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

Improving Enterprise Network Performance

V2.5

Huawei Technologies Co.,Ltd.

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 Improving Enterprise Network Performance

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.

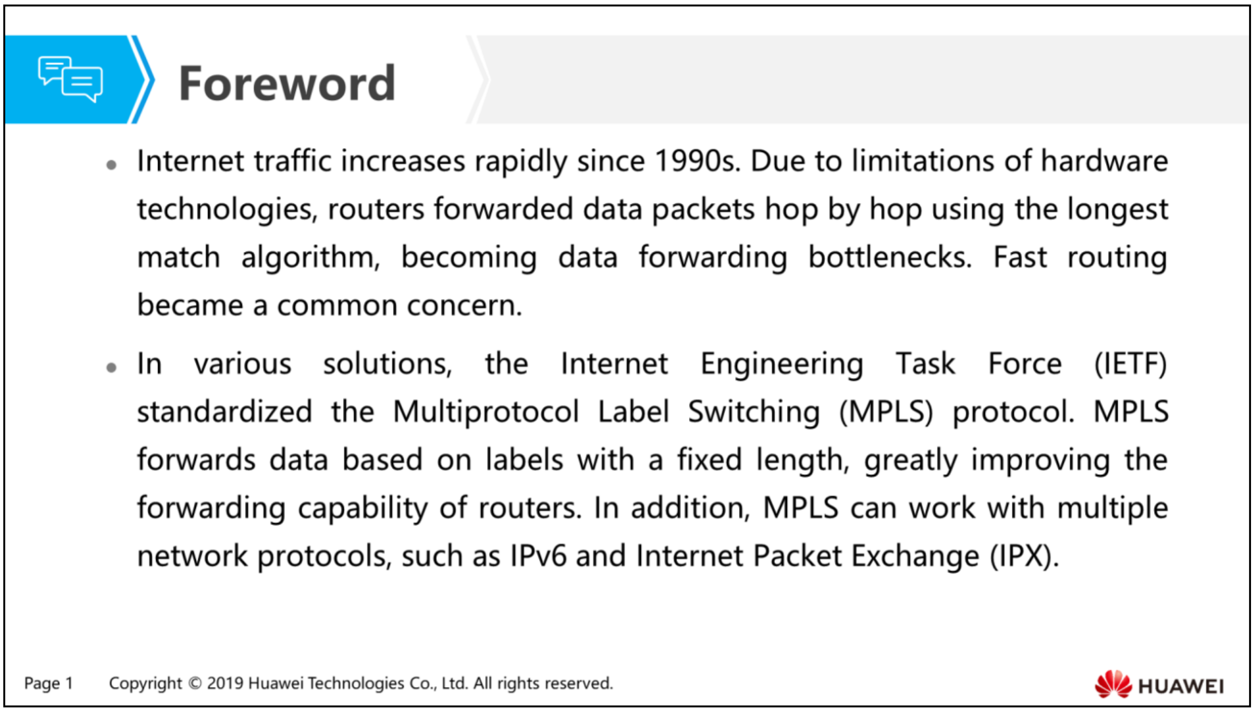
HCIA certification covers fundamentals skills for TCP/IP, routing, switching and related IP network technologies, together with Huawei data communications products, and skills for versatile routing platform (VRP) operation and management.

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

MPLS Principles and Configurations



Foreword

- Internet traffic increases rapidly since 1990s. Due to limitations of hardware technologies, routers forwarded data packets hop by hop using the longest match algorithm, becoming data forwarding bottlenecks. Fast routing became a common concern.
- In various solutions, the Internet Engineering Task Force (IETF) standardized the Multiprotocol Label Switching (MPLS) protocol. MPLS forwards data based on labels with a fixed length, greatly improving the forwarding capability of routers. In addition, MPLS can work with multiple network protocols, such as IPv6 and Internet Packet Exchange (IPX).

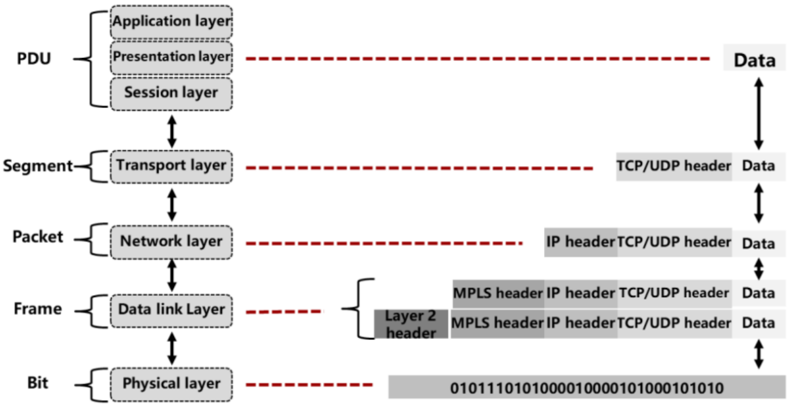
Objectives

- Upon completion of this section, you will be able to:
  - Understand the MPLS working principles
  - Master the MPLS configuration

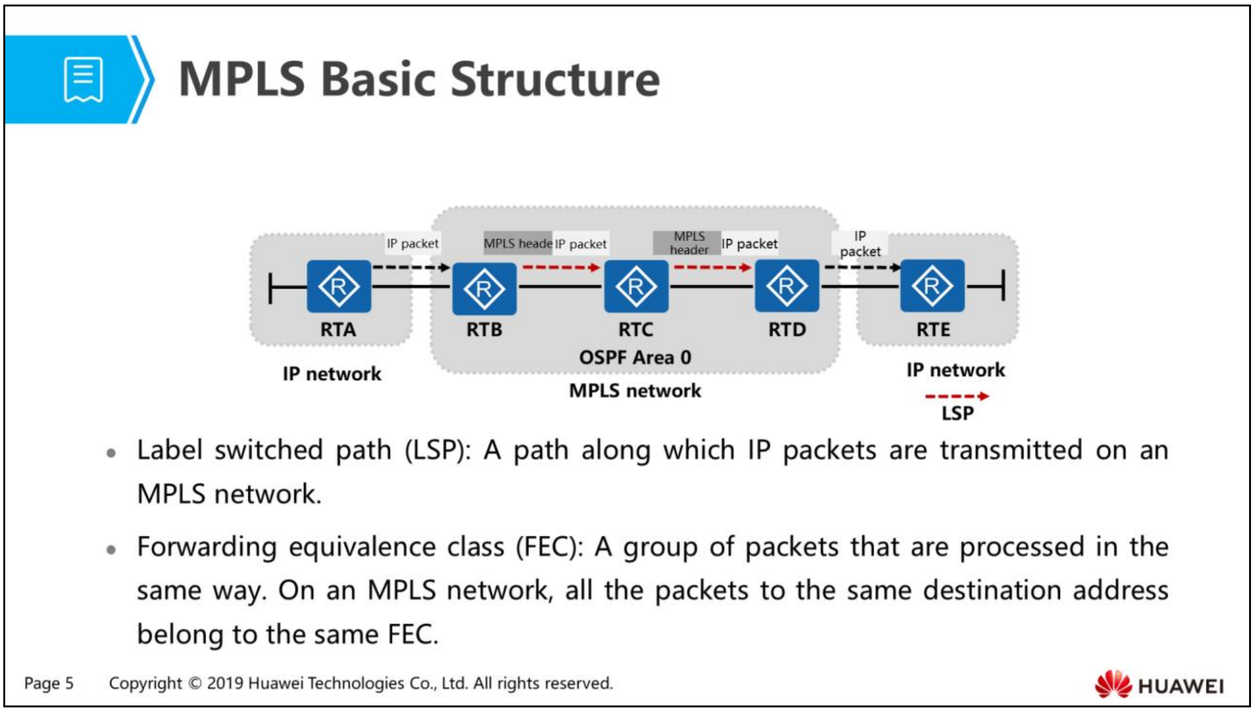
Contents

1. **MPLS Overview**
2. LSP Setup

MPLS Overview



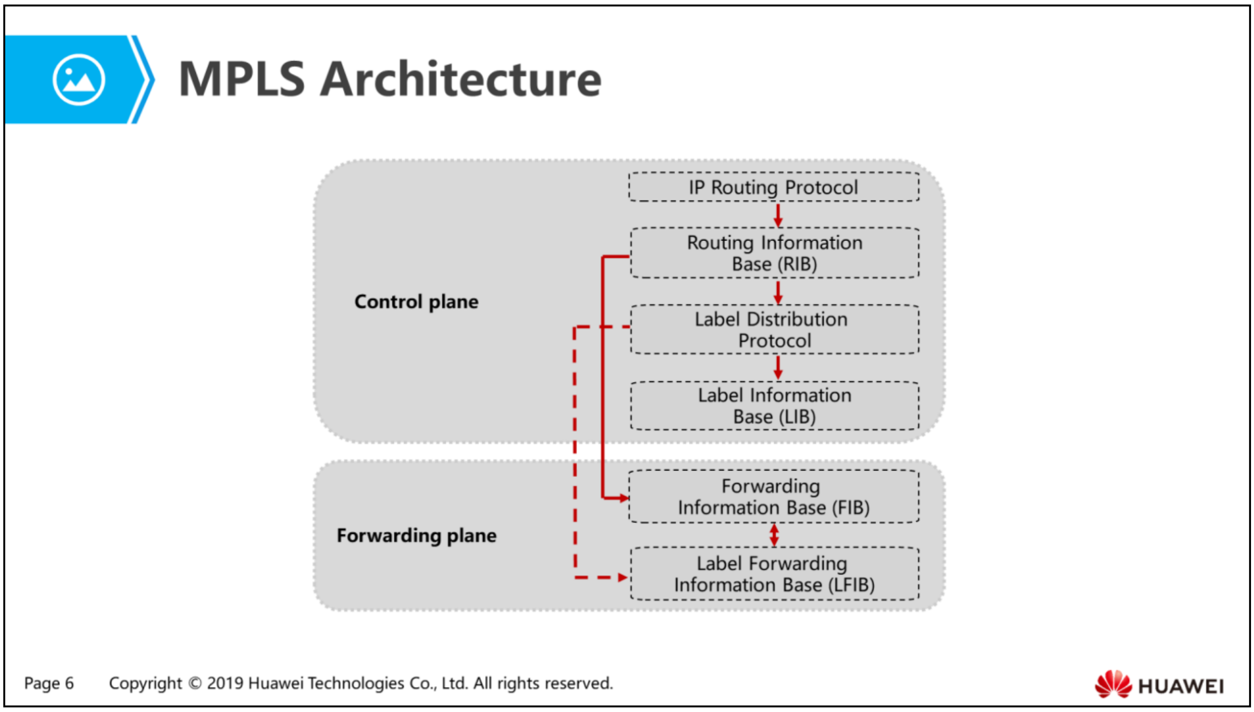
- MPLS obtains link layer services from various link-layer protocols such as PPP, ATM, frame relay, and Ethernet and provides connection-oriented services for the network layer. MPLS is implemented based on route entries generated using routing protocols, providing powerful and flexible routing functions to meet requirements by various new applications.
- This material describes the MPLS protocol from two aspects:
  - Basic MPLS architecture
  - MPLS LSP setup and data forwarding process



MPLS Basic Structure

- Label switched path (LSP): A path along which IP packets are transmitted on an MPLS network.
- Forwarding equivalence class (FEC): A group of packets that are processed in the same way. On an MPLS network, all the packets to the same destination address belong to the same FEC.

- On an MPLS network, the router roles are classified into two types:
  - Label edge router (LER): Adds a label to packets or pops a label out, such as RTB and RTD.
  - Label switched router (LSR): Switches labels in packets, such as RTC.
- The nodes on an LSP include the ingress, transit, and egress nodes, based on the direction of data flows.
  - The ingress node (upstream) sends MPLS packets to the transit node (downstream). Similarly, the transit node (upstream) forwards MPLS packets to the egress node (downstream).
- MPLS, a traffic-class-based forwarding technology, groups data packets that are processed in the same way into a forwarding equivalence class (FEC).
- FECs can be determined flexibly based on source IP address, destination IP address, source port, destination port, protocol type, VPN, or any combinations of them.



MPLS Architecture

Control plane

IP Routing Protocol

Routing Information Base (RIB)

Label Distribution Protocol

Label Information Base (LIB)

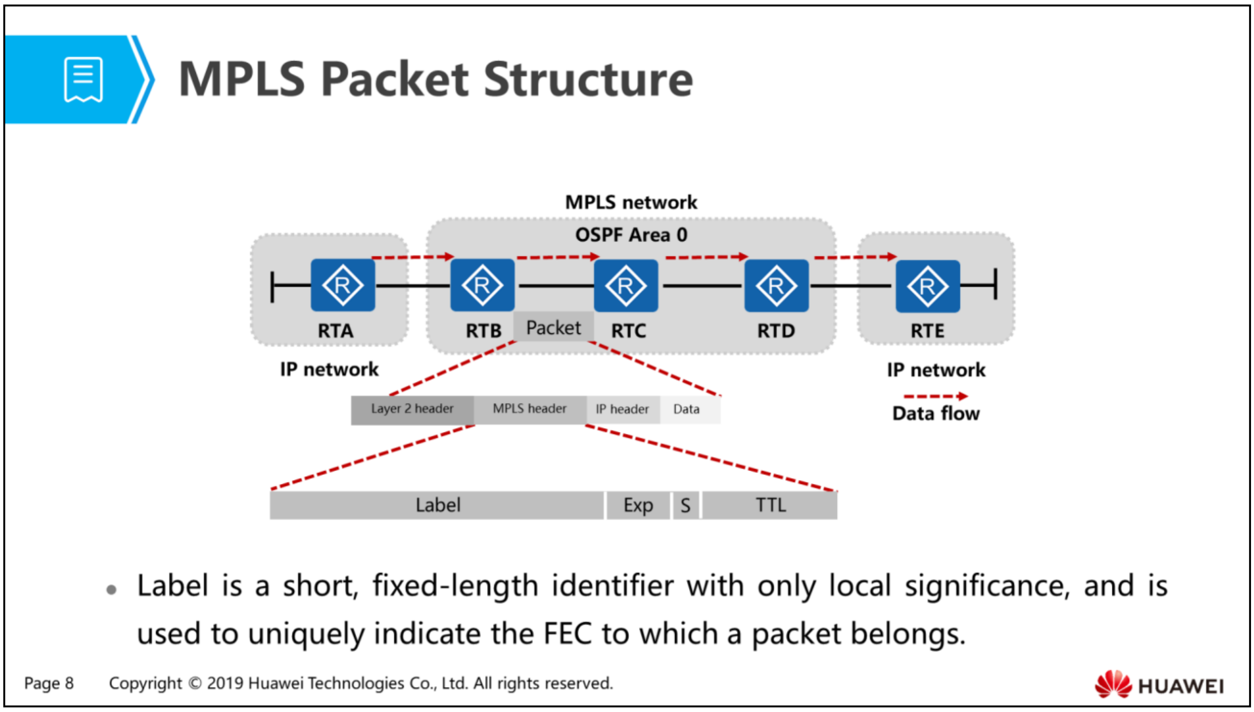
Forwarding plane

Forwarding Information Base (FIB)

Label Forwarding Information Base (LFIB)

- Control plane: is responsible for generating and maintaining routing and label information.
  - Routing information base (RIB): is generated by IP routing protocols and used to select routes.
  - Label distribution protocol (LDP): allocates labels, creates a label information base (LIB), and establishes and tears down LSPs.
  - Label information base (LIB): is generated by LDP and used to manage labels.
- Forwarding plane: also called data plane, is responsible for forwarding common IP packets and MPLS packets.
  - Forwarding information base (FIB): is generated based on routing information obtained from the RIB and used to forward common IP packets.
  - Label forwarding information base (LFIB): is created by LDP and used to forward MPLS packets. The LFIB is also called the label forwarding table.

- On an MPLS-capable router, the packet forwarding process is as follows:
    - When receiving a common IP packet, the router searches the FIB table. If the tunnel ID is 0x0, the router forwards the packet using the IP protocol. If the tunnel ID is not 0x0, the router forwards the packet using the MPLS protocol.
    - When receiving a labeled packet, the router searches the LFIB table. If the outgoing label is a common label, the router forwards the packet using the MPLS protocol. If the outgoing label is a special label, for example, 3, the router pops out the label from the packet and forwards it using the IP protocol.



MPLS Packet Structure

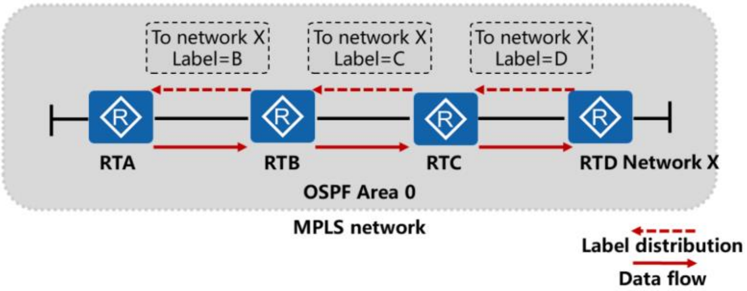
- Label is a short, fixed-length identifier with only local significance, and is used to uniquely indicate the FEC to which a packet belongs.

- The MPLS label is between the link layer header and the network layer header, and allows any link layer protocols. This figure shows the MPLS label structure.
- An MPLS label has four fields:
  - Label: 20-bit label value.
  - Exp: 3-bit, used as an extension value. Generally, this field is used as the class of service (CoS) field. When congestion occurs, the device forwards packets with high-priority preferentially.
  - S: 1-bit value indicating the bottom of a label stack. MPLS supports nesting of multiple labels. When the S field is 1, the label is at the bottom of the label stack.
  - TTL: time to live. This 8-bit field is the same as the TTL field in IP packets.
- The label space is the value range of the label. The following describes the label space classification:
  - 0 to 15: special labels. For example, label 3, called implicit null label, is used to for penultimate hop popping (PHP).
  - 16 to 1023: label space shared by static label switched path (LSPs) and static constraint-based routed LSPs (CR-LSPs).
  - 1024 and above: label space for dynamic signaling protocols, such as LDP, Resource Reservation Protocol-Traffic Engineering (RSVP-TE), and Multiprotocol Extensions for BGP (MP-BGP).

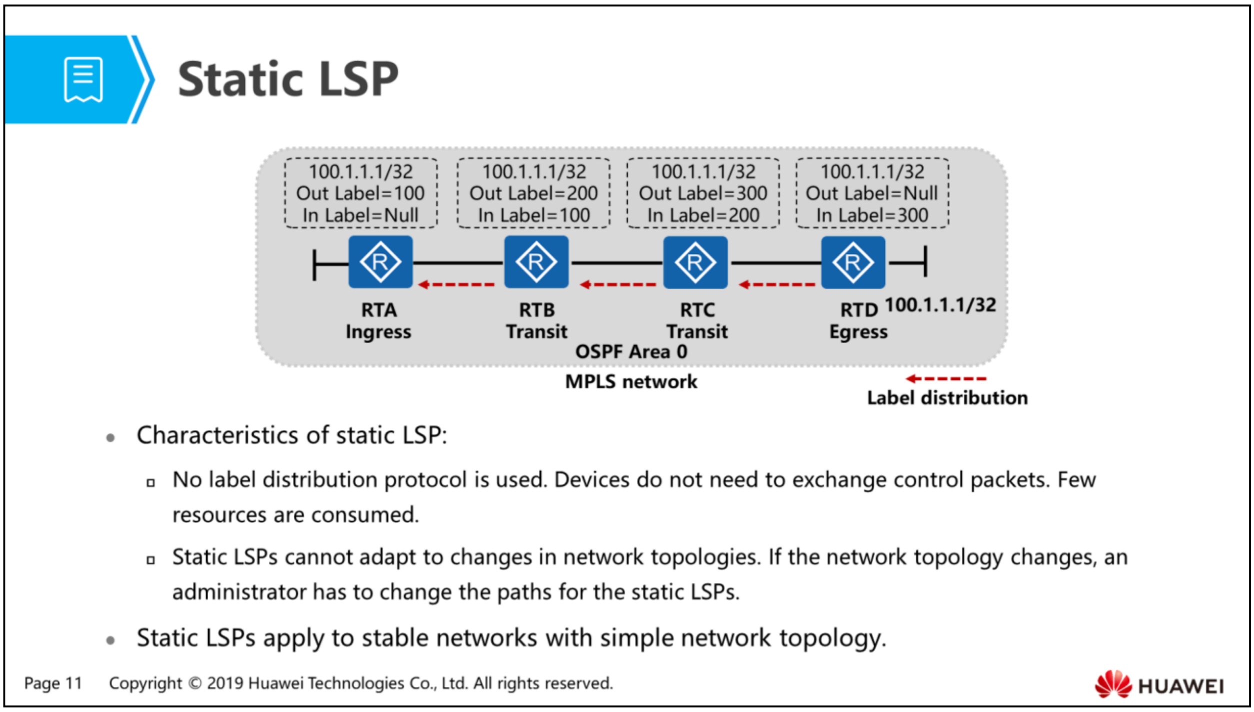
Contents

1. MPLS Overview
2. **LSP Setup**

LSP Setup Modes



- There are two LSP setup modes:
  - Static LSP: Users manually allocate labels to FECs for tunnel setup.
  - Dynamic LSP: Forwarding tunnels are established by the Label Distribution Protocol (LDP).



Static LSP

- Characteristics of static LSP:
  - No label distribution protocol is used. Devices do not need to exchange control packets. Few resources are consumed.
  - Static LSPs cannot adapt to changes in network topologies. If the network topology changes, an administrator has to change the paths for the static LSPs.
- Static LSPs apply to stable networks with simple network topology.

- When configuring a static LSP, the administrator needs to manually distribute labels for each router according to the following principle: the value of the outgoing label of the previous node is equal to the value of the incoming label of the next node.
- As shown in this figure, a user on the MPLS network uses the address 100.1.1.1/32. To configure a static LSP for this user, perform the following operations:
  - Configure an LSR ID to uniquely identify an MPLS-capable router on the network. No default LSR ID is provided, and the LSR ID needs to be configured manually. To improve network reliability, it is recommended that a loopback interface address of the LSR be used as the LSR ID.
    - Command: mpls lsr-id lsr-id
  - Enable MPLS on all nodes in the MPLS domain and corresponding interfaces.
    - Commands: system-view
  - mpls
  - interface interface-type interface-number
  - mpls
  - Run the following command on the ingress node:

        - static-lsp ingress lsp-name destination ip-address { mask-length | mask } { nexthop next-hop-address | outgoing-interface interface-type interface-number } * out-label out-label

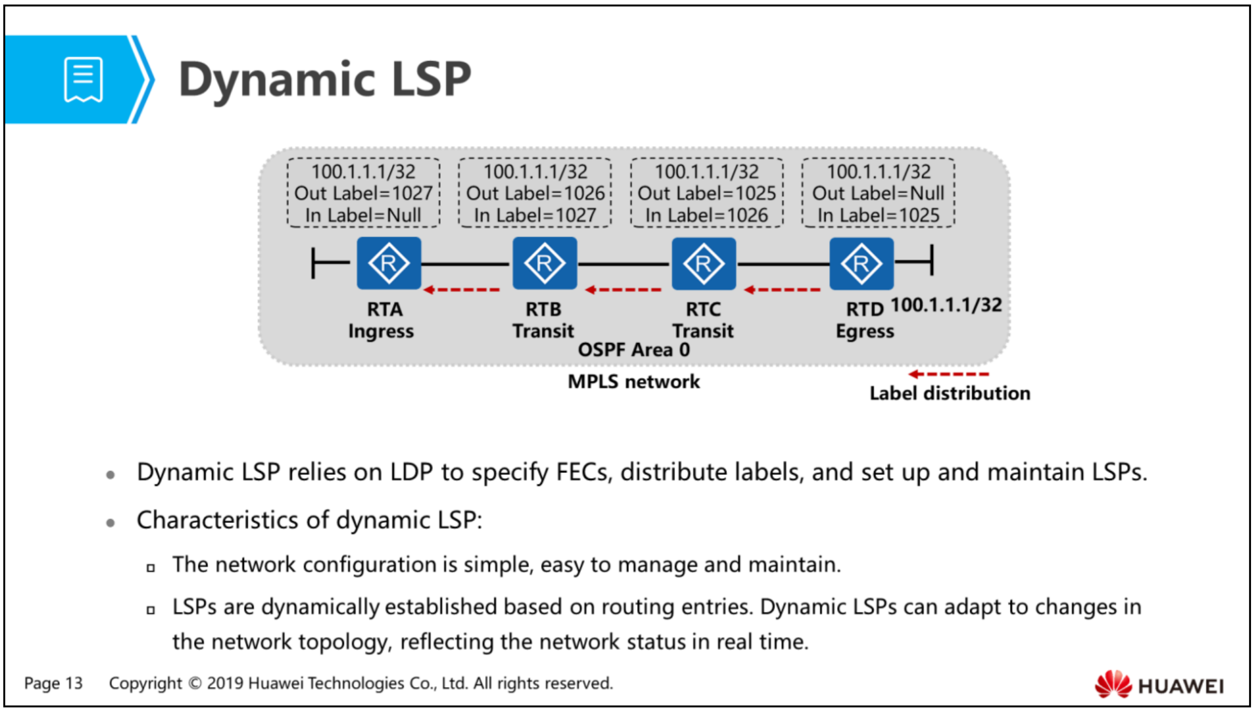
    - Run the following command on the transit node:

        - static-lsp transit lsp-name [incoming-interface interface-type interface-number] in-label in-label { nexthop next-hop-address | outgoing-interface interface-type interface-number } * out-label out-label

    - Run the following command on the egress node:

        - static-lsp egress lsp-name [incoming-interface interface-type interface-number] in-label in-label [lsrid ingress-lsr-id tunnel-id tunnel-id]

- After the preceding configuration is complete, a unidirectional LSP from RTA to RTD is created. RTA can normally access 100.1.1.1/32 connected to RTD only after the LSP from RTD to RTA is created.



Dynamic LSP

100.1.1.1/32
Out Label=1027
In Label=Null

100.1.1.1/32
Out Label=1026
In Label=1027

100.1.1.1/32
Out Label=1025
In Label=1026

100.1.1.1/32
Out Label=Null
In Label=1025

RTA
Ingress

RTB
Transit

RTC
Transit

RTD 100.1.1.1/32
Egress

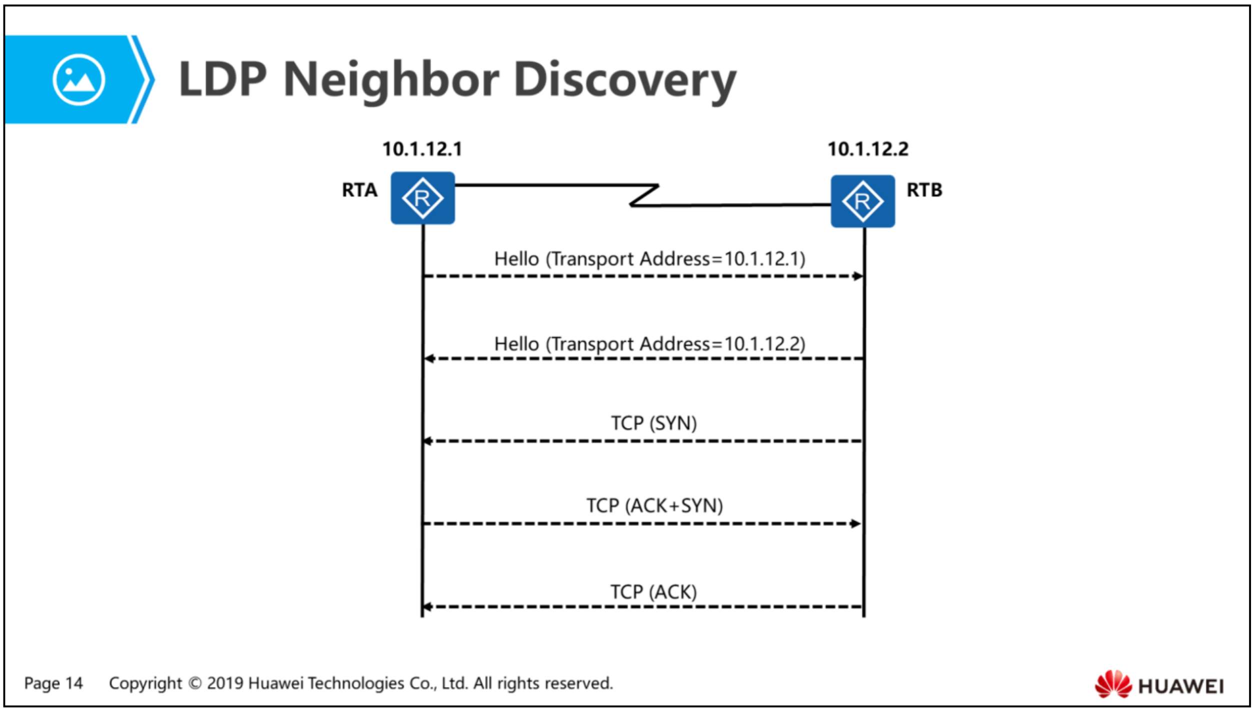
OSPF Area 0

MPLS network

Label distribution

- Dynamic LSP relies on LDP to specify FECs, distribute labels, and set up and maintain LSPs.
- Characteristics of dynamic LSP:
  - The network configuration is simple, easy to manage and maintain.
  - LSPs are dynamically established based on routing entries. Dynamic LSPs can adapt to changes in the network topology, reflecting the network status in real time.

- As shown in this figure:
  - The egress router RTD allocates labels to locally stored routes and sends the binding information about labels and routes to the upstream neighboring router RTC.
  - After receiving binding information from the downstream neighboring router RTD, RTC adds the information to the LIB and sends the binding information about labels allocated by itself and routes to its upstream neighboring router RTB.
  - Similarly, RTB sends the binding information about labels allocated by itself and routes to its upstream neighboring router RTA. RTA is the ingress node without an upstream neighbor; therefore, a dynamic LSP is established.



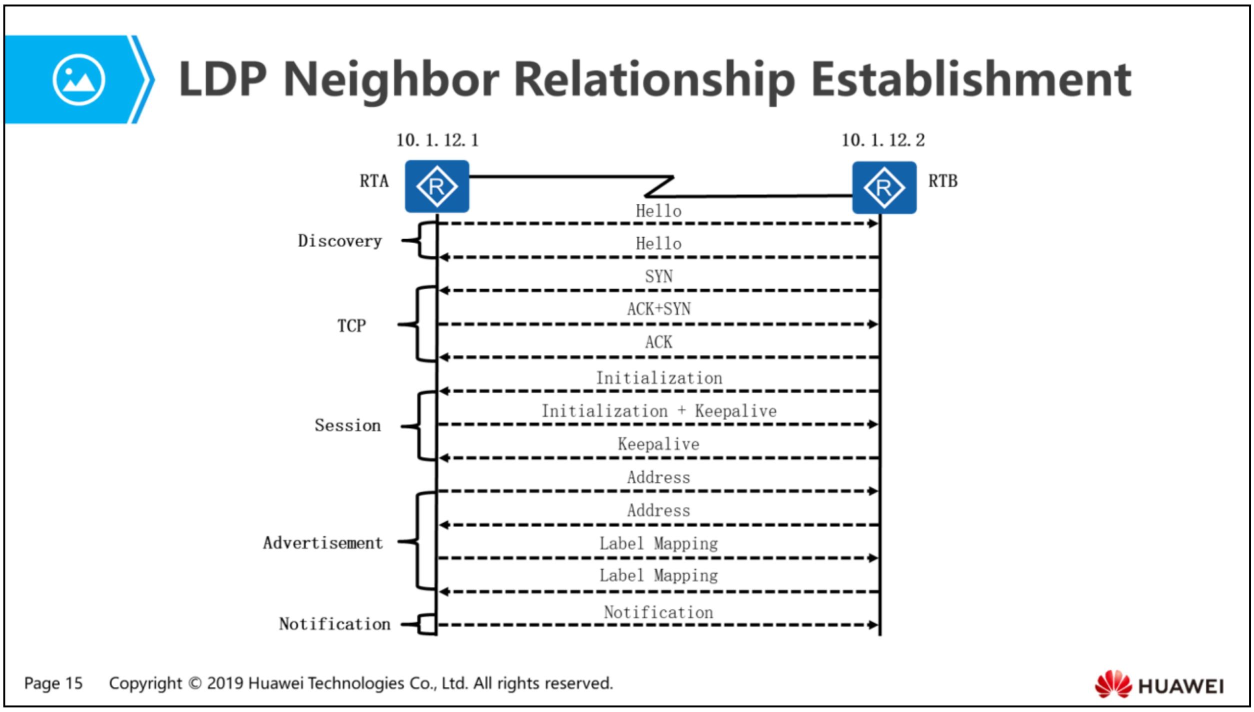
LDP Neighbor Discovery

10.1.12.1
10.1.12.2
RTA
RTB
Hello (Transport Address=10.1.12.1)
Hello (Transport Address=10.1.12.2)
TCP (SYN)
TCP (ACK+SYN)
TCP (ACK)

Page 14 Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- MPLS-capable routers periodically send LDP Link Hello messages to discover LDP neighbors and to establish local LDP sessions.
  - To allow LDP-enabled devices to quickly discover neighbors, LDP Hello messages are encapsulated using the UDP protocol. UDP is a connectionless protocol. To ensure effectiveness and reliability of neighbors, Hello messages are multicast to the destination IP address 224.0.0.2 at an interval of 5s. A message sent to a multicast address can be received by all the routers.
  - An LDP Hello message carries the Transport Address field. This field must be the same as the LSR ID of the device, indicating the IP address used to establish a neighbor relationship with the peer. If this field specifies an IP address of a directly connected interface, a neighbor relationship is established directly. If this field uses a loopback interface IP address, a neighbor relationship can be established only when the loopback interface IP address is reachable.



LDP Neighbor Relationship Establishment

10. 1. 12. 1

10. 1. 12. 2

RTA

RTB

Discovery

Hello

Hello

TCP

SYN

ACK+SYN

ACK

Session

Initialization

Initialization + Keepalive

Keepalive

Advertisement

Address

Address

Label Mapping

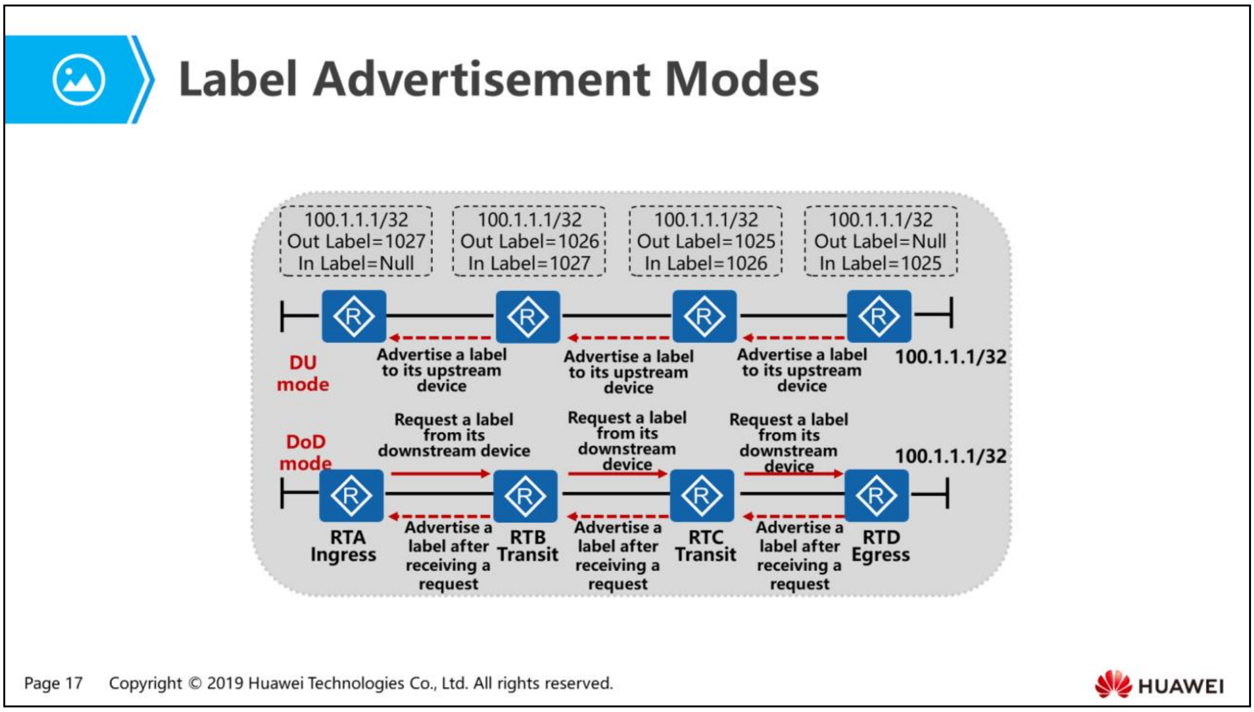
Label Mapping

Notification

Notification

- LDP defines four types of messages:
  - Discovery message: used to announce and maintain the presence of neighbors on the network. For example, Hello messages are discovery messages.
  - Session message: used to establish, maintain, and terminate sessions between LDP peers. For example, Initialization and Keepalive messages are session messages.
  - Advertisement message: used to create, change and delete label mappings for FECs. For example, Address and Label Mapping messages are advertisement messages.
  - Notification message: used to provide advisory and error information.
- The LDP neighbor relationship establishment process is as follows:
  - Two LSRs send a Hello message to each other.
    - The Hello message contains the transport address that the peers use to establish an LDP session.
  - The LSR with a larger transport address initiates a TCP connection.
    - As shown in this figure, RTB initiates a TCP connection and RTA waits for the TCP connection request.

- After the TCP connection is successfully established, RTB sends an Initialization message to negotiate with RTA about parameters used for establishing the LDP session.
    - These parameters include the LDP version, label distribution mode, Keepalive timer value, maximum PDU length, and label space.
- If RTA accepts parameters in the Initialization message, it sends an Initialization message and a Keepalive message to RTB.
    - If RTA rejects parameters in the Initialization message, it sends a Notification message to RTB to stop the establishment process of the LDP session.
- If RTB accepts the parameters in the Initialization message sent from RTA, it sends a Keepalive message to RTA.
    - If RTB rejects the parameters in the Initialization message, it sends a Notification message to RTA to stop the establishment process of the LDP session.
- After the peers receive the Keepalive message from each other, the LDP session is successfully established. After the LDP session is successfully established, FECs can be created and labels can be distributed.



Label Advertisement Modes

100.1.1.1/32
Out Label=1027
In Label=Null

100.1.1.1/32
Out Label=1026
In Label=1027

100.1.1.1/32
Out Label=1025
In Label=1026

100.1.1.1/32
Out Label=Null
In Label=1025

DU mode

Advertise a label to its upstream device

Advertise a label to its upstream device

Advertise a label to its upstream device

100.1.1.1/32

DoD mode

Request a label from its downstream device

Request a label from its downstream device

Request a label from its downstream device

100.1.1.1/32

RTA Ingress

Advertise a label after receiving a request

RTB Transit

Advertise a label after receiving a request

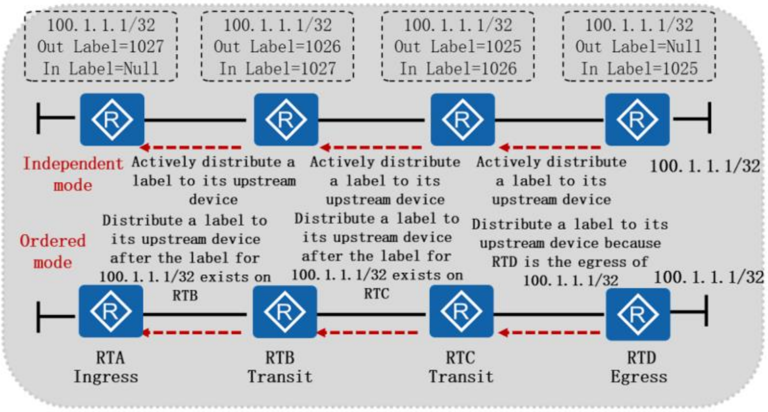
RTC Transit

Advertise a label after receiving a request

RTD Egress

- Label advertisement modes:
  - Downstream Unsolicited (DU): An LSR distributes a label for a specified FEC without receiving a Label Request message from an upstream LSR.
  - Downstream on Demand (DoD): An LSR distributes a label for a specified FEC only after receiving a Label Request message from an upstream LSR.
- As shown in this figure:
  - When the DU mode is used, the egress node RTD actively sends a Label Mapping message to the upstream transit node RTC to advertise the label for the host route 100.1.1.1/32 for packets with 100.1.1.1/32 as the destination address.
  - When the DoD mode is used, the downstream egress node RTD sends a Label Mapping message to the upstream transit node RTC to advertise the label for packets with 100.1.1.1/32 as the destination address, after receiving a Label Request message from the transit node RTC.
- By default, Huawei devices use the DU mode to advertise labels.
- In DU mode, a device advertises labels to neighbors without waiting for request messages from upstream devices. When the network topology changes, new labels can be quickly advertised in DU mode. Compared with the DoD mode, the DU mode improves the convergence performance.

Label Distribution Control Modes



100.1.1.1/32	100.1.1.1/32	100.1.1.1/32	100.1.1.1/32
Out Label=1027	Out Label=1026	Out Label=1025	Out Label=Null
In Label=Null	In Label=1027	In Label=1026	In Label=1025

Independent mode

Actively distribute a label to its upstream device

Actively distribute a label to its upstream device

Actively distribute a label to its upstream device

100.1.1.1/32

Ordered mode

Distribute a label to its upstream device after the label for 100.1.1.1/32 exists on RTB

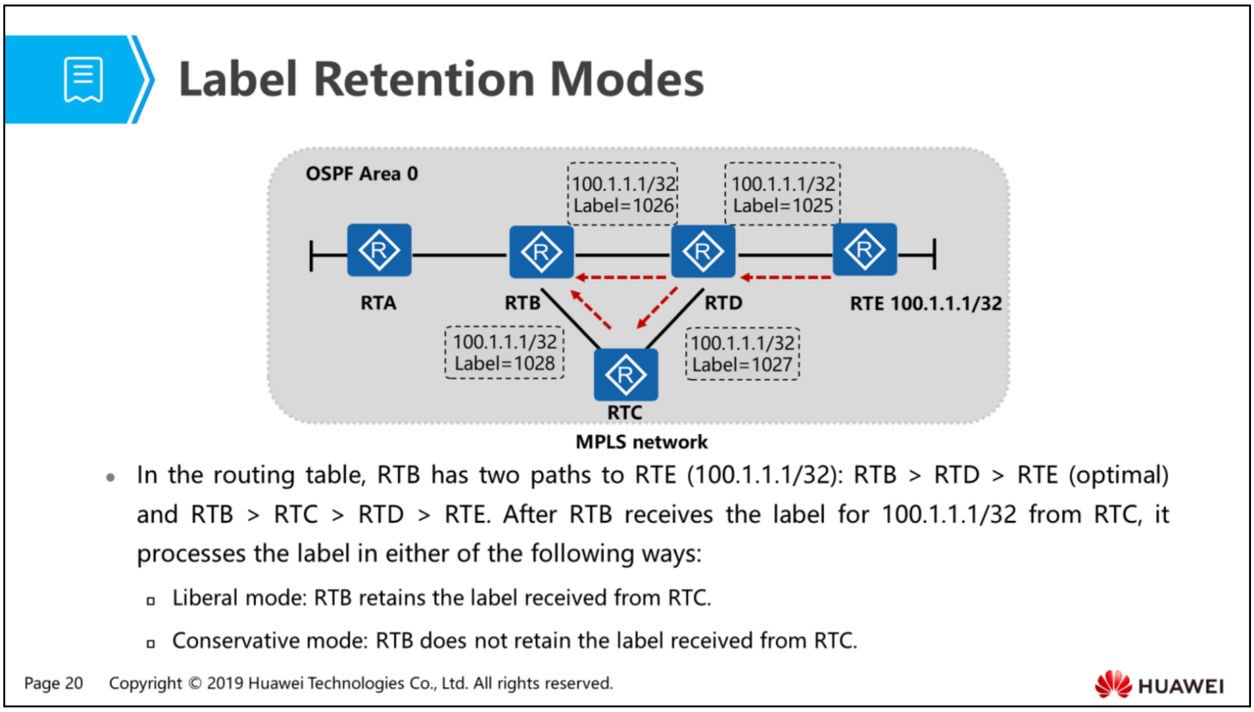
Distribute a label to its upstream device after the label for 100.1.1.1/32 exists on RTC

Distribute a label to its upstream device because RTD is the egress of 100.1.1.1/32

100.1.1.1/32

- Label distribution control modes:
  - Independent mode: A local LSR distributes a label and binds it to an FEC and informs its upstream LSR without waiting for the label distributed by its downstream LSR.
  - Ordered mode: An LSR advertises mappings between a label and an FEC to its upstream LSR only when the LSR is the outgoing node of the FEC or receives a Label Mapping message from the next hop.
- As shown in this figure:
  - In Independent mode:
    - If the label advertisement mode is DU and the label distribution control mode is Independent, the transit node RTC distributes labels to its upstream node RTB, without waiting for labels from the downstream egress node RTD.
    - If the label advertisement mode is DoD and the label distribution control mode is Independent, the directly-connected transit RTC of RTB that sends the Label Request message directly replies with labels without waiting for labels of the egress node RTD.

    - In Ordered mode:
        - If the label advertisement mode is DU and the label distribution control mode is Ordered, the transit node RTC distributes labels to its upstream node RTB, only after receiving labels from the downstream egress node RTD.
        - If the label advertisement mode is DoD and the label distribution control mode is Ordered, the directly-connected transit RTC of RTB that sends the Label Request message distributes labels only after receiving labels from the egress node RTD.
- By default, Huawei devices use the Ordered mode to distribute labels.
- In Ordered mode, an LSR distributes labels to its upstream LSR only when the LSR has obtained the label of its next hop. This prevents data loss that may occur if the LSR cannot distribute a label to its upstream node when its downstream node is not distributed with a label or the convergence time is too long.

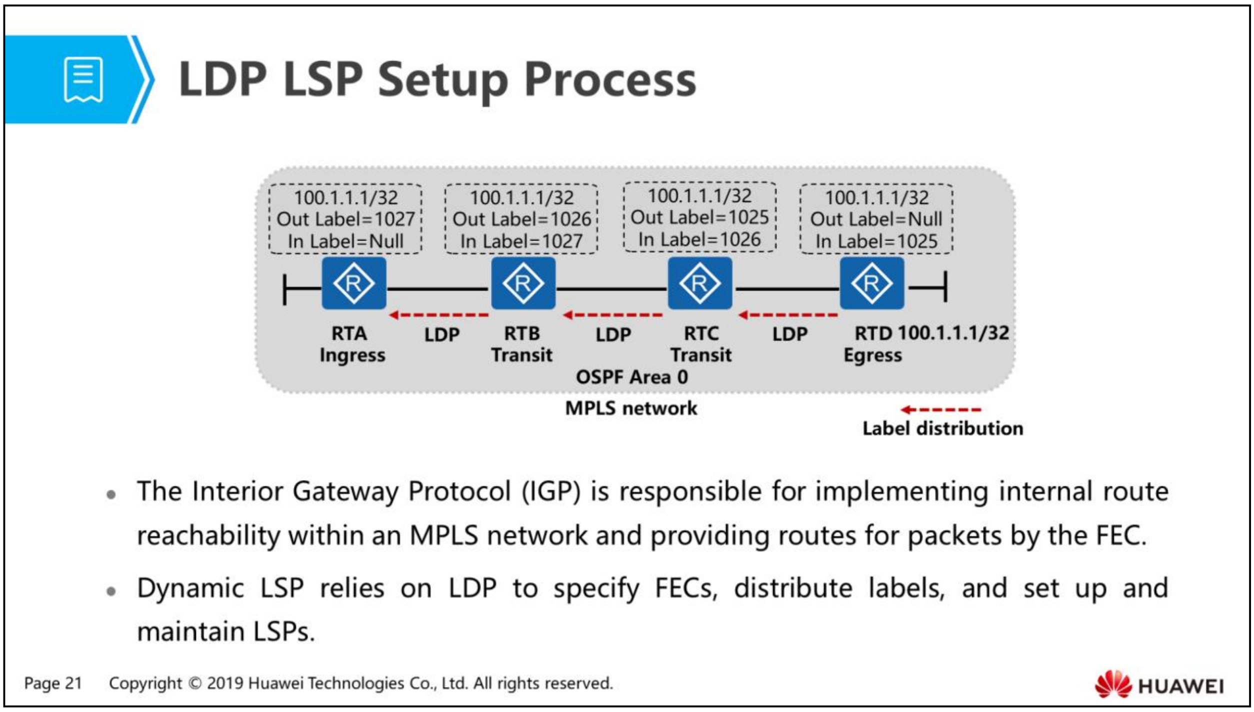


Label Retention Modes

- In the routing table, RTB has two paths to RTE (100.1.1.1/32): RTB > RTD > RTE (optimal) and RTB > RTC > RTD > RTE. After RTB receives the label for 100.1.1.1/32 from RTC, it processes the label in either of the following ways:
  - Liberal mode: RTB retains the label received from RTC.
  - Conservative mode: RTB does not retain the label received from RTC.

HUAWEI

- Label retention modes:
  - Liberal mode: For a Label Mapping message received from a neighboring LSR, the local LSR retains the label regardless of whether the neighbor LSR is its next hop.
  - Conservative mode: For a Label Mapping message received from a neighboring LSR, the local LSR retains the label only when the neighboring LSR is its next hop.
- When the next hop of an LSR changes due to a network topology change, note that:
  - In liberal mode, LSRs use previous labels sent by non-next hops to quickly reestablish LSPs. This requires more memory and label space than the conservative mode.
  - In conservative mode, LSRs only retain labels sent by next hops. This saves memory and label space but slows down the reestablishment of LSPs.
- By default, Huawei devices use the Liberal mode to retain labels.



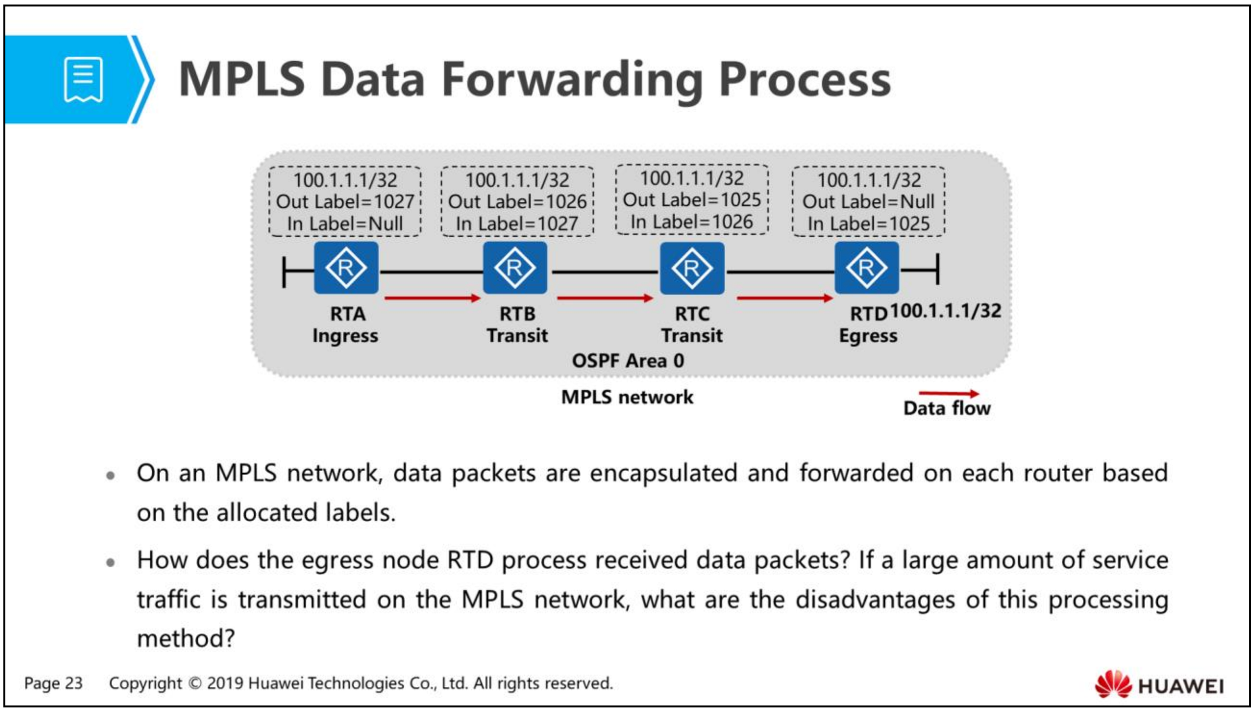
LDP LSP Setup Process

- The Interior Gateway Protocol (IGP) is responsible for implementing internal route reachability within an MPLS network and providing routes for packets by the FEC.
- Dynamic LSP relies on LDP to specify FECs, distribute labels, and set up and maintain LSPs.

Page 21

- As shown in this figure, the dynamic LDP LSP establishment process is as follows:
  - The host route 100.1.1.1/32 exists on RTD. Because RTD is the egress node, it directly advertises binding information between 100.1.1.1/32 and label to its upstream neighbor RTC.
  - After RTC receives the binding between 100.1.1.1/32 and label from RTD, RTC records the label in its own LIB table and advertises the binding between 100.1.1.1/32 and label to RTB. Meanwhile, RTC checks whether the next hop to 100.1.1.1/32 is RTD in its IP routing table. If the next hop is RTD, RTC uses the label distributed by RTD to encapsulate data destined for 100.1.1.1/32. If the next hop is not RTD, RTC retains the label distributed by RTD as a standby label.
  - After RTB receives binding information between 100.1.1.1/32 and label from RTC, it performs the same action as RTC.
  - After RTA receives the binding between 100.1.1.1/32 and label from RTB, it checks whether the next hop to 100.1.1.1/32 is RTB in its IP routing table. If the next hop is RTB, RTA uses the label distributed by RTB to encapsulate data destined for 100.1.1.1/32. If the next hop is not RTB, RTA retains the label distributed by RTB as a standby label. Because RTA is the ingress node, an LSP to 100.1.1.1/32 is established.

- The basic LDP configurations are as follows:
  - Run the mpls lsr-id lsr-id command to configure an LSR ID for the local node.
  - Run the mpls command to enable MPLS and enter the MPLS view.
  - Run the mpls ldp command to enable LDP and enter the MPLS LDP view.
  - Run the interface interface-type interface-number command to enter the view of the interface where an LDP session needs to be set up.
    - Run the mpls command to enable MPLS on the interface.
    - Run the mpls ldp command to enable MPLS LDP on the interface.



MPLS Data Forwarding Process

100.1.1.1/32
Out Label=1027
In Label=Null

100.1.1.1/32
Out Label=1026
In Label=1027

100.1.1.1/32
Out Label=1025
In Label=1026

100.1.1.1/32
Out Label=Null
In Label=1025

RTA
Ingress

RTB
Transit

RTC
Transit

RTD 100.1.1.1/32
Egress

OSPF Area 0

MPLS network

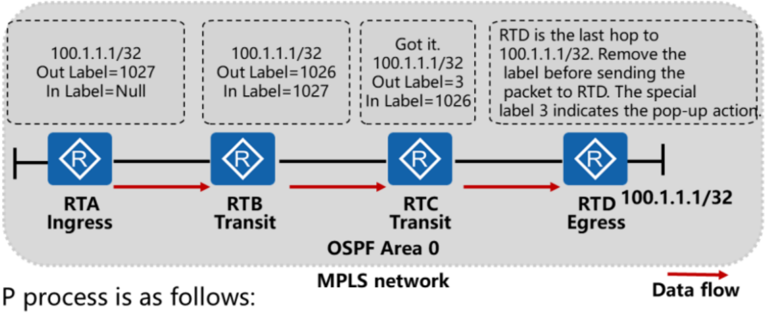
Data flow

- On an MPLS network, data packets are encapsulated and forwarded on each router based on the allocated labels.
- How does the egress node RTD process received data packets? If a large amount of service traffic is transmitted on the MPLS network, what are the disadvantages of this processing method?

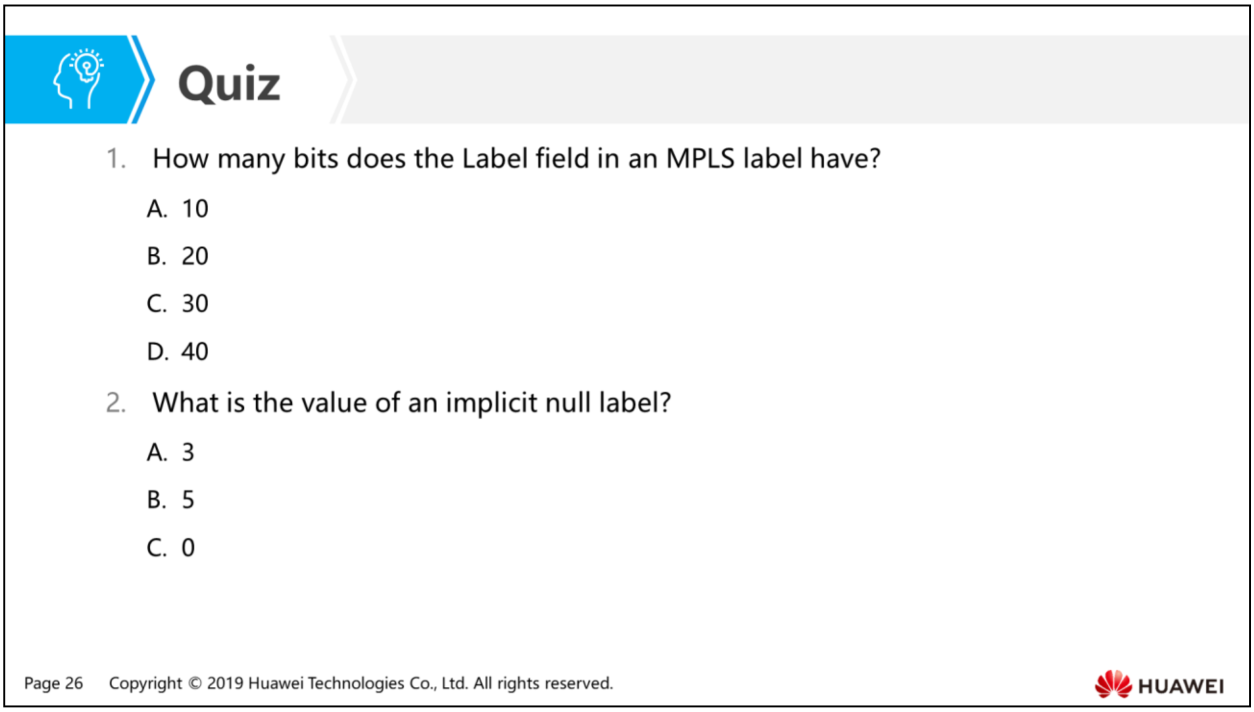
- As shown in this figure, MPLS data forwarding process is as follows:
  - RTA receives a data packet with the destination address 100.1.1.1/32. If the packet is a common IP packet, RTA searches the FIB table and adds label 1027 to the packet before forwarding it using MPLS, because the tunnel ID is not 0x0. If the packet is a labeled packet, RTA searches the LFIB table and adds label 1027 to the packet before forwarding it using MPLS.
  - After RTB receives the packet with label 1027 from RTA, it searches the LFIB table and adds the outgoing label 1026 to the packet before forwarding it to RTC using MPLS.
  - After RTC receives the packet with label 1026 from RTB, it searches the LFIB table and adds the outgoing label 1025 to the packet before forwarding it to RTD using MPLS.
  - After RTD receives the packet with label 1025 from RTC, it searches the LFIB table and finds that the outgoing label is Null, indicating that the data packet has reached the egress node. Therefore, RTD removes the label from the packet, processes the packet at Layer 3, and searches the IP routing table. RTD finds that 100.1.1.1/32 is a local route, so it encapsulates the packet and forwards it through the outbound interface in the IP routing table.

- If a large amount of service traffic is transmitted on the MPLS network, each data packet needs to be processed twice on the egress node before it can be correctly forwarded. This lowers the performance of the egress router. The PHP technology is developed to improve forwarding performance of the egress router to ensure that it can correctly forward data packets after processing them for one time.

Penultimate Hop Popping



- The PHP process is as follows:
  - After RTC receives the packet with label 1026 from RTB, it searches the LFIB table and finds that the outgoing label is the implicit null label 3. RTC then pops the label out and forwards the IP data packet to the downstream router RTD.
  - After RTD receives the IP packet from RTC, RTD searches its own FIB table, encapsulates the packet, and forwards it through the outbound interface in the FIB table.



Quiz

1. How many bits does the Label field in an MPLS label have?
   - A. 10
   - B. 20
   - C. 30
   - D. 40
2. What is the value of an implicit null label?
   - A. 3
   - B. 5
   - C. 0

- Answer: B.
- Answer: A.

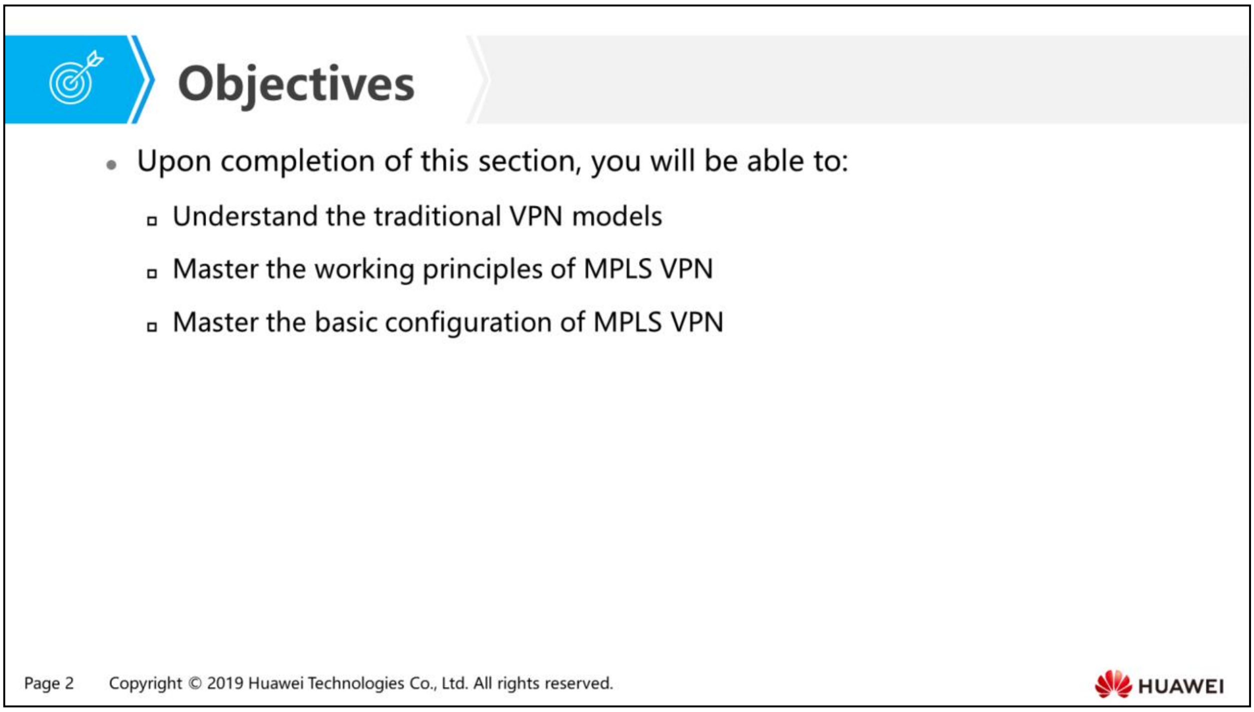
Thank You

www.huawei.com

MPLS VPN Principles and Configurations

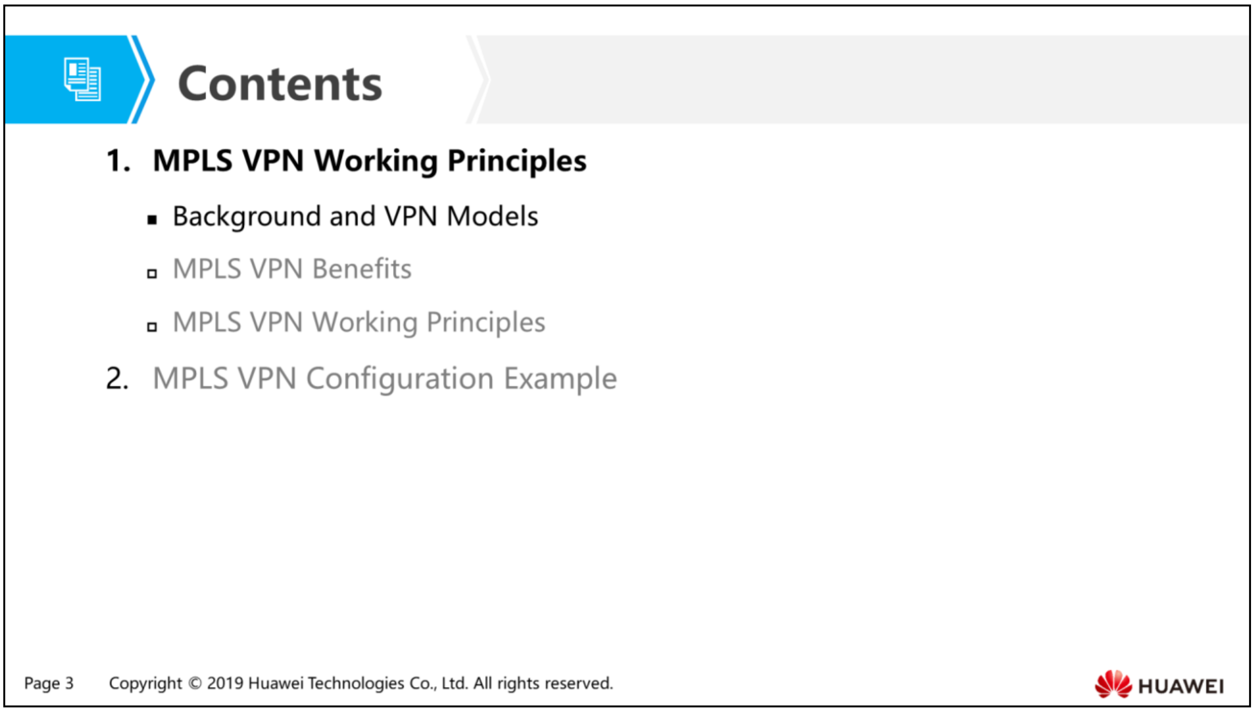
Foreword

- As the hardware performance is improved, Multiprotocol Label Switching (MPLS) no longer shows its advantages in data forwarding speed. However, MPLS is still widely used in new applications, such as virtual private network (VPN) and traffic engineering (TE) because it supports multi-layer labels and forwarding-control separation.
- Due to defects of traditional VPN, many customer requirements cannot be met during network deployment. MPLS VPN integrates two traditional VPN models, promoting the development of VPN.



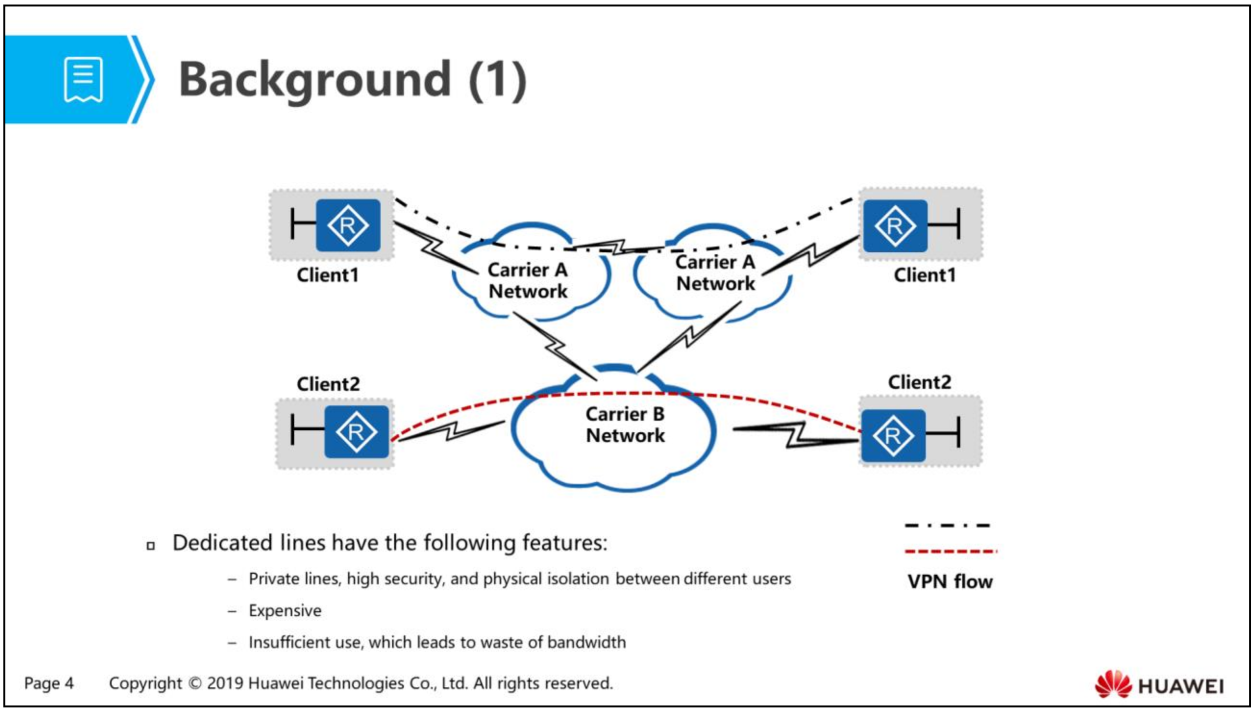
Objectives

- Upon completion of this section, you will be able to:
  - Understand the traditional VPN models
  - Master the working principles of MPLS VPN
  - Master the basic configuration of MPLS VPN



Contents

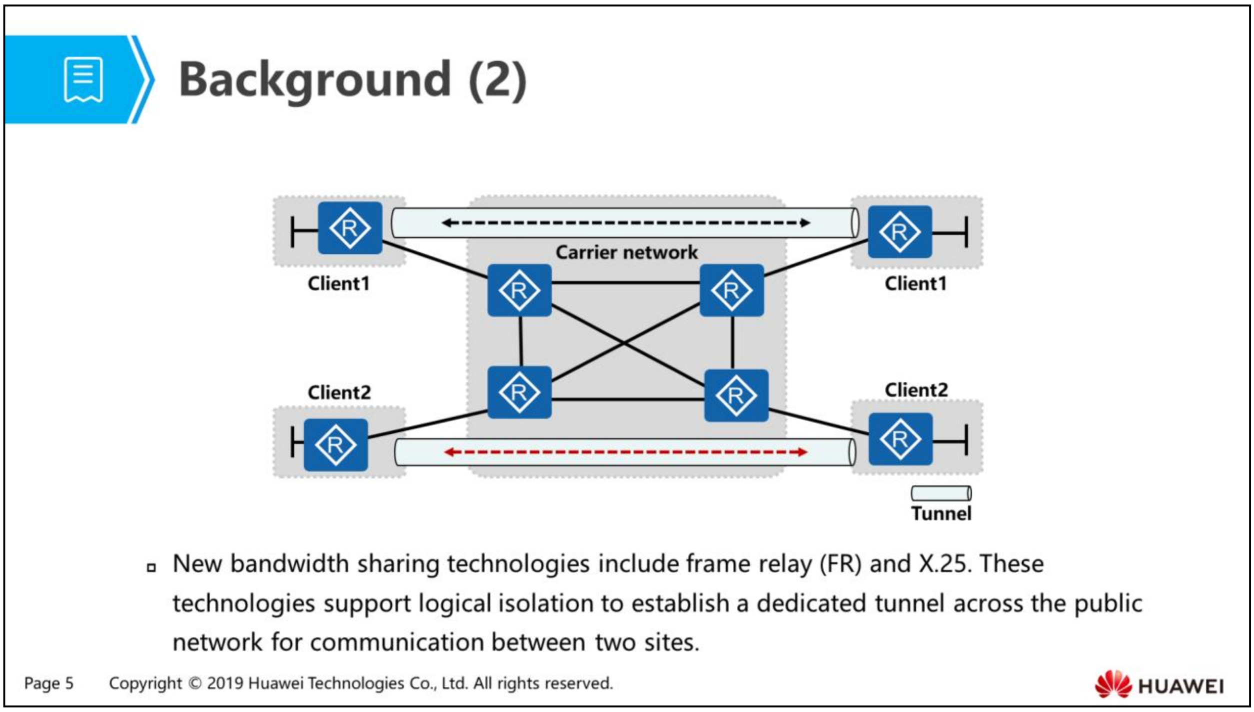
1. **MPLS VPN Working Principles**
   - Background and VPN Models
   - MPLS VPN Benefits
   - MPLS VPN Working Principles
2. MPLS VPN Configuration Example



Background (1)

- Dedicated lines have the following features:
  - Private lines, high security, and physical isolation between different users
  - Expensive
  - Insufficient use, which leads to waste of bandwidth

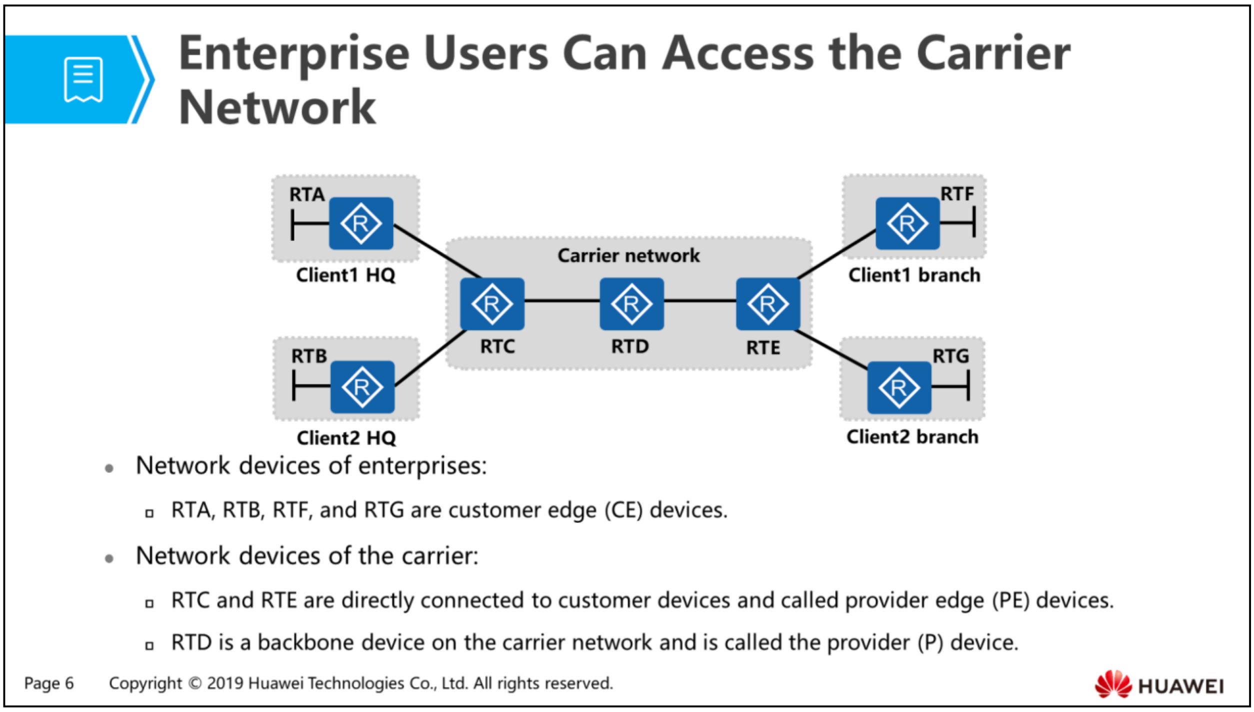
- In the past, dedicated lines are used to enable two sites to communicate with each other across the public network and protect private network security. Due to defects of traditional dedicated lines, some new bandwidth sharing technologies along with the multiplexing technology gradually replace traditional dedicated lines.



Background (2)

- New bandwidth sharing technologies include frame relay (FR) and X.25. These technologies support logical isolation to establish a dedicated tunnel across the public network for communication between two sites.

- The bandwidth sharing technologies can improve bandwidth utilization and are cost-effectiveness compared with dedicated lines. Therefore, they are frequently used to construct VPN networks in the early stage.
- VPN networks have the following features:
  - Use the shared public network to implement connections between private networks.
  - The private networks are invisible to each other.

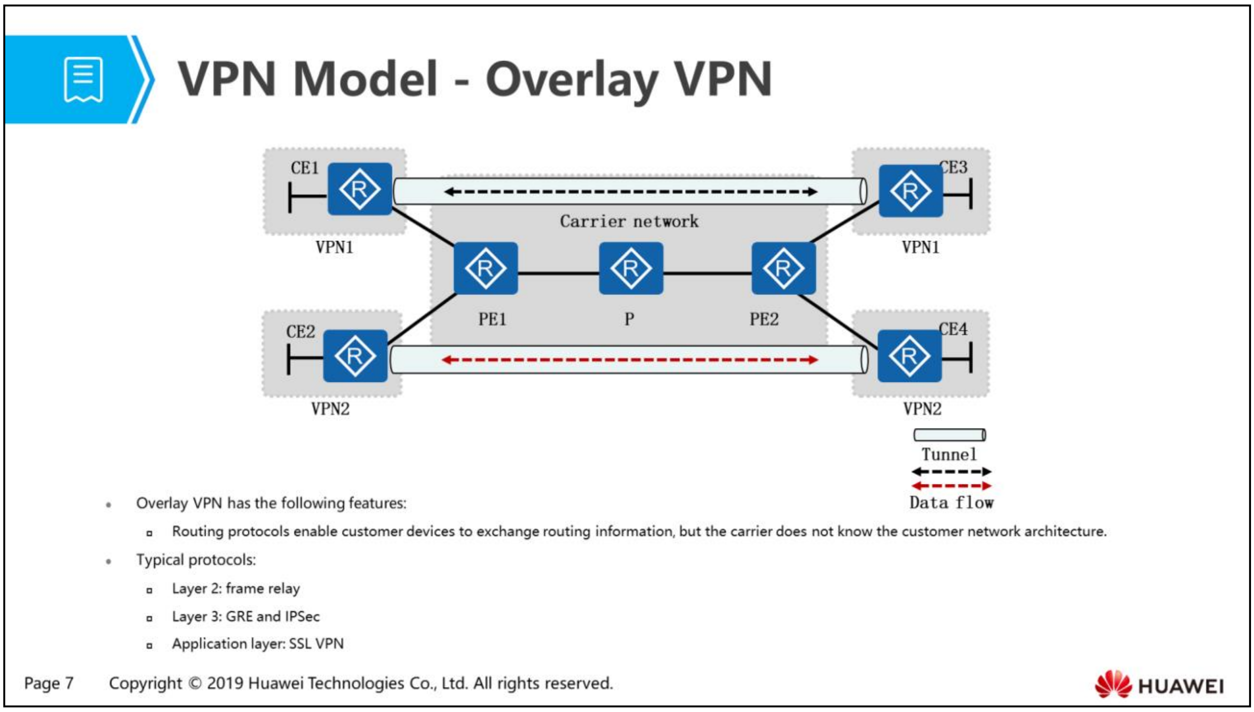


Enterprise Users Can Access the Carrier Network

- Network devices of enterprises:
  - RTA, RTB, RTF, and RTG are customer edge (CE) devices.
- Network devices of the carrier:
  - RTC and RTE are directly connected to customer devices and called provider edge (PE) devices.
  - RTD is a backbone device on the carrier network and is called the provider (P) device.

Page 6

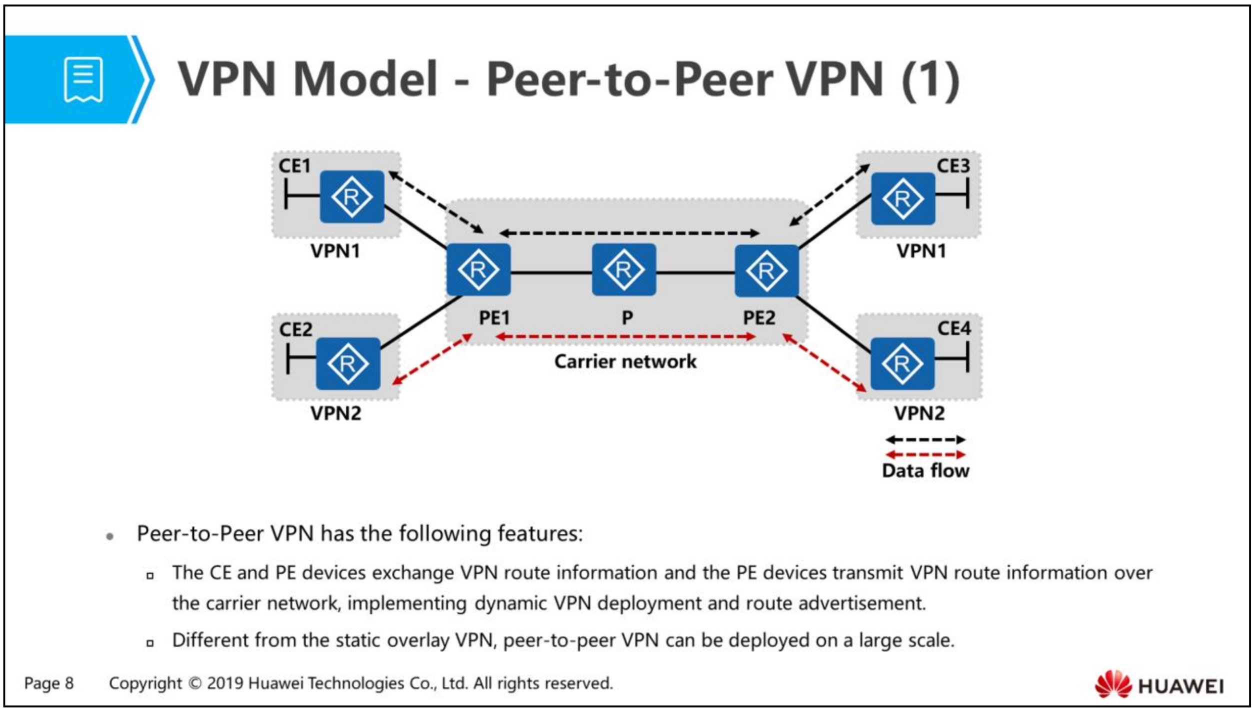
- As shown in the figure, the functions of each device are as follows:
  - Customer Edge (CE): a device that is deployed at the edge of a customer network and has interfaces directly connected to the carrier network. A CE device can be an SVN, a switch, or a host. Generally, CE devices do not detect VPNs and do not need to support MPLS.
  - Provider edge (PE): a device at the edge of a carrier network, directly connected to a CE device. On an MPLS network, PE devices are responsible for processing all VPN services.
  - P: It is a backbone device on the carrier network. A P device is not directly connected to CE devices. P devices only need to provide basic MPLS forwarding and do not maintain VPN information.
- The area in which CE devices are located is called a site. A site is a group of IP systems with IP connectivity that can be achieved independent of carrier networks.



VPN Model - Overlay VPN

- Overlay VPN has the following features:
  - Routing protocols enable customer devices to exchange routing information, but the carrier does not know the customer network architecture.
- Typical protocols:
  - Layer 2: frame relay
  - Layer 3: GRE and IPSec
  - Application layer: SSL VPN

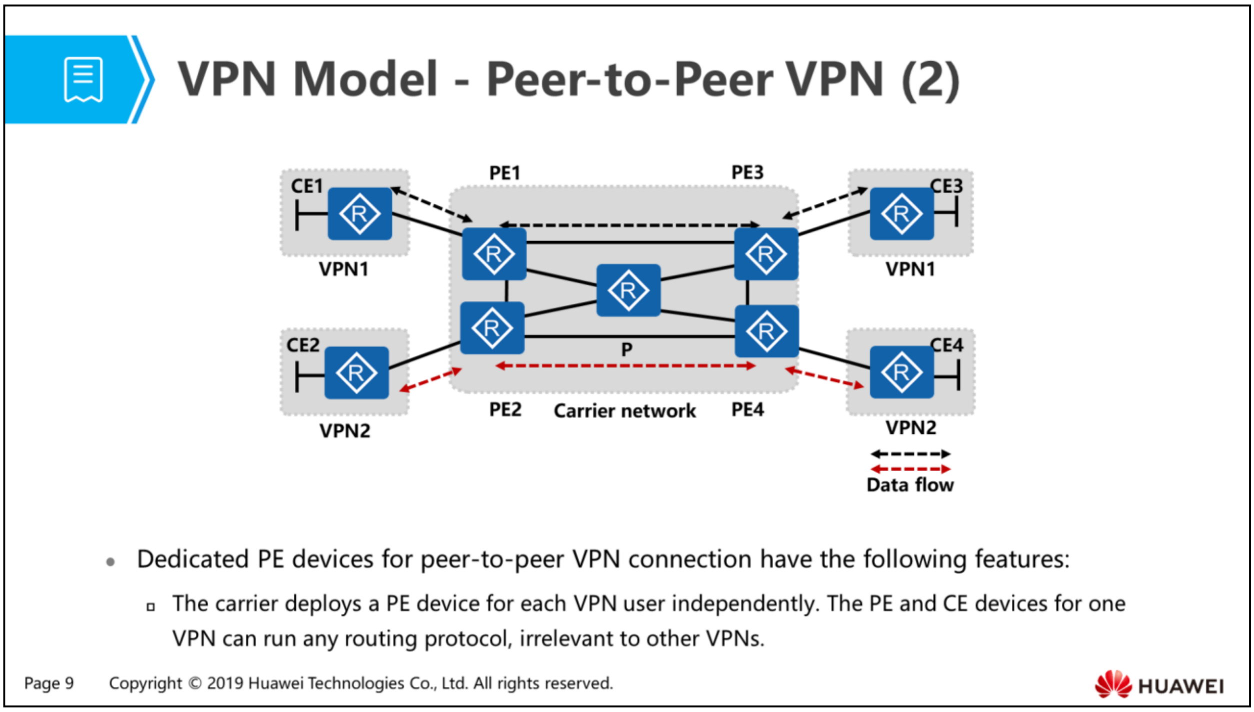
- Overlay VPN can establish a tunnel between two CE devices or two PE devices.
  - A tunnel established between two CE devices can directly transmit route information, so the carrier network cannot detect routing protocol data exchanged between CE devices.
    - Advantages: Customers can use overlapping address spaces. The confidentiality and security is high.
    - Disadvantage: The VPN is a static VPN, which cannot reflect network changes in real time. When a new site is created, you need to manually set up connections to this new site on all existing sites. The configuration and maintenance are complex and the management is difficult.
  - A tunnel can be established for each VPN user between two PE devices to directly transmit route information, so the P device on the public network cannot detect VPN route information.
    - Advantages: The carrier is responsible for creation and maintenance of VPNs. The confidentiality and security is relatively high.
    - Disadvantages: Different VPN users cannot share the same address space.



VPN Model - Peer-to-Peer VPN (1)

- Peer-to-Peer VPN has the following features:
  - The CE and PE devices exchange VPN route information and the PE devices transmit VPN route information over the carrier network, implementing dynamic VPN deployment and route advertisement.
  - Different from the static overlay VPN, peer-to-peer VPN can be deployed on a large scale.

- As shown in the preceding figure, CE devices of all VPN users connect to the same PE device. The CE devices run different routing protocols or different processes of the same routing protocol to communicate with the PE device. The source PE device advertises the routes to the public network, and the destination PE device filters received routes and sends them to the corresponding CE devices.
- In peer-to-peer VPN, the CE and PE devices exchange VPN route information and the PE devices transmit VPN route information over the carrier network. VPN routes are automatically transmitted to the PE devices because the PE and CE devices run routing protocols. A strict route filtering and selection mechanism is required to control transmission of VPN routes.
  - Disadvantages:
    - A large number of access control lists (ACLs) must be configured on the PE devices to prevent communication between different CE devices connected to the same PE device, resulting in heavy management workload of the PE device.
    - The PE device cannot identify VPN users if they use overlapping addresses.
- In this figure, peer-to-peer VPNs connect to the PE device in shared mode. To simplify configuration and management, you can connect peer-to-peer VPNs to dedicated PE devices.



VPN Model - Peer-to-Peer VPN (2)

- Dedicated PE devices for peer-to-peer VPN connection have the following features:
  - The carrier deploys a PE device for each VPN user independently. The PE and CE devices for one VPN can run any routing protocol, irrelevant to other VPNs.

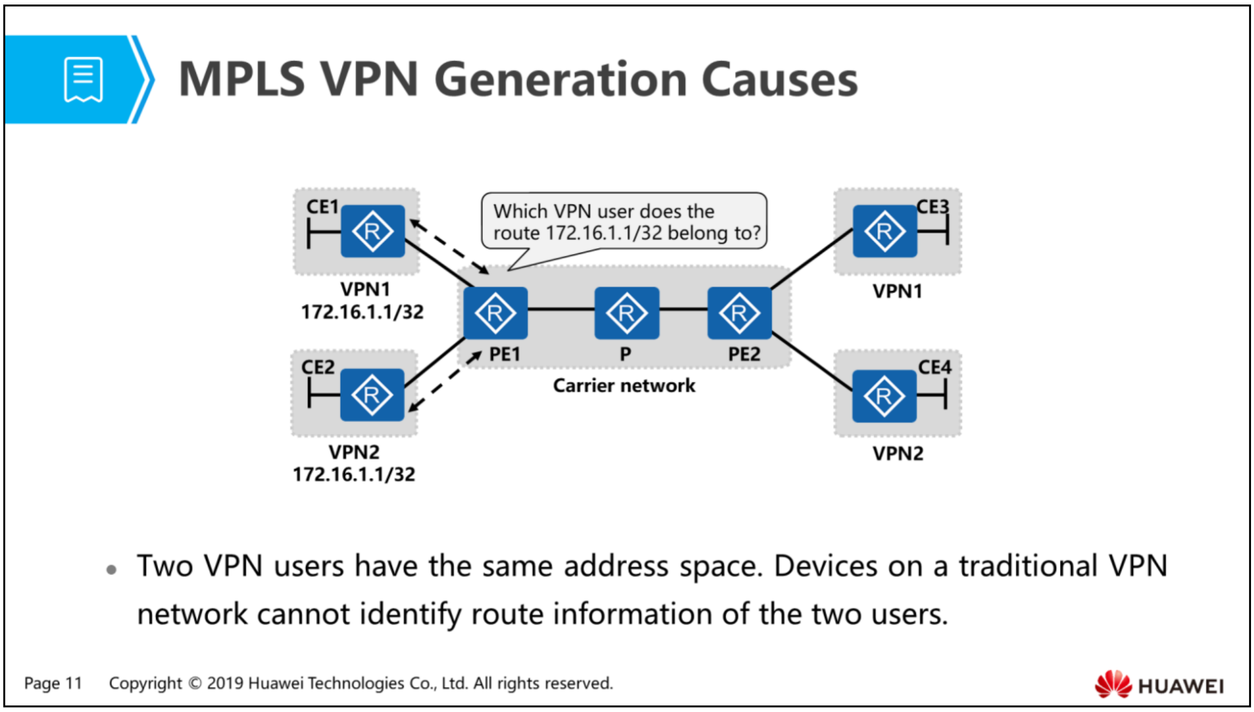
Page 9

HUAWEI

- Dedicated PE devices for peer-to-peer VPN connection have the following features:
  - Advantages: You do not need to configure any ACL, so the configuration and management are simplified.
  - Disadvantages: A dedicated PE device is required for each newly added VPN site, leading to high costs. In addition, VPN users cannot use overlapping address spaces.

Contents

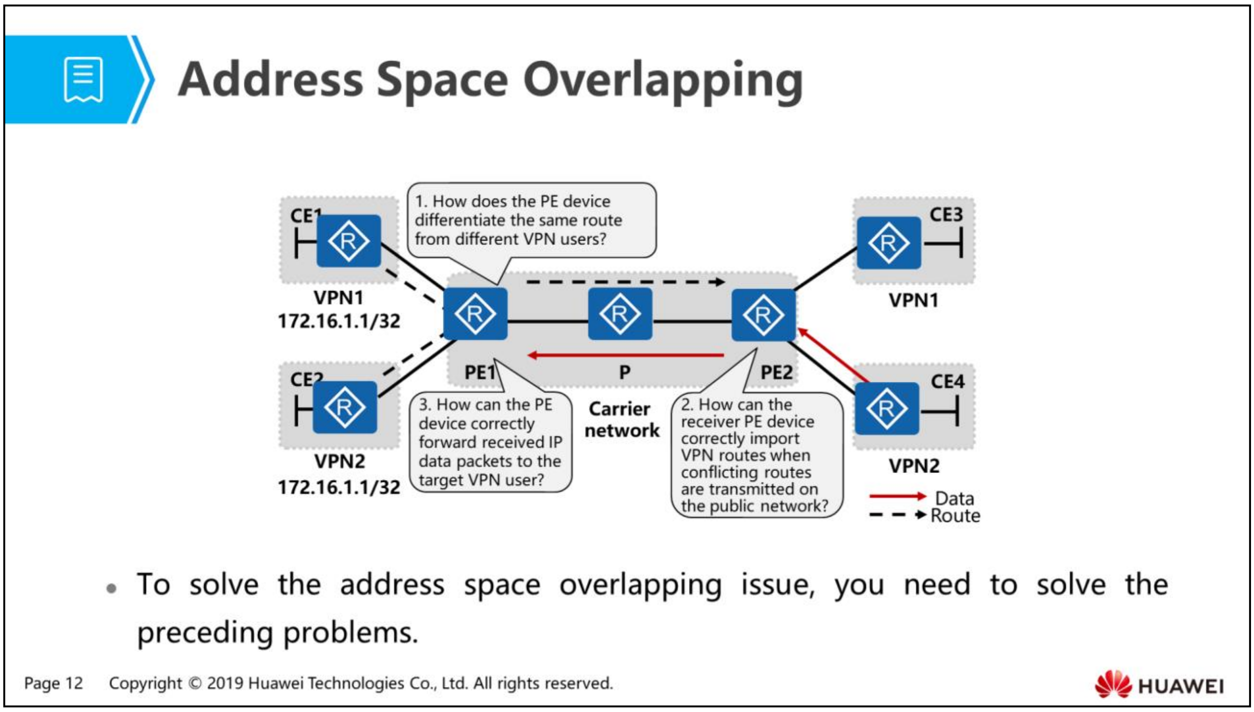
1. **MPLS VPN Working Principles**
   - ▫ Background and VPN Models
   - ▪ MPLS VPN Benefits
   - ▫ MPLS VPN Working Principles
2. MPLS VPN Configuration Example



MPLS VPN Generation Causes

- Two VPN users have the same address space. Devices on a traditional VPN network cannot identify route information of the two users.

- Due to defects of the traditional VPN technology, many customer networking requirements cannot be met or the implementation is complex. MPLS VPN addresses the problems caused by address space overlapping, which are the inherent defects of the traditional VPN technology.



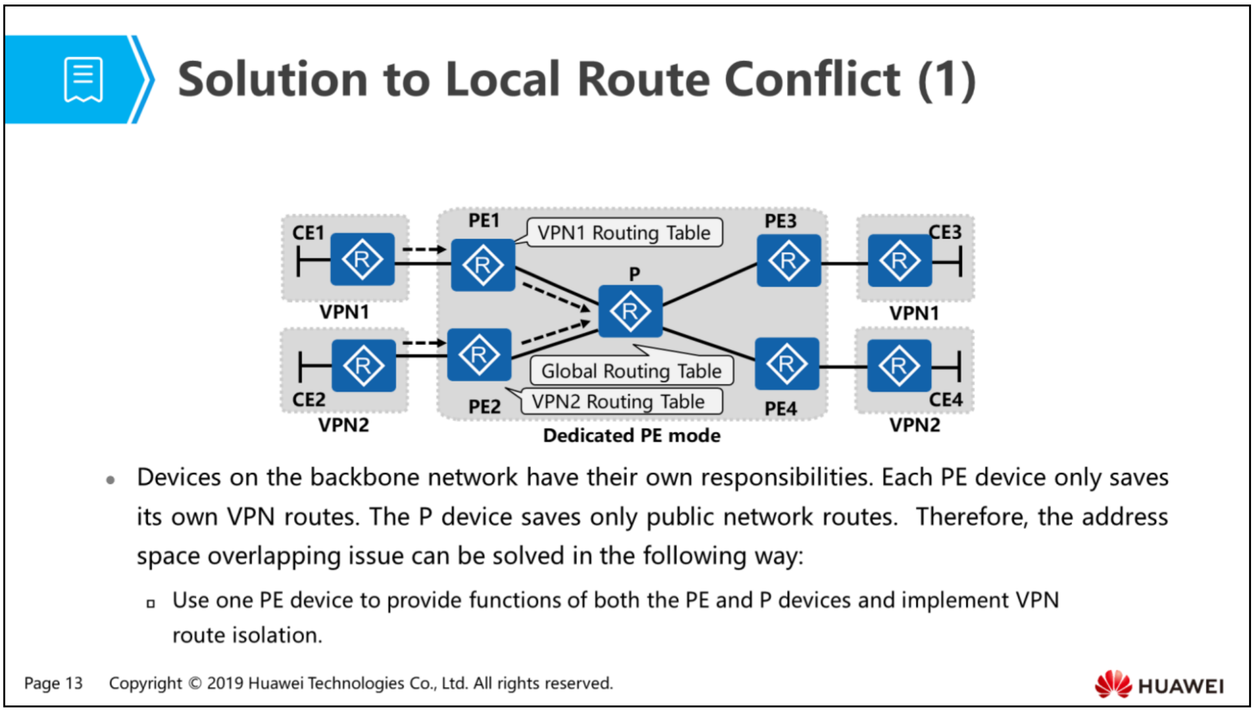
Address Space Overlapping

CE1
VPN1
172.16.1.1/32
CE2
VPN2
172.16.1.1/32
1. How does the PE device differentiate the same route from different VPN users?
PE1
P
PE2
Carrier network
3. How can the PE device correctly forward received IP data packets to the target VPN user?
2. How can the receiver PE device correctly import VPN routes when conflicting routes are transmitted on the public network?
CE3
VPN1
CE4
VPN2
Data
Route

- To solve the address space overlapping issue, you need to solve the preceding problems.

Page 12 HUAWEI

- Analysis on the preceding technical difficulties shows that route is the major concern, so we need to take routing protocols into consideration. The currently used routing protocols cannot solve these problems, so a new routing protocol is required.
- BGP provides solutions to these problems thanks to the following advantages:
  - BGP is the unique routing protocol that supports a large number of VPN routes.
  - BGP packets use the TLV structure, which facilitates expansion.
  - BGP can transmit any additional information attached to route information as optional attributes to BGP neighbors.
- The above mentioned three technical difficulties can be solved easily:
  - Different VPN routes can be created on one PE device to solve the issue of local route conflict.
  - Identifiers can be added to different VPN routes during route advertisement. The identifier can be transmitted as the BGP attribute.
  - The IP packets cannot be changed, but information can be added before the IP packet header. A sender adds a label to the IP packets and the receiver forwards the packets to the correct VPN based on the label in the received packets.
- The following pages describe solutions to these problems one by one.



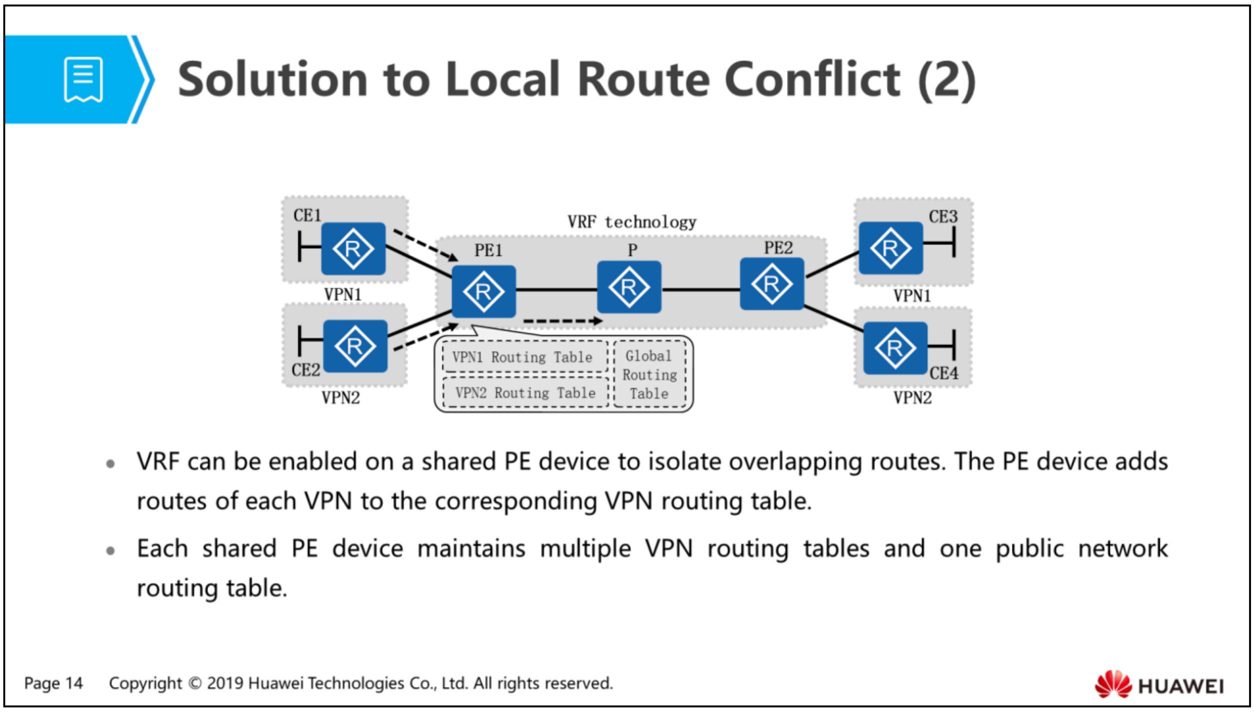
Solution to Local Route Conflict (1)

Dedicated PE mode

- Devices on the backbone network have their own responsibilities. Each PE device only saves its own VPN routes. The P device saves only public network routes. Therefore, the address space overlapping issue can be solved in the following way:
  - Use one PE device to provide functions of both the PE and P devices and implement VPN route isolation.

Page 13

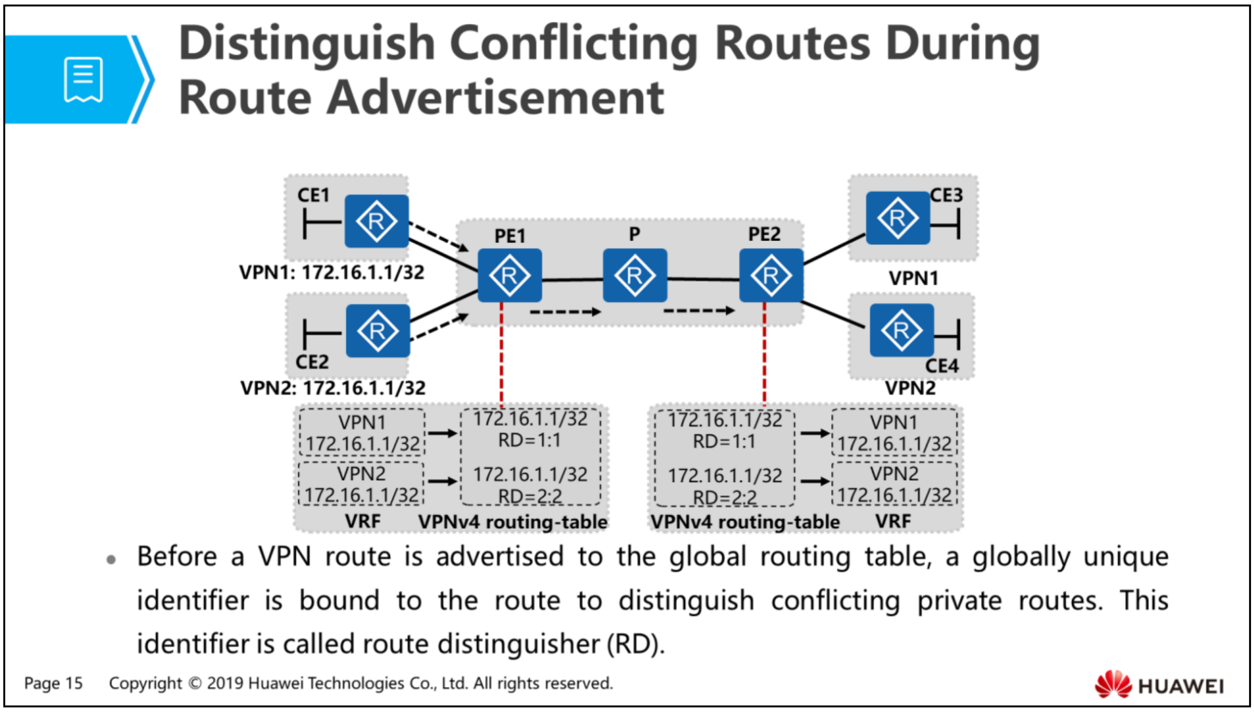
- The traditional VPN solves the address space overlapping issue by using ACLs and NAT. However, these methods cannot completely solve the problem. Theoretical breakthroughs are in urgent need. Devices on the backbone network have their own responsibilities. Each PE device only saves its own VPN routes. The P device saves only public network routes. Inspired by these, the functions of dedicated PE devices and the P device can be integrated on one PE device.



Solution to Local Route Conflict (2)

- VRF can be enabled on a shared PE device to isolate overlapping routes. The PE device adds routes of each VPN to the corresponding VPN routing table.
- Each shared PE device maintains multiple VPN routing tables and one public network routing table.

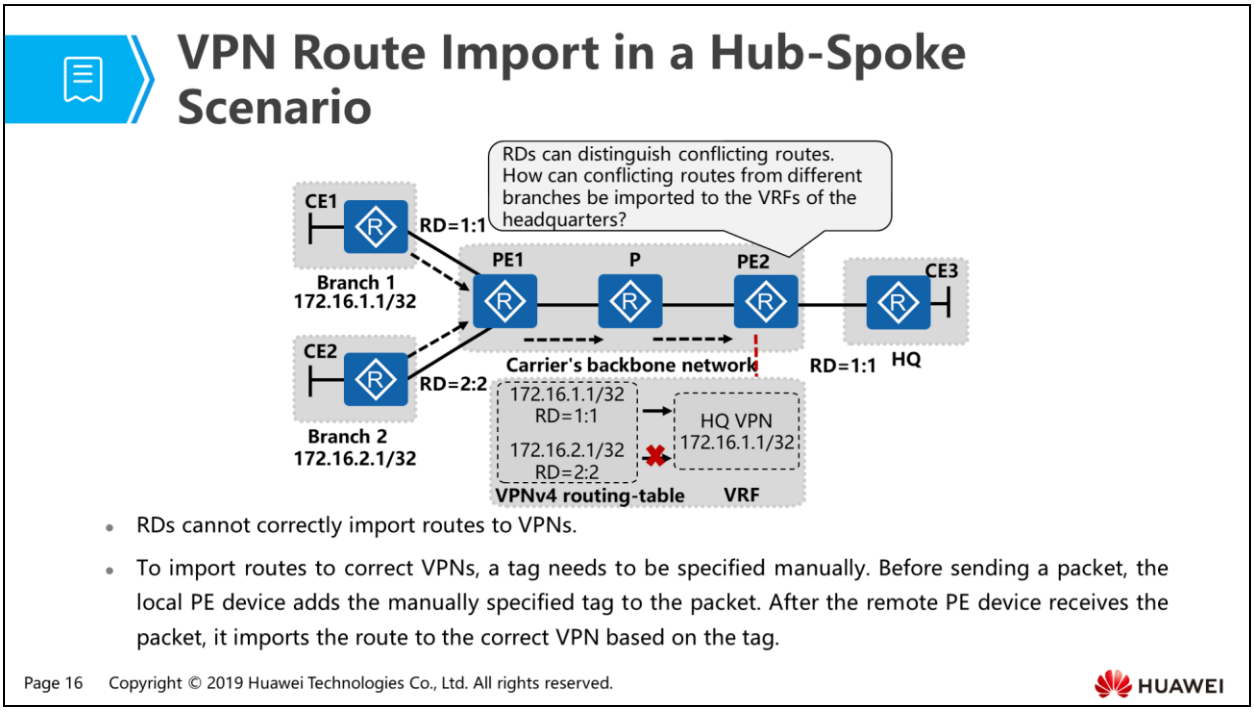
- A shared PE device isolates overlapping routes by adding routes of each VPN to the corresponding VPN routing table. Each VPN routing table records only routes learned from the corresponding VPN, providing the same function as a dedicated PE device. The VPN routing table is the VPN routing and forwarding table (VRF).
- Each VRF maps to a VPN instance. The corresponding interface connecting to a VPN user needs to be bound to a VPN instance.
- Each PE device maintains one or multiple VPN instances and a public network routing table (also known as the global routing table). The VPN instances are independent of each other. It is easy to create VPN instances, but specific policies need to be configured on each PE device to coordinate the relationship between each VPN instance and the global routing table.



Distinguish Conflicting Routes During Route Advertisement

- Before a VPN route is advertised to the global routing table, a globally unique identifier is bound to the route to distinguish conflicting private routes. This identifier is called route distinguisher (RD).

- An RD is a VPN route identifier consisting of eight bytes. On the same PE device, the RD for each VPN must be unique.
- RDs distinguish the IPv4 prefixes with the same address space. IPv4 addresses with RDs are VPN-IPv4 addresses (VPNv4 addresses).
- Devices on the carrier network use Multiprotocol Extensions for BGP (MP-BGP) to transmit VPN routes. After a PE device receives IPv4 private routes from a CE device, it adds identifiers to the private routes to convert them to VPNv4 routes and adds them to the VPNv4 routing table of MP-BGP. The VPNv4 routes are transmitted over the public network through MP-BGP.



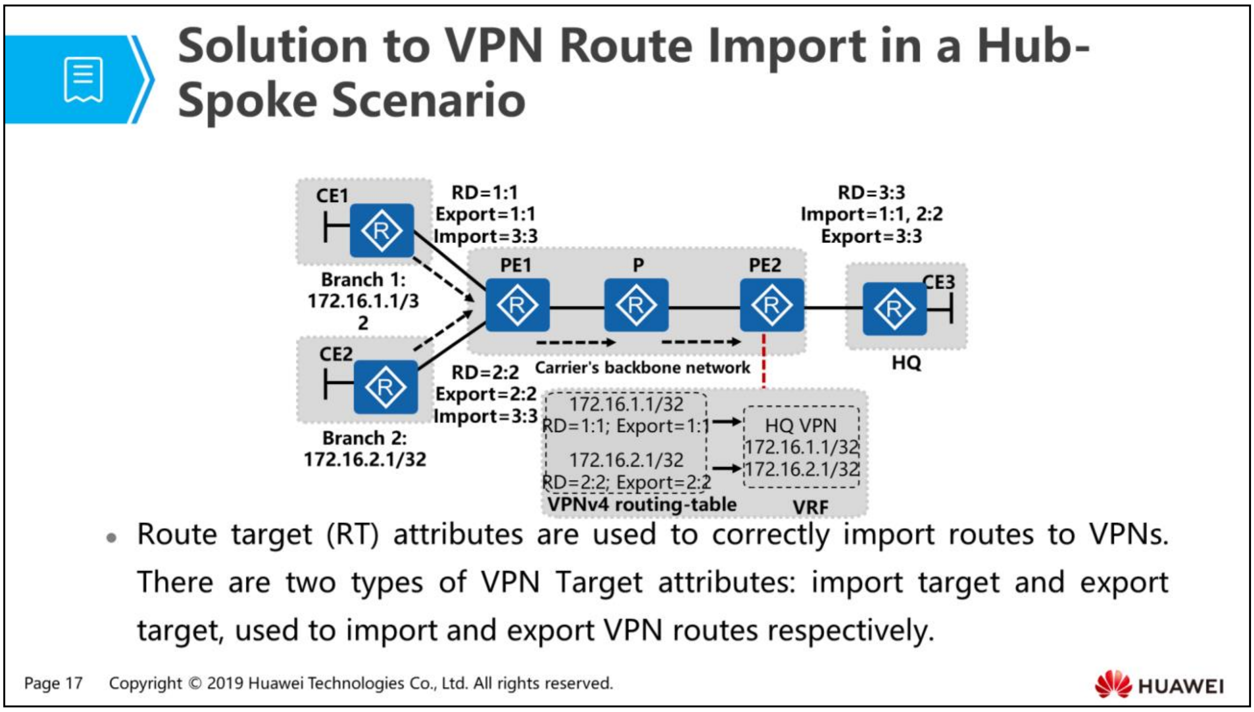
VPN Route Import in a Hub-Spoke Scenario

RDs can distinguish conflicting routes. How can conflicting routes from different branches be imported to the VRFs of the headquarters?

- RDs cannot correctly import routes to VPNs.
- To import routes to correct VPNs, a tag needs to be specified manually. Before sending a packet, the local PE device adds the manually specified tag to the packet. After the remote PE device receives the packet, it imports the route to the correct VPN based on the tag.

Page 16

- As shown in the preceding figure, users in branch 1 and branch 2 use private addresses 172.16.1.1/32 and 172.16.2.1/32, respectively. The enterprise requires that the branches can communicate with the headquarters but branches cannot communicate with each other. The VPN RD assigned to branch 1 is 1:1, and the VPN RD assigned to branch 2 is 2:2. If you want to import routes to correct VPNs based on the RDs, the RD value for communication between the headquarters and branch 1 needs to be 1:1, and the RD value for communication between the headquarters and branch 2 needs to be 2:2. However, the RD value is unique on a local PE device, and only one RD value can be configured on each PE device. Therefore, the RDs cannot be used to solve the problem of route import to VPN.



