Network Migration

Foreword

- With the development of enterprise services, enterprise networks need to be reconstructed and optimized to meet service requirements. For example, IPv4 networks need to be upgraded to IPv6 networks, Intermediate System-to-Intermediate System (IS-IS) levels need to be modified, and the virtual private network (VPN) architecture needs to be modified. Regardless of hardware capacity expansion, software upgrade, and configuration change, enterprises formulate strict operation processes and risk mitigation measures based on service security level requirements for operations that affect services on the live network (for example, service interruption), and define these operations as migration projects.
- This course introduces the migration process, operation specifications, and risk control measures, and describes how to efficiently and smoothly complete network migration.

Objectives

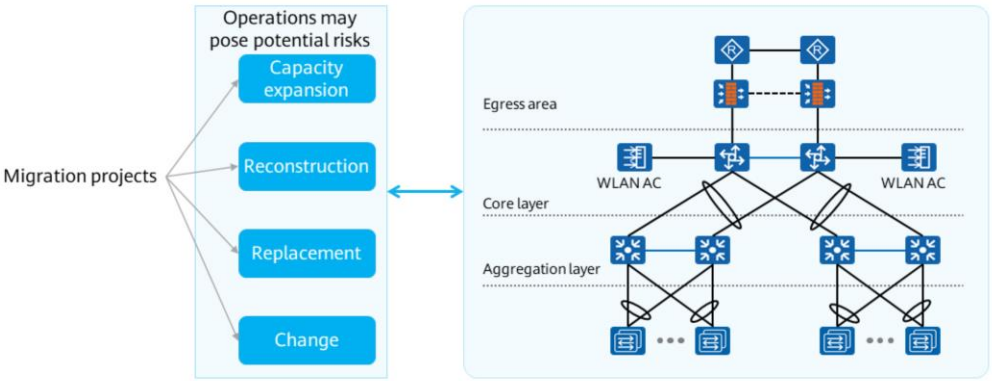
- Upon completion of this course, you will be able to:
  - Clarify the operation procedure and specifications of the migration.
  - Describe common migration scenarios.

Contents

HUAWEI

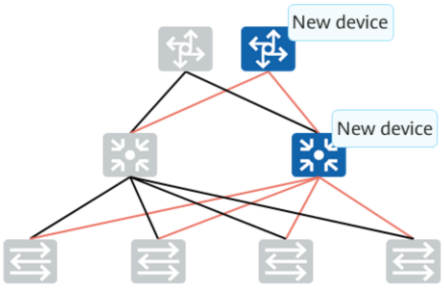
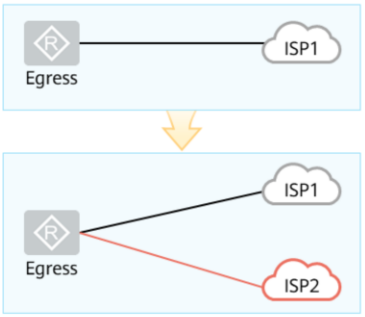
Basic Concepts

Migration project: If the technical migration performed on the network affects the services running on the live network, strictly comply with the preset operation process and risk control measures during the implementation of the technical migration project. Generally, this type of project is defined as a migration project.



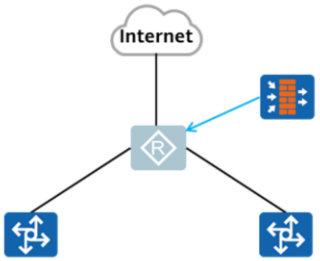
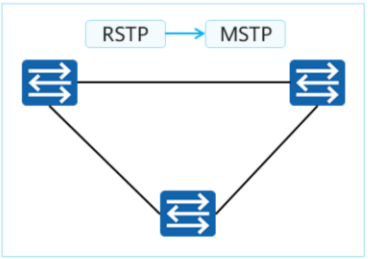
Common Migration Scenarios (1)

As service traffic increases, network devices and links need to be added to expand the network capacity.

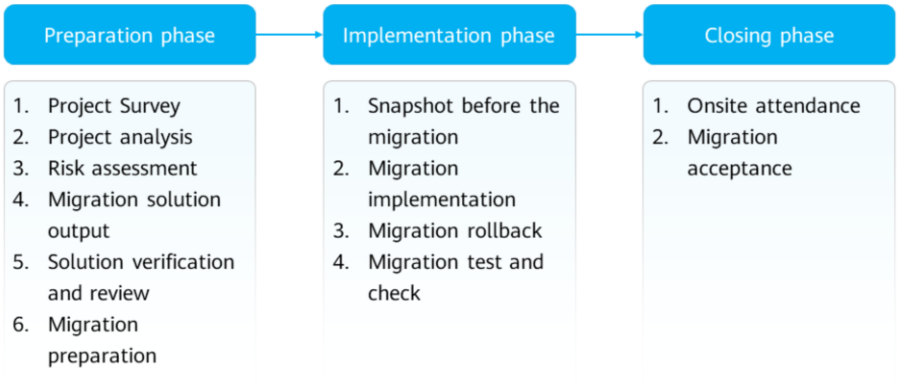
Network capacity expansion	Network reconstruction
	 The network architecture, including the physical architecture and logical architecture, needs to be adjusted.

