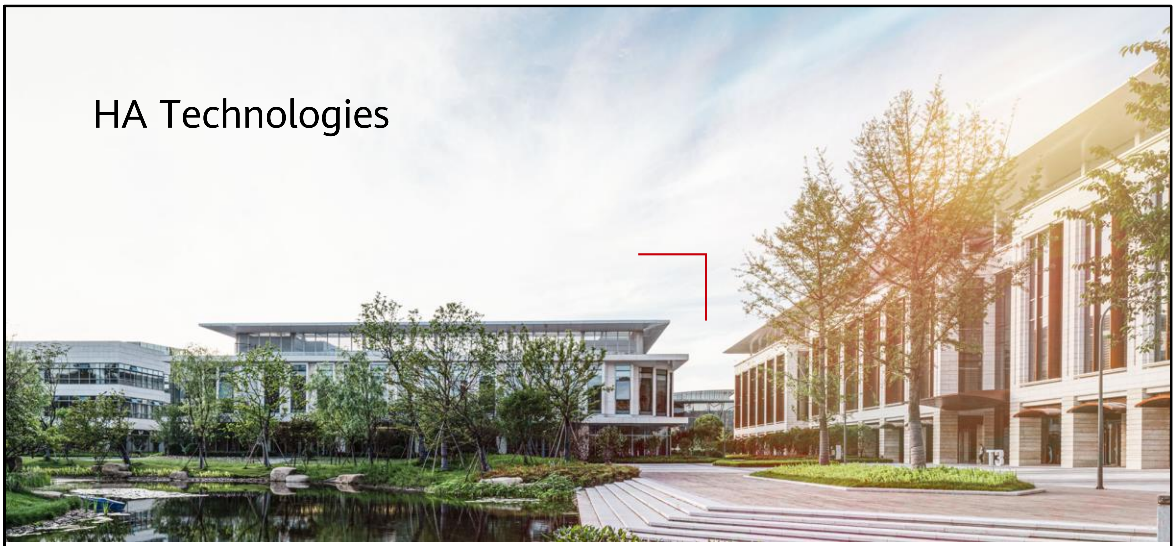
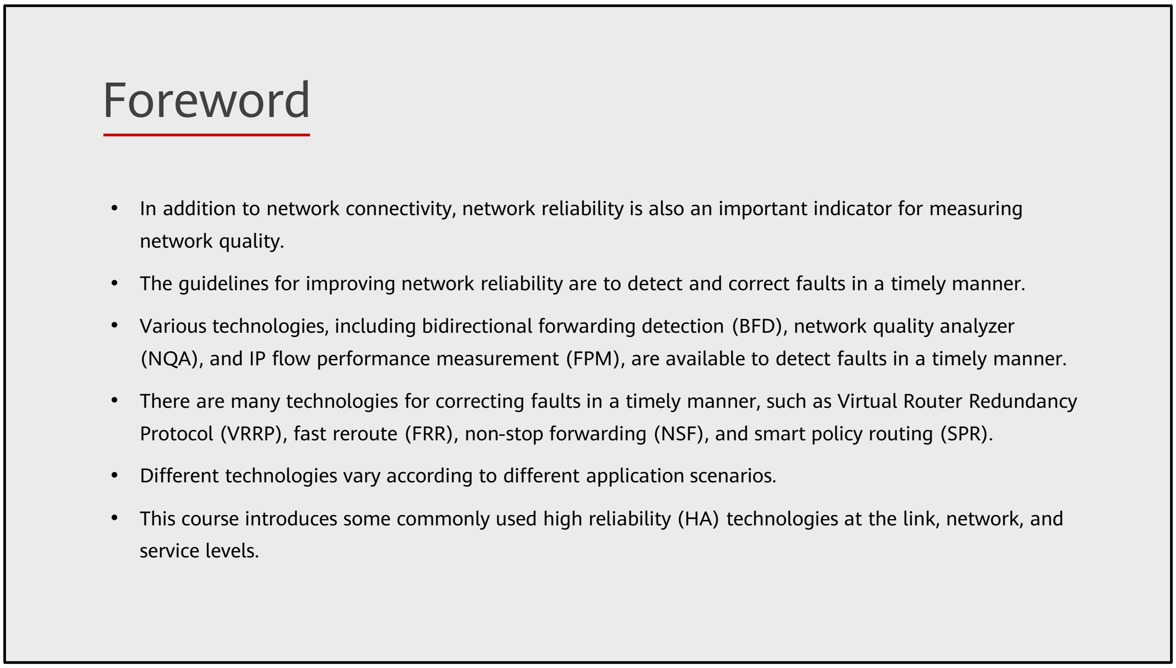
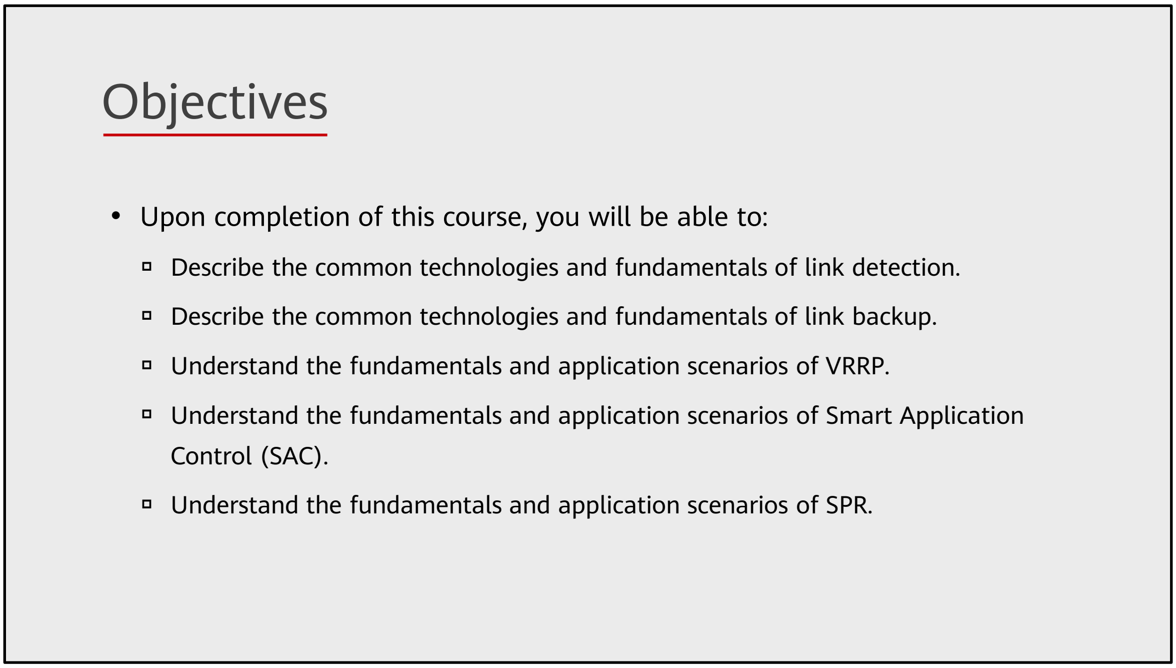
HA Technologies