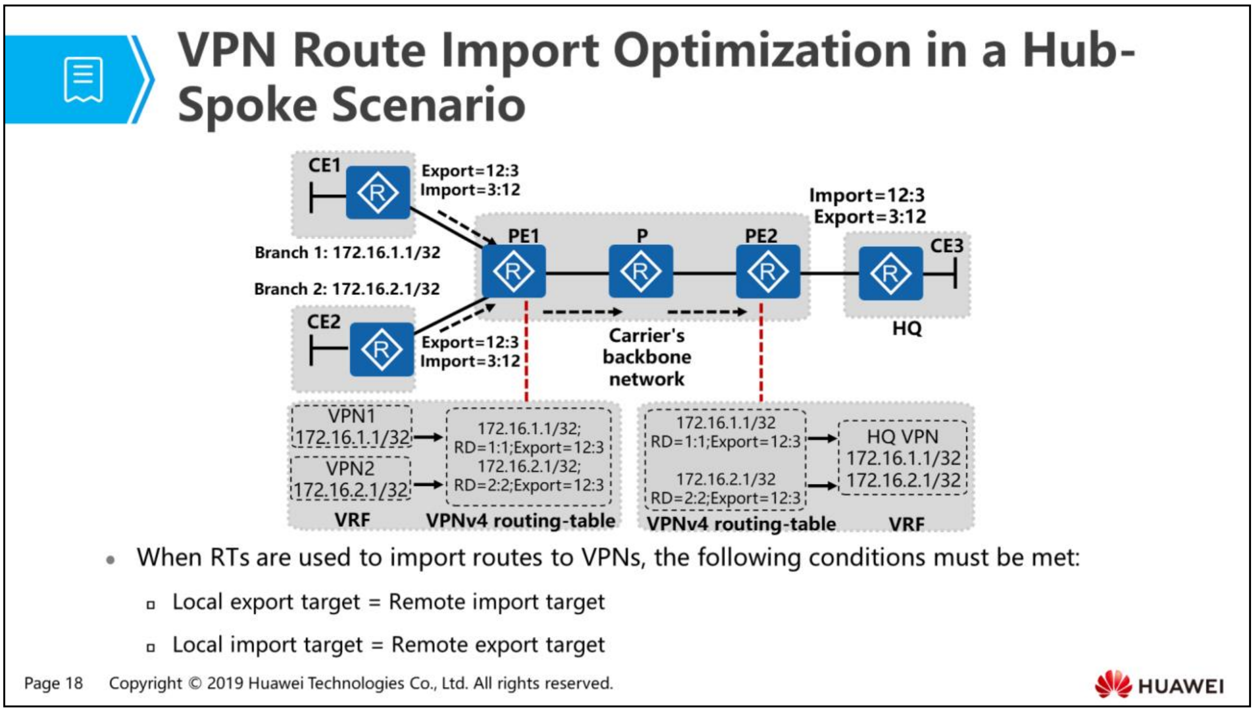
Solution to VPN Route Import in a Hub-Spoke Scenario

- Route target (RT) attributes are used to correctly import routes to VPNs. There are two types of VPN Target attributes: import target and export target, used to import and export VPN routes respectively.

Page 17

HUAWEI

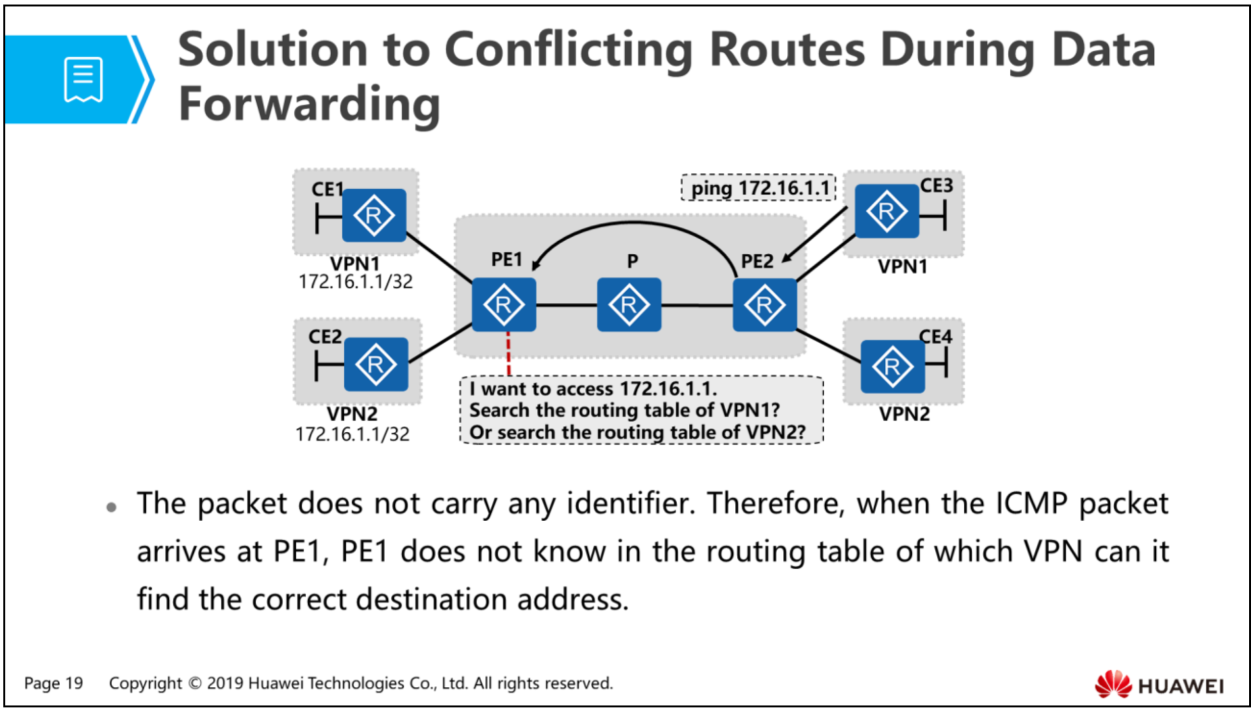
- As shown in the preceding figure, the enterprise requires that both branch 1 and branch 2 can communicate with the headquarters, but branches 1 and 2 cannot communicate with each other. Assume that the export target and import target for branch 1 is 1:1 and 3:3; the export target and import target for branch 2 is 2:2 and 3:3; the export target and import target for the headquarters is 3:3 and 1:1 and 2:2. After PE2 receives a VPNv4 route from PE1, PE2 checks the Export Target. Because the import target of the headquarters is 1:1 and 2:2, routes with the RT value 1:1 or 2:2 are imported to the headquarters VRF. The process of importing VPNv4 routes of PE1 to each branch VRF is similar.
- RTs are encapsulated in the BGP extended community attribute and are transmitted as an optional attribute.
- There are two types of RT attributes:
  - Export target: This attribute is added when a local route is exported from a VRF and converted to a VPNv4 route.
  - Import target: When a remote device receives a route, it checks the export target attribute in the route. If this attribute matches Import Target of a VPN instance on a PE, the PE adds the route to the corresponding VPN instance.



VPN Route Import Optimization in a Hub-Spoke Scenario

- When RTs are used to import routes to VPNs, the following conditions must be met:
  - Local export target = Remote import target
  - Local import target = Remote export target

- As shown in the following figure, the import target assigned to all branches is 3:12 and the export target is 12:3. The two values are opposite to those assigned to the headquarters, so all the branches can only communicate with the headquarters.



Solution to Conflicting Routes During Data Forwarding

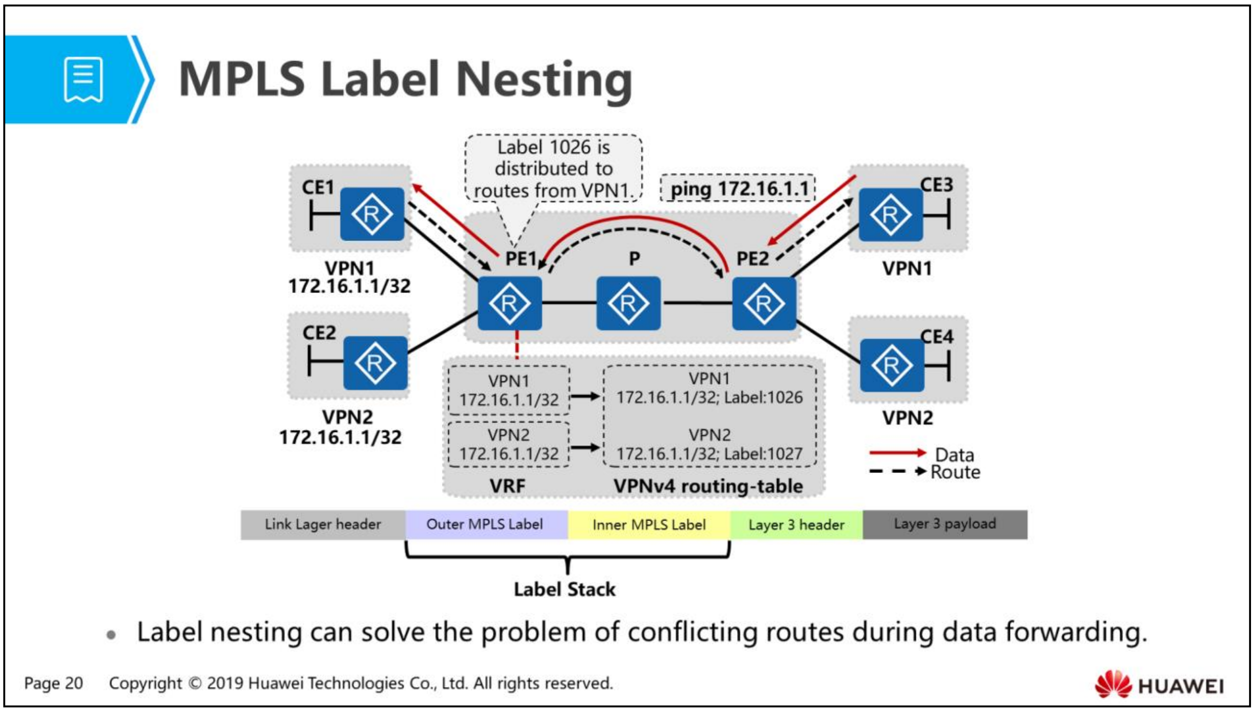
ping 172.16.1.1

I want to access 172.16.1.1.
Search the routing table of VPN1?
Or search the routing table of VPN2?

- The packet does not carry any identifier. Therefore, when the ICMP packet arrives at PE1, PE1 does not know in the routing table of which VPN can it find the correct destination address.

HUAWEI

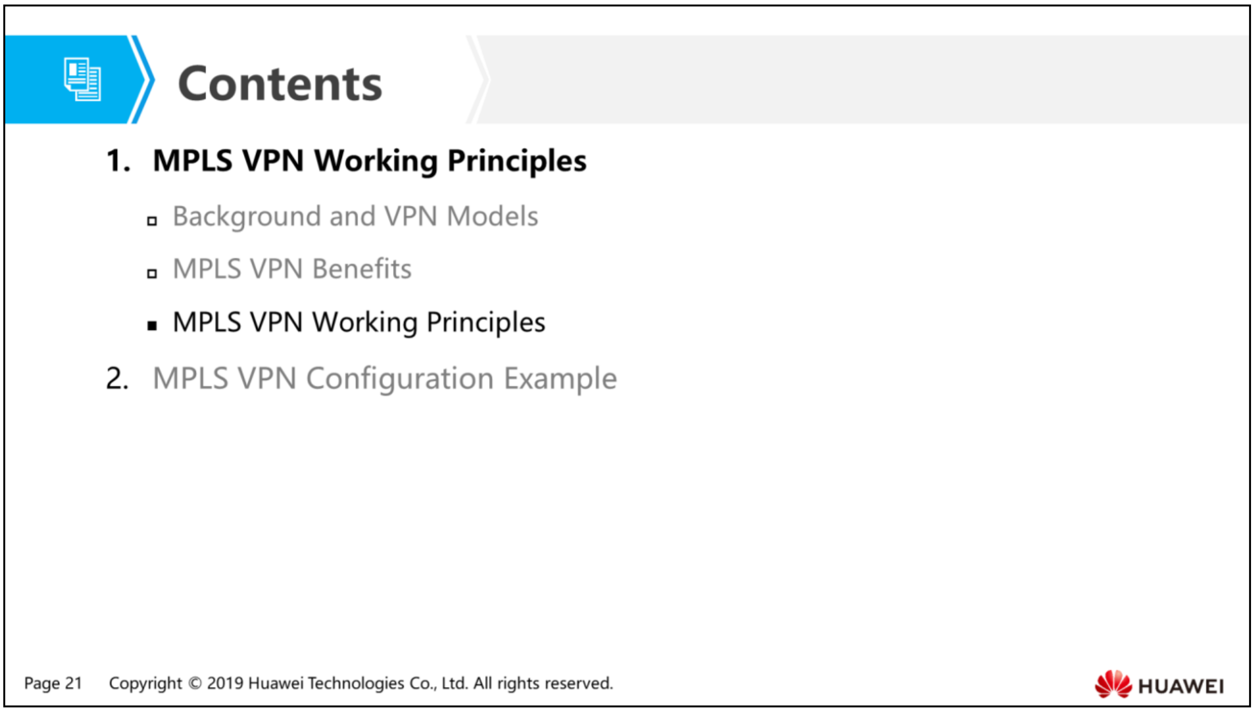
- Two solutions to this problem are as follows:
  - Add identifier information to the packet and use the RD to distinguish the VPN to which the packet belongs. The RD information is contained in the packet during data forwarding. The disadvantages are that the 8-byte RD increases the data size and lowers forwarding efficiency.
  - Use the MPLS protocol to establish a tunnel over the public network and forward the packet over the tunnel based on labels. MPLS labels can be nested in one another, so the label identifying the VPN to which the packet belongs can be encapsulated in the public network label.



MPLS Label Nesting

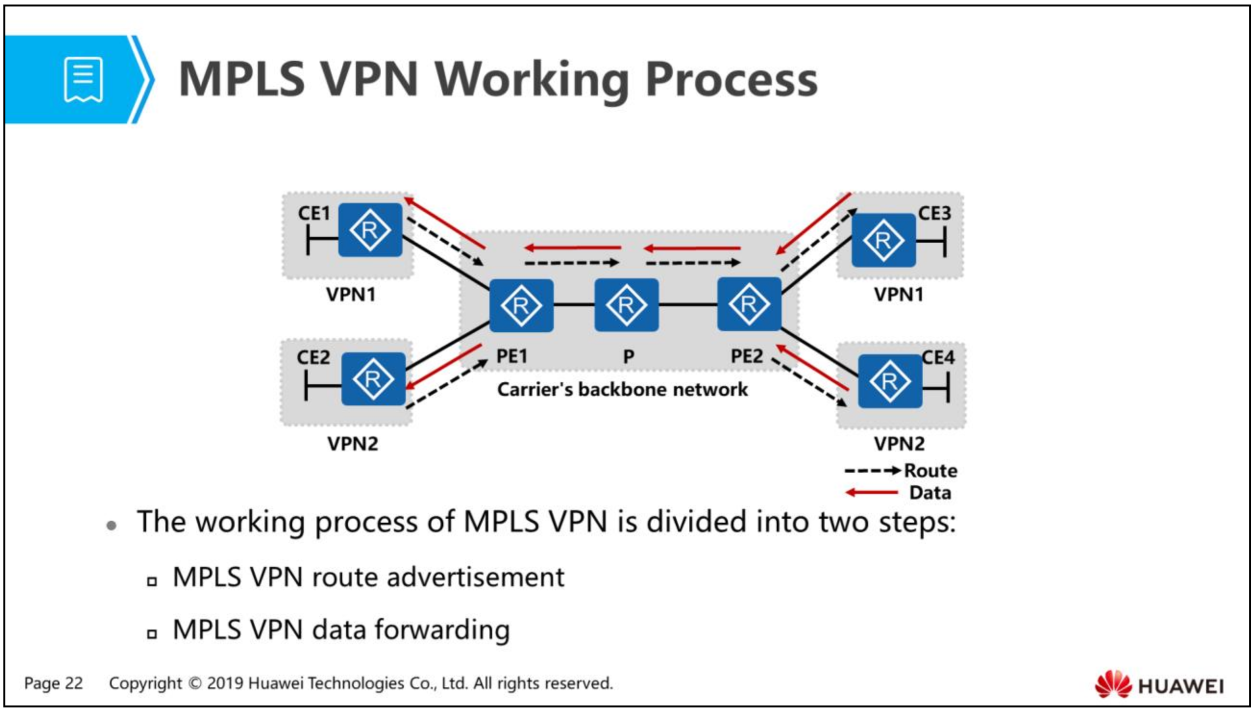
- Label nesting can solve the problem of conflicting routes during data forwarding.

- In MPLS VPN, an outer MPLS label is called the public network label, used for data forwarding over the MPLS network. Generally, the PHP node removes the outer label before sending packets to the last-hop PE device. The packets contain inner labels only. In MPLS VPN, an inner MPLS label is called the private network label, used to forward data to the corresponding VPN. The PE device determines the VPN to which a packet belongs based on the inner label.



Contents

1. **MPLS VPN Working Principles**
   - Background and VPN Models
   - MPLS VPN Benefits
   - MPLS VPN Working Principles
2. MPLS VPN Configuration Example



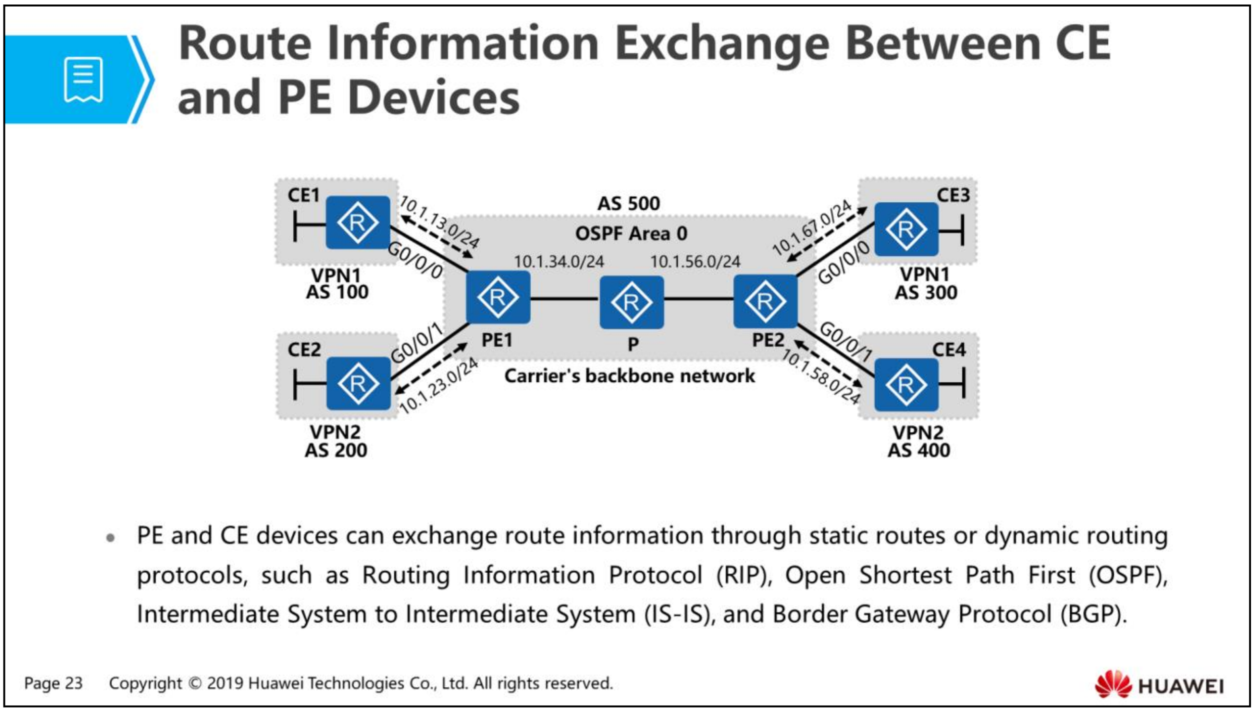
MPLS VPN Working Process

- The working process of MPLS VPN is divided into two steps:
  - MPLS VPN route advertisement
  - MPLS VPN data forwarding

Page 22

HUAWEI

- The MPLS VPN route advertisement process consists of four phases:
  - Route information exchange between CE and PE devices
  - VRF route injection to MP-BGP
  - Public network label distribution
  - MP-BGP route injection to VRF



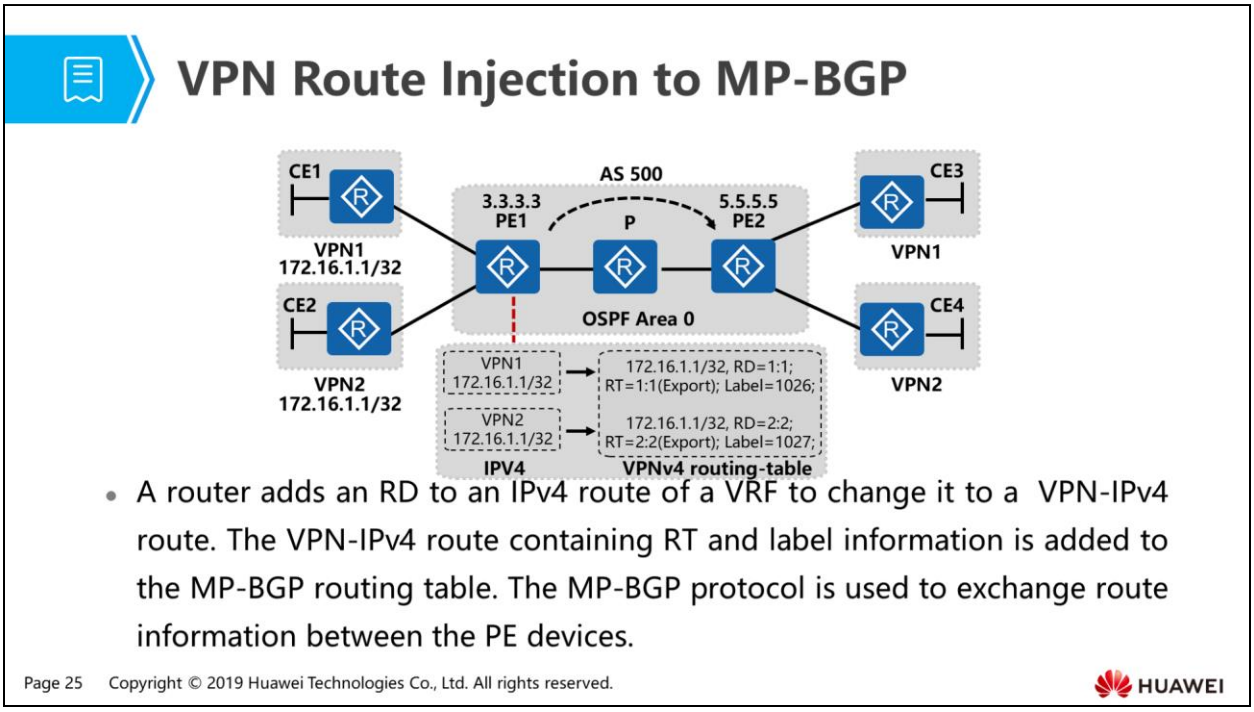
Route Information Exchange Between CE and PE Devices

- PE and CE devices can exchange route information through static routes or dynamic routing protocols, such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), and Border Gateway Protocol (BGP).

Page 23 HUAWEI

- As shown in the figure, the BGP protocol is used to exchange route information between CE1 and PE1. A instance named VPN1 is configured for VPN1, the RD is 1:1, and the RT is 1:1. The configuration commands are as follows:
  - Configurations on CE1:
    - bgp 100
    - peer 10.1.13.3 as-number 500
    - #
    - ipv4-family unicast
    - peer 10.1.13.3 enable
  - Configurations on PE1:
    - ip vpn-instance VPN1
    - ipv4-family
    - route-distinguisher 1:1
    - vpn-target 1:1 export-extcommunity
    - vpn-target 1:1 import-extcommunity
    - #

```
interface GigabitEthernet0/0/0
 ip binding vpn-instance VPN1
 ip address 10.1.13.3 255.255.255.0
#
bgp 500
#
 ipv4-family vpn-instance VPN1
  peer 10.1.13.1 as-number 100
```



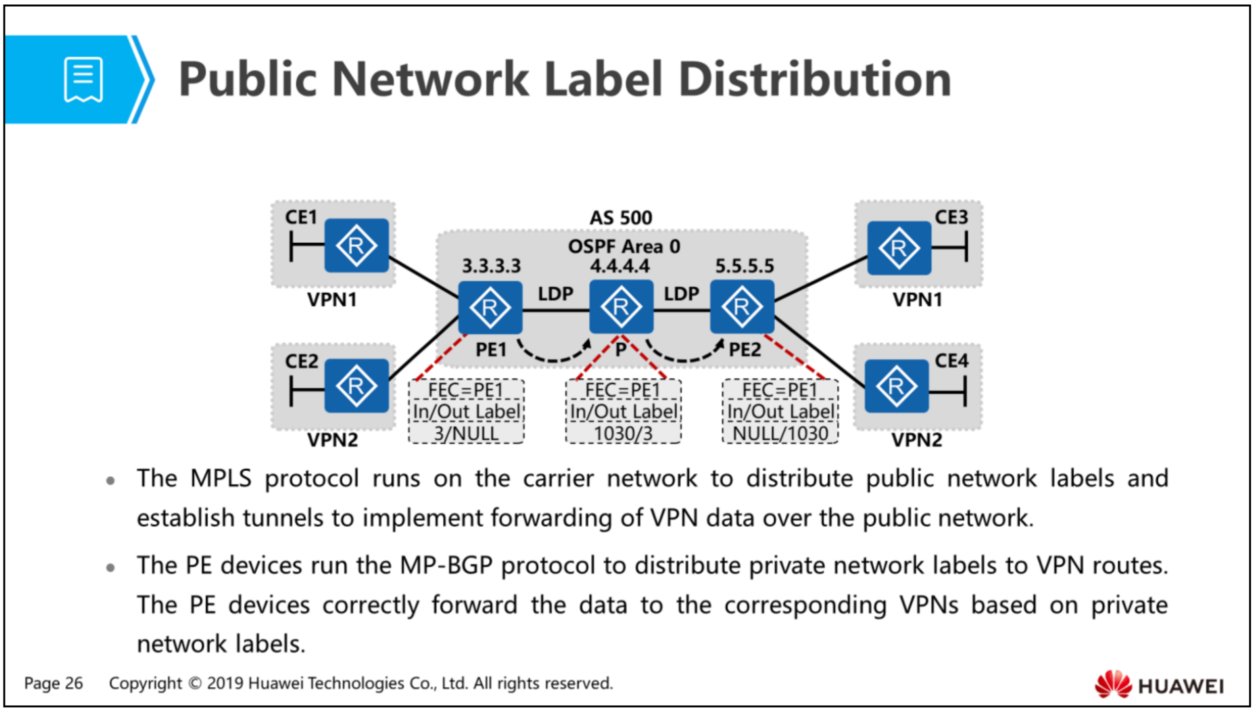
VPN Route Injection to MP-BGP

- A router adds an RD to an IPv4 route of a VRF to change it to a VPN-IPv4 route. The VPN-IPv4 route containing RT and label information is added to the MP-BGP routing table. The MP-BGP protocol is used to exchange route information between the PE devices.

Page 25 Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- The two PE devices run the MP-BGP protocol to transmit routes to each other over the public network. The configuration on PE1 is as follows:
  - bgp 500
  - peer 5.5.5.5 as-number 500
  - peer 5.5.5.5 connect-interface LoopBack0
  - #
  - ipv4-family unicast
  - undo synchronization
  - peer 5.5.5.5 enable
  - #
  - ipv4-family vpnv4
  - policy vpn-target
  - peer 5.5.5.5 enable



Public Network Label Distribution

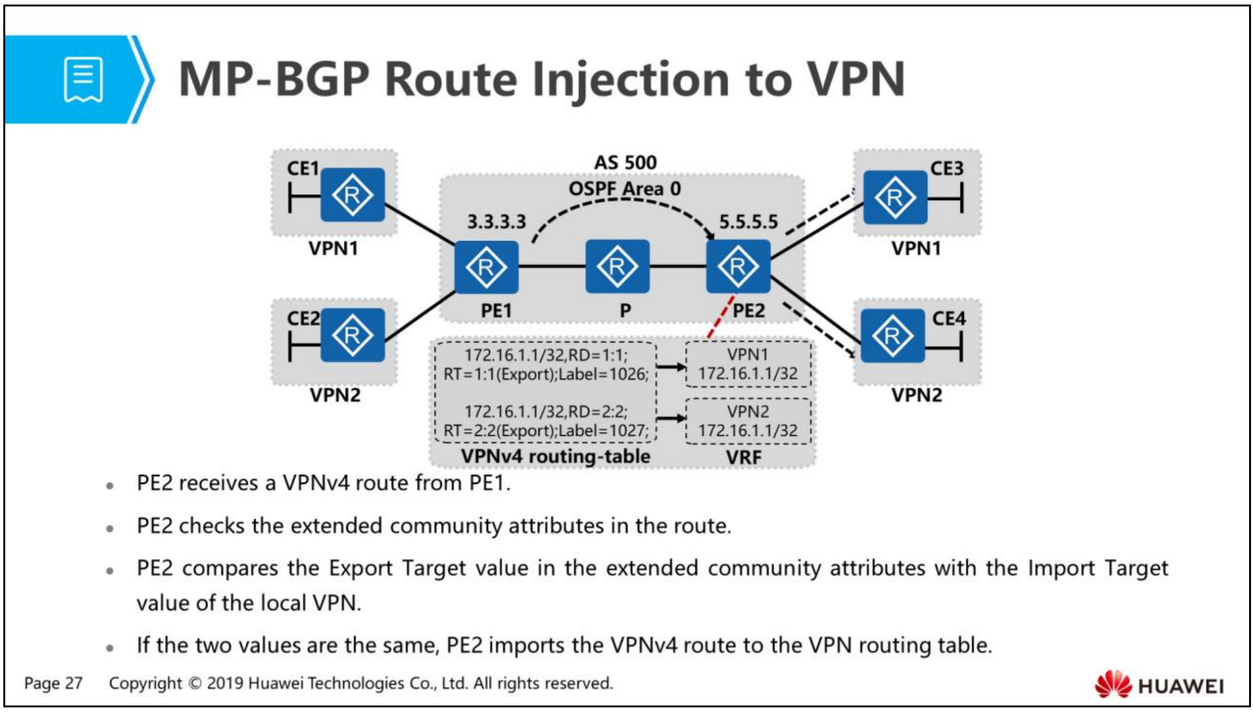
- The MPLS protocol runs on the carrier network to distribute public network labels and establish tunnels to implement forwarding of VPN data over the public network.
- The PE devices run the MP-BGP protocol to distribute private network labels to VPN routes. The PE devices correctly forward the data to the corresponding VPNs based on private network labels.

Page 26

HUAWEI

- An IGP protocol needs to be run on the PE and P devices on the backbone network to ensure route reachability over the carrier network. OSPF is used as an example in the preceding figure. The detailed configuration is not mentioned here.
- The PE and P devices need to run the LDP protocol to dynamically distribute labels and establish a tunnel. The configuration on the P device is as follows:

```
mpls lsr-id 4.4.4.4
mpls
mpls ldp
interface GigabitEthernet0/0/0
 ip address 10.1.34.4 255.255.255.0
 mpls
 mpls ldp
interface GigabitEthernet0/0/1
 ip address 10.1.45.4 255.255.255.0
 mpls
 mpls ldp
```



MP-BGP Route Injection to VPN

VPNv4 routing-table	VRF

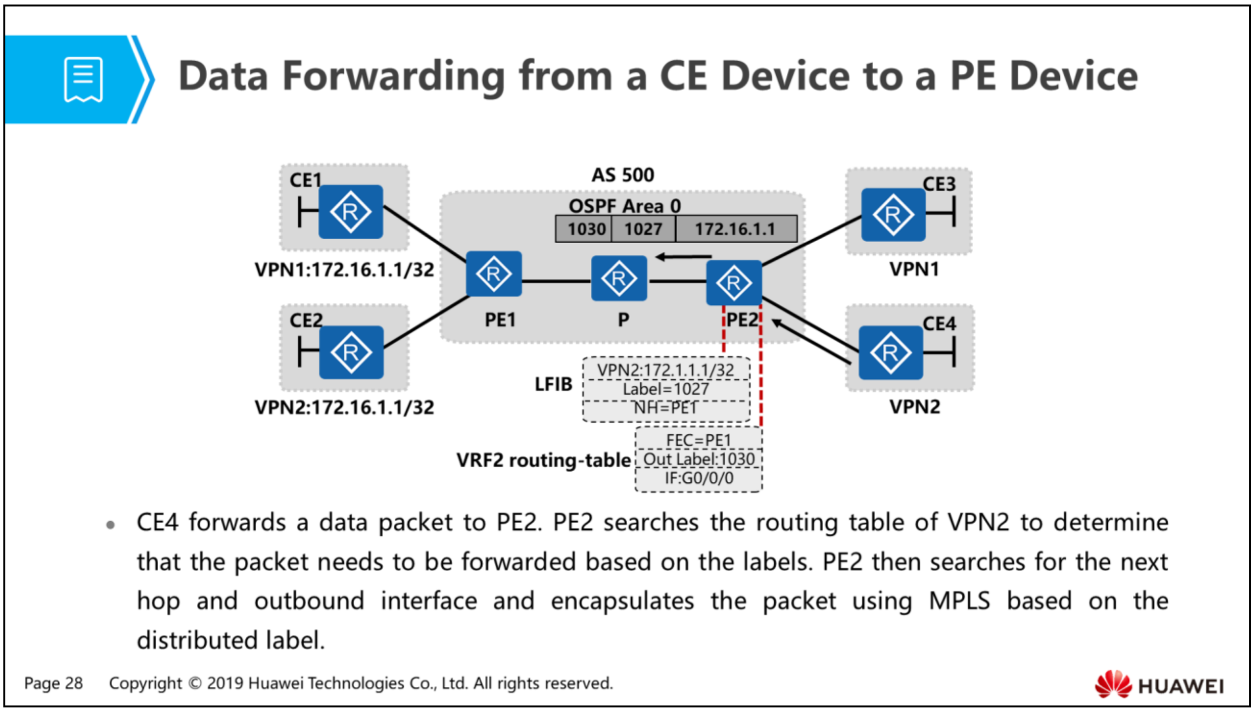
172.16.1.1/32,RD=1:1;
RT=1:1(Export);Label=1026;
	VPN1
	172.16.1.1/32

172.16.1.1/32,RD=2:2;
RT=2:2(Export);Label=1027;
	VPN2
	172.16.1.1/32

- PE2 receives a VPNv4 route from PE1.
- PE2 checks the extended community attributes in the route.
- PE2 compares the Export Target value in the extended community attributes with the Import Target value of the local VPN.
- If the two values are the same, PE2 imports the VPNv4 route to the VPN routing table.

HUAWEI

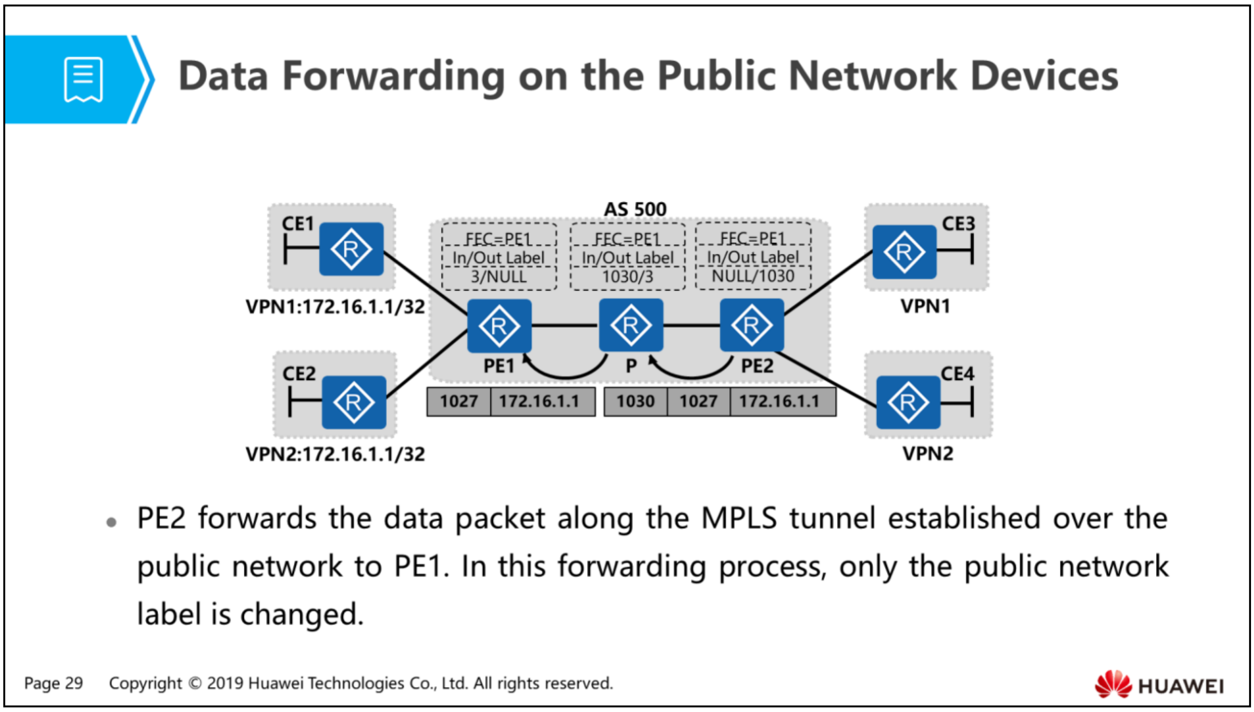
- After the four steps, route exchange on the MPLS VPN network is complete. This process describes route exchange in one direction. The route exchange process in the other direction is similar.
- The next section introduces the MPLS VPN data forwarding process in three steps:
  - Data forwarding from a CE device to a PE device
  - Data forwarding on the public network devices
  - Data forwarding from a PE device to a CE device



Data Forwarding from a CE Device to a PE Device

- CE4 forwards a data packet to PE2. PE2 searches the routing table of VPN2 to determine that the packet needs to be forwarded based on the labels. PE2 then searches for the next hop and outbound interface and encapsulates the packet using MPLS based on the distributed label.

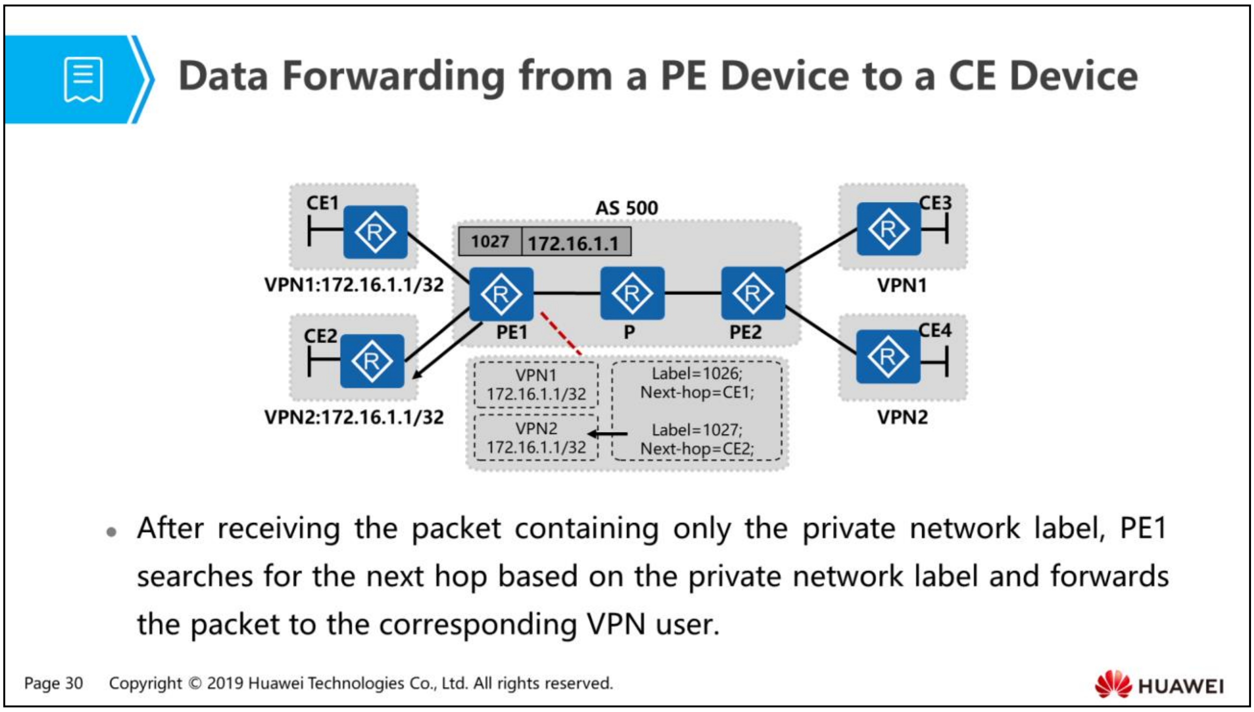
- The data forwarding process from a CE device to a PE device is as follows:
  - As shown in the preceding figure, a VPN2 user connected to CE4 needs to communicate with the remote VPN2 user at 172.16.1.1/32. After receiving the packet, PE2 searches the routing table of the local VPN2 and finds that the packet needs to be forwarded based on the labels, the distributed private network label is 1027, and the next hop to the destination is PE1.
  - PE2 searches the LFIB table and finds that the distributed public network label to PE1 is 1030 and the outbound interface is G0/0/0. PE2 adds the inner label 1027 and outer label 1030 to the packet and forwards the packet through G0/0/0.



Data Forwarding on the Public Network Devices

- PE2 forwards the data packet along the MPLS tunnel established over the public network to PE1. In this forwarding process, only the public network label is changed.

- The process of transmitting the data packet over the public network is as follows:
  - After receiving a data packet from a VPN user, PE2 adds the public network label 1030 to the packet and forwards it over the MPLS tunnel to the P device. The P device searches the LFIB table and finds that the outgoing label for this packet is 3. The P device then removes the public network label and sends the packet to PE1. PE1 receives the packet containing only the inner private network label.



Data Forwarding from a PE Device to a CE Device

- After receiving the packet containing only the private network label, PE1 searches for the next hop based on the private network label and forwards the packet to the corresponding VPN user.

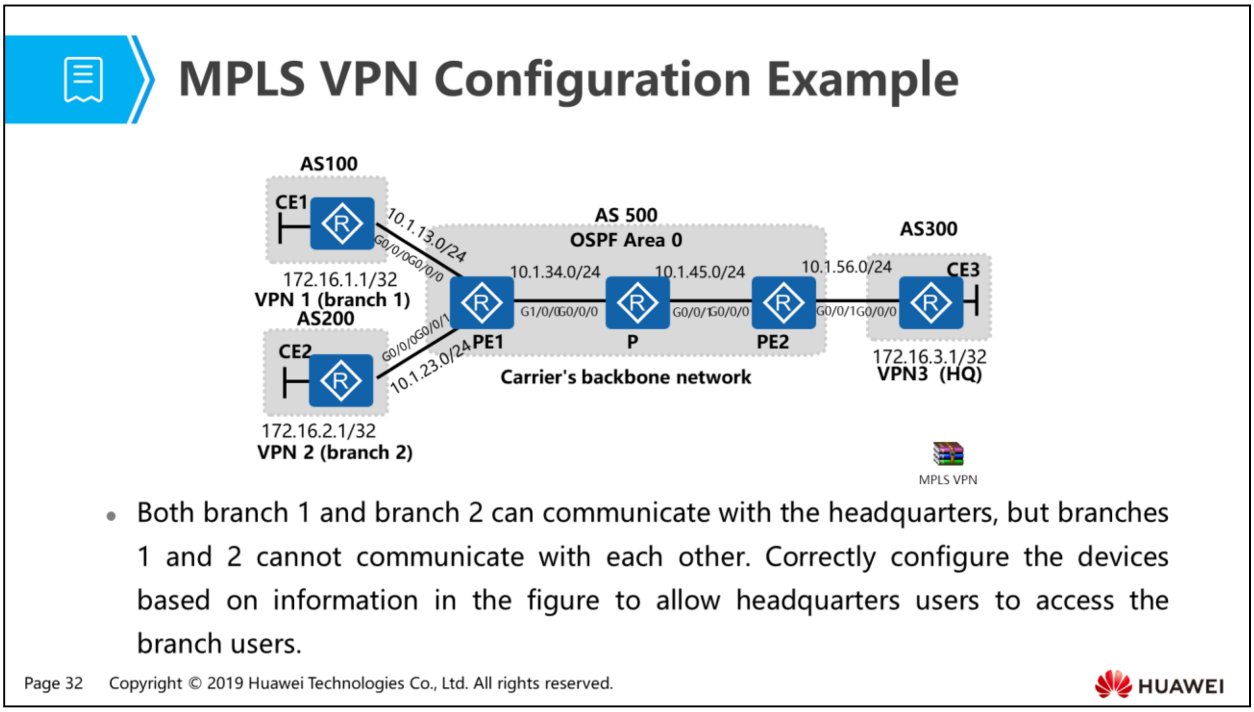
Page 30 HUAWEI

- The packet forwarding process is as follows:
  - After PE1 receives the packet containing only one label, it searches the label table and finds the next hop is CE2 based on the label 1027. PE2 removes the private network label, encapsulates the packet using IP, searches the outbound interface, and forwards the packet to CE2.
  - The packet arrives at the target user correctly. The data forwarding process in the other direction is similar.

Contents

1. MPLS VPN Working Principles

2. **MPLS VPN Configuration Example**

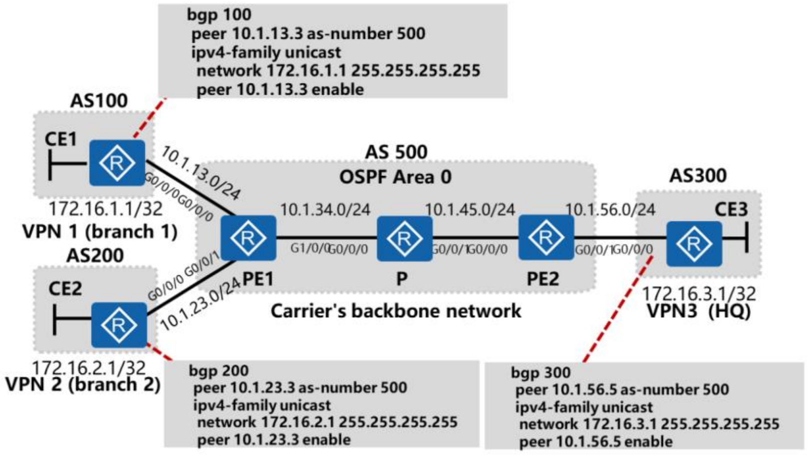


MPLS VPN Configuration Example

- Both branch 1 and branch 2 can communicate with the headquarters, but branches 1 and 2 cannot communicate with each other. Correctly configure the devices based on information in the figure to allow headquarters users to access the branch users.

- Configuration requirements:
  - Branches and the headquarters communicate through MPLS VPN, and the BGP protocol is used to transmit routes between user and carrier networks. Branch 1 is added to VPN1 and uses the RD 1:1, Export Target 12:3 and Import Target 3:12. Branch 2 is added to VPN2 and uses the RD 2:2, Export Target 12:3, and Import Target 3:12. The headquarters is added to VPN3 and uses the RD 3:3, Export Target, 3:12, and Import Target 12:3.
- When configuring MPLS VPN, pay attention to the following points:
  - User-side device configuration: Protocol used by the CE and PE devices to transmit VPN routes to the carrier network.
  - Carrier's backbone network configuration:
    - IGP configuration on the backbone network to ensure route reachability over the carrier network.
    - VPN configuration on the carrier devices to encapsulate and transmit VPN routes.
    - MP-BGP and MPLS configurations to enable VPN route advertisement and tunnel establishment.

Configuring User-side Devices

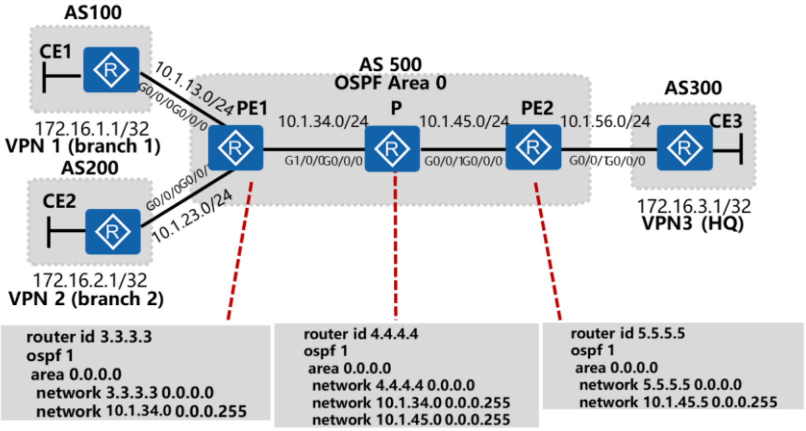


```
bgp 100
 peer 10.1.13.3 as-number 500
 ipv4-family unicast
  network 172.16.1.1 255.255.255.255
  peer 10.1.13.3 enable
```

```
bgp 200
 peer 10.1.23.3 as-number 500
 ipv4-family unicast
  network 172.16.2.1 255.255.255.255
  peer 10.1.23.3 enable
```

```
bgp 300
 peer 10.1.56.5 as-number 500
 ipv4-family unicast
  network 172.16.3.1 255.255.255.255
  peer 10.1.56.5 enable
```

Configuring IGP on the Backbone Network

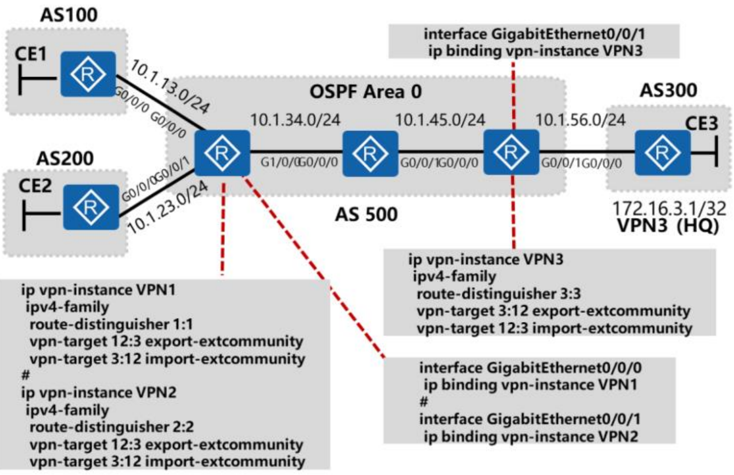


```
router id 3.3.3.3
ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 10.1.34.0 0.0.0.255
```

```
router id 4.4.4.4
ospf 1
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 10.1.34.0 0.0.0.255
  network 10.1.45.0 0.0.0.255
```

```
router id 5.5.5.5
ospf 1
 area 0.0.0.0
  network 5.5.5.5 0.0.0.0
  network 10.1.45.5 0.0.0.255
```

Configuring VPN Instances



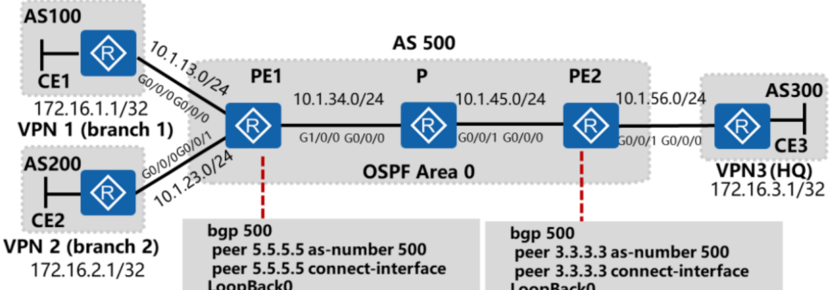
```
interface GigabitEthernet0/0/1
 ip binding vpn-instance VPN3
```

```
ip vpn-instance VPN3
 ipv4-family
  route-distinguisher 3:3
  vpn-target 3:12 export-extcommunity
  vpn-target 12:3 import-extcommunity
```

```
ip vpn-instance VPN1
 ipv4-family
  route-distinguisher 1:1
  vpn-target 12:3 export-extcommunity
  vpn-target 3:12 import-extcommunity
#
ip vpn-instance VPN2
 ipv4-family
  route-distinguisher 2:2
  vpn-target 12:3 export-extcommunity
  vpn-target 3:12 import-extcommunity
```

```
interface GigabitEthernet0/0/0
 ip binding vpn-instance VPN1
#
interface GigabitEthernet0/0/1
 ip binding vpn-instance VPN2
```

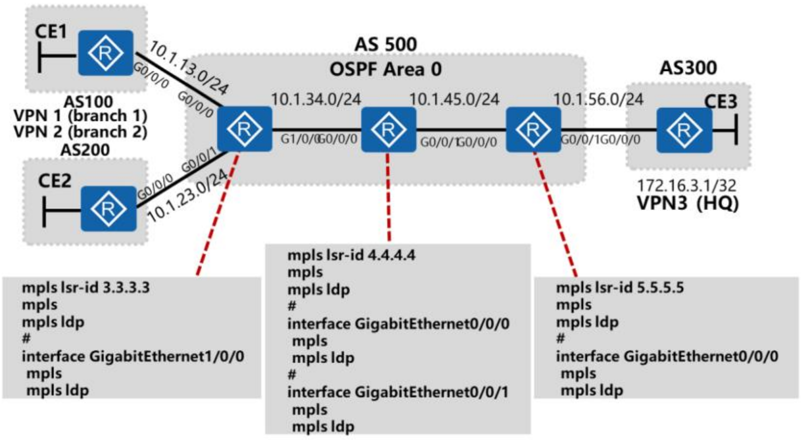
Configuring MP-BGP



```
bgp 500
 peer 5.5.5.5 as-number 500
 peer 5.5.5.5 connect-interface
LoopBack0
#
 ipv4-family vpnv4
  peer 5.5.5.5 enable
 #
 ipv4-family vpn-instance VPN1
  peer 10.1.13.1 as-number 100
 #
 ipv4-family vpn-instance VPN2
  peer 10.1.23.2 as-number 200
```

```
bgp 500
 peer 3.3.3.3 as-number 500
 peer 3.3.3.3 connect-interface
LoopBack0
 #
 ipv4-family vpnv4
  policy vpn-target
  peer 3.3.3.3 enable
 #
 ipv4-family vpn-instance VPN3
  peer 10.1.56.6 as-number 300
```

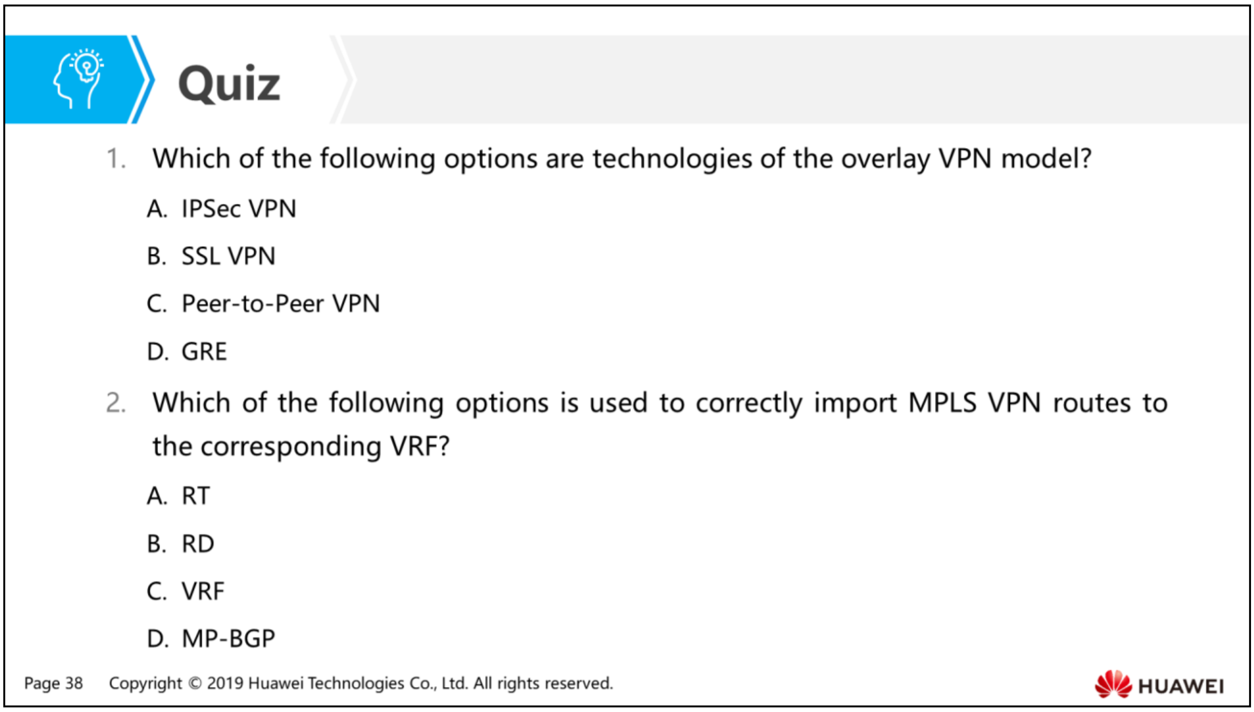
Configuring MPLS



```
mpls lsr-id 3.3.3.3
mpls
mpls ldp
#
interface GigabitEthernet1/0/0
 mpls
 mpls ldp
```

```
mpls lsr-id 4.4.4.4
mpls
mpls ldp
#
interface GigabitEthernet0/0/0
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
 mpls
 mpls ldp
```

```
mpls lsr-id 5.5.5.5
mpls
mpls ldp
#
interface GigabitEthernet0/0/0
 mpls
 mpls ldp
```



Quiz

1. Which of the following options are technologies of the overlay VPN model?

   A. IPSec VPN

   B. SSL VPN

   C. Peer-to-Peer VPN

   D. GRE

2. Which of the following options is used to correctly import MPLS VPN routes to the corresponding VRF?

   A. RT

   B. RD

   C. VRF

   D. MP-BGP

- Answer: ABD.
- Answer: A.

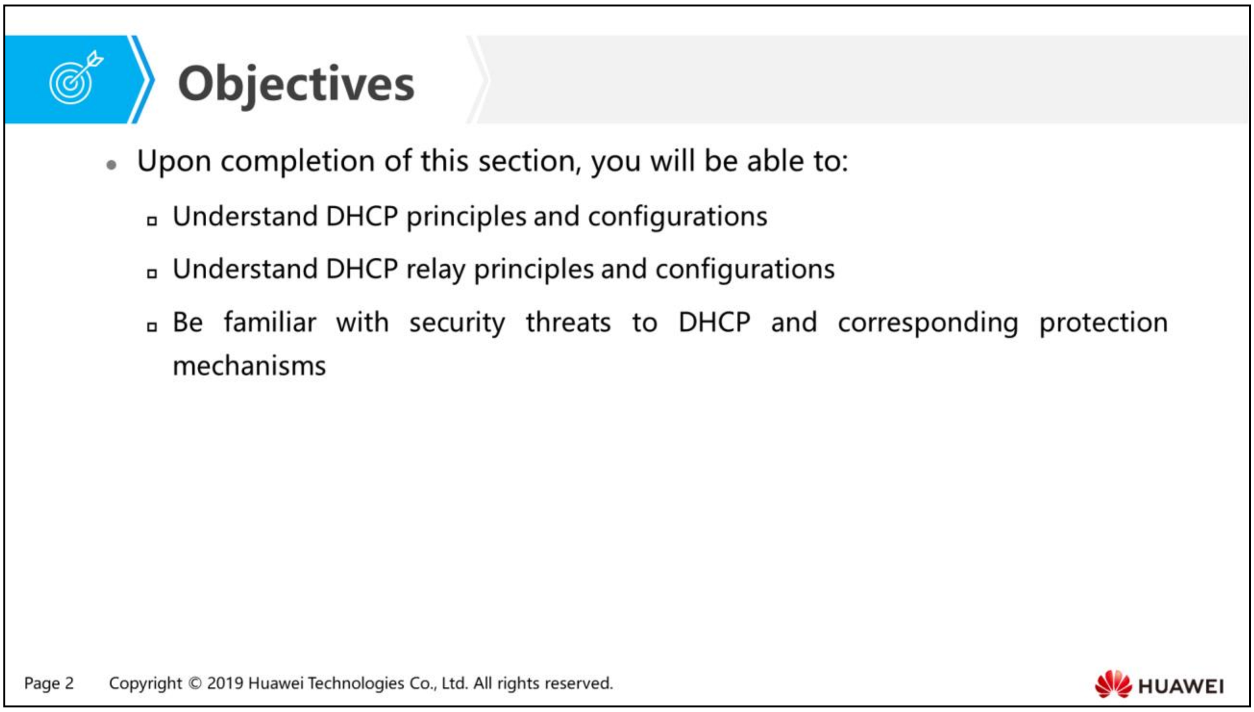
Thank You

www.huawei.com

DHCP Principles and Configurations

Foreword

- Hosts on a network must obtain some important network parameters including the IP address, network mask, gateway address, DNS server address, and network printer address to ensure network connectivity. Manually configuring these parameters on each host is difficult or even impossible.
- To address this issue, the Internet Engineering Task Force (IETF) released the Dynamic Host Configuration Protocol (DHCP) in 1993. DHCP implements automatic configuration of network parameters. How does DHCP work? How does DHCP cope with the increasing network size? How does DHCP defend against network attacks?

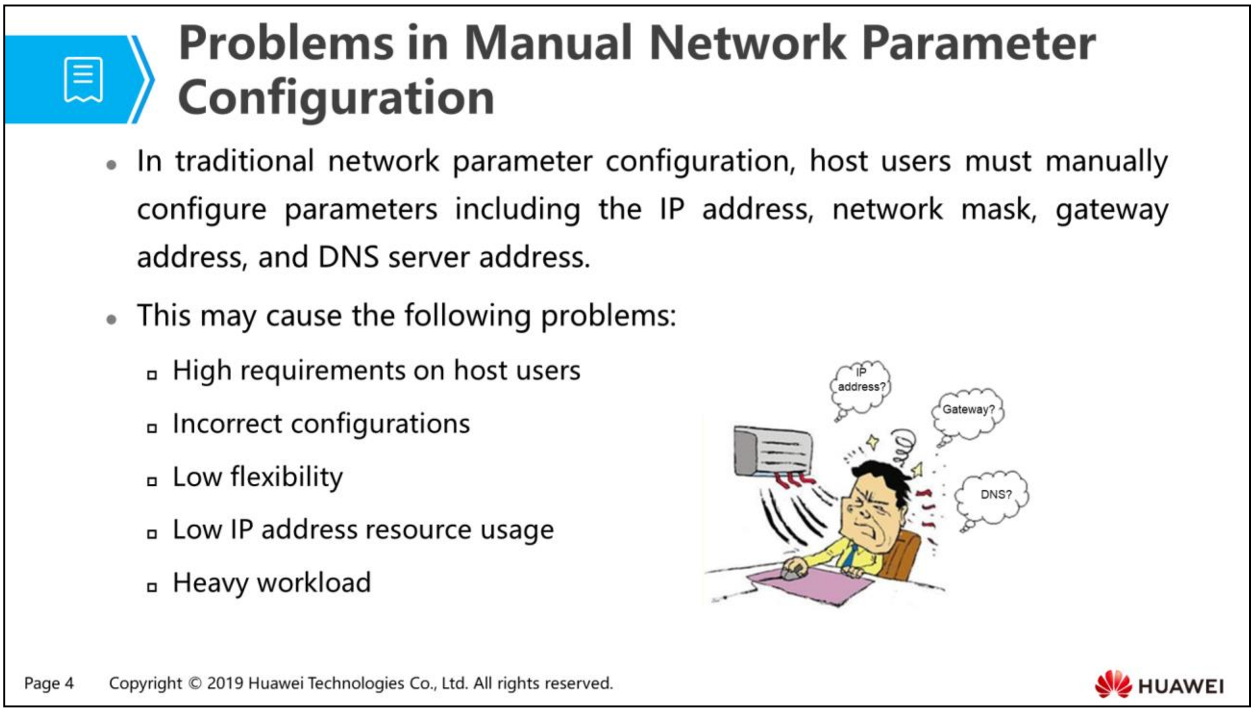


Objectives

- Upon completion of this section, you will be able to:
  - Understand DHCP principles and configurations
  - Understand DHCP relay principles and configurations
  - Be familiar with security threats to DHCP and corresponding protection mechanisms

Contents

1. **DHCP Background**
2. DHCP Principles and Configurations
3. DHCP Relay Background
4. DHCP Relay Principles and Configurations
5. Security Threats to DHCP and Corresponding Protection Mechanisms

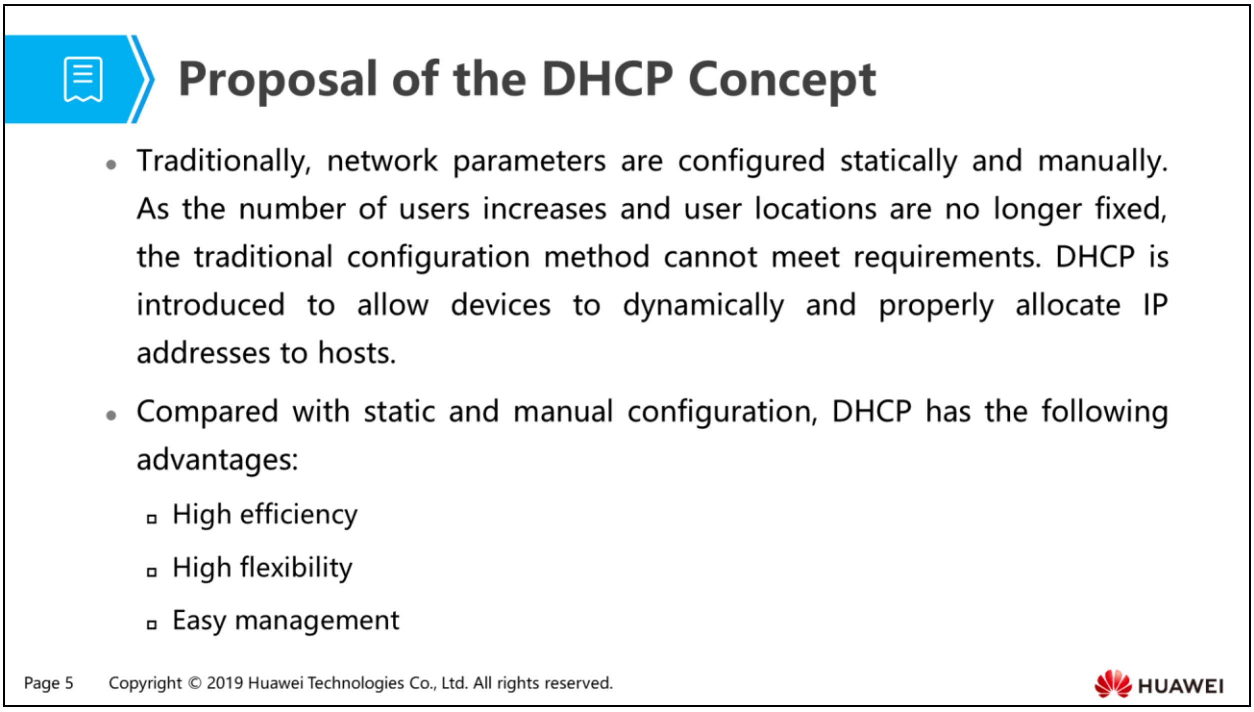


Problems in Manual Network Parameter Configuration

- In traditional network parameter configuration, host users must manually configure parameters including the IP address, network mask, gateway address, and DNS server address.
- This may cause the following problems:
  - High requirements on host users
  - Incorrect configurations
  - Low flexibility
  - Low IP address resource usage
  - Heavy workload

Page 4

- High requirements on host users
  - Host users need to know how to configure network parameters, which is difficult to achieve in actual scenarios.
- Incorrect configurations
  - Manual operations easily cause incorrect configurations.
- Low flexibility
  - Users need to perform configuration again when network parameters change. For example, when the location of a host changes, the gateway address may also change. Users need to reconfigure the host's gateway address.
- Low IP address resource usage
  - IP addresses cannot be reused.
- Heavy workload
  - The configuration workload increases with the growing hosts.

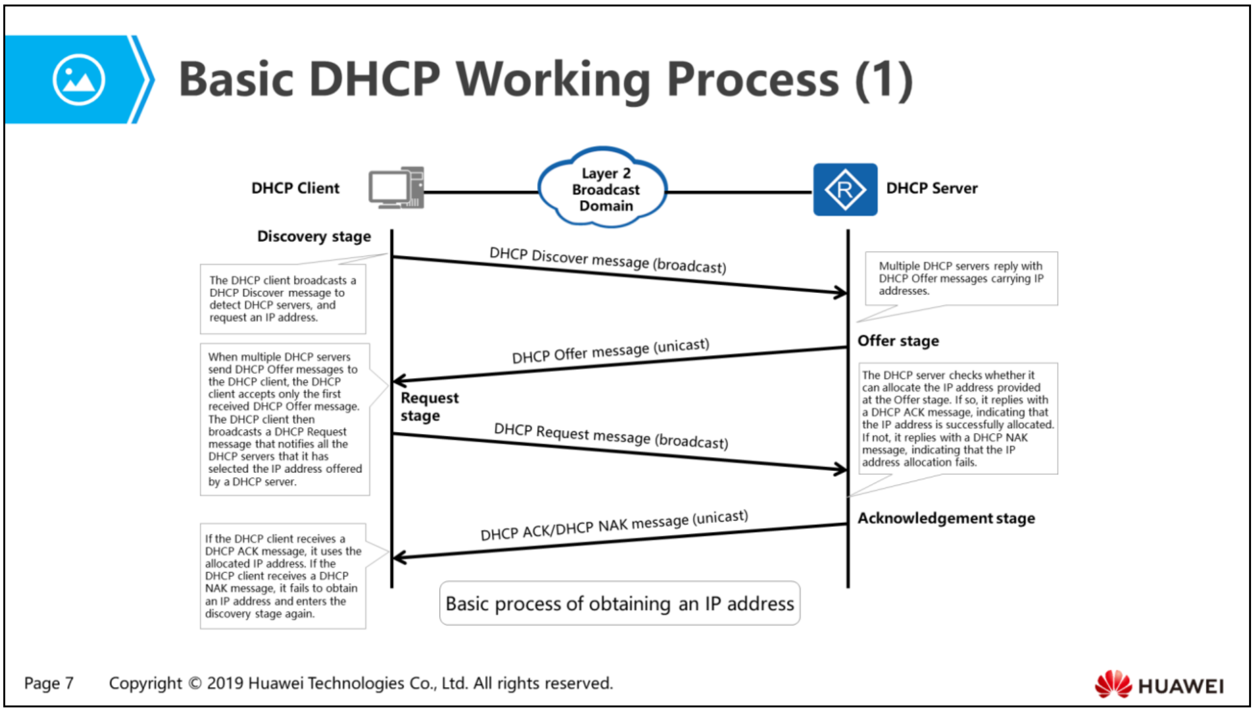


Proposal of the DHCP Concept

- Traditionally, network parameters are configured statically and manually. As the number of users increases and user locations are no longer fixed, the traditional configuration method cannot meet requirements. DHCP is introduced to allow devices to dynamically and properly allocate IP addresses to hosts.
- Compared with static and manual configuration, DHCP has the following advantages:
  - High efficiency
  - High flexibility
  - Easy management

Contents

1. DHCP Background
2. **DHCP Principles and Configurations**
3. DHCP Relay Background
4. DHCP Relay Principles and Configurations
5. Security Threats to DHCP and Corresponding Protection Mechanisms



Basic DHCP Working Process (1)

DHCP Client
Layer 2 Broadcast Domain
DHCP Server
Discovery stage
DHCP Discover message (broadcast)
Offer stage
DHCP Offer message (unicast)
Request stage
DHCP Request message (broadcast)
Acknowledgement stage
DHCP ACK/DHCP NAK message (unicast)

The DHCP client broadcasts a DHCP Discover message to detect DHCP servers, and request an IP address.

Multiple DHCP servers reply with DHCP Offer messages carrying IP addresses.

When multiple DHCP servers send DHCP Offer messages to the DHCP client, the DHCP client accepts only the first received DHCP Offer message. The DHCP client then broadcasts a DHCP Request message that notifies all the DHCP servers that it has selected the IP address offered by a DHCP server.

The DHCP server checks whether it can allocate the IP address provided at the Offer stage. If so, it replies with a DHCP ACK message, indicating that the IP address is successfully allocated. If not, it replies with a DHCP NAK message, indicating that the IP address allocation fails.

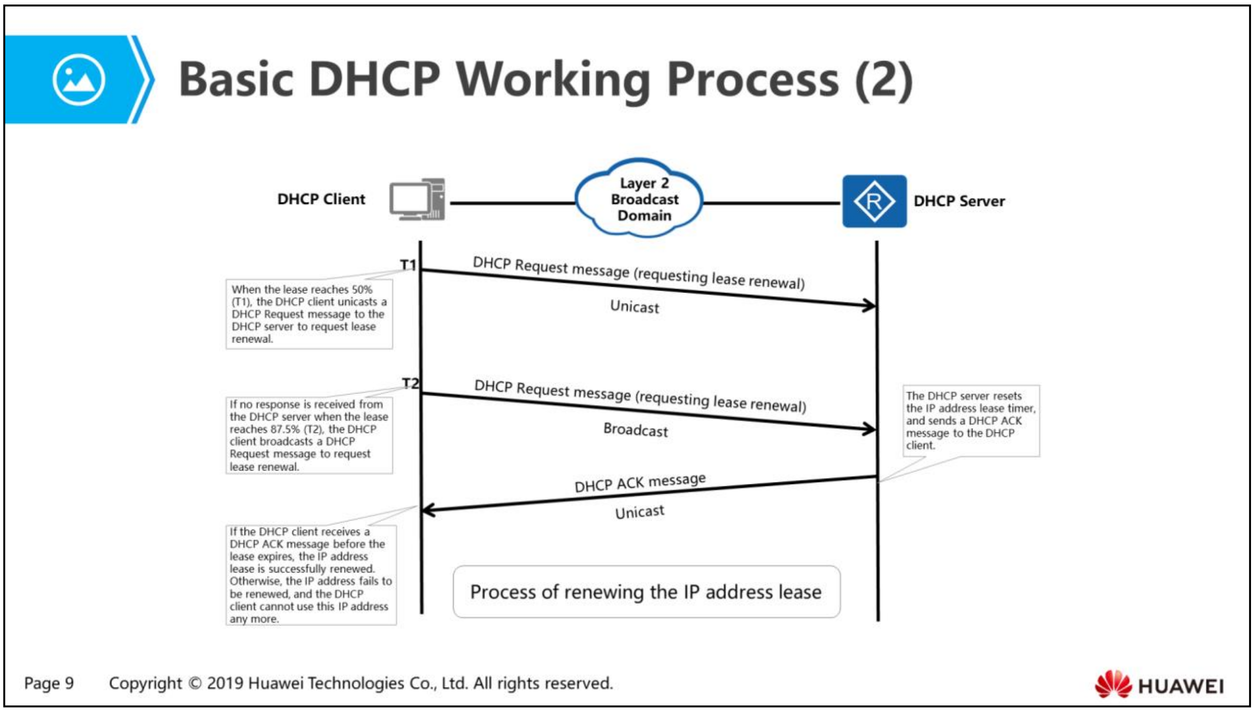
If the DHCP client receives a DHCP ACK message, it uses the allocated IP address. If the DHCP client receives a DHCP NAK message, it fails to obtain an IP address and enters the discovery stage again.

Basic process of obtaining an IP address

Page 7

- DHCP uses the client/server model. DHCP clients exchange DHCP messages with the DHCP server to obtain network parameters. DHCP messages are encapsulated in User Datagram Protocol (UDP) packets. DHCP servers and clients use UDP ports 67 and 68 to receive DHCP messages, respectively. This course focuses on how a DHCP client obtains an IP address from a DHCP server.
- The figure shows how a DHCP client requests an IP address through DHCP in the following four stages.
  - Discovery stage:
    - In this stage, the PC as a DHCP client detects DHCP servers by broadcasting a DHCP Discover message.
    - In the Layer 2 broadcast domain shown in the figure, the router works as a DHCP server and other devices may also function as DHCP servers. In this case, all DHCP servers in this domain receive and reply the DHCP Discover message.
  - Offer stage:
    - In this stage, DHCP servers offer IP addresses to the DHCP client. After receiving the DHCP Discover message, all DHCP servers including the router select an available IP address from their address pools, and unicast DHCP Offer messages carrying the selected IP addresses to the DHCP client.

- Request stage:
    - In this stage, the DHCP client selects a received DHCP Offer message according to some principle. Generally, it accepts only the first received DHCP Offer message. In the figure, assume that the first received DHCP Offer message comes from the router. The DHCP client then broadcasts a DHCP Request message to the router to request the offered IP address. The DHCP Request message carries the selected DHCP server identifier, indicating that the client accepts only the DHCP Offer message sent by the router.
- All DHCP servers in the Layer 2 broadcast domain receive the DHCP Request message. After analyzing the received DHCP Request message, the router realizes that the client accepts its DHCP Offer message, and the other DHCP servers realize that the client refuses their DHCP Offer messages. In this case, the other DHCP servers reclaim their IP addresses which can then be allocated to other clients.
    - Acknowledgment stage:
    - In this stage, the router sends a DHCP ACK message to the client. The DHCP server may fail to allocate the IP address because of some reasons. In this case, it replies with a DHCP NAK message to notify the DHCP client that the requested IP address cannot be allocated. The DHCP client then sends a DHCP Discover message to request a new IP address.



Basic DHCP Working Process (2)

DHCP Client

Layer 2 Broadcast Domain

DHCP Server

T1

When the lease reaches 50% (T1), the DHCP client unicasts a DHCP Request message to the DHCP server to request lease renewal.

DHCP Request message (requesting lease renewal)

Unicast

T2

If no response is received from the DHCP server when the lease reaches 87.5% (T2), the DHCP client broadcasts a DHCP Request message to request lease renewal.

DHCP Request message (requesting lease renewal)

Broadcast

The DHCP server resets the IP address lease timer, and sends a DHCP ACK message to the DHCP client.

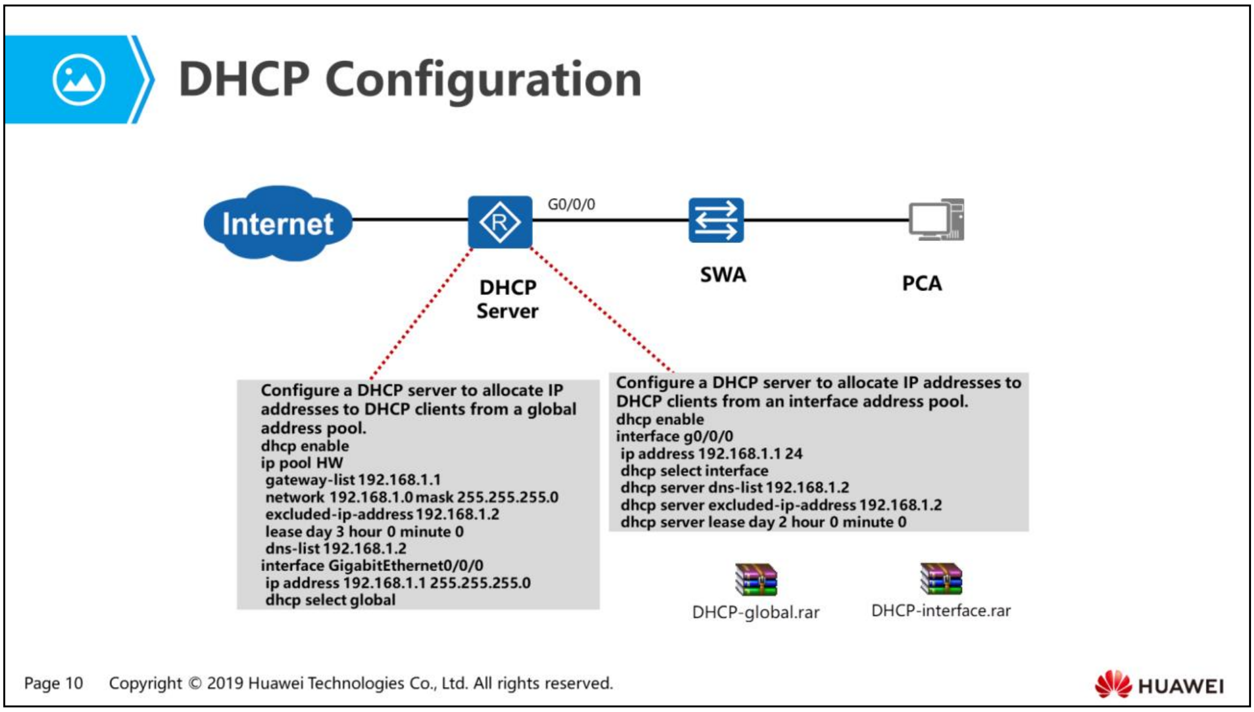
DHCP ACK message

Unicast

If the DHCP client receives a DHCP ACK message before the lease expires, the IP address lease is successfully renewed. Otherwise, the IP address fails to be renewed, and the DHCP client cannot use this IP address any more.

Process of renewing the IP address lease

- Each IP address allocated by a DHCP server has a lease. DHCP specifies that the default duration of lease is no less than 1 hour. The default value is generally 24 hours in actual DHCP deployment. The DHCP client uses the allocated IP address within the duration of lease. When the lease expires, the client cannot use the IP address any more. The figure shows how the DHCP client renews the IP address lease before the lease expires.
- By default, T1 is the time when the lease reaches 50%, while T2 is the time when the lease reaches 87.5%, as specified in DHCP. When the lease reaches 50% (T1), the DHCP client unicasts a DHCP Request message to the DHCP server to request lease renewal (resetting the lease timer). If the client receives a DHCP ACK message before the lease reaches 87.5% (T2), the lease is successfully renewed. If no response is received from the DHCP server when the lease reaches 87.5% (T2), the DHCP client broadcasts a DHCP Request message to request lease renewal again. If the client receives a DHCP ACK message before the lease expires, the lease is successfully renewed. If no response is received when the lease expires, the DHCP client stops using the IP address, and sends a DHCP Discover message to request a new IP address.
- Note: In general, the DHCP server will send DHCP OFFER, DHCP ACK and DHCP NAK by unicast to the client, other situations will not be reflected in the teaching materials. If you are interested in that, you can learn from other materials.



DHCP Configuration

Configure a DHCP server to allocate IP addresses to DHCP clients from a global address pool.

```
dhcp enable
ip pool HW
 gateway-list 192.168.1.1
 network 192.168.1.0 mask 255.255.255.0
 excluded-ip-address 192.168.1.2
 lease day 3 hour 0 minute 0
 dns-list 192.168.1.2
interface GigabitEthernet0/0/0
 ip address 192.168.1.1 255.255.255.0
 dhcp select global
```

Configure a DHCP server to allocate IP addresses to DHCP clients from an interface address pool.

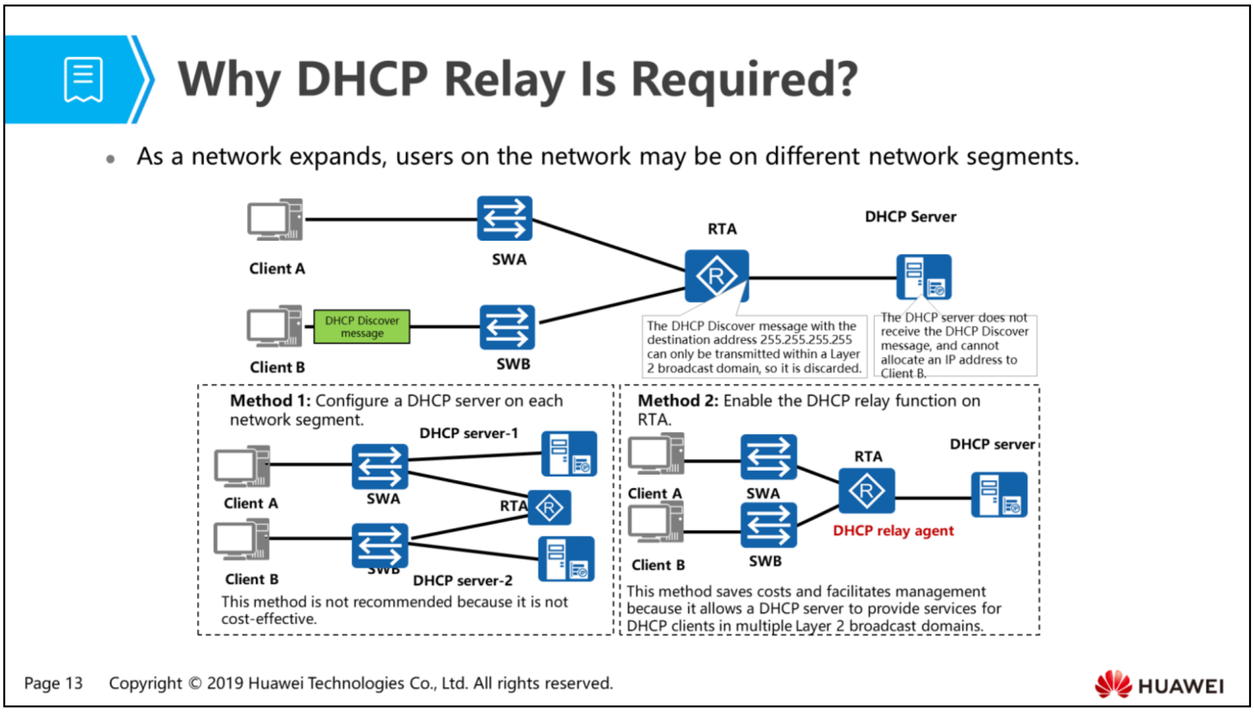
```
dhcp enable
interface g0/0/0
 ip address 192.168.1.1 24
 dhcp select interface
 dhcp server dns-list 192.168.1.2
 dhcp server excluded-ip-address 192.168.1.2
 dhcp server lease day 2 hour 0 minute 0
```

- If a DHCP server allocates IP addresses from an interface address pool, the DHCP server only responds to DHCP Request messages received by the interface. If a DHCP server allocates IP addresses from a global address pool, the DHCP server responds to DHCP Request messages received by all interfaces.
- dhcp enable //Enable DHCP. You must run this command first when deploying a DHCP server. Other DHCP functions then can be configured and take effect.
- ip pool HW //Configure a global address pool named HW.
  - gateway-list 192.168.1.1 //Specify the gateway IP address to be allocated.
  - network 192.168.1.0 mask 255.255.255.0 //Specify the IP address segment to be allocated.
  - excluded-ip-address 192.168.1.2 //Specify IP addresses that cannot be automatically allocated.
  - lease day 3 hour 0 minute 0 //Set the IP address lease. The default lease is 24 hours.
  - dns-list 192.168.1.2 //Specify the DNS server address to be allocated.
- interface GigabitEthernet0/0/0
  - ip address 192.168.1.1 255.255.255.0
  - dhcp select global //Allocate IP addresses from the global address pool.

- interface g0/0/0
  - ip address 192.168.1.1 24
  - dhcp select interface //Allocate IP addresses from an address pool associated with the interface.
  - dhcp server dns-list 192.168.1.2 //Specify the DNS server address to be allocated.
  - dhcp server excluded-ip-address 192.168.1.2 //Specify IP addresses that cannot be automatically allocated in the interface address pool.
  - dhcp server lease day 2 hour 0 minute 0 //Set the IP address lease. The default lease is 24 hours.

Contents

1. DHCP Background
2. DHCP Principles and Configurations
3. **DHCP Relay Background**
4. DHCP Relay Principles and Configurations
5. Security Threats to DHCP and Corresponding Protection Mechanisms



Why DHCP Relay Is Required?

- As a network expands, users on the network may be on different network segments.

The DHCP Discover message with the destination address 255.255.255.255 can only be transmitted within a Layer 2 broadcast domain, so it is discarded.

The DHCP server does not receive the DHCP Discover message, and cannot allocate an IP address to Client B.

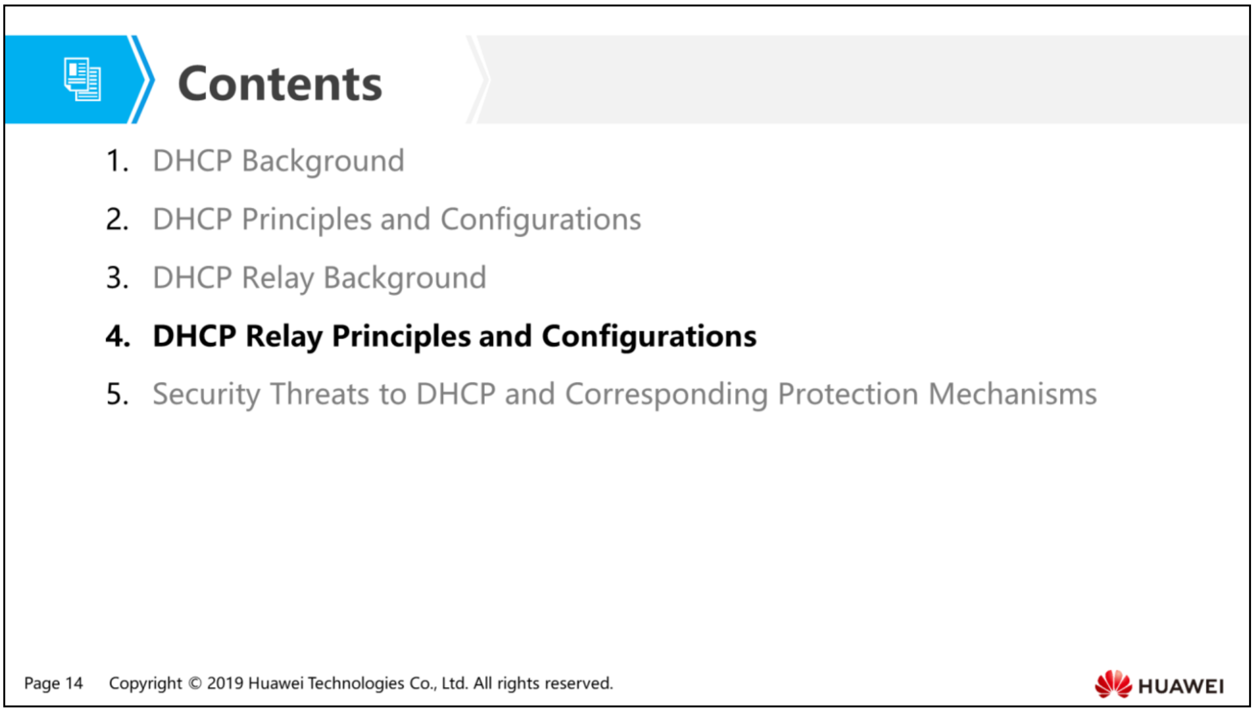
Method 1: Configure a DHCP server on each network segment.

This method is not recommended because it is not cost-effective.

Method 2: Enable the DHCP relay function on RTA.

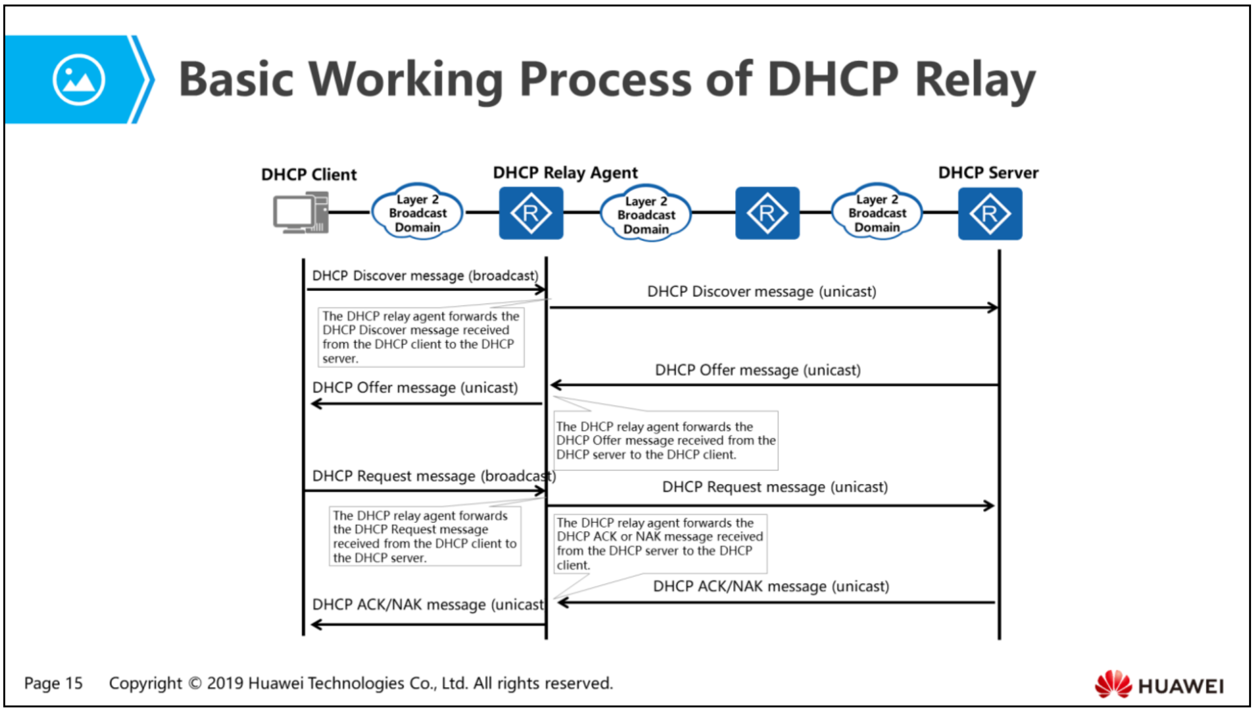
This method saves costs and facilitates management because it allows a DHCP server to provide services for DHCP clients in multiple Layer 2 broadcast domains.

- As you can see from the preceding description, the DHCP client and server must be in the same Layer 2 broadcast domain to receive DHCP messages sent by each other, because DHCP messages can only be transmitted within a Layer 2 broadcast domain.
- An IP network generally contains multiple Layer 2 broadcast domains, and DHCP can be deployed in the following two methods.
  - Method 1: Configure a DHCP server in each Layer 2 broadcast domain. (This method is not recommended because it requires high costs.)
  - Method 2: Configure a DHCP server to offer network parameters to DHCP clients in multiple Layer 2 broadcast domains. In this case, a DHCP relay agent is required.



Contents

1. DHCP Background
2. DHCP Principles and Configurations
3. DHCP Relay Background
4. **DHCP Relay Principles and Configurations**
5. Security Threats to DHCP and Corresponding Protection Mechanisms



Basic Working Process of DHCP Relay

DHCP Client

Layer 2 Broadcast Domain

DHCP Relay Agent

Layer 2 Broadcast Domain

Layer 2 Broadcast Domain

DHCP Server

DHCP Discover message (broadcast)

DHCP Discover message (unicast)

The DHCP relay agent forwards the DHCP Discover message received from the DHCP client to the DHCP server.

DHCP Offer message (unicast)

DHCP Offer message (unicast)

The DHCP relay agent forwards the DHCP Offer message received from the DHCP server to the DHCP client.

DHCP Request message (broadcast)

DHCP Request message (unicast)

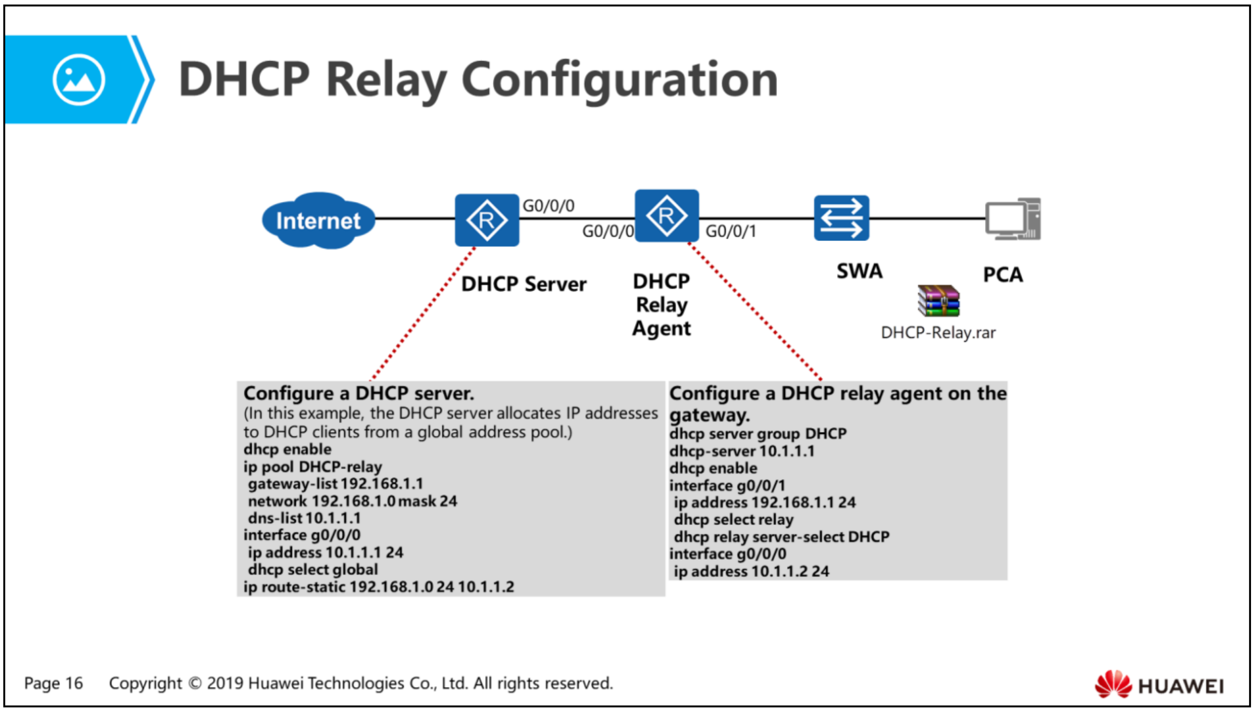
The DHCP relay agent forwards the DHCP Request message received from the DHCP client to the DHCP server.

The DHCP relay agent forwards the DHCP ACK or NAK message received from the DHCP server to the DHCP client.

DHCP ACK/NAK message (unicast)

DHCP ACK/NAK message (unicast)

- The basic function of a DHCP relay agent is to transmit DHCP messages between the DHCP server and DHCP clients.
- As shown in the figure, the DHCP client can obtain network parameters including the IP address from the DHCP server through the DHCP relay agent only when the DHCP relay agent and client are in the same Layer 2 broadcast domain. However, the DHCP server and DHCP relay agent can be in the same Layer 2 broadcast domain or different domains. The DHCP messages are exchanged between the DHCP relay agent and DHCP serve in unicast mode. Therefore, the DHCP relay agent must know the DHCP server's IP address before exchanging messages with it.



DHCP Relay Configuration

Configure a DHCP server.
(In this example, the DHCP server allocates IP addresses to DHCP clients from a global address pool.)

```
dhcp enable
ip pool DHCP-relay
 gateway-list 192.168.1.1
 network 192.168.1.0 mask 24
 dns-list 10.1.1.1
interface g0/0/0
 ip address 10.1.1.1 24
 dhcp select global
ip route-static 192.168.1.0 24 10.1.1.2
```

Configure a DHCP relay agent on the gateway.

```
dhcp server group DHCP
dhcp-server 10.1.1.1
dhcp enable
interface g0/0/1
 ip address 192.168.1.1 24
 dhcp select relay
 dhcp relay server-select DHCP
interface g0/0/0
 ip address 10.1.1.2 24
```

- Configure a DHCP server. //A DHCP server can allocate addresses from a global or an interface address pool. In this example, a global address pool is used.
  - dhcp enable
  - ip pool DHCP-relay //DHCP-relay is only the name of the DHCP address pool.
  - ip route-static 192.168.1.0 24 10.1.1.2 //Because DHCP messages forwarded by the DHCP relay agent are unicast messages with the source IP address 192.168.1.1, there must be a route to the network segment 192.168.1.0 on the DHCP server. For simplicity's sake, a static route is configured in this example. You can configure Interior Gateway Protocol (IGP) to enable the DHCP server and clients to communicate with each other in actual scenarios.
- Configure a DHCP relay agent on the gateway.
  - dhcp server group DHCP //Configure the DHCP server group name.
  - dhcp-server 10.1.1.1 //Specify the DHCP server address.
  - dhcp enable //Enable DHCP on the DHCP relay agent. Otherwise, commands cannot take effect in the interface view.

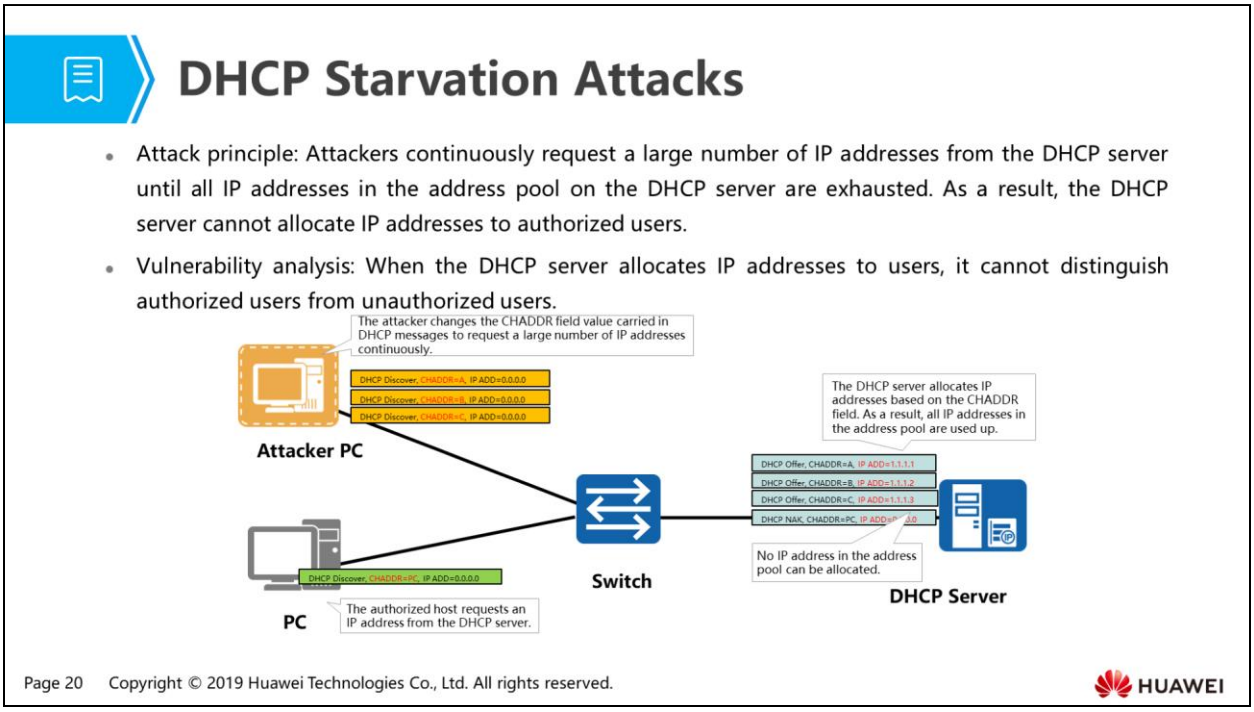
- interface g0/0/1 //Enter the view of the interface connected to clients.
    - ip address 192.168.1.1 24
    - dhcp select relay //Enable the DHCP relay function.
    - dhcp relay server-select DHCP //Specify the DHCP server group to be used by the DHCP relay agent.

Contents

1. DHCP Background
2. DHCP Principles and Configurations
3. DHCP Relay Background
4. DHCP Relay Principles and Configurations
5. **Security Threats to DHCP and Corresponding Protection Mechanisms**

Security Threats to DHCP

- Network attacks are ubiquitous, and DHCP attacks are no exception. For example, a large number of users in an enterprise suddenly cannot access the Internet. The check result shows that terminals of these users do not obtain IP addresses and all IP addresses in the address pool on the DHCP server have been allocated. In this case, a DHCP starvation attack may occur.
- Security factors are not fully considered in DHCP design and there are many security vulnerabilities, making DHCP vulnerable to attacks. DHCP attacks on actual networks can be classified into:
  - DHCP starvation attacks
  - Bogus DHCP server attacks
  - DHCP man-in-the-middle attacks



DHCP Starvation Attacks

- Attack principle: Attackers continuously request a large number of IP addresses from the DHCP server until all IP addresses in the address pool on the DHCP server are exhausted. As a result, the DHCP server cannot allocate IP addresses to authorized users.
- Vulnerability analysis: When the DHCP server allocates IP addresses to users, it cannot distinguish authorized users from unauthorized users.

The attacker changes the CHADDR field value carried in DHCP messages to request a large number of IP addresses continuously.

DHCP Discover, CHADDR=A, IP ADD=0.0.0.0

DHCP Discover, CHADDR=B, IP ADD=0.0.0.0

DHCP Discover, CHADDR=C, IP ADD=0.0.0.0

The DHCP server allocates IP addresses based on the CHADDR field. As a result, all IP addresses in the address pool are used up.

DHCP Offer, CHADDR=A, IP ADD=1.1.1.1

DHCP Offer, CHADDR=B, IP ADD=1.1.1.2

DHCP Offer, CHADDR=C, IP ADD=1.1.1.3

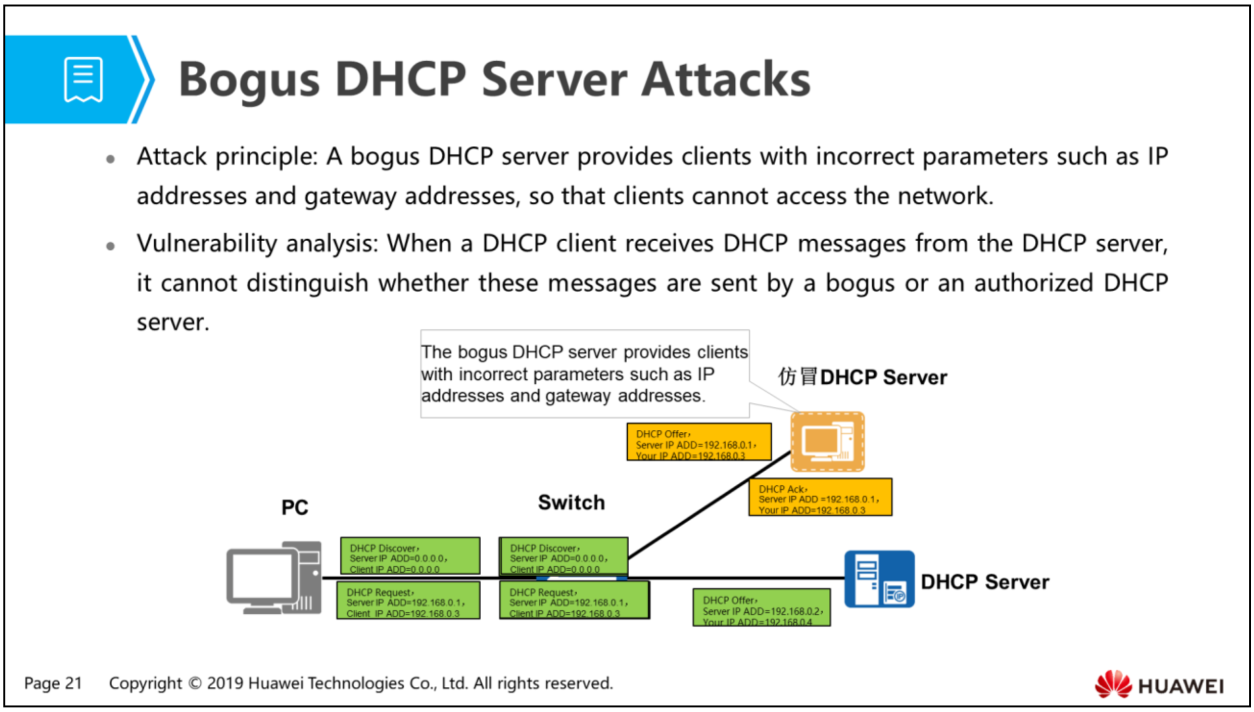
DHCP NAK, CHADDR=PC, IP ADD=0.0.0.0

No IP address in the address pool can be allocated.

DHCP Discover, CHADDR=PC, IP ADD=0.0.0.0

The authorized host requests an IP address from the DHCP server.

- An attacker launches DHCP starvation attacks by continuously requesting IP addresses to exhaust addresses in the address pool of the DHCP server. As a result, authorized users cannot obtain IP addresses. The Client Hardware Address (CHADDR) field in a DHCP message filled by the client is the hardware address (MAC address) of the client. The DHCP server allocates IP addresses based on the CHADDR field, and cannot distinguish authorized CHADDR fields from unauthorized CHADDR fields. The attacker takes advantage of this vulnerability and sends DHCP Request messages with different CHADDR field values to pretend that different users request IP addresses from the DHCP server.



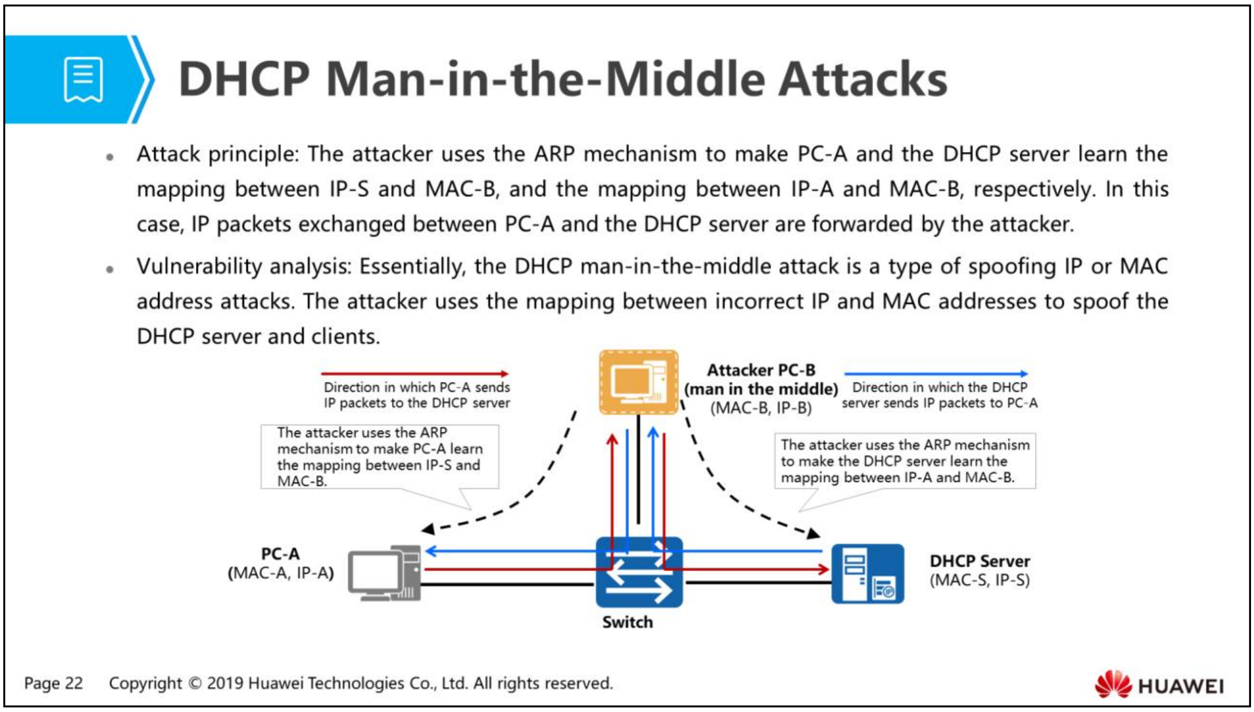
Bogus DHCP Server Attacks

- Attack principle: A bogus DHCP server provides clients with incorrect parameters such as IP addresses and gateway addresses, so that clients cannot access the network.
- Vulnerability analysis: When a DHCP client receives DHCP messages from the DHCP server, it cannot distinguish whether these messages are sent by a bogus or an authorized DHCP server.

The bogus DHCP server provides clients with incorrect parameters such as IP addresses and gateway addresses.

仿冒DHCP Server
DHCP Offer，Server IP ADD=192.168.0.1，Your IP ADD=192.168.0.3
DHCP Ack，Server IP ADD =192.168.0.1，Your IP ADD=192.168.0.3
PC
Switch
DHCP Discover，Server IP ADD=0.0.0.0，Client IP ADD=0.0.0.0
DHCP Discover，Server IP ADD=0.0.0.0，Client IP ADD=0.0.0.0
DHCP Request，Server IP ADD=192.168.0.1，Client IP ADD=192.168.0.3
DHCP Request，Server IP ADD=192.168.0.1，Client IP ADD=192.168.0.3
DHCP Offer，Server IP ADD=192.168.0.2，Your IP ADD=192.168.0.4
DHCP Server

- An attacker who installs and runs the DHCP server program on a PC without permission can make the PC pretend to be an authorized DHCP server. The PC is called a bogus DHCP server. Bogus and authorized DHCP servers use the same working principles, but the bogus DHCP server provides clients with incorrect parameters such as IP addresses and gateway addresses, so that clients cannot access the network.
- Both bogus and authorized DHCP servers can receive the DHCP Discover messages broadcast by the DHCP client, and reply with DHCP Offer messages. If the first received DHCP Offer message is from the bogus DHCP server, the client requests network parameters from the bogus DHCP server. The bogus DHCP server then provides incorrect parameters such as IP addresses and gateway addresses to the client.



DHCP Man-in-the-Middle Attacks

- Attack principle: The attacker uses the ARP mechanism to make PC-A and the DHCP server learn the mapping between IP-S and MAC-B, and the mapping between IP-A and MAC-B, respectively. In this case, IP packets exchanged between PC-A and the DHCP server are forwarded by the attacker.
- Vulnerability analysis: Essentially, the DHCP man-in-the-middle attack is a type of spoofing IP or MAC address attacks. The attacker uses the mapping between incorrect IP and MAC addresses to spoof the DHCP server and clients.

Direction in which PC-A sends IP packets to the DHCP server

Attacker PC-B (man in the middle) (MAC-B, IP-B)

Direction in which the DHCP server sends IP packets to PC-A

The attacker uses the ARP mechanism to make PC-A learn the mapping between IP-S and MAC-B.

The attacker uses the ARP mechanism to make the DHCP server learn the mapping between IP-A and MAC-B.

