



Recommendations

- Huawei Learning Website
 - <http://learning.huawei.com/en>
- Huawei e-Learning
 - <https://ilearningx.huawei.com/portal/#/portal/EBG/51>
- Huawei Certification
 - <http://support.huawei.com/learning/NavigationAction!createNavi?navId= 31&lang=en>
- Find Training
 - <http://support.huawei.com/learning/NavigationAction!createNavi?navId= trainingsearch&lang=en>



More Information

- Huawei learning APP



Huawei Certification

HCIP-Routing&Switching

**Implementing Enterprise Network
Engineering Project
V2.5**



Huawei Technologies Co.,Ltd.

Copyright © Huawei Technologies Co., Ltd. 2019.

All rights reserved.

Huawei owns all copyrights, except for references to other parties. No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

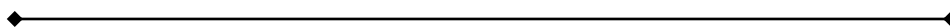
Trademarks and Permissions



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



Huawei Certification

HCIP-Routing&Switching Implementing Enterprise

Network Engineering Project

Version 2.5

Huawei Certification System

Relying on its strong technical and professional training and certification system and in accordance with customers of different ICT technology levels, Huawei certification is committed to providing customers with authentic, professional certification, and addresses the need for the development of quality engineers that are capable of supporting Enterprise networks in the face of an ever changing ICT industry. The Huawei certification portfolio for routing and switching (R&S) is comprised of three levels to support and validate the growth and value of customer skills and knowledge in routing and switching technologies.

The Huawei Certified Network Associate (HCIA) certification level validates the skills and knowledge of IP network engineers to implement and support small to medium-sized enterprise networks. The HCIA certification provides a rich foundation of skills and knowledge for the establishment of such enterprise networks, along with the capability to implement services and features within existing enterprise networks, to effectively support true industry operations.

HCIA certification covers fundamentals skills for TCP/IP, routing, switching and related IP network technologies, together with Huawei data communications products, and skills for versatile routing platform (VRP) operation and management.

The Huawei Certified Network Professional (HCIP-R&S) certification is aimed at enterprise network engineers involved in design and maintenance, as well as professionals who wish to develop an in depth knowledge of routing, switching, network efficiency and optimization technologies. HCIP-R&S consists of three units including Implementing Enterprise Routing and Switching Network (IERS), Improving Enterprise Network Performance (IENP), and Implementing Enterprise Network Engineering Project (IEEP), which includes advanced IPv4 routing and switching technology principles, network security, high availability and QoS, as well as application of the covered technologies in Huawei products.

The Huawei Certified Internet Expert (HCIE-R&S) certification is designed to imbue engineers with a variety of IP network technologies and proficiency in maintenance, for the diagnosis and troubleshooting of Huawei products, to equip engineers with in-depth competency in the planning, design and optimization of large-scale IP networks.

CONTENTS

Network Planning.....	1
Network Design	31
Network Implementation.....	154
Network Maintenance	195
Network Troubleshooting Overview	224
Troubleshooting Common Network Faults	262
Network Troubleshooting Scenario Cases.....	332
Network Optimization	357
Network Migration.....	381



Network Planning



Foreword

- Network planning is the beginning of a network project. A sound network planning creates a good environment for the implementation of follow-up projects.
- During the network planning, we make analysis on project background, make clear customers' requirements and objectives, and determine the project's technological roadmap.

- During the network planning, we make analysis on project background, make clear customers' requirements and objectives, and determine the project's technological roadmap.
- Network planning reviews a project from a macro view, and is abstract. No detailed technology is involved at this phase. And planning aims to set a framework for the entire project, which will add more details and implement them in the future guided by this framework.
- Network planning determines the general orientation, which directly influences project achievements.



Objectives

- Upon completion of this section, you will be able to:
 - Understand the content of network planning
 - Master the method of network planning
 - Perform network planning properly

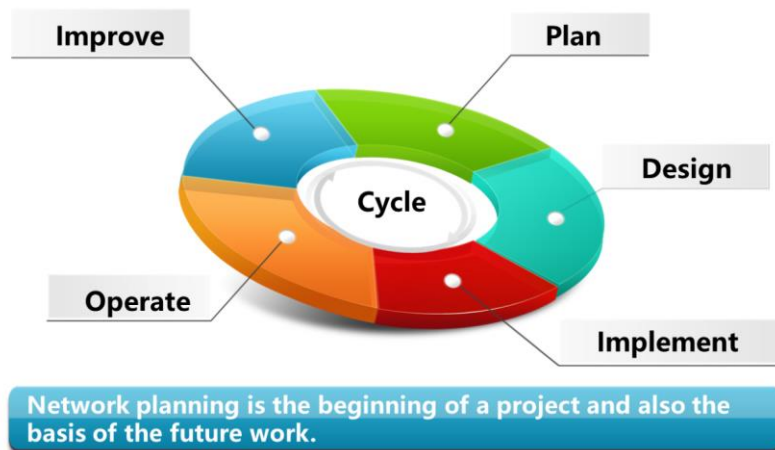


Contents

- 1. Network Planning Overview**
2. Project Background
3. Project Objectives
4. Project Technological Roadmap
5. Project Cases



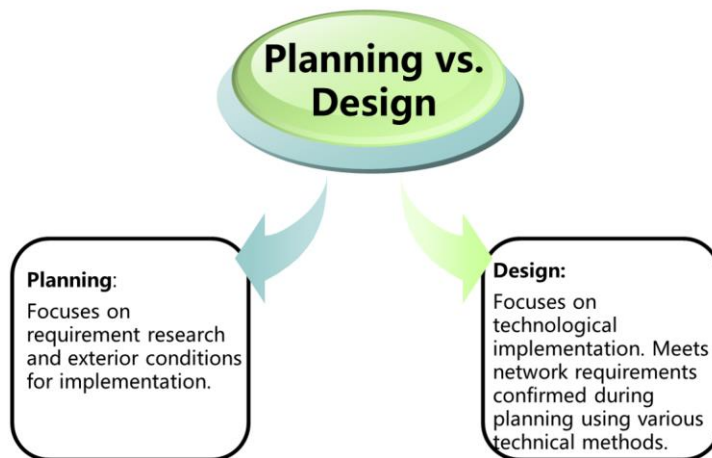
Positioning



- Network planning is the beginning of a project. Sound planning will be a solid foundation for future implementation. The planning details are as follows:
 - Setting a project's objectives is the basis for network planning. The objectives must be definite and measurable, and cannot be a general and blurry concept.
 - Grasp the general background of the project during planning, ensuring a sound exterior environment for smooth development.
 - Determine the work scope, which is the prerequisite for budgets and resources allocation. It defines responsibilities for matching projects and relevant systems respectively.
 - Make budgets according to objectives, scope, and content of the project.
 - Clarify guiding principles of network design, providing guidance and basis for future work.
- Feasibility research is required for large-scale innovative network projects during network planning. We need to make analysis and verification on economical aspects of the project and technologies to be used. This helps guarantee return on investment (ROI) and the total project success.



Network Planning vs. Network Design



- Network planning and network design are two phases at the beginning of a project. These two phases often cause confusion. In fact, planning is more macroscopic, focusing on what to do and what conditions are required, and only giving a general technological direction. In contrast, design work focuses on detailed technological implementation and procedure.
- Theoretically, planning and design are implemented in a certain sequence. In reality, however, the two phases combine with each other closely. For example, budgets, cycle, and personnel arrangement are included in project planning, which is related to detailed project design and operations. Therefore, project planning involves estimation about later implementation details.



Network Planning Objectives

Project Background

Clarify the exterior conditions for a network project.

Requirement Determination

Determine objectives of a project.

Technological Orientation

Select the technological roadmap.

- We must grasp the background and exterior conditions during network planning. A network project is not an independent system. It facilitates services, requires matching facilities, and demands cooperation and assistance from relevant O&M personnel. In this way, the project can be approved by end users finally. Therefore, we must determine the background and exterior conditions by doing research, laying a sound foundation for project implementation.
- We must clarify customer requirements. In most cases, customers have a general and blurry design roadmap instead of comprehensive and accurate project objectives. In this phase, the project team must communicate with customers in a more thorough way to understand their requirements so as to set clear objectives for future design.
- Detailed technological design is not involved in network planning. In spite of this, we still need to communicate with customers to define the technological orientation and roadmap, and understand the customer's technological inclination, major concerns, and taboos. This will avoid detours and prevent us from wasting time and human resources.



Network Planning Method



- The major network planning method is survey, which aims to collect relevant information. It falls into several forms: 1. Talks and queries. This method provides customers with sound experience and allows for flexible topic setting, which causes heavy workload and requires much negotiation on time. Usually, we use this method for named accounts. 2. Forms. This method requires us to design questions in advance for a wide range of respondents. 3. Instant communication tools such as emails. However, this method is informal. It is recommended that this method be used as a supplement to project survey after we have been more familiar with customers. 4. Working together. It is recommended that we work with customers for some time to know their service process, network requirements, and current pain points. In this way, we can obtain the firsthand materials about the project.
- After obtaining all the information about the network project, we need to make a preliminary analysis on the information, and evaluate feasibility of all requirements and their relationships. For example, balance and compromise between network performance and economical aspects of the project, or network security and ease of use. We need to discuss with customers on the analysis results, and strive to reach a consensus on focuses and compromise methods. In addition, we also have to communicate with customers to confirm some prerequisites for project implementation, such as some permits to enter the equipment room and relevant environmental standards. We must make preparations in advance for future project implementation.
- In the end of the planning phase, we need to summarize all the firsthand materials and consensuses, and send the summary as a report to both customers and members of the project team. The report will be used as the objective guiding the future work and serves as the basis for coordination with customers.

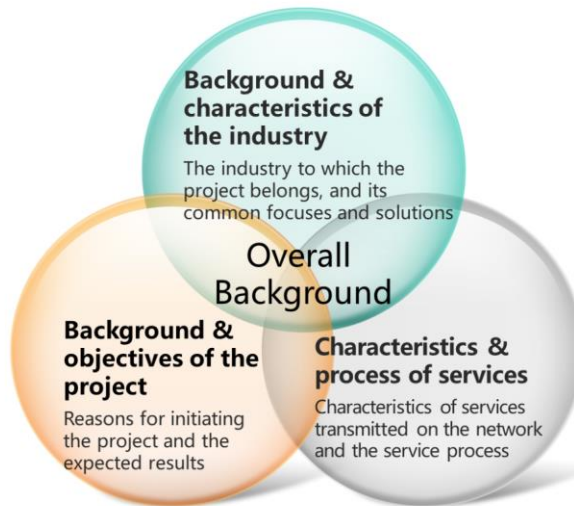


Contents

1. Network Planning Overview
- 2. Project Background**
3. Project Objectives
4. Project Technological Roadmap
5. Project Cases



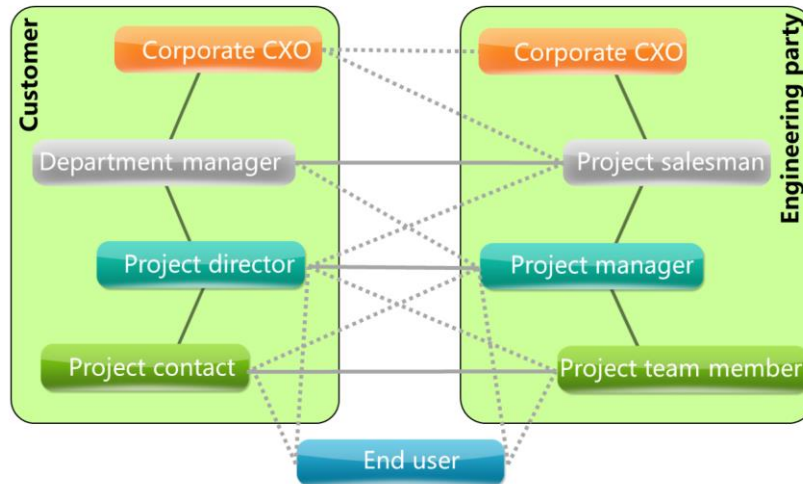
Project Background



- Before initiating the project requirement survey, we'd better get to know the project background. On this basis, we can conduct pertinent surveys and prevent common-sense mistakes to leave a good impression on customers.
 - Network has been applied to all walks of life, and forms a part of corporate services. Network solutions vary with services of a certain industry. We can grasp the industry situation, characteristics, and typical solutions for guiding future work.
 - Before initiating the project, we need to cooperate with sales personnel to understand the customer's objectives. In such a way, we can grasp key points and carry on work centering on the objectives. We can also do work in a flexible manner and optimize some details to save investment and improve efficiency.
 - Enterprise's networks are used for transmitting detailed services. Having a basic understanding of these services, data flow direction, and data flow characteristics can help us propose pertinent solutions in later design and implementation to mitigate risks.



Customer's Organizational Structure



- A customer has its own organizational structure consisting of many departments and employees. Departments may hold various opinions on a project based on their positions. In the preliminary phase of a project, getting a general understanding of the customer's organizational structure and knowing the requirement differences help us grasp key points and make right decisions during project implementation.
 - After a project is initiated, the customer usually sets up a project team leading by two key roles: the project director and the project contact. The project director is responsible for technical work such as determining the technical solution. The project contact is responsible for routine affairs such as leading engineers into and out of work places. During planning and design, we communicate more with the project director, while during project implementation, we communicate more with the project contact. In some small projects, the two roles may be assumed by the same person.
 - Business decisions are made by a higher level of personnel of the customer. They may be the leaders of the project department, or the executive leaders in charge of the work. Communication in this link is usually conducted by salesmen or executive leaders from the project implementation party. Technical personnel grasp the general situation to avert uncontrollable accidents in some special cases.
 - Generally, the end user of a project is not the team of the customer. In other words, the end user is the customer of the team. It is a common goal for both the customer and the engineering party to be recognized by the end user.
- A network project involves different departments of the customer and relevant personnel in different phases. Therefore, it is of importance to know the whole project operation procedure of the customer, collect information about departments and personnel involved in each phase, especially authorized signatory, and obtain recognition and cooperation from them.



Determining the Project Scope

Engineering boundary:
Responsibility division between the project and other matching systems

Functional boundary:
Functions and modules to be realized by a project

Coverage:
Geographical range

- During the project planning, we need to specify the project scope. Much of the later work is evaluated based on this scope including the workload and budgets. In detail, the project scope can be divided into the following aspects:
 - **Coverage:** Network coverage. For example, we must be sure about whether the network covers the whole country or just a province, or whether the network extends to counties or townships. These issues must be determined before the project is implemented. If we are handling a campus network project, we need to know which buildings are included in the project scope, and how many network sockets are located in each building.
 - **Engineering boundary:** A network project cannot be independent. The installation of network devices requires cooperation from other systems, such as equipment room engineering, matching power supply, air conditioning, and weak current systems. During project planning, we must ensure the responsibility division between the project and other matching systems to avoid later buckpassing issues.
 - **Functional boundary:** We hardly handle a project starting from scratch. Many reconstruction projects are initiated to realize certain functions, such as accessing a service system or reconstructing a network to improve security. During the project planning, we must confirm functions to be realized by the project, and regard related functions as prerequisites or exterior conditions.



Phases and Cycle



- Work Breakdown Structure (WBS)
 - The WBS divides the scope of the project work into smaller, manageable components.
- Gantt chart
 - The chart sorts the activities in time rank after dividing the work plan, and combines activities with time points in a chart.



- A project usually goes through the whole process from project initiation, planning, design, implementation, trial operation, acceptance, to O&M. In each phase, iconic events indicate where the phase starts and ends respectively.
- Although some projects may contain specific steps, generally, a complete procedure contains the above phases.
- Time arrangement and management of a project are implemented according to a set of systematic methods. The most common method is dividing the work into phases, making an estimation about each phase, and arranging work within a phase comprehensively to complete the whole work plan. The plan is usually presented in the Gantt chart.



Matching Systems

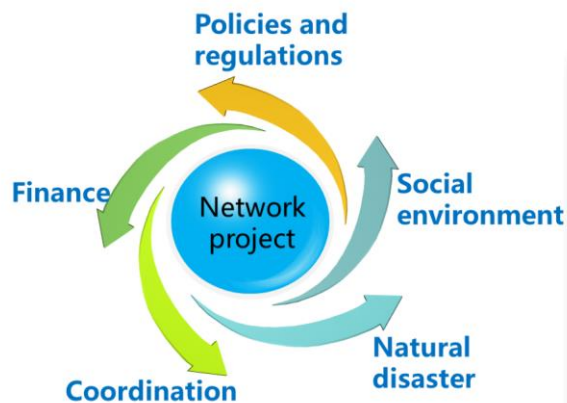


- These systems are closely related to the project.
- These systems need to be focused on and confirmed by the project team.

- A network project cannot be independent. It requires coordination with many relevant systems, which are not aimed to be resolved by the project but are critical to successful project implementation. Therefore, during the project planning, we need to specify the boundary between the project and relevant systems.
- Relevant systems can be classified into the following types:
 - Conditions for device installation: These conditions include space, power supply, and air conditioning. Parameters about all network devices must be provided, including physical dimensions, power consumption, weight, and working temperature range. The equipment room must conform to specific conditions such as load bearing capacity, power supply, and air quality requirement.
 - Network cables: These are connection lines used in the project, including cabling for the LAN in the charge of the customer and the leased WAN. Cabling for the LAN is regarded as an independent weak current project.



Exterior Risk Control



- Project risks refer to series of uncertain factors that influence progress, efficiency, profit, and objectives of the project.
- Exterior risks are usually out of control of the project team.

- A project is in a changing and complicated environment. Usually, a project team can control or exert impact on some events related to the project directly, but it can only prevent or avoid risks caused by the general background such as policies and trends.
- Common exterior risks are as follows:
 - Policies and regulations: Any project must conform to policies and regulations, especially some international projects. We must know and abide by local laws and regulations, take notice if they are changed, and take the actual law environment into consideration.
 - Social environment: Team members must understand and apply to the local social environment including social security, religious faith, custom, and daily life.
 - Natural disaster: These disasters include but are not limited to earthquakes and storms. A disaster may hinder a project's progress to a small extent, and ruin the whole project to a large extent.
 - Finance: Macroeconomic changes may cause fluctuations in project finances. For example, changes in the exchange rate, adjustments in the national interest rate, and currency inflation will lead to changes in the profit margin of the project.
 - Matching coordination: The project involves some external coordination systems such as the foreign trade cycle as well as quality and schedule of matching projects.
- In the planning phase, we must identify these risks and go all out to lessen the possibility of the project failure caused by these risks. For example, in a project contract, we can classify some cases into force majeure clauses. Or in a project planning scheme, we can define responsibilities of each party, provide definite engineering interfaces, and propose quality requirements.

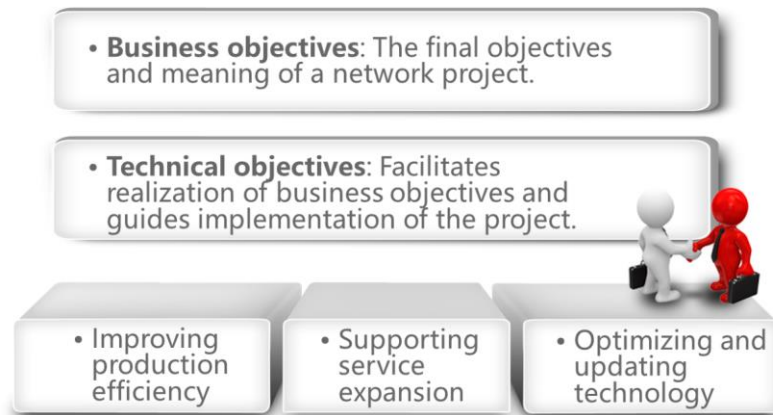


Contents

1. Network Planning Overview
2. Project Background
- 3. Project Objectives**
4. Project Technological Roadmap
5. Project Cases



Project Objectives



- The business significance is the fundamental reason for initiating a network project, including adding profits, cutting costs, and improving production efficiency.
- In the project planning phase, clarify the customer's business requirements and help the customer realize his objectives. All these factors contribute to a project success.
- Typical business objectives of a network project are listed as follow:
 - Cutting the enterprise's OPEX and improving work efficiency of employees.
 - Accelerating service processing and improving the enterprise's market competitiveness.
 - Supporting service expansion, and network capacity extension into new areas or capacity upgrade to higher performance.
 - Supporting new service development to extend network functions.
 - Improving network reliability to ensure service stability.
 - Reducing the total communication costs.



Project Budgets

ROI

Business objectives must involve ROI.

Project budgets refer to costs for implementing a project, including financial, labor, and material costs.

- The objective is to improve project management and increase ROI.

- Method
 - Top-down
 - Bottom-up

- Determining the project budgets is important in the planning phase.
- Granularity of project budgets is closely related to certainty and granularity of project planning.
- Determining the project budgets is important for customer's financial management. Combining objectives with costs facilitates cost control and improvement of capital use efficiency.
- The two most common methods of making budgets are as follow:
 - Top-down: Project costs are estimated according to experience and historic data.
 - Bottom-up: The total budgets consist of fees of each part of a project.



Composition of Cost

Total Cost of Ownership (TCO) =

Construction Investment + O&M + Optimization & Reconstruction

Construction Investment

- One-off investment
- Closely related to project objectives
- Including:
 - Device costs
 - Matching facility costs
 - Engineering costs

O&M

- Constantly occurs during the network cycle
- Including:
 - Energy consumption
 - Line maintenance
 - Repairing
 - Personnel costs

Optimization & Reconstruction

- Frequently occurs during the network cycle
- Can be operated as another project
- Difficult to calculate the cost

- A network project's budgets involve many aspects. The TCO of constructing and operating a network consists of the following aspects:
 - Construction investment: The network construction fees are one-off investment, which is closely related to project objectives. The construction investment contains device fees, construction fees of matching facilities, and engineering costs.
 - O&M: After network construction is completed, O&M requires continuous investment, including energy consumption fees, line maintenance fees, regular device repairing fees, and O&M personnel costs.
 - Optimization & reconstruction: During a network cycle, there will be multiple times of optimization and reconstruction, involving line capacity expansion, device upgrade, and network architecture reinforcement and hardening. A reconstruction task can be operated as an independent project. Since reconstruction is based on actual situation, which cannot be predicted in the initial phase, costs of optimization and reconstruction is difficult to evaluate.



Obtaining Original Quotation

- Device purchase fees:
 - Obtain quotations of Huawei devices from CSPs or ASPs
- Line construction and leasing fees:
 - Obtain quotations from carriers
- Devices such as racks and UPS:
 - Contact salesmen from corresponding vendors

- We need to obtain the original quotations for relevant fees to make construction budgets. Such quotations can be obtained through the following channels.
 - You can log in to the Huawei official website (<http://e.huawei.com/cn/how-to-buy>) to find the product procurement channels and submit procurement requirements on this page, or obtain quotations from Huawei partners.
 - Line construction fees are an important part of costs. In a LAN project, customers usually deploy lines on their own. Cabling is operated as an independent weak current project matching the network project, and is given quotations by the contractor. In a WAN project, customers usually rent carrier's links. Therefore, you can contact local carriers to know about the link type and price. In terms of this area, carriers have special department that is responsible for government and enterprise customers.
 - In a network project, customers may purchase some matching devices, such as racks and power systems. In this case, the project contractor usually contacts relevant vendors, hands over responsibility of providing relevant devices and their installation and commissioning to suppliers, and makes an overall quotation.

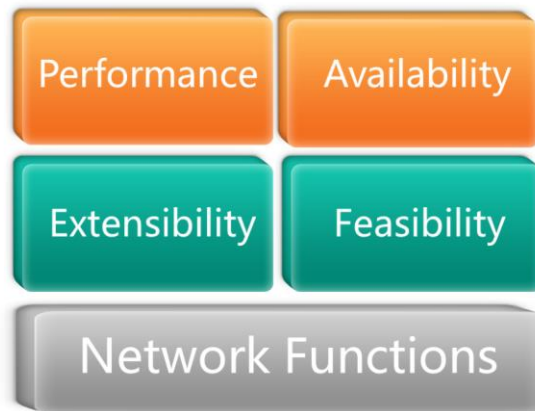


Contents

1. Network Planning Overview
2. Project Background
3. Project Objectives
- 4. Project Technological Roadmap**
5. Project Cases



Technological Requirement Analysis



- The project objectives are realized through detailed technologies. Usually, we need strike a balance between technological standards and business objectives, such as a balance between high performance and cost. Technological objectives that need to be included in the planning phase are listed as follows:
 - Function: This is the most fundamental technological objective, which serves as a prerequisite for other technological objectives. It is often regarded as one of the project objectives.
 - Performance: This is a key technological indicator, including many aspects such as throughput (bandwidth). In terms of requirements, network services require specific amount of throughput; technologically, line bandwidth and device performance determine the throughput. When talking about network throughput, we must take bandwidth use efficiency into consideration to ensure high ROI. Network performance also includes parameters such as latency and packet loss rate.
 - Availability: This indicates the tolerance of customers for network faults. When service development relies on network systems, customers require high network availability. For example, routine faults must not affect service operation. Recoverability is closely related to availability, and refers to the difficulty level of network recovery when disastrous faults occur on the network.
 - Extensibility: Based on the customer's service expansion plan in the next few years, we must reserve sufficient margins for service expansion. Extensibility can be measured by two criteria: one is the increasing number of sites and a growing number of access users, and the other is increasing requirements for higher performance and more service traffic.
 - Feasibility: We must take rationality and feasibility into consideration for implementing a project. Feasibility should be based on the current technological development and actual realization capability. We must never specify unrealistic indicators and requirements.



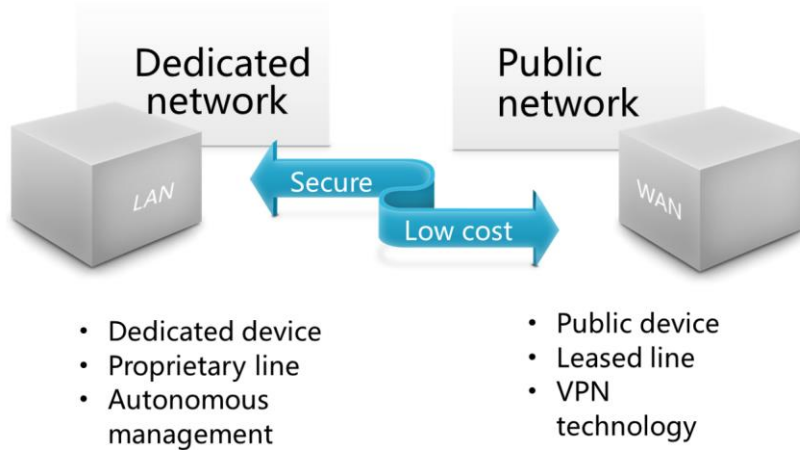
Service Traffic Characteristics Analysis



- To design a network that truly meets requirements, we must deeply understand service traffic to be transmitted on the network. We can analyze traffic characteristics to meet performance requirements and improve ROI.
- Traffic characteristics
 - Collect statistics on services transmitted on the network, and plan about traffic paths for each type of service.
 - Classify various types of network services including unicast, multicast, and broadcast traffic, or system traffic, protocol traffic, and application traffic.
 - Based on the requirements for various types of traffic, make an estimation about service capacity on each network segment.
- Behavior characteristics
 - Evaluate network behavior of end users. Measure and classify the types of user applications such as common Internet service, P2P application, and terminal service.
 - Draw the time curve of network traffic to know the traffic value during peak and valley time and other time segments.
- QoS requirements
 - Evaluate QoS requirements of each service, and arrange services in a priority order.
 - Specify QoS indicators of each service including bandwidth, latency, and jitter.
 - Determine which QoS model should be used.



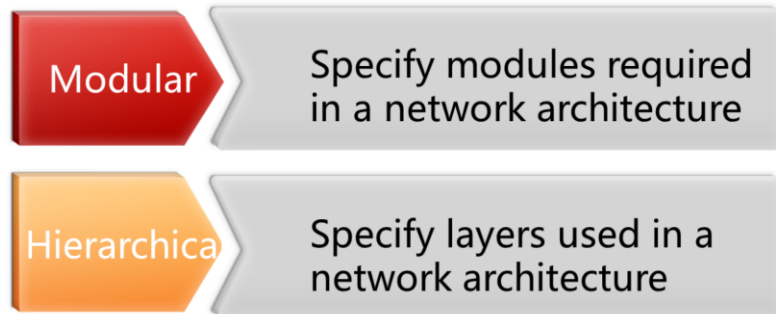
Dedicated Network vs. Public Network



- During network planning, we must know whether the network is dedicated or built on a public service platform. A dedicated network indicates that the customer has total property ownership of network infrastructure. A public network indicates that the customer leases part of devices on the public network, or constructs a Virtual Private Network (VPN) on the public network.
- A dedicated network is secure and controllable while a public network has a low cost.
- LANs of a customer are usually self-built and self-managed dedicated networks. Cross-WAN lines are generally leased public lines due to low cost.
- A special method is to construct VPNs on the public network using specific technologies, maintaining low costs while ensuring security.



Network Modules



- Generally, current networks are based on modular and hierarchical design. During network planning, we must specify which functional modules and hierarchical model are required.
- Common network modules include campus network modules, WAN backbone modules, network egress modules, data center modules, and wireless access modules. Select specific modules based on the project requirements.
- In a network module, we usually use the hierarchical structure. Traditionally, the three-layer network structure is employed. Currently, flattened network with a two-layer structure is popular. Therefore, we must determine a hierarchical structure during network planning.



Contents

1. Network Planning Overview
2. Project Background
3. Project Objectives
4. Project Technological Roadmap
5. **Project Cases**



Scenario 1

- Once a time, the department manager of a network integration company assigns a network project to Mr Wang and Mr Song. Mr Wang takes the role of an engineer and Mr Song assumes the responsibility of a sales manager.
 - Q1: What can Mr Wang do in the next phase?
 - Q2: What should Mr Wang prepare for the project?

- Generally, project tasks are assigned by the upper-director to the technical engineer. Small companies may work in a more flexible manner. For example, salesmen can cooperate with technical personnel to complete the project.
- Basically, a project team consists of a sales manager and a technical engineer. In the initial phase of a small- or medium-sized project, only two people are involved, and more people will be arranged for it in later phases. In this case, Mr Wang should cooperate with the sales manager after being assigned with the project. Mr Wang can obtain basic information about the customer from the sales manager to know more about the project such as the customer's industry background and the project objectives. Due to differentiated orientation, the sales manager does not focus on detailed technical implementation. In the initial phase, the sales manager also does not grasp many project details. Therefore, Mr Wang, as the technical responsible person, needs to work with the sales manager to track and survey the project.
- After obtaining the customer's basic information, the technical engineer and the sales manager should arrange customer visits. The visit schedule and contact issues are in the charge of the sales manager. Mr Wang, however, should grasp relevant information and prepare inquiry questions so that he can inquire the right person in appropriate occasions. As mentioned before, the project survey involves project background, project objectives, and technological roadmap.



Scenario 2

- Mr Wang goes with the sales manager to the customer for project survey.
 - Q1: What questions should Mr Wang prepare? Who should be talked with to find the answers?
 - Q2: Some questions may not have definite answers, so how should they handle it?

- When we initiate a project officially, customer visit is the most basic step. In the initial phase, we will have multiple times of contacts with the customer and many times of surveys. The first time survey demands a lot of preparation work in order to leave a good impression and promote subsequent work.
- In general, all the content in this slide should be involved during project planning. Though parts of them are not obtained from the survey, issues including project objectives, project scope, project progress, personnel organization, and matching projects must be determined through negotiation with the customer. Division of roles also exists within the customer. The customer's project manager will negotiate with higher-level leaders about the budgets, progress, and engineering scope. The project manager usually makes the final decision on some technical details such as network parameters while the project contact person is responsible for onsite engineering, and handover of materials and documents.
- During the survey, the customer may not provide answers directly due to incomplete documentation or unfamiliarity with relevant technical issues. In this case, the engineering party must cooperate with the customer to jointly find a solution. If technical issues are involved, the engineering party must give detailed explanation, present comparisons, and guide the customer to make a choice.



Quiz

1. Which of the following issues are going to be resolved during network planning?
 - Determining the technical solution
 - Knowing about the project background
 - Determining the project requirements
2. Which of the following issues needs its scope defined within a project?
 - Functional border
 - Engineering border
 - Coverage

- Answer: BC.
- Answer: ABC.



Thank You

www.huawei.com



Network Design



Foreword

- In the design phase, perform network designs based on the project requirements and guidelines specified in the planning phase.
- In the design phase, determine device selection, technological roadmap, network functions, and performance specifications.



Objectives

- Upon completion of this section, you will be able to:
 - Understand common network types
 - Understand each layer of the network design
 - Understand common products and technologies
 - Be familiar with advantages and disadvantages of common protocols
 - Be familiar with comprehensive applications of each technological module
 - Master the network design methodology



Contents

1. **Overview**
2. Physical Network Design
3. Logical Network Design
4. Other Network Technologies
5. Overall Technological Solution



Network Design Overview



In the network design phase, customer requirements obtained in the network planning phase are implemented through technological methods.



Network design generally follows the modular design principle. After design, network modules are integrated.

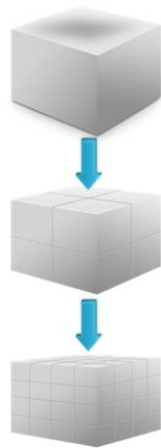


Network design deliverables must be standard, detailed, clear, and can be implemented.

- The network design is the second phase in a network construction project. In this phase, customer requirements obtained in the network planning phase are implemented through technological methods.
- Network design usually follows the modular design principle. During network planning, determine the modules used on networks and the specific requirements on each module, and then perform detailed design for each module during network design. The hierarchical architecture is often used in each module.
- Network design deliverables must be standard, detailed, clear, and can be implemented.
- The network design requires a network designer to:
 - Be familiar with network products and select proper products during solution design.
 - Understand network technologies and use proper ones during solution design.
 - Have certain project experience and understand each key link in the project implementation process.



Network Design Content



Physical network design:

- Physical topology design
- Hardware device selection
- Interconnection link selection
- Basic device configurations

Logical network design:

- LAN design
- WAN design
- Routing structure design
- Network egress design
- High availability design

Network subsystem design

- Network security design
- VPN design
- WLAN design
- Data center design
- Network management design

Key points of the design



- In this chapter, the network design is composed of three parts:
 - Physical network design: This involves physical network topology, and hardware device and link selection. This design is often relevant to project budgets and network performance. As the foundation of the entire network, all subsequent designs are based on the result of this phase.
 - Logical network design: Networks are designed from the perspective of protocols and network layers. A network can be divided into a Layer 2 or Layer 3 network by protocol layers. A Layer 2 network includes the LAN and WAN based on the region, while a Layer 3 network is designed based on IP addresses and routing protocols. Some special technologies used at the enterprise network egress will be discussed separately here. High availability design must be focused on in the network design.
 - Other network subsystems: In addition to the basic network architecture, other subsystems exist on an enterprise network, including network security, wireless network, data center, and network management subsystems. These subsystems are common functional modules on the enterprise network.



Key Points of Network Design

Function & performance	Connectivity, throughput, delay, jitter, and bit error rate (BER)
Cost-effectiveness	Human, material, and financial resources, as well as the construction period
Reliability	MTBF, MTTF, and MTTR
Scalability	Topology, network address, and protocol
Security	Asset, risks, and countermeasures
Manageability	SNMP, NETCONF, SDN, GUI, and NMS

- During the network design, you always need to focus on network requirements determined in the network planning phase and select proper technologies. The designed network solution needs to follow these points:
 - High performance: The balance between high performance and cost-effectiveness must be achieved. Network performance can be described using available bandwidth, delay, jitter, BER, usage, etc.
 - Cost-effectiveness: The network solution must be provided based on the customer's budget.
 - Network reliability: It refers to the ratio of normal working time of a network, which is relevant to availability and restorability. Redundancy is often used to improve system availability.
 - Scalability: It refers to the capability that networks can meet the requirements of future development.
 - Security: During network design, you need to consider security to improve network continuity and prevent information leakage.
 - Manageability: Network management includes the management of devices, configurations, faults, and accounting. Currently, the SNMP-based network management system (NMS) is most commonly used.
 - Note:
 - Mean Time Between Failures (MTBF)
 - Mean Time to Failures (MTTF)
 - Mean Time to Repair (MTTR)

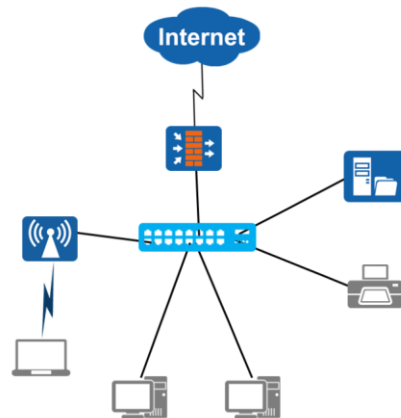


Contents

1. Overview
- 2. Physical Network Design**
 - Typical Topology
 - Device Selection
 - Media Selection
 - Network ID
3. Logical Network Design
4. Other Network Technologies
5. Overall Technological Solution



Typical Architecture of a Small-Scale Network



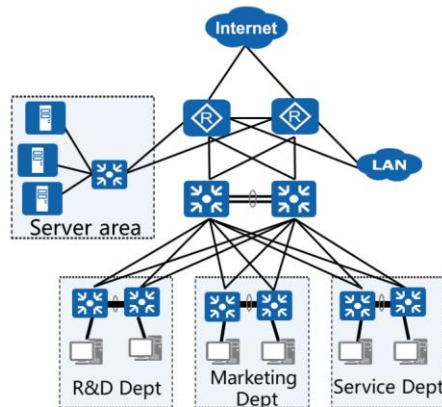
Characteristics:

- Small number of users
- Only one location
- Not hierarchical
- Simple requirements

- A small-scale network is applicable to scenarios where the number of access users is small (< 100). The network covers only one location without using the hierarchical architecture, and is often used to provide internal resource sharing (for example, printers and files) and Internet access.
- Internet and WLAN access are common requirements for current networks. For a small-scale network, the following functions need to be implemented:
 - In most cases, use routers or firewalls to connect to the Internet, and deploy network address translation(NAT) to translate private IP addresses into public IP addresses.
 - Use Fat APs to provide wireless access, and WEP or WPA for authentication.
- Select devices with multiple functions integrated, for example, AR G3 routers that can provide functions such as switching, routing, WLAN, and xDSL/EPON access.



Typical Architecture of a Medium-Scale Network

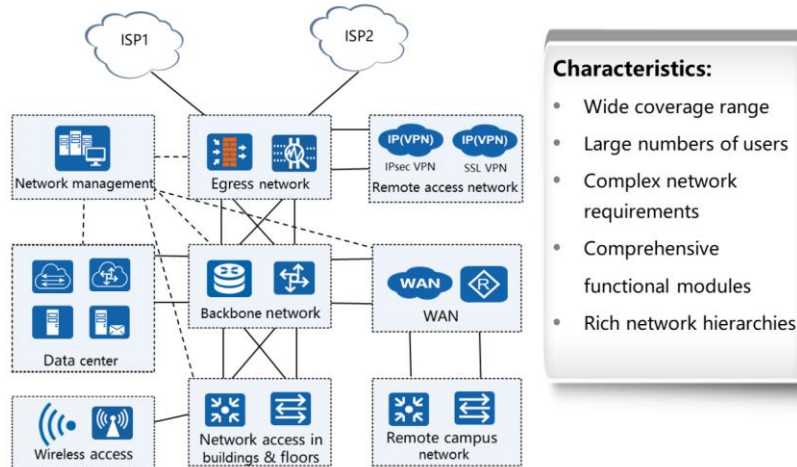


Characteristics:

- Medium scale
- Most commonly used
- Multiple functional areas
- Preliminary hierarchical architecture

- Medium-scale networks are most commonly deployed in projects. In most cases, enterprise networks are medium-scale networks, which support access of hundreds or thousands of users.
- The modular design is introduced to medium-scale networks, but the number of functional modules is small. Generally, areas are divided based on service requirements, without set standard rules.
- Medium-scale networks need to support more users, so the hierarchical design is used to improve network scalability.

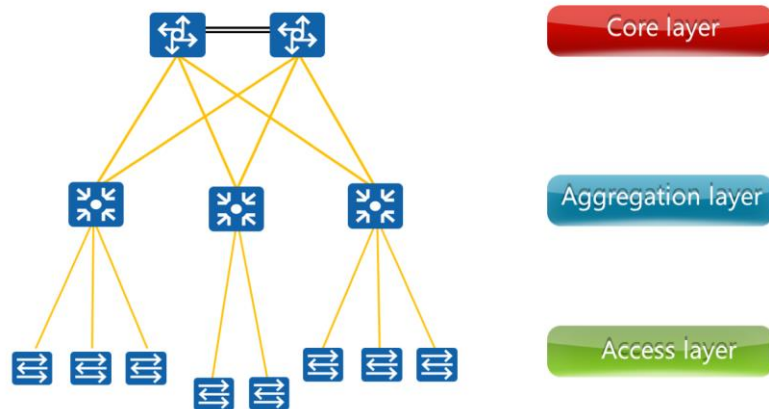
Typical Architecture of a Large-Scale Network



- Large-scale networks are applicable to large enterprises, and have the following characteristics:
 - Wide coverage: Large-scale networks can be campus networks that cover multiple buildings, municipal networks connecting multiple campuses in a city through the WAN, or nationwide networks that cover several provinces.
 - A large number of users: A large-scale network can deliver network access for thousands or millions of users, and can be extended based on the number of users.
 - Complex network requirements: Large-scale networks support multiple types of services, such as real-time, non-real-time, voice, and video services.
 - Comprehensive functional modules: They are provided by large-scale networks to meet various service demands.
 - Network layers: The scalability of network structures is implemented through proper network layer layout. For example, proper network layers are used so that the network can allow access of more users.
- The construction of large-scale networks is not completed at a time, and often involves several phases including construction, expansion, reconstruction, and maintenance.



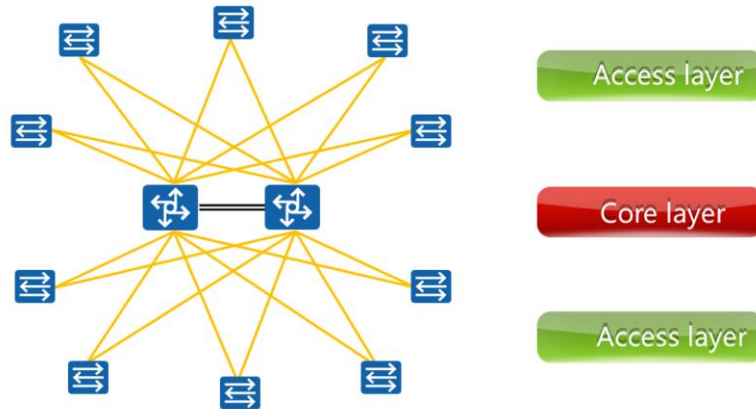
Hierarchical Network - Three-Layer Architecture



- In medium to large networks, the modular design is usually used to split network functions. To ensure network flexibility and scalability within each module, the hierarchical architecture is generally used, for example, in a campus network that provides access services for a large number of users.
- Traditional networks contain the core, aggregation, and access layers. The core layer provides high-speed data channels, the aggregation layer converges traffic and controls policies, and the access layer offers various access modes to terminals.
- This three-layer architecture delivers good scalability, and has been widely used in current networks, such as a large number of campus networks and WANs.



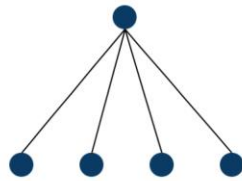
Hierarchical Network - Two-Layer Architecture



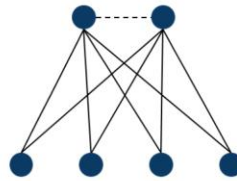
- With the change of service requirements and the development of network technologies, flattened two-layer networks are emerging. The two-layer architecture includes only the core and access layers, and raises new requirements on network devices as no aggregation layer exists. For example, core devices need to provide a higher port density for access from a large number of access devices.
- The two-layer architecture mainly applies to MANs, WANs, and data centers.



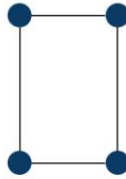
Common Network Topologies



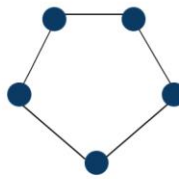
Star



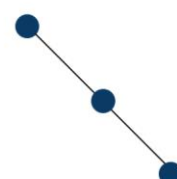
Dual-star



Square-shaped



Ring



Bus

- A large network often consists of multiple topology segments. Common network topologies include:
 - Star topology: common hierarchical topology where single-point failures may occur.
 - Dual-star topology: common hierarchical topology used for Layer 2 interconnection in a campus network, supporting redundancy.
 - Square-shaped topology: common hierarchical topology used for WAN interconnection, supporting redundancy.
 - Ring topology: used in some special protocols or in scenarios where the line resources are insufficient, supporting redundancy.
 - Bus topology: used when the line resources are limited, with low line utilization and no redundancy.



Case: Campus Network Topology

- A university needs to build a campus network to cover areas such as teaching buildings, dormitories, and canteens, as well as branch schools and equipment rooms.
 - How to define the campus network scale
 - How to design the campus network architecture
 - How to select the campus network topology

- The campus network in a university is a typical large-scale network (despite its limited coverage area) with a large number of access users and devices. The network needs to provide various services and network modules.
- Determine the modules used in the campus network first, and specify the network hierarchy for each of the following modules depending on the module scale.
 - Core module which functions as the central path of the entire network
 - Access module (teaching building, dormitory, and canteens)
 - Education network, WAN, and Internet access module
 - Data center module
 - Wireless access module
 - Network management and access authentication module
 - Other corresponding functional modules
- Use the star or dual-star topology, and select a corresponding redundancy structure based on network reliability and costs.



Contents

1. Overview
- 2. Physical Network Design**
 - Typical Topology
 - Device Selection
 - Media Selection
 - Network ID
3. Logical Network Design
4. Other Network Technologies
5. Overall Technological Solution



Network Device Classification



Layer 2 switch



Layer 3 switch

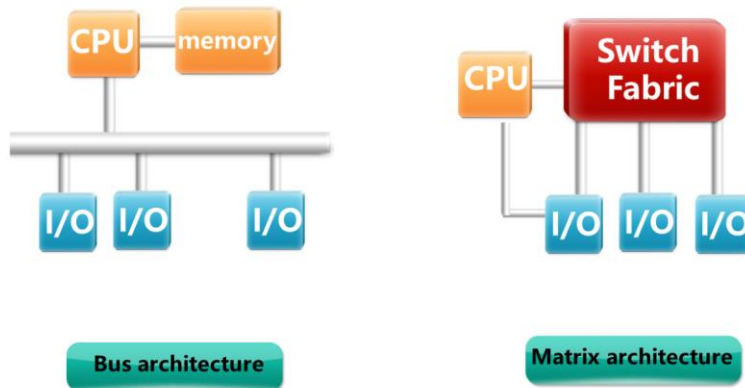


Router

- Network devices include switches and routers. Switches can provide network access for LAN users, and are classified into Layer 2 and Layer 3 switches based on whether the routing function is supported. Routers can provide connections between heterogeneous networks and the routing function.
- In addition to these devices, other types of network devices exist on current networks, such as firewalls, IDS/IPS, ACs, and APs. These devices will be described in corresponding slides.
- During the development of network technologies, some network devices are eliminated, such as hubs, bridges, token rings, and ATM switches.
- New network devices emerge with the development of network technologies, such as data center switches and SDN switches.



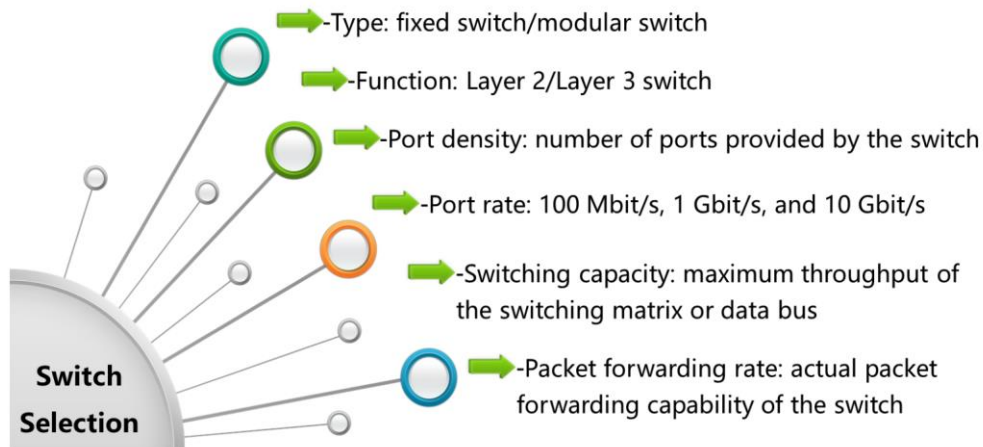
Architectures of Switches



- The current Ethernet architecture is switch-centric, while multiple methods such as bus and hub connection were used before.
- The commonly used switches can be classified into two types in terms of the architecture: switches using the bus architecture and switches using switching matrix (Switch Fabric).
 - Switch using the bus architecture: The bus architecture is the initial switching mode used by the switch. In this mode, all ports are connected to the switch's shared bus on the backplane, and each port occupies the bus to transmit data in a time-based sharing manner. The bus bandwidth is allocated for each port using a special bus arbitration algorithm. This structure is simple and cost-effective, but has poor scalability, which is mainly used for low-end switches.
 - Switch using switching matrix: Such switches can simultaneously exchange data on multiple ports, eliminating channel bottlenecks inside the switch. Currently, this structure is used in high-end switches.
- In addition to the two types of architectures, there are other architectures used by the switch, such as the memory sharing architecture.



Key Points for Switch Selection



- Currently, Layer 2 technology for LANs is generally Ethernet-based, so the switches described here are Ethernet switches.
- A vendor provides many switch models, each of which has different positions. Therefore, consider the following factors during switch selection:
 - Type: Switches are mainly classified into fixed and modular switches. In most cases, the configuration and number of ports on a fixed switch are fixed and are difficult to expand. Modular switches are based on chassis, and other components such as the power supply, engine, and interface cards can be independently configured based on requirements. Scalability of modular switches depends on the number of slots.
To improve scalability, multiple fixed switches can be integrated into one switch through a special card using stacking technology.
 - Function: The main difference lies in Layer 2 and Layer 3 switches. Other functions, such as link bundling, stacking, PoE, virtual functions, and IPv6, can also be different.
 - Port density: The number of ports on each fixed switch is generally fixed (24 or 48 access ports, and two to four uplink ports). For modular switches, the port density is related to the configured modules, and refers to the maximum number of ports supported in each chassis when highest-density interface cards are configured.
 - Port rate: The port rates supported by the current switches include 100 Mbit/s, 1 Gbit/s, and 10 Gbit/s.
 - Switching capacity: This varies depending on switch types, and is a theoretical value, which indicates the maximum switching capability that a switch may reach. For bus switches, the switching capacity refers to the bandwidth of the backplane bus. For switches using switching matrix, the switching capacity refers to the total interface bandwidth of the switching matrix. The current design of switches ensures that the switching capacity will not become the bottleneck of a switch.
 - Packet forwarding rate: This indicates the number of packets that a switch can forward in 1s. It is a measured result and indicates the actual forwarding performance of a switch. The Ethernet frame length is variable, but the processing capability for a switch to process each Ethernet frame is not related to the frame length. Therefore, if the bandwidth for a switch's port is fixed, the switch needs to process more frames and have a higher processing capability when the Ethernet frame length is shorter.
- For a specific switch, there are a large number of other parameters in addition to the preceding basic specifications, which are usually released on the official website of the vendor.



Huawei Fixed Switches



S2700: Layer 2 FE switch
This switch series provides 8, 16, 24, or 48 10M/100M self-adaptive access ports, as well as one to four GE uplink ports.



S3700: Layer 3 FE switch
This switch series provides 24 or 48 10M/100M self-adaptive access ports, as well as two GE uplink ports.



S5700: Layer 3 GE switch
This switch series provides 24 or 48 10M/100M/1000M self-adaptive access ports, as well as four GE/10GE uplink ports.



S6700: Layer 3 10GE switch
This switch series provides 24 or 48 10GE SFP+ optical ports.

- S2700 series switches: Layer 2 FE switches. This series provides a large number of models, which have 8, 16, 24, or 48 10M/100M self-adaptive access ports, and one to four GE uplink ports. Each model also supports different specifications in terms of PoE power supply, AC/DC, and optical/copper cable uplink, as well as basic/enhanced software versions.
- S3700 series switches: Layer 3 FE switches. This series provides 24 or 48 10M/100M self-adaptive access ports, and two GE uplink ports. Each model supports different specifications in terms of PoE power supply, AC/DC, and optical/copper cable uplink, as well as basic/enhanced software versions.
- S5700 series switches: provides 24 or 48 10M/100M/1000M self-adaptive access ports. Switches with the suffix LI are Layer 2 switches with four GE uplink ports. Switches with the suffix EI are Layer 3 switches with four GE uplink ports. Switches with the suffix HI are Layer 3 switches that support various extended card modules and 10GE/40GE uplink ports.
- S6700 series switches: high-performance 10GE fixed switches, which have 24 or 48 full-line-rate 10GE ports. The switches also support various service features, security policies, and QoS features, and can be used as access switches for servers in data centers and core switches on campus networks.



Huawei Modular Switches



S7700:

- Three models of this series provide 3, 6, or 12 slots for 100M/1G/10G/40G interface cards.
- MPUs, power supplies, and fans use redundancy design, and all modules are hot swappable.
- A single chassis supports a maximum of 480 10GE ports.
- Provides rich features such as MPLS VPN, traffic analysis, QoS, and multicast.



S9700:

- Three models of this series provide 3, 6, or 12 slots for interface cards.
- A single chassis provides a maximum of 576 10GE ports and 96 40GE ports, which support line rate forwarding.
- Provides modules such as the firewall, intrusion detection, and wireless control.
- Supports cluster switch system (CSS) technology.



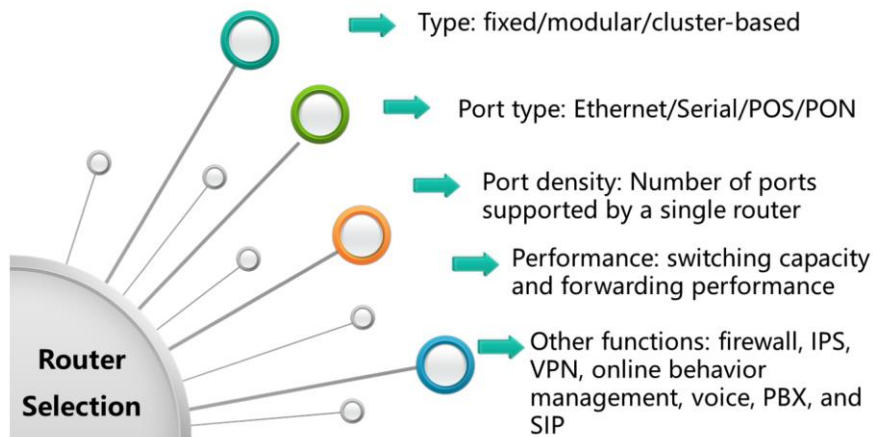
S12700:

- Three models of this series provide 3, 6, or 12 slots for interface cards.
- A single chassis provides a maximum of 576 10GE ports and 96 40GE ports, which support line rate forwarding.
- Supports data center features such as TRILL, FCoE (DCB), EVN, nCenter, EVB, SPB, and VXLAN.

- S7700:
 - Supports 100M/1G/10G/40G interface cards. Each device supports a maximum of 480 10GE ports, and the rate of each port can be upgraded to 40Gbit/s or 100Gbit/s.
 - Achieves high availability of over 0.99999. Key components such as MPUs, power supply units, and fans use the redundancy design, and all modules are hot swappable.
 - Uses switch fabric clustering technology and has an integrated built-in firewall card.
 - Supports features such as multicast, IPv6, wireless AC, and NetStream traffic analysis.
- S9700:
 - Designed for 100G platforms to ensure line rate forwarding on high-density GE/10GE ports. A single chassis supports a maximum of 96 40GE ports or 576 10GE ports, which comply with the 100GE Ethernet standard.
 - Supports CSS technology on MPUs and service ports. Key components such as MPUs, power supply units, and fans use the redundancy design.
 - Supports features such as multicast, IPv6, wireless AC, and NetStream traffic analysis.
- S12700:
 - Runs based on Huawei's innovative Ethernet network processors (ENPs) and Versatile Routing Platform (VRP).
 - Uses the CLOS architecture that provides up to 200Tbit/s switching capacity.
 - Supports up to 1M MAC address entries and 3M FIB entries, meeting large-scale routing requirements on the core layer.
 - Provides the native AC function to manage 4K APs and 64K users.
 - Supports CSS2 switch fabric hardware clustering with N+1 MPU backup, 1.92Tbit/s cluster bandwidth, and 4 μs inter-chassis delay.



Key Points for Router Selection



- Type: Routers are classified into fixed, modular, cluster-based routers. Cluster-based routers are developed to increase the port expansion capability.
- Interface type: Low-end routers are mainly used to carry IP packets over different types of links, so link types become an important reference for routers. Currently, Huawei routers support such interfaces as Ethernet, POS/CPOS, EPON/GPON, synchronous/asynchronous serial, E1/CE1, and 3G/LTE interfaces.
- Port density: High-end routers have a large number of access cables, so high-speed ports and high port density are important reference for high-end routers. In addition, there is only a small number of high-speed port types. Currently, the ports of high-end routers are mainly Ethernet-based, and a few are POS ports.
- Performance: Similar to switches, the performance of routers is based on the switching capacity and forwarding performance. As core network devices, the current high-end routers must support high-speed data forwarding. Therefore, the non-blocking structure is usually used.
- Other functions: Low-end routers tend to be platform-based, and can integrate multiple functions, such as network security and voice. But these functions are implemented based on software, which is only applicable to small networks. To efficiently implement these functions on a large scale, dedicated devices must be used.



AR Series Routers



AR1200:

- Multi-core CPU, non-blocking switching architecture
- Integration of services such as routing, switching, 3G/LTE, WLAN, and security; All-in-One networking capability
- Well-designed QoS mechanism
- Hot swappable LPUs



AR2200:

- Multi-core CPU, non-blocking switching architecture
- Four SIC slots, two WSIC slots, and two XSIC slots
- Integration of services such as the routing, switching, 3G/LTE, WLAN, and security
- Well-designed QoS mechanism, hot swappable LPUs



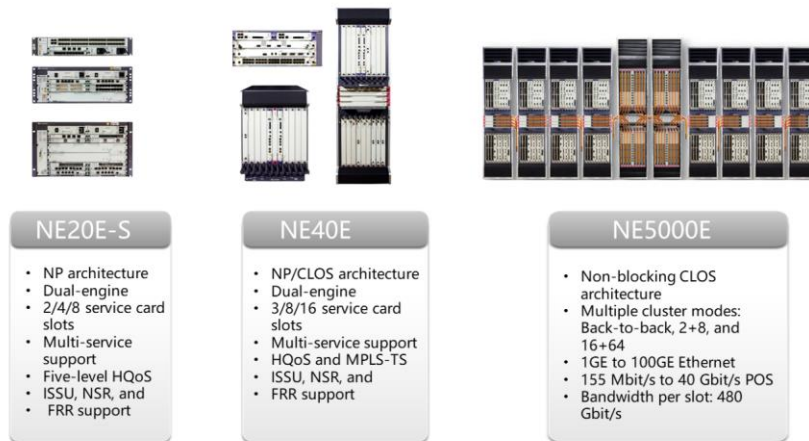
AR3200:

- Separated forwarding and control planes, 1:1 redundancy for MPUs
- Four SIC slots, two WSIC slots, and four XSIC slots
- Integration of services such as the routing, switching, 3G/LTE, WLAN, and security
- Well-designed QoS mechanism, hot swappable LPUs

- AR G3 series routers are next-generation network products for enterprise headquarters and branches. They are based on the VRP platform, and integrate functions such as routing, switching, WLAN, 3G/LTE, voice, and security. They use the multi-core CPU and non-blocking switching architecture, delivering best-in-class system performance and scalability. In addition, they provide an integrated solution. The common router types are as follows:
 - AR1200: two SIC slots
 - AR2200: four SIC slots, two WSIC slots, and two XSIC slots
 - AR3200: 1:1 redundancy for MPUs; four SIC slots, two WSIC slots, and four XSIC slots
- In addition to the preceding models, other AR G3 series routers such as AR120, AR150, AR160, and AR200 apply to small enterprises or SOHOs.



NE Series Routers



- NE series routers use Huawei-developed NP chips and are based on distributed hardware forwarding and non-blocking switching technologies. This series features good line-rate forwarding capability, carrier-level reliability, excellent expansibility, well-designed QoS mechanism, and great service-processing capability.
 - NE20E-S: high-end network product for industry customers, which is mainly used at the aggregation layer of IP backbone networks, core layer of small- and medium-sized enterprise networks, campus network edge, and access layer of small- and medium-sized campus networks.
 - NE40E: high-end network product which is usually deployed at core nodes on enterprise WANs, access nodes on large enterprise networks, interconnection and aggregation nodes on campus networks, and edges of various large IDC networks. The NE20E, NE40E, and NE5000E together provide a complete, layered IP network solution.
 - NE5000E: used at the backbone node on the Internet and interconnection node on data centers. It provides routing line cards with the industry's highest capacity of 1 Tbit/s and supports back-to-back and hybrid-chassis cluster systems. It features large capacity, high stability, and energy-saving design, ensuring the robustness and smooth evolution of networks.
- In addition to the preceding models, mid-range NE routers such as the NE08E and NE05E use Huawei-developed ENPs and the SDN architecture, and are characterized by small size and high bandwidth. They can also work properly in a wide range of temperatures (–40 °C to +65 °C) and can adapt to various harsh environments.



