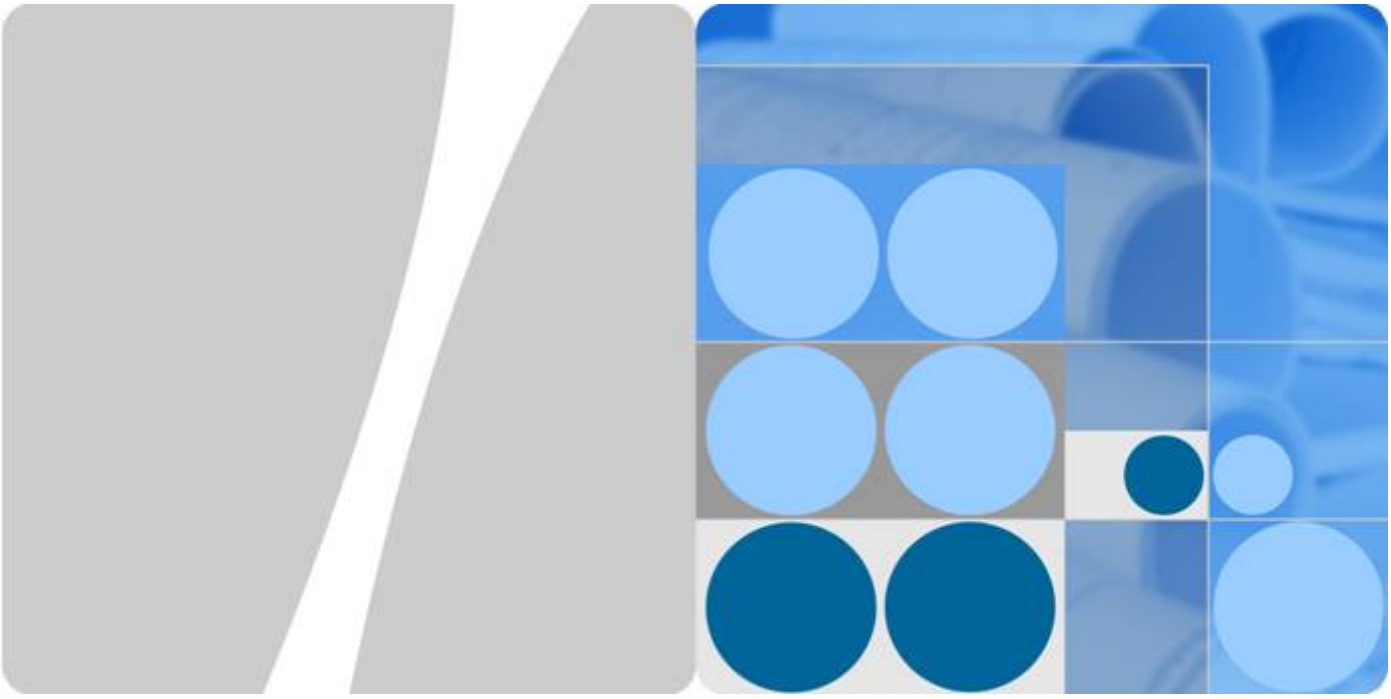


ATN 980B&950C&910C&950B&905 Multi-service Access Equipment

V300R003C10SPC500

Product Description

Issue 01

Date 2018-12-05

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

Contents

1 Product Positioning and Features

About This Chapter

1.1 Product Positioning

The ATN series are case-shaped products used for multi-service access on the edge of metropolitan area networks (MANs). The ATN series together with the CX600 series can be used to build route-based MANs that support end-to-end fixed mobile convergence (FMC) bearing.

To help carriers overcome the resource, cost, and service challenges inherent to the access layer during mobile network evolution, the ATN series adhere to Huawei's "Any Media" concept and provide sustainable IP RAN and enterprise leased line solutions to 2G, 3G, and Long Term Evolution (LTE) applications.

Appearance of the ATN 910C

Figure 1-1 Appearance of the ATN 910C-A

Figure 1-2 Appearance of the ATN 910C-B

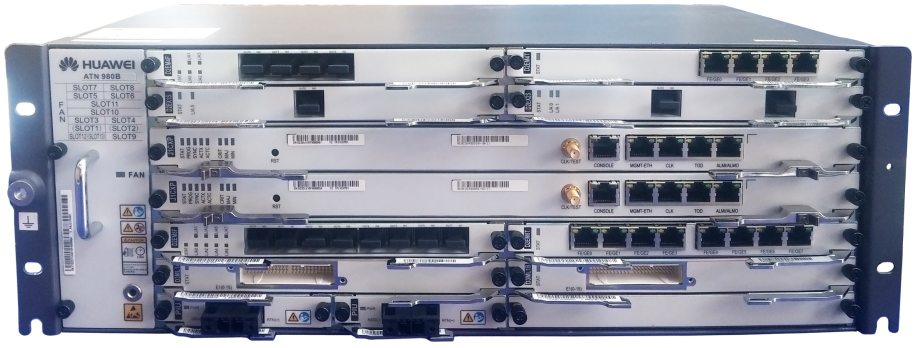
Figure 1-3 Appearance of the ATN 910C-D

Appearance of the ATN 950C

Figure 1-4 Appearance of the ATN 950C that has boards fully configured

Appearance of the ATN 980B

Figure 1-5 Appearance of the ATN 980B that has boards fully configured



Appearance of the ATN 950B

Appearance of the ATN 905

1.2 Product Features

Architecture

The ATN adopts an advanced routing architecture and a uniform platform to receive, transmit, and bear multiple types of services on an all-IP network. This improves network flexibility and transmission efficiency, helps construct reliable carrier-class packet transport networks (PTNs), and reduces the total cost of ownership (TCO).

Interfaces

The ATN provides the following high-density user- and network-side interfaces to meet the deployment requirements of different services and scenarios:

- GE/10GE interfaces

  NOTE

  - Colored optical modules can be installed on GE interfaces. Then the GE interfaces can be connected to the WDM transport network, saving optical fiber resources.
- 50GE FLEXETH interfaces
- 100GE interfaces
- E1 interfaces
- CPOS interfaces

Service Bearing

The ATN provides Layer 2, Layer 3, MPLS, and Layer 2/3 VPN functions to provide flexible and comprehensive bearing solutions for different scenarios, which helps achieve Metro services that are more intelligent. The MPLS function, which is based on MPLS/MPLS-TP standards, adopts a connection-oriented packet switching technology, meeting the requirements for the bearer network evolution to LTE and achieving the best cost-effectiveness.

Reliability

- IP FRR, LDP FRR, TE FRR, and VPN FRR
- TE-tunnel APS
- PW redundancy protection and PW APS

- Bit error-triggered protection switching
- ATN 980B/ATN 950C/ATN 950B/ATN 950C: 1+1 hot backup for CXP boards (functioning as MPUs, SFUs, and clock boards at the same time)
- ATN 980B/ATN 950C/ATN 950B/ATN 950C: non-stop routing (NSR)

QoS

The ATN supports behavior aggregate classification, multi-field classification, and three-level or five-level HQoS, so that flexible, guaranteed, and differentiated services and fine-grained traffic scheduling and traffic shaping can be provided for users.

NOTE

Only the ATN 980B/ATN 950C/ATN 950B/ATN 910Cs support five-level HQoS.

Security

- URPF: used to prevent network attacks based on source IP address spoofing.
- Local attack defense: includes management and control plane protection, attack source tracing, and alarm generation in the event that the discarded packet threshold is crossed.
- Whitelist association at the application layer
- IPSec provides security services for IP packets mainly through encryption and authentication.
- MACsec provides functions such as identity authentication, data encryption, integrity check, and replay protection to ensure the security of Ethernet data frames and prevent devices from processing packets with security threats.

  NOTE

  Only ANKD00CXPA00/ANKD00CXPA01s support MACsec of the ATN 950C.

Maintainability

- A network management system (NMS) with a graphical user interface, which simplifies NE management, improves O&M capabilities, and facilitates network-wide or end-to-end performance monitoring and fault diagnosis.
- Plug-and-play based on DHCP or DCN. The NMS can automatically detect and configure the newly connected devices, which helps to implement remote batch commissioning.
- Directional Forwarding Detection (BFD), Ethernet OAM MPLS OAM and MPLS-TP OAM
- ITU-T Y.1731
- Bandwidth association with microwave devices is supported. Bandwidth association simplifies QoS configurations and requirements on the microwave device, and the complex QoS logic is implemented on the ATN device.
- IP FPM
- ITU-T Y.1564
- Seamless MPLS
- ISSU: When the ATN is configured with two CXP boards, it can be upgraded in ISSU mode.

Synchronization

The Device supports complete clock synchronization solutions to provide precise frequency or time synchronization. The following clock features are used:

NOTE

Different device models or devices equipped with different boards support different clock features. For details, see **7.11 Clock**.

- Physical-layer synchronization, including Ethernet clock synchronization
- E1 clock synchronization
- Network Time Protocol (NTP)
- 1588v2, which meets the LTE network's requirements for clock synchronization
- G8275.1

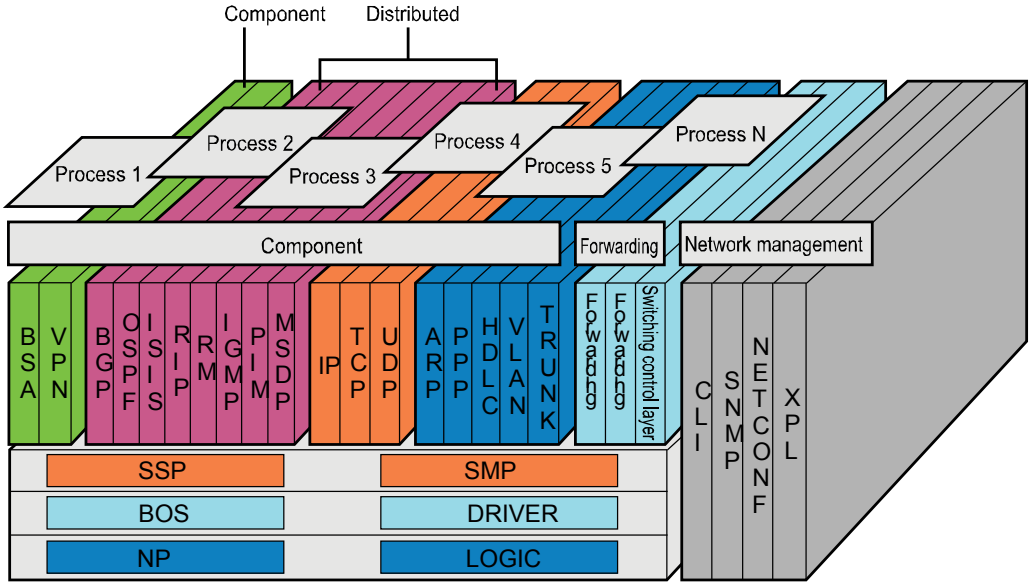
Others

- Energy conservation: Idle interfaces can be manually disabled.

2 Software Architecture

Based on the TCP/IP model, the ATN supports multiple data link layer protocols, network layer protocols, and application layer protocols, as shown in **Figure 2-1**. The ATN provide a multi-process and full-service software architecture that is reliable, scalable, and flexible.

Figure 2-1 Software architecture



- SSP: Service Splitting Platform
- BOS: Balance of System
- SMP:System Management Plane
- NP:Network Processor
- BSA:Basic Service Area

3 Technical Specifications and Environmental Requirements

About This Chapter

3.1 Technical Specifications

Item	ATN 905-F	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 950C	ATN 980B
Dimensions (H x W x D)	43.6 mm x 250 mm x 180 mm (1.72 in. x 9.84 in. x 7.09 in.)	44.45 mm x 442 mm x 220 mm (1.75 in. x 17.40 in. x 8.66 in.)	44.45 mm x 442 mm x 220 mm (1.75 in. x 17.40 in. x 8.66 in.)	44.45 mm x 442 mm x 220 mm (1.75 in. x 17.40 in. x 8.66 in.)	88.90 mm x 442 mm x 220 mm (3.50 in. x 17.40 in. x 8.66 in.)	88.90 mm x 442 mm x 220 mm (3.50 in. x 17.40 in. x 8.66 in.)	155.58 mm x 442 mm x 220 mm (6.12 in. x 17.40 in. x 8.66 in.)
Weight (empty)	N/A	N/A	N/A	N/A	3.5 kg	3.5 kg	• DC: 7.9 kg • AC: 10.3 kg

Item	ATN 905-F	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 950C	ATN 980B
Weight (full configuration)	1.7kg	● DC: 4.8kg ● AC: 5.0kg	● DC: 4.7kg ● AC: 4.9kg	● DC: 4.7kg ● AC: 4.9kg	9.03kg	11.19kg	● ANJ1CXP DC: 18.02 kg ● ANJ2CXP DC: 19.64 kg ● ANJ1CXP AC: 18.74 kg ● ANJ2CXP AC: 19.88 kg
Cabinet installation standard	IMB(3U), ETSI(21-inch), IEC(19-inch)	R01S100 Outdoor Cabinet, ETSI(21-inch), IEC(19-inch)	R01S100 Outdoor Cabinet, ETSI(21-inch), IEC(19-inch)	R01S100 Outdoor Cabinet, ETSI(21-inch), IEC(19-inch)	R01S200 Outdoor Cabinet, ETSI(21-inch), IEC(19-inch)	R01S200 Outdoor Cabinet, ETSI(21-inch), IEC(19-inch)	R01S300A Outdoor Cabinet, ETSI(21-inch), IEC(19-inch)

Item	ATN 905-F	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 950C	ATN 980B
Typical power consumption	● AC: 12.8 W ● DC: 15.3 W	● 2 channel DC System: 81.7w ● 2 channel AC System: 83.8w ● AC +DC system: 82.7w	● 2 channel DC System: 82.8w ● 2 channel AC System: 85.6w ● AC +DC system: 84.2w	● AC +DC system: 80.4w	● 2 channel DC System, with 160G CXP Protection: 115.5 W ● 2 channel DC System, without 160G CXP Protection: 60.3 W	● 2 channel DC System, with 160G CXP Protection: 111W ● 2 channel DC System, without 160G CXP Protection: 57.45 W ● 2 channel DC System, with 360G CXP Protection: 225.5 W ● 2 channel DC System, without 360G CXP Protection:	● ANJ1 CXP DC System with CXP Protection: 182w ● ANJ1 CXP AC System with CXP Protection: 254w ● ANJ2 CXP DC System with CXP Protection: 318.8 w ● ANJ2 CXP AC System with CXP Protection: 384.8 w

Item	ATN 905-F	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 950C	ATN 980B
						114.7 W	

Item	ATN 905-F	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 950C	ATN 980B
Typical heat dissipation	● AC: 41.5BTU/hour ● DC: 49.6BTU/hour	● 2 channel DC System: 265.1 BTU/hour ● 2 channel AC System: 272.0 BTU/hour ● AC+DC system: 268.4 BTU/hour	● 2 channel DC System: 268.6 BTU/hour ● 2 channel AC System: 277.7 BTU/hour ● AC+DC system: 273.1 BTU/hour	● 2 channel DC System: 254.4 BTU/hour ● 2 channel AC System: 267.3 BTU/hour ● AC+DC system: 260.8 BTU/hour	● 2 channel DC System, with 160G CXP Protection: 374.7 BTU/hour ● 2 channel DC System, without 160G CXP Protection: 195.6 BTU/hour	● 2 channel DC System, with 160G CXP Protection: 360.1 BTU/hour ● 2 channel DC System, without 160G CXP Protection: 184.4 BTU/hour ● 2 channel DC System, with 360G CXP Protection: 731.7 BTU/hour ● 2 channel DC System, without 360G	● ANJ1CXP DC: 590.4 BTU/hour ● ANJ1CXP AC: 824.0 BTU/hour ● ANJ2CXP DC: 1034.4BTU/hour ● ANJ2CXP AC: 1248.5BTU/hour

