China Telecom GPON Equipment Testing Program (GPON SFU)

China Telecom Corporation Limited

August, 2011

Table of Contents

Test Overview

1 Overview

This test specification was drafted by Shanghai Research Institute of China Telecom Corporation Limited; it was prepared with reference to *Technical Requirement for GPON Equipment of China Telecom V2.0* (No.382 ZGDX (2011) Document).

The test contents of this specification include: ONU PON interface test, PON basic function test, Layer-2 function test, security test, multicast test, ONU Layer-2 function test, OMCI interoperability test, local management and remote management test.

1.1 Equipment profile

1.1.1 OLT

Equipment model		
PON chip		
Shape (diagram)		
Dimension (W/H/D mm)		
Weight		
Power supply		
Power		
Number of Slots		
Control panel (whether support main and standby redundancy)		
Rear panel switching capability		
PON number of ports (single board/entire device)		
Number of uplink interfaces	**10GE**	
	GE (optical/electrical)	
	FE	
	STM-1	
	E1	

1.3.2 Version of the tested equipment

Description		Model	Hardware Version	Software Version	Test Remarks
Network management					
OLT	Main control board				
	PON panel				
	PON chip				
	Uplink board				
	Switching chip				
	Optical module				
	Others				
ONU					
Optical splitter					Indicate manufacturer and type

1.3.3 Networking topology of the testing equipment

Refer to Figure 1 for the topology structure of the testing system of GPON equipment. The configuration of such testing system is mainly used for testing the interoperability, basic function, system performance, and network management function. Such system consists of Optical Line Terminal (OLT), Optical Network Unit (ONU), passive optical splitter, and the supporting instruments and equipment; whereof the Optical Distribution Network (ODN) adopts passive optical network structure of passive optical splitter; a trunk optical fiber connects with several optical fibers, communicates with multiple ONUs, which can share the upstream bandwidth through the passive optical splitter.

dial-up networking, STP and other equipment

- VLAN2 is routing mode, dedicated channel for TR069; the users' application equipment (e.g. PC, STB, and etc.) can't access to internet through this channel.

- VLAN3 is routing mode, dedicated channel for VoIP, users' networking equipment (e.g. PC), IPTV device (e.g. STB) can't access to internet through this channel.

➢ When accessing to the internet, users' networking equipment (e.g. PC) must visit 1FE+1POTS SFU equipment.

The OLT and ONU devices involved into this test can come from different manufacturers.

	accuracy; 6. Adjust the optical attenuator, so that the power value shown by the PON optical power meter reach about -25dBm; repeat Procedure 3 to verify its measurement accuracy; 7. Adjust the optical attenuator, so that the power value shown by the PON optical power meter reach about -30dBm; repeat Procedure 3 to verify its measurement accuracy; 8. Set the low threshold of optical power received by ONU on the network management to be -20dBm; adjust the optical attenuator, gradually increase the attenuation value; when OLT downstream optical power received by ONU is lower than the setting optical power threshold, observe whether the network management shall generate corresponding over-limit alarm. 9. Read the ONU parameters like operating temperature, power supply voltage, bias current and sending optical power through OLT; verify whether ONU supports the measurement of its own optical module parameters.
Expected results	1. In Procedure 2: ONU can support the measurement of the downstream optical power of the OLT.。 2. In Procedures 3~7: within the range of -10dBm~-30dBm, the measurement accuracy of downstream optical power of ONU against OLT is ±2dB. 3. In Procedure 8: ONU supports over-limit alarm when receiving optical power, and the optical power threshold can be set. 4. In Procedure 9: ONU supports the real-time measurement of parameters of its own optical module, like operating temperature, power supply voltage, bias current, sending optical power.
Test instruction	Record the optical module's manufacturer, model and serial number.
Test results	Procedure 3 Procedure 4 Procedure 5 Procedure 6 Procedure 7 Procedure 8 Procedure 9 Optical module's manufacturer, model, and serial number.
Test remarks	

3 PON Basic Function Test

3.1 LOID authentication function test of the ONU

instrument	
Test environment	Refer to Figure 1 for the test configuration
Test procedures	1. Establish test environment according to the test configuration diagram of Figure 1; 2. Disconnect the optical fiber on the ONU interface; 3. Start the LOID authentication function of OLT, and set it to be authenticated according to LOID and password; configure a valid LOID and corresponding password on the EMS/CLI (note that avoid using the same ID saved in ONU currently); 4. After connecting the optical fiber, connect the ONU to OND; 5. Check whether the ONU can be authenticated on the EMS/CLI of the OLT; 6. Disconnect the optical fiber on the ONU interface; 7. Configure the LOID locally on the ONU, its value shall be consistent with LOID configured on EMS/CLI in Procedure 3; check whether the ONU is restarted; 8. Connect the ONU optical fiber, reconnect ONU to the ODN; 9. Check whether the ONU can be authenticated on the EMS/CLI of the OLT; 10. Disconnect the optical fiber on the ONU interface; 11. Configure corresponding password of LOID locally on the ONU, its value shall be consistent with the password configured on the EMS/CLI in Procedure 3; 12. Re-start the ONU, connect the ONU optical fiber, then re-connect the ONU to the ODN; 13. Check whether the ONU can be authenticated on the EMS/CLI of the OLT.
Expected results	1. In Procedure 5, the ONU shall be in the unauthorized state; the failure of authentication is because the LOID doesn't exist. 2. In Procedures 7 and 11, the ONU shall be restarted after the logical ID and password are modified locally. 3. In Procedure 9, the ONU shall be in the unauthorized state, the failure of authentication is because the password is wrong. 4. In Procedure 13, the ONU shall be in the authorized state, and the authentication succeeds. 5. The message exchange traffic and message format of ONU and OLT conform to the requirement of G.984, and the requirement of LOID authentication in the technical requirements of China Telecom GPON equipment.
Test instruction	1. During the test period, the encryption function of FEC function shall be closed.
Test results	
Test remarks	