Product Documentation

- Huawei Enterprise Network Products
 - <http://e.huawei.com/en/allproduct>
- Huawei Routers
 - <http://e.huawei.com/en/products/enterprise-networking/routers>
- Huawei Switches
 - <http://e.huawei.com/en/products/enterprise-networking/switches>
- Huawei Security Products
 - <http://e.huawei.com/en/products/enterprise-networking/security>
- Huawei Wireless Products
 - <http://e.huawei.com/en/products/enterprise-networking/wlan>

- Routers and switches are basic devices in the current network. In addition to the commonly used devices described in the preceding slides, Huawei also provides other types of routers and switches, and other network devices, including security devices such as the security gateway and anti-DDoS device, and WLAN devices such as ACs and APs. For more information about these devices, you can visit Huawei official website to obtain relevant information.



Case: Campus Network Device Selection

- A university plans to deploy a network for dormitories. There are eight dormitory buildings, each of which has six floors. One floor has four units, and each unit has five dormitory rooms with six students in each.
 - How to select access devices for the dormitories
 - How to select aggregation devices for the dormitories

- For this common case, engineers learn about some information related to device selection, but does not understand the customer's requirements, so device models cannot be completely determined. In this case, engineers need to further obtain more information and provide selections of possible device types. In addition, engineers need to negotiate with the customer and explain the differences between each selection, and then determine the final selection based on the customer's requirements.
- The following are recommended based on the current information:
 - Install access switches in the corridor and use the mains supply (AC) to reduce costs. Use copper cables for downlink access ports and optical fibers for uplink ports. One unit can accommodate about 30 students, so it is recommended that each unit install one 48-port access switch. In this way, one dormitory building requires 24 access switches. When selecting switches, determine the switch port rate, and whether Layer 3 functions are needed by access switches. This can be decided upon communication with the customer. The recommended models include the S2710-52P-SI-AC and S3700-52P-SI-AC. Both can provide 48 FE ports, four uplink GE ports with SFP slots, and AC power supply. The S3700 can support Layer 3 functions, IPv6, and other abundant features.
 - Deploy one aggregation switch for each building. The selection method of aggregation switches is similar to that of access switches. The recommended model is the S5720-36C-EI-28S-AC, which provides 28 GE SFP ports, four Combo 10/100/1000Base-T Ethernet ports, and four 10GE SFP+ ports. The switch also supports swappable dual power supplies (AC or DC).

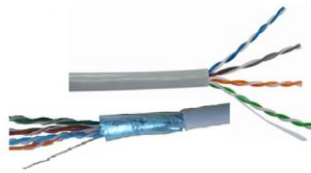


Contents

1. Overview
- 2. Physical Network Design**
 - Typical Topology
 - Device Selection
 - Media Selection
 - Network ID
3. Logical Network Design
4. Other Network Technologies
5. Overall Technological Solution



Common Media Types



Twisted pair



Optical fiber



Wireless



Telephone cable

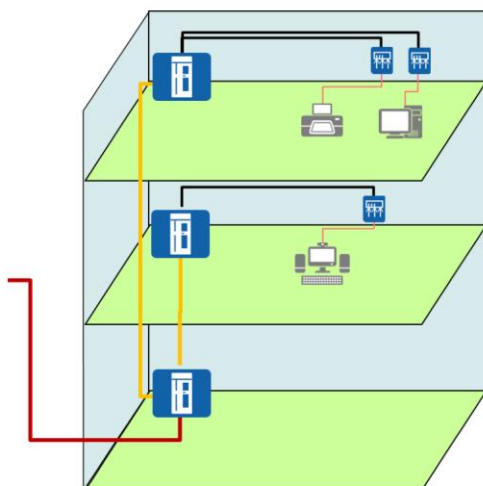


Coaxial cable

- Common network media types are as follows:
 - Twisted pair: categorized into the shielded twisted pair (STP) and unshielded twisted pair (UTP). According to the line transmission frequency, bandwidth, and crosstalk ratio, twisted pairs can also be classified into CAT5, CAT5e, CAT6, etc. CAT5 cables are used for fast Ethernet, and CAT5E and CAT6 cables are used for gigabit Ethernet.
 - Optical fiber: classified into single-mode and multimode fibers. The transmission distance of single-mode fibers ranges from 2 km to 70 km, while that of multimode fibers is shorter than 500 m. And the multimode fibers are orange, and single-mode fibers are yellow.
 - Telephone cable: generally dual-core copper cables. Telephone cables cannot transmit high-speed signals. However, due to historical reasons, telephone cables are deployed on a large scale, and a number of technologies are developed to transmit data signals, such as synchronous/asynchronous serial technology and DSL technology.
 - Coaxial cable: originally used to transmit video signals. To carry digital signals, bearer technologies such as Cable Modem are developed.
 - Wireless: Wireless communications (for example, WLAN and LTE) are rapidly developing and have been widely applied.



Structural Cabling in a Building

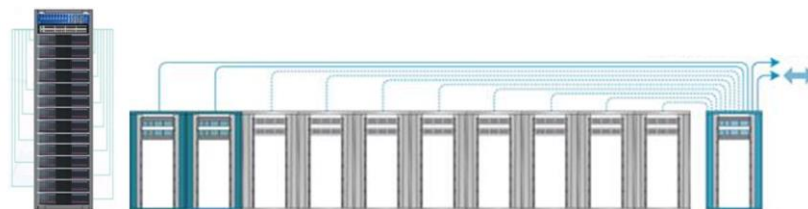


- Cabling subsystem in a building:
 - Horizontal subsystem: from information panels to equipment rooms in the floor (using twisted pairs)
 - Vertical subsystem: from equipment rooms in the floor to the central equipment room (using optical fibers)
 - Work area subsystem: from terminals to information panels (using network jumpers)

- Generally, network cabling systems include the building, vertical, horizontal, and work area subsystems. Various lines and components are involved in the cabling, which is not described here.
- In the current cabling system, twisted pairs are generally used in the horizontal system because the system connects to various terminals, which mainly use twisted pairs for network connection. Ensure that the distance of twisted pairs does not exceed 100 m.
- In the current cabling system, optical fibers are usually used in the vertical system. On the one hand, the distance between the central equipment room and each floor is long. On the other hand, as the vertical system serves as the backbone system, optical fibers can provide high data transmission rate.
- Generally, multimode fibers are often used in the building cabling to reduce construction costs. To reduce spare parts and O&M costs, single-mode fibers can also be used.



Data Center Cabling Structure



- Top of Rack (ToR): installing switches at the top of each rack.
- End of Row (EoR): installing switches at the tail of each row of racks.

- ToR and EoR are commonly used cabling modes in a data center. For ToR, access switches are installed at the top of each rack, reducing cabling workloads. For EoR, switches are installed at the tail of each row of racks.
- With the development of cloud computing, server density in data centers increases quickly, making the ToR cabling mode more popular.



Engineering Tools and Test



Twisted pair



Optical fiber



Twisted pair test



Optical fiber test

- In a cabling project, the termination point in the equipment room is usually distribution frames, and that in the work area is information panels. Jumpers are used to connect two ends of twisted pairs/optical fibers to the network port of a device. Generally, the twisted pair interface is RJ45.
- The end point of an optical fiber is connected to the fiber management tray after the fiber is connected to a device. The most common port types of optical fibers are as follows:
 - Lucent connector (LC): small square joints, commonly used by device interfaces and optical modules.
 - Subscriber connector (SC): large square joints, commonly used by device interfaces and optical modules.
 - Fiber connector (FC): round, threaded optical fiber connector, which is commonly used by optical distribution frames (ODFs).
 - Straight tip (ST): round, bayonet-type optical fiber connector, which is mainly used for ODFs.
- Generally, an acceptance test is performed after the cabling is complete to ensure that all lines can work properly. If the line status needs to be verified during network connection, perform the test using:
 - Network cable tester: used to check that lines are intact by connecting both ends of the lines. In addition, high-end testers can be used to test line integrity (testing the length of a network cable by connecting one end of it).
 - Red pointer: After one end of an optical cable is connected, red light can be seen from the other end. Due to the large power of the red pointer, do not connect devices at the other end to prevent photosensitive components from being damaged.
 - Optical power meter: used to test the received optical power. Some optical power meters can transmit light with specific optical power. When using an optical power meter to perform a test, you need to adjust the test wavelength, using dBm as the unit. The optical power that can properly transmit data ranges from -5 dBm to -20 dBm. The work range varies depending on optical modules, and can be obtained by querying relevant optical module parameters.



Telephone and Coaxial Cables



Telephone cable connection



Telephone cable loop test



Coaxial cable connection



Coaxial cable loop test

- Telephone cables and coaxial cables cannot directly transmit digital signals, so a modem is required for signal conversion. Initially, modems were independent, and digital signal output mainly used RS-232 and V.35 interfaces standard. Afterwards, modems integrate some data functions and often output data through Ethernet. Currently, the modem module can also be integrated in a router.
- Telephone and coaxial cables are often used for WAN link access. Compared with twisted pairs used for LAN, they can transmit signals at a longer distance and are often managed by different organizations. Therefore, coordination between organizations is required during a test. Loop tests are most commonly used. During a loop test, two lines are short-circuited at the remote end. The loop indicator on the modem turns on after the short circuit. In addition, some modem panels have a loop button or menu that can be used for loop tests at the local or remote end.
- Loop tests can be only used for qualitative tests on WAN links. Carriers providing the links have dedicated devices, which can be used to transmit and receive traffic during a line loopback to test the link BER.
- Generally, lines are managed by different responsible parties, and the modem is the cut-off point.



Contents

1. Overview
- 2. Physical Network Design**
 - Typical Topology
 - Device Selection
 - Media Selection
 - Network ID
3. Logical Network Design
4. Other Network Technologies
5. Overall Technological Solution



Device Identifier

Device Identifier

- Unique identifier of a device on a network
- Physical label and logical device name
- Unified rule and naming
- Content:
 - Device installation position
 - Device role
 - Device model
 - Logical number

<Huawei>**system-view**

Enter system view, return user view with Ctrl+Z.

[Huawei]**sysname HQ-CS-HW-S7706-1**

- A device on a network needs to have an identifier after rollout, which includes the logical device name and physical label. The logical device name is configured on a device. When administrators log in to the device, they can obtain information about the device. The physical label is pasted on the device to display device information.
- The identifier of a device does not have a unified standard, and is usually defined following the practical principle. The device identifier needs to be unified inside an enterprise. A logical device name generally contains the following information:
 - Device installation position
 - Device role
 - Device model
 - Device ID
- The physical label of a device does not have a unified standard, and is usually defined by enterprises according to their requirements. A physical label contains the following information:
 - Device model
 - Device ID
 - Responsible person/Contact information



Line Identifier

Line Identifier

- Unique identifier of a line on a network
- Physical label and device port description
- Unified rule and naming
- Content:
 - Local device name
 - Peer device name
 - Peer device ID
 - Link role
 - Logical number

```
[Huawei]interface  
gigabitethernet0/0/0  
[Huawei]description To- HQ-CS-  
HW-S7706-1-GE1/1/1
```



- On current networks, device connections are complex, with a large number of network cables. To facilitate routine management and fault location, device interfaces and network lines need to be identified.
- Description can be configured for device ports, and is usually used to describe the peer device and interface of a line. You can also add more information as required.
- Generally, labels are used to describe the routes of network lines. Different from the device port description, the current network lines are usually segmented and connected to fiber patch cords through network distribution frames.



Case: Device and Link Identifier Planning on a Campus Network

- A campus network has a large number of devices and lines, and requires unified naming rules for device and line diagnosis and management. Design the naming rules for devices and lines.
 - Device naming rule
 - Line naming rule

- The naming rule for a device can be "device type + device position + device model + number". For example:
 - ACC-B1F3U2-2710-1:
 - ACC: access switch
 - B1F3U2: 2nd unit on 3rd floor in 1st building
 - 2710: device model
 - 1: number
- The naming rule for a line can be "peer device name + device position number + peer port number". For example:
 - To-AGG-B1N1-G0/0/8:
 - AGG: aggregation switch
 - B1N1: 1st number in 1st building
 - GE0/0/8: peer port number



Contents

1. Overview
2. Physical Network Design
- 3. Logical Network Design**
 - LAN Design
 - WAN Design
 - Route Architecture Design
 - Network Egress Design
 - High Availability Design
 - Other Network Technologies
 - Overall Technological Solution



LAN Selection

LAN → **Ethernet** switch + twisted pair + optical fiber

Important Parameter				
Rate	100 Mbit/s	1 Gbit/s	10 Gbit/s	40 Gbit/s
Port type	Copper cable		Optical fiber	
MTU	1500		Jumbo frame	
Other functions	PoE/stacking/routing			

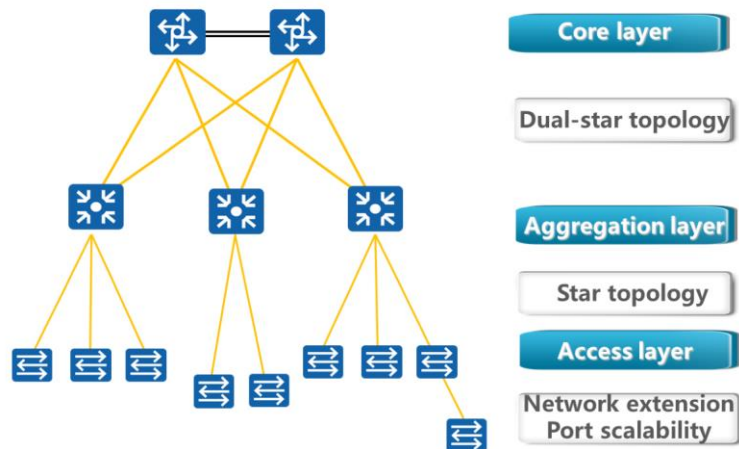


display interface.txt

- Currently, LANs are generally Ethernet-based, and use switches and category-5 cables/fibers together.
- During network design, the Ethernet rate must be the principle concern. The common Ethernet rates are 100 Mbit/s, 1 Gbit/s, 10 Gbit/s, and 40 Gbit/s.
- The line type is also one of the concerns. In most cases, twisted pairs are used if the Ethernet rate is lower than 1 Gbit/s, while optical fibers are used if the Ethernet rate is higher than 1 Gbit/s.
- When copper cables are used, the switch port rate is adaptive. That is, two interconnected switches can negotiate an optimal connection rate. When optical fibers are used, the rate is fixed.
- The copper cable port rate is auto-adaptive in duplex mode. You can manually set the duplex mode on devices at both ends. Fiber connections are in full-duplex mode.
- The maximum transmission unit (MTU) of traditional Ethernet frames is 1500 bytes (excluding the frame header and trailer). However, the rapidly developing tunnel and encapsulation technologies, such as MPLS, FCoE, and VXLAN, require the Ethernet to bear a larger MTU size. In scenarios with special requirements, the MTU supported by switches must be considered.



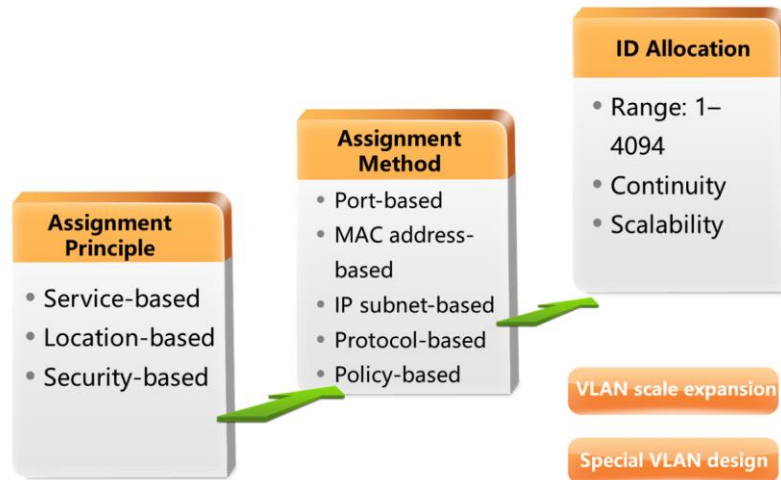
Commonly Used Topologies on a LAN



- The figure shows a common Layer 3 topology on a LAN. The redundant dual-star topology is used between the core layer and the aggregation layer, while the non-redundant star structure is used between the aggregation layer and the access layer.
- In some scenarios, access switches are cascaded to support a large number of terminals. It is recommended that the cascading mode not be used on a large scale.
- In actual networking, the topology structure can be optimized as required. For example, this topology provides device redundancy only at the core layer. If the two-node cluster redundancy needs to be configured at the aggregation layer, the full-mesh or square-shaped network topology can be used. In addition, if link redundancy needs to be implemented between the aggregation layer and the access layer, dual homing or link binding technology can be used.
- Generally, gigabit optical fibers or twisted pairs are used to connect switches.



VLAN Design



- VLAN design includes VLAN assignment principles, specific assignment methods, and VLAN ID allocation.
- First, determine the VLAN assignment principles. VLANs are generally assigned as follows:
 - Service-based: Generally, the organizational structure of a company is divided based on different services, so service-based VLAN assignment is actually based on a company's organizational structure. Such assignment mode is commonly used.
 - Location-based: VLANs are assigned according to the network extension range, for example, by buildings, floors, or rooms.
- Second, determine the specific VLAN assignment methods. Technologically, VLANs can be assigned using different methods, of which port-based assignment is most commonly used. This method is simple and direct, facilitating easy implementation and management. In addition, VLANs can be assigned based on the MAC address, IP address, and protocol type, which can be used in some special scenarios.
- Finally, allocate VLAN IDs. VLAN IDs range from 1 to 4094. Each port requires a PVID with the default value of 1. It is recommended that VLAN1 be used as the reserved VLAN. For the allocation of other IDs, there are no special requirements, and management and O&M convenience is mainly considered. You'd better allocate VLAN IDs according to the actual situation. For example, if VLANs are allocated by area, consecutive VLAN IDs can be allocated in a building.
- In many cases, 4094 VLANs are not sufficient. To solve this, some VLAN expansion technologies, such as QinQ, can be used.
- Some vendors have also designed some special VLAN technologies to meet some special requirements, such as MUX VLAN and VLAN aggregation.



STP Protocol

STP/RSTP/MSTP

- STP: basic version.
- RSTP: convergence speed improved.
- MSTP: concepts of region and instance introduced.

Default Configuration

- Huawei switches use the MSTP protocol.
- One switch belongs to one region.
- All VLANs are mapped to instance 0.

Compatibility

- Downward compatible.
- RSTP: enables STP for ports that receive STP BPDUs.
- MSTP: Switches running RSTP work in different regions.

MSTP Design

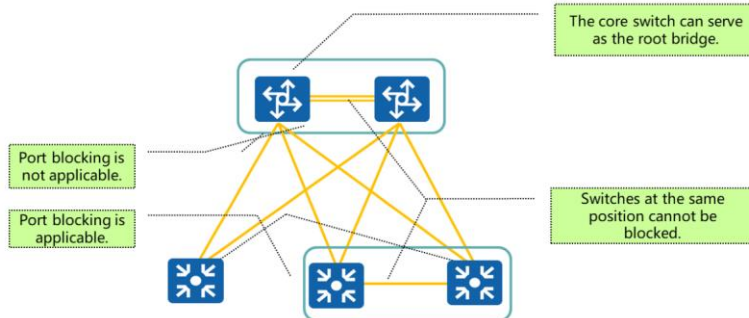
- Region definition.
- Revision version definition.
- Instance definition.
- VLAN mapping definition.

- The Spanning Tree Protocol (STP) is a network protocol that builds a logical loop-free Layer 2 network topology. The protocol has three versions: STP, RSTP, and MSTP, which have similar algorithms but differ in implementation.
- By default, Huawei switches use the MSTP protocol. Each switch forms an MSTP region, whose region name is the MAC address of the switch. In addition, all VLANs are mapped to instance 0 by default.
- When multiple STP protocols are used on a network, STP versions are backward compatible with each other, which ensures proper running in hybrid networking.
- In actual network deployments, interconnection with non-Huawei devices is often required, for example, interconnection between devices running STP. In this process, you need to pay attention to related interconnection cases and product features.



STP Settings

Key points Positions of the root bridge and blocked port

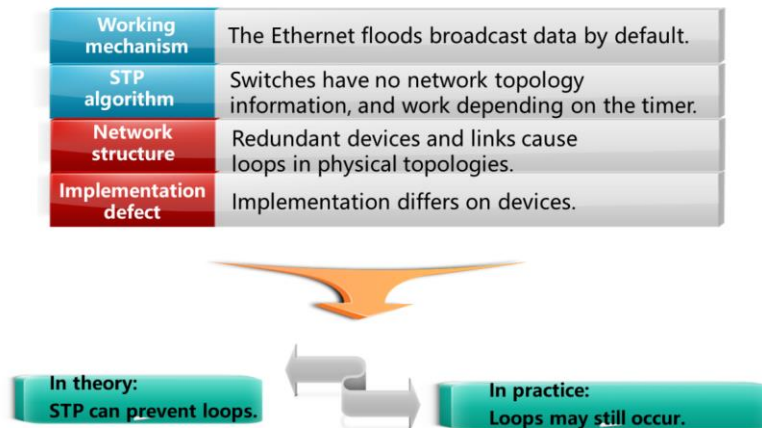


Adjustment methods BID priority, cost ...

- If redundant links exist on a network, the STP protocol can block some ports to prevent Layer 2 loops.
- The blocked ports must be on minor and non-critical links, not on backbone links.
- If device redundancy exists on a network, the interconnection links between two redundant devices should not be blocked.
- In device redundancy scenarios, the active and standby core switches are generally configured as the STP root bridge and backup root bridge, respectively.
- One of the access switch's dual uplink ports is usually blocked by the STP protocol.



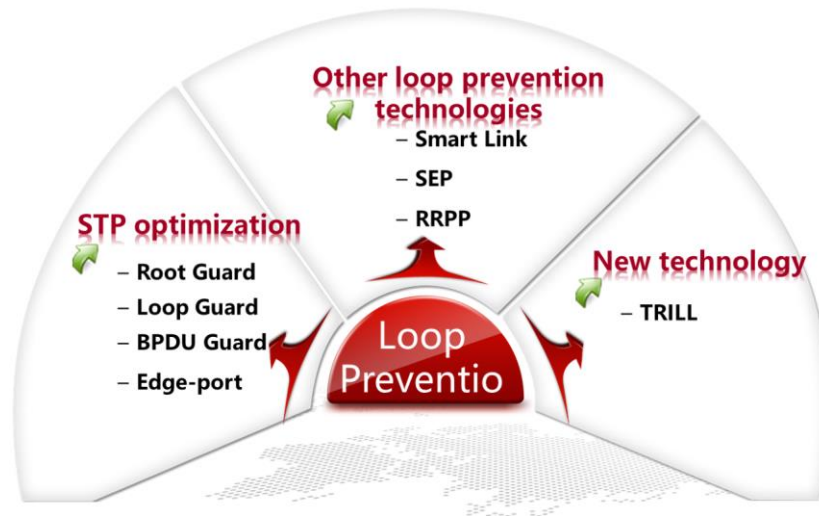
Layer 2 Network Loop



- The STP protocol is capable of preventing Layer 2 loops to some extent. However, in actual networking, loops occur more frequently on Layer 2 networks than on Layer 3 networks. Then, how are Layer 2 loops generated?
 - Loops on a topology: To improve reliability of a large network, redundant links and devices are used, which essentially provides detour paths.
 - STP algorithm: The STP algorithm does not collect the network-wide topology information and cannot fundamentally prevent loops.
 - Network structure: Switches on a switching network do not collect the network-wide convergence status. They can only estimate the information based on the timer. Once the timer expires, data is forwarded, causing network loops.
 - Implementation defect: The STP protocol is implemented based on specific devices, while unexpected situations may occur on products and networks, which causes network loops.




Loop Prevention Technologies



- Multiple methods can be adopted to prevent Layer 2 loops.
- STP optimization:
 - The default time parameters of STP are set based on recommended topology conditions. These parameters can be modified, but it is not recommended.
 - RSTP provides various protection technologies to improve the convergence speed, stability, and anti-attack capabilities of STP.
- Other loop prevention technologies:
 - More loop prevention technologies are developed, such as Smart Link, SEP, and RRPP. These technologies resolve STP loop convergence problems including slow Ethernet dual-uplink switchover convergence and inaccurate algorithms. However, these technologies have many limitations. For example, Smart Link focuses on problems in active/standby dual-uplinks of a single device, and SEP focuses on problems in ring topologies.
- TRILL is an excellent Layer 2 multi-link solution. It speeds up STP convergence and enhances link utilization efficiency by introducing routing-like technology to LANs. Currently, TRILL technology applies to data center networks and are not supported by all switches.



Layer 2 Network Security Design



Layer 2 Attack Type	Layer 2 Protection Mechanism
DoS attacks on devices	Switch CPU defense
Traffic overload	Traffic suppression and storm control
MAC address spoofing	Port security
DHCP attack	DHCP snooping
ARP attack	Rate limit, solidification, isolation, and DAI
IP address spoofing	IPSG

Select corresponding security mechanisms for different attacks.

- Huawei provides solutions to defend against various attacks on a Layer 2 network.
- **DoS attack:** This type of attack is targeted at switches. To defend against such attacks, the Control Plane Committed Access Rate (CPCAR) can be used to limit the number of packets sent to the CPU per unit time, defending against attacks on the control plane of switches.
- **Traffic overload:** When a broadcast storm occurs on a network or the network is attacked, excessive traffic is continuously generated on switch ports. In this case, traffic suppression can be configured on a switch to limit unicast, multicast, and broadcast packets by specifying their traffic thresholds.
- **MAC address spoofing:** A switch transmits data based on the MAC address table, which is obtained by the switch from listening to network data traffic. Attackers often forge MAC addresses to attack the MAC address table. Port security functions can be configured to defend against such attacks.
- **DHCP attack:** Hosts on the network usually obtain IP addresses using DHCP, which can be easily manipulated by attackers. Network administrators can enable DHCP snooping function on a switch to prevent such attacks.
- **ARP attack:** ARP plays an important role on a LAN, but is easily used by attackers due to its lack of an authentication mechanism. Multiple methods can be used to prevent ARP attacks.
 - For example, to prevent ARP flooding attacks, limit the rate of ARP traffic on switch ports or manually configure static ARP entries.
 - ARP works by broadcasting ARP packets. Therefore, segmenting the broadcast domains isolated by VLANs can reduce the impact of ARP attacks. Additionally, some special VLAN technologies such as the MUX VLAN and VLAN aggregation can be used to isolate users.
 - Use DHCP snooping to bind MAC and IP addresses with switch ports. Enable DAI to check ARP response packets.
- **IP address spoofing:** The IP protocol cannot verify source IP addresses, making IP address spoofing attacks rampant. Unicast Reverse Path Forwarding (URPF) is used to prevent such attacks on a Layer 3 network, and IP source guard (IPSG) is used on a Layer 2 network to check source IP addresses.



Case Study

- On a campus network, access switches and aggregation switches are connected at Layer 2. User gateways are deployed on aggregation switches. The aggregation and core switches are connected at Layer 3. To isolate broadcast domains, design a VLAN assignment solution for the Layer 2 network.

- Campus network overview: There are eight dormitory buildings on the campus, each of which has six floors. One floor has four units, and each unit has five dormitory rooms. Deploy a Layer 2 switch in each unit, and a Layer 3 switch in each dormitory building.
- VLANs can be assigned using the following modes:
 - For security purposes, reduce the scale of a single VLAN. Each dorm or even each user can be assigned to a VLAN.
 - To facilitate management, each access switch can be assigned to a VLAN, eliminating the need for VLAN configuration on the access switches.
- For example, each dormitory is assigned to a VLAN. In this scenario, one access switch requires five VLANs. A building has 24 units, so there are 24 access switches. The aggregation switches in each dormitory building terminate Layer 2 traffic. Therefore, VLANs between the buildings are independent of each other, and VLAN IDs can be reused in different buildings. A building requires 120 VLANs. For easy scalability and management, the VLAN ID can be used in the format of "VLAN + floor number + unit number + dormitory number". For example, VLAN425 is the VLAN ID assigned to No.5 dormitory, second unit, fourth floor.



Contents

1. Overview
2. Physical Network Design
- 3. Logical Network Design**
 - LAN Design
 - WAN Design
 - Route Architecture Design
 - Network Egress Design
 - High Availability Design
 - Other Network Technologies
 - Overall Technological Solution

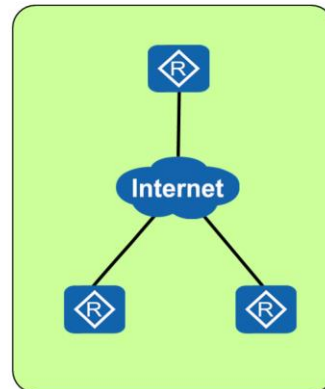


Characteristics of WAN

Wide coverage range

High leasing costs

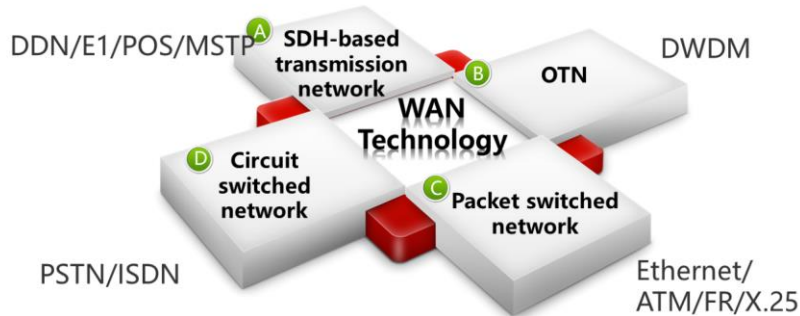
Complex O&M



- A WAN covers a wide geographical area of usually a few tens of or hundreds of square kilometers or even wider, while a LAN covers a room, floor, or building. Geographically, between the LAN and WAN is the campus network, which is commonly deployed in enterprises. A campus network can cover several buildings within a certain area, and uses LAN technologies. In addition, there are MANs and access networks for carriers.
- For enterprises, laying out cables in a wide geographical area is not cost-effective. They usually lease links from carriers by paying monthly rentals.
- WANs are managed by both enterprises and carriers, which may involve interface and negotiation issues. In addition, many outdoor lines on a long-span WAN cause a high failure rate and long recovery time.



WAN Technology Selection



- Enterprises lease synchronous digital hierarchy (SDH) transmission networks from carriers to transmit service data. SDH uses time-division multiplexing (TDM) technology in transmission networks, which is the most common WAN technology. SDH links can be classified into multiple types according to the bandwidth assigned to timeslots, such as, Digital Data Network (DDN) links (in 64 kbit/s), E1 links (in 2 Mbit/s), and packet over SDH/SONET (POS) links (in 155 Mbit/s) which can provide a transmission rate of 622 Mbit/s, 2.4 Gbit/s, or 10 Gbit/s. Besides, E1 and POS links support channelized transmission. For example, if one end provides a 155 Mbit/s POS link, the other end can divide the link into 63 E1 links based on channels. The Multi-Service Transfer Platform (MSTP) is a SDH-based platform that provides network interfaces such as Ethernet and ATM interfaces.
- The optical transport network (OTN) uses the wavelength division multiplexing (WDM) technology, and supports scheduling and transmission at a large bandwidth. OTN is the next-generation backbone transmission network that can replace the current SDH transmission network. It delivers GE or 10GE links and has been widely used in backbone networks.
- ATM, frame relay (FR), and X.25 networks forward data based on permanent virtual connection (PVC) or switched virtual connection (SVC). They can share physical links among multiple users, and have certain routing capabilities. However, these networks are not widely used due to such reasons as the efficiency, cost, and quality control.
- Circuit switched networks use traditional PSTNs to transmit data. Its single-line bandwidth is 64 kbit/s, while the improved integrated services digital network (ISDN) supports a 144 kbit/s bandwidth. Originally, circuit switched networks were often used as backups due to their hour-based charging and low bandwidth. Currently, circuit switching technology is no longer used because it cannot meet the demanding bandwidth requirements.
- Some carriers provide dark fiber leasing services within a certain range. However, the dark fiber leasing is expensive, and the transmission distance of dark fibers is limited if lack of signal amplifiers. Therefore, this type of fibers is not widely used.



Layer 2 Protocol for WAN

Link Type	Structural Feature	Layer 2 Protocol
DDN/E1/POS	P2P	HDLC/PPP
PSTN/ISDN	P2P	PPP
OTN	P2P	Ethernet
Packet switched network (PSN)	P2MP	Ethernet/X.25/FR/ATM

- P2P links are mainstream links used on WANs.
- Point-to-Point Protocol (PPP) is the mainstream protocol used by P2P links.
- OTNs provide Ethernet access services.

- High-Level Data Link Control (HDLC) is a bit-oriented link layer protocol, and is applicable to synchronous serial links. HDLC does not provide functions such as authentication and multi-protocol support, but is concise with high transmission efficiency. The HDLC protocol used in current data networks has been modified.
- PPP is the most commonly used link-layer WAN protocol, and can work on both synchronous serial and asynchronous serial links. The protocol can provide rich extension functions, such as authentication, link bundling, address negotiation, and data compression.
- As a new large-granularity transmission technology, OTN directly provides Ethernet interfaces for user access when carrying data services.



Replacement Technologies for WAN

Traditional WAN

- Bandwidth guaranteed
- Expensive
- QoS controllable
- High reliability
- High security

VPN

- Bandwidth uncontrollable
- Cost-effective
- QoS uncontrollable
- Poor reliability
- High security

- Traditional WANs provide dedicated bandwidth for data transmission by dividing links into different timeslots in a TDM system, or by dividing certain signal wavelength in a WDM system. The bandwidth of the divided part is dedicated. If user data is not transmitted on the WAN, the bandwidth assigned to the user is not used, which makes the leasing of traditional WAN lines expensive. Traditional WANs, however, provide high-quality QoS control, security, and reliability. The PSN has introduced some of the concepts of statistical multiplexing, and offers a good QoS mechanism to ensure user bandwidth.
- VPN technology is a good alternative for traditional WANs, and has been widely used in projects. The VPN described in this slide is the virtual private network established through the Internet. Users can connect to networks through the VPN anywhere, anytime, and they only need to pay the local Internet access fees, greatly reducing network costs. However, the VPN cannot guarantee the network bandwidth, and its QoS and reliability capabilities are only based on basic features of the Internet. Therefore, the security of VPNs is poor but can be improved using certain technological means.



Access Network Technology

Last-mile access

Enabling communication between user networks and carriers' backbone networks

DSL

- Telephone cables
- Asymmetric uplink and downlink bandwidths
- 1–10 Mbit/s

FTTx

- Twisted pairs
- Scenarios with a high user density
- 10 Mbit/s, 100 Mbit/s, or 1 Gbit/s

PON

- Optical fibers
- Future trend
- High bandwidth

Wireless

- Wi-Fi or LTE
- Future trend
- 1–100 Mbit/s

HFC

- Coaxial cables
- Broadcasting and TV carrier
- Sharing the 100 Mbit/s bandwidth

Asynchronous dialing

- Telephone cables
- Eliminated
- Rate < 64 kbit/s

- Strictly speaking, access networks are not WANs, and are usually used to provide access to network services. They are networks between user networks and the backbone networks, which is called the "last-mile access".
- To reduce investment costs, carriers develop various technologies based on the original line technologies. For example, the asynchronous dial-up technology used on telephone lines provides less than 64 kbit/s bandwidth. With the emergence of ISDN and DSL technologies, the bandwidth is increased to 128 kbit/s and 10 Mbit/s, respectively.
- Broadcasting and TV carriers develop the hybrid fiber-coaxial (HFC) technology based on coaxial cables, which provides bandwidth of 100 Mbit/s. This bandwidth, however, is shared between users over the same coaxial cable.
- Fiber to the x (FTTx) uses Ethernet technology to provide access for users. Ethernet itself is not an access network but is cost-effective and high-speed. It well adapts to scenarios with a large number of access users.
- Passive optical networks (PONs) provide fiber access for users. With the development of the mobile Internet, wireless access becomes an important access mode.



Case Study

- A campus network needs to connect to an education network on which access points are deployed in the same city. The straight-line distance between the two networks is about 10 km. It is estimated that the bandwidth requires about 1Gbit/s. Then, what link technologies can be used?

- In actual projects, multiple link technologies can be used. During link section, non-technological factors such as the price, cost, and availability must be considered, and the decision must be agreed by the customer.
- Currently, Ethernet and POS are main technologies that provide a bandwidth of over 1 Gbit/s. Ethernet is commonly used, while POS technology is expensive and rarely used. If Ethernet is used, OTN can be selected for the underlying network. We can also use bare fibers as the distance between the campus network and the education network is only 10 km. The bearer effects of the Ethernet and POS are not quite different. Therefore, considering the price and availability, we can negotiate with a local carrier and select one with a more acceptable rental. MPLS VPN can also be used if it is provided by the local carrier.
- This case may involve access network technologies, which are not end-to-end technologies, and are only applicable to links from user networks to carrier networks. Therefore, it is unlikely that access network technologies are used to connect the campus network to the education network in the whole process.



Contents

1. Overview
2. Physical Network Design
- 3. Logical Network Design**
 - LAN Design
 - WAN Design
 - Route Architecture Design
 - Network Egress Design
 - High Availability Design
 - Other Network Technologies
 - Overall Technological Solution



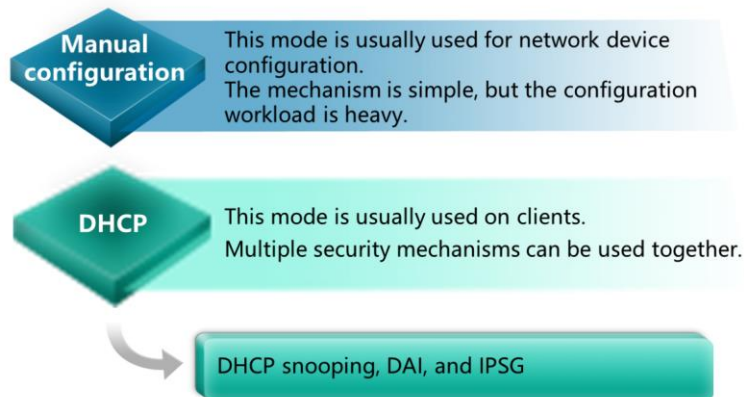
IP Address Allocation Rules



- IP address allocation design is the basis for Layer 3 network design.
- IP address is required to be unique on the entire network except some special applications. This is the basic condition for IP addressing.
- Initially, unicast IP addresses are classified into classes A, B, and C, and the masks are /8, /16, and /24 respectively. Such classification wastes IP addresses. Routing protocols, corresponding to these IP addresses, are called classful routes. Variable Length Subnet Mask (VLSM) technology is developed to fully utilize IP addresses, and the mask length can be specified as required. Currently, the most commonly used mask lengths are /32 and /30. The mask /32, called host route, is commonly used to identify a device. The mask /30 is used at both ends of point-to-point (P2P) link. Generally, the mask length is designed based on the user quantity on a LAN.
- The routing efficiency should be considered during address allocation design. For routers, fewer routes mean higher efficiency. In this case, you need to consider whether addresses can be aggregated when allocating IP addresses. Consecutive address blocks in network partitions need to be allocated for address aggregation. You need to reserve address expansion space in each network partition to ensure that addresses are not disordered for future expansion. Allocating addresses by area or block facilitates future maintenance.



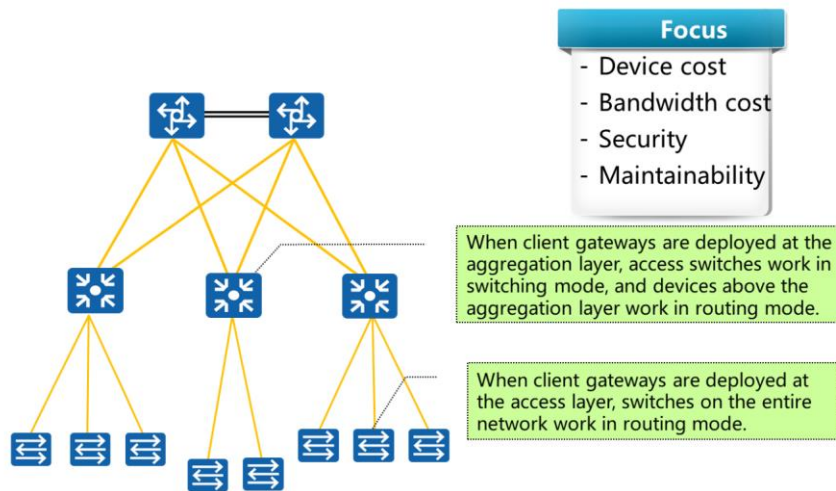
IP Address Configuration



- IP addresses of network devices except the devices that use dial-up virtual private network (VPN), are statically and manually configured. Such IP addresses are secure and reliable, and are not prone to attacks. However, the configuration workload is heavy. For clients, manual configurations may cause errors and address conflicts.
- The Dynamic Host Configuration Protocol (DHCP) is commonly used to configure IP addresses for clients. DHCP can be enabled on specified servers or router interfaces. You need to configure the DHCP relay agent on the gateway of each network segment if a specified server is deployed.
- DHCP may cause attacks, but security mechanisms can be used to defend against the attacks. For example, DHCP snooping can prevent attacks from bogus servers. In addition, the DHCP snooping binding tables can be used with dynamic ARP inspection (DAI) to prevent ARP attacks and used with IP source guard (IPSG) to prevent attacks with bogus source IP addresses.



Routing Boundary Identification



- Routing and switching modes have their own advantages. Layer 3 networks require routers or Layer 3 switches, whereas Layer 2 networks require only Layer 2 switches. The processing capability and switching capacity of switches are much higher than those of routers. However, each device on a Layer 2 network sends a certain number of broadcast packets. When the Layer 2 network scale is large, broadcast traffic will be overlapped.
- When links are redundant on a Layer 2 network, the Spanning Tree Protocol (STP) is used to remove loops. Compared with a routing protocol, STP has slower convergence and lower reliability. When loops occur, broadcast storms may cause the whole Layer 2 network to become unavailable. A Layer 3 network uses routing protocols. Currently, it uses link-state routing protocols that provide fast convergence and higher reliability than the layer 2 network, with no loops. Switches also support link bundling, two-node cluster, and other optimized loop prevention mechanisms so that the Layer 2 network can provide redundancy, improve reliability, and prevent loops.
- Layer 3 networks need to be configured with IP addresses and routing protocols. If a gateway is too close to users, address segments may be segmented again, increasing the management and maintenance workload.
- Currently, wide area networks (WANs) adopt the routing architecture. Broadcast data should be prevented because WAN links are expensive.
- On a campus network, you need to consider cost, bandwidth, reliability, security, and maintainability, and set the boundary between Layer 2 and Layer 3 networks according to different scenarios. The routine approach is to deploy gateways at the aggregation layer, and deploy one dual-link redundancy or no redundancy at the access layer, preventing or simplifying the usage of STP. In certain scenarios, gateways are deployed at the access layer, maximizing redundancy and accelerating convergence.
- On specified networks, some special technologies are developed for massive data and enormous access users. For example, for carrier access, a large-sized Layer 2 network is designed to reduce device costs and simplify management. To further improve security, QinQ is used to isolate users. In data centers, a large Layer 2 network is designed and gateways are deployed on core switches.



Routing Protocol Selection

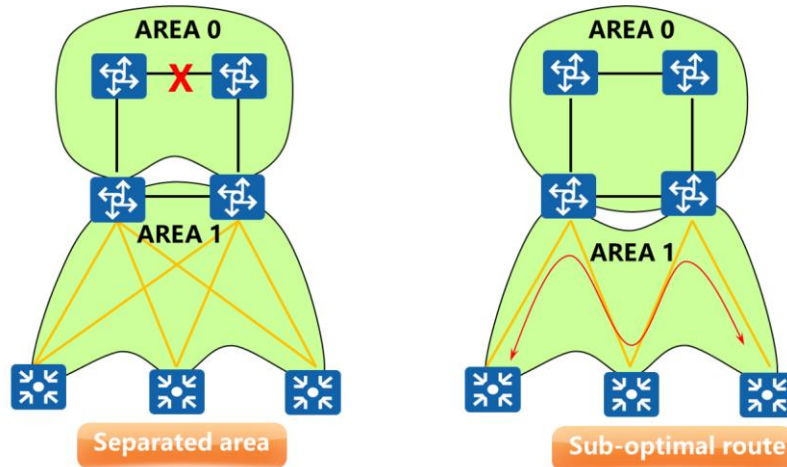
Classification	Protocol	Algorithm	Description
IGP	OSPF	LS	Hierarchical, bandwidth cost, fast, and loop-free
	IS-IS	LS	Similar to OSPF
EGP	BGP	DP	Inter-domain routing, strong bearing and manipulation capabilities, and loop-free

- In practice, OSPF is preferred, and IS-IS is commonly used on carrier backbone networks.
- BGP applies to inter-domain routes and MPLS/BGP VPN networks.
- Static routes are commonly used in scenarios where there is no redundant connections.

- Three routing protocols are often used on IPv4 networks: OSPF, IS-IS, and BGP.
- OSPF and IS-IS are link-state routing protocols. OSPF, designed by the IETF, is dedicated to IP networks, whereas IS-IS is specified by the ISO, and is developed earlier than OSPF. OSPF and IS-IS are similar in framework and algorithm, but different in design. For example, there are minor differences in the scalability and convergence speed. IS-IS are commonly used on carriers' backbone networks due to some historical factors, whereas OSPF is used in other scenarios.
- BGP is the only external routing protocol in use, and supports the inter-AS routing capability. BGP is commonly used for connections between multiple enterprises or carriers, but seldom used on small- and medium-sized enterprise networks. However, when the scale of large-sized enterprise networks exceeds the management capability of a single organization or support capability of a single IGP, internal networks are also divided into multiple ASs and BGP is used to connect ASs. Furthermore, when MPLS/BGP VPN is deployed on an enterprise network, BGP is mandatory.
- Besides dynamic routing protocols, you can also configure static routes. Static routes can be used easily and conveniently, and are commonly used at the end or egress of a network without redundant links.



Problems of OSPF Design



- Generally, OSPF provides precise algorithms to prevent serious problems such as loops. However, improper design may cause problems such as area split and sub-optimal routes.
- The first topology shows a routine route design scenario. No problem occurs during the initial design; however, link faults in the backbone area may cause area split and routing problems.
- The second topology also shows a routine route design scenario that sub-optimal routes exist. When two routers at the access layer access each other, traffic does not pass through links between aggregation routers. Instead, they use the dual-homed uplink access routers.
- OSPF is stable and reliable. Take OSPF design into full consideration to avoid problems similar to those presented in the topologies.



Case Discussion - Routing Boundary and Routing Protocol

- Routing protocols need to be deployed on campus networks to function as route bearers. Questions:
 - Which routing protocols do you want to select?
 - Where is the boundary between the Layer 3 routing network and Layer 2 switching network deployed?
 - What is the routing protocol design?

- OSPF is optimal for campus networks. It well adapts to such networks.
- In practice, user gateways are commonly deployed at the aggregation layer, compromising O&M complexity and network performance well. No redundant links exist between aggregation and access switches on current campus networks, so Layer 2 loops does not occur.
- Redundant links exist between aggregation and core switches. These devices work in routing mode, accelerating network convergence and improving link utilization.
- OSPF is a hierarchical routing protocol, and can be used to divide areas during deployment.
- On a campus network, access switches work on the Layer 2 network. Therefore, you do not need to use any routing protocol.
- You can allocate switches at the aggregation and core layers into different areas.
- Configure the OSPF backbone area at the core layer of the campus network. You can divide networks with other modules into areas.



Case Study - IP Address Allocation

- IP address allocation solution
 - The network segment 10.0.0.0/8 is recommended due to the scale of the campus network. (If education network segments are specified, use the corresponding ones.) In this case, network segments are divided based on the principle of one room per VLAN.

Building No.	Floor	Unit	Room No.	Network Segment	Gateway IP Address
Building 1	1st floor	Unit 1	1	10.11.11.0/29	10.11.11.1/29
			2	10.11.12.8/29	10.11.12.9/29
		Unit 2	1	10.11.21.0/29	10.11.21.9/29
			2	10.11.22.0/29	10.11.22.9/29
	2nd floor	Unit 1	1	10.12.11.0/29	10.12.11.1/29
			2	10.12.12.8/29	10.12.12.9/29
Building 2	1st floor	Unit 1	1	10.21.11.0/29	10.21.11.1/29

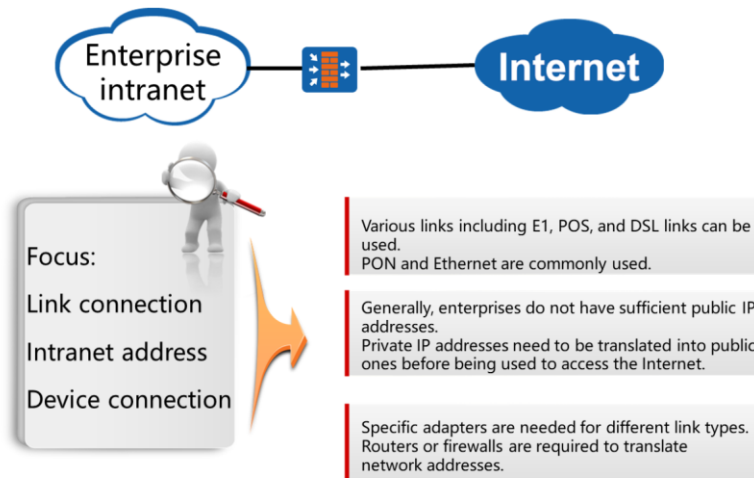


Contents

1. Overview
2. Physical Network Design
- 3. Logical Network Design**
 - LAN Design
 - WAN Design
 - Route Architecture Design
 - Network Egress Design
 - High Availability Design
4. Other Network Technologies
5. Overall Technological Solution



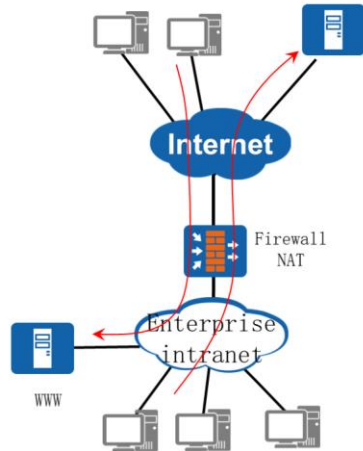
Network Egress Access Technology



- Internet access is a basic requirement for enterprise networks. You need to solve the following problems before accessing the Internet.
- Link selection: You can use any type of links to connect to the Internet; however, we need to consider multiple factors including bandwidth, cost, quality, and distance. Currently, enterprise networks use fibers to bear traffic at the egress. PON and Ethernet are commonly used. Some small-sized enterprise networks use home access technologies such as DSL.
- IP address: Enterprise networks commonly use private network segments due to insufficient public IPv4 addresses; therefore, Network Address Translation (NAT) is required before intranet users access the Internet.
- Device configuration: You need to deploy corresponding devices when using different links. For example, you need to configure DSL modems for DSL links and ONUs for PON links. Network egress devices need to translate IP addresses. Switches except modular switches do not support NAT. In this case, routers or firewalls commonly function as egress devices.
- NAT requires strong processing capability. Firewalls apply to networks with large scales and heavy traffic compared with routers. NAT is commonly deployed on network boundaries. Firewalls can also protect boundaries. In this case, firewalls are commonly deployed on enterprise network boundaries.



Single-Egress Network Architecture



Public IP address requirements

- Connection address
- Address pool

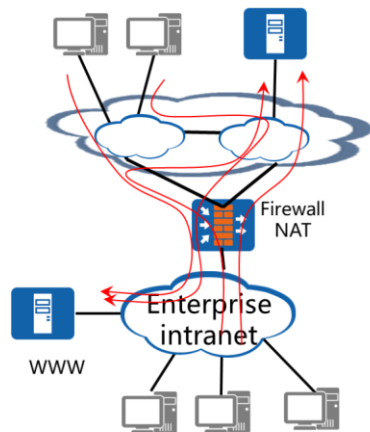
Traffic type

- Internal PCs access external servers
- Internal servers provide external services

- Single-egress networks are not highly reliable, but provide low cost and simplified architecture, and are widely used for non-key services of small-, medium-, and large-sized enterprises.
- Carriers provide two types of public addresses for Internet access. One type of public address is the connection address with the mask length of /30 and is configured on a connection link. The other one is an address pool, which is used for address translation when enterprise' internal devices connect to the Internet. Generally, this address pool does not have enough addresses to be allocated to each internal PC. When a small-sized enterprise uses PPPoE, the enterprise will obtain a dynamically allocated public IP address.
- An enterprise network with a single egress often uses static default routes pointing to the Internet. Carrier networks usually use static routes for return traffic due to trusted boundary problems.
- An enterprise's Internet traffic can be classified into: traffic generated by internal users to access external servers and traffic generated by external users to access internal servers. The major difference between the two types of traffic is that internal servers must have fixed public addresses to ensure that clients can access services at any time. In a project, static NAT is often used to map internal server addresses to public addresses, whereas internal users use dynamic Port Address Translation (PAT) to reuse public addresses to the maximum degree.



Single-Carrier and Multi- Egress Network Architecture

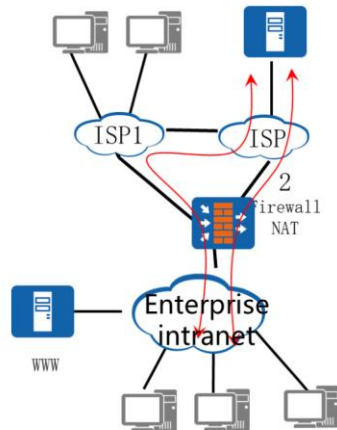


- Providing redundancy
- Two connection addresses, and one address pool
- Outbound path selection
 - Route direction
- Inbound path selection
 - Lack of controllability

- Some enterprises deploy two egresses to improve redundancy. When the two egresses are connected to the network of a single carrier, the carrier provides two connection addresses and an address pool. Address translation on this network is similar to that on the network with a single egress for exchange of internal and external data. However, paths need to be selected for the two links.
- Generally, a dynamic routing protocol is not deployed between a carrier network and an enterprise network due to trusted boundary problems. Data flows generated by accessing enterprise networks are not controlled, but are transmitted to corresponding interfaces based on routing protocols.
- For enterprises, data can be distributed based on detailed static routes because two egresses are connected to the network of a single carrier. Regardless of the link where data is transmitted, there is no difference in performance. Data distribution is to fully utilize egress bandwidth.
- Some enterprises use two egress links in active/standby mode, which can be implemented using floating static routes.



Multi-Carrier and Multi-Egress Network Architecture - Outgoing Traffic

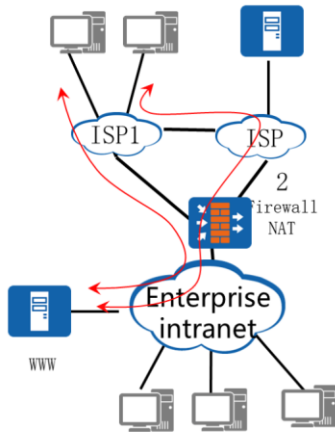


- Connection condition
 - Two connection addresses
 - Two address pools
- Outbound path selection
 - Optimal selection of path
- NAT address pool selection
 - Corresponding to path selection

- Medium- and large-sized enterprises commonly use dual-carrier and dual-egress solution. Each carrier provides a connection link, a group of connection addresses, and an address pool.
- Generally, a data path exists between two carrier networks, which is commonly deployed at the core layer but not in the local area, and the connection between carriers is not robust than an internal connection of a carrier network. In this case, when traffic passes between carriers, the service quality will deteriorate.
- When there is traffic of access to external networks by internal users, traffic must be transmitted over a correct link. If the traffic is transmitted over an incorrect link, the service quality will deteriorate. Because static routes are generally deployed between enterprises and carriers, carriers' public address space needs to be collected.
- You also need to consider returned traffic, which depends on address pool selection. When the NAT address pool for outbound traffic is provided by ISP1, returned traffic must pass through the link of ISP1. In this case, the NAT address pool needs to be bound to the outbound interface.



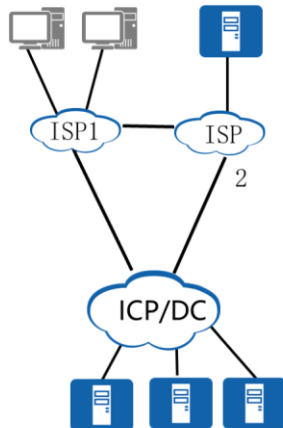
Multi-Carrier and Multi-Egress Network Architecture - Server Access Traffic



- NAT mapping
 - The server IP address is statically mapped to addresses of two address pools
 - The link through which users access a server depends on the address used for the connection
- Outbound path selection
 - Static route selection



Multi-Carrier and Multi-Egress Network Architecture - Peer-to-Peer Mode



- This mode is commonly used in ICP and DC scenarios.
- Public IP addresses and AS numbers are required.
- NAT is not performed.
- BGP route selection is required.

- The enterprise network egress discussed in the preceding slides is used to connect to the Internet. In another solution, the egress connects to the Internet as an entity. However, this connection mode requires a public address and AS number applied from the global network information center, and is commonly used in scenarios such as the ICP and DC where many servers provide services for the Internet.
- When the network egress is connected in this way and provides external services, NAT is not required. The egress exchanges routing information with ISPs using BGP, and follows the BGP principle during path selection.



Project Case

- A campus network connects to an education network using a single link, and internal servers provide services for the education network. Design network egress architecture for the campus network.

- This is a simple single-egress network architecture design. However, you need to consider two types of traffic. One is generated by internal users to access external servers, which requires NAPT. The other is generated by external users to access internal servers, which requires static NAT.



Contents

1. Overview
2. Physical Network Design
- 3. Logical Network Design**
 - LAN Design
 - WAN Design
 - Route Architecture Design
 - Network Egress Design
 - High Availability Design
4. Other Network Technologies
5. Overall Technological Solution



Definition of High Availability

Availability $\text{MTTF}/(\text{MTTF}+\text{MTTR}) * 100\%$

Mean Time to Failure (MTTF)

Mean Time to Restoration (MTTR)

Methods to improve availability:

Improve the MTTF

Shorten the MTTR

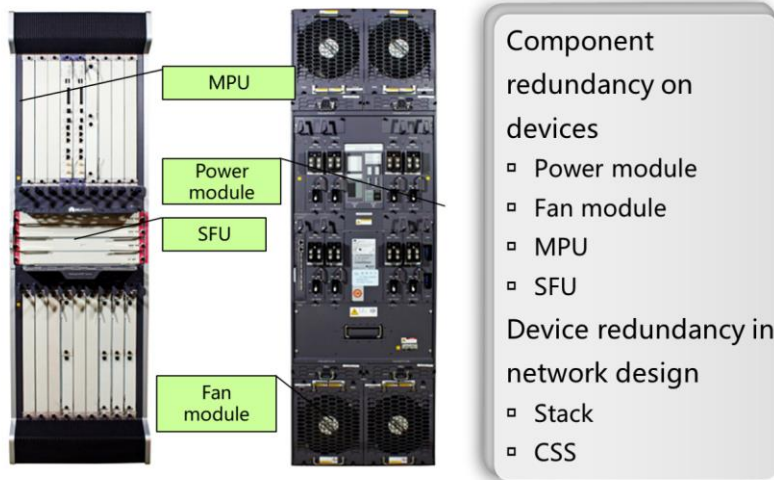
Implementation mode:

component, device, link, and service redundancy

- High availability is that network devices and systems can shorten the network interruption time and ensure network service availability time after design. Generally, high availability is measured using the MTTF and MTTR. To improve network availability, you need to increase the MTTF and shorten the MTTR.
- To improve network availability, you need to use highly reliable devices that often use redundant components. Multi-device and multi-link redundancy can be used. This design prevents service interruption and ensures that services are automatically switched to backup links when one device or link fails. Device and link switchover require protocols. Some protocols such as STP and routing protocols implement dynamic path selection and path switchover. Other protocols such as VRRP and BFD are designed to improve network system availability.



Component and Device Redundancy



- To improve system availability, first use proper devices. A component may become faulty. The way to improve system availability is to use redundant components. Generally, fixed switches are used as low-end access devices. There is no high requirement for availability and such switches do not use redundant components. In contrast, modular switches are often used as aggregation or core switches. Faulty modular switches affect a large network scope. Therefore, the modular switches often use redundant components such as redundant power modules, fan modules, MPU, and SFUs. When a component is faulty, the switch continues to provide services.
- To further improve network system reliability, switches provide stacking or CSS. Some fixed switches support stacking, which virtualizes multiple devices into one. Huawei modular switches provide the Cluster Switch System (CSS) function. CSS enables two modular switches to set up a cluster.



Link Redundancy



Multilink PPP



Eth-Trunk



E-Trunk

- Multilink PPP
 - Bandwidth increase
 - Data fragmentation and reassembly
 - Multi-link load balancing and backup
- Eth-Trunk
 - Link bundling
 - Load balancing and backup
 - Inter-device link bundling

- Some link-layer protocols provide multi-link bundling technologies to increase bandwidth and shorten the network delay. Such technologies also improve network availability. Bundled links load balance traffic. When a link is terminated, traffic can be dynamically transmitted to the other normal link. Such switchover is implemented at the link layer, which is much faster than that at the network layer.
- Common link bundling includes PPP Multilink and Eth-Trunk. PPP can maintain links dynamically, and implement packet fragmentation and assembly. Generally, Eth-Trunk only implements load balancing between links but not packet fragmentation. Eth-Trunk can work in manual or LACP mode. The LACP mode is recommended because Ethernet does not provide OAM.
- Huawei also provides E-Trunk that bundles Ethernet links across the devices and is used in scenarios demanding high reliability.