Item	ATN 905-F	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 950C	ATN 980B
						CXP Protection: 372.2 BTU/hour	
DC input voltage	● input voltage range: 19V to 30V or -38.4 V to -72V ● input rated voltage: 24/-48V/-60V	● input voltage range: -38.4 V to -72V ● input rated voltage: -48V/-60V	● input voltage range: -38.4 V to -72V ● input rated voltage: -48V/-60V	● input voltage range: -38.4 V to -72V ● input rated voltage: -48V/-60V	● input voltage range: -38.4 V to -72V ● input rated voltage: -48V/-60V	● input voltage range: -38.4 V to -72V ● input rated voltage: -48V/-60V	● input voltage range: -38.4 V to -72V ● input rated voltage: -48V/-60V
AC input voltage	● input voltage range: 100 to 240V ● input rated voltage: 110V/220V	● input voltage range: 100 to 240V ● input rated voltage: 110V/220V	● input voltage range: 100 to 240V ● input rated voltage: 110V/220V	● input voltage range: 100 to 240V ● input rated voltage: 110V/220V	● input voltage range: N/A ● input rated voltage: N/A	● input voltage range: N/A ● input rated voltage: N/A	● input voltage range: 100 to 240V ● input rated voltage: 110V/220V
MTBF	40 years	40 years	40 years	40 years	40 years	40 years	40 years
MTTR	2 hours	2 hours	2 hours	2 hours	2 hours	2 hours	2 hours
Availability	0.99999	0.99999	0.99999	0.99999	0.99999	0.99999	0.99999

Item	ATN 905-F	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 950C	ATN 980B
Redundant MPUs	-	-	-	-	1+1	1+1	1+1

Item	ATN 905-F	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 950C	ATN 980B
Redundant fans	Natural heat dissipation, no fan	If a single fan fails, the system can still work for a short period of time at an ambient temperature of 50°C.	If a single fan fails, the system can still work for a short period of time at an ambient temperature of 50°C.	If a single fan fails, the system can still work for a short period of time at an ambient temperature of 50°C.	• If a single fan fails, the system can still work for a short period of time at an ambient temperature of 50°C(64G System). • If a single fan fails, the system can still work for a short period of time at an ambient temperature of 40°C(160G System).	If a single fan fails, the system can still work for a short period of time at an ambient temperature of 40°C.	If a single fan fails, the system can still work for a short period of time at an ambient temperature of 40°C.

Item	ATN 905-F	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 950C	ATN 980B
Redundant power supply	N/A	1+1	1+1	1+1	1+1	1+1	1+1

Item	ATN 905-F	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 950C	ATN 980B
Switching capacity	12 Gbit/s (Bidirectional)	272 Gbit/s (Bidirectional)	272 Gbit/s (Bidirectional)	256 Gbit/s (Bidirectional)	● AND 3CXPA: 320 Gbit/s@256 bytes (Bidirectional). The maximum allowed error is 0.01 %. To be specific, 99.99 % of the line rate is guaranteed.	● ANK 1CXPA : 320 Gbit/s@256 bytes (Bidirectional). The maximum allowed error is 0.01 %. To be specific, 99.99 % of the line rate is guaranteed. ● ANK 1CXPB : 320 Gbit/s@256 bytes (Bidirectional). The maximum allowed error is 0.01	● ANJ1CXP : 320 Gbit/s@256 bytes (Bidirectional). The maximum allowed error is 0.01 %. To be specific, 99.99 % of the line rate is guaranteed. ● ANJ2CXP : 720 Gbit/s@256 bytes (Bidirectional). The maximum allowed error is 0.01 %. To be

Item	ATN 905-F	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 950C	ATN 980B
						%. To be specific, 99.99% of the line rate is guaranteed. ● ANK 2CXPB : 720 Gbit/s@256 bytes (Bidirectional). The maximum allowed error is 0.01 %. To be specific, 99.99% of the line rate is guaranteed.	specific, 99.99% of the line rate is guaranteed.

Item	ATN 905-F	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 950C	ATN 980B
Operating temperature	● Long-term: -40°C to 60°C ● Short-term: N/A ● Remark: Restriction on the temperature variation rate: 30 °C /hour	● Long-term: DC:-40°C to 65°C AC:-20°C to 65°C ● Short-term: N/A ● Remark: Restriction on the temperature variation rate: 30 °C /hour	● Long-term: DC:-40°C to 65°C AC:-20°C to 65°C ● Short-term: N/A ● Remark: Restriction on the temperature variation rate: 30 °C /hour	● Long-term: DC:-40°C to 65°C AC:-20°C to 65°C ● Short-term: N/A ● Remark: Restriction on the temperature variation rate: 30 °C /hour	● Long-term: -40°C to 65°C ● Short-term: N/A ● Remark: Restriction on the temperature variation rate: 30 °C /hour	● Long-term: DC:-40°C to 65°C(160G) ● Short-term: N/A ● Remark: Restriction on the temperature variation rate: 30 °C /hour	● Long-term: -40°C to 65°C ● Short-term: N/A ● Remark: Restriction on the temperature variation rate: 30 °C /hour
Storage temperature	-40°C to 70°C	-40°C to 70°C	-40°C to 70°C	-40°C to 70°C	-40°C to 70°C	-40°C to 70°C	-40°C to 70°C
Relative operating humidity	● Long term: 5% to 95% RH, non-condensing ● Short term: N/A	● Long term: 5% to 95% RH, non-condensing ● Short term: N/A	● Long term: 5% to 95% RH, non-condensing ● Short term: N/A	● Long term: 5% to 95% RH, non-condensing ● Short term: N/A	● Long term: 5% to 95% RH, non-condensing ● Short term: N/A	● Long term: 5% to 95% RH, non-condensing ● Short term: N/A	● Long term: 5% to 95% RH, non-condensing ● Short term: N/A

Item	ATN 905-F	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 950C	ATN 980B
Relative storage humidity	5% to 100% RH, non-condensing	5% to 100% RH, non-condensing	5% to 100% RH, non-condensing	5% to 100% RH, non-condensing	5% to 100% RH, non-condensing	5% to 100% RH, non-condensing	5% to 100% RH, non-condensing
Long-term operating altitude	≤ 4000 meters. If the altitude is between 1800 meters and 4000 meters, the operating temperature of the device must decrease by 1°C for every 220 meter increase in altitude.	≤4000 meters. If the altitude is between 1800 meters and 4000 meters, the operating temperature of the device must decrease by 1°C for every 220 meter increase in altitude.	≤ 4000 meters. If the altitude is between 1800 meters and 4000 meters, the operating temperature of the device must decrease by 1°C for every 220 meter increase in altitude.	≤ 4000 meters. If the altitude is between 1800 meters and 4000 meters, the operating temperature of the device must decrease by 1°C for every 220 meter increase in altitude.	≤ 4000 meters. If the altitude is between 1800 meters and 4000 meters, the operating temperature of the device must decrease by 1°C for every 220 meter increase in altitude.	≤ 4000 meters. If the altitude is between 1800 meters and 4000 meters, the operating temperature of the device must decrease by 1°C for every 220 meter increase in altitude.	≤ 4000 meters. If the altitude is between 1800 meters and 4000 meters, the operating temperature of the device must decrease by 1°C for every 220 meter increase in altitude.
Storage altitude	Lower than 5000 meters	Lower than 5000 meters	Lower than 5000 meters	Lower than 5000 meters	Lower than 5000 meters	Lower than 5000 meters	Lower than 5000 meters

NOTE

1. In the physical dimensions shown in the table, the width (W) does not include the rack-mounting ears.
2. Temperature and humidity are measured at 1.5 m (4.92 ft.) above the floor and 0.4 m (1.31 ft.) in front of the cabinet. There should be no protection board on the front or back of the cabinet.
3. "Short-term" refers to continuous working time that does not exceed 96 hours and accumulated working time per year that does not exceed 15 days. If the working time exceeds either of these values, it is considered "long-term".

3.2 Environmental Requirements

Specific Environmental Requirements

- **Storage requirements**

  NOTE

  The storage environment must comply with ETSI EN 300 019-1-1.

  - **Climate requirements**

Item	Description
Temperature	-40ºC to +70ºC (-40ºF to +158ºF)
Relative humidity	5% to 100%
Temperature change rate	≤ 1ºC/min
Atmospheric pressure	70 kPa to 106 kPa
Solar radiation	≤ 1120 W/m^2
Heat radiation	≤ 600 W/m^2

  - **Waterproof requirements**

    For equipment at a customer site, it is recommended that the equipment be stored indoors.

    Ensure that no water accumulates on the floor or drops to the equipment packaging. Keep the equipment away from places where water is apt to leak, such as the places near automatic fire-fighting facilities and heating facilities.

    If the equipment has to be stored outdoors, ensure that:

    - The packaging is intact.
    - Rainproof measures are taken to prevent water from entering the packaging.
    - No water accumulates under the packaging.
    - The packaging is not exposed to sunlight.

  - **Biological environment requirements**
    - Ensure that the location where the equipment is stored is free from microbial infestation.
    - There are no rodents, such as mice.
  - **Air cleanness requirements**
    - The air is free from explosive, electric-conductive, magnetic-conductive, or corrosive dust.
    - The concentrations of mechanically active substances meet the requirements defined in the following table.

Mechanically Active Substance	Concentration
Suspended dust	≤ 5.00 mg/m^3
Deposited dust	≤ 20.0 mg/(m^2·h)
Gravel	≤ 300 mg/m^3

- The concentrations of chemically active substances meet the requirements defined in the following table.

Chemically Active Substance	Monthly Average Concentration
SO_2	≤ 0.30 mg/m^3
H_2S	≤ 0.10 mg/m^3
NO_2	≤ 0.50 mg/m^3
HF	≤ 0.01 mg/m^3
NH_3	≤ 1.00 mg/m^3
Cl_2	≤ 0.10 mg/m^3
HCl	≤ 0.10 mg/m^3
O_3	≤ 0.05 mg/m^3

- **Mechanical stress requirements**

Item	Subitem	Range
Random vibration	Acceleration	0.02 m^2/s^3
	Frequency	● 5 Hz to 10 Hz ● 10 Hz to 50 Hz ● 50 Hz to 100 Hz
	dB/oct	-12 to +12

- **Transportation environment requirements**

  NOTE

  The transportation environment must comply with ETSI EN 300 019-1-2.

  - **Climate requirements**

Item	Description
Temperature	-40ºC to +70ºC (-40ºF to +158ºF)
Relative humidity	5% to 95%
Temperature change rate	≤ 1ºC/min
Atmospheric pressure	70 kPa to 106 kPa
Solar radiation	≤ 1120 W/m^2
Heat radiation	≤ 600 W/m^2

- **Waterproof requirements**
  - The equipment packaging is intact.
  - Rainproof measures are taken for the transportation tools to prevent water from entering the packaging.
  - No water accumulates in the transportation tools.
- **Biological environment requirements**
  - Ensure that the location where the equipment is placed is free from microbial infestation.
  - There are no rodents, such as mice.
- **Air cleanness requirements**
  - The air is free from explosive, electric-conductive, magnetic-conductive, or corrosive dust.
  - The concentrations of mechanically active substances meet the requirements defined in the following table.

Mechanically Active Substance	Concentration
Deposited dust	≤ 3.0 mg/(m^2·h)
Gravel	≤ 100 mg/m^3

  - The concentrations of chemically active substances meet the requirements defined in the following table.

Chemically Active Substance	Monthly Average Concentration
SO_2	≤ 1.00 mg/m^3
H_2S	≤ 0.50 mg/m^3

Chemically Active Substance	Monthly Average Concentration
NO_2	≤ 1.00 mg/m^3
HF	≤ 0.03 mg/m^3
NH_3	≤ 3.00 mg/m^3
HCl	≤ 0.50 mg/m^3
O_3	≤ 0.10 mg/m^3

- **Mechanical stress requirements**

Item	Subitem	Range
Random vibration	Acceleration	1 m^2/s^3
	Frequency	● 5 Hz to 20 Hz ● 20 Hz to 200 Hz
	dB/oct	-3
Collision	Shock response spectrum I (sample weight > 50 kg)	100 m/s^2, 11 ms, 100 times on each side
	Shock response spectrum II (sample weight ≤ 50 kg)	180 m/s^2, 6 ms, 100 times on each side
NOTE Shock response spectrum is a curve of the maximum acceleration responses generated by the equipment under specified impact excitation.		

- **Operating environment requirements**

  NOTE

  The operating environment must comply with ETSI EN 300 019-1-3.

  - **Climate requirements**

Item	Temperature	Relative humidity
ATN 910C	DC: -40ºC to +65ºC (-40ºF to +149ºF) AC: -20ºC to +65ºC (-4ºF to +149ºF)	5% to +95%
ATN 905	-40ºC to +60ºC (-40ºF to +140ºF)	5% to +95%

Item	Temperature	Relative humidity
ATN 950C	-40ºC to +65ºC (-40ºF to +149ºF)	5% to +95%
ATN 950B	-40ºC to +65ºC (-40ºF to +149ºF)	5% to +95%
ATN 980B	-40ºC to +65ºC (-40ºF to +149ºF)	5% to +95%
NOTE ● If the equipment is installed in a cabinet, the impact of radiation can be ignored. If the equipment is installed outdoors, proper protection must be provided for the equipment against radiation. ● The temperature and relative humidity are measured at the place 1.5 m (4.92 ft) above the floor and 0.4 m (1.31 ft) away from the front side of a cabinet without any front or rear protection panel.		

To improve product application reliability, it is recommended that a dedicated precision air conditioner be installed in an equipment room and the temperature and relative humidity be controlled within the following ranges:

- Temperature range: 15ºC to 30ºC (59ºF to 86ºF)
- Relative humidity range: 40% to 75%

NOTE

Do not install the air conditioner above the equipment and ensure that the air exhaust vent of the air conditioner does not face the equipment. Keep the air conditioner away from a window as far as possible to ensure that no moisture from the window is blown towards the equipment through the air conditioner.

Item	Description
Altitude	≤ 4000 m (13123.2 ft) (When the altitude is lower than 1800 m (5905.44 ft), the equipment operates normally. When the altitude is within the range from 1800 m to 4000 m (from 3280.8 ft to 13123.2 ft), the actual equipment operating temperature decreases by 1ºC (1.8ºF) for every 220 m (721.78 ft) increase in altitude.)
Temperature change rate	≤ 0.5ºC/min
Wind speed	≤ 5 m/s
Solar radiation	≤ 700 W/m^2
Heat radiation	≤ 600 W/m^2

- **Biological environment requirements**
  - Ensure that the location where the equipment is installed is free from microbial infestation.

- There are no rodents, such as mice.

– **Air cleanness requirements**

- The air is free from explosive, electric-conductive, magnetic-conductive, or corrosive dust.
- The concentrations of mechanically active substances meet the requirements defined in the following table.

Mechanically Active Substance	Concentration
Suspended dust	≤ 0.4 mg/m^3
Deposited dust	≤ 15 mg/(m^2·h)
Gravel	≤ 300 mg/m^3

- The concentrations of chemically active substances meet the requirements defined in the following table.

