP TCP port mapping for specific IP source address
167	cdrouter_upnp_40	Add/delete dynamic UPnP UDP port mapping for wildcard IP source address
168	cdrouter_upnp_41	Add/delete dynamic UPnP UDP port mapping for specific IP source address
169	cdrouter_upnp_45	Verify UPnP Router rejects new port mappings that conflict
170	cdrouter_upnp_50	Verify dynamic UPnP port mapping is deleted when lease expires
171	cdrouter_upnp_100	Maximum number of UPnP TCP dynamic port mappings
172	cdrouter_upnp_200	Verify UPnP clients can subscribe/unsubcribe to events for WANIPConnection or WANPPPConnection
173	cdrouter_upnp_201	Verify UPnP clients can subscribe to events with infinite subscription time
174	cdrouter_upnp_202	Verify UPnP clients can renew NOTIFY events for WANIPConnection or WANPPPConnection
175	cdrouter_upnp_203	Verify router sends UPnP NOTIFY events for ConnectionStatus
176	cdrouter_upnp_204	Verify router sends UPnP NOTIFY events with updated ExternalIPAddress
177	cdrouter_upnp_210	Verify router stops sending NOTIFY events when subscription expires
178	cdrouter_upnp_220	Verify the maximum number of UPnP event subscriptions that can be created
179	dns_10	Verify DNS proxy does not cache DNS entry when DNS TTL is 0
180	dns_11	Verify DNS proxy returns TTL of 0 when returned DNS TTL is 0
181	dns_40	Verify AAAA IPv6 DNS queries to router are forwarded to real DNS server
182	dns_41	Verify AAAA IPv6 DNS queries can return no address for IPv6 to IPv4 failover
183	dns_50	Verify Reverse DNS queries to router are forwarded to real DNS server
184	dns_51	Verify Reverse AAAA IPv6 DNS queries to router are forwarded to real DNS server
185	dns_60	Verify DNS proxy fails over when new primary DNS server is learned
186	dns_70	Verify DNS lookups with multiple IPv4 responses
187	dns_100	Verify DNS proxy recovers after DNS server outage
188	dns_110	Verify DNS queries including the EDNS0 option
189	dns_120	Verify large DNS responses using EDNS0 option
190	dns_121	Verify maximum UDP payload value in EDNS0 option
191	dns_130	Verify DNS queries for TXT records
192	dns_132	Verify DNS queries for CNAME records
193	dns_133	Verify DNS queries for responses returning both CNAME and A records
194	dns_134	Verify DNS queries for responses returning both CNAME and AAAA records
195	dns_140	Verify DNS queries for SPF records
196	dns_141	Verify DNS queries for SRV records
197	dns_150	Verify DNS proxy does not forward DNS server status requests
198	dns_200	Verify DNS proxy does not mangle DNSSEC queries
199	dns_201	Verify DNS proxy does not mangle large DNSSEC responses
200	dns_210	Verify DHCP server automatically registers DHCP client's hostname in DNS
201	dns_220	Verify DHCP server updates DHCP client's hostname when it changes
202	dns_230	Verify DHCP server supports FQDN hostname values
203	dns_240	Verify DNS proxy removes old DHCP hostname values when hostname changes
204	dns_250	Verify DHCP server handles DHCP hostname option with maximum size DNS subdomain length
205	dns_300	Verify DNS proxy honors TTL values when caching responses
206	dns_400	Verify parallel DNS queries
207	dns_410	Verify DNS does not deploy NXDOMAIN hijacking for type A records
208	dns_411	Verify DNS does not deploy NXDOMAIN hijacking for type AAAA records
209	xbox_2	DNS Test: Verify DNS lookups from LAN client
210	xbox_3	MTU Test: Verify IPv4 MTU of 1364 for Xbox LIVE
211	xbox_4	ICMP Test: Verify ICMP Destination Unreachable message from WAN does not destroy NAT mapping
212	xbox_5	NAT Test: Verify Xbox NAT classification of Open, Moderate, or Strict
213	xbox_6	UPnP Test: Verify UDP wildcard port mapping can be created
214	v4_lan_tcp_connect_info	NMap IPv4 TCP Connect scan
215	v4_lan_tcp_syn_info	NMap IPv4 TCP Syn scan
216	v4_lan_tcp_fin_info	NMap IPv4 TCP Fin scan
217	v4_lan_tcp_null_info	NMap IPv4 TCP Null scan
218	v4_lan_tcp_xmas_info	NMap IPv4 TCP XMAS scan
219	v4_lan_tcp_psh_info	NMap IPv4 TCP PSH scan
220	v4_lan_tcp_urg_info	NMap IPv4 TCP URG scan
221	v4_lan_tcp_finurg_info	NMap IPv4 TCP FIN+URG scan
222	v4_lan_tcp_finpsh_info	NMap IPv4 TCP FIN+PSH scan
223	v4_lan_tcp_maimon_info	NMap IPv4 TCP Maimon scan
224	v4_lan_tcp_ack_info	NMap IPv4 TCP ACK scan
225	v4_lan_udp_info	NMap IPv4 UDP scan
226	v4_lan_sctp_init_info	NMap IPv4 SCTP Init scan
227	v4_lan_sctp_cookie_info	NMap IPv4 SCTP Cookie scan
228	v4_lan_os_detection	NMap IPv4 OS Detection from LAN side of device
229	v4_lan_os_detection_version	NMap IPv4 OS Detection with version detection from LAN side of device
230	v4_wan_tcp_connect_info	NMap IPv4 TCP Connect scan
231	v4_wan_tcp_syn_info	NMap IPv4 TCP Syn scan
232	v4_wan_tcp_fin_info	NMap IPv4 TCP Fin scan
233	v4_wan_tcp_null_info	NMap IPv4 TCP Null scan
234	v4_wan_tcp_xmas_info	NMap IPv4 TCP XMAS scan
235	v4_wan_tcp_psh_info	NMap IPv4 TCP PSH scan
236	v4_wan_tcp_urg_info	NMap IPv4 TCP URG scan
237	v4_wan_tcp_finurg_info	NMap IPv4 TCP FIN+URG scan
238	v4_wan_tcp_finpsh_info	NMap IPv4 TCP FIN+PSH scan
239	v4_wan_tcp_maimon_info	NMap IPv4 TCP Maimon scan
240	v4_wan_tcp_ack_info	NMap IPv4 TCP ACK scan
241	v4_wan_udp_info	NMap IPv4 UDP scan

242	v4_wan_sctp_init_info	NMap IPv4 SCTP Init scan
243	v4_wan_sctp_cookie_info	NMap IPv4 SCTP Cookie scan
244	v4_wan_os_detection	NMap IPv4 OS Detection from WAN side of device
245	v4_wan_os_detection_version	NMap IPv4 OS Detection with version detection from WAN side of device