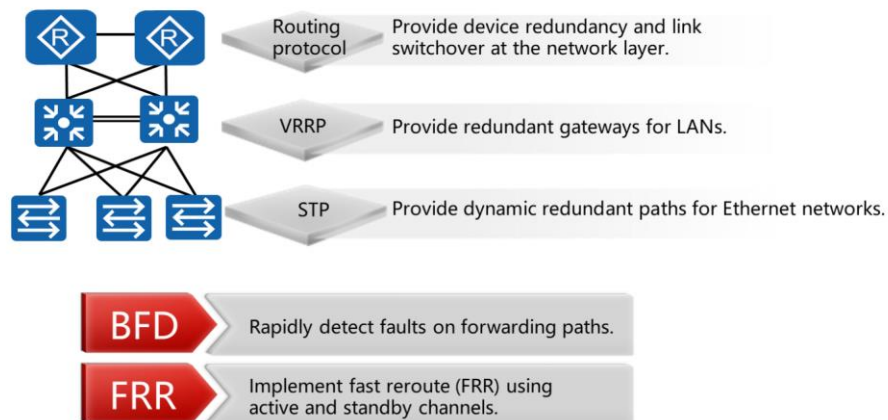
Project Case

- After the assessment by both parties, the engineering personnel and school campus network project group reach a consensus that requirements for network reliability are different on different components. For example, access in dormitories requires low reliability, while high reliability is required at the aggregation and core layers. Design a network as required.

- Many students access the campus network, and services are not the key issue. In this case, you do not need to use redundancy, especially device redundancy, at the access and aggregation layers. Considering bandwidth usage, you can connect access devices to aggregation devices through, and connect aggregation devices to core devices through dual links. Modular switches in dual-node redundancy mode are deployed at the core layer, and they work in load balancing mode normally.
- Access and aggregation devices work at the access and aggregation layers respectively, and gateways are deployed on aggregation devices. Aggregation devices and gateways do not need redundancy. STP is used to prevent loops caused by misoperations. Routing protocols provide failover and assurance at the core layer. Complex technologies such as BFD and FRR are not used because Internet access service is not the key service.



Protocols and Mechanisms to Improve Availability



- For the IP protocol design, the node fault problem is considered. Routing protocols and spanning tree protocols allow traffic to be switched between paths dynamically during path selection and provide switching when redundant links exist on networks, ensuring network availability.
- Generally, terminals do not run routing protocols and use static routes pointing to gateways. You can use VRRP to provide gateway redundancy. Generally, the VRRP switching time is about 3 seconds.
- For either routing protocols or VRRP, the prerequisite for a switchover is that faults are detected. Generally, the local device periodically sends specified packets to the remote device, and then monitors traffic on the corresponding interface. If no packets are received from the remote device after a period of time, the local device considers that the remote device fails. Such detection mode commonly lasts for less than 10 seconds to dozens of seconds. BFD is developed to shorten fault detection time. BFD can send detection packets and identify faults in milliseconds.
- FRR pre-calculates a backup route to protect the primary route. When the primary route is unreachable, FRR rapidly switches services to the backup route. Multiple steps including route update, SPF calculation, and loading of new routes are omitted during such a switchover, greatly reducing the switchover delay.
- Common datacom networks do not necessarily require millisecond-level convergence. In this case, BFD and FRR are widely used on IP bearer networks but not common datacom networks.

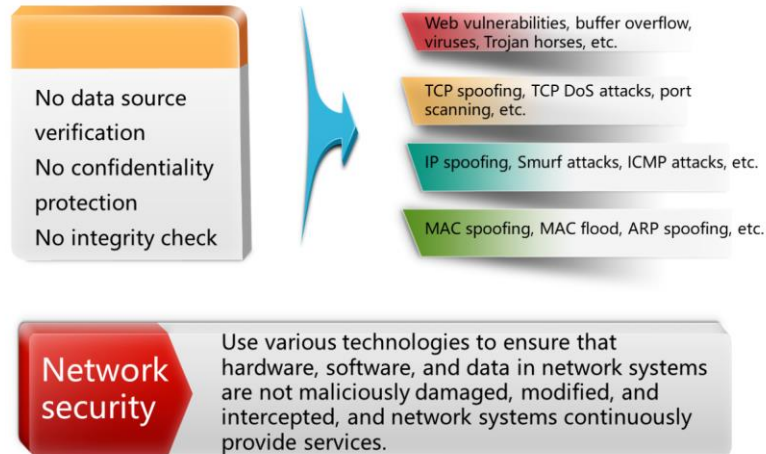


Contents

1. Overview
2. Physical Network Design
3. Logical Network Design
- 4. Other Network Technologies**
 - Network security
 - VPN
 - WLAN
 - DC
 - Network Management
5. Overall Technological Solution



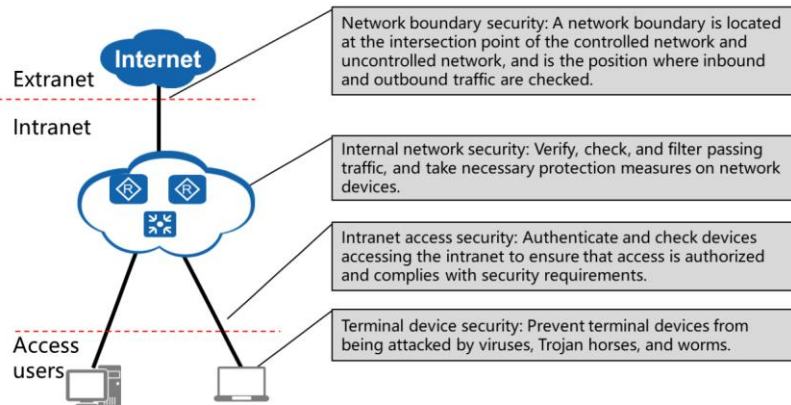
Network Security



- Most protocols in the TCP or IP protocol stack do not provide necessary security mechanisms. For example, they do not provide authentication services, transmit plain-text data, do not provide data confidentiality, data integrity, and non-repudiation service, and do not ensure availability.
- Network systems are usually attacked due to limitations on protocols and implementations. The preceding figure shows potential attacks at each network layer.
- Network security requires an all-round defense system that includes physical security, security management and so on. Security technology is one of the ways to realize network security. You can perform device configurations or deploy security devices to prevent network attacks and maintain network services.



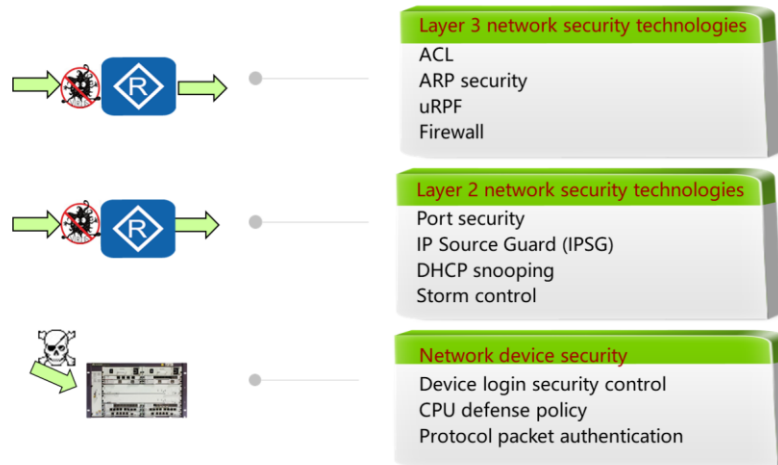
Network Security System



- For an enterprise network, the intranet is controllable and the extranet is uncontrollable. Generally, security isolation and check are configured at the boundary of the intranet and extranet.
- Intranet security threats such as information leakage due to employee violations and misuse of the intranet are increasing, so intranet security is important for network defense. Intranet security covers the following three aspects:
 - Intranet security: Network devices need to ensure their security so that they are not attacked and can work normally and continuously. Routers and switches on the intranet can use their security features to process network traffic.
 - Intranet access security: The devices that need to access the intranet should be authenticated, and unauthorized devices need to be prevented from accessing the intranet or using enterprise intranet resources.
 - Terminal device security: Security policies need to be configured and security software needs to be deployed on terminals to protect them.



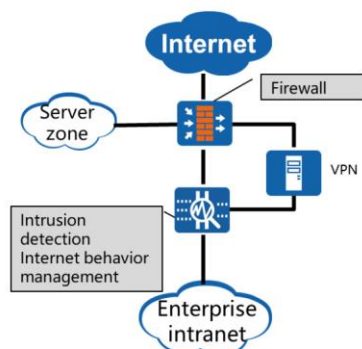
Security Technologies



- Basic network devices such as routers and switches on networks provide security features. Such security features just need to be configured correctly, without dedicated hardware. They apply to scenarios with required security features, low budget, and low performance requirements.
- Much calculation on routers is based on software. Routers can provide many security features after proper software is installed. For example, routers can control ARP entries to limit the ARP update speed. Routers check the source IP address of IP protocols to prevent attacks caused by forged source IP addresses. ACL technology, a basic security function of network devices, can filter packets based on the quintuple and provide control of routing protocols. Some firewalls provide more security features. For example, they can filter data based on the connection state and provide functions such as IPSec access.
- Switches work at Layer 2, and provide many security features to prevent Layer 2 attacks. For example, they use port security to prevent MAC address flood attacks, use DHCP snooping to prevent DHCP-based attacks, ARP attacks, and attacks from forged source IP addresses. Storm control is used when network traffic is abnormal.
- Network devices may be maliciously attacked, so they need to provide security features to ensure normal operating. For example, when a user remotely logs in to a network device, the user needs to be authenticated. To improve login security, you are advised to use encryption protocols such as SSH and HTTPS. Defense of the control plane on network devices is important. Devices provide rate limiting and filtering on the control plane, preventing exceptions caused by attacks. Besides, network devices run multiple protocols including routing protocols. Attackers may use protocols to attack a network. To prevent such attacks, enable neighbor authentication of protocols and disable protocols for ports on unauthorized devices.



Network Boundary Security

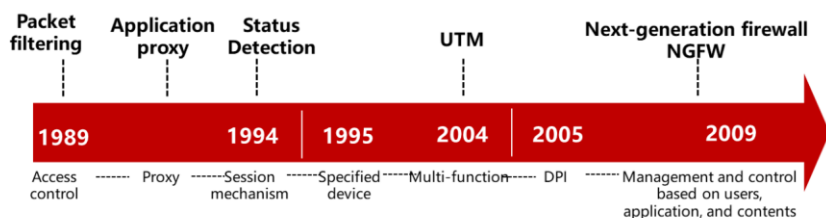


- Intersection point of the controlled network and uncontrolled network
- Firewalls- basic security devices
 - Filtering data flows based on the quintuple and session status
- IDS/ IPS
 - Scanning and monitoring application layer data of connections
- Other security systems
 - Antivirus system
 - External user access (VPN)

- An enterprise network often needs to connect to external networks including the Internet and partners' networks. An enterprise has full control of its intranet, but cannot control external networks. For enterprises, external networks are insecure and need to be isolated. There are address management problems between management entities, and NAT is required to translate addresses.
- Firewalls are deployed at the network edge to filter data traffic from external networks, and can defend against most attacks from external networks. Firewalls are configured with zones, and devices with different security levels are assigned to zones. For example, servers can be deployed in a separate zone.
- The IDS or IPS system is also used to protect boundary security. Firewalls can defend against attacks based on traffic information such as the protocol and port number, but cannot defend against some application-based attacks. The IDS or IPS system detects traffic based on traffic behaviors and attack databases, and can defend against intrusion threats that firewalls cannot defend against, improving the network boundary security. The IDS system is often deployed in bypass mode, and generates alarms and records about detected attack traffic only. The IPS system is deployed in inline mode, and can directly block the attack traffic.
- Other dedicated security devices can be also deployed at the network egress. The devices include antivirus walls and VPN devices for remote access. They provide specific functions to improve security, but are seldom used.



Evolution of Firewalls

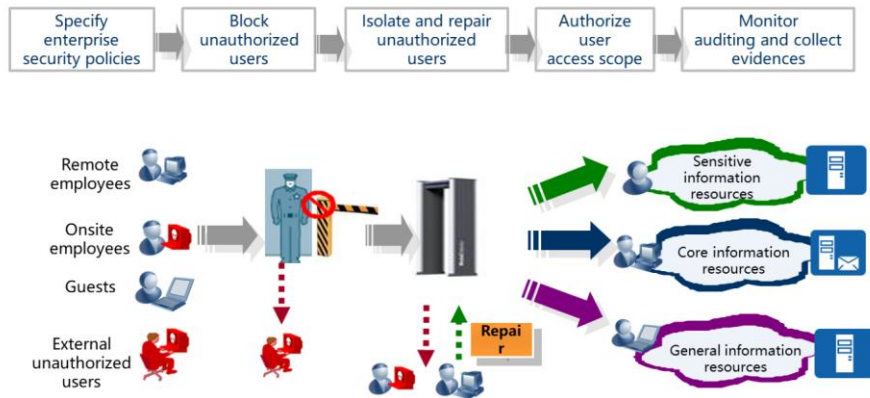


- Firewall technology has been developed and innovated for multiple times.
- Stateful inspection firewalls are mainstream ones.
- Firewalls integrate multiple security functions including intrusion detection and antivirus.
- Huawei USG firewalls are Next-Generation Firewalls (NGFWs).

- Firewalls emerged in the late 1980s, and have three generations during more than twenty years' development.
 - Packet filtering firewalls: The working mechanism is similar to that of ACL technology. A packet filtering firewall filters data flows based on the quintuple. Application proxy firewalls based on proxy technology also emerged during this period. They work at the application layer, providing high security but slow processing. Application proxy firewalls need to be separately developed for different applications. In this case, they are only used when a few applications or some specified applications require high security.
 - Stateful inspection firewalls: They are configured with zones and dynamically analyze the packet status to determine actions for packets. They can establish session information based on the quintuple of the first packet, and forward subsequent packets based on the session information. Compared with packet filtering firewalls, stateful inspection firewalls provide rapid processing and more security features. They do not need to be separately developed for different applications in the same manner as application proxy firewalls. Therefore, they become increasingly popular, but provide only basic firewall functions.
 - UTM devices and NGFWs: Besides firewalls, network security vendors developed some dedicated security devices including intrusion detection and antivirus walls. Some security vendors proposed the concept of United Threat Management (UTM) that integrates traditional firewall functions, intrusion detection, antivirus, URL filtering, application control, and mail filtering into a firewall, achieving comprehensive security protection. NGFWs are developed based on UTM, prevent performance deterioration when UTM is enabled with multiple functions, and perform management and control based on users, applications, and contents.
- Huawei promoted USG6000 series firewalls are NGFWs.



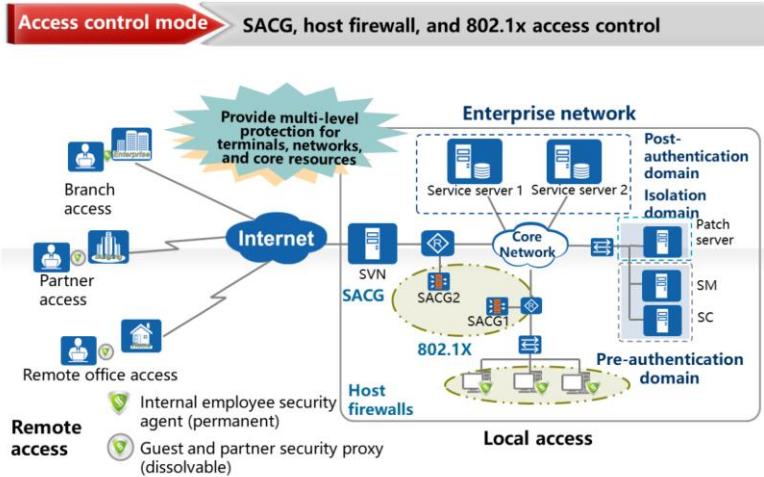
Intranet Access Security



- User intranet access is different from common network access. A user needs to be authenticated before accessing an enterprise intranet. After the user is authenticated successfully, mandatory compliance check including security status and system configuration check is performed. A server allows terminals that comply with compliance policies to access network resources based on check results. The terminals that do not comply with compliance policies can access the intranet only after violations are eliminated. The agent continuously monitors terminals, and responds to and records their violation behaviors. The entire process is a PDCA cycle.



Intranet Access Security Components



- Intranet access security covers the following aspects.
 - Identity authentication: ID, role definition, and external authentication system
 - Access control: software firewall, 802.1x switch, gateway access control, ARP, and DHCP
 - Security authentication: antivirus software, patch management, management of unauthorized access, storage media management, and online behavior management
 - Service authorization: right control for service systems and documents
 - Service audit: audit of service systems and documents



Introduction to Huawei Firewalls



USG6300/6500:

Is targeted for small- and medium-sized enterprises and chain organizations. Provides integrated security and management. Provides four to eight GE high-density interfaces. Two extended slots support 10GE interfaces. Provides integrated protection, integrates traditional firewall functions, VPN, intrusion prevention, and antivirus. Identifies more than 6,000 applications and provides high-precision access control.



USG6600:

Is the 10GE firewall that is targeted for medium- and large-sized enterprises and next-generation DCs. Is installed in a standard 19-inch rack with the height of 1U to 3U. Provides scalable 1000M electrical interfaces, 1000M optical interfaces, or 10GE optical interfaces, and support bypass cards. Provide integrated protection, integrate multiple functions, and be able to identify more than 6,000 applications. Support virtualization of multiple security services.



USG9000:

Is a Tbit/s firewall that is targeted for cloud service providers and large-sized DCs. Supports a maximum of 160Gbit/s service cards, 1.44Tbit/s throughput, and 1.44 billion concurrent connections. Supports GE, 10GE, 40GE, and 100GE interfaces and uses distributed framework. Provides integrated protection, and integrates firewall, IPS, VPN, and anti-DDoS functions. Provides superb reliability and 99.999% availability.

- The USG6000 uses next-generation firewall technology. It integrates multiple functions including traditional firewall functions, VPN, intrusion prevention, antivirus, data loss prevention (DLP), bandwidth management, anti-DDoS, URL filtering, and anti-spam. It can identify more than 6,000 applications, provide application-level access control, accurately detect and defend against network vulnerabilities and attacks, and identify and filter files and contents transmitted on a network. It also supports various high-reliability VPN features including IPsec VPN, SSL VPN, L2TP VPN, MPLS VPN, and GRE.
- The USG6000 is available in three models in ascending order of performance: USG6300, USG6500, and USG6600 series. And it supports virtualization of multiple security services. It can virtualize multiple firewalls, and intrusion prevention, antivirus, and VPN devices.
- The USG9000 is the next-generation Tbit/s firewall that is targeted for cloud service providers, large-sized DCs, and enterprise campus networks. It provides Tbit/s processing capabilities and 99.999% reliability, and integrates multiple security features including NAT, VPN, IPS, virtualization, and service awareness, helping enterprises implement DC boundary security protection oriented at cloud computing. It supports Carrier Grade Nat (CGN). A single firewall can virtualize a maximum of 4096 devices, and integrates multiple DDoS attack prevention functions including those at the application layer.



Other Huawei Boundary Security Products

**NIP6000:**

Is the next-generation intrusion prevention system that is targeted for enterprise, campus, and carrier networks. Effectively defends against common attacks including worms, Trojan horses, and SQL injection. Identifies multiple applications including mainstream P2P, IM, online games, and social networks. Extracts files from transmission protocols and analyzes them. Supports flow model self-learning.

**ASG2000:**

Is the enterprise-class professional online behavior management product. Identifies 1,200 mainstream applications and filters 85 million URLs. Provides professional audit reports and supports over 30 types of reports. Supports distributed deployment.

**USG2000BSR:**

Is targeted for small-sized enterprises, and integrates security, routing, switching, and wireless functions. Supports FE, GE, E1/CE1, serial, ADSL2+, and 3G access modes.

USG6000V:

Is an NFV- and cloud-based multi-service gateway. Supports 1 to 8 CPUs. Supports 1+1 or N+1 redundant deployment. Supports a maximum of 500 tenants.

- Huawei provides other boundary security products:
 - IDS or IPS: The NIP6000 is the next-generation intrusion prevention system, has environment perception, deep application perception, content perception, and defense against unknown threats. It can effectively defend against common attacks including worms, Trojan horses, botnets, cross-site attacks, and SQL injection, supports user-defined signature, and can flexibly and rapidly respond to sudden threats. It can identify over 6,000 application protocols including mainstream P2P, IM, online games, social networks, videos, and voice applications. It supports virus filtering and prevention for HTTP, FTP, SMTP, POP3, IMAP, NFS, and SMB. It can extract files from file transmission protocols including HTTP, SMB, FTP, SMTP, POP3, IMAP, and NFS protocols, and send files to the file detection engine for detection. It also can perform packet parsing, and threat detection and prevention for tunneling protocols including VLAN, QinQ, MPLS, GRE, IPv4 over IPv6, and IPv6 over IPv4.
 - The ASG2000 is an enterprise-class professional online behavior management product that is targeted for medium- and large-sized enterprises and carriers. It can identify 1,200 mainstream applications and filter 85 million URLs. It provides abundant application identification, comprehensive threat prevention, and comprehensive and professional reports. It integrates multiple security functions including application control, bandwidth management, URL filtering, malware defense, data loss prevention, and behavior audit.
 - The USG2000BSR is an enterprise-class multi-service security gateway that is targeted for small-scale enterprises. It integrates security, routing, switching, and wireless features (Wi-Fi/3G), provides abundant interfaces and high-density switching access, helping enterprises to realize all-WLAN networking. It also provides users with strong, scalable, and continuous security capabilities, and is the optimal choice for access of SOHO enterprises and small-sized offices.
 - The USG6000V is an NFV- and cloud-based multi-service gateway that is targeted for DCs. It runs on a VM platform and provides functions similar to those of a hardware firewall. It offers VM-based high-speed forwarding and supports 1+1 or N+1 redundancy.



Project Case

- Select devices to connect the school campus and education networks.
- On a school campus network, servers deployed in equipment rooms of some colleges contain sensitive information, and require high security. How is the network designed?

- There is the connected egress between the school campus and education networks. Common users on the school campus network do not require special security features. However, addresses need to be translated because the school campus network is connected to an extranet. You need to deploy a firewall at the egress. The firewall model depends on the estimated user quantity and concurrent session quantity. When a school campus network has a large number of users and massive concurrent sessions, you are advised to use the high-end USG6600. You are also advised to use dual-node redundancy because there are many users.
- You can use firewalls for isolation on some large-sized networks to improve network security. To further improve security, you can also deploy IPS devices on the network. Huawei USG firewalls only need to be enabled with corresponding functions.

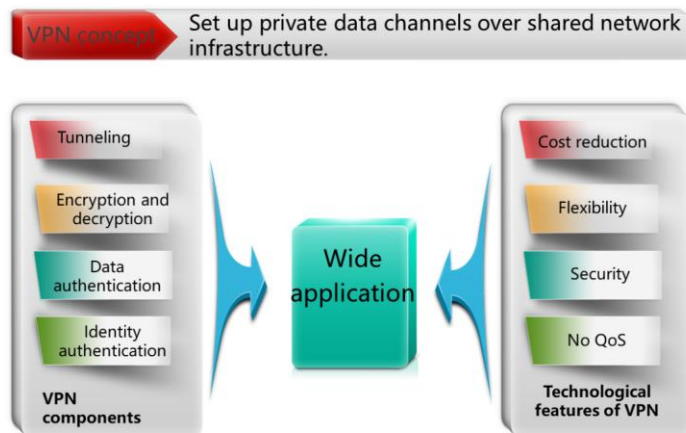


Contents

1. Overview
2. Physical Network Design
3. Logical Network Design
- 4. Other Network Technologies**
 - Network security
 - VPN
 - WLAN
 - DC
 - Network Management
5. Overall Technological Solution



VPN Introduction



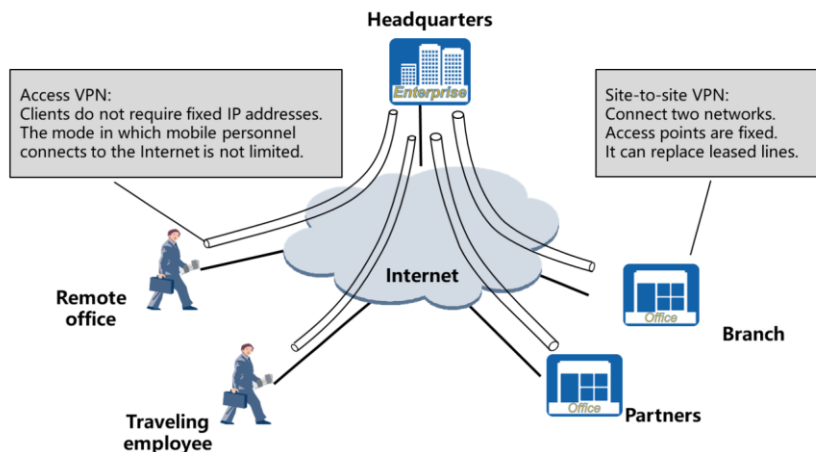
- Virtual Private Network (VPN) connects different networks and terminals that want to connect to the private network through private data channels created over shared network infrastructure. VPN provides security functions. Enterprises use Internet-based VPN.
- VPN is implemented using tunneling technology because enterprise data on a VPN needs to traverse public networks. To ensure network security, VPN also uses multiple security technologies including encryption and decryption, data authentication, and identity authentication.
 - Tunneling is the key technology of VPN. It establishes a data channel on a public network by using encapsulation and decapsulation at both ends of a tunnel, so that packets can be transmitted through this channel. Tunneling protocols used to establish tunnels are classified into Layer 2 and Layer 3 tunneling protocols. L2TP and GRE are typical Layer 2 and Layer 3 tunneling protocols, respectively.
 - Encryption and decryption technology converts data into encrypted data that cannot be identified, transmits the data, and decrypts the data at the destination. VPN ensures that data is not intercepted during transmission through encryption and decryption.
 - Data authentication technology ensures that data is not intercepted during transmission. Data authentication uses the hash algorithm that is irreversible and has a unique result. The algorithm can prevent data from being modified when digests are the same.

- Identity authentication can ensure validity of operators connected to VPNs. It authenticates user names and passwords, or uses the CA certificate to authenticate users when higher security is required.
- VPN has many advantages, and is widely used on an enterprise network and between enterprise networks.
 - VPN has low cost. With VPN, enterprises do not need to rent expensive WAN lines, and can build a network that geographically covers a large area through the Internet. In addition, connectivity between enterprise nodes is ensured through the Internet, reducing enterprises' O&M costs.
 - VPN greatly improves flexibility of network design, and can be used to establish connections on an enterprise network and between enterprise networks only when IP addresses are reachable. In this case, negotiation of lower-layer link parameters is not required. When you use VPN to expand networks, the cost is low because physical links are not required.
 - To ensure security of data transmission on the Internet, VPN uses identity authentication to determine identities of remote devices, encryption and decryption to ensure confidentiality of data transmission on the Internet, and data authentication to prevent data modification during transmission on the Internet.
 - VPN also has disadvantages. It is built across the Internet, so there is no good control on the intermediate network. For example, it is difficult to ensure QoS

such as the bandwidth and latency.



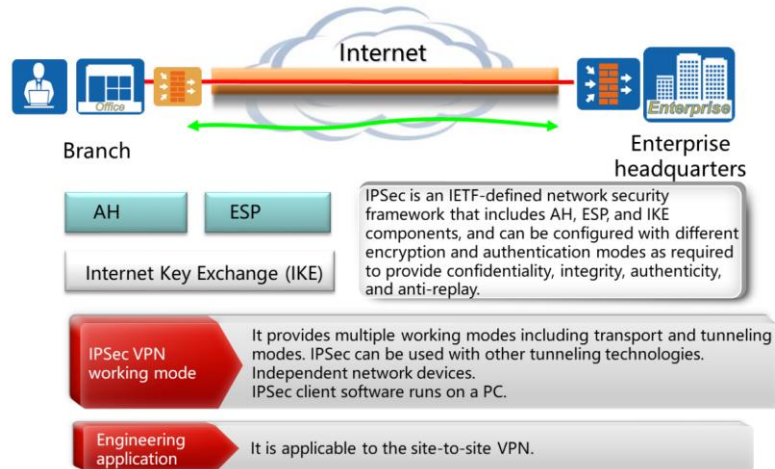
VPN Application Scenario



- VPN can be classified from different dimensions:
 - Layer 2 and Layer 3 VPNs based on the working layer
 - IPSec VPN, SSL VPN, and MPLS VPN based on the implementation technology
 - Access VPN and site-to-site VPN based on the application scenario and connection requirement
- Access VPN is widely used. You can use access VPN when enterprise internal users move or have the remote office requirement, or when merchants need to provide B2C security access services. Users without fixed IP addresses can remotely connect to the VPN using the PSTN, ISDN, xDSL, mobile IP addresses, and cables. In this case, users can access enterprise resources anytime and anywhere as required. Access devices are often PCs and other terminals. Enterprises often use dedicated network devices such as routers, firewalls, or VPN access devices to connect to servers. The servers connected to an access VPN use fixed IP addresses, whereas IP addresses of clients are commonly not fixed.
- Site-to-site VPN is the other common VPN mode. You can use the site-to-site VPN to connect two networks of the enterprise headquarters and branch or two enterprises. The traditional solution used to connect two fixed networks is to rent carriers' leased lines, and can be substituted by site-to-site VPN. Both ends of the site-to-site VPN use specified network devices, and devices at one or two ends need to use fixed IP addresses.
- Access VPN and site-to-site VPN have corresponding technologies. Some technologies apply to the two modes. However, technologies have their own characteristics and differences in various scenarios.



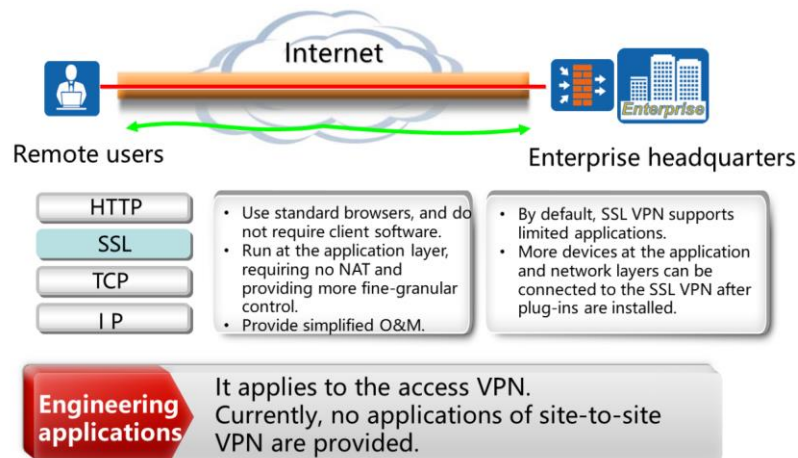
IPSec VPN Features and Applications



- IPSec VPN is one of the most widely used VPN technology. The IETF-defined IPSec VPN is an open and standard framework that includes a series of IP security protocols, and provides multiple functions including data encryption, integrity check, authenticity check, and anti-replay.
- IPSec VPN provides multiple working modes including transport and tunneling modes, so that it applies to various application scenarios. Besides, IPSec can be used with other tunneling technologies to implement corresponding functions.
- IPSec VPN is applicable to the site-to-site VPN and access VPN. When applying IPSec VPN to the site-to-site VPN, you need to enable IPSec VPN between specific network devices to connect networks through tunnels. The network devices need to support IPSec. Most routers and firewalls support IPSec. You also need to purchase licenses for some devices to implement data encryption.
- The currently popular desktop operating system does not provide the IPSec client. You need to install independent IPSec client software when applying IPSec VPN to the access VPN, which increases the maintenance workload of enterprises with massive users. Therefore, IPSec VPN is more applicable to the site-to-site VPN.



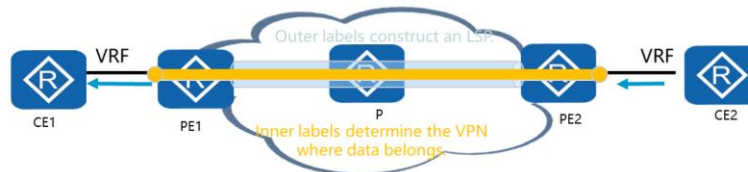
SSL VPN Features and Applications



- SSL is a security protocol, and provides security connections for TCP-based application layer protocols. SSL runs between the transport and application layers of the TCP or IP stack. It also provides security connections for HTTP. SSL VPN works at the high layer, so communication data is not limited by NAT and can traverse firewalls. This enables users to access intranet resources anywhere through SSL VPN virtual gateways.
- Users connected to the SSL VPN use standard browsers such as IE, Netscape, and Chrome to access internal applications of enterprises. In this case, mobile employees only require PCs with basic configurations but not dedicated VPN clients to implement secure remote access. SSL VPN is secure, easy, and available, greatly reducing the network O&M workload and improving working efficiency.
- Currently, SSL VPN only applies to the access VPN, and there is no case that SSL VPN applies to the site-to-site VPN.



MPLS VPN Features and Applications



- VPNs are implemented based on MPLS, BGP, or LDP, and are classified into Layer 2 and Layer 3 VPNs.
- VPN implementation is based on carrier networks, and VPNs are transparent to customer networks.
- MPLS VPN does not provide encryption and authentication functions.
- Carriers divide VPNs based on access ports.

Engineering applications

MPLS VPN can be the replacement of leased lines and applies to the site-to-site VPN. Contact local carriers for corresponding services.

- MPLS VPN technology provides VPN functions based on MPLS labels, and MPLS VPNs fall into Layer 2 and Layer 3 VPNs. You can use MPLS and BGP to implement the Layer 3 VPN. BGP advertises routes on the carrier backbone network so that MPLS can forward VPN packets on the carrier backbone network. To implement the Layer 2 VPN, you can use LDP or BGP to exchange Layer 2 control information on carrier's edge devices, establish LSP paths, and use MPLS to forward VPN packets on the carrier backbone network.
- MPLS is implemented on carrier networks, and the implementation is transparent to customer networks. Customers do not know data transmission on the carrier network. MPLS VPN especially Layer 2 VPN is similar to a carrier leased line in terms of customer perception.
- Unlike IPsec VPN and SSL VPN, MPLS VPN does not provide encryption and authentication functions. MPLS VPN only uses LSP tunnels based on MPLS labels to transmit data on a carrier network and isolate data. Customers need to implement data encryption if required.
- MPLS VPN is a type of carrier service but not the remote access solution of enterprises. When an enterprise requires remote links, the enterprise can contact the local carrier to use MPLS VPN links.



Huawei VPN Product Line



IPSec VPN:

IPSec VPN does not require dedicated devices, and is supported by common routers and firewalls. Note the number of connections, and purchase the required license. You need to configure IPSec VPN client software that runs on a PC when deploying the access VPN.

SSL VPN: SVN5600 or SVN5800

The SVN5600 or SVN5800 supports a maximum of 100,000 concurrent users, and mainstream operating systems including Android, Windows, iOS, MacOS, Linux, Symbian, and Blackberry. It supports SSL VPN, IPSec VPN, GRE VPN, and L2TP VPN. It supports web proxy, network extension, file sharing, and port forwarding.

Other VPNs:

MPLS VPN: There are no special requirements for client devices, and common network devices such as routers and switches can use MPLS VPN.
L2TP and GRE VPNs: Common routers and advanced switches support the functions.

- VPN does not require dedicated devices in many scenarios. VPN encryption and decryption are implemented through software, so many VPN technologies can be implemented on a universal hardware platform. When configuring devices, note that many network devices require the purchased license to provide VPN functions. VPN encryption and decryption require strong processing capabilities. The performance of the hardware platform must be sufficient to support large-scale VPN access. The hardware of some advanced devices is optimized to improve the connection quantity and encryption and decryption capabilities.
- Huawei provides the dedicated VPN platform: SVN5600 or SVN5800 series. The SVN5600 or SVN5800 provides the following functions:
 - A maximum of 100,000 concurrent users and 512 virtualized gateways
 - Multiple mainstream operating systems including Android, Windows, iOS, MacOS, Linux, Symbian, and Blackberry
 - VPN solutions including SSL VPN, IPSec VPN, GRE VPN, L2TP VPN, and MPLS VPN
 - 10 authentication modes, multi-level authentication, and hybrid authentication
 - Web proxy, network extension, file sharing, and port forwarding
 - Comprehensive protection that ensures security of terminals, data channels, servers, and remote access
 - Smart route selection in multi-egress scenarios, dynamic selection of distributed gateways, access bandwidth management, and agile access experience



Project Case

- A university has the headquarters and branch networks located in different cities. Design a cost-effective network solution for data exchange between the headquarters and the branch networks.
- Some college teachers want to log in to the school campus network when they are at home or on a business trip. What solution do you adopt?

- You can use the traditional WAN technology to connect college networks. For example, you can rent leased lines. However, renting leased lines especially long-distance leased lines is expensive. The cost-effective method is to use VPN, so that branch campus networks are connected over the Internet. You are advised to use IPSec VPN to connect two campus networks. You can deploy hardware devices such as Huawei USG series firewalls at the egress of the campus network, and determine the hardware performance requirement based on network traffic.
- You also can use VPN to ensure remote access of mobile users. You can use SSL VPN for access of many mobile users, eliminating the need to maintain mobile clients.

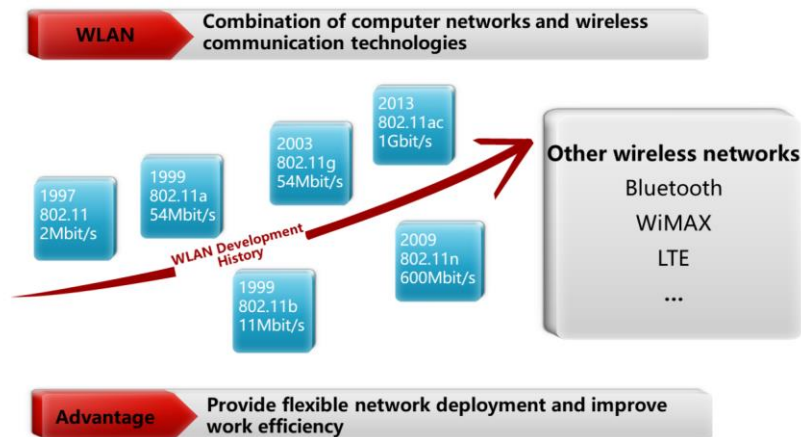


Contents

1. Overview
2. Physical Network Design
3. Logical Network Design
- 4. Other Network Technologies**
 - Network security
 - VPN
 - WLAN
 - DC
 - Network Management
5. Overall Technological Solution



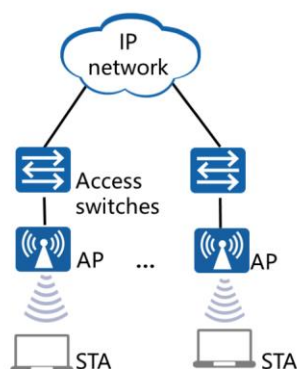
Introduction to WLAN



- WLAN technology was developed first in America and mainly applies to households. WLAN does not require cabling, so it becomes popular quickly. Recently, WLAN is widely used in scenarios including households, offices, schools, and enterprises.
- After over ten years of development, WLAN standards and products have become mature. The IEEE 802.11 working group has defined a series of WLAN standards that range from 802.1 standard (2Mbit/s) to 802.11ac standard (1Gbit/s).
- Compared with wired access technologies, WLAN has the following advantages:
 - ❑ Mobility: Mobile users can continuously connect to the network in a specific area without being restricted by any access position, greatly improving productivity.
 - ❑ Flexibility: For traditional wired networks, cabling is difficult in some scenarios. However, WLAN can be flexibly deployed in such scenarios. You can also use WLAN to rapidly build small and temporary networks.
 - ❑ Cost effectiveness: WLAN contributes to cost saving. Traditional wired networks require costly network cables, whereas WLAN does not require network cables, which also saves the cabling cost. Besides, you can use the wireless bridge to replace traditional carrier leased lines in certain scenarios such as network interconnection between two close buildings, greatly reducing network operation costs.
- A single AP of a WLAN covers the distance with a radius of about 100 meters, and is applied to most enterprise network application scenarios. Besides WLAN, the following common wireless network technologies are also provided:
 - ❑ Bluetooth works at the 2.4 GHz frequency band. It is used for Wireless Personal Area Network (WPAN)s, and covers the distance with a radius of no more than 10 meters.
 - ❑ WiMax (802.16) is a wireless MAN technology that covers the distance with a radius of 10 kilometers, and provides a rate of tens of Mbit/s.
 - ❑ Mobile data network: Widely used mobile access technologies such as GPRS, EVDO, HSDPA, and LTE are included.



Fat AP Wireless Network

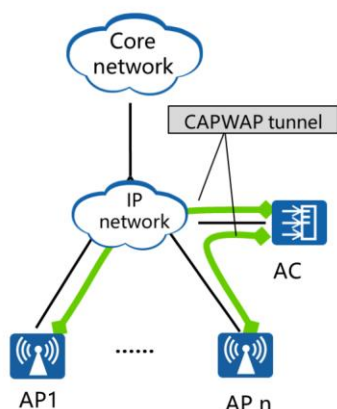


- A Fat AP provides complete protocol stack and runs independently.
- A Fat AP provides complete and abundant functions:
 - DHCP
 - FW-NAT
- Each Fat AP is separately managed.
- Inter-AP roaming is not supported.
- A Fat AP applies to a small-sized network.

- A Fat AP has a complete protocol stack, and can run independently without depending on other network devices. Besides, a Fat AP can implement wireless access, provide DHCP and NAT functions, and allocate IP addresses to clients.
- When multiple Fat APs are deployed on a network, they work independently. In this case, you need to manage and configure them independently or through the NMS.
- Fat APs do not support roaming between them. Users who move from one AP to another AP need to connect to the network again.
- Fat APs are often used in households and SOHO scenarios with small wireless coverage areas.



Fit AP+AC Wireless Network



- A Fit AP provides an incomplete protocol stack, and needs to be used with an AC.
- A Fit AP can be easily deployed and managed.
- Fit APs are managed in a centralized manner.
- Inter-AP roaming is supported.
- A Fit AP applies to a large-sized network.

- Fit APs cannot be independently configured or used. A Fit AP must be used with an AC to provide complete wireless access.
- CAPWAP runs between the AC and Fit APs. Control packets between APs and the AC must be forwarded through CAPWAP tunnels, whereas data packets can be forwarded directly or through CAPWAP tunnels. The AC can be configured in inline or bypass mode.
- An AC manages all connected Fit APs, greatly reducing the management burden. Fit APs support zero-touch configuration. New APs only need to be installed physically, and then they can automatically discover an AC, and are managed and configured by the AC.
- Users can roam between APs that are connected to the same AC, without connecting to the network again.
- Compared with Fat APs (independent APs), Fit APs achieve rapid deployment of WLANs, centralized management of network devices, and fine-grained user management. Fit APs are more applicable to wireless networking of large-sized enterprises in terms of O&M.



Huawei Wireless Network Products



- Indoor settled APs: are recommended in scenarios where the building structure is simple, the building area is small, there is a high density of users, and a high capacity is required, for example, small-scale meeting rooms, bars, and entertainment places. The APs can be flexibly deployed and works in both Fit AP and bridge mode.
- Outdoor settled APs: are recommended in scenarios with high-density users, for example, schools and large exhibition centers.
- Indoor distributed APs: are recommended in scenarios where the building area is large, users are distributed, and an indoor distribution system is used, for example, large-scale office buildings, business buildings, hotels, airports, and bus stations. They can implement indoor WLAN signal coverage.
- The AC6005 has a large capacity and high performance. It is highly reliable, and easy to install and maintain. It can manage 4 to 128 APs, and supports 4Gbit/s wireless processing capabilities.
- The AC6605 has a large capacity and high performance. It is highly reliable, and easy to install and maintain. It can manage 4 to 512 APs. It supports a maximum of 128Gbit/s switching capacity and 10K wireless users.
- The SPU for WLAN services is also called the ACU. It provides AC functions. It can be installed in the S9300. By default, an SPU can manage 128 APs. With purchased license, it can manage a maximum of 1024 APs. It supports a maximum of 32K wireless users.



Contents

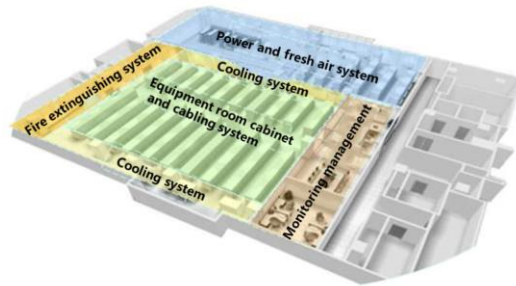
1. Overview
2. Physical Network Design
3. Logical Network Design
- 4. Other Network Technologies**
 - Network security
 - VPN
 - WLAN
 - DC
 - Network Management
5. Overall Technological Solution



Introduction to Enterprise DCs

DC

Provide IP infrastructure for enterprises' key service systems.
Function as the core data management center for enterprises



Comprehensive solution

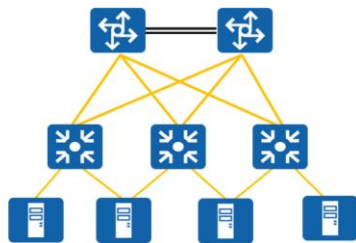
- Equipment room cabinet
- Power supply system
- Cooling system
- Cabling system
- Servers
- Network system

Network system is part of an enterprise DC

- Internal servers of an enterprise are often installed in an equipment room, or a DC when its scale is large enough.
- A DC is a comprehensive IP infrastructure that contains many integral subsystems such as power supply, cooling, and cabling systems. The network system is part of a DC.



Traditional DC Network



Characteristics of DCs

- Small geographic scope
- High bandwidth requirement
- High reliability requirement

The structure is similar to that of a campus network.

- Traditional routing and switching technologies
- On-demand layering

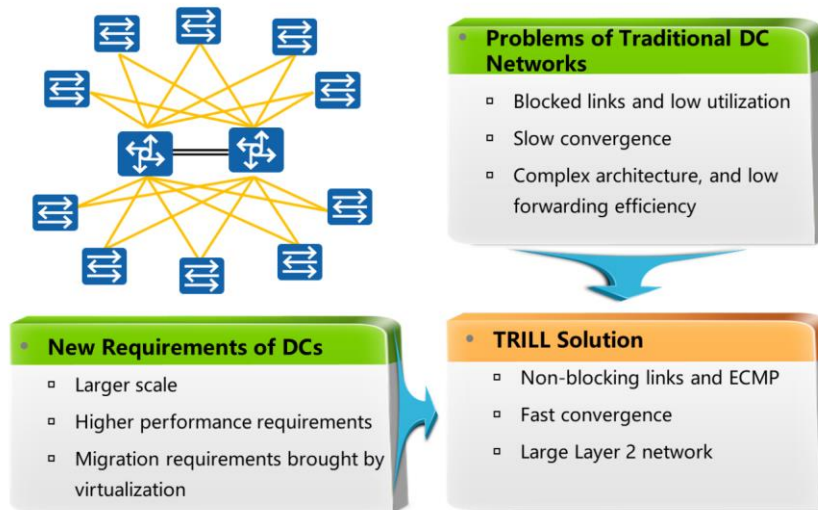
Characteristics of DC networks

- High-performance switches
- High-bandwidth or optical links
- Stacking/Multi-link redundancy

- Traditional DC networks directly use the routing and switching architecture similar to that of campus networks, without using any special new technologies. Network layering is based on the network scale.
- DCs have characteristics such as smaller geographic areas than those of campus networks. For an enterprise, a DC occupies one or more equipment rooms. Switches are mainly deployed in a DC, and routers and security devices are deployed at the egress.
- Devices in a DC are generally servers that provide services for enterprises, generating heavy data traffic. Servers are required to ensure continuity, so DCs have high requirements on network performance and reliability. During DC design, devices with high performance and high port density are often deployed. In addition, high-bandwidth fiber links, multi-link redundancy, device stacking, and clustering are used to improve network reliability.



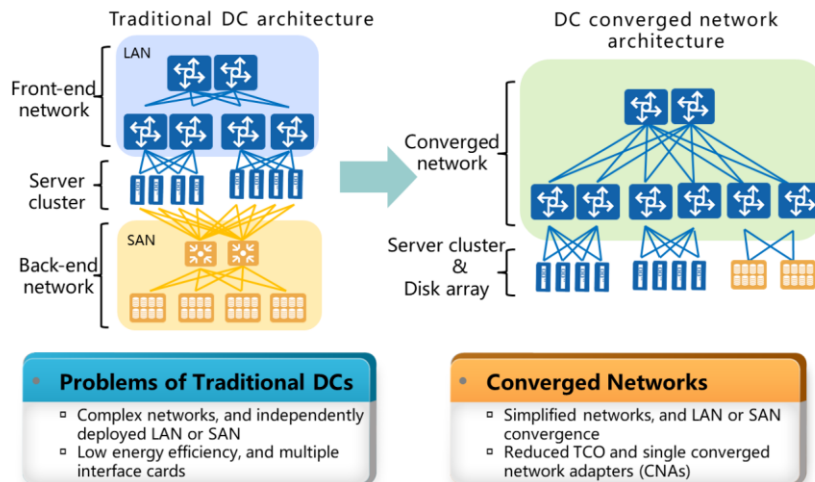
New Technology of DC Networks - TRILL



- The traditional DC architecture meets requirements of small- and medium-sized enterprises, but the traditional routing and switching network architecture has certain problems. For example, STP is used on a traditional Layer 2 switching network to block links to prevent loops. STP has slow convergence. For key application services, convergence of dozens of seconds is unacceptable. Blocked links do not transmit traffic, wasting links. The DC that transmits key enterprise services uses much redundancy in design, causing slower convergence and a great waste of links. Besides, traditional networks are extended by combining Layer 2 and Layer 3 networks. An additional layer means increasing network complexity, and the forwarding performance of a Layer 3 network is much lower than that of a Layer 2 network.
- The computing model of DCs has great changes. In particular, new technologies such as cloud computing have been widely used, bringing tremendous changes to the scale and traffic model of DCs. For example, the server quantity and data exchange in a DC increase dramatically. As virtualization is used, migration of VMs in a DC requires extension of Layer 2 networks.
- Transparent Interconnection of Lots of Link (TRILL) is a Layer 2 (link layer) network standard recommended by IETF. It can resolve multi-path problems on large Ethernet networks, and is well applicable to DCs. TRILL has the following features:
 - Forwards unicast traffic along the shortest path and uses SPF to calculate the outbound interfaces connected to destination nodes.
 - Uses ECMP to improve bandwidth use efficiency. Currently, Huawei products support a maximum of 16 equal-cost routes.
 - Provides fast convergence. If a fault occurs on a TRILL network, network convergence is complete within milliseconds.
 - Is applicable to larger networks. Currently, Huawei supports a maximum of 500 TRILL nodes.
 - Uses the TTL in the TRILL packet header to prevent loops.



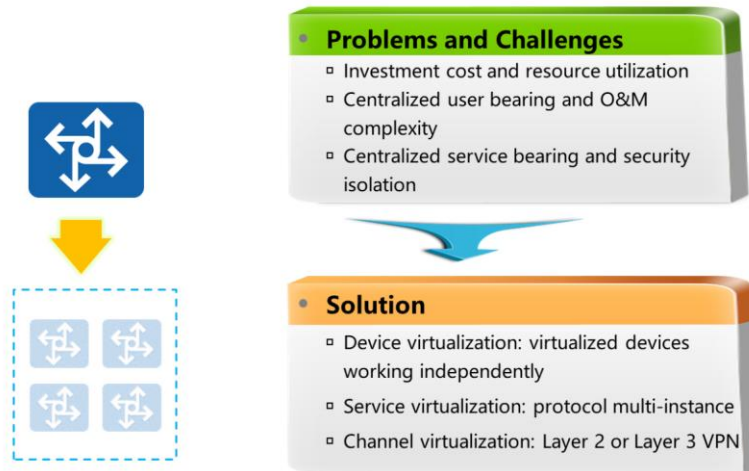
New Technology of DC Networks - FCoE



- For traditional DC network architecture, there are two independent networks: data network and SAN.
 - The front-end network is a high-speed data network, on which interfaces are connected through Ethernet links.
 - The back-end network uses the NAS and FC SAN.
 - Each server needs four to six interface cards, two HBAs connected to the FC SAN, and two Ethernet cards connected to the data network.
- Fiber Channel over Ethernet (FCoE) implements convergence of the SAN and data network. That is, one network is used to provide data communication and storage forwarding.
 - FC storage requires only FC switches to provide the access function, and the forwarding process is performed on the Ethernet (LAN).
 - Servers require the CNA that provides convergence.
- FCoE requirements for data networks:
 - High bandwidth: Heavy traffic between servers and storage devices requires high bandwidth. There are 10GE and 40GE Ethernet interfaces and future 100GE interfaces, and technologies such as link aggregation and load balancing, can meet access bandwidth requirements.
 - Low latency: The CutThrough forwarding mechanism on an Ethernet ensures low-latency data forwarding.
 - No packet loss: Traditional Ethernet technologies cannot ensure zero packet loss even if QoS is used. Data Center Bridge (DCB) is developed to prevent packet loss on an FCoE network.
- Huawei DC series switches support FCoE technology.



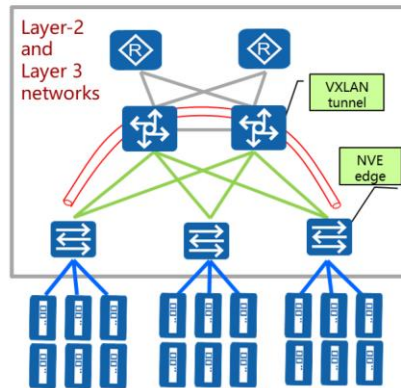
New Technology of DC Networks - Virtualization



- Virtualization is a crucial technology for cloud computing. Virtualization abstracts physical resources to implement cloud resource sharing and isolation. It greatly improves the resource utilization, and reduces resource running, management, and maintenance costs. Cloud-based virtualization includes computing, storage, and network virtualization. With virtualization, computing resources can be provisioned on demand in the same manner as computing resources. Network virtualization has two modes: N:1 and 1:N. In N:1 mode, multiple physical network resources are virtualized into a logical resource using technologies such as stacking and CSS. In 1:N mode, a physical network resource is virtualized into multiple logical resources.
- From the aspect of applications, 1:N virtualization includes channel and service virtualization. Channel virtualization includes technologies such as VPN, VLAN, and QinQ. These technologies provide logical channels to transmit and isolate traffic. Service virtualization includes MSTP multi-instance and MP-BGP multi-instance. Multiple instances are used to isolate logical services. Both channel virtualization and service virtualization are partial. The system-level network device virtualization is not limited to specific services or channels.



New Technology of DC Networks - VXLAN



Problems and Challenges

- Cloud computing, VM, capacity expansion and migration, and service continuity
- Large Layer 2 network

VXLAN Solution

- Reachable IP routes: ECMP
- Large scale: 16M virtual networks
- Fast convergence, loop prevention, and flexible deployment

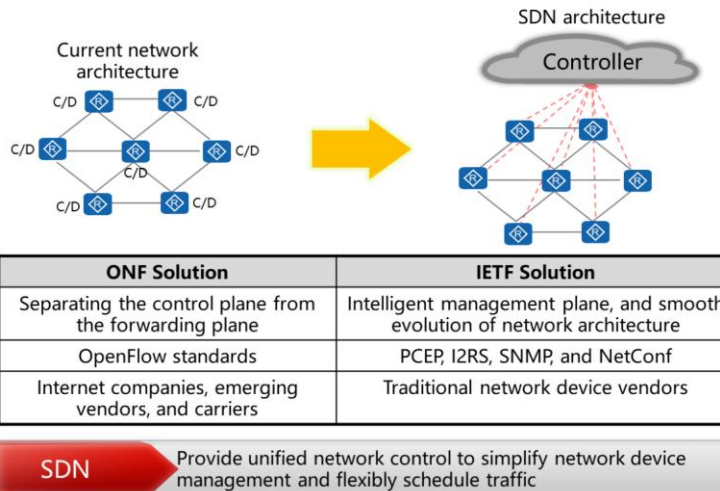
VXLAN

Encapsulate Layer 2 data packets into UDP packets, and provide tunneling technologies over IP networks.

- Many VMs are used on cloud computing networks. After VMs are started, they may need to be migrated from one server to another due to server resource problems (for example, CPU overload or insufficient memory). To ensure nonstop services during VM migration, IP and MAC addresses of the VMs must remain unchanged. In this case, the service network must be a Layer 2 network and also provide multi-path redundancy and reliability. TRILL meets urgent requirements of large Layer 2 networks; however, cloud computing requires large-scale migration, for example, migration across equipment rooms and DCs, to implement resource sharing and disaster recovery.
- Virtual eXtensible Local Area Network (VXLAN) is a Network Virtualization over Layer 3 (NVo3) technology and uses the MAC in User Datagram Protocol (MAC-in-UDP) mode to encapsulate packets. VXLAN can build larger Layer 2 networks with flattened fat tree topologies, increasing bandwidth usage.
- Compared with other Layer 2 network extension technologies, VXLAN has the following advantages:
 - Encapsulates packets in IP or UDP mode, and extends Layer 2 networks, and has low requirements.
 - Uses the 24-bit VXLAN Network ID (VNI) to identify users. The VNI is similar to a VLAN ID and supports a maximum of 16M $[(2^{24} - 1)/1024^2]$ VXLAN segments. (As defined in 802.1Q, the VLAN tag field is 12 bits.)
 - Makes full use of advantages of IP networks such as fast convergence and ECMP to transmit Layer 2 data that is encapsulated into IP packets. VXLAN based on IP packets prevents loops compared with common Layer 2 networks.



Future DC - SDN



- Traditional IP networks that use the distributed processing model provide self-healing and high reliability, but there are some negative impacts.
 - Complex management and O&M: IP technologies do not support unified network management and O&M, so network configurations on devices need to be adjusted one by one.
 - Difficulty in network innovations: Control and data planes are tightly coupled on IP network devices. The development of a new technology requires collaboration of network-wide devices. It takes about three to five years to introduce a new technology, adversely affecting network evolution.
 - Increasingly oversized devices: IP packet technologies are based on RFCs released by the IETF. The IETF has released over 7,000 RFC standards. The implementation is complex.
- SDN achieves global traffic control and optimal results based on global view and centralized control. SDN provides the following advantages: intelligent node centralization, simplified O&M, automatic scheduling, improved network utilization, network openness, and support for bandwidth and traffic management such as QoS.
- Currently, the mainstream SDN solutions are provided by the ONF and IETF:
 - ONF recommends that control functions of network devices (such as route calculation) should be centralized on a controller. The controller generates forwarding entries and delivers them to devices. Network devices are only responsible for forwarding packets. OpenFlow is a control interface between the controller and network devices. The ONF solution is mainly promoted by Internet companies, emerging vendors, and carriers.
 - IETF emphasizes smooth network evolution. It advocates automatic and intelligent network management on the current network architecture, and flexible traffic scheduling using traditional management interfaces. This solution is mainly promoted by traditional network device vendors.
- SDN is not exclusive for DCs. DCs have small geographical areas, heavy traffic, and complex service models, so SDN is rapidly applied to DCs.



Huawei DC Switches



CloudEngine X800 series switches:

CE5800 series switches provide high-density gigabit access and support 40GE uplinks.
CE6800 series switches provide high-density 10GE access and support 40GE uplinks.
CE7800 series switches provide high-density 40GE access.
They support IETF TRILL to build a large Layer 2 network with up to 512 nodes.
They support iStack and a stack of up to 16 devices.
They support FCoE, DCBX, and VXLAN.
Some models support OpenFlow and OPS.

CloudEngine 8800 series switches:

Provide high-density 100GE, 40GE, 25GE, and 10GE ports by flexibly combining cards, and support abundant DC features including TRILL, FCoE, and VXLAN, high-performance iStack, and OPS.

CloudEngine 12800 series switches:

Provide a maximum of 160Tbit/s switching capacity.
Support 1:16 virtualization, and TRILL networking with up to 512 nodes.
Support VXLAN and a maximum of 16 million tenants.
Provide OPS and ENP planes.
Provide the front-to-back airflow design, separate airflow for line cards, and multiple innovative energy saving technologies.

- Huawei CloudEngine series switches are high-performance cloud switches designed for next-generation data centers, including the flagship core switch CloudEngine 12800 series and high-performance aggregation/access switch CloudEngine 7800/6800/5800 series. The software platform of the CloudEngine series is based on the next-generation VRP8 operating system, and supports a variety of DC features such as TRILL, FCoE, and VXLAN, and SDN programming.
- CloudEngine 5800/6800/7800 series switches use fixed configurations. CE5800 series switches provide 24 or 48 GE interfaces, and four 10GE or two 40GE uplink interfaces. CE6800 series switches provide 24 or 48 10GE interfaces, and two, four, or six 40GE uplink interfaces. CE7800 series switches provide 32 40GE interfaces.
- CloudEngine 8800 series are 2-U TOR switches that support 4 half-width FPICs. The switch supports a maximum of 32 100GE, 64 40GE, 128 25GE, or 128 10GE interfaces.
- CloudEngine 12800 series switches are high-performance core switches designed for data center networks and high-end campus networks. The CE12800 series is available in six models: CE12816, CE12812, CE12808, CE12804, CE12808S, and CE12804S. The switch supports a maximum of 160Tbit/s switching capacity that can be smoothly upgraded to 320Tbit/s. It supports a maximum of 576 100GE, 576 40GE, 2304 25GE, or 22304 10GE line-speed interfaces. It provides industry-leading CLOS architecture, industrial-grade reliability, and patented front-to-back airflow design. It also uses multiple innovative energy saving technologies, greatly lowering device energy consumption.