Common Migration Scenarios (2)

Replace old devices with new devices, devices from other vendors, or devices of other types.

Device replacement	Configuration change
	 If you change the device configuration without changing the physical topology, the running services may be affected.

Migration Process



Contents

Project Investigation

- **Project survey**
- Project analysis
- Risk assessment
- Migration solution output
- Solution verification and review

Before the migration, communicate with the customer network information owner, frontline maintenance engineers, ISP technical contact person, and device vendor representatives, and collect customer network information.

Static information collection and analysis	Dynamic information analysis
Service model analysis	Hardware environment survey on the live network

Information Collection and Analysis

- **Project survey**
- Project analysis
- Risk assessment
- Migration solution output
- Solution verification and review

Static and dynamic information on the live network is used to analyze the network status and compare the network status before and after the migration to determine whether the service volume is normal before and after the migration.

Static information collection and analysis

Detailed topology information	Device type	License
Device configuration	Device version	Interface type

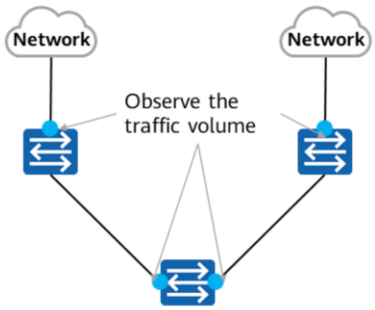
Dynamic information collection and analysis

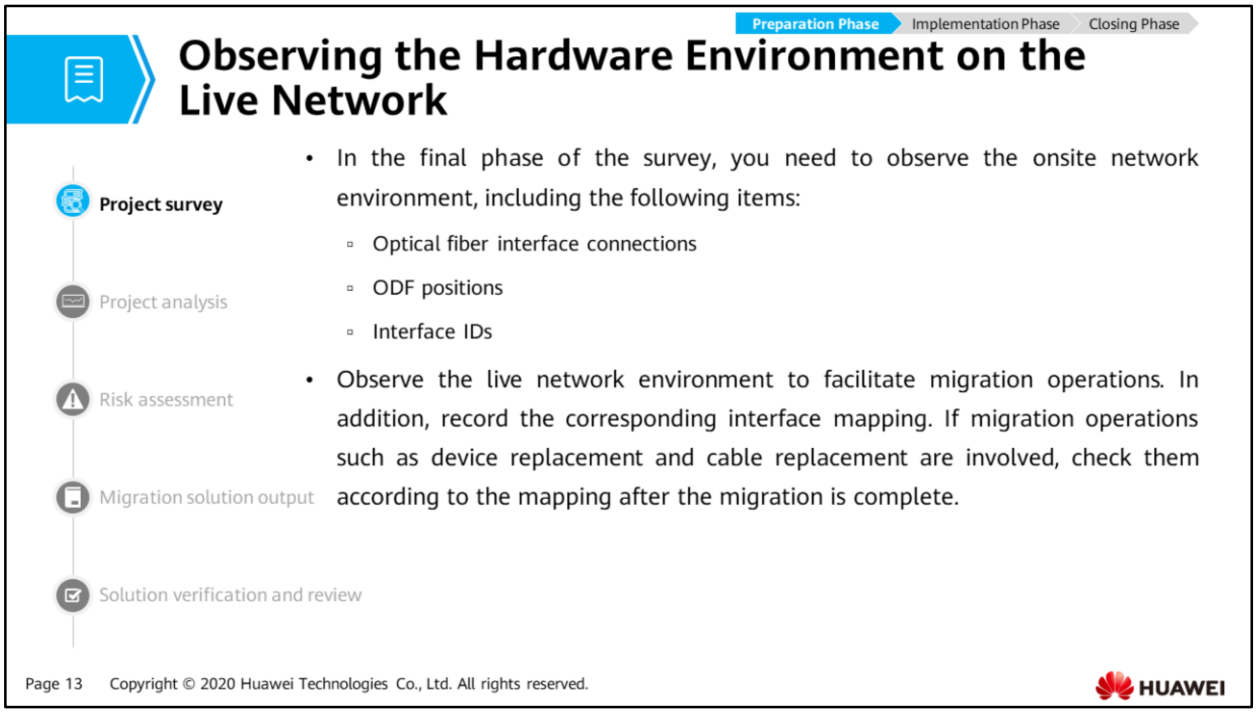
Network traffic	Bandwidth information	Protocol status
Protocol entry	Latency and jitter	Packet loss rate

Traffic Model Analysis

- **Project survey**
- Project analysis
- Risk assessment
- Migration solution output
- Solution verification and review

In the project survey phase, observe the customer's service traffic direction and volume, including the traffic direction change and link traffic volume, which can be used for comparison before and after the migration.