Chemically Active Substance	Monthly Average Concentration
SO_2	≤ 0.30 mg/m^3
H_2S	≤ 0.10 mg/m^3
NO_2	≤ 0.50 mg/m^3
HF	≤ 0.01 mg/m^3
NH_3	≤ 1.00 mg/m^3
Cl_2	≤ 0.10 mg/m^3
HCl	≤ 0.10 mg/m^3
O_3	≤ 0.05 mg/m^3

– **Mechanical stress requirements**

Item	Subitem	Range
Sinusoidal vibration	Velocity	≤ 5 mm/s
	Acceleration	≤ 2 m/s^2
	Frequency	● 5 Hz to 62 Hz ● 62 Hz to 200 Hz

Item	Subitem	Range
Collision	Shock response spectrum II	Half-sine wave, 30 m/s^2, 11 ms, 3 times on each side
	Static payload	0 kPa

NOTE

Shock response spectrum is a curve of the maximum acceleration responses generated by the equipment under specified impact excitation.

Static payload refers to the capability of the equipment in package to bear the pressure from the top in normal pile-up method.

4 Product Compatibility

The supported items of boards list in the Table 4-1 ("●" indicates supported items, "-" indicates unsupported items).

Table 4-1 Mapping products and versions

BOM	Module	Description	ATN 950C	ATN 980B	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 905-F
03031YJS	ANKD00CXPA00	System Control,Cross-connect and Multi-protocol Process Unit A	●	-	-	-	-	-	-
03032VCY	ANKD00CXPB02	System Control, Cross-connect and Multi-protocol Process Unit with 160G	●	-	-	-	-	-	-

BOM	Module	Description	ATN 950C	ATN 980B	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 905-F
03032UWQ	ANKD00CXPB01	System Control,Cross-connect and Multi-protocol Process Unit with 360G	●	-	-	-	-	-	-
03056920	ANJD00CXPA01	System Control,Cross-connect and Multi-protocol Process Unit	-	●	-	-	-	-	-
03057826	ANJ0002CXP00	System Control,Cross-connect and Multi-protocol Process Unit with 360G	-	●	-	-	-	-	-

BOM	Module	Description	ATN 950C	ATN 980B	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 905-F
03058118	ANDD03CXPA00	System Control, Cross-connect and Multi-protocol Process Unit	-	-	-	-	-	●	-
03057361	ANKD00EX4S00	4 Channels 10GE Optical Interface Board(SFP+)	●	●	-	-	-	-	-
03057134	ANKD00EX2S00	2 Channel 10GE Optical Interface Board(SFP+)	●	●	-	-	-	-	-
03056113	ANDD000EX1S0	1 Channel 10GE Optical Interface Board(SFP+)	●	●	-	-	-	●	-

BOM	Module	Description	ATN 950C	ATN 980B	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 905-F
03057018	LNDD01XE8F00	1 Channel 10GE Optical(SFP+) and 8 Channels GE/FE Optical Interface Board	●	●	-	-	-	●	-
03057467	ANKD0EM20F00	20 Channels GE BIDI(CSFP)/10 Channels GE(SFP) Optical Interface Board	●	●	-	-	-	-	-
03056114	ANDD00EM8F01	8 Channels GE/FE Optical Interface Board	●	●	-	-	-	●	-

BOM	Module	Description	ATN 950C	ATN 980B	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 905-F
03056115	ANDD00EM4F01	4 Channels GE/FE Optical Interface Board	●	●	-	-	-	●	-
03054570	ANDD00CQ1B00	4 Channels Channelized OC-3c/STM-1c POS Optical Interface Board	●	●	-	-	-	●	-
03056116	ANDD00EM8T01	8 Channels GE/FE Electrical Interface Board	●	●	-	-	-	●	-
03056117	ANDD00EM4T01	4 Channels GE/FE Electrical Interface Board	●	●	-	-	-	●	-

BOM	Module	Description	ATN 950C	ATN 980B	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 905-F
03054388	ANDD32E17502	32 Channels E1 Interface Board(75ohm)	●	●	-	-	-	●	-
03054389	ANDD32E11202	32 Channels E1 Interface Board(120ohm)	●	●	-	-	-	●	-
03054386	ANDD16E17502	16 Channels E1 Interface Board(75ohm)	●	●	-	-	-	●	-
03054387	ANDD16E11202	16 Channels E1 Interface Board(120ohm)	●	●	-	-	-	●	-
03030RJQ	CR5D08CWDM70	8-Channel Multiplexing & Demultiplexing Card	●	●	-	-	-	-	-

BOM	Module	Description	ATN 950C	ATN 980B	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 905-F
03057706	ANKD001EV200	2 Port 50GBase QSFP28 High Speed Interface Card	●	●	-	-	-	-	-
03056112	ANDD00EM8M00	4 Channels GE/FE Optical Interface and 4 Channels GE/FE Electric Interface Board	●	●	-	-	-	●	-
03054283	ANDD000EX100	1 Channel 10GE Optical Interface board	●	●	-	-	-	●	-

BOM	Module	Description	ATN 950C	ATN 980B	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 905-F
03054282	AND D00EM8F00	8 Channels GE/FE Optical Interface Board	●	●	-	-	-	●	-
03054280	AND D00EM8T00	8 Channels GE/FE Electric Interface Board	●	●	-	-	-	●	-
03054292	AND D00EM4F00	4 Channels GE/FE Optical Interface Board	●	●	-	-	-	●	-
03054281	AND D00EM4T00	4 Channels GE/FE Electric Interface Board	●	●	-	-	-	●	-

BOM	Module	Description	ATN 950C	ATN 980B	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 905-F
03056111	ANDD000EX2S0	2 Channels 10GE Optical Interface Board(SFP+)	-	-	-	-	-	●	-
03057838	ANKD01EXAS00	10 Channels 10GE Optical Interface Board(SFP+)	●	●	-	-	-	-	-
03057839	ANKD001EH100	1 Channel 100GE Optical Interface Board(CFP2)	●	●	-	-	-	-	-
03058102	ANKD001EV100	1 Channel 50GBase QSFP28 High Speed Interface Board	●	●	-	-	-	●	-

BOM	Module	Description	ATN 950C	ATN 980B	ATN 910C-A	ATN 910C-B	ATN 910C-D	ATN 950B	ATN 905-F
03032VBG	CR5D00E4XF20	4-Port 10GBase-SFP+MACsec Interface Card	●	-	-	-	-	-	-

5 Boards

About This Chapter

NOTE

The ATN 910C/ATN 905 is case-shaped devices with fixed boards configured, and they do not have pluggable boards.

5.1 ATN 950C Boards

5.1.1 Control Board

The control board (CXP) implements service scheduling, system control, and system clock processing, and provides auxiliary interfaces.

ATN 950Cs support the following control boards, which mainly differ in the line rate and memory capacity:

- For details about parameters of the ANKD00CXPA00, see System Control,Cross-connect and Multi-protocol Process Unit A.
- For details about parameters of the ANKD00CXPA01, see System Control, Cross-connect and Multi-protocol Process Unit with 160G.
- For details about parameters of the ANKD00CXPB00, see System Control,Cross-connect and Multi-protocol Process Unit with 360G.

5.1.2 Ethernet Service Interface Board

The device supports multiple types of Ethernet interface boards to address requirements for various interface quantities, interface rates, and interface types (optical/electrical). Ethernet service interface boards are widely used in various network environments. They can accept base station services on the user side, and transmit services upstream on the network side. The

Ethernet service interface board supports Layer 2 services, Layer 3 services, and hybrid transmission of Layer 2 and Layer 3 services. (When the main interface is in Layer 2 mode, configure the sub-interface to transmit Layer 2/Layer 3 services.)

Different Ethernet service interface boards provide the same service functions, but mainly differ from each other in terms of the number of interfaces and interface type. For details about parameters of interface boards, see Interface Board in *Hardware Description*.

- FE/GE electrical interfaces can work at the rates of 10 Mbit/s, 100 Mbit/s, and 1000 Mbit/s.
- FE/GE SFP interfaces support GE optical modules, GE electrical modules, and FE optical modules.
- 10GE interfaces support XFP/SFP+ optical modules.
- 100GE CFP interfaces support 100GE optical modules.

  NOTE

  100GE CFP interfaces support 100GE optical modules only on the ANKD00CXPB00 of the ATN 950C.
- 50G interfaces support QSFP28 optical modules (the first port of a two–port 50GBase QSFP28 optical module supports the 100G QSPF28 optical module).

5.1.3 E1 Service Interface Board

The E1 service interface board supports PPP, and TDM link-layer protocols.

PPP

Figure 5-1 and **Figure 5-2** show the application of the E1 service interface board using the PPP protocol.

Figure 5-1 Application of the E1 service interface board using the PPP protocol (user side)

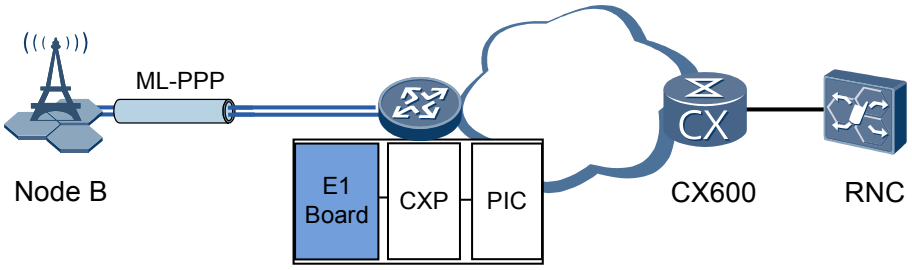
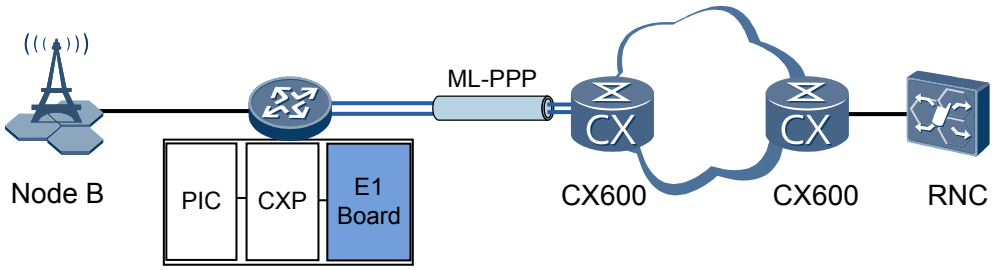


Figure 5-2 Application of the E1 service interface board using the PPP protocol (network side)



The device uses the E1 service interface board to support IP/MPLS services carried over ML-PPPs on both user side and network side.

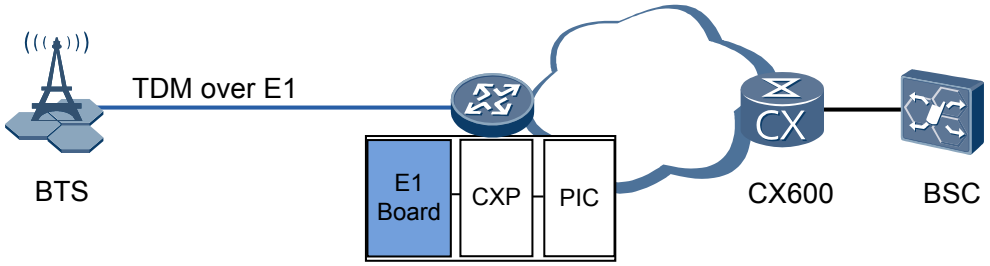
NOTE

An independent PPP link cannot carry service. PPP links must be added to an ML-PPP group to carry services.

TDM

Figure 5-3 shows the application of the E1 service interface board using the TDM protocol.

Figure 5-3 Application of the E1 service interface board using the TDM protocol



The device uses the E1 service interface board to access the TDM service, encapsulate the service signals into packets, and transparently transmit the packets through PWs over the PSN network. This achieves CES service emulation.

For details about parameters of the E1 interface board, see Interface Board in *Hardware Description*.

5.1.4 STM-1 Service Interface Board

Figure 5-4 and Figure 5-5 show the applications of STM-1 service interface boards on a network.

Figure 5-4 Application of the STM-1 service interface board (user side)

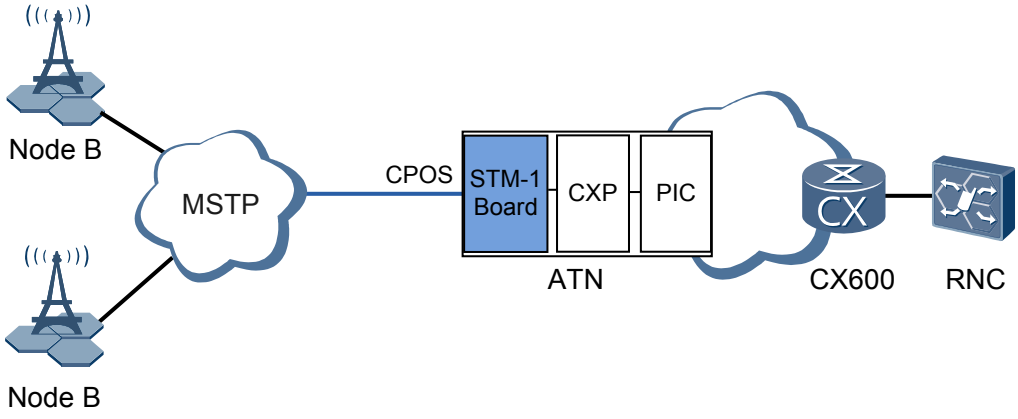
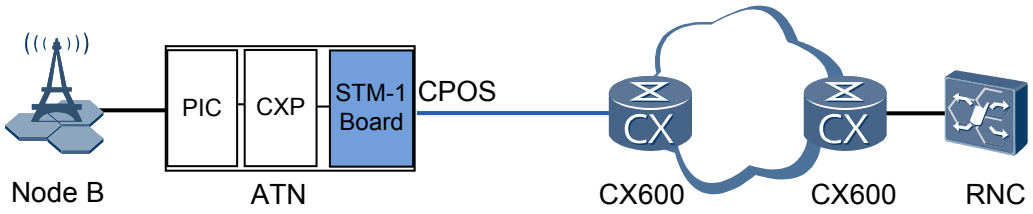


Figure 5-5 Application of the STM-1 service interface board (network side)



The AND2CQ1B interface board on the ATN supports STM-1 services and provides four CPOS interfaces. The CPOS physical interfaces are no longer used as service interfaces, but the channelized 63 E1 channels are used as synchronization serial interfaces that support the same services as the E1 service interface boards.

- The AND2CQ1B board can be used on the user or network side. It supports ML-PPP and carries IP services over E1 channels on CPOS interfaces.
- The AND2CQ1B board on the user side can access and converge TDM services over E1 channels on CPOS interfaces. It implements service emulation and transparent transmission over a packet switched network, achieving TDM PWE3 (CES) services.

The AND2CQ1B can use the APS protocol when services are accessed. When APS protection is used, the supported link layer protocol can only be TDM.

NOTE

Services supported by the E1 channel on the CPOS interface are basically the same as those provided by the E1 service interface board. The differences are listed as follows:

- The E1 channel of the AND2CQ1B supports IP and MPLS services carried over ML-PPPs; the E1 service interface board only supports IP services.
- The E1 channel of the AND2CQ1B does not support fractional E1; the E1 service interface board supports fractional E1 when the TDM protocol is used.

5.2 ATN 980B Boards

5.2.1 Control Board

The control board (CXP) implements service scheduling, system control, and system clock processing, and provides auxiliary interfaces.

Currently, the ATN 980B supports the ANJD00CXPA01 and ANJ0002CXP00 control boards. The two control boards mainly differ from each other in terms of line-rate forwarding capability and memory size.

- For details about parameters of the ANJD00CXPA01, see System Control,Cross-connect and Multi-protocol Process Unit.
- For details about parameters of the ANJ0002CXP00, see System Control,Cross-connect and Multi-protocol Process Unit with 360G.