3.1.3 ONU authentication state recovery test

Test purpose	Verify, after the ONU is restarted, the function of authentication state recovery
Test instrument	Data network analyzer
Test environment	Refer to Figure 1 for test configuration
Test procedures	1. Establish test environment according to the test configuration diagram of Figure 1; 2. Disconnect the optical fiber on the ONU interface; 3. Start the LOID authentication function of OLT, and set it to only authenticate the LOID; configure a valid LOID on the EMS/CLI; 4. Configure the LOID locally on the ONU, its value shall be consistent with LOID configured on EMS/CLI in Procedure 3; check whether the ONU is restarted; 5. Connect the ONU optical fiber, reconnect the ONUE to the ODN; 6. Check whether the ONU can be authenticated on the EMS/CLI of the OLT; 7. Check the authentication state locally on the ONU; 8. Disconnect the optical fiber on the ONU interface; 9. Restart the ONU; 10. Check the authentication state locally on the ONU.
Excepted results	1. In Procedure 6, the ONU is authorized state, the authentication succeeds. 2. In Procedure 7, the authentication state of the ONU shall succeed (0x01). 3. In Procedure 10, the authentication state of the ONU is initial state (0x00). 4. The message exchange traffic and message format of ONU and OLT conform to the requirement of G.984, and the requirement of LOID authentication in the technical requirements of China Telecom GPON equipment.
Test instruction	1. During the test period, the encryption function of FEC function shall be closed.
Test results	
Test Remarks	

3.2 FEC function test

Test purpose	Test whether the system has FEC function and FEC gains.
Test instrument	Data network analyzer

	5. Close the constant-luminescence function, send from the OLT to ONU the Disable_serial_number message with the “disable” option; 6. On the ONU, use the constant-luminescence command to force the ONU to emit light constantly, and read the sending optical power of the ONU from the optical power meter; 7. Close the constant-luminescence function, send from the OLT to ONU the Disable_serial_number message with the “enable” option; 8. On the ONU, use the constant-luminescence command to force the ONU to emit light constantly, and read the sending optical power of the ONU from the optical power meter; 9. Close the constant-luminescence function.
Expected results	
Test instruction	1. The power of ONU’s receiver and transmitter shall be separated, and shall not interfere with each other.
Test results	
Test remarks	

4 ONU Layer-2 Function Test

4.1 VLAN function test of the ONU

Test purpose	Verify the VLAN function on the user side of the ONU
Test instrument	Data network analyzer
Test environment	Refer to Figure 1 for the test system
Test procedures	1. Establish test environment according to the test configuration diagram of Figure 1; 2. Configure OLT as the VLAN transparent transmission mode; VLAN transparent transmission mode: 3. Configure ONU as the VLAN transparent transmission mode. Through analyzing of data network analyzer, send CVLAN＝100 Ethernet service traffic to OLT and ONU respectively. Observe the traffic receiving situation on

	the OLT and ONU ports, as well as the VLAN value; VLAN tagging mode: 4. Reconfigure ONU as the VLAN tag mode (configure 101 to t he VLAN list); through analyzing of the data network analyzer, send VLAN=101 data traffic to OLT, and send untag data traffic to the ONU respectively. Observe the traffic receiving situation on the OLT and ONU ports, as well as the VLAN value; VLAN Trunk mode: 5. Reconfigure the ONU as VLAN Trunk mode, add VLAN102, 103 to the VLAN list; 6. Data network analyzer sends two data traffic to the OLT and ONU respectively, carrying VLAN 102, 103; observe the traffic receiving situation on the OLT and ONU ports, as well as the VLAN value; 7. Data network analyzer sends two data traffic to the OLT and ONU respectively, carrying VLAN 104, 105; observe the traffic receiving situation on the OLT and ONU ports, as well as the VLAN value; 8. Data network analyzer sends one data traffic without VLAN to the OLT and ONU respectively; observe the traffic receiving situation on the OLT and ONU ports, as well as the VLAN value; 9. Test the maximum number of VLAN Trunk supported by the ONU's UNI port; and the maximum number of VLAN Trunk supported by the entire ONU; VLAN 1:1 converting: 10. Configure FE/GE ports on the ONU to perform 1:1 VLAN converting function: Convert 111 into 131, 112 into 132, … convert 110+N into 130+N (N is the maximum number of 1:1 VLAN conversion supported by the FE/GE port on the ONU); 11. Configure data network analyzer to send N pieces of upstream data traffic to the EF/GE ports on the ONU, carrying VLAN is 111~110+N respectively; data network analyzer sends N pieces of downstream data traffic to the OLT, carrying VLAN is 131~130+N respectively; 12. Observe the message captured by the data network analyzer of the EF/GE port on ONU, and upstream port of OLT, and observe its carrying VLAN value; verify ONU's 1:1 VLAN conversing function.