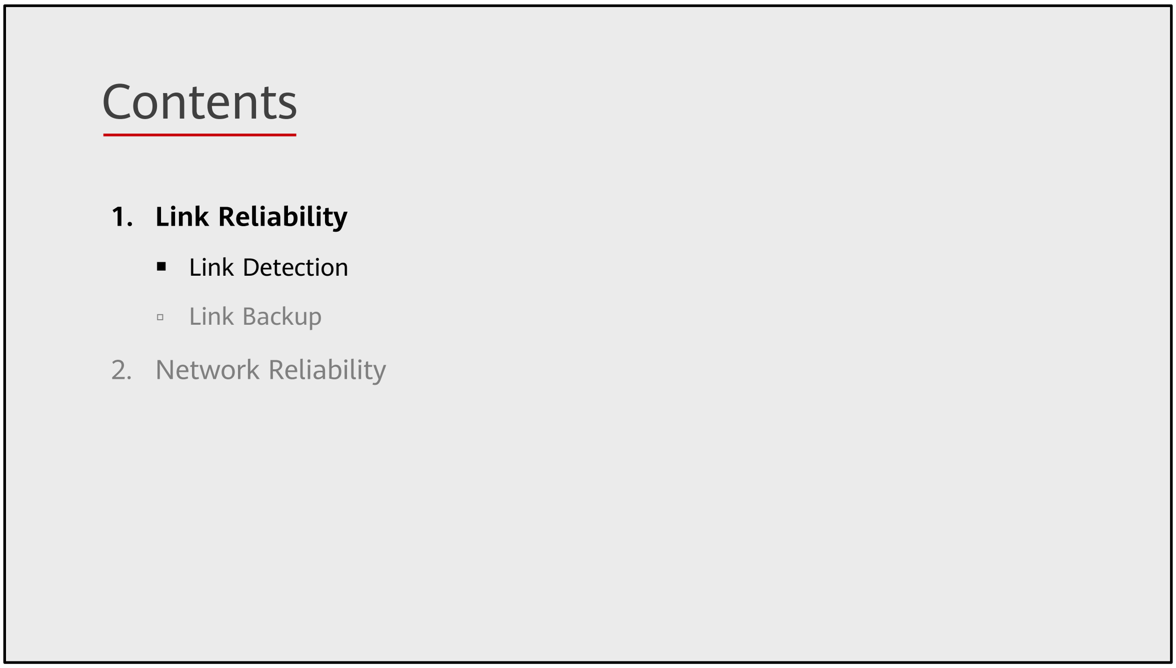
Foreword

- In addition to network connectivity, network reliability is also an important indicator for measuring network quality.
- The guidelines for improving network reliability are to detect and correct faults in a timely manner.
- Various technologies, including bidirectional forwarding detection (BFD), network quality analyzer (NQA), and IP flow performance measurement (FPM), are available to detect faults in a timely manner.
- There are many technologies for correcting faults in a timely manner, such as Virtual Router Redundancy Protocol (VRRP), fast reroute (FRR), non-stop forwarding (NSF), and smart policy routing (SPR).
- Different technologies vary according to different application scenarios.
- This course introduces some commonly used high reliability (HA) technologies at the link, network, and service levels.