5.2.2 Ethernet Service Interface Board

The device supports multiple types of Ethernet interface boards to address requirements for various interface quantities, interface rates, and interface types (optical/electrical). Ethernet

service interface boards are widely used in various network environments. They can accept base station services on the user side, and transmit services upstream on the network side. The Ethernet service interface board supports Layer 2 services, Layer 3 services, and hybrid transmission of Layer 2 and Layer 3 services. (When the main interface is in Layer 2 mode, configure the sub-interface to transmit Layer 2/Layer 3 services.)

Different Ethernet service interface boards provide the same service functions, but mainly differ from each other in terms of the number of interfaces and interface type. For details about parameters of interface boards, see Interface Board in *Hardware Description*.

- FE/GE electrical interfaces can work at the rates of 10 Mbit/s, 100 Mbit/s, and 1000 Mbit/s.
- FE/GE SFP interfaces support GE optical modules, GE electrical modules, and FE optical modules.
- 10GE interfaces support XFP/SFP+ optical modules.
- 100GE CFP interfaces support 100GE optical modules.

  NOTE

  100GE CFP interfaces support 100GE optical modules only on the ANJ0002CXP00.
- 50G interfaces support QSFP28 optical modules (the first port of a two–port 50GBase QSFP28 optical module supports the 100G QSPF28 optical module).

5.2.3 E1 Service Interface Board

The E1 service interface board supports PPP, and TDM link-layer protocols.

PPP

Figure 5-6 and Figure 5-7 show the application of the E1 service interface board using the PPP protocol.

Figure 5-6 Application of the E1 service interface board using the PPP protocol (user side)

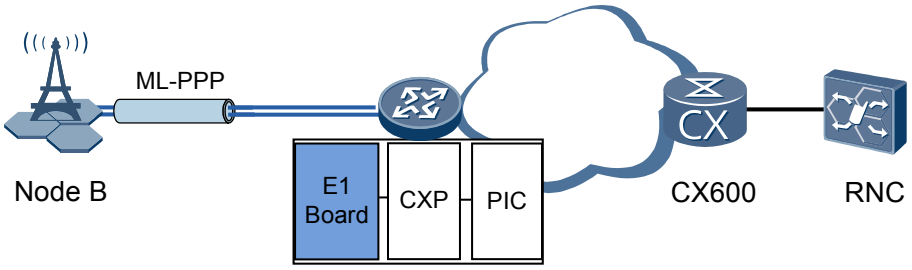
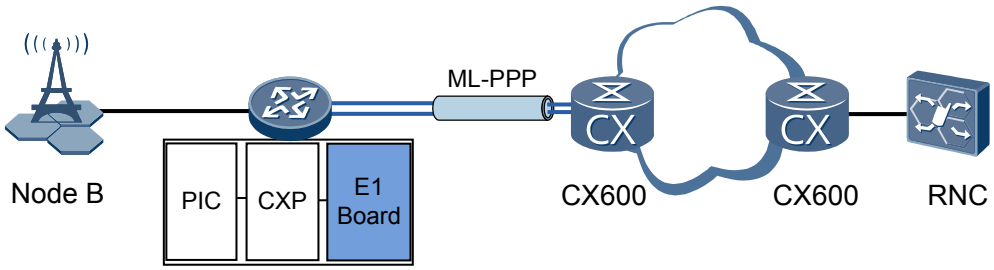


Figure 5-7 Application of the E1 service interface board using the PPP protocol (network side)



The device uses the E1 service interface board to support IP/MPLS services carried over ML-PPPs on both user side and network side.

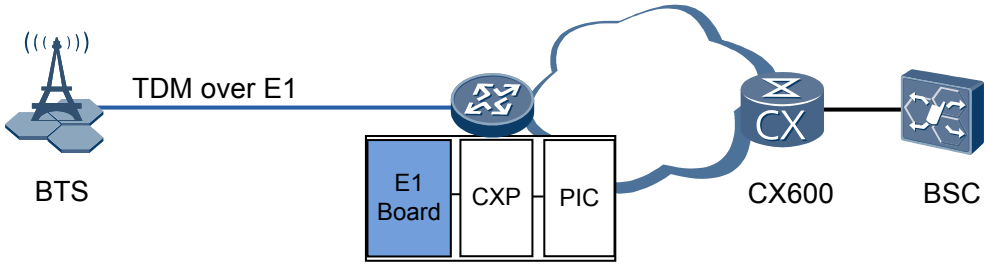
NOTE

An independent PPP link cannot carry service. PPP links must be added to an ML-PPP group to carry services.

TDM

Figure 5-8 shows the application of the E1 service interface board using the TDM protocol.

Figure 5-8 Application of the E1 service interface board using the TDM protocol



The device uses the E1 service interface board to access the TDM service, encapsulate the service signals into packets, and transparently transmit the packets through PWs over the PSN network. This achieves CES service emulation.

For details about parameters of the E1 interface board, see Interface Board in *Hardware Description*.

5.2.4 STM-1 Service Interface Board

Figure 5-9 and Figure 5-10 show the applications of STM-1 service interface boards on a network.

Figure 5-9 Application of the STM-1 service interface board (user side)

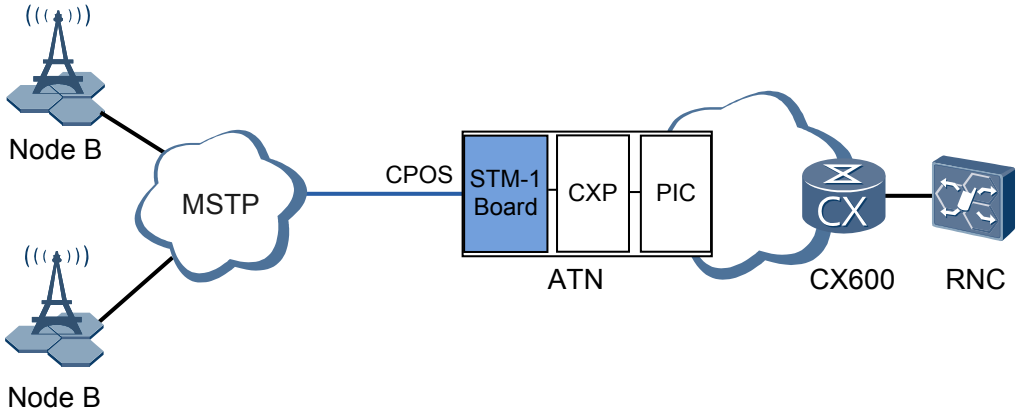
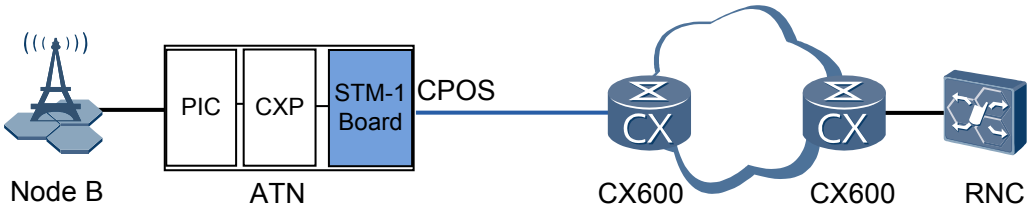


Figure 5-10 Application of the STM-1 service interface board (network side)



The AND2CQ1B interface board on the ATN supports STM-1 services and provides four CPOS interfaces. The CPOS physical interfaces are no longer used as service interfaces, but the channelized 63 E1 channels are used as synchronization serial interfaces that support the same services as the E1 service interface boards.

- The AND2CQ1B board can be used on the user or network side. It supports ML-PPP and carries IP services over E1 channels on CPOS interfaces.
- The AND2CQ1B board on the user side can access and converge TDM services over E1 channels on CPOS interfaces. It implements service emulation and transparent transmission over a packet switched network, achieving TDM PWE3 (CES) services.

The AND2CQ1B can use the APS protocol when services are accessed. When APS protection is used, the supported link layer protocol can only be TDM.

NOTE

Services supported by the E1 channel on the CPOS interface are basically the same as those provided by the E1 service interface board. The differences are listed as follows:

- The E1 channel of the AND2CQ1B supports IP and MPLS services carried over ML-PPPs; the E1 service interface board only supports IP services.
- The E1 channel of the AND2CQ1B does not support fractional E1; the E1 service interface board supports fractional E1 when the TDM protocol is used.

5.3 ATN 950B Boards

5.3.1 Control Board

The control board (CXP) implements service scheduling, system control, and system clock processing, and provides auxiliary interfaces.

Currently, the ATN 950B supports only the ANDD03CXPA00 control board. For details about parameters of the ANDD03CXPA00, see System Control, Cross-connect and Multi-protocol Process Unit.

5.3.2 Ethernet Service Interface Board

The device supports multiple types of Ethernet interface boards to address requirements for various interface quantities, interface rates, and interface types (optical/electrical). Ethernet service interface boards are widely used in various network environments. They can accept base station services on the user side, and transmit services upstream on the network side. The Ethernet service interface board supports Layer 2 services, Layer 3 services, and hybrid transmission of Layer 2 and Layer 3 services. (When the main interface is in Layer 2 mode, configure the sub-interface to transmit Layer 2/Layer 3 services.)

Different Ethernet service interface boards provide the same service functions, but mainly differ from each other in terms of the number of interfaces and interface type. For details about parameters of interface boards, see Interface Board in *Hardware Description*.

- FE/GE electrical interfaces can work at the rates of 10 Mbit/s, 100 Mbit/s, and 1000 Mbit/s.
- FE/GE SFP interfaces support GE optical modules, GE electrical modules, and FE optical modules.
- 10GE interfaces support XFP/SFP+ optical modules.
- 50G interfaces support QSFP28 optical modules.

5.3.3 E1 Service Interface Board

The E1 service interface board supports PPP, and TDM link-layer protocols.

PPP

Figure 5-11 and **Figure 5-12** show the application of the E1 service interface board using the PPP protocol.

Figure 5-11 Application of the E1 service interface board using the PPP protocol (user side)

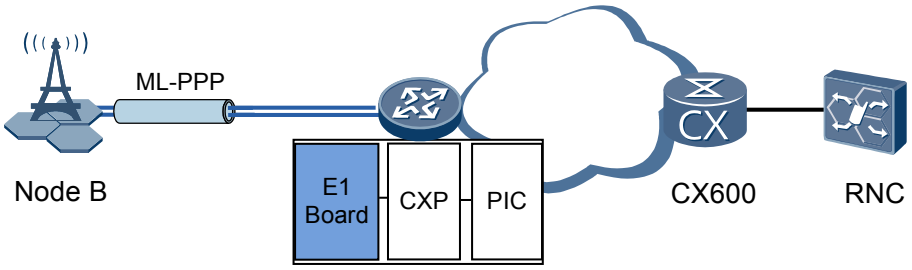
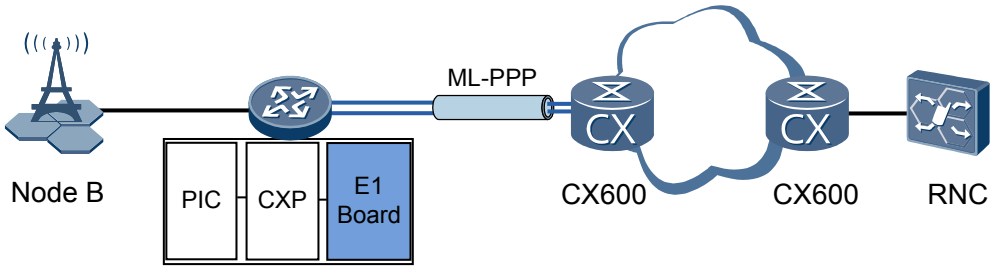


Figure 5-12 Application of the E1 service interface board using the PPP protocol (network side)



The device uses the E1 service interface board to support IP/MPLS services carried over ML-PPPs on both user side and network side.

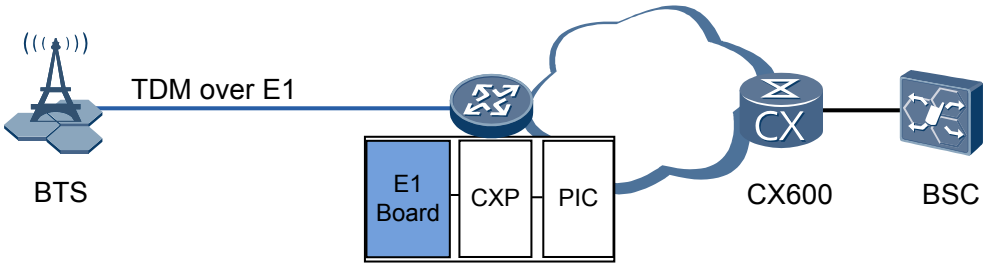
NOTE

An independent PPP link cannot carry service. PPP links must be added to an ML-PPP group to carry services.

TDM

Figure 5-13 shows the application of the E1 service interface board using the TDM protocol.

Figure 5-13 Application of the E1 service interface board using the TDM protocol



The device uses the E1 service interface board to access the TDM service, encapsulate the service signals into packets, and transparently transmit the packets through PWs over the PSN network. This achieves CES service emulation.

For details about parameters of the E1 interface board, see Interface Board in *Hardware Description*.

5.3.4 STM-1 Service Interface Board

Figure 5-14 and Figure 5-15 show the applications of STM-1 service interface boards on a network.

Figure 5-14 Application of the STM-1 service interface board (user side)

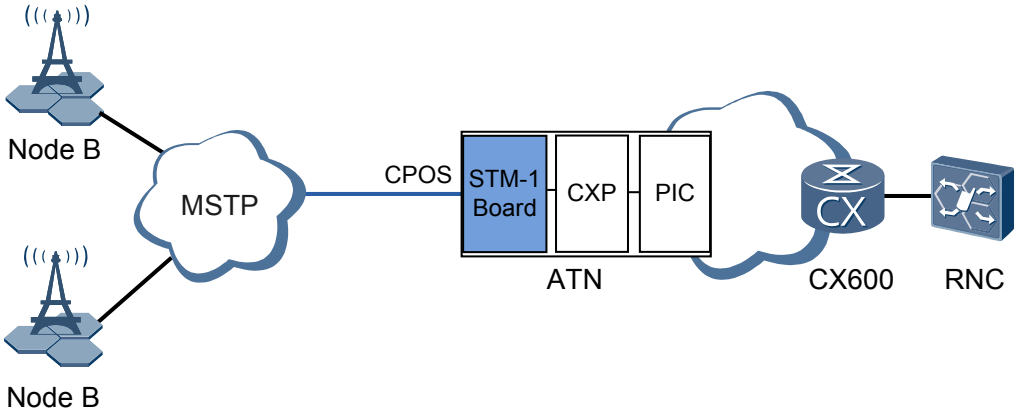
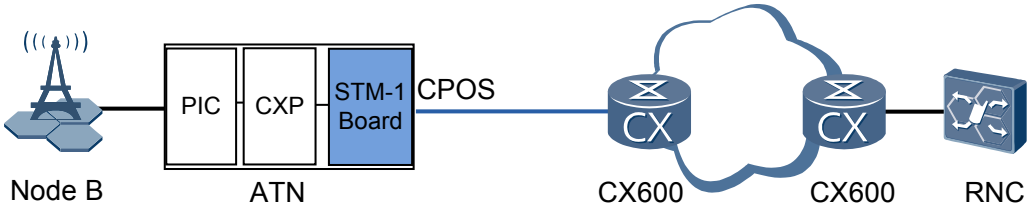


Figure 5-15 Application of the STM-1 service interface board (network side)



The AND2CQ1B interface board on the ATN supports STM-1 services and provides four CPOS interfaces. The CPOS physical interfaces are no longer used as service interfaces, but the channelized 63 E1 channels are used as synchronization serial interfaces that support the same services as the E1 service interface boards.