Test results	
Test remarks	

4.2.2 Speed limit test on the ONU upstream/downstream port (service traffic)

Test purpose	Test the upstream and downstream bandwidth speed limit function and granularity of the ONU
Test instrument	Data network analyzer
Test environment	Refer to Figure 1 for the test system
Test procedures	1. Connect according to the test configuration diagram of Figure 1; configuration can refer to the OLT, tested ONU and data network analyzer. 2. Configure the ONU PIR=CIR=100M through the EMS; 3. Configure the upstream and downstream speed limit function of the FE/GE port on the ONU through the EMS; limit the speed of the upstream and downstream of FE/GE port to be 50M; 4. Use data network analyzer to send 80M upstream and downstream bi-directional data traffic respectively; check the Ethernet service traffic received by OLT uplink port and FE/GE port on the ONU; verify the speed limit function of FE/GE port on the ONU;
Expected results	OLT can correctly configure the upstream and downstream limited speed rate of the FE/GE port on the ONU. OLT uplink port only received 50M Ethernet service traffic.
Test instruction	1. Record whether the ONU can support speed limit of upstream or downstream port; whether can support speed limit of service traffic. 2. Record the minimum bandwidth and granularity matched the speed limit of the port.
Test results	
Test remarks	

4.3 Traffic control function of the UNI port on the ONU

Test purpose	Verify, when the upstream traffic is too large, whether the ONU shall send PAUSE traffic flow frame to the user-side switch
Test instrument	Date network analyzer
Test environment	Refer to Figure 1 for the test system
Test procedures	1. Connect the test environment according to Figure 1; 2. Configure the maximum upstream speed (PIR) on the ONU through the EMS to be 20M; 3. Configure the port traffic control of the FE/GE port on the ONU through the EMS; 4. Configure the data network analyzer and send 40M upstream service traffic to the FE/GE port on the ONU; meanwhile in the “Port Setup” of such port of data network analyzer to set such port to be “Flow Control Enabled”; 5. Observe, under the circumstance that the upstream bandwidth is congested, whether the ONU shall start “Pause” traffic control against the FE/GE port; whether data network analyzer receives the “Pause” frame; whether upstream sending speed is reduced to 20M below; whether upstream service has packet loss.
Expected results	1. Support “Pause” traffic control; receive “Pause” frame. 2. The traffic control function of the UNI port on the ONU shall use the managed entity “Physical path termination point Ethernet UNI”.
Test instruction	Record whether the data network analyzer can receive PAUSE frame, and the whether the upstream sending speed is reduced to 20M below.
Test results	
Test remarks	

	3. Both ONU1 and ONU2 enable the IGMP snooping function; both ONU3 and ONU4 enable MLD snooping function. Multicast VLAN that configures service to the FE/GE port on the ONU1 and ONU2 is 4000; the multicast VLAN that configures service to the FE/GE port on the ONU3 and ONU4 is 4001; 4. Data network analyzer sends 2 multicast streams to the OLT; one multicast MAC address is 0x01-00-5e-01-01-01 (the value of target IP that is 224.1.1.1 mapped to the MAC address), correspondingly the multicast VLAN ID=4000; the other multicast MAC address is 0x33-0x33-01-01-01-01 (the value of target IP that is FF1E::0101:0101 mapped the MAC address), correspondingly the multicast VLAN ID=4001; 5. The FE/GE port on the OLT and ONU1/ONU2/ONU3/ONU4 send the data traffic with VLAN ID=3001/3002/3003/3004 respectively; 6. Configure IGMP REPORT message on the ONU1 and ONU2, which shall be marked with unicast VLAN ID=3001 and 3002 respectively; configure MLD REPORT message on the ONU3 and ONU4, which shall be marked with unicast VLAN ID=3003 and 3004 respectively. Data network analyzer sends IGMP REPORT message to the FE/GE port on the ONU1 and ONU2; also sends MLD REPORT message to the FE/GE port on the ONU3 and ONU4; 7. Observe the multicast VLAN received on the FE/GE port of the ONU1, ONU2, ONU3, ONU4; 8. Enable the cross-VLAN multicast function by configuring ONU1 and ONU3 through the EMS;
Expected results	1. In Procedure 7, the multicast VLAN received by the FE/GE port on the ONU1 and ONU2 is 4000; while the multicast VLAN received by the FE/GE port on the ONU3 and ONU4 is 4001. 2. In Procedure 9, the multicast VLAN received by the FE/GE port on the ONU1 is 3001; the multicast VLAN received by the FE2 port on the ONU2 is 4000; the multicast VLAN received by the FE/GE port on the ONU3 is 3003; the multicast VLAN received by the FE2 on the ONU4 is 4001.
Test instruction	

	unicast VLAN ID=3003 and 3004 respectively. Data network analyzer sends IGMP REPORT message to the FE/GE port on the ONU1 and ONU2; also sends MLD REPORT message to the FE/GE port on the ONU3 and ONU4; 7. Observe the multicast VLAN received on the FE/GE port of the ONU1, ONU2, ONU3, ONU4; 8. Configure ONU1 and ONU3 through the EMS, enabling the forced stripping downstream port multicast VLAN function; 9. Observe the multicast VLAN received on the FE/GE port of the ONU1, ONU2, ONU3, ONU4.
Expected results	1. In Procedure 7, the multicast VLAN received by the FE/GE port on the ONU1 and ONU2 is 4000; while the multicast VLAN received by the FE/GE port on the ONU3 and ONU4 is 4001. 2. In Procedure 9, the multicast received by the FE/GE port on the ONU1 is without VLAN; the multicast VLAN received by the FE/GE port on the ONU2 is 4000; the multicast received by the FE/GE port on the ONU3 is without VLAN ; the multicast VLAN received by the FE/GE port on the ONU4 is 4001.
Test instruction	
Test results	
Test remarks	