Objectives

- Upon completion of this course, you will be able to:
  - Describe the common technologies and fundamentals of link detection.
  - Describe the common technologies and fundamentals of link backup.
  - Understand the fundamentals and application scenarios of VRRP.
  - Understand the fundamentals and application scenarios of Smart Application Control (SAC).
  - Understand the fundamentals and application scenarios of SPR.

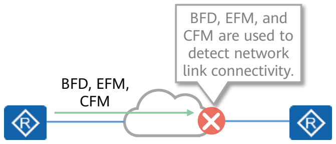


Contents

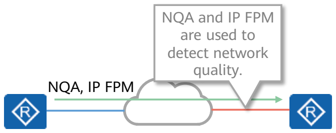
1. **Link Reliability**
   - Link Detection
   - Link Backup
2. Network Reliability

Overview of Link Detection

- Fluctuation of network link quality affects service quality. How to quickly detect link quality is the first step in improving link quality.
- There are many protocols and technologies for detecting link quality, which are classified into two types:
  - Link connectivity detection technologies:
    - BFD
    - Ethernet in the First Mile (EFM)
    - Connectivity Fault Management (CFM)
  - Link quality detection technologies:
    - NQA
    - IP FPM
- On the live network, BFD is typically used to detect link connectivity, and NQA is typically used to detect link quality.



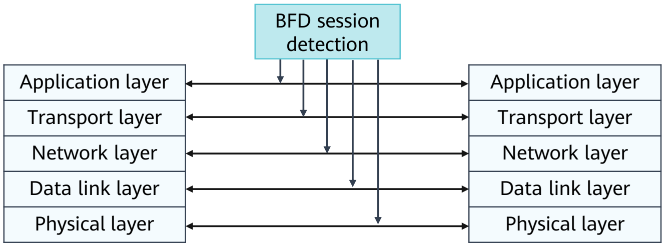
BFD, EFM, and CFM are used to detect network link connectivity.



NQA and IP FPM are used to detect network quality.

BFD

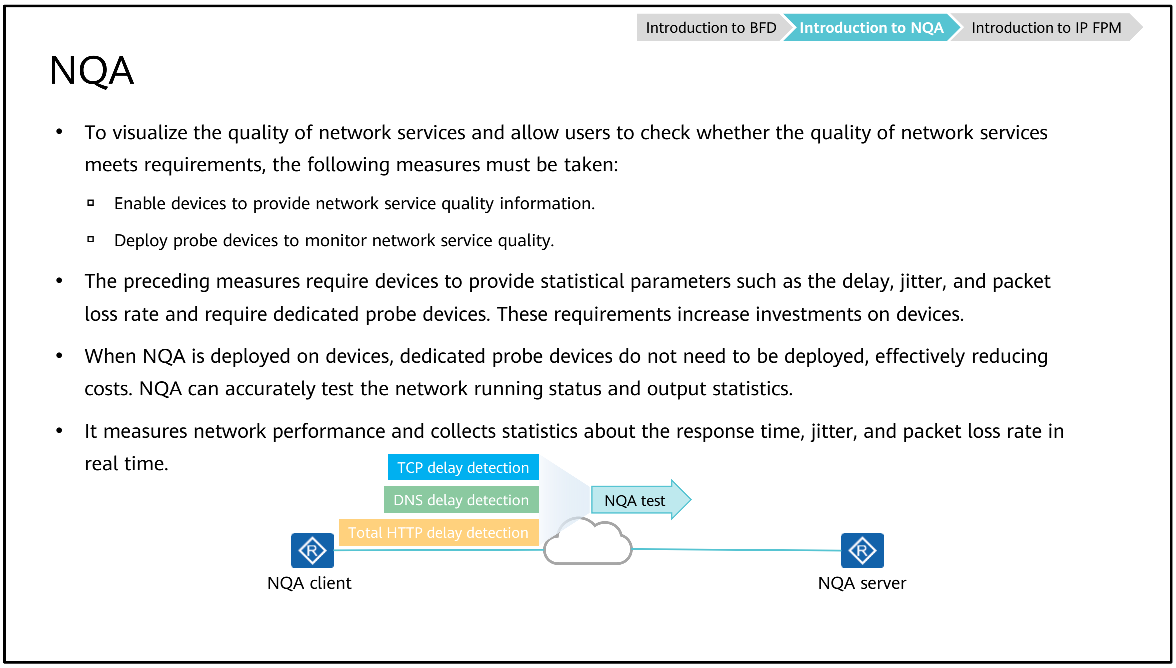
- BFD provides a universal, standardized, media-independent, and protocol-independent fast failure detection mechanism. It has the following advantages:
  - Provides low-overhead and fast failure detection for channels between adjacent forwarding engines.
  - Performs uniform detection for all media and protocol layers in real time.
- BFD is a simple Hello protocol. Two systems establish a BFD session channel and periodically send BFD packets to each other. If one system does not receive BFD packets from the other system within a certain period, the system considers that a fault occurs on the channel.