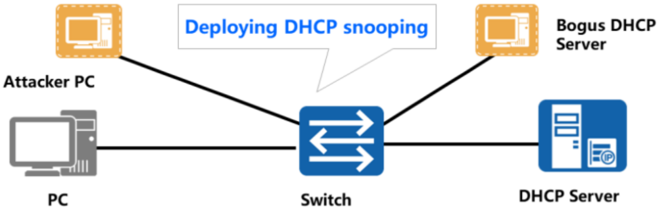
Page 22

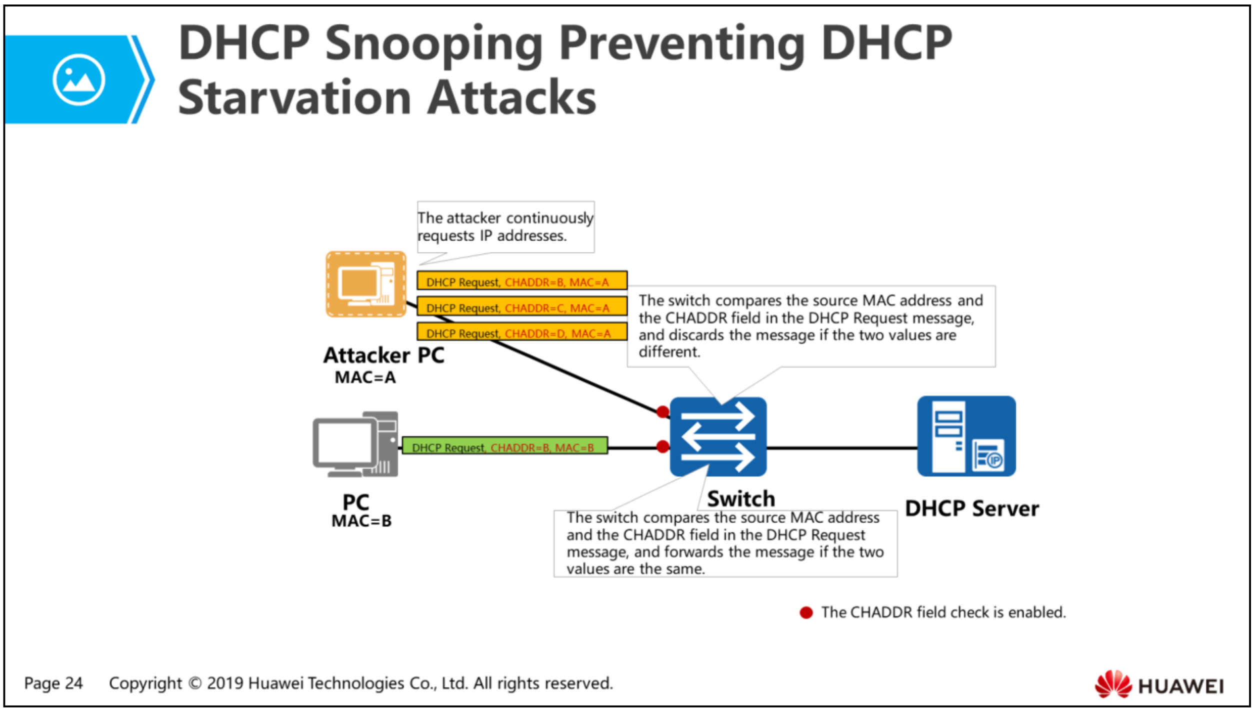
HUAWEI

- As shown in the figure, the attacker PC-B uses the ARP mechanism to make PC-A and the DHCP server learn the mapping between IP-S and MAC-B, and the mapping between IP-A and MAC-B, respectively. When PC-A sends an IP packet to the DHCP server using IP-S as the destination IP address, and IP-A as the source IP address, the IP packet is encapsulated into a frame using MAC-B as the destination MAC address and MAC-A as the source MAC address. As a result, the frame is first received by the attacker PC-B. When PC-B receives the frame, it changes the frame's destination MAC address to MAC-S, and source MAC address to MAC-B, and then sends the frame to the DHCP server. The DHCP server cannot detect the modification. When the DHCP server sends an IP packet to PC-A using IP-A as the destination IP address, and IP-S as the source IP address, the IP packet is encapsulated into a frame using MAC-B as the destination MAC address, and MAC-S as the source MAC address. The frame is also first received by the attacker PC-B. When PC-B receives the frame, it changes the frame's destination MAC address to MAC-A, and source MAC address to MAC-B, and then sends the frame to PC-A. PC-A cannot detect the modification either.
- IP packets exchanged between PC-A and the DHCP server are forwarded by the attacker (man in the middle), so the attacker can easily obtain information in the IP packets, and launch other attacks using the information. The attacker can also modify DHCP messages exchanged between PC-A and the DHCP server to directly initiate DHCP attacks. (These DHCP messages are encapsulated in UDP packets which are further encapsulated in IP packets.)

Background of DHCP Snooping

- DHCP snooping is introduced to improve network security and prevent DHCP attacks. DHCP snooping is not a standard technology, and has no unified standards and regulations. Different network device manufacturers implement DHCP snooping in different ways.
- DHCP snooping is deployed on switches and is equivalent to a firewall between DHCP clients and the DHCP server.





DHCP Snooping Preventing DHCP Starvation Attacks

The attacker continuously requests IP addresses.

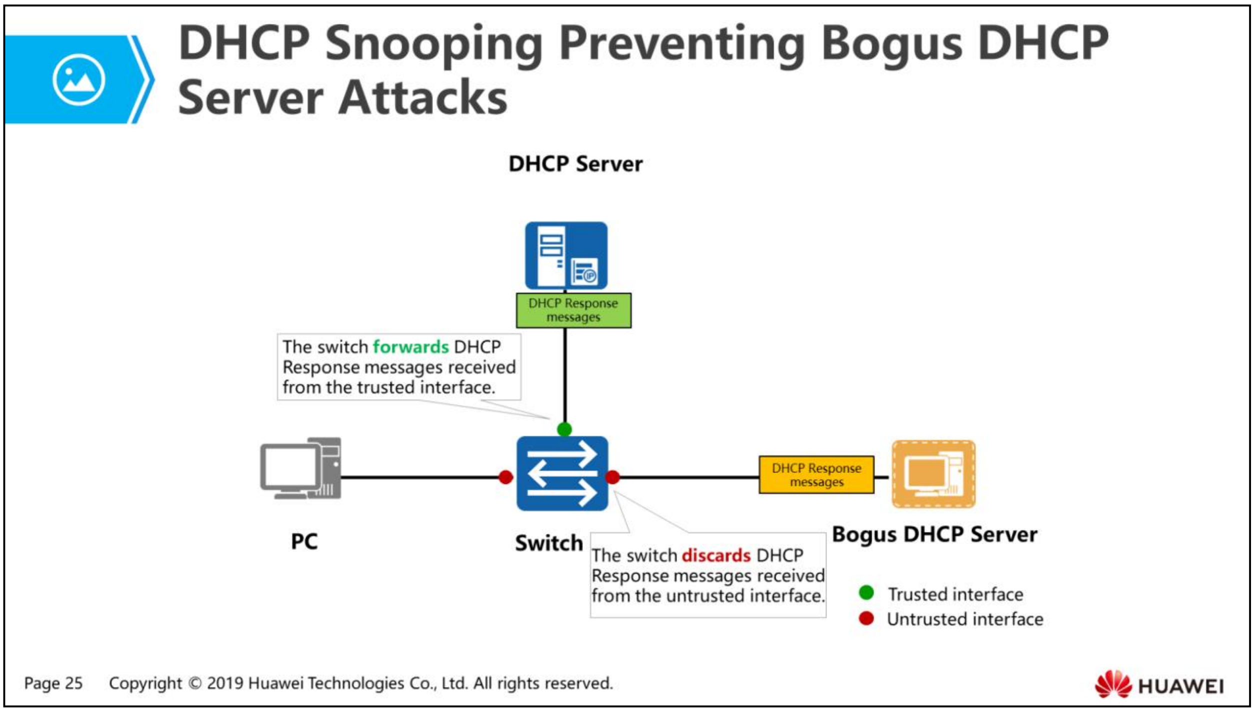
The switch compares the source MAC address and the CHADDR field in the DHCP Request message, and discards the message if the two values are different.

The switch compares the source MAC address and the CHADDR field in the DHCP Request message, and forwards the message if the two values are the same.

● The CHADDR field check is enabled.

DHCP Request, CHADDR=B, MAC=A
DHCP Request, CHADDR=C, MAC=A
DHCP Request, CHADDR=D, MAC=A
Attacker PC
MAC=A
DHCP Request, CHADDR=B, MAC=B
PC
MAC=B
Switch
DHCP Server

- An attacker launches DHCP starvation attacks by continuously requesting IP addresses to exhaust addresses in the address pool of the DHCP server. As a result, authorized users cannot obtain IP addresses. The CHADDR field in a DHCP message is filled by the client, representing the hardware address (MAC address) of the client. The DHCP server allocates IP addresses based on the CHADDR field, and cannot distinguish authorized CHADDR fields from unauthorized CHADDR fields. The attacker takes advantage of this vulnerability and sends DHCP Request messages with different CHADDR field values to pretend that different users request IP addresses from the DHCP server.
- To prevent DHCP starvation attacks, DHCP snooping allows an interface to compare the source MAC address and the CHADDR field in a DHCP Request message. If they are the same, the interface forwards the DHCP Request message; otherwise, the interface discards the message. To enable an interface to compare the source MAC addresses and the CHADDR fields in DHCP Request messages, run the dhcp snooping check dhcp-chaddr enable command on the interface.
- The attacker also launches DHCP starvation attacks by changing the source MAC addresses and CHADDR field values into the same to pass the preceding check.



DHCP Snooping Preventing Bogus DHCP Server Attacks

DHCP Server

DHCP Response messages

The switch **forwards** DHCP Response messages received from the trusted interface.

PC

Switch

DHCP Response messages

Bogus DHCP Server

The switch **discards** DHCP Response messages received from the untrusted interface.

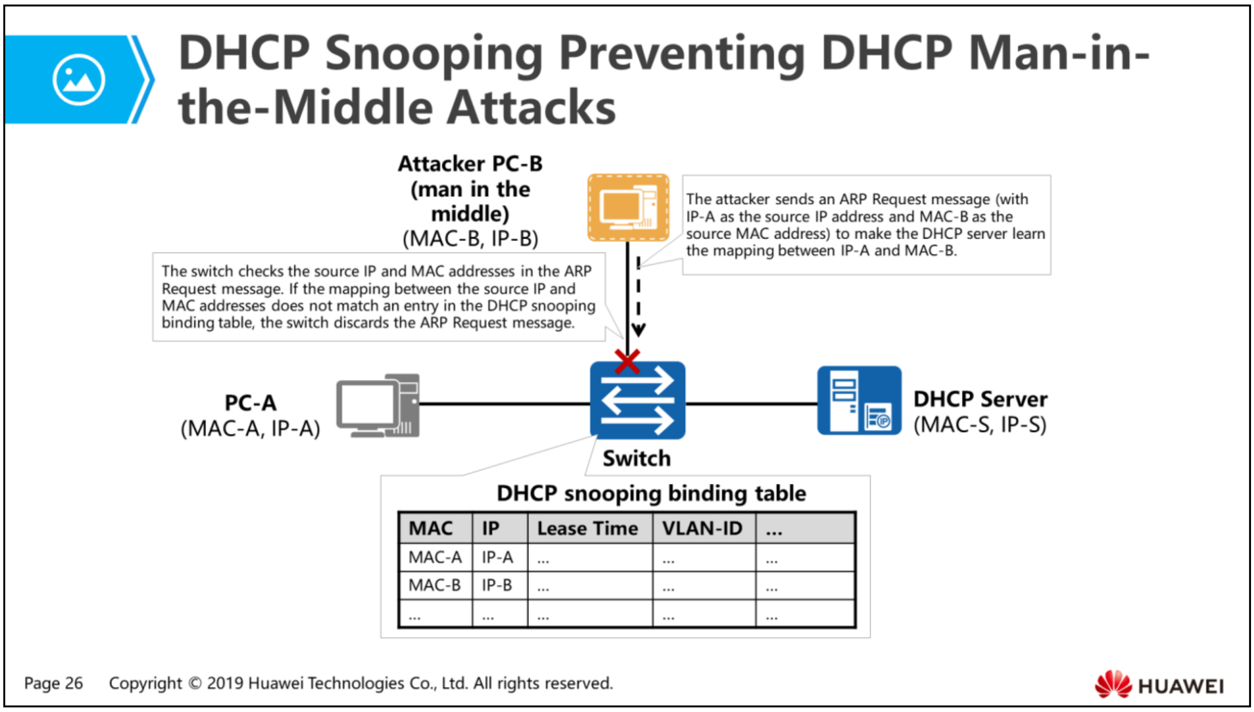
🟢 Trusted interface

🔴 Untrusted interface

Page 25

HUAWEI

- DHCP snooping involves two interface roles: trusted interface and untrusted interface. The interface connected to the authorized DHCP server is configured as the trusted interface, and other interfaces are configured as untrusted interfaces.
- After receiving DHCP Response messages including DHCP Offer and ACK messages from the trusted interface, the switch forwards these messages to ensure that the authorized DHCP server can properly allocate IP addresses and offer other network parameters to DHCP clients. The switch discards DHCP Response messages received from untrusted interfaces to prevent the bogus DHCP server from allocating IP addresses and offering other network parameters to DHCP clients.
- Key configuration commands: By default, interfaces on a switch are untrusted interfaces. You can run the dhcp snooping trusted command in the interface view to configure an interface as a trusted interface. To restore a trusted interface to an untrusted interface, run the undo dhcp snooping trusted command in the interface view.



DHCP Snooping Preventing DHCP Man-in-the-Middle Attacks

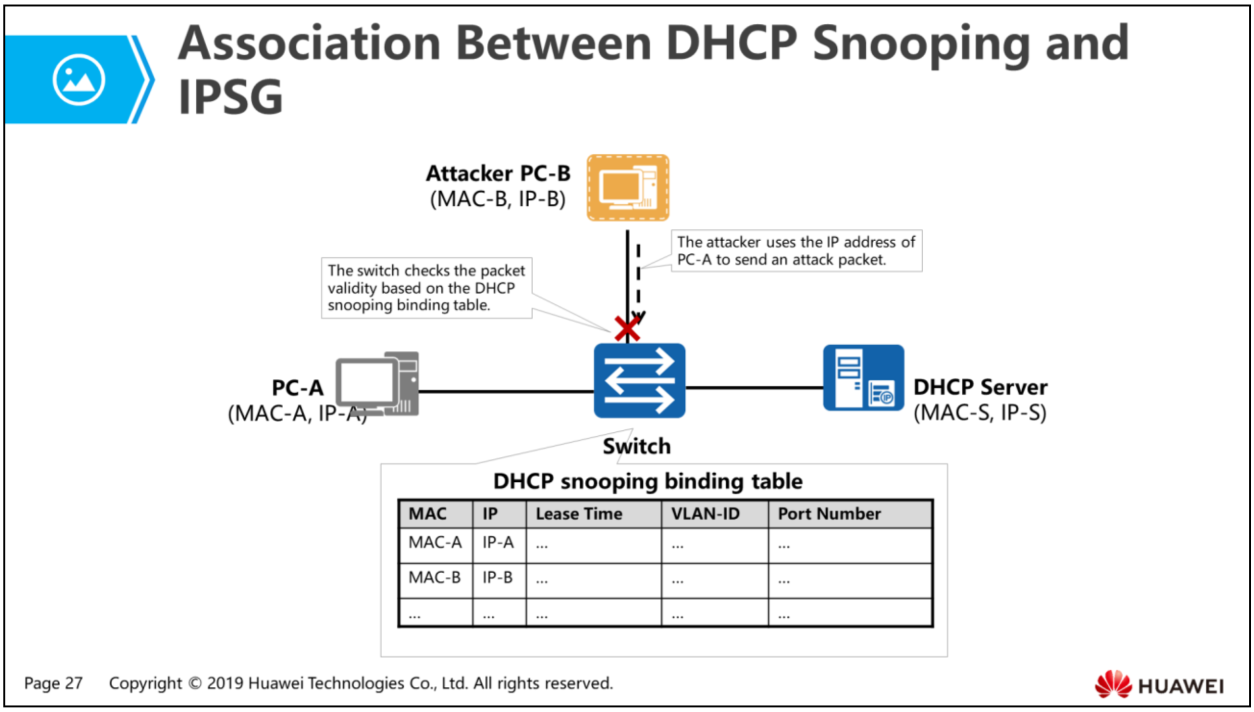
The attacker sends an ARP Request message (with IP-A as the source IP address and MAC-B as the source MAC address) to make the DHCP server learn the mapping between IP-A and MAC-B.

The switch checks the source IP and MAC addresses in the ARP Request message. If the mapping between the source IP and MAC addresses does not match an entry in the DHCP snooping binding table, the switch discards the ARP Request message.

DHCP snooping binding table

MAC	IP	Lease Time	VLAN-ID	...
MAC-A	IP-A	...	...	...
MAC-B	IP-B	...	...	...
...	...	...	...	...

- Essentially, the DHCP man-in-the-middle attack is a type of spoofing IP or MAC address attacks. To prevent DHCP man-in-the-middle attacks is to prevent spoofing IP or MAC address attacks.
- A DHCP snooping-enabled switch performs snooping on DHCP messages exchanged between clients and the DHCP server, and collects information including clients' MAC addresses (CHADDR field values of the DHCP messages) and IP addresses (addresses allocated by the DHCP server based on the CHADDR fields). The switch then stores the information in a database which is also called the DHCP snooping binding table. The DHCP snooping-enabled switch establishes and dynamically maintains the DHCP snooping binding table. Besides clients' MAC addresses and IP addresses, the table also contains information such as the IP address lease and VLAN ID.
- As shown in the figure, assume that the DHCP server allocates IP-A to PC-A, and IP-B to PC-B. The mapping between IP-A and MAC-A, and the mapping between IP-B and MAC-B are formed. The mappings are stored in the DHCP snooping binding table. An attacker sends an ARP Request message (with IP-A as the source IP address and MAC-B as the source MAC address) to make the DHCP server learn the mapping between IP-A and MAC-B. After receiving the ARP Request message, the switch checks the source IP and MAC addresses in the message. If the mapping between the source IP address (IP-A) and source MAC address (MAC-B) does not match an entry in the DHCP snooping binding table, the switch discards the ARP Request message, preventing spoofing IP or MAC address attacks.
- You need to run the arp dhcp-snooping-detect enable command in the system view of the switch to adopt the preceding method of preventing spoofing IP or MAC address attacks and man-in-the-middle attacks.



Association Between DHCP Snooping and IPSG

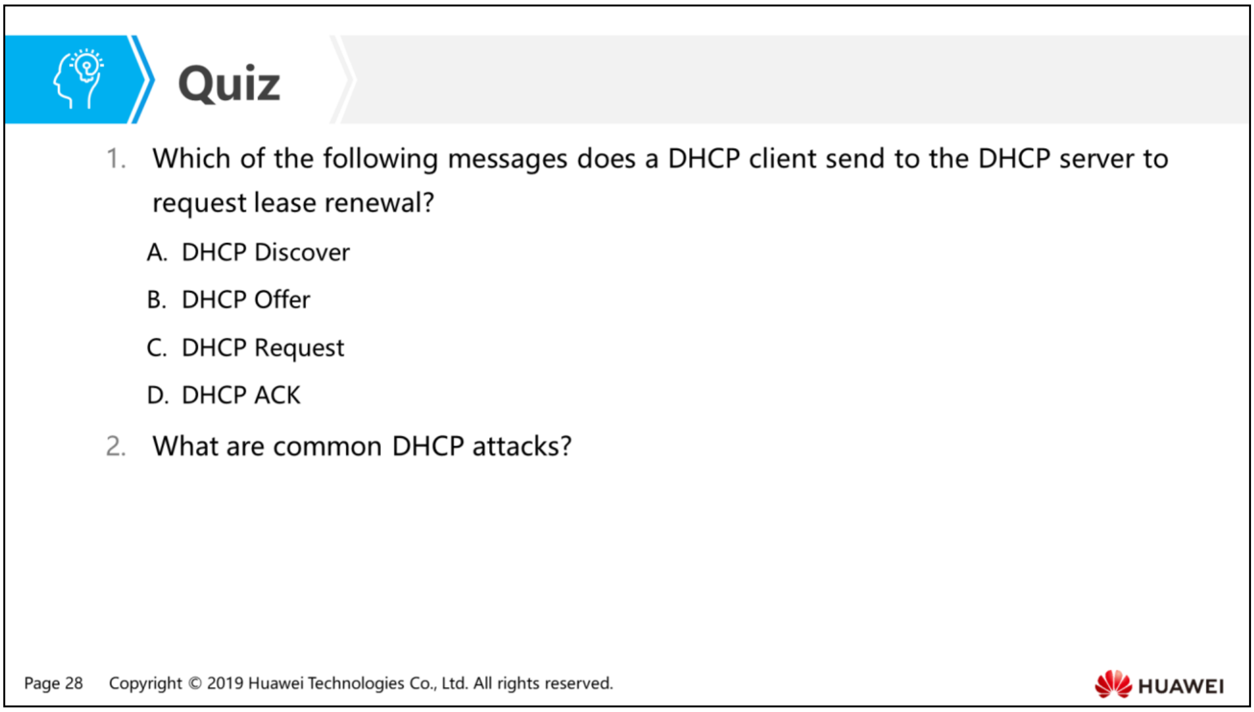
The attacker uses the IP address of PC-A to send an attack packet.

The switch checks the packet validity based on the DHCP snooping binding table.

DHCP snooping binding table

MAC	IP	Lease Time	VLAN-ID	Port Number
MAC-A	IP-A	...	...	...
MAC-B	IP-B	...	...	...
...	...	...	...	...

- The source IP address spoofing is a common attack on a network. For example, an attacker uses the IP address of an authorized user to send IP packets to servers. IP Source Guard (IPSG) is introduced to defend against such attacks.
- An IPSG-enabled switch checks the validity of packets received by an interface and filters packets. (The switch forwards valid packets and discards invalid packets.)
- DHCP snooping can be associated with IPSG. The switch checks whether information in a received packet matches a DHCP snooping binding entry. If the information matches an entry, the switch forwards the packet; otherwise, the switch discards the packet.
- The switch can check the source IP address, source MAC address, VLAN, physical interface number, or some combinations of them. For example, you can configure check of the IP address + MAC address, IP address + VLAN, and IP address + MAC address +VLAN combinations in the interface view of a switch, and configure check of IP address + MAC address, IP address + physical interface number, and IP address + MAC address + physical interface number combinations in the VLAN view.
- Key configuration command: Run the ip source check user-bind enable command in the interface view or VLAN view of the switch.



Quiz

1. Which of the following messages does a DHCP client send to the DHCP server to request lease renewal?
   A. DHCP Discover
   B. DHCP Offer
   C. DHCP Request
   D. DHCP ACK
2. What are common DHCP attacks?

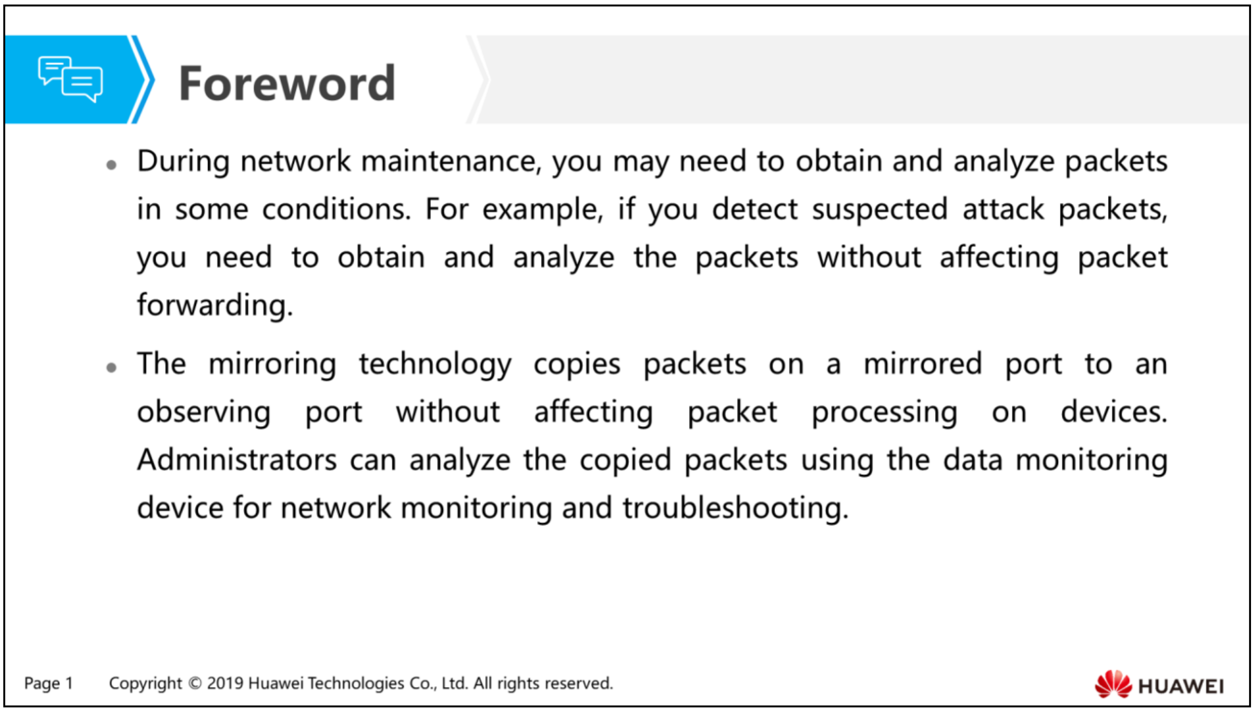
- Answer: C.
- Answer: DHCP starvation attacks, bogus DHCP server attacks, and DHCP man-in-the-middle attacks.

Thank You

www.huawei.com

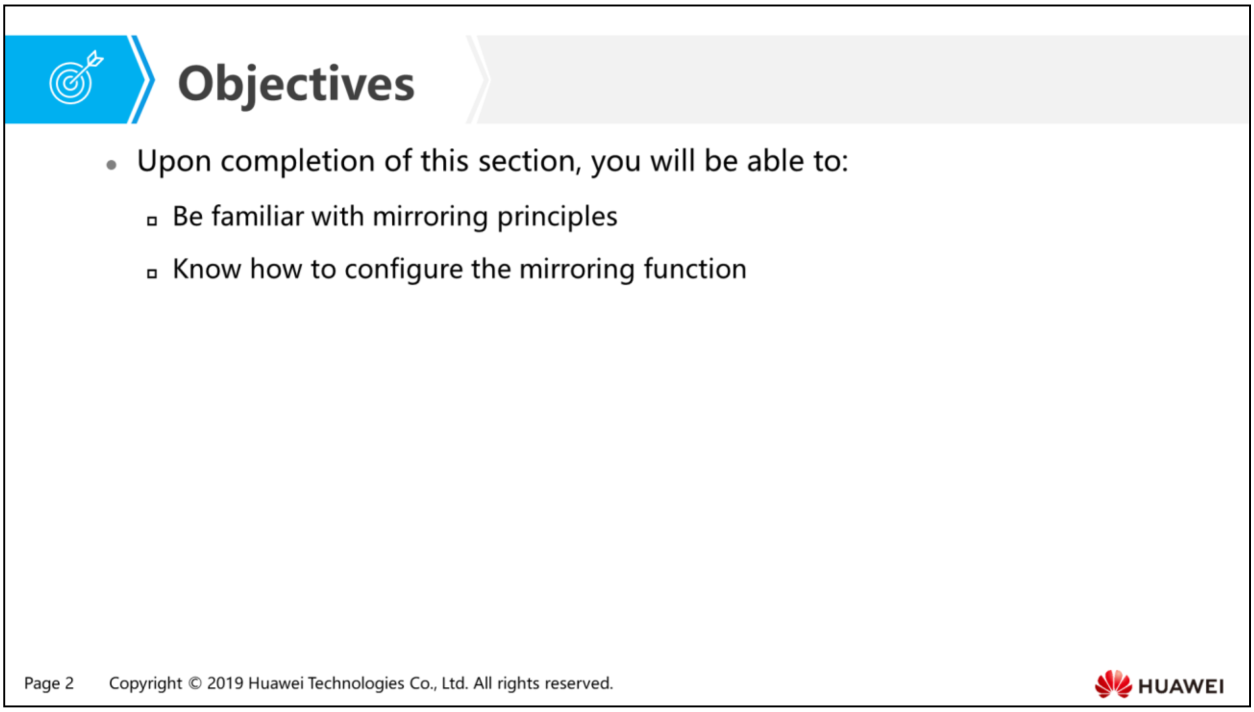
HUAWEI

Mirroring Principles and Configurations



Foreword

- During network maintenance, you may need to obtain and analyze packets in some conditions. For example, if you detect suspected attack packets, you need to obtain and analyze the packets without affecting packet forwarding.
- The mirroring technology copies packets on a mirrored port to an observing port without affecting packet processing on devices. Administrators can analyze the copied packets using the data monitoring device for network monitoring and troubleshooting.

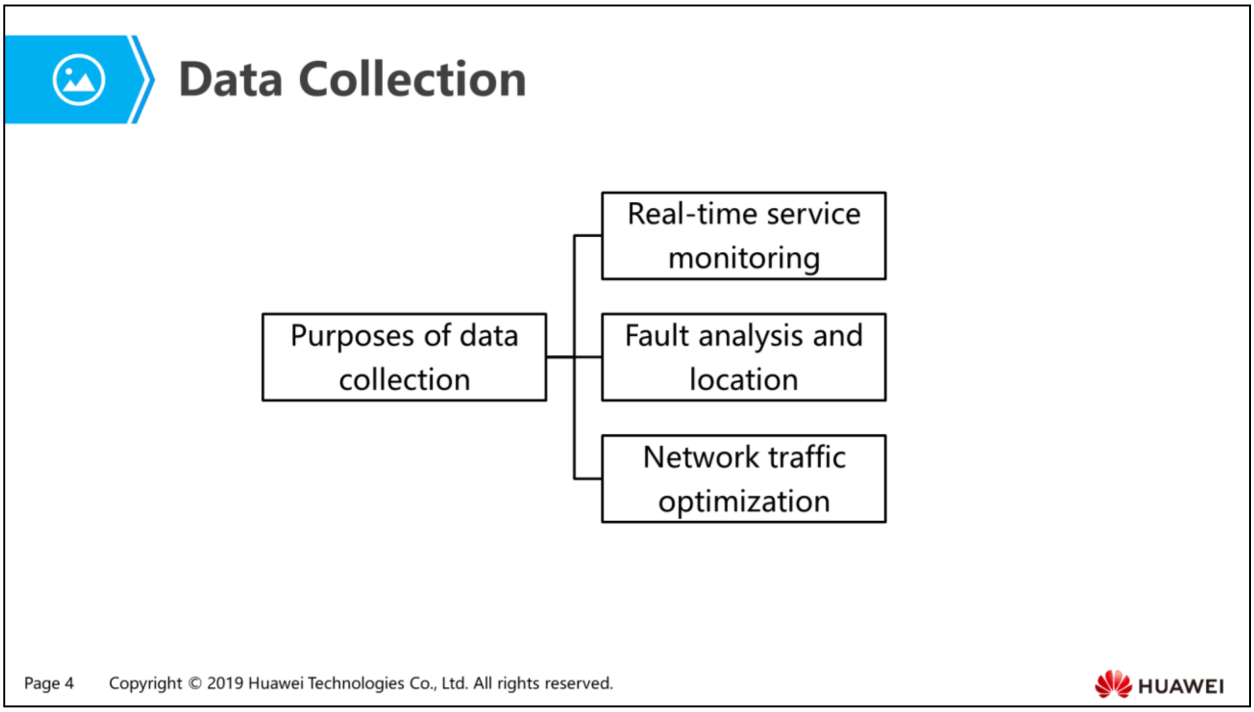


Objectives

- Upon completion of this section, you will be able to:
  - Be familiar with mirroring principles
  - Know how to configure the mirroring function

Contents

1. **Mirroring Background**
2. Mirroring Concepts
3. Mirroring Configuration



Data Collection

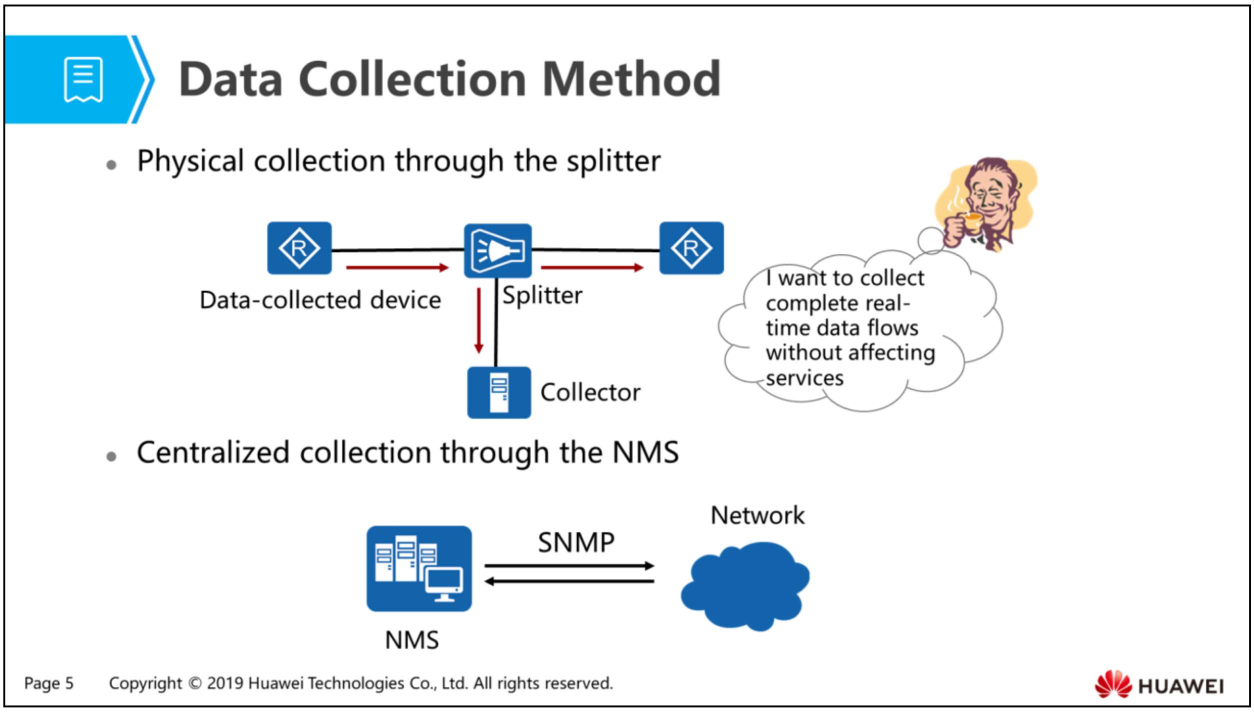
Purposes of data collection

Real-time service monitoring

Fault analysis and location

Network traffic optimization

- Real-time service monitoring:
  - In large networks or data centers, the monitoring system is often deployed on aggregation devices to monitor network data traffic in real time and prevent service abnormalities.
- Fault analysis and location:
  - Some faults need to be located using collected packet information.
- Network traffic optimization:
  - Refined data traffic control becomes particularly important when the network system expands. You can provide a better network solution only when you collect actual data traffic of the live network and use the professional traffic analysis system to locate specific network problems.



Data Collection Method

- Physical collection through the splitter

Data-collected device

Splitter

Collector

I want to collect complete real-time data flows without affecting services

- Centralized collection through the NMS

NMS

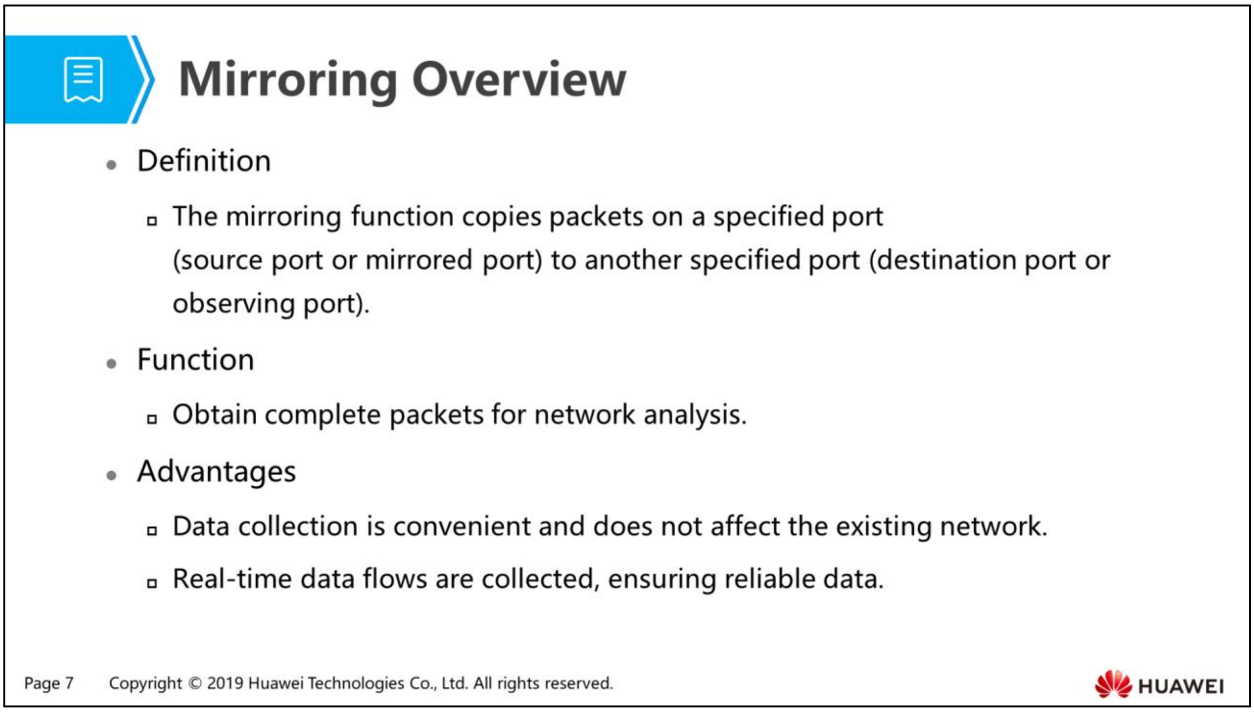
SNMP

Network

- Physical collection through the splitter
  - A splitter is physically connected to the link to copy normal data flows to the collector.
  - The collected data is complete and reliable and data collection is performed only on the intermediate link, without affecting performance of the data-collected device nor occupying link bandwidth.
  - The disadvantage is that a splitter needs to be physically connected to the link, which is complicate and risky.
  - This method is applicable to data flow collection of large ingress and egress network service devices and is often used in the network where an IDS device is connected.
- Centralized collection through the NMS
  - Standard MIB data is transmitted through the common standard protocol SNMP to collect the network-wide configuration and device interface data flows.
  - The advantage is that information about all the devices on the network can be collected. The disadvantage is that the collected interface data is not precise enough nor complete and most of the information is interface statistics.
  - This method is applicable when you need to view parameters, performance, and service statistics of devices on the NMS.

Contents

1. Mirroring Background
2. **Mirroring Concepts**
3. Mirroring Configuration

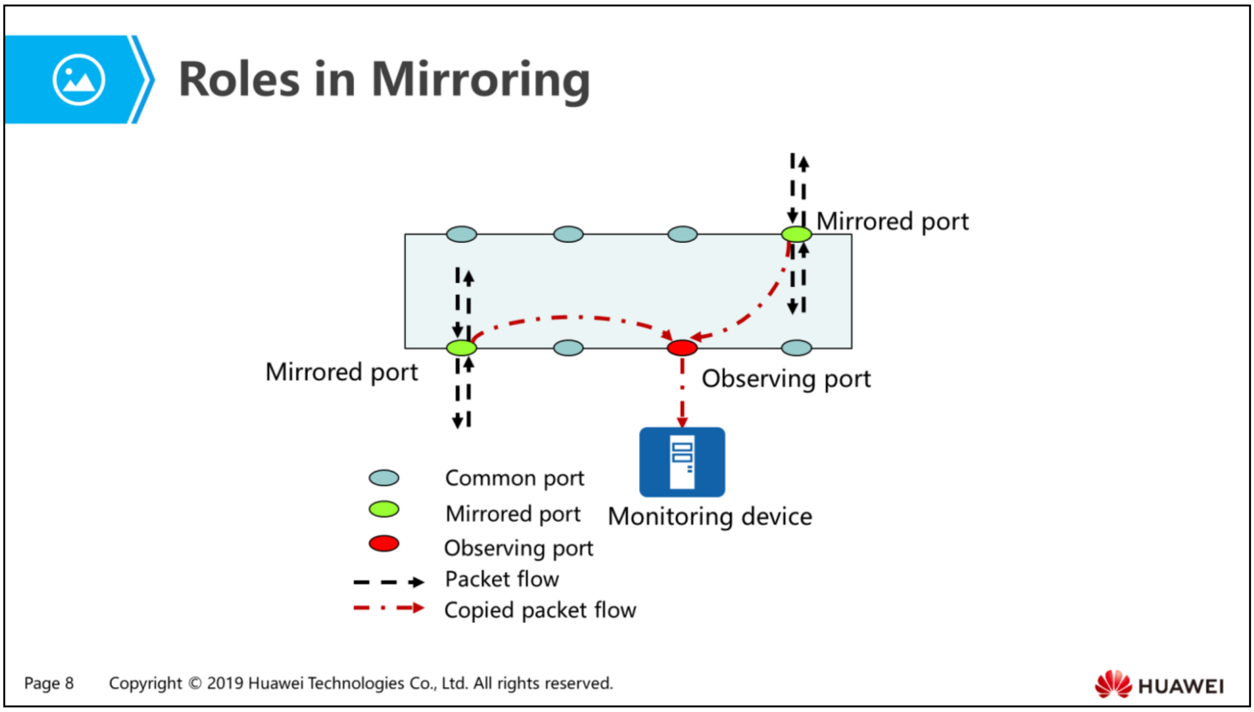


Mirroring Overview

- Definition
  - The mirroring function copies packets on a specified port (source port or mirrored port) to another specified port (destination port or observing port).
- Function
  - Obtain complete packets for network analysis.
- Advantages
  - Data collection is convenient and does not affect the existing network.
  - Real-time data flows are collected, ensuring reliable data.

HUAWEI

- Mirroring characteristics:
  - During network maintenance, you may need to obtain and analyze packets in some conditions. For example, if you detect suspected attack packets, you need to obtain and analyze the packets without affecting packet forwarding.
  - The mirroring function copies packets on a mirrored port to an observing port without affecting packet processing on devices. Administrators can analyze the copied packets using the data monitoring device for network monitoring and troubleshooting.
  - The mirroring function can copy traffic on multiple mirrored ports to the same observing port. There is no limit on the number of mirrored ports that can be configured. However, you need to check whether the actual traffic on the observing port exceeds the forwarding capability of this observing port. That is, you need to check whether the actual traffic exceeds the maximum bandwidth of this observing port.

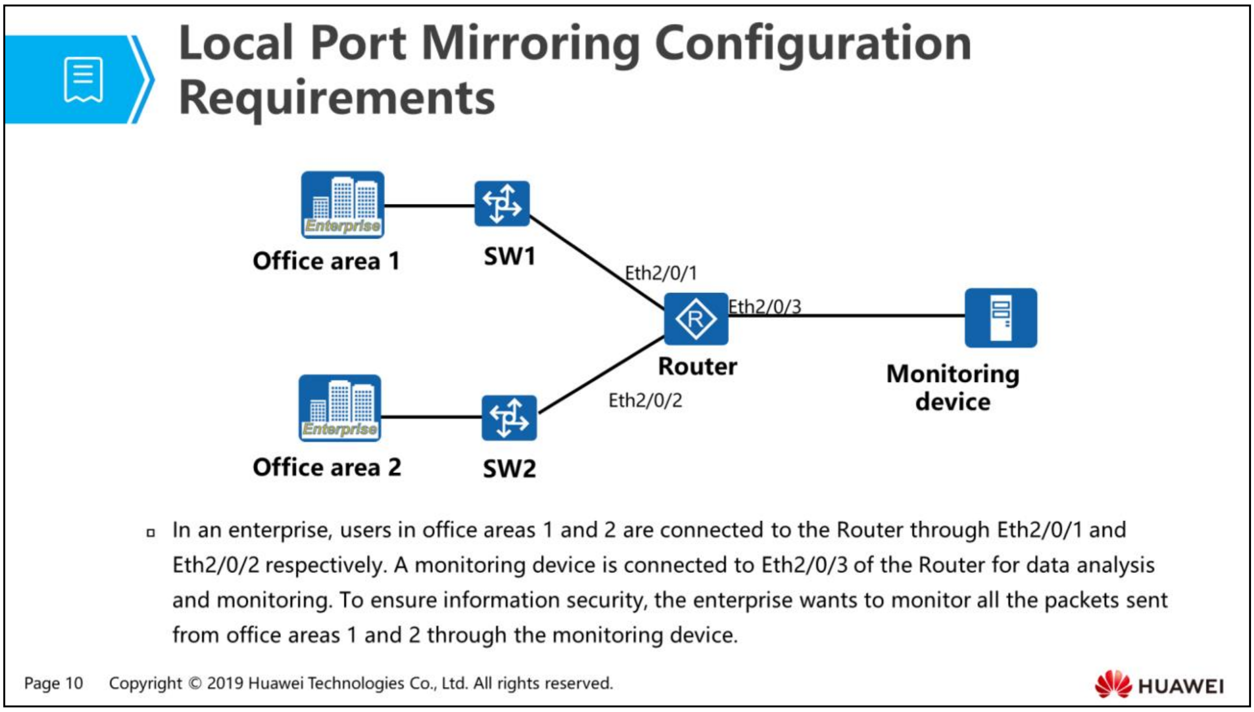


Roles in Mirroring

- Mirrored port:
  - A mirrored port is a monitored port, on which all the packets passing through or the packets matching traffic classification rules are copied to an observing port.
- Observing port:
  - An observing port is connected to a monitoring device to output the packets copied from mirrored ports.

Contents

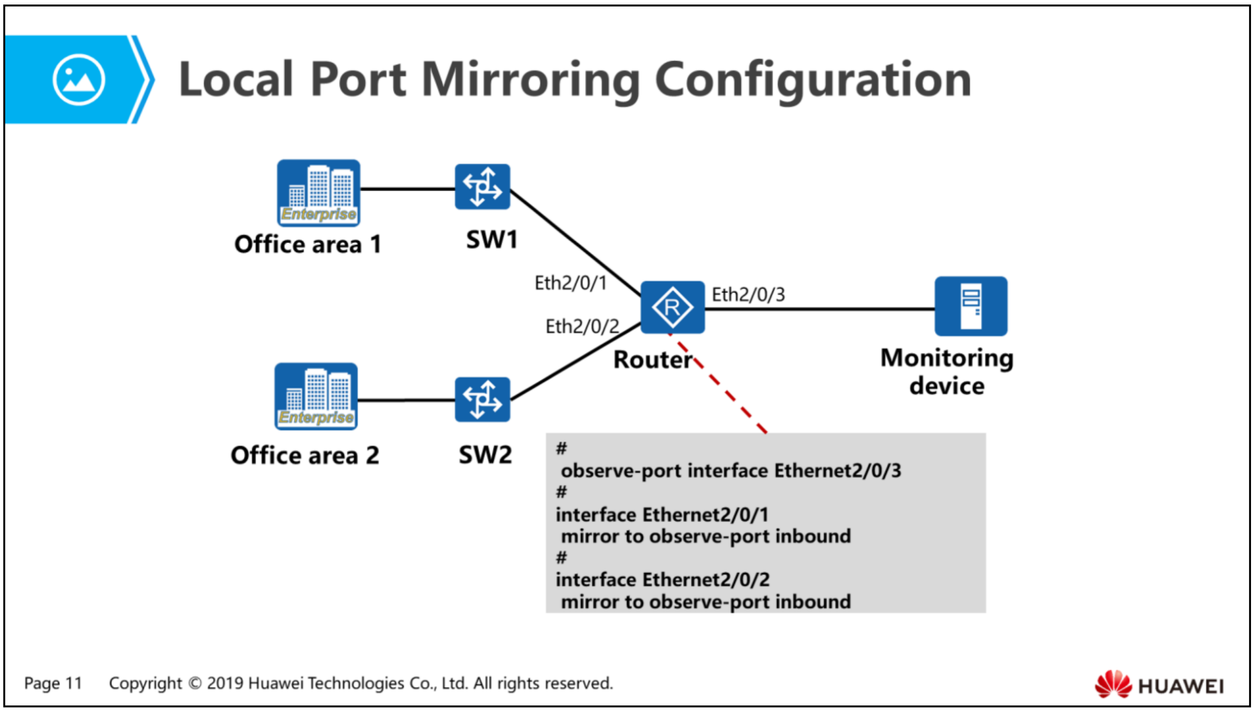
1. Mirroring Background
2. Mirroring Concepts
3. **Mirroring Configuration**



Local Port Mirroring Configuration Requirements

- In an enterprise, users in office areas 1 and 2 are connected to the Router through Eth2/0/1 and Eth2/0/2 respectively. A monitoring device is connected to Eth2/0/3 of the Router for data analysis and monitoring. To ensure information security, the enterprise wants to monitor all the packets sent from office areas 1 and 2 through the monitoring device.

- Configuration roadmap:
  - On the Router, configure Eth2/0/3 as the local observing port.
  - On the Router, configure Eth2/0/1 and Eth2/0/2 as mirrored ports for packet monitoring.

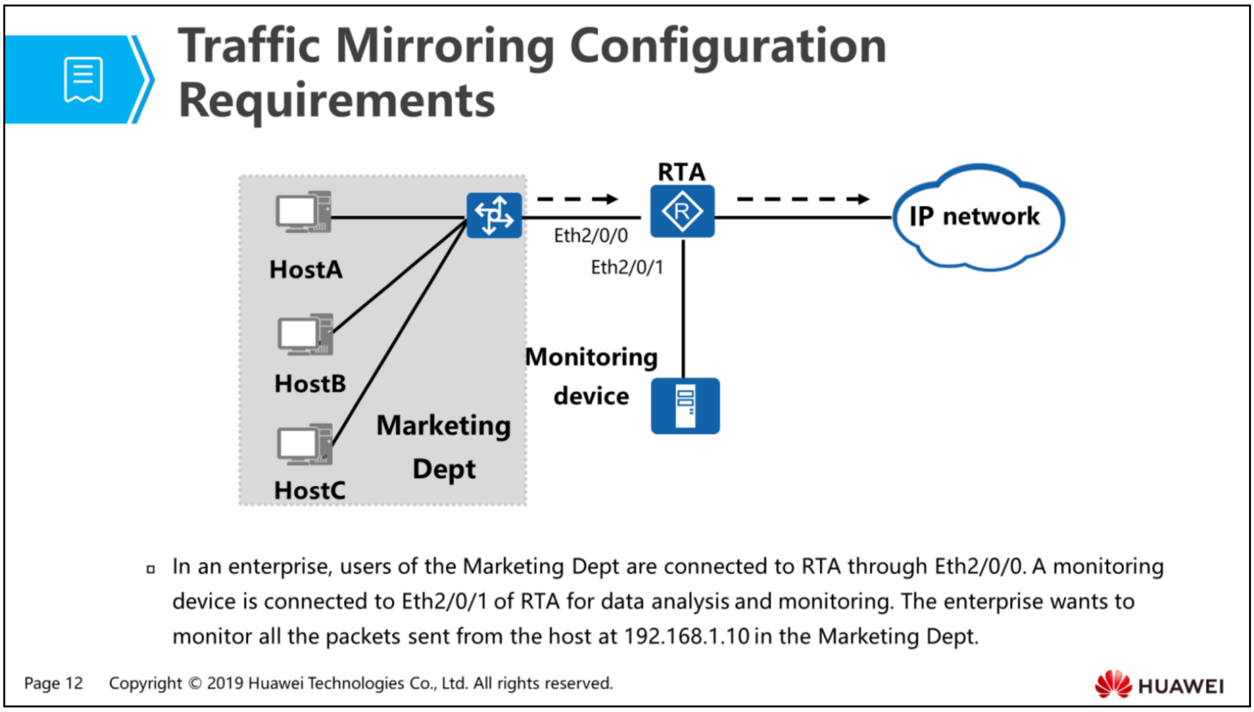


Local Port Mirroring Configuration

```
#
 observe-port interface Ethernet2/0/3
#
interface Ethernet2/0/1
 mirror to observe-port inbound
#
interface Ethernet2/0/2
 mirror to observe-port inbound
```

- Configuration commands:

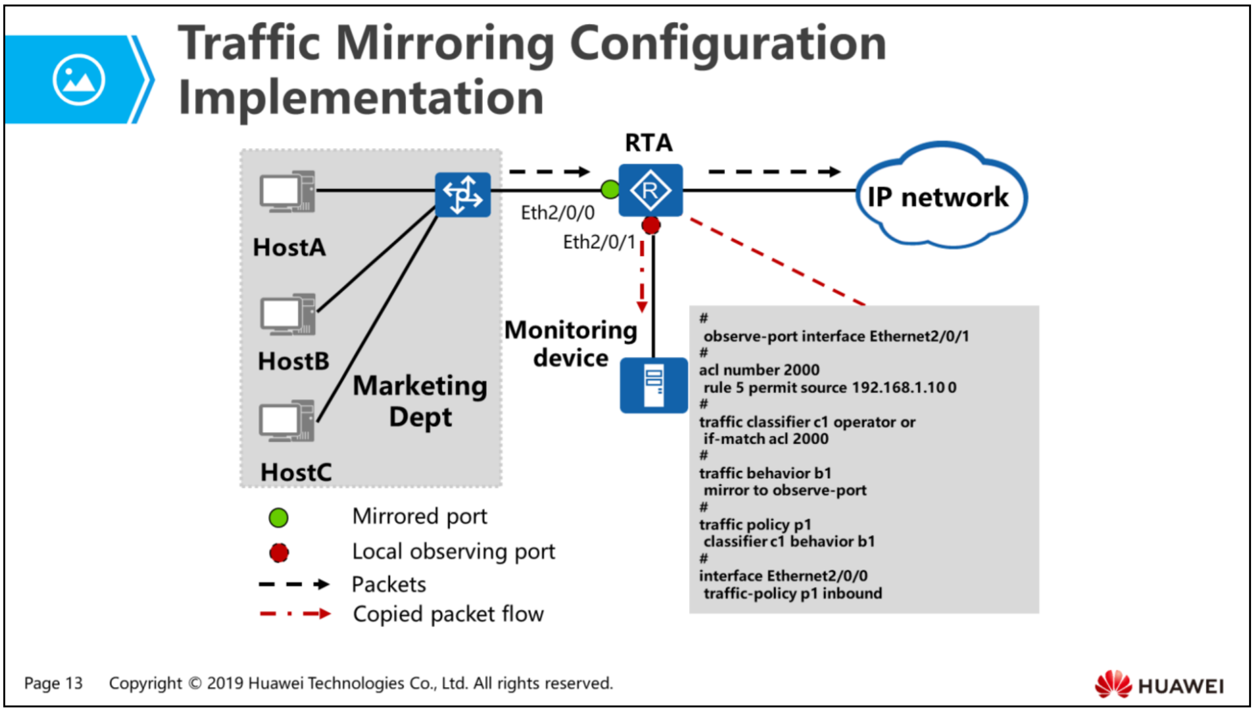
```
#
 observe-port interface Ethernet2/0/3     //Configure Eth2/0/3 as an observing port.
#
interface Ethernet2/0/1
 mirror to observe-port inbound           //Configure Eth2/0/1 as a mirrored port to copy all incoming packets.
#
interface Ethernet2/0/2
 mirror to observe-port inbound           //Configure Eth2/0/2 as a mirrored port to copy all incoming packets.
```



Traffic Mirroring Configuration Requirements

- In an enterprise, users of the Marketing Dept are connected to RTA through Eth2/0/0. A monitoring device is connected to Eth2/0/1 of RTA for data analysis and monitoring. The enterprise wants to monitor all the packets sent from the host at 192.168.1.10 in the Marketing Dept.

- Traffic mirroring:
  - Specified packets on a mirrored port are copied to a monitoring device for data analysis and monitoring. During traffic mirroring, a specified traffic policy is applied to the mirrored port. If packets passing through the mirrored port match this traffic policy, these packets are copied to the monitored device.
- Configuration roadmap:
  - Configure Eth2/0/1 as the local observing port.
  - Configure a traffic mirroring policy and apply it in the inbound direction of Eth2/0/0 to copy the packets with the source IP address 192.168.1.10 to the local observing port.



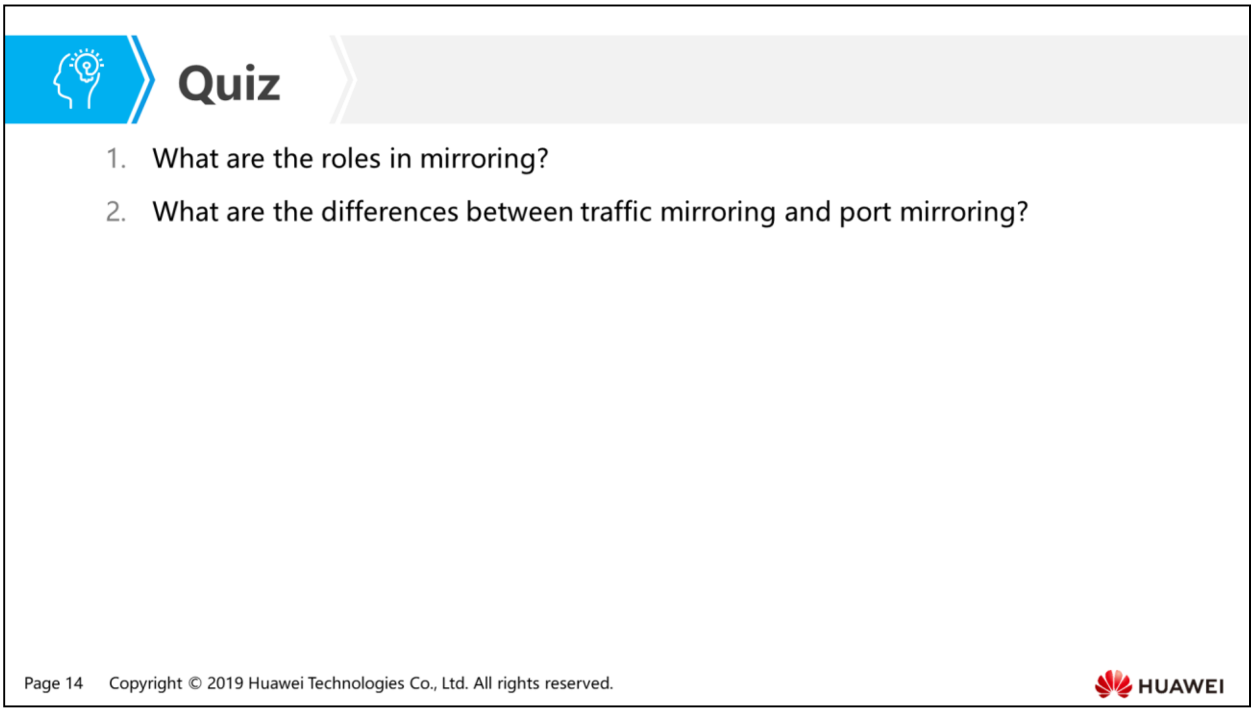
Traffic Mirroring Configuration Implementation

```
#
 observe-port interface Ethernet2/0/1
#
acl number 2000
 rule 5 permit source 192.168.1.10 0
#
traffic classifier c1 operator or
 if-match acl 2000
#
traffic behavior b1
 mirror to observe-port
#
traffic policy p1
 classifier c1 behavior b1
#
interface Ethernet2/0/0
 traffic-policy p1 inbound
```

Page 13   Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.   HUAWEI

- Configuration commands:

```
#
 observe-port interface Ethernet2/0/1     //Configure Eth2/0/1 as an observing port.
#
acl number 2000                           //Configure an ACL to match the packets
sent from the host 192.168.1.10.
 rule 5 permit source 192.168.1.10 0
#
traffic classifier c1 operator or
 if-match acl 2000
#
traffic behavior b1
 mirror to observe-port
#
traffic policy p1                         //Define a traffic policy to copy the packets
matching the ACL to the observing port.
 classifier c1 behavior b1
#
interface Ethernet2/0/0
 traffic-policy p1 inbound                //Apply the traffic policy in the inbound
direction of the mirrored port Eth2/0/0.
```



Quiz

1. What are the roles in mirroring?
2. What are the differences between traffic mirroring and port mirroring?

Page 14

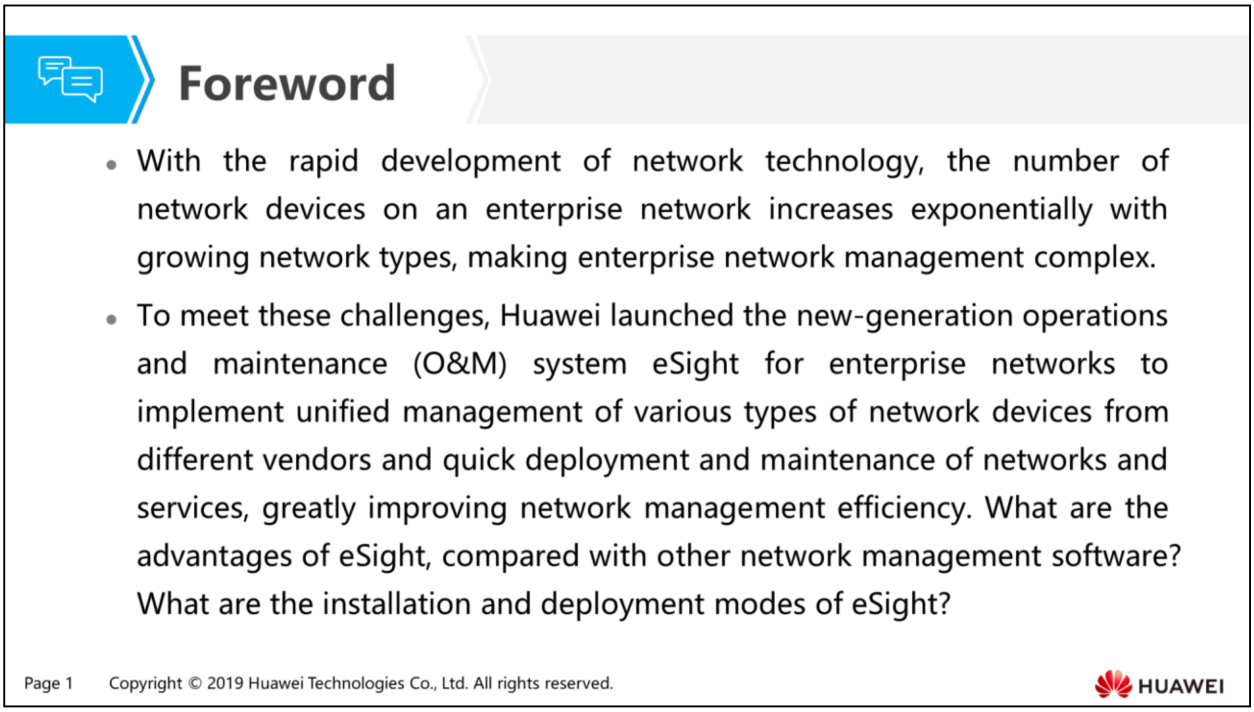
HUAWEI

- Answer: The roles include mirrored port and observing port.
- Answer: Traffic mirroring collects specific service flows on mirrored ports, whereas port mirroring collects all service flows on mirrored ports.

Thank You

www.huawei.com

eSight Overview

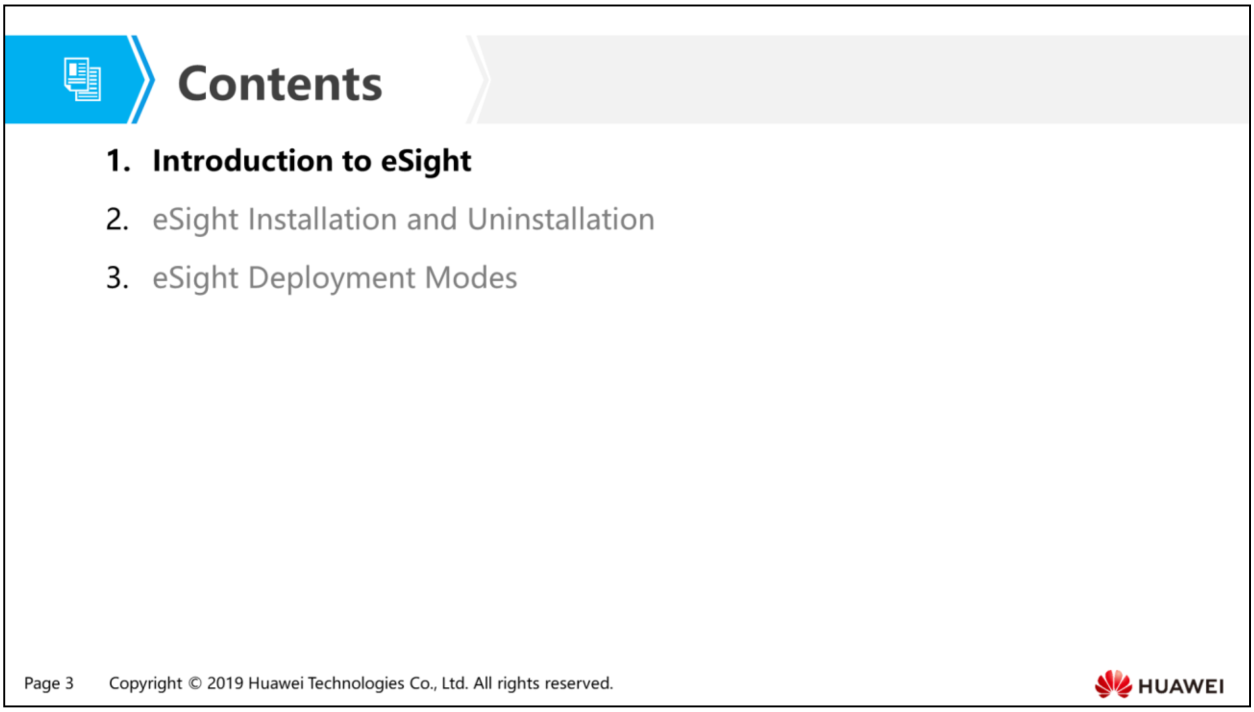


Foreword

- With the rapid development of network technology, the number of network devices on an enterprise network increases exponentially with growing network types, making enterprise network management complex.
- To meet these challenges, Huawei launched the new-generation operations and maintenance (O&M) system eSight for enterprise networks to implement unified management of various types of network devices from different vendors and quick deployment and maintenance of networks and services, greatly improving network management efficiency. What are the advantages of eSight, compared with other network management software? What are the installation and deployment modes of eSight?

Objectives

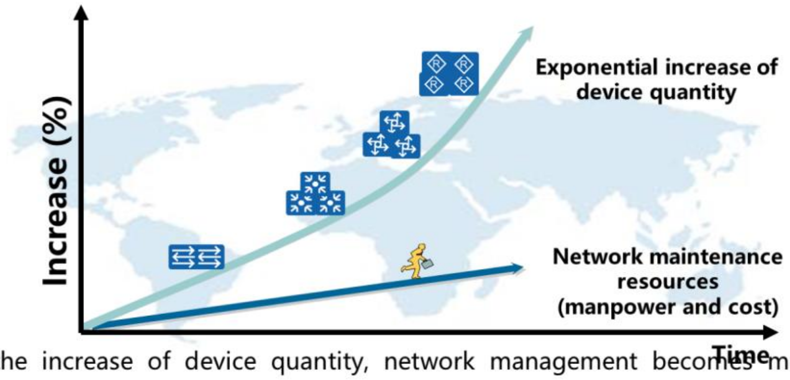
- Upon completion of this section, you will be able to:
  - Understand the background about eSight
  - Master eSight installation and uninstallation procedures
  - Master the eSight license application process



Contents

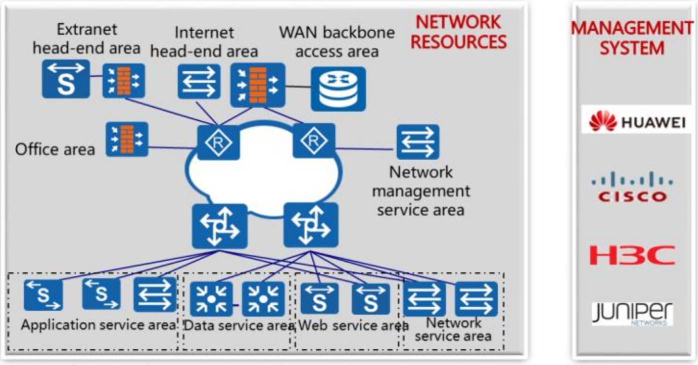
1. **Introduction to eSight**
2. eSight Installation and Uninstallation
3. eSight Deployment Modes

Enterprise Network Management Requirements: Increasing Device Quantity

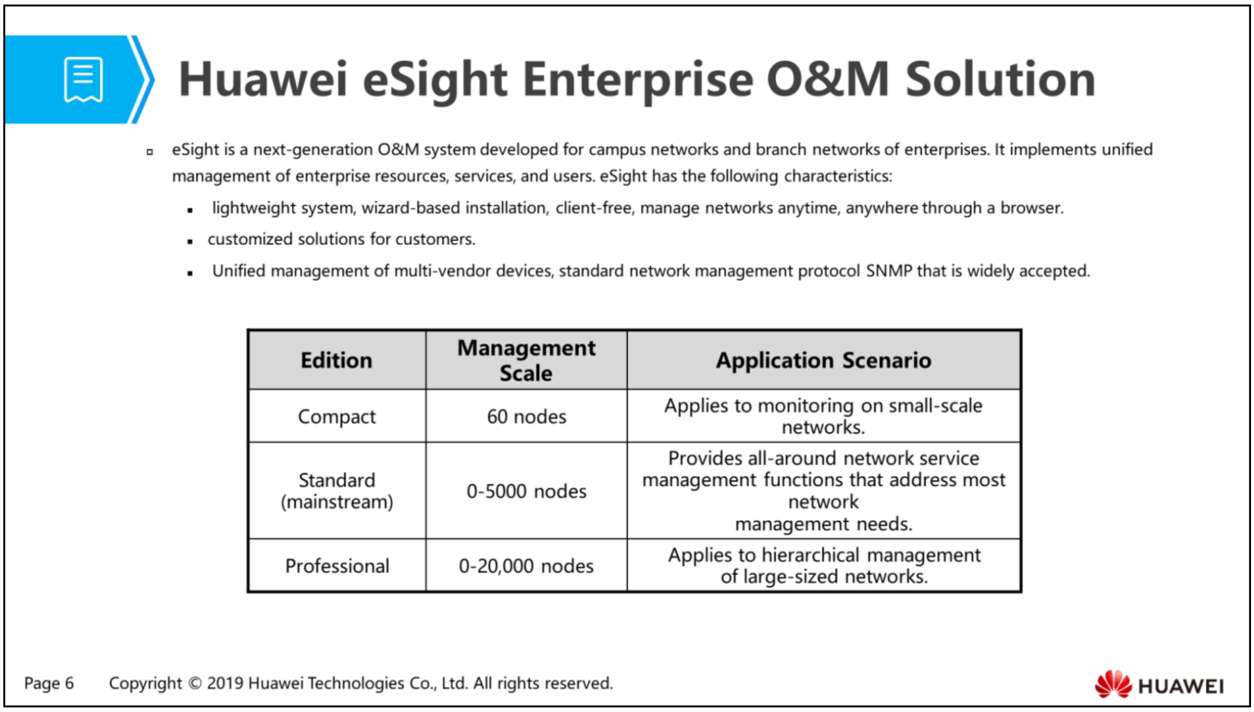


- With the increase of device quantity, network management becomes more and more complex. More maintenance personnel are required and the maintenance costs are increased. Enterprises are in urgent need for a network management platform that allows maintenance personnel to easily manage a large scale of devices.

Enterprise Network Management Requirements: Unified Management of Multi-Vendor Devices



- After network devices of a specific vendor are deployed on a network, a network management system (NMS) of this vendor needs to be installed to manage these devices because NMS vendors can only manage their own devices. Besides, the operation interfaces and fields of the NMSs are different. To realize efficient management of devices over the entire network, a standard universal network management protocol is required.



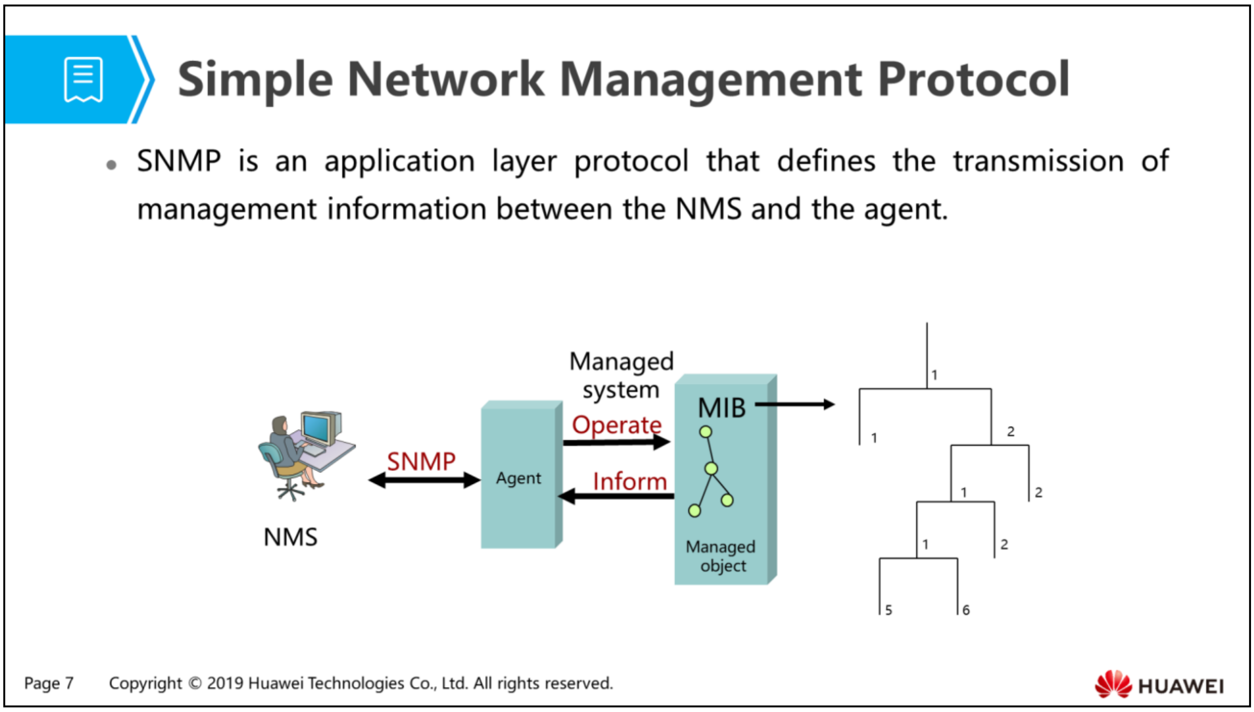
Huawei eSight Enterprise O&M Solution

- eSight is a next-generation O&M system developed for campus networks and branch networks of enterprises. It implements unified management of enterprise resources, services, and users. eSight has the following characteristics:
  - lightweight system, wizard-based installation, client-free, manage networks anytime, anywhere through a browser.
  - customized solutions for customers.
  - Unified management of multi-vendor devices, standard network management protocol SNMP that is widely accepted.

Edition	Management Scale	Application Scenario
Compact	60 nodes	Applies to monitoring on small-scale networks.
Standard (mainstream)	0-5000 nodes	Provides all-around network service management functions that address most network management needs.
Professional	0-20,000 nodes	Applies to hierarchical management of large-sized networks.

Page 6

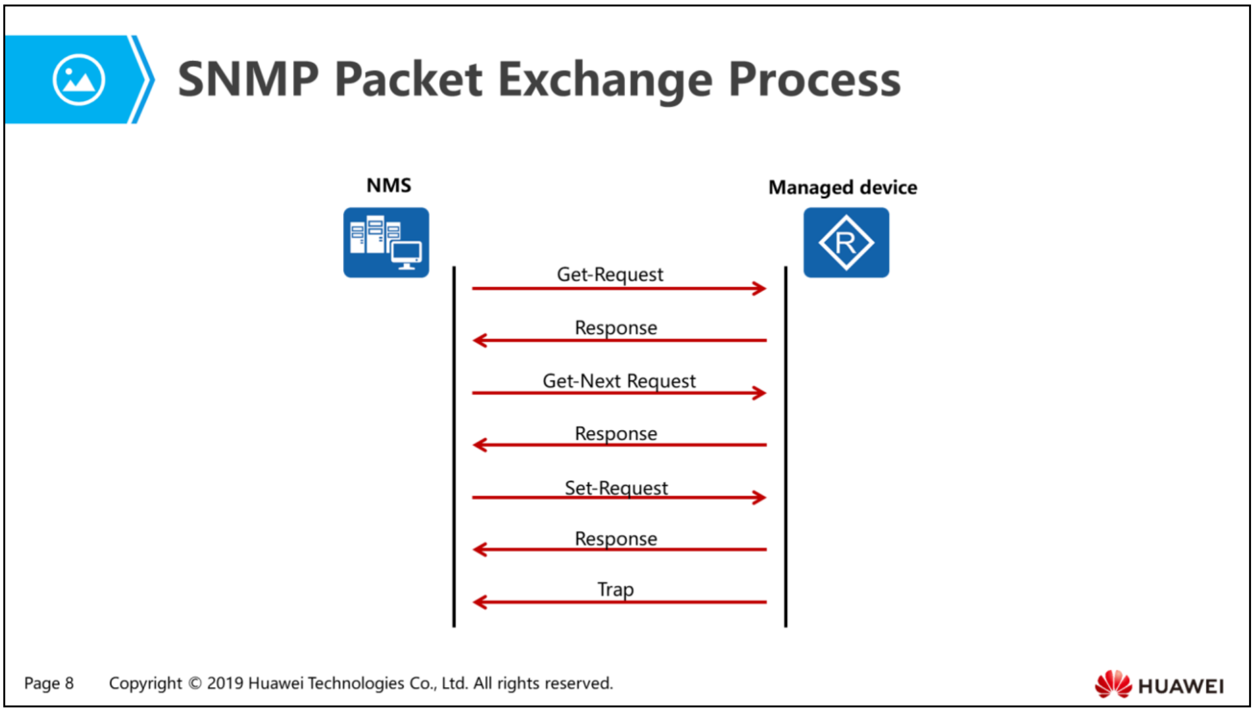
- eSight provides flexible management capabilities for Huawei and third-party devices as follows:
  - Network devices from Huawei, H3C, Cisco, and ZTE as well as IT devices from IBM, HP, and SUN.
  - Third-party devices that support standard management information base (MIB) (RFC1213-MIB, Entity-MIB, SNMPv2-MIB, and IF-MIB) through user-defined settings.
  - For third-party devices that do not support the standard MIB, you can install NE patches for device adaptation.
- How does eSight communicate with managed devices?



Simple Network Management Protocol

- SNMP is an application layer protocol that defines the transmission of management information between the NMS and the agent.

- An NMS is network management software that runs on the NMS workstation. Network administrators operate the NMS to send requests to managed devices, so that they can monitor and configure these devices.
- SNMP has three versions:
  - SNMPv1: is easy to implement but has poor security.
  - SNMPv2c: has moderate security and is most widely used.
  - SNMPv3: defines a management frame and references the user security model (USM) to provide a secure access control mechanism.
- An agent is a network management process running on a managed device. After the managed process receives a request from the NMS, the agent provides responses. The agent collects device status information, operates managed devices by executing commands on the NMS, and reports alarms to the NMS.
- The MIB is a virtual database of the device status maintained by the managed devices. An agent searches the MIB to collect device status information. An MIB organizes managed objects based on the hierarchical tree structure and uses the abstract syntax notation one (ASN.1) format to describe managed objects.



SNMP Packet Exchange Process

NMS

Managed device

Get-Request

Response

Get-Next Request

Response

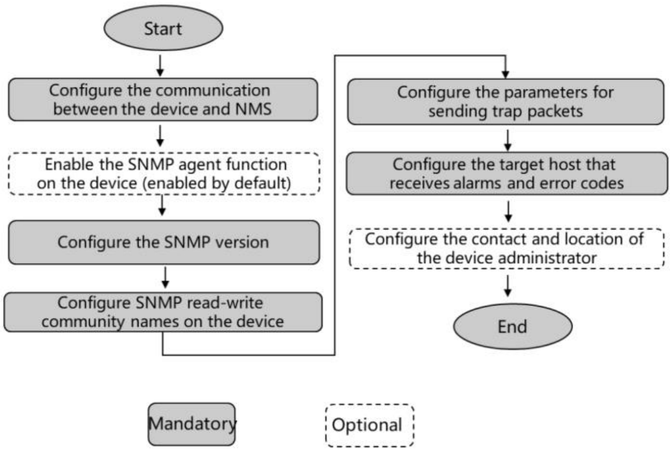
Set-Request

Response

Trap

- SNMPv1 defines five operations:
    - Get-Request: indicates that the NMS requests to retrieve one or more parameter values from the MIB of the agent process.
    - Get-Next-Request: indicates that the NMS requests to retrieve the next parameter value in the lexicographic order from the MIB of the agent process.
    - Set-Request: indicates that the NMS requests to set one or more parameter values for the MIB of the agent process.
    - Response: indicates the agent process returns one or more parameter values. This is a response to the previous three operations.
    - Trap: indicates that the agent process sends unsolicited packets to the NMS, notifying critical or major events on the device.

Configuring SNMP on a Router



Start

Configure the communication between the device and NMS

Enable the SNMP agent function on the device (enabled by default)

Configure the SNMP version

Configure SNMP read-write community names on the device

Configure the parameters for sending trap packets

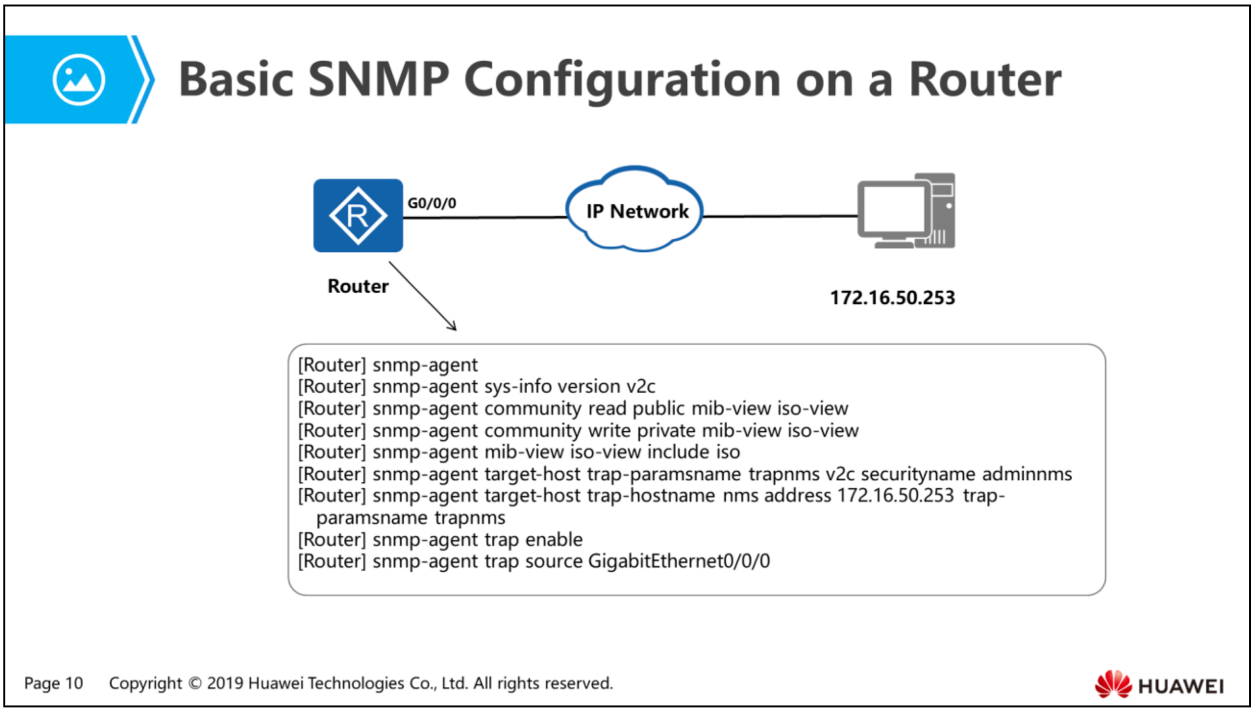
Configure the target host that receives alarms and error codes

Configure the contact and location of the device administrator

End

Mandatory

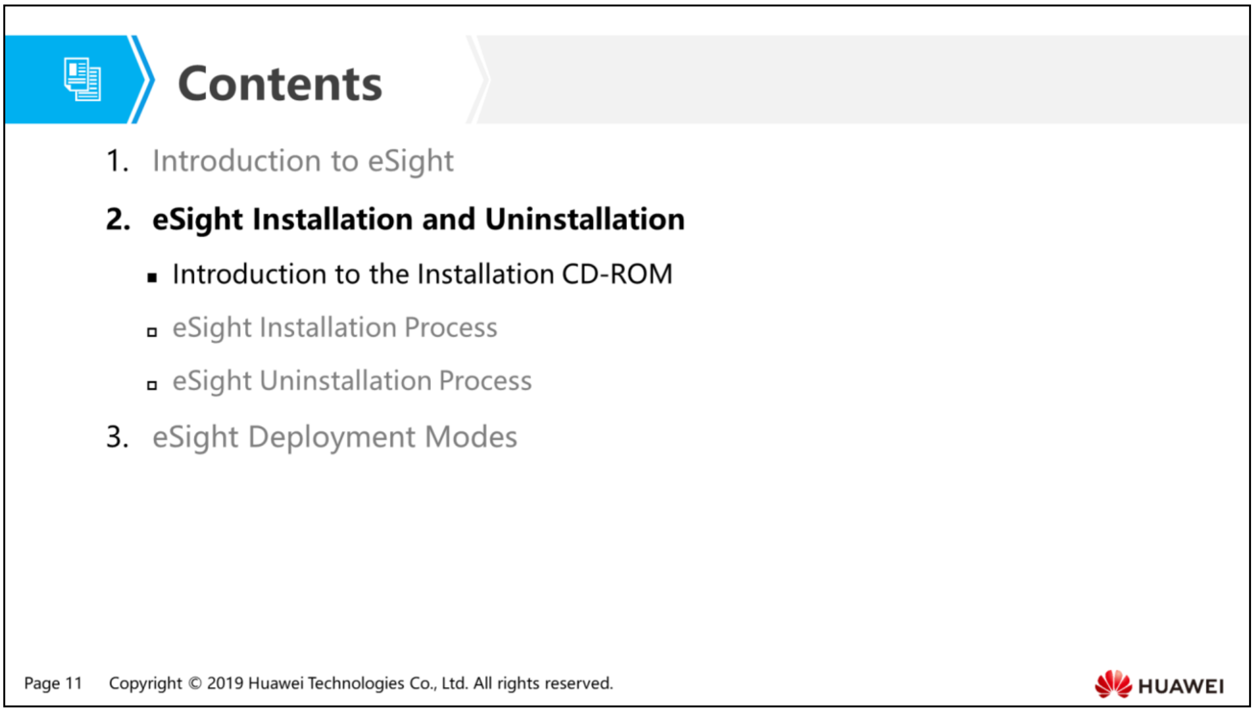
Optional



Basic SNMP Configuration on a Router

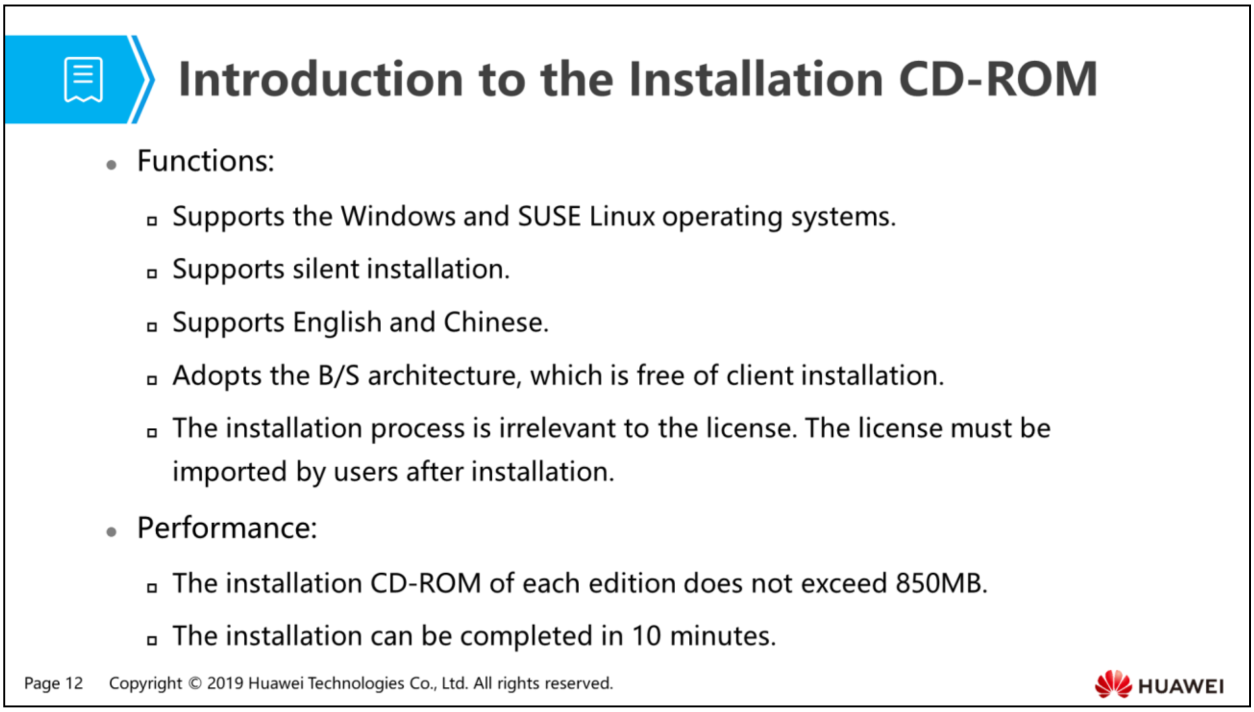
```
[Router] snmp-agent
[Router] snmp-agent sys-info version v2c
[Router] snmp-agent community read public mib-view iso-view
[Router] snmp-agent community write private mib-view iso-view
[Router] snmp-agent mib-view iso-view include iso
[Router] snmp-agent target-host trap-paramsname trapnms v2c securityname adminnms
[Router] snmp-agent target-host trap-hostname nms address 172.16.50.253 trap-
   paramsname trapnms
[Router] snmp-agent trap enable
[Router] snmp-agent trap source GigabitEthernet0/0/0
```

- Procedure
  - (Optional) Run the snmp-agent command to enable the SNMP agent function.
    - By default, the SNMP agent function is enabled.
  - Run the snmp-agent sys-info version v2c command to set the SNMP version to SNMPv2c.
  - Run the snmp-agent community { read | write } community-name [mib-view view-name | acl acl-number] command to configure the read-write community names for the device. Then run the mib-view view-name or acl acl-number command to control access from the NMS to the device.



Contents

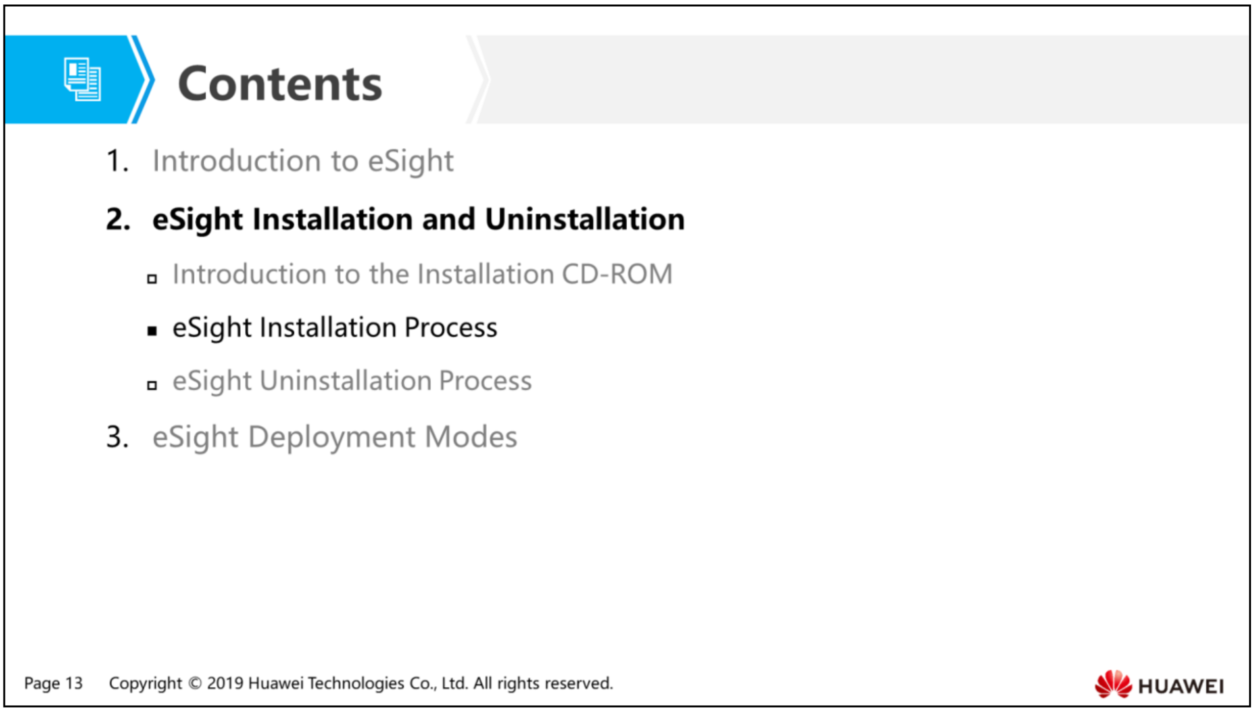
1. Introduction to eSight
2. **eSight Installation and Uninstallation**
   - Introduction to the Installation CD-ROM
   - eSight Installation Process
   - eSight Uninstallation Process
3. eSight Deployment Modes



Introduction to the Installation CD-ROM

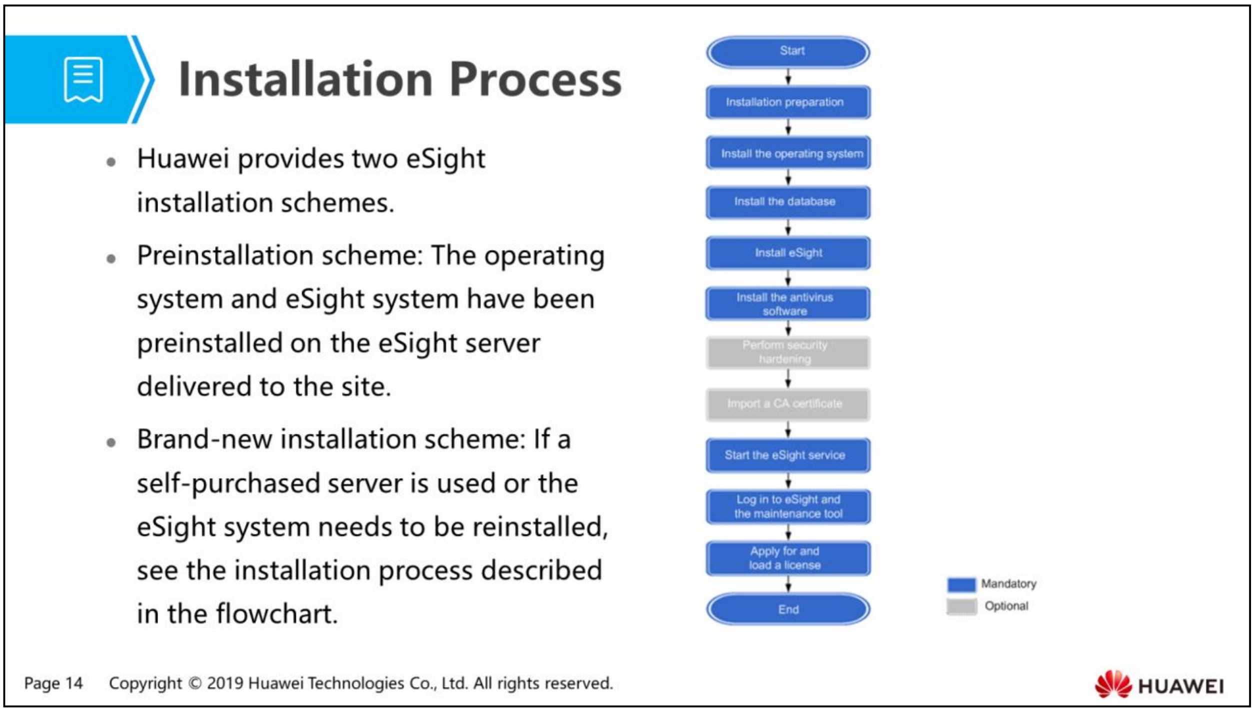
- Functions:
  - Supports the Windows and SUSE Linux operating systems.
  - Supports silent installation.
  - Supports English and Chinese.
  - Adopts the B/S architecture, which is free of client installation.
  - The installation process is irrelevant to the license. The license must be imported by users after installation.
- Performance:
  - The installation CD-ROM of each edition does not exceed 850MB.
  - The installation can be completed in 10 minutes.

- eSight can be installed in either of the following ways: installation CD-ROM or software package.



Contents

1. Introduction to eSight
2. **eSight Installation and Uninstallation**
   - Introduction to the Installation CD-ROM
   - eSight Installation Process
   - eSight Uninstallation Process
3. eSight Deployment Modes



Installation Process

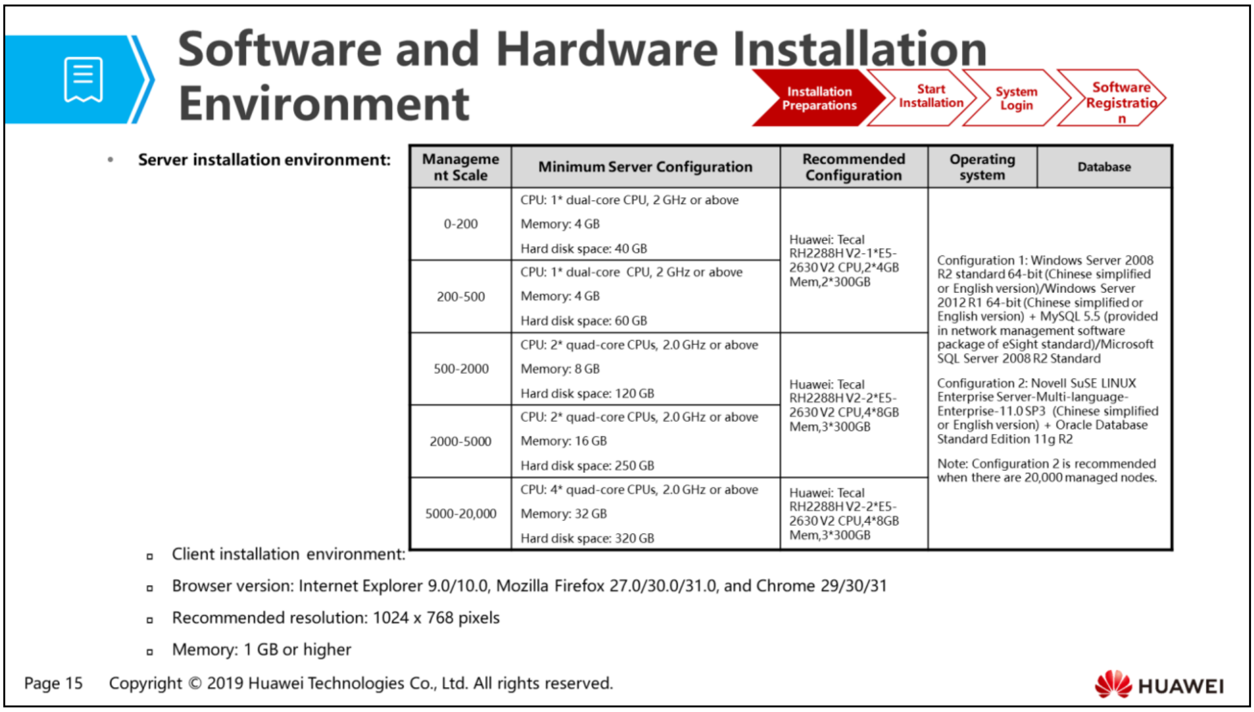
- Huawei provides two eSight installation schemes.
- Preinstallation scheme: The operating system and eSight system have been preinstalled on the eSight server delivered to the site.
- Brand-new installation scheme: If a self-purchased server is used or the eSight system needs to be reinstalled, see the installation process described in the flowchart.

Start
↓
Installation preparation
↓
Install the operating system
↓
Install the database
↓
Install eSight
↓
Install the antivirus software
↓
Perform security hardening
↓
Import a CA certificate
↓
Start the eSight service
↓
Log in to eSight and the maintenance tool
↓
Apply for and load a license
↓
End

🟦 Mandatory
▨ Optional

HUAWEI

- Install antivirus software: Trend Micro OfficeScan is recommended as the matching antivirus software of eSight. Users can purchase OfficeScan when ordering eSight from Huawei.
- Import a CA certificate:
  - The security certificate is a digital certificate used to create a secure channel between the client browser and web server for data encryption and transmission.
  - The differences between a self-signed certificate and a CA certificate are as follows:
    - Self-signed certificate: Specifies a temporary security certificate generated during eSight installation and used to ensure the normal running of eSight after the installation. A self-signed certificate is automatically generated during eSight installation.
    - A CA certificate is a security certificate issued by an authorized organization. Users need to send an application to the organization.



Software and Hardware Installation Environment

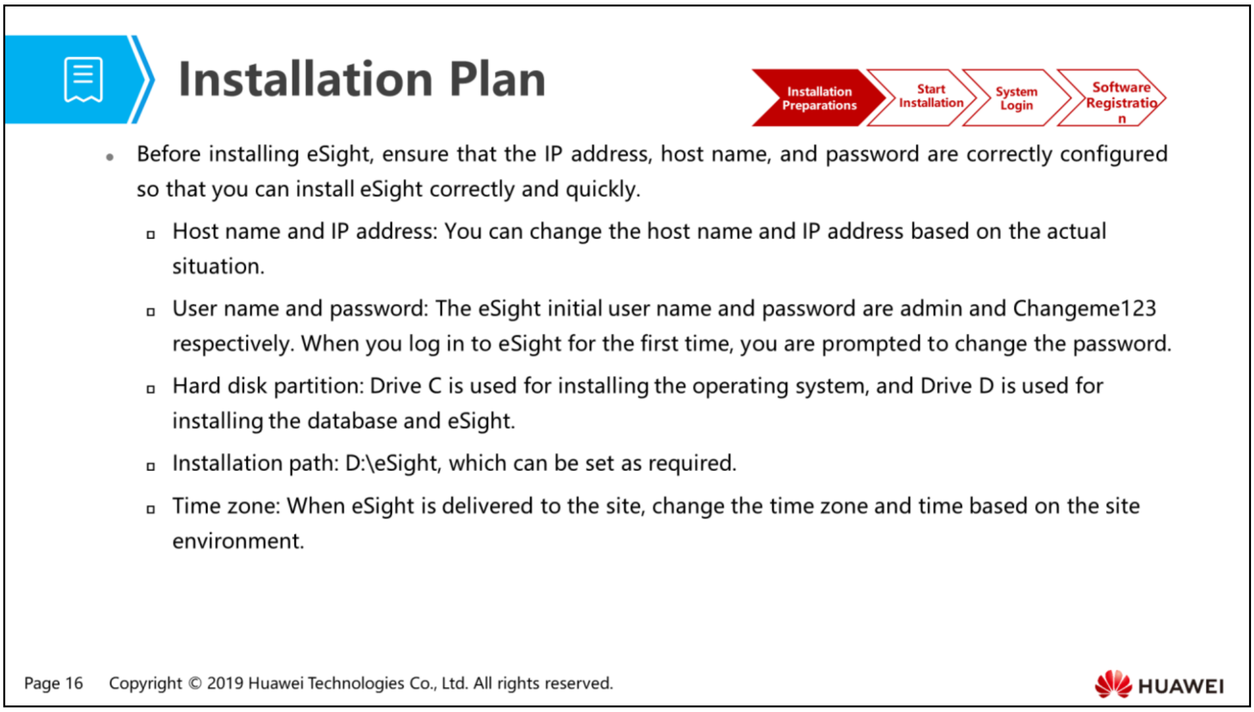
Installation Preparations
Start Installation
System Login
Software Registration

- **Server installation environment:**

Management Scale	Minimum Server Configuration	Recommended Configuration	Operating system	Database
0-200	CPU: 1* dual-core CPU, 2 GHz or above Memory: 4 GB Hard disk space: 40 GB	Huawei: Tecal RH2288H V2-1*E5-2630 V2 CPU,2*4GB Mem,2*300GB	Configuration 1: Windows Server 2008 R2 standard 64-bit (Chinese simplified or English version)/Windows Server 2012 R1 64-bit (Chinese simplified or English version) + MySQL 5.5 (provided in network management software package of eSight standard)/Microsoft SQL Server 2008 R2 Standard Configuration 2: Novell SuSE LINUX Enterprise Server-Multi-language-Enterprise-11.0 SP3 (Chinese simplified or English version) + Oracle Database Standard Edition 11g R2 Note: Configuration 2 is recommended when there are 20,000 managed nodes.	
200-500	CPU: 1* dual-core CPU, 2 GHz or above Memory: 4 GB Hard disk space: 60 GB			
500-2000	CPU: 2* quad-core CPUs, 2.0 GHz or above Memory: 8 GB Hard disk space: 120 GB	Huawei: Tecal RH2288H V2-2*E5-2630 V2 CPU,4*8GB Mem,3*300GB		
2000-5000	CPU: 2* quad-core CPUs, 2.0 GHz or above Memory: 16 GB Hard disk space: 250 GB			
5000-20,000	CPU: 4* quad-core CPUs, 2.0 GHz or above Memory: 32 GB Hard disk space: 320 GB	Huawei: Tecal RH2288H V2-2*E5-2630 V2 CPU,4*8GB Mem,3*300GB		

- Client installation environment:
- Browser version: Internet Explorer 9.0/10.0, Mozilla Firefox 27.0/30.0/31.0, and Chrome 29/30/31
- Recommended resolution: 1024 x 768 pixels
- Memory: 1 GB or higher

- The client has no special requirement on the operating system, but the browser version and memory must meet the requirements.



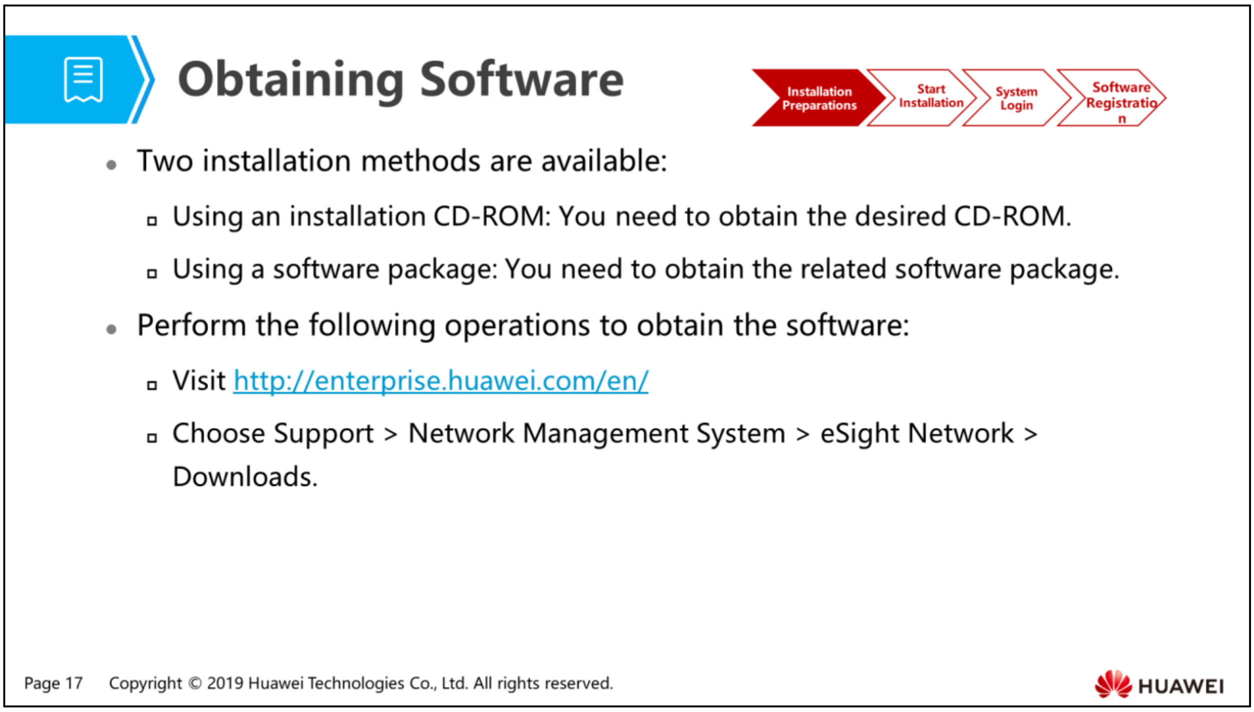
Installation Plan

Installation Preparations → Start Installation → System Login → Software Registratio n

- Before installing eSight, ensure that the IP address, host name, and password are correctly configured so that you can install eSight correctly and quickly.
  - Host name and IP address: You can change the host name and IP address based on the actual situation.
  - User name and password: The eSight initial user name and password are admin and Changeme123 respectively. When you log in to eSight for the first time, you are prompted to change the password.
  - Hard disk partition: Drive C is used for installing the operating system, and Drive D is used for installing the database and eSight.
  - Installation path: D:\eSight, which can be set as required.
  - Time zone: When eSight is delivered to the site, change the time zone and time based on the site environment.

HUAWEI

- IP address of the eSight server:
  - Must be a static IP address.
  - Can be an IPv4, IPv6, or IPv4/IPv6 dual-stack address, depending on the actual networking planning.
  - The server and managed devices can communicate properly.
  - The server and client can communicate properly.



Obtaining Software

Installation Preparations

Start Installation

System Login

Software Registration

- Two installation methods are available:
  - Using an installation CD-ROM: You need to obtain the desired CD-ROM.
  - Using a software package: You need to obtain the related software package.
- Perform the following operations to obtain the software:
  - Visit http://enterprise.huawei.com/en/
  - Choose Support > Network Management System > eSight Network > Downloads.

Installing the Database

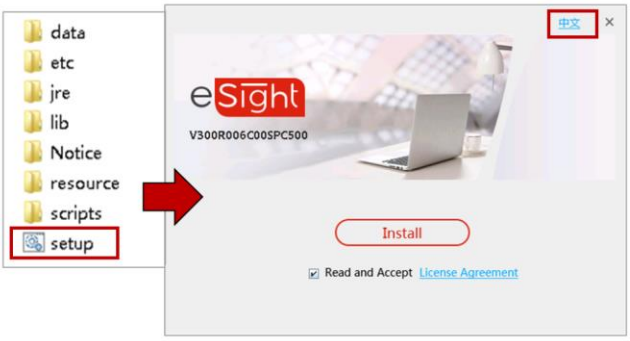
Installation Preparations
Start Installation
System Login
Software Registratio n

- On the Windows Server 2008 R2, two types of databases are supported. You can select one as required.
  - MySQL database: It is automatically installed with eSight software. Users do not need to install the MySQL database separately.
  - SQL Server 2008 database: It requires manual installation before eSight installation. Users are advised to install the SQL Server 2008 database by referring to its delivered installation manual.

Installation Preparations > Start Installation > System Login > Software Registration

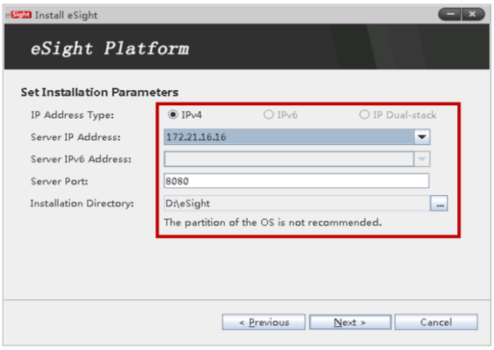
Starting the eSight Installation Program

- Double-click setup.bat to start the installation process. Select a language to determine the language of the installation GUI and operation GUI.



- Once the installation language is selected, it cannot be changed after the installation is complete. To use another language, reinstall eSight.

Setting Installation Parameters



Install eSight

eSight Platform

Set Installation Parameters

IP Address Type: ● IPv4 ○ IPv6 ○ IP Dual-stack

Server IP Address: 172.21.16.16

Server IPv6 Address:

Server Port: 8080

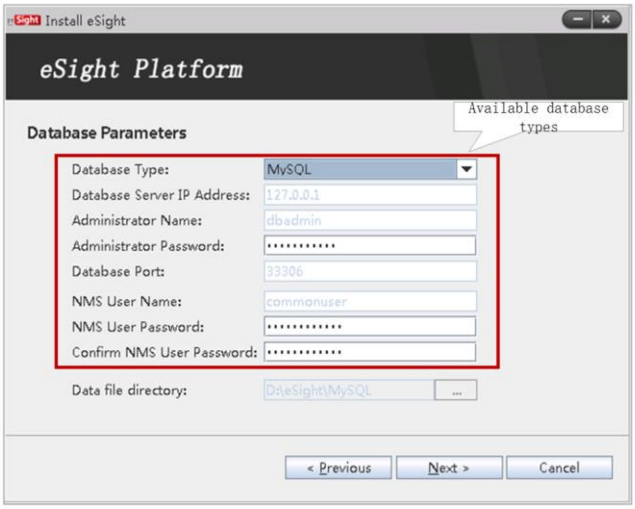
Installation Directory: D:\eSight

The partition of the OS is not recommended.

- Server IP Address: specifies the default IP address of the current server. If the server has multiple IP addresses in the drop-down list box, select a routable IP address.
- Server Port: The default port number is 8080. If port 8080 has been used, change the port number.
- Installation Directory: specifies the installation directory of eSight, which can be modified by users.

Installation Preparations > Start Installation > System Login > Software Registration

Setting Database Parameters



Install eSight

eSight Platform

Available database types

Database Parameters

Database Type:	MySQL
Database Server IP Address:	127.0.0.1
Administrator Name:	dbadmin
Administrator Password:	•••••••••••
Database Port:	33306
NMS User Name:	commonuser
NMS User Password:	•••••••••••••
Confirm NMS User Password:	•••••••••••••
Data file directory:	D:\eSight\MySQL

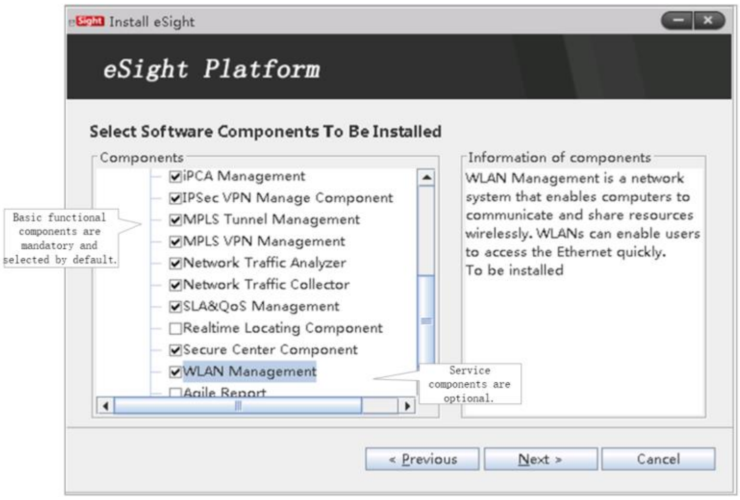
< Previous | Next > | Cancel

HUAWEI

- When Database Type is set to MySQL, the system uses the default database user name root and password Changeme123. The root is default user name of the MySQL database. This user is the database system administrator and has all the database rights.
- When Database Type is set to SQLServer and eSight is installed for the first time, you need to manually enter the user name sa and password Changme123. The sa is default user name of the SQL Server database. This user is the database system administrator and has all the database rights.
- In incremental installation, you do not need to set the password as the password parameters are unavailable.