Case Study

- A university plans to construct a central equipment room where all colleges' servers (about 1,000) are centralized for unified management. The number of servers will increase in the future. How is the network in the equipment room designed?

- You need to decide whether to use the traditional or new DC architecture. Engineering practices require you to leverage technologies, costs, and network reliability. The traditional DC architecture is applicable considering the DC scale. You can also use the new architecture for trial.
- According to the DC scale, you are advised to use the traditional DC architecture in which core and access layers are deployed. The equipment room has all colleges' servers deployed. You are advised to assign network segments based on colleges to implement service isolation. You can deploy gateways at the access layer and allocate access switches by college.

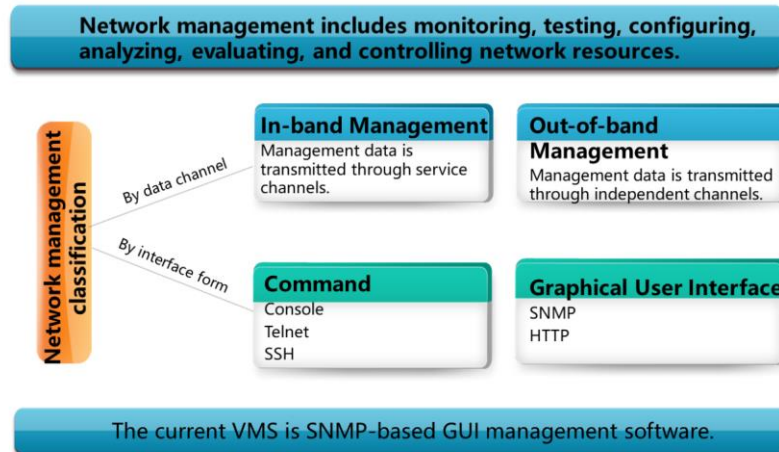


Contents

1. Overview
2. Physical Network Design
3. Logical Network Design
- 4. Other Network Technologies**
 - Network security
 - VPN
 - WLAN
 - DC
 - Network Management
5. Overall Technological Solution



Network Management Concept

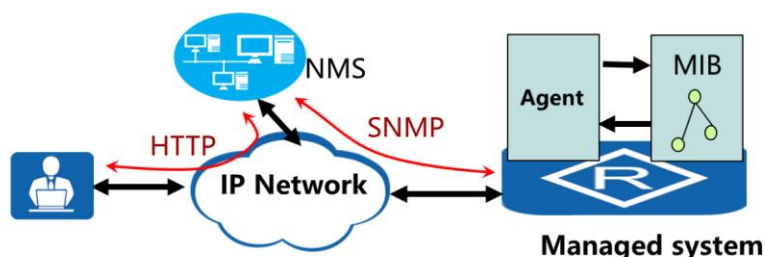


- You need to configure network devices during or after network construction, and monitor and control network resources during network operation. All the preceding work refers to network management.
- Network management is implemented in multiple modes that are classified based on dimensions. For example, when performing the initial on a new device, we often connect the console interface of the device to a terminal, which is out-of-band management of the character interface. When devices are running, we remotely log in to the devices to manage them through Telnet or SSH, which is in-band management of the character interface. For network management, the NMS that collects network status data and delivers configuration parameters through SNMP is often used, which is GUI-based in-band management.
- All networks need to be managed. You do not have to configure an independent NMS to manage small-sized networks with few devices and users. This is because the network management workload is not heavy. You can log in to the character interface of each device to manage the device. However, an independent NMS reduces the network management workload when the network scale increases.



NMS

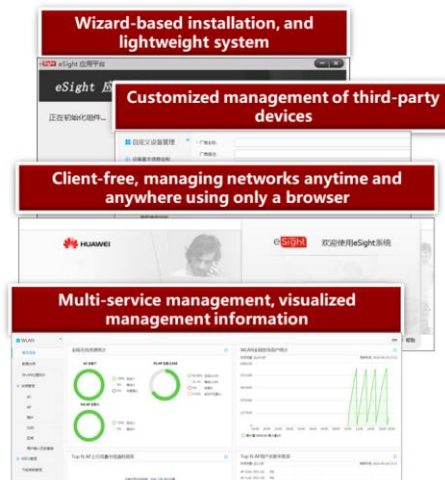
- The mainstream NMSs are based on the Simple Network Management Protocol (SNMP).
- Most NMS products provide web interfaces and GUI-based management.



- SNMP-based network management involves the following entities:
 - A network device is configured with the NM agent and an management information base (MIB). The MIB contains device status information on managed devices, and stores it in a hierarchical tree structure. The NM agent is an agent program running on managed devices, responds to requests from the NMS, and performs corresponding operations. The NM agent collects device status information, performs remote operations on managed devices, and reports alarms to the NMS.
 - The NMS is network management software that runs on the NMS workstation. Network administrators send requests to managed devices by performing operations on the NMS to monitor and configure the devices.
 - SNMP provides standard communication interfaces between the NMS workstation and managed devices.
- To simplify network management, the NMS is generally integrated with a web server, so that administrators can log in to the GUI of the NMS anytime and anywhere to view network management information.



Huawei NMS - eSight



No.	Function
1	User management
2	Log management
3	Resource management
4	Topology management
5	Alarm management
6	Performance management
7	Physical resources
8	Report management
9	Customized device management
10	Configuration file management
11	Smart configuration tool
12	WLAN service management
13	SLA service management
14	MPLS VPN service management
15	Management of subordinate NMSs
16	Single NE feature management
17	Homepage of the system Portal
18	Data dumping and backup
19	NE adaptation package management

- Huawei eSight is a unified NMS of enterprise networks and manages products of different vendors using standard NMS protocols. It can uniformly manage application software systems, IT devices such as servers and printers, and network devices.
- eSight AppBase uses the B/S architecture, and achieves componentization and decoupling of functional modules. A client requires only a web browser. You only need to upgrade the server software to upgrade and maintain eSight. eSight is elastic and applies to various enterprise networks.
- eSight provides abundant management functions including common system management, network management, and service-oriented WLAN or MPLS VPN management.



eSight Product Differences

Item		Compact Edition	Standard Edition	Professional Edition
Management scale		60 nodes	5,000 nodes	20,000 nodes
Function		Topology management, NE management, link management, physical resources, electronic labels, alarm management, performance management, configuration file management, log management, and single-user management	Functions provided by the compact edition, customized device management, report management, smart configuration tool, IPsec VPN, MPLS VPN, WLAN, SLA, IP topology, SNMP alarm northbound interface, security management, database backup tool, fault collection tool, and multi-user management	Standard NMS functions Hierarchical NMS
Market-oriented		Small-sized networks requiring only device management, with cheap price	Medium- and large-sized networks requiring mainstream application platforms, flexible solutions, and flexible component sales	Super-large networks requiring hierarchical management
Storage capacity	Number of current alarms	20,000	20,000	20,000
	Number of historical alarms	---	1.5 million	1.5 million
	Number of logs	1,000,000	1,000,000	1,000,000
	Number of performance records	---	60,000,000	60,000,000

- Huawei provides three editions of eSight. The compact edition that provides simplified NMS functions applies to small-sized networks. The standard edition that provides complete NMS functions is the mainstream NMS application platform. The professional edition that offers hierarchical NMS functions can manage super-large networks.



Case Study

- Configure an NMS for a campus network.

- Standard edition of eSight is recommended.
- You need to confirm the NMS running platform when configuring NMS software. Or, you can directly purchase the pre-installation version of Huawei NMS (server hardware is included). You can also purchase server hardware, configure the proper CPU, memory capacity, and hard disk capacity of the server based on the number of managed nodes, and install the operating system and database software as required.

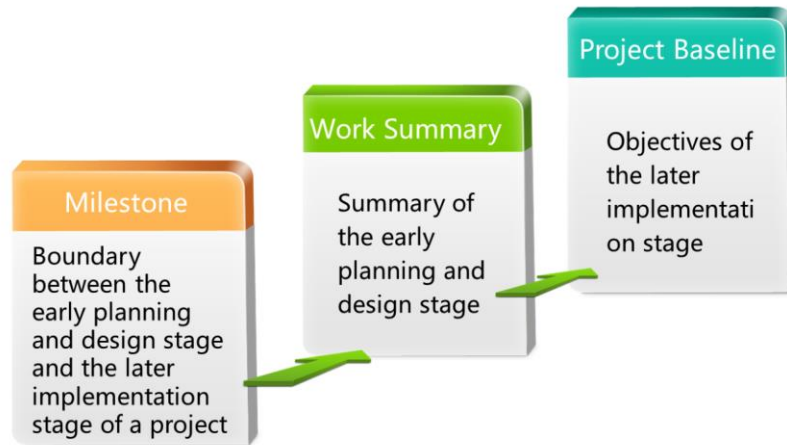


Contents

1. Overview
2. Physical Network Design
3. Logical Network Design
4. Other Network Technologies
- 5. Overall Technological Solution**



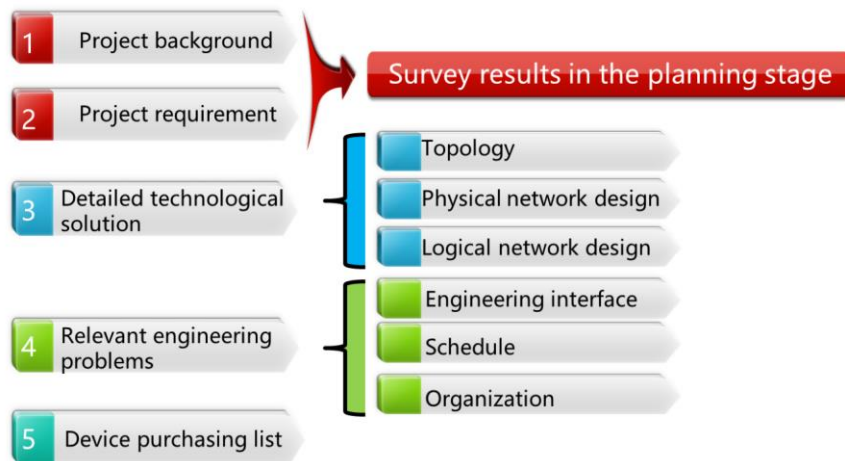
Significance of Technological Solution



- A network technological solution is an important milestone during the entire project, and represents completion and summary of the early planning and design stage. A technological solution comprehensively lists objectives and implementation details of a project, and is used as a reference for project implementation.
- The project technological solution is the most important part of bidding documents. In most cases, the quality of a technological solution determines the bidding result.



Technological Solution Content



- A technological solution contains all achievements in the project planning and design stage.
- Some work in the project planning stage determines the project design. For example, requirements and technology selection of a project are the prerequisites for the technological solution, and need to be demonstrated.
- A technological solution mainly focuses on details of the network design including all contents mentioned in the preceding part. Network modules need to be adjusted based on actual project requirements.
- A technological solution also involves engineering implementation contents. The engineering implementation contents are not detailed engineering implementation steps, but are conditions such as personnel organization and schedule to ensure that the technological solution is implemented successfully.
- The final part of a technological solution is generally the purchase list including network devices and auxiliary materials such as fiber pigtailed and twisted pairs. Generally, the purchase list does not include quotations which are given in the commercial solution.



Relevant Files of the Technological Solution



- Besides technological solution, a set of project files also includes other supporting materials. These materials provide other project-related information to ensure that the project is implemented successfully.
- A commercial file involves legal issues such as engineering quotations, responsibilities and duties of each party, and mechanisms for resolving disputes.
- An authorization file involves project authorization from engineering partners such as device suppliers to ensure device supply and warranty.
- Qualification certificates of engineering parties and project members ensure that the project is implemented by engineering units authenticated by authorities.
- Technological parameters of devices and products involved in the project are provided as attachments.



Quiz

1. Which of the following cabling modes are popular for a DC currently?

TOR

DOD

EOR

NSF

2. Which of the following subsystems are involved in building cabling?

Horizontal subsystem

Vertical subsystem

Access subsystem

- Answer: AC.
- Answer: AB.



Thank You

www.huawei.com



Network Implementation



Foreword

- Project implementation indicates the operation process of delivering a project. Systematic management along with efficient process ensures successful project implementation.
- This document describes the project delivery process, risky operation implementation process, and engineer service standards.
- The project delivery process ensures high efficiency of project management. The risky operation implementation process is a guide to minimize risks during implementation. The engineer service standards provide good vocational standards for engineers.



Objectives

- Upon completion of this section, you will be able to:
 - Comprehend the project delivery process
 - Be familiar with the risky operation implementation process
 - Understand the engineer service standards



Contents

- 1. Project Delivery Process**
2. Risky Operation Implementation Process
3. Engineer Service Standards



Importance of the Project Delivery Process

- Definition of project delivery process:
 - The project delivery process specifies the requirements on project implementation management and operation control, ensuring that the project is implemented based on the specified process.



Enhance customer satisfaction



Improve work efficiency

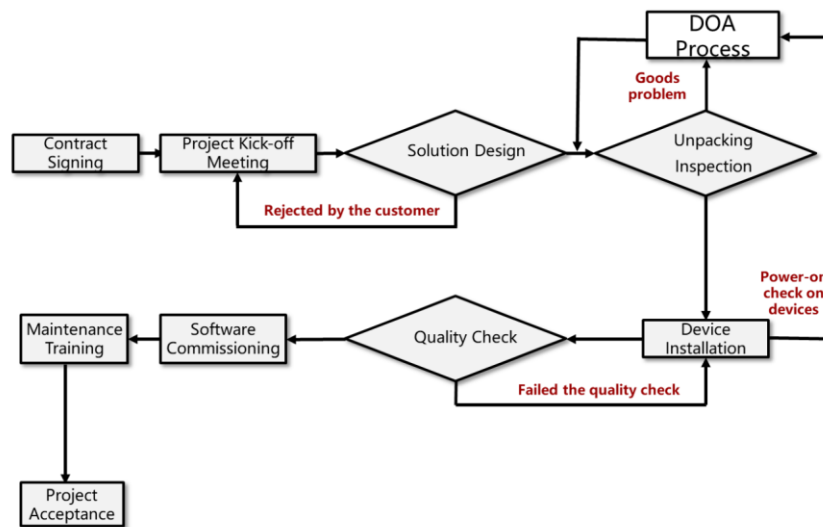


Reduce project risks

- The standard project delivery process will:
 - Enhance customer satisfaction.
 - Improve work efficiency and reduce costs.
 - Reduce project delivery risks.



Project Delivery Flowchart



- Contract Signing
 - Output tendering document, bidding document, design solution, and device list. Set up a project team and specify project members.
- Project Kick-off Meeting
 - Understand customer requirements, confirm project plan and duration, and specify the delivery owner. Understand the customer's implementation requirements and decide project management regulations, such as daily reports, weekly reports, problem management and tracking, and project routine meetings.
- Solution Design
 - After learning about customer requirements, the project implementation personnel will compile the implementation solution and send the implementation solution to the project technical director (TD) for preliminary review. After the solution passes the review, the project implementation personnel will deliver the solution to the customer for review. If the solution is rejected, the project implementation personnel communicates with the customer again and modifies the solution based on customer needs.
- Unpacking Inspection
 - After the arrival of goods, the supplier, customer, and supervision party perform an unpacking inspection, and sign the Goods Receipt or Packing List. If there are problems with the goods, the supplier needs to call the Huawei service hotline and follow the DOA process.

- Device Installation
 - Before installing devices, inspect the installation environment, such as the device installation location, load bearing capacity of the equipment room, temperature and humidity of the equipment room, cabinet space, and power of the power supply system. Once inspected, install and connect devices, label the cables, and perform a power-on check.
- Quality Check
 - After device installation, the construction party and the customer check the device installation quality. Device installation needs to comply with engineering standards and the customer's equipment room standards, such as standards for weak- and strong- current cable routing, device labeling, and cable labeling.
- Software Commissioning
 - Includes single-node commissioning, joint service commissioning, and migration.
- Maintenance Training
 - Includes training on networking, network configuration, routine maintenance, and emergency fault rectification.
- Project Acceptance
 - Arrange and hand over project-related materials to the customer, such as the topology diagram, device list, device configuration, device connection table, IP address assignment table, and device user name and password. After the project is completed, ask the customer to sign the Acceptance Certificate.



Project Delivery Process - Project Kick-off Meeting

- After the contract is signed, hold a project kick-off meeting with the customer:
 - Clarify customer requirements based on the tendering and bidding solutions.
 - Confirm the project plan and duration.
 - Determine project owners from both parties and project members.
 - Decide project management regulations.
 - Confirm the device installation environment.



- The project manager organizes and holds the project kick-off meeting with the customer to understand customer requirements and specify the technical implementation mode.
- Before implementation, confirm the required device installation environment with the customer. This avoids delay of work caused by the installation environment.
- Before implementation, obtain the Packing List and familiarize yourself with the device delivery scope.
- Decide project management regulations, such as daily reports, project problem reports, and routine meetings.
- Remind the customer of project survey preparation and survey requirements.



Project Delivery Process - Solution Design

- Compile the implementation solution based on the customer's requirements.
The solution must include:
 - Project background and objectives.
 - Engineering scope clarification and responsibility division.
 - Timeline and personnel arrangement.
 - Detailed configuration and implementation procedure.
 - Service migration and acceptance test.
 - Quality assurance and risk control.



- The implementation solution must be compiled based on tendering and bidding documents, live network environment, and customer requirements.
- Project background and objectives
 - Describe status and problems of the live network along with project construction objectives.
- Timeline and personnel arrangement
 - Formulate the implementation solution based on customer requirements and specify work to be completed at key points in the timeline.
 - Confirm project members and their responsibilities.
- Detailed configuration and implementation procedure
 - Confirm the physical design, logical design, and command configuration of devices.
 - Formulate a detailed implementation procedure, including hardware installation and software commissioning.
- Service migration and acceptance test
 - Perform service migration based on the implementation solution and collaborate with the customer to test services.
- Quality assurance and risk control
 - Project management regulations ensure project implementation quality and reduce potential project risks.



Project Delivery Process - Checking Goods



- The following information must be confirmed after the arrival of goods:
 - The quantity of packing boxes is the same as that noted in the Logistics List.
 - The device quantity is the same as that noted in the Packing List.
 - The device quantity and models are the same as those noted in the contract product list.
- If the quantity or content of goods is not the same as that what is required, the goods are wrongly delivered. Contact the vendor to deal with the problem.

- Confirm the following information in the Packing List:
 - Project name: Confirm that the project name is correct.
 - Contract number: Each project has a unique contract number.
 - Box name and quantity: A large device may be stored in several cardboard/wooden boxes. Each cardboard/wooden box has a unique name. The onsite engineer needs to confirm that box names, components, and box quantities are correct.
 - Product model: Confirm that the required device models are the same as the models of arrival devices.



Project Delivery Process - Unpacking and Inspecting Goods

- Check whether the part numbers, models, and quantities listed in the Packing List are the same as those of the goods arrived.
- Check whether components are physically damaged.
- Once the goods have been inspected and are deemed to be of the right quantity and be intact, both the installation supervisor and the customer's representative need to sign the Packing List.

PACKING LIST																
P.A. No.		Date		Project												
Contract No.		L/C No.		P.O. No.		BILL		PU No. 1								
CASE NO.	MATERIAL	CTN NO.	PART NUMBER	DESCRIPTION	QTY	UNIT	HW SERIAL NO.	CRACK	HW NO.	SIZE (MM)	VOLUME (CM)	Brand	Model	Country of Origin	DATE	
1	Plywood pallet		030205AT	ARMORIS24000	2-Port Serial/Armp Serial/Port Interface Card	PCS			00	30.4	1184*420*400	0.0475	HUAWEI	ARMORIS24000	CN	2020/05/04

- Quantity and model check:
 - PART NUMBER: Each code defined by Huawei to uniquely identify a component.
 - QTY: Quantity of delivered goods.
 - If an outer packing box is damaged, do not open it. Take photos and contact Huawei's local representative office.
- Completeness check:
 - Outer packing box deformation.
 - Outer packing box damage.
 - Damage of goods.



Project Delivery Process - DOA Process

- Definition of Dead On Arrival (DOA):
 - A device is physically intact upon arrival but fails to work properly once powered on or fails within 48 hours of the device being powered on.
 - DOA process:
 - The onsite engineer calls Huawei service hotline immediately to contact the Technical Assistance Center (TAC) for help.
 - The TAC identifies whether it is a DOA issue.
 - The onsite engineer sends the Goods Problem Report to the TAC and obtains assistance from the TAC to complete subsequent processes.
- Goods Problem Report:
 - Fill detailed description about the goods problem in the Detailed Information About the Problem row.
 - Ensure that the address for receiving the replenishment goods, required arrival time, consignee, and phone number are correct.



Goods Problem
Report

- DOA handling condition:
 - The device is not a test or sample device.
 - The customer should provide original outer packing boxes and materials.
 - The original outer packing boxes are intact (no fissures, holes, wet, caved in, or hollow areas).
 - The packing materials are complete (including foams and plastic bags).
 - The accessories are complete. (Subject to the Packing List).
 - The goods should look intact without physical damages. (Note: Contact the transportation service supplier for compensation for physical damages).
 - All seals on the host machine are not torn.
 - All identifiers on the machine are complete.
 - The hardware, pre-installed software (OS) and drives are original.



Project Delivery Process - Checking the Device Installation Environment



Equipment room environment
(Space, temperature, humidity)



Power distribution status
(voltage, power consumption)



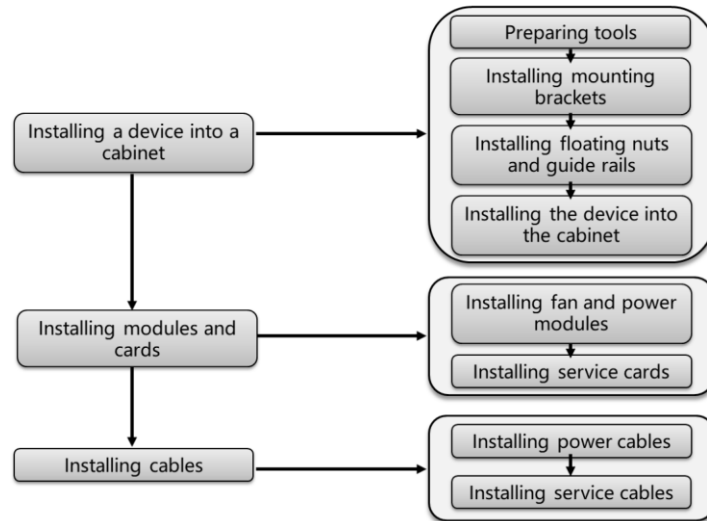
Cabinet status
(Dimension, cabling, device grounding status)



- Carefully check the installation environment before installation as this will ensure a smooth installation process and avoid possible faults.
 - Equipment room environment: Temperature, humidity, cleanliness, height, floor type, floor height, load bearing capacity of the floor, and cabling method.
 - Cabinet: The cabinet dimension must meet requirements of the device. For detailed device dimensions, refer to the hardware description part in product documentation.
 - Device power supply: Based on device configuration, confirm the required number and specification of power supply interfaces.
 - Device power: Confirm whether the power of the device exceeds the specification of communications power supplies. The device power is calculated based on the maximum power consumption of the device. For the actual power consumption, refer to the Huawei Enterprise Network Product PCC & PDA, which is available at http://support.huawei.com/online/toolsweb/pda_en/.
 - Interconnection cable: Confirm cable provider and quantity.
- Before device installation, if the equipment room environment cannot meet installation requirements, inform the customer of potential risks as soon as possible and remind the customer to rectify the environment.



Project Delivery Process - Installing a Device



- Preparing tools
 - Refer to related product documentation to prepare installation tools and accessories, such as scissors, flat-head screwdriver, Phillips screwdriver, marker, installation template, floating nuts and matching screws, guide rails and matching screws (prepared by the customer), and device handles.
- Installing mounting brackets
 - Measure the distance between the front mounting rails and interior side of the front door. Adjust the installation locations of mounting brackets depending on the distance. Install the mounting brackets on the device.
- Installing floating nuts and guide rails
 - Install floating nuts based on the installation template that was delivered with the device.
 - Take the installation template. Install the floating screws based on the installation template matching the device model.
 - Install the guide rails into the cabinet.
- Installing the device into the cabinet
 - For a large device, multiple people need to lift the device onto the guide rails from the front door, slowly push the device into the cabinet using the guide rails, and use screws to fix the device onto the cabinet.
- Installing modules and cards
 - Generally, there are fixed slots for fan modules and power modules. Service cards are installed based on service requirements. The onsite engineer must put on an electrostatic discharge (ESD) wrist strap before touching a card.
- Installing cables
 - For power cables, confirm that the power consumption meets requirements and ensure correct polarity when connecting the power cables. Arrange service cables in a clear manner. After installing the service cables, label the cables to make it clear for engineers in the future.



Project Delivery Process - Checking Hardware

- Perform the following checks before powering on a device:
 - Check the device hardware carefully based on the checklist.
 - Perform multiple checks on the power system's security.
- Perform the following checks after powering on the device:
 - Check the device status indicators based on the product manual. If device faults occur, initiate the DOA process in time.

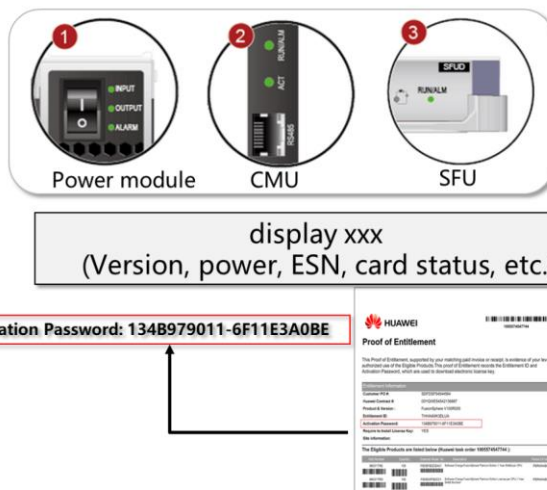


- Perform the following checks before powering on a device
 - Once the device is installed, the onsite engineer needs to check the device installation quality. In addition, device installation must meet customer requirements, such as requirements on cabling, device labeling, and cable labeling.
 - Cabinet installation check: The cabinet must be stable and secure. Doors and locks can be smoothly opened and closed. The vertical deviation of a cabinet is less than 3 cm. The cabinets in the same row are flush with each other. The cabinet exterior is not distorted.
 - Cable routing: Cables are properly arranged and bound. Cable ties are installed at equal spacing and in the same direction. The excess of cable ties is trimmed off. Signal cables are routed correctly inside the cabinet. The power cables, ground cables, and signal cables are routed separately, with a spacing of more than 3 cm. The label template must meet customer requirements. Labels are neatly aligned and face the same direction.
 - Grounding: The cabinet uses ground cables (with a diameter of more than 16 mm) to connect to the nearest ground bar in the equipment room. The ground cables for the shells of the device and chassis are securely connected to the ground points of the cabinet. The front, rear doors and side panels of the cabinet are properly grounded. The diameter of the ground cables is no less than 6 mm.
 - Equipment room environment: The power voltage and circuit breaker capacity of the equipment room ensure long-term device stability. The ambient temperature and relative humidity in the equipment room meet the requirements for long-term safe operation of the device.
- Perform the following checks after powering on the device:
 - After powering on the device, check status of indicators, including the power module, fan module, MPU, SFU, and interface card indicators.
 - If an indicator shows an abnormal status, log in to the device to further check the working status of the device.
 - If the device cannot start properly after it is powered on or fails within 48 hours after it has been power on, the device is considered as DOA. Contact the vendor for further processing.



Project Delivery Process - Single-Node Commissioning

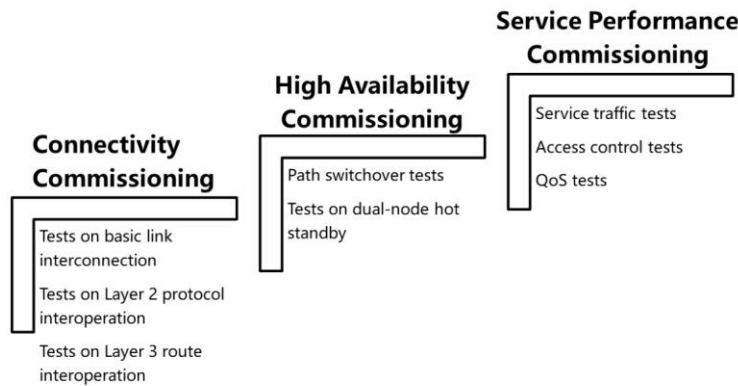
- Check indicator status
- Query the running status
- Apply a license



- Checking indicator status
 - Figure 1 shows power module indicators. If the INPUT and OUTPUT indicators are steady green, the power input and output are normal. If the ALARM indicator is off, the power module is operating normally. If the ALARM indicator is steady red, the power module is not operating normally.
 - Figure 2 shows CMU indicators. If the RUN/ALM indicator (running status indicator) blinks green slowly, the CMU is running normally. If the RUN/ALM indicator blinks green fast, the system software of the CMU is unregistered. If the ACT indicator (active/standby status indicator) is steady green, the CMU is working in an active state. If the ACT indicator is off, the CMU is working in a standby state.
 - Figure 3 shows the SFU indicator. If the RUN/ALM indicator is steady green, the SFU has been powered on but the system software is not running. If the RUN/ALM indicator blinks green slowly, the SFU is running normally. If the RUN/ALM indicator blinks green fast, the SFU is powering on or is restarting. If the RUN/ALM indicator is steady yellow, the SFU is powered off.
 - For more information on the card indicator status, refer to the operation manual of the device.
- Querying the running status
 - Run the **display device** command to view the registration status of a card and confirm that the card is working in Normal status.
 - Run the **display device slot xxx** (xxx indicates slot number) to view the status of the card in a specific slot.
 - Run the **display power** command to view the power status of the device.
 - Run the **display power system** command to view the power consumption of the device.
 - Run the **display version** command to view the device version.
 - Run the **display esn** to view the ESN of the device.
 - For more view and test commands, refer to the operation manual of the device.
- Applying for a license
 - To apply for a license, collect the device ESN and activation password in the printed license document and log in to <http://app.huawei.com/isdp> to apply for a license.
 - After the license is successfully applied, load the license to the device and check whether related functions have taken effect.



Project Delivery Process - Joint Commissioning



- Joint commissioning content

- Tests on basic link interconnection: Run the **display interface brief** command to check whether the interface is Up. If the interface is Down, check the cable connection, negotiation mode of interfaces, and optical power.
- Tests on Layer 2 protocol interoperation: Check the 802.1Q configuration, spanning tree configuration, link switchover, and LLDP neighbor status.
- Tests on Layer 3 route interoperation: Perform interoperation tests. Check the routing protocol neighbor status and route quantity. Simulate path failures for path tests.
- Tests on dual-node hot standby: To verify reliability of dual-node hot standby, check whether the standby device can successfully switch its working state to the active state when the active test link and device fail.
- Service traffic tests: Run the **tracert** command to check service traffic direction.
- QoS tests: Check whether the QoS for user traffic takes effect and whether it achieves the expected result.
- Access control tests: Test network user access permissions, such as Authentication, Authorization and Accounting (AAA).
- Tests on other services: Perform tests on multicast, MPLS, and SNMP based on customer requirements.

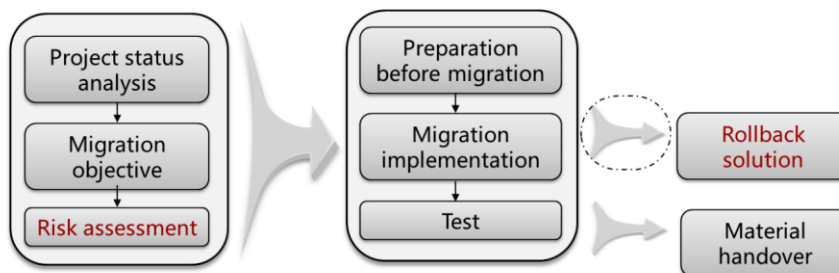
- Joint commissioning roadmap

- Topology-based north-south device configuration -> Topology-based east-west device configuration
- Basis configuration -> Protocol configuration
- Core -> Aggregation -> Access -> Edge
- Intranet -> Extranet



Project Delivery Process - Network Migration

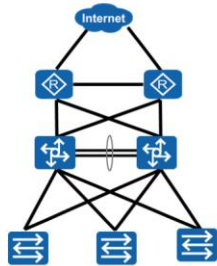
- Risk assessment is the most important step.



- Tips for service migration and network integration
 - Avoid peak service hours.
 - Prepare the migration configuration file in advance and set up a test environment for verification.
 - Prepare the rollback configuration file in advance to prepare for unexpected migration failure.
 - Arrange operation personnel and plan points in the operation timeline.
 - Perform network tests after migration.
 - Ask the customer to perform application service tests after network tests.

Project Delivery Process - Maintenance Training

Training on networking and configuration



Training on routine maintenance

Routine Inspection Report

Component	Inspection Time		
Inspection	Device Name	Inspection Method	Result
1	Check whether clock indicators on the device	Check the clock indicators	Normal
2	Check whether the power status indicator is on	Check the device status	Normal
3	Check whether status is reported by logging in to the device and returning the log	Log in to the device and get the display background command	Normal
4	Check whether the interface has been powered	Log in to the device and get the display background command	Normal
5	Check UEFI negative status on the device	Log in to the device and get the display background command	Normal
6	Check the number of UEFI related error	Log in to the device and get the display background command	Normal
7	Check UEFI status	Log in to the device and get the display background command	Normal
8	Check consistency of the BIOS version	Use the plug command to compare the BIOS version of the PC	Normal
9	See whether the BIOS version is accurate	Log in to the device and get the display background command	Normal

Legend
 N/A: Not applicable (such as device is reported)

Training on emergency fault rectification



Maintenance
Training Sign-in S

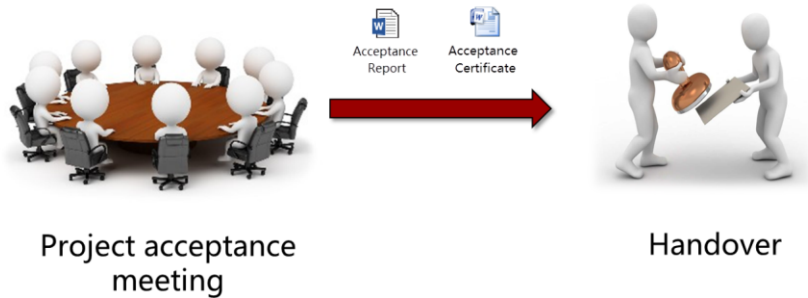


Routine Inspection Report

- Training on networking and configuration
 - Training on network topology, technical principles, address planning, traffic direction, and information security.
- Training on routine maintenance
 - Training on how to check the device environment, basic device information, device running status, and service running status.
- Training on emergency fault rectification
 - Training on how to quickly deal with emergency faults.



Project Delivery Process - Acceptance



- After project delivery, the project manager holds the project acceptance meeting with the customer, supervision party, and construction party.
- Agenda of the project acceptance meeting
 - Project overview.
 - The construction party introduces implementation status and quality status.
 - The supervision party elaborates upon the supervisory situation and provides quality assessment.
 - Onsite checking.
 - Material archiving.
 - Acceptance certificate signing.



Contents

1. Project Delivery Process
- 2. Risky Operation Implementation Process**
3. Engineer Service Standards



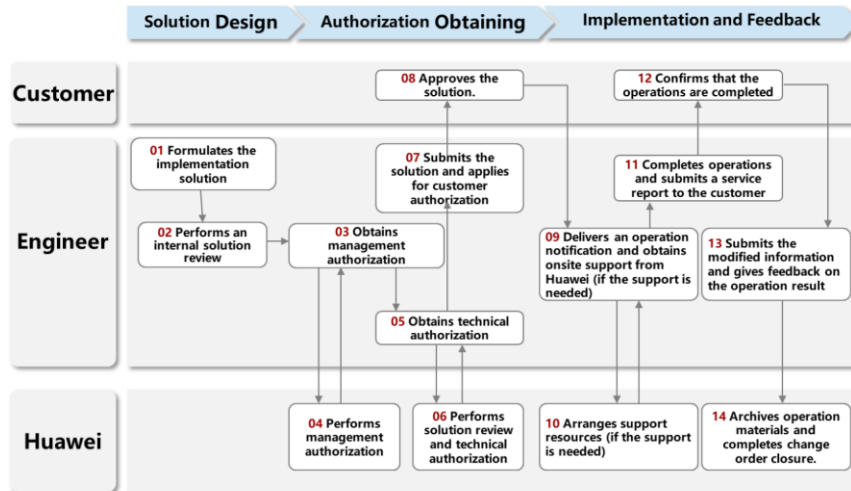
Introduction to Risky Operation

- Definition
 - A risky operation is any operation that may affect normal device running, service running, or monitoring function of the network management system (NMS).
- Purpose
 - The risky operation implementation process is used to regulate engineering and maintenance behavior of engineers, improve delivery quality, and prevent accidents.
- Identification
 - If the onsite engineer cannot identify whether an operation is a risky operation, the engineer needs to consult service engineers at the local representative office in time.

- Scope of risky operations
 - Operations that are considered risky include but are not limited to: data adjustment, data migration, data recovery, service migration, system capacity expansion, software upgrade/downgrade, hot swappable operation, power-off and resetting, active/standby switchover, disaster recovery test, connection or disconnection with physical interfaces of devices on the live network (that is, interconnection status change of physical interfaces of network elements), and operation on hardware such as power supplies, trunk cables, and optical fibers bearing services.
- Risky operations are classified into two levels
 - Level 1: Operations, such as migration, reconstruction, expansion, and upgrade, in all important projects and on all important networks.
 - Level 2: Other risky operations, especially operations in scenarios such as during communication, initial application of a version, re-operation after operation failure, and encountering frequent failures on the network.

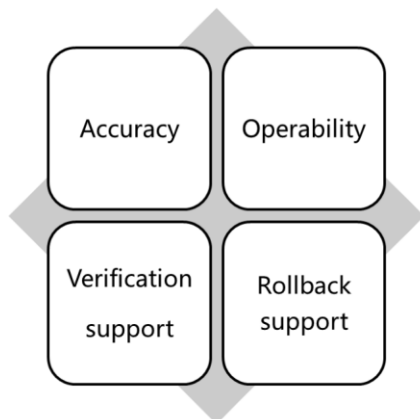


Risky Operation Implementation Process





Risky Operation Implementation Process - Solution Formulation



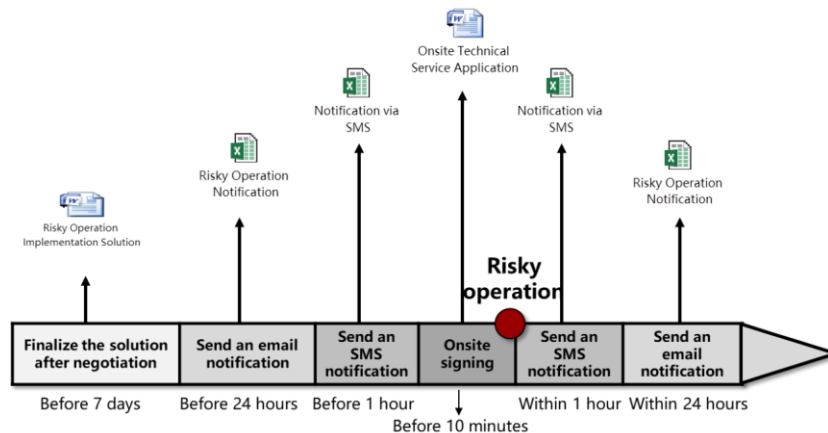


Risky Operation Implementation Process - Authorization Obtaining

- Management authorization:
 - Based on the project situation, the engineer sends an email to Huawei's project manager to apply for management authorization.
- Technical authorization:
 - The engineer sends the technical solution to Huawei's technical experts by email to apply for technical authorization. The solution must be submitted for review at least 3 days before implementation.
- Authorization from the customer:
 - The customer's department that is responsible for project construction approves the operation with written or email confirmation.



Risky Operation Implementation Process - Operation Process



- Before implementation

- The *Risky Operation Implementation Solution* must be finalized and signed by both parties at least 7 days before the operation.
- Send the *Risky Operation Notification* to the customer and the product contact person at the local representative office 24 hours prior to the operation.
- Before implementation, prepare related tools, cards, software version files, and spare parts and arrange related personnel.
- Send an SMS message to notify the customer authorizer, and the network maintenance contact person and service leader at the local representative office at least one hour before implementation.
- Operate devices on the live network only when the *Onsite Technical Service Application* in written form is delivered to the customer and the customer approves the application by signature or seal.

- During implementation

- If unexpected problems occur during implementation, contact the network maintenance contact person at the local representative office for help. If the operation is not finished on time, perform the rollback operation according to the implementation solution.

- After implementation

- After implementation, send an SMS message to notify the project owner of the customer and the network maintenance contact person at the local representative office.
- After implementation, send modified information to the customer and deliver the *Risky Operation Feedback* to the product contact person at the local representative office within 24 hours.

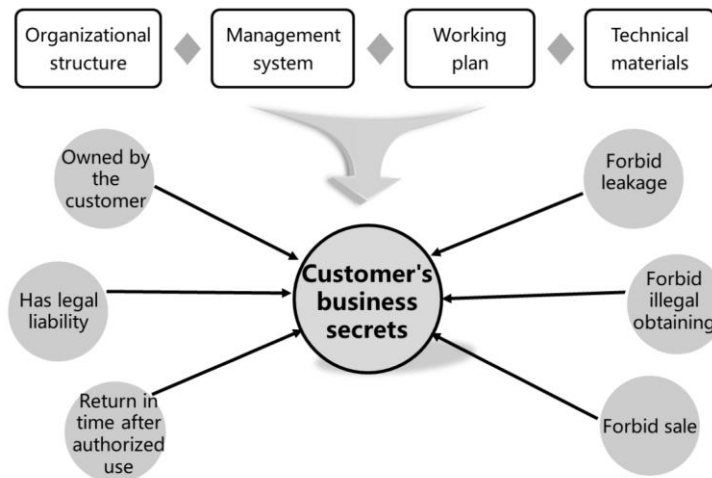


Contents

1. Project Delivery Process
2. Risky Operation Implementation Process
- 3. Engineer Service Standards**



Information Security Standards - Customer Information Security

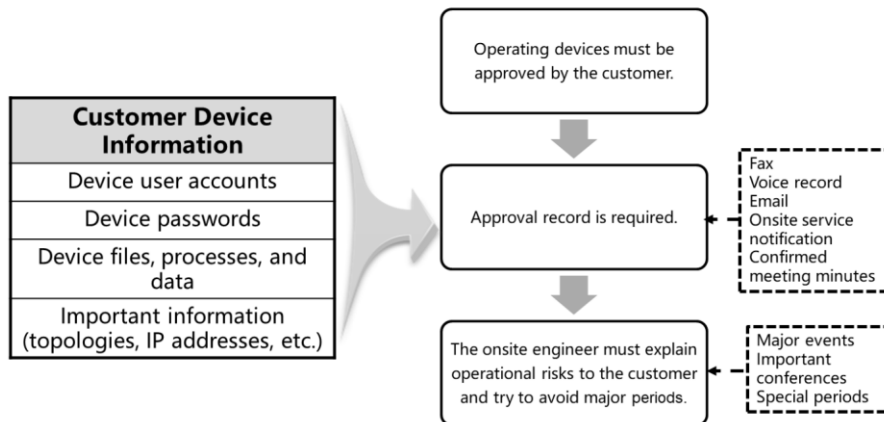


- The customer's business secrets
 - Service operating system, organizational structure, service relationship, and responsibilities.
 - Management system and service process.
 - Working plan and operation plan.
 - Technical files and materials and work records.
 - Technical specifications for the maintenance of devices.
 - Quality management system and data.
 - Other business secrets.
- Standards regarding business secrets
 - Keep confidentiality of the business secrets obtained from the customer.
 - Return the customer's accounts and passwords after authorized use and suggest immediate modification.
 - Do not use theft, inducement, coercion, or other improper means to obtain the customer's business secrets.
 - Do not violate customer requirements on keeping business secrets. Do not disclose, use, or allow others to use the business secrets.
 - Do not monitor the customer's calls. If call monitoring is needed to meet service requirements, comply with management regulations established by the customer.

- Do not disclose, sell, lease, transfer, share or permit the use of the customer's technical information or operation information to any third party in any way or provide tools that can be used to access the customer's technical information or operation information.
- If the engineering service personnel needs to provide the customer's confidential information to a cooperation organization for the purpose of implementing the cooperation project, the engineering service personnel must obtain the prior written consent from the customer, and ensure that the cooperation organization will not disclose such information to any person unrelated to the cooperation project.
- When the cooperation project ends, return all or part of the written or electrical materials containing "technical information" or "business secrets" according to the specific request of the customer.
- Confidentiality obligations shall not be terminated with the end of project cooperation. The confidentiality obligations exist as long as related customer information belongs to business secrets defined by the law.
- All engineering service personnel shall strictly comply with the preceding standards. The person who violates the information security provisions and causes losses to the customer shall compensate for all losses and bear relevant legal responsibilities, including civil responsibility and criminal responsibility.



Information Security Standards -Information Security on Customer Devices

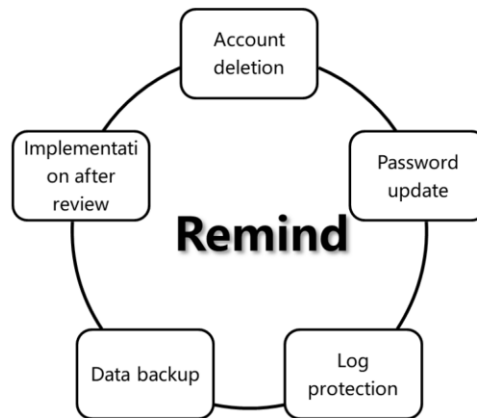


- Information security on customer devices
 - ❑ Do not retain or disclose customer device passwords without customer permission.
 - ❑ Do not retain or disclose the encryption and decryption programs, algorithms, and data files of customer devices. Files and programs required for relevant work must be deleted from PCs after the work is complete.
 - ❑ All materials for outside publications must not constitute an infringement of the business secrets of other persons, or a debasement or attack to the competitors and other enterprises, or infringement of the copy rights of other persons. Training materials for internal use only should be appropriately treated according to confidentiality levels. Internal training (training materials for Huawei staff) and external training (training materials for customers) must be strictly differentiated. External training materials and technical materials must not include specific customer information.
 - ❑ Documents of customer devices with the confidentiality levels no lower than SECRET obtained through appropriate authorization must not be transmitted to other persons without customer permission.
 - ❑ Do not disclose or examine important information on or regarding customer devices. This includes network topologies and IP addresses.
- Information security requirements when operating customer devices

- Without customer permission, do not connect your own PCs to the network that the customer devices are connected to. In the engineering and maintenance processes, maintenance can be conducted only when permission is granted by the customer and specific interfaces and IP addresses are assigned. Permission can only be granted in forms of fax, voice record, onsite service confirmation form, confirmed meeting minutes, and email.
- In the exception handling process, do not modify the programs, configuration files, data, and logs on customer devices without customer permission.
- Operations that carry risk can be performed on customer devices after they have been explained to and approved by the customer in written form. In the maintenance process, operations with high impact on devices should be performed within the period stipulated by the customer (typically from 00:00 to 05:00, but this may vary based on the customer).
- Devices must be operated with caution during communication assurance periods. This particularly refers to major events, important conferences, service peak hours, and special periods designated by the customer.
- Do not use the customer's network to use software that will affect the customer's network.



Information Security Standards - Reminders to the Customer with Regard to Information Security



- Reminders to the customer with regard to information security
 - Remind the customer to delete unneeded accounts.
 - Remind the customer to update all device passwords regularly and ensure that passwords are sufficiently complex. This should be performed based on the guide for routine maintenance.
 - Remind the customer that the customer cannot modify device log settings, close product record and log processes, or add, delete, or modify device logs.
 - Remind the customer to periodically back up the systems and data of devices, and to properly store that backup data.
 - Remind the customer that before scripts compiled by the customer are run on devices, the scripts must be delivered for review to the Huawei R&D department through the local representative office. After scripts pass review, they can then be implemented.



Information Security Standards - Project Information Security

- Project preparation phase:
 - Project member information, site survey design, network planning, site information.
 - Project plan, project budget.
- Project implementation phase:
 - Project-related version, configuration script, and interconnection commissioning information.
 - Comply with equipment room management regulations and properly store purchased hardware.
 - Remove the remote login feature and delete the test account.
- Project acceptance phase:
 - Return test tools and hand over test reports.
 - Hand over as-built documents, reports of known issues, and accounts and passwords to the corresponding personnel.

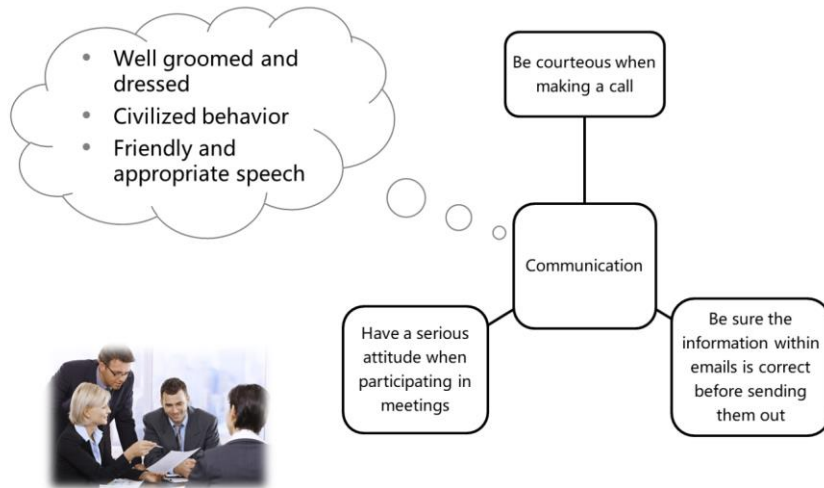
Project
Information
security
scope

- Project preparation phase
 - Member and communication information related to project organizational structure.
 - The customer's communication information related to output files for site survey, network planning, and site information investigations.
 - Business secrets of the customers related to the project plan and budget documents.
- Project implementation phase
 - The received license files involve the customer's business information, such as user quantity and service function information, and must be held strictly confidential.
 - During the commissioning of modules, interconnection and commissioning information obtained from the customer must be deleted after commissioning is completed. This includes information such as system login account and network device access information.
 - During the installation phase, operating system and database software purchased by the customer must not be installed on non-customer devices. Additionally, ESNs or software licenses purchased by the customer must not be used for purposes not directly related to the current project.
 - Documents generated during the installation phase include information on purchased hardware (such as ESNs and barcodes) and are included in the document security scope.

- Comply with the customer's equipment room management regulations when entering, utilizing, or exiting the customer's equipment room.
 - Test tools (test devices) and test cards obtained from the customer in the commissioning phase must be registered and safeguarded by dedicated personnel. They can be used for no purpose other than system testing. After commissioning is completed, these must be returned to the customer and the customer must sign to confirm receipt.
 - The login information used in the remote login environment that is established during the commissioning phase must be modified or deleted after commissioning is completed. The customer must sign to confirm modification or deletion.
 - The test account and balance change information created in the commissioning phase can be retained only if the customer requires that such information be retained and signs to that effect.
 - During commissioning, do not add test account information and account service functions without customer permission. This includes functions such as Ring Back Tone service (RBT service) testing, international calling service testing, and international short message service testing.
 - During the commissioning phase, all access terminals must be configured with antivirus software. Devices to be migrated or transitioned into commercial use must be configured with antivirus software based on the configuration requirements of the contract. Do not install unnecessary software or tools on customer devices without customer permission. Additionally, the customer must be informed of risks associated with installing the software or tools.
 - Acceptance manuals generated during the commissioning phase contain customer business secrets such as service features and accounting information, and are included in the document security scope.
- Project acceptance phase
 - All passwords set for commissioning purposes should be uniformly changed before project handover and included in the handover list. The customer will be prompted to change these passwords and sign to confirm handover content.
 - Internal and external project handover materials can only be delivered to specified internal and external contact persons.
 - The output information on known issues involves the customer's business secrets and is included in the document security scope.
 - The output files include sensitive information, such as project name and project start and end times, and are included in the document security scope.



Etiquette and Daily Behavior



- Appearance

- The dress code is business or business casual. Personal hygiene must be maintained. Behave in a polite manner. Smile to others.

- Behavior

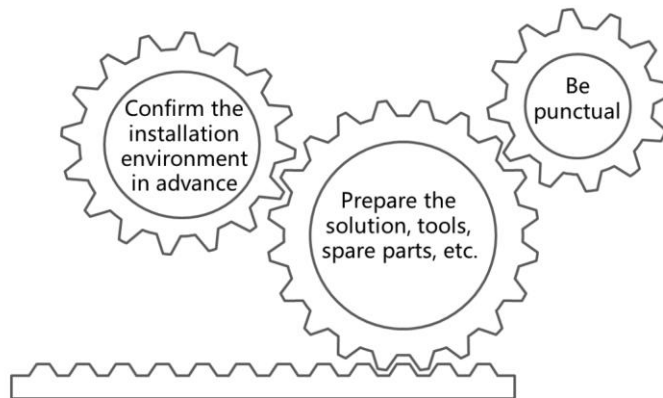
- Maintain appropriate posture. Walk purposefully and steadily. Be calm in case of emergency. Do not cross or shake your legs. Do not slouch in when seated. Be punctual. Comply with social norms and local customs.

- Communication

- Be true to your word. Speak correctly and appropriately. Communicate with a sincere attitude. Respect others and be good at listening. Be concise to express clear information. Be mindful of the situation.
- When answering a call, say hello and introduce yourself by name. Say goodbye when communication ends. Use polite and concise words and a moderate voice volume and tone. Ensure unobstructed communication regardless of time-of-day.
- When participating in a meeting, listen carefully to the words of others. Applaud when a speech concludes. Deliver concise speeches with clear views. Answer questions with courtesy. Listen carefully to criticisms and suggestions. Do not react poorly even when receiving criticisms. Do not affect others if you have to leave during a meeting.
- When sending or receiving an email, ensure the recipient, subject, and sender are clear. Be cautious in emails to avoid blunt, aggressive, or impolite words. If business secrets are involved, consider the scope of recipients.



Onsite Service Behavior Standards - Preparation Before Departure



- Preparation standards

- ❑ After receiving an onsite service task, complete preparations prior to departure. This includes the service solution, operation steps, tools, and spare parts for this task. Doing so will prevent last-minute rush and issues such as consulting instruction documents, borrowing tools, waiting for spare parts, and making emergency calls.
- ❑ Confirm in advance that the installation or maintenance environment, products, and accessories are ready. This will prevent situations where service cannot be begun upon arrival.
- ❑ Confirm in advance the onsite installation or maintenance time. Consider possible external factors such as traffic congestion. When making an appointment, alert the customer that actual arrival may occur up to half an hour later than the appointed time.
- ❑ Once the onsite service time is confirmed, arrive punctually with all required tools and information.
- ❑ Arrive punctually (ideally at least three minutes prior to the appointed time). If extenuating circumstances prevent punctuality, alert the customer at least 30 minutes in advance, and inform them of the new arrival time. Additionally, inform the service project manager of the change by phone call.



Onsite Service Behavior Standards - Service Implementation

- Rights standards:
 - Do not enter the equipment room without permission or take prohibited articles.
 - Only work on things related to the project.
 - Do not operate other vendors' devices that are unrelated to the project.
- Operation standards:
 - The operation scope cannot go beyond the scope approved by the customer.
 - Try to operate devices at off-peak hours.
 - Take ESD measures during operation to avoid damages to devices.
- Attitude standards:
 - Reply to the customer' inquiries patiently.
 - Tolerate criticisms even if the negative consequences are not caused by you and avoid being impolite.

- Rights standards
 - Enter the equipment room with the customer's consent, adhere to the procedures required by the customer, and register articles that enter and exit the equipment room according to the customer's management requirements.
 - Strictly adhere to the customer's rules and regulations. These include regulations on whether shoe covers or work clothes must be worn in the equipment room.
 - Any activities unrelated to work are prohibited at the work site. These include smoking, playing games, visiting non-work websites, and sleeping.
 - Do not use the phone of the customer without permission.
 - Do not operate devices unrelated to the onsite service or the devices of other vendors.
 - Do not install software from illegal sources on customer devices. If the customer requires software to meet service requirements, a disclaimer must be provided by the customer.
- Operation standards
 - Perform maintenance operations on devices with the customer's consent and presence onsite. Use only the temporary account and password provided by the customer. The operation scope cannot exceed previously approved operations. If extra operations are required, submit an application to the customer and explain potential operation impacts.

- Avoid performing service during peak or sensitive hours. Instruct the customer to backup data.
- Take ESD measures including wearing ESD clothing, ESD wrist strap, and ESD gloves when performing operations such as opening a chassis door, plugging or removing boards, or performing operations on the control panel, controller, or hard disk.
- After a spare part replacement, pack the replaced part in appropriate packaging. Use an ESD bag if available.
- Strictly adhere to the customer's management regulations and rules during onsite service. Do not remove customer property from site without permission.
- Attitude standards
 - If the customer has any problems during the onsite service, explain to them patiently and professionally. Do not be rude to or ignore the customer. If the customer requires further explanation, call Huawei's service contact person or the service hotline, provide feedback, and wait for the processing result.
 - In situations where you do not know the answer to a technical question raised by the customer, do not answer hastily. Rather, "Sorry, I need to verify the answer to that question. I will respond as soon as possible." Then contact Huawei's service experts, and pass on the answer to the customer.
 - If the customer asks a question about a function or performance that is currently not provided by the product, do not directly answer that the product does not provide such function or performance. Instead, contact Huawei's service contact person to consult how to reply.
 - Respect and listen to the customer. Do not engage in confrontation with the customer even in cases where the customer is unfriendly or makes impertinent remarks. If agreement cannot be achieved, contact Huawei's service contact person for assistance.
 - If an unfamiliar situation or problem is encountered, directly contact Huawei's service experts for help. Do not seek external assistance through irregular channels, nor should irregular solutions be attempted.



Onsite Service Behavior Standards - Service Completion



Face-to-face
handover

Confirmation

Polite
farewell

- Standards on behavior after service completion
 - If service delivery cannot be completed as scheduled for objective reasons, communicate with the customer, integrator, and Huawei's service contact person either face-to-face or via phone calls. Share your contact information with the customer, and leave the site only when confirmed by the customer.
 - When onsite service is completed, clean any mess created at the work site, give relevant articles and documents to the customer, and explain to the customer how to use and maintain the products. Ask the customer to sign and write feedback in the service report.
 - Express your thanks to the customer prior to leaving. ("Thank you, happy to be of service. Please contact our after-sales service hotline if you have any questions.")



Quiz

1. What are the main steps in the project delivery process?
2. What authorizations are required for implementing a risky operation?
3. What should you remind the customer to do to ensure information security?

- Answer: Project kick-off meeting, solution formulation, unpacking inspection (DOA process), device installation, quality check, software commissioning, maintenance training, and project acceptance.
- Answer: Management authorization, technical authorization, and customer authorization.
- Answer: Remind the customer to delete unneeded accounts, update passwords, protect logs, and back up data.



Thank You

www.huawei.com



Network Maintenance



Foreword

- Stable running of a network ensures smooth implementation of user services and depends on routine maintenance and fault rectification. Routine network maintenance is a preventive measure based on plans, and fault rectification is triggered by events.
- This course describes methods, regulations, and skills of routine maintenance.



Objectives

- Upon completion of this section, you will be able to:
 - Be familiar with routine maintenance tasks
 - Use network management software to maintain networks
 - Master methods of upgrading device software
 - Be familiar with the formats of routine maintenance reports



Contents

1. **Routine Maintenance Overview**
2. Use Method of Network Management Software
3. Device Software Upgrade
4. Routine Maintenance Report



Network Operation - Overview

- Tasks during network operation include routine maintenance and fault rectification.
 - Routine maintenance is **performed regularly** as planned.
 - Fault rectification is **driven by events**.



- After a project is accepted, the project enters the maintenance phase. Tasks at the maintenance phase are classified into routine maintenance and fault rectification by triggering condition. Tasks of these two types do not need to be executed in sequence. Routine maintenance is a planned preventive measure, and fault rectification is event-driven. The purpose of routine maintenance is to prevent problems and decrease the frequency of faults, and that of fault rectification is to find out causes of faults and provide reference for routine maintenance. Routine maintenance also makes fault rectification easier. For example, periodic upgrade of system software helps prevent network faults caused by bugs in the operating system of network devices. The maintenance phase is also called O&M, operation, and operation and maintenance.



Routine Maintenance

- Routine maintenance is a preventive measure.
 - It is conducted regularly when a network is running normally to discover and eliminate defects or faults of network devices. It ensures the long-term, secure, stable, and reliable network running.
- Routine maintenance helps obtain the network baseline, making it easier to troubleshoot network faults.

- Routine maintenance is a preventive measure. It is carried out regularly when a network is running normally to discover and eliminate defects or faults of network devices. It ensures the long-term, secure, stable, and reliable running of networks. You are advised to set up routine maintenance rules based on network conditions to ensure orderly and standardized network maintenance.
- Network maintenance requires both technical measures and a management system. It has low requirements on the operator's skills, but high requirements on operation standardization.
- Routine maintenance helps obtain the network baseline (namely, normal network parameters, such as network devices, performance, and security), making it easier to troubleshoot network faults.