- The AND2CQ1B board can be used on the user or network side. It supports ML-PPP and carries IP services over E1 channels on CPOS interfaces.
- The AND2CQ1B board on the user side can access and converge TDM services over E1 channels on CPOS interfaces. It implements service emulation and transparent transmission over a packet switched network, achieving TDM PWE3 (CES) services.

The AND2CQ1B can use the APS protocol when services are accessed. When APS protection is used, the supported link layer protocol can only be TDM.

NOTE

Services supported by the E1 channel on the CPOS interface are basically the same as those provided by the E1 service interface board. The differences are listed as follows:

- The E1 channel of the AND2CQ1B supports IP and MPLS services carried over ML-PPPs; the E1 service interface board only supports IP services.
- The E1 channel of the AND2CQ1B does not support fractional E1; the E1 service interface board supports fractional E1 when the TDM protocol is used.

6 Link Features

About This Chapter

6.1 Ethernet Link Features

The ATN supports the following Ethernet link features:

- Flow control and rate autonegotiation on GE interfaces
- Eth-Trunk
  - Layer 2 and Layer 3 Eth-Trunk interfaces
  - The Eth-Trunk interface support various services like common Ethernet interfaces.
  - Addition or deletion of member interfaces to or from an Eth-Trunk interface. The system can sense the state (Up or Down) change of member interfaces, thereby dynamically changing the bandwidth of the Eth-Trunk interface.
  - Association between Eth-Trunk and BFD
  - Link Aggregation Control Protocol (LACP) defined in IEEE 802.3ad. LACP maintains link status based on interface status. LACP adjusts or disables link aggregation in the event of an aggregation change.
- VLAN sub-interfaces
- Dot1q termination sub-interfaces
- QinQ stacking sub-interfaces
- Interface loopbacks, including local loopback and remote loopback
- Configuration of the MTUs for IP and MPLS packets
- Clock synchronization.
- FlexEth interfaces

  Only ATN 950C/ATN 950B/ATN 980B(ANJ0002CXP00) support FlexEth interfaces.

6.2 E1 Link Features

E1 interfaces support the following link protocols: TDM and PPP. PPP on E1 interfaces supports: LCP, IPCP, MPLSCP and ML-PPP.

E1 interfaces support the loopback function, including local loopback and remote loopback.

TDM on E1 interfaces supports:

- Emulation of TDM E1 services for transparent transmission
- Circuit emulation service (CES) implemented by using pseudo wire emulation edge-to-edge (PWE3)
- Fractional E1. Different timeslots of an E1 can be bound into different CES PWs.
- Structure-Aware TDM Circuit Emulation Service over Packet Switched Network (CESoPSN) and Structure-Agnostic Time Division Multiplexing over Packet (SAToP) services

7 Service Features

About This Chapter

7.1 Ethernet Features

7.1.1 Layer 2 Ethernet Features

Ethernet interfaces can work in switched mode at Layer 2 and support VLAN and QoS services. When functioning as UNIs, Layer 2 Ethernet interfaces support MPLS VPN services.

The ATN supports the following Layer 2 Ethernet features:

- VLAN trunk
- QinQ stacking
- Dot1q/QinQ termination sub-interfaces

- Inter-VLAN interface isolation
- Interface-based VLAN planning
- VLAN Mapping
- VLAN Stacking
- MAC address entry limit
- Unknown unicast/multicast/broadcast suppression
- Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP)

7.1.2 Layer 3 Ethernet Features

The ATN supports the following Layer 3 Ethernet features:

- IPv4
- IPv6
- MPLS
- Multicast
- QoS
- Ethernet sub-interfaces
- VLANIF interfaces

7.1.3 STP/RSTP/MSTP Features

The ATN uses the following spanning tree protocols to eliminate loops on Ethernet switching networks:

- STP: blocks redundant links on a switching network to trim the network into a loop-free tree topology.
- RSTP: an enhancement of STP. RSTP achieves fast convergence of the network topology.
- MSTP: an enhancement of STP and RSTP. MSTP works with the VLAN technology to calculate the spanning tree for each VLAN, achieving load balancing among VLANs.

7.1.4 VXLAN Features

Virtual extensible local area network (VXLAN) is a Network Virtualization over Layer 3 (NVO3) technology that uses MAC-in-UDP encapsulation.

- Rate limiting based on VNI
- VXLAN Layer 2 gateway
- Layer 2 VXLAN gateway supporting the Spoken split horizon mode
- Layer 3 forwarding between the same Vxlan tunnels
- VXLAN Layer 3 gateway
- Intergrate Routing and Bridge (IRB) routes used to advertise host routes between VXLAN tunnels
- Application of traffic policies to VXLAN tunnels
- MAC address learning using EVPN on the VXLAN control plane

- VXLAN tunnel encapsulation before forwarding over L3VPN in Ethernet scenarios
- Interface-based sampling; packet parsing after sampling; VNI identification; flow aggregation and output based on VNI and IP
- BA classification and MF classification

7.2 IP Features

7.2.1 IPv4 Features

The ATN supports the following IPv4 features:

- TCP/IP protocol suite, including ICMP, IP, TCP, UDP, socket (TCP/UDP/Raw IP), and ARP
- ACL
- FTP server/client and TFTP client
- DHCP Relay/Server
- Configuration of secondary IP addresses for all physical and logical interfaces

7.2.2 IPv6 Features

The ATN supports the following IPv6 features:

- IPv6 neighbor discovery
- DHCPv6 relay
- Path MTU discovery
- TCP6, ping IPv6, tracert IPv6, socket IPv6

7.2.3 IPv4/IPv6 Transition Technologies

The ATN supports the following IPv4/IPv6 transition technologies:

- 6VPE and 6PE
- IPv6 over IPv4 tunnel
- NAT
  - NAT44
  - VPN NAT
  - NAT ALG (FTP/ICMP/PPTP/RTSP/SIP)
  - NAT Server
  - DNS-MAPPING
  - NOPAT
  - Outbound-interface NAT

7.3 Routing Protocol

The ATN supports the following unicast routing features:

- IPv4 routing protocols, including RIP, OSPF, IS-IS, and BGP
- Static routes that are manually configured by the administrator to simplify network configuration and improve network performance
- Large-capacity routing table entries, which effectively support the operation of a MAN
- Password authentication and MD5 authentication, which improve network security
- Restart of protocol processes through command lines
- Importing of routing information of other protocols
- Automatic restoration after the number of IPv4 routes exceeds the upper limit
- Routing policy configuration:
  - Selection of the optimal route through the routing policy
  - Use of the routing policy in advertising and receiving routes, and filtering of routes through route attributes
- RIP
  - RIP-1 (classful routing protocol) and RIP-2 (classless routing protocol)
  - Advertisement of a default route from a RIP-enabled device to its peers and setting of the metric of this route
  - RIP-triggered update
  - Disabling of a specified interface from sending or receiving RIP packets
- OSPF
  - Association between OSPF and BGP
  - Association between OSPF and LDP
  - Disabling of a specified interface from sending or receiving OSPF packets
  - OSPF I-SPF: I-SPF re-calculates only the affected routes of a shortest path tree (SPT) rather the entire SPT.
  - OSPF GR helper
  - Fast OSPF convergence, which can be implemented in the following manners:
    - Adjusting the interval at which LSAs are sent
    - Configuring BFD for OSPF
  - OSPF calculation of link costs based on the reference bandwidth

    Link costs can be manually configured or automatically calculated by the system based on the reference bandwidth by using the following formula:

    Link cost = Reference bandwidth/Interface bandwidth

    The integer of the calculated result is the link cost. If the calculated result is less than 1, the cost is 1. The link cost can be changed by changing the reference bandwidth. The default reference bandwidth is 100 Mbit/s. The reference bandwidth can be changed to a value in the range of 1 Mbit/s to 2147483648 Mbit/s by running commands.
- IS-IS
  - Two-level IS-IS in a routing domain
  - Association between IS-IS and LDP
  - IS-IS GR helper
  - IS-IS I-SPF: I-SPF re-calculates only the affected routes of a shortest path tree (SPT) rather the entire SPT.

- BGP
  - BGP indirect next hop and dynamic update peer-groups
  - Policy-based route selection by BGP when there are multiple routes to the same destination
  - BGP GR helper
  - BGP route reflector (RR), which addresses the problem of high costs for establishing a full-mesh network when there are many IBGP peers
  - Sending of BGP update packets that carry no private AS number
  - Route dampening, which suppresses unstable routes (unstable routes are neither added to the BGP routing table nor advertised to other BGP peers)
  - BGP fast convergence

    BGP fast convergence includes the following features:
    - Indirect next hop
    - On-demand route iteration

The ATN support the following multicast routing features:

- Multicast protocols, including the Internet Group Management Protocol (IGMP) (IGMPv1, IGMPv2 and IGMPv3), Protocol Independent Multicast-Sparse Mode (PIM-SM), Multicast Source Discovery Protocol (MSDP), and Multi-protocol Border Gateway Protocol (MBGP)
- Reverse Path Forwarding (RPF)
- PIM-SSM
- Anycast rendezvous point (RP)
- Multicast static routes
- PIM-IPv6-SM and PIM-IPv6-SSM
- Multicast listener discovery (MLD), which can be:
  - MLDv1: MLDv1 is derived from IGMPv2 and supports the Any-source multicast (ASM) model. With the help of SSM mapping, MLDv1 supports the source-specific multicast (SSM) model.
  - MLDv2: MLDv2 is derived from IGMPv3 and supports ASM and SSM models.
- Configuration of multicast protocols on Ethernet and Trunk interfaces
- Filtering of routes based on the routing policy when the multicast routing module receives, imports, or advertises multicast routes, and filtering and forwarding of multicast packets based on the routing policy when IP multicast packets are forwarded
- Addition and deletion of dummy entries
- Query of PIM neighbors and the number of control messages
- Filtering of PIM neighbors, control of the forwarding boundary, and control of the BSR service and management boundary
- Filtering and suppression of PIM register messages
- MSDP authentication
- Fast leave of IGMP group members
- Multicast group-based, multicast source-based, multicast source/group-based, and stable-preferred load splitting
- Multicast fast leave

7.4 MPLS Features

The ATN supports MPLS features, static CR-LSPs, and dynamic LSPs. Static CR-LSPs are manually set up by administrators by configuring label switching routers (LSRs) along the LSPs. Dynamic LSPs are dynamically set up by the Label Distribution Protocol (LDP) or RSVP-TE based on routing information.

The delay for MPLS packets can be controlled in the following aspects:

- When no traffic congestion occurs, the ATN uses a high-speed processor to ensure line-rate forwarding and low delay.
- When traffic congestion occurs, the ATN uses multiple mechanisms, such as QoS, HQoS, and MPLS TE, to ensure preferential forwarding and low delay for traffic with a high priority.

MPLS

The ATN supports the following MPLS functions:

- Basic MPLS functions and service forwarding
- LDP used as the signaling protocol, which distributes labels, sets up LSPs, and transfers parameters used for setting up LSPs
  - Label advertisement mode: downstream unsolicited (DU)
  - Ordered label distribution control mode
  - Liberal label retention mode
  - Basic discovery mechanism and extended discovery mechanism of LDP sessions
  - LDP Auto FRR
    - LDP LFA FRR
    - LDP Remote LFA FRR
- MPLS OAM
  - MPLS ping and traceroute. MPLS echo request packets and MPLS echo reply packets are used to check the availability of LSPs.
  - TE LSP-based traffic statistics
  - LSP loop detection mechanism
  - MPLS trap function
- MPLS QoS
  - Mapping from the ToS field in IP packets to the EXP field in MPLS packets in MPLS uniform or pipe modes
  - Static configuration of LSPs and label forwarding based on traffic classification
- Association between LDP and IGP, which minimizes traffic loss through the synchronization between the LDP status and IGP status in case of network faults
- Functioning as a label edge router (LER) or an LSR
  - An LER is an edge device on an MPLS network that connects the MPLS network to other networks. The LER classifies services, distributes labels, adds or removes multiple labels.

  - An LSR is a core router on an MPLS network. The LSR switches and distributes labels.
- Setup of LSPs between routers of different IS-IS levels and between Huawei devices and non-Huawei devices through LDP
- LDP and RSVP-TE, which are used for interoperating with non-Huawei devices

MPLS TE

The MPLS TE technology combines the MPLS technology with traffic engineering. It can reserve resources by setting up LSPs for specified paths in an attempt to avoid network congestion and balance network traffic.

In the case of resource scarcity, MPLS TE allows the preemption of bandwidth resources of LSPs with low priorities, meeting the requirements of important services or high-bandwidth LSPs. When an LSP fails or congestion occurs on a node, MPLS TE can ensure smooth network communication using the backup path and the fast reroute (FRR) function. Through automatic re-optimization, MPLS TE improves the self-adaptation capability of tunnels and properly allocates network resources.

The process of updating the network topology through the TEDB is as follows: When a link goes Down, the CSPF failed link timer starts. If the IGP route is deleted or the link is changed before the CSPF failed link timer expires, CSPF deletes the timer and updates the TEDB. If the IGP route is not deleted or the link is not changed after the CSPF failed link timer expires, the link is considered Up.

MPLS TE provides the following functions:

- Processing of static CR-LSPs. MPLS TE can create and delete static CR-LSPs, which require bandwidth and are manually configured.
- Processing of CR-LSPs of various types and route calculation using the CSPF algorithm

For CR-LSPs, MPLS TE support the following functions:

- RSVP-TE
- Automatic routing

  Automatic routing works in either of the following modes:
  - IGP shortcut: An LSP is not advertised to neighboring routers. Therefore, other routers cannot use the LSP.
  - Forwarding adjacency: An LSP is advertised to neighboring routers. Therefore, other routers can use the LSP.
- FRR

  The FRR switching can be completed within 50 ms, which minimizes data loss caused by network faults.
- CR-LSP backup

  The following backup modes are supported:
  - Hot backup: A backup CR-LSP is set up immediately after the primary CR-LSP is set up. When the primary CR-LSP fails, MPLS TE switches traffic to the backup CR-LSP.
  - Ordinary backup: A backup CR-LSP is set up when the primary CR-LSP fails.
- LDP over TE

  On existing networks, not all devices support MPLS TE. Maybe only the core devices support TE whereas the edge devices use LDP. In this case, LDP over TE can be

introduced. LDP over TE indicates that a TE tunnel is considered as a hop of the entire LDP LSP.

- Make-before-break

  Make-before-break is a technology that ensures highly reliable CR-LSP switching. Before a new CR-LSP is created, the original CR-LSP is not deleted. After a new CR-LSP is created, traffic is switched to the new CR-LSP, and then the original CR-LSP is deleted. This technology ensures non-stop traffic forwarding.

Segment Routing

Segment routing (SR) is a protocol designed to forward data packets on a network based on source routes. Segment Routing MPLS is segment routing based on the MPLS forwarding plane, which is segment routing for short hereafter. Segment routing divides a network path into several segments and assigns a segment ID to each segment and network forwarding node. The segments and nodes are sequentially arranged (segment list) to form a forwarding path.

- SR-Traffic Engineering (SR-TE) is a new Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) tunneling technique implemented based on an Interior Gateway Protocol (IGP) extension. The controller calculates a path for an SR-TE tunnel and forwards a computed label stack to the ingress configured on a forwarder. The ingress uses the label stack to generate an LSP in the SR-TE tunnel. Therefore, the label stack is used to control the path along which packets are transmitted on a network.
- SR LSPs are established using the segment routing technique, uses prefix or node segments to guide data packet forwarding. Segment Routing Best Effort (SR-BE) uses an IGP to run the shortest path algorithm to compute an optimal SR LSP.