Installation Preparations → Start Installation → System Login → Software Registration

Selecting Components to Be Installed


Install eSight

eSight Platform

Select Software Components To Be Installed

Components
- ☑ iPCA Management
- ☑ IPSec VPN Manage Component
- ☑ MPLS Tunnel Management
- ☑ MPLS VPN Management
- ☑ Network Traffic Analyzer
- ☑ Network Traffic Collector
- ☑ SLA&QoS Management
- □ Realtime Locating Component
- ☑ Secure Center Component
- ☑ WLAN Management
- □ Agile Report

Information of components

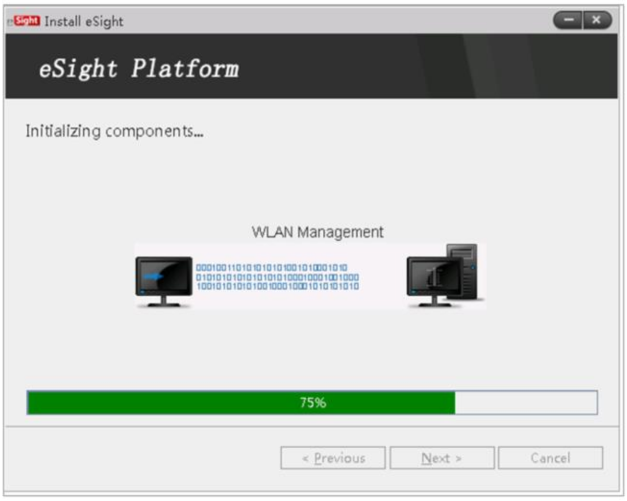
WLAN Management is a network system that enables computers to communicate and share resources wirelessly. WLANs can enable users to access the Ethernet quickly.
To be installed

Basic functional components are mandatory and selected by default.

Service components are optional.

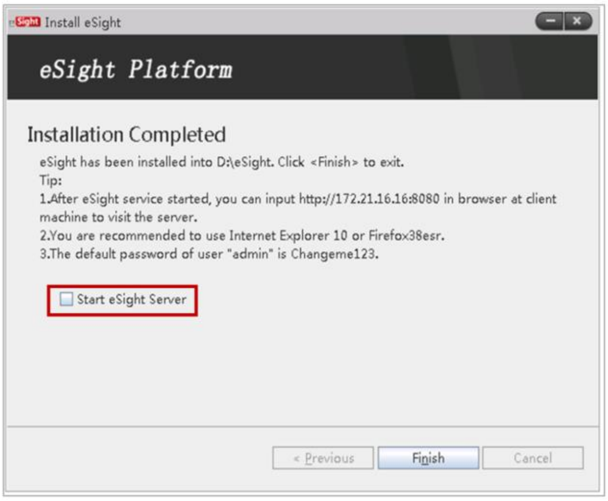
- Basic functional components are dimmed.
- Select service components as required. eSight components support incremental installation. If a component is not installed during the first eSight installation, it can be installed during the next eSight installation.
- Different licenses cover different components.

Displaying the Installation Progress



Initializing components...

Installation Completed



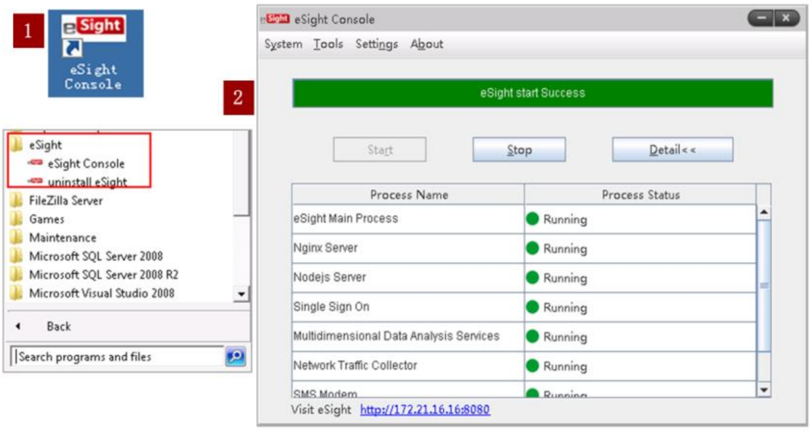
Installation Completed

eSight has been installed into D:\eSight. Click <Finish> to exit.
Tip:
1.After eSight service started, you can input http://172.21.16.16:8080 in browser at client machine to visit the server.
2.You are recommended to use Internet Explorer 10 or Firefox38esr.
3.The default password of user "admin" is Changeme123.

□ Start eSight Server

Installation Preparations > Start Installation > System Login > Software Registration

Starting the eSight Service



eSight
eSight Console
uninstall eSight
FileZilla Server
Games
Maintenance
Microsoft SQL Server 2008
Microsoft SQL Server 2008 R2
Microsoft Visual Studio 2008
Back
Search programs and files

eSight Console

System Tools Settings About

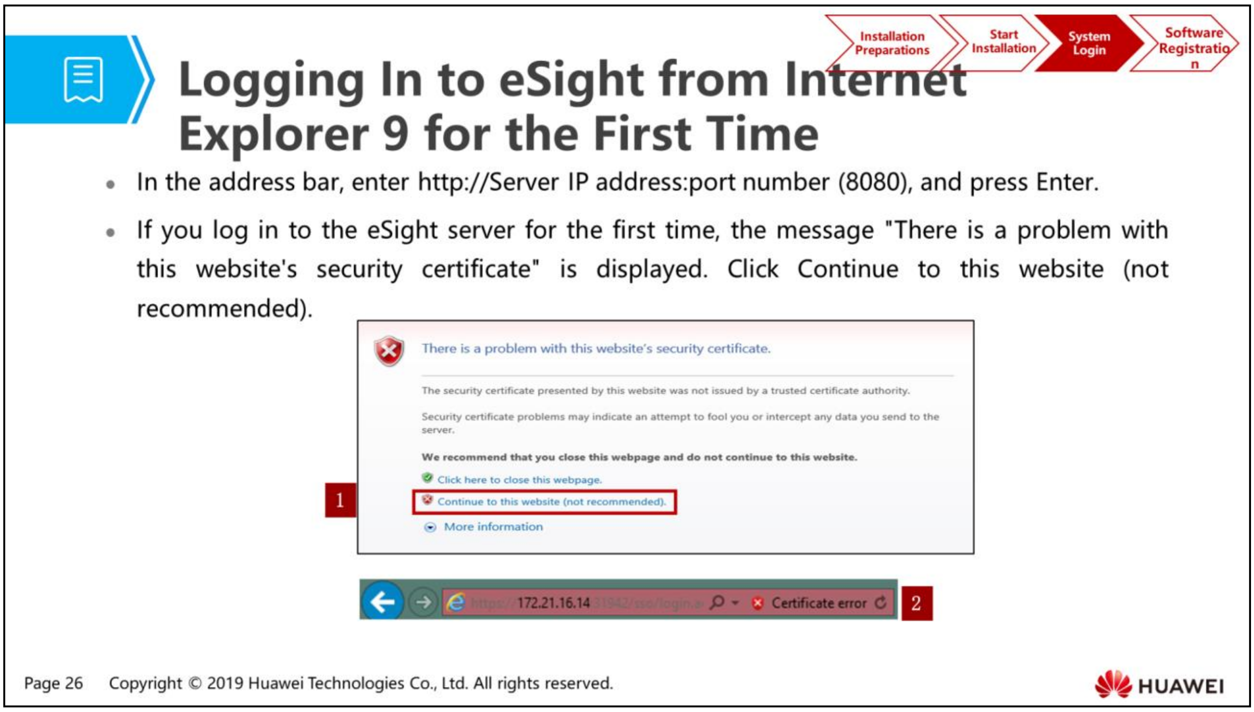
eSight start Success

Start Stop Detail<<

Process Name	Process Status
eSight Main Process	● Running
Nginx Server	● Running
Nodejs Server	● Running
Single Sign On	● Running
Multidimensional Data Analysis Services	● Running
Network Traffic Collector	● Running
SMS Modem	● Running

Visit eSight http://172.21.16.16:8080

- Start the eSight service using either of the following methods:
  - On the desktop, double-click the shortcut icon of eSight Console and choose Start.
  - Choose Start > All Programs > eSight > eSight Console and click Start.
- On the eSight Console that runs on the Windows operating system, you can click Settings, select or clear Startup with Windows automatically to enable whether eSight automatically starts with the operating system.



Logging In to eSight from Internet Explorer 9 for the First Time

- In the address bar, enter http://Server IP address:port number (8080), and press Enter.
- If you log in to the eSight server for the first time, the message "There is a problem with this website's security certificate" is displayed. Click Continue to this website (not recommended).

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

1 Continue to this website (not recommended).

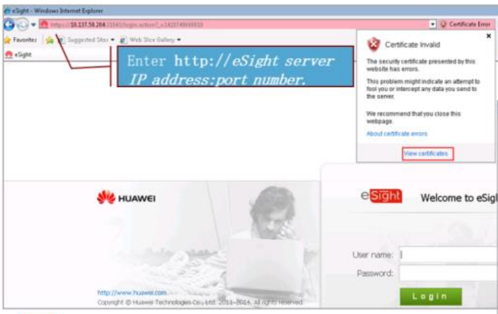
More information

https://172.21.16.14:31942/sso/login.a Certificate error 2

Page 26

- Login from Internet Explorer: If you log in to eSight for the first time, a message is displayed indicating that the connection is not trusted. Click Certificate error, View Certificate, and Install Certificate in sequence.

Installing a Certificate


eSight - Windows Internet Explorer
https://10.137.58.204:31943/login.action?_=1420749449919
Certificate Error
Favorites
Suggested Sites
Web Slice Gallery
eSight
HUAWEI
eSight
Welcome to eSig
User name:
Password:
Login
http://www.huawei.com
Copyright © Huawei Technologies Co., Ltd. 2011-2014. All rights reserved.

Enter http://*eSight server IP address:port number.*

Certificate Invalid

The security certificate presented by this website has errors.

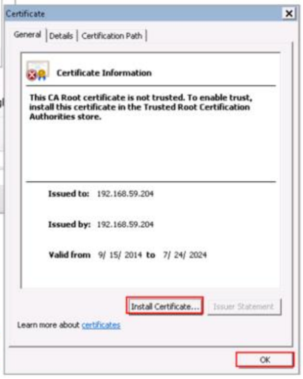
This problem might indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

About certificate errors

View certificates

1



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: 192.168.59.204

Issued by: 192.168.59.204

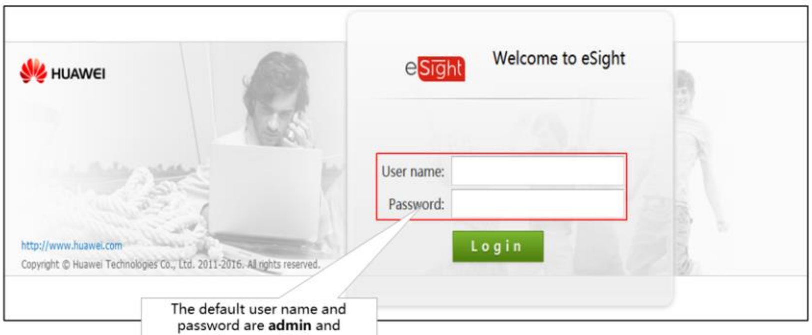
Valid from 9/ 15/ 2014 to 7/ 24/ 2024

Learn more about certificates

2

Entering the User Name and Password to Log In to eSight

Installation Preparations | Start Installation | System Login | Software Registration

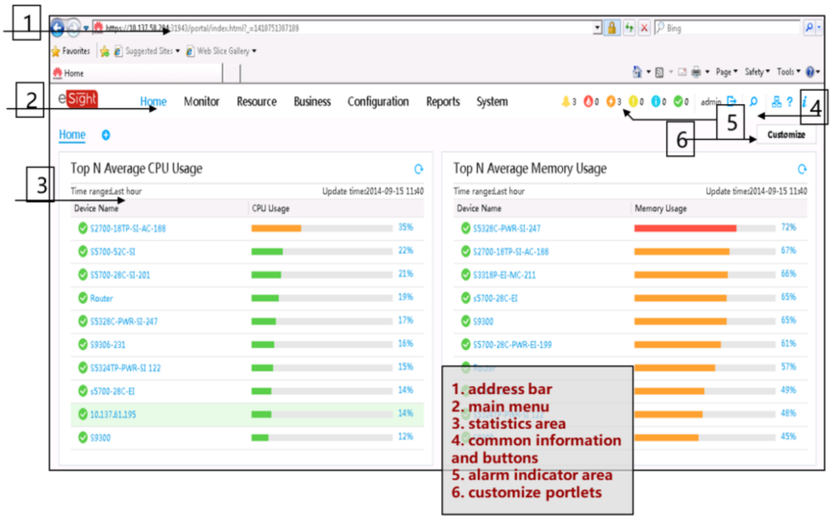


The default user name and password are **admin** and **Changeme123**.

- You need to change the password as prompted upon the first login to eSight. Keep your new password secure. If you forget the password of the admin user, you can only reinstall eSight to restore the initial password.
- You will be prompted to change the password several days before the validity period will due.

Login Succeeded

Installation Preparations → Start Installation → **System Login** → Software Registration



Top N Average CPU Usage

Time range:Last hour — Update time:2014-09-15 11:40

Device Name	CPU Usage
S2700-18TP-SI-AC-188	35%
S5700-52C-SI	22%
S5700-28C-SI-201	21%
Router	19%
S5328C-PWR-SI-247	17%
S9306-231	16%
S5324TP-PWR-SI 122	15%
s5700-28C-EI	14%
10.137.61.195	14%
S9300	12%

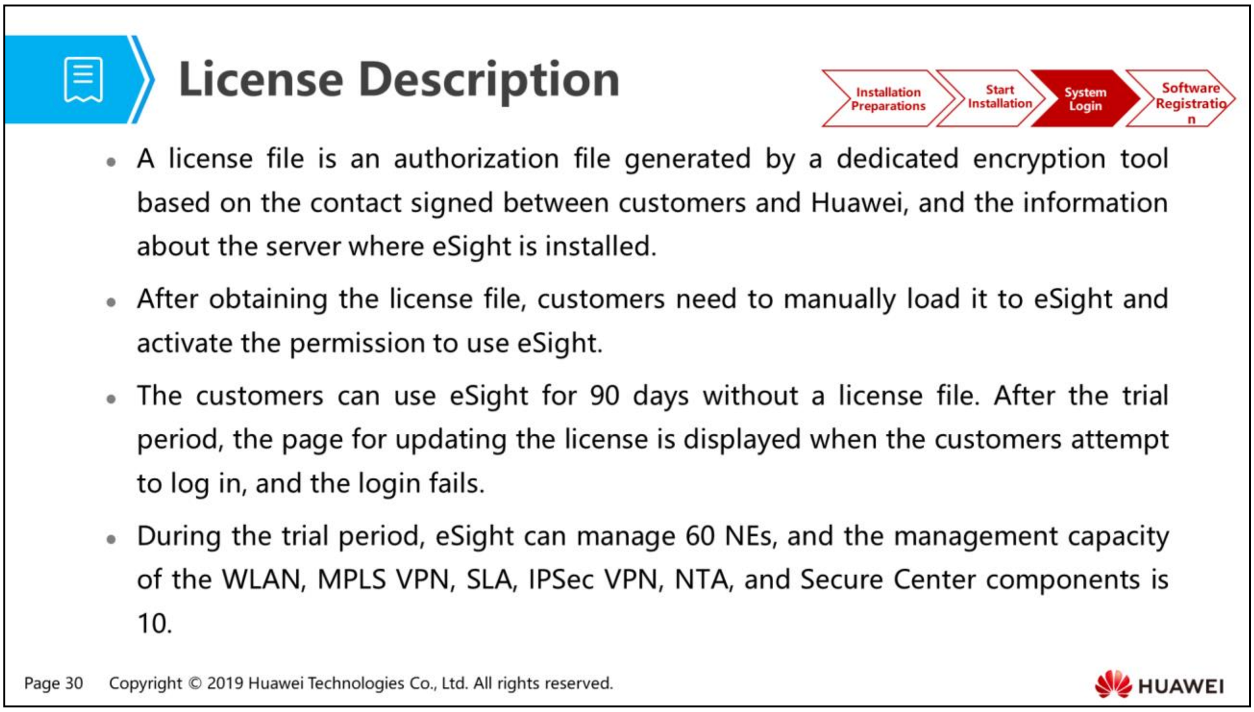
Top N Average Memory Usage

Time range:Last hour — Update time:2014-09-15 11:40

Device Name	Memory Usage
S5328C-PWR-SI-247	72%
S2700-18TP-SI-AC-188	67%
S3318P-EI-MC-211	66%
s5700-28C-EI	65%
S9300	65%
S5700-28C-PWR-EI-199	61%
Router	57%
[illegible]	49%
S5324TP-PWR-SI 122	48%
S9300	45%

1. address bar
2. main menu
3. statistics area
4. common information and buttons
5. alarm indicator area
6. customize portlets

- Portlets are small blocks on the home page that display the device and network status in a list, curve chart, or bar chart.



License Description

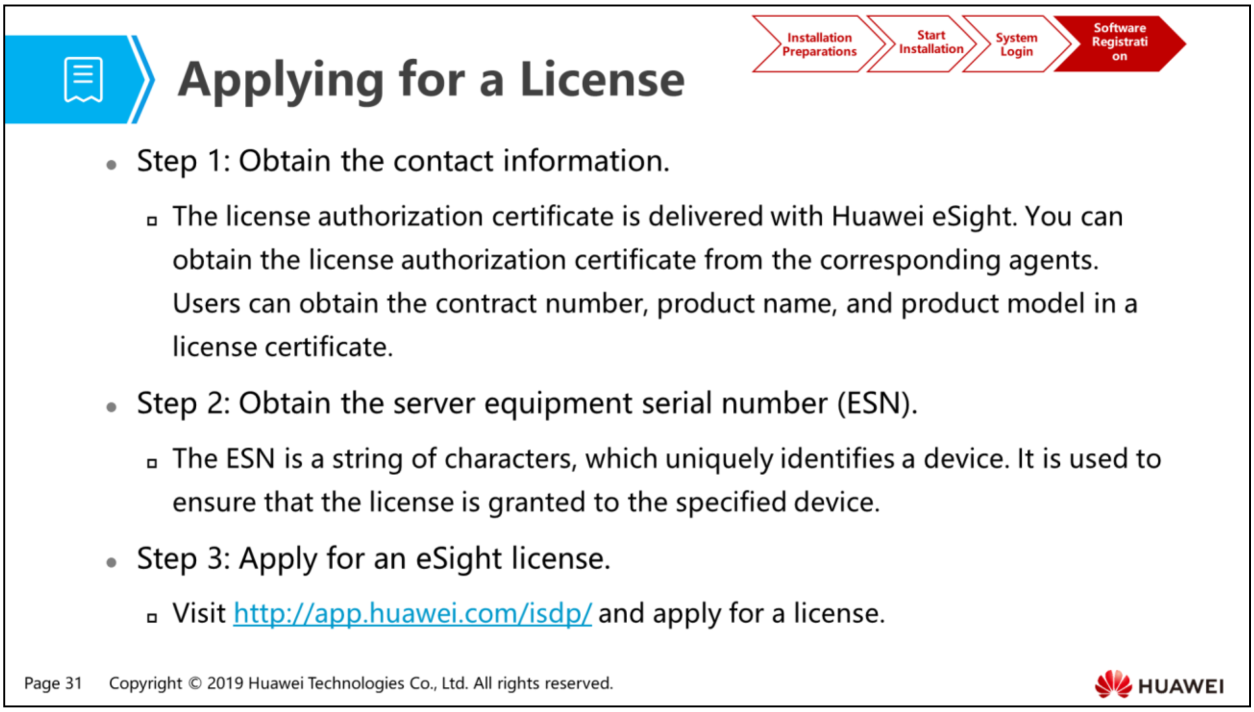
Installation Preparations > Start Installation > System Login > Software Registratio n

- A license file is an authorization file generated by a dedicated encryption tool based on the contact signed between customers and Huawei, and the information about the server where eSight is installed.
- After obtaining the license file, customers need to manually load it to eSight and activate the permission to use eSight.
- The customers can use eSight for 90 days without a license file. After the trial period, the page for updating the license is displayed when the customers attempt to log in, and the login fails.
- During the trial period, eSight can manage 60 NEs, and the management capacity of the WLAN, MPLS VPN, SLA, IPSec VPN, NTA, and Secure Center components is 10.

Page 30

HUAWEI

- When the system is started, it checks whether a license file is present. If the license file is absent, it automatically enters the trial period. The trial period lasts for 90 days, during which users can use all the installed functions.
- After the trial period, the page for updating the license is displayed when users attempt to log in, and the login fails.



Installation Preparations
Start Installation
System Login
Software Registrati on

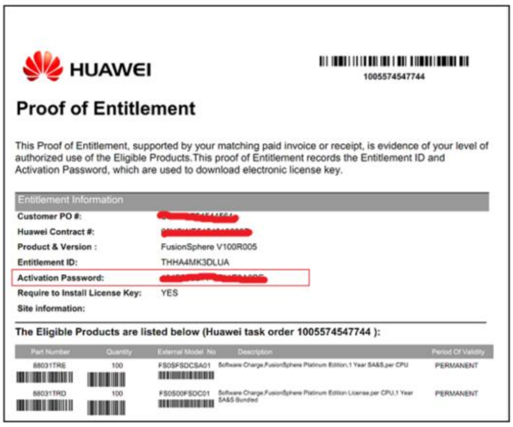
Applying for a License

- Step 1: Obtain the contact information.
  - The license authorization certificate is delivered with Huawei eSight. You can obtain the license authorization certificate from the corresponding agents. Users can obtain the contract number, product name, and product model in a license certificate.
- Step 2: Obtain the server equipment serial number (ESN).
  - The ESN is a string of characters, which uniquely identifies a device. It is used to ensure that the license is granted to the specified device.
- Step 3: Apply for an eSight license.
  - Visit http://app.huawei.com/isdp/ and apply for a license.

- For any problem encountered in the license application process, contact Huawei local eSight product manager or call the Huawei service hotline.

Obtaining Contract Information

- Obtain the contract number, product name, and product model.



HUAWEI

1005574547744

Proof of Entitlement

This Proof of Entitlement, supported by your matching paid invoice or receipt, is evidence of your level of authorized use of the Eligible Products.This proof of Entitlement records the Entitlement ID and Activation Password, which are used to download electronic license key.

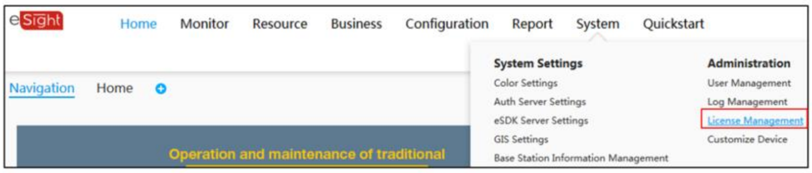
Entitlement Information	
Customer PO #:	[redacted]
Huawei Contract #:	[redacted]
Product & Version :	FusionSphere V100R005
Entitlement ID:	THHA4MK3DLUA
Activation Password:	[redacted]
Require to Install License Key:	YES
Site information:	

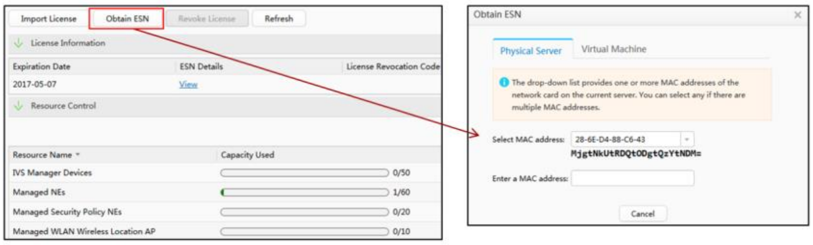
The Eligible Products are listed below (Huawei task order 1005574547744):

Part Number	Quantity	External Model No	Description	Period Of Validity
88031TRE	100	FS0SFSDCSA01	Software Charge,FusionSphere Platinum Edition,1 Year SA&S,per CPU	PERMANENT
88031TRD	100	FS0S00FSDC01	Software Charge,FusionSphere Platinum Edition License,per CPU,1 Year SA&S Bundled	PERMANENT

Obtaining the ESN

- Choose System > Administration > License Management from the main menu.





Expiration Date	ESN Details	License Revocation Code
2017-05-07	View	

Resource Name	Capacity Used
IVS Manager Devices	0/50
Managed NEs	1/60
Managed Security Policy NEs	0/20
Managed WLAN Wireless Location AP	0/10

The drop-down list provides one or more MAC addresses of the network card on the current server. You can select any if there are multiple MAC addresses.

Select MAC address: 28-6E-D4-88-C6-43

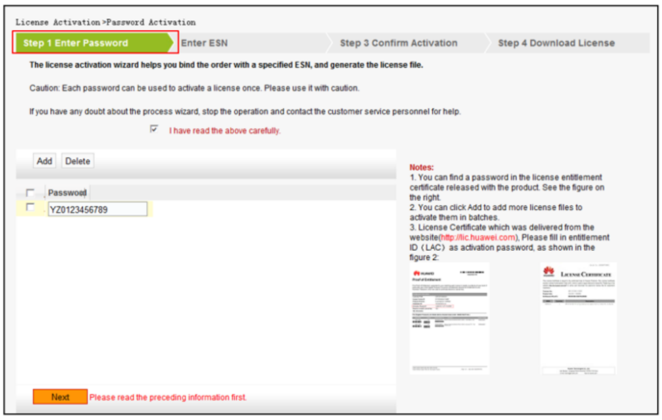
MjgtNkUtRDQtODgtQzYtNDM=

Enter a MAC address:

- After the license is successfully loaded, log in to the eSight system as the administrator. Choose System > Administration > License Management to view license expiration date, and check whether the function items and resource items are correct based on the applied license.
- eSight uses the character string generated through encrypted conversion of the MAC address as the ESN.

Activating the License (1)

- Choose License Activation > Password Activation from the main menu and enter the activation code.



The license activation wizard helps you bind the order with a specified ESN, and generate the license file.

Caution: Each password can be used to activate a license once. Please use it with caution.

If you have any doubt about the process wizard, stop the operation and contact the customer service personnel for help.

☑ I have read the above carefully.

□ Passwoed

□ YZ0123456789

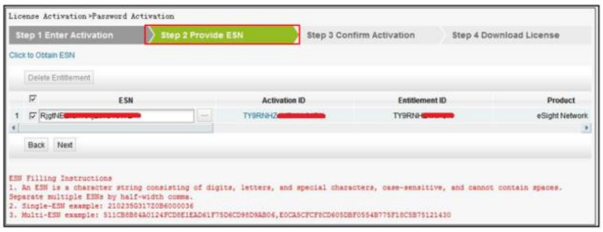
Please read the preceding information first.

Notes:
1. You can find a password in the license entitlement certificate released with the product. See the figure on the right.
2. You can click Add to add more license files to activate them in batches.
3. License Certificate which was delivered from the website(http://lic.huawei.com), Please fill in entitlement ID（LAC）as activation password, as shown in the figure 2:

Installation Preparations
Start Installation
System Login
Software Registration

Activating the License (2)

- Enter the ESN of the server to be bound.


License Activation >Password Activation

Step 1 Enter Activation | Step 2 Provide ESN | Step 3 Confirm Activation | Step 4 Download License

Click to Obtain ESN

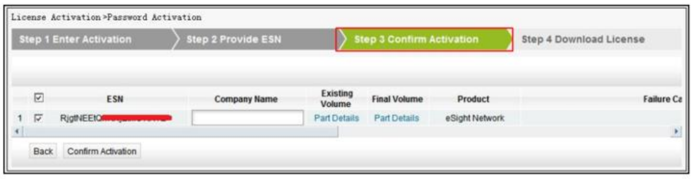
Delete Entitlement

	☑	ESN	Activation ID	Entitlement ID	Product
1	☑	RjgtNE[redacted]	TY9RNHZ[redacted]	TY9RNH[redacted]	eSight Network

Back   Next

ESN Filling Instructions
1. An ESN is a character string consisting of digits, letters, and special characters, case-sensitive, and cannot contain spaces. Separate multiple ESNs by half-width comma.
2. Single-ESN example: 210235G317Z0B6000036
3. Multi-ESN example: 511CB8B84A0124FCD8E1EAD61F75D6CD98D9AB06,E0CA5CFCF8CD605DBF0554B775F18C5B75121430

- Confirm the activation and download the license file.


License Activation >Password Activation

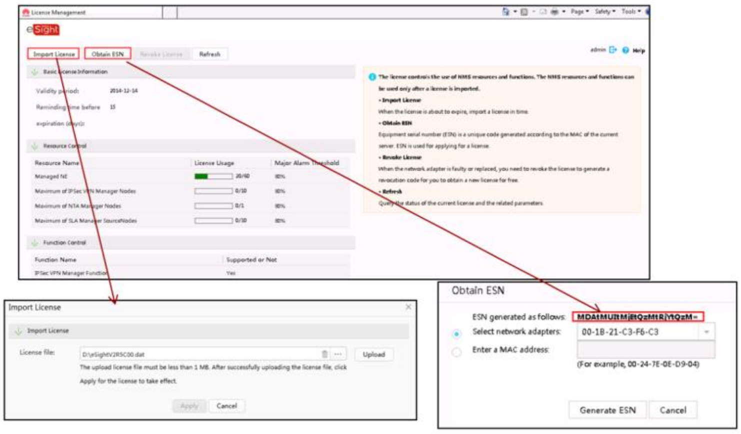
Step 1 Enter Activation | Step 2 Provide ESN | Step 3 Confirm Activation | Step 4 Download License

	☑	ESN	Company Name	Existing Volume	Final Volume	Product	Failure Ca
1	☑	RjgtNEEtQ[redacted]		Part Details	Part Details	eSight Network	

Back   Confirm Activation

Loading and Managing the License

- Choose System > Administration > License Management from the main menu.



Validity period: 2014-12-14

Reminding time before expiration (days): 15

Resource Name	License Usage	Major Alarm Threshold
Managed NE	20/50	80%
Maximum of IPSec VPN Manager Nodes	0/10	80%
Maximum of NTA Manager Nodes	0/1	80%
Maximum of SLA Manager SourceNodes	0/10	80%

Function Name	Supported or Not
IPSec VPN Manager Function	Yes

The license controls the use of NMS resources and functions. The NMS resources and functions can be used only after a license is imported.

- Import License

When the license is about to expire, import a license in time.

- Obtain ESN

Equipment serial number (ESN) is a unique code generated according to the MAC of the current server. ESN is used for applying for a license.

- Revoke License

When the network adapter is faulty or replaced, you need to revoke the license to generate a revocation code for you to obtain a new license for free.

- Refresh

Query the status of the current license and the related parameters.

Import License

License file: D:\eSightV2R5C00.dat

The upload license file must be less than 1 MB. After successfully uploading the license file, click Apply for the license to take effect.

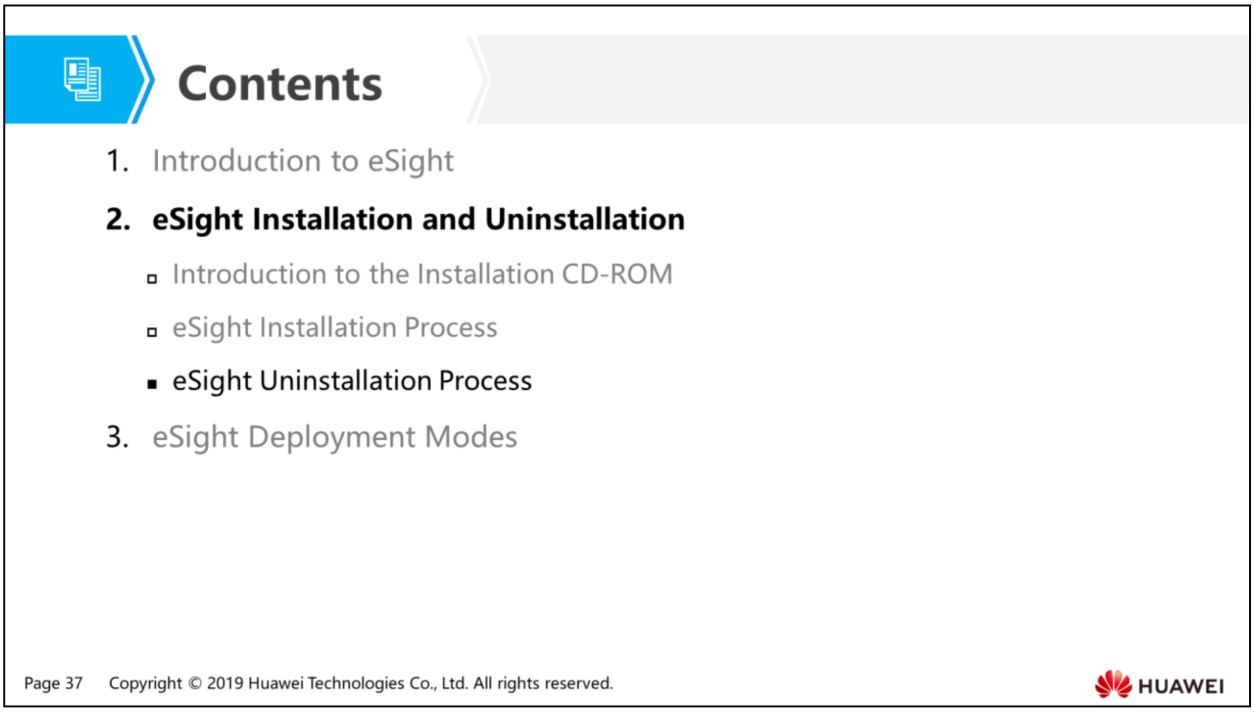
Obtain ESN

ESN generated as follows: MDAtMUItMjEtQzMtRjYtQzM=

● Select network adapters: 00-1B-21-C3-F6-C3

○ Enter a MAC address:

(For example, 00-24-7E-0E-D9-04)

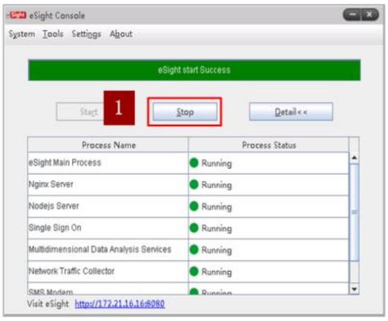


Contents

1. Introduction to eSight
2. **eSight Installation and Uninstallation**
   - Introduction to the Installation CD-ROM
   - eSight Installation Process
   - eSight Uninstallation Process
3. eSight Deployment Modes

Uninstalling eSight

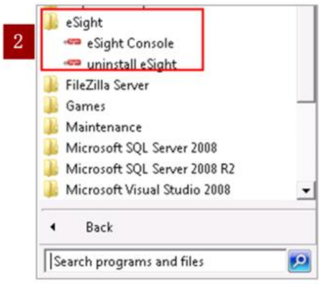
- To stop the eSight service, choose Start > All Programs > eSight > eSight Console and click Stop in the dialog box that is displayed.
- To uninstall eSight, choose Start > All Programs > eSight > Uninstall eSight.



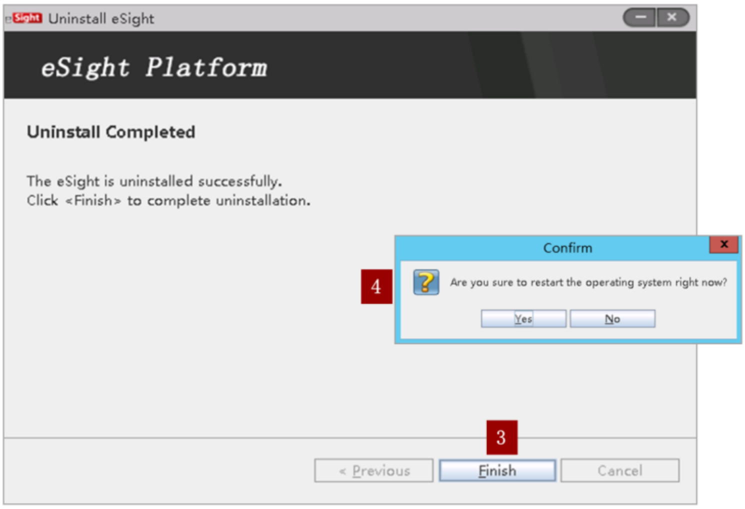
eSight start Success

Process Name	Process Status
eSight Main Process	● Running
Nginx Server	● Running
Nodejs Server	● Running
Single Sign On	● Running
Multidimensional Data Analysis Services	● Running
Network Traffic Collector	● Running
SMS Modem	● Running

Visit eSight http://172.21.16.16:8080


2
eSight
eSight Console
uninstall eSight
FileZilla Server
Games
Maintenance
Microsoft SQL Server 2008
Microsoft SQL Server 2008 R2
Microsoft Visual Studio 2008
Back
Search programs and files

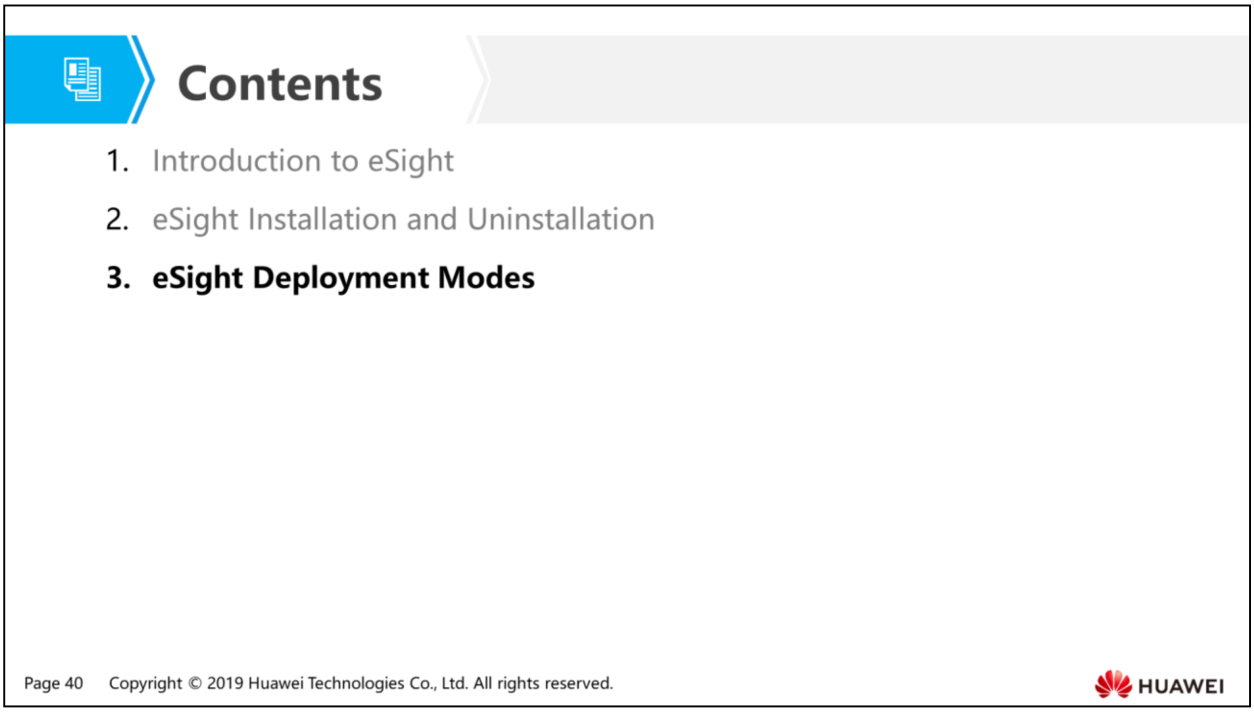
Uninstallation Completed



Uninstall Completed

The eSight is uninstalled successfully.
Click <Finish> to complete uninstallation.

4 Are you sure to restart the operating system right now?

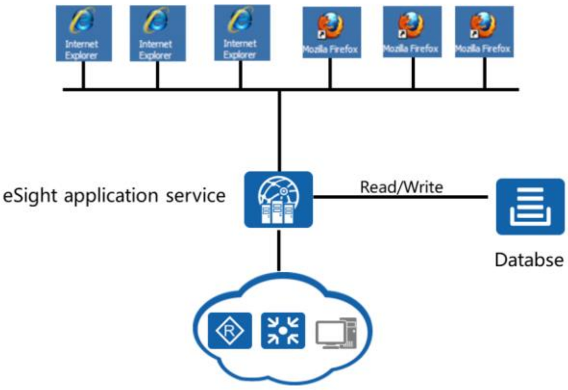


Contents

1. Introduction to eSight
2. eSight Installation and Uninstallation
3. **eSight Deployment Modes**

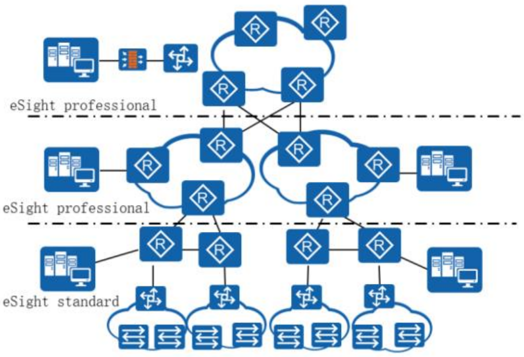
Single-Node Server Mode

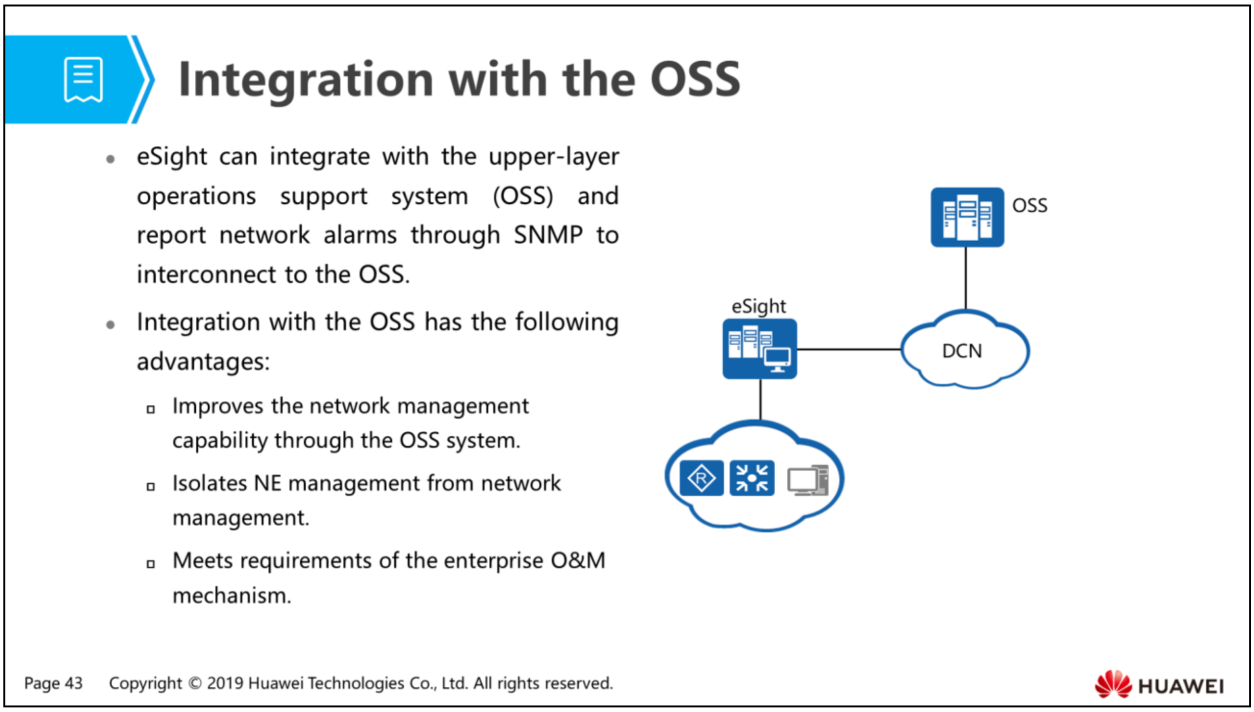
- eSight AppBase works in browser/server mode and allows simultaneous access by multiple Web browsers.



Hierarchical Deployment Mode

- eSight also supports hierarchical management to allow an enterprise headquarters to monitor networks in branches.
- In the hierarchical deployment mode, the upper-layer NMS can add lower-layer NMSs to the system and provide links to lower-layer NMSs. When you click such a link, a new browser window is displayed, where you can log in to a lower-layer NMS.





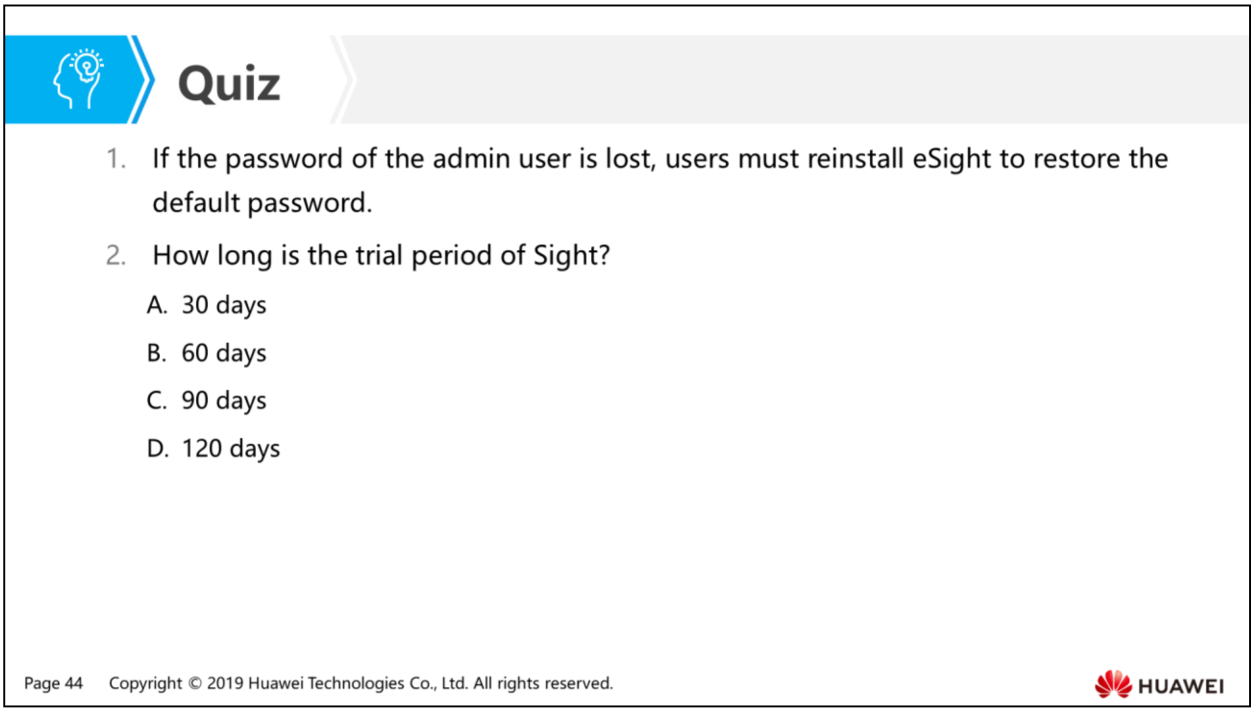
Integration with the OSS

- eSight can integrate with the upper-layer operations support system (OSS) and report network alarms through SNMP to interconnect to the OSS.
- Integration with the OSS has the following advantages:
  - Improves the network management capability through the OSS system.
  - Isolates NE management from network management.
  - Meets requirements of the enterprise O&M mechanism.

Page 43

HUAWEI

- The OSS is network management software running on the network management workstation. Network administrators operate the OSS to send requests to managed devices, so that they can monitor and configure these devices.



Quiz

1. If the password of the admin user is lost, users must reinstall eSight to restore the default password.
2. How long is the trial period of Sight?

   A. 30 days

   B. 60 days

   C. 90 days

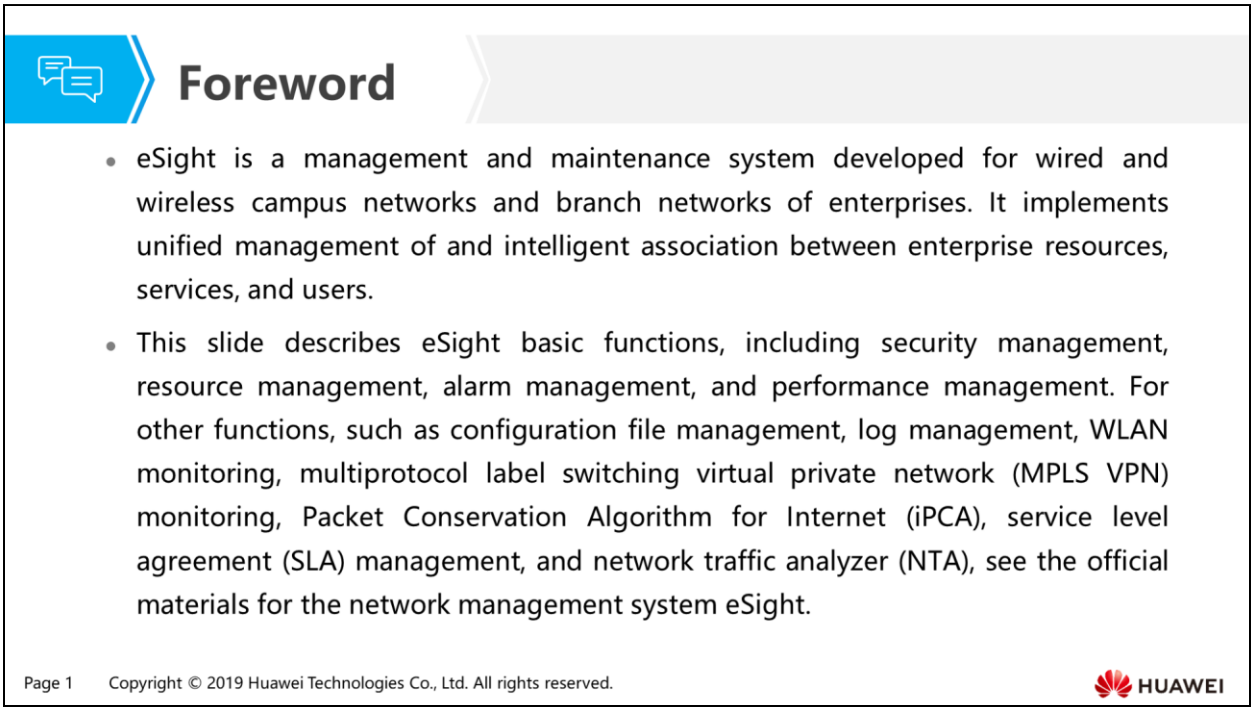
   D. 120 days

- Answer: True.
- Answer: C.

Thank You

www.huawei.com

eSight Basic Functions



Foreword

- eSight is a management and maintenance system developed for wired and wireless campus networks and branch networks of enterprises. It implements unified management of and intelligent association between enterprise resources, services, and users.
- This slide describes eSight basic functions, including security management, resource management, alarm management, and performance management. For other functions, such as configuration file management, log management, WLAN monitoring, multiprotocol label switching virtual private network (MPLS VPN) monitoring, Packet Conservation Algorithm for Internet (iPCA), service level agreement (SLA) management, and network traffic analyzer (NTA), see the official materials for the network management system eSight.

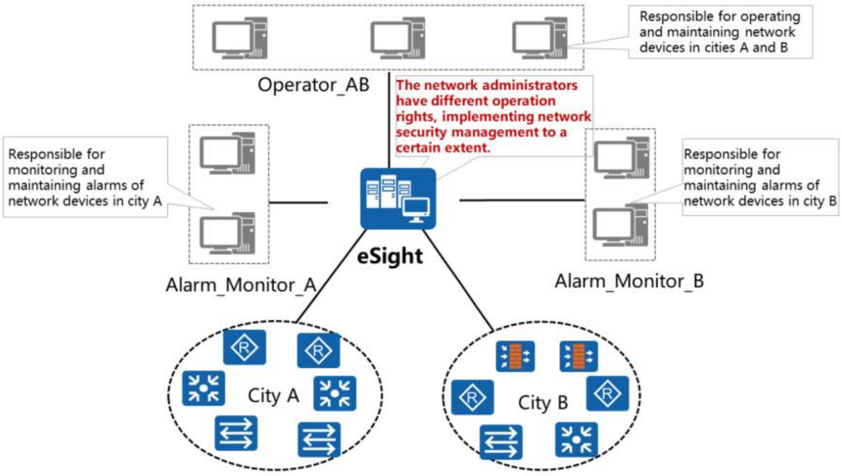
Objectives

- Upon completion of this section, you will be able to:
  - Be familiar with eSight basic functions
  - Master operations of eSight basic functions

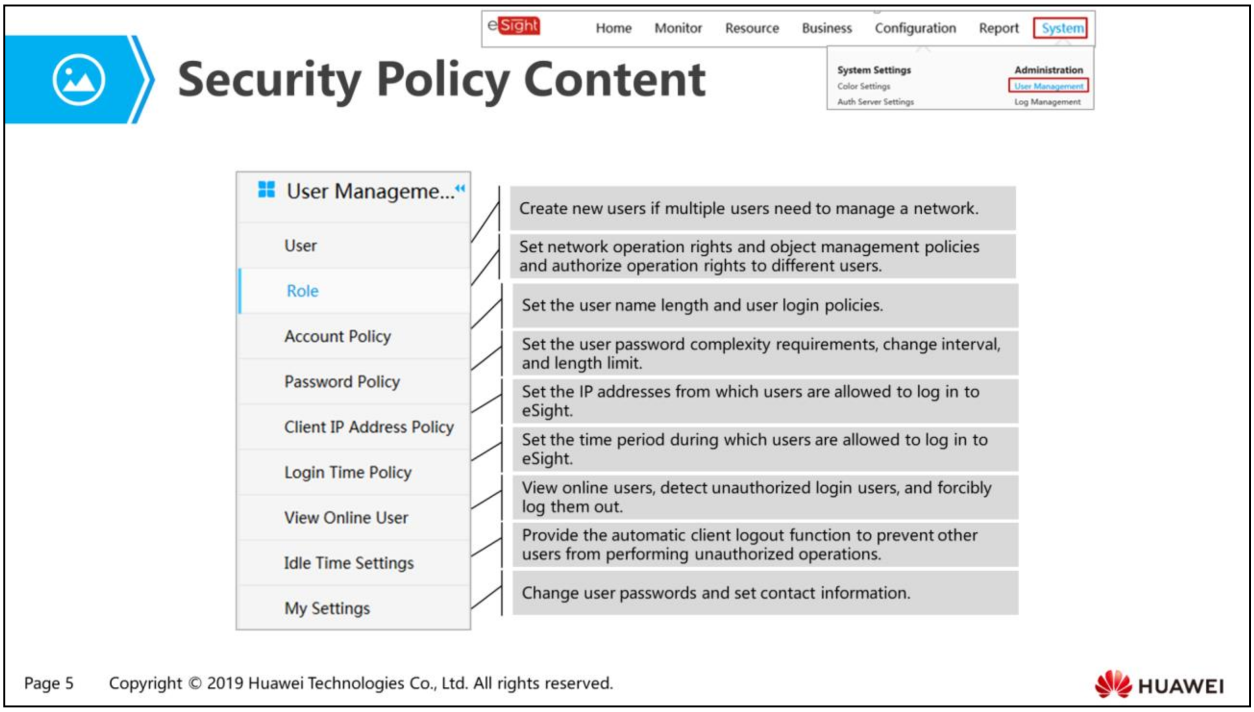
Contents

1. **Security Management**
2. Resource Management
3. Alarm Management
4. Performance Management

How Can Network Security Management Be Implemented?



Responsible for operating and maintaining network devices in cities A and B
Operator_AB
The network administrators have different operation rights, implementing network security management to a certain extent.
Responsible for monitoring and maintaining alarms of network devices in city A
Responsible for monitoring and maintaining alarms of network devices in city B
eSight
Alarm_Monitor_A
Alarm_Monitor_B
City A
City B



Security Policy Content

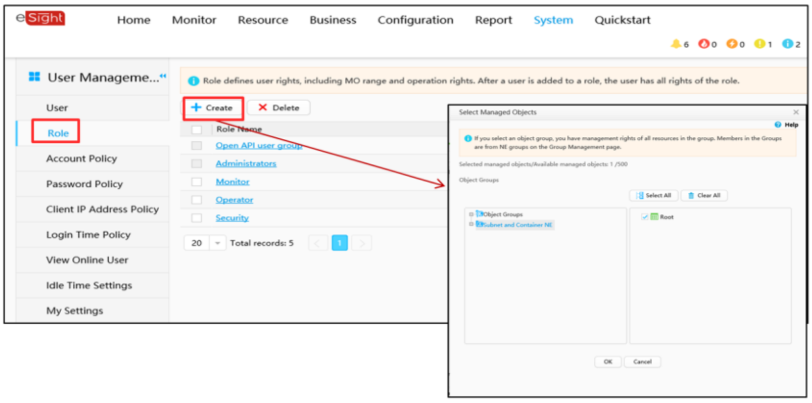
User Manageme...	
User	Create new users if multiple users need to manage a network.
Role	Set network operation rights and object management policies and authorize operation rights to different users.
Account Policy	Set the user name length and user login policies.
Password Policy	Set the user password complexity requirements, change interval, and length limit.
Client IP Address Policy	Set the IP addresses from which users are allowed to log in to eSight.
Login Time Policy	Set the time period during which users are allowed to log in to eSight.
View Online User	View online users, detect unauthorized login users, and forcibly log them out.
Idle Time Settings	Provide the automatic client logout function to prevent other users from performing unauthorized operations.
My Settings	Change user passwords and set contact information.

- Add users and roles: You can create users and assign operation rights to users. After eSight assigns operation rights and managed objects to a role and specify a role for a user, the user has operation rights of the role.
- Account policy: You can set the minimum account length, account disabling policy (number of days during which an account is not used), account lockout policy (account locking conditions, specified time period, number of consecutive login failures in the period, specified lock duration) to avoid risks brought by improper account settings.
- Password policy: You can set the minimum password length, password repetition not allowed (number of times), and password validity period to prevent thefts of simple passwords.
- Client IP address policy: You can set the IP address range from which users are allowed to log in to eSight.
  - After an access control policy is set, the online users will be automatically logged out if they log in beyond the allowed time period or from IP addresses outside the specified IP address range.
  - Login time policy: You can set a login time policy by specifying the start and end dates, daily start and end time, or weekday.
    - eSight does not support login time control for the default user admin who needs to log in to eSight at any time.

- View online user: You can view the current online users as well as related information, such as their login time, login IP addresses, and roles. In addition, you can perform the following operations:
  - Refresh online user information: Update online user information to the latest.
  - Forcibly log out users: Prevent unauthorized operations on the eSight client.
  - Enter the SSO mode: Only one user is allowed to log in to eSight each time. Other users will be forced to log out.
  - Exit the SSO mode: After completing maintenance operations in SSO mode, you need to exit the SSO mode.
- Idle time settings: If a user does not perform any operations within a specified period of time, the client is automatically logged out.
- My setting: You can Change user passwords and set contact information if you need.

Create a Role (1)

- Assign an administrative domain to a role, so that the role can manage specified objects in the domain.



Role defines user rights, including MO range and operation rights. After a user is added to a role, the user has all rights of the role.

Role Name
Open API user group
Administrators
Monitor
Operator
Security

20 Total records: 5 1

Select Managed Objects

If you select an object group, you have management rights of all resources in the group. Members in the Groups are from NE groups on the Group Management page.

Selected managed objects/Available managed objects: 1 /500

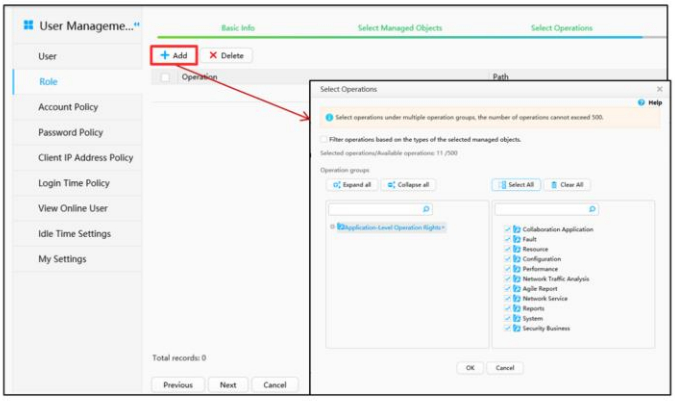
Object Groups

- Object Groups
- Subnet and Container NE

☑ Root

Create a Role (2)

- Assign management rights to a role, so that the role can have operation rights for managed objects.



Select operations under multiple operation groups, the number of operations cannot exceed 500.

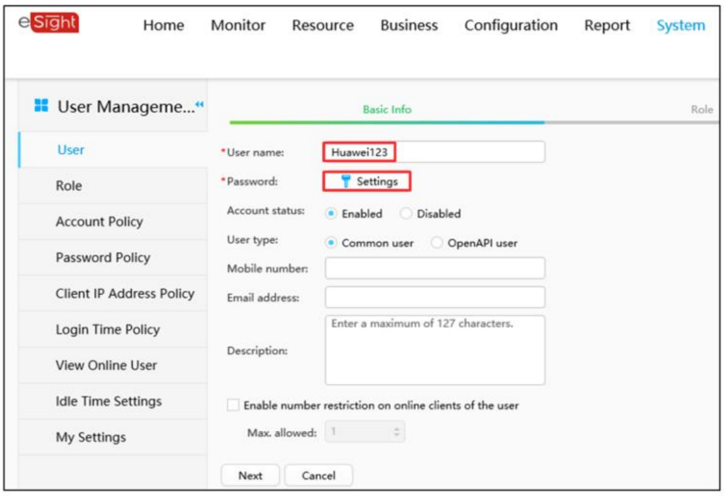
□ Filter operations based on the types of the selected managed objects.

Selected operations/Available operations: 11 /500

Operation groups

- ✓ Collaboration Application
- ✓ Fault
- ✓ Resource
- ✓ Configuration
- ✓ Performance
- ✓ Network Traffic Analysis
- ✓ Agile Report
- ✓ Network Service
- ✓ Reports
- ✓ System
- ✓ Security Business

Create Users - Set the User Name and Password



*User name: Huawei123

*Password: Settings

Account status: ● Enabled ○ Disabled

User type: ● Common user ○ OpenAPI user

Mobile number:

Email address:

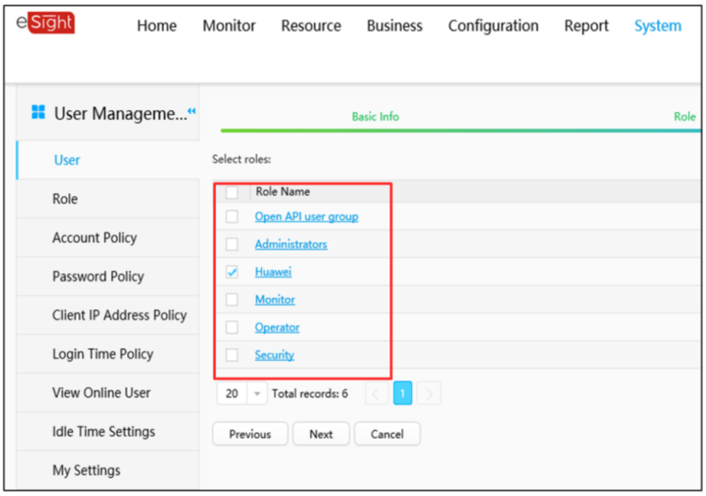
Description: Enter a maximum of 127 characters.

□ Enable number restriction on online clients of the user

Max. allowed: 1

Next Cancel

Create Users - Set a Role

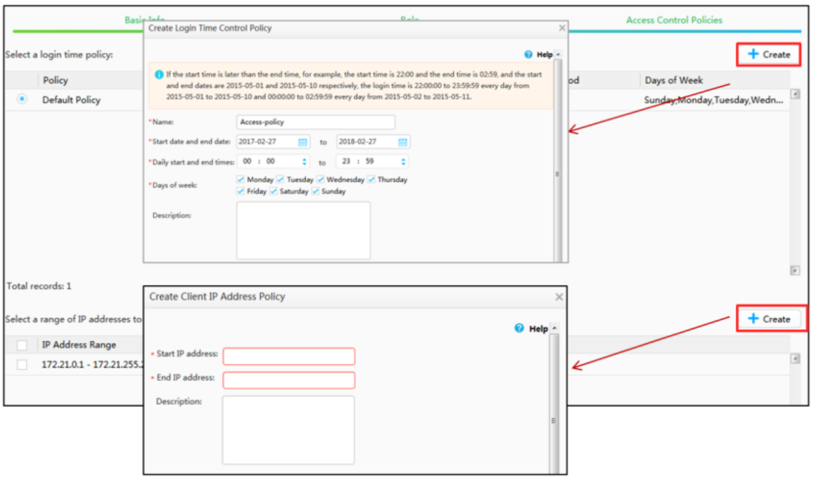


Select roles:

□	Role Name
□	Open API user group
□	Administrators
☑	Huawei
□	Monitor
□	Operator
□	Security

20 Total records: 6 1

Create Users - Configure Access Control Policies



Select a login time policy:

	Policy	...od	Days of Week
●	Default Policy		Sunday,Monday,Tuesday,Wedn...

Total records: 1

Select a range of IP addresses to...

□	IP Address Range
□	172.21.0.1 - 172.21.255.2...

Create Login Time Control Policy

If the start time is later than the end time, for example, the start time is 22:00 and the end time is 02:59, and the start and end dates are 2015-05-01 and 2015-05-10 respectively, the login time is 22:00:00 to 23:59:59 every day from 2015-05-01 to 2015-05-10 and 00:00:00 to 02:59:59 every day from 2015-05-02 to 2015-05-11.

*Name: Access-policy

*Start date and end date: 2017-02-27 to 2018-02-27

*Daily start and end times: 00 : 00 to 23 : 59

*Days of week: ✓ Monday ✓ Tuesday ✓ Wednesday ✓ Thursday ✓ Friday ✓ Saturday ✓ Sunday

Description:

Create Client IP Address Policy

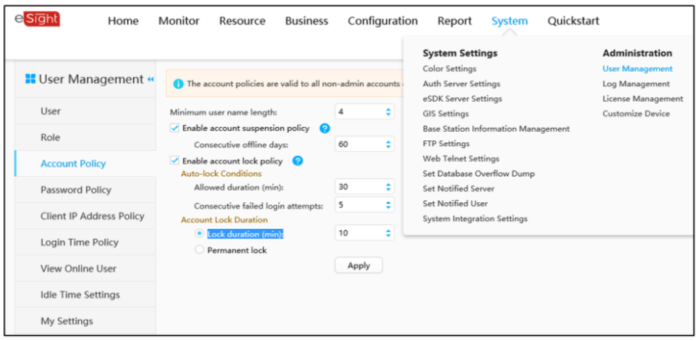
• Start IP address:

• End IP address:

Description:

Configure Account PoliciesConfigure Account Policies

- Proper user name length limits and user login policies can improve eSight access security. An account policy applies to all users. Therefore, it must be set by the security administrator.



The account policies are valid to all non-admin accounts

Minimum user name length: 4

☑ Enable account suspension policy

Consecutive offline days: 60

☑ Enable account lock policy

Auto-lock Conditions

Allowed duration (min): 30

Consecutive failed login attempts: 5

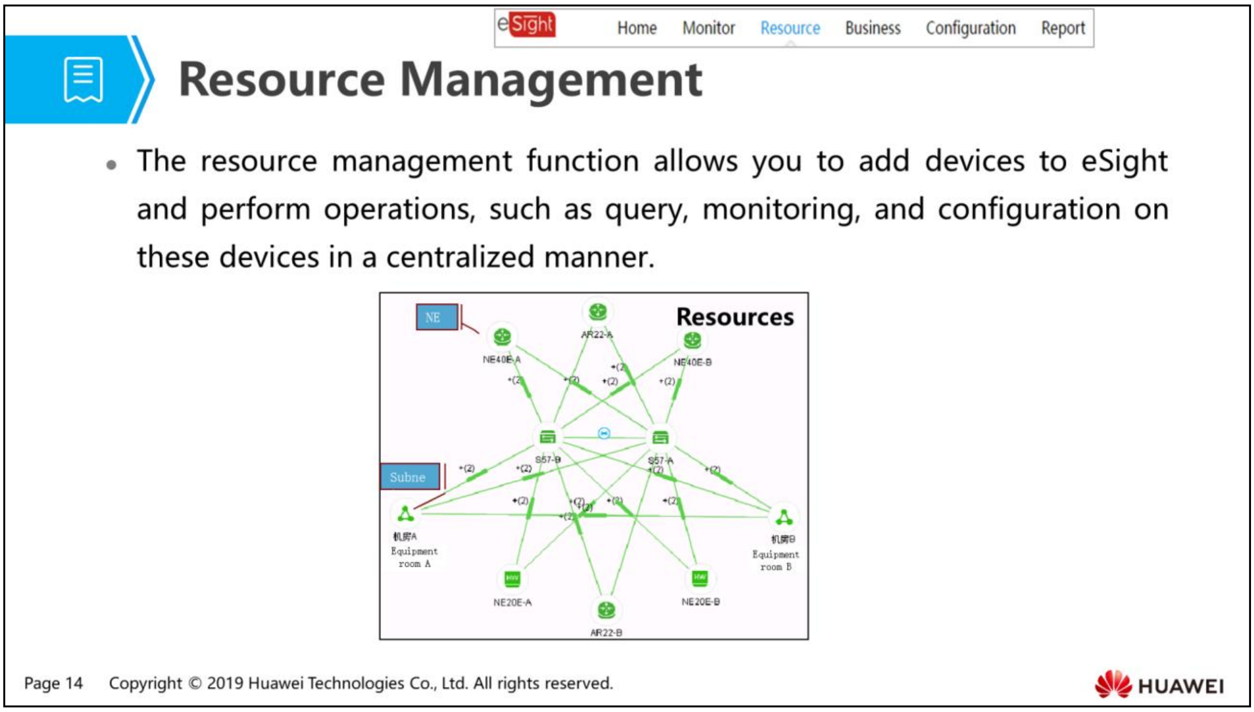
Account Lock Duration

● Lock duration (min): 10

○ Permanent lock

Contents

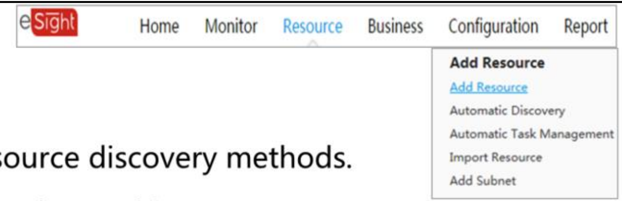
1. Security Management
2. **Resource Management**
3. Alarm Management
4. Performance Management



Resource Management

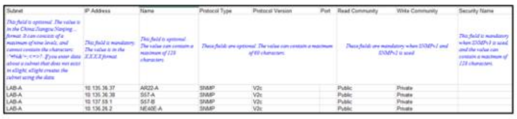
- The resource management function allows you to add devices to eSight and perform operations, such as query, monitoring, and configuration on these devices in a centralized manner.

- Resource: refers to managed objects of eSight, such as devices and subnets.
- NE (network element): is short for network element, including hardware devices and software running on them.
- Subnet: refers to a smaller network divided from a large network based on specific rules (such as region) to simplify network management.
  - Network resources that can be managed on a subnet include subnets, devices, and links.
  - Subnets can be nested to one another.

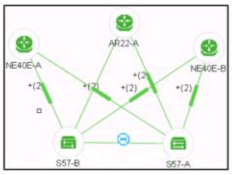


Add Devices

- eSight supports three resource discovery methods.
  - Method 1: Single Addition (by IP Address)
    - 10.135.59.18
  - Method 2: Automatic Discovery (by IP Address Segment)
    - 10.137.61.1 to 10.137.61.255
  - Method 3: Device Import (Using an Excel File)



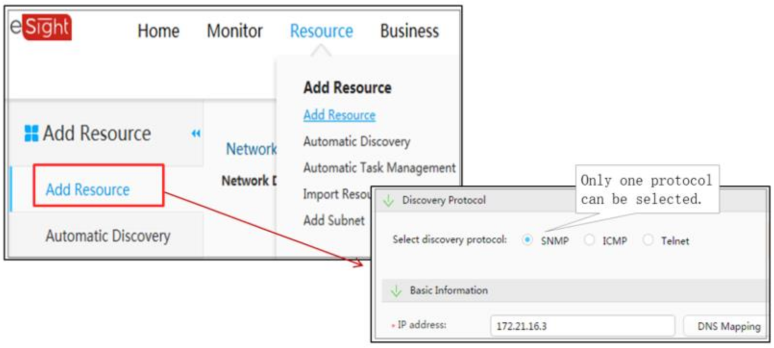
Subnet	IP Address	Name	Protocol Type	Protocol Version	Port	Read Community	Write Community	Security Name
This field is optional. The value is in the China/Jiangsu/Nanjing... format. It can consist of a maximum of nine levels, and cannot contain the characters: :"#/|<>;:<=>?. If you enter data about a subnet that does not exist in eSight, eSight creates the subnet using the data.*	*This field is mandatory. The value is in the X.X.X.X format.*	*This field is optional. The value can contain a maximum of 128 characters.*	*These fields are optional. The value can contain a maximum of 60 characters.*			*These fields are mandatory when SNMPv1 and SNMPv2 is used.*		*This field is mandatory when SNMPv3 is used and the value can contain a maximum of 128 characters.*
LAB-A	10.135.36.37	AR22-A	SNMP	V2c		Public	Private	
LAB-A	10.135.36.38	S57-A	SNMP	V2c		Public	Private	
LAB-A	10.137.59.1	S57-B	SNMP	V2c		Public	Private	
LAB-A	10.136.26.2	NE40E-A	SNMP	V2c		Public	Private	



- View the topology after device addition.
  - Choose Monitor > Topology Management

- Manually create a single NE: When only a small number of NEs of different types need to be added to eSight, you can add them one by one.

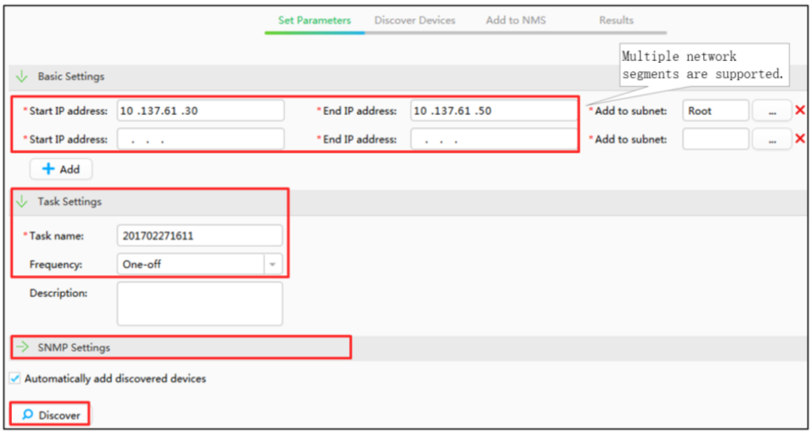
Single Addition



Only one protocol can be selected.

- SNMP: Network devices must support SNMP and have SNMP access parameters configured.
- ICMP: If network devices do not have SNMP parameters configured but can ping the eSight server, they can be added to eSight through ICMP.

Automatic Discovery



Multiple network segments are supported.

*Start IP address: 10 .137.61 .30 *End IP address: 10 .137.61 .50 *Add to subnet: Root

*Start IP address: . . . *End IP address: . . . *Add to subnet:

*Task name: 201702271611

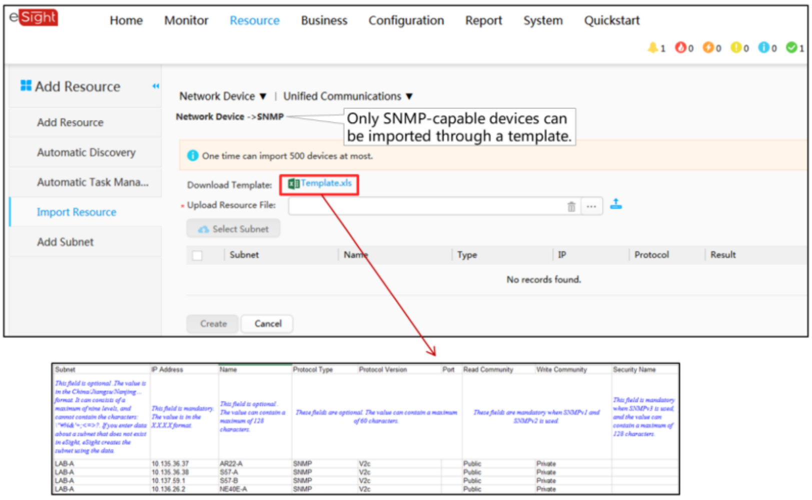
Frequency: One-off

Description:

☑ Automatically add discovered devices

- Automatically add discovered devices: If this option is selected, discovered devices will be added to eSight automatically. If this option is deselected, you need to manually add discovered devices.

Device Import



Only SNMP-capable devices can be imported through a template.

One time can import 500 devices at most.

Download Template: Template.xls

* Upload Resource File:

□	Subnet	Name	Type	IP	Protocol	Result

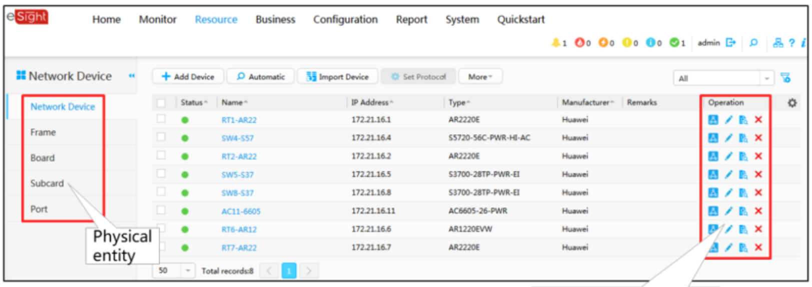
No records found.

Subnet	IP Address	Name	Protocol Type	Protocol Version	Port	Read Community	Write Community	Security Name
This field is optional . The value is in the China/Jiangsu/Nanjing... format. It can consists of a maximum of nine levels, and cannot contain the characters: \"#%&'+;<=>?. If you enter data about a subnet that does not exist in eSight, eSight creates the subnet using the data.	*This field is mandatory. The value is in the X.X.X.X format.*	*This field is optional . The value can contain a maximum of 128 characters.*	*These fields are optional. The value can contain a maximum of 60 characters.*			*These fields are mandatory when SNMPv1 and SNMPv2 is used.*		*This field is mandatory when SNMPv3 is used, and the value can contain a maximum of 128 characters.*
LAB-A	10.135.36.37	AR22-A	SNMP	V2c		Public	Private	
LAB-A	10.135.36.38	S57-A	SNMP	V2c		Public	Private	
LAB-A	10.137.59.1	S57-B	SNMP	V2c		Public	Private	
LAB-A	10.136.26.2	NE40E-A	SNMP	V2c		Public	Private	

- Pay attention to the following points during device import:
  - Use a built-in template of eSight. When entering data in this template, do not modify the template structure. Otherwise, devices cannot be imported.
  - A maximum of 500 device records can be imported each time.

Physical Resource Management

- Physical resources include devices and physical entities of devices, such as the chassis, card, subcard, and port.



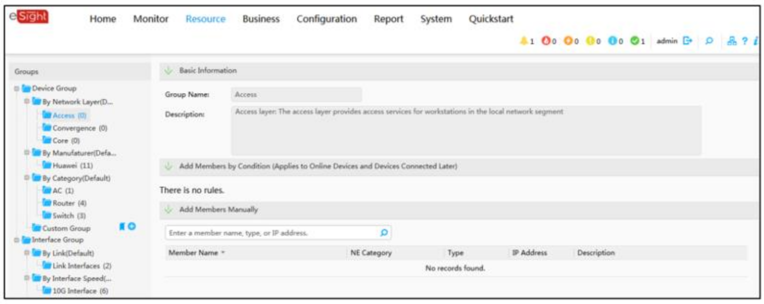
□	Status	Name	IP Address	Type	Manufacturer	Remarks	Operation
□	●	RT1-AR22	172.21.16.1	AR2220E	Huawei		
□	●	SW4-S57	172.21.16.4	S5720-56C-PWR-HI-AC	Huawei		
□	●	RT2-AR22	172.21.16.2	AR2220E	Huawei		
□	●	SW5-S37	172.21.16.5	S3700-28TP-PWR-EI	Huawei		
□	●	SW8-S37	172.21.16.8	S3700-28TP-PWR-EI	Huawei		
□	●	AC11-6605	172.21.16.11	AC6605-26-PWR	Huawei		
□	●	RT6-AR12	172.21.16.6	AR1220EVW	Huawei		
□	●	RT7-AR22	172.21.16.7	AR2220E	Huawei		

Physical entity

1. Switch to topology
2. Modify remarks
3. View resource details
4. Delete

Group Management

- You can create a group and add NEs in different subnets to the group, which is considered as one object. You can assign the object (a group of NEs) to a user, which improves the batch device management efficiency.



Basic Information

Group Name: Access

Description: Access layer: The access layer provides access services for workstations in the local network segment

Add Members by Condition (Applies to Online Devices and Devices Connected Later)

There is no rules.

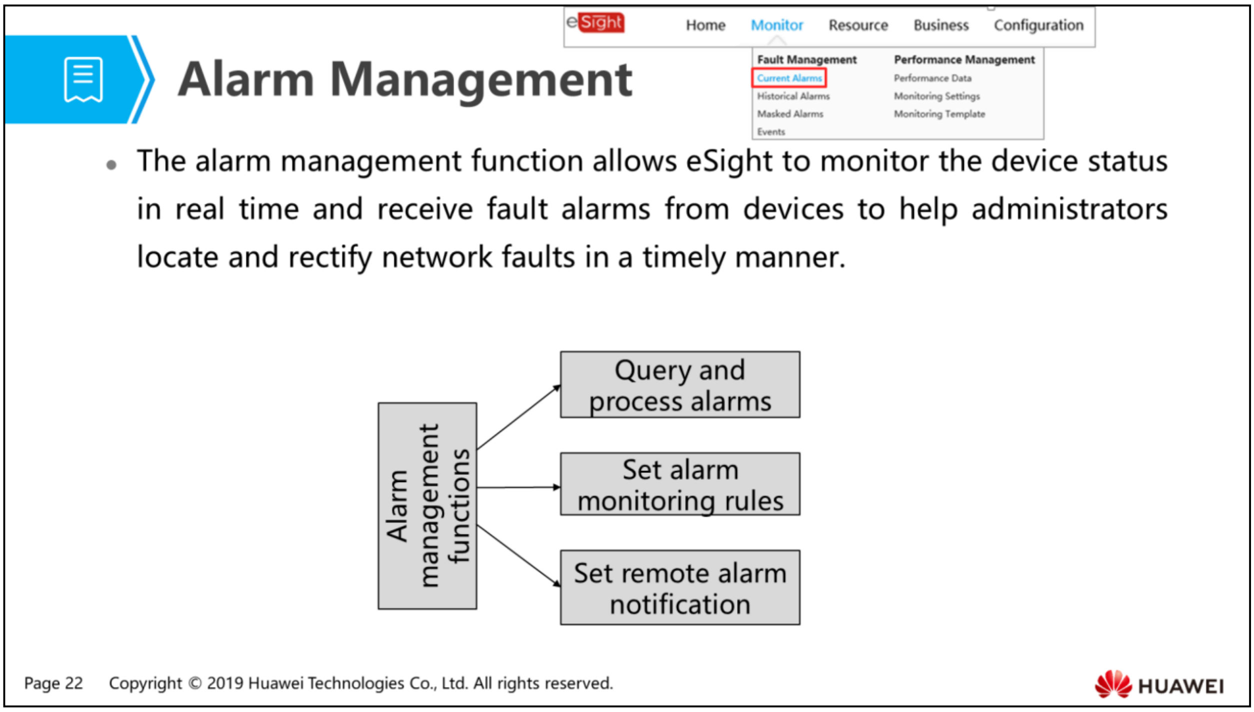
Add Members Manually

Enter a member name, type, or IP address.

Member Name	NE Category	Type	IP Address	Description
No records found.				

Contents

1. Security Management
2. Resource Management
3. **Alarm Management**
4. Performance Management



Alarm Management

- The alarm management function allows eSight to monitor the device status in real time and receive fault alarms from devices to help administrators locate and rectify network faults in a timely manner.

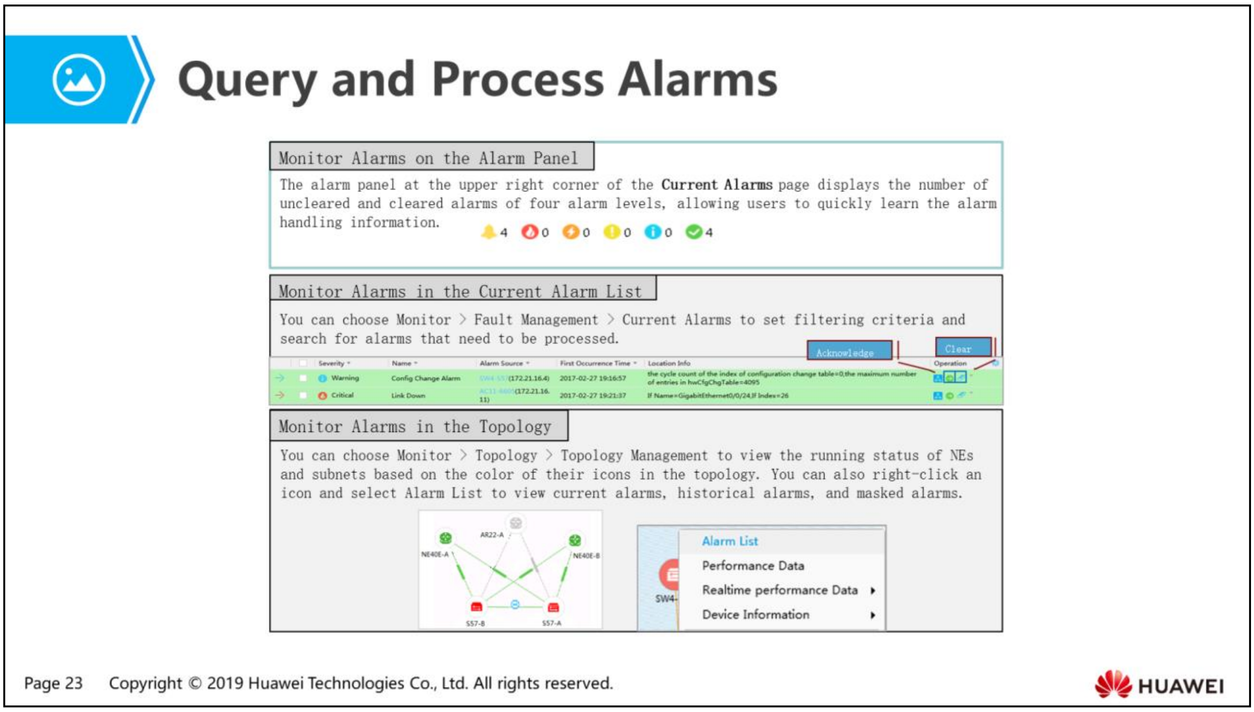
Alarm management functions

Query and process alarms

Set alarm monitoring rules

Set remote alarm notification

- The alarm management function helps network maintenance personnel quickly and accurately to monitor and process alarms, thereby increasing the O&M efficiency.
- Based on the locations where alarms are generated, alarms are classified into NE alarms and NMS alarms.
  - NE alarms are generated when NEs become faulty.
  - NMS alarms are generated when connections between the NMS and NEs are interrupted or the NMS itself becomes faulty.



Query and Process Alarms

Monitor Alarms on the Alarm Panel

The alarm panel at the upper right corner of the **Current Alarms** page displays the number of uncleared and cleared alarms of four alarm levels, allowing users to quickly learn the alarm handling information.

Monitor Alarms in the Current Alarm List

You can choose Monitor > Fault Management > Current Alarms to set filtering criteria and search for alarms that need to be processed.

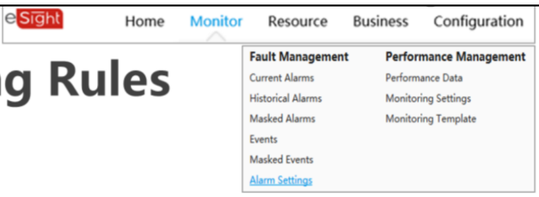
	Severity	Name	Alarm Source	First Occurrence Time	Location Info	Operation
□	Warning	Config Change Alarm	SW4-S57(172.21.16.4)	2017-02-27 19:16:57	the cycle count of the index of configuration change table=0,the maximum number of entries in hwCfgChgTable=4095	
□	Critical	Link Down	AC11-6605(172.21.16.11)	2017-02-27 19:21:37	If Name=GigabitEthernet0/0/24,If Index=26	

Monitor Alarms in the Topology

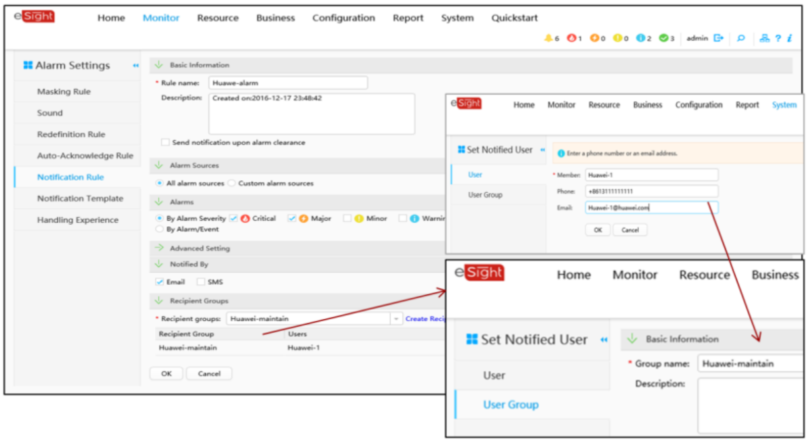
You can choose Monitor > Topology > Topology Management to view the running status of NEs and subnets based on the color of their icons in the topology. You can also right-click an icon and select Alarm List to view current alarms, historical alarms, and masked alarms.

- Monitor Alarms on the Alarm Panel:
    - Alarm severity identifies how serious an alarm is. Alarms can be classified into four severities in descending order: critical, major, minor, and warning.
- Monitor Alarms in the Current Alarm List:
    - The white background color indicates that the alarm is not cleared. The green background color indicates that the alarm has been cleared. As shown in the preceding figure, the background color of the "Link Down" alarm is green. It indicates that the alarm has been cleared.
    - Clear alarm: On eSight, you can manually clear the alarms that cannot be automatically cleared or have been recovered.
    - Acknowledge alarm: You can acknowledge an alarm to indicate that the alarm has been processed. You can unacknowledge an acknowledged alarm and take measures accordingly.

Set Alarm Monitoring Rules



- Create remote notification rules.



Basic Information

* Rule name: Huawe-alarm

Description: Created on:2016-12-17 23:48:42

□ Send notification upon alarm clearance

Alarm Sources

● All alarm sources ○ Custom alarm sources

Alarms

● By Alarm Severity ☑ Critical ☑ Major □ Minor □ Warnir

○ By Alarm/Event

Advanced Setting

Notified By

☑ Email □ SMS

Recipient Groups

* Recipient groups: Huawei-maintain

Recipient Group	Users
Huawei-maintain	Huawei-1

OK Cancel

Enter a phone number or an email address.

* Member: Huawei-1

Phone: +8613111111111

Email: Huawei-1@huawei.com

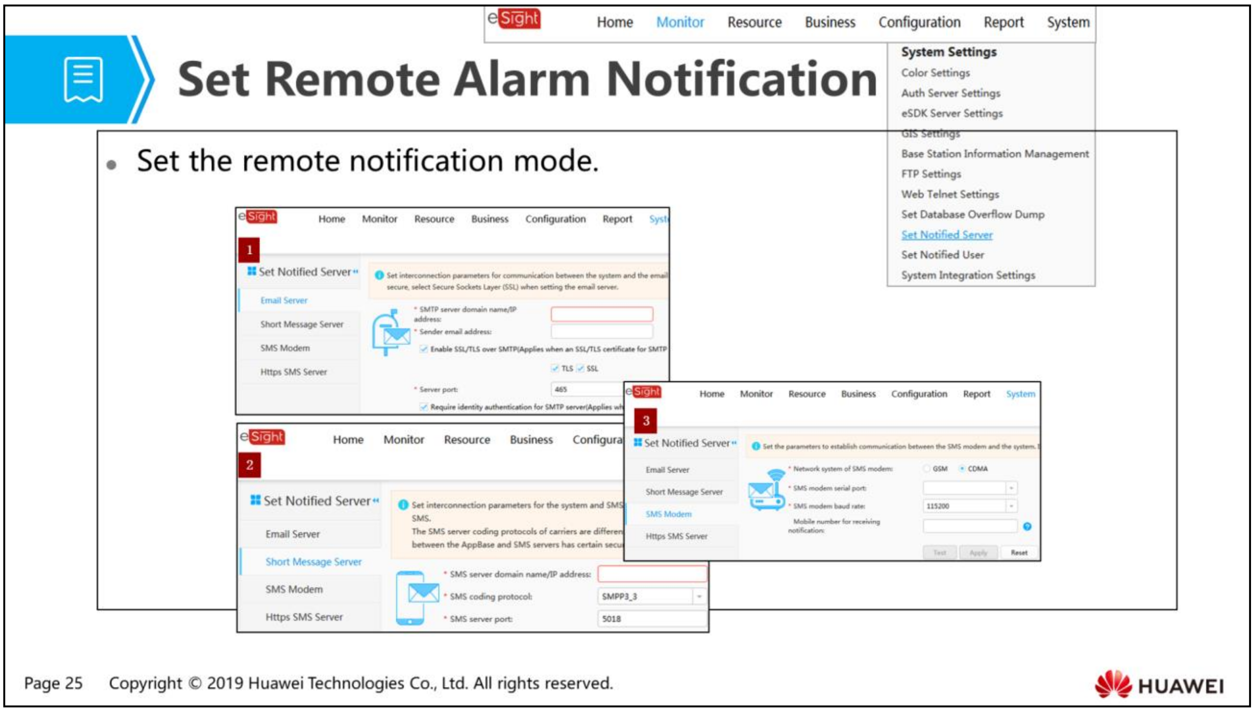
OK Cancel

Basic Information

* Group name: Huawei-maintain

Description:

- Remote notification rules: You can set the alarm source, alarm severity, detailed event, and notified users to send alarm notifications selectively.
- Remote alarm notification: When alarms meeting specified conditions are generated, eSight notifies the maintenance personnel through emails or SMS messages so that the maintenance personnel can learn alarms in a timely manner and take measures.



Set Remote Alarm Notification

- Set the remote notification mode.

1

Set Notified Server

Set interconnection parameters for communication between the system and the email
secure, select Secure Sockets Layer (SSL) when setting the email server.

* SMTP server domain name/IP address:

* Sender email address:

☑ Enable SSL/TLS over SMTP(Applies when an SSL/TLS certificate for SMTP

☑ TLS ☑ SSL

* Server port: 465

☑ Require identity authentication for SMTP server(Applies wh

2

Set Notified Server

Set interconnection parameters for the system and SMS
SMS.
The SMS server coding protocols of carriers are differen
between the AppBase and SMS servers has certain secu

* SMS server domain name/IP address:

* SMS coding protocol: SMPP3_3

* SMS server port: 5018

3

Set Notified Server

Set the parameters to establish communication between the SMS modem and the system. I

* Network system of SMS modem: ○ GSM ● CDMA

* SMS modem serial port:

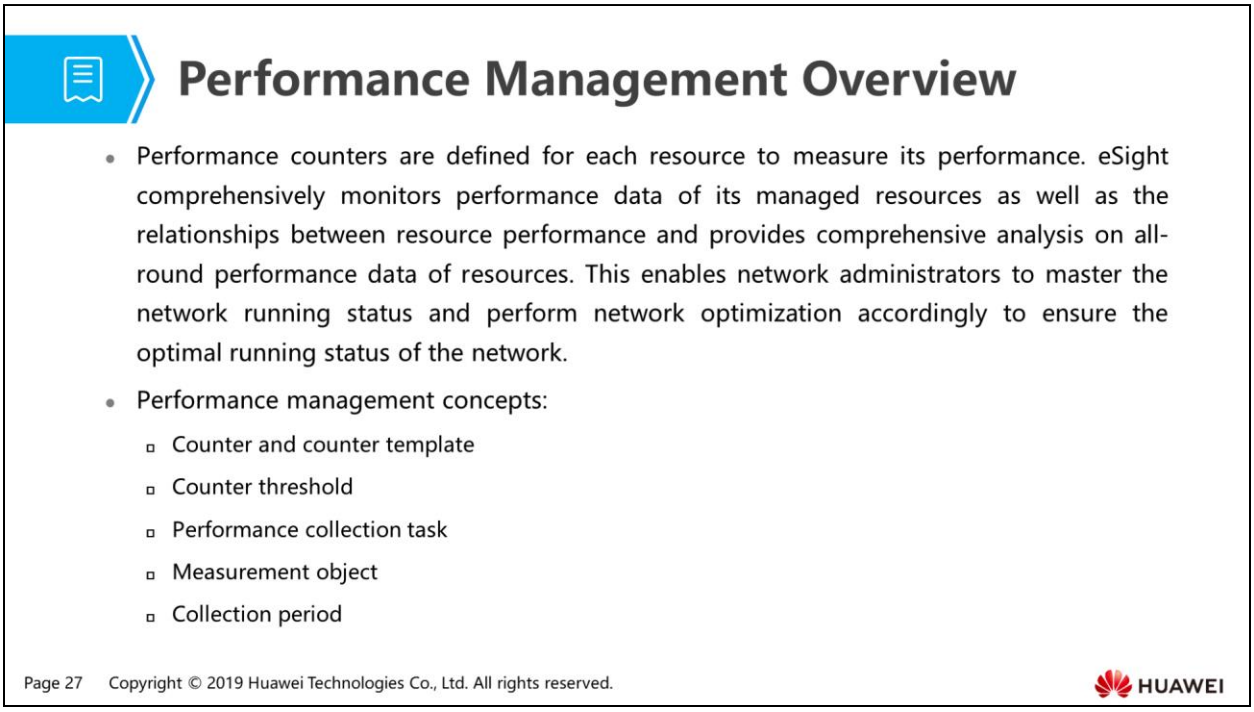
* SMS modem baud rate: 115200

Mobile number for receiving notification:

- Email server: You can set the domain name or IP address of the SMTP server, as well as the email address and port that send an email.
- SMS server: You can set the domain name or IP address of the SMS server, SMS message coding protocol, SMS server port, user name of the SMS server, and mobile numbers for sending and receiving SMS messages.
- SMS modem: You can set the network system of SMS modem, serial port connected to the SMS modem, baud rate of the SMS modem, and mobile number for receiving notifications.

Contents

1. Security Management
2. Resource Management
3. Alarm Management
4. **Performance Management**



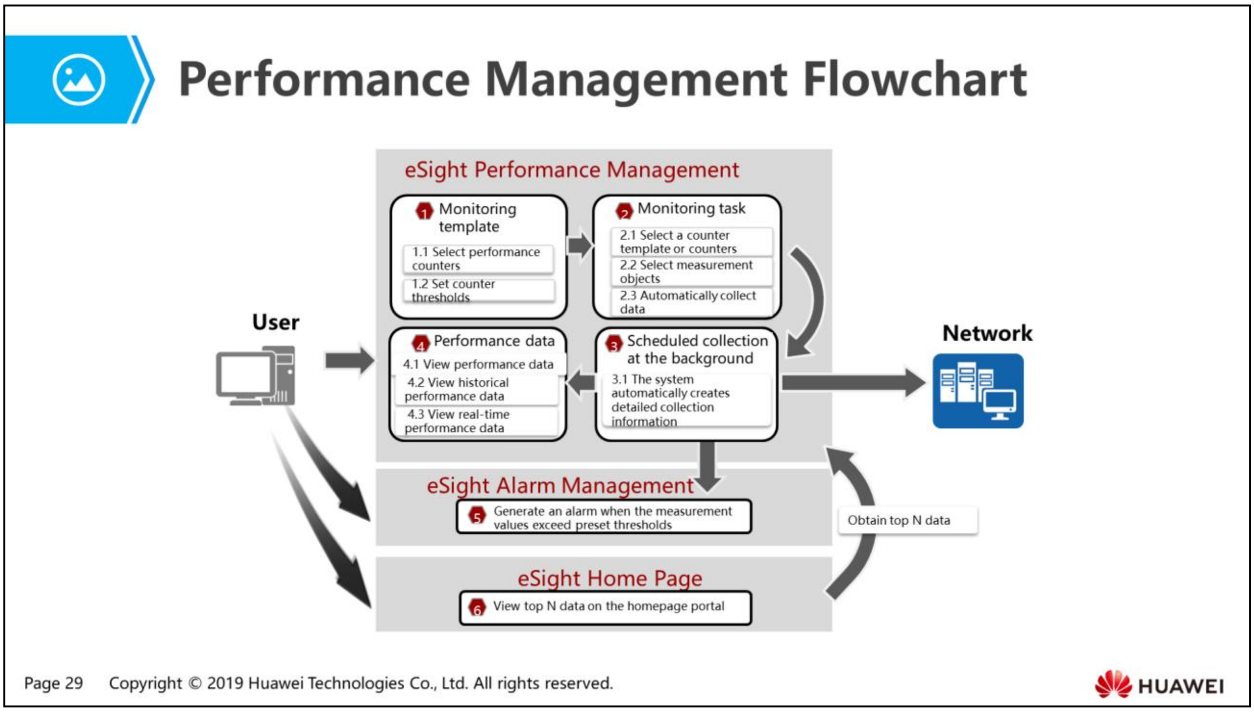
Performance Management Overview

- Performance counters are defined for each resource to measure its performance. eSight comprehensively monitors performance data of its managed resources as well as the relationships between resource performance and provides comprehensive analysis on all-round performance data of resources. This enables network administrators to master the network running status and perform network optimization accordingly to ensure the optimal running status of the network.
- Performance management concepts:
  - Counter and counter template
  - Counter threshold
  - Performance collection task
  - Measurement object
  - Collection period

HUAWEI

- Counter: a measure used to evaluate the performance of resources. For example, devices, ports, central processing unit (CPU), and memory are resources. CPU usage and memory usage are performance counters. Monitoring counters help administrators detect the service deterioration trend, based on which users can rectify potential problems before faults occur.
- Counter template: Devices of the same type have the same counter attributes. These counters can be freely combined to form a template. You can select a template when creating a performance collection task to improve the operation efficiency.
- Counter threshold: A counter threshold determines whether to report alarms and the level of reported alarms. When a measurement value of a counter exceeds the preset threshold, an alarm is generated. When the measurement value falls down to the allowed range, the alarm is automatically cleared.
- Performance collection task: A performance collection task is created to collect performance data of devices. eSight collects device performance data based on the task and displays performance data in graphs, so that users can view and analyze performance data.

- Measurement object: specifies the object to be measured if a specific resource has multiple objects. For example, if a device has multiple CPUs, a measurement object identifies the CPU to be measured.
- Collection period: specifies the interval at which performance data is collected. If the collection period is 5 minutes, eSight collects performance data of specified objects every 5 minutes.



Performance Management Flowchart

eSight Performance Management

1 Monitoring template
- 1.1 Select performance counters
- 1.2 Set counter thresholds

2 Monitoring task
- 2.1 Select a counter template or counters
- 2.2 Select measurement objects
- 2.3 Automatically collect data

3 Scheduled collection at the background
- 3.1 The system automatically creates detailed collection information

4 Performance data
- 4.1 View performance data
- 4.2 View historical performance data
- 4.3 View real-time performance data

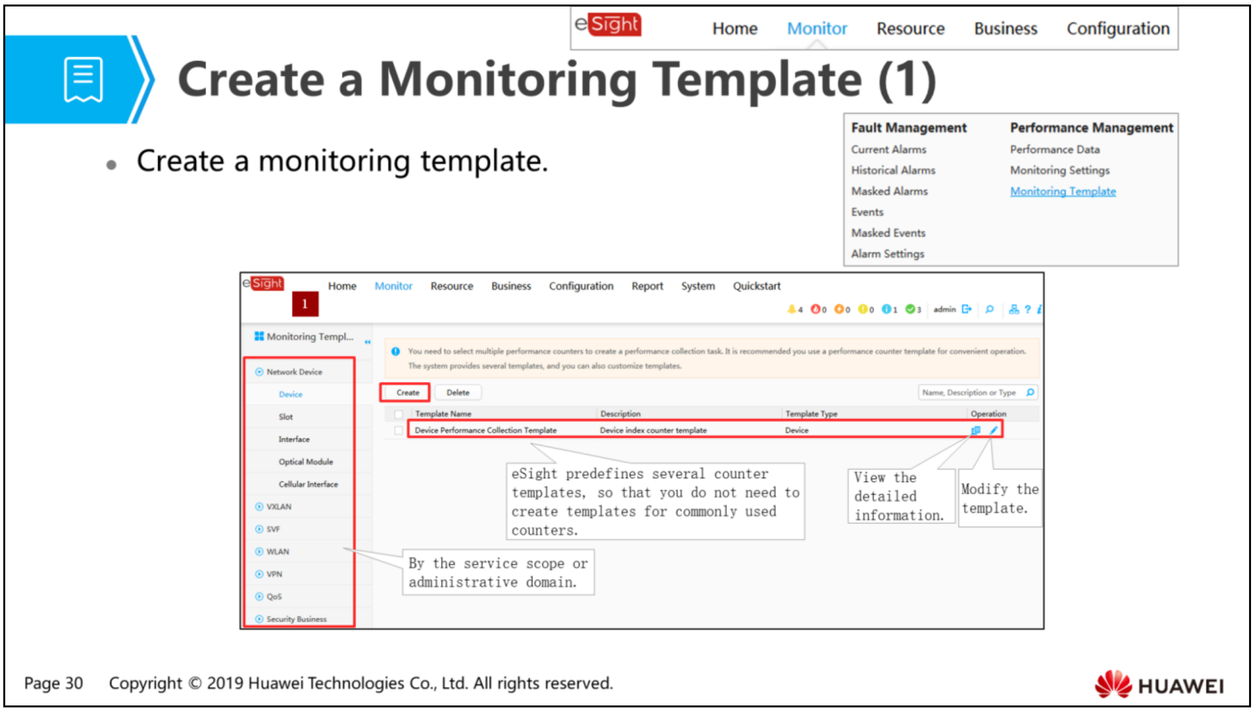
eSight Alarm Management

5 Generate an alarm when the measurement values exceed preset thresholds

eSight Home Page

6 View top N data on the homepage portal

- After you create a monitoring template and a monitoring task on the eSight client, eSight automatically collects device performance data based on task attributes and displays collected performance data on the eSight client. If measurement values exceed the preset alarm thresholds, alarms are generated and displayed in the current alarm list. If a performance portal is created, you can view performance data on the homepage.



Create a Monitoring Template (1)

- Create a monitoring template.

You need to select multiple performance counters to create a performance collection task. It is recommended you use a performance counter template for convenient operation. The system provides several templates, and you can also customize templates.

Template Name	Description	Template Type	Operation
Device Performance Collection Template	Device index counter template	Device	

eSight predefines several counter templates, so that you do not need to create templates for commonly used counters.

View the detailed information.

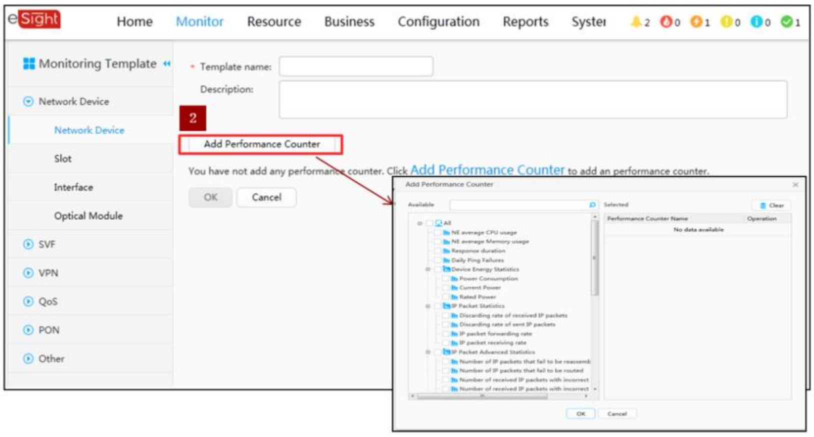
Modify the template.

By the service scope or administrative domain.

- To create a monitoring template, perform the following steps:
  - Start
  - Add counters
  - Set thresholds
  - Completed

Create a Monitoring Template (2)

- Add counters.



* Template name:

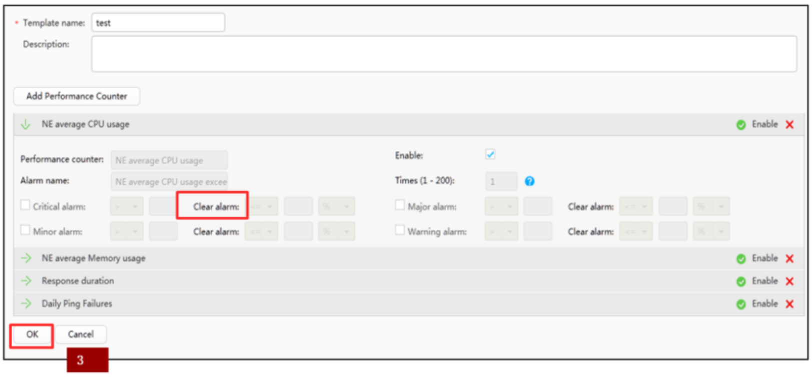
Description:

You have not add any performance counter. Click Add Performance Counter to add an performance counter.

Performance Counter Name	Operation
No data available	

Create a Monitoring Template (3)

- Set thresholds.



* Template name: test

Description:

NE average CPU usage

Performance counter: NE average CPU usage

Alarm name: NE average CPU usage excee

Enable: ☑

Times (1 - 200): 1

☐ Critical alarm: > Clear alarm: <= %

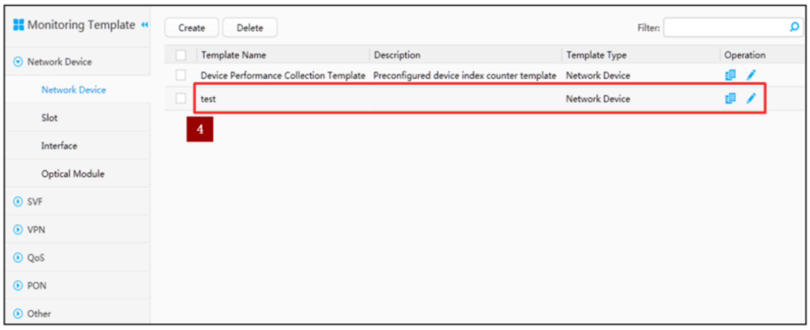
☐ Major alarm: > Clear alarm: <= %

☐ Minor alarm: > Clear alarm: <= %

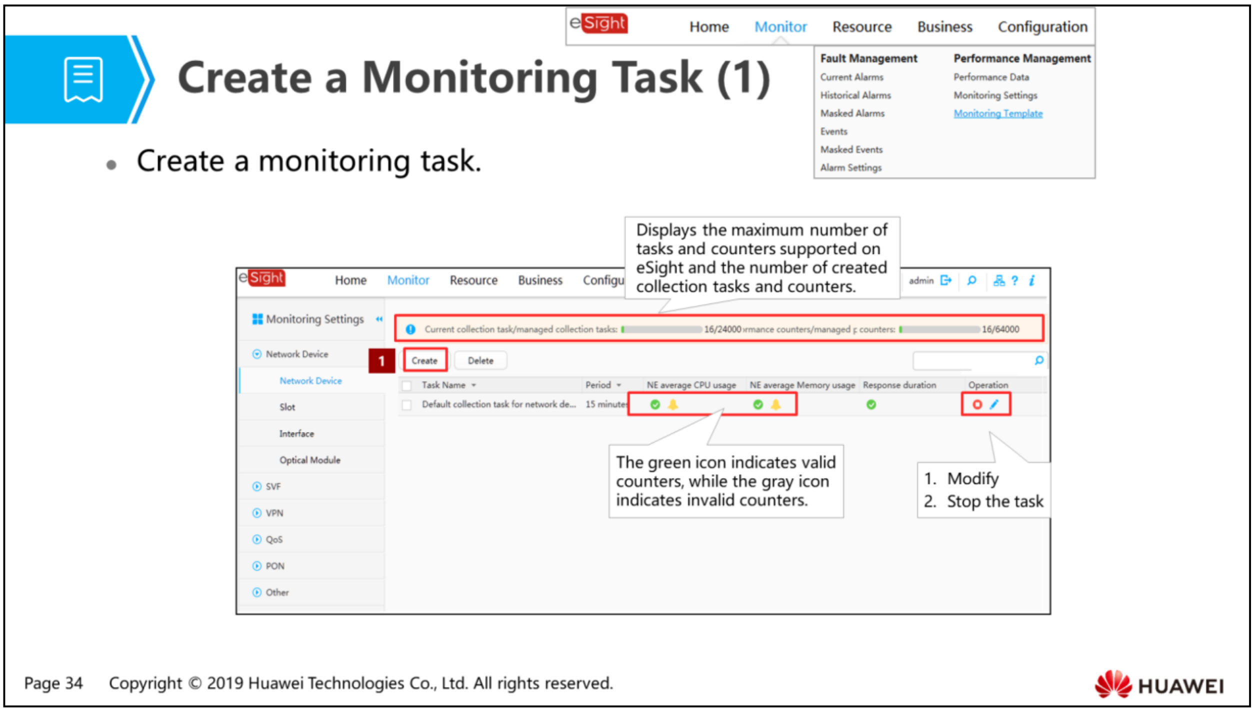
☐ Warning alarm: > Clear alarm: <= %

Create a Monitoring Template (4)

- A template is created.



□	Template Name	Description	Template Type	Operation
□	Device Performance Collection Template	Preconfigured device index counter template	Network Device	
□	test		Network Device	



Create a Monitoring Task (1)

- Create a monitoring task.

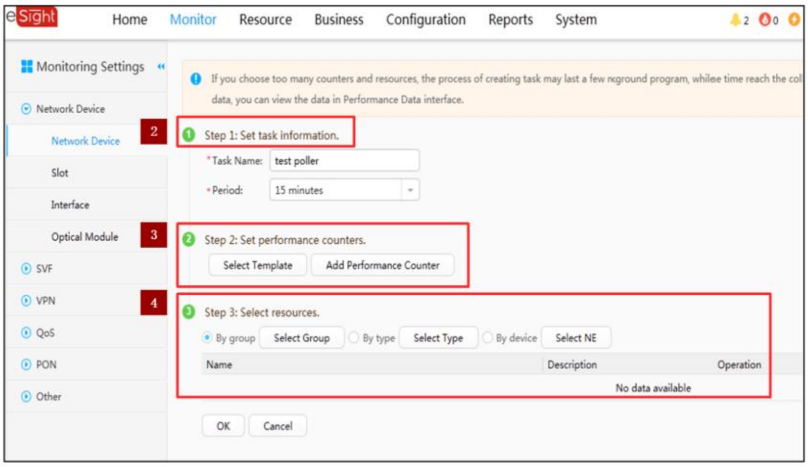
Displays the maximum number of tasks and counters supported on eSight and the number of created collection tasks and counters.