5.2 Multicast performance verification

5.2.1 Multicast capacity test of the ONU

Test purpose	Test the maximum group number of the multicast frame that the ONU can register and forward;
Test instrument	Data network analyzer
Test environment	Refer to Figure 1 for the test system

Test procedures	1. Connect the tested OLT, tested ONU1 and ONU2, as well as the data network analyzer according to the above Figure; 2. Configure data service through the network management; analyzer sends upstream and downstream data through ONU/OLT; OLT mutually communicates with ONU1 for 20M data traffic; OLT mutually communicates with ONU2 for 900M data traffic, adopting 512Bytes. The upstream and downstream forwarding of the data service is normal; 3. 2 PON port protection of the different PON boards for the OLT PON port and trunk optical fiber redundancy protection test; 4. Enable OLT trunk optical fiber Type A/Type B/Type C/Type D protection switching function through the network management; **Test of coordinating OLT to finish TYPE A/TYPE B protection mode ,** 5. Unplug the operating trunk optical fiber; 6. Check whether the service can be switched to the standby optical fiber automatically; check the situation of the packet loss; and record the service interruption time; 7. The operating optical fiber is forced to switch to the standby optical fiber through the trigging of the network management; record the service interruption time; 8. Unplug the operating distribution optical fiber; check whether the service can be switched to the standby optical fiber; check the situation of the packet loss; and record the service interruption time; 9. Unplug the operating trunk and distribution optical fibers at the same time; check whether the service can be switched to the standby optical fiber; check the situation of the packet loss; and record the service interruption time.
Expected results	
Test instruction	1. Check which protection types are supported by the GPON, record the switching time indicator. 2. Check whether the system is re-registered during the protection switching period. 3. Record whether the traffic size of the bidirectional service traffic between ONU/OLT is relevant to the protection switching time.
Test results	
Test remarks	If the test equipment supports any type of protection switching mode among Type A/B/C/D, then it shall be provided with the test; otherwise, the equipment shall not be equipped with this capacity.

7 RFC2544 Function of the Single ONU

Test purpose	Test 1 ONU, and the throughput, delay, packet loss rate performance
Test instrument	Data network analyzer
Test environment	Refer to Figure 1 for the test system
Test procedures	1. Connect according to the test configuration diagram of Figure 1; test in one-way respectively. 2. When testing RFC2544, turn off the equipment address meter switch (turn off both OLT and ONU). 3. The test uses 7 typical packet size: 64 bytes (in downstream direction, it is 72bytes), 128 bytes, 256 bytes, 512 bytes, 1024 bytes, 1280 bytes, 1514 bytes (in downstream direction, it is 1522 bytes). 4. Set the test time to be 30s. 5. In the upstream direction, the instrument sends untag Ethernet service traffic to the FE/GE port on the ONU; the service traffic on the FE/GE port of the ONU is tagged with CLAN=1001; OLT marks each CVLAN with SVLAN, and CVLAN=SVLAN. 6. In the downstream direction, the instrument sends double-layer tag of the Ethernet service traffic to the uplink port of the OLT; CVLAN=SVLAN; and CVLAN=1001; SVLAN and CVLAN de-tagged service traffic by the OLT and ONU. 7. Use the automated script test of the data network analyzer tot test transmission delay, overload packet loss. Observe whether the VLAN receiving the service traffic on the OLT and ONU conforms to the requirement.
Expected results	
Test instruction	
Test results	
Test remarks	

	that in Proceudre 7. 6. In Procedure 14, MIB upload contains no LOID Authentication ME. 7. The message exchange traffic and message format of ONU and OLT conform to the requirement of G.984, and the requirement of logic identification authentication in the technical requirements of China Telecom GPON equipment.
Test instruction	1. Close the encryption function and FEC function during the test period;
Test results	
Test remarks	

8.2 Capability set query of OLT against ONU

Test purpose	Verify the OLT, in the GPON system, can query the ONU state and type correctly
Test instrument	
Test environment	Refer to Figure 1 for the test system
Test procedures	1. Establish test evnironment accortding to Figure 1; 2. Configure ONU type under multiple state of OLT, such as SFU, HGU, MDU, and etc.; 3. Use OLT to query SFU, and obtain its capability set information ; 4. Use OLT to query HGU, SFU in turn, and obtain their capability set information.
Expected results	1. In Procedure 2, OLT can obtain query result of SFU capability set correctly. Compared with the actual ONU state, ONU type, Ethernet interface type, quantity and other infroamtion are consistent with the query results; 2. In Procedure 3, OLT can obtain query result of the HGU and SFU capability set correctly. Compared with the actual ONU state, HGU and SFU type, and other information are consistent with the query results;
Test Instruction	1. To facilitate the OLT to understand the ONU, increase the ME: ONU capability; such ME is a globally unique ME created locally by the ONU. After the ONU is powered on, the ME shall be created and can only be read.
Test results	
Test remarks	