BFD session detection

Application layer
Transport layer
Network layer
Data link layer
Physical layer

Application layer
Transport layer
Network layer
Data link layer
Physical layer



Introduction to BFD > Introduction to NQA > Introduction to IP FPM

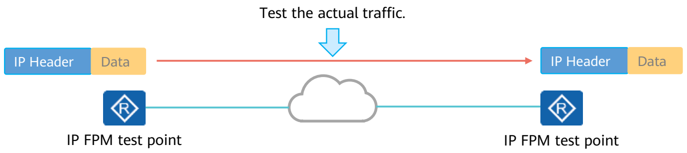
NQA

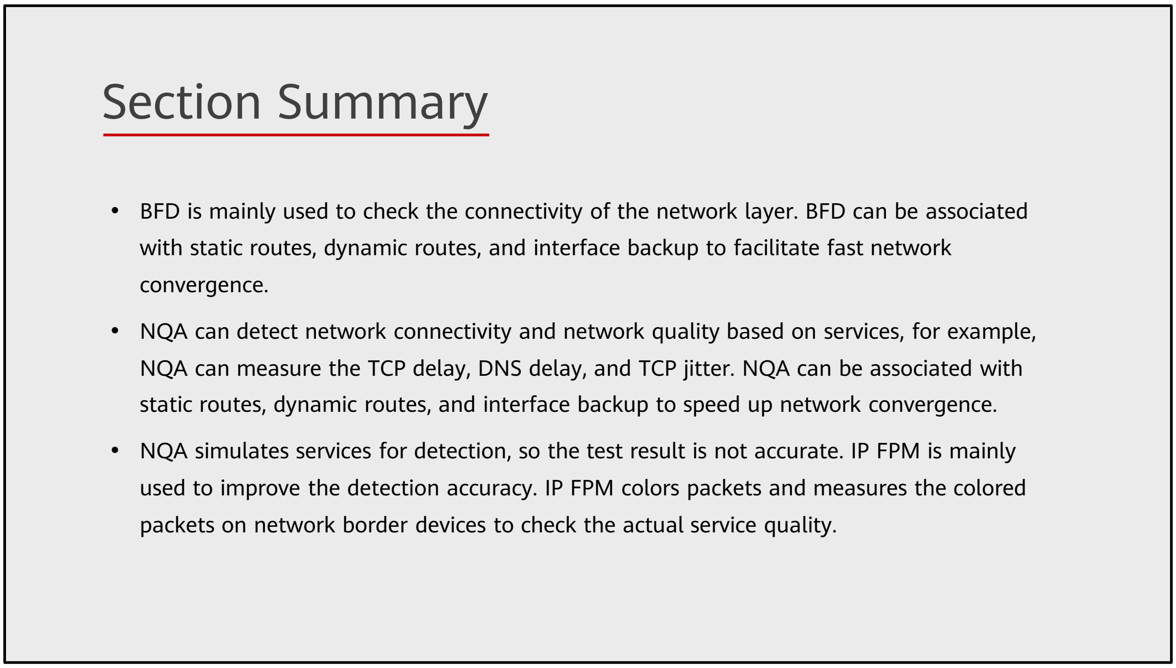
- To visualize the quality of network services and allow users to check whether the quality of network services meets requirements, the following measures must be taken:
  - Enable devices to provide network service quality information.
  - Deploy probe devices to monitor network service quality.
- The preceding measures require devices to provide statistical parameters such as the delay, jitter, and packet loss rate and require dedicated probe devices. These requirements increase investments on devices.
- When NQA is deployed on devices, dedicated probe devices do not need to be deployed, effectively reducing costs. NQA can accurately test the network running status and output statistics.
- It measures network performance and collects statistics about the response time, jitter, and packet loss rate in real time.

- Additionally, NQA measures the performance of different protocols running on the network. This facilitates real-time collection of network performance counters, such as the total HTTP connection delay, TCP connection delay, DNS resolution delay, file transfer rate, FTP connection delay, and DNS resolution error rate.