The green icon indicates valid counters, while the gray icon indicates invalid counters.

1. Modify
2. Stop the task

- To create a monitoring task, perform the following steps:
  - Start
  - Set task information.
  - Set the monitoring counters.
  - Select resources.
  - Completed

Create a Monitoring Task (2)



If you choose too many counters and resources, the process of creating task may last a few nxground program, whilee time reach the col data, you can view the data in Performance Data interface.

1 Step 1: Set task information.

*Task Name: test poller

*Period: 15 minutes

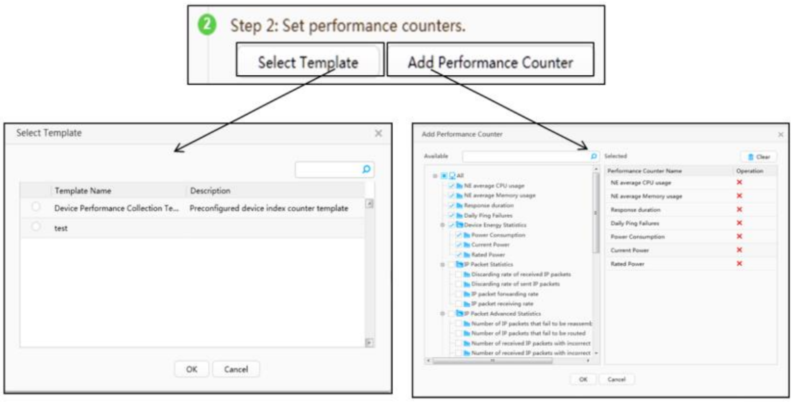
2 Step 2: Set performance counters.

3 Step 3: Select resources.

● By group ○ By type ○ By device

Name	Description	Operation
No data available		

Create a Monitoring Task (3)



2 Step 2: Set performance counters.

Select Template

	Template Name	Description
○	Device Performance Collection Te...	Preconfigured device index counter template
○	test	

Add Performance Counter

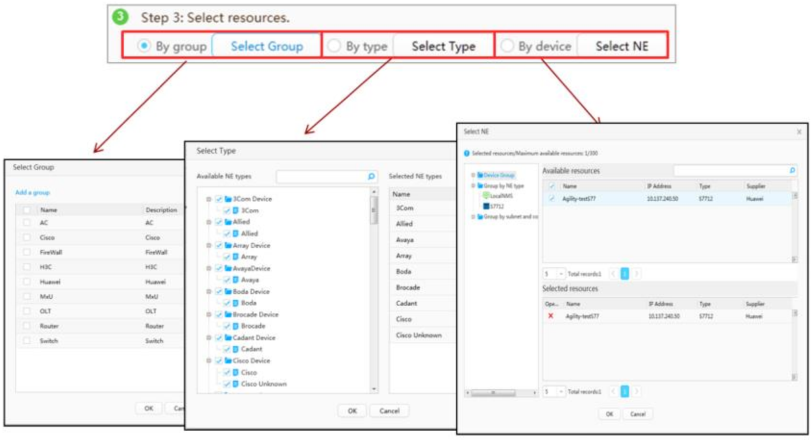
Available

- ☑ All
  - ✓ NE average CPU usage
  - ✓ NE average Memory usage
  - ✓ Response duration
  - ✓ Daily Ping Failures
  - ✓ Device Energy Statistics
    - ✓ Power Consumption
    - ✓ Current Power
    - ✓ Rated Power
  - □ IP Packet Statistics
    - □ Discarding rate of received IP packets
    - □ Discarding rate of sent IP packets
    - □ IP packet forwarding rate
    - □ IP packet receiving rate
  - □ IP Packet Advanced Statistics
    - □ Number of IP packets that fail to be reassemb
    - □ Number of IP packets that fail to be routed
    - □ Number of received IP packets with incorrect
    - □ Number of received IP packets with incorrect

Selected

Performance Counter Name	Operation
NE average CPU usage	✕
NE average Memory usage	✕
Response duration	✕
Daily Ping Failures	✕
Power Consumption	✕
Current Power	✕
Rated Power	✕

Create a Monitoring Task (4)



Step 3: Select resources.

● By group Select Group ○ By type Select Type ○ By device Select NE

Select Group

Add a group

□	Name	Description
□	AC	AC
□	Cisco	Cisco
□	FireWall	FireWall
□	H3C	H3C
□	Huawei	Huawei
□	MxU	MxU
□	OLT	OLT
□	Router	Router
□	Switch	Switch

Select Type

Available NE types

- ☑ 3Com Device
  - ☑ 3Com
- ☑ Allied
  - ☑ Allied
- ☑ Array Device
  - ☑ Array
- ☑ AvayaDevice
  - ☑ Avaya
- ☑ Boda Device
  - ☑ Boda
- ☑ Brocade Device
  - ☑ Brocade
- ☑ Cadant Device
  - ☑ Cadant
- ☑ Cisco Device
  - ☑ Cisco
  - ☑ Cisco Unknown

Selected NE types

Name
3Com
Allied
Avaya
Array
Boda
Brocade
Cadant
Cisco
Cisco Unknown

Select NE

Selected resources/Maximum available resources: 1/300

- Device Group
- Group by NE type
  - LocalNMS
  - S7712
- Group by subnet and co

Available resources

☑	Name	IP Address	Type	Supplier
☑	Agility-test577	10.137.240.50	S7712	Huawei

5 Total records:1

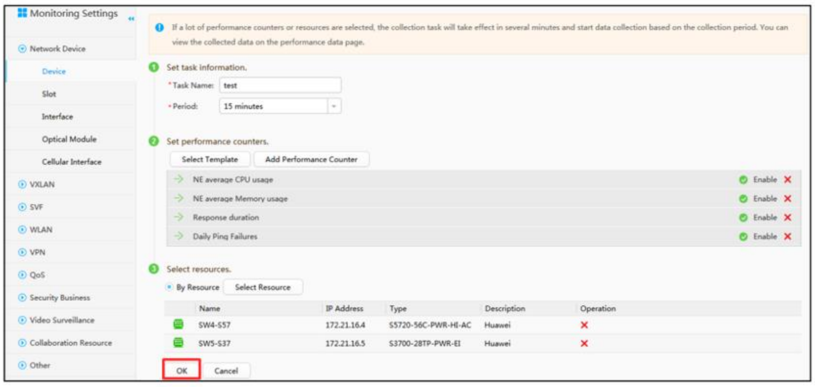
Selected resources

Ope...	Name	IP Address	Type	Supplier
✗	Agility-test577	10.137.240.50	S7712	Huawei

5 Total records:1

Create a Monitoring Task (5)

- A monitoring task is created.



If a lot of performance counters or resources are selected, the collection task will take effect in several minutes and start data collection based on the collection period. You can view the collected data on the performance data page.

1. Set task information.

*Task Name: test

*Period: 15 minutes

2. Set performance counters.

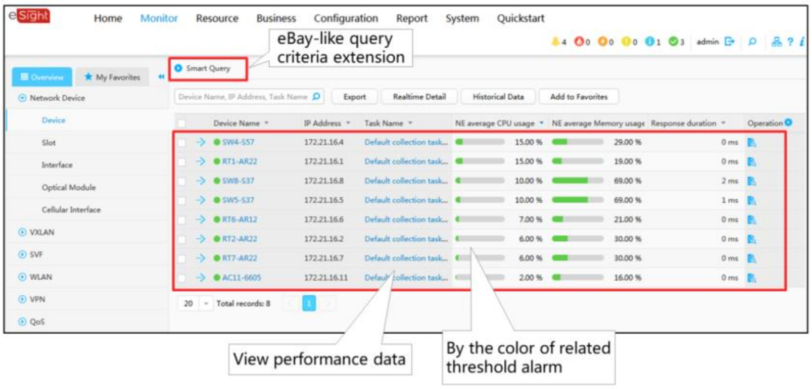
NE average CPU usage	✓ Enable	✗
NE average Memory usage	✓ Enable	✗
Response duration	✓ Enable	✗
Daily Ping Failures	✓ Enable	✗

3. Select resources.

● By Resource

Name	IP Address	Type	Description	Operation
SW4-S57	172.21.16.4	S5720-56C-PWR-HI-AC	Huawei	✗
SW5-S37	172.21.16.5	S3700-28TP-PWR-EI	Huawei	✗

View Performance Data - Home Page



Device Name	IP Address	Task Name	NE average CPU usage	NE average Memory usage	Response duration	Operation
SW4-S57	172.21.16.4	Default collection task...	15.00 %	29.00 %	0 ms	
RT1-AR22	172.21.16.1	Default collection task...	15.00 %	19.00 %	0 ms	
SW8-S37	172.21.16.8	Default collection task...	10.00 %	69.00 %	2 ms	
SW5-S37	172.21.16.5	Default collection task...	10.00 %	69.00 %	1 ms	
RT6-AR12	172.21.16.6	Default collection task...	7.00 %	21.00 %	0 ms	
RT2-AR22	172.21.16.2	Default collection task...	6.00 %	30.00 %	0 ms	
RT7-AR22	172.21.16.7	Default collection task...	6.00 %	30.00 %	0 ms	
AC11-6605	172.21.16.11	Default collection task...	2.00 %	16.00 %	0 ms	

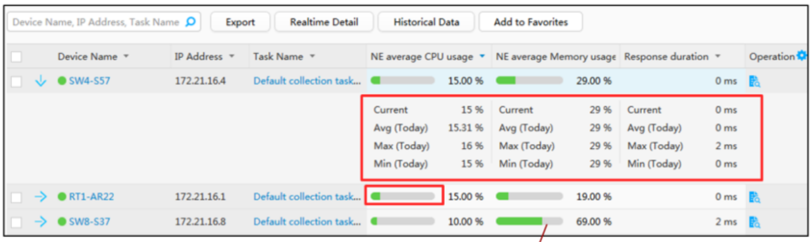
20 Total records: 8 1

eBay-like query criteria extension

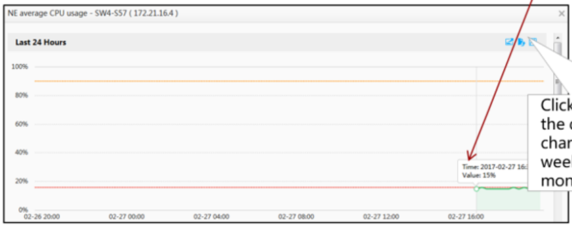
View performance data

By the color of related threshold alarm

View Performance Data - View Details

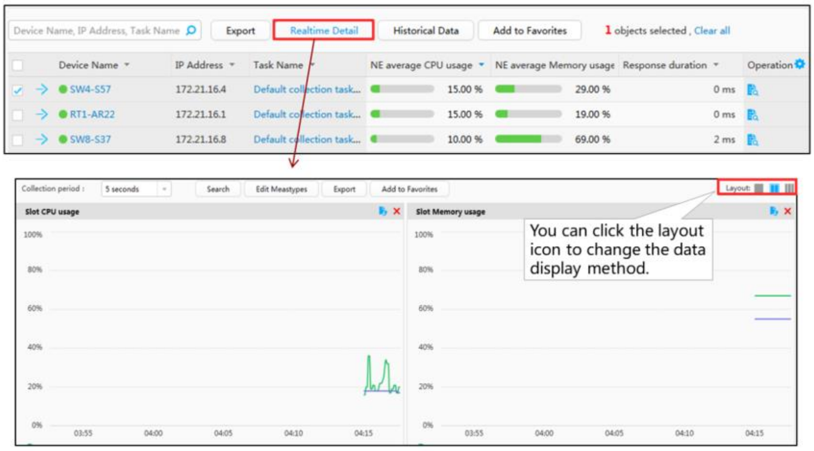


□	Device Name	IP Address	Task Name	NE average CPU usage	NE average Memory usage	Response duration
□	● SW4-S57	172.21.16.4	Default collection task...	15.00 %	29.00 %	0 ms
				Current 15 % Avg (Today) 15.31 % Max (Today) 16 % Min (Today) 15 %	Current 29 % Avg (Today) 29 % Max (Today) 29 % Min (Today) 29 %	Current 0 ms Avg (Today) 0 ms Max (Today) 2 ms Min (Today) 0 ms
□	● RT1-AR22	172.21.16.1	Default collection task...	15.00 %	19.00 %	0 ms
□	● SW8-S37	172.21.16.8	Default collection task...	10.00 %	69.00 %	2 ms



Click a proportion bar to view the detailed historical trend chart of the last 24 hours, last week, last month, or last three months.

View Real - Time Performance Data



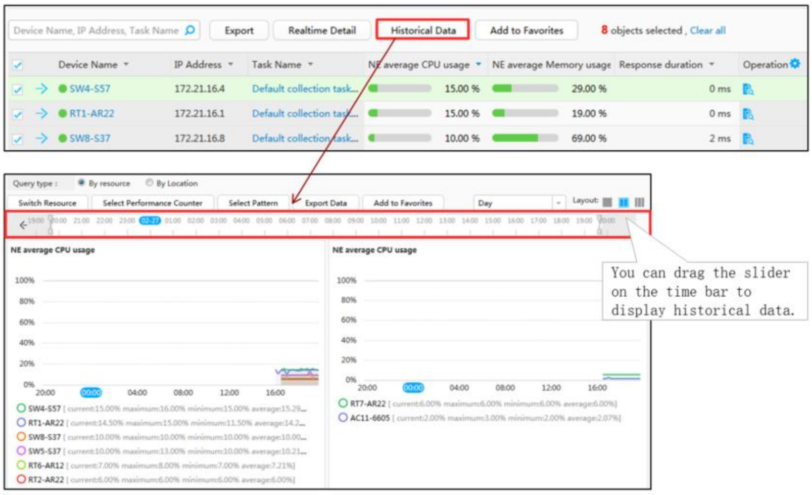
Device Name, IP Address, Task Name | Export | Realtime Detail | Historical Data | Add to Favorites | 1 objects selected , Clear all

		Device Name	IP Address	Task Name	NE average CPU usage	NE average Memory usage	Response duration	Operation
☑	→	● SW4-S57	172.21.16.4	Default collection task...	15.00 %	29.00 %	0 ms	
□	→	● RT1-AR22	172.21.16.1	Default collection task...	15.00 %	19.00 %	0 ms	
□	→	● SW8-S37	172.21.16.8	Default collection task...	10.00 %	69.00 %	2 ms	

Collection period : 5 seconds | Search | Edit Meastypes | Export | Add to Favorites | Layout:

You can click the layout icon to change the data display method.

View Historical Performance Data


Device Name, IP Address, Task Name
Export
Realtime Detail
Historical Data
Add to Favorites
8 objects selected , Clear all

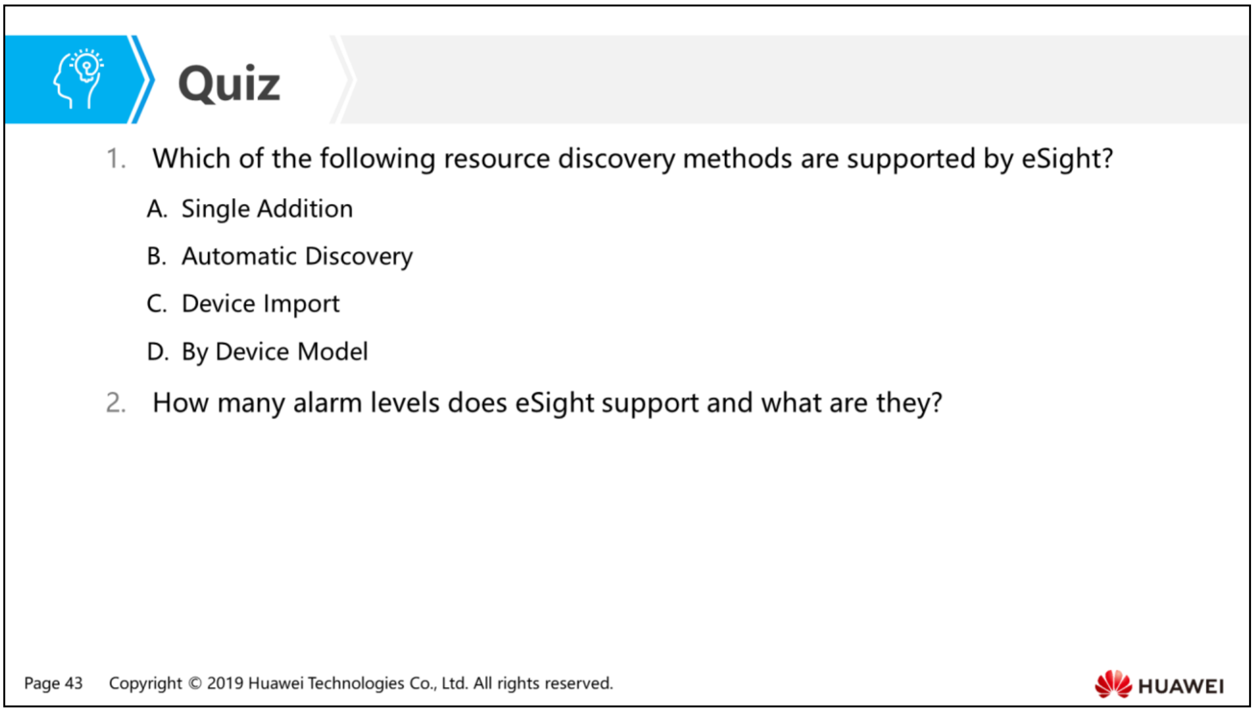
	Device Name	IP Address	Task Name	NE average CPU usage	NE average Memory usage	Response duration	Operation
☑	SW4-S57	172.21.16.4	Default collection task...	15.00 %	29.00 %	0 ms	
☑	RT1-AR22	172.21.16.1	Default collection task...	15.00 %	19.00 %	0 ms	
☑	SW8-S37	172.21.16.8	Default collection task...	10.00 %	69.00 %	2 ms	

Query type : ● By resource ○ By Location

○ SW4-S57 [current:15.00% maximum:16.00% minimum:15.00% average:15.29...
○ RT1-AR22 [current:14.50% maximum:15.00% minimum:11.50% average:14.2...
○ SW8-S37 [current:10.00% maximum:10.00% minimum:10.00% average:10.00...
○ SW5-S37 [current:10.00% maximum:13.00% minimum:10.00% average:10.21...
○ RT6-AR12 [current:7.00% maximum:8.00% minimum:7.00% average:7.21%]
○ RT2-AR22 [current:6.00% maximum:6.00% minimum:6.00% average:6.00%]

○ RT7-AR22 [current:6.00% maximum:6.00% minimum:6.00% average:6.00%]
○ AC11-6605 [current:2.00% maximum:3.00% minimum:2.00% average:2.07%]

You can drag the slider on the time bar to display historical data.



Quiz

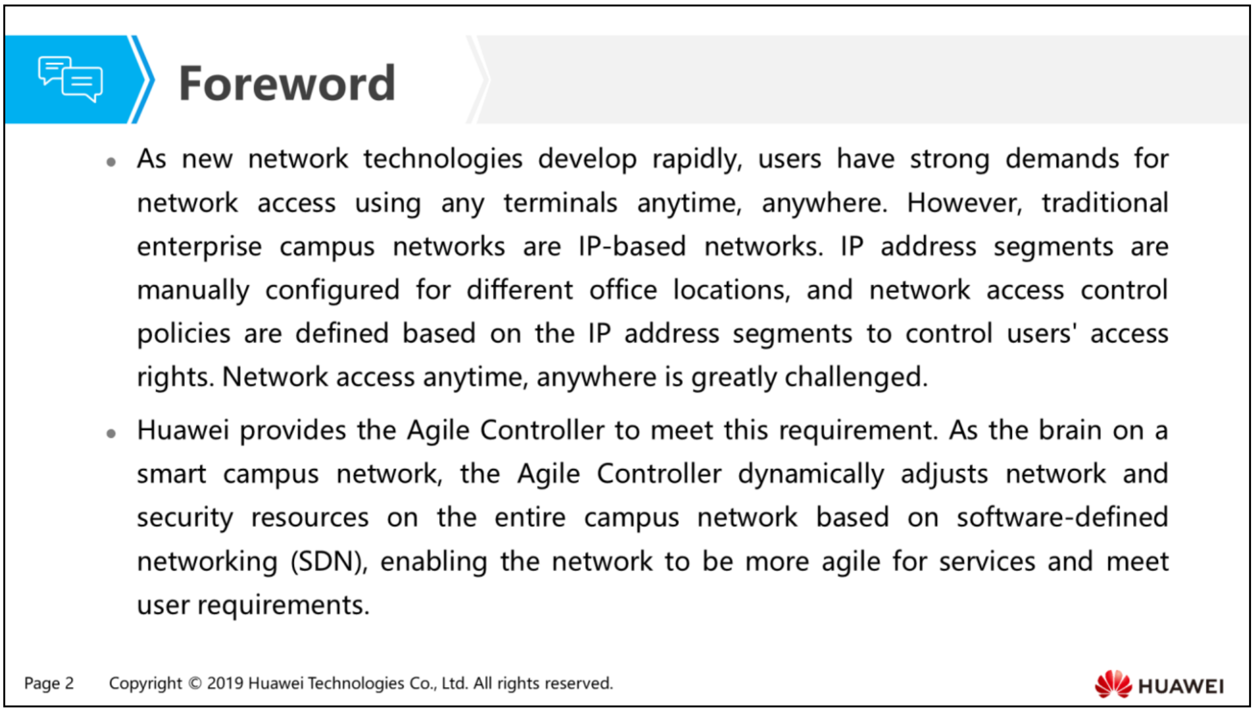
1. Which of the following resource discovery methods are supported by eSight?
   - A. Single Addition
   - B. Automatic Discovery
   - C. Device Import
   - D. By Device Model
2. How many alarm levels does eSight support and what are they?

- Answer: ABC.
- Answer: eSight supports four alarm levels and they are critical, major, minor, and warning in descending order of severity.

Thank You

www.huawei.com

Agile Controller Product Features



Foreword

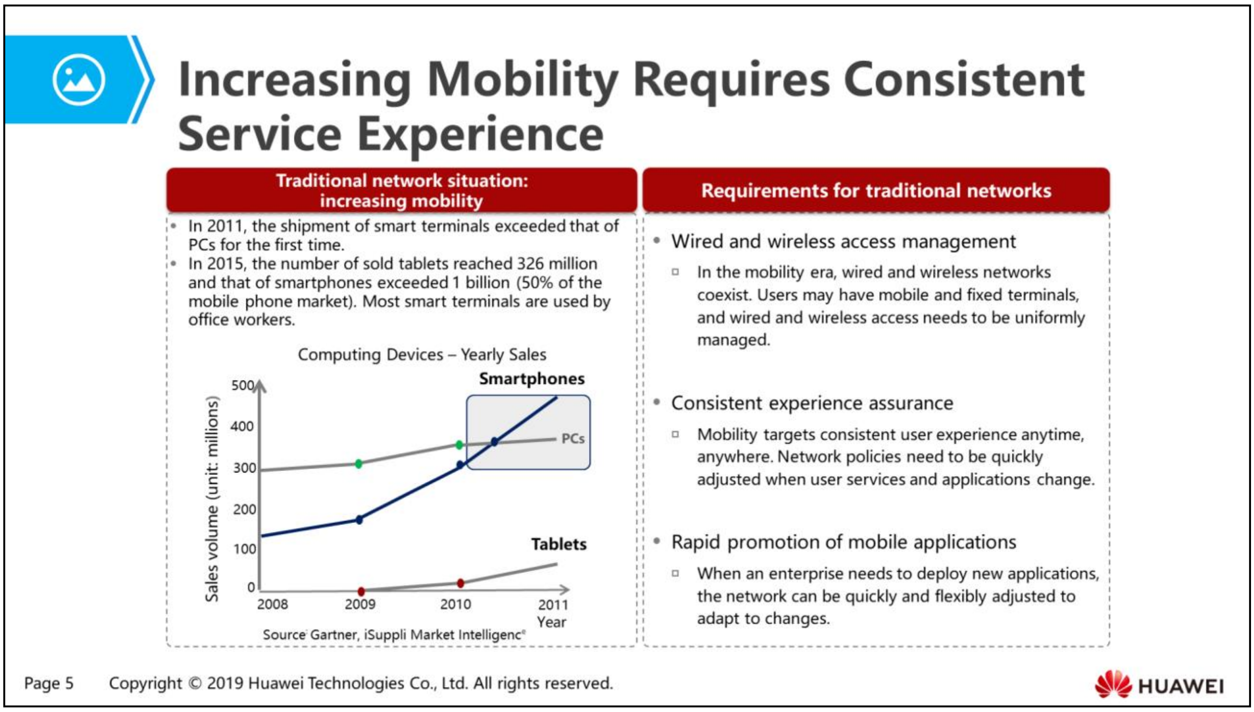
- As new network technologies develop rapidly, users have strong demands for network access using any terminals anytime, anywhere. However, traditional enterprise campus networks are IP-based networks. IP address segments are manually configured for different office locations, and network access control policies are defined based on the IP address segments to control users' access rights. Network access anytime, anywhere is greatly challenged.
- Huawei provides the Agile Controller to meet this requirement. As the brain on a smart campus network, the Agile Controller dynamically adjusts network and security resources on the entire campus network based on software-defined networking (SDN), enabling the network to be more agile for services and meet user requirements.

Objectives

- On completion of this section, you will be able to:
  - Understand challenges facing traditional networks
  - Master basic functions and features of the Agile Controller
  - Be familiar with the Agile Controller configuration process

Contents

1. **Challenges Facing Traditional Networks**
2. Agile Controller Function Implementation
3. Agile Controller Configuration Example



Increasing Mobility Requires Consistent Service Experience

Traditional network situation: increasing mobility

- In 2011, the shipment of smart terminals exceeded that of PCs for the first time.
- In 2015, the number of sold tablets reached 326 million and that of smartphones exceeded 1 billion (50% of the mobile phone market). Most smart terminals are used by office workers.

Computing Devices – Yearly Sales

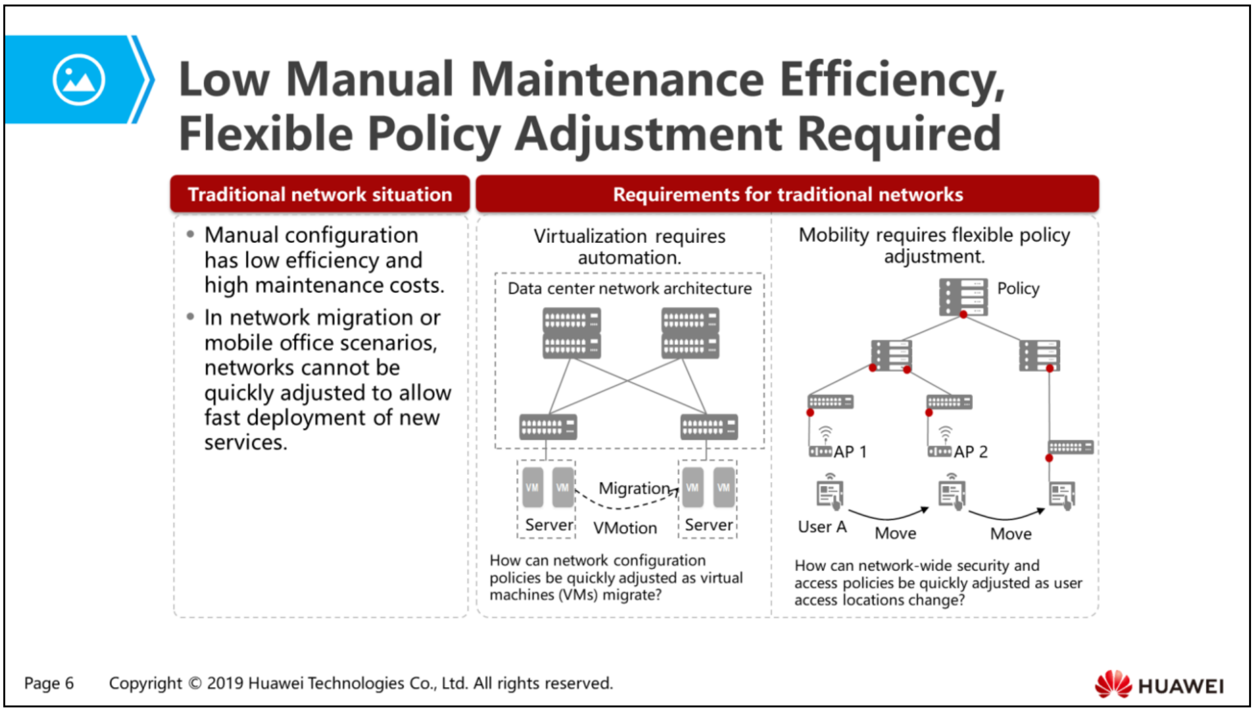
Source Gartner, iSuppli Market Intelligenc°

Requirements for traditional networks

- Wired and wireless access management
    - In the mobility era, wired and wireless networks coexist. Users may have mobile and fixed terminals, and wired and wireless access needs to be uniformly managed.
- Consistent experience assurance
    - Mobility targets consistent user experience anytime, anywhere. Network policies need to be quickly adjusted when user services and applications change.
- Rapid promotion of mobile applications
    - When an enterprise needs to deploy new applications, the network can be quickly and flexibly adjusted to adapt to changes.

HUAWEI

- Traditional network situation:
    - With the development of mobility, users obtain different IP addresses when accessing a network at different locations. Network access rights control based on IP addresses can hardly provide consistent user experience to end users.
- Requirements for traditional networks:
    - Huawei Agile Controller provides user-based unified control to control access rights of mobile users, meeting requirements of policy mobility, dynamic resource allocation, and unified experience.



Low Manual Maintenance Efficiency, Flexible Policy Adjustment Required

Traditional network situation

- Manual configuration has low efficiency and high maintenance costs.
- In network migration or mobile office scenarios, networks cannot be quickly adjusted to allow fast deployment of new services.

Requirements for traditional networks

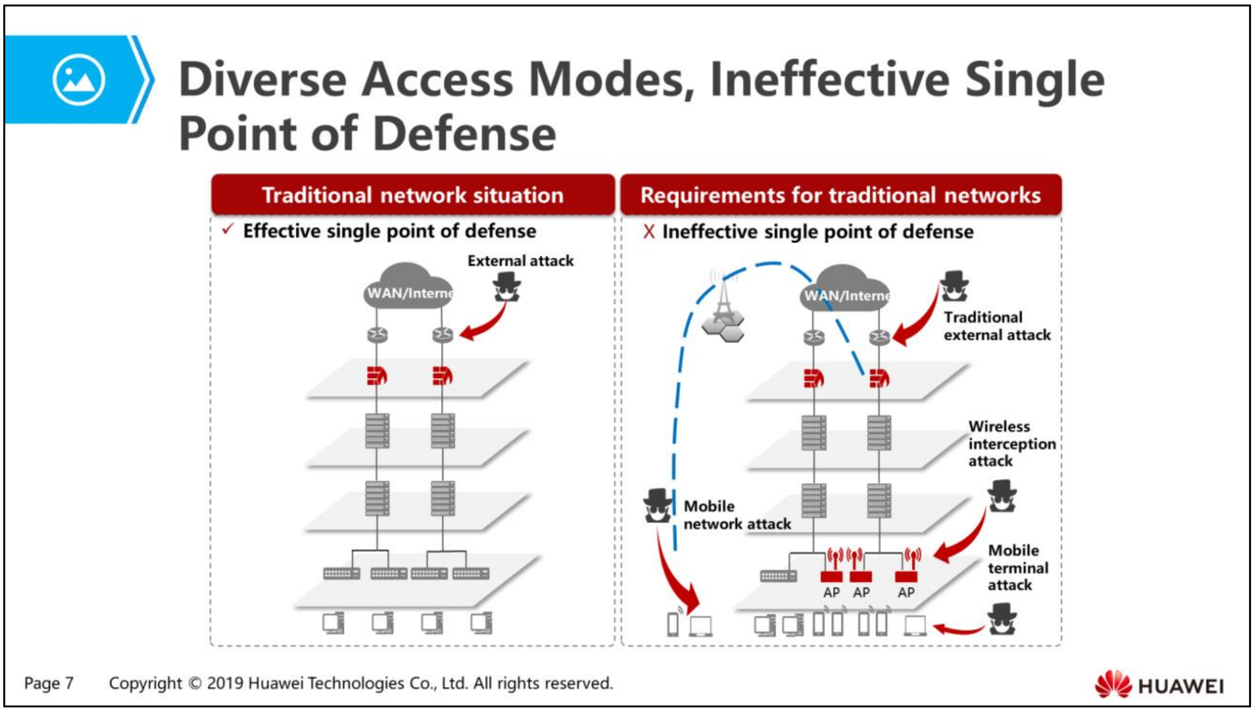
Virtualization requires automation.

How can network configuration policies be quickly adjusted as virtual machines (VMs) migrate?

Mobility requires flexible policy adjustment.

How can network-wide security and access policies be quickly adjusted as user access locations change?

- Traditional network situation:
  - Traditionally, IT personnel in an enterprise configure static network access control policies on network devices manually or through a network management system (NMS). When there are a large number of mobile users on the network, manual policy adjustment has low efficiency and is difficult. In addition, network configuration errors may occur, and the workload of IT maintenance personnel increases.
  - When new services are deployed, the network cannot be quickly adjusted to allow fast deployment of new services.
- Requirements for traditional networks:
  - Automated management and short deployment period.
  - Flexible policy adjustment in network migration or mobile office scenarios.



Diverse Access Modes, Ineffective Single Point of Defense

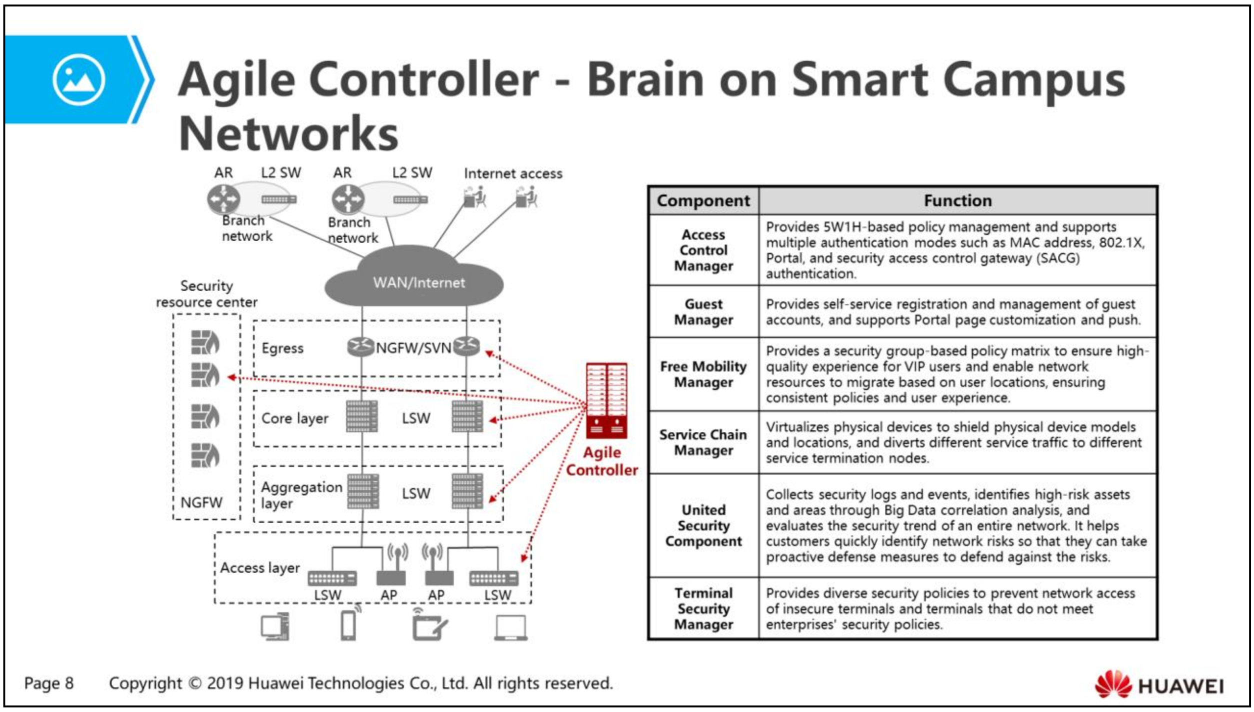
Traditional network situation

✓ Effective single point of defense

Requirements for traditional networks

X Ineffective single point of defense

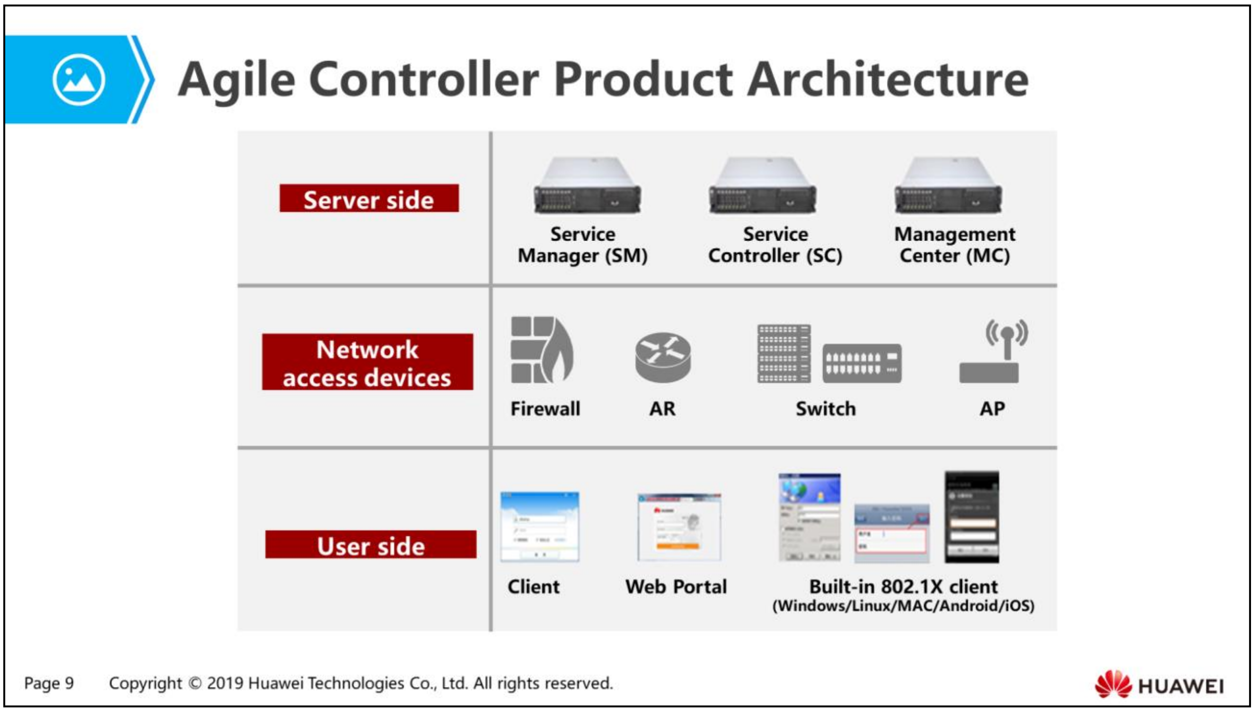
- Traditional network situation:
  - On a traditional network, the access mode and location are fixed, and the attack points and methods are monotonous.
  - Extended office places and diverse access terminals allowed by office mobilization result in a variety of attack points and methods.
- Requirements for traditional networks:
  - The Agile Controller abstracts security devices into a security resource center and redirects user traffic to the security resource center for processing, improving security resource use efficiency and enhancing network security protection capabilities.



Agile Controller - Brain on Smart Campus Networks

Component	Function
Access Control Manager	Provides 5W1H-based policy management and supports multiple authentication modes such as MAC address, 802.1X, Portal, and security access control gateway (SACG) authentication.
Guest Manager	Provides self-service registration and management of guest accounts, and supports Portal page customization and push.
Free Mobility Manager	Provides a security group-based policy matrix to ensure high-quality experience for VIP users and enable network resources to migrate based on user locations, ensuring consistent policies and user experience.
Service Chain Manager	Virtualizes physical devices to shield physical device models and locations, and diverts different service traffic to different service termination nodes.
United Security Component	Collects security logs and events, identifies high-risk assets and areas through Big Data correlation analysis, and evaluates the security trend of an entire network. It helps customers quickly identify network risks so that they can take proactive defense measures to defend against the risks.
Terminal Security Manager	Provides diverse security policies to prevent network access of insecure terminals and terminals that do not meet enterprises' security policies.

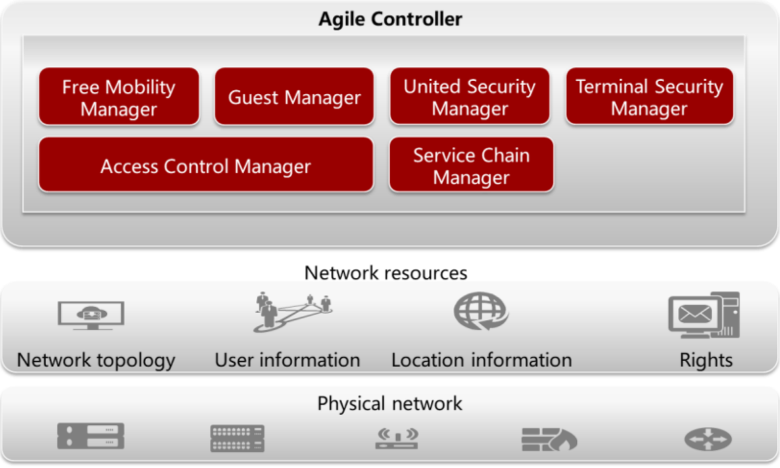
- As the brain on smart campus networks, the Agile Controller dynamically allocates network and security resources on the entire campus networks based on SDN, enabling the networks to be more agile for services. The Agile Controller provides the following functions:
  - Provides a unified policy engine to realize unified access control policies within the entire organization, and implements authentication and authorization based on 5W1H (Who, When, Where, What, Whose, How).
  - Provides full lifecyle guest management and enables customers to customize Portal login pages to meet their own needs. The customized Portal login pages can be pushed to users based on access locations to help users quickly access networks, improve enterprise images, and reduce the IT O&M workload.
  - Provides priority-based network access rights planning and network-wide automatic policy deployment and status monitoring based on 5W1H policy control. In this way, consistent policies can be applied to users regardless of users' access locations, delivering consistent service experience to mobile users.
  - Provides the service chain capability to abstract security devices into a security resource center and redirect user traffic to the security resource center for processing. The service chain capability improves security resource use efficiency and enhances network security protection capabilities.



Agile Controller Product Architecture

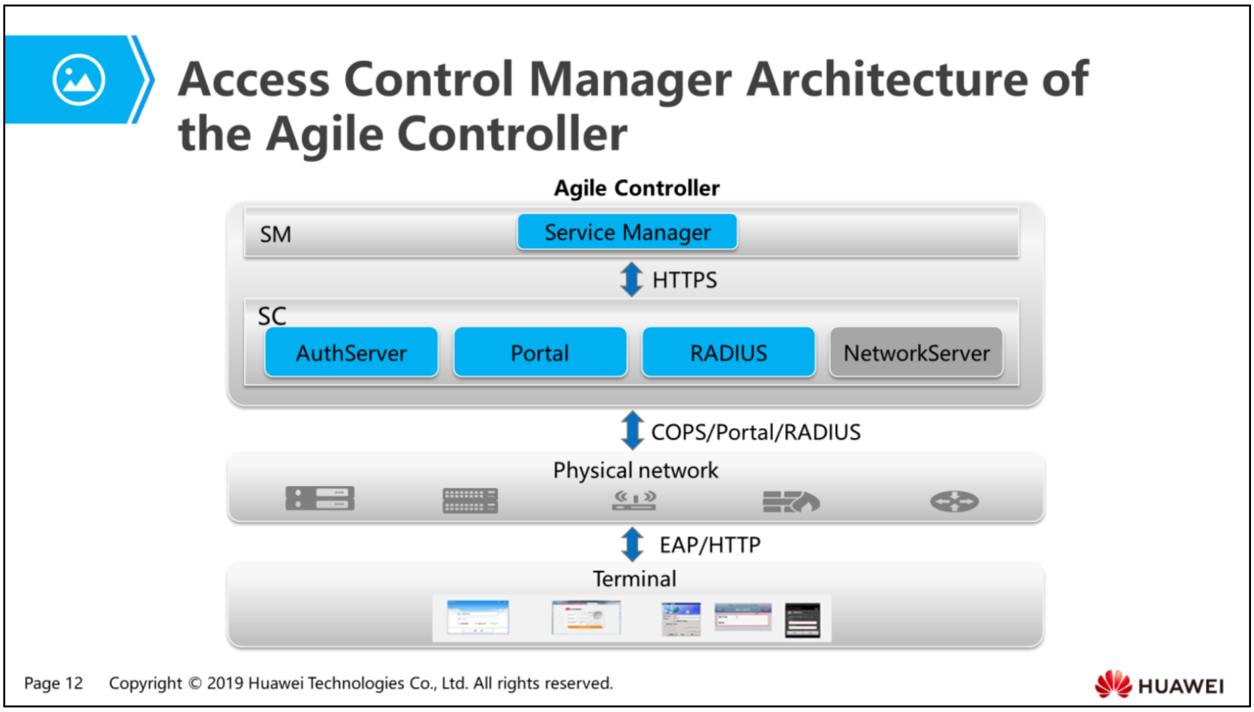
- Server side:
    - MC: As the management center of the Agile Controller, the MC formulates overall policies including secure access control, terminal security management, patch management, software distribution, and license management policies, delivers the policies to each SM node, and monitors policy execution on the SM nodes.
    - SM: The SM is responsible for service management. The system administrator can complete access control, user management, and free mobility configuration on the web management page. As the manager of the Agile Controller system, the SM manages connected SCs and sends real-time instructions to the SCs to transmit services.
    - SC: The SC integrates standard RADIUS and Portal servers, and associates with network access devices to implement user-based network access control policies. The SC provides the following functions:
        - Associates with network access devices such as switches, routers, WLAN devices, and firewalls to uniformly manage and automatically deploy network-wide access policies. It notifies the network access devices to change the users' network access rights after they pass identity authentication.
        - Associates with an orchestration device to deliver service chain policies and direct specified service flows to the next-generation firewall (NGFW) in the security resource center.
- Network access devices are deployed to provide access control and other service processing capabilities such as security protection and online behavior management.
- On the user side, users use clients to connect to a network for authentication. The clients usually use the Extensible Authentication Protocol (EAP) or Hypertext Transfer Protocol (HTTP) for authentication.

Agile Controller Software Function Panorama



Contents

1. Challenges Facing Traditional Networks
2. **Agile Controller Function Implementation**
   - Access Control
   - Guest Management
   - Free Mobility
   - Service Chain
   - United Security
   - Terminal Security
3. Agile Controller Configuration Example



Access Control Manager Architecture of the Agile Controller

Agile Controller

SM

Service Manager

HTTPS

SC

AuthServer

Portal

RADIUS

NetworkServer

COPS/Portal/RADIUS

Physical network

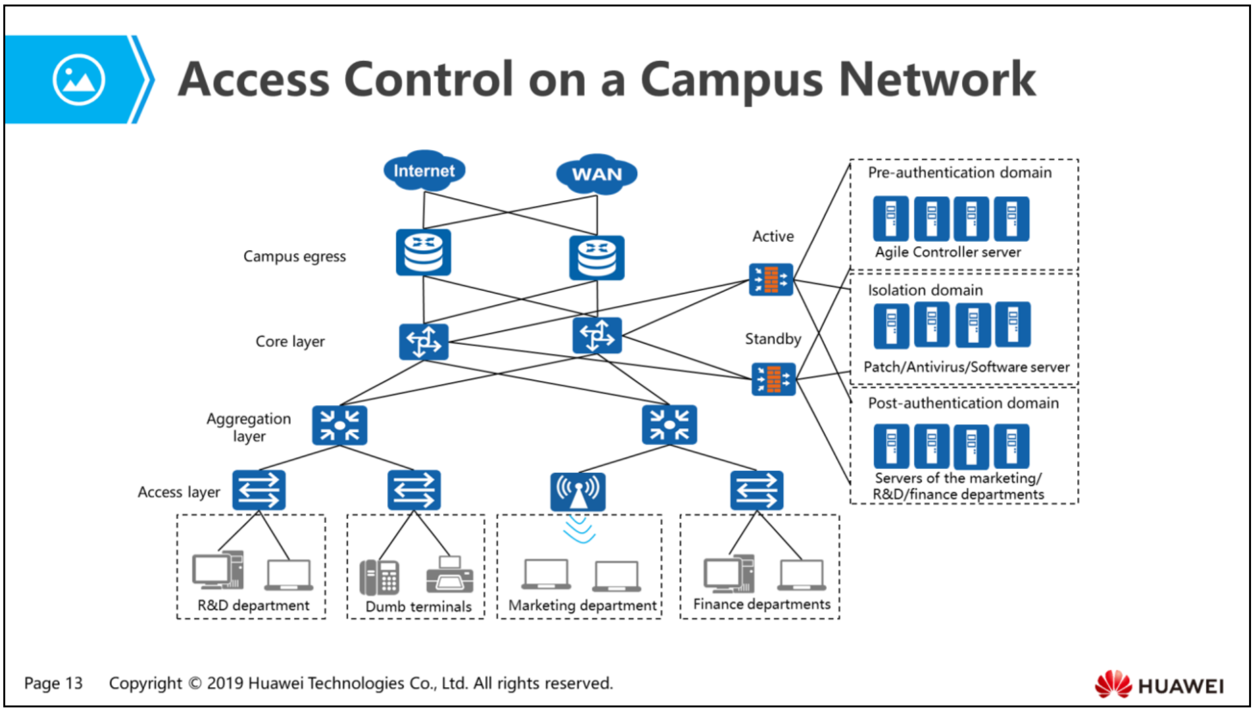
EAP/HTTP

Terminal

Page 12

HUAWEI

- The SM is responsible for service management. System administrators can complete service configuration and management on the web management page. As the manager of the Agile Controller, the SM manages connected SCs and sends real-time instructions to the SCs to complete service configuration.
- As the service controller of the Agile Controller, the SC associates with network access devices to implement service control for users.
    - The AuthServer component implements access control for network devices that have the Common Open Policy Service (COPS) protocol enabled.
    - The Portal component implements access control for network devices that have the Portal protocol enabled.
    - The RADIUS component implements access control for network devices that have the RADIUS protocol enabled.
    - The NetworkServer component does not implement access control.
- The physical network provides access control and other service processing capabilities such as security protection and online behavior management.
- Users use a client to connect to a network for authentication. The client usually uses EAP or HTTP for authentication.



Access Control on a Campus Network

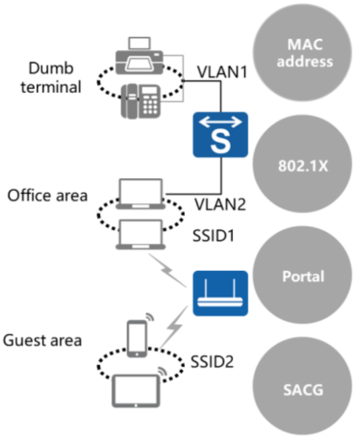
Page 13 Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

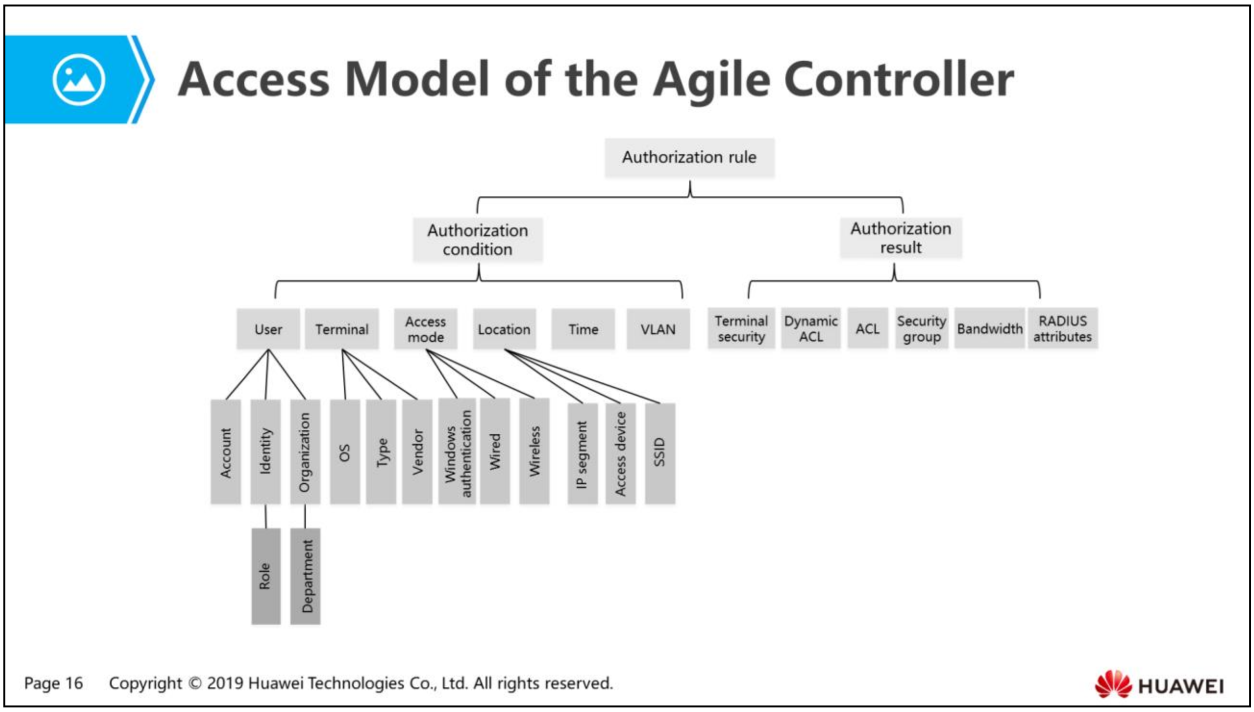
- The Agile Controller can work with WLAN devices, Huawei Portal switches, and standard 802.1X switches to provide multi-dimensional network access control functions. It provides flexible network access authorization policies based on user identity, terminal type, access location, access time, and terminal compliance check result.
- Use the access control deployment solution for a campus network:
  - Enable the 802.1X function on the switches at the core or aggregation layer, and configure user control lists (UCLs) (supported by agile switches), VLANs, and access control lists (ACLs) to control user rights.
  - Configure access control policies for devices in each department based on department requirements, user identity, terminal type, access location, and access time.
  - Configure MAC address bypass authentication for dumb terminals to access the network because dumb terminals cannot provide the page for entering the user name and password.
- Authentication domains are classified into the pre-authentication, isolation, and post-authentication domains:
  - A pre-authentication domain is the area that can be accessed by terminal hosts before they pass identity authentication. On the network shown in the above figure, the SC will instruct the security access control gateway (SACG) to prohibit end users that have not passed identity authentication from accessing the post-authentication or isolation domain, and only allow them to access the pre-authentication domain.

    - Public network resources such as the DNS server, external authentication sources, SCs, and SM are deployed in a pre-authentication domain, and can be accessed by end users without identity authentication.
- An isolation domain is the area that can be accessed by terminal hosts that have passed identity authentication but have not passed security authentication. On the network shown in the above figure, the SC will instruct the SACG to allow end users that have passed identity authentication but have not passed security authentication to access the pre-authentication and isolation domains, and prohibit them from accessing the post-authentication domain.
    - Security protection resources (such as the patch server and antivirus server) that can help end users eliminate violation information are located in an isolation domain.
- A post-authentication domain is the area that can be accessed by terminal hosts after they pass identity and security authentication. On the network shown in the above figure, the SC will instruct the SACG to allow end users that have passed identity and security authentication to access the post-authentication.
    - Network resources to be protected such as the ERP system, financial system, and database system are deployed in a post-authentication domain.

Comprehensive Access Control, Applicable to Multiple Types of Networks

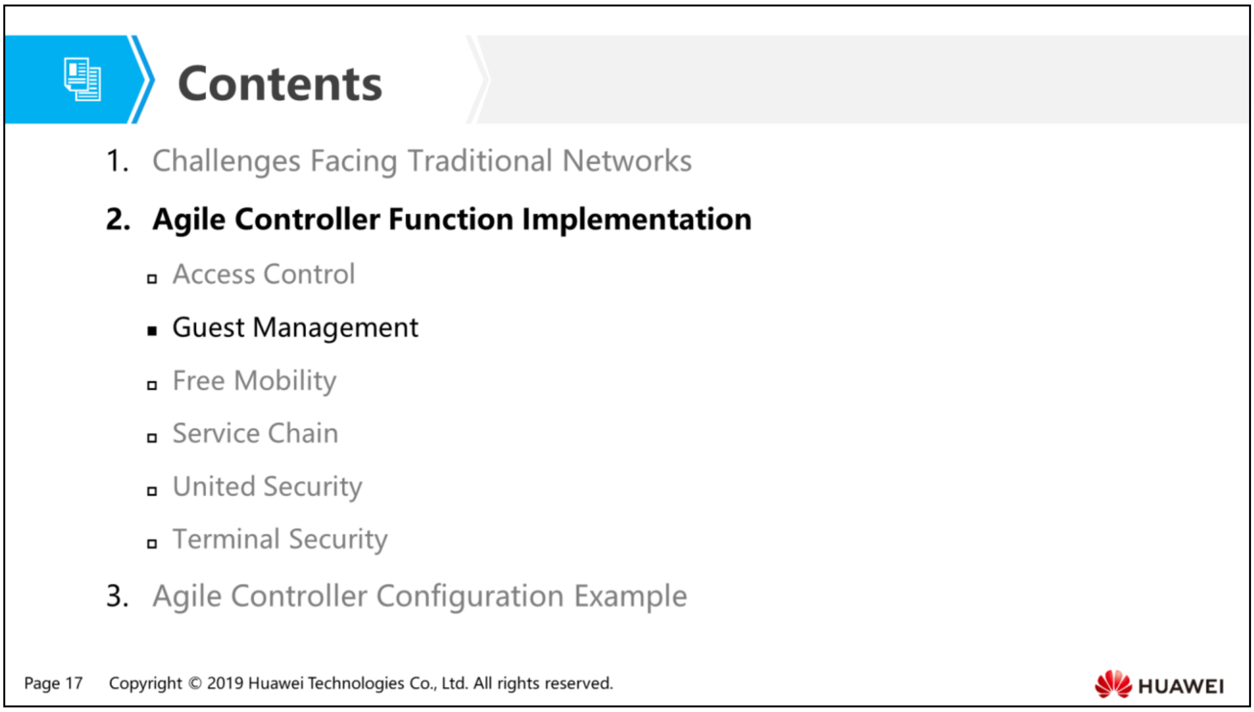


- **MAC address authentication**
  - The authentication server authenticates terminals based on their MAC addresses.
  - It is applicable to dumb terminals such as IP phones and printers.
- **802.1X authentication**
  - Clients, devices, and authentication servers exchange authentication messages using EAP.
  - It supports association with Huawei all series switches, routers, WLAN devices, and third-party 802.1X switches.
- **Portal authentication**
  - Portal authentication is also called web authentication. Users can enter their user names and passwords on the web authentication page for identity authentication.
  - It supports association with Huawei all series switches, routers, and WLAN devices.
- **SACG authentication**
  - A USG firewall is connected to a router or switch in bypass mode and controls terminal access through policy-based routing.



Access Model of the Agile Controller

- The core of the access model is the authorization condition and authorization result.
  - Authorization conditions are combinations of objects (such as users and terminals that access a network) and access elements (such as the access location, time, and mode).
  - Authorization results are policies that devices use to control user access.



Contents

1. Challenges Facing Traditional Networks
2. **Agile Controller Function Implementation**
   - Access Control
   - Guest Management
   - Free Mobility
   - Service Chain
   - United Security
   - Terminal Security
3. Agile Controller Configuration Example

Guest Definition and Access Scenarios

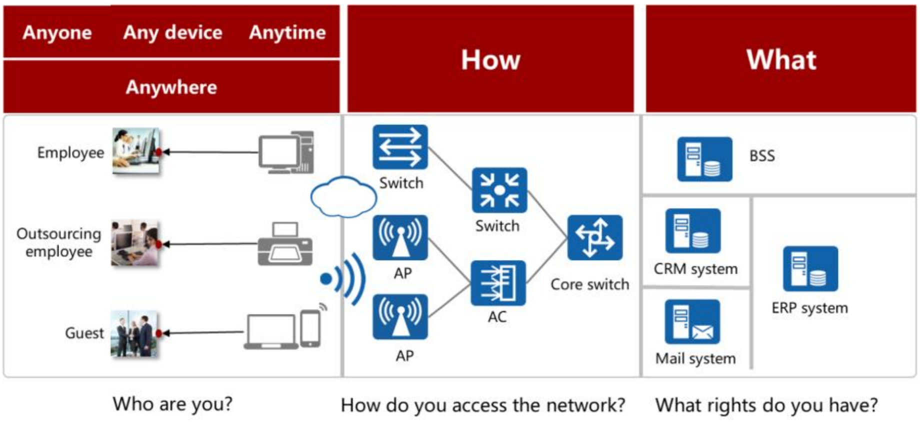
Definition and network access characteristics of enterprise guests

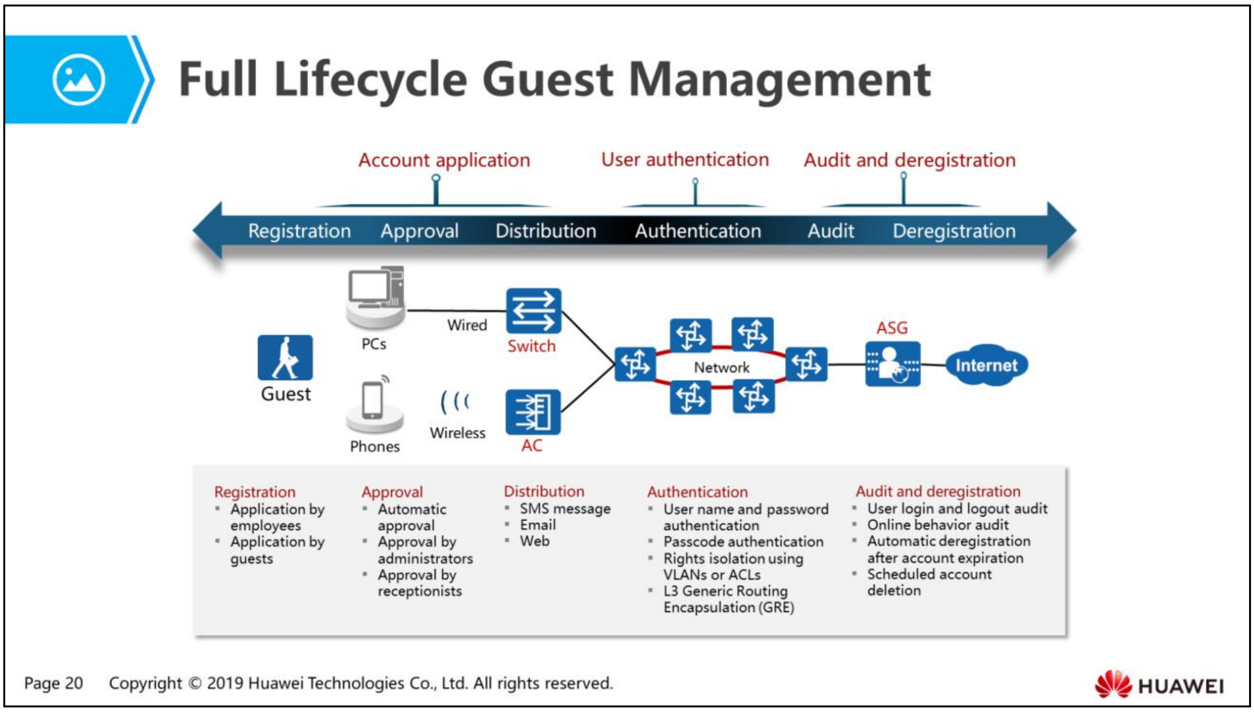
- Who are guests?
  - Non-employees in enterprises
  - Customers who visit enterprises or outsourcing employees from partners
  - Consumers of enterprises
  - Common people
- What characteristics do guests have?
  - Network access using their own terminals
  - Uncontrollable online behavior
  - Uncontrollable network access scope

Typical guest access scenarios

- Large-sized enterprises
  - Typical enterprises: Huawei, Lenovo, etc.
  - Typical scenarios: Customers access enterprise networks, enterprises' public resources, or the Internet during communication and visits.
- Public utilities
  - Typical units: subways, airports, etc.
  - Typical scenarios: People access the Internet through networks provided by public utilities.
- Consumption enterprises
  - Typical enterprises: luxury hotels, coffee shops, etc.
  - Typical scenarios: Consumers of enterprises need to access the Internet.

Guest Authentication System Panorama





Full Lifecycle Guest Management

Registration
- Application by employees
- Application by guests

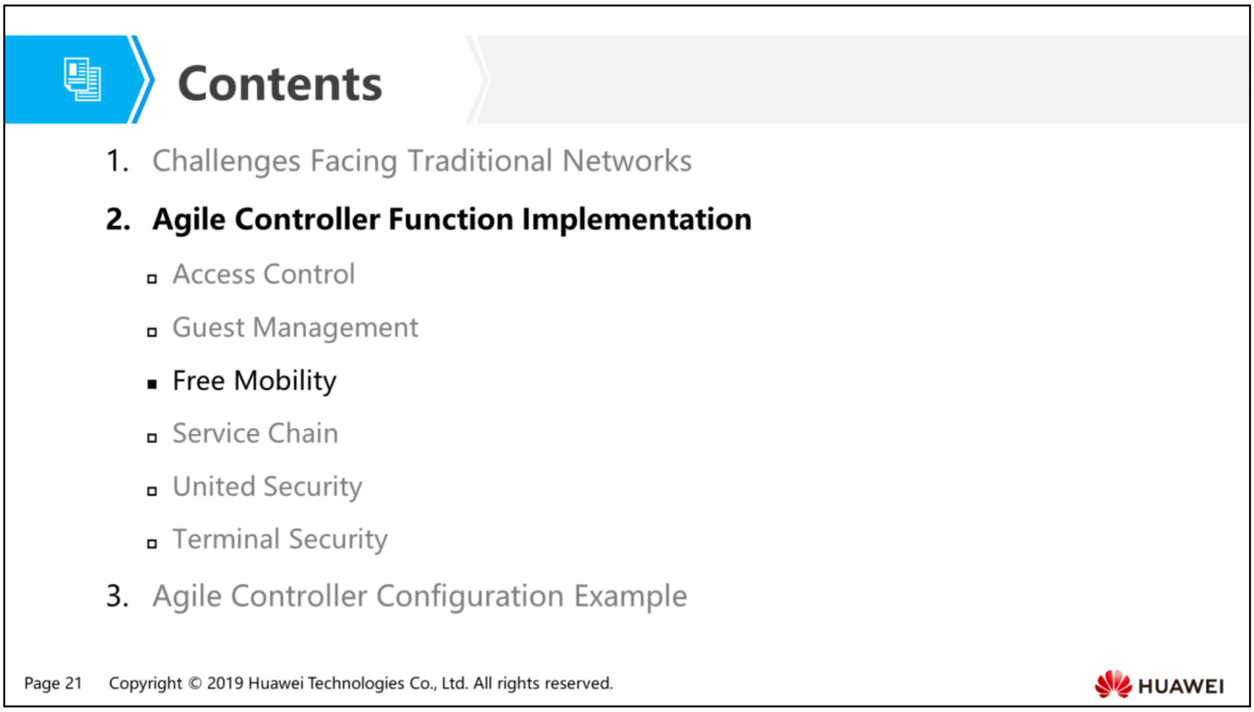
Approval
- Automatic approval
- Approval by administrators
- Approval by receptionists

Distribution
- SMS message
- Email
- Web

Authentication
- User name and password authentication
- Passcode authentication
- Rights isolation using VLANs or ACLs
- L3 Generic Routing Encapsulation (GRE)

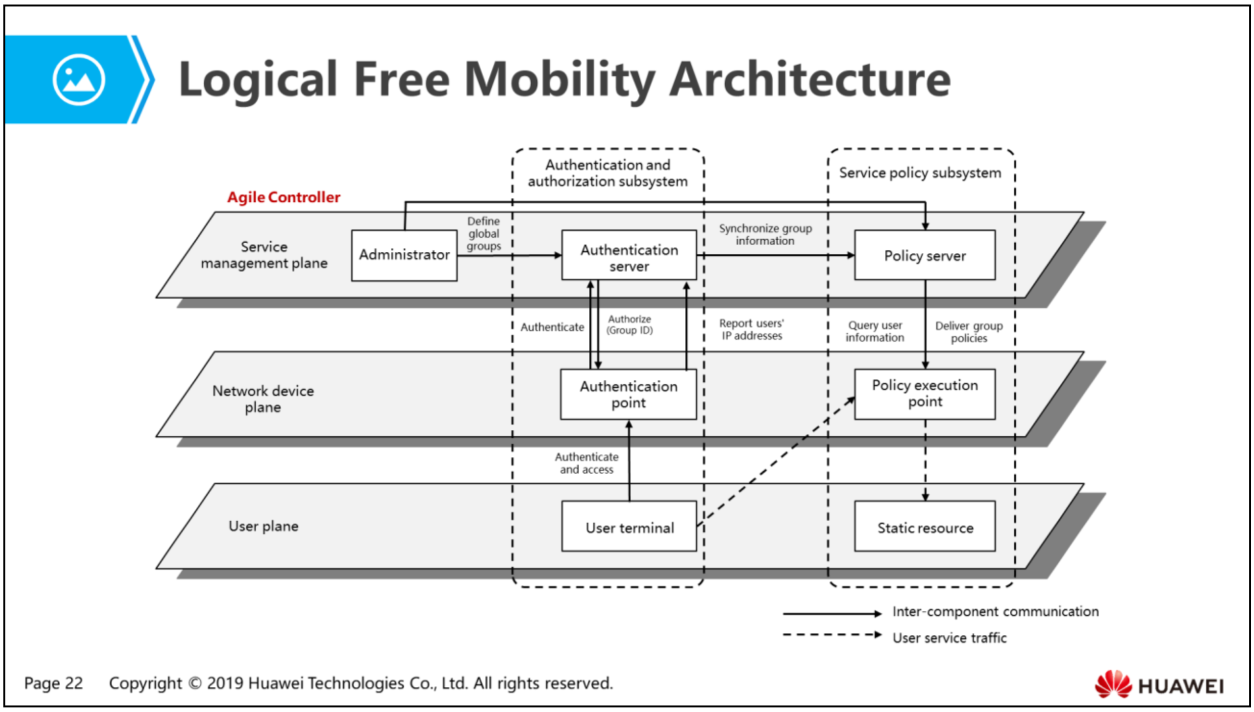
Audit and deregistration
- User login and logout audit
- Online behavior audit
- Automatic deregistration after account expiration
- Scheduled account deletion

- The Agile Controller provides the full lifecycle guest management function, covering management of guest account application, approval, distribution, authentication, and deregistration. This function has the following characteristics:
  - Allows guests to access networks using bring your own devices (BYODs) and multiple types of terminals such as PCs, tablets, iPhones, and Android terminals.
  - Supports full lifecycle management covering guest account registration, approval, distribution, and deregistration.
  - Supports authentication page customization and push based on IP addresses and access locations, and flexibly displays advertisements.
  - Supports 5W1H-based guest access authorization to strictly control access rights of guests.
  - Supports guest login, logout, and network behavior audit.



Contents

1. Challenges Facing Traditional Networks
2. **Agile Controller Function Implementation**
   - Access Control
   - Guest Management
   - Free Mobility
   - Service Chain
   - United Security
   - Terminal Security
3. Agile Controller Configuration Example



Logical Free Mobility Architecture

Agile Controller

Authentication and authorization subsystem

Service policy subsystem

Service management plane

Administrator

Define global groups

Authentication server

Synchronize group information

Policy server

Authenticate

Authorize (Group ID)

Report users' IP addresses

Query user information

Deliver group policies

Network device plane

Authentication point

Policy execution point

Authenticate and access

User plane

User terminal

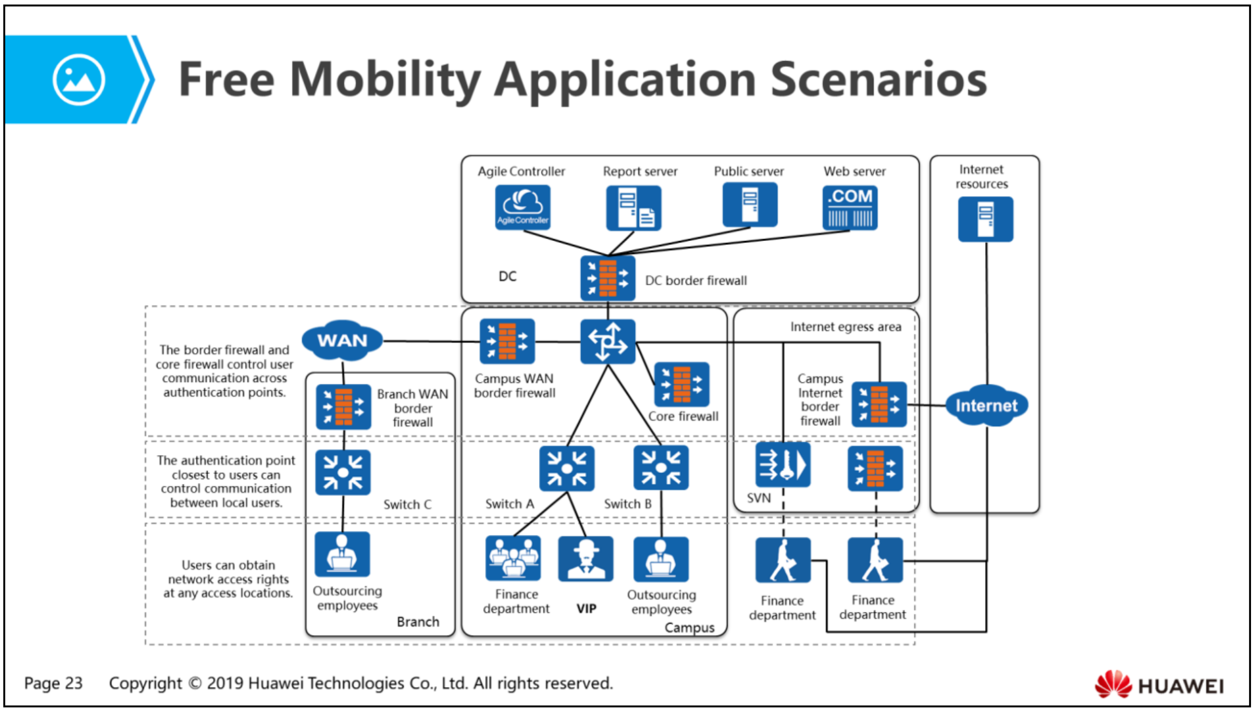
Static resource

Inter-component communication

User service traffic

HUAWEI

- In the above figure, the authentication server contains the RADIUS, Portal, and AuthServer components of the Agile Controller server, and the policy server contains the NetworkServer component.

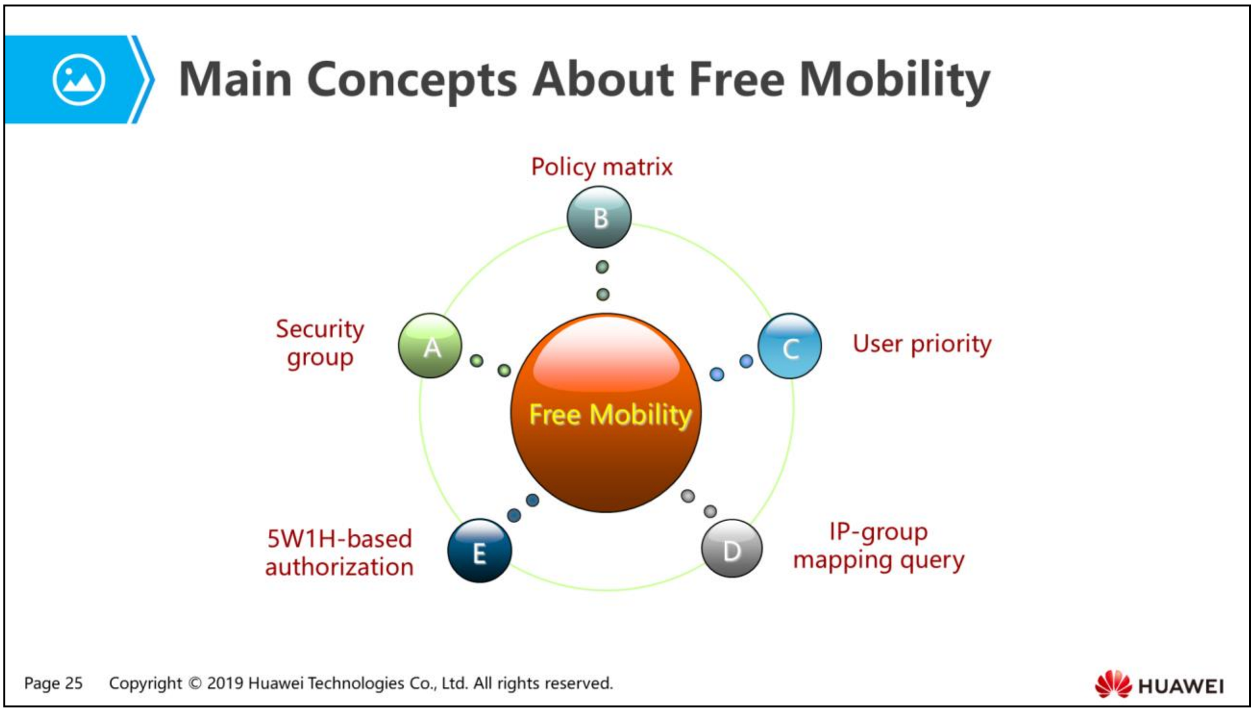


Free Mobility Application Scenarios

Agile Controller
Report server
Public server
Web server
.COM
DC
DC border firewall
Internet resources
The border firewall and core firewall control user communication across authentication points.
WAN
Campus WAN border firewall
Core firewall
Internet egress area
Campus Internet border firewall
Internet
Branch WAN border firewall
The authentication point closest to users can control communication between local users.
Switch C
Switch A
Switch B
SVN
Users can obtain network access rights at any access locations.
Outsourcing employees
Branch
Finance department
VIP
Outsourcing employees
Campus
Finance department
Finance department

- Free Mobility of the Agile Controller is applicable to the following scenarios:
    - Data center access rights control:
        - Automatic policy deployment: The Agile Controller uniformly and automatically deploys access policies to grant rights for employees in each department to access server resources in the DC. The administrator only needs to pay attention to inter-group access relationship design and selects key devices on the campus network as policy execution points (authentication switches, core firewalls, and border firewalls/SVN devices). After the initial configuration is complete, users can obtain network access rights regardless of the access location or mode.
    - Inter-user communication control:
        - Cross-team collaborative work: As shown in the above figure, using the automatic policy deployment function based on IP addresses, the administrator can enable outsourcing employees and financial personnel to work collaboratively and ensure that each user can have correct network access rights, without the need of modifying any configurations. The administrator can control data sharing to ensure security of enterprise data.

- VIP user experience assurance:
  - Egress route selection: At the WAN and Internet egresses, egress routes with different quality assurance can be selected based on source and destination groups.
  - Preferential access of users on a virtual private network over Secure Sockets Layer (SSL VPN): When the SVN gateway resources are limited, automatic gateway selection and preferential access of VIP users ensure that VIP users can access the nearest SVN gateway and enjoy the optimal network experience.



Main Concepts About Free Mobility

Free Mobility

A Security group

B Policy matrix

C User priority

D IP-group mapping query

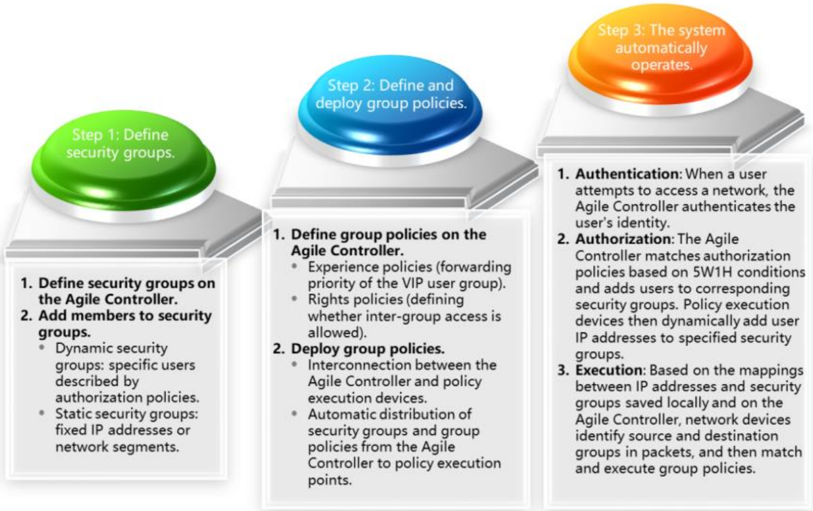
E 5W1H-based authorization

Page 25

HUAWEI

- Security group: On an agile network, a security group identifies the source and destination of a traffic flow.
- There are two types of security groups:
  - User security group: Members in a user security group include users and dumb terminals that access a network. The binding relationship between a group and IP addresses of members in the group is determined during authentication.
  - Resource security group: Members in a resource security group include static network segments or server resources on a network. IP addresses of members in a group need to be bound manually to the group.
- Policy matrix: A policy matrix defines whether a security group (such as a user group) has rights to access another security group (such as a server group).
- User priority: The forwarding priority of a security group to which VIP users belong can be defined to ensure the network access experience of these VIP users.
- 5W1H-based authorization: User security groups are not equal to user departments or roles. User security groups are dynamically planned for users based on 5W1H (Who, Where, When, Whose, What, and How).
- IP-group mapping query: Policies are defined based on security groups but not authentication point devices. These policies cannot identify the security group to which an IP address or a user belongs. The IP-group mapping query function is needed to obtain the mappings between IP addresses and security groups, so that correct policies can be implemented based on security groups.

Free Mobility Deployment Procedure



Step 1: Define security groups.

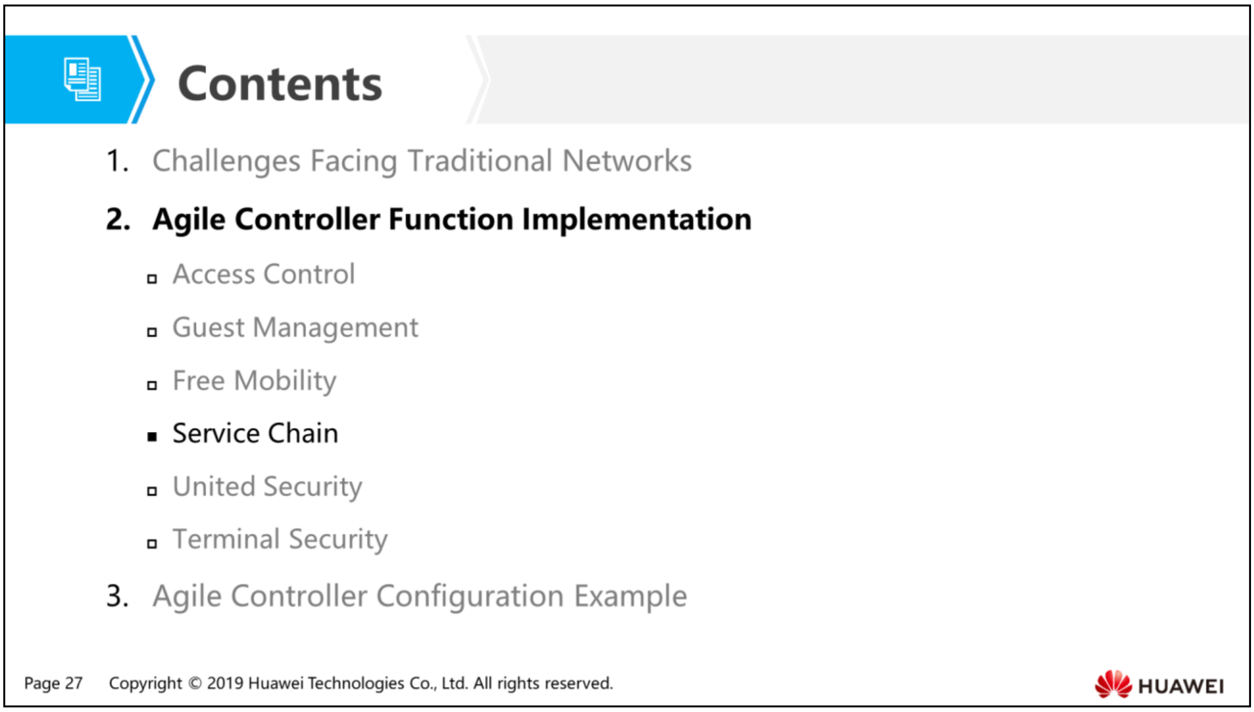
1. **Define security groups on the Agile Controller.**
2. **Add members to security groups.**
   - Dynamic security groups: specific users described by authorization policies.
   - Static security groups: fixed IP addresses or network segments.

Step 2: Define and deploy group policies.

1. **Define group policies on the Agile Controller.**
   - Experience policies (forwarding priority of the VIP user group).
   - Rights policies (defining whether inter-group access is allowed).
2. **Deploy group policies.**
   - Interconnection between the Agile Controller and policy execution devices.
   - Automatic distribution of security groups and group policies from the Agile Controller to policy execution points.

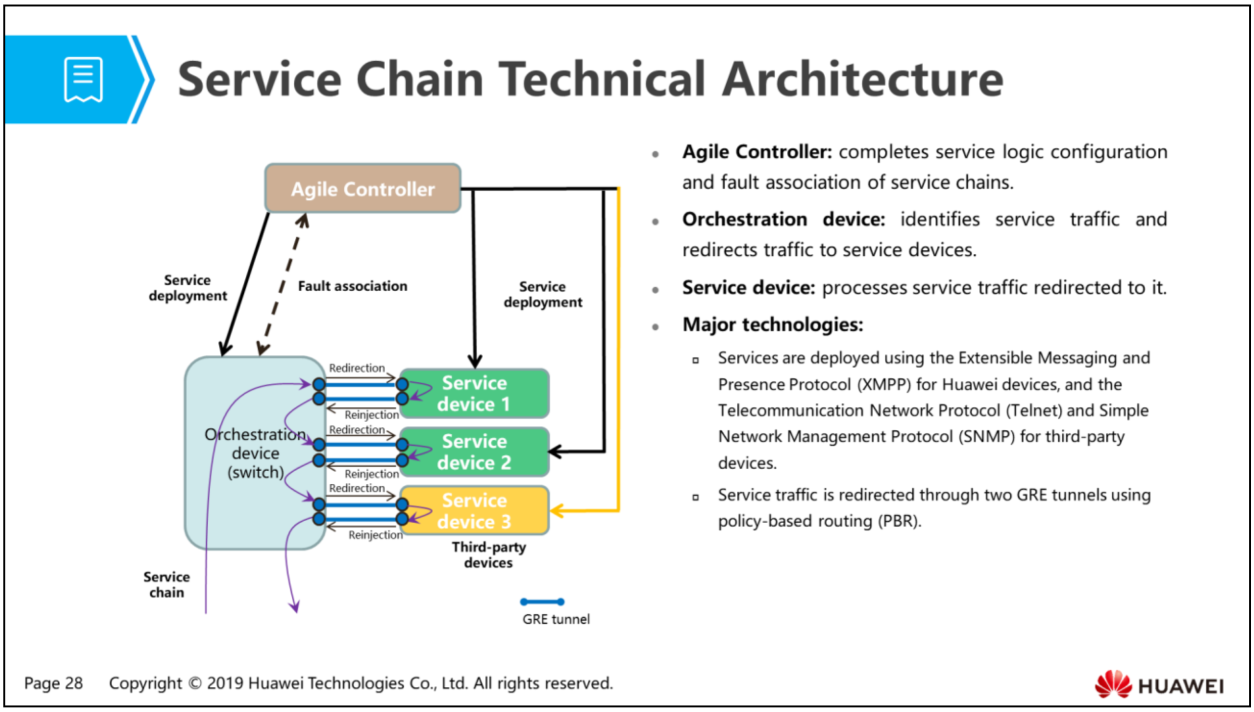
Step 3: The system automatically operates.

1. **Authentication**: When a user attempts to access a network, the Agile Controller authenticates the user's identity.
2. **Authorization**: The Agile Controller matches authorization policies based on 5W1H conditions and adds users to corresponding security groups. Policy execution devices then dynamically add user IP addresses to specified security groups.
3. **Execution**: Based on the mappings between IP addresses and security groups saved locally and on the Agile Controller, network devices identify source and destination groups in packets, and then match and execute group policies.



Contents

1. Challenges Facing Traditional Networks
2. **Agile Controller Function Implementation**
   - Access Control
   - Guest Management
   - Free Mobility
   - Service Chain
   - United Security
   - Terminal Security
3. Agile Controller Configuration Example

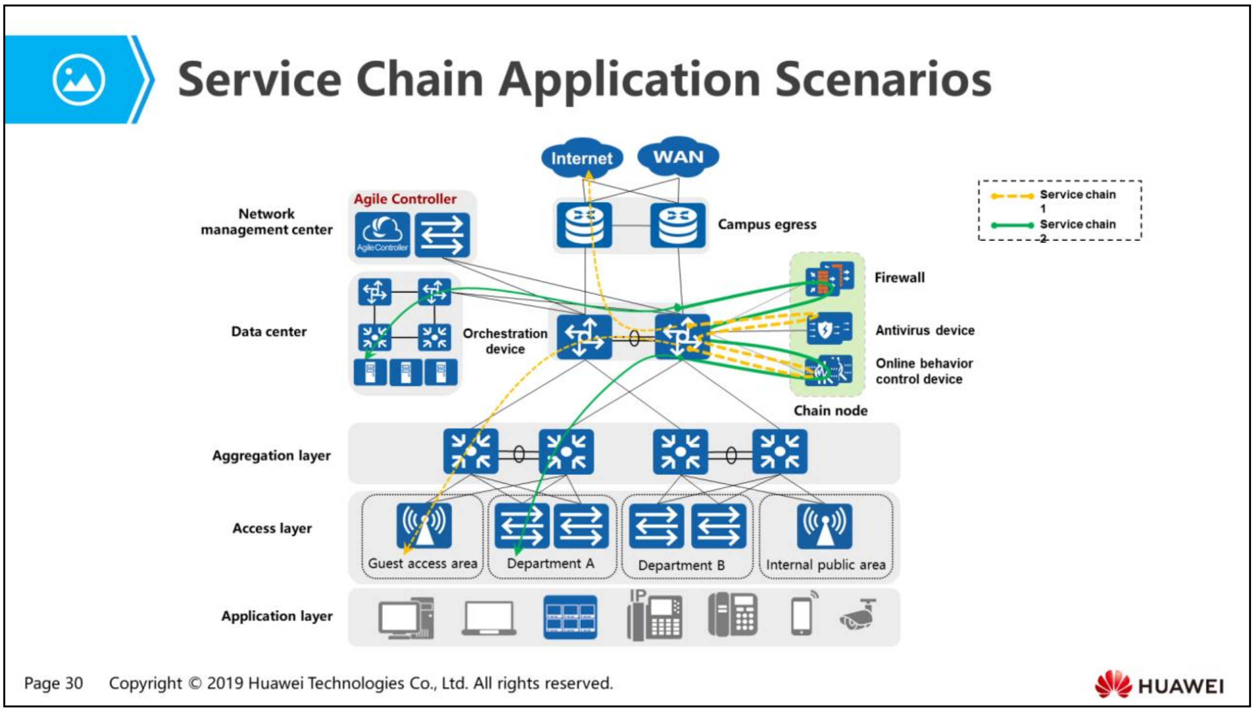


Service Chain Technical Architecture

- **Agile Controller:** completes service logic configuration and fault association of service chains.
- **Orchestration device:** identifies service traffic and redirects traffic to service devices.
- **Service device:** processes service traffic redirected to it.
- **Major technologies:**
  - Services are deployed using the Extensible Messaging and Presence Protocol (XMPP) for Huawei devices, and the Telecommunication Network Protocol (Telnet) and Simple Network Management Protocol (SNMP) for third-party devices.
  - Service traffic is redirected through two GRE tunnels using policy-based routing (PBR).

- Basic concepts about service chain:
  - ACL: refers to a collection of orderly rules used by a device to filter network traffic. These rules are described based on source addresses, destination addresses, and port numbers of data packets.
  - UCL: refers to a user level–based access control list. Rules in a UCL are defined based on source security groups, destination security groups, and port numbers of data packets.
  - Service flow: refers to network traffic that matches a certain ACL or UCL rule.
  - Orchestration device: orderly redirects service flows, which is usually a switch.
  - Service device: performs security processing on service flows imported by an orchestration device. Service devices include firewalls, antivirus devices, and online behavior control devices.
  - GRE tunnel: refers to a P2P virtual connection for transmitting encapsulated data packets. The devices at the two ends of a GRE tunnel encapsulate and decapsulate data packets respectively, and set up a data transmission channel between an orchestration device and a service device.
  - Service chain resource: refers to orchestration devices, service devices, and GRE tunnels between them.
  - Service chain: refers to ordered links established between orchestration devices and service devices for processing service flows.

    - XMPP (originally named Jabber) is an open real-time communication protocol based on the Extensible Markup Language (XML), and contains a series of Internet standards including RFC 3920, RFC 3921, RFC3922, and RFC3923 approved by the Internet Engineering Task Force (IETF).
        - XMPP defines three roles: client, server, and gateway. Bidirectional communication between any two roles is supported. A server records client information, manages connections, and forwards information. A gateway interconnects with a heterogeneous instant messaging system such as the SMS, MSN, and ICQ system. In basic networking, a single client uses TCP/IP to connect to a single server and transmits XML files.
        - Transport Layer Security (TLS) can be used to ensure secure XMPP transmission. The simple authentication and security layer (SASL) can be added to support XMPP authentication. XMPP message communication starts only after authentication succeeds.
- The service chain function of the Agile Controller has the following advantages:
    - The Service Chain Manager can specify policies for specified group traffic on network access devices, schedule traffic in a specific orchestration sequence, and define the traffic that needs to be processed by security devices and the processing sequence. Generally, user traffic from insecure areas and guest traffic needs to be scheduled to the security resource center for detection.
    - The Service Chain Manager virtualizes physical devices' capabilities to virtual services to shield physical device models, and redirects service traffic to corresponding service termination nodes.
    - The Agile Controller allows administrators to configure an independent service device as a chain node, which can have a bypass device deployed to improve reliability. Each service chain can have a maximum of four nodes. Service traffic redirection based on security groups is also supported. On the Agile Controller, administrators can define service flows based on source user groups (source IP address segments), destination resource groups (destination IP address segments), source resource groups, and destination user groups. Administrators can define service flows that need to be filtered by security devices.



Service Chain Application Scenarios

Page 30 Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

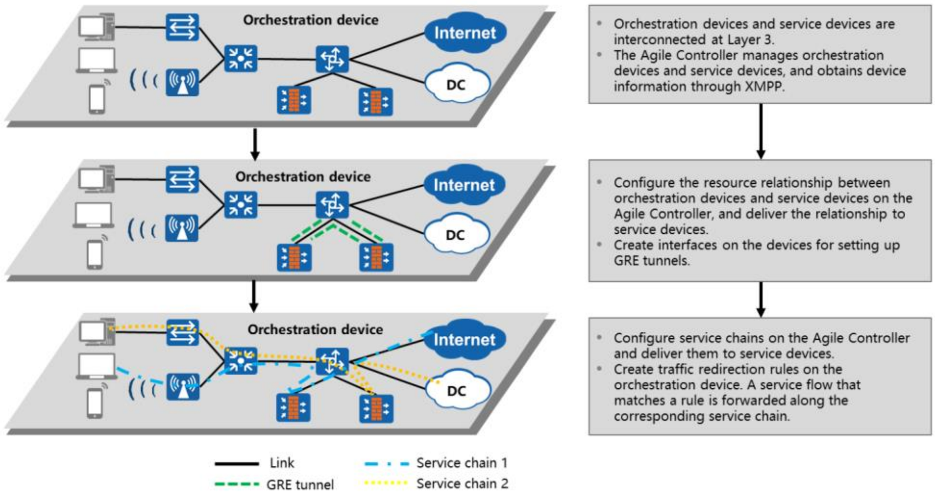
- Traditional serial connection of service devices faces the following problems:
  - Service traffic cannot be flexibly scheduled.
  - Service devices require high performance and are complex to manage.
  - Device replacement or upgrade is complex.
- The Service Chain Manager solves these problems and provides the following advantages:
  - Flexible networking: Service chains based on L3 GRE tunnels allow more flexible networking and deployment of service devices.
  - Visualized orchestration and simplified management: Service orchestration on virtualized topologies simplifies configuration and facilitates management.
  - Easy expansion: Service devices can be added or deleted without changing forwarding routes or physical topologies of the live network.
- In the above networking, to ensure network security, administrators expect that data flows from users of department A to the data center and from guests to the Internet can be processed by security service devices. Network administrators need to perform the following service chain configurations:
  - Create service flows.
    - Define ACL or UCL rules for data flows from users of department A to the data center and from guests to the Internet.

- Create and deploy service chain resources.
  - Configure core switches as orchestration devices, and firewalls, antivirus devices, and online behavior control devices as service devices.
  - Set up bidirectional GRE tunnels between orchestration devices and service devices to ensure proper data communication.
- Create and deploy service chains.
  - A service chain consists of service flows as well as the orchestration devices and service devices through which the service flows pass.
  - After the service chains are created and deployed, core switches will orderly redirect data flows from users of department A to the data center or from guests to the Internet to corresponding service devices for security processing.

In the figure, the orange lines indicate data flows from guests to the Internet. When passing through the core switch, the service flows are redirected to the online behavior control device and then the antivirus device.

The green lines indicate data flows from users of department A to the data center. When passing through the core switch, the service flows are redirected to the online behavior control device and then the firewall.

Service Chain Procedure



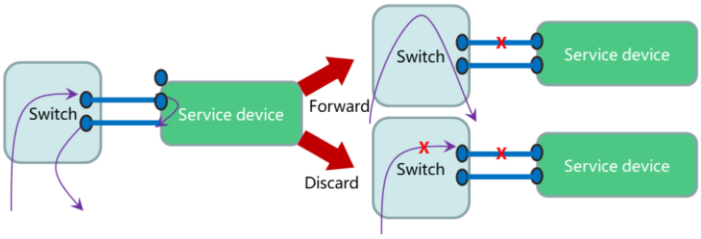
- Orchestration devices and service devices are interconnected at Layer 3.
- The Agile Controller manages orchestration devices and service devices, and obtains device information through XMPP.

- Configure the resource relationship between orchestration devices and service devices on the Agile Controller, and deliver the relationship to service devices.
- Create interfaces on the devices for setting up GRE tunnels.

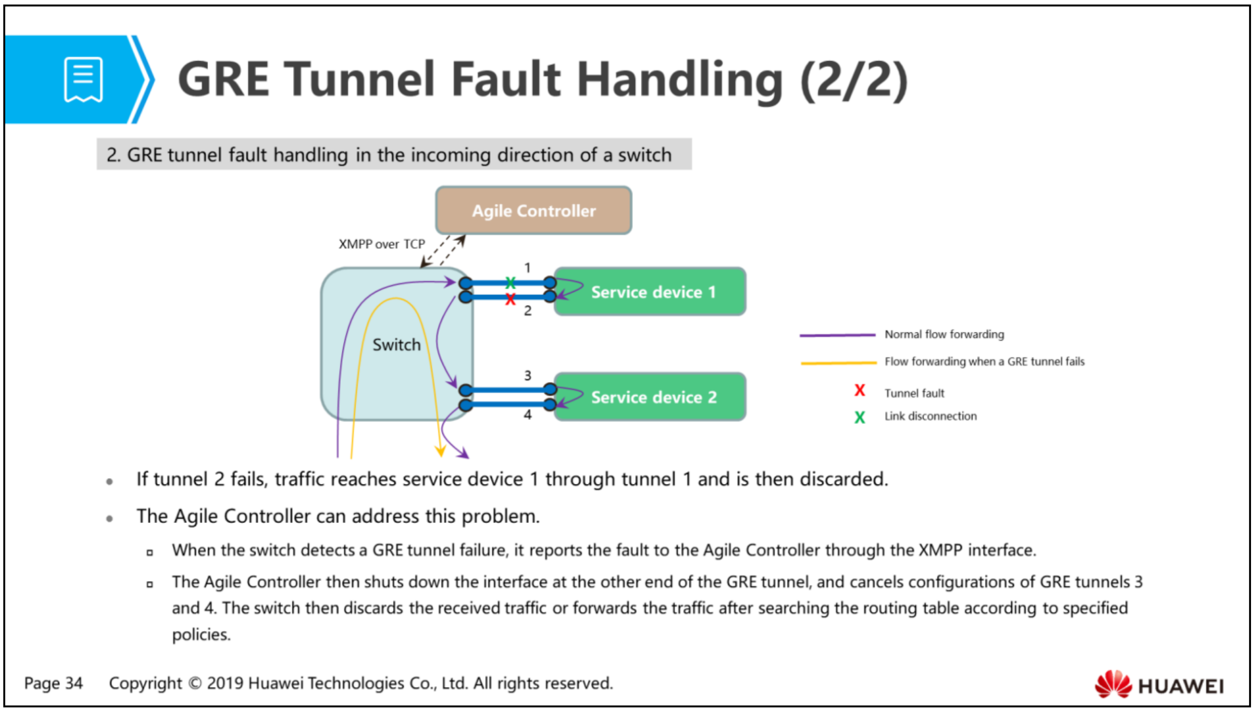
- Configure service chains on the Agile Controller and deliver them to service devices.
- Create traffic redirection rules on the orchestration device. A service flow that matches a rule is forwarded along the corresponding service chain.

GRE Tunnel Fault Handling (1/2)

1. GRE tunnel fault handling in the outgoing direction of a switch



- Troubleshooting:
  - GRE tunnel Keepalive mechanism: This mechanism is enabled on a GRE tunnel by default.
  - GRE tunnel fault troubleshooting: To improve reliability of service chains, configure the switch to discard or directly forward packets when a GRE tunnel fails.



GRE Tunnel Fault Handling (2/2)

2. GRE tunnel fault handling in the incoming direction of a switch

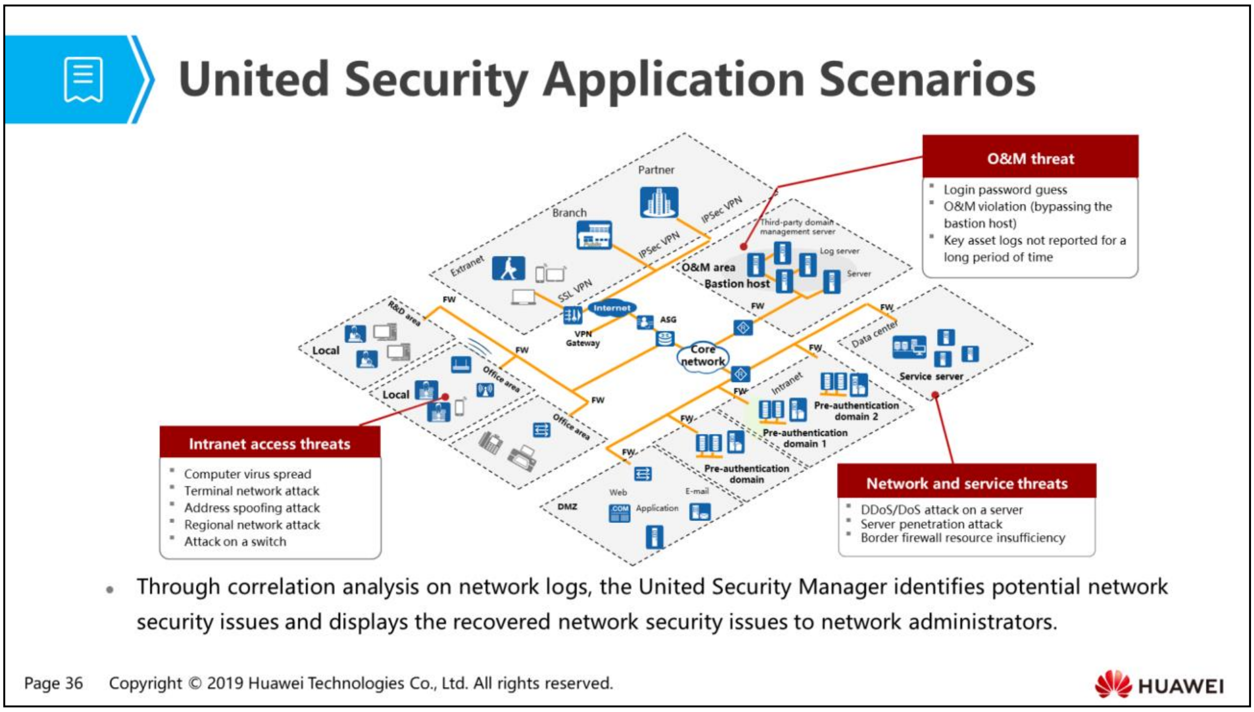
- If tunnel 2 fails, traffic reaches service device 1 through tunnel 1 and is then discarded.
- The Agile Controller can address this problem.
  - When the switch detects a GRE tunnel failure, it reports the fault to the Agile Controller through the XMPP interface.
  - The Agile Controller then shuts down the interface at the other end of the GRE tunnel, and cancels configurations of GRE tunnels 3 and 4. The switch then discards the received traffic or forwards the traffic after searching the routing table according to specified policies.

HUAWEI

- The normal fault handling process is as follows:
  - When a GRE tunnel fails as shown in the figure, the switch redirects received traffic to a specified tunnel interface according to the matched rules and then forwards the traffic to the application security gateway through GRE tunnel 1.
  - After processing the traffic, service device 1 redirects the traffic to a specified tunnel interface and returns the traffic to the switch through GRE tunnel 2.
  - The switch redirects the service traffic received through GRE tunnel 2 to the interface where GRE tunnel 3 resides, and then forwards the traffic to service device 2. In this way, service traffic is processed by service device 2 and then returned to the switch.
  - After the switch receives the service traffic through GRE tunnel 4, it forwards the traffic to the external network according to the routing table because the traffic does not need to be processed by other service devices.

Contents

1. Challenges Facing Traditional Networks
2. **Agile Controller Function Implementation**
   - Access Control
   - Guest Management
   - Free Mobility
   - Service Chain
   - United Security
   - Terminal Security
3. Agile Controller Configuration Example



United Security Application Scenarios

O&M threat

- Login password guess
- O&M violation (bypassing the bastion host)
- Key asset logs not reported for a long period of time

Intranet access threats

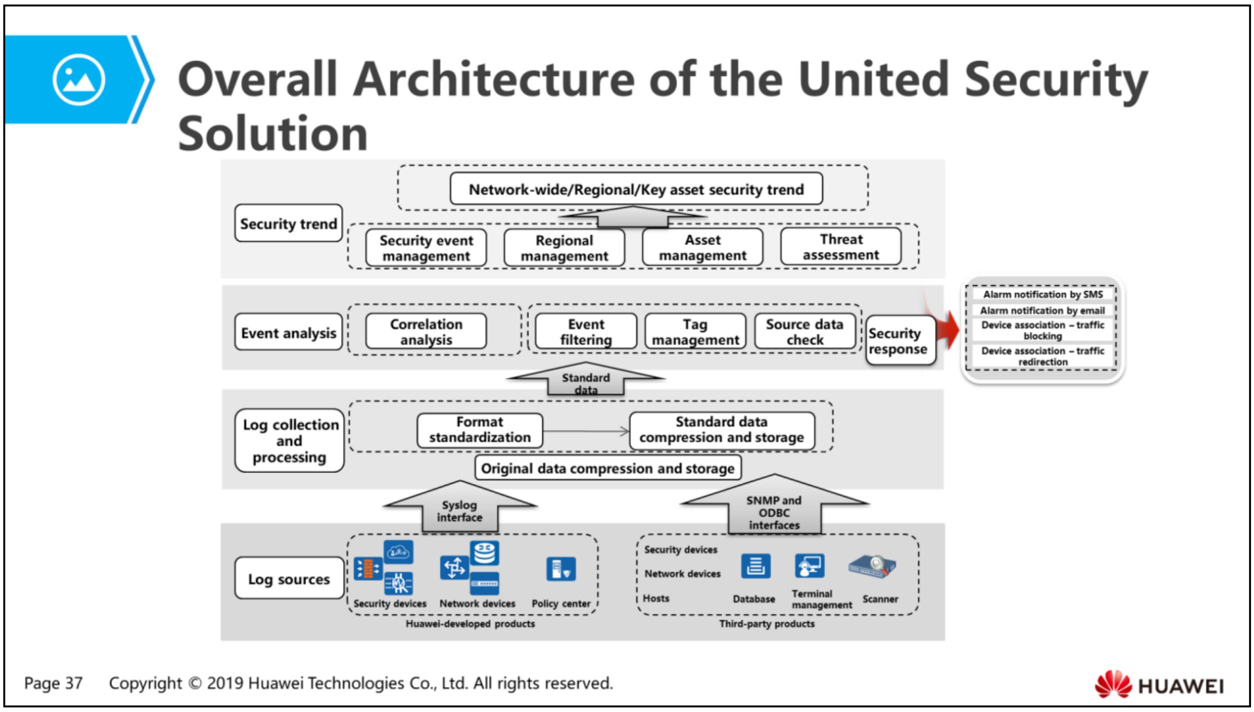
- Computer virus spread
- Terminal network attack
- Address spoofing attack
- Regional network attack
- Attack on a switch

Network and service threats

- DDoS/DoS attack on a server
- Server penetration attack
- Border firewall resource insufficiency

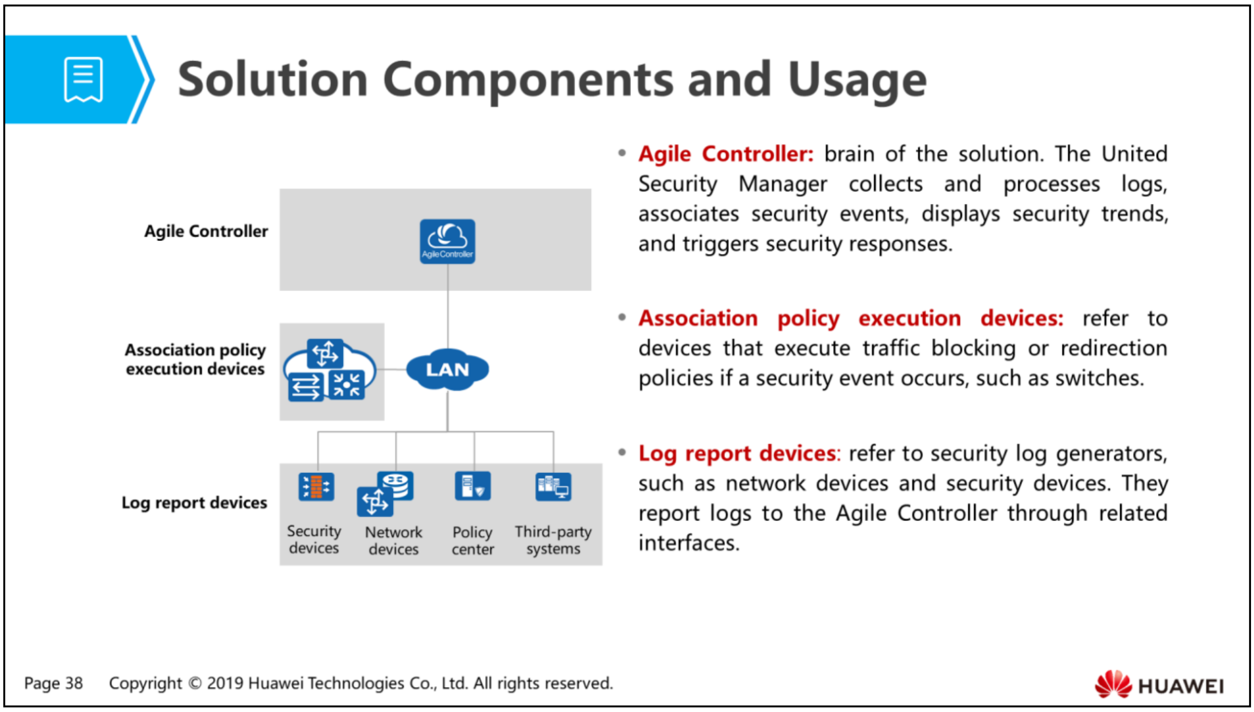
- Through correlation analysis on network logs, the United Security Manager identifies potential network security issues and displays the recovered network security issues to network administrators.

- Administrators can add assets to the United Security Manager to implement unified management and control. Through correlation analysis on asset report logs, the United Security Manager helps administrators identify potential security threats on networks, and displays security trends in network topologies or lists to administrators, helping them easily obtain security status of all assets and build secure networks.
- Bastion hosts are deployed in a specific network environment to defend networks and data against internal and external intrusions and attacks. Bastion hosts use various techniques to monitor and collect information in real time, including the system status, security events, and network activities of each component in the network environment. Bastion hosts record, analyze, and process the information, and then centrally report alarms.



