Government of India
Department of Telecommunications
Telecommunication Engineering Centre
Gate No. 5, Khurshid Lal Bhawan, Janpath, New Delhi-110001.
(IT Division)

File No. 4-1/2022-IT/TEC/MTCTE issues-Part(3) Dated: 05.06.2025

Subject: **Formulation of new Standard for Essential Requirements(ER) of "Carrier Grade NAT (CGNAT) Equipment" - Inviting comments.**

In exercise of the powers conferred by rule 5(1) of the Telecommunications (Framework to Notify Standards, Conformity Assessment and Certification) Rules 2025, a draft new Standard for Essential Requirements (ER) of "Carrier Grade NAT(CGNAT) Equipment" is enclosed herewith (**Annexure-I**) for stakeholder consultation. It is requested to go through the aforesaid enclosed draft Standard and offer your inputs/comments.

2. The comments may please be furnished in the template sheet enclosed herewith as Annexure-II through email to **adic1.tec@gov.in** & **diri.tec@nic.in** at the earliest and latest within **sixty days** please.

Enclosures:
(i) Draft Standard for Essential Requirements (ER) of "Carrier Grade NAT (CGNAT) Equipment" (**Annexure-I**)
(ii) Template/Format sheet for providing comments (**Annexure-II**)

(Jasvir Singh Panesar)
Director (IT), TEC
Email: diri.tec@nic.in

To,

All Manufacturer & Stakeholders

Copy to:
1. Sr DDG TEC
2. AD(IT), TEC - with request for uploading on TEC website/Portal
3. AD(IMP&TEP), TEC - with request for uploading on TBT Enquiry Point

Annexure-I

Draft ER - Carrier Grade NAT (CGNAT) Equipment

Scope: This ER covers all types of CGNAT Equipment

Definition: Any network device that performs large-scale Network Address Translation (NAT), IP address management, and IPv6 transition functions can be tested as per these CGNAT parameters.

1. Variant 1: Carrier Grade NAT Equipment

1.1 Parameters Linked with Product Variant:

S.No.	Parameter Name	Standard Name (Name of Standard RFC/ Functional Test)
1.1.1	Conducted And Radiated Emission - Class A	TEC EMI EMC Standard CISPR 32 EN55032. Annex-B
1.1.2	Immunity to AC Voltage Dips and Short Interruptions	TEC EMI EMC Standard EN/IEC:61000-4-11. Annex-B
1.1.3	Immunity to DC Voltage Dips and Short Interruptions	EN/IEC:61000-4-29. Annex-B
1.1.4	Immunity to Electrostatic Discharge	TEC EMI EMC Standard EN/IEC:61000-4-2. Annex-B
1.1.5	Immunity to Fast Transients (Burst)	TEC EMI EMC Standard EN/IEC:61000-4-4. Annex-B
1.1.6	Immunity to Radiated RF	TEC EMI EMC Standard EN/IEC:61000-4-3. Annex-B
1.1.7	Immunity to RF Field Induced Conducted Disturbance	TEC EMI EMC Standard EN/IEC:61000-4-6. Annex-B
1.1.8	Immunity to Surges	TEC EMI EMC Standard EN/IEC:61000-4-5. Annex-B
1.1.9	IT Equipment Safety	IS 13252-1 or IEC:60950-1 or IEC 62368-1. Annex-A1
1.1.10	IPv4 Parameters Set-D	RFC 791. Annex-P11
1.1.11	IPv6 Parameters	RFC 8200, 4861, 4862, 8201, 4443 Annex-P11
1.1.12	Manageability SNMP V2 or V3	RFC 3416 or RFC 3410. Functional Test No 38 or 39
1.1.13	NAT Functional test	Annex-P11, Functional Test No. 17 & 18
1.1.14	NAT44 Functionality	Functional Test No. 1
1.1.15	Deterministic NAT	Functional Test No. 2