8.3 ONU performance statistics

Test purpose	Test the Ethernet performance statistics function on the Ethernet port of the ONU
Test instrument	Data network analyzer
Test environment	Refer to Figure 1 for the test configuration
Test procedures	1. Establish test environment accorindg to Figure 1; 2. Configure ONU that can only authenticate the LOID; start ONU power supply, ONU authentication succeeds. The OMCI channel is established and finish the initialization synchronization; 3. Data network analyzer makes the OLT and FE1 port of ONU send upstream and downstream data; data service is normal; 4. Clear the number of GEM port performance statistics of the ONU through the EMS/CLI; 5. Use data network analyzer to send 10000 unicast Ethernet packets in bidirection; observe the performance statistics on the EMS/CLI; check the OMCI message; 6. If the OLT can't conduct statistics against the performance of the ONU port, then analyze the cause of it.
Expected results	1. OLT can count the performance of ONU Ethernet port through the OMIC message; 2. Ethernet performance statistics of Ethernet port shall use managed entity Ethernet frame extended PM, through ONU Get current data action, to query the current statistics value; the statistic value of the previous statistic cycle shall be queried through Get History data.
Test instruction	
Test results	
Test remarks	

8.4 ONU status alarm reporting function

Test purpose	Verify the ONU Ethernet port status alarm reporting function
Test instrument	
Test environment	Refer to Figure 1 for the test configuration

	managed entity ONT-G ONU.
Test instruction	
Test results	
Test remarks	

8.6 ONU software upgrade function

Test purpose	Verify the status alarm reporting function of the ONU Ethernet port
Test instrument	
Test environment	Refer to Figure 1 for the test configuration
Test procedures	1. Establish the test environment according to the Figure 1; 2. Configure ONU that can only authenticate the LOID; start ONU power supply, ONU authentication succeeds. The OMCI channel is established and finish the initialization synchronization 3. Check the version information of the ONU through the EMS/CLI; for instance, VerA, check the OMCI message during the configuration period; 4. Upgrade the version of the ONU through the EMS/CLI, after upgrading to the Ver B; check the OMCI message during the confiiguring period; reocrd the upgrade time; 5. Aftet upgrading, reset and restart the ONU, check whether the version information of the ONU is VerB through the EMS/CLI; 6. If it fails to upgrade, find out the causes through analyzing the format and flow of the OMCI message; 7. Configure at least 8 ONUs for the OLT single PON port; configure 8 ONUs upstream and downstream service channel, the bidirectional service sending is normal; 8. Upgrade the version of 8 ONUs through the OLT; record the upgrade time; after upgrading, reset and restart all ONUs; check whether the version information of the ONU upgrade successfully through the EMS/CLI; 9. Prepare upgrading strategy, for instance, ONU-type-based, date-time-based, ONU-version-information-based; and bind to the OLT PON port;
Expected results	1. ONU version information can be checked through EMS/CLI. 2. ONU version can be upgraded through the EMS/CLI. 3. ONU software upgrade function can be realized through the action of the managed entity Software Image of Start download, Download section, End download, Activate image, Commit image; the specific flow conforms to the status machine described in the managed entity of Software image in the

9 ONU Local Management Function Test

The local management function of the ONU shall be mainly recorded; mainly investigate the local management function provided by the ONU; this specification provides no detailed requirement against it, but only lists the basic framework and the following table.

Test Items	Test Instruction	Test Results
Basic requirements	Check and record whether the ONU supports the following functions: a) ONU local management interface type: Ethernet user interface; b) Whether the local management system adopts Web mode; preferably Chinese interface.	
Configuration management requirements	Verify the ONU supported local configuration function through checking the ONU local management interface; for instance, LOID and password configuration; Record the other local security management functions of the ONU (if the ONU supports them).	
Security management requirements	Verify the ONU supported local configuration function through checking the ONU local management interface; for instance, ONU local management shall provide the security measures against the administrator/operating system through defining the individual access right; the illegal users or users with wrong password is denied to conduct the local operation, maintenance, and management; Record other local security management function of the ONU (if the ONU supports them).	

10 ONU Remote Management Test (Only against 1FE+1POTS SFU)

10.1 Voice service function test

10.1.1 SIP agreement test

10.1.1.1 Voice code test

Test Purpose	Verify the type of the voice code supported by the 1FE+1POTS SFU
Test Instrument	