Routine Maintenance - Contents and Methods

- Onsite observing
 - Observe the hardware running environment.
- Remote operation
 - Check the software running status.



```
[AR3260]display current-configuration
[V200R003C00]
#
sysname AR3260
#
snmp-agent local-engineid 800007EB03000000000000
snmp-agent
#
clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load portalpage.zip
#
drop illegal-mac alarm
#
set cpu-usage threshold 80 restore 75
#
```

- The device running environment and device software require routine maintenance.
 - Hardware running environment
 - The hardware running environment includes the equipment room, power supply, and heat dissipation, providing a basis for stable device running.
 - Maintenance personnel need to maintain the hardware running environment onsite. They sometimes need to use professional tools for observation and measurement.
 - Running status of device software
 - Running status of device software is closely related to services. Huawei data communication products use the universal VRP platform. Network engineers must understand common maintenance commands on VRP.
 - Maintenance personnel can maintain device software onsite or remotely, in most cases, using the **display** commands.



Routine Maintenance - Checklists

Checking Interface Information					
No.	Check Item	Check Method	Check Method	Evaluation Criterion	Result Remarks
1	Error packets	Run the display interface counters command.		No error packets, including CRC error packets, exist on the interface.	
2	Negotiation mode	Run the display interface counters command.		The negotiation mode of the interface is correct. The negotiation modes of two	
Checking Basic Device Information					
No.	Check Item	Check Method	Check Method	Evaluation Criterion	Result Remarks
3	Interface configurations	Run the display version command.		The PCB versions of cards and the software version are correct.	
4	Interface status	Run the display status command.		The names of the following system files are correct: Current startup software package, Next startup software package.	
5	Full power supply	Run the display status command.		The device is powered on in a hot position in a well-ventilated and dry environment. No sunlight point around the device.	
Checking Device Operating Environment					
No.	Check Item	Method/Tool	Method/Tool	Evaluation Criterion and Description	Result Remarks
1	Device position	Observe		The operating temperature range for the equipment's long-term running is 0°C to 45°C, and that for the short-term	
2	Ambient temperature in the equipment room	Run the display command.		The in-position information about the status of each unit and subunits are normal.	
3	Ambient humidity	Run the display command.		The Online host is displayed as Present . The Power field is displayed as PowerOn .	
Checking Device Running Status					
No.	Check Item	Check Method	Check Method	Evaluation Criterion	Result Remarks
1	Card running status	Run the display device command.		The in-position information about the status of each unit and subunits are normal.	
2	Resetting	Run the display command.		The Online host is displayed as Present . The Power field is displayed as PowerOn .	
3	Multicast packet statistics	Run the display command.		The in-position information about the status of each unit and subunits are normal.	
4	Multicast forwarding entries	Run the display command.		The in-position information about the status of each unit and subunits are normal.	
5	Multicast routing protocol	Run the display command.		The in-position information about the status of each unit and subunits are normal.	
6	CHCP Snooping	Run the display command.		The in-position information about the status of each unit and subunits are normal.	



- Make a checklist for each check category.

- Routine maintenance is performed based on plans. Therefore, a checklist for each check category is necessary.
- For details about checklists of network devices, see the product documentation of each product model.



Checking Device Operating Environment

Checking Device Operating Environment					
No.	Check Item	Method/Tool	Evaluation Criterion and Description	Result	Remarks
1	Device position	Observe	The device is placed stably in a flat position in a ventilated and dry environment. No sundries exist around the device.		
2	Ambient temperature in the equipment room	Observe/Thermometer	The operating temperature range for the equipment's long-term running is 0°C to 45°C, and that for the short-term running is -5°C to +55°C. <i>Note: The operating temperature requirements of different devices may differ. For details, see the product documentation of each specific product model.</i>		
3	Ambient humidity	Observe/Hygrometer	The relative humidity in long-term operating environment is between 5% RH and 85% RH, non-condensing. The relative humidity in short-term operating environment is between 0% RH and 95% RH, non-condensing. <i>Note: The relative operating humidity requirements of different devices may differ. For details, see the product documentation of each specific product model.</i>		
4	Air conditioner in the equipment room	Observe/Air conditioner	The air conditioner keeps running steadily so that the temperature and humidity in the equipment room is within an acceptable range.		
5	Cleanness condition	Observe	No obvious dust exists. The air filter is cleaned and replaced in time to prevent dust on cabinet doors or fan assembly from affecting heat		

- Focus on the temperature, humidity, and cleanliness.
- If you discover any problem, record it and report it to related personnel. If the problem is difficult, seek help from technical support personnel.
- You are advised to check the device operating environment every day.

- A normal running environment is the prerequisite for proper device running.
- Normal device running requires appropriate temperature and humidity. A standard equipment room must have thermometer and hygrometer installed. Maintenance personnel should check and record the temperature and humidity in the equipment room every day.
- To ensure proper device running, the equipment room must be kept clean and neat.
 - If the equipment room is not clean, devices cannot dissipate heat properly.
 - Devices and cables must be placed and routed in compliance with standard installation and deployment requirements. During network running, temporary adjustments are often made. For example, temporary jumper tests are performed. After several times of adjustments, the equipment room may become disordered. The purpose of checking the device operating environment is to discover and correct such problems.
- When checking a nonstandard equipment room (for example, the equipment room of a floor), focus on the cleanliness and heat dissipation conditions.



Checking Basic Device Information

Checking Basic Device Information					
No.	Check Item	Check Method	Evaluation Criterion	Result	Remarks
1	Software version	Run the display version command.	The PCB versions of cards and the software version are correct.		
2	Software package	Run the display startup command.	The names of the following system files are correct: Current startup software package Next startup software package Backup software package Current and next startup configuration, license, patch, and voice files		
3	License information	Run the display license and display license state commands.	The name, version, and configuration items of the GTL license file are correct. Based on the obtained information, check whether the version needs to be upgraded. The Master board license state field is displayed as Normal . If the Master board license state field is displayed as Demo or Trial , the license is in the validity period.		
4	Patch information	Run the display patch-information command.	The installed patches meet actual requirements. The latest patches of the product released by Huawei are recommended. The patches are valid. That is, the total number of patches is the same as the number of running patches.		

- Focus on the version, startup information, license, and storage space.
- If you discover any problem, record it and report it to related personnel. Find out the cause and plan for rectification.
- You are advised to check basic device information every week or month.

- Software version information

- The version of software run by devices should be determined during project construction and does not change in normal conditions. During device maintenance, if you discover that the version information changes, find out the reason. In most cases, the software version information changes due to improper management.
- If a device is added, it may run software of a different version. In addition, the software of some devices may be upgraded or rolled back. Devices of the same model may run software of different versions, especially on a large-scale network. In this case, check whether all these software versions meet network function requirements.

- Startup information

- A network device may have different system versions or configuration files. In this case, changing device startup information will cause serious risks to proper network running. If the device restarts (for example, due to a power supply failure), the entire network may be affected.

- License information

- License rules of devices may vary. Pay attention to the devices that use licenses having a validity period.

- Storage space

- Most devices have tens or even hundreds of gigabytes storage space. However, devices generate files, such as log files, when they are running. In certain situations, for example, when a device is attacked or the device information frequently changes, the device generates a large number of log files. If log files keep increasing, the storage space of the device will be used up, and key information will be lost.



Checking Device Running Status

Checking Device Running Status					
No.	Check Item	Check Method	Evaluation Criterion	Result	Remarks
1	Card running status	Run the display device command.	The in-position information about the status of cards and subcards are normal. The Online field is displayed as Present . The Power field is displayed as PowerOn . The Register field is displayed as Registered . The Alarm field is displayed as Normal .		
2	Resetting	Run the display reset-reason command (on AR routers or S series modular switches) or the display reboot-info command (on S series fixed switches).	The reset information, including reset time and causes, shows that no abnormal reset occurs.		
3	Device temperature	Run the display temperature command (on AR routers, NE routers, or S series modular switches) or the display environment command (on S series fixed switches).	The temperature of each module of an AR router or S series switch falls between the upper limit and lower limit. That is, the value of Temperature is between the value of Upper and Lower . If the temperature of an NE router (the value of Temp(C)) is higher than the value of Minor for a long time, check the operating environment of the router, such as the air conditioner, vent, and air filter.		

- Focus on alarms of cards, power supply, fans, temperature, CPU, and memory.
- If you discover any problem, record it and report it to related personnel. If the hardware is faulty, contact the provider for technical support.
- You are advised to check the device running status every week or month.

- When checking device running status, focus on the running status of hardware, such as the cards, power supply, fans, temperature, CPU, and memory. Most devices have alarm indicators. When a hardware fault occurs on a device, the alarm indicator on the device is on (the indicator status depends on the specific product model). Therefore, you can observe device indicators to discover errors.
- Check and determine the running status of a card, power supply, or fan based on guides provided by the device manufacturer. If necessary, contact the device manufacturer for technical support. If you confirm that a hardware failure occurs, contact the supplier. (Maintenance solutions of different projects and devices differ. In some scenarios, if the device hardware is faulty, you can contact the manufacturer for replacement. In other scenarios, you need to contact the supplier for help.)



Checking Interface Information

Checking Interface Information					
No.	Check Item	Check Method	Evaluation Criterion	Result	Remarks
1	Error packets	Run the display interface command.	No error packets, including CRC error packets, exist on the interface.		
2	Negotiation mode	Run the display interface command.	The negotiation mode of the interface is correct. The negotiation modes of two connected interfaces must be the same. No interface is in half-duplex mode.		
3	Interface configurations	Run the display current-configuration interface command.	The interface configurations, such as the duplex mode, negotiation mode, rate, and loopback configuration, are correct.		
4	Interface status	Run the display interface brief command.	The Up and Down states of interfaces are correct. The traffic transmitted and sent by the interface does not exceed 70% of the bandwidth for a long time.		
5	PoE power supply	Run the display poe power-state interface interface-type interface-number command.	The PoE power supply is normal. If the Port power ON/OFF field of an interface is displayed as ON , the Port power status field of the interface is displayed as Delivering-power .		

- Focus on error packet statistics, duplex mode, and traffic statistics.
- If you discover any problem, record it and report it to related personnel. If a fault is discovered, analyze it and find out the cause.
- You are advised to check interface information every week or month.

- Network devices exchange data packets through interfaces. If an interface fails, network functions will be affected.
- If a large number of error packets are received on an interface and the number increases within a short period of time, a link (including the physical ports) may be faulty.



Checking Services

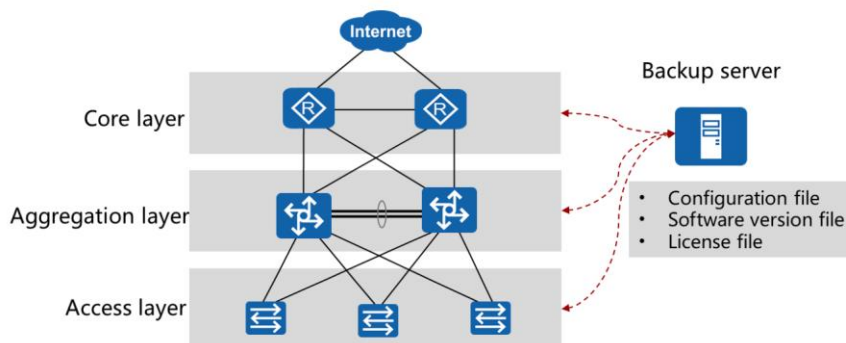
Checking Services					
No.	Check Item	Check Method	Evaluation Criterion	Result	Remarks
1	Information about multicast member interfaces and router interfaces	<HUAWEI> display igmp-snooping port-info	Information about static member interfaces, dynamic member interfaces, static router interfaces, and dynamic router interfaces is correct.		
2	Multicast packet statistics	<HUAWEI> display igmp-snooping statistics vlan	The number of IGMP packets and PIM Hello packets received and sent by a VLAN is correct, and the number of Layer 2 events in all the VLANs is correct.		
3	Multicast forwarding entries	Run the display l2-multicast forwarding-table command to view the Layer 2 multicast forwarding entries. Run the display multicast forwarding-table command to view the Layer 3 multicast forwarding entries.	The multicast forwarding entries are correct.		
4	Multicast routing protocol	Run the display multicast routing-table command.	PIM-SM is used as the intra-AS multicast routing protocol. IGMP is enabled on all multicast interfaces.		
5	DHCP Snooping binding table	<HUAWEI> display dhcp snooping user-bind all	Static and dynamic entries are correct.		
6	MAC address table	<HUAWEI> display mac-address	MAC address table information is correct.		

- Focus on functions or protocols related to the running services, such as multicast, OSPF, and BGP.
- If you discover any problem, record it and report it to related personnel. If an exception occurs, analyze it and find out the cause.
- You are advised to check service every week or month.

- Service running status is the running status of network protocols, which are related to specific services. For example, a relatively large-scale network uses routing protocols such as OSPF, and a large-scale routing network may use BGP. Set a checklist based on deployed services.
- The neighbor status mechanisms of protocols may differ. For example, if two routers establish an OSPF neighbor relationship, the OSPF neighbor state must remain Full. If two routers establish a BGP peer relationship, the BGP peer state must remain Established.



Backing Up Software and Configurations



- The purpose of backup is to recover networks in certain situations.
- You are advised to back up software and configurations every week.

- Both software and configurations (including the license file) need to be backed up for network function recovery in certain situations.
 - When a device cannot start due to a hardware failure or when a device is replaced by another device of the same model, services can hardly recover fast if no backup configuration file exists.
 - Software versions also need to be backed up. Back up the software of the same product model and version once. You can also download a corresponding version file from the official website of the manufacturer to your PC.
 - A license file is set for a specific product. If the license file of a device is accidentally lost (for example, the file is deleted by accident), apply for a new license through the manufacturer's application flow. You need to provide information such as the contract number and device SN. The application takes a long time. If the license file is backed up, you can restore the license on the device fast.
- To back up files, upload the files to the backup server. You can consider a device as an FTP or a TFTP client, and run commands to transmit files to be backed up to the backup server.
- You are advised to back up configuration files every week. Before changing the configuration of a device, back up the configuration file of the device.

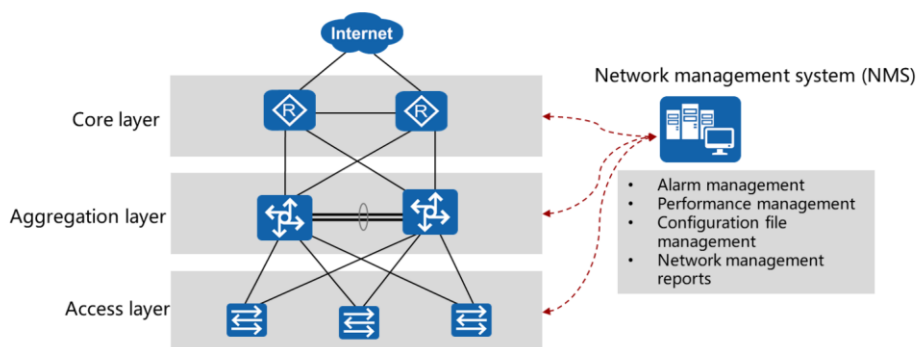


Contents

1. Routine Maintenance Overview
- 2. Use Method of Network Management Software**
3. Device Software Upgrade
4. Routine Maintenance Report



Network Management System (eSight)

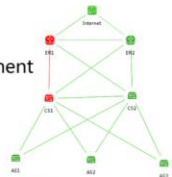


- Routine maintenance involves many repeated and simple tasks. Network management software can be used to improve network maintenance efficiency.

- Most software operations can be performed on a network management system.
 - Alarm management: For example, the status change of a device interface is reported to the network management software through trap messages, so that network faults can be discovered immediately.
 - Performance management: For example, the network management software can automatically collect and calculate the usage of CPU and memory, helping analyze the network performance bottleneck.
 - Configuration file management: The network management software automatically compares and restores configuration files. It can automatically back up configuration files in a batch.
 - In addition, the network management software can also generate reports periodically for network optimization based on user requirements.

eSight Functions

- Alarm management



Rule Name	Rule Type	Description	Created	Start Time	End Time	Status	Operation
all-permy	All permissions	Created aws07-02-...				Enabled	
Link Down	Link down	Created aws07-02-...	2017-02-27 19:35:57	2017-02-27 19:35:57		Enabled	
Link Up	Link up	Created aws07-02-...	2017-02-27 19:35:57	2017-02-27 19:35:57		Enabled	

- Configuration file management

Device Name	Device ID	Subnet	Device Type	FTP Type	Latest Backup Time	Startup Configuration	Running Configuration	Operation
1000-537	172.28.38	/	13700-2079-P000	5770				View Download
1000-537	172.28.38	/	13700-2079-P000	5770				View Download
1000-619	172.30.164	/	13700-5607-P000	6070				View Download

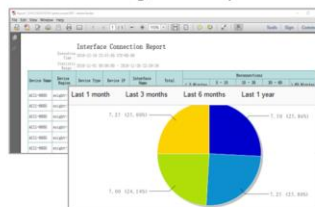
- Performance management

Top N Average Memory Usage

Time range: Last hour Update time: 2017-02-22 19:56

Device Name	Memory Usage	Percentage
i-405-537	<div></div>	69.2%
i-408-537	<div></div>	69.0%
i-17-4822	<div></div>	50.0%
i-12-4822	<div></div>	50.0%
i-504-537	<div></div>	29.0%
i-16-4812	<div></div>	21.0%
i-11-4822	<div></div>	18.0%
AC11-4605	<div></div>	14.0%

- Network management reports



- Alarm management
 - Alarm management provides the following functions:
 - Provides methods such as network-wide alarm monitoring and remote alarm notifications to inform maintenance personnel of faults right after faults occur, ensuring fault troubleshooting efficiency.
 - Provides customized functions such as alarm masking, alarm filtering, and alarm severity redefinition to meet requirements in various scenarios.
 - The eSight provides advanced management functions to uniformly manage alarms of network-wide devices and displays device and interface alarm information on a topology, improving working efficiency.
 - One alarm of a device can be considered as a single event. However, if alarms generated by multiple devices simultaneously or a series of alarms generated by a device within a certain period are summarized and processed on the network management system, potential problems are readily discovered. This helps prevent serious network faults.

- Performance management
 - During network operation, the network performance may deteriorate due to internal or external problems, causing network faults. To plan, monitor, and measure network performance such as the throughput rate and usage, performance management ensures that the network works properly and prepares the network for future expansions. Performance management also helps discover and resolve network performance deterioration to prevent network faults. The eSight provides a visualized operation page that allows users to monitor network KPIs and collect performance data statistics, facilitating network performance management.
 - In most cases, default thresholds are set for key performance indicators on the network management system. Once a threshold is exceeded, the system generates an alarm. To meet actual service requirements, you can modify the thresholds to proper values based on observations on network running for a period.
- Configuration file management
 - The eSight provides the device configuration management function, in which the configuration file backup, restoration, comparing, and baseline are managed. When a network fault occurs, eSight compares configuration files backed up when the network is running properly with the current configuration files. Based on the comparison, the network maintenance can rapidly locate and rectify the fault. In addition, eSight also manages configuration modifications. After a configuration file is backed up, eSight automatically compares the backup configuration file with the current configuration file. If the configuration file is modified, eSight generates an alarm and sends an email to a preset contact to notify the contact of the modification.
 - Configuration file management improves the routine maintenance efficiency.
- Network management reports
 - For example, eSight provides the report management function to execute report tasks periodically or allow users to execute report tasks manually. Reports can be exported in common file formats, including PDF, Excel, and Word. The eSight integrates multiple report templates to meet common network operation and maintenance requirements. You can customize the contents and formats of reports as required.
 - By analyzing reports, you can better understand and control the entire network.
 - You can specify a time period, and eSight provides you with statistics within that period and analysis on the statistics.
 - The eSight can also provide information statistics and analysis on the entire network.



Contents

1. Routine Maintenance Overview
2. Use Method of Network Management Software
- 3. Device Software Upgrade**
4. Routine Maintenance Report



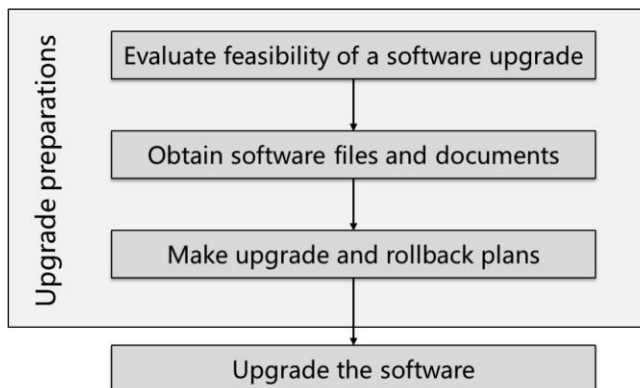
Software Upgrade - Necessity

- New versions support new functions or new hardware modules.
 - New functions are developed.
 - Usability is improved.
 - Stability is higher.
 - Newly developed hardware modules require new software versions.
- New versions fix the bugs in old versions.
 - Software has bugs.
 - Latest versions fix known bugs.

- When designing products, manufacturers use advanced hardware architecture and upgrade software to improve or optimize product performance.
- Device functions are implemented by both hardware and software.
 - Hardware features are relatively fixed.
 - Software needs to be updated continuously.
 - Software reflects hardware features.
- Updating software brings benefits, but a new version may not be better than the current software version. If the current software can support proper service running and does not have major security risks, it does not need to be upgraded. You are advised to contact the device manufacturer or supplier for suggestions before a software upgrade.



Preparing for Software Upgrade

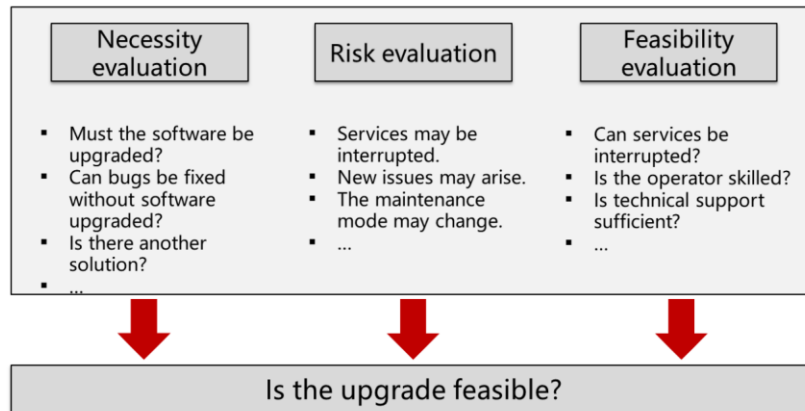


- Prepare well before a software upgrade.

- During network design and construction, better preparations in the overall design phase facilitate the network deployment. The same is true for a software upgrade. Prepare well for the upgrade, and then upgrade software step by step.
- Prepare well before a software upgrade.
 - Evaluate the feasibility of software upgrade and determine whether to upgrade the software.
 - Copy the target software and relevant documents through the official channel.
 - Make an upgrade plan and an emergency rollback plan.
 - Perform the upgrade.



Evaluating Feasibility of Software Upgrade

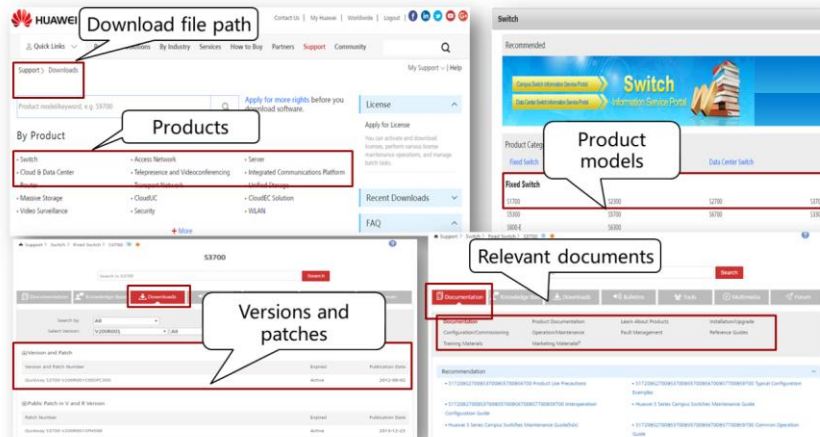


- To ensure stable network device running, you are not advised to upgrade device software unless necessary. You can upgrade device software in the following situations:
 - A new hardware module is added to devices and the current software does not support the module.
 - Services that are only supported by new software versions are required.
 - The current version has bugs that cannot be fixed. You can fix the bugs by upgrading the software only.
- Determine whether to upgrade the software according to professional suggestions of the product manufacturer or supplier.
- Software upgrade may affect the running stability of the network. Before upgrading the software, evaluate the risks and take preventive measures. Consider technologies and services comprehensively when evaluating upgrade risks and take preventive measures. If there are risks cannot be prevented, seek technical support. Do not upgrade the software hastily. Software upgrade has the following risks:
 - If the features provided by the new version differ from those in the old version, services may be affected.
 - The device needs to be restarted after the upgrade, resulting in temporary service interruption.
 - The device may fail to restart due to incorrect operations during the upgrade.

- Take the following measures to control risks:
 - Before the upgrade, ask professional personnel whether the device can be upgraded.
 - Make an upgrade plan and prepare upgrade tools and software.
 - Back up the configurations and license files and prepare a rollback plan.
- Software upgrade is feasible only when technical conditions are met. Determine whether to perform the upgrade after considering user services, maintenance personnel's maintenance plans, operators' skills, and technical support assurance. Online device upgrade affects proper services running. Take the following precautions:
 - The upgrade may interrupt services for a short period of time. Before the software upgrade, confirm whether the user can accept service interruptions.
 - After the upgrade, operation modes (such as commands) of the device may change. Confirm whether the user can accept the changes.
 - Evaluate the importance and complexity of the upgrade and ensure that the operator must be able to manage emergencies during the upgrade.
 - Coordinate with technical support personnel during the upgrade.
 - If the upgrade is important or complex, test the commissioning, upgrade, and emergency plans in a simulation environment.



Obtaining Software Files and Upgrade Guides



You can obtain software of latest versions from the official websites of network equipment manufacturers.

- You can obtain latest software versions from the official websites of network equipment manufacturers. For example, on Huawei website, you can download the latest software for Huawei products as well as related documents, including the following:
 - Upgrade guide: Describes upgrade operations. The upgrade operations on Huawei data communication products are similar. However, there are exceptions. Before an upgrade, read carefully the upgrade guide.
 - Command, alarm, MIB, and trap delta information: Describes updates in commands, traps, and MIBs.
 - Feature delta information: Describes updates in software and hardware features and specifications.
 - Release notes: Describe version mapping and known issues.



Upgrade and Rollback Plans

- An upgrade plan includes the following:
 - Upgrade time and operation window (service interruption duration)
 - Upgrade object and tool (including relevant scripts)
 - Operating personnel and technical support (responsibility division)
 - Verification method (before and after the upgrade)
- A rollback plan includes the following:
 - Rollback triggering conditions
 - Rollback process (including verification)
 - Emergency measures in case the upgrade cannot be rolled back

- Upgrade time and operation window
 - The upgrade time depends on the urgency of an upgrade requirement. If it is not urgent, reserve sufficient time for preparations.
 - The operation window must be within the period when the user services can be interrupted and longer than the time of upgrade execution. Reserve a period of time for fault rectification.
- Upgrade object and method
 - The upgrade object involves the number of devices to be upgraded, device locations, versions of currently running software, supported upgrade modes, whether the current software can be upgraded directly to the target version, and whether remote upgrade is supported.
 - Select an upgrade method based on the upgrade object. In most cases, devices are upgraded online by using command lines.
- Operating personnel and technical support
 - Determine an operator to perform upgrade operations. The operator must possess required technical skills.
 - Repeat evaluating upgrade risks. Contact technical support personnel in advance. If necessary, set up a technical support team.
- If you upgrade software to rectify a fault, confirm the following issues:
 - Before the upgrade, locate the fault and confirm that no other fault exists.
 - After the upgrade, confirm that the fault is rectified and no new fault arises.

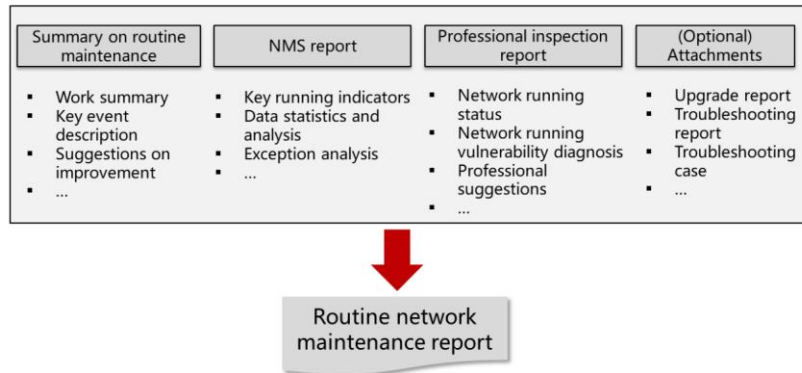


Contents

1. Routine Maintenance Overview
2. Use Method of Network Management Software
3. Device Software Upgrade
4. **Routine Maintenance Report**



Routine Maintenance Report



- Routine maintenance based reports include the following:
 - Summary on routine maintenance, for example, whether routine check on the equipment room environment is normally conducted and if an exception is discovered, whether the exception is properly removed.
 - Description of key events, especially of the events affecting services.
 - Suggestions on rectification of problems discovered during network maintenance, which also help the network maintenance personnel improve maintenance skills.
- NMS reports
 - If network management software is deployed, reports generated by the software can be included in routine maintenance reports.
 - The network management software provides accurate statistics in a timely manner. Network maintenance personnel analyze the statistics and make decisions. For example, when the network management software detects that the CPU usage of some devices is high, it cannot determine the cause or offer further O&M suggestions. The root cause (for example, the devices are attacked or the devices have insufficient performances) can only be located by the maintenance personnel after the maintenance personnel comprehensively analyze the statistics. After locating the root cause, the maintenance personnel can rectify the fault (by removing the attack source or replacing the devices with other devices with higher performance).
- Professional inspection tools
 - As a leading network device vendor, Huawei provides professional inspection tools to check the running status of devices and networks and provide professional reports. Based on the reports, network maintenance personnel can discover potential network risks and take proper measures to minimize the risks.
 - The inspection tools are professional services and need to be purchased separately if required.



Quiz

1. Which statements about functions of network maintenance are correct?

Routine maintenance is a preventive measure.

Routine maintenance helps obtain the network baseline, making it easier to troubleshoot network faults.

Routine maintenance has high requirements on the operator's skills, but low requirements on operation standardization.

Network maintenance requires both technical measures and management systems.

- Answer: ABD.



Thank You
www.huawei.com



Network Troubleshooting Overview



Foreword

- To most modernized enterprises, the stable running of network infrastructure is of great importance. Service interruption due to network faults may lead to output loss, profit loss, and damaged reputation. Therefore, network troubleshooting is indispensable in the Plan, Design, Implement, Operate, Improve (PDIOI) model.



Objectives

- Upon completion of this section, you will be able to:
 - Master a structured network troubleshooting process
 - Master network troubleshooting methods based on paths that service traffic passes through



Contents

1. **PDIOT and Network Troubleshooting**
2. Structured Network Troubleshooting Process
3. Core Theories and Common Methods of Network Troubleshooting



What Is a Network Fault?

- When a specific network function fails due to certain reasons and services are affected, a network fault occurs.
- For a network user, any symptom that affects services can be defined as a network fault.

- When a specific network function fails due to certain reasons and services are affected, a network fault occurs.
- For a network user, any symptom that affects services can be defined as a network fault. It can be a system or compatibility fault, but is not limited to device faults.



Network Fault Type

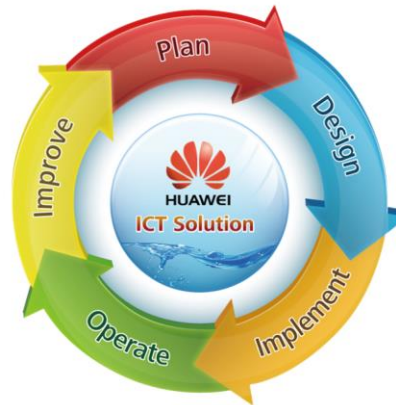
Symptom Type	Alarm	Loop	Service failure	Service interruption	Temporary service interruption	Packet loss	Protocol exception	Protocol flapping	Route exception
Hardware	√			√		√			
Configuration		√	√				√		√
Network		√	√	√	√	√	√	√	√
Performance	√				√	√		√	√
Software							√		√
Interconnection		√	√				√		
Others	√		√	√	√	√			

- Network faults can be divided into the following types: hardware, configuration, network, performance, software, interconnection, and other faults. Different network faults have different symptoms, as described in the table.



PDIOI and Network Troubleshooting

- Operate:
 - Routine maintenance
 - **Troubleshooting**



- Network troubleshooting is critical in the Operate phase of PDIOI.
- The aim of routine maintenance is to prevent faults, and that of troubleshooting is to take measures to let the system recover quickly when a fault occurs.
- Troubleshooting is an event-driven task and often unexpected. Therefore, the requirements on technical capabilities of engineers are high.
- Proper routine maintenance can prevent a large number of abrupt faults. However, due to network running limitations, even the best routine maintenance cannot totally eliminate the possibility of faults. Therefore, network maintenance personnel must master key techniques, including the troubleshooting process and methods.



Contents

1. PDIOI and Network Troubleshooting
- 2. Structured Network Troubleshooting Process**
3. Core Theories and Common Methods of Network Troubleshooting



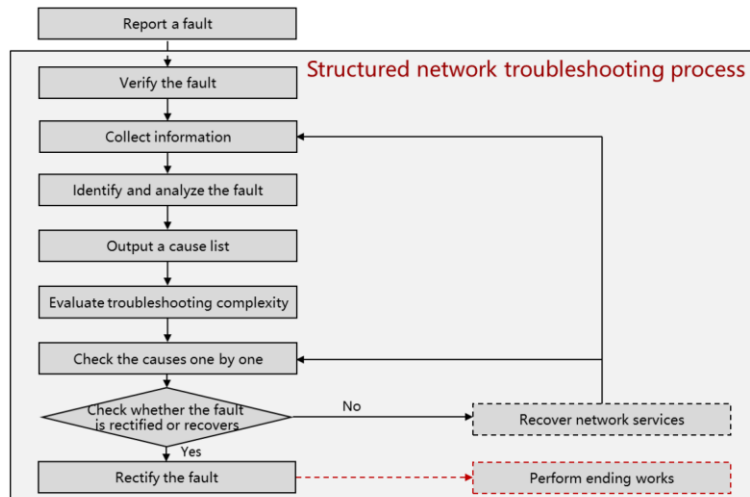
Raising a Problem

- If network troubleshooting is performed based on personal intuitions or past experiences, it may cause the following issues:
 - Difficulties in team collaboration
 - No summary documents for troubleshooting
 - Failure to ensure troubleshooting continuity

- If network troubleshooting is performed based on personal intuitions or past experiences, you may find the final solution, but you will struggle to transfer the work to others, which poses difficulties on teamwork. Troubleshooting results may be forgotten or lost. After a certain period, when you detect an old fault again, there is a possibility that this fault cannot be rectified.



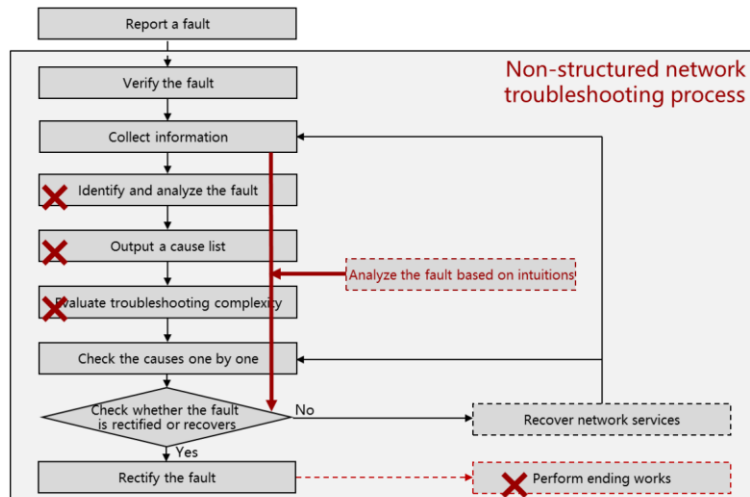
Structured Network Troubleshooting Process



- The structured network troubleshooting process is triggered by a fault report. It provides a rational method for locating the cause and rectifying a fault. Generally, troubleshooting steps include verifying faults, collecting information, identifying and analyzing faults, outputting cause lists, evaluating troubleshooting complexity, checking causes one by one, and rectifying faults. In this process, the possible causes of a fault can be grouped into multiple cause sets, making troubleshooting easier.
- After rectifying a fault, perform ending works, including outputting troubleshooting reports, reporting to related departments, and notifying troubleshooting results.



Non-structured Network Troubleshooting Process



- If a non-structured network troubleshooting process is used, and steps are repeated based on intuitions, you may find the final solution. However, troubleshooting may be inefficient.
- In a complex network environment, a non-structured network troubleshooting process may cause new faults, making troubleshooting more difficult.



Reporting a Fault

- On Monday morning, you received a call from an employee reporting a fault: "I cannot access the Internet on my PC. Please rectify the fault as soon as possible."



- What should you do after receiving this call?



Reporting a Fault: Verifying the Fault Through Proactive Communication

Fault Reporter	The name, department, job position and level, and responsible field, PC location (including the room, floor, and whether wireless or wired access is used), and the website that is accessed when the fault occurs
Fault Frequency	Whether the fault is unexpected, occasional, or frequent
User Operation	User operations on the terminal before and after the fault occurs, for example, whether the IP address or domain name server (DNS) is changed, and whether desktop firewall or security control software is installed

- Query the user about the preceding information over the phone and record it in the troubleshooting report.

- Generally, the network troubleshooting process is triggered by a fault report from a user. Information provided by the user is often unclear and ambiguous. Therefore, proactive communication and verification are necessary.



Reporting a Fault: Speculating the Cause

- Question:
 - Why should I obtain the job position and level, and responsible field of the user?
- Answer:
 - In an enterprise, users of different job levels may have different network access rights. Also, for users of the same job level, they may only have the rights to access network services that are related to their individual works.



Reason for Verifying the Fault

- The fault description of a user may be unclear, and the failure point reported by a user may be mistaken. Therefore, an experienced engineer is required to verify the fault.



- For example, in this simple network environment, a user may report that: "The server is faulty and I cannot access it." However, the root cause may be a link failure.



Verifying the Fault

- Four key elements in fault verification:
 - Entity
 - Symptom
 - Time
 - Location
- Provide an accurate description of the symptom.
- Determine whether the fault is within your scope of responsibility.

- Verify the following items to determine the fault:
 - Entity: Which network service fails?
 - Symptom: What is the fault symptom?
 - Time: When does the user detect the fault and when does the fault actually occur? (Deduced by professional personnel.)
 - Location: Which network component fails?
- Provide an accurate description of the symptom.
- Determine whether the fault is within your scope of responsibility and whether you have corresponding rights to rectify the fault.



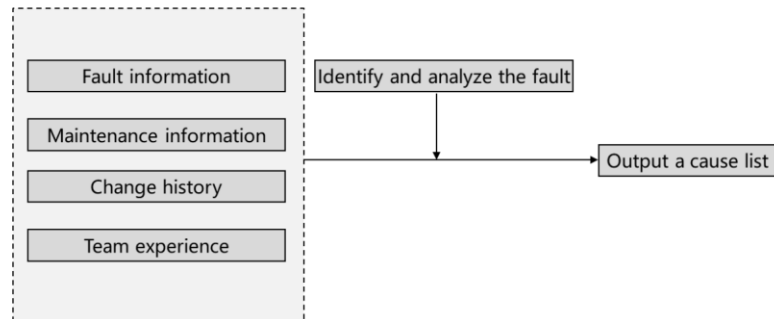
Collecting Information

- Information to be collected
- Collection methods
- Authorization requirements
- Risk assessment for information collection

- Information to be collected: Collect fault information, including document and network changes.
- Collection methods: Execute CLIs on devices or use information collection tools, such as a packet capturing tool and NMS software.
- Authorization requirements: In a network environment with strict the information security requirements, information collection shall be authorized and signed authorization documents in written form may be required.
- Risk assessment for information collection: Some information collection operations (for example, running the **debug** command on a router or switch) may result in high CPU usage, or even lead to a response failure of a device and cause new faults. Therefore, assess risks for information collection and balance the risks of causing new faults and with urgency for solving existing faults. Users shall be notified of these risks and determine whether information collection tasks with a high risk should be performed.



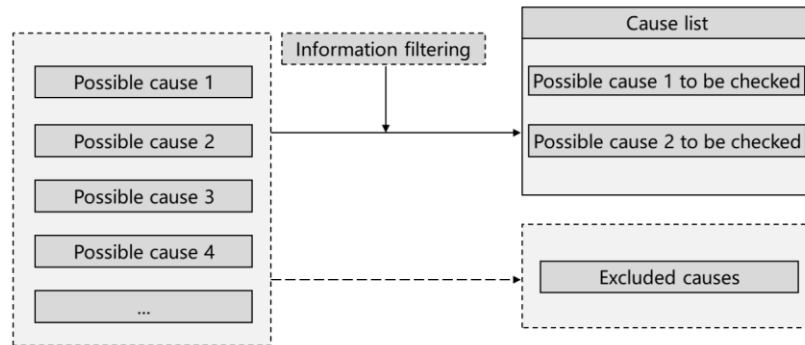
Identifying and Analyzing the Fault



- In this phase, analyze and summarize collected information.
- Identify and analyze the fault by summarizing information about faults, maintenance, and changes and combining team or personal experiences, and then output a list of possible causes.



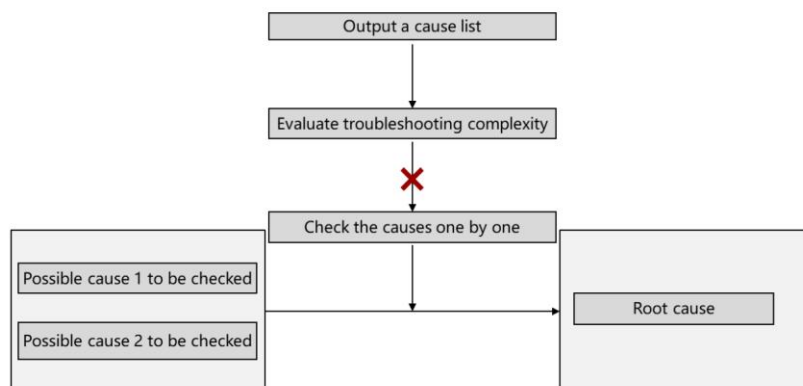
Outputting a Cause List



- In this phase, list all possible causes, and then eliminate the least possible causes and output the most possible causes, so that the possible cause scope is narrowed.



Evaluating Troubleshooting Complexity

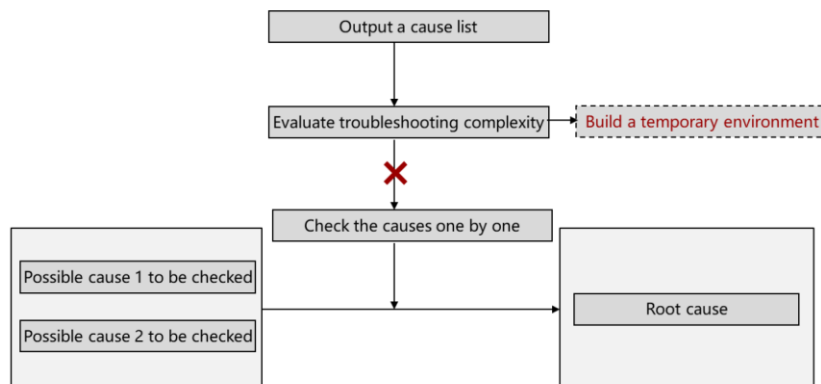


- Evaluate troubleshooting complexity before checking the causes one by one.

- After listing causes to be checked, evaluate troubleshooting complexity (such as difficulties and duration) before checking the causes one by one.



Evaluating Troubleshooting Complexity: Building a Temporary Environment



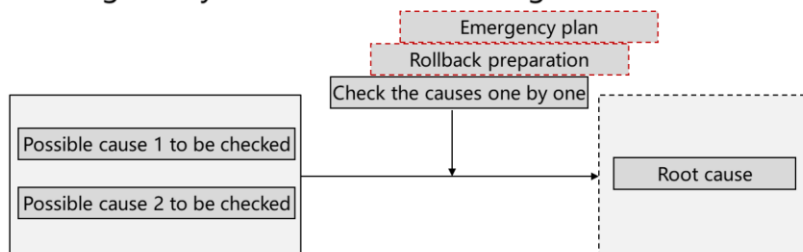
- A temporary network environment may need to be built for troubleshooting complexity evaluation.

- After evaluation, if a complex network fault cannot be rectified quickly but a user needs to access network services immediately, a temporary network environment should be built to bypass the failed node.
- Before building a temporary network environment, consider both the urgency for rectifying the fault and the risks in bypassing some security limitations, communicate with users to verify details, and obtain corresponding permissions.



Checking the Causes One by One

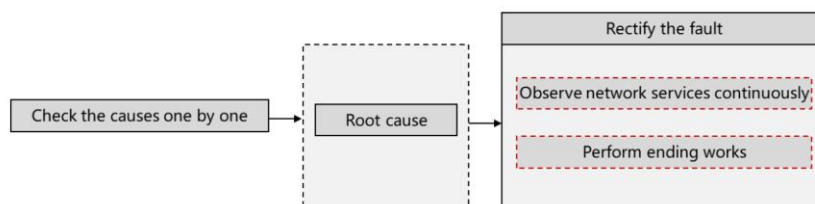
- Network changes may be involved in checking the cause.



- In this phase, you also need to balance the urgency for solving existing faults against the risks of causing new faults. Notify users of the risks of troubleshooting and perform operations only after corresponding permissions are obtained.
- In some cases, network changes may be involved in checking the cause. If so, comprehensive emergency plans and rollback must be prepared.



Rectifying the Fault

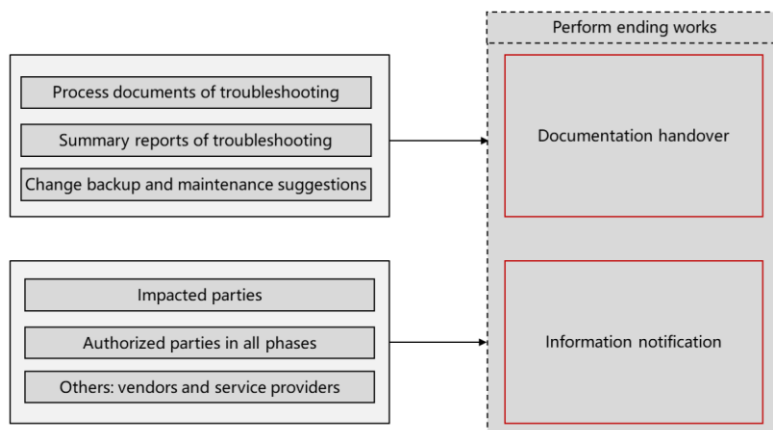


- In some cases, you need to observe network services for a certain period after the fault is rectified.

- When you find the root cause of a fault and rectify the fault, the network troubleshooting process ends.
- In a complex network environment, you need to observe network services after the fault symptom disappears to ensure that the fault reported by a user is rectified and no new fault was introduced during troubleshooting.



Rectifying the Fault: Performing Ending Works

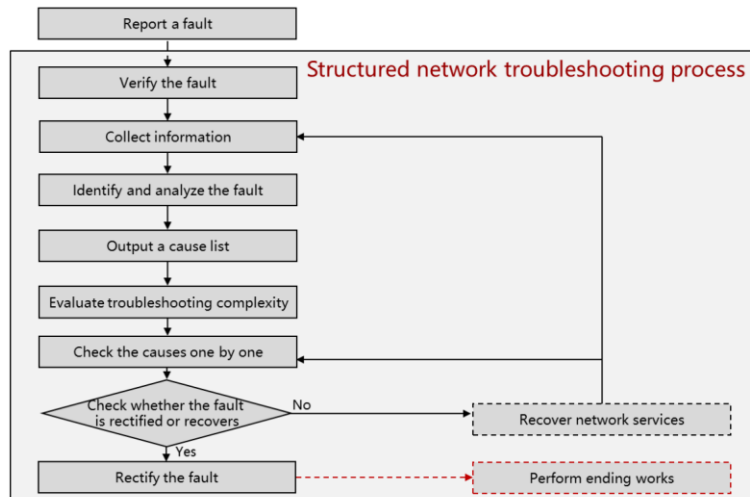


- Ending works after troubleshooting are equally important.

- Ending works include documentation organization and information notification. Back up configurations and software that are changed in the network troubleshooting process, and organize and hand over corresponding documentations. To avoid the fault, propose improvement suggestions to users.



Review: Structured Network Troubleshooting Process



- Compared with a non-structured network troubleshooting process, the results of the structured network troubleshooting process are predictable. The troubleshooting affects are easily controlled, and the risks in causing new faults are easily evaluated.

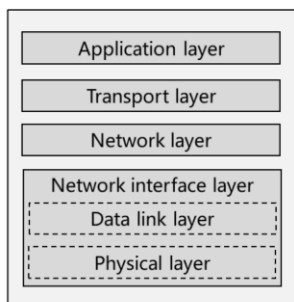


Contents

1. PDIOI and Network Troubleshooting
2. Structured Network Troubleshooting Process
3. **Core Theories and Common Methods of Network Troubleshooting**



TCP/IP Reference Model and Network Troubleshooting

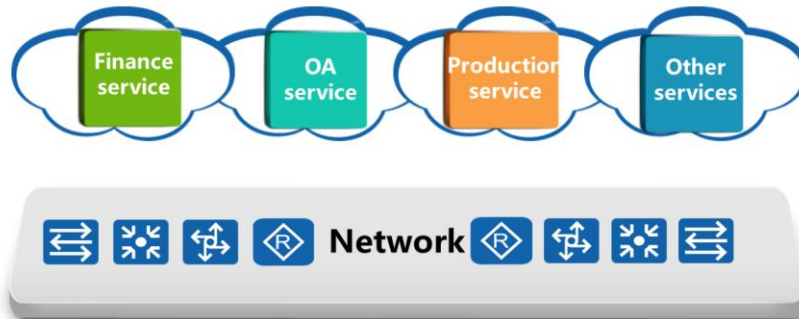


- The Transmission Control Protocol/Internet Protocol (TCP/IP) model forms the basis of network troubleshooting theories. The physical and data link layers in the Open Systems Interconnection (OSI) reference model also require attention.

- The TCP/IP model forms the basis of network troubleshooting theories. The physical and data link layers (correspond to the network interface layer of the TCP/IP model) in the OSI reference model also require attention. It is recommended that you first determine and test service traffic paths at the network interface layer and network layer of the TCP/IP model separately, and then use the top-down or bottom-up method to locate the fault.



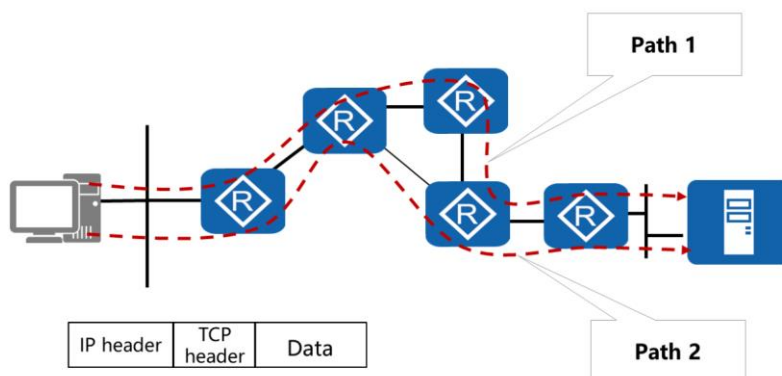
Troubleshooting Theories Based on Service Traffic Paths



- How can I implement troubleshooting in a complex network environment?
- This figure shows a complex network environment involving finance, OA (Office Automation) systems, production services, and even more service systems. In this situation, check data flow directions of all service systems first.
- In an enterprise, the function of a network is to support services. Therefore, you can locate the fault by identifying the traffic of an affected service and tracing the traffic paths in the transmit and receive directions.
- In most cases, the service traffic paths of a network are designed in the network planning phase. You can first ask users about the traffic paths designed for affected services, and then use the **ping** command or Tracert tool to test whether the current paths are consistent with the designed paths.



Confirming Service Traffic Paths: Network Layer

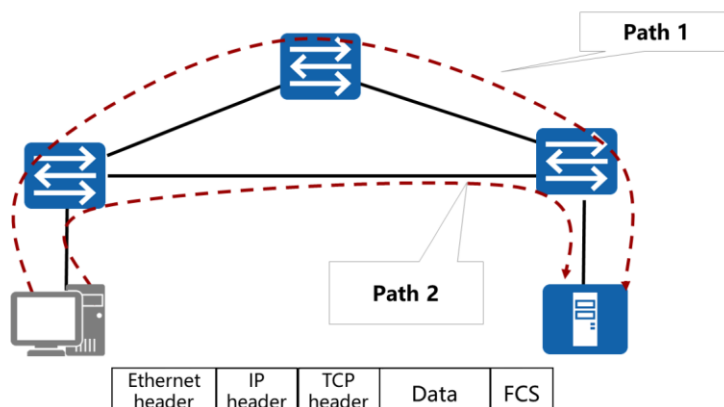


- Check routing paths of packets at the network layer.

- At the network layer, check routing paths of data packets on devices that have routing functions (such as routers, switches with routing functions, and firewalls).



Confirming Service Traffic Paths: Data Link Layer

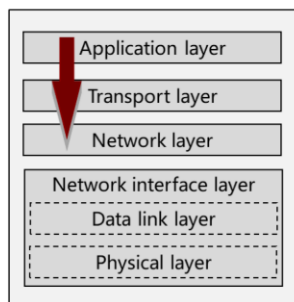


- Check forwarding paths of data frames on switches at the network interface layer.

- At the data link layer, check forwarding paths of data frames on switches. That is, check the MAC address tables on switches and port roles after Spanning Tree Protocol (STP) convergence. In some cases, packet capturing tools are required.



Top-down Method

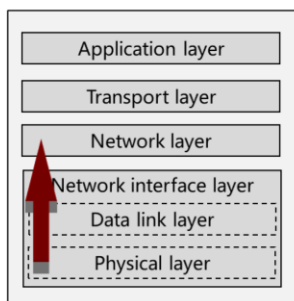


- If no fault is detected in network layer connectivity, use this method to locate the fault.

- Check network layer connectivity by checking the service traffic paths.
- If no fault is detected in network layer connectivity, use the top-down method to locate the fault. That is, start at the application layer: Compare the working statuses of the same applications and check whether a proxy or firewall exists.



Bottom-up Method



- If a fault is detected in network layer connectivity, use this method to locate the fault.

- If a fault is detected in the network layer connectivity, a fault may occur at the network layer or lower layers. In this situation, use the bottom-up method to locate the fault. At the physical layer, check whether a network cable is faulty. At the data link layer, check whether a Layer 2 loop or mismatched protocol exists. At the network layer, check whether a routing protocol configuration error exists or the filtering function of firewalls is enabled.



Comparing Configurations

```
[R1]display isis 1 brief

                ISIS Protocol Information for ISIS(1)
SystemId:
Area-Auth:
Domain-Auth:
Ipv6 is not enabled
ISIS is in invalid restart status
Interface: 10.1.1.1(Loop0)
Cost: L1 0      L2 0
State: IPV4 Up
Type: P2P
Priority: L1 64  L2 64
Timers:  Csnp: L12 10 , Retransmit: L12 5 , Hello: 10 ,
Hello Multiplier: 3 , LSP-Throttle Timer: L12 50

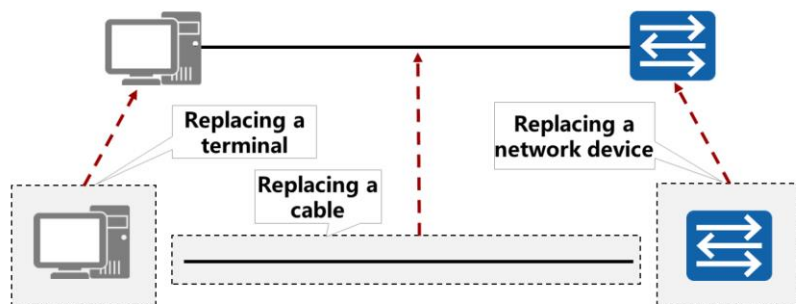
[R2]display isis 1 brief

                ISIS Protocol Information for ISIS(1)
-----
SystemId: 0000.0000.0001      System Level: L1
Area-Authentication-mode: NULL
Domain-Authentication-mode: NULL
Ipv6 is not enabled
ISIS is in invalid restart status
Interface: 10.1.1.1(Loop0)
Cost: L1 0      L2 0      Ipv6 Cost: L1 0      L2 0
State: IPV4 Up      IPV6 Down
Type: P2P      MTU: 1500
Priority: L1 64  L2 64
Timers:  Csnp: L12 10 , Retransmit: L12 5 , Hello: 10 ,
Hello Multiplier: 3 , LSP-Throttle Timer: L12 50
```

- Compare the configurations, software versions, and hardware versions in normal and faulty states.
- This method is commonly used by network troubleshooting personnel who have limited experience.



Replacing Entities



- This method is frequently used in hardware troubleshooting.

- This method is frequently used in hardware troubleshooting. When no more information can be collected for fault locating, you can replace entities to narrow down the fault scope.
- This method can also be used at the application layer. For example, when a user from a finance department reports a finance server access failure, check whether the other users in the same department have this problem.



Part-by-Part Troubleshooting

- Analyze the configuration files of network devices part by part:

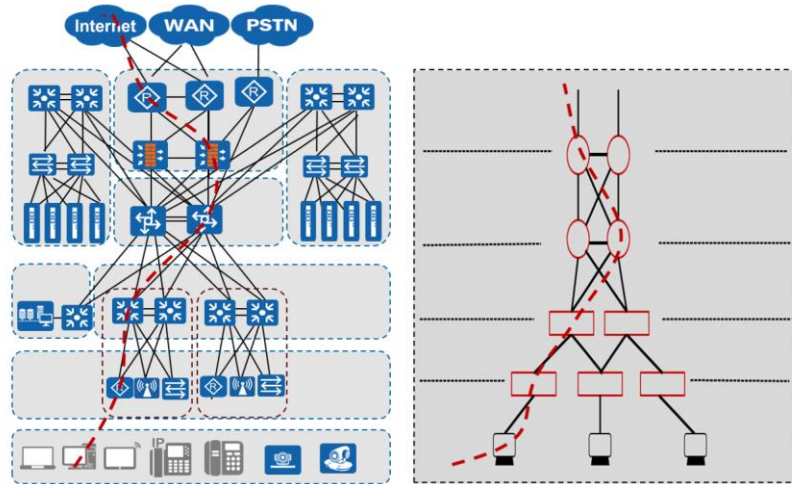


Configuration	Content
Management part	Router names, passwords, services, logs, and so on.
Interface part	Addresses, encapsulation, costs, authentication, and so on.
Routing protocol part	Static routes, Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), route import, and so on.
Policy part	Routing policies, policy-based routing, security configurations, and so on.
Access part	Telnet login, and so on.
Other applications part	Quality of service(QoS) configurations, and so on.

- Configuration files of Huawei's network devices (including routers and switches) have a clear structure, which includes the following parts:
 - Management part: router names, passwords, services, logs, and so on.
 - Interface part: addresses, encapsulation modes, costs, authentication modes, and so on.
 - Routing protocol part: static routes, RIP, OSPF, BGP, route import, and so on.
 - Policy part: routing policies, policy-based routing, security configurations, and so on.
 - Access part: Telnet login, and so on.
 - Other applications part: QoS configurations, and so on.
- When a network fault is located on a specific network device, you can use the part-by-part troubleshooting method to analyze the configuration file of this device to further narrow down the fault scope.



Segment-by-Segment Troubleshooting



- When locating a network fault on a large-scale network, you can use the segment-by-segment troubleshooting method to narrow down the fault scope based on traffic paths of affected services.



Quiz

1. In the ending works of the structured network troubleshooting process, which of the following parties need to be notified?

Impacted parties

Authorized parties in all phases

Vendors and service providers

Unrelated personnel who are interested in the root cause of the fault

- Answer: ABC.



Thank You

www.huawei.com



Troubleshooting Common Network Faults

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.



Foreword

- When a fault occurs on a network, it is more difficult to fast locate the fault and determine the cause than to rectify the fault. By learning this course, you will understand methods of troubleshooting common network faults. You will be able to fast locate fault points, find out the causes, and rectify the faults to restore networks.



Objectives

- Upon completion of this section, you will be able to:
 - Master methods of troubleshooting common network faults



Contents

1. Basic Configuration Faults

- Telnet Login Failure
- SSH Login Failure

2. LAN Faults

3. IP Routing Protocol Faults

4. IP Service Faults

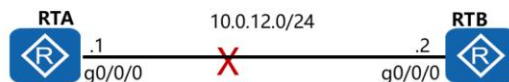
5. Reliability Faults

6. Security Faults

7. Network Management Faults



Telnet Login Failure



No.	Procedure
1	Enable the Telnet server function and set parameters.
2	Configure a user interface for Telnet login.
3	Configure a local Telnet user (AAA authentication mode).
4	Log in to the device through Telnet from a terminal.