- The optical distribution frame (ODF) is mainly used on backbone networks, metropolitan area networks (MANs), and optical fiber and cable networks. It connects, terminates, distributes, splits, and schedules backbone optical cables.

Project Analysis

- Project survey
- **Project analysis**
- Risk assessment
- Migration solution output
- Solution verification and review

- After the project survey is complete, analyze the customer's new requirements on the network after the migration, such as the bandwidth, network KPIs, and new service bearer capability.
- In addition, clarify the migration change requirements in the migration solution in this phase.
- Output the Customer Requirement Analysis Form.

Risk Assessment

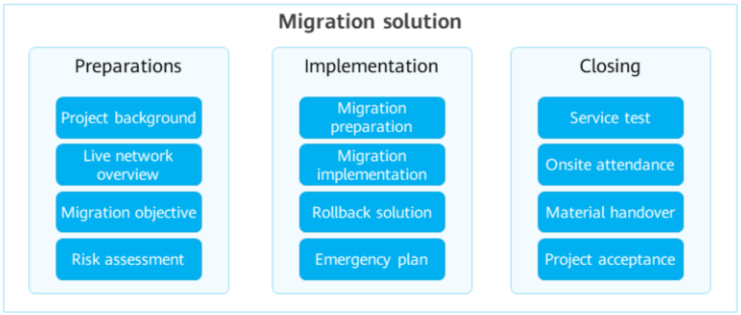
Project survey
Project analysis
Risk assessment
Migration solution output
Solution verification and review

- Analyze and evaluate migration risks based on the survey result, requirement analysis result, and cutover solution framework, formulate countermeasures for projects with potential risks in advance, and confirm the owners of the countermeasures for corresponding risk items.
- The technical personnel involved in the risk assessment need to participate in the discussion, and the specific technical personnel needs to be specified for each risk.

Migration Solution Output

Project survey
Project analysis
Risk assessment
Migration solution output
Solution verification and review

- Formulate the migration solution based on the survey result, project analysis result, and risk evaluation of technical personnel.
- In the migration solution, the detailed steps and procedures of the preparation, implementation, and closing phases must be specified.



Implementation Solution

- Project survey
- Project analysis
- Risk assessment
- **Migration solution output**
- Solution verification and review

- To implement efficient and standard migration, plan each step in advance, including the specific action, specific command lines, and time required for performing each step.
- In the migration implementation solution, prepare the corresponding migration operation confirmation record table. The table records the operation time, confirmation result after operations are performed, and exception information.

Migration solution

Migration Procedure

Step	Operation	Time
Power off old devices.	Power off old devices and remove cables.	0:00-0:30
Deploy devices on the rack.	Power on new devices and connect cables.	0:30-1:00
Configure new devices.	Import the pre-configured script to the new device.	1:00-1:20
Check the network status.	Check network entries.	1:20-2:00
Test services.	Coordinate Party A's personnel to test services and applications.	2:00-2:30

Rollback Solution

- Project survey
- Project analysis
- Risk assessment
- **Migration solution output**
- Solution verification and review

- Rollback solution: If the migration fails (for example, service test fails after the migration or the migration is not complete after the migration time), roll back the network to the status before the migration. In this case, perform operations according to the rollback solution to restore the network.
- A detailed rollback solution must be included in the migration solution. Similar to migration operations, each step in the rollback solution must be specified. In this way, rollback can be performed in an orderly manner when the migration fails.

Migration plan

Rollback Procedure

Step	Operation	Time
Remove new devices.	Power off new devices and remove cables.	3:00-3:20
Place the old devices on the rack.	Power on the old devices and connect cables.	3:20-3:40
Test services.	Coordinate Party A's personnel to test services and applications.	3:50-4:00

Solution Verification and Review

Project survey
Project analysis
Risk assessment
Migration solution output
Solution verification and review

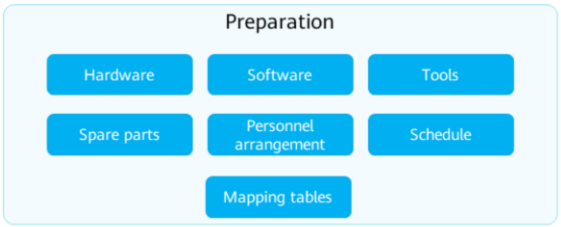
- For large-scale and important migration projects, an environment must be set up in the lab for verification in advance. The previous risk points must be tested and the feasibility of the entire solution must be confirmed. This type of verification in the lab environment is called the pilot office test.
- In addition to FOA solution verification, a technical review meeting needs to be held with the customer and implementation party to verify the technologies in the migration solution so as to understand actual requirements and difficulties of both parties, and solve problems face to face.

Customer network　　Pilot office test

Migration Preparation

- Project analysis
- Risk assessment
- Migration solution output
- Solution verification and review
- **Migration preparation**

- 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 arrangement). All aspects should be considered to ensure migration success.