Overall Architecture of the United Security Solution

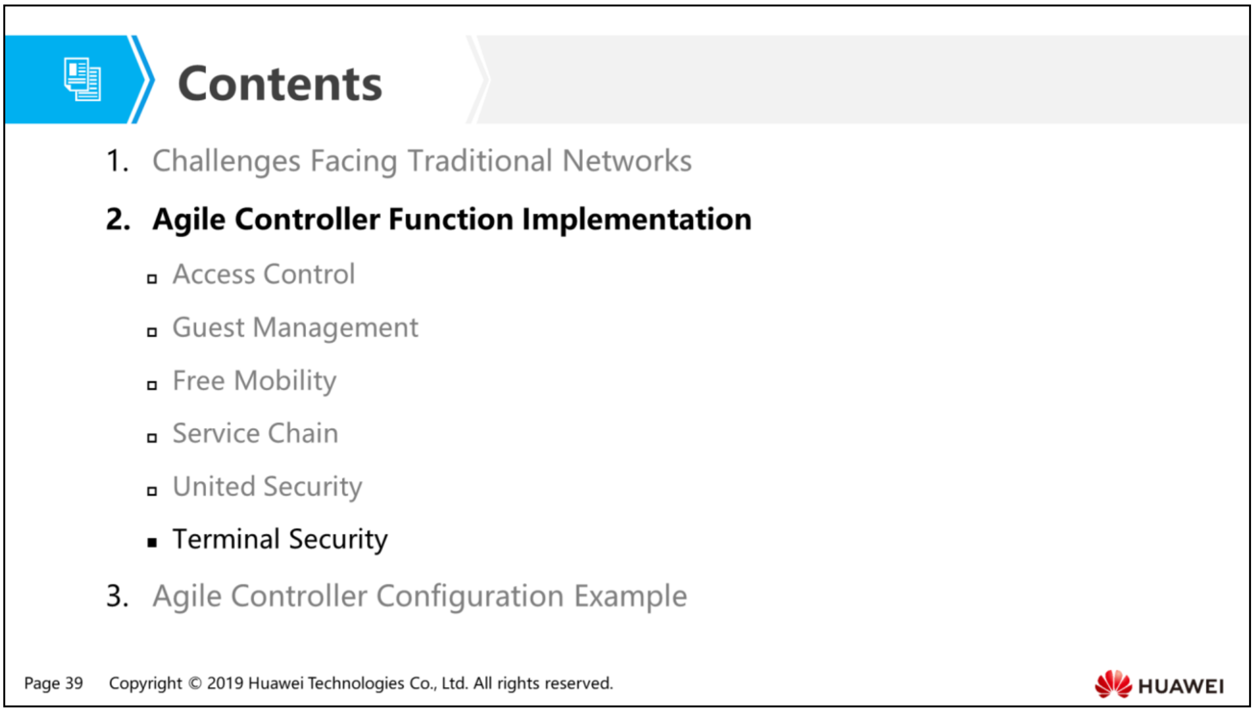
- This United Security solution architecture is composed of the following:
  - Log sources: refer to devices or servers providing log information. In this solution, logs of Huawei-developed devices are collected and processed. Logs of third-party devices can also be collected. For details, see the list of devices supporting log collection in the product documentation.
  - Log collection and processing: After log sources provide log information to the log collection and processing layer through corresponding interfaces, original logs are compressed, standardized, and stored. Logs are standardized to improve data processing efficiency.
  - Event analysis: Standardized data and configured correlation rules are calculated by the correlation analysis engine to obtain valuable security threat events. Security response measures are taken to handle security events, including sending alarms (by SMS and email) and device association (traffic blocking and redirection).
  - Security trend: Based on security events on an entire network, the Agile Controller can take regional management, asset management, threat assessment, and other measures to obtain security trends of key assets, regions, and the overall network.



Solution Components and Usage

- **Agile Controller:** brain of the solution. The United Security Manager collects and processes logs, associates security events, displays security trends, and triggers security responses.
- **Association policy execution devices:** refer to devices that execute traffic blocking or redirection policies if a security event occurs, such as switches.
- **Log report devices**: refer to security log generators, such as network devices and security devices. They report logs to the Agile Controller through related interfaces.

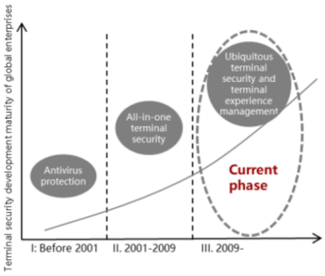
- The following components are used in the United Security solution:
  - Log report devices: devices deployed on networks which provide network and security logs, such as network devices, security devices, policy servers, and third-party systems.
  - Association policy execution devices: switches. They trigger security responses for device association if a security event occurs, and execute traffic blocking or redirection policies.
  - Agile Controller: brain of the solution. This solution uses the United Security Manager of the Agile Controller to collect and process logs, associate events, display security trends, and trigger security responses.



Contents

1. Challenges Facing Traditional Networks
2. **Agile Controller Function Implementation**
   - Access Control
   - Guest Management
   - Free Mobility
   - Service Chain
   - United Security
   - Terminal Security
3. Agile Controller Configuration Example

Current Situation and Development Trend of Terminal Security Management



- Before 2001, antivirus and anti-spy software technologies were used for terminal security management. As technologies develop and security threats diversify, terminal security events occur frequently. As a result, users do not trust antivirus software and concern that antivirus software may outdated.
- Between 2001 and 2009, **one-in-all terminal security solutions** involving access control, terminal security, and terminal behavior management and control were developed to replace simple antivirus protection.
- After 2009, as the number of mobile office users grows rapidly, the terminal security management scope is extended from only PC management to **unified management on ubiquitous terminals** including smart terminals and IP devices. Terminal security management is no longer event-driven but focuses on **proactive defense, comprehensive prevention, and improved experience**.

Terminal Security Management Development Trends

Ubiquitous terminals

- Unified management of various types of terminals
- Unified management of physical and virtual terminals

Full functions

- Access control + security management
- Passive defense + proactive control

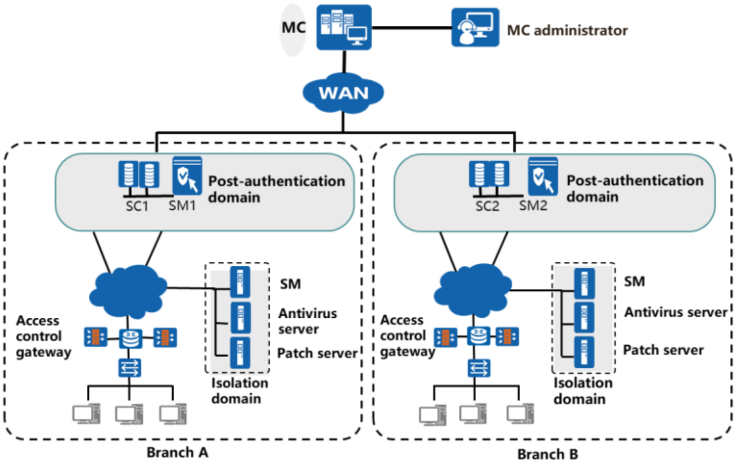
Platform-based

- Network-wide association and collaboration
- Open integration capabilities

Personalized

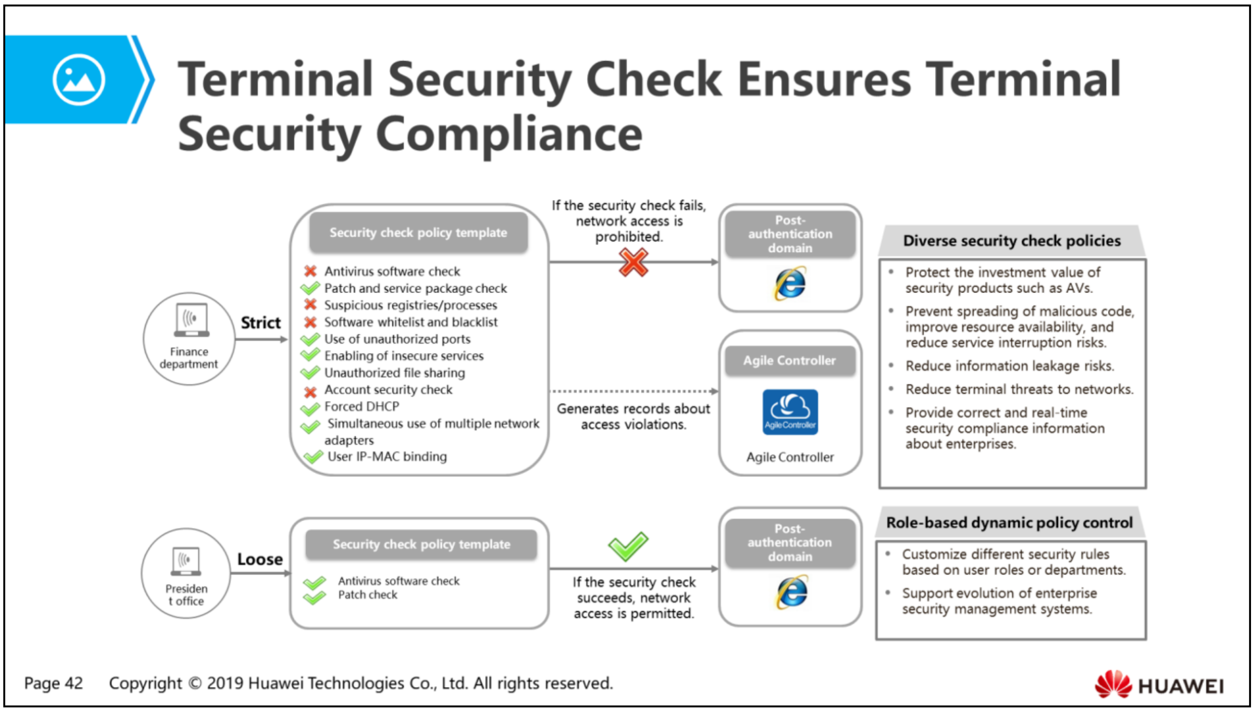
- Desktop manager application
- Desktop user services

Terminal Security Technical Architecture



Multi-level Management Model

- Security policies can be centrally configured on the MC and delivered to lower-level terminal security management servers.
- Terminal security clients check terminals based on the delivered security policies. If the check succeeds, terminal security management servers instruct access control gateways to grant network access permission to the terminals. If the check fails, the servers isolate the terminals for repair.



Terminal Security Check Ensures Terminal Security Compliance

Finance department

Strict

Security check policy template

- ✗ Antivirus software check
- ✓ Patch and service package check
- ✗ Suspicious registries/processes
- ✗ Software whitelist and blacklist
- ✓ Use of unauthorized ports
- ✓ Enabling of insecure services
- ✓ Unauthorized file sharing
- ✗ Account security check
- ✓ Forced DHCP
- ✓ Simultaneous use of multiple network adapters
- ✓ User IP-MAC binding

If the security check fails, network access is prohibited.

Post-authentication domain

Generates records about access violations.

Agile Controller

Agile Controller

Presiden t office

Loose

Security check policy template

- ✓ Antivirus software check
- ✓ Patch check

If the security check succeeds, network access is permitted.

Post-authentication domain

Diverse security check policies

- Protect the investment value of security products such as AVs.
- Prevent spreading of malicious code, improve resource availability, and reduce service interruption risks.
- Reduce information leakage risks.
- Reduce terminal threats to networks.
- Provide correct and real-time security compliance information about enterprises.

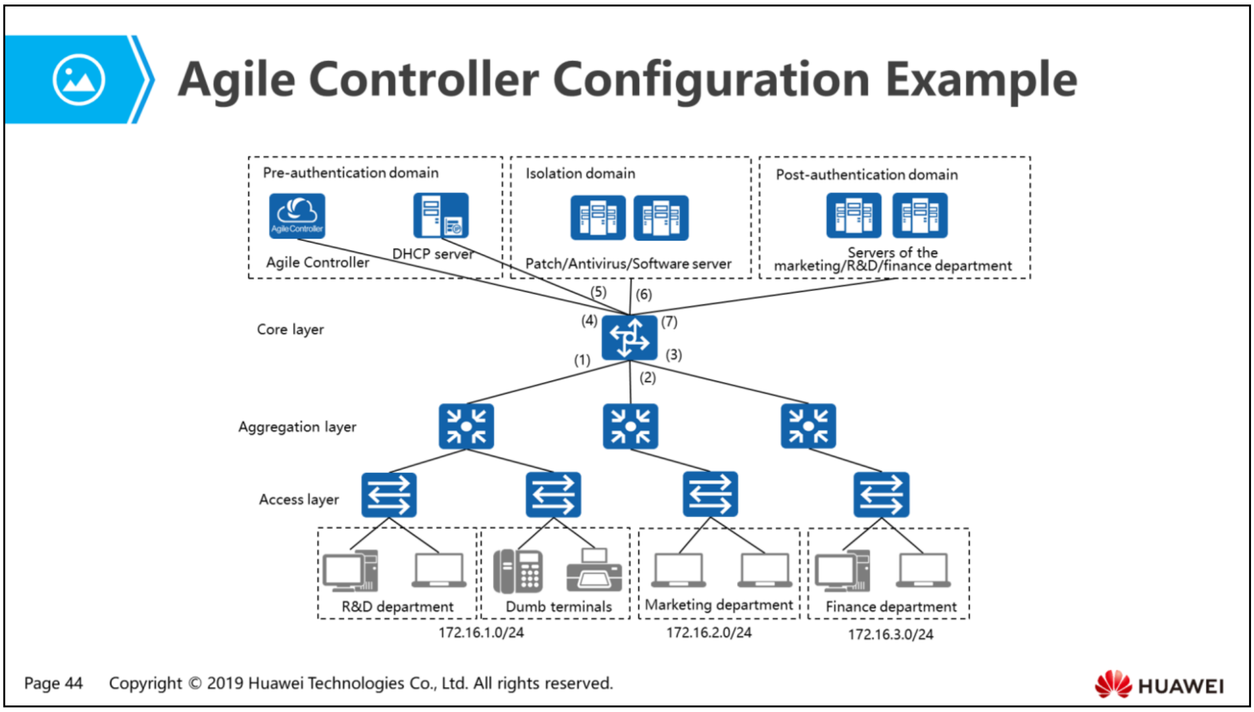
Role-based dynamic policy control

- Customize different security rules based on user roles or departments.
- Support evolution of enterprise security management systems.

- Terminal security management has the following characteristics:
    - One-click repair, lowering terminal management and maintenance costs.
        - If terminals do not comply with enterprise security policies, automatic repair is required. Currently, automatic repair can be achieved for terminal violations. Users can repair terminals quickly through one-click.
    - Desktop security standardization, reducing virus infection risks.
        - Only standard software is allowed to install on the desktop.
        - Unauthorized web access is prohibited to improve work efficiency.
        - Installation of non-standard software is prevented to reduce virus infection risks.
    - Terminal peripheral device management and behavior monitoring.
        - Information leakage from terminals is prevented. Access control is implemented to ensure that network access terminals have clients installed and comply with security requirements. The use of peripheral devices and online behavior are monitored to prevent information leakage. Comprehensive audit is provided to meet post-event audit requirements.

Contents

1. Challenges Facing Traditional Networks
2. Agile Controller Function Implementation
3. **Agile Controller Configuration Example**



Agile Controller Configuration Example

Pre-authentication domain

Agile Controller

DHCP server

Isolation domain

Patch/Antivirus/Software server

Post-authentication domain

Servers of the marketing/R&D/finance department

(5)

(6)

(4)

(7)

(1)

(3)

(2)

Core layer

Aggregation layer

Access layer

R&D department

Dumb terminals

Marketing department

Finance department

172.16.1.0/24

172.16.2.0/24

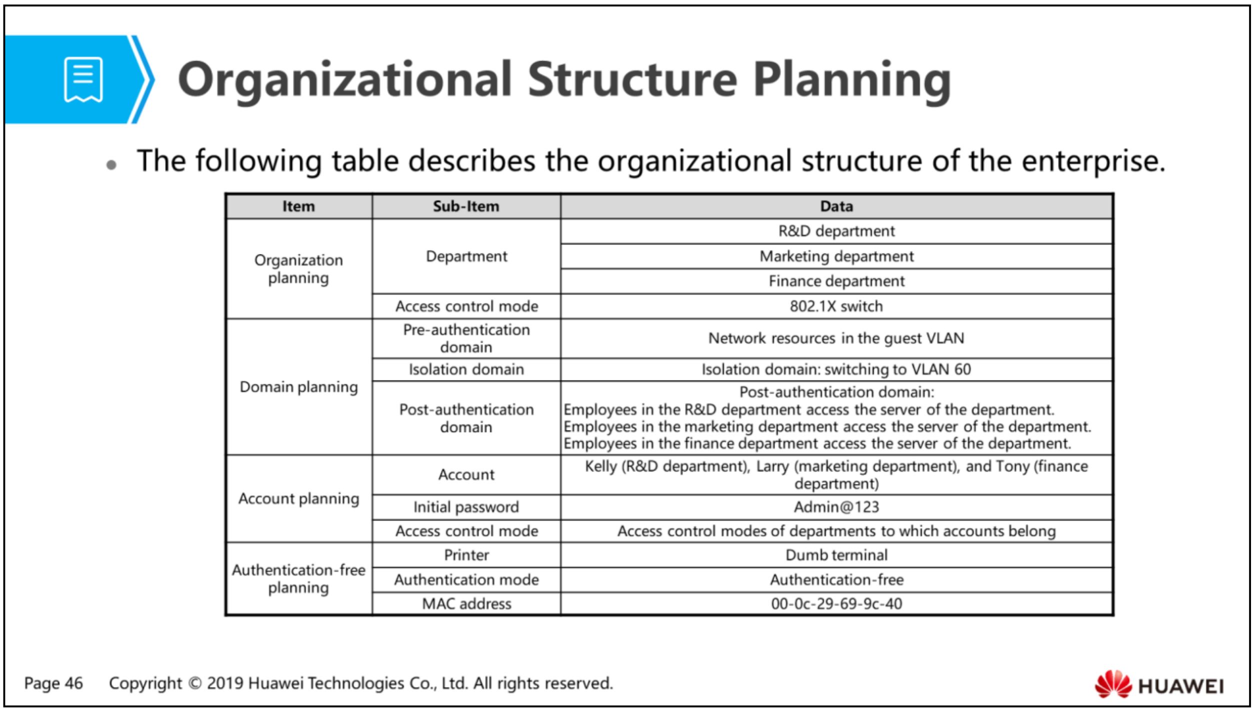
172.16.3.0/24

- An enterprise deploys the Agile Controller to access-control terminals and meet the following requirements:
  - The core switch functions as the network access device that associates with the Agile Controller.
  - Unauthorized users are permitted to access only the Agile Controller and DHCP server, and prohibited from accessing the isolation domain and post-authentication domain.
  - User terminals who have passed authentication but do not pass security check are repaired in the isolation domain.
  - After successful authentication, employees in the marketing, R&D, and finance departments can access servers of their departments, respectively.
  - In campus access scenarios, users' access rights are controlled based on accounts, terminal types, and access modes to ensure consistent access rights regardless of users' access locations.
  - Dumb terminals access the network through MAC address bypass authentication.

Campus IP Address Planning

- The following table describes campus IP address planning.

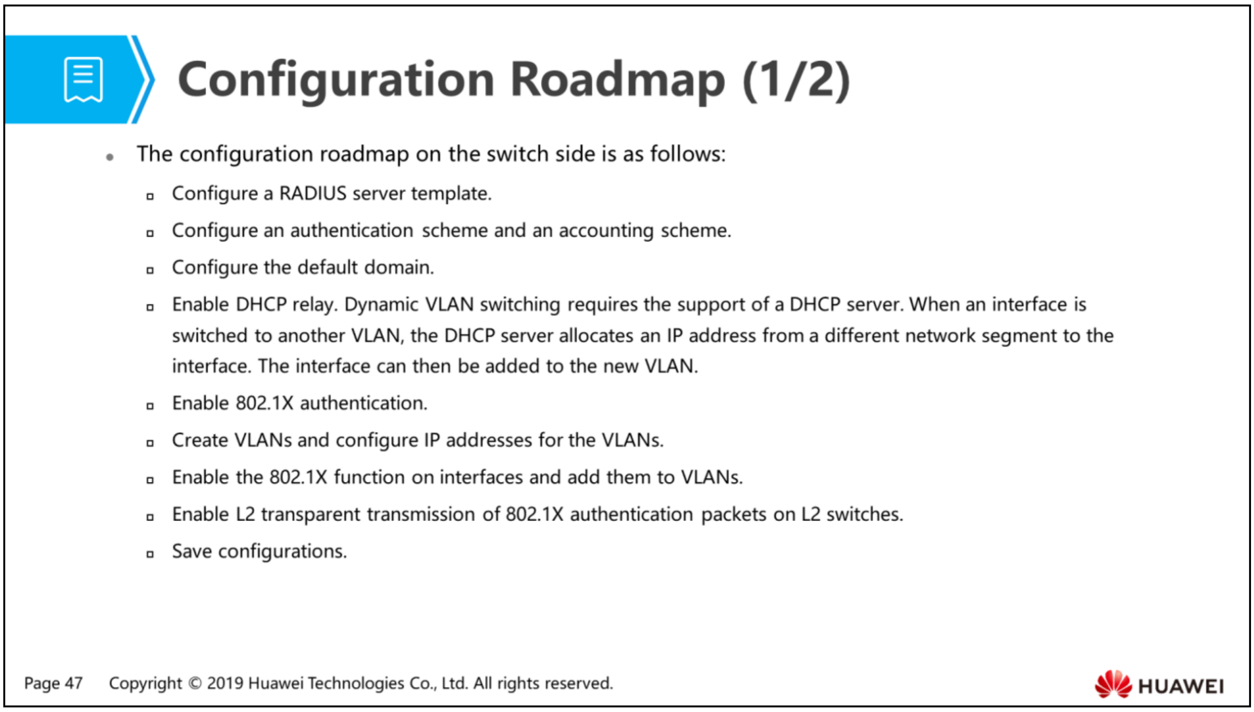
Item	Data
(1)	IP address 172.16.1.254 and VLAN 10 for GigbitEthernet 0/0/1 on the core switch
(2)	IP address 172.16.2.254 and VLAN 20 for GigbitEthernet 0/0/2 on the core switch
(3)	IP address 172.16.3.254 and VLAN 30 for GigbitEthernet 0/0/3 on the core switch
(4)	IP address 172.16.4.254 and VLAN 40 for GigbitEthernet 0/0/4 on the core switch
	IP address 172.16.4.253 for the SM and SC
(5)	IP address 172.16.5.254 and VLAN 50 for GigbitEthernet 0/0/5 on the core switch
	IP address of the DHCP server: 172.16.5.253
(6)	IP address 172.16.6.254 and VLAN 60 for GigbitEthernet 0/0/6 on the core switch
	IP address 172.16.5.253 for the patch server and antivirus server
(7)	IP address 172.16.7.254 and VLAN 70 for GigbitEthernet 0/0/7 on the core switch
	IP address 172.16.7.253 for the server of the R&D department
	IP address 172.16.7.252 for the server of the marketing department
	IP address 172.16.7.251 for the server of the finance department



Organizational Structure Planning

- The following table describes the organizational structure of the enterprise.

Item	Sub-Item	Data
Organization planning	Department	R&D department
		Marketing department
		Finance department
	Access control mode	802.1X switch
Domain planning	Pre-authentication domain	Network resources in the guest VLAN
	Isolation domain	Isolation domain: switching to VLAN 60
	Post-authentication domain	Post-authentication domain: Employees in the R&D department access the server of the department. Employees in the marketing department access the server of the department. Employees in the finance department access the server of the department.
Account planning	Account	Kelly (R&D department), Larry (marketing department), and Tony (finance department)
	Initial password	Admin@123
	Access control mode	Access control modes of departments to which accounts belong
Authentication-free planning	Printer	Dumb terminal
	Authentication mode	Authentication-free
	MAC address	00-0c-29-69-9c-40



Configuration Roadmap (1/2)

- The configuration roadmap on the switch side is as follows:
  - Configure a RADIUS server template.
  - Configure an authentication scheme and an accounting scheme.
  - Configure the default domain.
  - Enable DHCP relay. Dynamic VLAN switching requires the support of a DHCP server. When an interface is switched to another VLAN, the DHCP server allocates an IP address from a different network segment to the interface. The interface can then be added to the new VLAN.
  - Enable 802.1X authentication.
  - Create VLANs and configure IP addresses for the VLANs.
  - Enable the 802.1X function on interfaces and add them to VLANs.
  - Enable L2 transparent transmission of 802.1X authentication packets on L2 switches.
  - Save configurations.

Configuration Roadmap (2/2)

- The configuration roadmap on the SM side is as follows:
  - Add a switch group. In practice, there may be multiple switches on which 802.1X access control is executed. A switch group is a suite of switches implementing 802.1X authentication and requiring central management.
  - Add an isolation domain.
  - Add a post-authentication domain.
  - Apply the isolation domain and post-authentication domain to departments. If an end user fails to pass security check, the SC switches the end user to the isolation domain. If an end user passes security check, the SC switches the end user to the post-authentication domain. In this way, network isolation and network access authorization are implemented.
  - Add devices that need to access the network through MAC address bypass authentication. Enable authentication-free for devices that cannot have the AnyOffice installed or perform 802.1X authentication.

Switch Configuration (1/6)

- Configure a RADIUS server template.

```
<Quidway> system-view
[Quidway] radius-server template template1
# Set the IP address of the authentication server to the IP address of the SC, and the authentication
port number to 1812.
[Quidway-radius-template1] radius-server authentication 172.16.4.253 1812
# Set the IP address of the accounting server to the IP address of the SC, and the authentication port
number to 1813.
[Quidway-radius-template1] radius-server accounting 172.16.4.253 1813
# Set the RADIUS authentication shared key to Admin@123.
# When configuring 802.1X switches on the SM, ensure that the authentication key and accounting key
are the same as the RADIUS authentication shared key.
[Quidway-radius-template1] radius-server shared-key cipher Admin@123
[Quidway-radius-template1] quit
# After creating a RADIUS server template, check the template configuration. Verify the IP address,
port number, and key of the RADIUS server.
[Quidway] display radius-server configuration template template1
```

Switch Configuration (2/6)

- Create authentication scheme auth and accounting scheme acco.

```
 [Quidway] aaa
 [Quidway-aaa] authentication-scheme auth
 # Set the authentication  mode and accounting mode to RADIUS. After the configuration is complete,
check the configuration.
 [Quidway-aaa-authen-auth]  authentication-mode radius
 [Quidway-aaa-authen-auth]  quit
 [Quidway-aaa] display authentication-scheme
 [Quidway-aaa] accounting-scheme acco
 [Quidway-aaa-accounting-acco]  accounting-mode radius
 [Quidway-aaa-accounting-acco]  quit
 [Quidway-aaa] display accounting-scheme
```

Switch Configuration (3/6)

- Apply RADIUS server template template1, authentication scheme auth, and accounting scheme acco to the default domain.

```
[Quidway-aaa] domain default
# Apply RADIUS server template template1.
[Quidway-aaa-domain-default] radius-server template1
# Apply authentication scheme auth.
[Quidway-aaa-domain-default] authentication-scheme auth
# Apply accounting scheme acco.
[Quidway-aaa-domain-default] accounting-scheme acco
[Quidway-aaa-domain-default] quit
[Quidway-aaa] quit

# Check the AAA configuration and verify that the applied authentication scheme, accounting scheme, and RADIUS server template
are correct.
[Quidway] display domain name default
```

- Configure the RADIUS server as the authorization server. The RADIUS server then can instruct the switch to change interface VLANs based on the authentication status of end users.

```
[Quidway] radius-server authorization 172.16.4.253 shared-key cipher Admin@123
```

Switch Configuration (4/6)

- Enable the DHCP function.

```
[Quidway] dhcp enable
```

- Enable 802.1X authentication.

```
[Quidway] dot1x enable
[Quidway] dot1x authentication-method eap
```

- Create VLANs 10, 20, 30, 40, 50, 60, and 70, and configure IP addresses for VLAN interfaces.

```
[Quidway] vlan batch 10 20 30 40 50 60 70
```

- Configure IP address 172.16.1.254 for VLANIF 10, and enable DHCP relay to ensure that the devices in VLAN 10 can obtain IP addresses from the DHCP server on a different network segment.

```
[Quidway] interface Vlanif 10
[Quidway-Vlanif10] ip address 172.16.1.254 255.255.255.0
[Quidway-Vlanif10] dhcp select relay
[Quidway-Vlanif10] dhcp relay server-ip 172.16.5.253
[Quidway-Vlanif10] quit
# The configuration for VLAN 20 and VLAN 30 is similar and not described here.
```

Switch Configuration (5/6)

- Enable 802.1X authentication on an interface of the switch connected to terminal hosts, and add the interface to the corresponding VLAN.

```
[Quidway] interface GigbitEthernet 0/0/1
# Add the interface to VLAN 10. Other interfaces on the switch are added to VLANs in the similar way, which is not
described here.
[Quidway-GigbitEthernet0/0/1] port hybrid pvid vlan 10
[Quidway-GigbitEthernet0/0/1] port hybrid untagged vlan 10
```

- Enable 802.1X authentication on GigbitEthernet0/0/1. Enable 802.1X authentication on GigbitEthernet0/0/2 and GigbitEthernet0/0/3 in the similar way, which is not described here.

```
[Quidway-GigbitEthernet0/0/1] dot1x enable
[Quidway-GigbitEthernet0/0/1] dot1x port-control auto
# Enable the port-based access mode.
[Quidway-GigbitEthernet0/0/1] dot1x port-method port
# Ensure that the AnyOffice can access the VLAN where the SC resides before authentication.
[Quidway-GigbitEthernet0/0/1] authentication guest-vlan 40
[Quidway-GigbitEthernet0/0/1] quit
# Configure MAC address bypass authentication on the interface connected to a printer and ensure that the printer can
access the network without authentication.
[Quidway-GigbitEthernet0/0/1] dot1x mac-bypass
[Quidway-GigbitEthernet0/0/1] quit
```

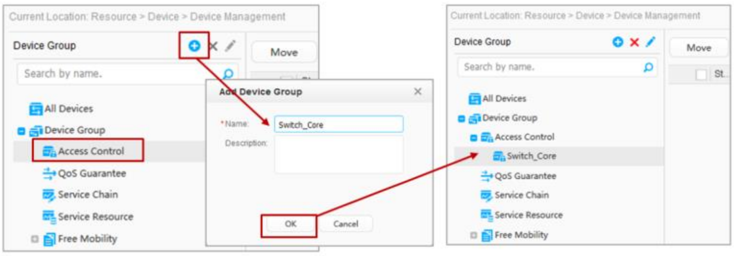
Switch Configuration (6/6)

- L2 aggregation and access switches are located between users and switches on which 802.1X authentication is enabled. To ensure that 802.1X authentication packets from users can pass through L2 switches, perform the following configurations on the aggregation and access switches (for example, the S5700HI):

```
<HUAWEI> system-view
[HUAWEI] sysname LAN Switch
[LAN Switch] l2protocol-tunnel user-defined-protocol dot1x protocol-mac 0180-c200-0003 group-
mac 0100-0000-0002
# group-mac cannot be set to one of the reserved multicast MAC addresses (0180-C200-0000 to 0180-
C200-002F) or other special MAC addresses.
[LAN Switch] interface gigabitethernet 0/0/1
# Perform the following configurations on all interfaces on the L2 switch connected to upper-layer
networks and users.
[LAN Switch-GigabitEthernet0/0/1] l2protocol-tunnel user-defined-protocol dot1x enable
[LAN Switch-GigabitEthernet0/0/1] bpdu enable
[LAN Switch-GigabitEthernet0/0/1] quit
```

SM Configuration (1/2)

- Log in to the Agile Controller using the Admin account.
- Add a switch group.
  - # Choose Resource > Device > Device Management.
  - # Choose Device Group > Access Control from the navigation tree, and click ⊕ , and set switch group parameters.

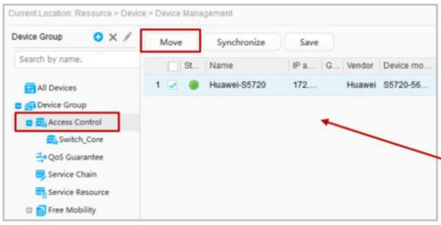


*Name: Switch_Core

  - # Click OK. A switch group is added.

SM Configuration (2/2)

- # When adding a device, set IP address to 172.16.4.254. When RADIUS authentication is used, set Authentication/Accounting key to Admin@123.
- # Click OK.
- # Choose Access Control, select Huawei-S5720, and click Move to move Huawei-S5720 to switch group Switch_Core.



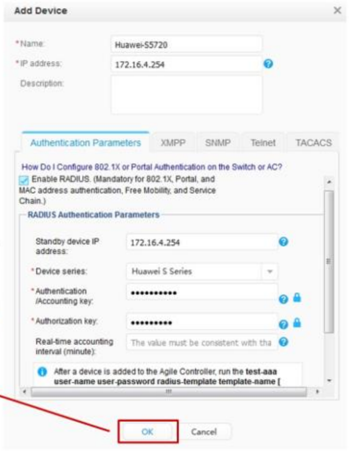
Current Location: Resource > Device > Device Management

Device Group

Search by name.

- All Devices
- Device Group
  - Access Control
    - Switch_Core
  - QoS Guarantee
  - Service Chain
  - Service Resource
  - Free Mobility

	□	St...	Name	IP a...	G...	Vendor	Device mo...
1	☑	●	Huawei-S5720	172....		Huawei	S5720-56...



Add Device

*Name: Huawei-S5720

*IP address: 172.16.4.254

Description:

How Do I Configure 802.1X or Portal Authentication on the Switch or AC?

☑ Enable RADIUS. (Mandatory for 802.1X, Portal, and MAC address authentication, Free Mobility, and Service Chain.)

RADIUS Authentication Parameters

Standby device IP address: 172.16.4.254

*Device series: Huawei S Series

*Authentication /Accounting key: ●●●●●●●●●●●

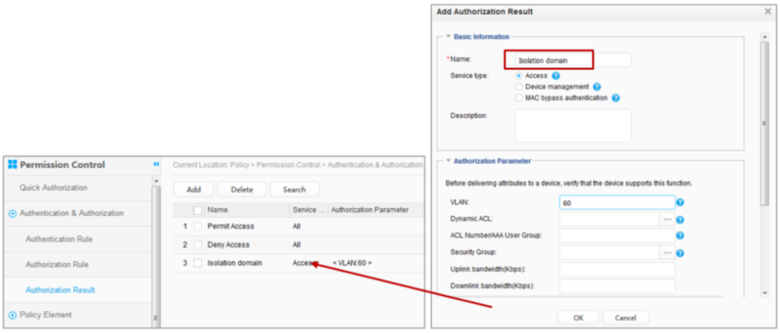
*Authorization key: ●●●●●●●●●●

Real-time accounting interval (minute): The value must be consistent with tha

After a device is added to the Agile Controller, run the **test-aaa user-name user-password radius-template template-name [**

Adding Authorization Results - Isolation Domains

- # Choose Policy > Permission Control > Authentication & Authorization > Authorization Result. Click Add and configure VLAN 60 as an isolation domain.
- # Set authorization result parameters as shown in the right figure.



Current Location: Policy > Permission Control > Authentication & Authorization

	□ Name	Service ...	Authorization Parameter
1	□ Permit Access	All	
2	□ Deny Access	All	
3	□ Isolation domain	Access	< VLAN:60 >

*Name: Isolation domain

Service type: ● Access ○ Device management ○ MAC bypass authentication

Description:

Before delivering attributes to a device, verify that the device supports this function.

VLAN: 60

Dynamic ACL:

ACL Number/AAA User Group:

Security Group:

Uplink bandwidth(Kbps):

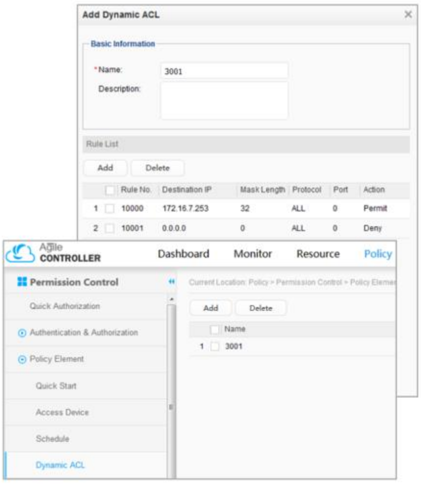
Downlink bandwidth(Kbps):

Adding Authorization Results - Post-Authentication Domains (1/2)

- # Servers of all departments are added to the same VLAN. To enable employees in a department to access only servers of the department, set dynamic ACLs on the Agile Controller to control access permission. Set ACLs 3001, 3002, and 3003 to allow employees in the R&D, marketing, and finance departments to access only servers of corresponding departments, respectively.

- # Choose Policy > Permission Control > Policy Element > Dynamic ACL. Click Add and add ACL 3001.

- # The right figure shows the configuration of ACL 3001.



Add Dynamic ACL

Basic Information

*Name: 3001

Description:

Rule List

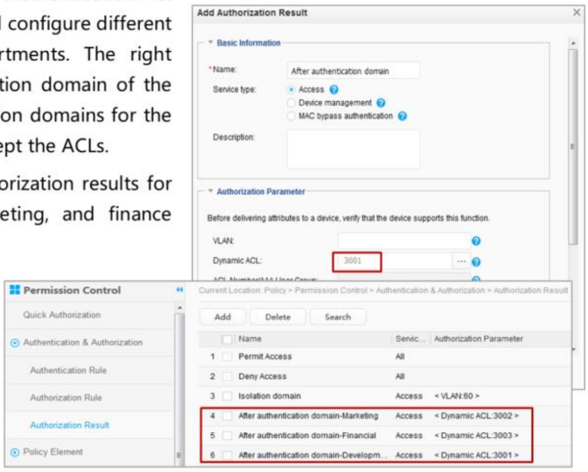
	Rule No.	Destination IP	Mask Length	Protocol	Port	Action
1 □	10000	172.16.7.253	32	ALL	0	Permit
2 □	10001	0.0.0.0	0	ALL	0	Deny

Current Location: Policy > Permission Control > Policy Elemer

	Name
1 □	3001

Adding Authorization Results - Post-Authentication Domains (2/2)

- # Choose Policy > Permission Control > Authentication & Authorization > Authorization Result. Click Add and configure different post-authentication domains for different departments. The right figure shows the settings for the post-authentication domain of the R&D department. Settings of the post-authentication domains for the marketing and finance departments are similar except the ACLs.
- # The following figure shows the configured authorization results for post-authentication domains of the R&D, marketing, and finance departments.



Add Authorization Result

Basic Information

*Name: After authentication domain

Service type: ● Access ○ Device management ○ MAC bypass authentication

Description:

Authorization Parameter

Before delivering attributes to a device, verify that the device supports this function.

VLAN:

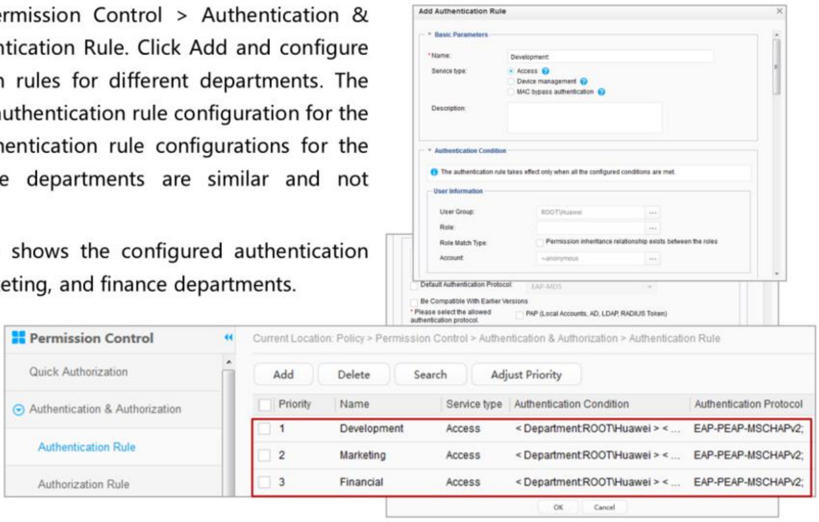
Dynamic ACL: 3001

Current Location: Policy > Permission Control > Authentication & Authorization > Authorization Result

		Name	Servic...	Authorization Parameter
1	□	Permit Access	All	
2	□	Deny Access	All	
3	□	Isolation domain	Access	< VLAN:60 >
4	□	After authentication domain-Marketing	Access	< Dynamic ACL:3002 >
5	□	After authentication domain-Financial	Access	< Dynamic ACL:3003 >
6	□	After authentication domain-Developm...	Access	< Dynamic ACL:3001 >

Adding Authentication Rules

- # Choose Policy > Permission Control > Authentication & Authorization > Authentication Rule. Click Add and configure different authentication rules for different departments. The right figure shows the authentication rule configuration for the R&D department. Authentication rule configurations for the marketing and finance departments are similar and not described here.
- # The following figure shows the configured authentication rules for the R&D, marketing, and finance departments.



Add Authentication Rule

Basic Parameters

- *Name: Development
- Service type: ● Access ○ Device management ○ MAC bypass authentication
- Description:

Authentication Condition

The authentication rule takes effect only when all the configured conditions are met.

User Information

- User Group: ROOT\Huawei
- Role:
- Role Match Type: □ Permission inheritance relationship exists between the roles
- Account: ~anonymous

□ Default Authentication Protocol: EAP-MD5

□ Be Compatible With Earlier Versions

* Please select the allowed authentication protocol. □ PAP (Local Accounts, AD, LDAP, RADIUS Token)

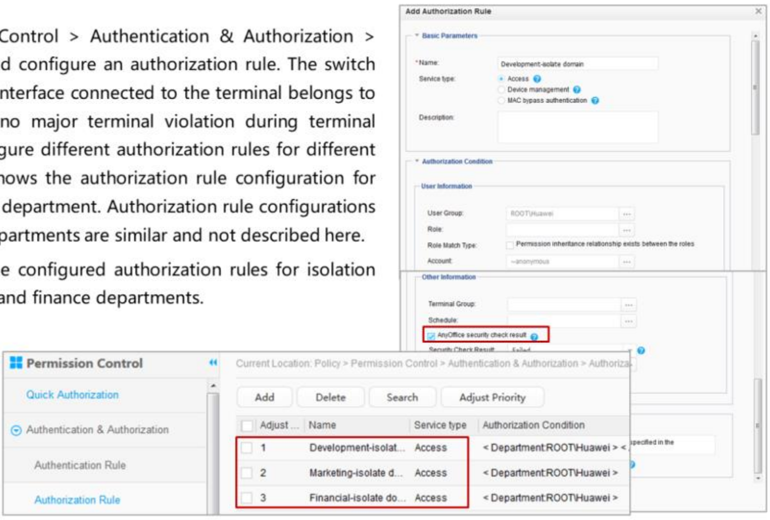
OK Cancel

Current Location: Policy > Permission Control > Authentication & Authorization > Authentication Rule

□	Priority	Name	Service type	Authentication Condition	Authentication Protocol
□	1	Development	Access	< Department:ROOT\Huawei > < ...	EAP-PEAP-MSCHAPv2;
□	2	Marketing	Access	< Department:ROOT\Huawei > < ...	EAP-PEAP-MSCHAPv2;
□	3	Financial	Access	< Department:ROOT\Huawei > < ...	EAP-PEAP-MSCHAPv2;

Adding Authorization Rules - Isolation Domains

- # Choose Policy > Permission Control > Authentication & Authorization > Authorization Rule. Click Add and configure an authorization rule. The switch changes the VLAN to which the interface connected to the terminal belongs to VLAN 60 (isolation domain) if no major terminal violation during terminal security check is detected. Configure different authorization rules for different departments. The right figure shows the authorization rule configuration for the isolation domain of the R&D department. Authorization rule configurations for the marketing and finance departments are similar and not described here.
- # The following figure shows the configured authorization rules for isolation domains of the R&D, marketing, and finance departments.



Add Authorization Rule

Basic Parameters

*Name: Development-isolate domain

Service type: ● Access ○ Device management ○ MAC bypass authentication

Description:

Authorization Condition

User Information

User Group: ROOT\Huawei

Role:

Role Match Type: □ Permission inheritance relationship exists between the roles

Account: ~anonymous

Other Information

Terminal Group:

Schedule:

☑ AnyOffice security check result

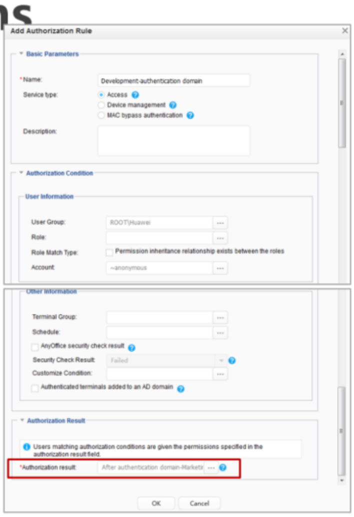
Security Check Result: Failed

Current Location: Policy > Permission Control > Authentication & Authorization > Authoriza

□	Adjust ...	Name	Service type	Authorization Condition
□	1	Development-isolat...	Access	< Department:ROOT\Huawei > <
□	2	Marketing-isolate d...	Access	< Department:ROOT\Huawei >
□	3	Financial-isolate do...	Access	< Department:ROOT\Huawei >

Adding Authorization Rules - Post-Authentication Domains

- # Choose Policy > Permission Control > Authentication & Authorization > Authorization Rule. Click Add and configure an authorization rule. The switch changes the VLAN to which the interface connected to the terminal belongs to VLAN 70 (post-authentication domain) if no major terminal violation during terminal security check is detected. Configure different authorization rules for different departments. The right figure shows the authorization rule configuration for post-authentication domain of the R&D department. Authorization rule configurations for the marketing and finance departments are similar and not described here.



Add Authorization Rule

Basic Parameters

*Name: Development-authentication domain

Service type: ● Access ○ Device management ○ MAC bypass authentication

Description:

Authorization Condition

User Information

User Group: ROOT\Huawei

Role:

Role Match Type: □ Permission inheritance relationship exists between the roles

Account: ~anonymous

Other Information

Terminal Group:

Schedule:

□ AnyOffice security check result

Security Check Result: Failed

Customize Condition:

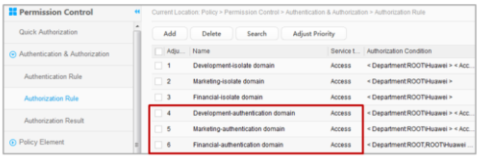
□ Authenticated terminals added to an AD domain

Authorization Result

Users matching authorization conditions are given the permissions specified in the authorization result field.

*Authorization result: After authentication domain-Marketi

- # The following figure shows the configured authorization rules for the R&D, marketing, and finance departments.



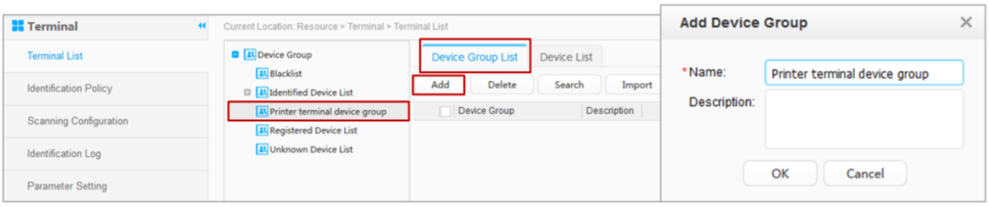
Permission Control

Current Location: Policy > Permission Control > Authentication & Authorization > Authorization Rule

Adju...	Name	Service t...	Authorization Condition
1	Development-isolate domain	Access	< Department:ROOT\Huawei > < Acc...
2	Marketing-isolate domain	Access	< Department:ROOT\Huawei >
3	Financial-isolate domain	Access	< Department:ROOT\Huawei >
4	Development-authentication domain	Access	< Department:ROOT\Huawei > < Acc...
5	Marketing-authentication domain	Access	< Department:ROOT\Huawei > < Acc...
6	Financial-authentication domain	Access	< Department:ROOT,ROOT\Huawei ...

Adding Devices Requiring MAC Address Bypass Authentication (1/2)

- # Choose Resource > Terminal > Terminal List. Choose Device Group and then click Add. Create a device group named Printer terminal device group.
- # Choose Printer terminal device group. On the Device Group List tab page, click Add and add device group Printer.



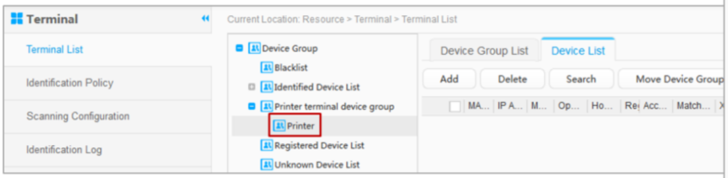
*Name: Printer terminal device group

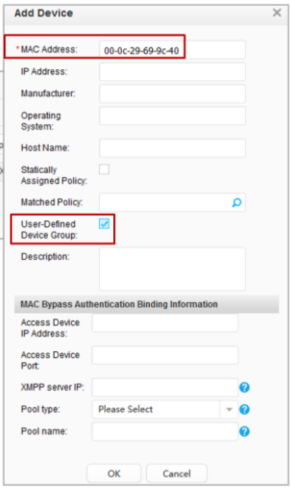
Description:

- # Click OK. Device group **Printer** is created.

Adding Devices Requiring MAC Address Bypass Authentication (2/2)

- # Choose Printer and click Add on the Device List page.





* MAC Address: 00-0c-29-69-9c-40

User-Defined Device Group: ☑

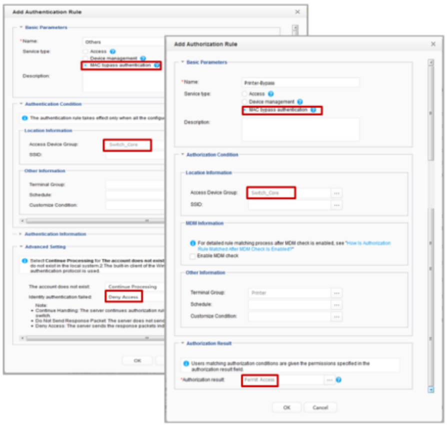
- # Set MAC Address to the MAC address of the printer requiring MAC address bypass authentication, and select User-Defined Device Group. Click OK. The printer is added.

Adding Devices Requiring MAC Address Bypass Authentication - Authentication and Authorization

- # Choose Policy > Permission Control > Authentication & Authorization > Authentication Rule. Click Add. Configure an authentication rule to enable the Agile Controller to permit network access using MAC address bypass authentication packets.

- # Choose Policy > Permission Control > Authentication & Authorization > Authorization Rule. Click Add. Configure an authorization rule to enable switches in a device group to permit network access using MAC address bypass authentication packets.

- # MAC address bypass authentication requests from devices that are not in Printer terminal device group need to be rejected. Choose Policy > Permission Control > Authentication & Authorization > Authorization Rule. Click Add and configure an authorization rule to deny network access from devices that are not in Printer terminal device group.



Add Authentication Rule

Basic Parameters

*Name: Others

Service type: ○ Access ○ Device management ● MAC bypass authentication

Description:

Authentication Condition

The authentication rule takes effect only when all the configu

Location Information

Access Device Group: Switch_Core

SSID:

Other Information

Terminal Group:

Schedule:

Customize Condition:

Authentication Information

Advanced Setting

Select **Continue Processing** for **The account does not exist** do not exist in the local system.2.The built-in client of the Win authentication protocol is used.

The account does not exist: Continue Processing

Identity authentication failed: Deny Access

Note:
- Continue Handling: The server continues authorization rul switch.
- Do Not Send Response Packet: The server does not send
- Deny Access: The server sends the response packets ind

Add Authorization Rule

Basic Parameters

*Name: Printer-Bypass

Service type: ○ Access ○ Device management ● MAC bypass authentication

Description:

Authorization Condition

Location Information

Access Device Group: Switch_Core

SSID:

MDM Information

For detailed rule matching process after MDM check is enabled, see "How Is Authorization Rule Matched After MDM Check Is Enabled?"

□ Enable MDM check

Other Information

Terminal Group: Printer

Schedule:

Customize Condition:

Authorization Result

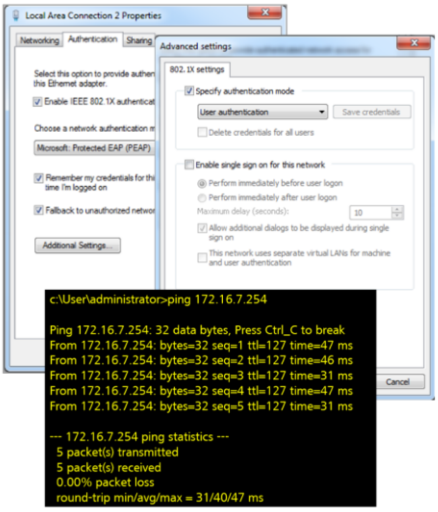
Users matching authorization conditions are given the permissions specified in the authorization result field.

*Authorization result: Permit Access

Verifying the Configuration

- When the built-in 802.1X client of the Windows operating system is used for identity authentication, select Enable IEEE 802.1X authentication.

- # After passing both identity authentication and security check, a terminal in the R&D department can access the server of the R&D department. The ping test shows that the network between the terminal host and the server works properly.



Local Area Connection 2 Properties

Select this option to provide authen
this Ethernet adapter.

☑ Enable IEEE 802.1X authenticat

Choose a network authentication m

Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for thi
time I'm logged on

☑ Fallback to unauthorized networ

Advanced settings

802. 1X settings

☑ Specify authentication mode

User authentication

□ Delete credentials for all users

□ Enable single sign on for this network

● Perform immediately before user logon

○ Perform immediately after user logon

Maximum delay (seconds): 10

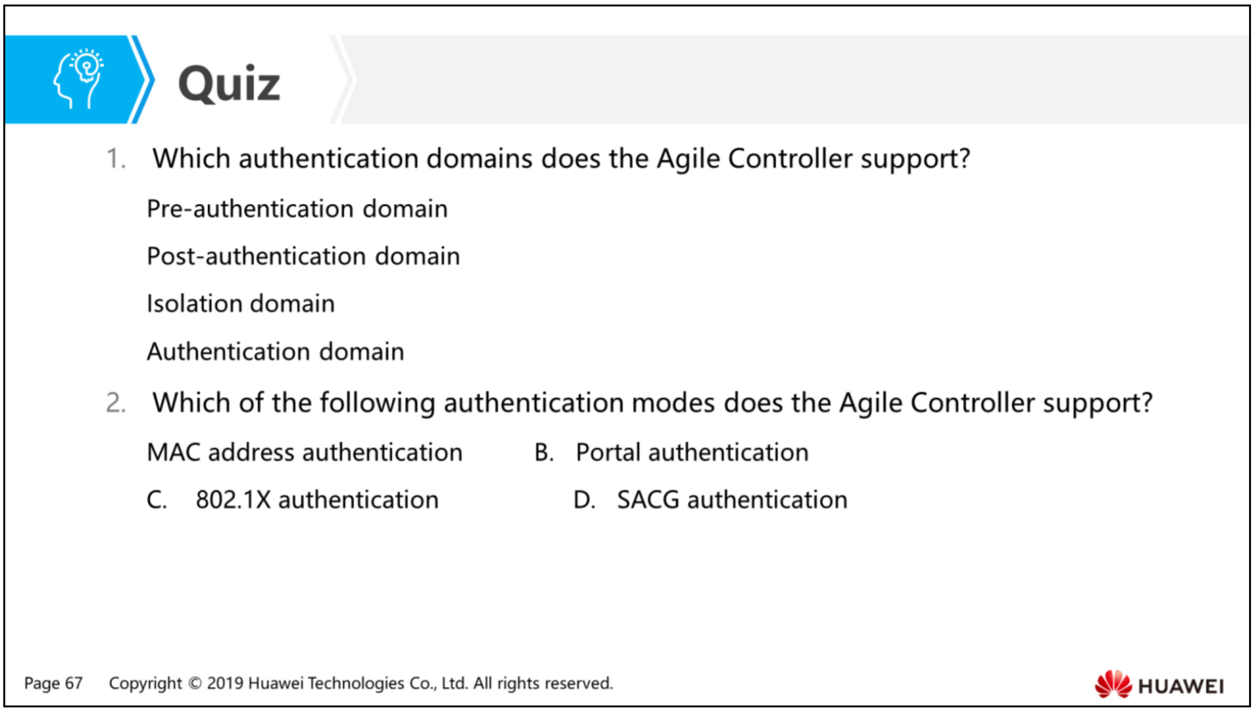
☑ Allow additional dialogs to be displayed during single sign on

□ This network uses separate virtual LANs for machine and user authentication

```
c:\User\administrator>ping 172.16.7.254

Ping 172.16.7.254: 32 data bytes, Press Ctrl_C to break
From 172.16.7.254: bytes=32 seq=1 ttl=127 time=47 ms
From 172.16.7.254: bytes=32 seq=2 ttl=127 time=46 ms
From 172.16.7.254: bytes=32 seq=3 ttl=127 time=31 ms
From 172.16.7.254: bytes=32 seq=4 ttl=127 time=47 ms
From 172.16.7.254: bytes=32 seq=5 ttl=127 time=31 ms

--- 172.16.7.254 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 31/40/47 ms
```



Quiz

1. Which authentication domains does the Agile Controller support?

   Pre-authentication domain

   Post-authentication domain

   Isolation domain

   Authentication domain

2. Which of the following authentication modes does the Agile Controller support?

   MAC address authentication B. Portal authentication

   C. 802.1X authentication D. SACG authentication

- Answer: ABC.
- Answer: ABCD.

Thank You

www.huawei.com

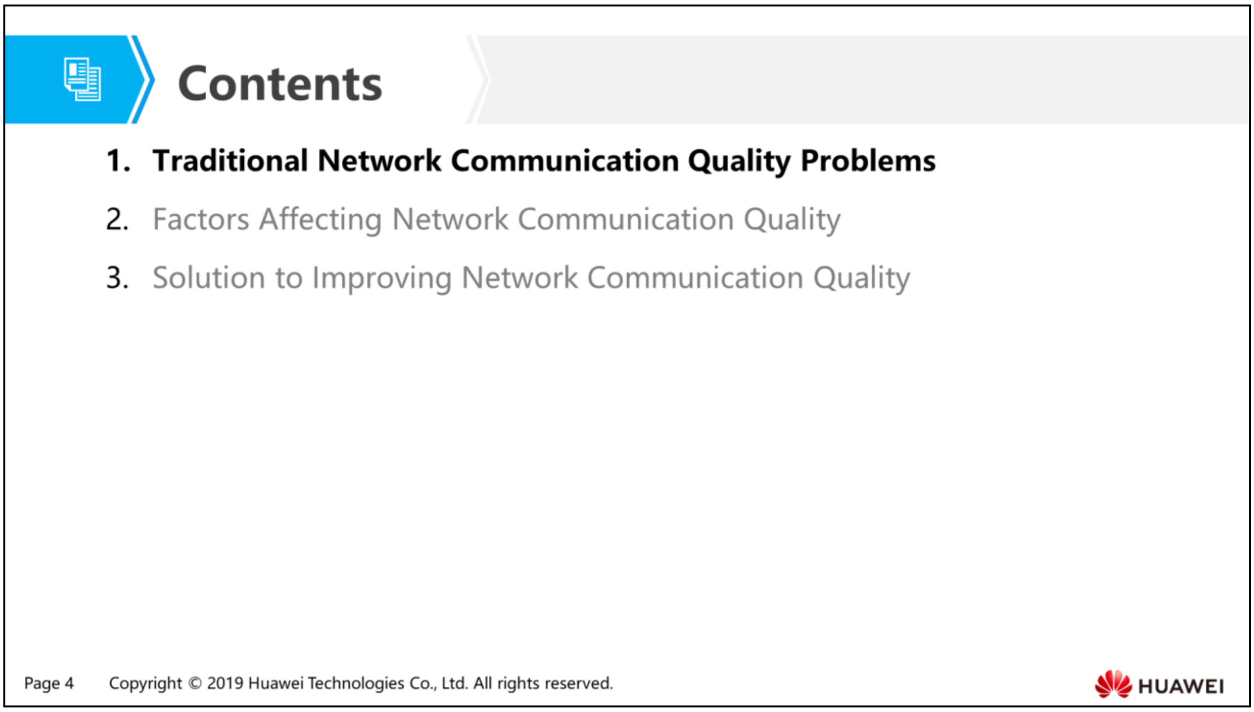
QoS Service Models

Foreword

- Continuous network development and increasing network scale and traffic types cause Internet traffic increase and the risk of traffic congestion. When traffic congestion occurs, services encounter long delays or even packet loss. As a result, services deteriorate or even become unavailable. Therefore, a solution to eliminate traffic congestion on the IP network is urgently needed. The best way to eliminate traffic congestion is to increase network bandwidth. However, increasing network bandwidths is infeasible due to the high network construction costs.
- QoS technology is used to solve the problem. With limited bandwidth, this technology uses guaranteed policies to manage network traffic and offer differentiated services.

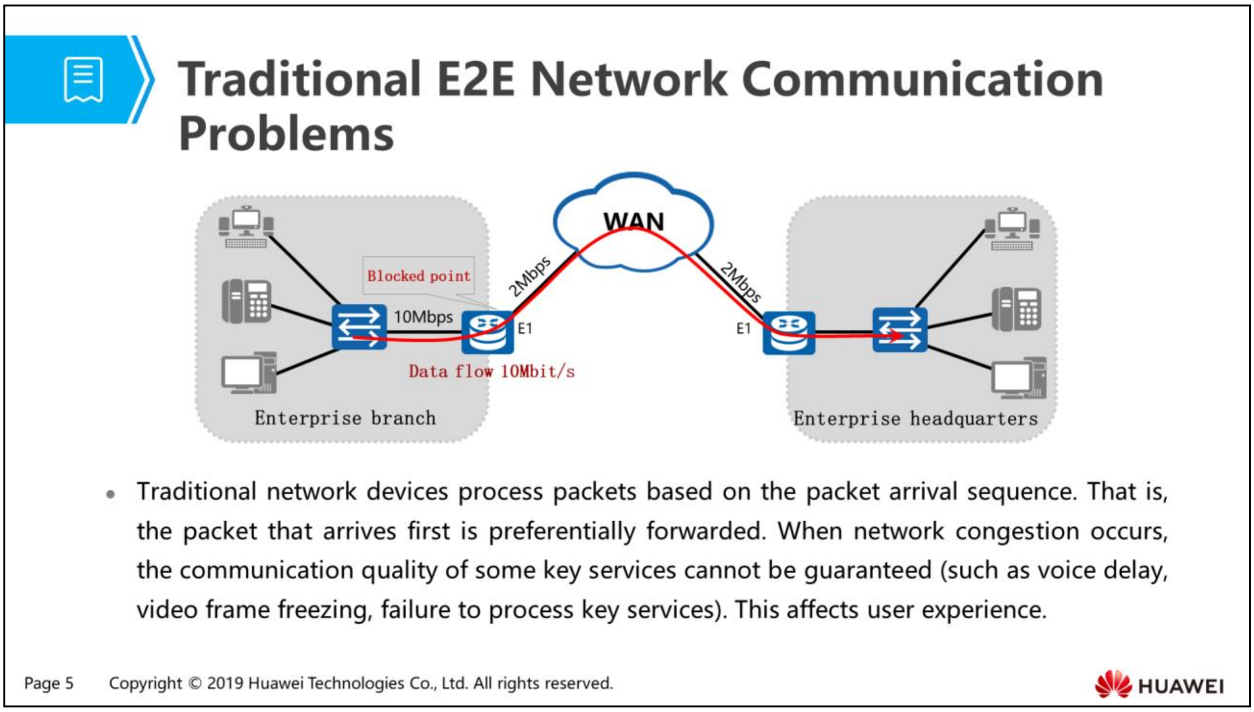
Objectives

- Upon completion of this section, you will be able to:
  - Understand the factors affecting QoS
  - Be familiar with QoS service models
  - Understand the implementation of the DiffServ model



Contents

1. **Traditional Network Communication Quality Problems**
2. Factors Affecting Network Communication Quality
3. Solution to Improving Network Communication Quality



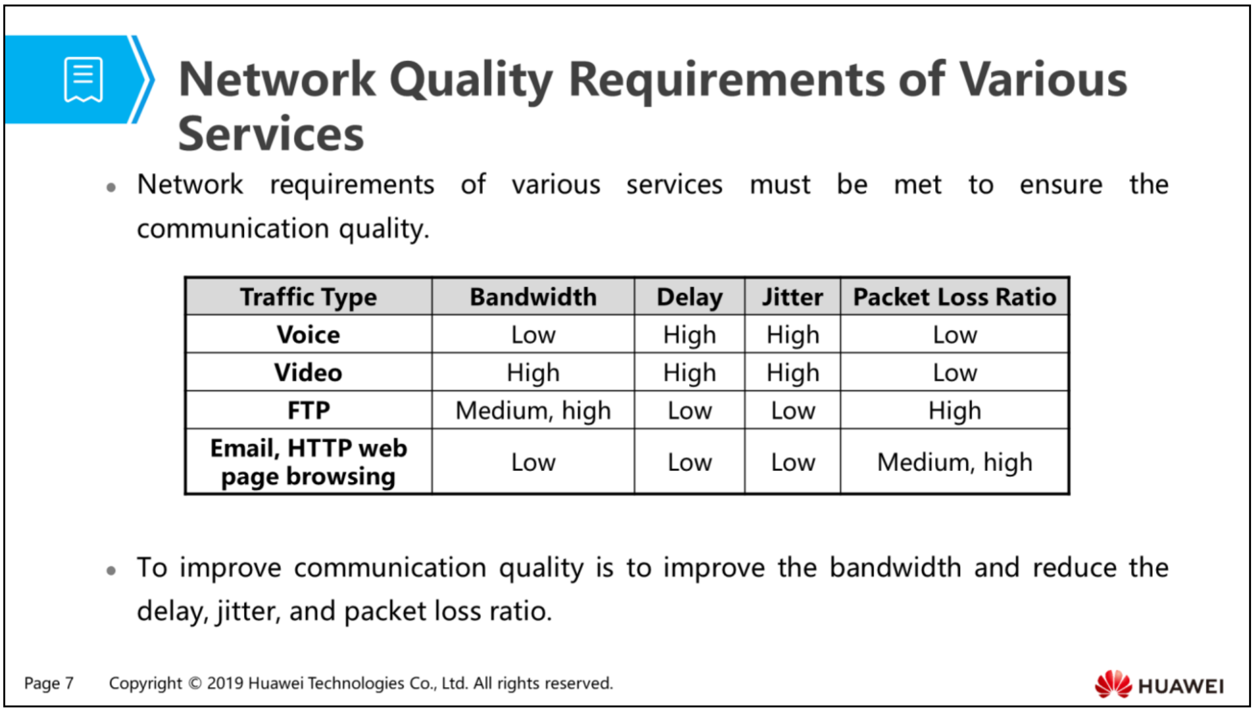
Traditional E2E Network Communication Problems

- Traditional network devices process packets based on the packet arrival sequence. That is, the packet that arrives first is preferentially forwarded. When network congestion occurs, the communication quality of some key services cannot be guaranteed (such as voice delay, video frame freezing, failure to process key services). This affects user experience.

- On the traditional IP network, devices use the First In First Out (FIFO) policy to process all packets and allocate resources for packet forwarding based on the packet arrival time. All packets share resources such as the bandwidth of the network and devices. The obtained resources depend on the arrival time.
- FIFO technology sends packets to the destination on a best-effort basis, but does not guarantee the delay, jitter, packet loss ratio, and reliability. Therefore, the communication quality of some key services (such as voice and video services) cannot be ensured.
- How is the end-to-end communication quality improved? What are factors affecting the communication quality?

Contents

1. Traditional Network Communication Quality Problems
2. **Factors Affecting Network Communication Quality**
3. Solution to Improving Network Communication Quality



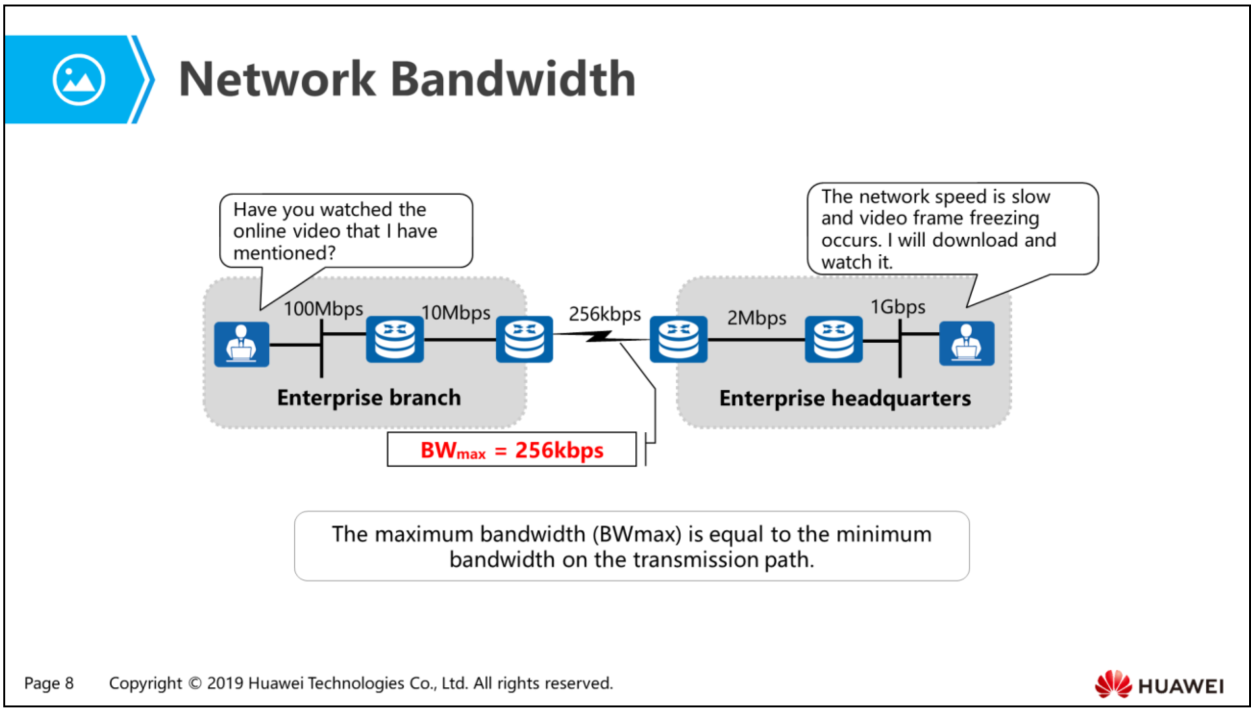
Network Quality Requirements of Various Services

- Network requirements of various services must be met to ensure the communication quality.

Traffic Type	Bandwidth	Delay	Jitter	Packet Loss Ratio
Voice	Low	High	High	Low
Video	High	High	High	Low
FTP	Medium, high	Low	Low	High
Email, HTTP web page browsing	Low	Low	Low	Medium, high

- To improve communication quality is to improve the bandwidth and reduce the delay, jitter, and packet loss ratio.

- We know the factors that affect end-to-end communication quality, so the communication quality can be ensured considering these factors. What are characteristics of these factors?



Network Bandwidth

Have you watched the online video that I have mentioned?

The network speed is slow and video frame freezing occurs. I will download and watch it.

100Mbps

10Mbps

256kbps

2Mbps

1Gbps

Enterprise branch

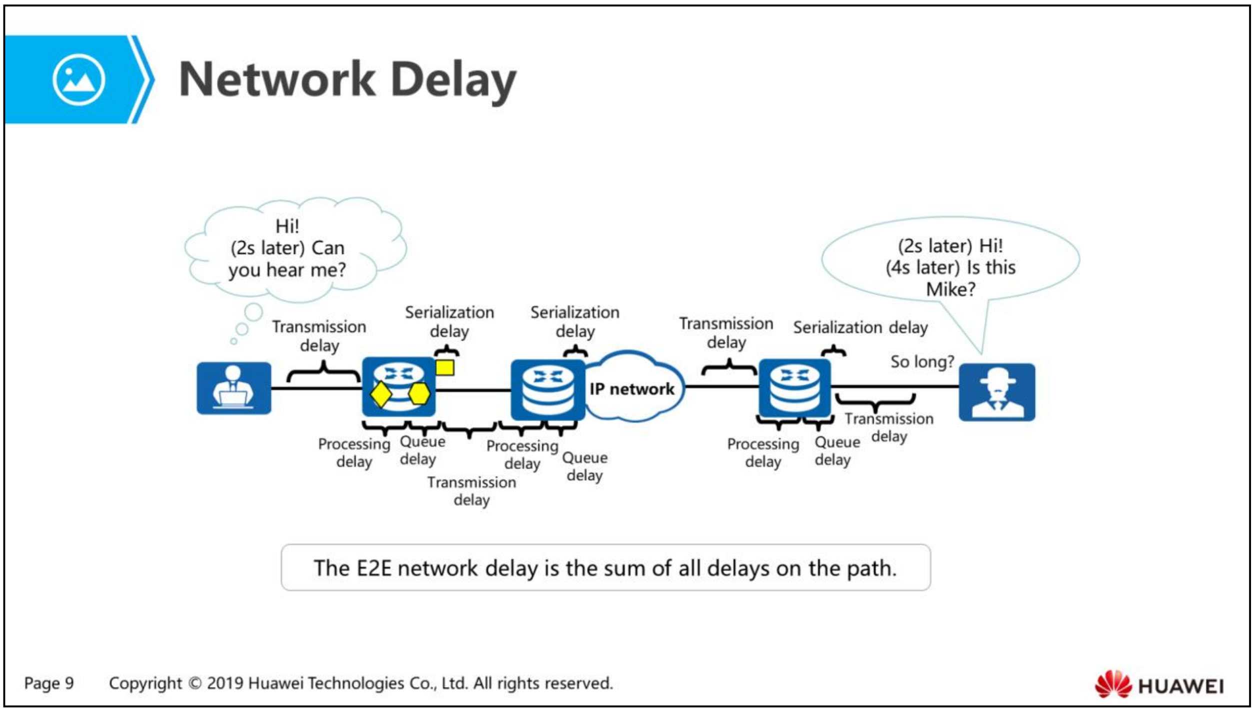
Enterprise headquarters

BW_{max} = 256kbps

The maximum bandwidth (BWmax) is equal to the minimum bandwidth on the transmission path.

HUAWEI

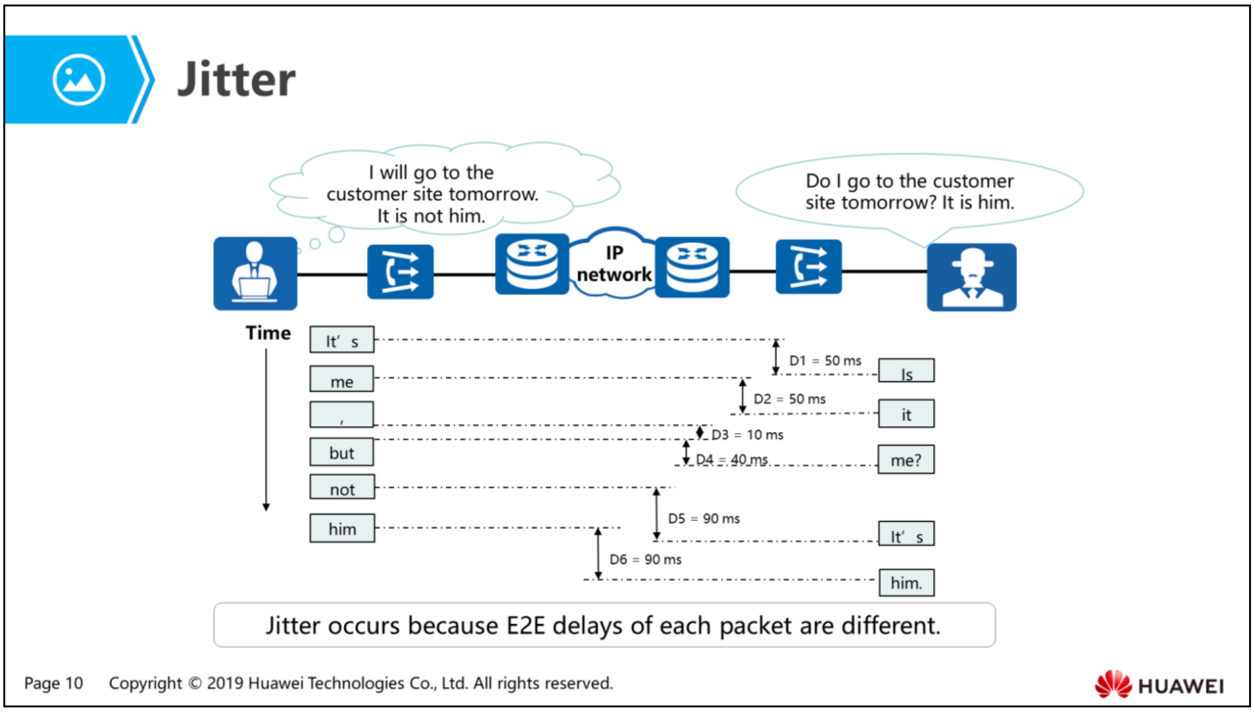
- The network bandwidth refers to the data amount transmitted in the unit time (1 second).
- As shown in the preceding figure, the maximum link bandwidth is 1Gbit/s, but the maximum transmission rate of data sent from a user to another user is 256kbit/s. This is because the maximum bandwidth is determined by the minimum link bandwidth on the transmission path. The minimum link bandwidth mainly affects the transmission rate.
- If there are multiple data flows on the network and compete the bandwidth, you can increase the bandwidth to achieve better network experience. Improving the bandwidth causes generation of new applications, so the network bandwidth cannot be increased without limitation. In addition, more bandwidth indicates a higher cost. Can we first ensure bandwidth of important services?



Network Delay

The E2E network delay is the sum of all delays on the path.

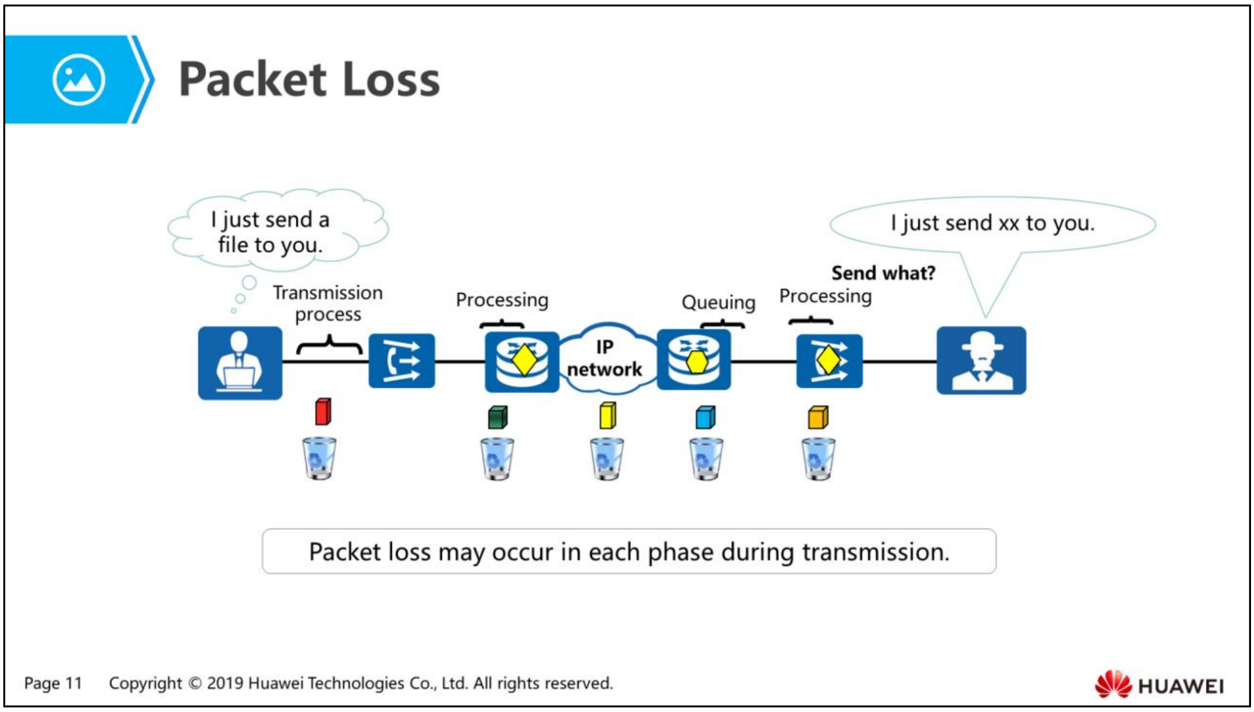
- The delay refers to the period of time during which a packet is transmitted from the source to the destination. The communication quality of real-time services such as voice and video services focuses on the delay. Use voice transmission as an example. A delay refers to the period during which words are spoken and then heard. If there is a long delay, voices become unclear or interrupted.
- The delay of a single network device includes the transmission delay, serialization delay, processing delay, and queue delay.
  - Transmission delay: indicates the time for one bit from the sender to the receiver. The delay depends on the transmission distance and media, and is irrelevant to the bandwidth.
  - Serialization delay: refers to the time used by the sending node to send the first bit of a packet to the last bit of the packet. The delay depends on the link bandwidth and packet size.
  - Processing delay: indicates the time used by a router to put packets on the inbound interface into the outbound interface queue. The delay depends on the processing performance of the router.
  - Queue delay: indicates the waiting time of packets in queues. The delay depends on the size and number of packets in queues, bandwidth, and queue mechanism.



Jitter

Jitter occurs because E2E delays of each packet are different.

- The end-to-end delay of each packet is different, so packets cannot reach the destination with the same interval. A jitter occurs. Generally, a smaller delay indicates a smaller jitter.
- Specific services, especially real-time services such as voice and video services, are zero-tolerant of jitters. The packet arrival time difference causes interruptions of voice and video services. In addition, the jitter also affects processing of network protocols. Interaction packets of some protocols are sent at fixed intervals. A large jitter causes protocol flapping. Actually, there is the jitter in all transmission systems. As long as the jitter is within the tolerance, the service quality is not affected. In addition, the buffer can be used to solve the problem of excessive jitter, increasing the delay.
- The jitter is relevant to the delay. A small delay indicates a small jitter.

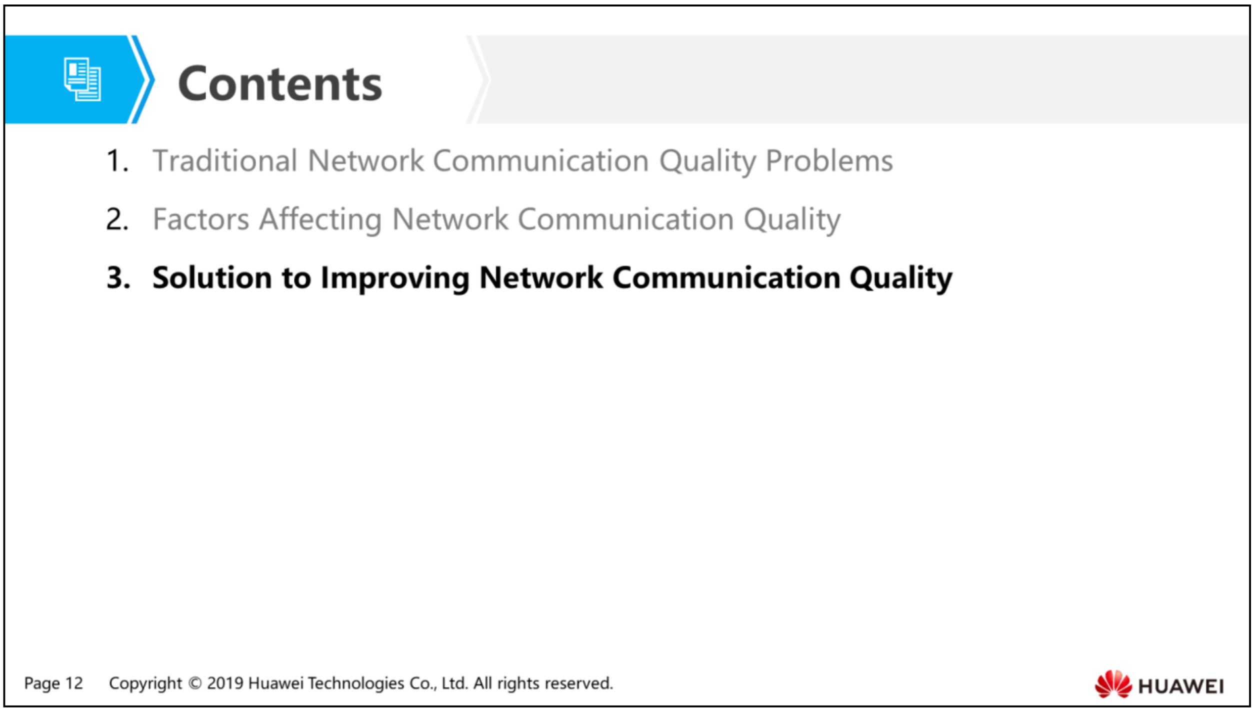


Packet Loss

Packet loss may occur in each phase during transmission.

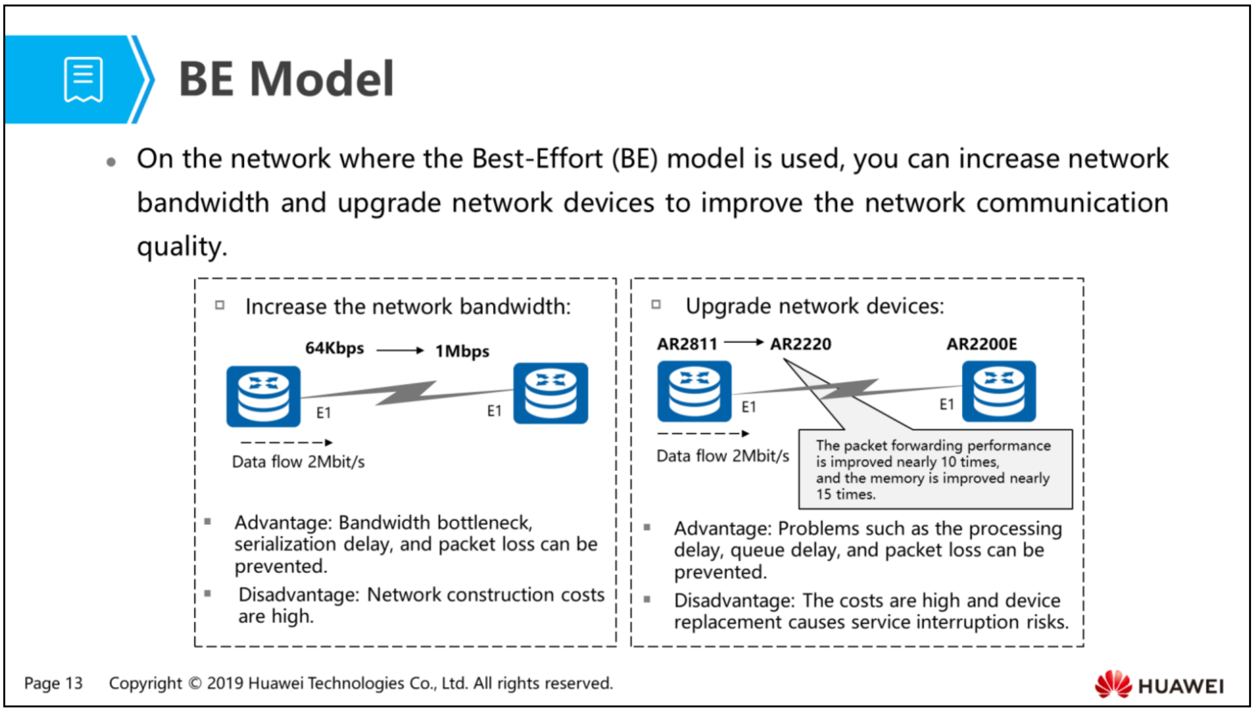
HUAWEI

- The packet loss ratio refers to the ratio of lost packets to transmitted packets. The packet loss ratio is used to measure network reliability. Packet loss may occur in all phases. For example:
    - Processing: The CPU of a router may be busy when the router receives packets. In this case, the router cannot process the packets in a timely manner, causing packet loss.
    - Queuing: When packets are scheduled in queues, packet loss may occur because the queue is full.
    - Transmission: During packet transmission on the link, packet loss may occur due to various causes such as the link fault.
- Loss of few packets does not affect services. For example, communicating parties do not detect the loss of one bit or packet during voice transmission. During video broadcasting, the loss of one bit or packet may cause transient waveform interference, but the video is restored immediately. When TCP is used to transmit data, TCP can process few lost packets. However, many lost packets seriously affect the transmission efficiency.
- After learning characteristics of the factors that affect the communication quality, which method can we use to improve the communication quality during network deployment?



Contents

1. Traditional Network Communication Quality Problems
2. Factors Affecting Network Communication Quality
3. **Solution to Improving Network Communication Quality**



BE Model

- On the network where the Best-Effort (BE) model is used, you can increase network bandwidth and upgrade network devices to improve the network communication quality.

- Increase the network bandwidth:

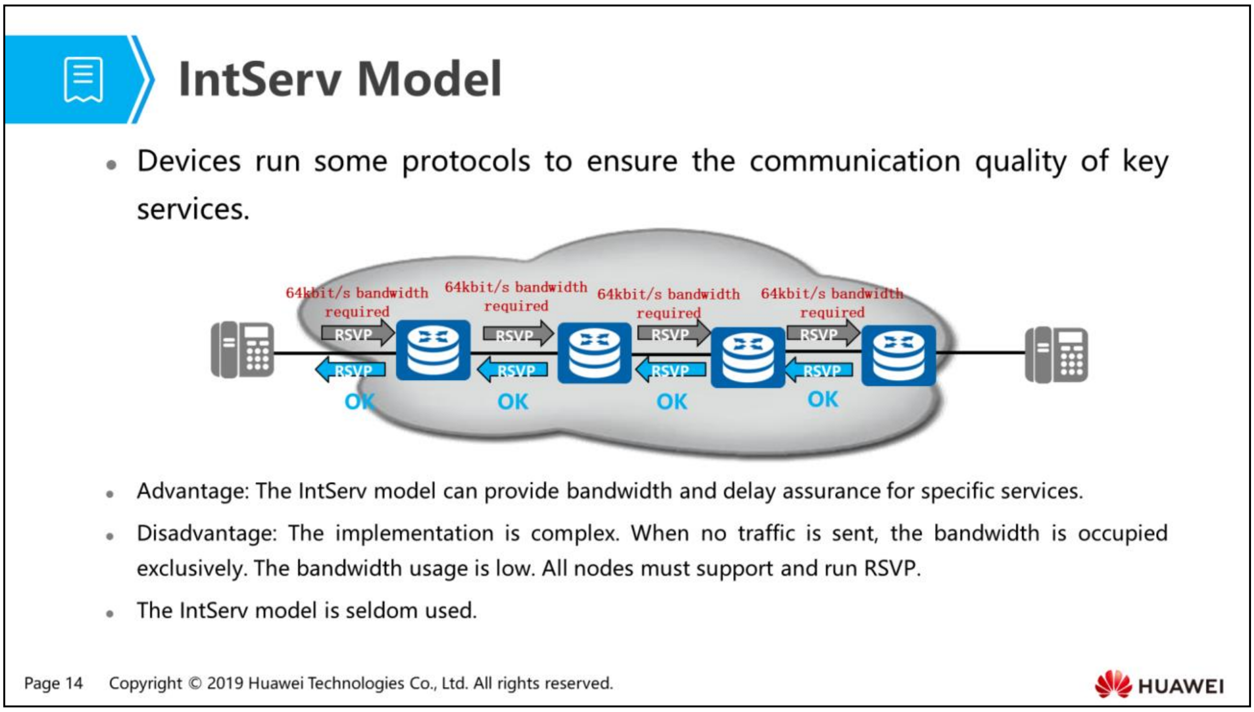
  - Advantage: Bandwidth bottleneck, serialization delay, and packet loss can be prevented.
  - Disadvantage: Network construction costs are high.

- Upgrade network devices:

The packet forwarding performance is improved nearly 10 times, and the memory is improved nearly 15 times.

  - Advantage: Problems such as the processing delay, queue delay, and packet loss can be prevented.
  - Disadvantage: The costs are high and device replacement causes service interruption risks.

- Traditional FIFO uses the Best-Effort (BE) model:
  - BE model is a unitary and the simplest service model. An application can send any number of packets at any time without any approval or notifying the network.
  - In the BE model, a network attempts to send packets, but cannot ensure performance such as delay and reliability. The BE model can be applied to various network applications, such as FTP and email.
  - The BE model is the default service model on the Internet and is implemented through the FIFO scheduling.
- In the BE model, you can increase the network bandwidth and upgrade network devices to improve the E2E network communication quality.
  - Network bandwidth increase: You can increase the amount of transmitted data in a unit time so that more data can be transmitted using FIFO. The network congestion problem can be relieved.
  - Network device upgrade: You can increase the data processing capability so that more data can be transmitted using FIFO. The network congestion problem can be relieved.



IntServ Model

- Devices run some protocols to ensure the communication quality of key services.

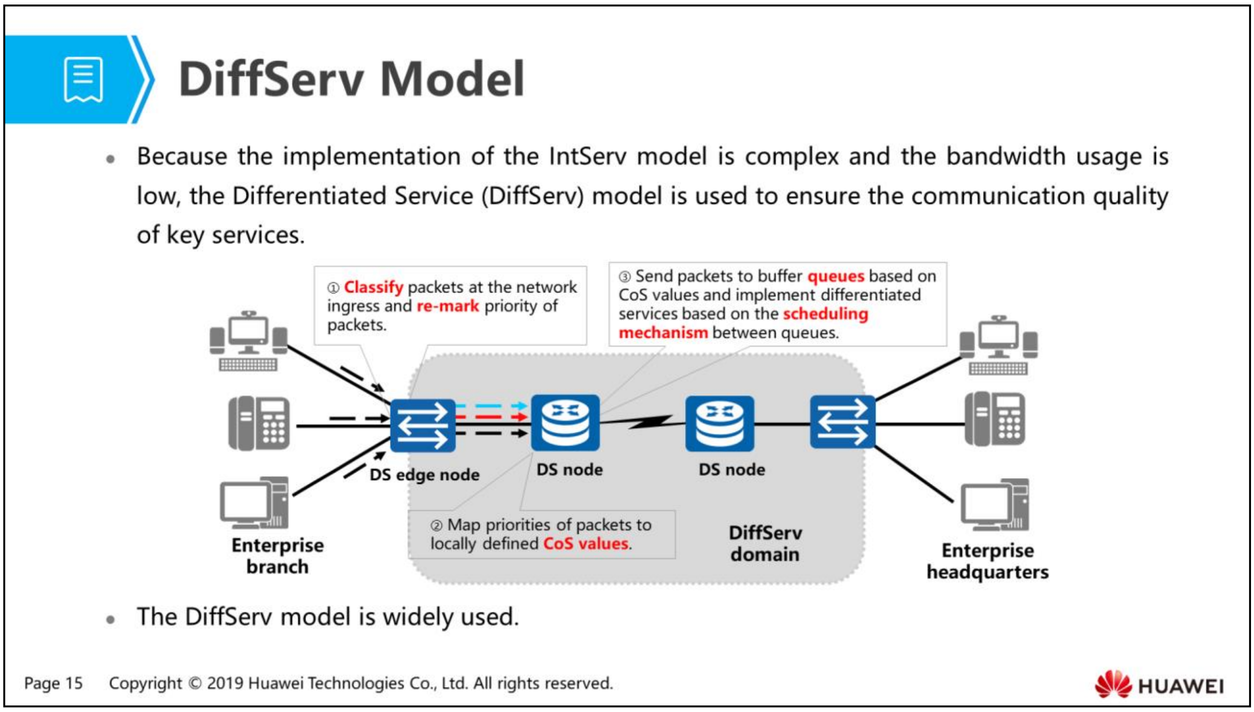
64kbit/s bandwidth required
64kbit/s bandwidth required
64kbit/s bandwidth required
64kbit/s bandwidth required
RSVP
RSVP
RSVP
RSVP
RSVP
RSVP
RSVP
RSVP
OK
OK
OK
OK

- Advantage: The IntServ model can provide bandwidth and delay assurance for specific services.
- Disadvantage: The implementation is complex. When no traffic is sent, the bandwidth is occupied exclusively. The bandwidth usage is low. All nodes must support and run RSVP.
- The IntServ model is seldom used.

Page 14

HUAWEI

- RSVP working process: Before an application sends packets, the application needs to request specific bandwidth and service quality. After receiving the acknowledgement message, the application sends packets.
- Integrated service model (InteServ model):
  - The IntServ model is complex and needs to use the Resource Reservation Protocol (RSVP). Before transmitting packets, the IntServ model needs to apply to the network for specific services. The request is implemented using signaling. An application notifies the network of its traffic parameters and the required specific service quality request, such as the bandwidth and delay. When receiving the acknowledgement information of the network, an application considers that the network has reserved resources for packet sending. Then the application immediately sends packets.
  - The IntServ model requires that all nodes on the network support RSVP and each node should periodically exchange status information with the neighboring node. This increases the costs of protocol packets. All network nodes need to maintain status information for each data flow. Tens of thousands of data flows are transmitted on the Internet backbone network are millions of data flows, so the IntServ model cannot be widely used on the Internet backbone network.



DiffServ Model

- Because the implementation of the IntServ model is complex and the bandwidth usage is low, the Differentiated Service (DiffServ) model is used to ensure the communication quality of key services.

① **Classify** packets at the network ingress and **re-mark** priority of packets.

③ Send packets to buffer **queues** based on CoS values and implement differentiated services based on the **scheduling mechanism** between queues.

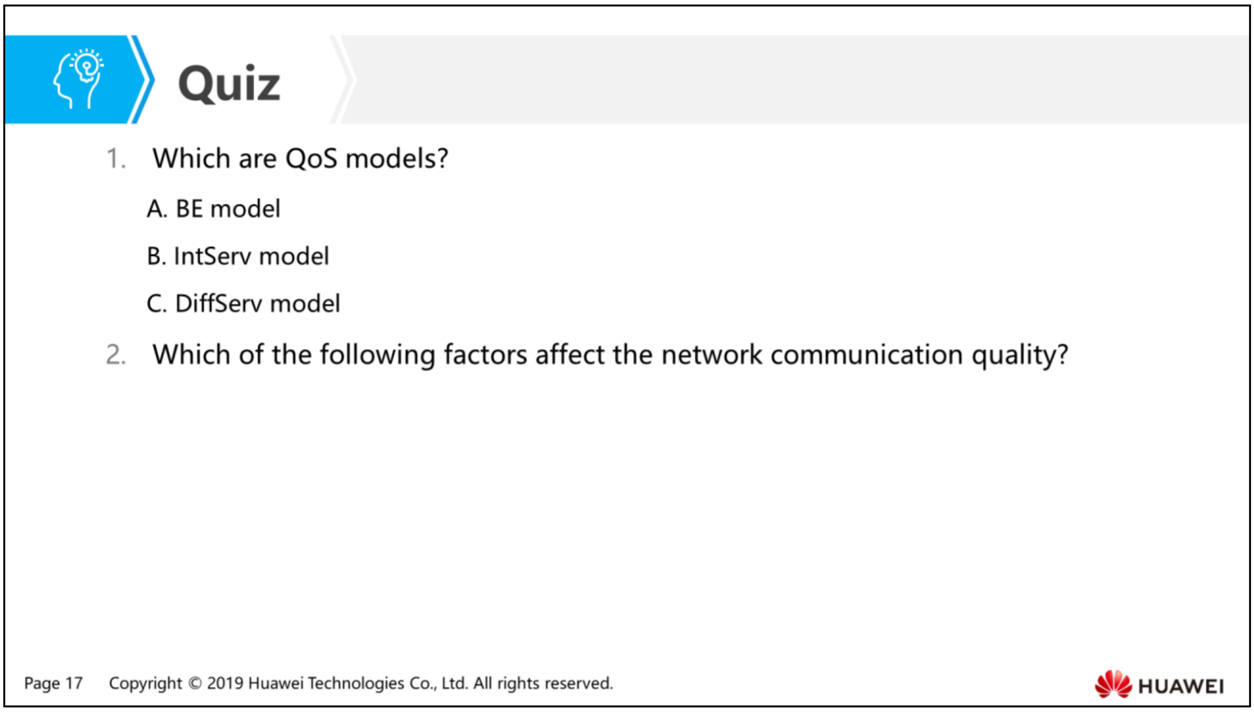
② Map priorities of packets to locally defined **CoS values**.

- The DiffServ model is widely used.

- Working process of the DiffServ model: Traffic is classified into multiple types and an action is defined for each type so that different traffic has different forwarding priorities, packet loss ratios, and delays.
- DiffServ model:
  - Traffic classification and marking are implemented by the edge router. Edge routers classify packets based on a combination of fields, such as the source and destination addresses of packets, precedence in the ToS field, and protocol type. Edge routers also re-mark packets with different priorities, which can be identified by other routers for resource allocation and traffic control. Therefore, DiffServ is a flow-based QoS model.
  - It contains only a limited number of service classes and less status information to provide differentiated traffic control and forwarding.
  - A DS node is a network node that implements the DiffServ function.
  - A DS edge node connects to another DS domain or a non-DS-aware domain. The DS edge node classifies and adjusts the traffic entering the DS domain.
  - A DS internal node connects to DS edge nodes and other internal nodes in the same DS domain. DS internal nodes implement simple traffic classification based on EXP, 802.1p, and IPP values, and manage traffic.
  - A DS domain consists of DS nodes that use the same service policy and Per Hop Behavior (PHB). One DS domain consists of one or more networks under the same administration. For example, a DS domain can be an ISP's networks or an enterprise's intranet.
  - DiffServ considers advantages of network flexibility and extensibility of the IP network and transforms information in packets into PHBs, greatly reducing signaling operations. This model is the most widely used model.

Comparison Between Three Service Models

Service Models	Advantage	Disadvantage
BE Model	The implementation is simple.	It cannot differentiate different service flows.
IntServ Model	The IntServ model provides E2E QoS services and ensures the bandwidth and delay.	The IntServ model needs to trace and record the status of each data flow. The implementation is complex, the scalability is low, and the bandwidth usage is low.
DiffServ Model	The DiffServ model does not need to trace the status of each data flow, occupies a few resources, and has strong extensibility. In addition, this model can implement differentiated services.	The DiffServ model needs to be deployed on each node, and there are high requirements for technical personnel's capabilities.



Quiz

1. Which are QoS models?

   A. BE model

   B. IntServ model

   C. DiffServ model

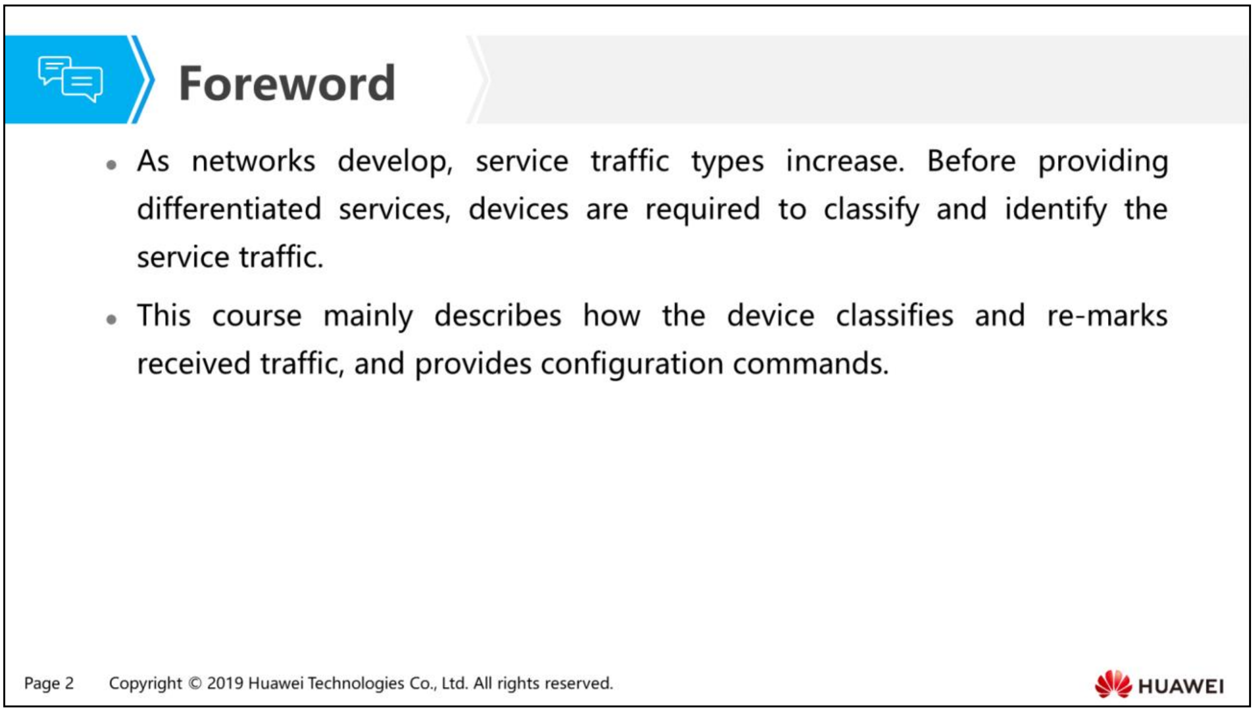
2. Which of the following factors affect the network communication quality?

- Answer: ABC.
- Answer: bandwidth, delay, jitter, packet loss ratio.

Thank You

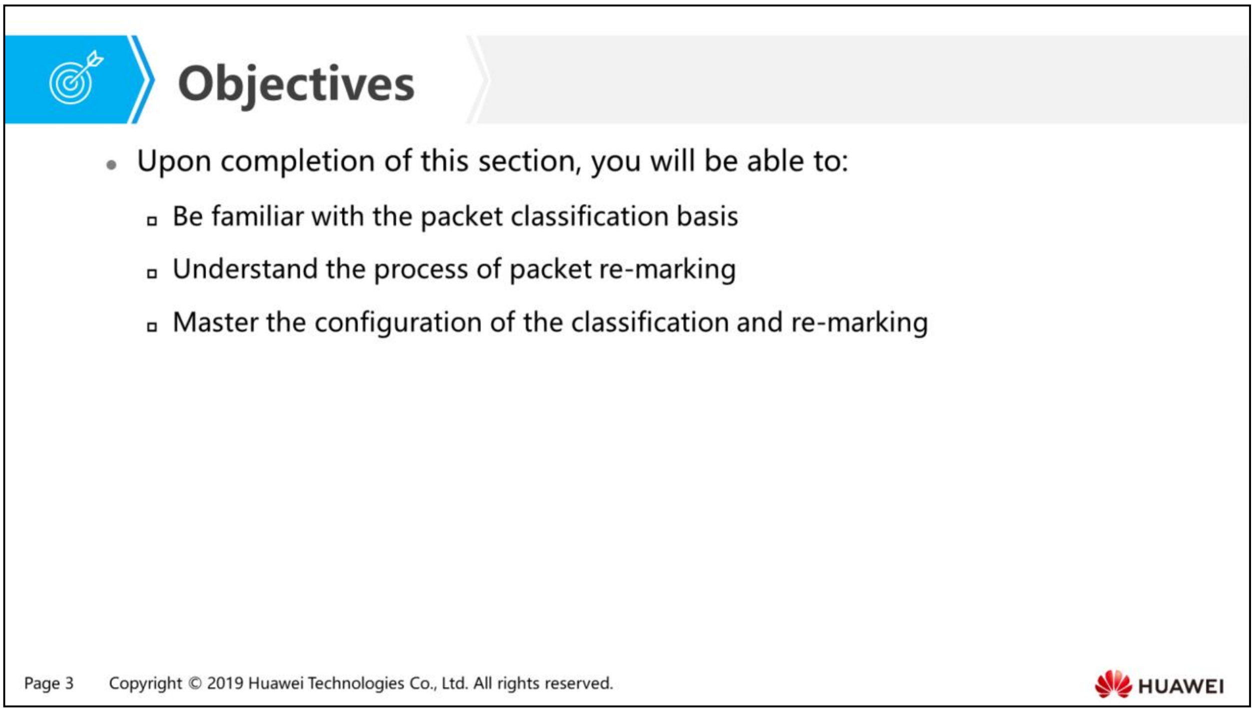
www.huawei.com

Traffic Classification and Re-marking



Foreword

- As networks develop, service traffic types increase. Before providing differentiated services, devices are required to classify and identify the service traffic.
- This course mainly describes how the device classifies and re-marks received traffic, and provides configuration commands.

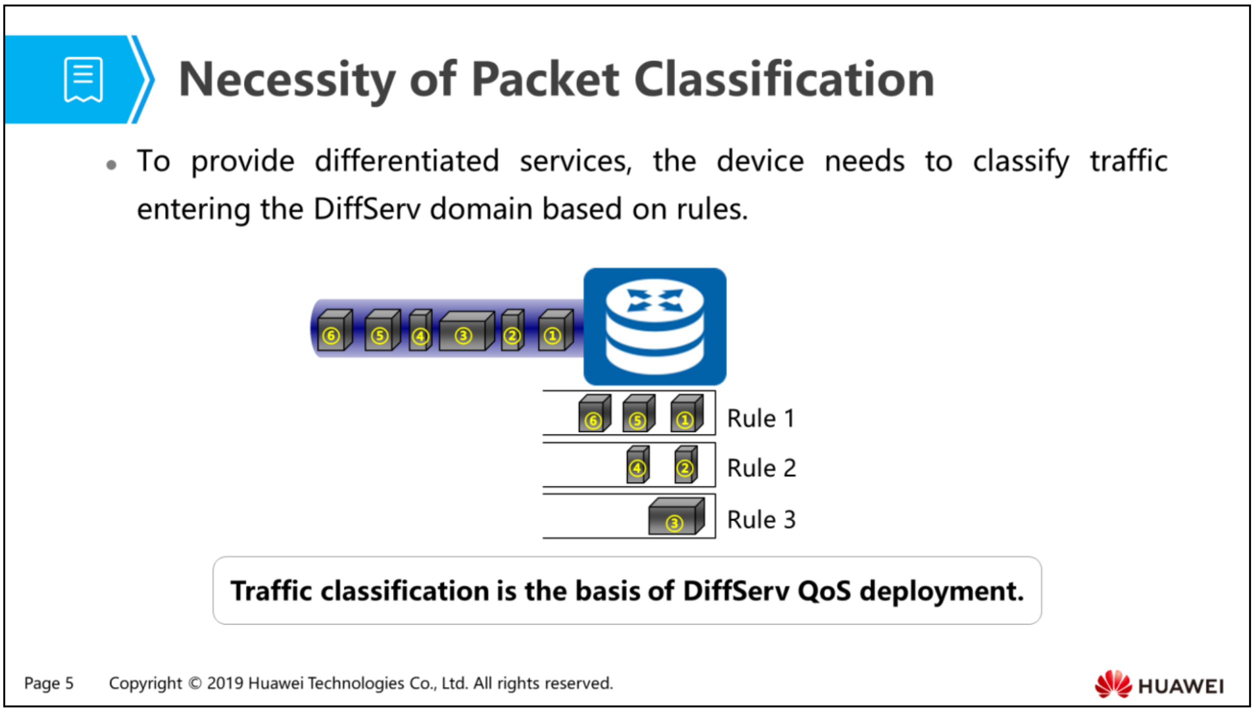


Objectives

- Upon completion of this section, you will be able to:
  - Be familiar with the packet classification basis
  - Understand the process of packet re-marking
  - Master the configuration of the classification and re-marking

Contents

1. **Packet Classification Process**
2. Packet Classification Configuration
3. Packet Re-marking Process
4. Packet Re-marking Configuration



Necessity of Packet Classification

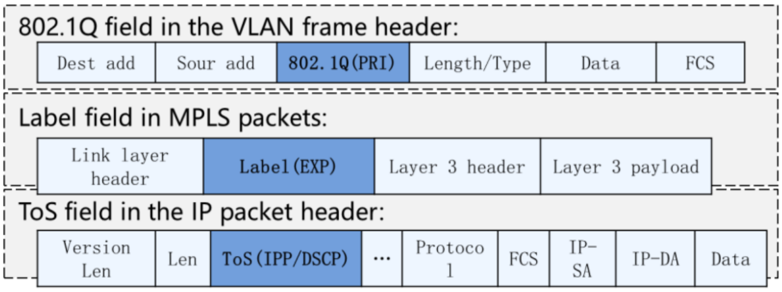
- To provide differentiated services, the device needs to classify traffic entering the DiffServ domain based on rules.

Traffic classification is the basis of DiffServ QoS deployment.

- What is the packet classification basis? ACLs can be used to match the 5-tuple of packets for classification? What are traffic classification modes?

Packet Classification Basis

- Packet classification technology can transmit different types of packets based on link types and QoS priority fields in packets.



802.1Q field in the VLAN frame header:

Dest add	Sour add	802.1Q(PRI)	Length/Type	Data	FCS

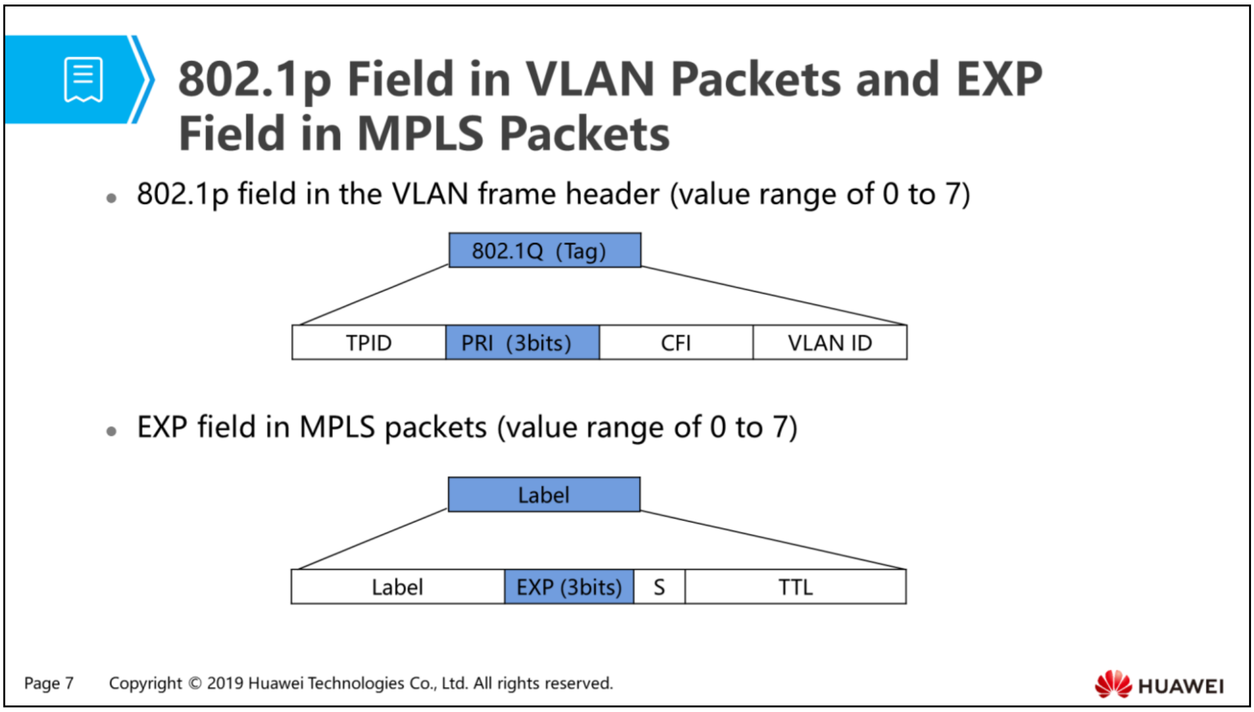
Label field in MPLS packets:

Link layer header	Label(EXP)	Layer 3 header	Layer 3 payload

ToS field in the IP packet header:

Version Len	Len	ToS(IPP/DSCP)	…	Protocol	FCS	IP-SA	IP-DA	Data

- One traffic classification mode is used and matching rules are simple, so this classification is called simple traffic classification.