Segment routing offers the following benefits:

- The control plane of MPLS network is simplified.

  A controller or an IGP is used to uniformly compute paths and distribute labels, without using RSVP-TE or LDP. Segment Routing can be directly applied to the MPLS architecture without any change in the forwarding plane.
- Provides efficient topology independent-loop-free alternate (TI-LFA) FRR protection for fast path failure recovery.

  Based on the Segment Routing technology, combined with the RLFA (Remote Loop-free Alternate) FRR algorithm, an efficient TI-LFA FRR algorithm is formed. TI-LFA FRR supports node and link protection of any topology and overcomes drawbacks in conventional tunnel protection.
- Provides the higher network capacity expansion capability.

  MPLS TE is a connection-oriented technique. To maintain connections, nodes need to send and process a large number of Keepalive packets, posing heavy burdens on the control plane. Segment routing controls any service paths by merely operating labels on the ingress, and transit node do not have to maintain path information, which reduces the burdens on the control plane.

  In addition, segment routing labels equal to the sum of the number of network-wide nodes and the number of local adjacencies. The label quantity is related only to the network scale, not to the number of tunnels or the service volume.
- Better smooth evolution to SDN network.

  Segment routing is designed based on the source routing concept. Using the source node alone can control forwarding paths over which packets are transmitted across a network.

The segment routing technique and the centralized path computing module are used together to flexibly and conveniently control and adjust paths.

Segment Routing supports both traditional networks and SDN networks. It is compatible with existing equipment and ensures smooth evolution of existing networks to SDN networks instead of subverting existing networks.

7.5 VPN Features

7.5.1 Tunnel Policy

Tunnel policies are used to select tunnels based on destination IP addresses. In applications, tunnels are selected based on tunnel policies. If no tunnel policy is configured, the tunnel management module searches for a tunnel based on the default tunnel policy.

The ATN supports the following tunnel policies:

- Tunnel policy in select-sequence mode

  A tunnel policy in select-sequence mode determines the sequence in which tunnels to the same destination are selected. If a tunnel listed earlier is Up, it is selected regardless of whether other services have selected it. A tunnel listed later is not selected unless the preceding tunnels are all Down.
- VPN tunnel binding

  VPN tunnel binding means that the peer end of the VPN on a PE of the VPN backbone network is associated with a certain MPLS TE tunnel. The data from the VPN to the peer end is transmitted over the TE tunnel. The TE tunnel carries only specified VPN services. This ensures QoS of the specified VPN services.

7.5.2 VPN Tunnel

The ATN supports the following types of VPN tunnels:

- LDP LSPs
- TE tunnels
- SR-TE and SR-BE tunnels

7.5.3 MPLS L2VPN

The ATN supports L2VPN services over an MPLS network. On the MPLS network, carriers can provide L2VPNs over different media. The following L2VPN functions are supported: VLL, VPLS and PWE3.

VLL

The ATN supports the following VLL functions:

- Martini VLL

  Martini VLL supports double labels. The inner label uses extended LDP as the signaling protocol.
- CCC VLL

  CCC VLL supports the local inter-board switching of packets in compliance with 802.1Q.

- SVC VLL
- Configuration of transparent BPDU or LACP packet transmission on interfaces

VPLS

In a VPLS network, Layer 2 loops can be prevented through fully-meshed connections between PEs and the split horizon function.

The implementation of the VPLS control plane through LDP is called Martini VPLS. Martini VPLS uses LDP as the signaling protocol. LDP peer relationships must be manually configured between PEs on a full-mesh VPLS network. When a PE is added to the VPLS network, the configurations on all the related PEs must be modified. Therefore, Martini VPLS has poor scalability. Because PWs are point-to-point links, using LDP to create, maintain, and delete PWs is more efficient.

Supports the following VPLS functions:

- One MAC address space for each VSI
- VPLS learns MAC addresses in the unqualified mode: In this mode, a VSI can contain multiple VLANs sharing a MAC address space and a broadcast domain.

PWE3

Supports the following PWE3 functions:

- Virtual Circuit Connectivity Verification PING (VCCV-PING)
- Supports the manual LDP PW connectivity detection on the UPE, including the connectivity of static single-hop PWs, dynamic single-hop PWs, single-hop PWs, and multi-hop PWs.
- PW template
- Supports the binding between a PW and a PW template, and the reset of PWs.
- Supports heterogeneous interworking.
- TDM/ETH PWE3

7.5.4 BGP/MPLS L3VPN

The ATN supports BGP/MPLS L3VPN, providing an end-to-end VPN solution for carriers. Carriers can provide VPN services for users as a new type of value-added service. The ATN supports:

- Access of CEs to an L3VPN through Layer 3 interfaces such as Ethernet interfaces
- Static routes, BGP, RIP, OSPF, or IS-IS between CEs and PEs
- HoVPN
- IPv4 VPN

  The following IPv4 VPN networking solutions are supported: Intranet VPN, Extranet VPN, and Hub&Spoke.

7.6 Network Reliability

MPLS Tunnel Protection

- TE-Tunnel Hot-standby protection
- Manual switching of APS groups
- Forcible switching of APS groups
- Locking of traffic on the working link of an APS group
- N:1 ($1 \leq N \leq 16$) TE tunnel protection groups

Bit Error-Triggered Protection Switching

The ATN supports bit error-triggered protection switching, which minimizes the impact of bit errors on services.

The function of bit error-triggered protection switching includes interface bit error detection, bit error-triggered Trunk interface protection switching, bit error-triggered section-layer protection switching, and bit error-triggered tunnel protection switching.

FRR

The ATN provides multiple types of fast reroute (FRR) features. You can deploy FRR as required to improve network reliability.

- IP FRR
  - IP FRR switching can be completed within 50 ms. It can minimize data loss caused by network failures.

    NOTE

    If the traffic ingress and egress do not reside on a subcard during a device restart, the switching time is 100 ms.
  - IP FRR enables the system to monitor and save the status of LPUs and interfaces in real time and to check the status of interfaces during packet forwarding. When a fault occurs on an interface, the system can rapidly switch traffic to another preset route, thereby increasing the mean time between failures (MTBF) and reducing the number of lost packets.
- LDP FRR

  LDP FRR switching can be completed within 50 ms.
- TE FRR
  - TE FRR is an MPLS TE technology used to protect part of a network. TE FRR switching can be completed within 50 ms. It can minimize data loss caused by network failures.
  - TE FRR protects traffic temporarily. When the protected LSP becomes normal or a new LSP is established, traffic is switched back to the protected LSP or the newly established LSP.
  - If an LSP is configured with TE FRR, traffic is switched to the protection link and the LSP ingress node attempts to establish a new LSP when a link or node on the LSP fails.

  - TE FRR can provide link protection or node protection based on protected objects.
- VPN FRR

  VPN FRR switching can be completed within 50 ms.

Backup of Key Parts

An ATN device can be equipped with one CXP (system control, switching, and timing board) or two CXPs. The CXPs support hot backup. If an ATN device is configured with two CXPs, the active CXP works and the standby CXP is in the standby state. The standby CXP cannot be accessed by users, but the active CXP can be accessed by users through the management network interface on the standby CXP. The standby CXP exchanges information (including heartbeat messages and backup data) only with the active CXP.

If the system detects that the active CXP becomes faulty or is reset by a command, the system automatically executes a switchover between the active and standby CXP boards. The switchover time is less than 5 ms. The switchover does not result in phase offsets or interrupt services.

The system supports two types of CXP switchover: automatic switchover and forcible switchover. The automatic switchover is triggered by a critical fault in the active CXP or a reset of the active CXP. The forcible switchover is triggered by a command that is run on the console interface. You can forbid a CXP switchover by running a command on the console interface. After a switchover, the system records log information and notifies the NMS. The switchover cause and the associated operations are recorded in the system diagnosis information base for users to analyze.

GR

Graceful restart (GR) is one of the high availability (HA) technologies, which comprise a series of comprehensive technologies such as fault-tolerant redundancy, link protection, faulty node recovery, and traffic engineering. As a fault-tolerant redundancy technology, GR ensures normal forwarding of data during the restart of routing protocols to prevent interruption of key services. Currently, GR has been widely applied to the master/slave switchover and system upgrade.

NOTE

The ATN can only function as a GR Helper.

- BGP GR
- OSPF GR
- ISIS GR
- LDP GR
- RSVP GR
- L3VPN GR

Non-Stop Routing (NSR)

Non-stop routing (NSR) ensures that the control plane of a neighbor does not sense the fault on the control plane of an ATN device that has a backup control plane. In this process, the neighbor relationships set up through routing protocols, MPLS, and other protocols for carrying services are not interrupted.

An ATN device configured with two CXPs supports NSR. When experiencing a fault, upgrade, or service switchover, the ATN device does not need to exchange extended protocol packets with other devices or depend on peer devices for recovery. This masks the device's status changes to the most extent and therefore the peer devices do not sense these changes, eliminating or minimizing the impact of hardware faults on user services.

- OSPF/OSPFv3 NSR
- LDP NSR
- RSVP-TE NSR
- PIM/MSDP/IGMP NSR
- ARP NSR
- L3VPN NSR
- ISIS/ISIS6 NSR
- BGP/BGP4+ NSR
- VRRP NSR

Load Balancing

- Load balancing among IPv4 unicast routes
- Load balancing among VLL tunnels (Tunnels that support load balancing include LSPs and TE tunnels.)
- Load balancing among L3VPN tunnels (Tunnels that support load balancing include: LSPs and TE tunnels.)

7.7 QoS

You can collect traffic statistics on packets on which QoS is performed and view the statistics results through the corresponding display commands.

This section describes the QoS functions supported by the ATN.

DiffServ Model

Multiple service flows can be aggregated into a behavior aggregate (BA) and then processed based on the same per-hop behavior (PHB). This simplifies the processing and storage of services.

On the DiffServ core network, packet-specific QoS is provided. Therefore, signaling processing is not required.

BA Classification

The ATN supports BA classification on both physical and logical interfaces, including:

- Ethernet interface, Ethernet sub-interface, Layer 2 Ethernet interface
- GE interface, GE sub-interface carrying VLL services, Layer 2 GE interface
- Eth-Trunk interface, Eth-Trunk sub-interface, Layer 2 Eth-Trunk interface

The ATN also supports forced traffic classification, which is independent of the DiffServ domain mapping table. Based on the interface, Eth-Trunk interface, and Eth-Trunk sub-

interface views, users can directly specify CoSs and drop priorities for packets. In this manner, received packets can directly enter the queues with the specified CoSs.

By default, protocol packets enter the CS7 queue without the color during internal queue scheduling. To facilitate internal scheduling of protocol packets, configure mappings between the priority value of protocol packets and internal priorities and between the priority value and colors.

MF Classification

During MF classification, packets are classified by source/destination address, source/destination interface number, or protocol type. Generally, MF classification is applied on network edges. Traffic is classified based on certain rules and behavior (traffic control or resource allocation) is performed on traffic of the same class, enabling class-based traffic policing, packet filtering, priority re-marking, and providing differentiated service for user services.

The ATN supports the following MF classification features:

- Allows users to configure MF classification in the ingress direction at UNI-side interfaces.

  UNI-side interfaces include main interfaces, sub-interfaces, interfaces+VLANs, trunk interfaces, and trunk sub-interfaces.
- Classifies traffic by source MAC address, destination MAC address, ID of the protocol carried at the link layer, VLAN, or 802.1p priority in Ethernet packet headers.
- Classifies traffic by IP priority/DSCP/ToS value, source IP address prefix, destination IP address prefix, IP packet bearer protocol ID, fragmentation flag, TCPSYN flag, TCP/UDP source interface number or interface number range, TCP/UDP destination interface number or interface number range, or ICMP flag in IPv4 packet headers.
- Classifies traffic based on the EXP value of MPLS packet headers.
- Performs behavior on classified traffic, such as CAR, Permit/Deny, remarking CoS in the ATN, remarking user packet priority, and traffic statistics collection.

Traffic Policing

CAR is mainly used for rate limiting. With CAR enabled, a token bucket is used to measure the data flows that pass through an interface, and only the packets assigned tokens can pass through the interface in the specified period of time. In this manner, the traffic rate at the interface can be controlled.

CAR is usually applied on the edge of a network to ensure that core devices process data properly.

Queue Scheduling

The ATN supports PQ and WFQ for queue scheduling on interfaces.

Packets of different priorities are mapped into different queues. Round robin (RR) is used on each interface for queue scheduling.

SP scheduling applies to PQ queues. Packets in high-priority queues are scheduled preferentially. Therefore, services that are sensitive to delays (such as VoIP) can be configured with high priorities. If PQ scheduling is applied to all queues, the priorities of CS7, CS6, EF, AF4, AF3, AF2, AF1, and BE queues are placed in descending order. If PQ scheduling is

applied to BE queues (not configured generally) and WFQ scheduling is applied to other queues, the priority of BE queues is higher than that of other queues.

In PQ queues, however, if the bandwidth of high-priority packets is not restricted, low-priority packets cannot obtain bandwidth and are starved out.

Weight fair queuing (WFQ) is a complex queuing process, which ensures that services with the same priority are treated equally and services with different priorities are treated based on weights. WFQ weights services based on their requirements for the bandwidth and delay. Weights are determined by the IP precedence in IP packet headers. Packets in the same flow are placed in the same queue using the Hash algorithm. When flows enter queues, WFQ automatically places different flows in different queues using the Hash algorithm. When flows leave queues, WFQ allocates bandwidths to the flows based on IP precedence of the flows. The smaller the IP precedence value of a flow, the smaller the bandwidth allocated to the flow. In this manner, services of the same precedence are treated equally, and services of different precedence are treated based on their weights.

PQ and WFQ queues use SP scheduling. PQ queues are scheduled preferentially, and then WFQ queues are scheduled. Packets in PQ queues are preferentially forwarded. Packets in WFQ queues are forwarded only after packets in PQ queues are all forwarded.

Congestion Avoidance

Congestion avoidance is a traffic control mechanism used to avoid network overload by adjusting network traffic. With this mechanism, the ATN can monitor the usage of network resources (such as queues and buffer) and discard packets when network congestion intensifies.

Random early detection (RED) and weighted random early detection (WRED) are usually used for congestion avoidance.

The RED algorithm sets the upper and lower limits for each queue and specifies the following rules:

- When the length of a queue is below the lower limit, no packet is discarded.
- When the length of a queue exceeds the upper limit, all the incoming packets are discarded.
- When the length of a queue is between the lower and upper limits, incoming packets are discarded randomly. A random number is set for each incoming packet, and the random number is compared with the drop probability of the queue. The packet is discarded when the random number is greater than the drop probability. The longer the queue, the higher the drop probability. The drop probability has an upper limit.

Unlike RED, the random number in WRED is based on the IP precedence of IP packets. WRED keeps a lower drop probability for the packets that have higher IP precedence.

RED and WRED employ the random packet drop policy to avoid global TCP synchronization. The ATN uses WRED for congestion avoidance.

The ATN supports congestion avoidance in the outbound direction of an interface. The WRED template is applied in the outbound direction.

The ATN supports congestion avoidance based on services. Eight service queues (BE, AF1, AF2, AF3, AF4, EF, CS6, and CS7) are reserved on each interface. Packets of different colors (red, yellow, and green) correspond to different drop precedence.

HQoS

The ATN supports the following HQoS functions:

- Provides three/five levels of scheduling to ensure diverse services.
- Sets parameters such as WRED, low delay, SP/WFQ, CBS, PBS, and statistics function for each queue.
- Sets parameters such as the CIR, PIR, number of queues, and scheduling algorithm for each user.
- Provides a complete traffic statistics function. Users can view the bandwidth usage of services and properly plan bandwidth for services by analyzing traffic.
- Supports interface- and VLAN-based HQoS.