Software and Hardware Preparation

- Project analysis
- Risk assessment
- Migration solution output
- Solution verification and review
- **Migration preparation**

Hardware

Device	Power-on test
Board	Check whether the tested board is normal.
Cable	Connectivity test

Software

Versions	Check the device version and interconnection version mapping.
License	Check whether the authorized license is available.
Scripts	Overall script, segment configuration script, and rollback script

Tool and Spare Part Preparation

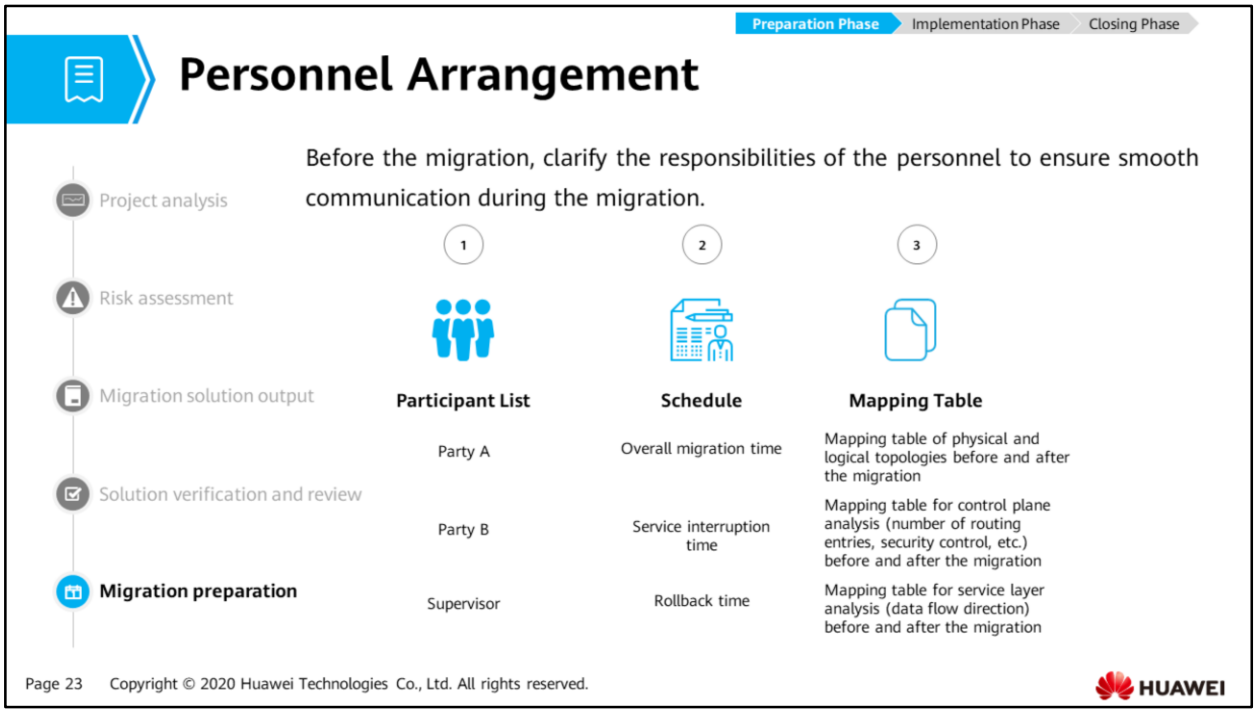
- Project analysis
- Risk assessment
- Migration solution output
- Solution verification and review
- **Migration preparation**

Tools

Transportation tools	Vehicles, landing tools, and installation tools
Test tools	Network cable tester, network tester, and optical power meter
Debugging tools	PC terminal and debugging software CRT
Monitoring tools	Service monitoring tool, traffic monitoring platform, and network analysis tool

Spare parts

- Important boards and device spare parts
- Backup of software of old and new versions
- Backup of old and new scripts



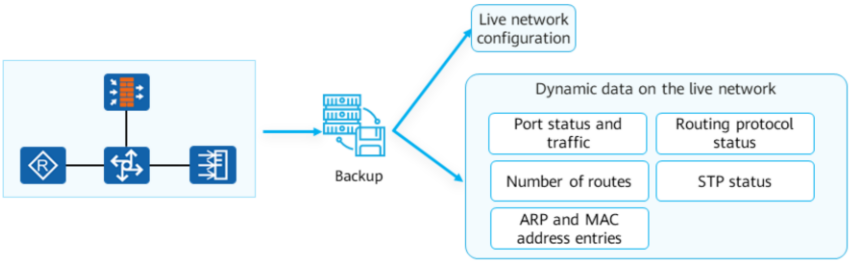
- Time arrangement preparation:
  - Negotiate the time arrangement with the customer and obtain customer's approval.
  - Make an overall time schedule.
  - Specify actions to be performed in each time segment.
  - In the migration phase, time arrangement should be accurate to minutes.
  - Reserve some time for major operations to avoid engineering accidents due to timeout.
  - Do not perform migration in peak hours (such as holidays and off-duty time).