IP FPM

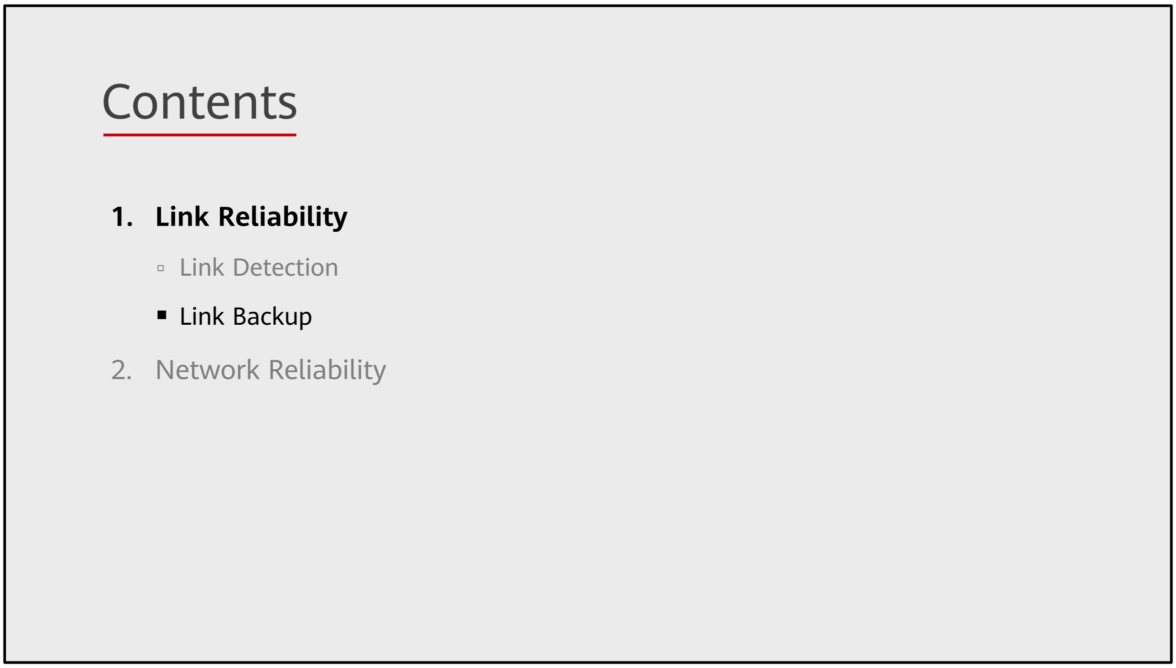
- With the advent of the cloud computing era, end-to-end service performance measurement becomes essential. However, the commonly used NQA technology has the following defects in end-to-end network performance measurement scenarios:
  - NQA simulates service packet forwarding on the network by constructing service packets. Therefore, the collected performance statistics are not accurate.
  - NQA does not support end-to-end performance measurement across network layers, and cannot monitor or measure network performance in a multipath scenario of IP networks.
- IP flow performance measurement (IP FPM) can effectively solve these problems. It is a general IP network performance measurement solution. IP FPM can directly measure service packets, and the measurement data can reflect the performance of IP networks. In addition, IP FPM can monitor the changes of services carried by IP networks online and accurately reflect the running status of services.





Section Summary

- BFD is mainly used to check the connectivity of the network layer. BFD can be associated with static routes, dynamic routes, and interface backup to facilitate fast network convergence.
- NQA can detect network connectivity and network quality based on services, for example, NQA can measure the TCP delay, DNS delay, and TCP jitter. NQA can be associated with static routes, dynamic routes, and interface backup to speed up network convergence.
- NQA simulates services for detection, so the test result is not accurate. IP FPM is mainly used to improve the detection accuracy. IP FPM colors packets and measures the colored packets on network border devices to check the actual service quality.

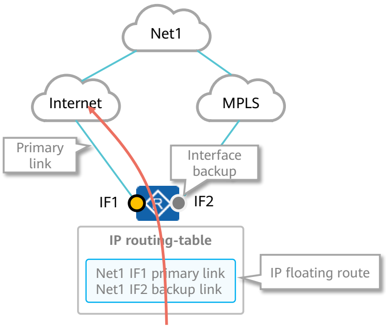


Contents

1. **Link Reliability**
   - ▫ Link Detection
   - ▪ Link Backup
2. Network Reliability

Link Backup

- To ensure reliability, a network egress is typically connected to multiple WAN links in active/standby mode. When one link is faulty (for example, an interface is faulty, the link is faulty, or the link bandwidth is insufficient), services can be immediately switched to another link. To meet this requirement, the following technologies are often used on the live network:
  - Interface backup
  - IP floating route