QoS for Ethernet

The ATN can perform BA classification based on the 802.1p field in VLAN packets. On the ingress PE, the 802.1p field in a Layer 2 packet is mapped to the precedence field defined by the upper layer protocol, such as MPLS EXP. Then, DiffServ can be implemented for packets on the backbone network. On the egress PE, the precedence field of the upper layer protocol is mapped back to the 802.1p field.

7.8 Security Features

Security Authentication

The ATN supports the following security authentication functions:

- Authentication, accounting, and authorization implemented locally or on the RADIUS or HWTACACS server
- Plaintext authentication and MD5 encrypted text authentication supported by routing protocols that include RIPv2, OSPF, IS-IS, and BGP
- MD5 encrypted text authentication supported by LDP and RSVP
- SNMPv3 encryption and authentication
- NETCONF authentication

URPF

The ATN supports unicast reverse path forwarding (URPF) for IPv4 traffic.

MAC Address Limit

The ATN supports the following MAC address limit functions:

- Limit on the number of VLAN-based MAC address forwarding table entries
- Limit on the number of VSI-based MAC address forwarding table entries

Entries in a MAC address forwarding table are classified into three types:

- Dynamic entries

- Dynamic entries are learned by interfaces and stored in the hardware of the system control board. Dynamic entries will age. Dynamic entries will be lost when the system is reset.
- Static entries
- Static entries are configured by users and stored on the system control board. Static entries will not age. Static entries will not be lost when the system is reset.
- Blackhole entries
- Blackhole entries are used to filter out the data frames that contain specific destination MAC addresses. Blackhole entries are configured by users and stored on the system control board. Blackhole entries will not age. Blackhole entries will not be lost when the system is reset.

MAC Address Deletion

The ATN supports the deletion of MAC addresses from the MAC address forwarding table:

- VLAN-based MAC address deletion
- Trunk-based MAC address deletion
- Entire system-based MAC address deletion

Unknown Traffic Limit

With the unknown traffic limit function, the ATN can implement the following functions:

- Manages user traffic.
- Allocates bandwidth to users.
- Limits the rate of unknown unicast, unknown multicast, and broadcast traffic.

In this manner, the network bandwidth is properly used and network security is guaranteed.

Whitelist- or Blacklist-based MAC Address Filtering

The ATN can filter MAC addresses based on a source MAC address whitelist or blacklist at Ethernet interfaces. Then, the ATN forwards packets from MAC addresses in the whitelist and discards packets from MAC addresses in the blacklist.

Local Attack Defense

The ATN provides a uniform local attack defense module to manage and maintain the attack defense policies of the entire system, thereby offering an all-around, feasible, and maintainable attack defense solution for users.

The ATN supports the following attack defense functions:

- Management and service plane protection
- Attack source tracing
- When the ATN is attacked, it obtains and saves suspicious packets, and then displays the packets in a certain format using command lines or offline tools. This helps locate the attack source easily.
- When attacks occur, the system automatically removes the data encapsulated at upper layers of the transmission layer and then caches the packets. When the number of

packets in the cache reaches a certain number (for example, 20000 packets on each LPU), the earliest cached packets are overridden when more packets are cached.

SSHv2

The ATN supports the STelnet client and server as well as the SFTP client and server, which support SSHv1.5 and SSHv2.

IPSec

IPsec can be configured to authenticate and encrypt protocol packets, greatly improving transmission security. To be specific, IPsec provides high-quality, interoperable, and password-based security for protocol packets.

MACsec

Media Access Control Security (MACsec) is an 802.1AE- and 802.1X-based secure communication method for local area networks (LANs). It provides functions such as identity authentication, data encryption, integrity check, and replay protection to ensure the security of Ethernet data frames and prevent devices from processing packets with security threats.

Only the ANKD00CXPA00/ANKD00CXPA01s of ATN 950Cs support MACsec.

7.9 Maintainability

Plug-and-Play

Plug-and-play (PNP) enables the NMS to automatically configure newly powered-on devices with empty configurations using DHCP and allows commissioning engineers to remotely commission the devices in a centralized manner.

PNP frees commissioning engineers from visiting sites for software commissioning, significantly speeding up the engineering progress.

DCN

After a device is powered on, the initial IP address is generated based on the NE ID. The device uses the initial IP address to access the network through the data communication network (DCN) protocol. Then the NMS automatically discovers and configures the new device, and commissioning engineers remotely commission the new device.

DCN frees commissioning engineers from visiting sites for software commissioning, significantly speeding up the engineering progress.

The device integrates virtual routing and forwarding (VRF) routes on the control plane into the hardware forwarding plane. Therefore, DCN packets are forwarded directly by chips, accelerating DCN packet transmission and enabling larger coverage of a DCN.

ITU-T Y.1731

ITU-T Y.1731 supports the following functions:

- Statistics on single-ended packet loss and two-way delay

- VLL alarm indication signal (AIS) and VLAN AIS

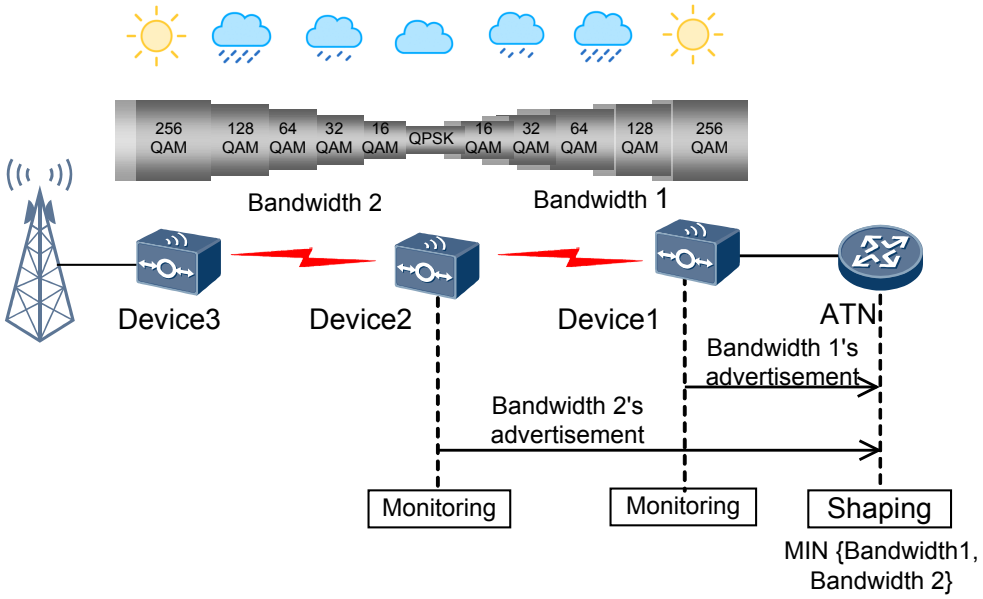
Bandwidth Association with Microwave Devices

Microwave links are prone to weather and environment impact and easily become network congestion points. An ATN device can periodically receive bandwidth advertisements from a microwave device and perform shaping on an ATN interface, so that the ATN interface becomes a congestion point. The ATN device has a large cache, which reduces the packet loss ratio and increases the E2E network throughput.

Bandwidth association simplifies QoS configurations and requirements on the microwave device, and the complex QoS logic is implemented on the ATN device.

The microwave device periodically sends advertisement frames, which contain the nominal and current bandwidths, to instruct the ATN device to update the interface's shaping value.

- Common scenario 1: On the network shown in the following figure, the microwave devices form a single chain. The bottleneck point is the link with minimum air interface bandwidth.

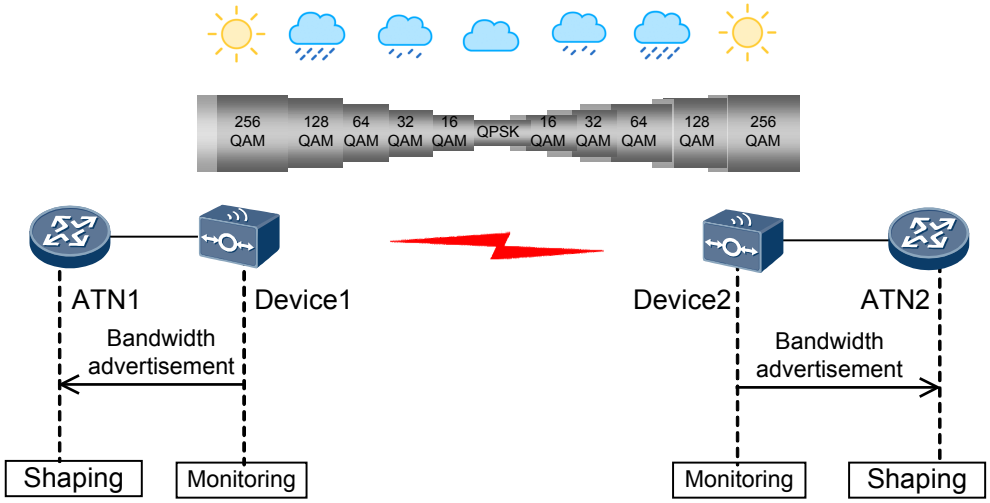


Device1: monitors the local air interface bandwidth and advertises it to the ATN device.

Device2: monitors the local air interface bandwidth and advertises it to the ATN device.

The ATN interface receives two bandwidths and calculates the minimum value between them for shaping within a period.

- Common scenario 2: On the network shown in the following figure, the microwave devices are server-layer devices, and the ATN devices are client-layer devices. The server layer advertises an air interface bandwidth to the client layer, and the corresponding ATN device performs shaping on the bandwidth within a period.



MPLS OAM

MPLS OAM supports the following functions:

- MPLS ping and traceroute. MPLS echo request packets and MPLS echo reply packets are used to check the availability of LSPs.
- TE LSP-based traffic statistics
- LSP loop detection mechanism
- MPLS trap function

Ethernet OAM Fault Management

Ethernet OAM fault management includes the following functions:

- Link-level Ethernet OAM: Ethernet in the First Mile OAM (EFM OAM)

  Link-level Ethernet OAM monitors physical Ethernet links directly connecting carrier networks to user networks. For example, IEEE 802.3ah, also known as Ethernet in the First Mile (EFM), supports Ethernet OAM for the last-mile links and also monitors physical Ethernet links between devices.

  EFM supports link continuity check, fault detection, fault advertisement, and remote loopback for point-to-point Ethernet link maintenance. Unlike CFM that is used for a specific type of service, EFM is used on links transmitting various services.

  Per packet delivery time can be configured ranging from 100 ms to 1s.

- Network-level Ethernet OAM: connectivity fault management OAM (CFM OAM) and ITU-T Y.1731

  Network-level Ethernet OAM checks network connectivity, locates connectivity faults, and monitors end-to-end network performance at the access and aggregation layers. Network-level Ethernet OAM complies with protocols such as IEEE 802.1ag (connectivity fault management) and ITU-T Y.1731.

  - IEEE 802.1ag defines OAM functions, such as continuity check (CC), loopback (LB), and link trace (LT), for Ethernet bearer networks. CFM applies to large-scale end-to-end Ethernet networks.
  - ITU-T Y.1731 covers the content defined in IEEE 802.1ag and defines more OAM messages for fault management and performance monitoring. Fault management

includes alarm indication signal (AIS), remote defect indication (RDI), locked signal (LCK), test signal, automatic protection switching (APS), maintenance communication channel (MCC), experimental (EXP) OAM, and vendor specific (VSP) OAM. Performance monitoring includes frame loss measurement (LM) and delay measurement (DM).

Ethernet OAM Performance Management

The ATN provides Ethernet performance management in compliance with ITU-T Y.1731. The NMS can periodically collect end-to-end performance data of a service flow from an ATN device and generate a statistics report accordingly.

By using performance management tools, an ISP can monitor the network status in real time using the NMS. The ISP then checks whether the forwarding capacity of the network complies with the Service Level Agreement (SLA) signed with users and quickly locates network faults. The ISP does not need to perform the check on the user side, which significantly decreases maintenance costs.

BFD

Bidirectional Forwarding Detection (BFD) is a detection mechanism used uniformly in an entire network. It is used to quickly check and monitor the connectivity of links or IP routes on a network.

BFD sends detection packets at both ends of a bidirectional link to check the link status in both directions. A link fault can be detected within milliseconds. The ATN supports single-hop BFD and multi-hop BFD.

The ATN supports the following BFD applications:

- BFD for FRR
  - BFD for LDP FRR
  - LDP FRR switchover triggered after BFD detects faults on protected interfaces
  - BFD for IP FRR and BFD for VPN FRR

    IP FRR and VPN FRR are triggered after BFD detects faults and reports fault information to the upper layer applications.
- BFD for static route
- BFD for RIP

  BFD for RIP can rapidly detect link faults, report the faults to RIP, and speed up the RIP's response to network topology changes.
- BFD for IS-IS

  Statically configured BFD sessions can check IS-IS adjacency.
- BFD for OSPF/BGP

  OSPF and BGP can be used to dynamically set up and delete BFD sessions.
- BFD for PIM

  The distinguishing feature of BFD for PIM is that the PIM module can be notified of the fault within milliseconds, but not until the neighbor relationship times out. DR election is triggered quickly after the DR fails. This greatly shortens multicast data transmission interruptions and improves multicast network reliability.
- BFD for trunks

BFD can check a trunk and the member links of the trunk separately. Therefore, it can check the connectivity of the trunk and that of an important member link of the trunk.

- BFD for LSP

  BFD can quickly detect faults on LDP LSPs, TE tunnels, TE LSPs, and PWs, thereby implementing fast switchovers such as VPN FRR, TE hot-standby, and VLL FRR.
- BFD for Dot1q sub-interface
- Interconnection with SPE nodes supporting multi-hop BFD
- BFD priority change

IP FPM

IP flow performance measurement (FPM) is used to directly measure multipoint-to-multipoint (MP2MP) service flows to obtain performance statistics such as the packet loss ratio and service trail delay.

IP FPM supports the following functions:

- Packet loss detection, including single- and dual-ended packet loss detection
- Delay detection, including one- and two-way delay detection

RFC2544

IETF RFC2544 defines a series of test schemes that are used to test performance of interconnected equipment on a network. In this document, RFC2544 refers to test functions implemented using the test schemes defined in IETF RFC2544. RFC2544 includes initiating-end test and reflecting-end test.

The test functions are divided into three types of application: Layer 2 ETH RFC2544, Layer 3 IP RFC2544, and L2+L3 (Layer 2 service access to Layer 3) RFC2544 by application. The three types of application support the throughput test, delay and jitter test, and packet loss test.

NOTICE

During an RFC2544 test, the system sends a certain number of packets that occupy some or even all network bandwidth resources. Therefore, an RFC2544 test affects services. Perform an RFC2544 test only on a network where no services are deployed.

- The throughput test is used to check the maximum bandwidth that meets accuracy requirements within a specified bandwidth range.
- The delay and jitter test is used to check two-way delay and jitter in the case of a specified packet length and rate.
- The packet loss test is used to check the packet loss ratio in the case of a specified packet length and rate.

Y.1564

Y.1564 is a specification for the test before the Ethernet service is activated. The test contents include the configuration detection on multiple service flows and concurrent performance detection. Y.1564 can be used to perform the IR, latency, jitter, sequence error, and QoS tests at the same time to test the CIR, latency, jitter value, and sequence error value of different packets, which greatly shortens the test period.

7.10 Traffic Statistics

The ATN can collect statistics on traffic of various user services.