Snapshot Before the Migration

- **Snapshot before the migration**
- Migration implementation
- Migration rollback
- Migration test and check

To facilitate migration rollback and service comparison after the migration, you need to take snapshots of the live network configuration and data before the migration.

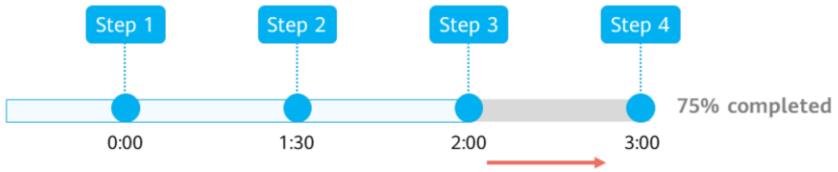
- Back up live network configuration.
- Collect dynamic data on the live network, including the port status, traffic, routing protocol status, number of routes, STP status, and ARP/MAC address entries of each interface.
- Test services before the migration to ensure that the services involved in the migration are normal.



Migration Implementation

- Snapshot before the migration
- **Migration implementation**
- Migration rollback
- Migration test

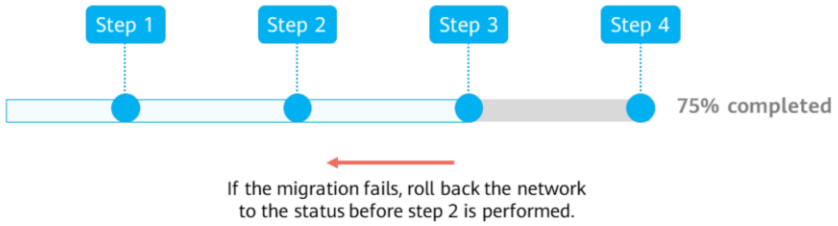
- The onsite migration personnel must strictly follow the prepared migration procedure. The implementation procedure cannot be changed temporarily unless there are special reasons.
- Record the time, actions, and results of each step.



Migration Rollback

- Snapshot before the migration
- Migration implementation
- **Migration rollback**
- Migration test and check

- If the migration is not complete before the specified time, perform the rollback step by step according to the prepared rollback scheme to restore the network.
- You can negotiate with the customer to determine whether to perform partial or full rollback based on the actual situation.

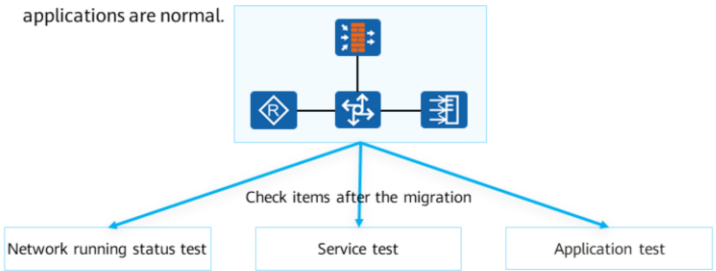


Migration test

- Snapshot before the migration
- Migration implementation
- Migration rollback
- **Migration test and check**

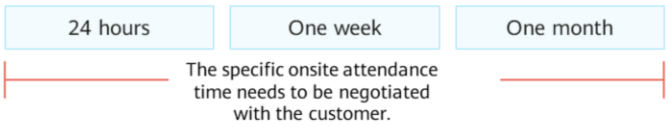
After the migration is complete, you need to test the network and services from the following aspects to check whether the migration is successful:

- Network running status test: Collect dynamic data on the live network and compare the data with that before the migration.
- Service test: Perform the ping or tracert operation or use third-party software on the client side to check whether the network connectivity, delay, and jitter meet service requirements.
- Customer application test: Test customer applications carried by the network and check whether applications are normal.



Onsite Attendance

After the migration is complete and the customer's application service test is passed, the network enters a special observation period. During this period, engineers usually stay at the customer's site and observe the network running status to prevent unexpected faults.



Migration Acceptance

After the migration is complete and no exception occurs, we need to provide maintenance training for the customer and hand over documents to the customer.

Transfer-to-maintenance training

If the migration project involves new devices and new configurations, organize training for the customer after the migration is complete.

Material handover

To facilitate subsequent maintenance, transfer the documents involved in the migration to the customer after the migration is complete.

Contents

Migration Cases — Precautions

- The key point is to master the migration process and method based on actual migration cases, in addition to device configuration planning required by the migration.
- Discuss migration scenarios based on the migration process and output the migration document based on the Project Migration Solution Template. The document includes the following contents:
  - Project survey and analysis: Analyze the live network topology and services, and identify the devices whose dynamic and static information needs to be collected.
  - Risk evaluation: Evaluate the risks that may occur during the migration and how to avoid the risks.
  - Migration solution: Specify the commands to be executed in each step and the time point of each step.
  - Test and check items: Determine the contents to be checked and tested after the migration.