1.1.16	Port Block Allocation	Functional Test No. 3
1.1.17	DS-Lite Functionality	Functional Test No. 4

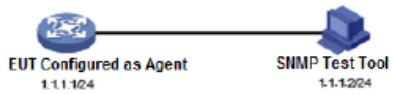
Test No.17

Parameter Name	Test Source NAT with PAT with multiple source ip addresses.
Test instruments required	One Linux client with hping2 tool installed One linux machines
Pre-Test Setup And Test Setup	 1. Install hping2 on Linux Client to initiate traffic from multiple source addresses 2. On Linux server, add route for nat-pool address used in nat configuration on DUT 3. Configure source nat pool on DUT with single IP address 4. Configure source nat rule-set on DUT with 'from' and 'to' and also match condition like 'source-address' and 'destination-address' Note:PAT is enabled by default
Test Case Steps	1. Start sending traffic with hping2 tool from Linux client with first IP to Linux server IP address 2. Again, Initiate hping2 by incrementing the source IP in 'source-ip' field
Expected Results	1. For Step 1, verify that cli output of flow session shows nat-translation. Test considered pass if the source address is natted with the address from the pool specified. 2. Also, check source nat-translation hit count is incrementing in cli output 3. For step 2, Verify that port address translation is seen in cli output of security flow session

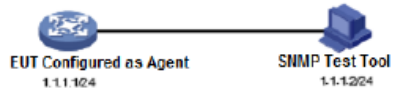
Test No.18

Parameter Name	Test Source NAT NAT64 related feature
Test instruments required	One Linux client One linux server
Pre-Test Setup And Test Setup	 1. To configure NAT64, you need to have a pool of single IPs which will be the IPv4 address of the server. 2. We need a destination NAT configuration to translate the IPv6 address into IPv4 address in the destination field of the incoming packet. 3. The destination address is IPv4, but the source address is IPv6. Thus, we must apply the source NAT in order to change the IPv6 address to IPv4 in the source field of the packet.
Test Case Steps	1. Initiate traffic from Linux client 2. Verify nat translation has worked by checking flow session on DUT
Expected Results	1. Check how the sessions are being established:

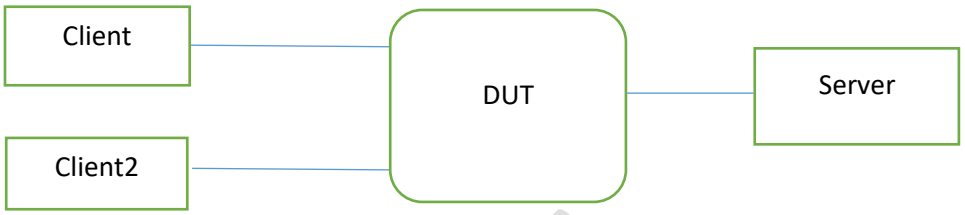
Test No.38

Parameter Name	SNMPv2 Functional Tests
Test Details	Test for management: SNMPv2 (check TRAP, GET and SET operations)
Test instruments required	SNMP Test Tool (SNMP Manager)
Test Setup	
Test Procedure	1. Configure the EUT to run SNMP agent and SNMP Test Tool (NMS) to run SNMP manager application by using correct parameters. 2. Testing of TRAP message: The NMS uses SNMPv2 to manage the SNMP agent, and the agent automatically sends notifications to report events to the NMS. 3. Configure the SNMP agent to send traps to the manager. 4. Use a wrong community name to get the value of a MIB node on the agent. You can see an authentication failure trap on the SNMP manager. 5. Test "SetRequest" operation: SNMP Testing node (SNMP manager) sends SNMPv2c "SetRequest" to set SysName to "EUT1". Verify the SysName value on the EUT. It should match the value "EUT1" set using 'SetRequest' function from the SNMP manger. 6. Test SNMP GET Operation (single Object): Testing node (SNMP Manager) sends SNMPv2c "GetRequest" scalar object to get sysName.0 1.3.6.1.2.1.1.5.0 in system group in MIB II, to Agent. The agent should respond with "SysName value as "EUT1" as set in the previous step, verifying that the EUT support SNMP GET function.
Expected Results	1. TRAP should be sent by EUT (Agent) to Testing Node (SNMP Manager). 2. SetRequest operation should be able to set SysName object in agent (EUT) 3. GetRequest operation should be able to get SysName Object from agent (EUT) 4. Attach screenshots for above successful operations.