The traffic statistics function:

- Helps carriers analyze the traffic model of a network.
- Provides reference data for deploying and maintaining Diff-Serv TE.

URPF Traffic Statistics

The ATN can globally collect statistics on discarded traffic that does not comply with URPF.

Traffic statistics collection allows carriers to discover network spoofs and attacks on the source address and provides evidence on security defense.

CAR Traffic Statistics

The ATN provides diverse QoS features such as traffic classification, traffic policing (CAR), and queue scheduling. For these features, the ATN provides the following QoS traffic statistics functions:

- In traffic classification, the system can collect statistics on traffic that matches rules and traffic that does not match rules.
- The traffic statistics for traffic policing include:
  - Statistics on the total traffic that complies with CAR
  - Statistics on the traffic that is permitted or discarded by CAR
  - Interface-based traffic statistics
  - Interface-based CAR traffic statistics when the same traffic policy is applied to different interfaces

HQoS Traffic Statistics

Supports statistics on flow queues, including counts of forwarded and lost packets of each flow queue (eight priority flow queues in total).

Interface-Based Traffic Statistics

- Traffic statistics on the following interfaces: physical interfaces, sub-interfaces, loopback interfaces, null interfaces, and ETH-Trunk interfaces.
- Statistics on IPv4.
- The device uses the 64-bit register to store the interface-based traffic statistics. For example, the register on a GE interface can store traffic statistics for 585 years.

VPN Traffic Statistics

On an L3VPN network, ATN functioning as a PE, can collect statistics on incoming and outgoing traffic of L2VPN PW.

Traffic Statistics on TE Tunnels

ATN functioning as a PE on an MPLS TE network, can collect statistics on the total incoming and outgoing traffic of a tunnel.

Telemetry

Telemetry is a technology developed to fast collect data from physical or virtual devices remotely. Devices use the push mode to proactively send their data information, such as traffic statistics on interfaces, CPU usage, and memory data, to the collector at a specific interval. In the conventional pull mode, devices interact with the collector using questions and answers. The push mode implements real-time and quick data collection.

7.11 Clock

The ATN supports the following clock features:

- Ethernet clock synchronization

  The Ethernet interfaces of the ATN support Ethernet clock synchronization, which ensures clock quality and stratum on the network.
- E1 clock synchronization
- Network Time Protocol (NTP) clock

  The Network Time Protocol (NTP) is used for synchronizing clocks of all devices in a network so that the devices can provide various applications based on the uniform time.
- Internal clock

  The ATN provides an internal clock and can extract clock information from LPUs. The clock precision reaches 4.6 ppm.
- 1588v2
- Compliance with G8275.1
- 1588 ACR Client
- 1588 ATR Client/Server
- Atom GPS
- CES ACR

  NOTE

  Only the ATN 910C-D of the ATN 910C supports CES ACR.

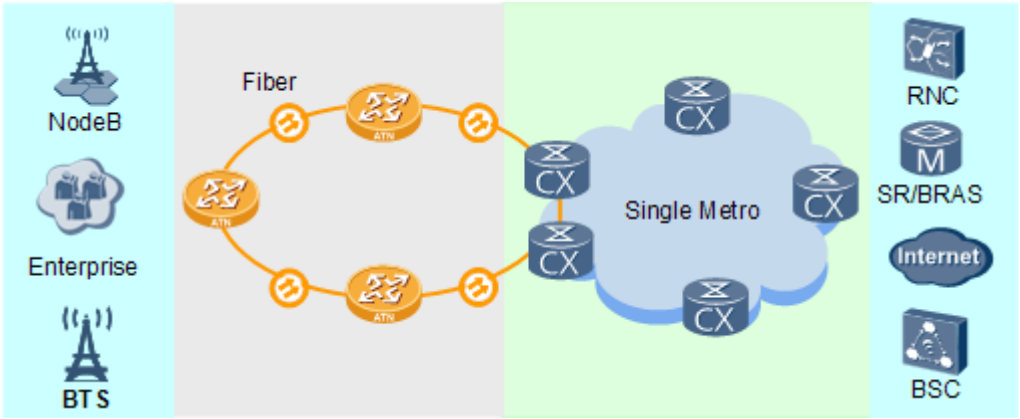
8 Usage Scenarios

About This Chapter

8.1 Mobile Bearer Usage Scenario

The ATN can be deployed at the access layer of the FMC MAN or at access sites that process heavy service traffic, to build an ALL IP-oriented mobile bearer network with high efficiency. The following figures show the typical applications of the ATN series.

Figure 8-1 Typical applications of the ATN series



9 Operation and Maintenance

About This Chapter

9.1 System Configuration Modes

The ATN supports two configuration modes: command line-based configuration and NMS-based configuration.

Command Line-based Configuration

- A user can locally log in to a device to configure management interfaces. The ETH/OAM interface integrates the network management interface and console interface. The console interface is a non-standard pin assignment RS-232 interface. For pin assignment, see *Hardware Description*. An MGMT-ETH interface is a network management interface and a console interface is a management serial interface.
  - As a command input interface, the management interface can send command lines to the control plane.

- As a debugging interface, the management interface can receive debugging information from the control plane and data plane, and deliver debugging commands and control commands.

NOTE

After the ATN is powered on, it automatically binds the management network interface to the reserved VPN (__LOCAL_OAM_VPN__) and configures the IP address 192.168.0.1/24 for the management interface.

A user can configure another IP address in the network segment 192.168.0.0/24 for a computer, and log in to the ATN from the computer using a user name and password for on-site maintenance.

The IP address of the management interface can be changed or deleted. The management interface can be disabled as required.

- Users can configure the ATN after remotely logging in through Telnet/SSH.

NMS-based Configuration

A user can use an SNMP-based NMS to configure the ATN. For details, see **10 NMS**.

9.2 System Management and Maintenance

The ATN supports the following system management and maintenance functions:

- Board detection, hot swap detection, Watchdog, board reset, RUN indicator, fan and power supply monitoring, system debugging, and version query
- Local and remote software upgrade and data loading, version rollback, and backup, saving, and clearing of data
- Hierarchical user authority management, operation log management, command line help information, and comments on commands
- Inband and outband NMS interfaces
- Three user authentication modes: local authentication, RADIUS authentication, and HWTACACS authentication; user authorization using command lines and SNMP
- Plug-and-play
- Multi-user operation
- Query of Layer 2 or Layer 3 interface information
- Hierarchical alarm management, alarm classification, and alarm filtering
- Manual enabling and disabling of interfaces and optical modules

9.3 Device Running Status Monitoring

The device running status can be monitored through the information center.

Syslog is a sub-function of the information center. Using UDP/TCP, Syslog outputs log information to the log host through interface 38514.

The information center receives and processes the following types of information:

- Log information
- Debugging information
- Trap information

Information is classified into eight levels in terms of severity, which are described in the following table.

Level	Severity	Description
0	Emergency	A fatal exception occurs on a device. The system is unable to function properly and must be restarted. For example, the device is restarted due to program exceptions, or memory usage errors are detected.
1	Alert	A serious exception occurs on a device, which needs to be handled immediately. For example, the device memory usage reaches the upper threshold.
2	Critical	A critical exception occurs on a device, which needs to be handled and analyzed. For example, the device memory usage exceeds the alarm threshold; the temperature exceeds the alarm threshold; Bidirectional Forwarding Detection (BFD) detects that a device is unreachable or detects error messages generated by the local device.
3	Error	An improper operation is performed or an abnormal process occurs on a device, which does not affect subsequent services but requires attention and cause analysis. For example, users enter incorrect commands or passwords; error protocol packets are received by other devices.
4	Warning	An abnormality that may cause a device to malfunction occurs, which requires attention. For example, a routing process is disabled by a user; BFD detects packet loss; error protocol packets are detected.
5	Notice	A key operation is performed to keep a device running normally. For example, a user runs the **shutdown** command on an interface; a neighbor is discovered; the protocol state machine changes status.
6	Informational	A routine operation is performed. For example, a user runs the **display** command.
7	Debugging	A routine operation is performed, which requires no action.

The information center supports 10 channels, of which channels 0 to 5 each have a default channel name. By default, the six channels correspond to six directions in which information is output. The log information on the CF card is output to a log file through channel 9 by default. Therefore, a total of seven default output directions are supported.

When multiple log hosts are configured, you can configure log information to be output to different log hosts through one channel or multiple channels. For example, you can configure some log information to be output to a log host through channel 2 (loghost), and some log information to a log host through channel 6. In addition, you can change the name of channel 6 to facilitate channel management.

All alarms are stored in a log file on a CF card. How long alarms can be stored depends on the number of alarms. Generally, alarms can be stored for months.

9.4 System Service and Status Tracking

The ATN provides the following functions for tracking system services and status:

- Monitors the transition of the routing protocol state machine.
- Monitors the transition of the MPLS LDP state machine.
- Monitors the transition of the VPN state machine.
- Monitors the types of protocol packets sent by the forwarding engine to the control plane and displays detailed information about packets by enabling debugging.
- Detects error packets and collects the statistics on them.
- Displays a notification when the abnormality processing starts.
- Collects statistics on system resources used by each feature.

9.5 System Test and Diagnosis

The ATN supports the debugging of running services, including online recording of key events, packet processing, packet parsing, and status switching at specified time. The debugging function provides powerful support for device commissioning and networking. Debugging can be enabled or disabled through the console interface for a specific service (information about a routing protocol) or a specific interface (information about a routing protocol on a specific interface).

The ATN provides the system-based trace function to detect and diagnose running software. The trace function supports online recording of important events such as task switchover and interruption, queue reading and writing, and system exceptions. If the system is restarted after a fault occurs, the ATN can read trace information, which functions as a reference for fault diagnosis. The trace function can be enabled and disabled through commands on the console interface.

The ATN supports real-time query of CPU usage of the system control board.

Debugging and trace information provided by the ATN is classified into several levels. The information with different levels can be output to different destinations according to configurations. For example, information can be output to the console interface, Syslog server, or SNMP Trap.

9.6 NQA

Network quality analysis (NQA) measures the performance of each protocol running on a network and helps carriers to collect network operation counters in real time, such as the FTP connection delay, TCP connection delay, and file transmission rate. By controlling these counters, carriers can provide differentiated services for users and charge users differently. NQA is also an effective tool to diagnose network faults.

NQA supports the following functions:

NOTE

Jitter tests support the continuous transmission of 3000 packets at most and support voice traffic simulation.

- ICMP, UDP, TCP, and SNMP tests
- PWE3 ping and PWE3 traceroute tests
- LSP ping, LSP traceroute, and LSP jitter tests
- ICMP jitter and UDP jitter tests
- UDP traceroute tests
- VPLS MAC ping tests
- PATH MTU tests
- Management of all NQA functions through the NMS

9.7 Netstream

NetStream is a Huawei-patented technology used to collect statistics about network traffic and export the statistics. The following applications of Netstream are supported:

- Accounting
- Network planning and analysis
- Network monitoring
- Application monitoring and analysis
- Abnormal traffic detection

NetStream mainly includes Netstream Data Exporter (NDE), Netstream Collector (NSC), and Netstream Data Analyzer (NDA). The ATN functions as the NDE to sample packets, aggregate data flows, and export data flows.

The ATN supports the following sampling functions:

- Sampling on the inbound and outbound interfaces
- Sampling of the IPv4 unicast or multicast packets, fragmented packets, MPLS packets, MPLS L3VPN packets
- Regular packet sampling, random packet sampling, sampling at regular time, and sampling at random time
- Sampling on various physical and logical interfaces such as Ethernet interfaces, VLAN sub-interfaces, and trunk interfaces.

The following flow aggregation and output functions are supported:

- IPv4 packets can be aggregated based on options including AS, AS-ToS, protocol-port, protocol-port-ToS, source-prefix, source-prefix-ToS, destination-prefix, destination-prefix-ToS, prefix, and prefix-ToS.
- MPLS packets support aggregation based on the Layer 3 label.
- Collected statistics can be exported in the V5, V8, and V9 format. The 16-bit and 32-bit AS numbers are supported (and can be configured using commands). When the packets are exported in the V9 format, both the 16-bit and 32-bit NetStream interface indexes are supported, which can be set using commands based on the actual requirements.

9.8 Port Mirroring

NOTE

The mirroring function complies with industry standards. It can be used to analyze communication information of specific end users for maintenance and operation purposes. Strictly observe the local laws and regulations when using the mirroring function. Ensure that users' privacy is protected when you collect and save communication information.

The ATN provides port mirroring to map specific traffic to a certain monitored interface. Using the traffic information, senior maintenance engineers can perform in-service debugging and analyze the network operating status.

9.9 System Software Upgrade

In-Service Upgrade

The ATN supports in-service software upgrades and patching. The in-service patching function allows you to upgrade specific features.

Upgrade Method

The ATN can be upgraded by means of resets. When the device is configured with two system control boards, it can also be upgraded in ISSU mode without causing service interruption.

Software Version Rollback

During the upgrade process, if the system fails to start by using the new system software, the system software in the last successful startup is used.

The rollback function can prevent the adverse impact of an upgrade failure on services.

9.10 Other Operation and Maintenance Features

The ATN supports the following operation and maintenance features in addition to the preceding features:

- Configures hierarchical command protection to prevent access of unauthorized users.
- Allows users to enter a question mark (?) to obtain help information.
- Provides detailed debugging information for network fault diagnosis.
- Provides DosKey-like functions to execute a history command.

- Provides a command line interpreter that supports fuzzy match of keywords. For example, you can enter **disp** to search for the **display** command.

10 NMS

SNMP

Supports device operation and management by the network management station through SNMP.

Supports SNMPv1, SNMPv2c, and SNMPv3.

- SNMPv1

  SNMPv1 supports community name-based and MIB view-based access control.
- SNMPv2c

  SNMPv2c supports community name-based and MIB view-based access control.
- SNMPv3
  - SNMPv3 inherits the basic functions of SNMPv2c, defines a management frame, and introduces a User-based Security Model (USM) to provide a more secure access control mechanism for users.
  - SNMPv3 supports user groups, user group-based access control, user-based access control, and authentication and encryption mechanisms.

NMS

The device adopts Huawei iManager U2000 network management system. It supports SNMPv1/v2c/v3 and the client/server architecture. The network management system can run independently on many operation systems, such as Windows NT/2000/XP, UNIX (Sun, HP, and IBM). The device also provides a multi-lingual graphical user interface.

The U2000 can be seamlessly integrated with the NMS provided by the other fixed network telecommunications devices developed by Huawei, ensuring uniform management of multiple devices. In addition, the U2000 can be integrated with the widely applied NMSs such as HP OpenView, IBM NetView, What's up Gold, and SNMPc, ensuring uniform management of devices of different vendors. The U2000 manages topologies, faults, performance, configuration tools, logs, users and user security, QoS policies, and VPN services in a real-time manner. The device can download, store, modify, and upload configuration files on the U2000, and software of the device can be upgraded through the U2000.

LLDP

The Link Layer Discovery Protocol (LLDP) is a Layer 2 protocol defined in IEEE 802.1ab. LLDP specifies that the status information is stored on all interfaces and the device can send

its status to the neighbor stations. The interfaces can also send information about changes in the status to the neighbor stations as required. The neighbor stations then store the received information in the standard SNMP MIB. The NMS can search for Layer 2 information in the MIB. As specified in the IEEE 802.1ab standard, the NMS can also discover unreasonable Layer 2 configurations based on information provided by LLDP.

When LLDP runs on the devices, the NMS can obtain Layer 2 information about all the devices to which it connects and detailed network topology information. This is helpful to the rapid expansion of the network and acquirement of detailed network topologies and changes. LLDP also helps discover unreasonable configurations on networks and reports the configurations to the NMS. This removes incorrect configurations in time.