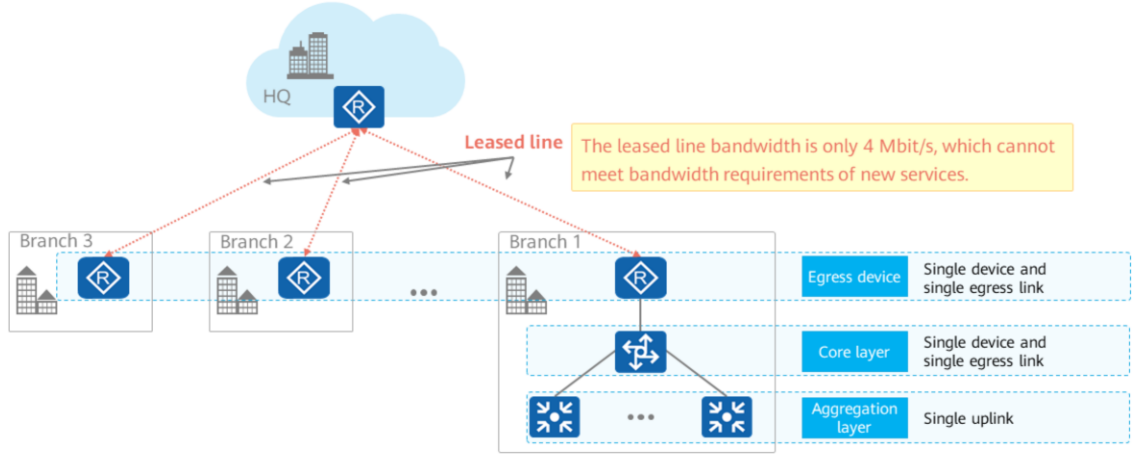
Class Activities

Background 15 minutes	• The teacher introduces the scenario of the migration case, inputs the topology diagram and service planning, and conducts group discussion, make a summary, and output the migration cutover process, and cutover-related documents).
Grouping communication 5 minutes	• Each group discusses and selects a team leader. The team leader is responsible for the final summary and report.
Discussion 30 minutes	• Each group discusses the migration procedure, designs the contents to be configured, and outputs the migration document.
Summary 20 minutes	• Each group reports the discussion results and submits related documents.

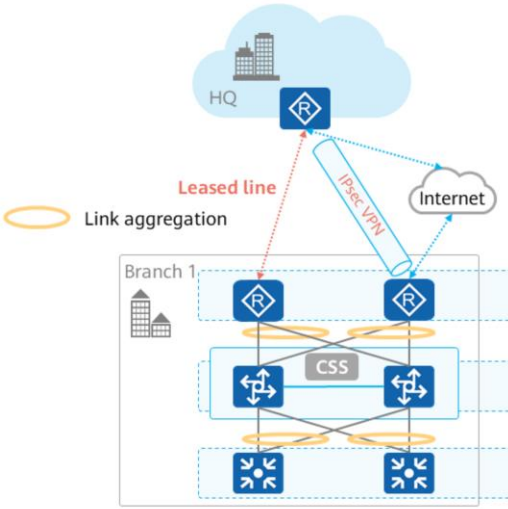
Introduction to the Early Stage of the Reconstruction Project

- A company has multiple branches that are connected to the headquarters network through leased lines. The following problems exist:
  - The leased line rate is low and cannot meet bandwidth-intensive requirements of new services.
  - A single egress device and a single uplink (leased line) are deployed at the egress of a branch, which may cause a single point of failure (SPOF).
  - Increasing the leased line rate causes a high cost.
  - The standalone core switch is deployed, which may cause an SPOF.
  - The performance of core switches and egress routers cannot provide good support for increasing end users in branches.
- To solve the problems, the company decides to reconstruct the branch network to improve the reliability of the branch network and increase the bandwidth for communication with the headquarters.

Original Topology



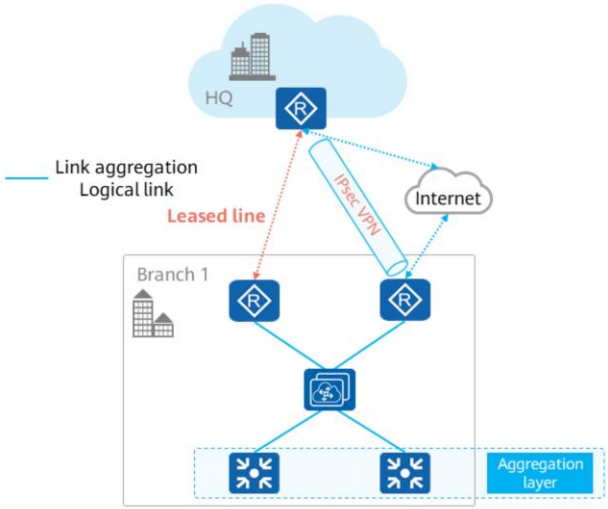
Target Topology



Device redundancy and link redundancy are used to improve reliability. Internet connections are added at the egress, and IPsec VPNs are established with the headquarters to carry services that demand low delay and high bandwidth.