Test No.39

Parameter Name	SNMPv3 Functional Tests
Test Details	Test for SNMPv3 management
Test instruments required	SNMP Test Tool (SNMP Manager)
Test Setup	
Test Procedure	1. Configure the agent on EUT and SNMP manager on SNMP Test Tool to use SNMPv3 with security level setting to AuthPriv. Set Authentication to SHA and Privacy (encryption) to DES. 2. The NMS uses SNMPv3 to monitor and manage the agent 3. The agent automatically sends notifications to report events to the NMS. 4. The NMS and the agent perform authentication when they establish an SNMP session. The authentication algorithm is SHA and the authentication key is xxxxxx. The NMS and the agent also encrypt the SNMP packets between them by using the DES algorithm and encryption key yyyyyy
Expected Results	1. Use correct authentication credentials to access the agent. 2. Attach traces for successful encrypted authentication with correct credentials 3. Use incorrect authentication credentials to access the agent 4. Attach traces for failed authentication with incorrect credentials

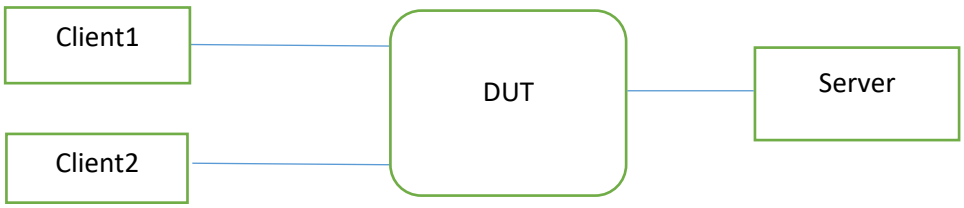
Functional Test No. 1

Parameter Name	NAT44 Functionality	**Requirement**	The CGN equipment should have NAT44 functionality
Objective	Verify NAT44 Functionality		
Topology			

Pre-Test Conditions
1. Power on the DUT. 2. Configure two client networks that connects to DUT 3. Configure Server and connects to DUT egress interface

Test Procedure	**Expected Results**
1. Configure pool-based Source NAT (NAT44) on the DUT with the desired pool of IP addresses. 2. Initiate traffic sessions from Client1 and Client2 to the target server. 3. Verify the NAT mappings created for each session, ensuring source IP addresses are translated as per the configured NAT pool.	1. Ensure the device successfully translates source IPs using the specified NAT pool. 2. Logs from the client side and server side should clearly indicate the original source IPs from the clients. 3. The NAT-translated IPs on the server side should be as per the configured NAT pool.

Functional Test No. 2

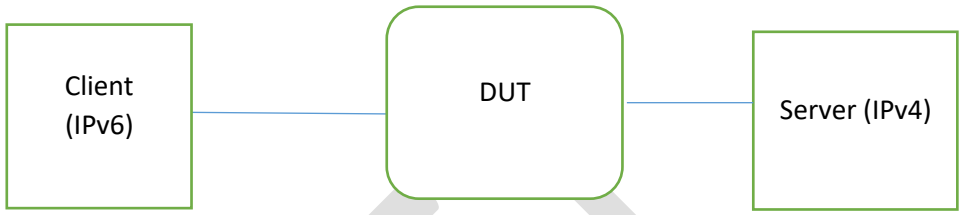
Parameter Name	Deterministic NAT	**Requirement**	The CGN equipment should have Deterministic NAT
Objective	Verify Deterministic NAT Functionality		
Topology			
Pre-Test Conditions			
1. Power on the DUT. 2. Configure two client networks that connects to DUT 3. Configure Server and connects to DUT egress interface			
Test Procedure		**Expected Results**	
1. Assign Client1 and Client2 specific deterministic NAT IP addresses on the DUT. 2. Initiate traffic sessions from Client1 and Client2 to the target Server. 3. Check the NAT mappings for each session. Confirm that the source IP addresses of Client1 and Client2 are translated to their respective NAT IPs. 4. Disable the deterministic NAT mapping for Client2 on the DUT. 5. Verify Client1 traffic is still NATed using its assigned NAT IP. 6. Verify Client2 traffic reaches the server without NAT.		1. Ensure the device successfully translates source IPs using the specified deterministic NAT IP. 2. Logs from the client side and server side should clearly indicate the original source IPs from the clients and the NAT-translated IPs on the server side as per the configured deterministic NAT IP. 3. Ensure after disabling Deterministic NAT for client2 the traffic from client2 should not be NATed.	