Test Environment	1. Refer to Figure 2 for the test configuration; 2. 2 sets of 1FE+1POTS SFU are powered on normally; 3. 2 sets of 1FE+1POTS SFU are successfully registered to the soft-switch, and the downstream are connected to the Telephone A and B, respectively.
Test procedures	1. Check the priority codec type of the 1FE+1POTS SFU through ITMS; 2. Use Ethereal packet capture analysis; 3. Telephone A is turned off; call Telephone B, and the latter answer; 4. Use Ethereal to observe the codec type of the call; 5. Remotely modify the highest priority codec for 1FE+1POTS SFUB through the ITMS to be G.711u rate; 6. Telephone A is turned off; call Telephone B, and the latter answer; 7. Use Ethereal to observe the codec type of the call; 8. Modify the highest priority codec for 1FE+1POTS SFUB through the GUI to be G.711a rate; 9. Telephone A is turned off; call Telephone B, and the latter answer; 10. Use Ethereal to observe the codec type of the call; 11. Modify the highest priority codec for 1FE+1POTS SFUB through the GUI to be G.729 OR G.729a; 12. Telephone A is turned off; call Telephone B, and the latter answer Use Ethereal to observe the codec type of the call.
Expected results	1. In Procedures 1, 4; codec type is G.722; 2. In Procedure 7, codec type is G.711u rate; 3. In Procedure 10, codec type is G.711a rate; In Procedure 13, codec type is G.729 or G.729a.
Test instruction	
Test results	
Test remarks	

10.1.1.2 G.711 fax

Test purpose	Verify 1FE+1POTS SFU supported fax transmission and reception of the G.711 code mode
Test instrument	
Test environment	1. Refer to Figure 2 for the test configuration; 2. 2 sets of 1FE+1POTS SFU are powered on normally; 3. 2 sets of 1FE+1POTS SFU are successfully registered to the soft-switch; 2 sets of 1FE+1POTS SFU downstream are connected to the Fax Machine A and B; and 1 set of PSTN Fax Machine C.
Test procedures	1. Remotely turn off T.38 code through ITMS; 1FE+1POTS SFU is set to be G.711 fax; 2. Use Ethereal packet capture analysis; 3. 2 sets of 1FE+1POTS SFU are powered on; and successfully registered; 4. Fax is sent between A and B (high-and-low-speed fax counter, low-speed fax counter, and high-speed fax counter); Fax is sent between A and C (high-and-low-speed fax counter, low-speed fax counter, and high-speed fax counter).
Expected results	1. Fax is sent between A and B successfully; 2. Fax is sent between A and C successfully; Packet capture analysis, SDP required by the re-INVITE establishing the fax channel includes m=audio ***** RTP/AVP 0 and a=Fax.
Test instruction	
Test results	
Test remarks	

10.1.2.2 G.711 fax

Test purpose	Verify 1FE+1POTS SFU supported fax transmission and reception of the G.711 code mode
Test instrument	
Test environment	1. Refer to Figure 2 for the test configuration; 2. 2 sets of 1FE+1POTS SFU are powered on normally; connect to various equipment correctly; 3. 2 sets of 1FE+1POTS SFU downstream are connected to the Fax Machine A and B; 4. 1 set of PSTN Fax Machine C.
Test procedures	1. Remotely turn off T.38 code through ITMS; 1FE+1POTS SFU is set to be G.711 fax; RTP packing time period is set to be 20ms, and the control mode is soft-switch full control; 2. Use Ethereal packet capture analysis; 3. 2 sets of 1FE+1POTS SFU are powered on; and successfully registered; 4. Fax is sent between A and B (high-and-low-speed fax counter, low-speed fax counter, and high-speed fax counter); 5. Fax is sent between A and C (high-and-low-speed fax counter, low-speed fax counter, and high-speed fax counter).
Expected results	1. Fax is sent between A and B successfully; 2. Fax is sent between A and C successfully; 3. Packet capture analysis can be observed through the tester; media stream between the two equipment is faxed in the G.711 code mode..
Test instruction	
Test results	
Test remarks	

10.2 TR-069 remote configuration test (only against 1FE+1POTS SFU)

10.2.1 Service remote configuration test

Test purpose	Test ITMS remotely configuring 1FE+1POTS SFU service
Test instrument	

Test environment	1. Refer to Figure 2 for the test configuration; **2.** 1FE+1POTS SFU remains the state leaving the factory; it is powered on normally.
Test procedures	1. 1FE+1POTS SFU uses Networking Mode I, only start VLAN2 (not typical service is TR069); check enabled situation of the 1FE+1POTS SFU service; 2. ITMS receives service enabled order (enabling the networking service); bind the tested 1FE+1POTS SFU with such order; send service configuration to the 1FE+1POTS SFU; check the enabled situation of the 1FE+1POTS SFU service; 3. ITMS receives service enabled order (increasingly enable VoIP service); bind the tested 1FE+1POTS SFU with such order; send service configuration to the 1FE+1POTS SFU; check the enabled situation of the 1FE+1POTS SFU service; 4. ITMS receives service cancellation order (cancelling the previous VoIP service configuration); bind the tested 1FE+1POTS SFU with such order; send service configuration to the 1FE+1POTS SFU; check the enabled situation of the 1FE+1POTS SFU service; 5. ITMS receives service cancellation order (cancelling the networking or IPTV service); bind the tested 1FE+1POTS SFU with such order; send service configuration to the 1FE+1POTS SFU; check the enabled situation of the 1FE+1POTS SFU service ; check whether ITMS can manage 1FE+1POTS SFU .
Expected results	1. In Procedure 1, 1FE+1POTS SFU is not enabled to access the internet, VoIP service, so it can't access the public internet, or make VoIP call; 2. In Procedure 2, 1FE+1POTS SFU successfully receives the service configuration; it can access the public internet through the LAN port bound to the networking service; but it can't make VoIP call; 3. In Procedure 3, 1FE+1POTS SFU successfully receives the service configuration; it can access the public internet through the LAN port bound to the networking service; but also can make VoIP call; 4. In Procedure 4, 1FE+1POTS SFU successfully receives the service configuration; it can access the public internet through the LAN port bound to the networking service; but it can't make VoIP call; 5. In Procedure 5, 1FE+1POTS SFU successfully receives the service configuration; it can't access the public internet, can't make VoIP call; ITMS can manage the 1FE+1POTS SFU.
Test instruction	
Test results	
Test remarks	