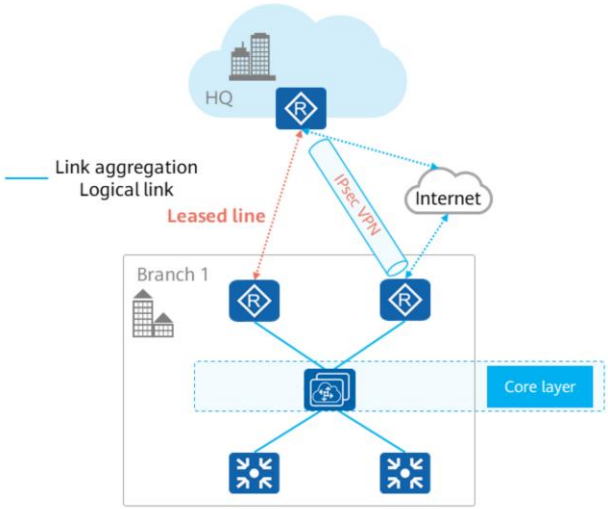
Egress device	Add an Internet connection and establish an IPsec VPN to carry some services.
Core layer	The CSS composed of core switches establishes inter-chassis link aggregation with uplink and downlink devices.
Aggregation layer	Dual uplinks set up a link aggregation group with the CSS composed of core switches.

Target Logical Topology (1)



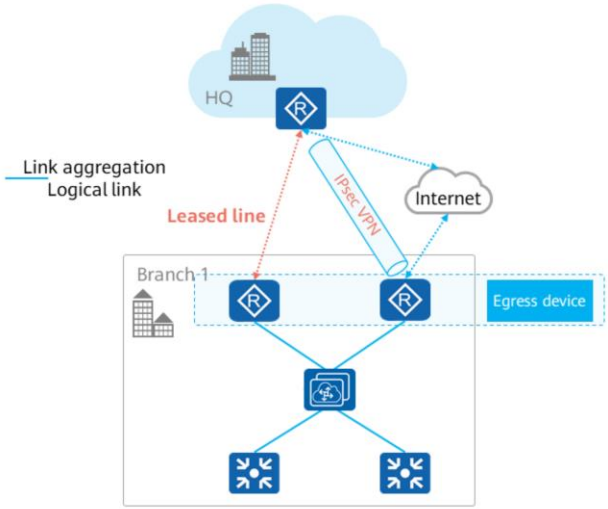
The aggregation layer uses dual uplinks to connect to the CSS composed of core switches.
The gateway is configured on the VLANIF interface of the core switch. The CSS composed of core switches and link aggregation technology are deployed to improve reliability, so VRRP does not need to be deployed.

Target Logical Topology (2)



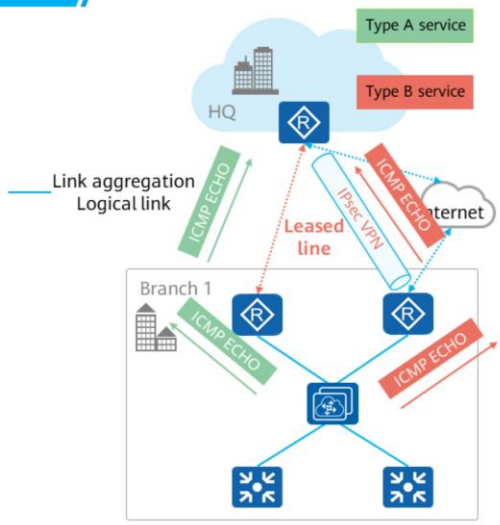
The core device serves as the gateway of intranet terminals. Static routes are configured to direct traffic of different services to the leased line and IPsec VPN egress devices, and floating routes are configured for route backup.
NQA is configured to detect the availability of the leased line and IPsec VPN. Static routes are associated with NQA so that traffic can be switched to the backup path when a link fault occurs.

Target Logical Topology (3)



The two egress devices are connected to the leased line and Internet to carry different services. Traffic of intranet terminals' access to different services is forwarded based on routes of the core switch. If the routes change, the traffic forwarding path changes accordingly.

NQA Design



Configure NQA on the core switch to check connectivity between the core switch and the headquarters through the leased line or IPsec VPN, and associate NQA with static routes.