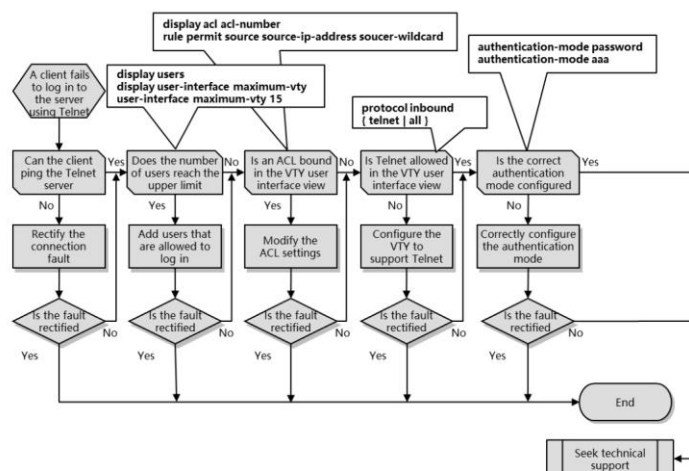
```
acl number 2001
rule 5 permit source 10.0.12.1 0
rule 10 deny #
aaa
local-user admin1234 password cipher
huawei
local-user admin1234 privilege level 3
local-user admin1234 service-type telnet
#
user-interface maximum-vty 8
#
user-interface vty 0 7
acl 2001 inbound
authentication-mode aaa
```

- The route between the Telnet client and server is unreachable. As a result, a TCP connection cannot be established between the client and server.
- The number of users logging in to the server has reached the upper limit.
- An access control list (ACL) is bound in the virtual type terminal (VTY) user interface view.
- Telnet is not configured as an allowed protocol in the VTY user interface view. For example, the **protocol inbound ssh** command is configured.

- Telnet is an application layer protocol in the TCP/IP protocol suite and provides remote login and virtual terminal functions. The server/client mode is used. Telnet clients send requests to the Telnet server, which provides the Telnet service. The devices support the Telnet client and server functions.
- By default, you cannot log in to a device directly using Telnet. Before using Telnet to log in, you must locally log in to the device through a console port and perform the following configurations:
 - Configure a route between a terminal and the device.
 - Enable the Telnet server function and set parameters.
 - Configure a user interface for Telnet login.
 - Configure a local Telnet user (AAA authentication mode).
 - Log in to the device through Telnet from the terminal.
- Common causes of Telnet login failure are as follows:
 - The route between the client and server is unreachable. As a result, a TCP connection cannot be established between the client and server.
 - The number of users logging in to the server has reached the upper limit.
 - An ACL is bound in the VTY user interface view.
 - Telnet is not configured as an allowed protocol in the VTY user interface view. For example, if the **protocol inbound ssh** command is configured, you cannot log in to this VTY channel through Telnet.



Telnet Login Failure - Troubleshooting Process



- Check whether the client can ping the server.
 - Run the **ping** command on the client to check the network connection. If the ping operation fails, a Telnet connection cannot be set up between the Telnet client and server.
 - If the ping operation fails, rectify the fault in the connection between the client and server to enable the Telnet client to ping the server.
- Check whether the number of login users reaches the upper limit.
 - Log in to the device through the console port and run the **display users** command to check whether all VTY channels are in use. By default, a maximum of five users are allowed. You can run the **display user-interface maximum-vty** command to check the maximum number of users allowed in the current VTY channel.
 - If the number of users logging in to the server has reached the upper limit, run the **user-interface maximum-vty 15** command to increase the maximum number of users allowed to log in to the server through VTY channels to 15.
- Check whether an ACL is configured in the VTY user interface view.
 - Run the **user-interface vty** command on the Telnet server to enter the user interface view and then run the **display this** command to check whether an ACL is configured in the VTY user interface view. If yes, record the ACL number.

- Run the **display acl** *acl-number* command on the Telnet server to check whether the IP address of the Telnet client is denied in the ACL. If yes, run the **undo rule** *rule-id* command in the ACL view to delete the deny rule, and then run the **rule permit source source-ip-address soucer-wildcard** command to permit the IP address of the client.
- Check whether the correct access protocol is configured in the VTY user interface view.
 - Run the **user-interface vty** command on the Telnet server to enter the user interface view, and then run the **display this** command to check whether **protocol inbound** is set to **telnet** or **all**. By default, the system supports the SSH and Telnet protocols. If **protocol inbound** is not set to **telnet** or **all**, run the **protocol inbound { telnet | all }** command to allow Telnet users to connect to the device.
- Check whether an authentication mode is set for login users in the user interface view.
 - If the password authentication mode for login is configured in the VTY channel using the **authentication-mode password** command, you must enter the password upon login.
 - If the AAA authentication mode is configured using the **authentication-mode aaa** command, you must run the **local-user user-name password** command to create a local AAA user.
- If the fault persists after the preceding operations are performed, collect the following information and contact Huawei technical support personnel.
 - Results of the preceding troubleshooting procedure.
 - Configuration files, logs, and alarms of the devices.



Contents

1. Basic Configuration Faults

- Telnet Login Failure
- SSH Login Failure

2. LAN Faults

3. IP Routing Protocol Faults

4. IP Service Faults

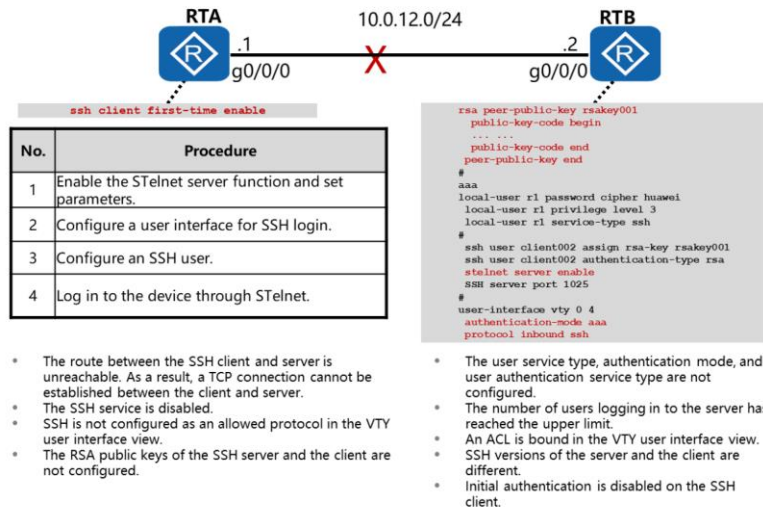
5. Reliability Faults

6. Security Faults

7. Network Management Faults



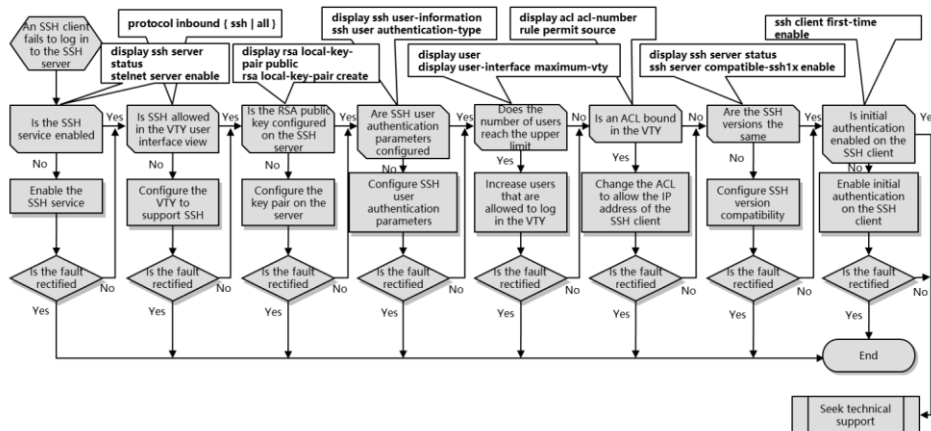
SSH Login Failure



- Telnet uses the TCP protocol to transmit plain texts, which does not have a secure authentication mode and is vulnerable to Denial of Service (DoS), IP address spoofing, and route spoofing attacks.
- Through STelnet based on SSH2.0, a client and the server establish a secure connection through negotiation, and the client can then log in to the server.
- By default, you cannot log in to a device directly using STelnet. Before using STelnet to log in, you must locally log in to the device through a console port or remotely log in using Telnet and perform the following configurations:
 - Configure a route between a terminal and the device.
 - Enable the STelnet server function and set parameters.
 - Configure a user interface for SSH login.
 - Configure an SSH user.
 - Log in to the device through STelnet.
- Common causes of SSH login failure are as follows:
 - The route between the SSH client and server is unreachable. As a result, a TCP connection cannot be established between the client and server.
 - The SSH service is disabled.
 - SSH is not configured as an allowed protocol in the VTY user interface view.
 - The RSA public keys of the SSH server and the client are not configured.
 - The user service type, authentication mode, and user authentication service type are not configured.
 - The number of users logging in to the server has reached the upper limit.
 - An ACL is bound in the VTY user interface view.
 - SSH versions of the server and the client are different.
 - Initial authentication is disabled on the SSH client.



SSH Login Failure - Troubleshooting Process



- Check whether the SSH service is enabled on the SSH server.
 - Log in to the SSH server through a console port or using Telnet. Run the **display ssh server status** command to check the SSH server configuration.
 - If the STelnet service is disabled, run the **stelnet server enable** command to enable the STelnet service on the SSH server.
- Check whether the correct access protocol is configured in the VTY user interface view.
 - Run the **user-interface vty** command on the SSH server to enter the user interface view, and then run the **display this** command to check whether **protocol inbound** is set to **ssh** or **all**. If not, run the **protocol inbound { ssh | all }** command to allow STelnet users to connect to the device.
- Check whether an RSA public key is configured on the SSH server.
 - A local key pair must be configured when the device functions as an SSH server.
 - Run the **display rsa local-key-pair public** command on the SSH server to check the current key pair. If no information is displayed, no key pair is configured on the server. Run the **rsa local-key-pair create** command to create a key pair.
- Check whether an SSH user is configured on the SSH server.

- Run the **display ssh user-information** command to check the SSH user configuration. If no configuration is displayed, run the **ssh user authentication-type** command in the system view to create an SSH user and set the authentication mode for the SSH user.
- Check whether the number of login users on the SSH server reaches the upper limit.
 - Log in to the device through the console port and run the **display users** command to check whether all VTY channels are in use. By default, a maximum of five users are allowed. You can run the **display user-interface maximum-vty** command to check the maximum number of users allowed in the current VTY channel.
 - If the number of users logging in to the server has reached the upper limit, run the **user-interface maximum-vty 15** command to increase the maximum number of users allowed to log in to the server through VTY channels to 15.
- Check whether an ACL is bound to the VTY user interface of the SSH server.
 - Run the **user-interface vty** command on the SSH server to enter the SSH user interface view. Run the **display this** command to check whether an ACL has been configured in the VTY user interface view. If yes, record the ACL number.
 - Run the **display acl acl-number** command on the SSH server to check whether the IP address of the SSH client is denied in the ACL. If yes, run the **undo rule rule-id** command in the ACL view to delete the deny rule, and then run the **rule permit source source-ip-address soucer-wildcard** command to permit the IP address of the client.
- Check the SSH versions of the SSH client and server.
 - Run the **display ssh server status** command on the SSH server to check the SSH version.
 - If the version is SSH v1, run the **ssh server compatible-ssh1x enable** command to configure the version compatibility function on the server.
- Check whether initial authentication is enabled on the SSH client.
 - Run the **display this** command in the system view on the SSH client to check whether initial authentication is enabled on the SSH client.
 - If not, the initial login of the SSH client fails because validity check on the RSA public key of the SSH server fails. Run the **ssh client first-time enable** command to enable initial authentication on the SSH client.
- If the fault persists after the preceding operations are performed, collect the following information and contact Huawei technical support personnel.
 - Results of the preceding troubleshooting procedure.
 - Configuration files, logs, and alarms of the devices.

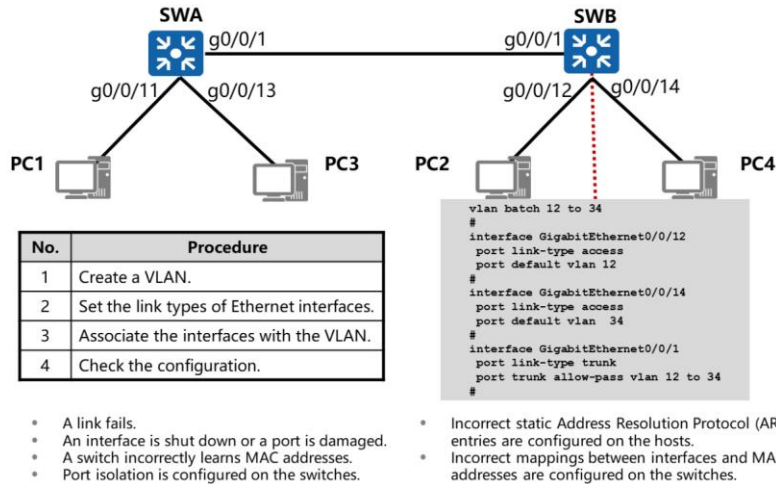


Contents

1. Basic Configuration Faults
- 2. LAN Faults**
 - VLAN Faults
 - MSTP Faults
 - Loops
3. IP Routing Protocol Faults
4. IP Service Faults
5. Reliability Faults
6. Security Faults
7. Network Management Faults



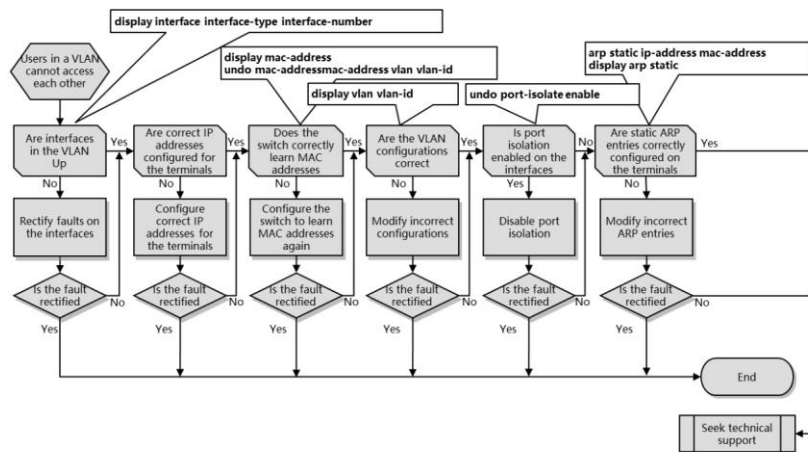
VLAN Faults



- Ethernet technology implements data communication over shared media based on Carrier Sense Multiple Access/Collision Detection (CSMA/CD). When an Ethernet network has a large number of hosts, collision becomes a serious problem and can lead to broadcast storms. As a result, network performance deteriorates, or the entire network breaks down. Using switches to connect local area networks (LANs) can mitigate collisions, but cannot isolate broadcast packets or improve network quality. The VLAN technology divides a physical LAN into multiple VLANs to isolate broadcast domains. Hosts within a VLAN can communicate with each other but cannot communicate with hosts in other VLANs directly. Therefore, broadcast packets are restricted within a VLAN.
- Configure a VLAN as follows:
 - Create a VLAN.
 - Set the link types of Ethernet interfaces.
 - Associate the interfaces with the VLAN.
 - Check the configuration.
- Common causes of VLAN faults are as follows:
 - A link fails.
 - An interface is shut down or a port is damaged.
 - A switch incorrectly learns MAC addresses.
 - Port isolation is configured on the switches.
 - Incorrect static Address Resolution Protocol (ARP) entries are configured on the hosts.
 - Incorrect mappings between interfaces and MAC addresses are configured on the switches.



VLAN Faults - Troubleshooting Process



- Check whether the interfaces connected to the user terminals in the VLAN are Up.
 - Run the **display interface interface-type interface-number** command to check the running status of the interfaces. If an interface is Down, rectify the fault on the interface.
- Check whether the IP addresses of the user terminals are on the same network segment. If not, change the IP addresses of the user terminals to IP addresses on the same network segment.
- Check whether the MAC address entries on the switch are correct.
 - Run the **display mac-address** command on the switch to check whether the MAC addresses, interfaces, and VLAN in the learned MAC address entries are correct. If any item is incorrect, run the **undo mac-address mac-address vlan vlan-id** command to delete the MAC address entries so that the switch learns specified MAC addresses again.
- Check whether the VLAN configurations are correct.
 - Run the **display vlan vlan-id** command in any view to check whether the VLAN to which the interfaces belong are created. If not, run the **vlan** command in the system view to create the VLAN.
 - Run the **display vlan vlan-id** command to check whether the interfaces to communicate are added to the VLAN. If not, add the interfaces to the VLAN. If the interfaces are on different switches, add the interfaces connecting the switches to the VLAN and configure the interfaces to allow packets of the VLAN to pass.
- Check whether port isolation is configured on the switch.
 - Run the **interface interface-type interface-number** command in the system view to enter the faulty interface view, and then run the **display this** command to check whether port isolation is configured on the interface. If yes, run the **undo port-isolate enable** command to disable port isolation configured on the interface.
- Check whether incorrect static ARP entries are configured on the terminals. If any incorrect static ARP entry is configured on a terminal, modify it.
 - Run the **display arp static** command to check the configured static ARP entries. Run the **arp static ip-address mac-address** command to modify static ARP entries.
- If the fault persists after the preceding operations are performed, collect the following information and contact Huawei technical support personnel.
 - Results of the preceding troubleshooting procedure.
 - Configuration files, logs, and alarms of the devices.

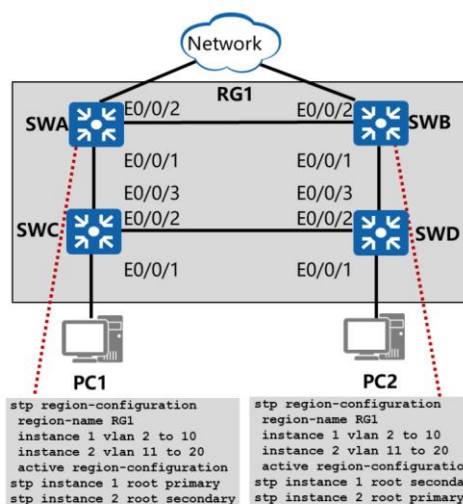


Contents

1. Basic Configuration Faults
- 2. LAN Faults**
 - VLAN Faults
 - MSTP Faults
 - Loops
3. IP Routing Protocol Faults
4. IP Service Faults
5. Reliability Faults
6. Security Faults
7. Network Management Faults



MSTP Faults



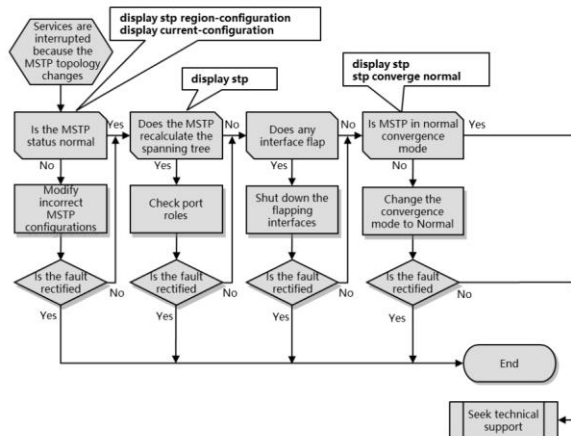
No.	Procedure
1	Configure the MSTP mode.
2	Configure a Multiple Spanning Tree (MST) region and activate the configuration.
3	(Optional) Configure the root bridge and the backup root bridge.
4	(Optional) Set the priorities of the switches in the specified multiple spanning tree instances (MSTIs).
5	(Optional) Set the path costs of ports in the specified MSTIs.
6	(Optional) Set the priorities of ports in the specified MSTIs.
7	Enable MSTP.

- The configuration of Multiple Spanning Tree Protocol (MSTP) is incorrect.
- A physical link flaps, and the devices send many TC packets.
- Devices on which MSTP is enabled receive MSTP TC packets from clients or transparently transmitted.

- To implement redundancy on a complex network, network designers tend to deploy multiple physical links between two devices, one of which is the primary link and the others are the backup links. In this situation, loops may occur, causing broadcast storms or damaging MAC address entries. MSTP can be deployed to prevent loops. MSTP blocks redundant links on a Layer 2 network and prunes the network into a tree topology free from loops.
- Configure MSTP as follows:
 - Configure the MSTP mode.
 - Configure an MST region and activate the configuration.
 - (Optional) Configure the root bridge and the backup root bridge.
 - (Optional) Set the priorities of the switches in specified MSTIs.
 - (Optional) Set the path costs of ports in the specified MSTIs.
 - (Optional) Set the priorities of ports in the specified MSTIs.
 - Enable MSTP.
 - Check the configuration.
- Common causes of MSTP faults are as follows:
 - The MSTP configuration is incorrect.
 - A physical link flaps, and the devices send many TC packets.
 - Devices on which MSTP is enabled receive MSTP TC packets from clients or transparently transmitted.



MSTP Faults - Troubleshooting Process



- Check whether the status of the interfaces on the MSTP network is normal.
 - Check the interface status in MSTP instances to confirm the connectivity of each interface in each instance.
- Check whether the MSTP configuration is correct.
 - Run the **display stp region-configuration** command to check the mappings between VLANs and instances.
 - Check whether the mappings between the VLANs and instances are correct. If not, run the **instance** command to map a specified VLAN to a specified spanning tree instance, and then run the **active region-configuration** command to activate the mapping between the VLAN and instance.
 - Run the **display current-configuration** command to obtain the configuration files of devices and check the MSTP configuration of the devices.
 - Check the interface configuration. Check whether the protocol packet sending function is enabled on the interfaces on which MSTP is enabled using commands (for example, **bpdu enable**).
 - Check whether MSTP is disabled on the interfaces connecting to user terminals or whether the interfaces are set to edge ports.
 - If bridge protocol data unit (BPDU) tunneling is configured on the devices on which MSTP is enabled, check whether the BPDU tunneling configuration is correct.

- Check whether the device interfaces are added to correct VLANs.
- Check whether MSTP recalculation occurs on the network.
 - Run the **display stp** command in any view to check whether the devices receive TC packets.
 - If the values of **TC or TCN received, TC count per hello, TC received,** and **TC count per hello** in the command output increase, the devices have received TC packets and the network topology has changed. Check the **MSTP/6/SET_PORT_DISCARDING** and **MSTP/6/SET_PORT_FORWARDING** logs to check whether the roles of the interfaces on which MSTP is enabled change.
 - If the values of **TC or TCN received, TC count per hello, TC received,** and **TC count per hello** in the command output are 0, the devices do not receive TC packets. Contact senior technical support personnel.
- Check whether any interface flaps.
 - If the status of an interface on which MSTP is enabled frequently changes between Up and Down, the interface flaps. If physical interfaces alternate between Up and Down states frequently, the MSTP status of devices on the network will be unstable, many TC packets will be generated, and ARP and MAC address entries will be deleted frequently. As a result, services will be interrupted. Shut down the flapping physical interfaces.
- Check whether the MSTP convergence mode is Normal.
 - Run the **display stp** command in any view to check the MSTP convergence mode. If the mode is Fast, run the **stp converge normal** command to change the mode to Normal.
- If the fault persists after the preceding operations are performed, collect the following information and contact Huawei technical support personnel.
 - Results of the preceding troubleshooting procedure.
 - Configuration files, logs, and alarms of the devices

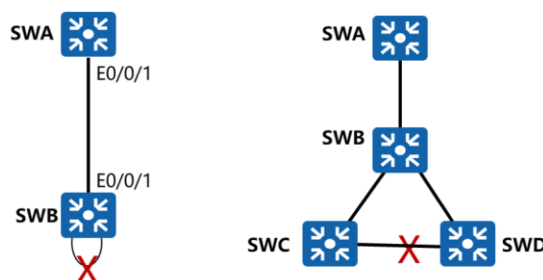


Contents

1. Basic Configuration Faults
- 2. LAN Faults**
 - VLAN Faults
 - MSTP Faults
 - Loops
3. IP Routing Protocol Faults
4. IP Service Faults
5. Reliability Faults
6. Security Faults
7. Network Management Faults



Loops

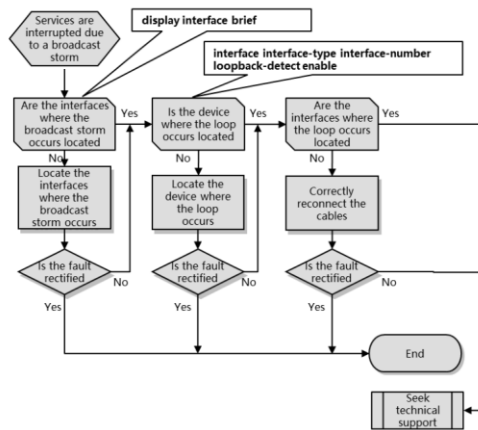


- If loops cause broadcast storms, the communication quality deteriorates and communication services may be interrupted.

- If no loop has occurred on an Ethernet, broadcast Ethernet frames are flood on the network to ensure that they can be received by every device. Each Layer 2 device forwards received broadcast frames to all interfaces except the interface receiving these frames. However, if a loop occurs, this broadcast mechanism will affect the entire network.
- When broadcast storm is generated, Ethernet frames are forwarded permanently, and the forwarding speed reaches or approximates the line speed on an interface to consume link bandwidth. According to Ethernet forwarding rules, these broadcast frames are copied to all interfaces. Therefore, the entire network is full of broadcast frames. Assume that an Ethernet uses GE connections, every link is full of broadcast frames at the speed of 1000 Mbit/s. Other data packets cannot be forwarded. As a result, services are affected. The communication quality deteriorates, and the communication service may even be interrupted.
- The following situations may occur:
 - Users cannot remotely log in to switches.
 - The **display interface** command output shows a large number of broadcast packets received on an interface.
 - It takes a long time to log in to a switch from the serial port.
 - The CPU usage of a switch exceeds 70%.
 - A lot of Internet Control Message Protocol (ICMP) packets are lost in ping tests.
 - Indicators of interfaces in the VLAN where a loop has occurred blink at a higher frequency than usual.
 - PCs receive a large number of broadcast packets.
 - Loop alarms are generated after loop detection is enabled.
- Loops occur because of incorrect cable connections, causing the preceding faults.



Loops - Troubleshooting Process



- Locate the interface where a broadcast storm has occurred.
 - Use either of the following methods:
 - Check the indicator of each interface. If the indicator of an interface blinks at a higher frequency than usual, a broadcast storm may have occurred on the interface.
 - Run the **display interface brief** command to check the inbound and outbound bandwidth usage in a recent period of time on each interface. In the command output, **InUti** indicates the inbound bandwidth usage, and **OutUti** indicates the outbound bandwidth usage. If both the inbound bandwidth usage and outbound bandwidth usage on an interface approximate to 100%, a broadcast storm may have occurred on the interface.
- Locate the device where a loop has occurred.
 - If a broadcast storm has occurred on a single interface and the interface is not connected to any switch, the loop has occurred on the local switch.
 - If the interface is connected to a switch, the loop may have occurred on the local switch or the switch connected to the interface.
 - Enable loopback detection in the VLAN where the loop has occurred and configure the switch to generate an alarm when detecting a loop. If the **LDT 1.3.6.1.4.1.2011.5.25.174.3.3 hwLdtPortLoopDetect** alarm is generated, the interface displayed in the alarm message is the interface where the loop has occurred. If the interface displayed in the alarm

- message is the interface connected to a switch, the loop has occurred on one of the downstream switches connected to the interface. If this alarm is not generated, the loop has occurred on the local switch.
- If the loop has occurred on one of the downstream switches, repeat the preceding operations until the switch where the loop has occurred is located.
- If broadcast storms occur on multiple interfaces and each of the interfaces is connected to a switch, the loop may occur between switches.
- Run the **shutdown** command on the interface connected to the local switch, and check whether the broadcast storm persists on the local switch and the entire network.
 - If the broadcast storm persists on the local switch but disappears on the downstream switch, the loop has occurred on the local switch.
 - If the broadcast storm has occurred on an interface that is not connected to any switch, the loop has occurred on the switch where this interface resides.
 - If the broadcast storm disappears on the local switch and the entire network, the loop has occurred between switches.
 - If the interface where a broadcast storm has occurred is connected to downstream switches, and these switches also encounter a broadcast storm, repeat the preceding operations on the switches until the switch where the loop has occurred is located.
- Locate the interfaces where the loop has occurred and remove the loop.
 - If the loop has occurred on a single switch, the loop is generated because two interfaces in the same VLAN on the switch are directly connected. Remove the loop as follows:
 - Check whether the interface where a broadcast storm has occurred is connected to another interface on the local switch. If yes, remove the network cable between the interfaces.
 - Run the **shutdown** command on the interface where a broadcast storm has occurred. If the broadcast storm disappears, and another interface on the local switch goes Down, there is a loop between the two interfaces. Remove the network cable between the interfaces after gaining the network administrator's permission.
 - If the loop exists between switches, check for incorrect cable connections between switches based on the network plan. Check the cable connection of each interface encountering a broadcast storm. If the connection between an interface and the remote switch does not conform to the network plan, remove the cable from the interface.
- If the fault persists after the preceding operations are performed, collect the following information and contact Huawei technical support personnel.
 - Results of the preceding troubleshooting procedure.
 - Configuration files, logs, and alarms of the devices.

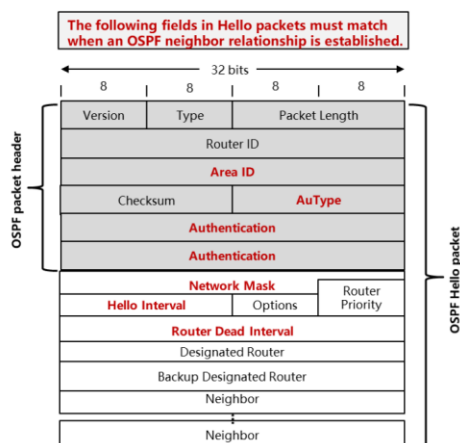


Contents

1. Basic Configuration Faults
2. LAN Faults
- 3. IP Routing Protocol Faults**
 - OSPF Faults and Troubleshooting Methods
 - IS-IS Faults and Troubleshooting Methods
 - BGP Faults and Troubleshooting Methods
4. IP Service Faults
5. Reliability Faults
6. Security Faults
7. Network Management Faults



OSPF Neighbor Relationship Faults and Troubleshooting Roadmap (1/2)

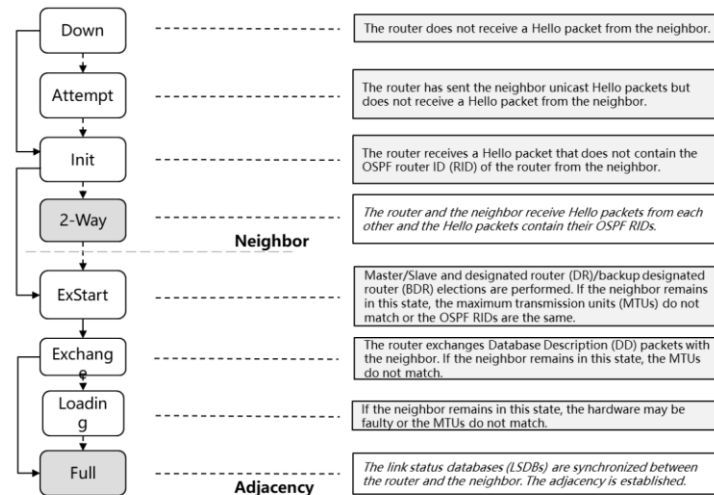


- Open Shortest Path First (OSPF) neighbor relationship faults:
 - The OSPF neighbor information table is empty.
 - The OSPF neighbor remains in Init state.
 - The OSPF neighbor remains in 2-Way state.
 - The OSPF neighbor remains in ExStart or Exchange state.

- An OSPF neighbor relationship can only be established when the values of **Area ID**, **AuType**, **Authentication**, **Network Mask**, **Hello Interval**, **Router Dead Interval**, and other options in a Hello packet are the same as those configured on the interface receiving the packet. If not, the data package is discarded and the OSPF neighbor relationship cannot be established.
- Common OSPF neighbor relationship faults are as follows:
 - The OSPF neighbor information table is empty.
 - The OSPF neighbor remains in Init state.
 - The OSPF neighbor remains in 2-Way state.
 - The OSPF neighbor remains in ExStart or Exchange state.



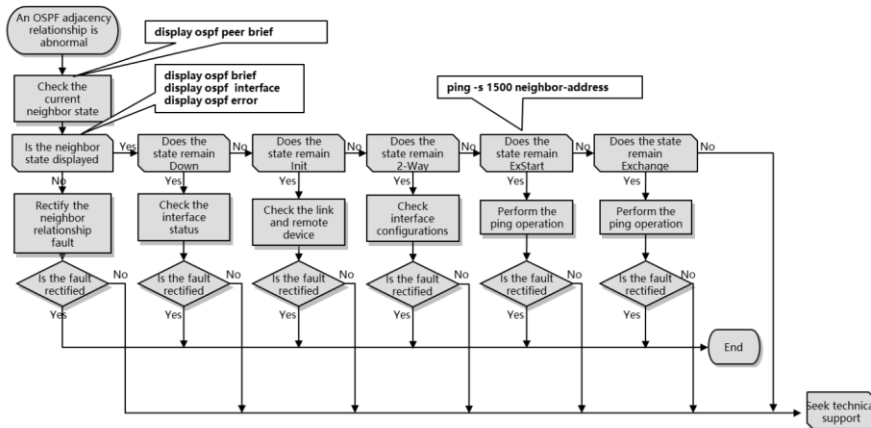
OSPF Neighbor Relationship Faults and Troubleshooting Roadmap (2/2)



- If the neighbor remains in one of the following states for a long time, a fault occurs during OSPF neighbor relationship establishment.
 - **Down:** It is the initial state of the neighbor, which indicates that the router does not receive any message from the neighbor. If the neighbor remains in this state, this indicates that the router receives no Hello packet from the neighbor.
 - **Attempt:** This state is only valid for neighbors attached to non-broadcast multiple access (NBMA) networks. It indicates that the router receives no recent information from the neighbor but has sent the neighbor Hello packets at intervals. If the router receives no Hello packet from the neighbor within a period of RouterDeadInterval seconds, the state changes to Down. If the neighbor remains in this state, the router has sent the configured neighbor unicast Hello packets but does not receive a Hello packet from the neighbor.
 - **Init:** In this state, the router has received a Hello packet from the neighbor but the router itself does not appear in neighbor list in the neighbor's Hello packet. The router has not established bidirectional communication with the neighbor. If the neighbor remains in this state, the router receives a Hello packet that does not contain the OSPF RID of the router from the neighbor.
 - **2-Way:** In this state, the router has established bidirectional communication with the neighbor. Namely, a neighbor relationship has been established. However, the adjacency has not been established. If the neighbor remains in this state, the router and the neighbor have received Hello packets from each other and the Hello packets contain their OSPF RIDs. If the router is a DR other (a router other than the DR or BDR) on an Ethernet link, the 2-Way neighbor state is acceptable.
 - **ExStart:** After the neighbor status changes to ExStart, the router starts to send the neighbor DD packets. In the ExStart state, the two nodes negotiate the master and slave relationship through DD packets and determine the initial sequence number of DD packets. The DD packets do not describe link status. If the neighbor remains in this state, the MTUs of the router and neighbor do not match or the OSPF RIDs are the same.
 - **Exchange:** In this state, the router and neighbor exchange DD packets that briefly describe link status with each other. If the neighbor remains in this state, the MTUs of the router and neighbor do not match.
 - **Loading:** In this state, the router and neighbor send link state request (LSR) packets, link state update (LSU) packets, and link state acknowledgment (LSAck) packets to each other. If the neighbor remains in this state, the hardware may be faulty or the MTUs do not match.
 - **Full:** The LSDBs are synchronized between the router and the neighbor. The adjacency is established.



OSPF Neighbor Relationship Faults - Troubleshooting Process



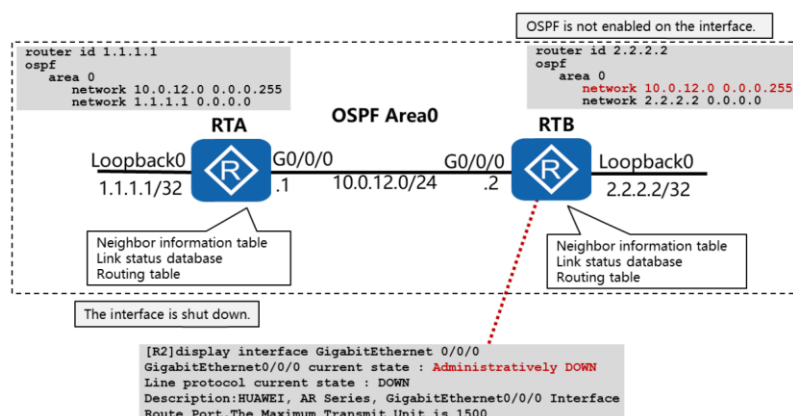
- The OSPF neighbor state cannot be displayed.
 - Run the **display interface** [*interface-type* [*interface-number*]] command to check physical status of the interfaces. Check whether the links (including the transmission device) are faulty.
 - If an interface is connected to a broadcast network or an NBMA network, check whether IP addresses of the two interfaces on both ends on the same network segment.
 - If the **ospf mtu-enable** command is executed on interfaces on both ends, MTUs of the two interfaces must be consistent. If the MTUs are inconsistent, the OSPF neighbor relationship cannot be established. Run the **mtu mtu** command in the interface view to change MTUs of the two interfaces to be consistent.
 - On broadcast and NBMA network segments, there must be at least one interface with a priority that is not 0 to ensure that the DR can be correctly elected. Otherwise, the OSPF neighbor relationship can only reach the 2-Way state. Run the **display ospf interface** command to check the interface priority.
 - Check whether OSPF configurations on the two devices are correct.
 - Run the **display ospf brief** command to check whether the OSPF router IDs of the two devices are the same. If the router IDs are the same, run the **ospf router-id router-id** command to modify the OSPF router IDs of the two devices to be different. The router ID of each device must be unique within an AS.
 - Run the **display ospf interface** command to check whether OSPF area configurations of the two devices are consistent.

- To check whether other OSPF configurations of the two devices are consistent, run the **display ospf error** command every 10 seconds for 5 minutes.
- Check the **Bad authentication type** field. If the value of this field keeps increasing, the OSPF authentication types of the two devices that establish the neighbor relationship are inconsistent. In this case, run the **area-authentication-mode** command to configure the same authentication type for the two devices.
- Check the **Hello timer mismatch** field. If the value of this field keeps increasing, the values of the Hello timers on the two devices are inconsistent. In this case, check the interface configurations of the two devices and run the **ospf timer hello** command to set the same value for the Hello timers.
- Check the **Dead timer mismatch** field. If the value of this field keeps increasing, the values of the dead timers on the two devices are inconsistent. In this case, check the interface configurations of the two devices and run the **ospf timer dead** command to set the same value for the dead timers.
- Check the **Extern option mismatch** field. If the value of this field keeps increasing, the area types of the two devices are inconsistent (the area type of one device is common area, while the area type of the other device is stub area or NSSA). In this case, configure the same area type for the two devices (in the OSPF area view, the **stub** command sets the area type to **stub** and the **nssa** command sets the area type to **nssa**).
- If the state remains Down:
 - Run the **display interface** [*interface-type* [*interface-number*]] command to check the physical status of a specified interface. If the physical status of the interface is Down, troubleshoot the interface fault.
 - If the physical status of the interface is Up, run the **display ospf interface** command to check whether the OSPF status of the interface is Up.
- If the state remains Init:
 - If the neighbor remains in Init state, this indicates that the remote device cannot receive Hello packets from the local device. In this case, check whether the link or the remote device is faulty.
- If the state remains 2-Way:
 - If the neighbor remains in 2-Way state, run the **display ospf interface** command to check whether the DR priorities configured for the OSPF-enabled interfaces are 0. If the DR priorities of the OSPF-enabled interfaces are 0 and the state is DROther, both the local device and its neighbor are not the DR or BDR and they do not need to exchange LSAs. In this case, no action is required.
- If the state remains ExStart:
 - If the neighbor remains in Exstart state, the two devices remain in DD negotiation and cannot synchronize their DDs. Two possible causes are listed as follows:
 - Oversized packets cannot be received or sent. Run the **ping -s 1500 neighbor-address** command to check oversized packet transmission. If the ping operation fails, rectify the link fault.
 - The two devices have different OSPF MTUs configured. If one OSPF interface has the **ospf mtu-enable** command configured, check whether the MTUs of the two interfaces are the same. If not, change the MTUs to be the same.
- If the state remains Exchange:
 - If the neighbor remains in Exchange state, the two devices are exchanging DD packets. Check whether the link and remote device is faulty.
- If the fault persists, collect the following information and contact senior technical support personnel.
 - Results of the preceding troubleshooting procedure.
 - Configuration files, logs, and alarms of the devices.



OSPF Intra-area Route Fault and Troubleshooting Roadmap

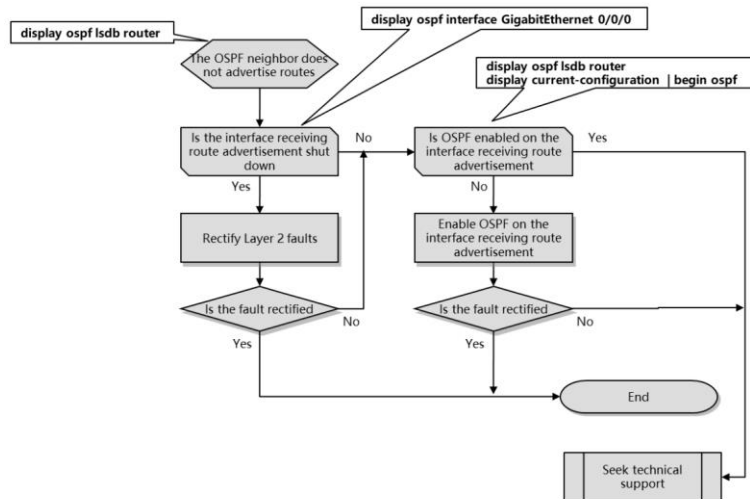
- The neighbor router does not advertise some or all routes.



- The symptom of an OSPF intra-area route fault is that the neighbor router does not advertise some or all routes. The following are two possible causes:
 - OSPF is disabled on the interface receiving route advertisement.
 - The interface receiving route advertisement is shut down.
- OSPF is an Interior Gateway Routing Protocol (IGRP) based on the link status. An LSDB exists. For a router that runs OSPF, focus on the neighbor list, LSDB (also called link status table), and routing table. If the neighbor does not advertise a route, this route cannot be displayed in the routing table and OSPF LSDB of the local router. The neighbor does not add this route to its OSPF LSDB either.



OSPF Intra-area Route Fault - Troubleshooting Process

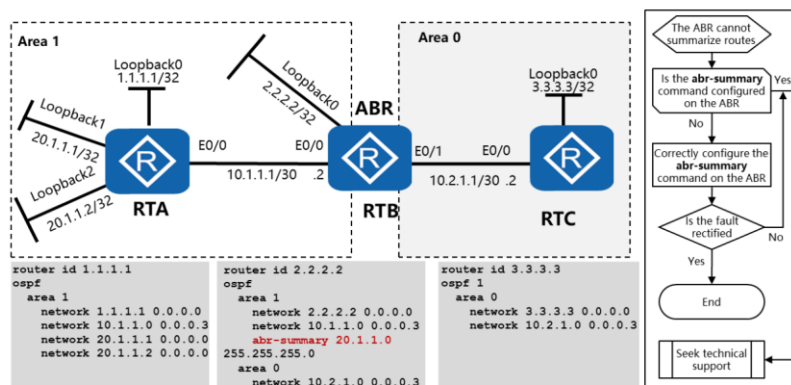


- Check whether the interface receiving route advertisement is shut down.
 - OSPF does not support advertisement of routes to disconnected interfaces. Therefore, if an interface is shut down, the route to the IP address of the interface will not be advertised to the neighbor router.
 - Run the **display ospf lsdb router** command to check whether the route exists in the LSDB.
 - The **display ospf interface GigabitEthernet 0/0/0** command output displays link protocol status.
 - Enable the interface that is shut down and rectify Layer 2 faults.
- Check whether OSPF is enabled on the interface receiving route advertisement.
 - The network to which an interface is connected is contained in the LSDB of the interface only when OSPF is enabled on the interface. If the network conditions are lost or the network configuration is incorrect, routes of the network to which the interface is connected do not exist in the LSDB.
 - Run the **display ospf lsdb router** command to check whether information about a network exists in the LSDB.
 - Run the **display current-configuration | begin ospf** command to display the OSPF configuration command. Check whether the network conditions are correctly configured.
- If the fault persists, collect the following information and contact senior technical support personnel.
 - Results of the preceding troubleshooting procedure.
 - Configuration files, logs, and alarms of the devices.



OSPF Inter-area Route Fault and Troubleshooting Process

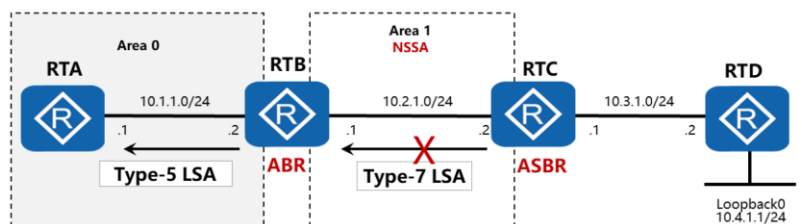
- The ABR cannot summarize routes.



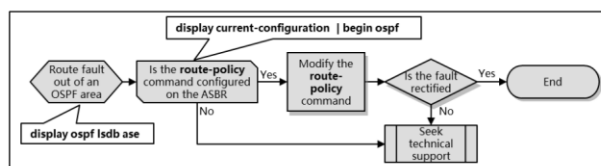
- An OSPF ABR is a router directly connected to multiple areas. An ABR maintains an LSDB for each area to which the ABR is directly connected. An ABR converts link status information (including router LSA and network LSA) for the connected non-backbone area into routing information (network summary LSA) and advertises the routing information to the backbone area. The backbone area then advertises this information to other non-backbone areas. An ABR also converts link status information for the backbone area into routing information and advertises the routing information to the connected non-backbone area.
- The symptom of an OSPF inter-area route fault is that the ABR cannot summarize routes. Run the **display current-configuration | begin ospf** command to check whether the **abr-summary** command is configured on the ABR.



Route Fault Out of an OSPF Area and Troubleshooting Process



- The autonomous system boundary router (ASBR) does not advertise re-advertised routes.



- In an NSSA area, an ASBR can import external routes and advertise the routes by means of type 7 LSAs (NSSA LSAs). ASBRs in an NSSA area can only generate and advertise type 7 LSAs (NSSA LSAs), but not type 5 LSAs (AS external LSAs). When type 7 LSAs reach the ABR in an NSSA area, the ABR converts the type 7 LSAs into type 5 LSAs and transmits them to other areas.
- The symptom of a route fault out of an OSPF area is that the ASBR does not advertise re-advertised routes. Run the **display ospf lsdb ase** command to check information on the AS external connection state database. When the **filter-policy** command is enabled on the ASBR, the OSPF cannot install external routes to the LSDB. Modify the ACL.

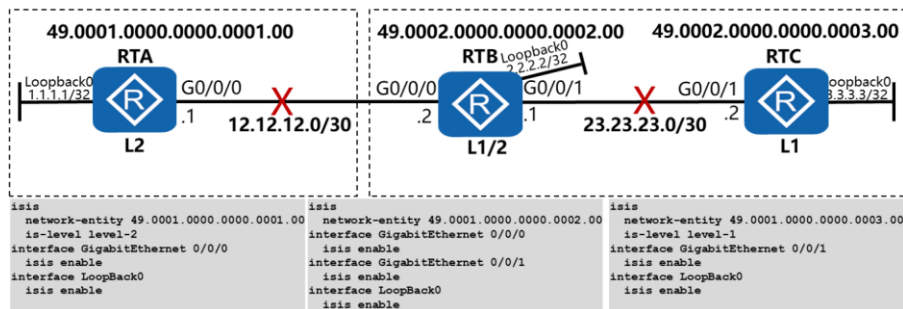


Contents

1. Basic Configuration Faults
2. LAN Faults
- 3. IP Routing Protocol Faults**
 - OSPF Faults and Troubleshooting Methods
 - IS-IS Faults and Troubleshooting Methods
 - BGP Faults and Troubleshooting Methods
4. IP Service Faults
5. Reliability Faults
6. Security Faults
7. Network Management Faults



IS-IS Neighbor Relationship Faults and Troubleshooting Roadmap

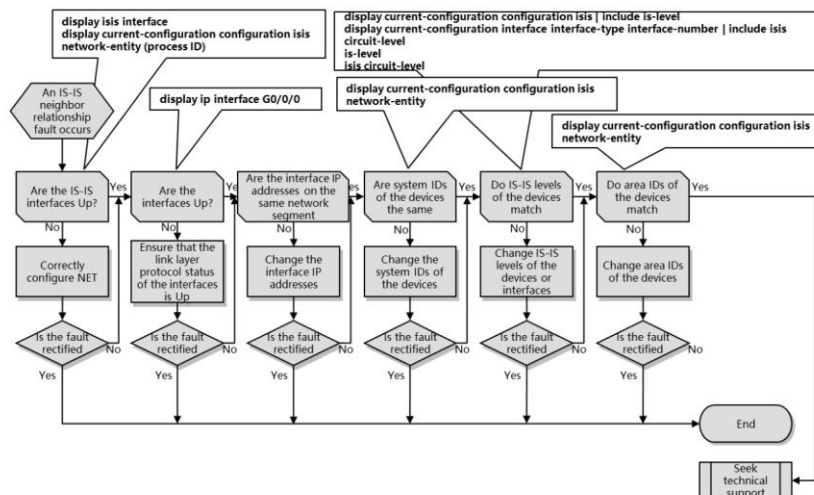


- Intermediate system to intermediate system (IS-IS) interfaces cannot normally receive and send Hello packets due to a lower-layer device fault or link fault.
 - The devices on both ends of the link have the same system ID.
 - The devices on both ends of the link have mismatching IS-IS levels.
- When a Level-1 neighbor relationship is established, the devices on both ends of the link have mismatching area IDs.
- IP addresses of the related interfaces on the two routers are on different network segments.

- The IS-IS network structure is the two-layer structure consisting of a backbone area and non-backbone areas. IS-IS routers are classified into the following levels: level-1, level-2, and level-1/2 (or L1, L2, and L1/2). An L1 router can only forward packets within an area, and establish an L1 neighbor relationship with an L1 or L1/2 router in the same area only. An L1 router cannot establish a neighbor relationship with an L1 router in another area. An L2 router can forward packets to other areas, and establish an L2 neighbor relationship with an L2 or L1/2 router in the same or another area. L1/2 routers belong to both L1 and L2. An L1/2 router can establish an L1 neighbor relationship with an L1 or L1/2 router in the same area, and can also establish an L2 neighbor relationship with an L2 or L1/2 router in the same or another area.
- The following are possible causes of IS-IS neighbor relationship faults, and here, we focus on the first five causes when troubleshooting a fault.
 - ❑ IS-IS interfaces cannot normally receive or send Hello packets due to a lower-layer device fault or link fault.
 - ❑ The devices on both ends of the link have the same system ID.
 - ❑ The devices on both ends of the link have mismatching IS-IS levels.
 - ❑ When a Level-1 neighbor relationship is established, the devices on both ends of the link have mismatching area IDs.
 - ❑ IP addresses of the related interfaces on the two routers are on different network segments.
 - ❑ The MTU is inconsistently configured for the related interfaces on the two routers, or the MTU size configured for the interfaces is smaller than the size of transmitted Hello packets.
 - ❑ IS-IS interfaces on both ends of the link use different authentication modes.



IS-IS Neighbor Relationship Faults - Troubleshooting Process



- Check the status of the IS-IS interfaces.

- Run the **display isis interface** command to check the status of the interfaces on which IS-IS is enabled. If **Down** is displayed under **IPv4.State** in the command output, run the **display current-configuration configuration isis** command to check whether NET is configured on the interfaces. If not, run the **network-entity** command.
- If the IP address is incorrectly configured for an interface, the IS-IS state of the interface is as follows:

```
[R1-Serial1/0/0]display isis interface
Interface information for ISIS(10)
```

Interface	Id	IPv4.State	IPv6.State	MTU	Type	DIS
Loop0	002	Up	Down	1500	L1/L2	--
S1/0/0	001	Mtu:Up/Lnk:Dn/IP:Dn	Down	1500	L1/L2	--

- Check whether the interfaces are Up.

- Run the **display ip interface [interface-type [interface-number]]** command to check the status of the specified interfaces. If the link layer status of the interface (the **Line protocol current state** field) is not Up, rectify the interface fault to ensure that the link layer status of the interface is Up.
- **Line protocol** configured for the Ethernet interface is not a link layer protocol, but a Layer 3 protocol. Check whether the interface is correctly configured with an IP address.

```
[R1]display ip int g0/0/0
```

```
GigabitEthernet0/0/0 current state : UP
```

```
Line protocol current state : DOWN
```

If the interfaces are wide area network interfaces, both ends of the link must use the same encapsulation mode. Otherwise, **Line protocol current state** is **Down**. For example, the link layer protocol of one end is High-Level Data Link Control (HDLC) and the protocol of the other end is Point-to-Point Protocol (PPP). Therefore, you need check whether the link layer protocols of both ends are the same and contact the communication maintenance personnel to check whether the transmission circuit is normal.

[R1-Serial1/0/0]display int se1/0/0

Serial1/0/0 current state : UP

Line protocol current state : DOWN

Description:HUAWEI, AR Series, Serial1/0/0 Interface

Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)

Internet Address is 33.1.1.1/24

Link layer protocol is nonstandard HDLC

- Check whether IP addresses of the related interfaces on the two routers are on the same network segment. (Only Ethernet links require that the IP addresses be on the same network segment. If the link connecting the interfaces is a point-to-point link, run the **[R1-Serial1/0/0]isis peer-ip-ignore** command to delete the limit.)
 - If not, modify the IP addresses to ensure that they are on the same network segment.
- Check whether the devices on both ends of the link have the same system ID.
 - Run the **display current-configuration configuration isis** command to check the system IDs of the devices. If the two devices have the same system ID, modify the configuration to ensure that the system IDs of the devices are different.
- Check whether the devices on both ends of the link have matching IS-IS levels.
 - Run the **display current-configuration configuration isis | include is-level** command to check the level configurations of IS-IS processes on both ends. Run the **display current-configuration interface *interface-type interface-number* | include isis circuit-level** command to check the IS-IS level configuration of the specified interfaces. An IS-IS neighbor relationship can be established only when IS-IS interfaces on both ends of the link have the matching IS-IS levels.
 - If the IS-IS levels of both ends do not match, run the **is-level** command in the IS-IS view to change the IS-IS level of devices, or run the **isis circuit-level** command in the interface view to change the interface IS-IS level.
 - In interface configuration mode, run the **display this** command to check the network types of the IS-IS interfaces on both ends of the link are the same.

```
interface GigabitEthernet0/0/1
ip address 10.1.1.2 255.255.255.0
isis enable 10
isis circuit-type p2p
```
- Check whether the devices on both ends of the link have matching area IDs.
 - If an IS-IS Level-1 neighbor relationship needs to be established between two devices on both ends of a link, ensure that the two devices reside in the same area. If an IS-IS Level-2 neighbor relationship needs to be established, area IDs of the devices do not need to be the same.
 - If the devices on both ends of the link have different area IDs, run the **network-entity** command in the IS-IS view to modify the area IDs of the devices.
- If the fault persists, collect the following information and contact senior technical support personnel.
 - Results of the preceding troubleshooting procedure.
 - Configuration files, logs, and alarms of the devices.

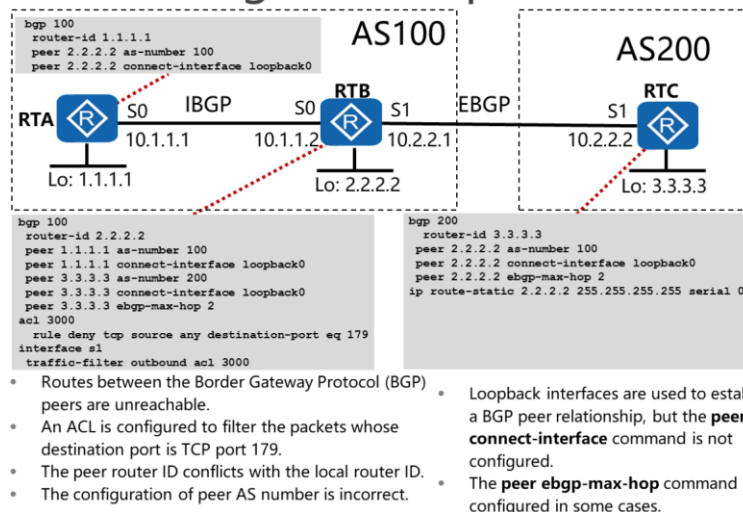


Contents

1. Basic Configuration Faults
2. LAN Faults
- 3. IP Routing Protocol Faults**
 - OSPF Faults and Troubleshooting Methods
 - IS-IS Faults and Troubleshooting Methods
 - BGP Faults and Troubleshooting Methods
4. IP Service Faults
5. Reliability Faults
6. Security Faults
7. Network Management Faults



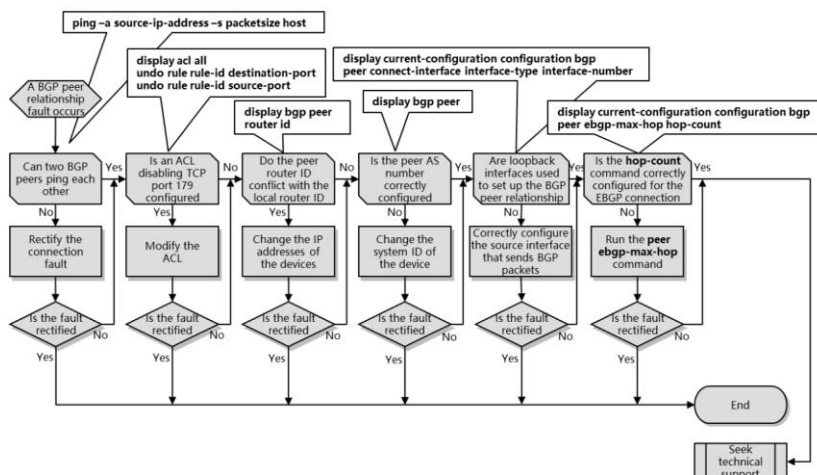
BGP Peer Relationship Faults and Troubleshooting Roadmap



- The Border Gateway Protocol (BGP) protocols are classified into External/Exterior BGP (EBGP) and Internal/Interior BGP (IBGP) based on running modes. BGP is called EBGP when it runs between ASs. To avoid loops between ASs, a BGP router discards routes with the local AS number received from EBGP peers. BGP is called IBGP when it runs within an AS. To avoid loops within an AS, a BGP router does not advertise the routes it learns from an IBGP peer to other IBGP peers and fully connects to all IBGP peers. If the BGP peer relationship cannot enter the Established state, it indicates that the BGP peer relationship fails to be established.
- Possible causes of a BGP peer relationship fault are as follows:
 - BGP packets cannot be forwarded.
 - An ACL is configured to filter the packets whose destination port is TCP port 179.
 - The peer router ID conflicts with the local router ID.
 - The configured peer AS number is incorrect.
 - Loopback interfaces are used to establish a BGP peer relationship, but the **peer connect-interface** command is not configured.
 - Loopback interfaces are used to establish an EBGP peer relationship, but the **peer ebgp-max-hop** command is not configured.
 - The number of routes sent by the remote router exceeds the maximum limit configured using the **peer route-limit** command.
 - The **peer ignore** command is configured on the peer router.
 - Address families of devices on both ends do not match.
- The last three causes are not common. Here, we focus on the first six causes when troubleshooting a BGP peer relationship fault.



BGP Peer Relationship Faults - Troubleshooting Process



- Run the **ping** command to check whether the two devices that need to establish a BGP peer relationship can ping each other.
 - Run the **ping -a source-ip-address -s packetsize host** command to detect connectivity of the devices on both ends. Because the source address is specified in this command, you can check whether routes between the two devices are accessible. By specifying the size of a Ping packet, you can check whether large Ping packets can be normally transmitted over the link.
 - If they can ping each other successfully, there are accessible routes between the BGP peers and that the link transmission is normal.
- Check whether an ACL is configured to filter the packets whose destination port is TCP port 179.
 - Run the **display acl all** command on the two devices to check whether an ACL is configured to disable TCP port 179. If yes, run the **undo rule rule-id destination-port** and **undo rule rule-id source-port** commands to cancel the configuration.
- Check whether the peer router ID conflicts with the local router ID.
 - View information about the BGP peer on each device. Run the **display bgp peer** command to check whether the peer router ID conflicts with the local router ID.
 - If the peer router ID conflicts with the local router ID, run the **router id** command in the BGP view to change the two router IDs to be different. A loopback interface address is often used as the local router ID.
- Check whether the peer AS number is correctly configured.
 - Run the **display bgp peer** command on each device to check whether the displayed peer AS number is the same as the remote AS number. If the peer AS number is configured incorrectly, change it to be the same as the remote AS number.

- If Loopback interfaces are used to establish the BGP peer relationship, check whether the **peer connect-interface** command is configured.
 - Run the **display current-configuration configuration bgp** command to check the BGP configurations. If two devices use loopback interfaces to establish the BGP peer relationship, run the **peer connect-interface *interface-type interface-number*** command to specify the associated loopback interface as the source interface that sends BGP packets.
- If two directly connected devices use loopback interfaces to establish an EBGP peer relationship or two indirectly connected devices establish an EBGP peer relationship, run the **peer ebgp-max-hop *hop-count*** command to specify the maximum hop count between the two devices. Run the **display current-configuration configuration bgp** command to check the BGP configurations.
 - If two directly connected devices use loopback interfaces to establish an EBGP peer relationship, **hop-count** must be larger than 1.
 - If two indirectly connected devices establish an EBGP peer relationship, **hop-count** must be specified to the actual hop count.
- If the fault persists, collect the following information and contact senior technical support personnel.
 - Results of the preceding troubleshooting procedure.
 - Configuration files, logs, and alarms of the devices.