10.2.2 Software remote upgrade test

Test purpose	Test whether 1FE+1POTS SFU can perform the whole software upgrading remotely
Test instrument	
Test environment	1. Refer to Figure 2 for the test configuration; 2. 1FE+1POTS SFU can be powered on normally; use SIP agreement version; 3. Correctly set ITMS connection parameters on the 1FE+1POTS SFU; 4. Set VLAN to be PPPoE dial-up, which can successfully dial-up; and 1FE+1POTS SFU can access to ITMS.
Test procedures	1. Correctly set the upgrading parameters on the ITMS side; issue the entire software upgrading command of the software (upgrading to H.248 version); after the software upgrading, check the 1FE+1POTS SFU software version; check whether the H.248 function is normal; 2. Correctly set the upgrading parameter on the ITMS side; issue the entire software upgrading command; download software through FTP server or HTTP server; 1FE+1POTS SFU shall be powered off and restarted during the downloading period; check whether 1FE+1POTS SFU can re-connect the ITMS after restarting; check whether the H.248 function is normal; 3. Correctly set the upgrading parameters on the ITMS side; issue the entire software upgrading command (upgrading to SIP version); 1FE+1POTS SFU shall be powered off and restarted after the downloading is finished, and the Flash is begun to write for 5s; check whether 1FE+1POTS SFU can re-connect the ITMS after restarting; check whether the H.248 function is normal; 4. Correctly set the upgrading parameters on the ITMS side; issue the entire software upgrading command (upgrading to be SIP version); 1FE+1POTS SFU shall be powered off and restarted after the downloading is finished, and the Flash is begun to write for 10s; check whether 1FE+1POTS SFU can re-connect the ITMS after restarting; check whether the H.248 function is normal; 5. Correctly set the upgrading parameters on the ITMS side; issue the entire software upgrading command (upgrading to be SIP version); check whether the upgrading is successful; check whether 1FE+1POTS SFU can re-connect the ITMS after restarting; and whether the SIP function is normal.

Test procedures	1. 1FE+1POTS SFU only configures 1 strip of TR069; check whether it can register to the OLT; whether it can connect to the ITMS. 2. Connect PC to 1FE+1POTS SFU; input 192.168.1.1, and visit 1FE+1POTS SFU, check whether the 1FE+1POTS SFU login interface has the “equipment registration” button; click it and check whether it pops-up logic ID first-time authentication interface; input correct logic ID information (such as broadband account number and ID number); check whether the user inputting logic ID information is used, and it registered OLT successfully; and check whether the user inputting logic ID information is used, and it can register ITMS successfully; check whether it can correctly receive ITMS service order issuing (for instance, issuing a bridge online service order); check whether the interface display conforms to the regulatory requirements; 3. Repeat Procedure 2; 4. Modify the service sending state to be sending failure through the ITMS (namely, the value ofInternet¬Gateway-Device.X_CT-COM_UserInfo.Result is 2); power off and restart the 1FE+1POTS SFU; input 192.168.1.1; and visit 1FE+1POTS SFU; check whether the 1FE+1POTS SFU login interface has the “equipment registration” button; click it and check whether it can pop-up the logic ID equipment first-time authentication interface; input the correct logic ID (such as the broadband account number and ID number); check whether it can register successfully; whether it can correctly receive the ITMS service order sending (for instance, sending a voice service order); check whether the interface display conforms to the regulatory requirements.
Expected results	1. In Procedure 1, 1FE+1POTS SFU can’t register to the OLT; and can’t connect to the ITMS; 2. In Procedure 2, 1FE+1POTS SFU can pop-up Logic ID equipment first-time authentication interface; can register OLT successfully, and used the user inputting the logic ID information; can register ITMS successfully, and used the user inputting the logic ID information; can receive ITMS sending service order, and the interface conforms to the regulatory requirements; 3. In Procedure 3, 1FE+1POTS SFU can pop-up logic ID equipment first-time authentication interface; and can display the words like “have registered successfully; and needn’t to be registered any more”; 4. In Procedure 4, 1FE+1POTS SFU can pop-up logic ID equipment first-time authentication interface; can register ITMS successfully, and used user inputting logic ID information; can receive ITMS sending service order, interface conforms to regulatory requirements; during the whole process, OLT registration state is kept into “success” (except for the equipment restart required by the order).