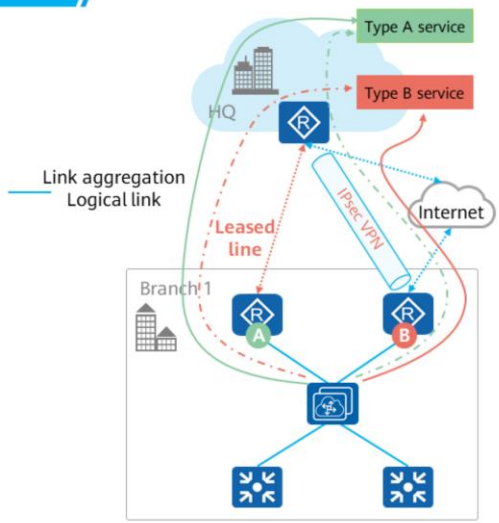
NQA configuration (type A services are used as an example):

```
nqa test-instance service_a icmp
 test-type icmp
 destination-address ipv4 Server address for type A services
 source-address ipv4 IP address of the interface for interconnection between the core switch and the router through the leased line
 source-interface Interface for interconnection between the core switch and the router through the leased line
```


HUAWEI

- Type A service: service demanding low latency and bandwidth. These services are carried over leased lines.
- Type B service: service that has low requirements on the latency but occupies much bandwidth. These services are carried over IPsec VPNs.
- Static return routes are manually specified for the headquarters, and NQA is used to switch services to the standby path upon faults. This case focuses on the branch network and does not involve the headquarters network.

Route Backup Design



Active path of type A service
Active path of type B service
Standby path of type A service
Standby path of type B service

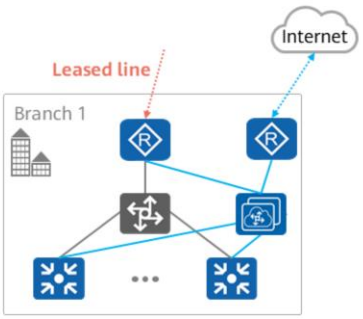
On the core switches, the routes to type A and type B services are destined for different egress devices and carried by different links. Floating routes are configured so that the two egress devices to back up each other.

Association between static routes and NQA on core switches:

ip route-static *IP address of type A service mask A* track *nqa service_a icmp*
ip route-static *IP address of type A service mask B*

ip route-static *IP address of type B service mask B* track *nqa service_b icmp*
ip route-static *IP address of type B service mask A*

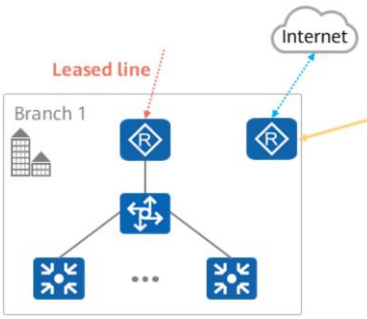
Migration Solution (1)



Perform the following steps to migrate the original network to the target network (overview):

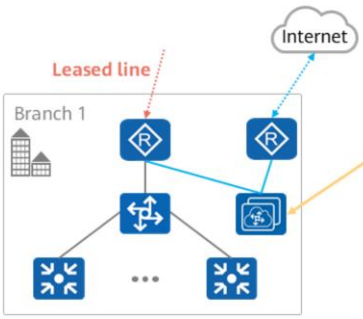
- Deploy a new egress router and connect it to the Internet. Establish an IPsec VPN and configure routes.
- Deploy two new core switches, establish the CSS and routes, and configure inter-chassis aggregation between the core switches and egress routers. In this case, the core switches are not connected to the aggregation switch.
- Disconnect the original core switches from uplink and downlink devices, and connect the aggregation switch to the new core switches.

Migration Solution (2)



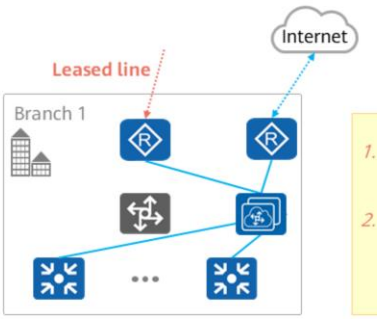
1. *Connect the egress router to the Internet.*
2. *Deploy IPsec VPN with the headquarters.*
3. *Configure routes to network segments of type A and type B services of the headquarters.*
4. *Configure a return route to the intranet.*

Migration Solution (3)



1. *Deploy core switches and configure the CSS.*
2. *Configure routes to network segments of type A and type B services and complete the NQA configuration.*

Migration Solution (4)



1. *Connect the original aggregation switch to the new core switch in the CSS and disconnect the original core switches.*
2. *Modify the configuration of the original egress router and change the next hop of the return route to the intranet to the interconnection address of the new core switch in the CSS.*

HUAWEI

Migration Document Output

Output the *Project Migration Solution Template* based on the preceding migration project information.

Quiz

1. (Essay) What operations can be performed locally to verify risks before the migration?
2. (Essay) Which of the following items must be backed up for the customer network before the migration?

HUAWEI

1. We can set up a local pilot office and simulate the customer's network to verify the feasibility of the entire migration solution.
2. The configuration of the live network needs to be backed up. To verify the network status before and after the migration, collect dynamic data of the live network, including the port status, traffic, status of each routing protocol, number of routes, STP status, and ARP/MAC address entries of each port.

Summary

- The migration changes the network and may affect the customer's services. Therefore, the migration must be based on the customer's requirements to control risks in real time.
- Before the migration, perform survey and verification, and prepare each step in advance. After the migration, verify services. The migration can be successful and efficient only when the migration process is strictly followed.


Thank You
www.huawei.com