802.1p Field in VLAN Packets and EXP Field in MPLS Packets

- 802.1p field in the VLAN frame header (value range of 0 to 7)

802.1Q (Tag)

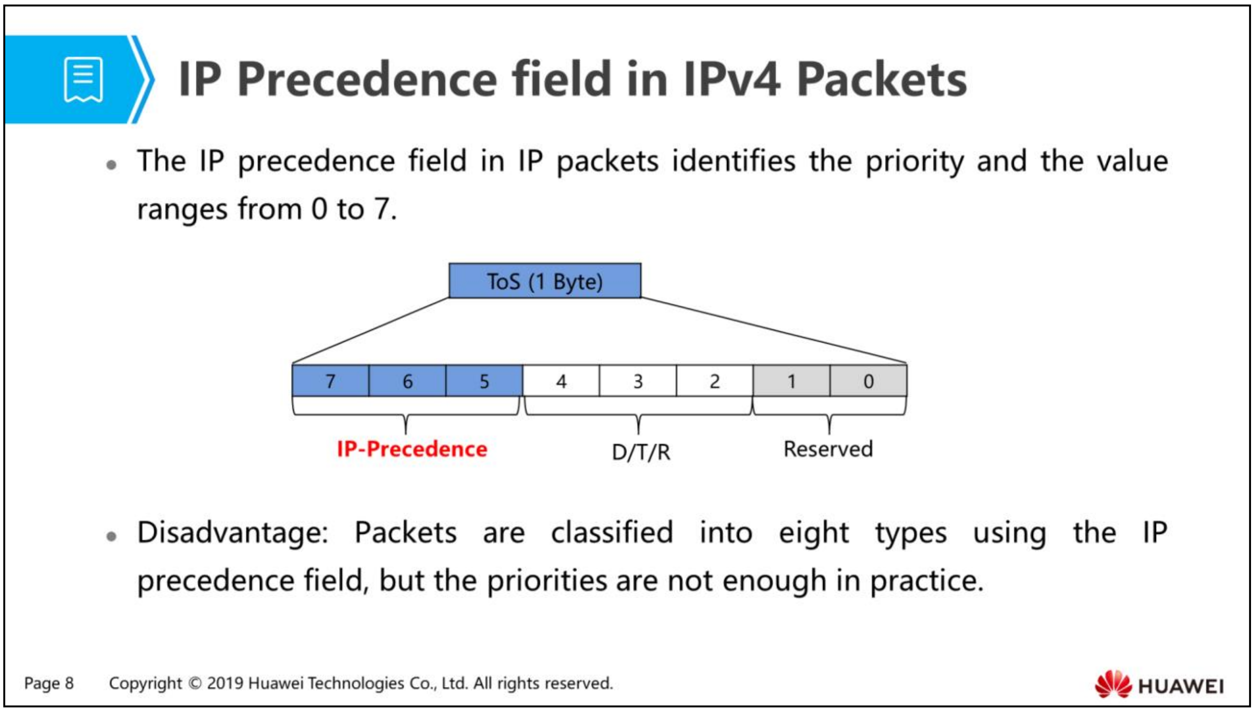
TPID	PRI (3bits)	CFI	VLAN ID

- EXP field in MPLS packets (value range of 0 to 7)

Label

Label	EXP (3bits)	S	TTL

- As defined by IEEE 802.1Q, the PRI field in the VLAN tag is used to identify the QoS service level.
- The EXP field is used as the CoS field in MPLS packets and is equivalent to the ToS field in IP packets. The EXP field is used to differentiate data flows on MPLS networks.

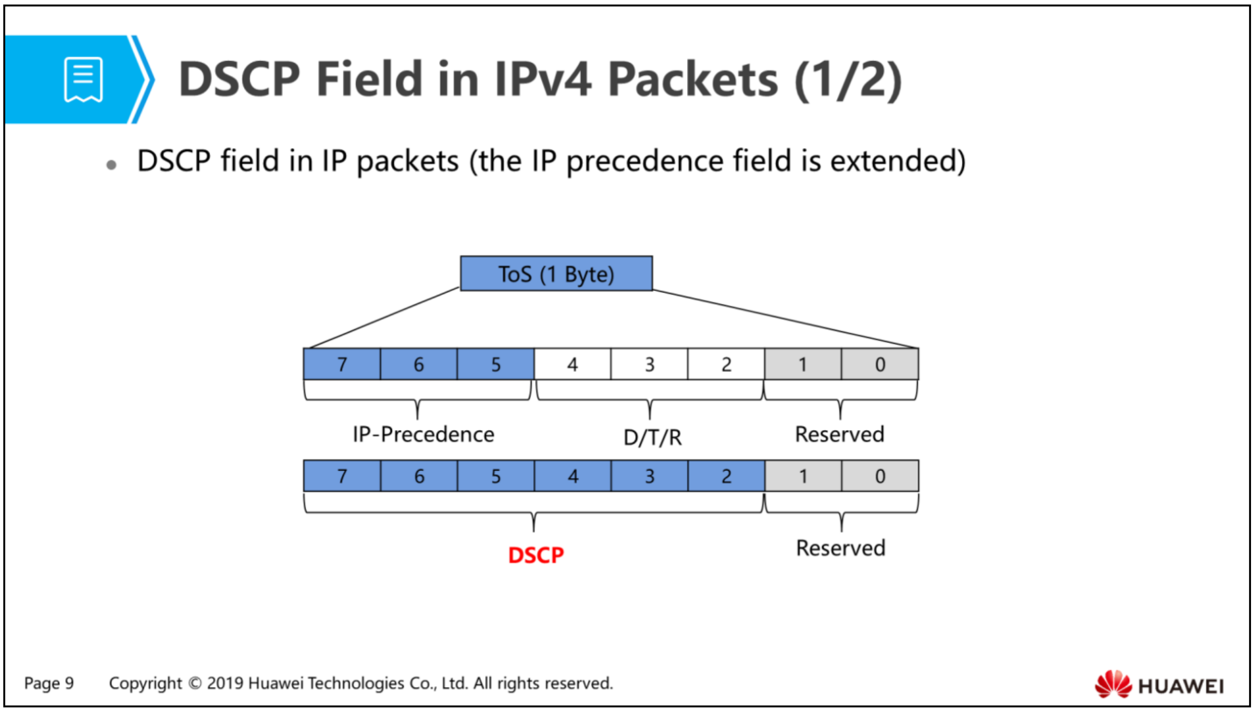


IP Precedence field in IPv4 Packets

- The IP precedence field in IP packets identifies the priority and the value ranges from 0 to 7.

- Disadvantage: Packets are classified into eight types using the IP precedence field, but the priorities are not enough in practice.

- Bit D represents the delay, bit T represents the throughput, and bit R represents the reliability.
- As defined by RFC 791, the precedence subfield in the ToS field of the IP packet header identifies the priority of a packet.



DSCP Field in IPv4 Packets (1/2)

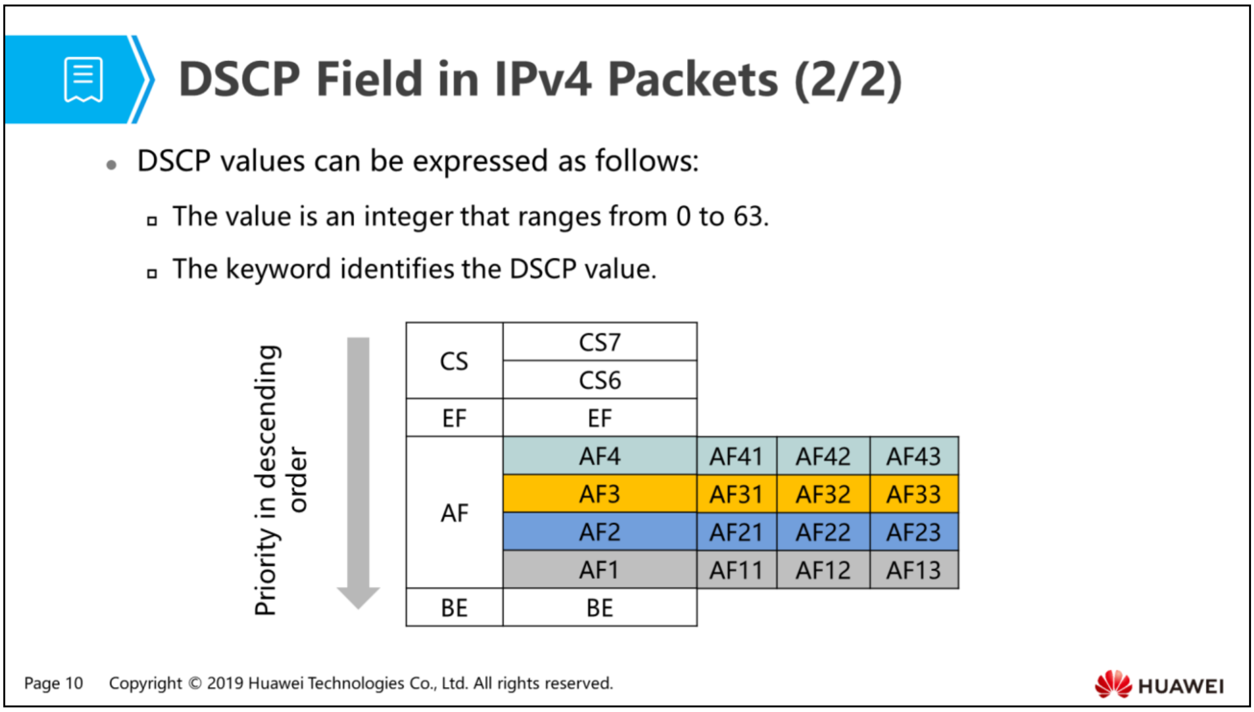
- DSCP field in IP packets (the IP precedence field is extended)

ToS (1 Byte)

7	6	5	4	3	2	1	0
IP-Precedence			D/T/R			Reserved	

7	6	5	4	3	2	1	0
DSCP						Reserved	

- RFC 2474 redefines the ToS field in the IPv4 packet header as the Differentiated Service (DS) field.



DSCP Field in IPv4 Packets (2/2)

- DSCP values can be expressed as follows:
  - The value is an integer that ranges from 0 to 63.
  - The keyword identifies the DSCP value.

Priority in descending order

CS	CS7			
	CS6			
EF	EF			
AF	AF4	AF41	AF42	AF43
	AF3	AF31	AF32	AF33
	AF2	AF21	AF22	AF23
	AF1	AF11	AF12	AF13
BE	BE			

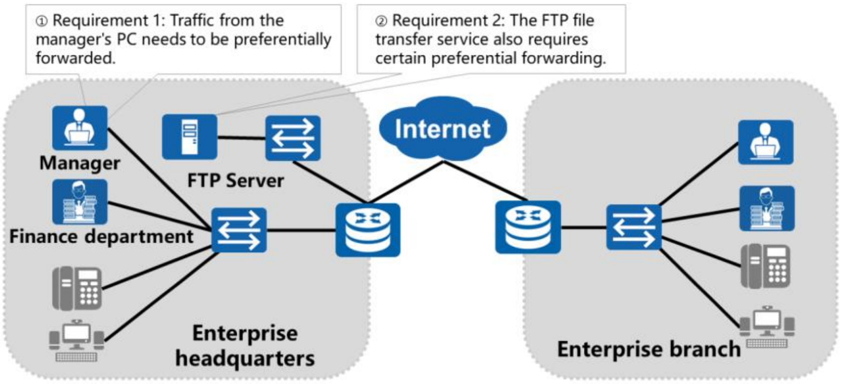
- For AFxy, x represents a different type. Queues can be defined based on types. y indicates the packet loss probability when queues are full. For packets of AF1, the packet loss probability is AF11, AF12, and AF13 in ascending order.
- Different keywords are usually used to identify packets:
  - CS6 and CS7 are used to transmit protocol packets by default. For devices of most vendors, CS6 and CS7 queues have the highest priority among hardware queues. If the protocols packets cannot be received, protocol services are interrupted.
  - EF is often used to carry voice services. This is because voice services require low delay, low jitter, and low packet loss ratio, and voice packets are second only to protocol packets in terms of importance.
  - AF4 is used to transmit voice signaling traffic. Why does voice have a higher priority than signaling? Here, signaling refers to telephone call control. Users can wait for several seconds before call connections, but cannot tolerate communication interruption. This is the reason why voice has a higher priority than signaling.
  - AF3 is used to carry live broadcast traffic generated by IPTV. The real-time live broadcast requires high continuity and throughout.
  - AF2 is used to transmit VoD (Video on Demand) traffic. Compared with live traffic, VoD traffic allows delay or buffer.
  - AF1 is used to carry common Internet access services.

DSCP/IP Precedence/802.1p/EXP

DSCP Name				DSCP Value			IP-Precedence	802.1p	EXP
BE	BE (CS0)			0			0		
CS	CS1			8			1		
	CS2			16			2		
	CS3			24			3		
	CS4			32			4		
	CS5			40			5		
	CS6			48			6		
	CS7			56			7		
AF	AF11	AF12	AF13	10	12	14	1		
	AF21	AF22	AF23	18	20	22	2		
	AF31	AF32	AF33	26	28	30	3		
	AF41	AF42	AF43	34	36	38	4		
EF	EF			46			5		

Limitations of Simple Traffic Classification

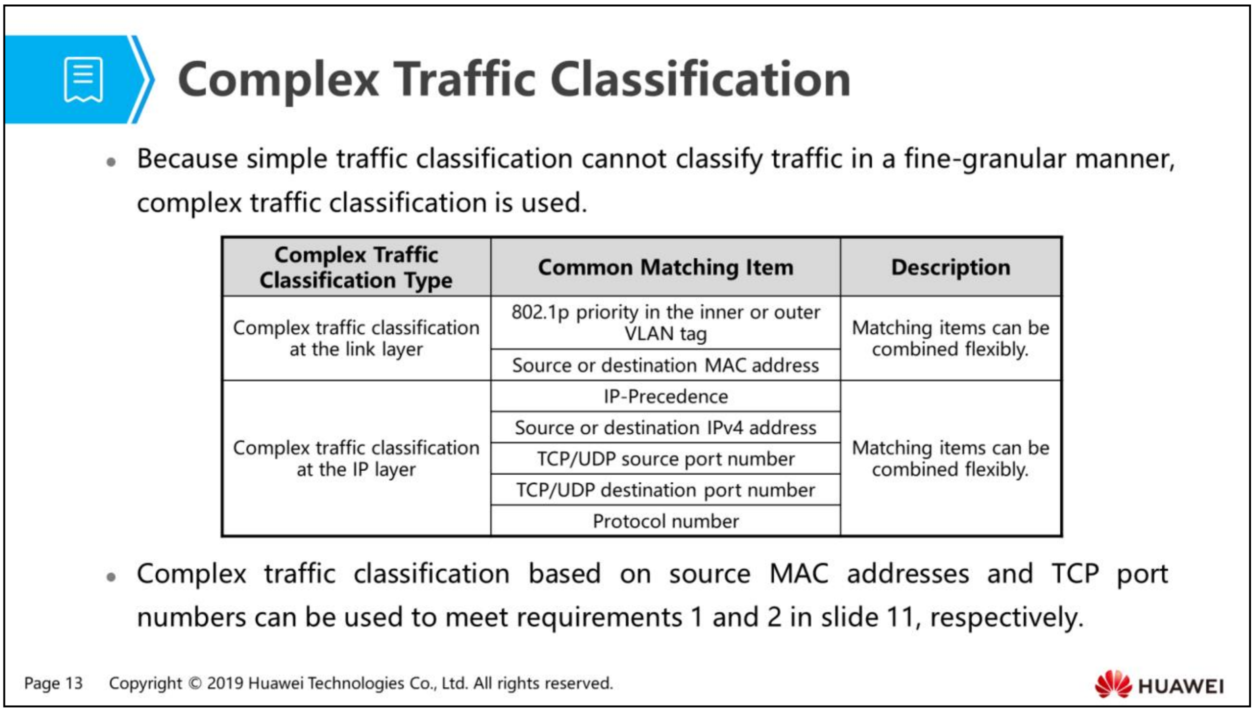
- In practice, there are more complex classification requirements:



① Requirement 1: Traffic from the manager's PC needs to be preferentially forwarded.

② Requirement 2: The FTP file transfer service also requires certain preferential forwarding.

- Simple traffic classification cannot meet the preceding requirements.



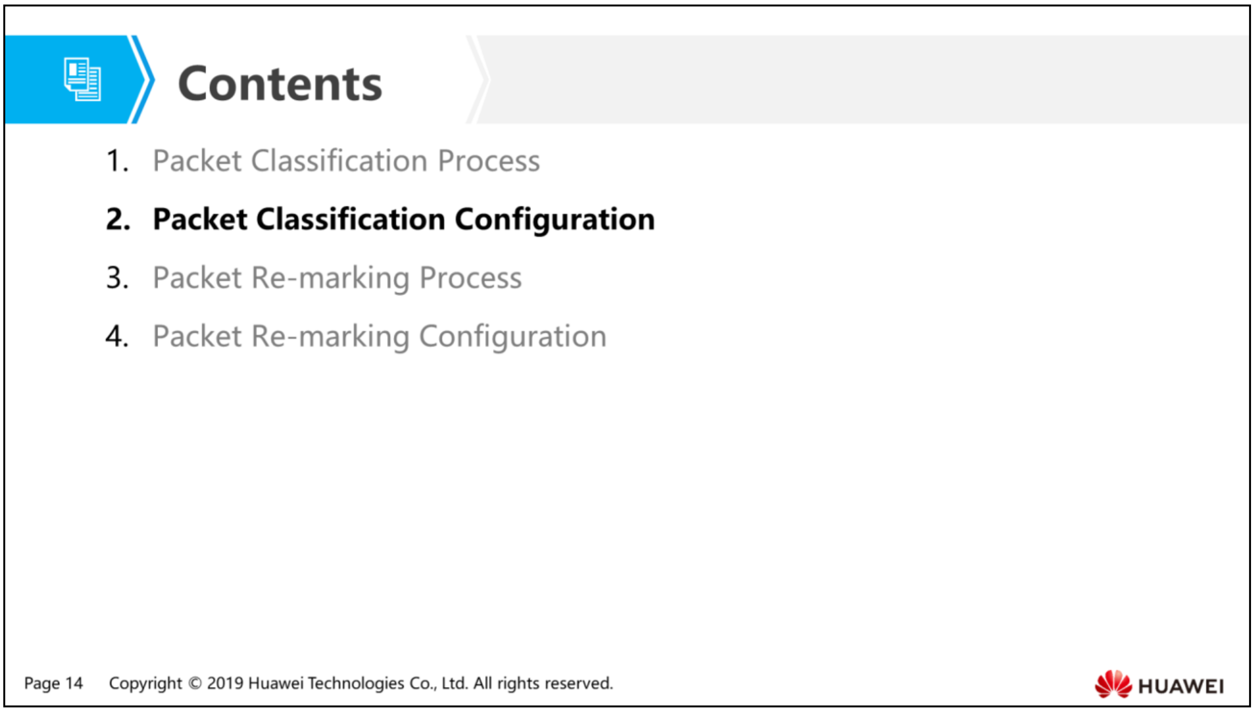
Complex Traffic Classification

- Because simple traffic classification cannot classify traffic in a fine-granular manner, complex traffic classification is used.

Complex Traffic Classification Type	Common Matching Item	Description
Complex traffic classification at the link layer	802.1p priority in the inner or outer VLAN tag	Matching items can be combined flexibly.
	Source or destination MAC address	
Complex traffic classification at the IP layer	IP-Precedence	Matching items can be combined flexibly.
	Source or destination IPv4 address	
	TCP/UDP source port number	
	TCP/UDP destination port number	
	Protocol number	

- Complex traffic classification based on source MAC addresses and TCP port numbers can be used to meet requirements 1 and 2 in slide 11, respectively.

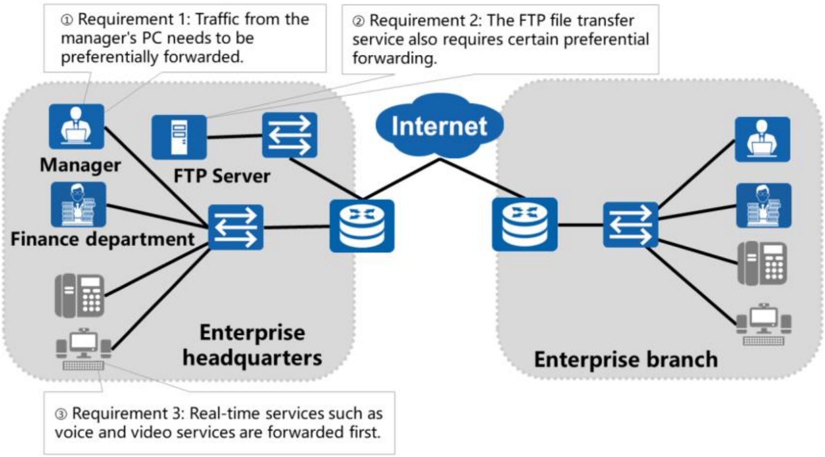
- Complex traffic classification
    - Complex traffic classification classifies packets based on 5-tuple information (source IP address, destination IP address, source port number, destination port number, and protocol number) in a fine-granular manner. Generally, packets are classified based on packet header information, and packet contents are seldom used for classification.
    - Complex traffic classification is applied at the network edge by default. When packets enter the edge node, network administrators can flexibly configure classification rules.



Contents

1. Packet Classification Process
2. **Packet Classification Configuration**
3. Packet Re-marking Process
4. Packet Re-marking Configuration

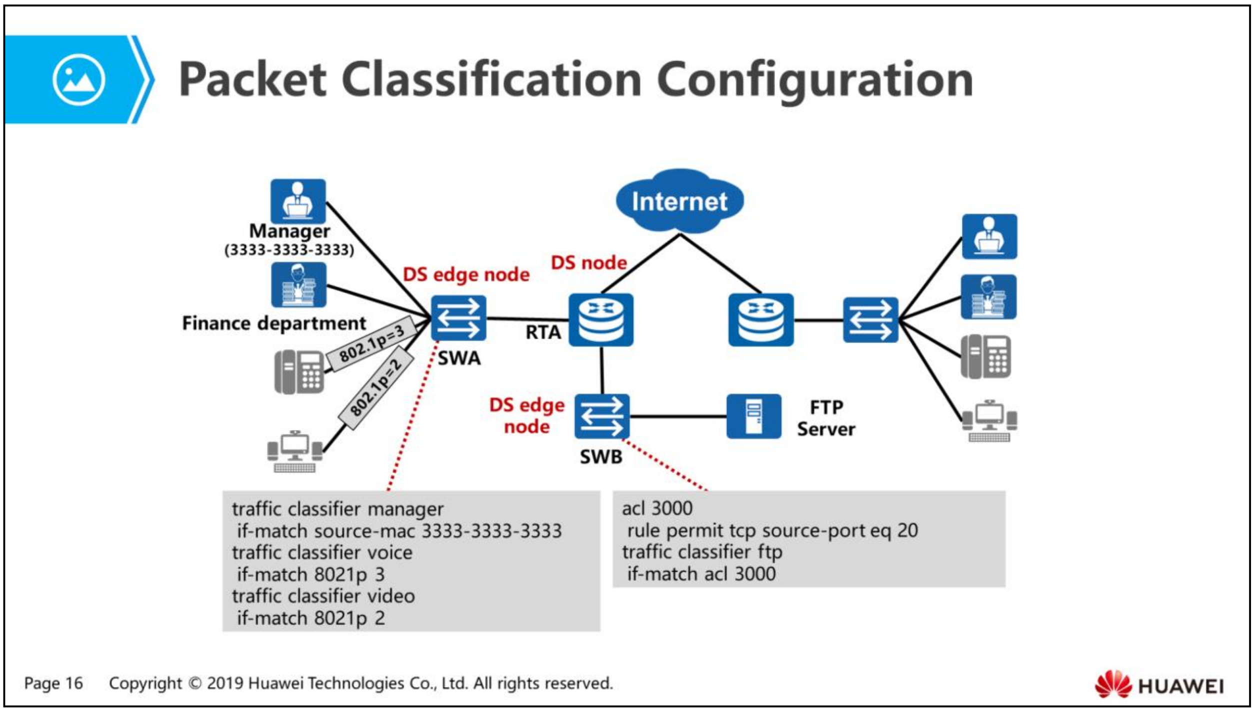
Packet Classification Configuration Requirements



① Requirement 1: Traffic from the manager's PC needs to be preferentially forwarded.

② Requirement 2: The FTP file transfer service also requires certain preferential forwarding.

③ Requirement 3: Real-time services such as voice and video services are forwarded first.



Packet Classification Configuration

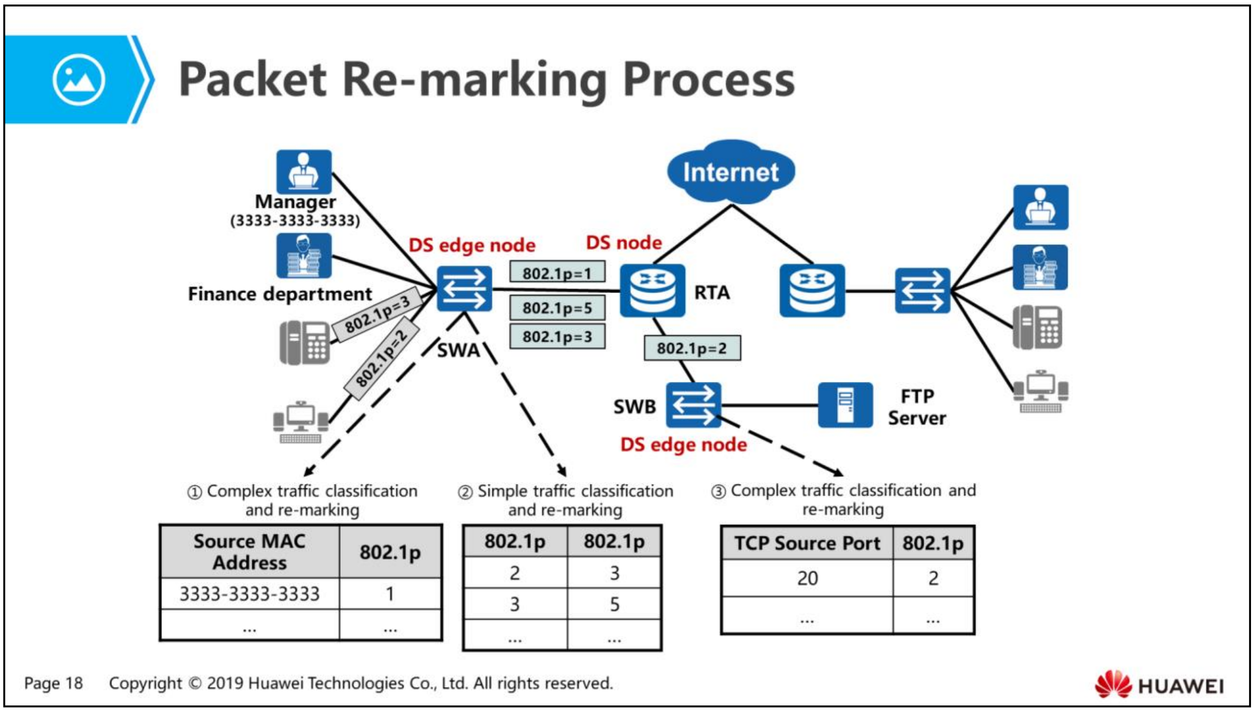
```
traffic classifier manager
 if-match source-mac 3333-3333-3333
traffic classifier voice
 if-match 8021p 3
traffic classifier video
 if-match 8021p 2
```

```
acl 3000
 rule permit tcp source-port eq 20
traffic classifier ftp
 if-match acl 3000
```

- Generally, packets are often classified on the DS edge nodes (for example, SWA and SWB).
- The downstream device can accept the classification result of the upstream device or re-classify packets based on its classification standard.
- During E2E QoS deployment, if each device needs to classify packets, many device processing resources are consumed. In this case, packet re-marking is used so that the downstream device only needs to identify re-marked priorities to provide differentiated services. How re-marking is implemented?

Contents

1. Packet Classification Process
2. Packet Classification Configuration
3. **Packet Re-marking Process**
4. Packet Re-marking Configuration



Packet Re-marking Process

① Complex traffic classification and re-marking

Source MAC Address	802.1p
3333-3333-3333	1
...	...

② Simple traffic classification and re-marking

802.1p	802.1p
2	3
3	5
...	...

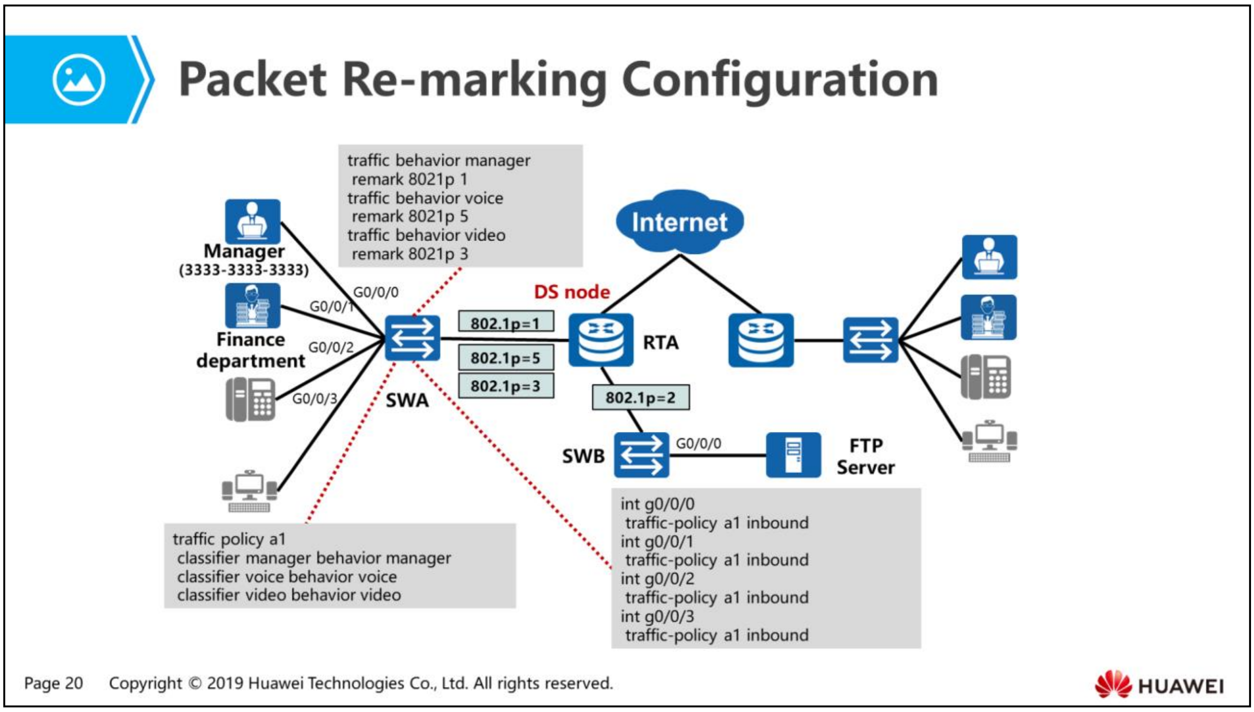
③ Complex traffic classification and re-marking

TCP Source Port	802.1p
20	2
...	...

- Packets are often re-marked on the DS edge nodes (for example, SWA and SWB). The DS node identifies re-marked priorities to provide differentiated services.
- The packets sent by devices such as voice phones and video terminals often carry default priorities of devices. To use user-defined values to provide differentiated services, configure the device to re-mark packets.

Contents

1. Packet Classification Process
2. Packet Classification Configuration
3. Packet Re-marking Process
4. **Packet Re-marking Configuration**



Packet Re-marking Configuration

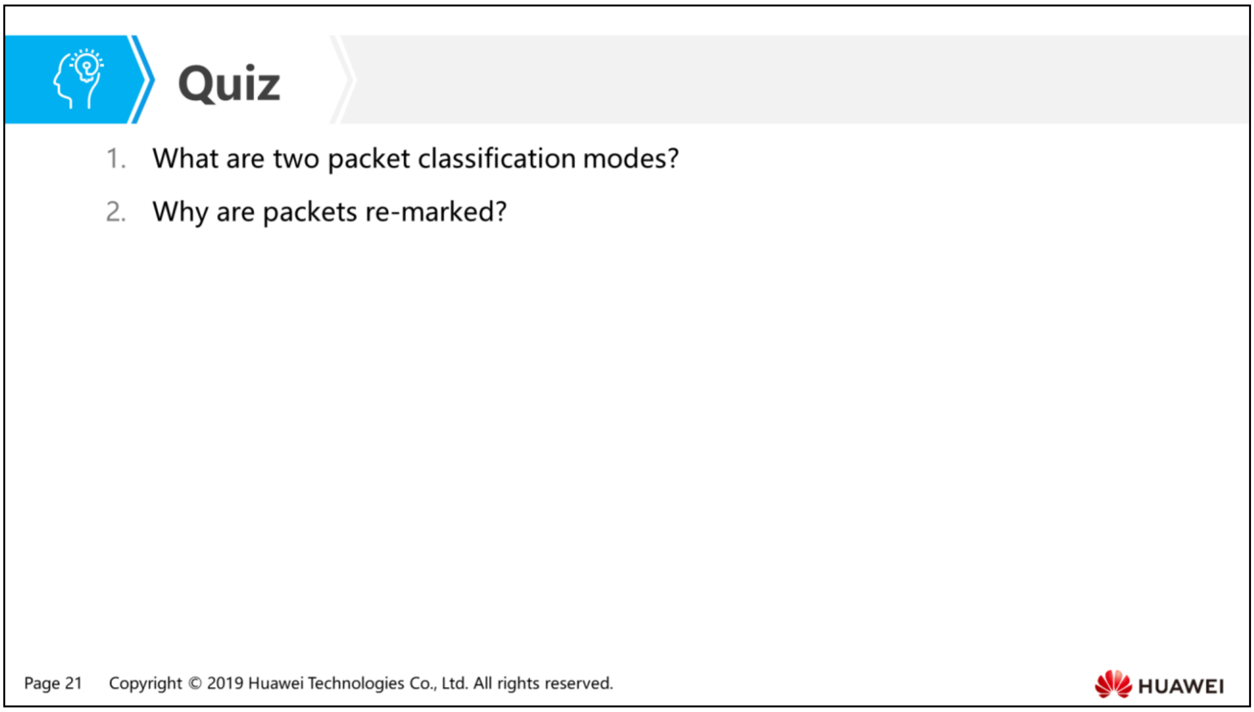
```
traffic behavior manager
 remark 8021p 1
traffic behavior voice
 remark 8021p 5
traffic behavior video
 remark 8021p 3
```

```
traffic policy a1
 classifier manager behavior manager
 classifier voice behavior voice
 classifier video behavior video
```

```
int g0/0/0
 traffic-policy a1 inbound
int g0/0/1
 traffic-policy a1 inbound
int g0/0/2
 traffic-policy a1 inbound
int g0/0/3
 traffic-policy a1 inbound
```

HUAWEI

- SWA re-marks packets and provides the trusted priority for the DS domain. The DS node can provide QoS scheduling services based on the re-marked value.
- In this example, SWA is called trusted boundary.



Quiz

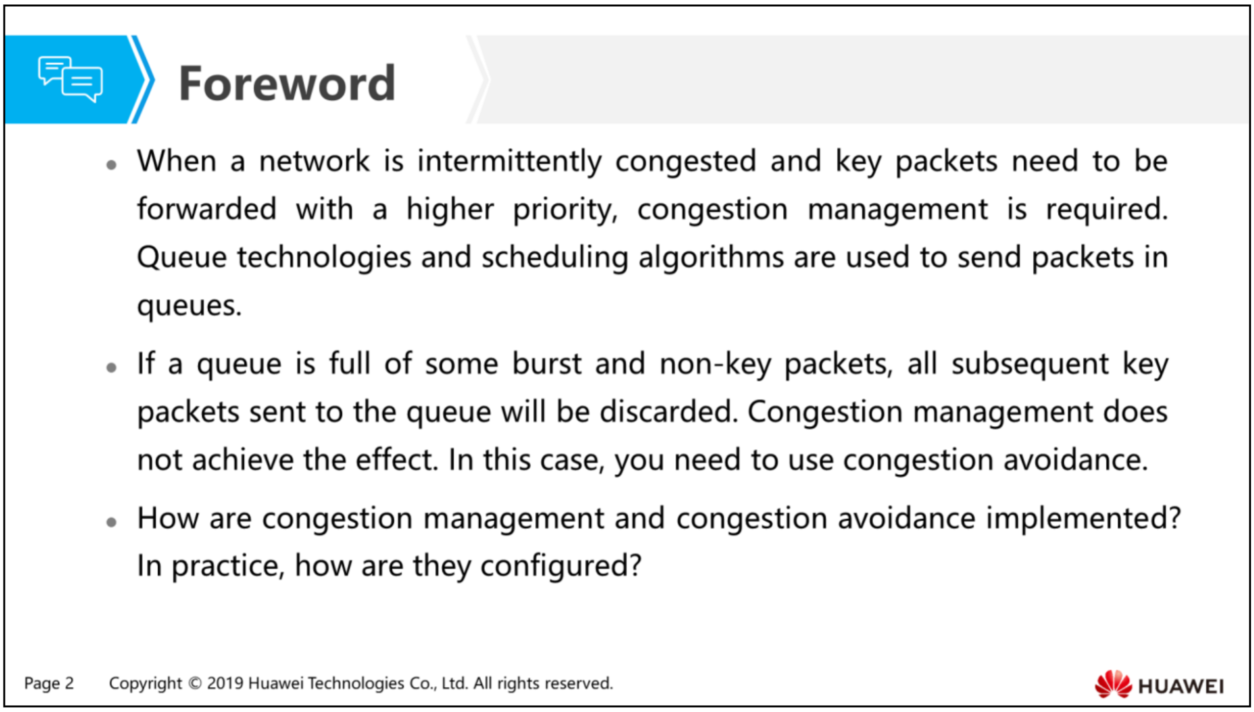
1. What are two packet classification modes?
2. Why are packets re-marked?

- Answer: Simple traffic classification and complex traffic classification.
- Answer: During E2E QoS deployment, if each device needs to classify packets, many device processing resources are consumed. In this case, packet re-marking is used so that the downstream device only needs to identify re-marked priorities to provide differentiated services.

Thank You

www.huawei.com

Congestion Management and Congestion Avoidance



Foreword

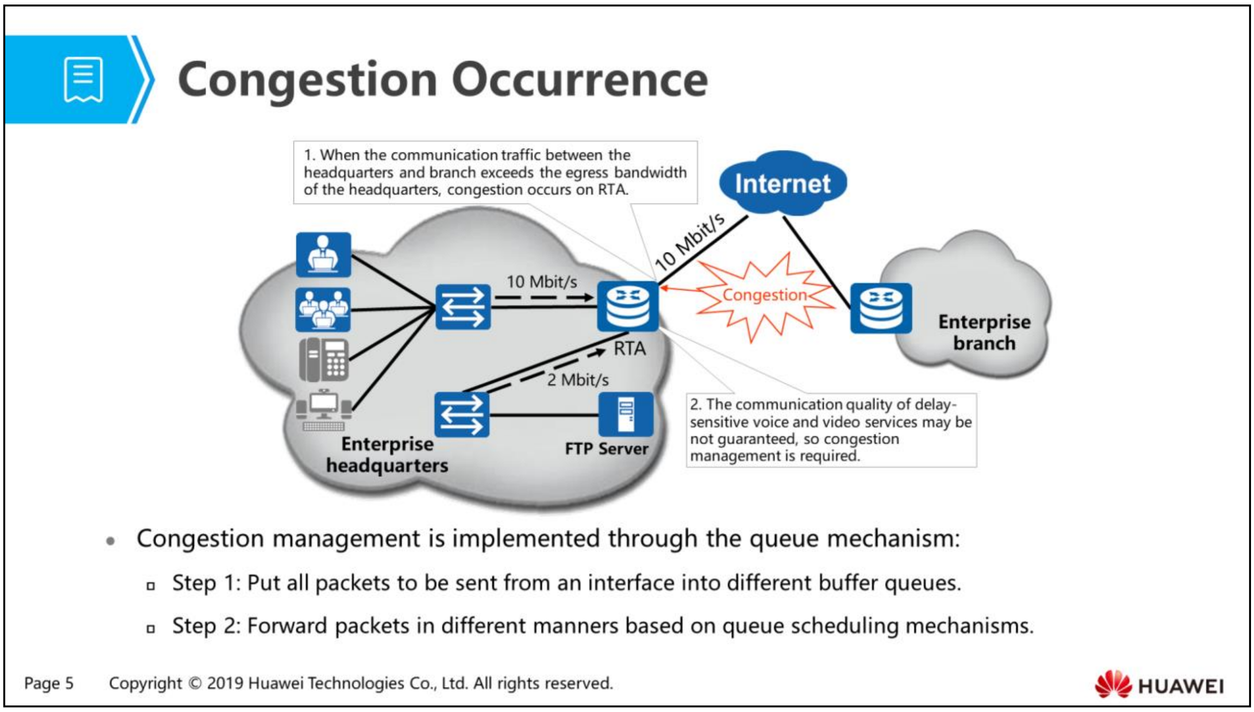
- When a network is intermittently congested and key packets need to be forwarded with a higher priority, congestion management is required. Queue technologies and scheduling algorithms are used to send packets in queues.
- If a queue is full of some burst and non-key packets, all subsequent key packets sent to the queue will be discarded. Congestion management does not achieve the effect. In this case, you need to use congestion avoidance.
- How are congestion management and congestion avoidance implemented? In practice, how are they configured?

Objectives

- Upon completion of this section, you will be able to:
  - Understand the implementation of congestion management
  - Be familiar with common queue scheduling algorithms
  - Be familiar with the disadvantages and solution of tail drop

Contents

1. **Congestion Management**
    - Congestion Occurrence and Solution
    - Common Queue Scheduling Algorithms
    - Implementation of Congestion Management
2. Congestion Avoidance



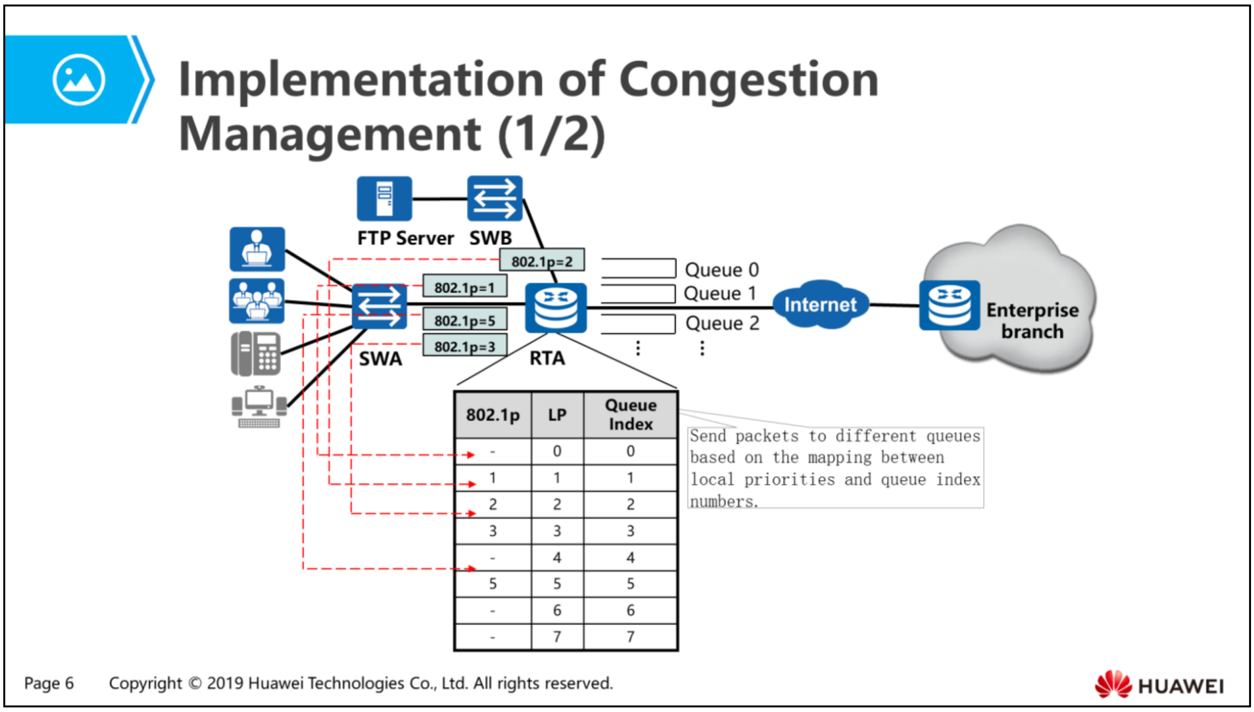
Congestion Occurrence

1. When the communication traffic between the headquarters and branch exceeds the egress bandwidth of the headquarters, congestion occurs on RTA.

2. The communication quality of delay-sensitive voice and video services may be not guaranteed, so congestion management is required.

- Congestion management is implemented through the queue mechanism:
  - Step 1: Put all packets to be sent from an interface into different buffer queues.
  - Step 2: Forward packets in different manners based on queue scheduling mechanisms.

- Congestion occurs in the following scenarios:
  - Rate not matched: Packets enter a device through a high-speed link and are forwarded through a low-speed link.
  - Aggregation: Packets are transmitted to a device from multiple interfaces and are forwarded through a single interface without enough bandwidth.
- Traffic congestion has the following adverse impacts:
  - Increases the packet transmission delay and jitter.
  - Causes packet retransmission due to overlong delays.
  - Lowers the network throughput.
  - Occupies a large number of network resources, especially the storage resources. Improper resource allocation may cause resources to be locked and the system to go Down.
- Due to traffic congestion, traffic cannot obtain resources in a timely manner. Traffic congestion is the main cause for performance deterioration. Traffic congestion often occurs on the packet switched network (PSN) and in multi-service scenarios, so traffic congestion must be prevented or effectively controlled. What is the implementation?

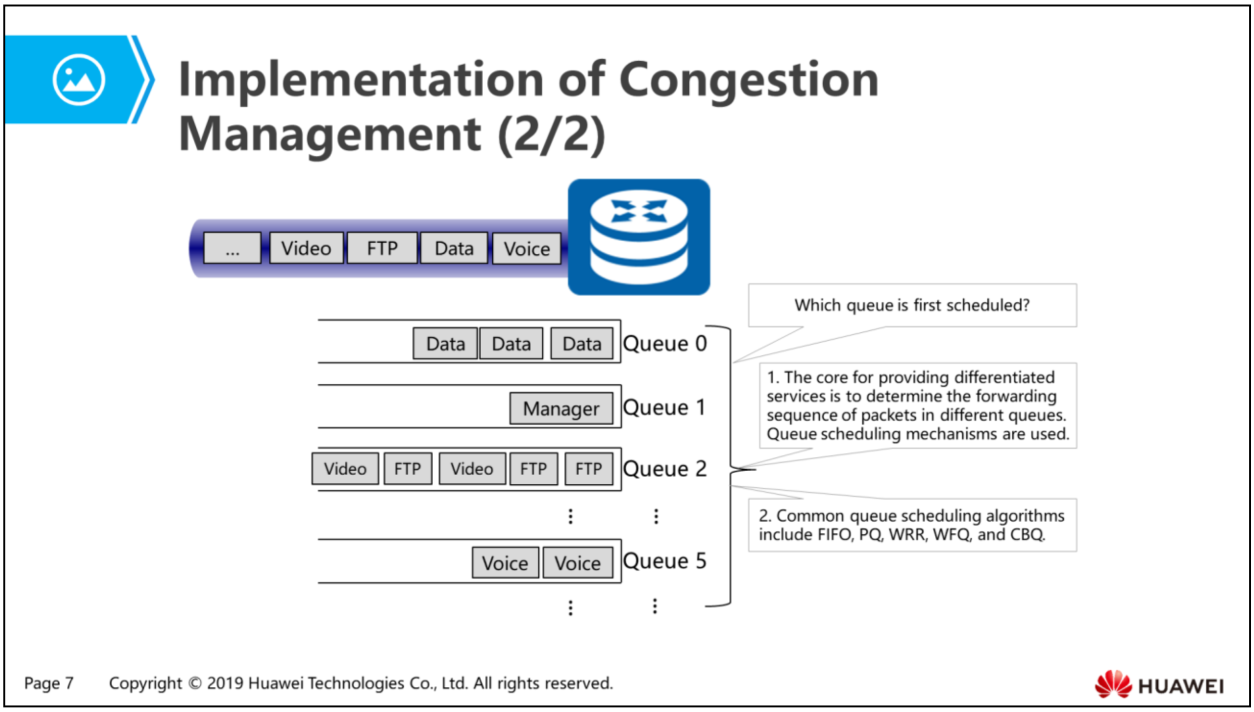


Implementation of Congestion Management (1/2)

802.1p	LP	Queue Index
-	0	0
1	1	1
2	2	2
3	3	3
-	4	4
5	5	5
-	6	6
-	7	7

Send packets to different queues based on the mapping between local priorities and queue index numbers.

- The local priority is also called internal priority. Priority mapping technology implements mapping from QoS priorities to internal priorities or from internal priorities to QoS priorities.
  - For the packets entering the device, the device maps packet or interface priorities to internal priorities and determines the queues that packets enter based on the mapping between internal priorities and queues.



Implementation of Congestion Management (2/2)

Which queue is first scheduled?

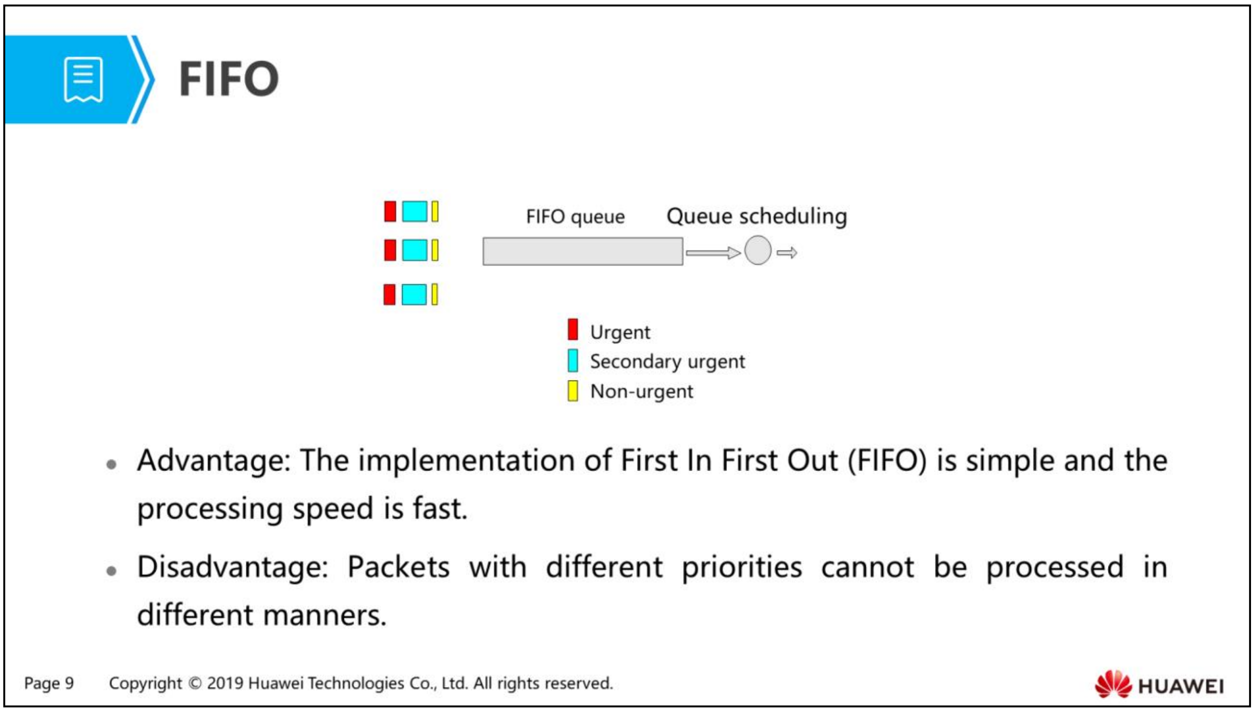
1. The core for providing differentiated services is to determine the forwarding sequence of packets in different queues. Queue scheduling mechanisms are used.

2. Common queue scheduling algorithms include FIFO, PQ, WRR, WFQ, and CBQ.

- How differentiated services are implemented through queue scheduling? What is the working mechanism of each queue scheduling algorithm? What are their respective advantages and disadvantages?

Contents

1. **Congestion Management**
   - Congestion Occurrence and Solution
   - Common Queue Scheduling Algorithms
   - Implementation of Congestion Management
2. Congestion Avoidance



FIFO

FIFO queue

Queue scheduling

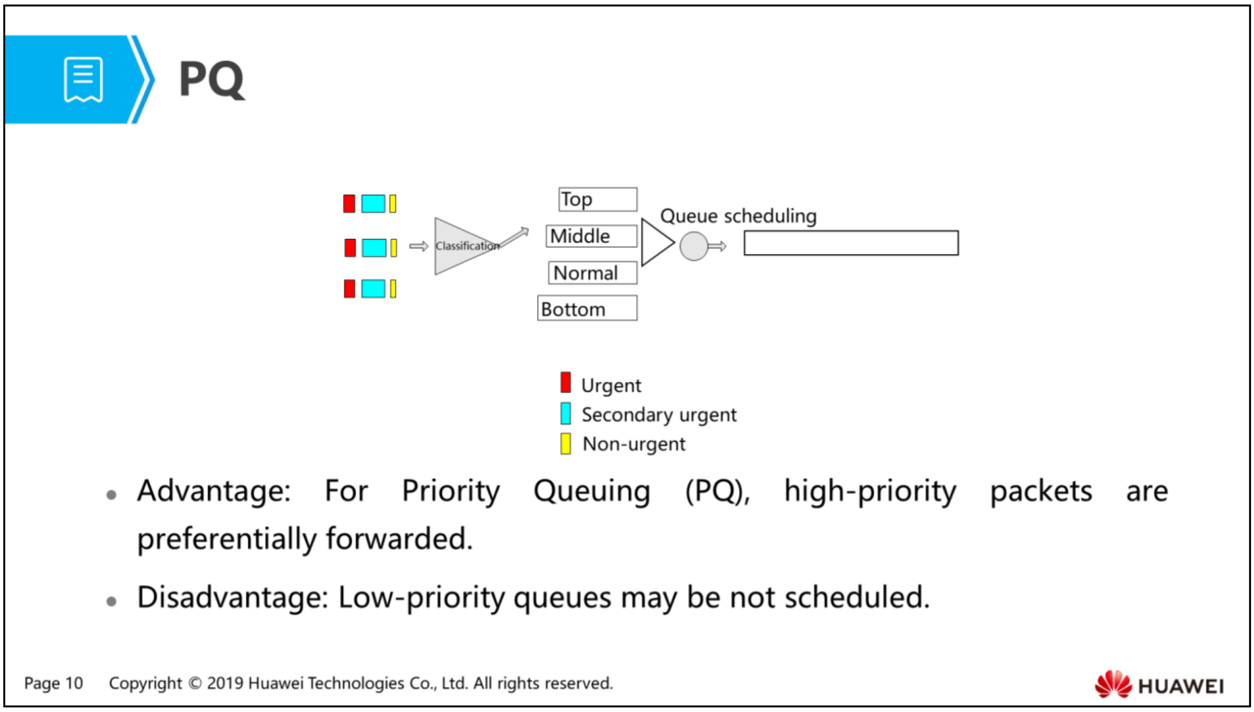
🟥 Urgent

🟦 Secondary urgent

🟨 Non-urgent

- Advantage: The implementation of First In First Out (FIFO) is simple and the processing speed is fast.
- Disadvantage: Packets with different priorities cannot be processed in different manners.

- FIFO does not classify packets. When the receive rate of packets on an interface is larger than the transmit rate, FIFO sends packets to queues based on the packet arrival sequence. In addition, packets are sent out from queues based on the sequence in which the packets enter queues.
- FIFO provides simple processing and low cost. FIFO does not differentiate packet types. It uses the BE model, so delay-sensitive real-time applications cannot be ensured and bandwidth of key services cannot be guaranteed.

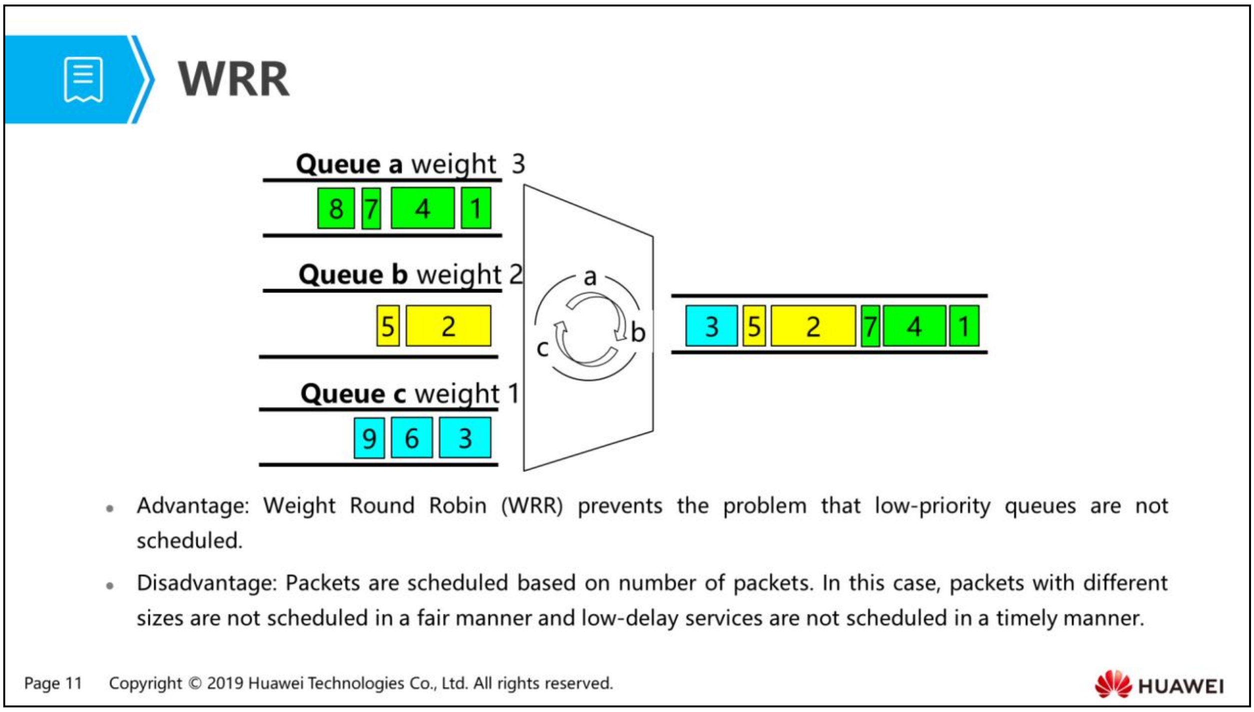


PQ

🟥 Urgent
🟦 Secondary urgent
🟨 Non-urgent

- Advantage: For Priority Queuing (PQ), high-priority packets are preferentially forwarded.
- Disadvantage: Low-priority queues may be not scheduled.

- PQ scheduling is designed for key service applications. In this mode, key services are scheduled preferentially to reduce the response delay when congestion occurs.
- PQ scheduling mechanism: There are four queues: high-priority, medium-priority, normal-priority, and low-priority queues. When packets go out of queues, the device forwards packets in the higher-priority queue. After all packets in the higher-priority queue are sent, the device forwards packets in the medium-priority queue. After all packets in the medium-priority queue are sent, the device forwards packets in the normal-priority queue, and so on. The packets of core services are placed into higher-priority queues, and the packets of non-core services such as emails are placed into lower-priority queues so that the packets of key services are processed first and non-core services are sent when core services are not processed.
- If packets in the high-priority queue are sent continuously, the packets in the lower-priority queue cannot be sent.

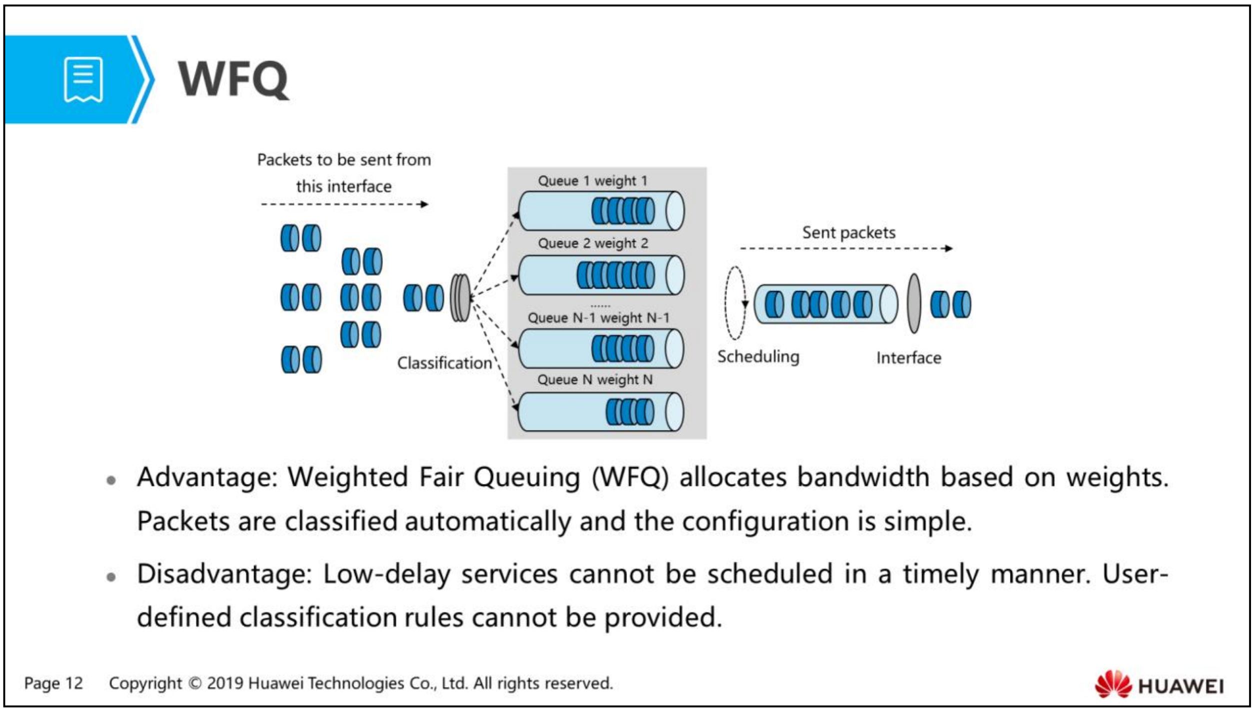


WRR

- Advantage: Weight Round Robin (WRR) prevents the problem that low-priority queues are not scheduled.
- Disadvantage: Packets are scheduled based on number of packets. In this case, packets with different sizes are not scheduled in a fair manner and low-delay services are not scheduled in a timely manner.

HUAWEI

- Based on Round Robin (RR) scheduling, Weight Round Robin (WRR) scheduling is used to schedule packet flows based on weights of queues. RR scheduling equals WRR scheduling with the weight of 1.

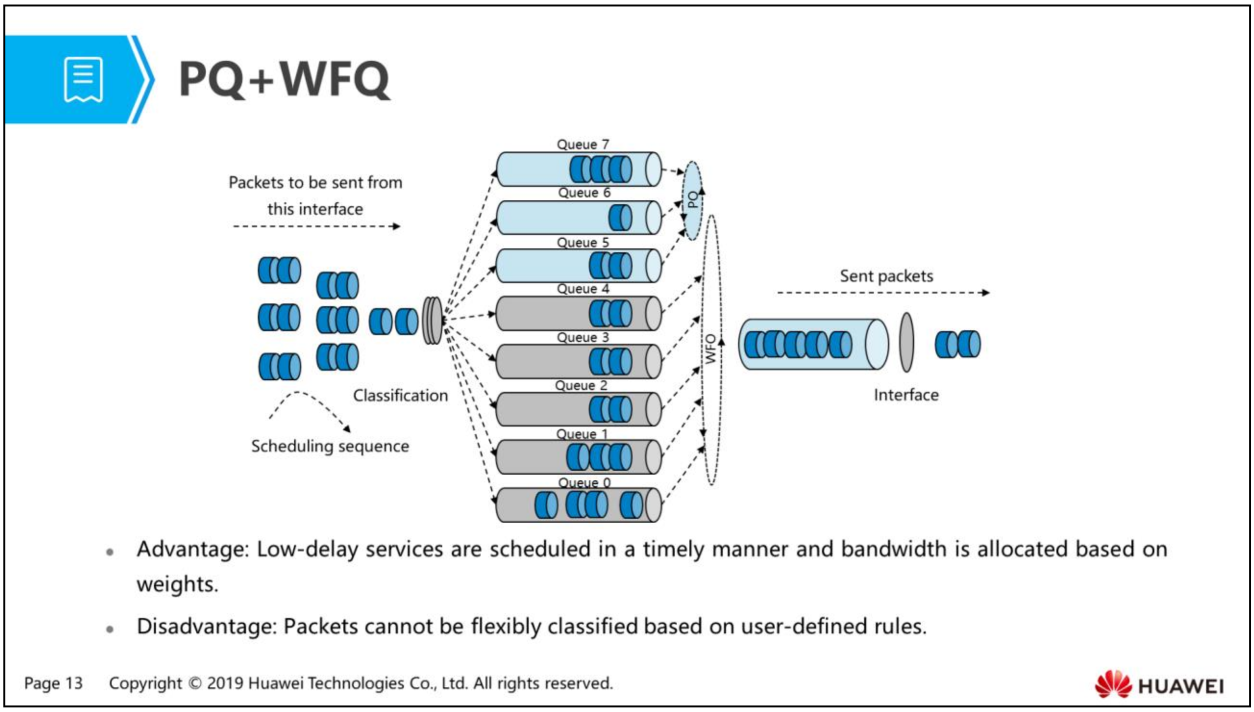


WFQ

- Advantage: Weighted Fair Queuing (WFQ) allocates bandwidth based on weights. Packets are classified automatically and the configuration is simple.
- Disadvantage: Low-delay services cannot be scheduled in a timely manner. User-defined classification rules cannot be provided.

Page 12 HUAWEI

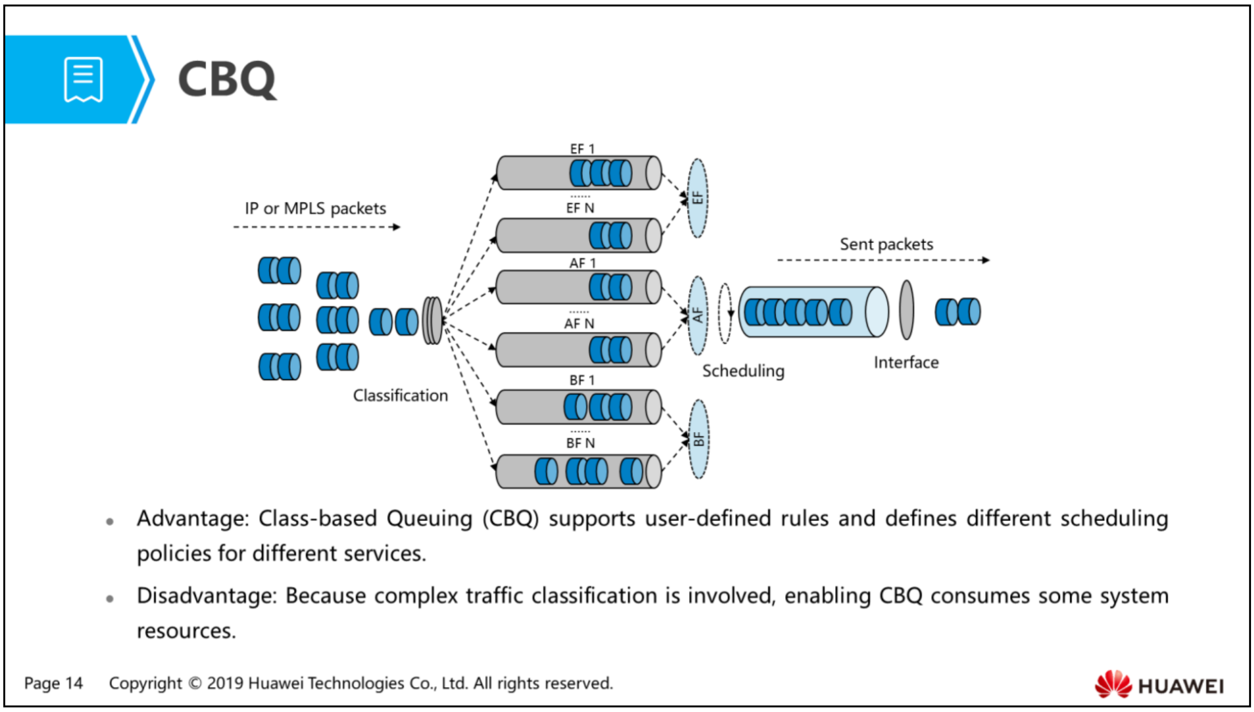
- WFQ classifies packets based on traffic characteristics. For the IP network, packets with the same source IP address, destination IP address, source port number, destination port number, protocol number, and ToS belong to the same flow. For the MPLS network, packets with the same labels and EXP priority belong to the same flow. Each flow is assigned to a queue. This process is completed using the HASH algorithm. Flows with different characteristics are sent to different queues. The number of queues allowed by WFQ is limited and configurable.
- When flows leave queues, WFQ allocates the egress bandwidth to each flow based on the precedence of each flow. Flows with the lowest priorities obtain the least bandwidth. In this manner, services of the same priority are treated in the same manner; services of different priorities are allocated with different weights.
- WFQ configuration is simple. Traffic is classified automatically, without manual intervention. WFQ is inflexible. When multiple flows enter the same queue, WFQ limited by resources cannot provide accurate services and cannot ensure resources obtained by each service. WFQ balances the delay and jitter of each flow, so it is not suitable for delay-sensitive service applications.
- According to the preceding analysis, if all queues use one scheduling algorithm, a scheduling algorithm has respective advantages and disadvantages and cannot meet service requirements. Some scheduling algorithms are complementary. If different queue scheduling algorithms are used for different queues, can service requirements be met?



PQ+WFQ

- Advantage: Low-delay services are scheduled in a timely manner and bandwidth is allocated based on weights.
- Disadvantage: Packets cannot be flexibly classified based on user-defined rules.

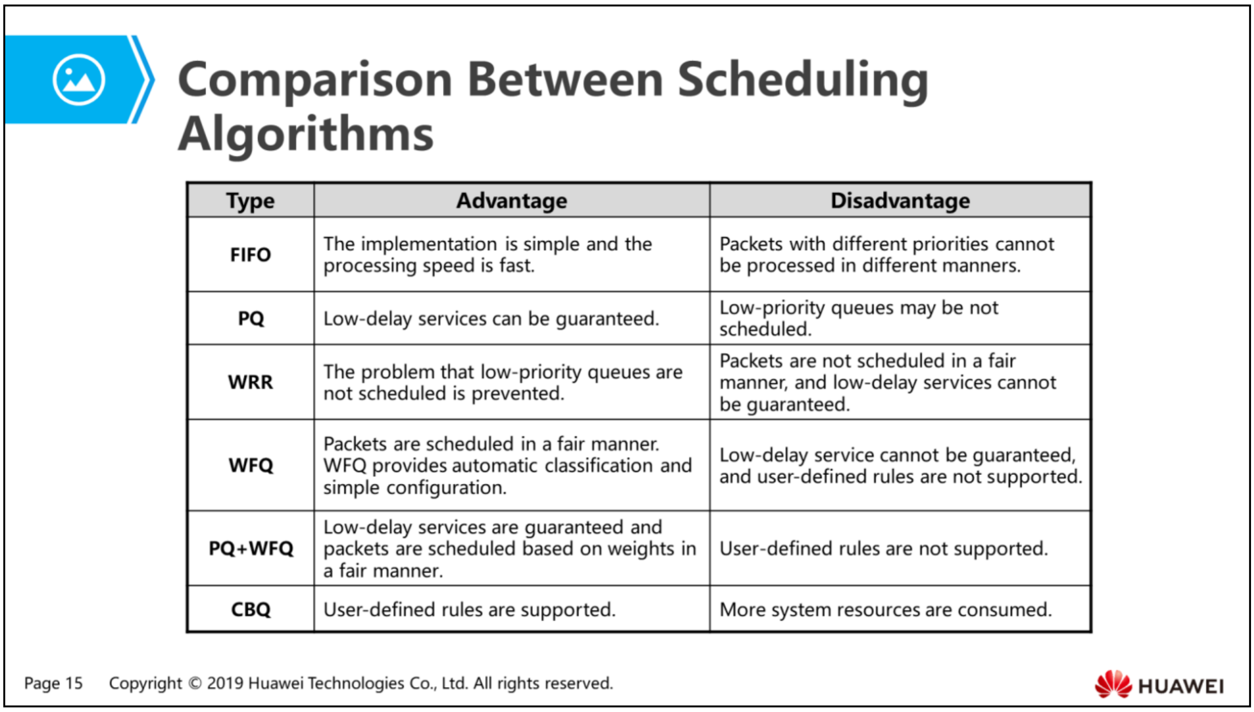
- PQ+WFQ scheduling process:
  - As shown in the preceding figure, the device first schedules traffic in queue 7, queue 6, and queue 5 in PQ mode. After traffic scheduling in the three queues is complete, the device schedules traffic in queue 4, queue 3, queue 2, queue 1, and queue 0 in WFQ mode. Queue 4, queue 3, queue 2, queue 1, and queue 0 have their weights.
  - Important protocol packets or short-delay service packets are placed in queues using PQ scheduling so that they can be scheduled first. Other packets are placed in queues using WFQ scheduling.
- Advantages and disadvantages of PQ+WFQ:
  - This combination integrates advantages and disadvantages of PQ and WFQ. If only PQ scheduling is used, packets in queues with lower priorities may not obtain bandwidth for a long period of time. If only WFQ scheduling is used, short-delay services such as voice services cannot be scheduled first. To solve the problem, configure PQ+WFQ scheduling.



CBQ

- Advantage: Class-based Queuing (CBQ) supports user-defined rules and defines different scheduling policies for different services.
- Disadvantage: Because complex traffic classification is involved, enabling CBQ consumes some system resources.

- CBQ is an extension of WFQ and matches packets with traffic classifiers. CBQ classifies packets based on the IP priority or DSCP priority, inbound interface, or 5-tuple (protocol type, source IP address and mask, destination IP address and mask, source port range, and destination port range). Then CBQ puts packets into different queues. CBQ matches packets that do not match configured traffic classifiers with the default traffic classifier defined by the system.
- CBQ provides the following types of queues:
  - Expedited Forwarding (EF) queues: used for delay-sensitive services.
    - EF: After packets matching traffic classification rules enter EF queues, they are scheduled in Strict Priority (SP) mode. Packets in other queues are scheduled only after all the packets in EF queues are scheduled.
  - Assured Forwarding (AF) queues: used for key data services that require assured bandwidth.
    - Each AF queue corresponds to one type of packets. You can set bandwidth for each type of packets. During scheduling, the system sends packets based on the configured bandwidth. AF implements fair scheduling.
  - Best-Effort (BE) queues: used for best-effort services that require no strict QoS assurance.
    - If packets do not match any configured traffic classifiers, packets match the default traffic classifier defined by the system. BE queues use the remaining bandwidth of an interface in WFQ scheduling mode.



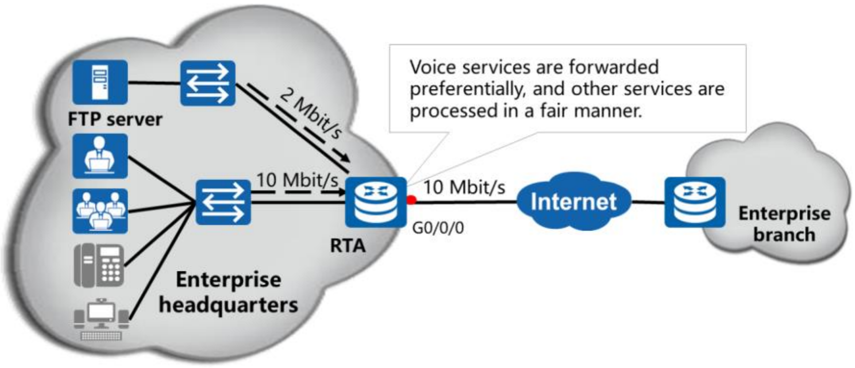
Comparison Between Scheduling Algorithms

Type	Advantage	Disadvantage
FIFO	The implementation is simple and the processing speed is fast.	Packets with different priorities cannot be processed in different manners.
PQ	Low-delay services can be guaranteed.	Low-priority queues may be not scheduled.
WRR	The problem that low-priority queues are not scheduled is prevented.	Packets are not scheduled in a fair manner, and low-delay services cannot be guaranteed.
WFQ	Packets are scheduled in a fair manner. WFQ provides automatic classification and simple configuration.	Low-delay service cannot be guaranteed, and user-defined rules are not supported.
PQ+WFQ	Low-delay services are guaranteed and packets are scheduled based on weights in a fair manner.	User-defined rules are not supported.
CBQ	User-defined rules are supported.	More system resources are consumed.

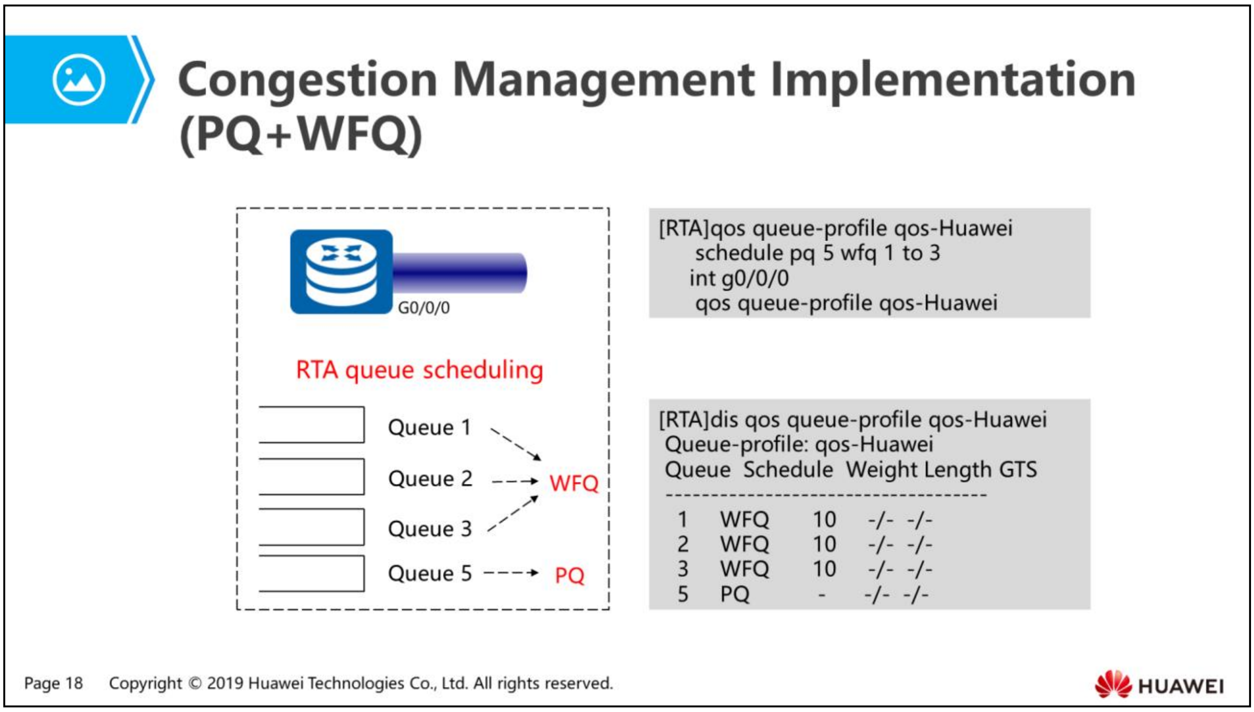
Contents

1. **Congestion Management**
   - Congestion Occurrence and Solution
   - Common Queue Scheduling Algorithms
   - Implementation of Congestion Management
2. Congestion Avoidance

Congestion Management Requirements (PQ+WFQ)



Voice services are forwarded preferentially, and other services are processed in a fair manner.



Congestion Management Implementation (PQ+WFQ)

G0/0/0

RTA queue scheduling

Queue 1

Queue 2

Queue 3

Queue 5

WFQ

PQ

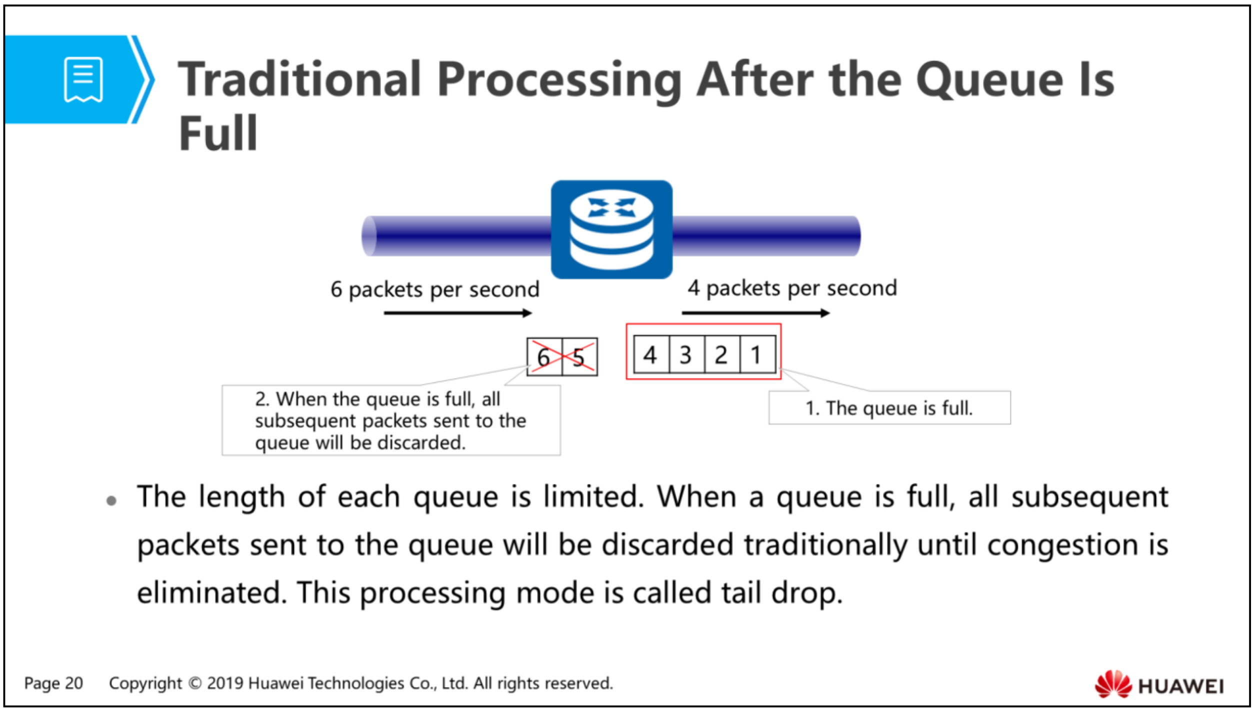
```
[RTA]qos queue-profile qos-Huawei
     schedule pq 5 wfq 1 to 3
    int g0/0/0
     qos queue-profile qos-Huawei
```

```
[RTA]dis qos queue-profile qos-Huawei
 Queue-profile: qos-Huawei
 Queue  Schedule  Weight Length GTS
 -----------------------------------
   1    WFQ       10    -/-  -/-
   2    WFQ       10    -/-  -/-
   3    WFQ       10    -/-  -/-
   5    PQ         -    -/-  -/-
```

- The parameters here correspond to parameters in slide Implementation of Congestion Management (1/2).

Contents

1. Congestion Management
2. **Congestion Avoidance**
   - Disadvantages and Solution of Tail Drop
   - WRED Configuration



Traditional Processing After the Queue Is Full

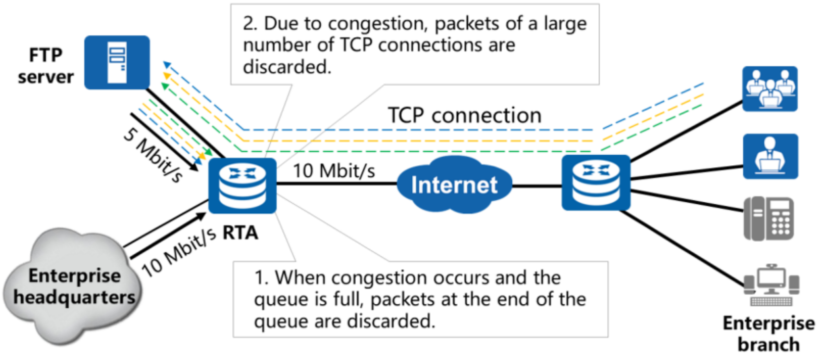
2. When the queue is full, all subsequent packets sent to the queue will be discarded.

1. The queue is full.

- The length of each queue is limited. When a queue is full, all subsequent packets sent to the queue will be discarded traditionally until congestion is eliminated. This processing mode is called tail drop.

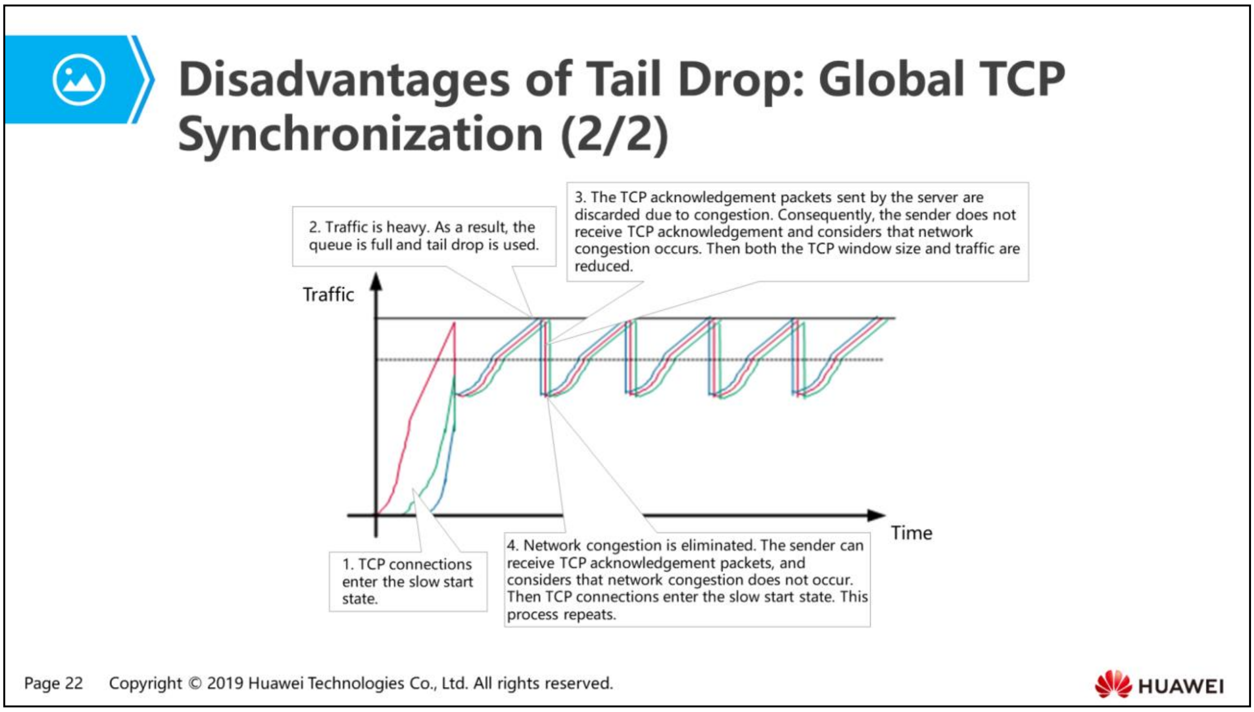
- What are advantages and disadvantages of tail drop?

Disadvantages of Tail Drop: Global TCP Synchronization (1/2)



2. Due to congestion, packets of a large number of TCP connections are discarded.

1. When congestion occurs and the queue is full, packets at the end of the queue are discarded.



Disadvantages of Tail Drop: Global TCP Synchronization (2/2)

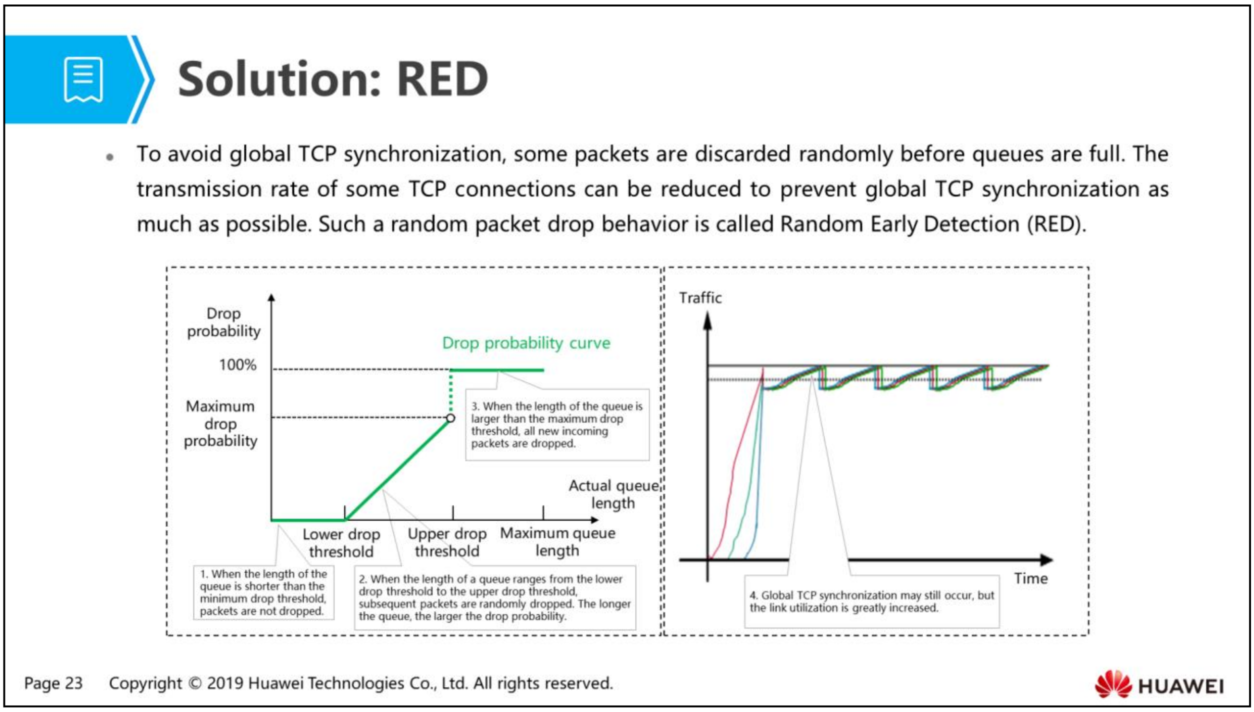
2. Traffic is heavy. As a result, the queue is full and tail drop is used.

3. The TCP acknowledgement packets sent by the server are discarded due to congestion. Consequently, the sender does not receive TCP acknowledgement and considers that network congestion occurs. Then both the TCP window size and traffic are reduced.

1. TCP connections enter the slow start state.

4. Network congestion is eliminated. The sender can receive TCP acknowledgement packets, and considers that network congestion does not occur. Then TCP connections enter the slow start state. This process repeats.

- Global TCP synchronization: If a large number of TCP packets of a TCP connection are discarded, the TCP connection times out and enters the slow start state. Then TCP packets to be sent are reduced. When a queue discards packets of multiple TCP connections simultaneously, the TCP connections enter the congestion avoidance and slow start state to adjust and reduce the traffic. This phenomenon is called global TCP synchronization. The number of packets of TCP connections sent to queues is reduced and a traffic peak occurs. This situation is repeated, and the network resource utilization is low.
- How is global TCP synchronization prevented. What is the core of the problem?



Solution: RED

- To avoid global TCP synchronization, some packets are discarded randomly before queues are full. The transmission rate of some TCP connections can be reduced to prevent global TCP synchronization as much as possible. Such a random packet drop behavior is called Random Early Detection (RED).

1. When the length of the queue is shorter than the minimum drop threshold, packets are not dropped.

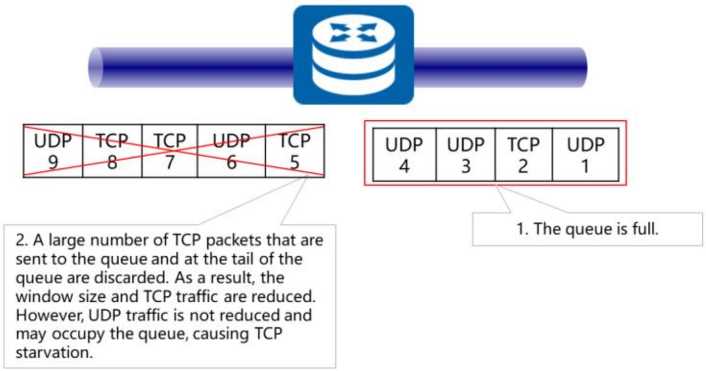
2. When the length of a queue ranges from the lower drop threshold to the upper drop threshold, subsequent packets are randomly dropped. The longer the queue, the larger the drop probability.

3. When the length of the queue is larger than the maximum drop threshold, all new incoming packets are dropped.

4. Global TCP synchronization may still occur, but the link utilization is greatly increased.

- To prevent global TCP synchronization, RED is used. RED randomly discards packets to prevent the transmission speed of multiple TCP connections from being reduced simultaneously. Global TCP synchronization is therefore prevented. The TCP traffic rate and network traffic become stable.
- RED defines upper and lower threshold for the length of each queue. The packet drop policy is as follows:
  - When the length of the queue is shorter than the lower drop threshold, packets are not dropped.
  - When the queue length is greater than the upper drop threshold, all packets are discarded.
  - When the length of the queue is between the lower drop threshold and the upper drop threshold, incoming packets are dropped randomly. RED generates a random number for each incoming packet and compares it with the drop probability of the current queue. If the random number is greater than the drop probability, the packet is discarded. A longer queue indicates a higher drop probability.
- In addition to global TCP synchronization, does tail drop cause other effects?

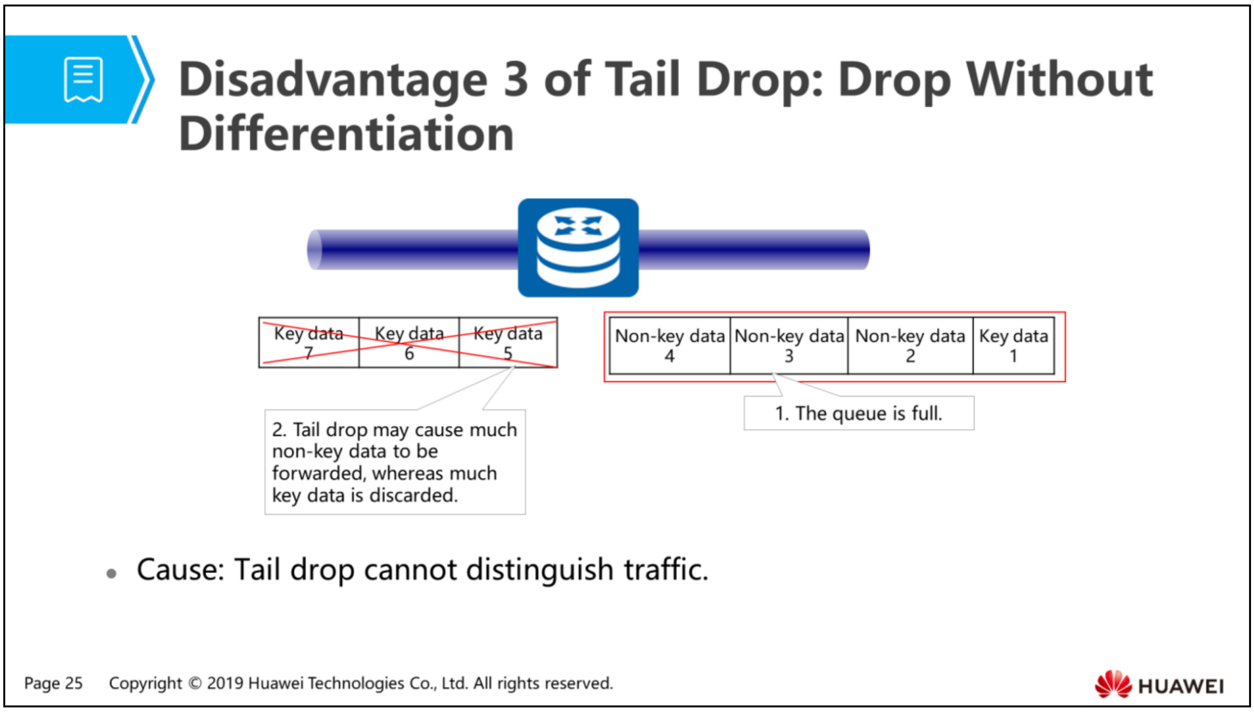
Disadvantage 2 of Tail Drop: TCP Starvation



1. The queue is full.

2. A large number of TCP packets that are sent to the queue and at the tail of the queue are discarded. As a result, the window size and TCP traffic are reduced. However, UDP traffic is not reduced and may occupy the queue, causing TCP starvation.

- Cause: Tail drop cannot distinguish traffic.



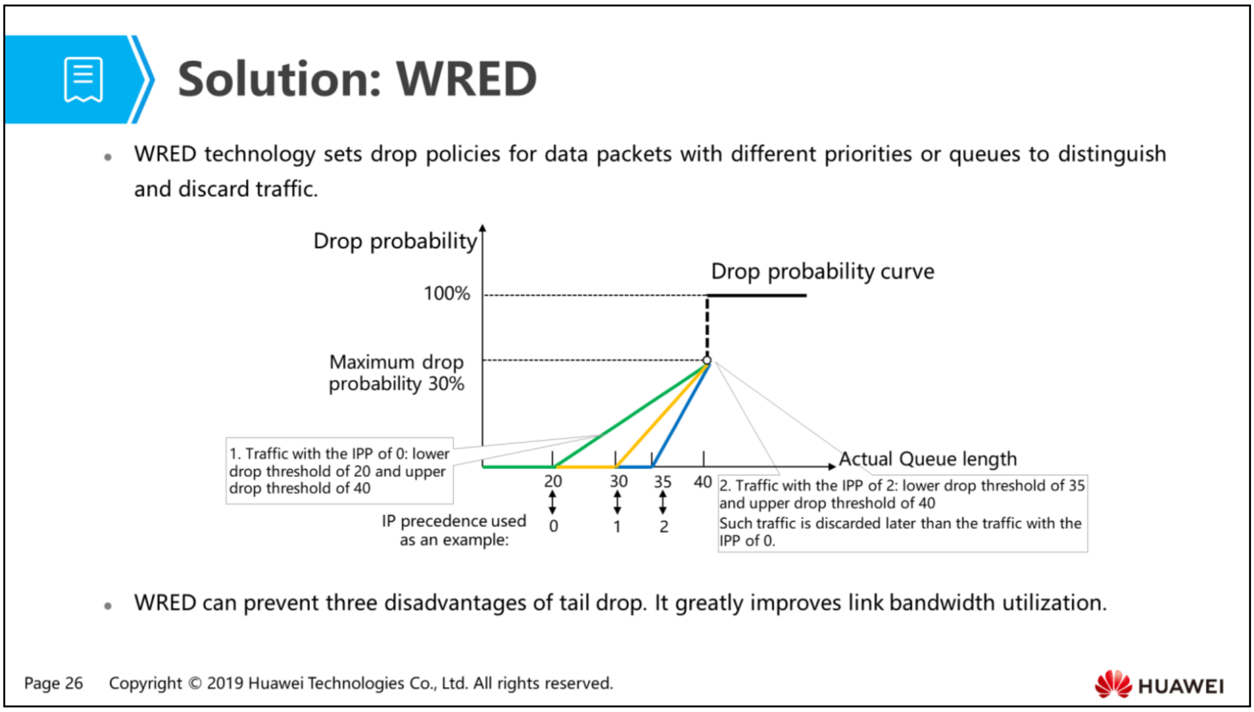
Disadvantage 3 of Tail Drop: Drop Without Differentiation

2. Tail drop may cause much non-key data to be forwarded, whereas much key data is discarded.

1. The queue is full.

- Cause: Tail drop cannot distinguish traffic.

- Can RED solve disadvantages 2 and 3 of tail drop? Why?



Solution: WRED

- WRED technology sets drop policies for data packets with different priorities or queues to distinguish and discard traffic.

Drop probability
Drop probability curve
100%
Maximum drop probability 30%
1. Traffic with the IPP of 0: lower drop threshold of 20 and upper drop threshold of 40
Actual Queue length
20
30
35
40
0
1
2
IP precedence used as an example:
2. Traffic with the IPP of 2: lower drop threshold of 35 and upper drop threshold of 40
Such traffic is discarded later than the traffic with the IPP of 0.

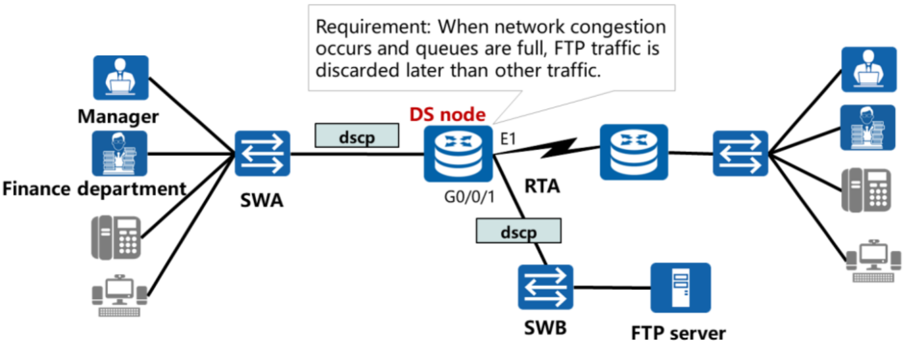
- WRED can prevent three disadvantages of tail drop. It greatly improves link bandwidth utilization.

- WRED is based on RED. You can set the upper drop threshold, lower drop threshold, and maximum drop probability for different types of packets independently. When the number of packets reaches the lower drop threshold, the device starts to discard packets. When the number of packets reaches the upper drop threshold, the device discards all the packets. With the increase of the threshold, the drop probability increases. The maximum drop probability cannot be exceeded. WRED discards packets in queues based on the drop probability, preventing all disadvantages of tail drop.

Contents

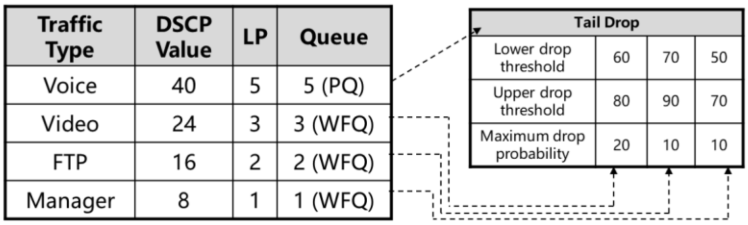
1. Congestion Management
2. **Congestion Avoidance**
   - Disadvantages and Solution of Tail Drop
   - WRED Configuration

WRED Configuration Requirement



Requirement: When network congestion occurs and queues are full, FTP traffic is discarded later than other traffic.

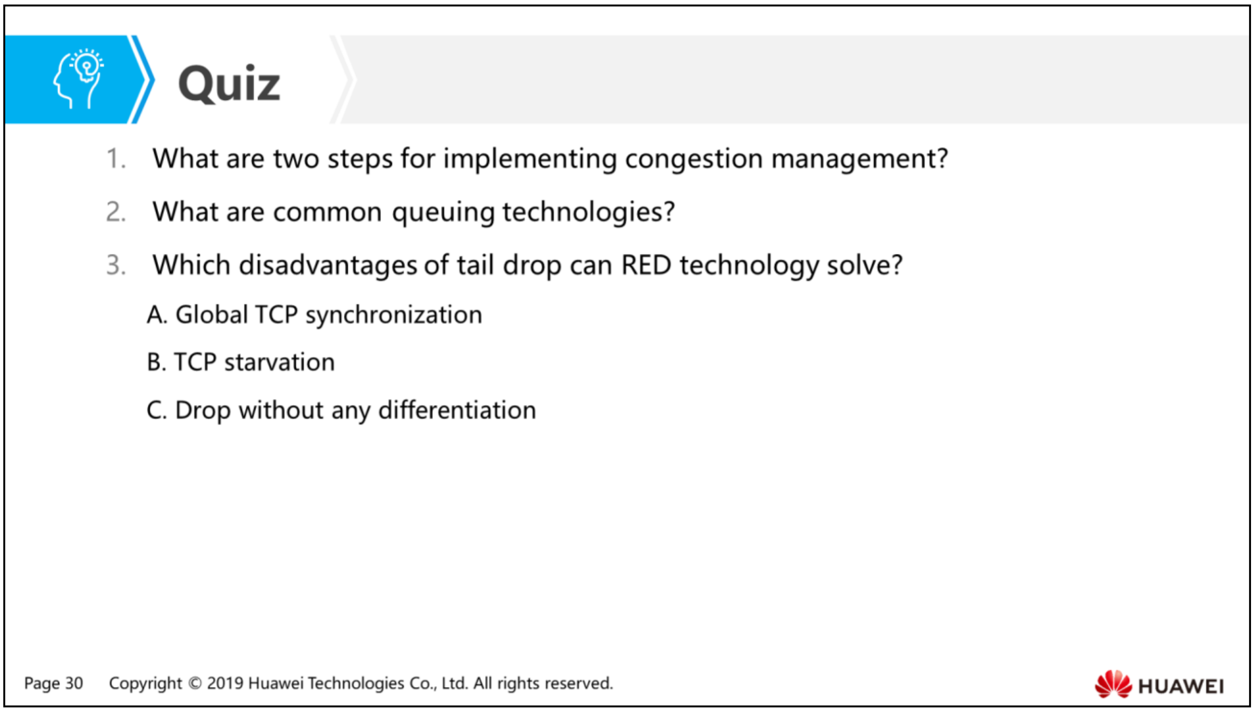
WRED Configuration Implementation



Traffic Type	DSCP Value	LP	Queue
Voice	40	5	5 (PQ)
Video	24	3	3 (WFQ)
FTP	16	2	2 (WFQ)
Manager	8	1	1 (WFQ)

Tail Drop			
Lower drop threshold	60	70	50
Upper drop threshold	80	90	70
Maximum drop probability	20	10	10

```
[RTA]drop-profile manager
      wred dscp
      dscp 8 low-limit 50 high-limit 70 discard-percentage 10
     drop-profile ftp
      wred dscp
      dscp 16 low-limit 70 high-limit 90 discard-percentage 10
     drop-profile video
      wred dscp
      dscp 24 low-limit 60 high-limit 80 discard-percentage 20
     qos queue-profile qos-Huawei
      queue 1 drop-profile manager
      queue 2 drop-profile ftp
      queue 3 drop-profile video
     interface E1
      qos queue-profile qos-Huawei
```



Quiz

1. What are two steps for implementing congestion management?
2. What are common queuing technologies?
3. Which disadvantages of tail drop can RED technology solve?

A. Global TCP synchronization

B. TCP starvation

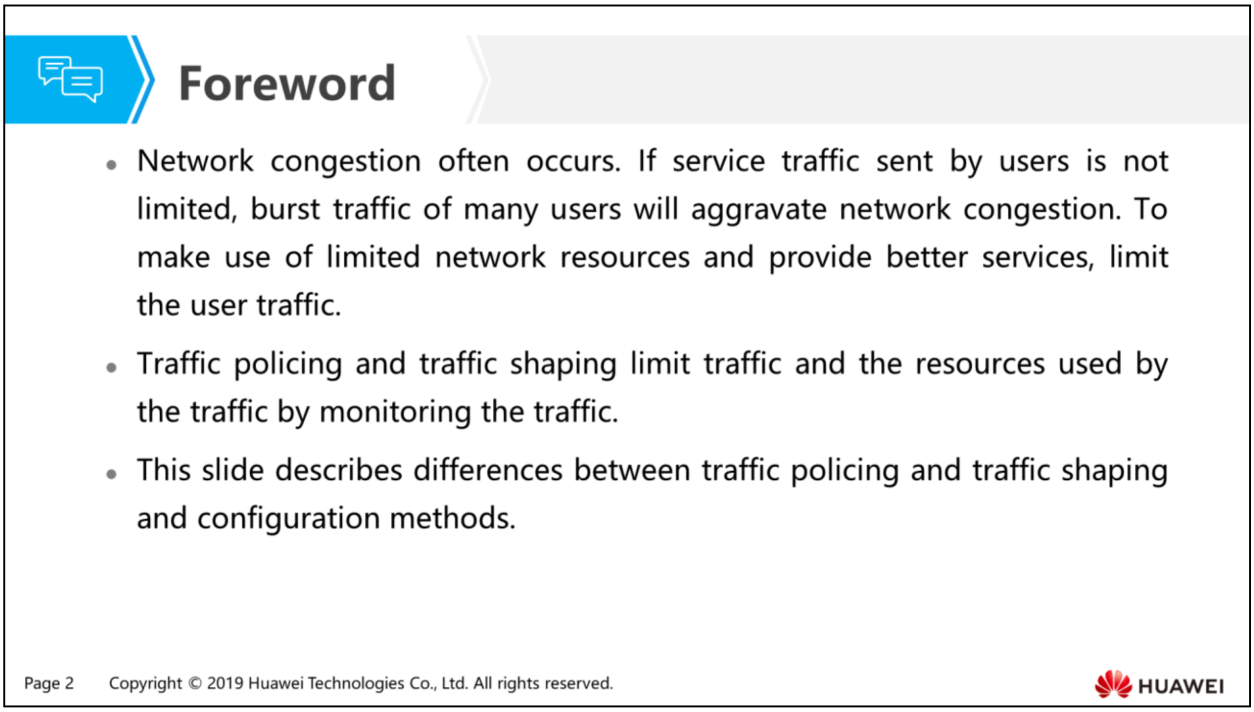
C. Drop without any differentiation

- Answer:
  - Step 1: Send all packets from one interface to different queues.
  - Step 2: Forward packets based on scheduling mechanism between queues.
- Answer: FIFO, PQ, WFQ, PQ+WFQ, CBQ.
- Answer: A.

Thank You

www.huawei.com

Traffic Policing and Traffic Shaping



Foreword

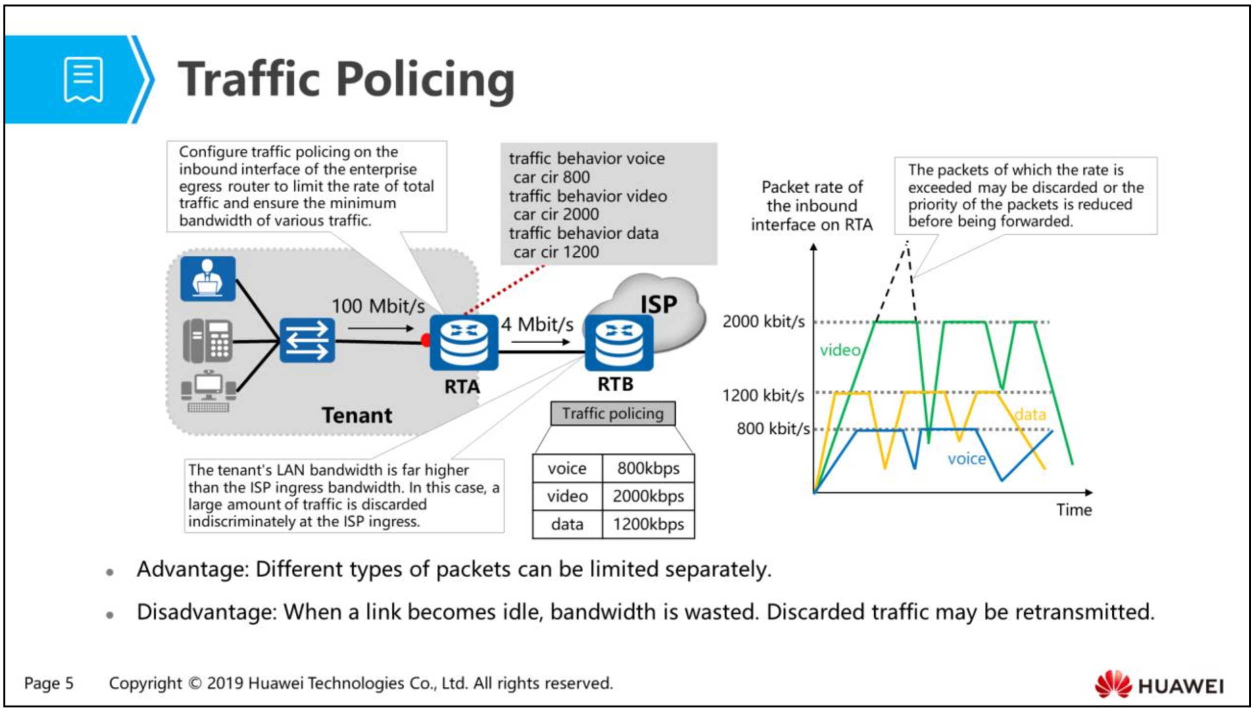
- Network congestion often occurs. If service traffic sent by users is not limited, burst traffic of many users will aggravate network congestion. To make use of limited network resources and provide better services, limit the user traffic.
- Traffic policing and traffic shaping limit traffic and the resources used by the traffic by monitoring the traffic.
- This slide describes differences between traffic policing and traffic shaping and configuration methods.