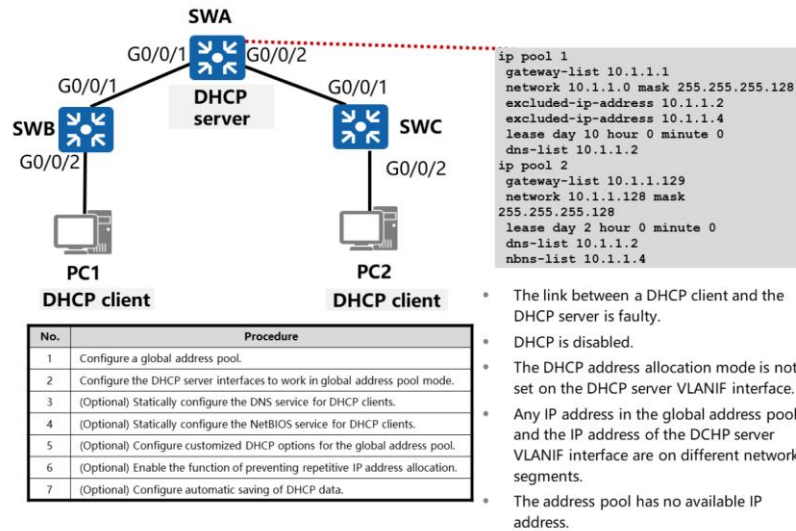


Contents

1. Basic Configuration Faults
2. LAN Faults
3. IP Routing Protocol Faults
- 4. IP Service Faults**
 - DHCP Server Faults
 - DHCP Relay Faults
5. Reliability Faults
6. Security Faults
7. Network Management Faults



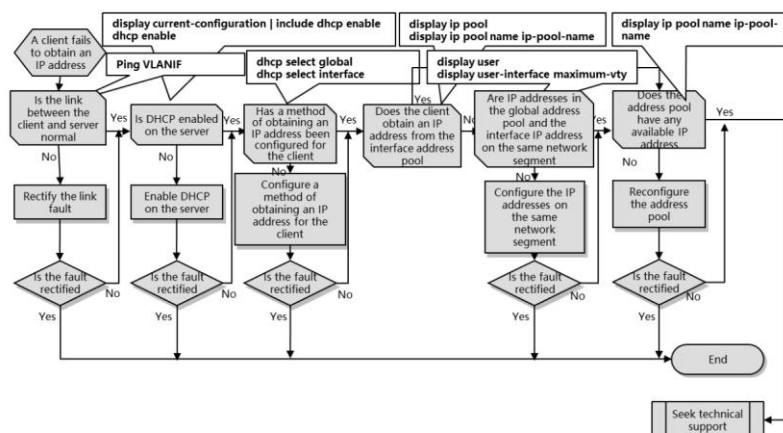
DHCP Server Faults



- As the network expands and becomes complex, the number of hosts often exceeds the number of available IP addresses. As portable computers and wireless networks are widely used, the positions of computers often change, causing IP addresses of the computers to be changed accordingly. As a result, network configurations become increasingly complex. To properly and dynamically assign IP addresses to hosts, Dynamic Host Configuration Protocol (DHCP) is used.
- DHCP is used to dynamically assign IP addresses for users and centrally manage user configurations. DHCP uses the client/server model. The client applies to the server for configurations, such as the IP address, subnet mask, and default gateway. The server replies with configurations. DHCP rapidly and dynamically allocates IP addresses, which improves IP address usage.
- Common causes of DHCP faults are as follows:
 - The link between a DHCP client and the DHCP server is faulty.
 - DHCP is disabled.
 - The DHCP address allocation mode is not set on the DHCP server VLANIF interface.
 - When IP addresses are allocated from the global address pool:
 - If the client and server are located on the same network segment and no relay agent is deployed, any IP address in the global address pool and the IP address of the DHCP server VLANIF interface are on different network segments.
 - If the client and server are located on different network segments and a relay agent is deployed, any IP address in the global address pool and the IP address of the relay agent VLANIF interface are on different network segments.
 - The address pool has no available IP address.



DHCP Server Faults - Troubleshooting Process



- Check whether the link between the client and the DHCP server is faulty.
 - If the client and server are on the same network segment and no relay agent is deployed, configure an IP address for the network adapter between the client and the server. Ensure that the IP address of the network adapter and the IP address of the user-side VLANIF interface on the server are on the same network segment. Ping the VLANIF interface IP address from the client. If the ping operation fails, rectify the link fault.
 - If the client and server are on different network segments and a relay agent is deployed, ping the links between the client and the relay agent and between the relay agent and the server. If the ping operations fail, rectify the faults on the links.
- Check whether DHCP is enabled.
 - Run the **display current-configuration | include dhcp enable** command to check whether DHCP is enabled. If no DHCP information is displayed, DHCP is disabled. Run the **dhcp enable** command to enable DHCP. By default, DHCP is disabled.
- Check whether the DHCP address allocation mode is set on the DHCP server VLANIF interface.
 - If the DHCP address allocation mode is not set on the DHCP server VLANIF interface, the client cannot obtain an IP address in DHCP mode using the VLANIF interface.
 - Run the **display this** command in the VLANIF interface view to check whether the DHCP address allocation mode is set.
 - If **dhcp select global** is displayed, the VLANIF interface uses the global address pool to allocate IP addresses.
 - If **dhcp select interface** is displayed, the VLANIF interface uses the interface address pool to allocate IP addresses.

- If neither of the preceding information is displayed, the DHCP address allocation mode is not set on the VLANIF interface. Run the **dhcp select global** or **dhcp select interface** command to set a DHCP address allocation mode for the VLANIF interface.
- Check whether IP addresses in the global address pool and the VLANIF interface IP address are on the same network segment.
 - Run the **display ip pool** command to check whether a global address pool has been created.
 - If not, run the **ip pool** *ip-pool-name* and **network** *ip-address* [**mask** { *mask* | *mask-length* }] commands to create a global address pool and set the range of IP addresses that can be dynamically allocated.
 - If yes, obtain the value of *ip-pool-name*, and then go to next step.
 - Run the **display ip pool name** *ip-pool-name* command to check the IP addresses in the global address pool are on the same network segment as the VLANIF interface IP address.
 - The client and server are on the same network segment and no relay agent is deployed. If the IP addresses in the global address pool and the IP address of the VLANIF interface are on different network segments, run the **ip address** *ip-address* command to change the IP addresses of the VLANIF interface. Ensure that the interface IP address and IP addresses in the global address pool are on the same network segment.
 - The client and server are on different network segments and a relay agent is deployed. If the IP addresses in the global address pool and the IP address of the VLANIF interface on the relay agent are on different network segments, run the **ip address** *ip-address* command to change the IP address of the VLANIF interface. Ensure that the interface IP address and IP addresses in the global address pool are on the same network segment.
- Check whether the address pool has available IP addresses.
 - Run the **display ip pool name** *ip-pool-name* command to check whether there are available IP addresses in the global or interface address pool.
 - If the value of **Idle (Expired)** is 0, all IP addresses in the IP address pool are used.
 - If the DHCP server allocates IP addresses to clients from the global address pool through the VLANIF interface, re-create a global address pool where the network segment can be connected to the previous network segment but cannot overlap with the previous network segment.
 - If the DHCP server allocates IP addresses to clients from the interface address pool using the VLANIF interface, reconfigure an IP address for the VLANIF interface. This IP address and the previous IP address must be on different network segments.
- If the fault persists after the preceding operations are performed, collect the following information and contact Huawei technical support personnel.
 - Results of the preceding troubleshooting procedure.
 - Configuration files, logs, and alarms of the devices.

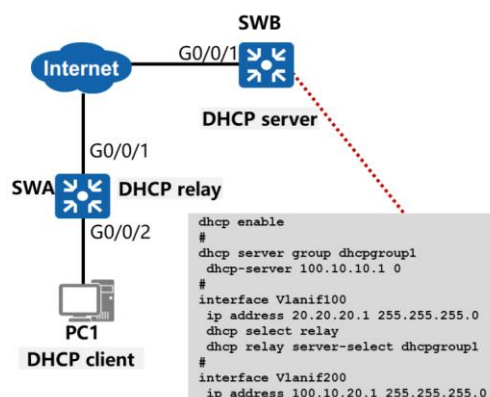


Contents

1. Basic Configuration Faults
2. LAN Faults
3. IP Routing Protocol Faults
- 4. IP Service Faults**
 - DHCP Server Faults
 - DHCP Relay Faults
5. Reliability Faults
6. Security Faults
7. Network Management Faults



DHCP Relay Faults



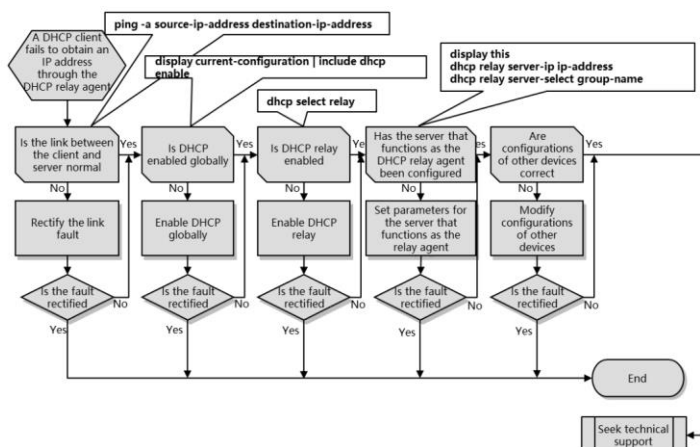
No.	Procedure
1	Configure DHCP relay on an interface.
2	Configure a destination DHCP server group.
3	Bind an interface on the DHCP relay agent to the DHCP server group.
4	(Optional) Configure the DHCP relay agent to send DHCP release message.
5	(Optional) Configure an Option82 message processing policy for the DHCP relay agent.

- The link between a DHCP client and the DHCP server is faulty.
- DHCP is not enabled globally. As a result, the DHCP function does not take effect.
- The DHCP relay function is disabled. As a result, the DHCP relay function does not take effect.
- The DHCP server IP address is not configured on the DHCP relay agent.
- Configurations of other devices along the link are incorrect.

- When a switch functions as a DHCP relay agent, a client can communicate with the DHCP server on another network segment through the relay agent, and obtain an IP address and other configuration parameters from the global address pool on the DHCP server. In this manner, DHCP clients on multiple network segments can share one DHCP server. This reduces costs and facilitates centralized management.
- Common causes of DHCP relay faults are as follows:
 - The link between a DHCP client and the DHCP server is faulty.
 - The link between a client and the DHCP relay agent is faulty.
 - The link between the DHCP relay agent and the DHCP server is faulty.
 - DHCP is not enabled globally. As a result, the DHCP function does not take effect.
 - The DHCP relay function is not enabled globally. As a result, the DHCP relay function does not take effect.
 - The DHCP relay agent is not bound to the DHCP server.
 - The DHCP server IP address is not configured on the DHCP relay agent.
 - The VLANIF interface on the DHCP relay agent is not bound to a DHCP server group or the DHCP server is not in the bound DHCP server group.
 - The configuration of the other devices on the link is faulty.



DHCP Relay Faults - Troubleshooting Process



- Check whether the link between the client and the DHCP server is faulty.
 - Check whether the link between the client and the DHCP relay agent is faulty. Set an idle IP address for the DHCP client. The IP address must be on the same network segment with the IP address of the user-side VLANIF interface on the DHCP relay agent. Ping the IP addresses from either side to check whether the link is normal. If the ping operation fails, rectify the link fault.
 - Check whether the link between the DHCP relay agent and the DHCP server is faulty. Run the **ping -a source-ip-address destination-ip-address** command on the DHCP relay agent. *source-ip-address* indicates the IP address of the user-side interface on the DHCP relay agent, and *destination-ip-address* indicates the IP address of the DHCP server. If the ping operation fails, rectify the link fault.
- Check whether DHCP is globally enabled on the DHCP relay agent.
 - Run the **display current-configuration | include dhcp enable** command to check whether DHCP is enabled. If no information about DHCP is displayed, DHCP is disabled. Run the **dhcp enable** command to enable DHCP. By default, DHCP is disabled.
- Check whether the DHCP relay function is enabled.
 - If the DHCP relay function is disabled, DHCP clients cannot obtain IP addresses from the DHCP server on a different network segment.
 - If the address allocation mode (global/interface) and relay are configured on the switch simultaneously, the switch preferentially functions as the DHCP server. When the DHCP server fails to allocate IP addresses, the switch functions as the DHCP relay agent.
 - Run the **display this** command in the VLANIF interface view to check whether the DHCP relay function is enabled. If **dhcp select relay** is displayed, the DHCP relay function is enabled. If the preceding information is not displayed,

- the DHCP relay function is disabled. Run the **dhcp select relay** command to enable the DHCP relay function.
- Check whether the DHCP relay agent is bound to the DHCP server.
 - If not, no DHCP server can allocate IP addresses for the clients connected to the DHCP relay agent.
 - Run the **display this** command in the VLANIF interface view to check whether the DHCP relay agent is bound to the DHCP server.
 - If **dhcp relay server-ip ip-address** is displayed, the DHCP relay agent has been bound to the DHCP server.
 - If **dhcp relay server-select group-name** is displayed, the VLANIF interface on the DHCP relay agent has been bound to a DHCP server group.
 - If neither of the preceding information is displayed, the DHCP relay agent is not bound to the DHCP server. Configure the DHCP server using one of the following methods:
 - 1) Run the **dhcp relay server-ip ip-address** command to configure the IP address of the DHCP server on the DHCP relay agent.
 - 2) Run the **dhcp relay server-select group-name** command to bind the DHCP relay agent to the DHCP server group that contains the DHCP server.
 - 3) Run the **dhcp-server** command to add the DHCP server to the DHCP server group that is bound to the DHCP relay agent.
- Check whether the DHCP server is configured in the DHCP server group that is bound to the VLANIF interface on the DHCP relay agent.
 - If the VLANIF interface on the DHCP relay agent is bound to a DHCP server group but the DHCP server is not configured in the DHCP server group, no DHCP server can allocate IP addresses for the clients connected to the DHCP relay agent.
 - Run the **display dhcp server group group-name** command to check whether the DHCP server is configured in the DHCP server group.
 - If the **Server-IP** field is displayed in the command output, the DHCP server is configured in the DHCP server group.
 - If the preceding field is not displayed, the DHCP server is not configured in the DHCP server group. Run the **dhcp-server** command to add the DHCP server to the DHCP server group.
- Check whether the configurations of other devices along the link between the DHCP client and the DHCP server are correct. The devices include the DHCP server, digital subscriber line access multiplexers (DSLAMs), LAN switches, and the client. If not, modify the configurations.
- If the fault persists after the preceding operations are performed, collect the following information and contact Huawei technical support personnel.
 - Results of the preceding troubleshooting procedure.
 - Configuration files, logs, and alarms of the devices.

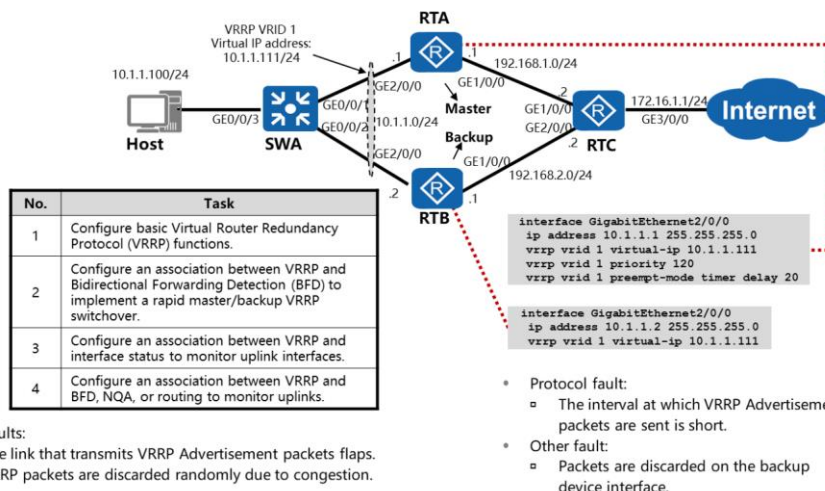


Contents

1. Basic Configuration Faults
2. LAN Faults
3. IP Routing Protocol Faults
4. IP Service Faults
- 5. Reliability Faults**
 - VRRP Backup Group Flapping
 - Two Master Devices Existing in a VRRP Backup Group
6. Security Faults
7. Network Management Faults



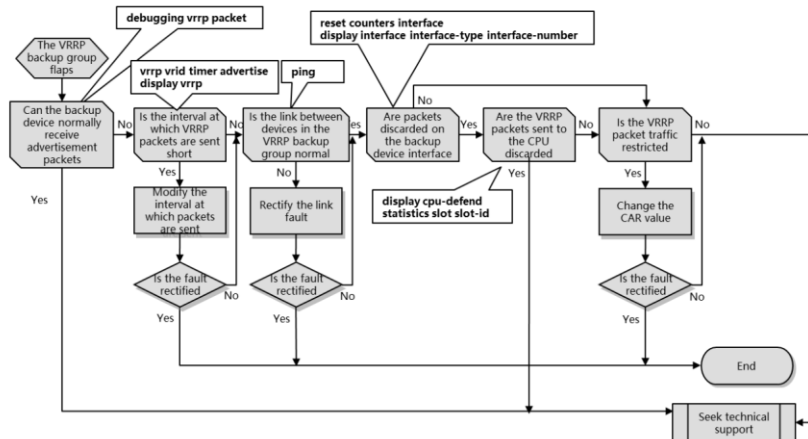
VRRP Backup Group Flapping



- Virtual Router Redundancy Protocol (VRRP) integrates multiple routing devices to a virtual router without changing the networking. The IP address of the virtual router is configured as the default gateway IP address to implement default gateway backup. When the gateway fails, VRRP can select a new gateway to transmit data traffic, ensuring network reliability.
- Common causes of VRRP backup group flapping are as follows:
 - The link that transmits VRRP Advertisement packets flaps.
 - The interval at which VRRP Advertisement packets are sent is short.
 - Packets are discarded on the backup device interface.
 - VRRP packets are discarded randomly due to congestion.



VRRP Backup Group Flapping - Troubleshooting Process



- Check whether the backup device has received VRRP Advertisement packets.
 - Run the **debugging vrrp packet** command on the backup device to check whether the device has received VRRP Advertisement packets.
 - By default, the master device sends one Advertisement packet every second.
- Check whether the interval at which VRRP Advertisement packets are sent is short.
 - Run the **vrrp vrid timer advertise** command to increase the interval at which VRRP packets are sent. Then run the **display vrrp** command on the backup device multiple times and check the **State** field. If the value keeps the same, the backup device runs stably.
 - If the backup device runs stably, the backup device status flapped may because the interval at which VRRP Advertisement packets are sent is short.
 - If the backup device runs unstably, restore the interval.
- Check whether the link between devices in the VRRP backup group is faulty.
 - Run the **ping** command multiple times to check whether the physical IP addresses in the same VRRP backup group can ping each other.
 - If the ping operation fails, rectify the link fault.
 - If some IP addresses can be pinged and some cannot, a loop may occur. Detect the loop and remove it.
- Check whether packets are discarded on the backup device interface.

- Run the **display interface** *interface-type interface-number* command and check the **Discard** fields in **Input** and **Output** to determine whether packets are discarded on the interface.
- Before running the **display interface** command, run the **reset counters interface** command to clear the statistics on the interface.
- Check whether the VRRP packets sent to the CPU are discarded.
 - Run the **display cpu-defend statistics slot** *slot-id* command to check whether the VRRP packets sent to the CPU are discarded.
 - If the value of **Drop (Packets)** is not 0, the VRRP packets sent to the CPU are discarded.
 - If the value of **Drop (Packets)** is 0, the VRRP packets sent to the CPU are not discarded.
- Check whether a threshold for the rate at which VRRP packets are transmitted is configured.
- If the fault persists after the preceding operations are performed, collect the following information and contact Huawei technical support personnel.
 - Results of the preceding troubleshooting procedure.
 - Configuration files, logs, and alarms of the devices.

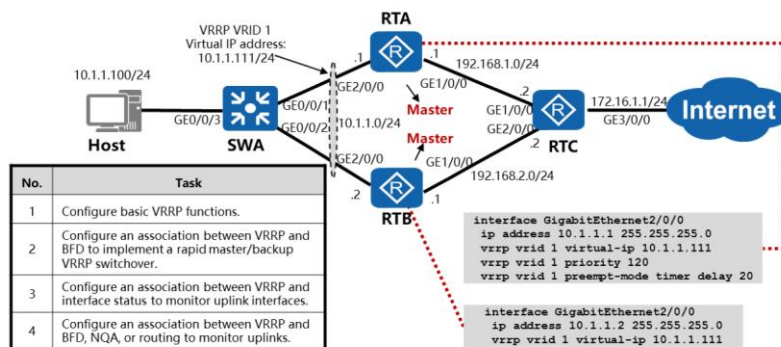


Contents

1. Basic Configuration Faults
2. LAN Faults
3. IP Routing Protocol Faults
4. IP Service Faults
- 5. Reliability Faults**
 - VRRP Backup Group Flapping
 - Two Master Devices Existing in a VRRP Backup Group
6. Security Faults
7. Network Management Faults



Two Master Devices Existing in a VRRP Backup Group

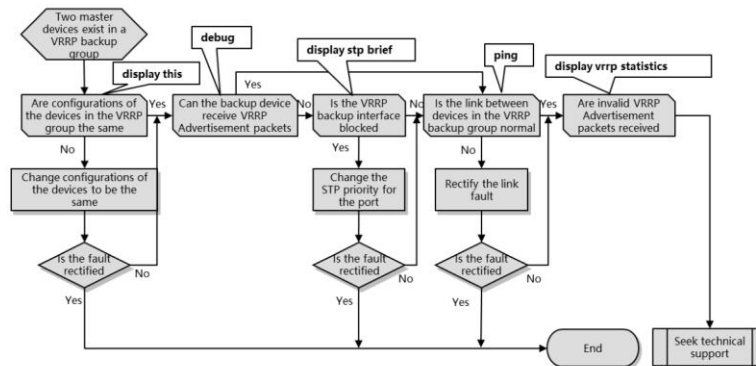


- Link faults:
 - The link that transmits VRRP Advertisement packets is faulty.
 - A loop occurs on the link.
- Configuration fault:
 - The VRRP backup group configurations of the devices are different.
- Protocol fault:
 - The VRRP Advertisement packets received by the VRRP backup group with a lower priority are taken as invalid packets and are discarded.

- A VRRP backup group consisting of two devices (one is the master device and the other is the backup device) is equivalent to a virtual gateway. This virtual gateway obtains a virtual IP address and a virtual MAC address. Hosts only monitor the presence of the virtual gateway and communicate with devices on other network segments through the virtual gateway. Normally, traffic from users is forwarded by the master device. If the master device fails, the backup device is elected as the new master through VRRP negotiation and takes over the traffic forwarding task.
- Common causes of two master devices existing in a VRRP backup group are as follows:
 - The configurations of the devices in the VRRP backup group are different.
 - The link that transmits VRRP Advertisement packets is faulty.
 - A loop occurs on the link.
 - The VRRP Advertisement packets received by the VRRP backup group with a lower priority are taken as invalid packets and are discarded.



Two Master Devices Existing in a VRRP Backup Group - Troubleshooting Process



- Check whether the configurations of the devices in the VRRP group are the same.
 - Run the **display this** command on VLANIF interfaces of the devices to check the following configurations:
 - **ip address**: to check whether the IP addresses of the interfaces are on the same network segment. If not, run the **ip address** command to modify them to ensure that they are on the same network segment.
 - **vrid**: to check whether the VRRP backup group IDs on the interfaces are the same. If not, run the **vrrp vrid virtual-router-id virtual-ip virtual-address** command to change the VRRP backup group IDs to be the same.
 - **Virtual IP**: to check whether the virtual IP addresses on the interfaces are the same. If not, run the **vrrp vrid virtual-router-id virtual-ip virtual-address** command to change the virtual IP addresses to be the same.
 - **TimerRun**: to check whether the interfaces are configured with the same interval for sending VRRP Advertisement packets. If not, run the **vrrp vrid virtual-router-id timer advertise adver-interval** command to change the intervals to be the same.
 - **Auth Type**: to check whether VRRP packet authentication modes on the interfaces are the same. If not, run the **vrrp vrid virtual-router-id authentication-mode { simple key | md5 md5-key }** command to change the authentication modes to be the same.
- Check whether the backup device can receive VRRP Advertisement packets.

- Enable debugging of the backup device and check whether the following information is displayed:
 - *Aug 27 19:45:04 2010 Quidway VRRP/7/DebugPacket:
 - Vlanif45 | Virtual Router 45:receiving from 45.1.1.4, priority = 100,timer = 1,
 - auth type is no, SysUptime: (0,121496722)
 - By default, the master device sends one Advertisement packet every second.
- Check whether any interface on the devices in the VRRP group and devices on the transmission path of VRRP Advertisement packets is blocked.
 - Run the **display stp brief** command and check the **STP State** field.
 - If the value of the **STP State** field is **FORWARDING**, the corresponding interface is not blocked.
 - If the value of the **STP State** field is **DISCARDING**, the corresponding interface is blocked. Change the STP priority of the interface so that the interconnected interfaces can properly forward VRRP packets.
- Run the **ping** command to check whether the link between devices in the VRRP backup group is faulty.
 - If the ping operation fails, rectify the link fault.
- Check whether the VRRP backup group with a lower priority receives invalid VRRP Advertisement packets.
 - Run the **display vrrp statistics** command and check the **Received invalid type packets** field. Record the collected information.
- If the fault persists after the preceding operations are performed, collect the following information and contact Huawei technical support personnel.
 - Results of the preceding troubleshooting procedure.
 - Configuration files, logs, and alarms of the devices.

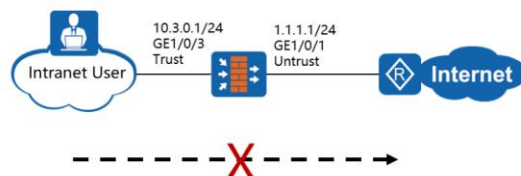


Contents

1. Basic Configuration Faults
2. LAN Faults
3. IP Routing Protocol Faults
4. IP Service Faults
5. Reliability Faults
- 6. Security Faults**
 - Intranet Users Cannot Access the Internet
 - Internet Users Cannot Access the Intranet
7. Network Management Faults



Intranet Users Cannot Access the Internet

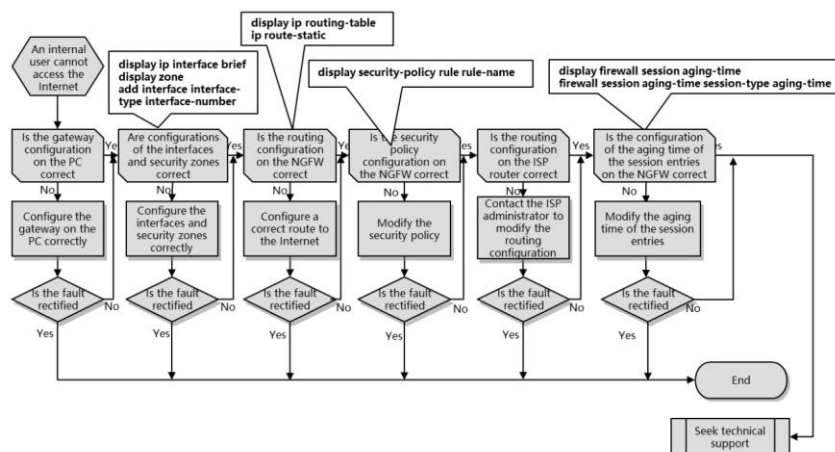


- The gateway configuration on the PC used by the intranet user is incorrect.
- Configurations of interfaces and security zone on the NGFW are incorrect.
- The routing configuration on the NGFW is incorrect.
- The security policy configuration on the NGFW is incorrect.
- The routing configuration on the ISP router is incorrect.
- The configuration of the aging time of session entries on the NGFW is incorrect.

- A Next-Generation Firewall (NGFW) can function as an egress gateway at the border of an enterprise network. The NGFW provides network address translation (NAT) to allow the enterprise intranet users to access the Internet. After configurations, an enterprise intranet user cannot access the Internet. Possible causes are as follows:
 - The gateway configuration on the PC used by the intranet user is incorrect.
 - Configurations of interfaces and security zone on the NGFW are incorrect.
 - The routing configuration on the NGFW is incorrect.
 - The security policy configuration on the NGFW is incorrect.
 - The routing configuration on the ISP router is incorrect.
 - The configuration of the aging time of session entries on the NGFW is incorrect.



Intranet Users Cannot Access the Internet - Troubleshooting Process



- Check whether the gateway of the PC is set to the IP address of the interface on the NGFW connecting to the enterprise intranet.
- Check whether the interfaces on the NGFW connecting to the intranet and Internet are configured with correct IP addresses and added to security zones.
 - Run the **display ip interface brief** command in the CLI of the NGFW to check whether correct IP addresses are configured on the interfaces.
 - Check the **IP Address** column. If the IP address of an interface is incorrect, run the **ip address ip-address mask** command to reconfigure an IP address for the interface.
 - Run the **display zone** command to check whether the interfaces are added to correct security zones.
 - If any interface is added to an incorrect security zone, run the **add interface interface-type interface-number** command in the security zone interface to add the interface to the correct security zone.
- Check whether the NGFW has a route to the Internet.
 - Run the **display ip routing-table** command to check the routing entries in the CLI of the NGFW.
 - If the configuration is incorrect, run the **ip route-static** command to reconfigure a route.
- Check whether the security policy configured on the NGFW and configuration files referenced by the security policy are correct.

- Run the **display security-policy rule** *rule-name* command on the CLI of the NGFW to check the security policy configurations.
 - Check whether the security policy conditions correctly match user traffic, and check whether the action is permit. If the configurations are incorrect, run the **source-address** command in the security policy rule view to change the source IP address associated with the security policy, or run the **action** command to change the action of the security policy rules.
 - If the content security configuration file is referenced by the security policy, run the **display profile type** { **app-control** | **av** | **data-filter** | **file-block** | **ips** | **mail-filter** | **url-filter** } **name** *name* command to check configurations in the content security configuration file. Check whether the traffic sent by users is blocked. If yes, modify configurations of the security configuration file.
- Contact the ISP network administrator to check whether a route to the NGFW is configured on the ISP router. If not, contact the ISP network administrator to modify the routing configuration.
- Check whether the configuration of the aging time of session entries on the NGFW is correct.
 - A user accesses an Internet server when using a service, the user and the server exchange packets to prevent disconnection due to no data transmission. Run the **display firewall session aging-time** command in the CLI of the NGFW to check the aging time of the session table. If the aging time of the protocol that carries the service is shorter than the interval at which the server sends response packets, the session table is aged out before a response packet reaches to the NGFW. As a result, the response packets sent by the server do not belong to any session and are discarded.
 - Run the **firewall session aging-time** *session-type aging-time* command in the CLI of the NGFW to increase the aging time of the related protocol.
- If the fault persists after the preceding operations are performed, collect the following information and contact Huawei technical support personnel.
 - Results of the preceding troubleshooting procedure.
 - Configuration files, logs, and alarms of the devices.

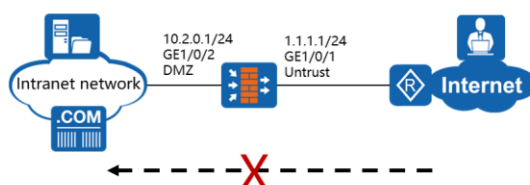


Contents

1. Basic Configuration Faults
2. LAN Faults
3. IP Routing Protocol Faults
4. IP Service Faults
5. Reliability Faults
- 6. Security Faults**
 - Intranet Users Cannot Access the Internet
 - Internet Users Cannot Access the Intranet
7. Network Management Faults



Internet Users Cannot Access the Intranet

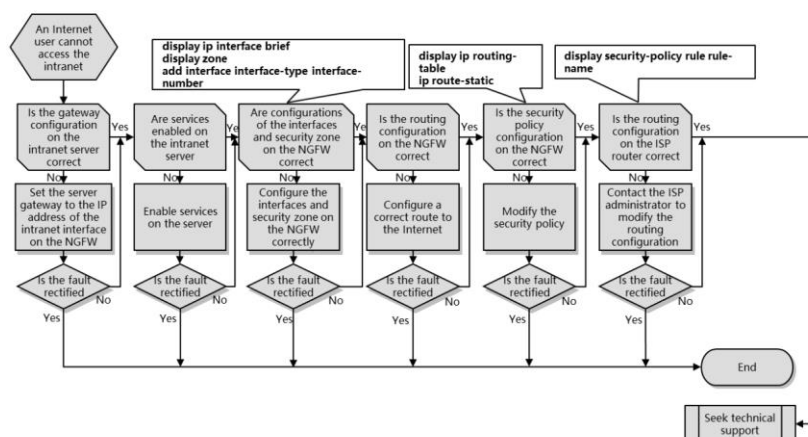


- The gateway configuration on the intranet server is incorrect.
- Services are disabled on the intranet server.
- Configurations of interfaces and security zone on the NGFW are incorrect.
- The routing configuration on the NGFW is incorrect.
- The security policy configuration on the NGFW is incorrect.
- The ISP router discards packets.

- Possible causes of an enterprise intranet user's failure in accessing the Internet are as follows:
 - The gateway configuration on the intranet server is incorrect.
 - Services are disabled on the intranet server.
 - Configurations of interfaces and security zone on the NGFW are incorrect.
 - The routing configuration on the NGFW is incorrect.
 - The security policy configuration on the NGFW is incorrect.
 - The ISP router discards packets.



Internet Users Cannot Access the Intranet - Troubleshooting Process



- Check whether the gateway of the intranet server is set to the IP address of the interface on the NGFW connecting to the enterprise intranet.
- Check whether services are enabled on the intranet server.
- Check whether the interfaces on the NGFW connecting to the intranet and Internet are configured with correct IP addresses and added to security zones.
 - Run the **display ip interface brief** command in the CLI of the NGFW to check whether correct IP addresses are configured on the interfaces. If the IP address of an interface is incorrect, run the **ip address ip-address mask** command in the interface view to reconfigure an IP address for the interface.
 - Run the **display zone** command to check whether the interfaces are added to correct security zones. If any interface is added to an incorrect security zone, run the **add interface interface-type interface-number** command in the security zone interface view to add the interface to the correct security zone.
- Check the routing configuration on the NGFW.
 - Run the **display ip routing-table** command to check the routing entries in the CLI of the NGFW. If the configuration is incorrect, run the **ip route-static** command to reconfigure a route.
- Check whether the security policy configured on the NGFW and configuration files referenced by the security policy are correct.
 - Run the **display security-policy rule rule-name** command on the CLI of the NGFW to check the security policy configurations.
 - Check whether the security policy conditions correctly match the traffic of the Internet user's access to the intranet server. The destination IP address must be the private network address of the intranet server. Check whether the action is permit. If the configurations are incorrect, run the **source-address** command in the security policy rule view to change the source IP address associated with the security policy, or run the **action** command to change the action of the security policy rules.
 - If the content security configuration file is referenced by the security policy, run the **display profile type { app-control | av | data-filter | file-block | ips | mail-filter | url-filter } name name** command to check configurations in the content security configuration file. Check whether the traffic between the Internet user and intranet server is blocked. If yes, modify configurations of the security configuration file.
- Contact the ISP network administrator to check whether the ISP router discards packets sent by the Internet user to the intranet server. If yes, contact the ISP administrator to rectify the fault.
- If the fault persists after the preceding operations are performed, collect the following information and contact Huawei technical support personnel.
 - Results of the preceding troubleshooting procedure.
 - Configuration files, logs, and alarms of the devices.



Contents

1. Basic Configuration Faults
2. LAN Faults
3. IP Routing Protocol Faults
4. IP Service Faults
5. Reliability Faults
6. Security Faults

7. Network

Management Faults

- SNMP Hosts Cannot Connect to the NMS
- The NMS Cannot Receive SNMP Alarms



SNMP Hosts Cannot Connect to the NMS

NMS1
10.1.1.1/24

NMS2
10.1.1.2/24



Internet

GE1/0/0
10.1.2.1/24



Router

No.	Task
1	Configure basic functions for the SNMPv2c.
2	(Optional) Control the rights of the NMS to manage the device.
3	(Optional) Configure the SNMP host to send alarms to the NMS.
4	(Optional) Configure the extended error code function on the SNMP host.

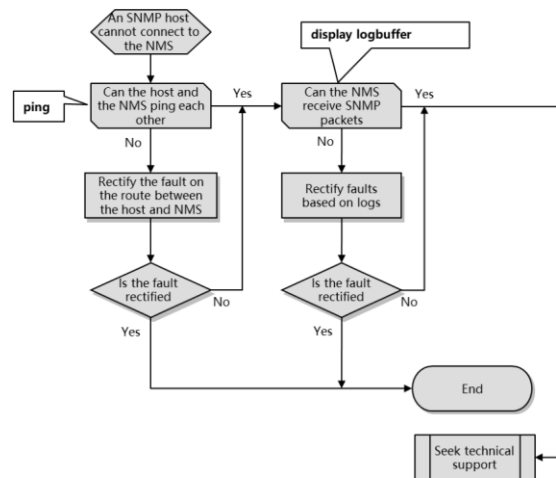
```
snmp-agent
snmp-agent sys-info version v2c
acl 2001
rule 5 permit source 10.1.1.2 0.0.0.0
rule 6 deny source 10.1.1.1 0.0.0.0
snmp-agent mib-view dnsmib include 1.3.6.1.4.1.2011.5.25.194
snmp-agent community write adminnms2 mib-view dnsmib acl 2001
snmp-agent target-host trap-paramsname trapnms2 v2c securityname adminnms2
snmp-agent target-host trap-hostname nms2 address 10.1.1.2 trap-paramsname
trapnms2
snmp-agent trap queue-size 200
snmp-agent trap life 60
snmp-agent trap enable
snmp-agent sys-info contact call Operator at 010-12345678
```

- Packets cannot reach the network management system (NMS). As a result, the Simple Network Management Protocol (SNMP) host cannot connect to the NMS.
- The configuration is incorrect. As a result, the SNMP host cannot connect to the NMS.

- The Simple Network Management Protocol (SNMP) is a standard network management protocol widely used on TCP/IP networks. It uses a central computer (a network management station) that runs network management software to manage network elements. SNMPv1, SNMPv2c, and SNMPv3 are available, and you can configure one or more versions as required.
- To configure SNMP, configure an SNMP management application, for example, network management system (NMS), on the managing device and an SNMP agent on the managed device. The NMS obtains status information about the device through the agent and remotely controls the device. The agent reports the device's status to the NMS in a timely manner.
- Common causes of SNMP login failure are as follows:
 - Packets cannot reach the NMS. As a result, the SNMP host cannot connect to the NMS.
 - The configuration is incorrect. As a result, the SNMP host cannot connect to the NMS.



SNMP Hosts Cannot Connect to the NMS - Troubleshooting Process



- Run the **ping** command to check whether the host and NMS can ping each other.
 - If the ping operation succeeds, there is a reachable route between the host and NMS.
 - If the ping operation fails, rectify the link fault.
- Run the **display logbuffer** command to check whether a log indicating SNMP user login failures is recorded on the host.
 - **Failed to login through SNMP, because the version was incorrect. (Ip=[STRING], Times=[ULONG])**
(The host does not support the SNMP version used by the NMS to send a login request.)
 - Run the **display snmp-agent sys-info version** command to check whether the host supports the SNMP version used by the NMS to send a login request.
 - Run the **snmp-agent sys-info version** command to check the SNMP versions supported by the host.
 - **Failed to login through SNMP, because the packet was too large. (Ip=[STRING], Times=[ULONG])**
(The packet size exceeds the threshold.)
 - Run the **snmp-agent packet max-size** command to increase the maximum packet size threshold.
 - **Failed to login through SNMP, because the community was incorrect. (Ip=[STRING], Times=[ULONG])**
(The community string is incorrectly configured.)
 - Run the **display snmp-agent community** command to check the community string configured on the host.
 - Run the **snmp-agent community** command to configure a read-write community name for the host and ensure that the read-write community name is the same as that configured on the NMS.
 - **Failed to login through SNMP, because of the ACL filter function. (Ip=[STRING], Times=[ULONG])**
(The IP address used by the NMS to send SNMP request packets is denied by an ACL.)
 - Run the **display acl** command to check the ACL configuration on the host. If the IP address used by the NMS to send SNMP request packets is denied by an ACL, run the **rule** command to allow the IP address of the NMS.
- If the fault persists after the preceding operations are performed, collect the following information and contact Huawei technical support personnel.
 - Results of the preceding troubleshooting procedure.
 - Configuration files, logs, and alarms of the devices.



Contents

1. Basic Configuration Faults
2. LAN Faults
3. IP Routing Protocol Faults
4. IP Service Faults
5. Reliability Faults
6. Security Faults

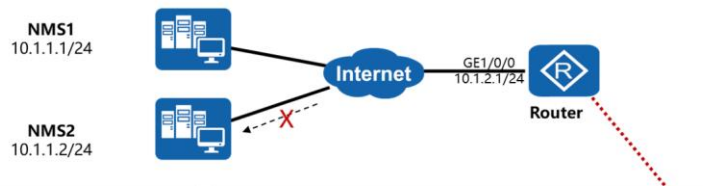
7. Network

Management Faults

- SNMP Hosts Cannot Connect to the NMS
- The NMS Cannot Receive SNMP Alarms



The NMS Cannot Receive SNMP Alarms



No.	Task
1	Configure basic functions for the SNMPv2c.
2	(Optional) Control the rights of the NMS to manage the device.
3	(Optional) Configure the SNMP host to send alarms to the NMS.
4	(Optional) Configure the extended error code function on the SNMP host.

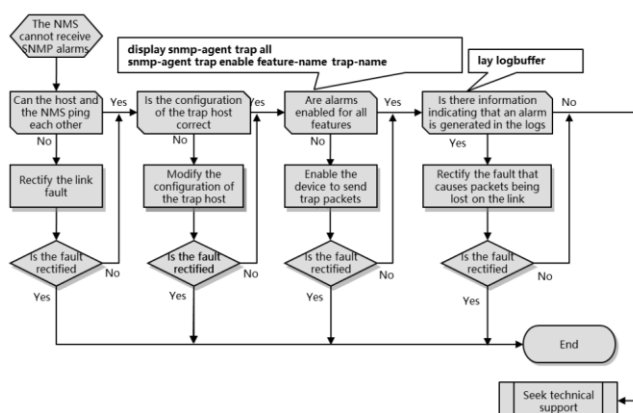
```
snmp-agent
snmp-agent sys-info version v2c
acl 2001
rule 5 permit source 10.1.1.2 0.0.0.0
rule 6 deny source 10.1.1.1 0.0.0.0
snmp-agent mib-view dnmib include 1.3.6.1.4.1.2011.5.25.194
snmp-agent community write adminnms2 mib-view dnmib acl 2001
snmp-agent target-host trap-paramsname trapnms2 v2c securityname adminnms2
snmp-agent target-host trap-hostname nms2 address 10.1.1.2 trap-paramsname
trapnms2
snmp-agent trap queue-size 200
snmp-agent trap life 60
snmp-agent trap enable
snmp-agent sys-info contact call Operator at 010-12345678
```

- Packets are lost. As a result, the NMS cannot receive the alarm.
- The SNMP configuration on the host is incorrect. As a result, alarms cannot be transmitted.
- The service module on the host does not generate alarms, or the format of the alarms generated are incorrect.

- Common causes of SNMP alarm receiving failure are as follows:
 - The packet is lost. As a result, the NMS cannot receive the alarm.
 - The SNMP configuration on the host is incorrect. As a result, alarms cannot be transmitted.
 - The service module on the host does not generate alarms, or the format of the alarms generated are incorrect.



The NMS Cannot Receive SNMP Alarms - Troubleshooting Process



- Ensure that the host and the NMS can ping each other.
- Check whether the configuration of the host that generates alarms is correct. If not, modify the configuration of the host based on the product documentation.
- Check whether the alarm function is enabled.
 - Run the **display snmp-agent trap all** command check whether alarms are enabled for all features. If not, run the **snmp-agent trap enable feature-name trap-name** command to enable the device to send traps and set trap parameters.
- Obtain the host logs and check for alarms on the host. If there are alarm records, the alarms have been generated but failed to be reported to the NMS. Check whether packets are lost on the link.
- If the fault persists after the preceding operations are performed, collect the following information and contact Huawei technical support personnel.
 - Results of the preceding troubleshooting procedure.
 - Configuration files, logs, and alarms of the devices.



Quiz

1. Which of the following may cause a BGP peer relationship fault?

An ACL is configured to filter the packets whose destination port is TCP port 179.

A peer router ID conflicts with the local router ID.

The peer ebgp-max-hop command is not configured on Loopback interfaces to establish an EBGP peer relationship.

Loopback interfaces are used to establish a BGP peer relationship, but the peer connect-interface command is not configured.

- Answer: ABCD.



Thank You
www.huawei.com



Network Troubleshooting Scenario Cases

Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.



Foreword

- This presentation provides a recommended teaching schedule, topology designs for scenario cases, and description of faults to be checked for network troubleshooting.
- The appendix at the end includes the answers to troubleshooting cases, topology files on the Enterprise Network Simulation Platform (eNSP), and failure point configurations of scenario cases. Teachers and trainees can use them as a reference.



Objectives

- Upon completion of this section, you will be able to:
 - Master the skills to flexibly use network troubleshooting methods based on practices



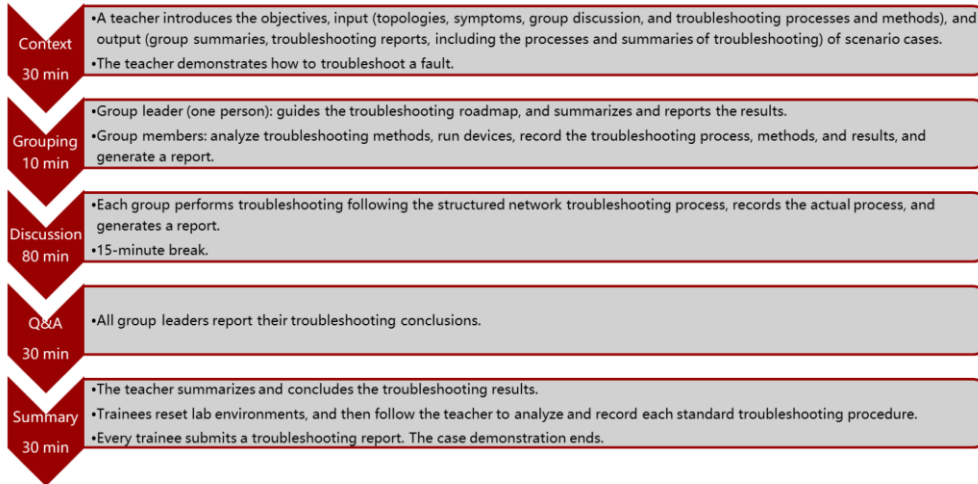
Contents

- 1. Troubleshooting Precautions and Class Sequence**
2. Topology Designs for Scenario Cases
3. Faults to Be Checked
4. Appendix

Network Troubleshooting Scenario Cases: Precautions

- A teacher proposes several faults for discussion.
- **Emphasis should be on mastering the troubleshooting process and methods through practices, not rectifying many faults in a short period.**
- **Troubleshooting operations must be authorized, and related documents must be generated.** Ensure that each troubleshooting operation complies with the process and is recorded.
- **The aim of troubleshooting is not to carry out independent, onsite rectification of faults, but to quickly locate a failure point using a clear roadmap.** When you locate a fault on a device and cannot rectify it, contact senior engineers, service providers, or vendors (teachers, in class) immediately for technical support.

Network Troubleshooting Scenario Cases: Class Sequence



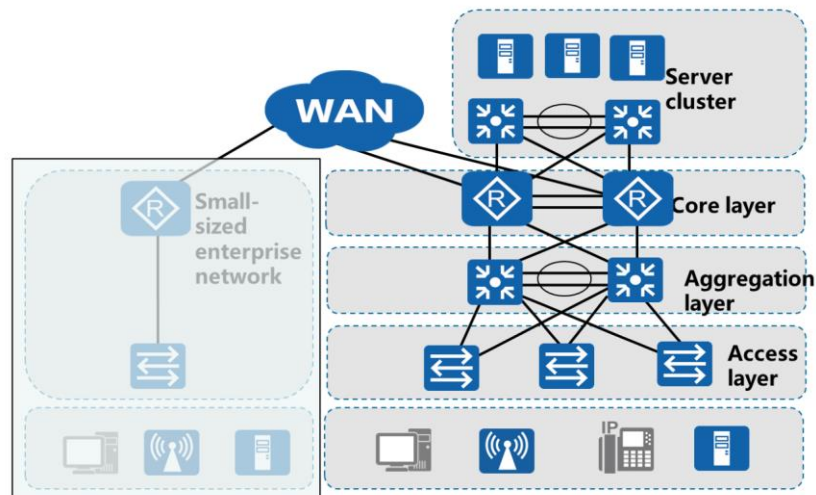
- Each case has four failure points and lasts for 90 min.



Contents

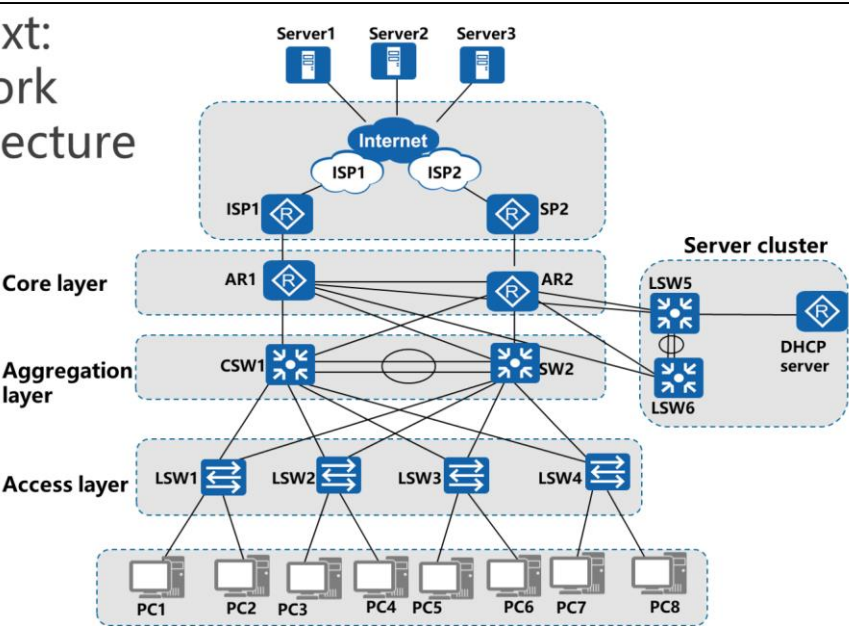
1. Troubleshooting Precautions and Class Sequence
- 2. Topology Designs for Scenario Cases**
3. Faults to Be Checked
4. Appendix

Context: Enterprise Network Architecture

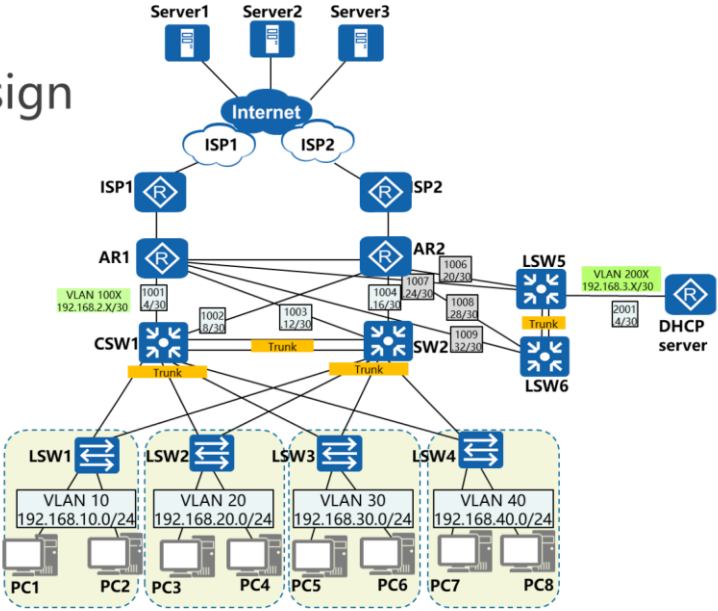


- The architecture of an enterprise network depends on the requirements of the enterprise or organization. In most cases, a small-sized enterprise only has one office, so a flat network architecture is used. This architecture satisfies the requirements of customers on resource access, provides strong flexibility, and saves deployment and maintenance costs. Generally, small-sized enterprises do not have redundancy mechanisms, so the network reliability is poor and service interruption may occur.
- For large-sized enterprises that have strict requirements on service continuity, network redundancy is deployed to ensure availability and stability, so that routine service operations can be guaranteed. Additionally, resource access control is configured, and multi-layer network architectures are used to optimize traffic distribution. Various policies are used to manage traffic and control resource access. A multi-layer architecture makes the network easy to expand. Further, a modular design enables effective network isolation and simplifies network maintenance, so that the failure of a single area will not affect the entire network.

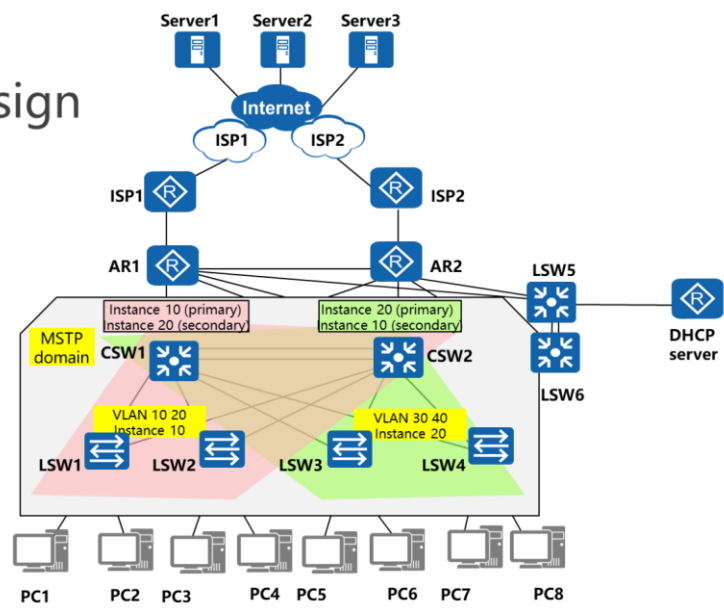
Context: Network Architecture



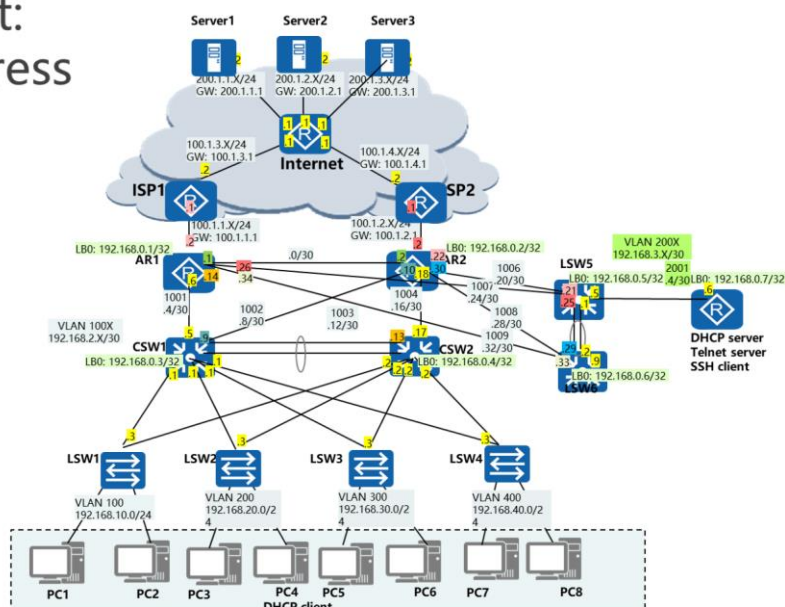
Context: VLAN Design



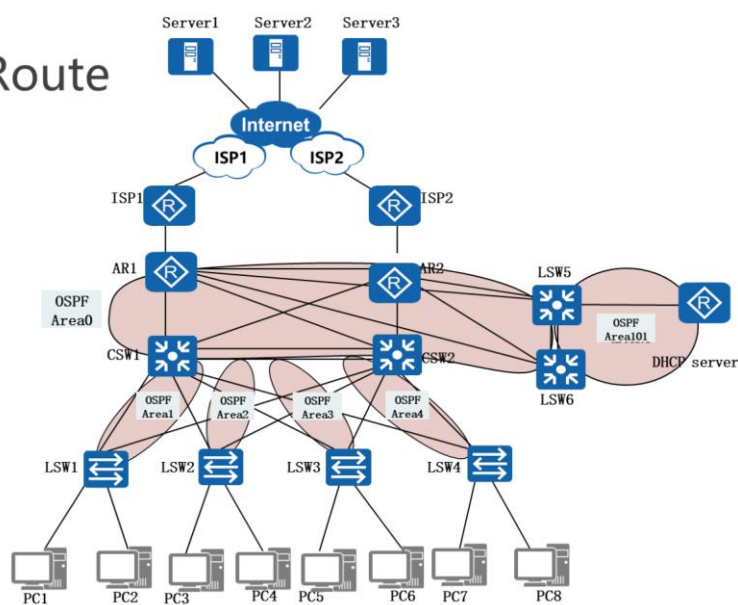
Context: MSTP Design



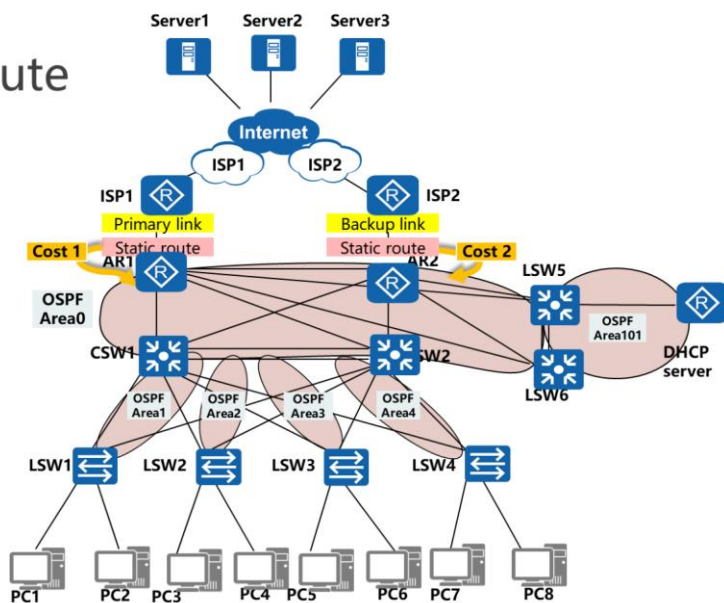
Context: IP Address Design



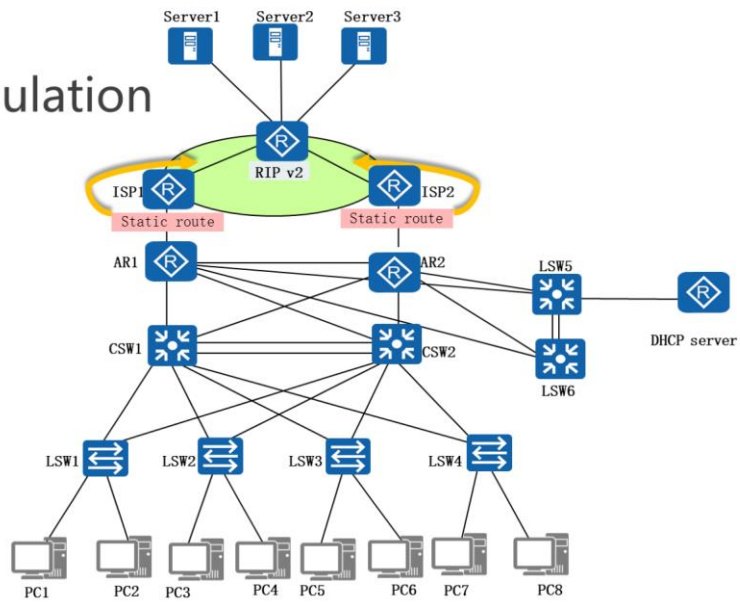
Context: Intranet Route Design



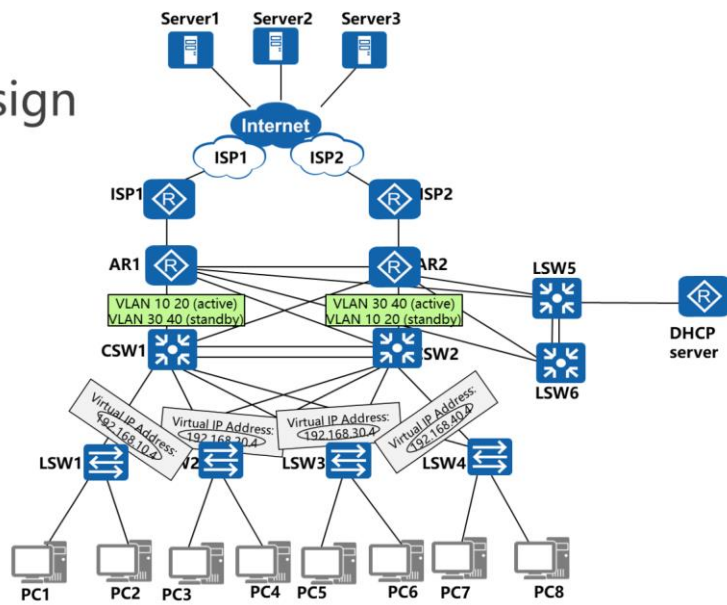
Context: Egress Route Design



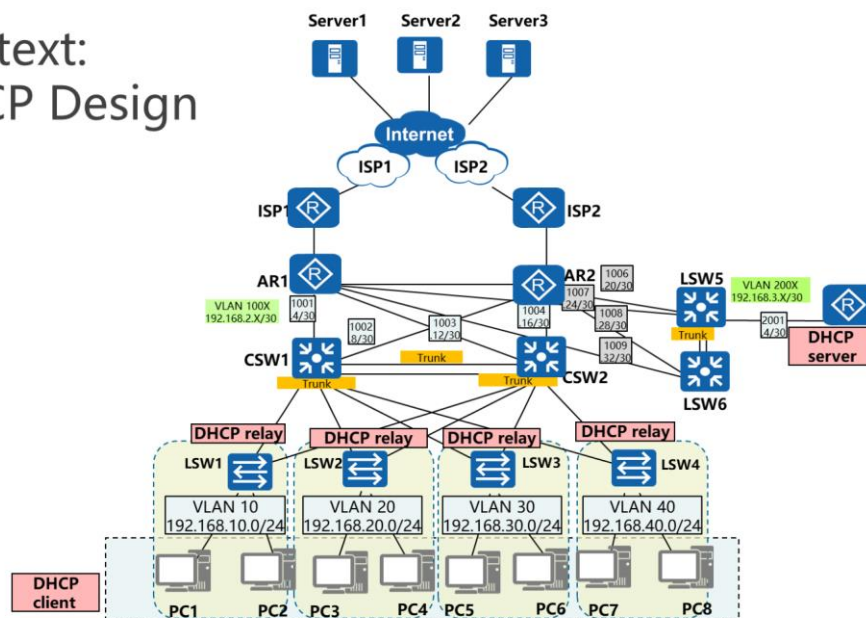
Context: WAN Simulation



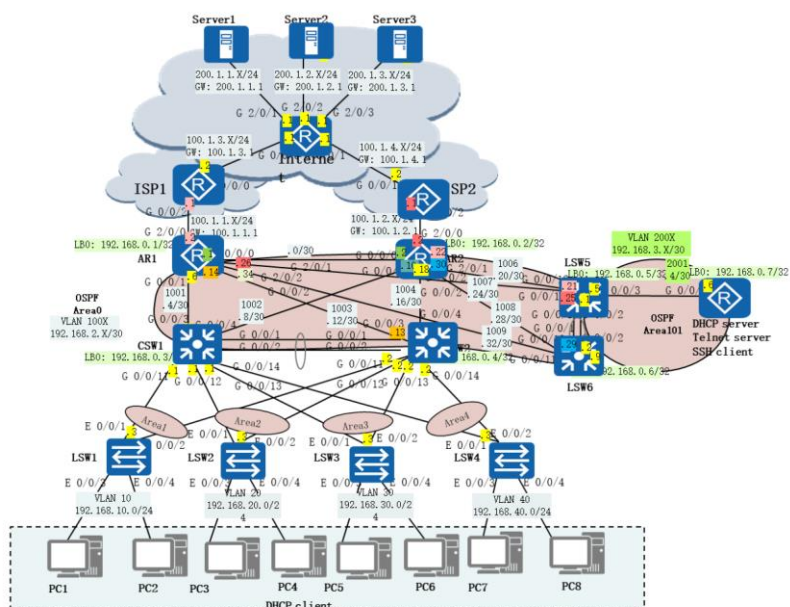
Context: VRRP Design



Context: DHCP Design



Context: Topology Overview





Contents

1. Troubleshooting Precautions and Class Sequence
2. Topology Designs for Scenario Cases
- 3. Faults to Be Checked**
4. Appendix

Scenario Case 1: Faults to Be Checked

- A company changed to two new Internet service providers (ISPs) and performed line switching during the weekend. Network administrators may have performed other operations on the network.
- On Monday morning, you received a phone call from an employee who complained about failing to access the Internet (Server1) through a terminal (PC7).