Functional Test No. 3

Parameter Name	Port Block Allocation	**Requirement**	The CGN equipment shall have PBA functionality
Objective	Verify Port Block Allocation Functionality in the CGNAT		
Topology			
Pre-Test Conditions			
1. Power on the DUT. 2. Configure two client networks that connect to DUT. 3. Configure Server and connects to DUT egress interface			
Test Procedure		**Expected Results**	
1. Configure NAT on the device. 2. Assign a specific port block(range) to the NAT address. 3. Test the setup by sending different types of traffic, such as HTTP or SSH, from the client to server to verify that the traffic is being		1. Ensure the device successfully translates source IPs using the specified NAT IP. 2. Logs from the client side and server side should clearly indicate: ➢ The original source IPs from the clients. ➢ The NAT-translated IPs on the server	

NATed using the allocated port block(range). 4. Monitor the logs to validate and analyse the NAT functionality	side as per the configured port block(range) with NAT.

Functional Test No. 4

Parameter Name	DS-Lite Functionality	**Requirement**	The CGN equipment should have DS-Lite functionality with logging
Objective	To verify that the DSLite functionality on the DUT		
Topology			

Pre-Test Conditions
1. Configure DUT with CGN configuration. If DUT is with Firewall + CGN then configure security zones and policies 2. Configure Server and connects to DUT egress interface 3. Configure DSLite config – Software Concentrator, source type and pool 3. Configure NTP and security logging.

Test Procedure	**Expected Results**
1. Initiate traffic by sending IPv4 packets encapsulated within IPv6 from the client to server. 2. Verify whether the DUT process the encapsulated packet or not. 3. Check the flow session for the NAT process 4. verify that the NAT mapping is created and the NAT pool is being used appropriately. 4. Stop the traffic and clear NAT mappings at DUT 5. Ensure that logs are generated for the creation and deletion of the NAT mappings	1. Monitor the ingress interface of DUT to ensure that traffic is properly being received 2. As per DS-Lite configuration DUT should process the encapsulated traffic correctly and strip the IPv6 header then extract the IPv4 packet for further processing 3. DS-Lite processed and Flow should be seen 4. The DUT should correctly translate the private IPv4 Address to a public IPv4 Address according to the NAT rule. 5. Flow session created. NAT mapping summary and pool usage should match no of sessions 6.Once traffic is stopped, no NAT mappings or sessions should remain visible in the DUT 7. Logs should be generated for both the creation and deletion of NAT mappings, as well as for any relevant system events.

Interfaces: Inputs may be given for various types interfaces applicable to this Equipment.

ANNEXURE-II

Comments on draft for new Standard for Essential Requirements (ER) of "**Carrier Grade NAT Equipment**"

Name of Manufacturer/Stakeholder:

Organization:

Contact details:

TABLE-A: Inputs/ Comments on the technical test parameters for the Carrier Grade NAT Equipment

Clause No./ Sr. No.	Technical Parameter Name Description	Comments	Justification/ Remarks

TABLE-B: Inputs/ Comments for the Suggested Applicable Interfaces for the Carrier Grade NAT Equipment

Sr. No.	Interface Name