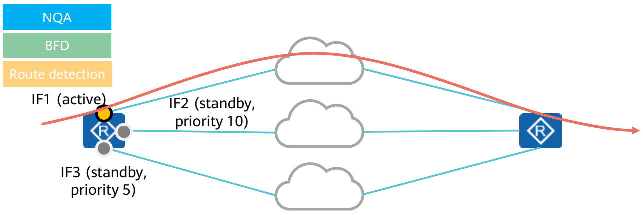
Interface Backup IP Floating Route

Interface Backup

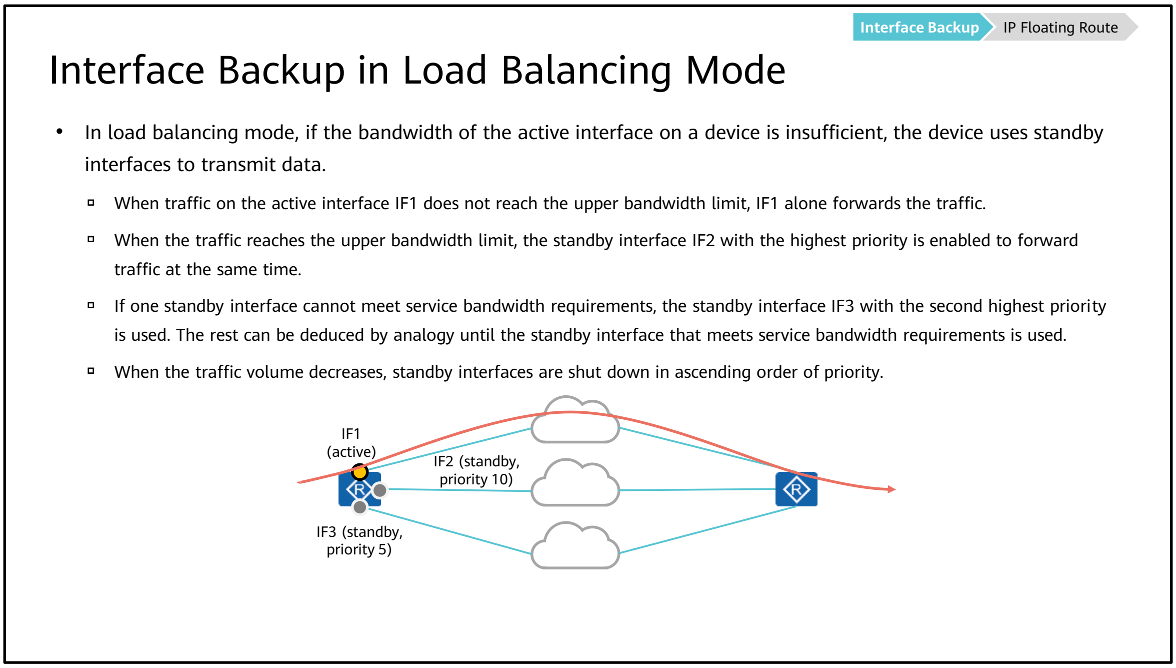
- Interface backup refers to the backup between specific interfaces on the same device. When an interface is faulty or the bandwidth is insufficient, traffic can be fast switched to a standby interface. The standby interface then transmits services or load balances network traffic.
- Interface backup operates in either active/standby or load balancing mode.
  - Interface backup in active/standby mode: One interface is the active interface, and the others are standby interfaces. When the active interface fails or the network quality is poor, a standby interface transmits data.
  - Interface backup in load balancing mode: One interface is the active interface, and the others are standby interfaces. When the bandwidth of the active interface is insufficient, a standby interface is enabled. Then both the active and standby interfaces transmit data.

Interface Backup in Active/Standby Mode

- In active/standby mode, only a single interface transmits services at any time. The mechanism of interface backup in active/standby mode is as follows:
  - When the active interface IF1 is working properly, interfaces IF2 and IF3 are in the standby state.
  - When IF1 is faulty or the link quality does not meet requirements, IF2 with the highest priority enters the forwarding state.
  - After IF1 recovers, traffic is switched back to IF1.



- Interface backup in active/standby mode can detect only faults on direct links but not the remote link status or overall link quality. In this case, interface backup in active/standby mode can be associated with NQA, BFD, or routing tables.



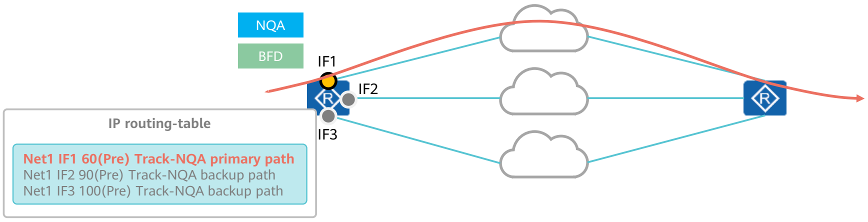
Interface Backup in Load Balancing Mode

- In load balancing mode, if the bandwidth of the active interface on a device is insufficient, the device uses standby interfaces to transmit data.
  - When traffic on the active interface IF1 does not reach the upper bandwidth limit, IF1 alone forwards the traffic.
  - When the traffic reaches the upper bandwidth limit, the standby interface IF2 with the highest priority is enabled to forward traffic at the same time.
  - If one standby interface cannot meet service bandwidth requirements, the standby interface IF3 with the second highest priority is used. The rest can be deduced by analogy until the standby interface that meets service bandwidth requirements is used.
  - When the traffic volume decreases, standby interfaces are shut down in ascending order of priority.