Test procedures	1. From binding to the networking WAN connected user port ping www website, capture DNS, APR, ICMP and other packets beside the WAN; analyze which WAN connect is used (judging as per the VLAN ID); 2. Visit the equipment on the ITMS; read the equipment TR069 node parameters; capture DNS packet beside the WAN; analyze which WAN connection is used (judging as per the VLAN ID); 3. Select the WAN connection of the VoIP; perform the ping operation; analyze which WAN connection is used (judging as per the VLAN ID); 4. Use Testcenter or PC (ip is set to be the tested terminal user side ip; ping packet sends arp) to send e users side private internet segment of arp packet on the source ip; capture packet on the LAN side port; and see if such packet can be captured; 5. Use Testcenter or PC (ping packet target ip is e users side private internet segment) to send e users side private internet segment of arp packet on the target ip; capture packet on the LAN side port; and see if such packet can be captured; 6. Configure the public multicast VLAN; set-top box plays iptv and switches the multicast channel, and on-demand channel; capture packet beside the WAN; analyze whether the IGMP message takes the public multicast VLAN channel; analyze whether the multicast data traffic takes public multicast VLAN channel; analyze whether the public multicast has the tested equipment issue the upstream data packet.
Expected results	1. In Procedure 1 , the data, DNS, ARP, ICMP and etc. takes one WAN connection (for instance, the internet); 2. In Procedure 2, the TR069 data takes the TR069 WAN connection; 3. In Procedure 3, all data take the VoIP WAN connection; 4. In Procedure 4, no ARP packet can be captured on the LAN port; 5. In Procedure 5, no ARP packet can be captured on the LAN port; 6. In Procedure 6, IGMP message takes no public multicast VLAN channel; multicast data traffic takes the public multicast VLAN; there are no upstream data packet issued by the equipment in the public multicast VLAN.
Test instruction	
Test results	
Test remarks	

10.4 Restore factory settings test

10.4.1 Locally restore factory settings test

Test purpose	Test whether 1FE+1POTS SFU supports locally restore factory settings function
Test instrument	
Test environment	1. Refer to Figure 2 for the test configuration; 2. 1FE+1POTS SFU is powered on normally; 3. Set correct ITMS connection parameter on the 1FE+1POTS SFU; 4. Connect the 1FE+1POTS SFULAN port with PC Ethernet interface through the direct network cable.
Test procedures	1. Modify non-critical parameter configuration (for instance clock server address, DHCP lease period, and etc.) through ITMS (or Web administration page) , and confirm it is different from the factory default settings; 2. ITMS modifies the password of telecom maintenance account (critical parameters, for instance modify to be testpass_22), relevant remote link maintenance parameters (critical parameters); 3. Modify the following critical parameters through ITMS (or Web administration page), confirm it is different from the factory default settings; ➢ VLAN-related configuration (including VLAN ID, LAN port binding and other settings is modified into 4000) ➢ VoIP-related configuration: VoIP user number, SIP Proxy address, and etc. 4. Save the configuration and restart 1FE+1POTS SFU; login the Web after restarting, confirm that the parameter modification becomes valid; use the restore button of the entire machine to restore the factory default settings of 1FE+1POTS SFU; 5. After 1 min, check whether 1FE+1POTS SFU can reconnect the ITMS; whether the Inform message first-time sends “0 BOOTSTRAP”; 6. Check whether the non-critical parameter configuration restores the factory default settings; check whether the critical parameter configuration is retained; 7. Repeat Procedures 1~6, in Procedure 4, use telecom maintenance account of GUI to restore the factory default settings; 8. Establish all connection in the Networking Mode I through the 1FE+1POTS SFU GUI; use the restore button of the entire machine to restore the factory default settings of 1FE+1POTS SFU; verify whether the networking (or IPTV), VoIP are normal.
Expected results	When restore the factory default settings of 1FE+1POTS SFU, it can reconnect the ITMS; the first-time Inform message sends no “0 BOOTSTRAP”; non-critical parameter configuration restores the factory default settings; critical parameter settings are retained; various implemented service can be used normally.

Test procedures	1. Configure 1 set of 1FE+1POTS SFU that is absent of ACS URL, and has the same environment with the current internet; modify the following remotely restored non-critical parameter configuration through ITMS (Web administration page); and confirm it is different from the factory default settings ➢ Clock service address (e.g. modify into www.123.com) ➢ Establish a connection for non-TR069 ➢ DHCP lease cycle 2. Modify the following critical parameters through ITMS (or Web administration page), and confirm it is different from the factory default settings ➢ Telecom maintenance account password (critical parameter: e.g. testpass_22) ➢ VoIP user number, SIP Proxy address ➢ Relevant remote link maintenance parameters 3. Save configuration and restart 1FE+1POTS SFU; after restarting, confirm that the parameter modification becomes valid through 1FE+1POTS SFU GUI or ITMS; 4. Restore the factory default settings of 1FE+1POTS SFU from the ITMS port; 5. After 1 min, check whether 1FE+1POTS SFU reconnects the ITMS; whether the first-time Inform message issues “0 BOOTSTRAP”; 6. Configure 1 set of 1FE+1POTS SFU that is absent of ACS URL, and has the same environment with the test internet; repeat Procedures 1-5; 7. Check whether the following parameters restore the factory default settings through 1FE+1POTS SFUGUI or ITMS ➢ Clock server address ➢ DHCP lease cycle ➢ Telecom maintenance account password ➢ Connection for non-TR069 (factory default doesn’t exist) ➢ VoIP user number, SIP Proxy address ➢ Relevant remote link maintenance parameters ➢ Equipment authentication state (InternetGatewayDevice. X_CT-COM_ UserInfo.Times, InternetGatewayDevice. X_CT-COM_ UserInfo.Limit, InternetGatewayDevice. X_CT-COM_ UserInfo.Status, InternetGatewayDevice. X_CT-COM_ UserInfo.Result)

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------