Scenario Case 2: Faults to Be Checked








- On Sunday, a network administrator carried out device maintenance and detected that the PC5 user could not access the Internet (Server1) when the cable between LSW3 and CSW2 was disconnected.
- After the network maintenance on Sunday, users reported that the Internet connection was slow. Please locate the root cause and rectify this fault.



Contents

1. Troubleshooting Precautions and Class Sequence
2. Topology Designs for Scenario Cases
3. Faults to Be Checked
- 4. Appendix**

Appendix

Description		List
Scenario case 1	Topology files on the eNSP with failure points pre-configured	 Scenario Case 1 eNSP Topology File
	Reference answer for scenario case 1	 Scenario Case 1 Reference Answer
Scenario case 2	Topology files on the eNSP with failure points pre-configured	 Scenario Case 2 eNSP Topology Files
	Reference answer for scenario case 2	 Scenario Case 2 Reference Answer
Troubleshooting reports of trainees	Network troubleshooting reports (template)	 Network Troubleshooting Report (Tem
Failure point configurations (reference for teachers to design scenario cases)	Topology files on the eNSP (with normal networks pre-configured)	 eNSP Topology Files
	Basic network configurations and failure point settings	 Basic Network Configurations and Fault



Quiz

1. Which of the following statements about fault verification in the structured network troubleshooting process is true?

Focus on how to rectify a fault in a better way, no matter if the fault is within or beyond your scope of responsibility.

Value users' opinions and determine the fault based on their judgment.

To minimize the impact, do not notify others of the fault.

Determine whether the fault is within your scope of responsibility.

- Answer: D.



Thank You

www.huawei.com



Network Optimization



Foreword

- As users' services develop, the users' requirements on network functions increase. When a network fails to meet service requirements or potential problems are found while the network is running, the network needs to be optimized.
- Different from network construction, network optimization is implemented on a running network. Precautions must be taken when you design and implement a network optimization solution.
- This course describes the basic concept of network optimization. Typical principles and methods of network optimization are also described with two examples of improving network security and user experience.



Objectives

- Upon completion of this section, you will be able to:
 - Understand the contents of the professional network optimization service
 - Understand network optimization principles
 - Master methods of improving network security
 - Master methods of improving user experience
 - Be familiar with the contents of a network optimization solution



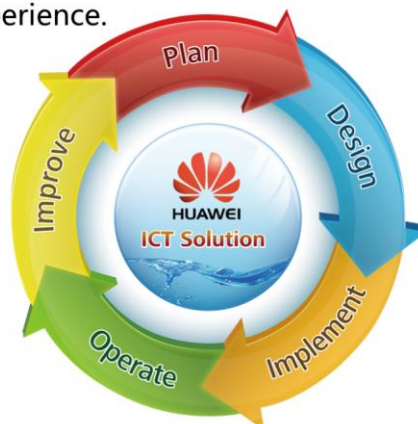
Contents

- 1. Network Optimization Overview**
2. Improving Network Security
3. Improving Network User Experience
4. Adding Network Functions
5. Network Optimization Solution



Network Optimization Overview

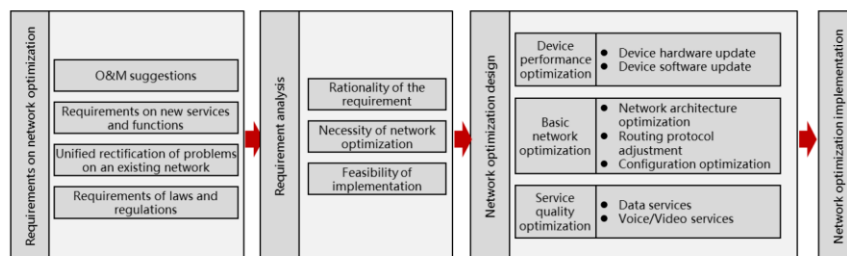
- The purpose of network optimization is to improve network performances, network security, and network user experience.
- Network optimization includes:
 - Hardware optimization
 - Software optimization
 - Network expansion
 - Technology update



- Network optimization is using hardware or software technologies to optimize network performances and enable networks to meet service requirements. Network optimization includes hardware optimization, software optimization, network expansion, and technology update.
 - Hardware optimization refers to providing an optimal scheme on device performances and prices based on hardware requirement analysis.
 - Software optimization refers to optimizing system performances through setting software parameters.
 - Network expansion refers to adding new network services to an existing network, including replacing or adding network devices and changing the network topology.
 - Technology update refers to updating some or all technologies used by a network.
- Network optimization can be considered as a new cycle of plan, design, implementation, operation, and improvement (PDIOI) of a project.



Network Optimization Principles



- After network optimization, a network is more secure and reliable, and can better support enterprise service development.

- Sources of requirements on network optimization include O&M suggestions, requirements on new services and functions, unified rectification of problems on an existing network, and requirements of laws and regulations.
 - O&M suggestions: Network maintenance personnel summarize problems on a network during a long-term network maintenance and provide suggestions on unified rectification of the problems.
 - Requirements on new services and functions: For example, video conference services are deployed on a network and generate a large number of Layer 2 network multicast packets. Switches that support Layer 2 multicast need to be added to the network to improve the network performance. (IGMP snooping can be enabled on switches to reduce packet flooding, but this also increases the load of the switches.)
 - Unified rectification of problems on an existing network: For example, the signal cables of a weak electricity well age seriously and need to be replaced in a centralized manner.
 - Requirements of laws and regulations: For example, new security devices are required to ensure security of enterprise information.
- Requirement analysis focuses on the following:
 - Rationality of the requirement: Whether network optimization is necessary to meet the actual service requirements and deserves the investment
 - Necessity of network optimization: Whether the requirement is urgent and necessary
 - Feasibility of implementation: Whether the network optimization is feasible on the existing network and allowed by policies
- After analyzing the requirement on network optimization, design a network optimization solution and implement the solution to achieve the following goals:
 - Improve network security: For example, improve the security of an enterprise network by deploying border gateways on the network.
 - Improve network user experience: For example, improve the communication quality of VoIP services by optimizing the network traffic.
 - Add network functions: For example, add the Wi-Fi function by deploying WLAN.



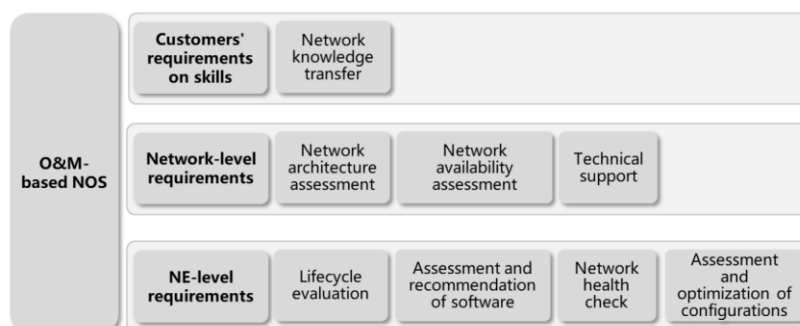
Professional Network Optimization Service

- Different from common network optimization services, the professional network optimization service (NOS) provided by Huawei (or other service providers) is a comprehensive service using professional network optimization tools. The following functions are provided to help enterprises maximize their profits and improve customer satisfaction.
 - Improving service performance
 - Improving network availability and performance
 - Improving productivity
 - Lowering costs
 - Transferring knowledge

- Huawei NOS is a comprehensive service aiming to improve the network performance, scalability, and availability, so as to help enterprises maximize their profits and improve customer satisfaction.
- Improving service performance
 - Improve the availability of an enterprise network and the quality of the enterprise's services to enhance the enterprise's competitiveness.
 - Help enterprises improve the competitiveness of their networks and achieve their short-term and long-term strategic goals.
- Improving network availability and performance
 - Provide continuous technical support on network capacity management to ensure the network availability.
 - Accelerate the application of advanced network solutions without affecting the network availability based on best practice experience.
- Improving productivity
 - Use software and hardware devices or tools to implement performance plan, availability improvement, and network optimization based on Huawei's rich experience in the industry to greatly increase the network running time, improving productivity.
- Lowering costs
 - Provide network planning and maintenance services to fully use the network resources and minimize the costs of hardware upgrade and network re-design.
 - Provide professional technical support and maintenance to greatly increase the network running time and lifecycle and improve the network performance.
 - Shorten the time for training network O&M personnel from enterprises.
- Transferring knowledge
 - Provide training to the enterprise network O&M personnel to enable them to learn the latest network technologies and solutions. Experience and skills of the personnel will improve the network O&M efficiency, and strengthen core competitiveness of the network departments.



Contents of Professional Network Optimization Service



- Core value: NOS aims to improve enterprises' competitiveness and help them obtain leading positions in the industry.

- The purpose of Huawei NOS is to improve the competitive strength of an enterprise network and help the enterprise to obtain a leading position in the industry.
- Customers' requirements on skills
 - Network knowledge transfer
 - Based on the network construction and O&M experience accumulated at global sites, the knowledge transfer service provides the engineers with desired network O&M information.
- Network-level requirements
 - Network architecture assessment
 - Huawei specialists use the industry-leading practice to review the network architecture, focusing on the feasibility, security, and scalability, and offer optimization suggestions based on the assessment.
 - Network availability assessment
 - Huawei engineers evaluate the availability of an enterprise network, offer a network availability indicator system, construct a network availability model applicable to the enterprise, and provide procedure and methods for continuous network availability improvement.
 - Technical support

- Huawei possesses a reliable technical support team, composed of experts with strong troubleshooting skills. They can help customers rectify service faults quickly to minimize impacts on services. Additionally, Huawei also provides field technical support in a specified period.
- NE-level requirements
 - Lifecycle evaluation
 - Periodically check and analyze the lifecycle of software and hardware on the existing network, and manage the products that have reached the end of marketing (EOM), end of production (EOP), end of software update, or end of service and support (EOS) accordingly to prevent risks.
 - Assessment and recommendation of software
 - Evaluate and analyze all software platforms used by Party A during the service period, and recommend software versions to prevent exceptions caused by known bugs.
 - Network health check
 - The purpose of network health check is to help users fully understand the technical features and potential risks of their network systems, so that they can make suitable and feasible network expansion, reconstruction, and maintenance plans to improve network security based on service development requirements and current network resources.
 - Assessment and optimization of configurations
 - Develop and continuously maintain device configuration templates as required by customers. Based on the periodic software assessment and recommendation, add commands to specific features of recommended software to implement refined configuration management.

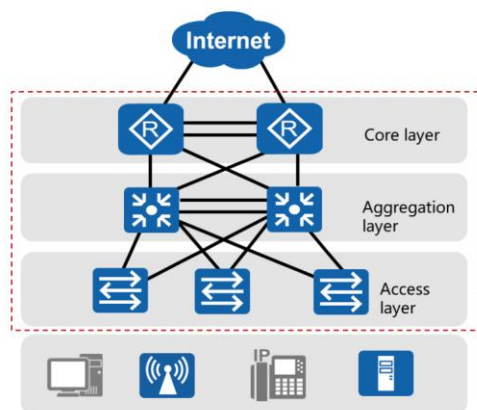


Contents

1. Network Optimization Overview
- 2. Improving Network Security**
3. Improving Network User Experience
4. Adding Network Functions
5. Network Optimization Solution



Improving Network Security

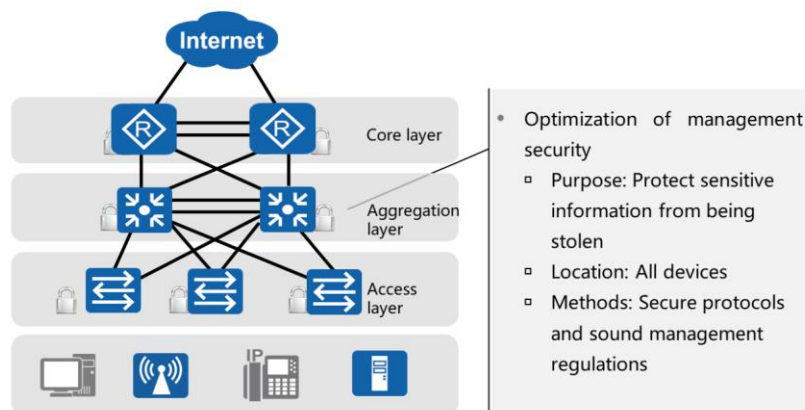


- Network security is a systemic issue, involving the following:
 - All devices on a network
 - Security management
- Network security includes the following sub-items:
 - Management security
 - Border security
 - Access control
 - Access security
 - Traffic monitoring

- Consider the following aspects when improving the network security:
 - Management security
 - Border security
 - Access control
 - Access security
 - Traffic monitoring



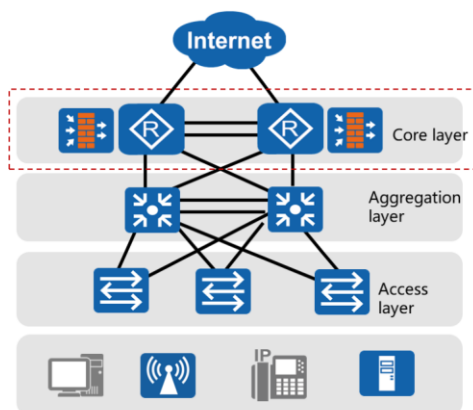
Optimization of Management Security



- Here, management security refers to ensuring the security of management methods using technologies instead of management systems. Management systems are not described here. For example, an enterprise needs to improve the security of network device management and add a security policy for network access control to prevent unauthorized access to network devices or configuration tampering. In this way, the enterprise improves the security of its network device management.



Optimization of Border Security

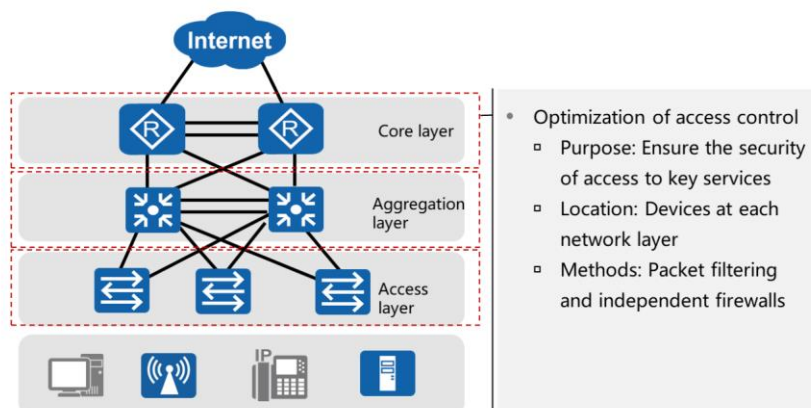


- Optimization of border security
 - Purpose: Prevent and reduce attacks from external networks, which bring risks to the intranet
 - Location: Network border
 - Methods: Attack defense, packet filtering, and hardware firewalls

- Optimization of network border security is to protect intranet resources (including network devices and information assets) and user terminals from external attacks. For example, the intranet servers of an enterprise are frequently attacked by external distributed denial of service (DDoS). To solve this problem, the enterprise can deploy appropriate protection measures (such as firewalls or other defense policies) at the network border.



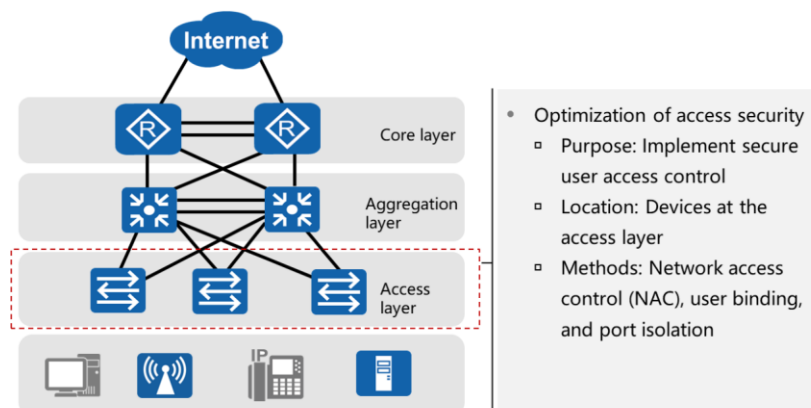
Optimization of Access Control



- Access control is to restrict or block specified traffic without affecting current routes based on service control requirements. For example, an enterprise uses specific technologies to prevent other departments from accessing the server of the financial department.



Optimization of Access Security

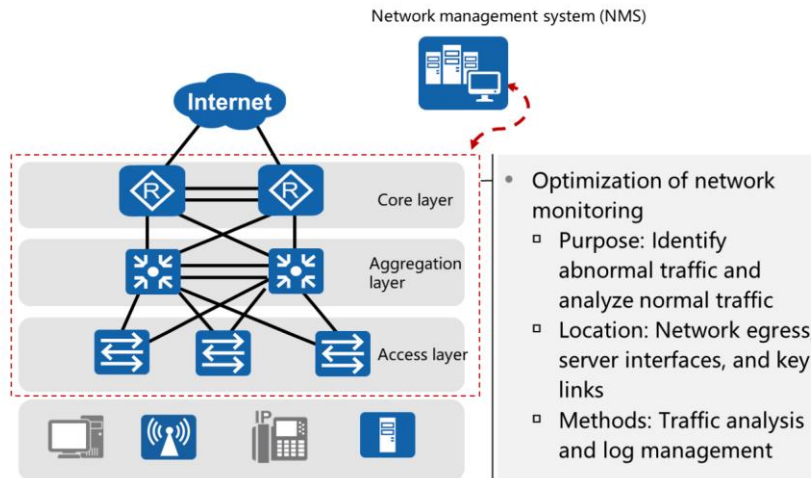


- Optimization of access security
 - Purpose: Implement secure user access control
 - Location: Devices at the access layer
 - Methods: Network access control (NAC), user binding, and port isolation

- Network access security refers to protection of network resources (including network devices and information assets) against accidental or intentional attacks from intranet users. For example, specific technologies can be used to prevent unauthorized external users from accessing an enterprise network. Network access security can be implemented through network access control (NAC). Users must enter the user name and password for authentication to access the network.



Optimization of Network Monitoring



- Network monitoring is to monitor and analyze network traffic in real time or periodically. For example, an enterprise monitors its network to block abnormal traffic in a timely manner. Network monitoring software or hardware can be deployed to monitor and analyze traffic on networks.

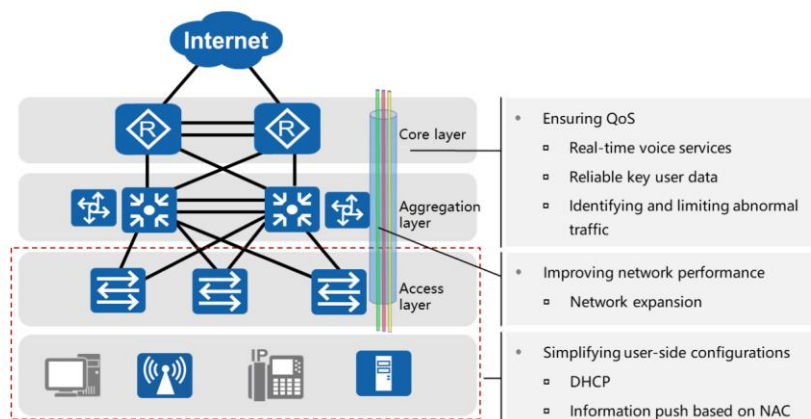


Contents

1. Network Optimization Overview
2. Improving Network Security
- 3. Improving Network User Experience**
4. Adding Network Functions
5. Network Optimization Solution



Improving Network User Experience



- According to the ISO 9241-210 criteria, user experience refers to people's impression on and response to products, systems, or services they use or expect to use. To put it simple, user experience refers to how users feel about a product or service, whether it is useful and convenient or not. Therefore, user experience is subjective and depends on actual application effects.
- Ensuring QoS
 - QoS is a systemic issue. In addition to traditional data services such as WWW, email, and FTP, enterprise networks also transmit the services such as video surveillance, teleconference, voice call, and production scheduling, which are sensitive to bandwidth, delay, and jitters. For example, video surveillance and teleconference require high bandwidth, low delay, and low jitter. Voice services do not require high bandwidth, but require low delay. When traffic congestion occurs, voice services must be processed first.
- Improving network performance
 - As an enterprise expands and its services develop, the current network may fail to effectively support the enterprise services. In this case, the network scale needs to be enlarged or the network devices need to be upgraded to meet the service development requirements.
- Simplifying user-side configurations
 - Here, users refer to end users of networks, namely, the users of PCs on networks.
 - Terminal configurations can be simplified to improve user experience. For example, DHCP servers are deployed on a network to enable user terminals to obtain IP addresses dynamically. (Network servers and printers must be configured with the IP addresses bound to their MAC addresses to ensure service availability.)

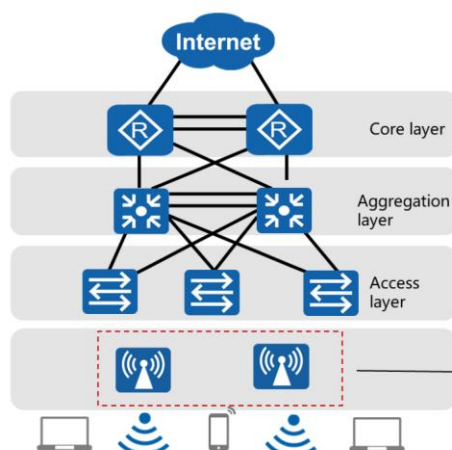


Contents

1. Network Optimization Overview
2. Improving Network Security
3. Improving Network User Experience
- 4. Adding Network Functions**
5. Network Optimization Solution



Adding a Network Function - WLAN Access



- Allowing wireless devices to access an existing network is a typical example of adding new network functions.
- Before deploying WLAN, consider the following:
 - Impacts on the existing network
 - Expected results
 - Investment budget

- Before adding a new network function, consider the impacts of the function on the existing network. An added network function cannot affect the existing normal services in a long period. Only controllable and temporary impacts are acceptable.
- Fully evaluate expected effects of an added function. For example, before implementing WLAN access, determine whether to provide WLAN access in all offices or only in some key areas (such as conference rooms) and evaluate the expected effects. The technical solution and investment budget must be determined based on evaluation results. If WLAN signals cover all offices, fit APs are required. If WLAN signals only cover some areas, fat APs are more appropriate.
- The investment budget is determined based on requirements and the applied technical solution. Enterprises must consider the investment budget during network optimization. In scenarios where new network functions are added, optimization solutions must be sufficient, fast, excellent, and cost-effective. That is, new functions should be added with no extra or the minimum investments. For example, in some scenarios, only a technical solution is required to enable the multicast function on a network. This is because most network devices support multicast. However, in more scenarios, new devices are required to enable a network to provide new functions. As shown in the figure, APs and even radio access controllers (RACs) must be deployed on a network to provide wireless access.
- Test a new network function within a small range. After confirming that the function causes no risk, deploy the function on the entire network. For example, before deploying APs to enable WLAN access in a large scale, deploy APs in some offices and evaluate the impacts on the current network.

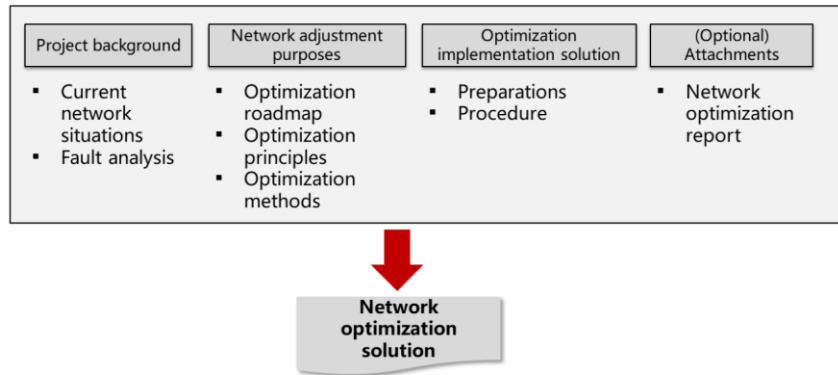


Contents

1. Network Optimization Overview
2. Improving Network Security
3. Improving Network User Experience
4. Adding Network Functions
5. **Network Optimization Solution**



Network Optimization Solution



- Project background
 - Current network situations: Describe the current network architecture, service description, and problems with the current network.
 - Fault analysis: Analyze main causes why the current network cannot support services in details.
- Network adjustment purposes
 - Optimization roadmap: Briefly describe the solution of problems on the current network.
 - Optimization principles: Describe the differences between the networks before and after the network optimization and the return on investment.
 - Optimization methods: Describe strategies and methods of optimization (for example, replacing core switches) in details.
- Optimization implementation solution
 - Preparations for network optimization are similar to preparations for network construction. For example, conduct a survey and output an optimization solution before implementation.



Quiz

1. Which of the following are sources of requirements on network optimization?

Network maintenance personnel summarize problems and points to be improved during long-term network maintenance and provide suggestions on unified rectification.

Switching devices that support Layer 2 multicast need to be added to a network to support video conference services.

The signal cables of a weak electricity well age seriously and need to be replaced in a centralized manner.

New security devices are required to ensure the security of enterprise information.

- Answer: ABCD.



Thank You

www.huawei.com



Network Migration



Foreword

- With the development of enterprise services, enterprise networks are reconstructed and optimized continuously to meet service requirements. Operations that affect running services on the live network are defined as migration projects. For example, operations leading to service interruption, hardware capacity expansion, software upgrade, and configuration changes. Before performing these operations, enterprises prepare strict operation flows and risk mitigation measures based on service security level requirements.
- This course allows trainees to get familiar with the migration flow and operation specifications, master risk control measures, and thereby efficiently and smoothly complete the network migration.



Objectives

- Upon completion of this section, you will be able to:
 - Understand the definition of network migration
 - Master the standard migration operation procedure
 - Be familiar with common migration scenarios



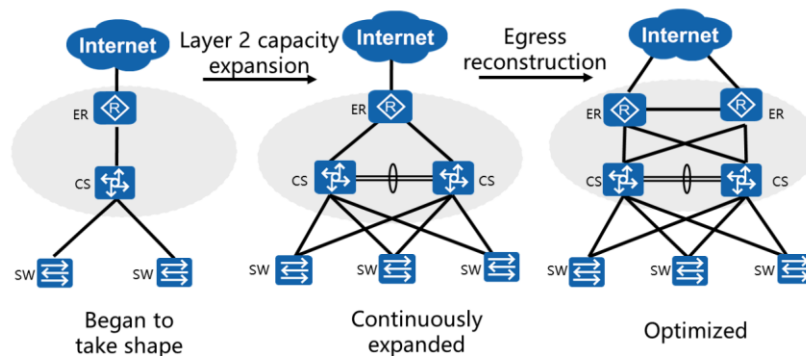
Contents

1. **Migration Overview**
2. Migration Operation Procedure
3. Common Migration Scenarios



Changing Enterprise Networks

- Networks, the basis of enterprise services, are developing and changing continuously.



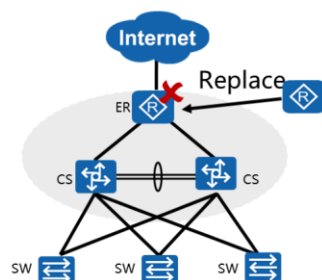
- How can we ensure smooth service transition when networks are upgraded, expanded, and reconstructed continuously?

- This is the development history of an enterprise network:
 - In 2012, the company only had a small office area. The service traffic volume was small, and only simple network access was required.
 - In the next two years, the number of employees increased, the service traffic volume grew, and key services developed continuously. The network capacity was expanded and one switching device was added. A new network architecture was set up, and load balancing was configured at the aggregation layer.
 - In 2016, the egress bandwidth could not meet service requirements. Therefore, another core router was deployed at the network egress, forming an active/standby architecture.



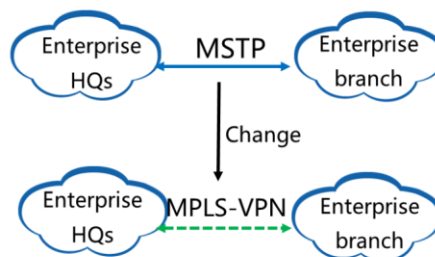
Network Maintenance Methods

- A device has a life cycle.



- When a core egress device is replaced, a large number of services may be interrupted.

- Links are changing constantly.



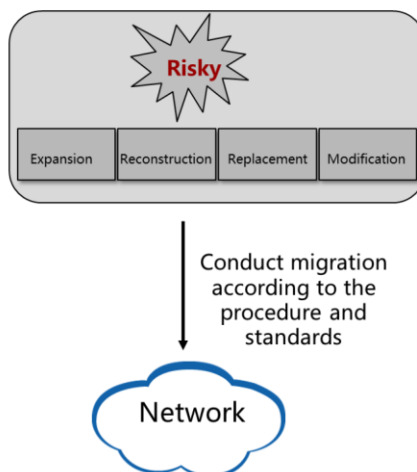
- Link changes involve service configuration adjustment, as well as physical line switchover.

- Every product has a life cycle. For security purposes, an ICT device that has been running for 5 to 10 years should exit from the network and be replaced with a high-performance device. It is important to implement secure and smooth transition.
- Network lines are upgraded based on market environments and company's requirements. For example, most large-sized enterprises used expensive MSTP (SDH) lines provided by ISPs to enable communications between their HQs and branches. Nowadays, leasing MPLS VPN lines that can save vast expense has become the mainstream. Therefore, to ensure proper service running, a company needs to secure the process of switching MSTP lines to MPLS VPN lines.



Migration Overview

- If technical migration operations may affect running services on a live network, perform the operations in strict compliance with the preset operation procedure and take risk control measures. Generally, these projects are defined as migration projects.





Migration Difficulties



Where do the risks exist?



Which implementation methods should be used?

- Estimate risks → Make a scheme → Strictly comply with the scheme

- Migration difficulties:
 - Control the scope of services that will be affected.
 - Master risk mitigation methods.
 - Make a perfect migration scheme.
 - Perform the migration smoothly.



Contents

1. Migration Overview
- 2. Migration Operation Procedure**
3. Common Migration Scenarios



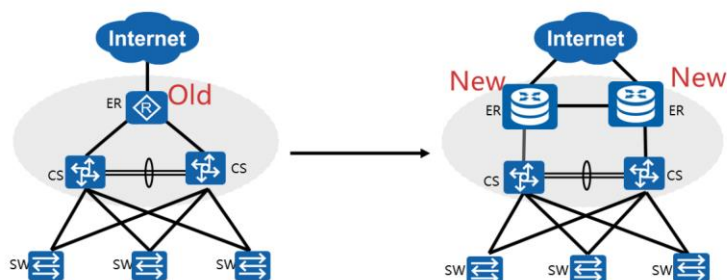
Migration Operation Procedure

- Preparation phase:
 - Project survey, requirement analysis, risk assessment, scheme preparation, and scheme approval
- Implementation phase:
 - Migration preparation, migration, and service tests
- Closure phase:
 - Site attendance and project acceptance



Network Status Analysis

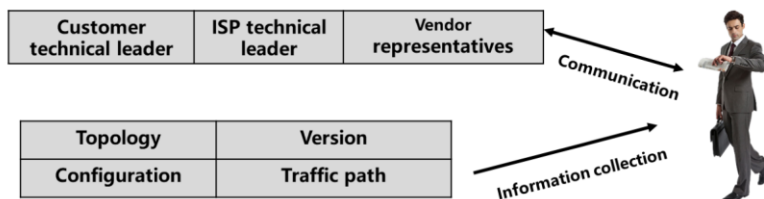
- The network of Company A has been running for many years. With the development of services, the traffic carried by the core egress router is increasing, and the router's in-service period is close to the device service life specified by Company A. Therefore, Company A requests to replace the old router at the core layer with two high-performance routers.





Project Survey

- Company B is responsible for the network construction and maintenance of Company A. When receiving the network reconstruction request from Company A, Company B assigns network expert Tom to visit the site and conduct analysis and surveys.
- Tom communicates with Company A's network owner, frontline maintenance engineers, technical contact person of the Internet Service Provider (ISP), and vendor representatives, and collects network information (including topology, configurations, versions, traffic types, and traffic paths) onsite.





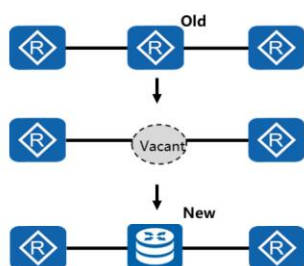
Project Analysis

- After one week research, Tom analyzes customer requirements based on his rich engineering experience:
 - **Necessity:** The core egress router has been running for a long time and is carrying more and more services. Therefore, it needs to be replaced and the network needs to be reconstructed.
 - **Feasibility:** After communication with vendor representatives about technical details, migration is considered to be feasible based on personal experience and historical cases.
 - **Risk analysis:** The replacement of the core egress router involves service switchover, which may lead to service interruption.
 - **Project qualitative analysis:** The network architecture, especially the core egress, will be changed greatly. Therefore, it is defined as a network reconstruction project.
 - **Technical positioning:** The core egress reconstruction may cause great risks to services running on the entire network. Therefore, it is defined as a migration project.

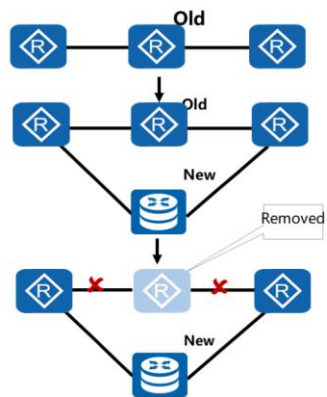


Scheme Selection

- Tom proposes two migration schemes for subsequent discussions with customers.



Direct replacement



Gradual replacement

- Direct replacement:
 - Advantage: high execution efficiency, short migration cycle, and less resources consumed.
 - Disadvantage: high risks and long service interruption time.
 - Application scenario: small-sized network with no key services affected and high project cost requirements.
- Gradual replacement:
 - Advantage: low risks and easy for rollback.
 - Disadvantage: long migration cycle with low efficiency.
 - Application scenario: large-sized network with key services affected and low project cost requirements.



Risk Assessment

- Detailed analysis and assessment on the migration risks:

Risk Assessment	Company A's Migration Project
Risk	Service switchover
Affected scope	Entire network
Affected duration	Service interruption for 5 minutes to 120 minutes
Loss caused by risks	Failing to recover company's services
Risk mitigation methods	Segment-by-segment migration + rollback + onsite spare part replacement

- Key points in risk assessment:
 - Service interruption time and affected service scope must be analyzed and specified, and corresponding description and countermeasures must be provided.



Communication and Coordination Meeting

Vendor



ISP



Party A



Party B



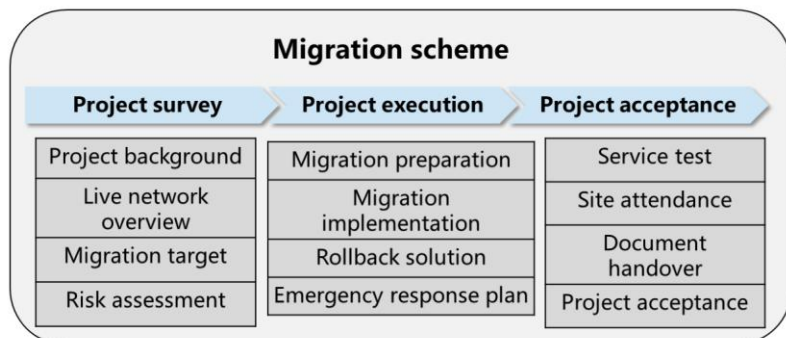
Model Selection	Vendor: Huawei provides high-performance routers of new models that apply to various scenarios. Corresponding quality reports and cases are available.
Egress Interconnection	ISP (carrier): We have cooperated and completed many similar projects successfully.
Risk Assessment	Party A (customer): We are willing to invest a large amount of time and funds to ensure that services are running properly.
Scheme Selection	Party B (contractor): Gradual replacement will minimize the risks.
Supervisor: We should cooperate with each other and work together to complete the reconstruction project.	

Supervisor





Scheme Preparation





Scheme Verification and Review



First Office Application (FOA) deployment for testing



Vendor expert reviews

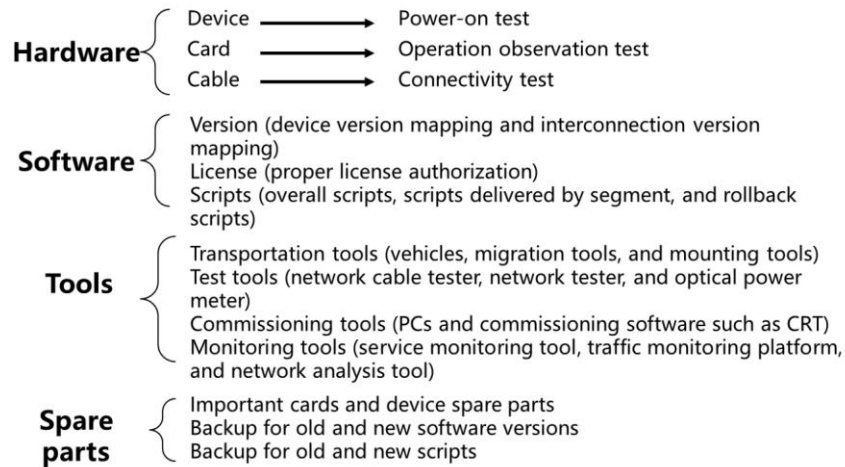


Scheme determination

- FOA deployment for testing:
 - If the migration project is large, the customer may require first office application (FOA) deployment to test the network in advance. The FOA environment must be the same as the real network environment.
- Technical review of all parties:
 - The customer and implementation party should proactively communicate with each other to understand the actual requirements of and difficulties facing the other party and solve problems face to face.
- Vendor expert reviews:
 - If the device version changes or new device functions are added, the migration scheme should be sent to the experts from the vendor for review.
- Special for this example:
 - A router is added in this example. Mount the router to its rack, power on it, and test its running status before the migration.
 - Apply for onsite technical review as required, so that engineers from the vendor will check device running status onsite.



Migration Preparation (1/2)



- Migration preparation is a key procedure before migration and is the basis for successful migration.
- The following items should be included: environment preparation (hardware, software, tools, and spare parts), personnel preparation (party A, party B, and supervisor), and procedure preparation (execution time dividing). All aspects should be considered to ensure migration success.



Migration Preparation (2/2)

Personnel preparation

- Participant list (party A, party B, and supervisor)
- Participants' responsibilities (implementation personnel, test personnel, and monitoring personnel)
- Participants' contact details

Time schedule

- Overall migration time
- Service interruption time
- Rollback time

Comparison tables

- Comparison of physical topologies, logical topologies, and service configurations before and after the migration
- Comparison of software versions before and after the migration
- Analysis and comparison of the control planes (such as routing, security control, and QoS information) before and after the migration
- Analysis and comparison of the data planes (data flows) before and after the migration

- Personnel preparation:
 - Clear responsibility assignment ensures smooth communication among all parties and prevent responsibility shirking.
- Time arrangement preparation:
 - Negotiate the time arrangement with the customer and obtain customer's approval.
 - Make an overall time schedule.
 - Specify the operations for each time period.
 - In the migration phase, time arrangement should be accurate to minute.
 - Reserve some time for major operations to avoid engineering accidents due to time exceeding.
 - Do not perform migration in peak hours (such as holidays and off-duty time).



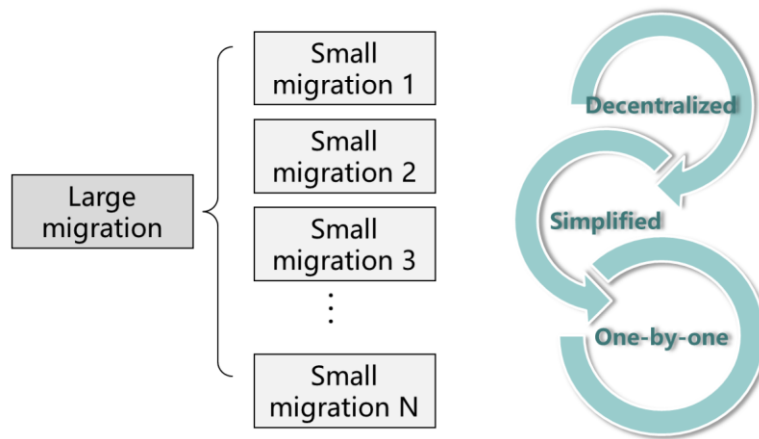
Implementation Approval

- After the overall Migration Scheme is approved, it must be signed by the customer.
- A Change Application Form must be submitted before each specific operation.
- The Change Application Form must contain the signature of the specific owner authorized by the customer.
- Before each migration change, all involved personnel must be notified through email, telephone, or SMS.

Critical!



Implementation: Migration by Segment

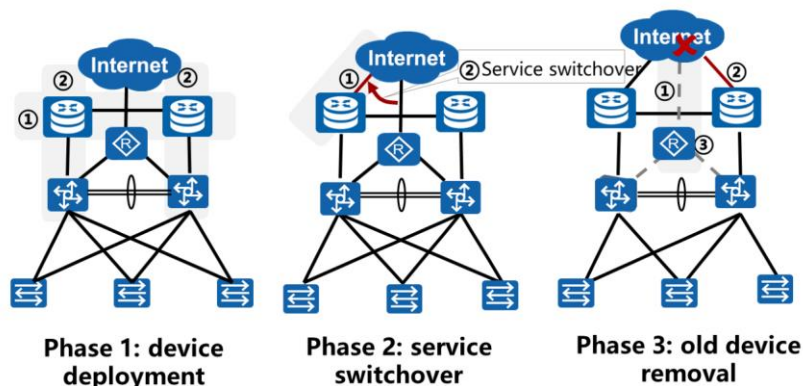


- Migration by segment:
 - A migration project is usually complex. Therefore, specify risk control for each step if possible.
 - Decentralize a large migration process into multiple small migrations, which are independent of one other and support each other. In addition, the operation procedure of each small migration must be specified.



Implementation: Migration Roadmap

- Tom divides the migration into three phases:



- Device deployment:
 - Step 1: Add two core routers to the network and connect corresponding links.
 - Step 2: Connect the new core routers to the original aggregation switches.
 - Step 3: Observe device running stability for at least two weeks.
- Service switchover:
 - Step 1: Connect physical lines between the core routers and the ISP's network.
 - Step 2: Perform service switchover. Switch the traffic egress from the old core router to the new core router. Use the default routes advertised by the old router and new router to perform the operation.
 - Step 3: Observe service running stability for 2 hours to 24 hours.
- Old device removal:
 - Step 1: Disconnect the line between the old core router and the ISP's network.
 - Step 2: Connect the second new core router to the ISP's network and configure service connectivity.
 - Step 3: Uninstall the old core router and remove its physical cables.



Implementation: Migration Procedure (1/4)

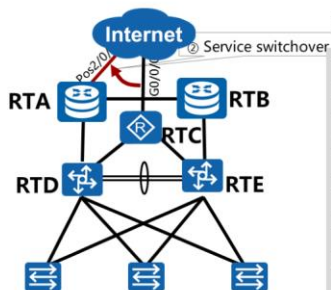
- **Snapshot before the migration**
 - Before the migration, the operation object status (including interface, line, protocol, and traffic information) must be recorded, and configuration files must be backed up again.
- **Migration**
 - Deliver configuration commands or perform physical operations.
 - The execution time of each step must be specified.
- **Check after the migration**
 - Run the **display/ping/tracert** commands or use testers and meters to test the device.

- Snapshot before the migration
 - Record current running status of the device. When a migration failure occurs, you can analyze failure causes and perform rollback quickly.
- Migration
 - Deliver commands one by one or in a batch based on actual network environments.
 - When performing physical operations, pay attention to personal safety, protect devices and lines, and exercise caution in every detail.
- Check after the migration
 - After the migration, use multiple sets of methods to conduct a test. Do not determine the migration result using only one testing method. If the customer's requirement is high, observe network stability for a certain period.



Implementation: Migration Procedure (2/4)

- In this example, phase 2 service switchover is the key point. This phase can be performed as follows:



1. Snapshot (June 8, 2016, 02:30–02:35)

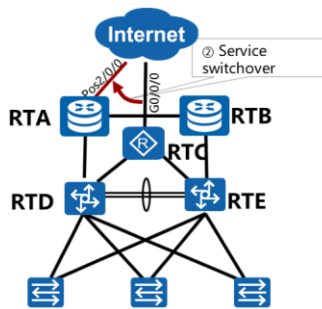
```
<RTC>display ip routing-table #Check route
information.
<RTC>display time-range all #Check the configured
time range information.
<RTC>display log all #Check user operation records.
<RTC>display device #Check device component status
information.
<RTC>display version #Check device version
information.
<RTC>display ospf peer #Check device neighbor
information.
<RTC>display acl all #Check access control
information.
...
```

- In this example, snapshot of network environment information must be collected. Here, the commands on RTC are used as an example. Commands on other routers are similar.

- Snapshot
 - In this example, before delivering migration commands, collect current configuration information and status of RTC, RTD, RTE, or other related routers, especially information related to the network environment.



Implementation: Migration Procedure (3/4)



2. Migration (June 8, 2016, 02:35–02:40)

```
[RTA]ip route-static 0.0.0.0 0.0.0.0
pos2/0/0
#Configure a default route to the Internet
on RTA.
[RTA-ospf-1]default-route-advertise cost 5
#Configure RTA to advertise the default
route to the Open Shortest Path First (OSPF)
routing domain.
```

3. Verification (June 8, 2016, 02:40–02:45)

```
<RTD>display ip routing-table #Check route
information.
<RTD>display ospf lsdb ase 0.0.0.0
#Check the default routes in the OSPF
database.
```

- Set the cost to 5 when advertising the default route, so that RTC is still the egress of network services.
- RTA is still not the egress of network services, but it has "penetrated into" the OSPF database.

• Migration

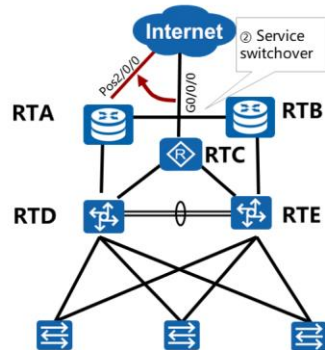
- In this example, configure a default route to the Internet on RTA. Then configure RTA to advertise the default route to the Open Shortest Path First (OSPF) routing domain so that all routers on the network can learn the route. You can use one of the three configuration methods:
 - Configure RTA to advertise a new default route with a priority lower than that of the original default route. For example, run the **[RTA-ospf-1]default-route-advertise type 2** command. The priority of a Type 2 external route is lower than that of a Type 1 external route, so the new route delivered by RTA will not be selected.
 - Configure RTA to advertise a new default route with a cost higher than that of the original default route. Although the new default route will not preempt the original default route immediately, it is saved in the OSPF link state database (LSDB) as a backup route ready to preempt the original default route anytime. (This configuration method is used in this example.)
 - Configure RTA to advertise a new default route with the same cost as the original default route. The two default routes implement load balancing. However, traffic paths cannot be identified. Therefore, this configuration method is not recommended.

• Verification

- Check the routing tables of RTD and RTE to verify that their default routes are destined for RTC.
- Check the LSDBs of OSPF of RTD and RTE to verify that both RTC and RTA have generated Type 5 LSAs of default routes.



Implementation: Migration Procedure (4/4)



4. Migration (June 8, 2016, 02:45–

```
[RTC-ospf-1]undo default-route-advertise  
#Cancel the default route advertised by RTC  
to the OSPF routing domain.
```

5. Verification (June 8, 2016, 02:50–

```
<RTD>display ip routing-table #Check route  
information.  
<RTD>tracert 119.145.15.60 #Verify traffic  
paths.  
If the migration fails, perform a rollback.
```

6. Rollback (June 8, 2016, 03:10–03:15)

- Migration
 - Disable the advertisement of the default route on the original route egress RTC. RTD and RTE do not have a default route to RTC, and the default route to RTA is added to their IP routing table immediately.
- Verification
 - Check the routing tables of RTD and RTE. If their default routes to the Internet are destined for RTA, run the **tracert** command to trace the data layer traffic path. If the traffic passes through RTA before reaching the network egress, test user services. If services are available, the migration is successful. If not, perform a rollback.



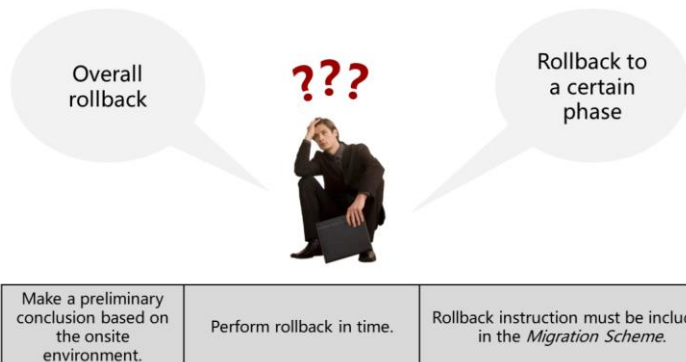
Rollback

- Definition
 - Rollback is to restore the status before the change.
- Scenario
 - When the migration or one step fails, rollback must be performed.
- Example

6. Rollback (June 8, 2016, 03:10–
[RTC-ospf-1]default-route-advertise
#Configure RTC to advertise the default route to all
routers on the network again.
- Requirement
 - For each small migration procedure, the last item must be the rollback instruction.



Rollback Time



- In this example, the migration procedure is divided into three phases. Rollback requirements and execution time should be specified for each phase.



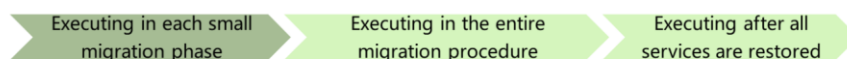
Rollback Failure

- Normally, when the migration fails, the network can be rolled back to the original status.
- If the migration failure is caused by force majeure and rollback cannot be performed, the emergency response plan can be executed.
- Emergency response plan must be included in the Migration Scheme.
- The emergency response plan should contain the following workarounds: system software reloading, onsite spare part replacement, and emergent device invoking.



Test

Network running status test	Network service status test	Customer's application service test
Check device running status.	Test service connectivity.	Test customer's upper-layer application services.
Check protocol status.	Test service performance.	Observe stability.



- The test is passed only when customer's application service requirements are met.

- Network running status test
 - Run the **display** command to check device status including device versions, logs, interfaces, neighbor relationships in protocols, routing tables, and feature status (such as NAT, VRRP, NQA, VPN, and QoS).
- Network service status test
 - Run the **ping** command to test service connectivity. Run the **tracert** command to trace service paths. Use third-party software or network analyzer (such as SmartBits and IXIA tester) to check whether service bandwidths and delays meet requirements.
- Customer's application service test
 - After the migration, the customer should test running status of upper-layer services. If the customer has special requirements on test indicators, adjust the network to meet the requirements.



Site Attendance

- After the migration is complete and the test on customer's application services is passed, the network enters a special observation period. During this period, engineers usually reside on the customer site and observe network running status to prevent faults.

24 hours	One week	One month
----------	----------	-----------

Negotiate with the customer to
determine the attendance duration.



Migration Acceptance



Transfer-to-
maintenance training



Document
handover



Acceptance
summary meeting

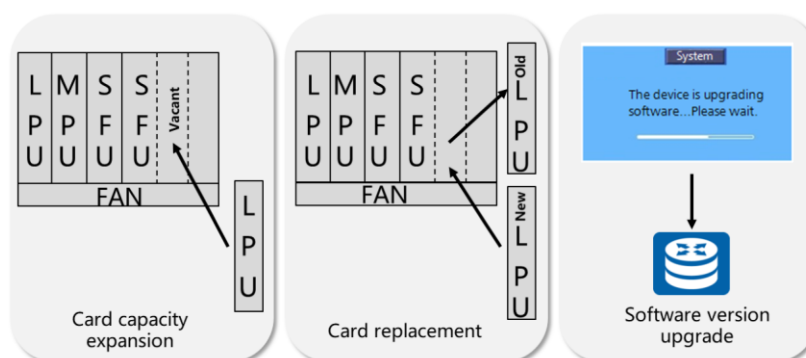


Contents

1. Migration Overview
2. Migration Operation Procedure
3. **Common Migration Scenarios**



Common Migration Scenario: Device Upgrade

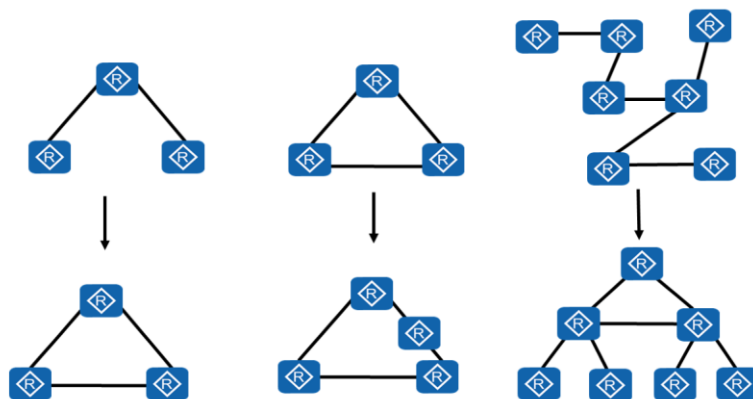


- In this migration scenario, you are advised to contact the vendor for technical support.

- Device upgrade migration
 - Before upgrading a device, check whether the new component version matches the device, whether the software version meets the requirements specified in the version matching table of existing devices, and whether the cards are hot swappable.
 - Device software upgrade must be authorized by the vendor, and official software should be downloaded for upgrade. Prepare physical spare parts and a rollback plan before a device software upgrade.



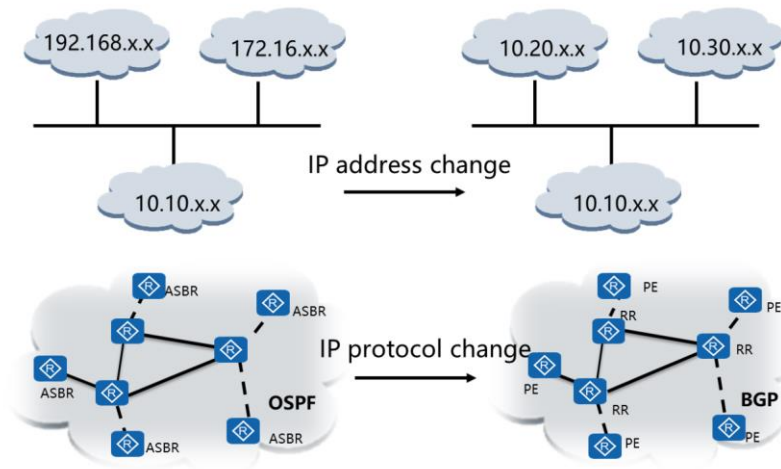
Common Migration Scenario: Physical Structure Reconstruction



- Adding a link
- Adding a device
- Adjusting the structure

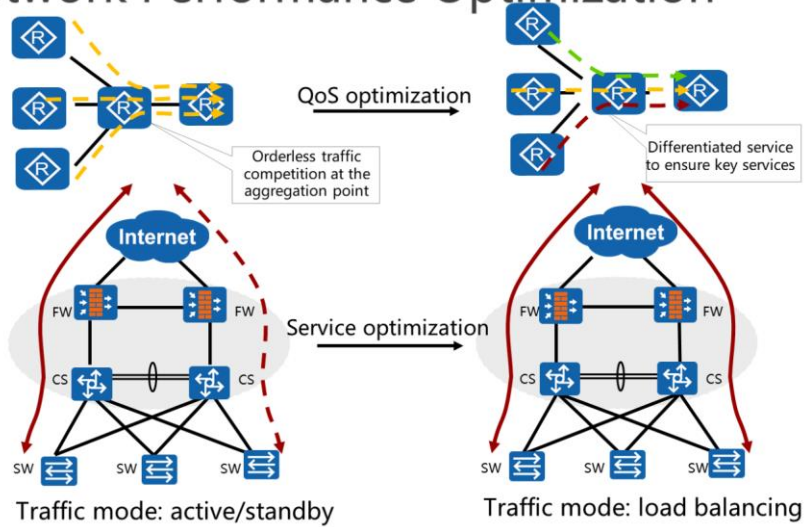


Common Migration Scenario: Network System Adjustment



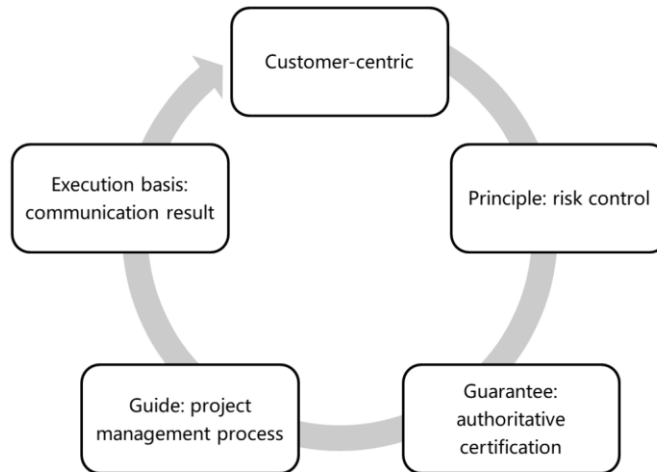


Common Migration Scenario: Network Performance Optimization





Migration Summary





Quiz

1. Which methods can be used in the migration scheme verification and review?
2. The three specific migration steps are ().
3. What can we do to prevent risks caused by a migration failure?

- Answer: FOA deployment, technical review of all parties, and vendor expert reviews.
- Answer: Snapshot before the migration, migration, and check after the migration.
- Answer: If a migration failure occurs, perform a rollback. If the rollback fails, execute the emergency response plan.



Thank You

www.huawei.com



Recommendations

- Huawei Learning Website
 - <http://learning.huawei.com/en>
- Huawei e-Learning
 - <https://ilearningx.huawei.com/portal/#/portal/EBG/51>
- Huawei Certification
 - <http://support.huawei.com/learning/NavigationAction!createNavi?navId= 31&lang=en>
- Find Training
 - <http://support.huawei.com/learning/NavigationAction!createNavi?navId= trainingsearch&lang=en>



More Information

- Huawei learning APP