- Interface backup in load balancing mode is implemented only based on interface bandwidth usage and cannot be associated with BFD or NQA.

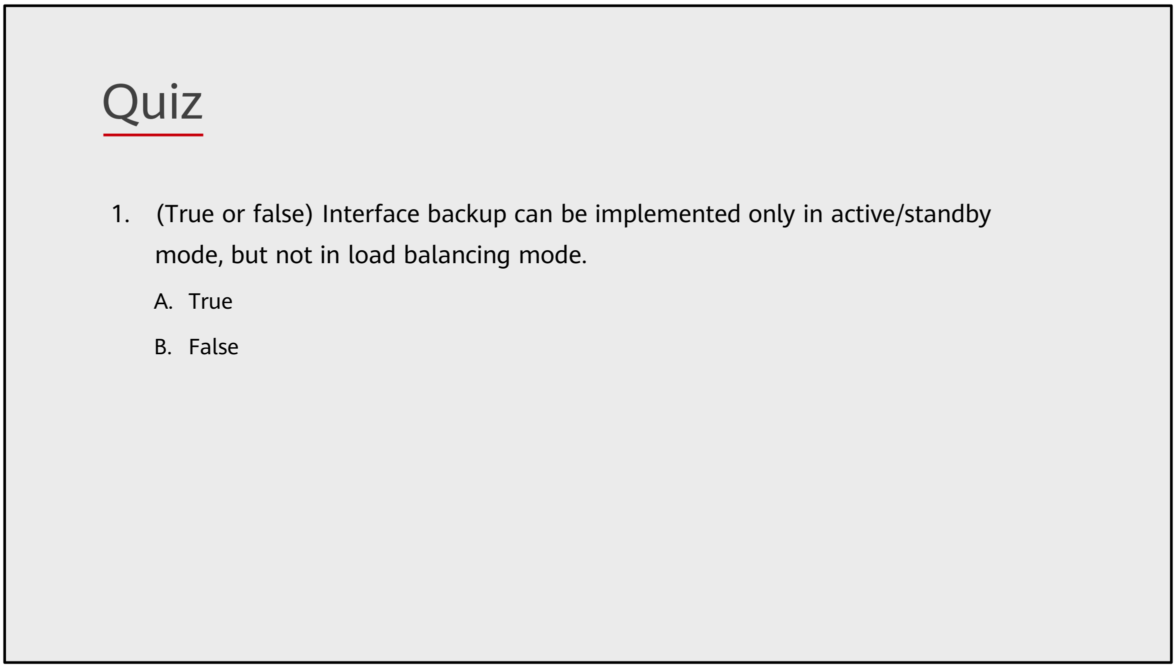
IP Floating Route

- An IP floating route is a static route. It provides a backup route when the primary route fails. A floating route is installed in the IP routing table only when the next hop of the primary route is unreachable.
- The IP floating route is implemented based on the Pre value in the IP routing table. In most cases, the Pre value of the backup route is set to be greater than that of the primary route.
- The active/standby switchover of IP floating routes is typically performed based on the interface status. Therefore, to detect the status of the entire path, NQA or BFD on the live network is often associated with IP floating routes. If NQA or BFD sessions fail, the primary route is considered ineffective.



IP routing-table

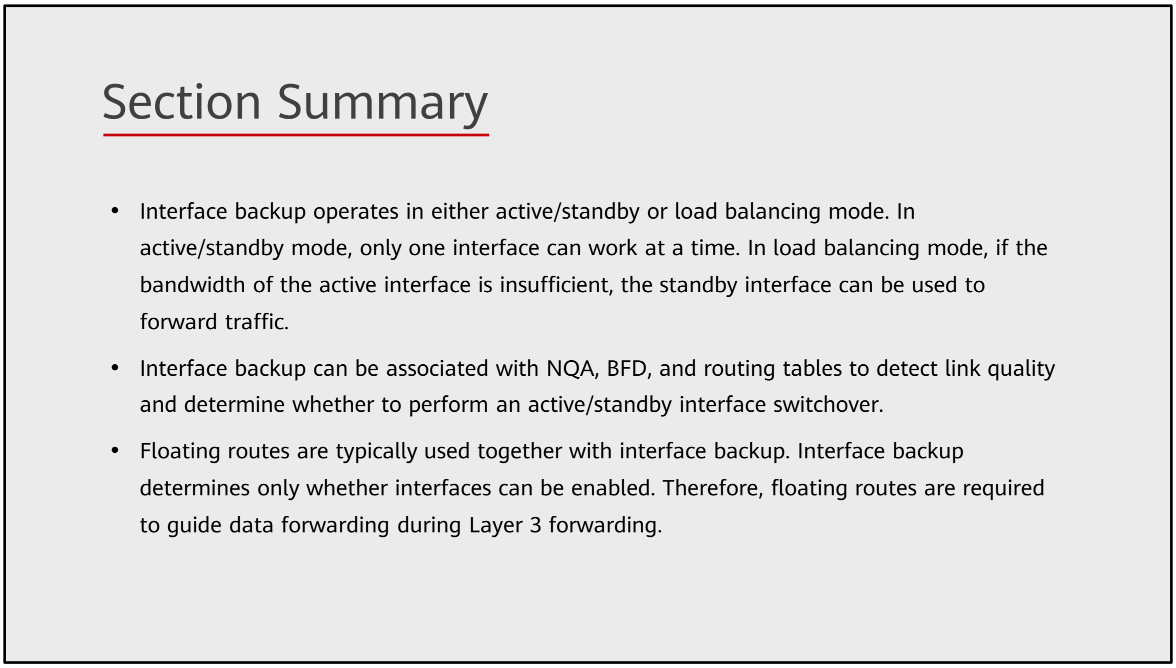
Net1 IF1 60(Pre) Track-NQA primary path
Net1 IF2 90(Pre) Track-NQA backup path
Net1 IF3 100(Pre) Track-NQA backup path



Quiz

1. (True or false) Interface backup can be implemented only in active/standby mode, but not in load balancing mode.
   A. True
   B. False

- 1. B



Section Summary

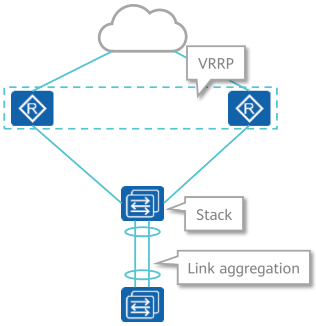
- Interface backup operates in either active/standby or load balancing mode. In active/standby mode, only one interface can work at a time. In load balancing mode, if the bandwidth of the active interface is insufficient, the standby interface can be used to forward traffic.
- Interface backup can be associated with NQA, BFD, and routing tables to detect link quality and determine whether to perform an active/standby interface switchover.
- Floating routes are typically used together with interface backup. Interface backup determines only whether interfaces can be enabled. Therefore, floating routes are required to guide data forwarding during Layer 3 forwarding.

Contents

1. Link Reliability
2. **Network Reliability**

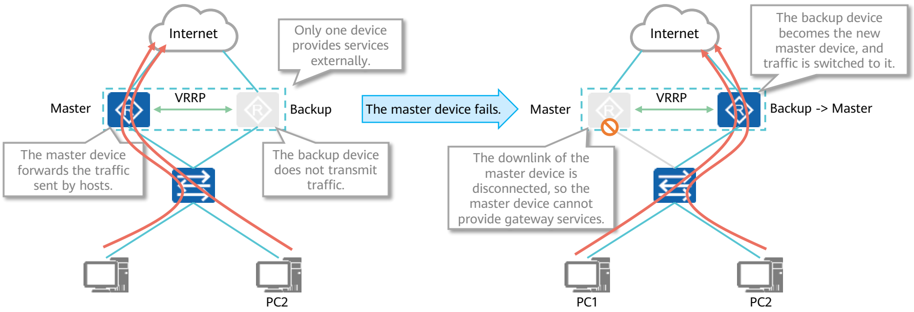
Network Reliability

- If a fault occurs on the network, the fault may not be detected or rectified in a timely manner. Therefore, redundancy technologies are required.
- Common redundancy technologies include stack, link aggregation, and VRRP.
- VRRP is the most widely used network redundancy technology on egress devices or gateways.



Overview of VRRP

- Hosts are connected to external networks through gateways. If a single gateway fails, services will be interrupted for a long time. Adding egress gateways is a common method to improve system reliability. In this case, route selection among multiple egresses becomes essential.
- VRRP groups multiple routing devices into a single virtual routing device. If a gateway fails, VRRP selects a new gateway to transmit data traffic, ensuring high network reliability.



Only one device provides services externally.

The master device forwards the traffic sent by hosts.

The backup device does not transmit traffic.

The downlink of the master device is disconnected, so the master device cannot provide gateway services.

The backup device becomes the new master device, and traffic is switched to it.

Section Summary

- VRRP is typically deployed on gateways or egresses. Terminals are unaware of the master/backup VRRP switchover, and can access the network after the switchover.
- After a master/backup VRRP switchover is performed, the switch connected to the VRRP devices guides traffic switching.
- VRRP can be associated with multiple detection technologies to detect the uplink quality, which helps VRRP accurately perform a master/backup switchover.

Summary

- There are many HA technologies. In the past, HA technologies focused on the high reliability of the network layer. With the development of cloud computing, there are more and more service HA requirements.