Objectives

- Upon completion of this section, you will be able to:
  - Be familiar with features of traffic policing and traffic shaping
  - Master the configuration of traffic policing and traffic shaping

Contents

1. **Traffic Policing and Traffic Shaping**



Traffic Policing

Configure traffic policing on the inbound interface of the enterprise egress router to limit the rate of total traffic and ensure the minimum bandwidth of various traffic.

```
traffic behavior voice
 car cir 800
traffic behavior video
 car cir 2000
traffic behavior data
 car cir 1200
```

Traffic policing

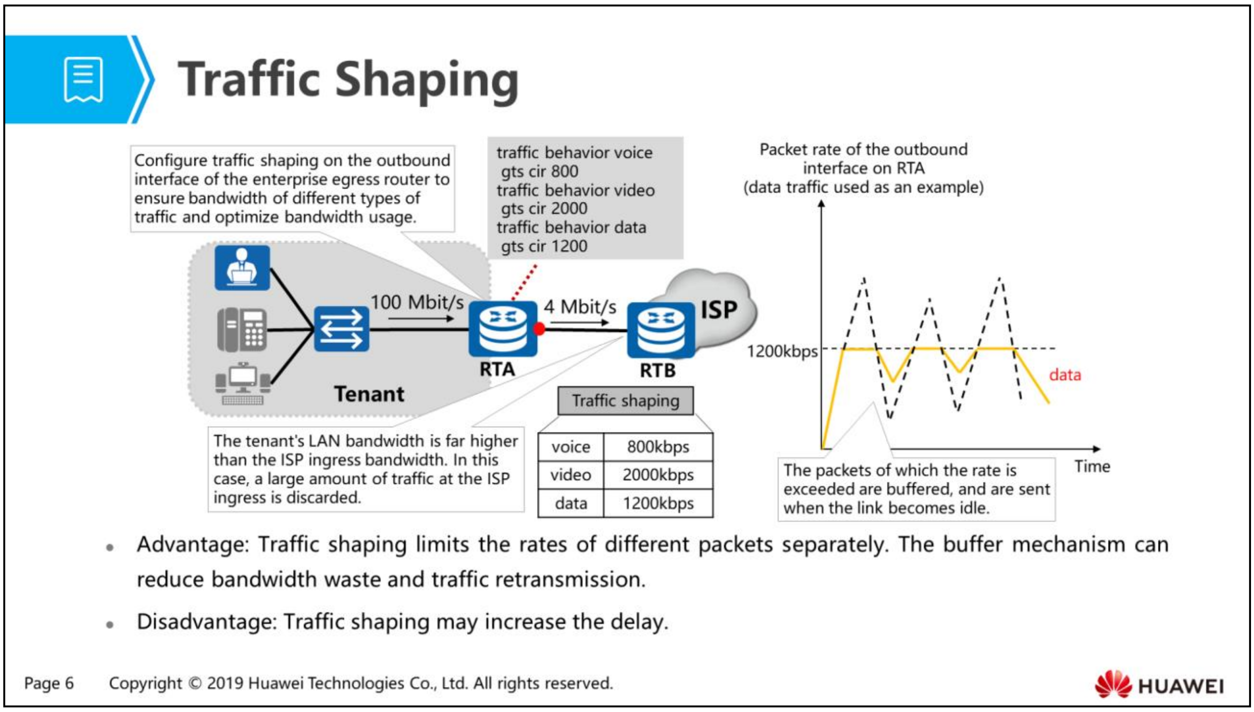
voice	800kbps
video	2000kbps
data	1200kbps

The tenant's LAN bandwidth is far higher than the ISP ingress bandwidth. In this case, a large amount of traffic is discarded indiscriminately at the ISP ingress.

The packets of which the rate is exceeded may be discarded or the priority of the packets is reduced before being forwarded.

- Advantage: Different types of packets can be limited separately.
- Disadvantage: When a link becomes idle, bandwidth is wasted. Discarded traffic may be retransmitted.

- Traffic policing can control the rate of received or sent traffic to limit burst traffic entering the network, providing basic QoS functions.
- Traffic policing is usually used to monitor the volume of the traffic that enters a network and limits the traffic within a specified range. In addition, traffic policing optimizes network resources and protects the interests of carriers by penalizing traffic that exceeds the rate limit.
- Traffic policing uses Committed Access Rate (CAR) to limit traffic of a certain type of packets.



Traffic Shaping

Configure traffic shaping on the outbound interface of the enterprise egress router to ensure bandwidth of different types of traffic and optimize bandwidth usage.

```
traffic behavior voice
 gts cir 800
traffic behavior video
 gts cir 2000
traffic behavior data
 gts cir 1200
```

The tenant's LAN bandwidth is far higher than the ISP ingress bandwidth. In this case, a large amount of traffic at the ISP ingress is discarded.

Traffic shaping

voice	800kbps
video	2000kbps
data	1200kbps

Packet rate of the outbound interface on RTA (data traffic used as an example)

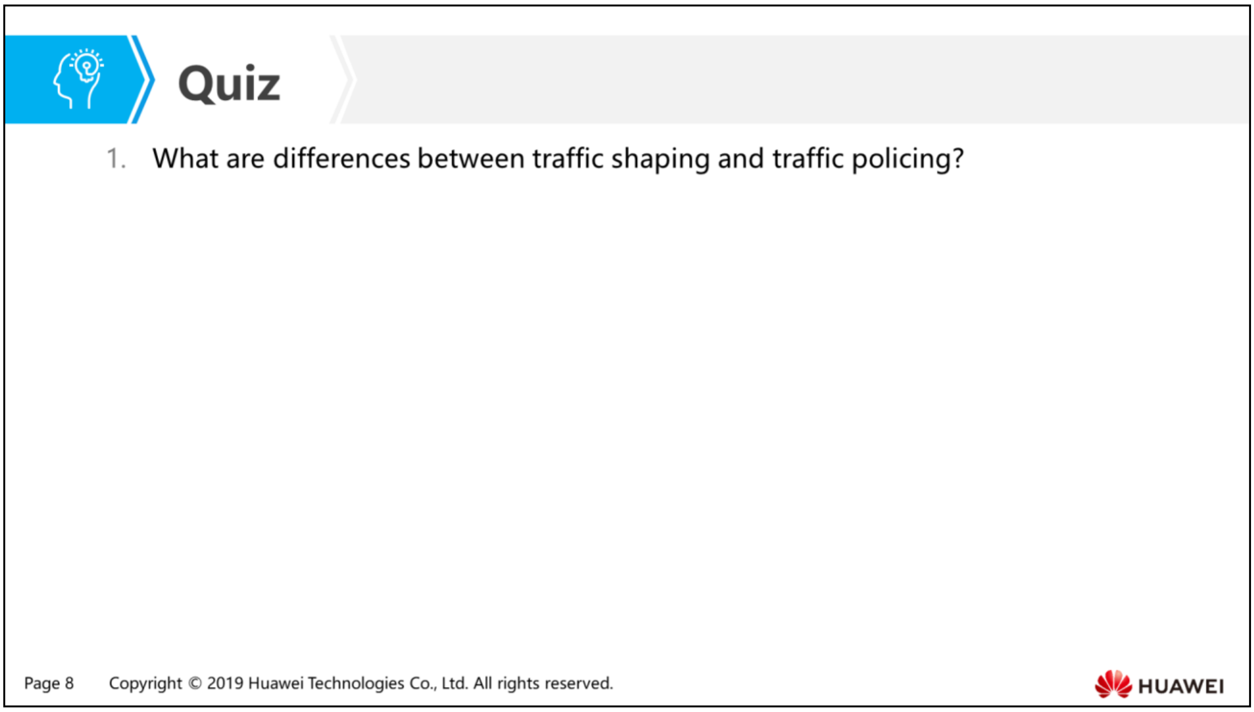
The packets of which the rate is exceeded are buffered, and are sent when the link becomes idle.

- Advantage: Traffic shaping limits the rates of different packets separately. The buffer mechanism can reduce bandwidth waste and traffic retransmission.
- Disadvantage: Traffic shaping may increase the delay.

- Traffic shaping limits the rate of normal traffic and burst traffic over a network connection so that the traffic can be sent out at an even rate. It adjusts the transmission rate of traffic and can control only the rate of outgoing traffic. Generic Traffic Shaping (GTS) technology is often used to limit a certain type of traffic.
- Application scenario: When the bandwidths of uplink and downlink interfaces do not match and the bandwidth of the uplink interface is higher than that of the downlink interface, network congestion occurs on the downstream network. To prevent this situation, configure traffic shaping on the outbound interface of the upstream device so that all the traffic sent by the upstream device can be processed by the downstream device. Packets can be sent evenly. Excess packets are buffered and sent when the link becomes idle.

Comparisons Between Traffic Policing and Traffic Shaping

Rate Limiting Type	Advantage	Disadvantage
Traffic policing	Limits the rate of different types of packets and re-marks the packets.	Causes a high packet loss ratio. When the link is idle, the bandwidth cannot be fully used.
Traffic shaping	Discards fewer packets and makes full use of bandwidth.	Causes extra delay and jitter and requires more device buffer resources.



Quiz

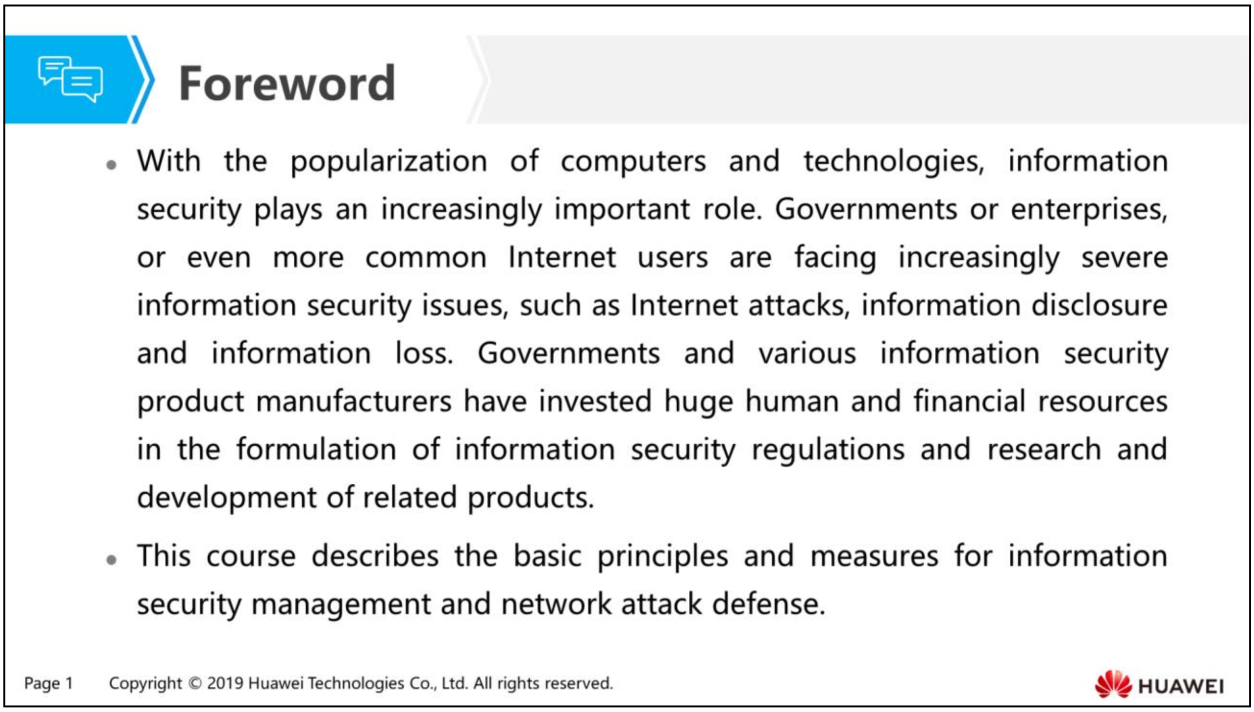
1. What are differences between traffic shaping and traffic policing?

- Answer: For control of packets, traffic policing discards excess packets, whereas traffic shaping buffers packets in queues and sends them when the link becomes idle.

Thank You

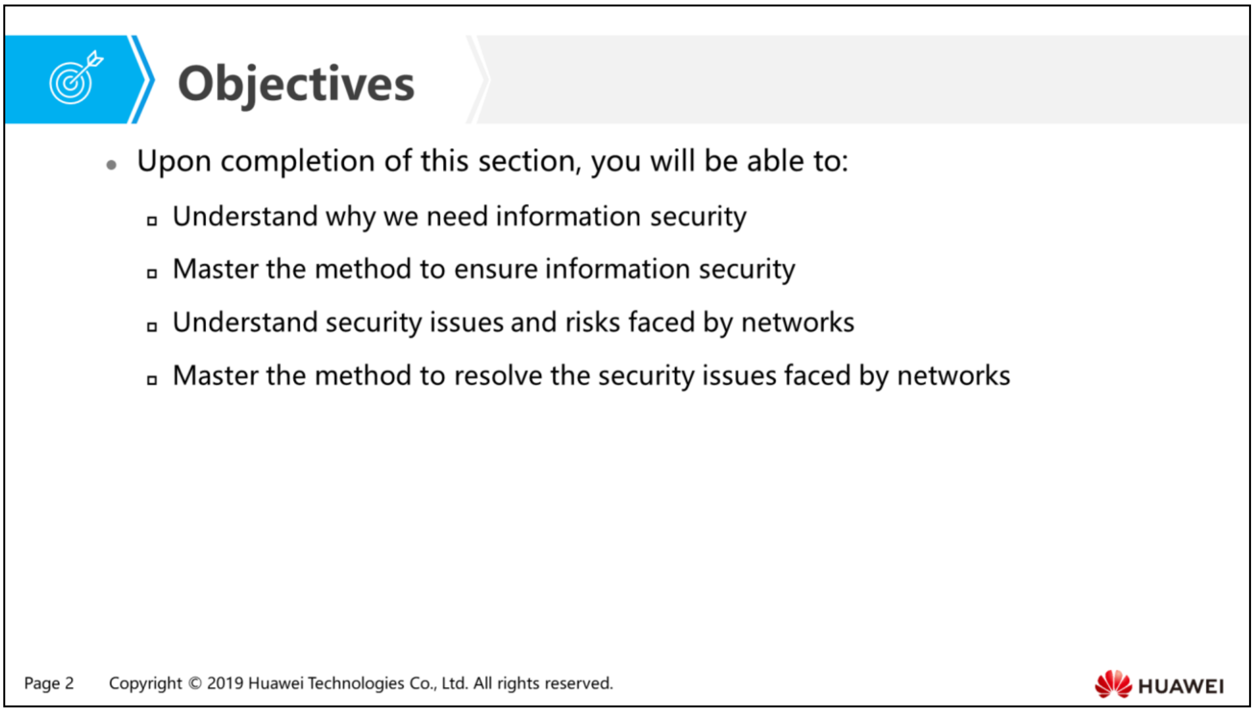
www.huawei.com

Information Security Overview



Foreword

- With the popularization of computers and technologies, information security plays an increasingly important role. Governments or enterprises, or even more common Internet users are facing increasingly severe information security issues, such as Internet attacks, information disclosure and information loss. Governments and various information security product manufacturers have invested huge human and financial resources in the formulation of information security regulations and research and development of related products.
- This course describes the basic principles and measures for information security management and network attack defense.

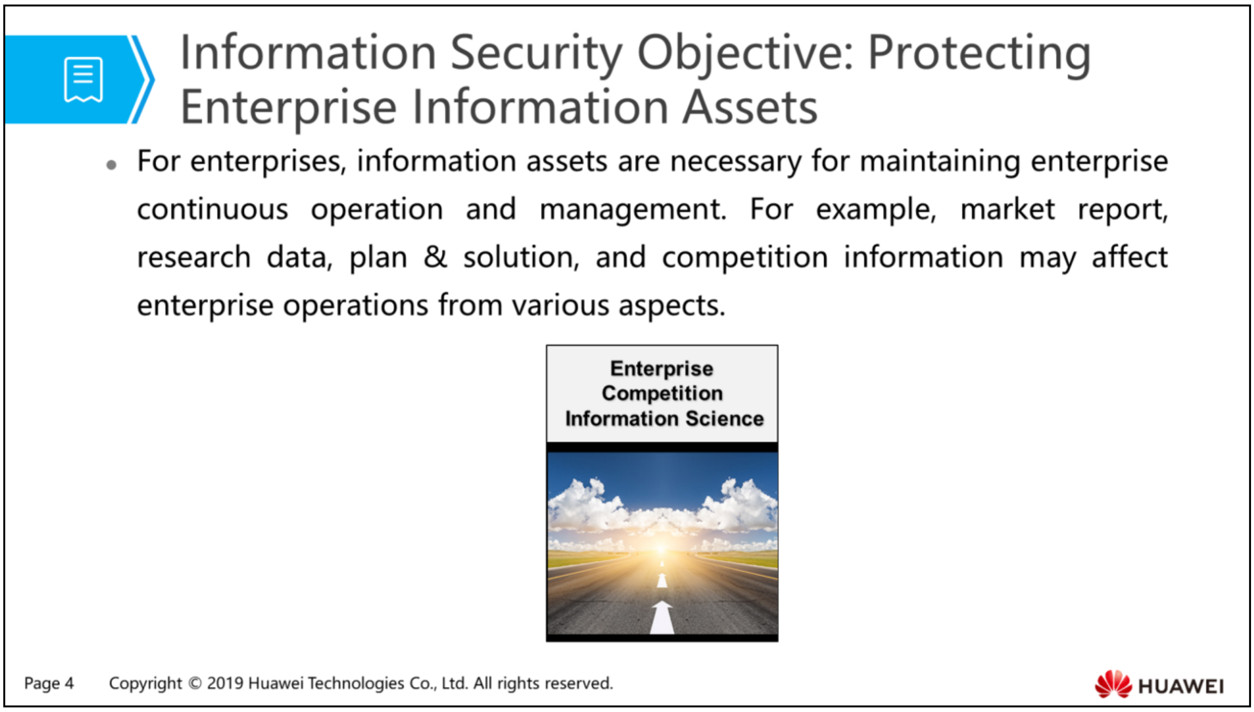


Objectives

- Upon completion of this section, you will be able to:
  - Understand why we need information security
  - Master the method to ensure information security
  - Understand security issues and risks faced by networks
  - Master the method to resolve the security issues faced by networks

Contents

1. **Why Do We Need Information Security?**
2. What is Information Security?
3. How to Ensure Information Security?
4. Network Security

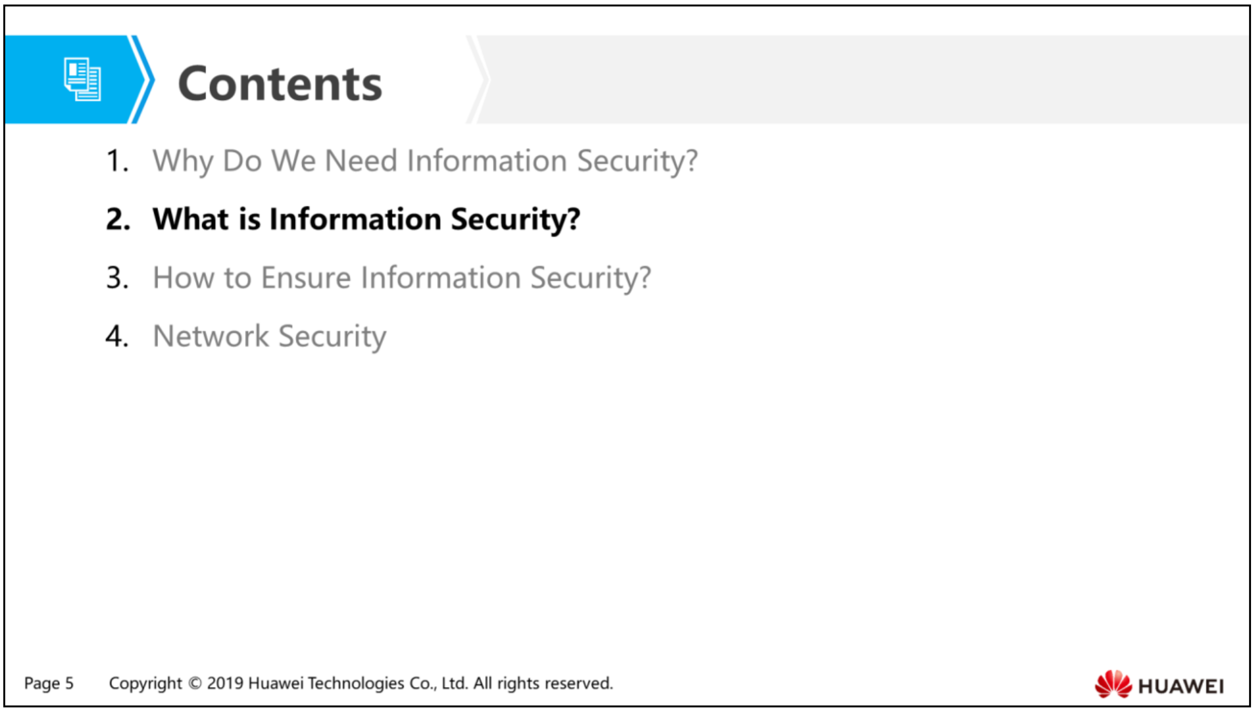


Information Security Objective: Protecting Enterprise Information Assets

- For enterprises, information assets are necessary for maintaining enterprise continuous operation and management. For example, market report, research data, plan & solution, and competition information may affect enterprise operations from various aspects.

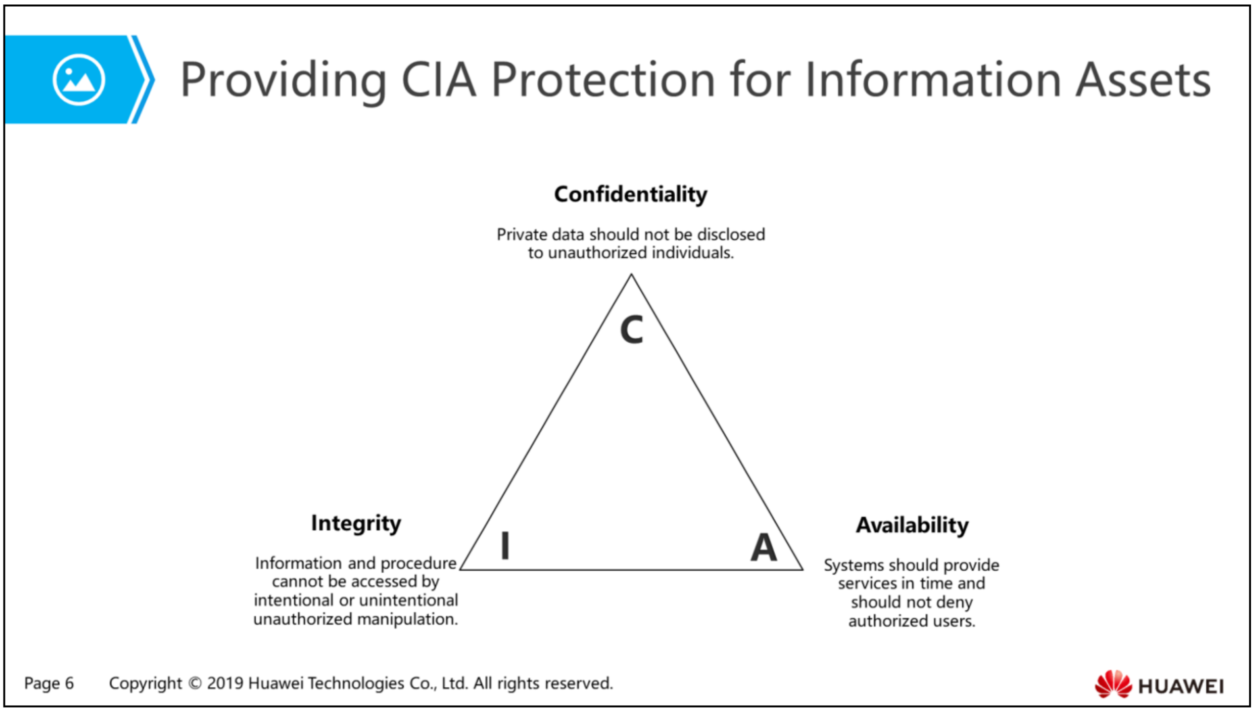
Enterprise
Competition
Information Science

- Nowadays, the importance of protecting enterprise and personal information is indisputable. To the network engineers, the objective of learning information security is to understand how to systematically ensure enterprise information assets security, especially the role of internet technology that they have learned. So, what are information assets?
- With the development of technologies, enterprise service process and information management become more and more dependent on IT facilities. Out of concern over rapid information processing, many enterprises even digitalize all of their service information. Therefore, normal running of IT infrastructure and fine protection of electronic information become one of the key factors for the smooth process and development of enterprise services.
- Information plays such an important role in enterprise services that we can consider it a kind of asset and call it information asset. Although information asset is intangible, it includes a large amount of service data, client information, and commercial secrets which are closely related to enterprise business and the survival of the enterprise. Therefore, information assets are facing various threats and risks, including intentional or accidental destruction, hacker attack, data loss caused by malicious software and internal information leakage. Among these threats and risks, confidential information leakage is most likely to happen and cause serious consequences. Once data leakage occurs, enterprises not only need to undertake the loss of the value of confidential data itself, their reputation and public image may even be damaged, or be liable to penalties or prosecution.



Contents

1. Why Do We Need Information Security?
2. **What is Information Security?**
3. How to Ensure Information Security?
4. Network Security



Providing CIA Protection for Information Assets

Confidentiality

Private data should not be disclosed to unauthorized individuals.

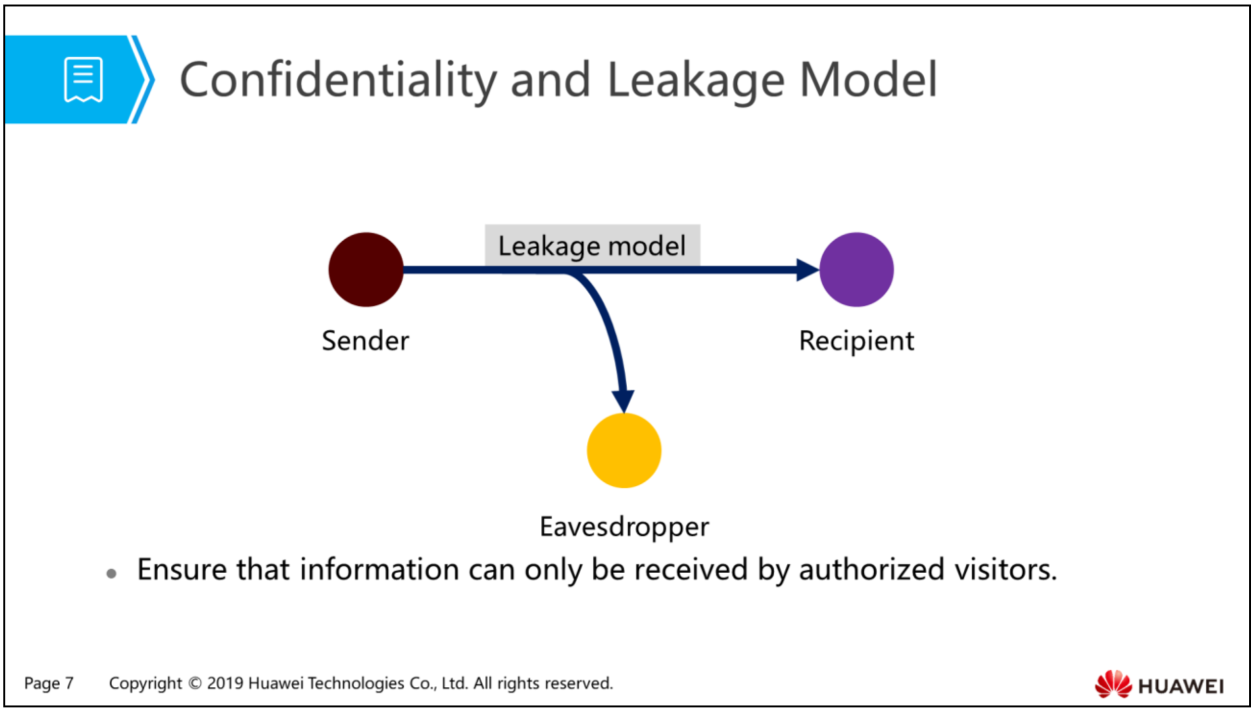
Integrity

Information and procedure cannot be accessed by intentional or unintentional unauthorized manipulation.

Availability

Systems should provide services in time and should not deny authorized users.

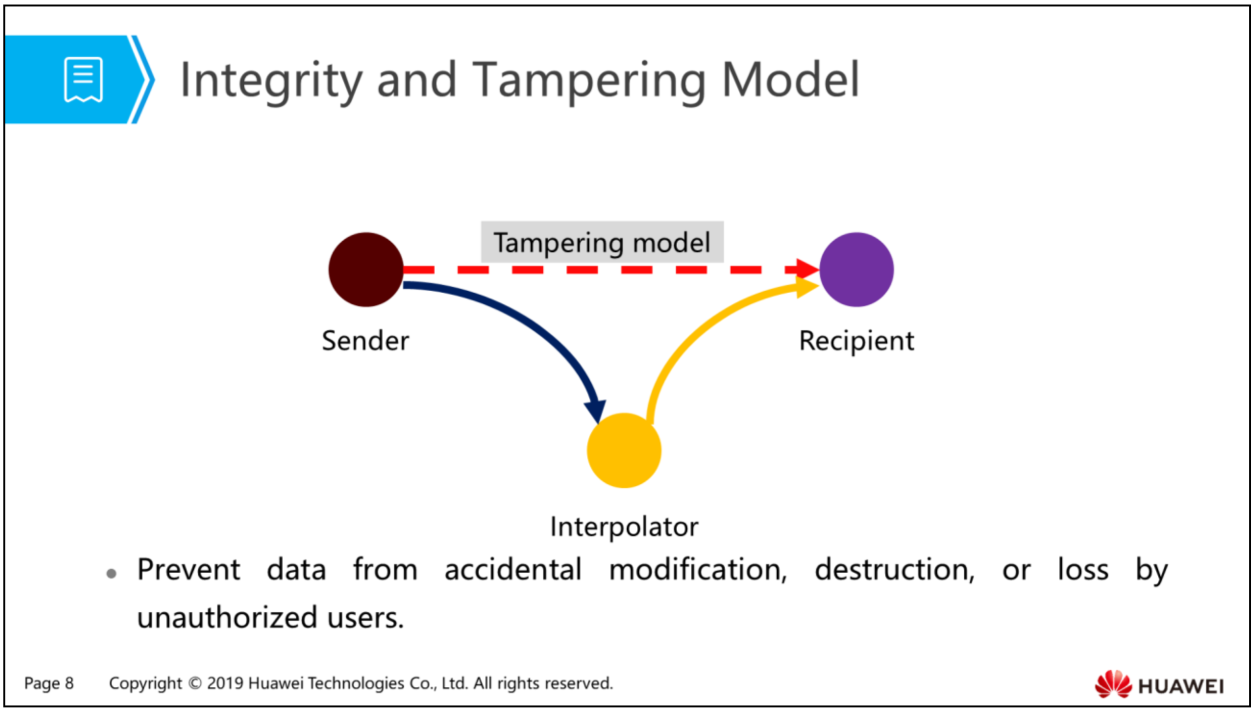
- The core target of information security is to provide key assets with CIA protection. CIA refers to confidentiality, integrity, and availability. The implementation of all security control, mechanism and prevention measures is to provide one or more of these principles.
- Confidentiality, Integrity, and Availability (CIA) are the three most basic objectives of information security:
  - Confidentiality: Information is not disclosed to unauthorized users or entities during the process of storage, transmission, and usage.
  - Integrity: Information is not modified by unauthorized users or improper modification on information by authorized users is prevented during the process of storage, transmission, and usage.
  - Availability: ensure that the normal usage of information resources by authorized users or entities is not rejected and their reliable and timely access to information resources is allowed.



Confidentiality and Leakage Model

- Ensure that information can only be received by authorized visitors.

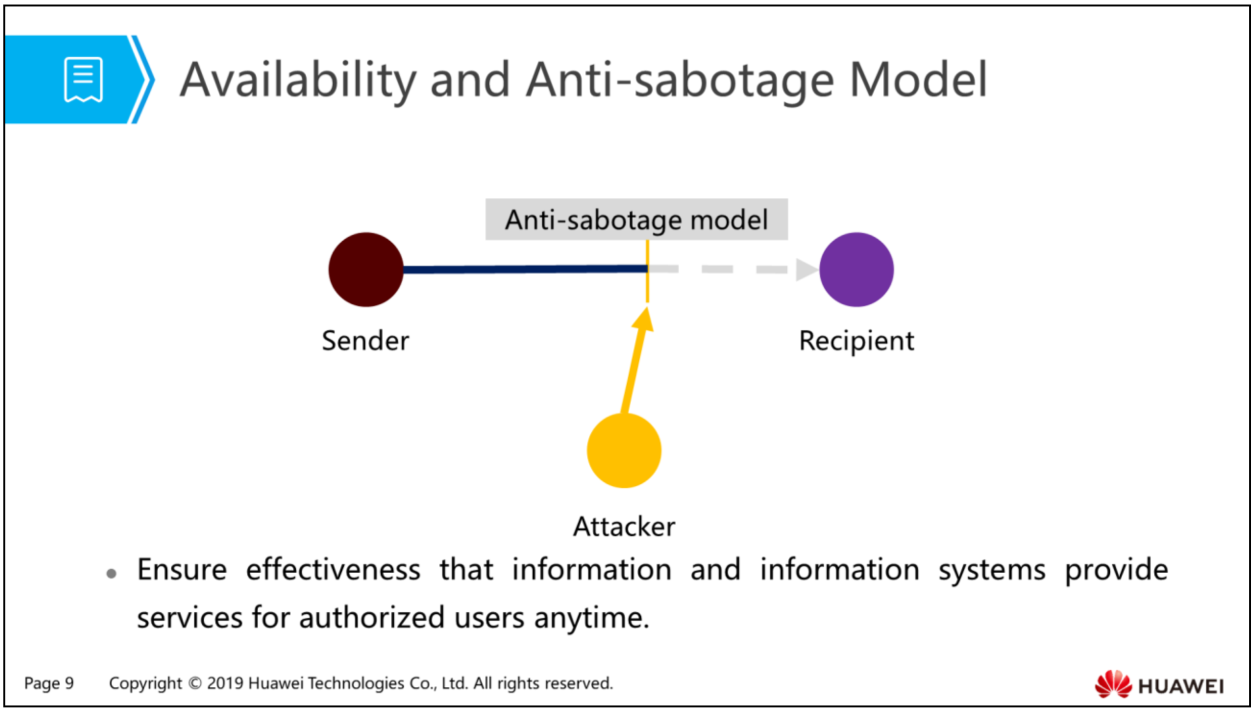
- We can understand confidentiality in this simple way: only authorized individuals, entities, or processes can access protected information. We can adopt proper encryption modes to guarantee confidentiality.
- Confidentiality indicates that information cannot be disclosed to unauthorized ones, which may include individuals, entities, and processes. There are various information leakage ways, such as verbal disclosure or through networks, printers, copiers and USB storage devices. Confidentiality is the attribute emphasized the most in daily information security work and the easiest to be understood. This is because confidentiality is not as broad as the other two attributes in terms of meaning and users can compare it with the concept of secrets in the real world easily.
- The basic process of data encryption is to process files or data which is originally in plain text through certain algorithms, so as to render it as a segment of unreadable codes which is commonly called cipher-text and can be displayed only after entering the corresponding key. Through this method, the protected data will not be stolen or read illegally. The reverse process is decryption, which is the process of converting the coded information into the original data.



Integrity and Tampering Model

- Prevent data from accidental modification, destruction, or loss by unauthorized users.

- Integrity is usually perceived as "preventing unauthorized modification" and "tamper-proofing" and its meaning varies according to different environments.
- In the information security field, information asset integrity also means:
  - Accurate and correct, instead of vague;
  - Not being tampered;
  - Being modified only through approved method;
  - Being modified only by authorized personnel or processes;
  - Meaningful and useful.
- Common factors that affect information integrity include: the source of information, which involves where to obtain, how to obtain and through whom to obtain the information; the protection status before and after information arrives the organization.
- Message digest is also called digital digest. It is a value which maps only the fixed length of information or text and generated through a one-way hash function towards the information. Recipients calculate received messages and compare the generated digests with the original ones. If messages were changed in transit, the result is inconsistent, which can help determine whether the message has been changed. Therefore, message digest guarantees message integrity.



Availability and Anti-sabotage Model

Anti-sabotage model

Sender

Recipient

Attacker

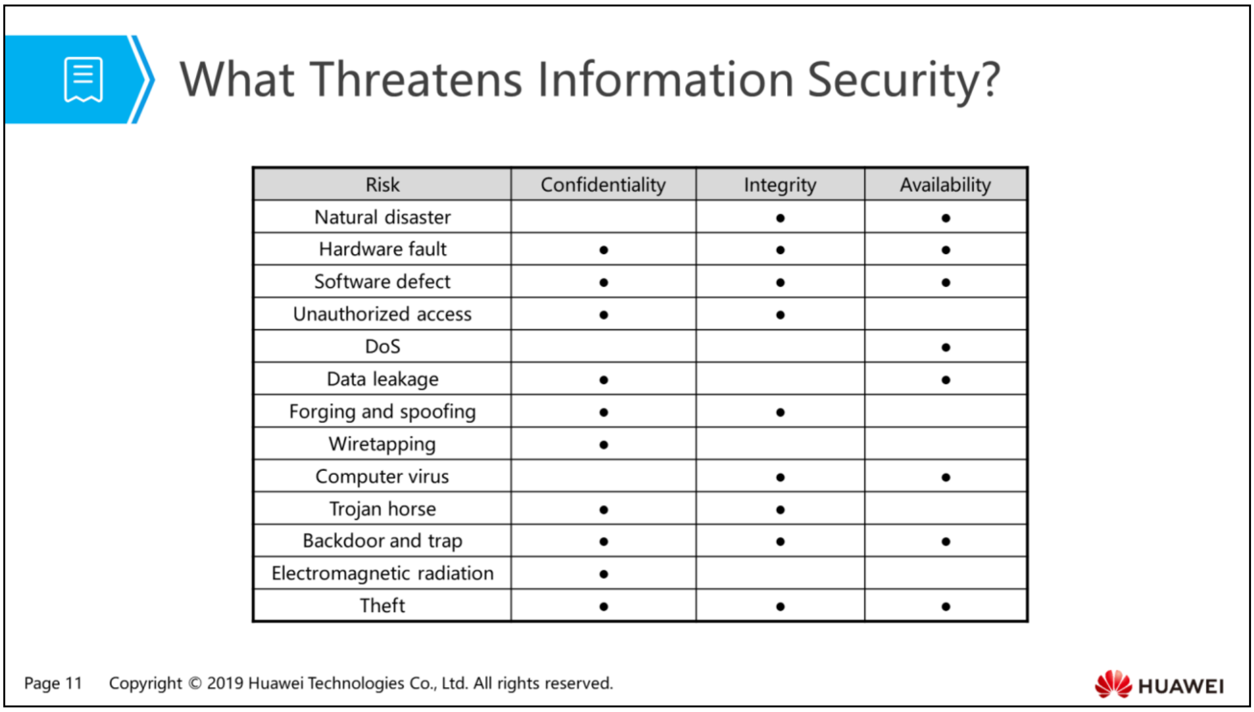
- Ensure effectiveness that information and information systems provide services for authorized users anytime.

Page 9 Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved. HUAWEI

- Simply speaking, availability means that "authorized users can use anytime they want". If an objective or service is considered available, the following requirements must be satisfied:
  - Presented in a way that can be used;
  - Has the capability to satisfy service requirements;
  - Has a clear process and the waiting duration is limited in the wait status;
  - Services can be completed within an acceptable time segment.
- Access rejection and system outage are important aspects of unavailability, while business continuity management is an important measure to maintain information availability. Generally speaking, requirement for information processing facilities availability is higher.

Contents

1. Why Do We Need Information Security?
2. What is Information Security?
3. **How to Ensure Information Security?**
4. Network Security



What Threatens Information Security?

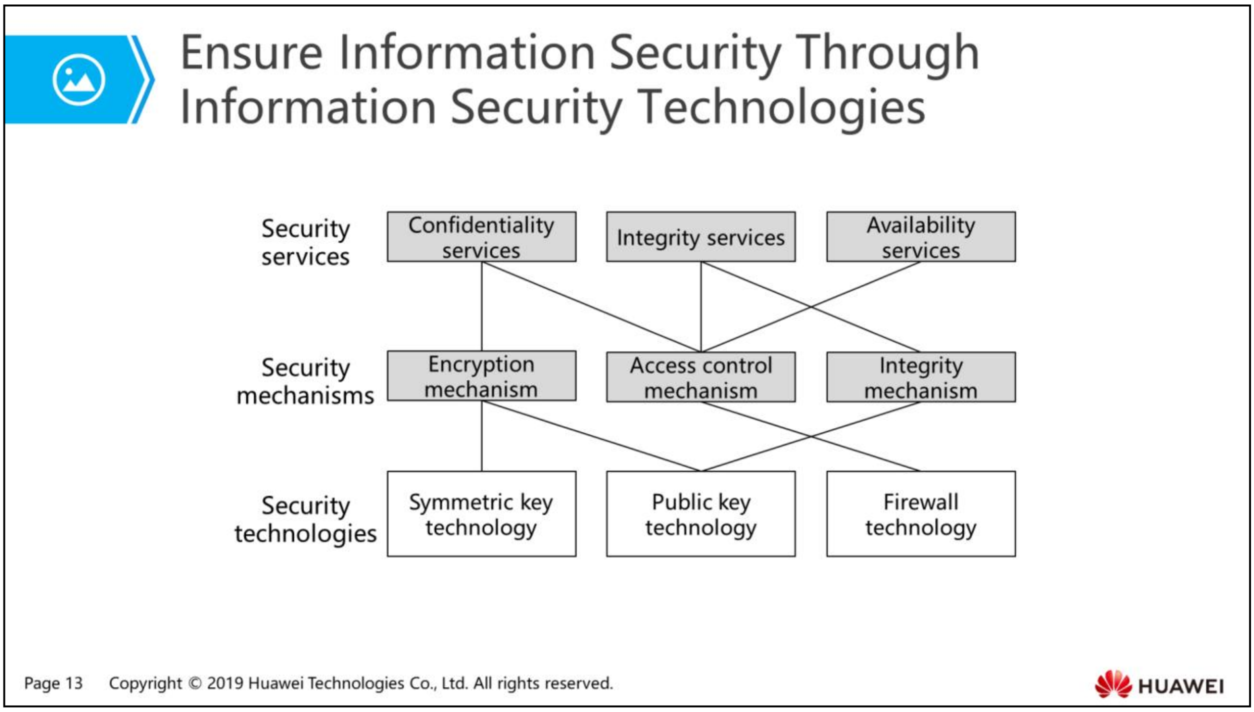
Risk	Confidentiality	Integrity	Availability
Natural disaster		●	●
Hardware fault	●	●	●
Software defect	●	●	●
Unauthorized access	●	●	
DoS			●
Data leakage	●		●
Forging and spoofing	●	●	
Wiretapping	●		
Computer virus		●	●
Trojan horse	●	●	
Backdoor and trap	●	●	●
Electromagnetic radiation	●		
Theft	●	●	●

Page 11

HUAWEI

- There are many factors that threaten information security and each of them has different impact on confidentiality, integrity, and availability. For example, if the data on the hard disk is lost due to some faults on the hard disk, the integrity of data is damaged; if users cannot access these data when they are in need, the availability of data is damaged; if someone copies the data for competitors when the hard disk is repaired by a third party, the confidentiality of data is damaged.
- The preceding table describes the main factors that threaten information security:
    - Natural disaster: refers to earthquake, fire, flood, and storm which will directly threaten the information system entity security.
    - Hardware fault: indicates the security and reliability of the system hardware, including the security of hardware, storage system, auxiliary equipment, data communication facility, and information storage medium.
    - Software defect: refers to the problems and errors that interrupt the normal operation of the software or program, or some hidden functional defects.
    - Unauthorized access: the action of using network or computer resources without agreement in advance. Such as intentional avoidance of system access control mechanism, improper use of network equipment and resources, privilege expansion without permission, unauthorized access to information. It mainly has the following forms: spoofing, identity attack, access to the network system and illegal operations by unauthorized users, and unauthorized operations by authorized users.
    - DoS: Denial of Service (DoS) means that attackers send a large amount of junk or interference information to the server, making normal users cannot access the server.

- Data leakage: unencrypted database is insecure and liable to disclose commercial data.
- Forging and spoofing: indicates that an illegal user pretends to be a legal one through spoofing communication system or the user, or a user with little privilege pretends to be a highly privileged one. Most hackers adopt spoofing attack.
- Wiretapping: steal information resources and sensitive information in the system by any legal or illegal means. For example, wiretap signals transmitted in communication lines, or intercept useful information by using electromagnetic leakage of communication equipment during the working process.
- Computer virus: a program that can infect and damage computer system during its operational process.
- Trojan horse: a malicious and unperceivable program segment contained in software. When executed, it will damage user security. This program is called Trojan Horse.
- Backdoor and trap: an "organ" set in a system or a part. When specific data is input, violation of security policy is allowed.
- Electromagnetic radiation: the computer system and its information and data transmission channel can generate electromagnetic wave radiation during their working process which is easy to be detected and received by radio receivers in certain geographical scope. That will result in information leakage through electromagnetic radiation. In addition, space electromagnetic radiation may cause electromagnetic interference to the system and affect its operation.
- Theft: important security items such as token or ID card are stolen.

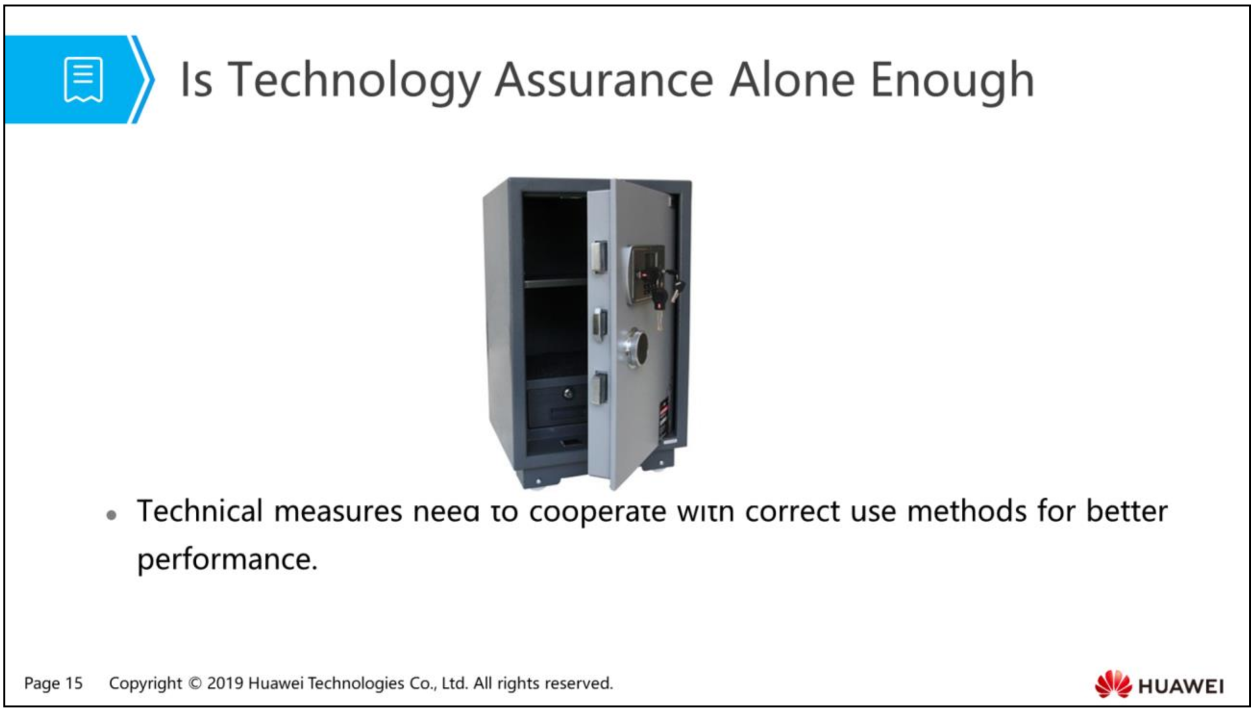


Ensure Information Security Through Information Security Technologies

Page 13 Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved. HUAWEI

- To guarantee information confidentiality, integrity and availability, corresponding security mechanisms can be used:
  - Confidentiality service can be implemented through encryption mechanism and access control mechanism.
  - Integrity service can be implemented through access control mechanism and integrity mechanism.
  - Availability service can be implemented through access control mechanism.
- Security mechanism is implemented through security technologies:
  - Encryption mechanism can be implemented through symmetric key technology and public key technology.
  - Access control mechanism can be implemented through firewall technology.
  - Integrity mechanism can be implemented through public key technology.
- As described above, security services indicate security safeguards provided for protecting information security, security mechanisms are measures which support security services, and security technology is the specific manifestation of security mechanism.
- Symmetric key technology:
  - Symmetric key encryption is also called secret key encryption, which means that data senders and recipients must use the same key to encrypt and decrypt plaintext. Symmetric key encryption algorithms mainly refer to DES, 3DES.

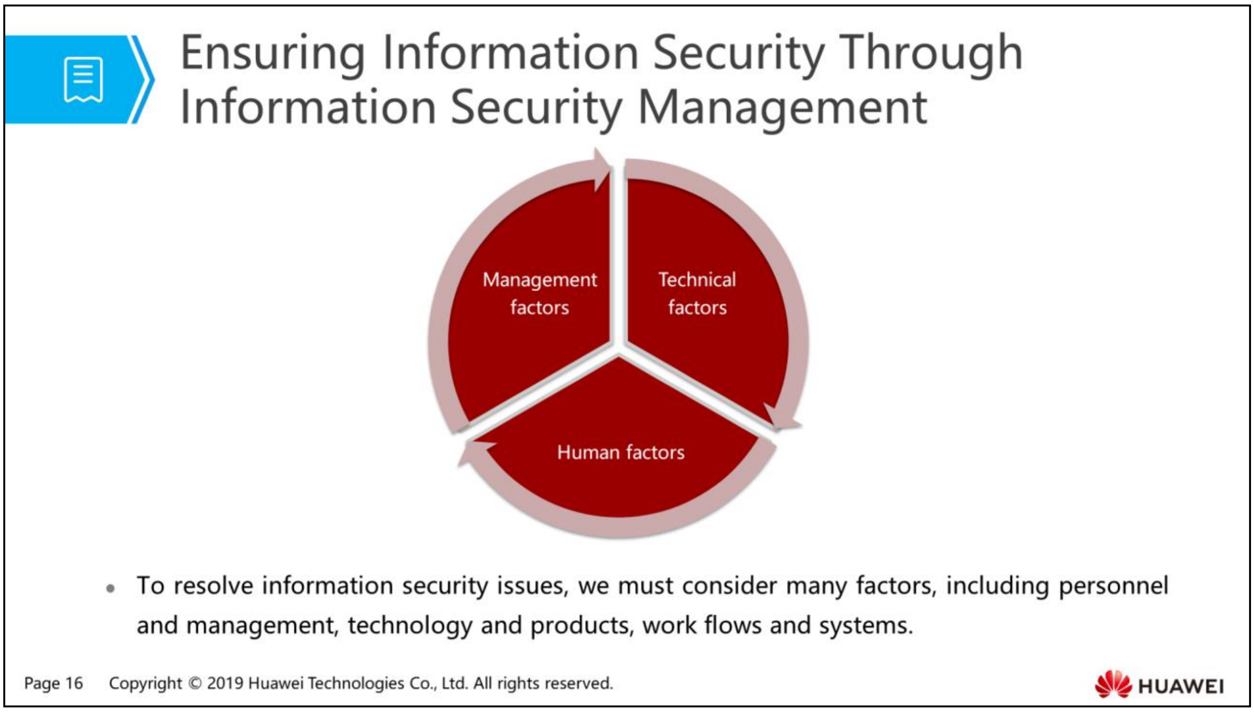
    - DES is a data encryption standard developed by the National Institute of Standards and Technology (NIST) of the United States in 1977. DES, whose file number is FIPS PUB46, was developed according to the German Enigma encryptor seized by the allies during World War II, but more complicated and rigorous. This is a long-established and strong encryption algorithm which enjoys high reputation due to wide usage. The algorithm is named Data Encryption Algorithm (DEA). DES is the most commonly used symmetric encryption algorithm. Its key length is 56 bytes, and the packet length is 64 bytes. To strengthen encryption, the triple DES encryption is developed, that is, 3DES.
    - 3DES or Triple DES is the generic term of Triple Data Encryption Algorithm (TDEA) block cipher. It equals to the application of the DES encryption algorithm three times to each data block. Due to the enhancement of computers calculation capability, the key length of original DES password is prone to violent cracking; 3DES is designed to provide a relatively easy method, that is, to increase DES key length, to avoid similar attacks, rather than designing a new block cipher algorithm.
- Public key technology:
    - Public key encryption algorithm is also called asymmetric key algorithm which uses two pairs of keys: one public key and one private key. Users need to ensure the security of the private key; the public key can be released. The public key is closely related to the private key. Information encrypted with the public key can be decrypted only by the private key, and vice versa. Because the public key algorithm does not need online key server and the key distribution protocol is simple, key management is greatly simplified. Apart from encryption function, the public key system can also provide digital signature.
    - The advantage of public key password is that keys do not need to be transmitted through secure channels, which greatly simplify key management.
- Firewall technology:
    - Firewall is a technical measure to protect computer network security. It isolates the communication between the internal and external network by establishing a network communication monitoring system on the network borders, so as to prevent network intrusion from external network.



Is Technology Assurance Alone Enough

- Technical measures need to cooperate with correct use methods for better performance.

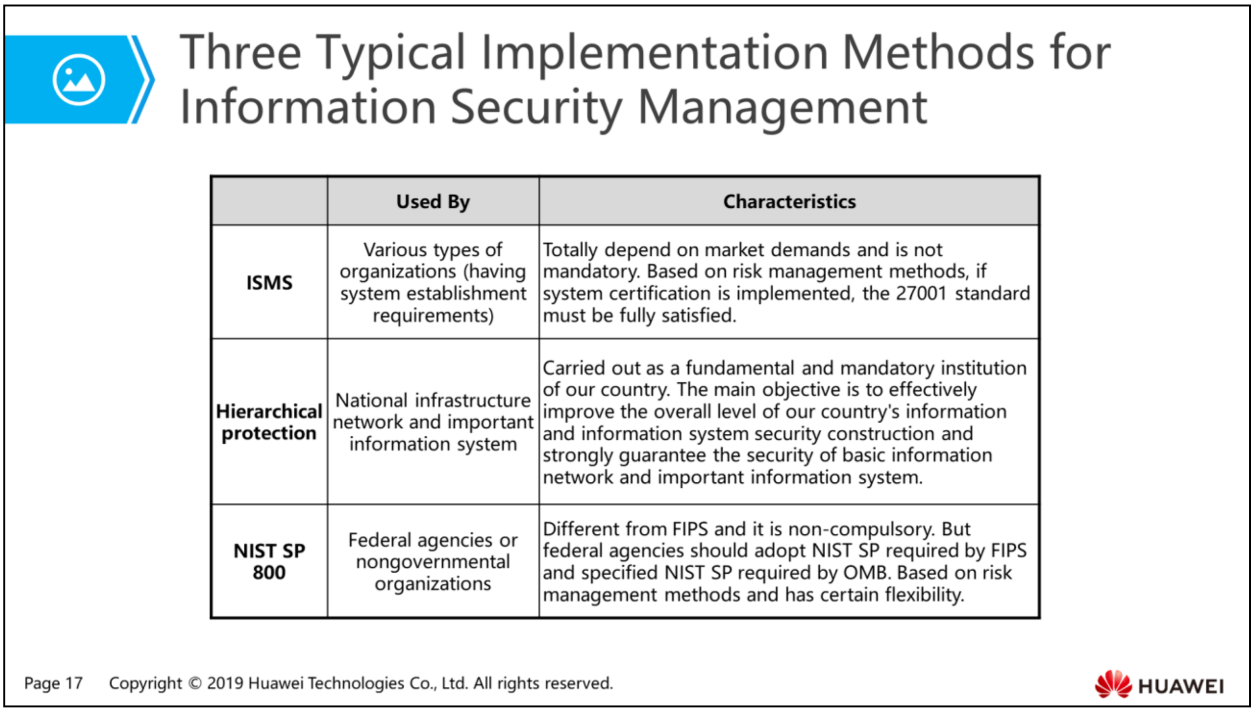
- Just like leaving the safe key on the keyhole, a well-designed network defense system barely functions due to invalid external connections.



Ensuring Information Security Through Information Security Management

- To resolve information security issues, we must consider many factors, including personnel and management, technology and products, work flows and systems.

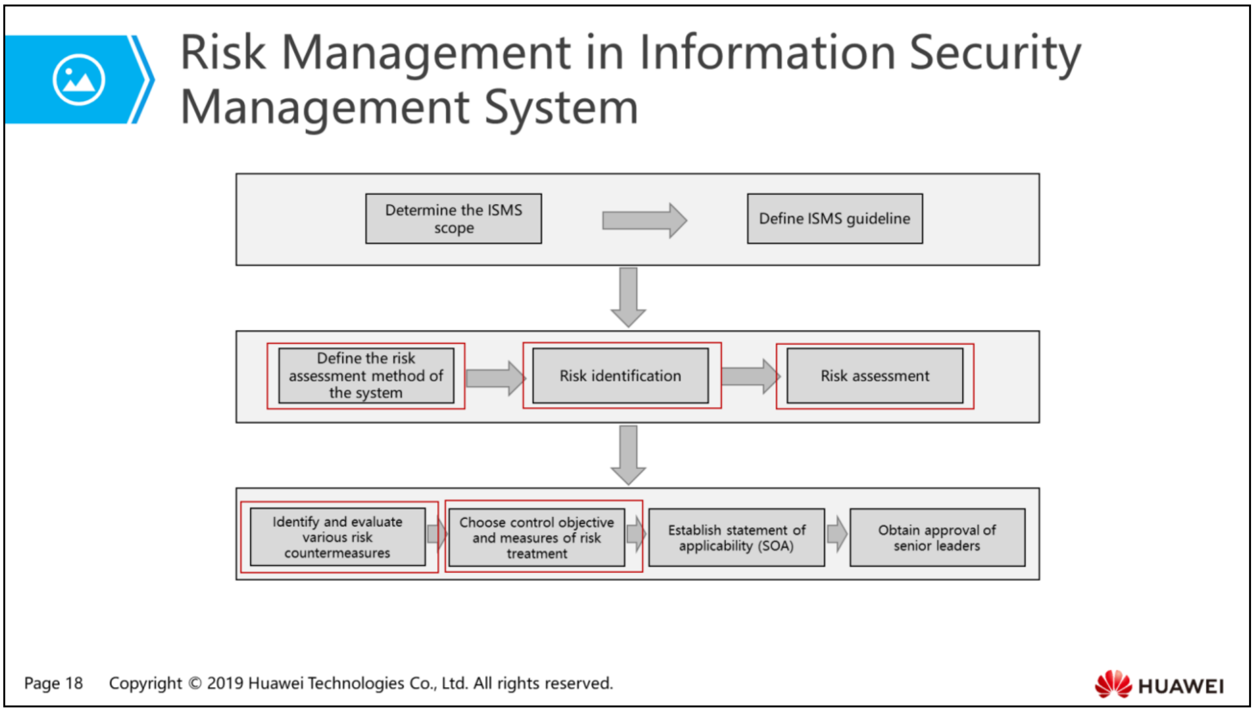
- To resolve information security issues, we must consider many factors, including personnel and management, technology and products, work flows and systems. Information security management system is interaction among personnel, management, and technology.



Three Typical Implementation Methods for Information Security Management

	Used By	Characteristics
ISMS	Various types of organizations (having system establishment requirements)	Totally depend on market demands and is not mandatory. Based on risk management methods, if system certification is implemented, the 27001 standard must be fully satisfied.
Hierarchical protection	National infrastructure network and important information system	Carried out as a fundamental and mandatory institution of our country. The main objective is to effectively improve the overall level of our country's information and information system security construction and strongly guarantee the security of basic information network and important information system.
NIST SP 800	Federal agencies or nongovernmental organizations	Different from FIPS and it is non-compulsory. But federal agencies should adopt NIST SP required by FIPS and specified NIST SP required by OMB. Based on risk management methods and has certain flexibility.

- Three typical methods for information security management are: information security management system (international standard), hierarchical protection (Chinese standard), NIST SP 800 (the United States standard). We will focus on Information Security Management System (ISMS).
- Information Security Management System (ISMS) was originated from the British standard BS7799 set by British Standards Institution (BSI) in the 1990s. It is the application of systemic management in information security field. After the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) converted the relevant work of BSI into ISMS international standard (ISO/IEC 27001:2005), ISMS has been accepted and recognized quickly by all kinds of organizations in the world and becomes a powerful weapon to solve information security problems for organizations in different countries and regions, types and scales. ISMS certificate has also become a symbol for organizations to prove its information security ability and level to their interested parties, such as customers and partners, and the social public.
- Hierarchical protection: information security hierarchical protection is a work which protects information and information carrier in a hierarchical way according to their importance level and exists in information security field of many countries, such as China and the United States.
- NIST SP 800: it is a series of information security guideline published by the National Institute of Standards and Technology (NIST) of the U.S. (SP is short for Special Publications). Although NIST SP is not an official mandatory standard in the series of standard documents of NIST, it has become a practice standard and authoritative guideline recognized by the U.S. and the international security community. NIST SP 800 series has become the main standard and reference to guide American information security management construction.



Risk Management in Information Security Management System

Determine the ISMS scope → Define ISMS guideline

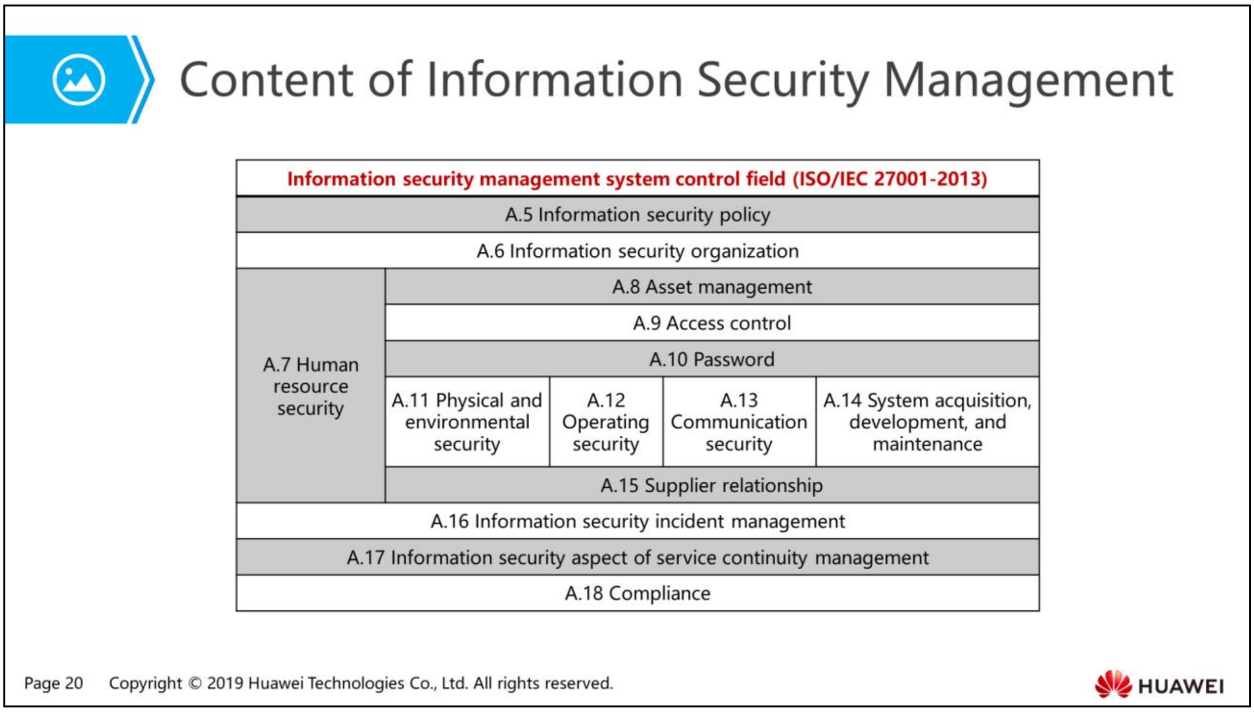
Define the risk assessment method of the system → Risk identification → Risk assessment

Identify and evaluate various risk countermeasures → Choose control objective and measures of risk treatment → Establish statement of applicability (SOA) → Obtain approval of senior leaders

Page 18

- As shown in the picture, the construction flow of the information security management system can follow certain standards. Here we focus on the position and roles of risk assessment, risk treatment, risk management and control measures of risk management.
- Risk assessment is the foundation of information security management:
  - The construction of information security management system must identify information security demands.
  - The main method of obtaining the information security demands is security risk assessment.
  - The risk assessment of information security is the foundation of constructing the information security management system. Without risk assessment, there will be no basis of constructing the information security management system.
  - Risk assessment refers to the process of appraising and assessing information assets within the information security management system, evaluating threats and vulnerabilities of information assets, and defining existing or planned security control measures.
- Risk treatment is the core of information security management:
  - Risk treatment is to make decisions toward risks recognized in the risk assessment process, deal with unacceptable risks through proper measures and control the risk within an acceptable scope.
  - Risk assessment can only demonstrate risks of the system but cannot change risk status.

  - Only the risk treatment can enhance the information security capability, meet the demand of information security and achieve the goal of information security.
  - The core of information security management lies in the integrated risk treatment measures.
- Risk management is the fundamental method of information security management:
  - Corresponding risk treatment should be taken to deal with the results of risk assessment. In essence, the optimal collective of risk treatment is collective control measures of information security management system.
  - The process of figuring out these collective risk control measures is the process of constructing the information security management system.
  - Periodical risk assessment and risk treatment constitute the dynamic risk management.
  - The dynamic risk management is the basic way to conduct information security management, achieve information security objectives and maintain the level of information security.
- Control measures are specific methods of risk management:
  - Specific methods of risk management are control measures.
  - When dealing with risks, it is necessary to choose and determine proper control objectives and measures. Only by implementing appropriate control measures can we reduce those unacceptable high risks to an acceptable range.



Content of Information Security Management

Information security management system control field (ISO/IEC 27001-2013)

A.5 Information security policy

A.6 Information security organization

A.7 Human resource security

A.8 Asset management

A.9 Access control

A.10 Password

A.11 Physical and environmental security

A.12 Operating security

A.13 Communication security

A.14 System acquisition, development, and maintenance

A.15 Supplier relationship

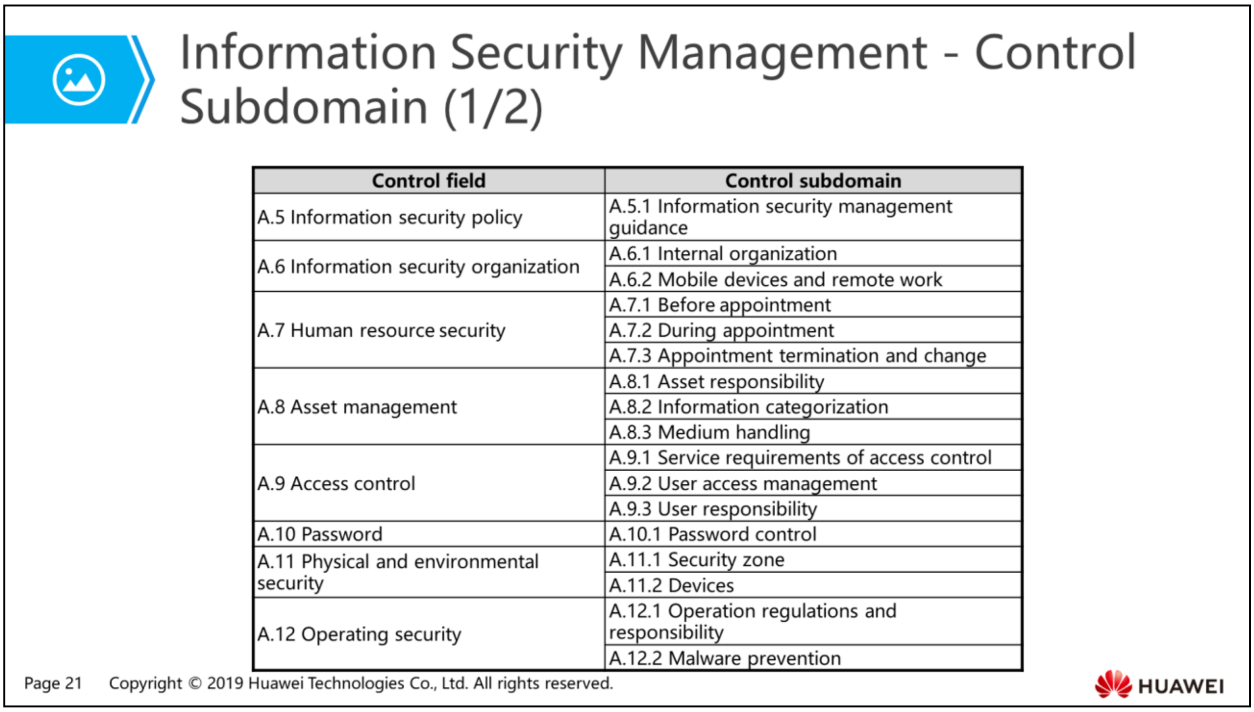
A.16 Information security incident management

A.17 Information security aspect of service continuity management

A.18 Compliance

Page 20

- ISO/IEC 27000 series international standard is the best industry practice about how to manage information security in a holistic way. It divides the essential components of information security management system into different modules. We need to master which control fields should be paid attention to in the information security management system. Subdomains and objectives of each control field only need basic understanding.
- International standard ISO/IEC 27001:2013 *Information technology-Security techniques-Information security management systems-Requirements* lists 14 fields and 113 control measures that need to be paid attention to in information security management. The 14 control fields are shown in the picture (the number before each article indicates its chapter location in this international standard).
    - A.5 Security policy
    - A.6 Information security organization
    - A.7 Human resource security
    - A.8 Asset management
    - A.9 Access control
    - A.10 Cryptology
    - A.11 Physical and environmental security
    - A.12 Operational security
    - A.13 Communication security
    - A.14 Information system obtaining, development and maintenance
    - A.15 Supplier relationship
    - A.16 Information security incident management
    - A.17 Service continuity management in information security aspect
    - A.18 Compliance



Information Security Management - Control Subdomain (1/2)

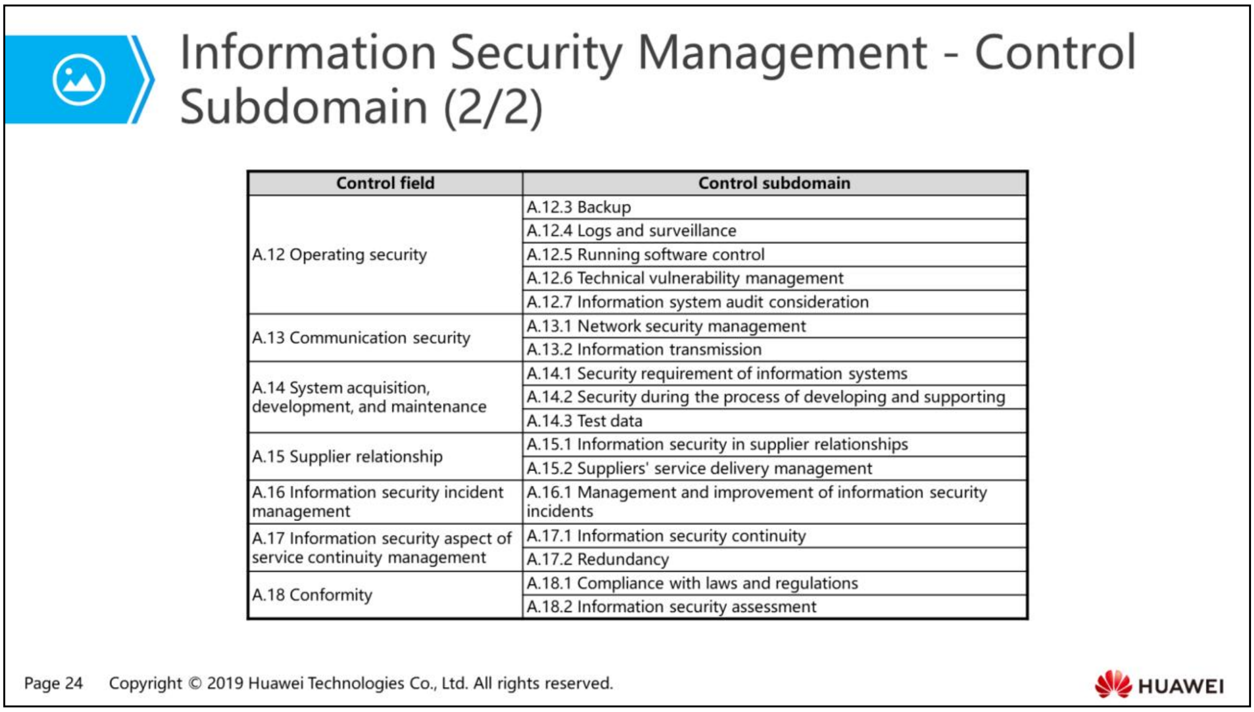
Control field	Control subdomain
A.5 Information security policy	A.5.1 Information security management guidance
A.6 Information security organization	A.6.1 Internal organization
	A.6.2 Mobile devices and remote work
A.7 Human resource security	A.7.1 Before appointment
	A.7.2 During appointment
	A.7.3 Appointment termination and change
A.8 Asset management	A.8.1 Asset responsibility
	A.8.2 Information categorization
	A.8.3 Medium handling
A.9 Access control	A.9.1 Service requirements of access control
	A.9.2 User access management
	A.9.3 User responsibility
A.10 Password	A.10.1 Password control
A.11 Physical and environmental security	A.11.1 Security zone
	A.11.2 Devices
A.12 Operating security	A.12.1 Operation regulations and responsibility
	A.12.2 Malware prevention

Page 21

- A.5 Information security policy:
  - A.5.1 Information security management guidance:
    - Objective: Provide management guidance and support for information security according to service requirements and relevant laws and regulations.
- A.6 Information security organization:
  - A.6.1 Internal organization:
    - Objective: Establish a management framework to start and control the implementation and operation of information security within an organization.
  - A.6.2 Mobile devices and remote work:
    - Objective: Ensure the security of mobile devices remote work and usage.
- A.7 Human resource security:
  - A.7.1 Before appointment:
    - Objective: Ensure that employees and contractors understand their responsibilities and match their roles.
  - A.7.2 During appointment:
    - Objective: Ensure that employees and contractors recognize and fulfill their information security responsibilities.
  - A.7.3 Appointment termination and change:
    - Objective: Protect organization interest during appointment change and termination.
- A.8 Asset management:
  - A.8.1 Asset responsibility:

        - Objective: Identify organization asset and define proper protection responsibilities.
    - A.8.2 Information categorization:
        - Objective: Ensure that information is protected in proper levels according to its importance to the organization.
    - A.8.3 Medium handling:
        - Objective: Prevent information stored in medium from unauthorized leakage, modification, removal or destruction.
- A.9 Access control:
    - A.9.1 Service requirements of access control:
        - Objective: Restrict access to information and information handling facilities.
    - A.9.2 User access management:
        - Objective: Ensure authorized users' access to systems and services and prevent unauthorized access.
    - A.9.3 User responsibility:
        - Objective: Make users undertake their responsibilities of protecting authentication information.
- A.10 Password:
    - A.10.1 Password control:
        - Objective: Ensure proper and effective use of password technology to protect information confidentiality, authenticity and (or) integrity.
- A.11 Physical and environmental security:
    - A.11.1 Security zone:
        - Objective: Prevent unauthorized physical access, damage and interference to organization information and information handling facilities.
    - A.11.2 Devices:
        - Objective: Prevent asset loss, damage, theft or security threats and the disruption of organization activities.
- A.12 Operating security:
    - A.12.1 Operation regulations and responsibility:
        - Objective: Ensure correct and secure operations on information handling facilities.
    - A.12.2 Malware prevention:
        - Objective: Ensure malware prevention of information and information handling facilities.
    - A.12.3 Backup:
        - Objective: Prevent data loss.
    - A.12.4 Logs and surveillance:
        - Objective: Record incidents and generate evidence.
    - A.12.5 Running software control:
    - Objective: Ensure system integrity. A.12.6 Technical vulnerability management:
        - Objective: Prevent utilization of technical vulnerability.

    - A.12.7 Information system audit consideration:
        - Objective: Minimize the impact of audit activities on operating system.
- A.13 Communication security:
    - A.13.1 Network security management:
        - Objective: Ensure that information and supporting information handling facilities on the network are protected.
    - A.13.2 Information transmission:
        - Objective: Ensure the security of information transmission between the organization and external entities.
- A.14 System obtaining, development and maintenance:
    - A.14.1 Security requirement of information systems:
        - Objective: Ensure that information security is an integral part of the whole lifecycle of information system. It also includes the requirement of information system that provides public network services.
    - A.14.2 Security during the process of developing and supporting:
        - Objective: Ensure that information security is designed and implemented during the lifecycle of information system developing.
    - A.14.3 Test data:
        - Objective: Ensure that the test data is protected.
- A.15 Supplier relationship:
    - A.15.1 Information security in supplier relationships:
        - Objective: Ensure that the organization asset that can be accessed by the supplier is protected.
    - A.15.2 Suppliers' service delivery management:
        - Objective: Maintain the security of information that complies with the supplier and the agreed level of service delivery.
- A.16 Information security incident management:
    - A.16.1 Management and improvement of information security incidents:
        - Objective: Ensure the adoption of consistent and effective method for management of information security incidents, including the communication about security incidents and vulnerabilities.
- A.17 Information security aspect of service continuity management:
    - A.17.1 Information security continuity:
        - Objective: Information security continuity should be integrated with service continuity management.
    - A.17.2 Redundancy:
        - Objective: Ensure the availability of information handling facilities.
- A.18 Compliance:
    - A.18.1 Compliance with laws and regulations:
        - Objective: Avoid violation of laws, regulations, rules or contract obligations related to information security and any security requirements.
    - A.18.2 Information security assessment:
        - Objective: Ensure the implementation and running of information security according to organization policies and rules.

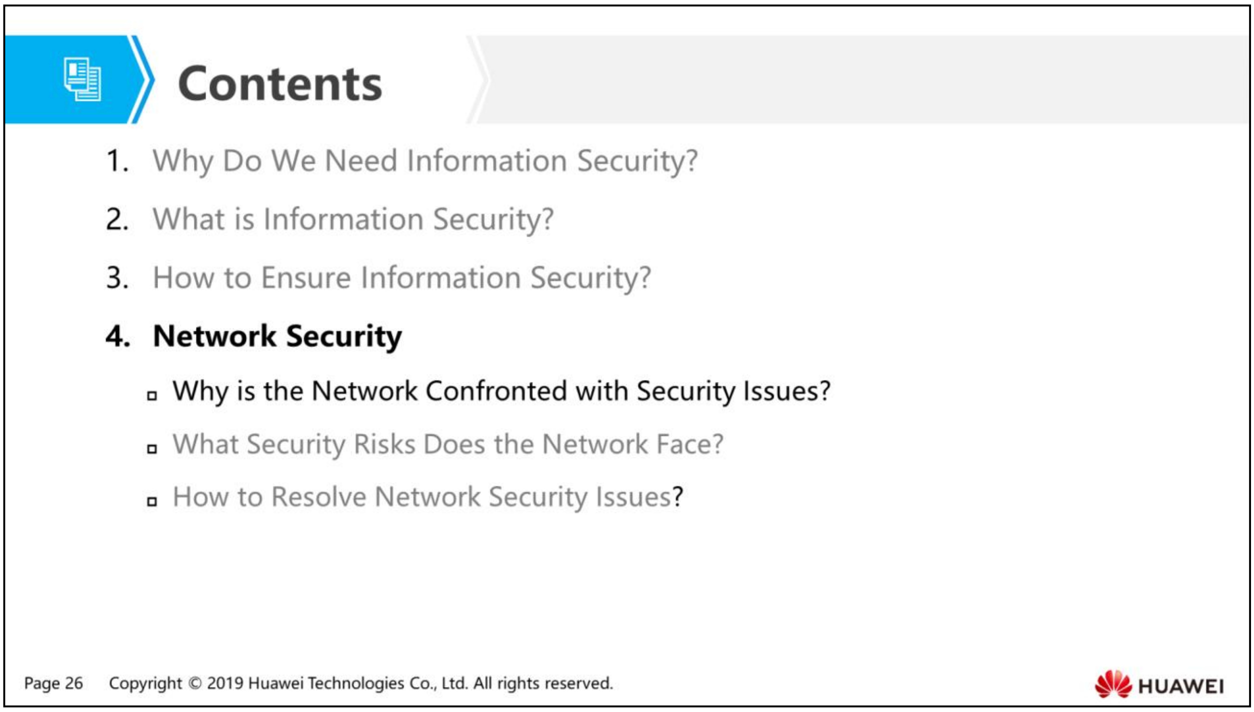


Information Security Management - Control Subdomain (2/2)

Control field	Control subdomain
A.12 Operating security	A.12.3 Backup
	A.12.4 Logs and surveillance
	A.12.5 Running software control
	A.12.6 Technical vulnerability management
	A.12.7 Information system audit consideration
A.13 Communication security	A.13.1 Network security management
	A.13.2 Information transmission
A.14 System acquisition, development, and maintenance	A.14.1 Security requirement of information systems
	A.14.2 Security during the process of developing and supporting
	A.14.3 Test data
A.15 Supplier relationship	A.15.1 Information security in supplier relationships
	A.15.2 Suppliers' service delivery management
A.16 Information security incident management	A.16.1 Management and improvement of information security incidents
A.17 Information security aspect of service continuity management	A.17.1 Information security continuity
	A.17.2 Redundancy
A.18 Conformity	A.18.1 Compliance with laws and regulations
	A.18.2 Information security assessment

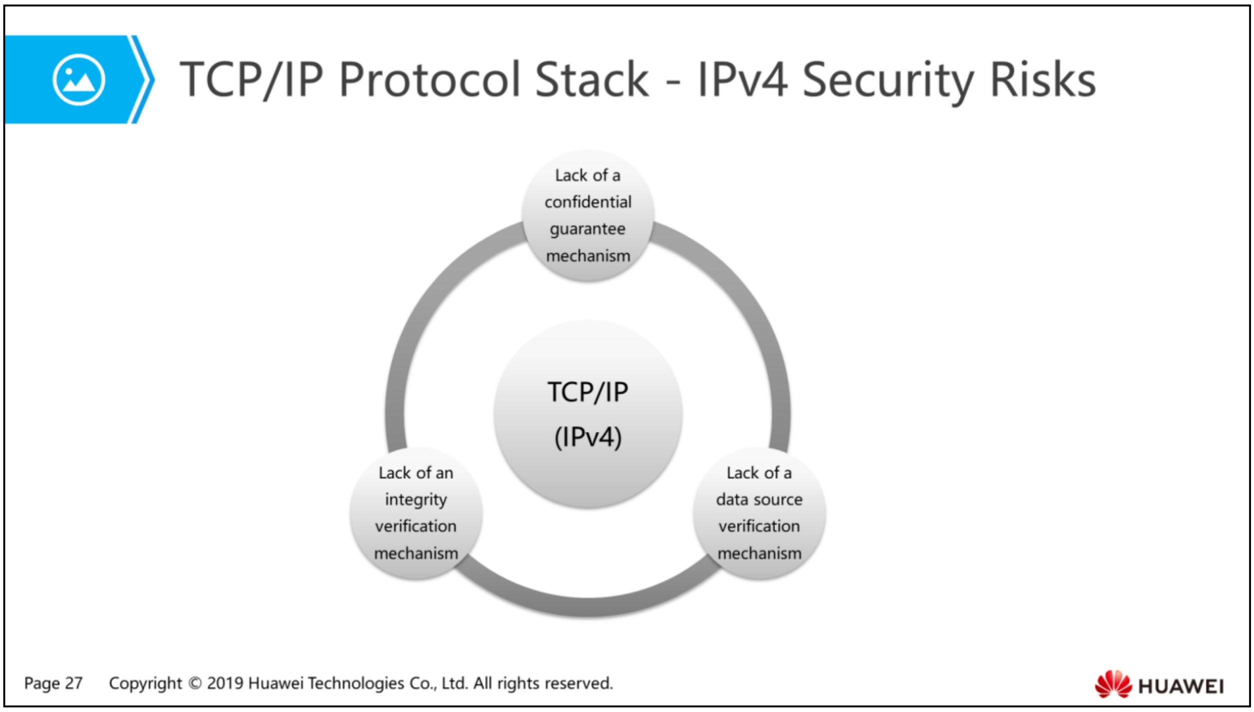
- A.12 Operating security:
  - A.12.3 Backup:
    - Objective: Prevent data loss.
  - A.12.4 Logs and surveillance:
    - Objective: Record incidents and generate evidence.
  - A.12.5 Running software control:
    - Objective: Ensure system integrity.
  - A.12.6 Technical vulnerability management:
    - Objective: Prevent utilization of technical vulnerability.
  - A.12.7 Information system audit consideration:
    - Objective: Minimize the impact of audit activities on operating system.
- A.13 Communication security:
  - A.13.1 Network security management:
    - Objective: Ensure that information and supporting information handling facilities on the network are protected.
  - A.13.2 Information transmission:
    - Objective: Ensure the security of information transmission between the organization and external entities.

- A.14 System obtaining, development and maintenance:
    - A.14.1 Security requirement of information systems:
        - Objective: Ensure that information security is an integral part of the whole lifecycle of information system. It also includes the requirement of information system that provides public network services.
    - A.14.2 Security during the process of developing and supporting:
        - Objective: Ensure that information security is designed and implemented during the lifecycle of information system developing.
    - A.14.3 Test data:
        - Objective: Ensure that the test data is protected.
- A.15 Supplier relationship:
    - A.15.1 Information security in supplier relationships:
        - Objective: Ensure that the organization asset that can be accessed by the supplier is protected.
    - A.15.2 Suppliers' service delivery management:
        - Objective: Maintain the security of information that complies with the supplier and the agreed level of service delivery.
- A.16 Information security incident management:
    - A.16.1 Management and improvement of information security incidents:
        - Objective: Ensure the adoption of consistent and effective method for management of information security incidents, including the communication about security incidents and vulnerabilities.
- A.17 Information security aspect of service continuity management:
    - A.17.1 Information security continuity:
        - Objective: Information security continuity should be integrated with service continuity management.
    - A.17.2 Redundancy:
        - Objective: Ensure the availability of information handling facilities.
- A.18 Conformity:
    - A.18.1 Compliance with laws and regulations:
        - Objective: Avoid violation of laws, regulations, rules or contract obligations related to information security and any security requirements.
    - A.18.2 Information security assessment:
        - Objective: Ensure the implementation and running of information security according to organization policies and rules.



Contents

1. Why Do We Need Information Security?
2. What is Information Security?
3. How to Ensure Information Security?
4. **Network Security**
   - Why is the Network Confronted with Security Issues?
   - What Security Risks Does the Network Face?
   - How to Resolve Network Security Issues?



TCP/IP Protocol Stack - IPv4 Security Risks

TCP/IP (IPv4)

Lack of a confidential guarantee mechanism

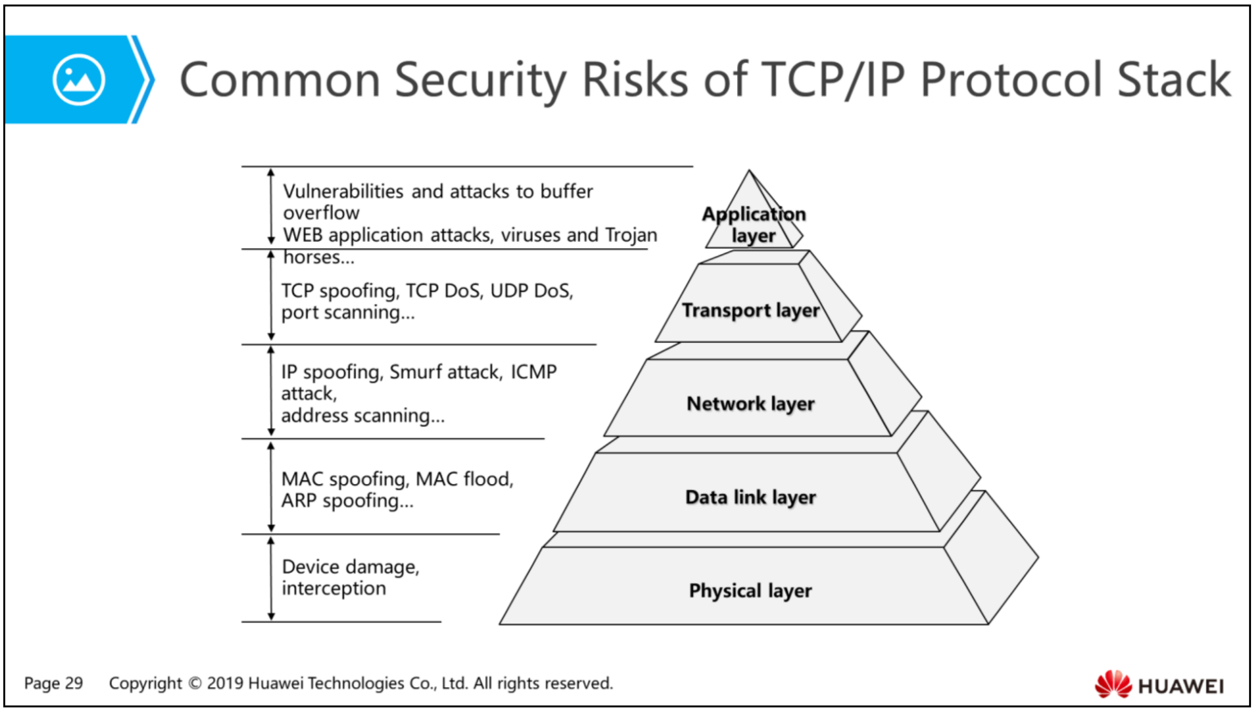
Lack of an integrity verification mechanism

Lack of a data source verification mechanism

- With the continuous development of the Internet, TCP/IP protocol family has become the most widely used internetworking protocol. However, due to insufficient consideration about security in design, the protocol has some security risks. Internet is firstly applied in the research environment for few reliable user groups, so the network security problem is not the major consideration. Therefore, most protocols in the TCP/IP protocol stack are not provided with necessary security mechanism. For example:
  - Authentication service is not provided.
  - Plaintext transmission without data confidentiality service.
  - Data integrity protection is not provided.
  - Non-repudiation service is not provided.
  - Availability is not assured—Quality of Service (QoS).

Contents

1. Why Do We Need Information Security?
2. What is Information Security?
3. How to Ensure Information Security?
4. **Network Security**
   - Why Is the Network Confronted with Security Issues?
   - What Security Risks Does the Network Face?
   - How to Resolve Network Security Issues?



Common Security Risks of TCP/IP Protocol Stack

Vulnerabilities and attacks to buffer overflow
WEB application attacks, viruses and Trojan horses...

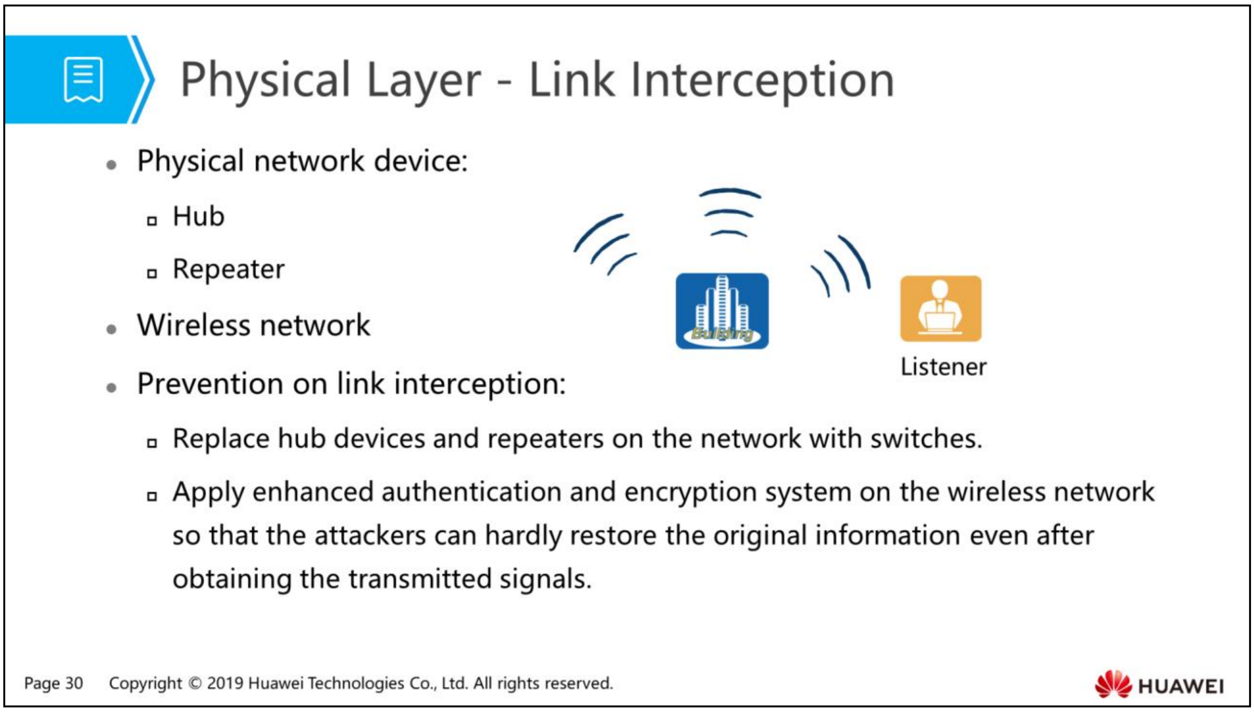
TCP spoofing, TCP DoS, UDP DoS, port scanning...

IP spoofing, Smurf attack, ICMP attack, address scanning...

MAC spoofing, MAC flood, ARP spoofing...

Device damage, interception

- Each layer in TCP/IP protocol stack has its own protocol. These protocols did not pay much attention to security factors at the beginning of the development and lacked essential security mechanisms. Therefore, with the increasing of security threats and attacks, the security problems of TCP/IP protocol stack becomes more and more serious. Next, we will have an overview on several attack types.

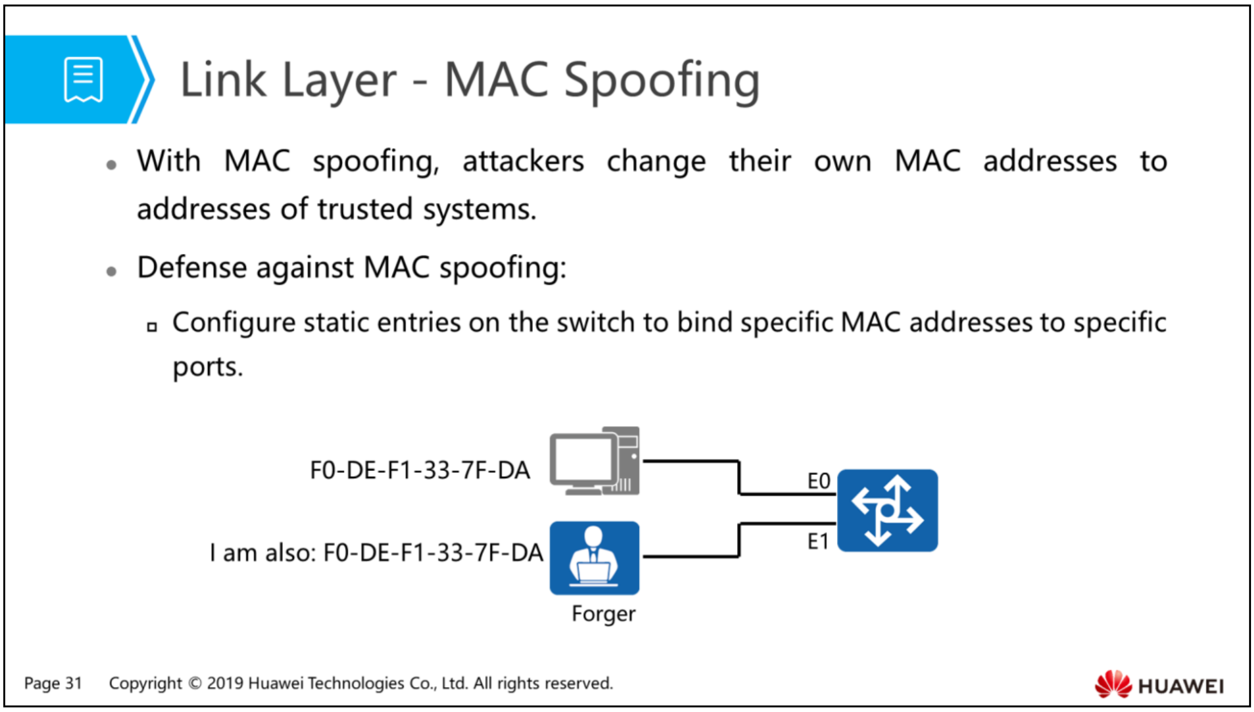


Physical Layer - Link Interception

- Physical network device:
  - Hub
  - Repeater
- Wireless network
- Prevention on link interception:
  - Replace hub devices and repeaters on the network with switches.
  - Apply enhanced authentication and encryption system on the wireless network so that the attackers can hardly restore the original information even after obtaining the transmitted signals.

Page 30

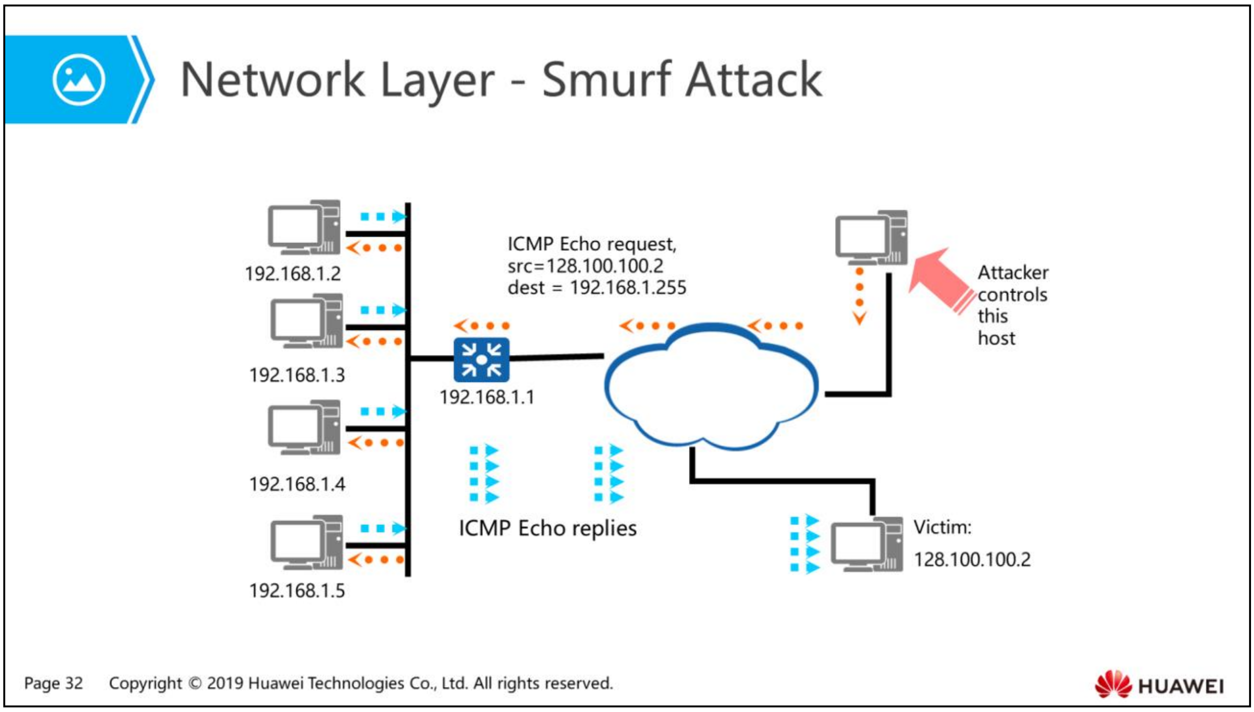
- Hub devices and repeaters function similarly on the network. Both of them forward data received from one port to other ports. Therefore, if an attacker accesses the hub device or repeater, the attacker can use sniffer tools to read data from the network.
- On the wireless network, data is transmitted in the form of wireless signals, which are easy for attackers to obtain.
- Interception is commonly used on Ethernet networks and is implemented based on transmission. An attack host that is equipped with the network card in hybrid mode can intercept all packets on the same physical network segment. The user name and password will be leaked when protocols (SNMP/POP3/Telnet) are authenticated in plaintext mode. The packet contents will be leaked and the packet header can be used when packets are transmitted in plaintext.



Link Layer - MAC Spoofing

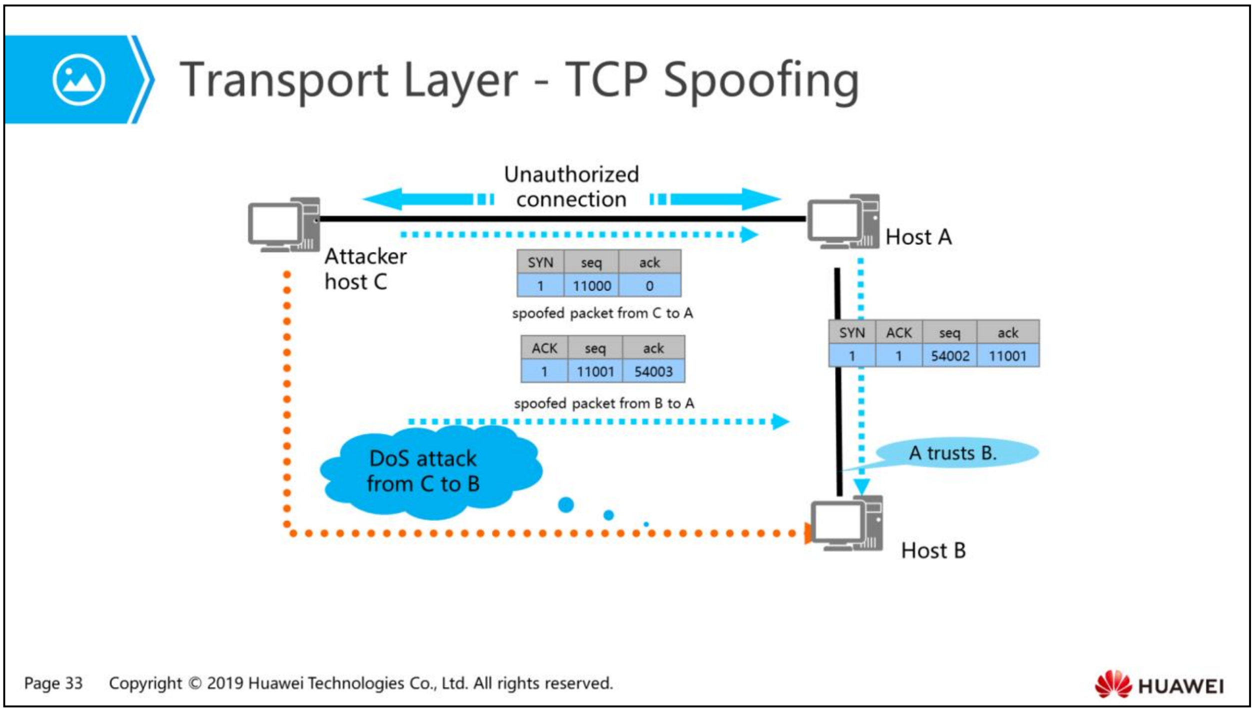
- With MAC spoofing, attackers change their own MAC addresses to addresses of trusted systems.
- Defense against MAC spoofing:
  - Configure static entries on the switch to bind specific MAC addresses to specific ports.

- An attacker sends packets with bogus MAC addresses to the switch, causing the switch to learn the incorrect mapping between MAC addresses and ports. As a result, the switch incorrectly sends packets to the forger. The forger then uses specific tools to obtain information for further attacks.
- You can configure static MAC entries on the switch to bind MAC addresses to correct outbound interfaces, preventing MAC spoofing.



Network Layer - Smurf Attack

- The attacker sends an ICMP echo request, and the destination IP address is specified to the broadcast address of the victim network. In this case, all hosts on the network reply to this ICMP echo request, causing network congestion. An advanced Smurf attack is used to attack a single host. The attacker changes the source address of the ICMP echo request to the address of the victim host and sends the request, crashing the victim host. A real attack requires sufficient traffic and time. Theoretically, the more hosts exist on the network, the more obvious the attack effect is.
- To protect a device against Smurf attacks, configure the device to check whether the destination address of the ICMP request packet is the broadcast or network address of the subnet. If yes, deny the request.



Transport Layer - TCP Spoofing

SYN	seq	ack
1	11000	0

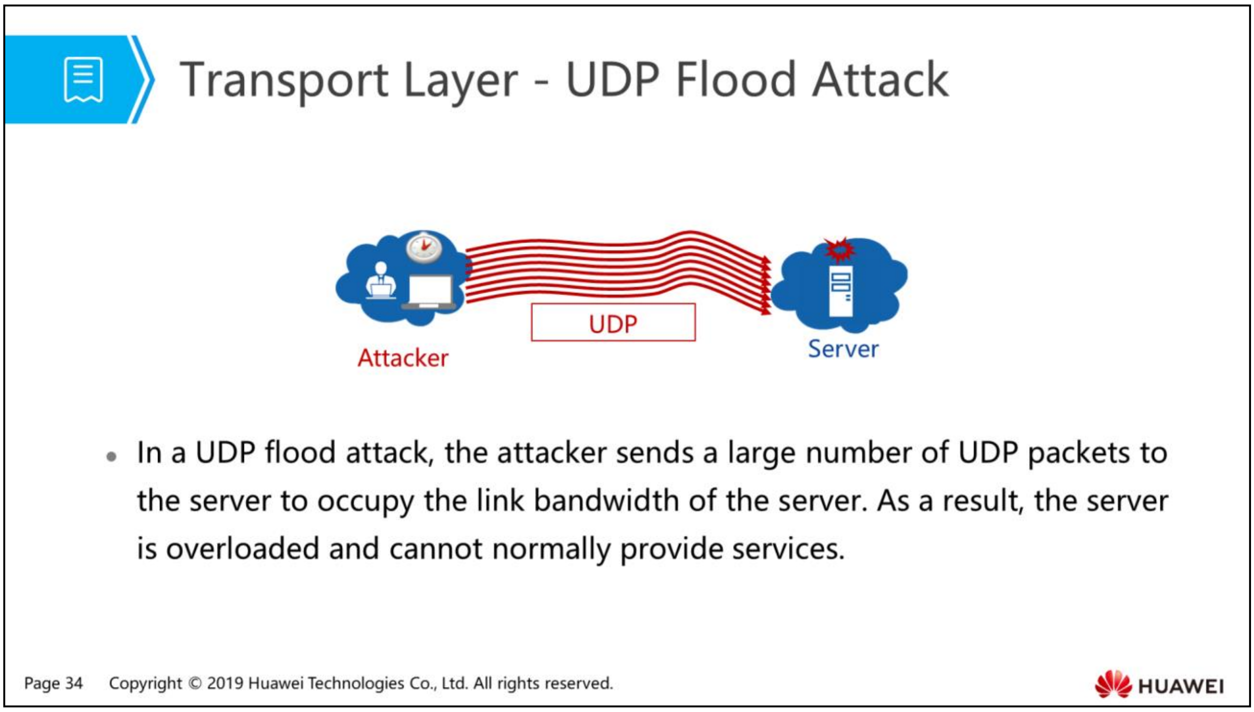
spoofed packet from C to A

ACK	seq	ack
1	11001	54003

spoofed packet from B to A

SYN	ACK	seq	ack
1	1	54002	11001

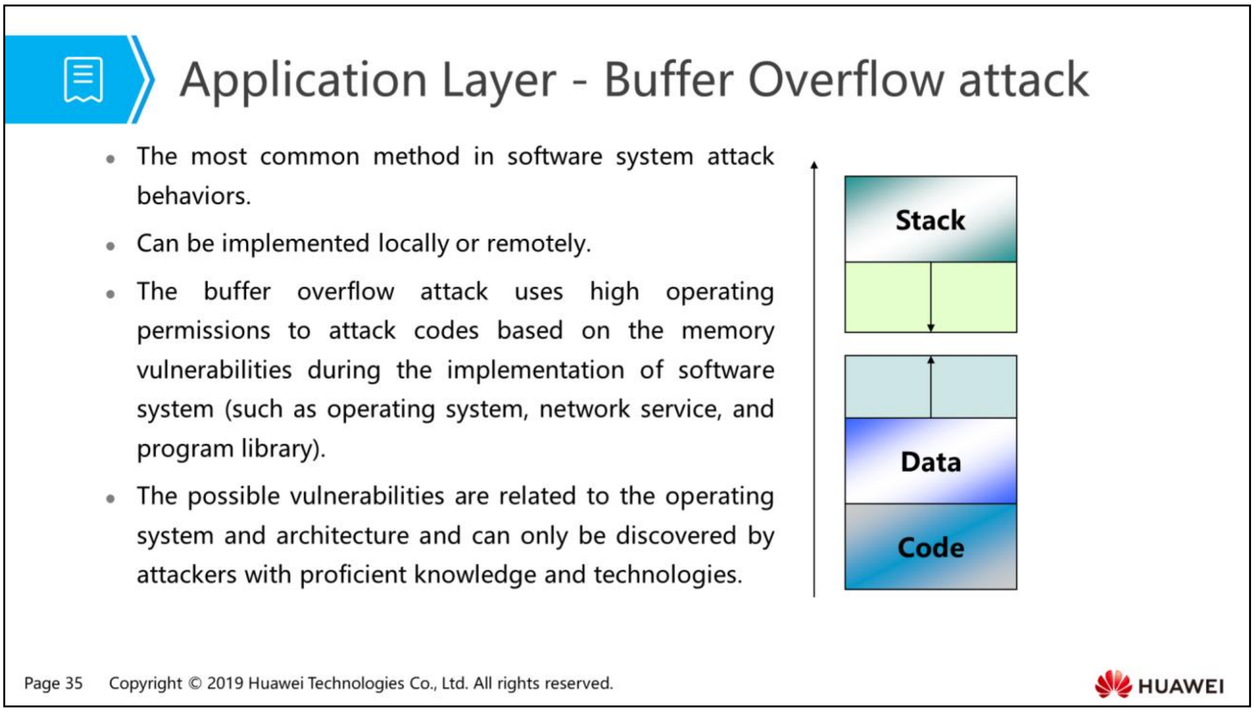
- TCP spoofing mostly occurs during TCP connection establishment. An attacker makes use of the trust relationships between two hosts to set up a fake TCP connection and simulates the target host to obtain information from the server. The process is similar to the IP spoofing.
- For example: A trusts B. C is an attacker and attempts to simulate B to set up a connection with A.
  - C damages B first, for example, using floogin, redirect, and crashing.
  - C uses B's address as the source address and sends TCP SYN packet to A.
  - A sends to B a TCP SYN/ACK packet with the sequence number S.
  - C cannot receive the sequence number. However, to achieve the handshake, C must respond with S+1 as the sequence number. At this time, C can use one of the following methods to obtain S:
    - C intercepts the SYN/ACK packet and obtains the sequence number.
    - C guesses the sequence number based on the OS features of host A.
  - After obtaining the sequence number S to respond to A, C can set up a fake connection with A.



Transport Layer - UDP Flood Attack

- In a UDP flood attack, the attacker sends a large number of UDP packets to the server to occupy the link bandwidth of the server. As a result, the server is overloaded and cannot normally provide services.

- Since UDP is connectionless, connection status detection becomes unavailable. By proactively collecting the statistics and learning UDP packets, the server can analyze the rules and features of UDP packets sent by a certain host. If a host sends a large number of identical, similar or regularly-changed UDP packets, the host is regarded as an attacker.
- The device implements UDP flood attack defense through the configuration of UDP packet rate limit.



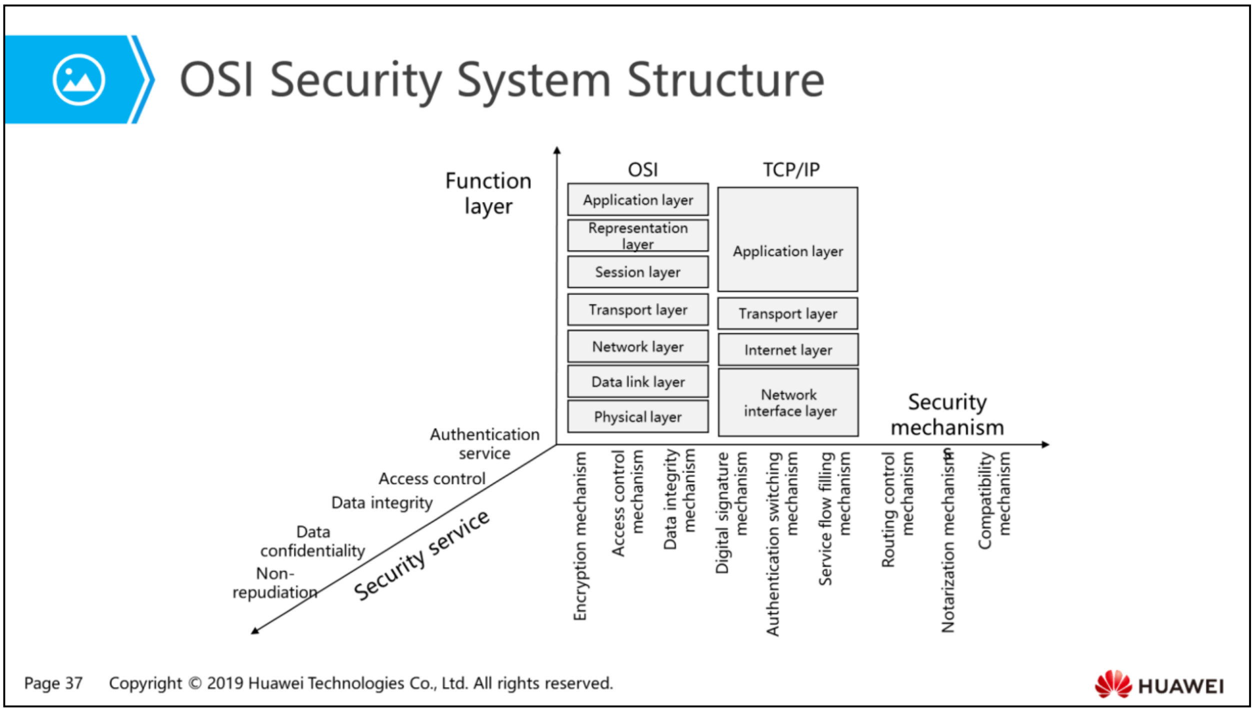
Application Layer - Buffer Overflow attack

- The most common method in software system attack behaviors.
- Can be implemented locally or remotely.
- The buffer overflow attack uses high operating permissions to attack codes based on the memory vulnerabilities during the implementation of software system (such as operating system, network service, and program library).
- The possible vulnerabilities are related to the operating system and architecture and can only be discovered by attackers with proficient knowledge and technologies.

- Buffer is the place where data is restored in memory. When a program tries to place the data within the machine memory, buffer overflow occurs if there is insufficient space. While man-made overflow is intentional. If the attacker writes a character string which is longer than the buffer length and put it in the buffer area, and then inputs an extra long character string in the buffer of a limited space, the following two results may occur: one is that the extra long character string overlaps the adjacent storing unit, causing the failure of program running or even system crash; the other one is that the attacker can use this vulnerability to execute any command or even obtain root permissions.

Contents

1. Why Do We Need Information Security?
2. What is Information Security?
3. How to Ensure Information Security?
4. **Network Security**
    - Why Is the Network Confronted with Security Issues?
    - What Security Risks Does the Network Face?
    - How to Resolve Network Security Issues?



OSI Security System Structure

Function layer

OSI

Application layer

Representation layer

Session layer

Transport layer

Network layer

Data link layer

Physical layer

TCP/IP

Application layer

Transport layer

Internet layer

Network interface layer

Security mechanism

Encryption mechanism

Access control mechanism

Data integrity mechanism

Digital signature mechanism

Authentication switching mechanism

Service flow filling mechanism

Routing control mechanism

Notarization mechanism

Compatibility mechanism

Security service

Authentication service

Access control

Data integrity

Data confidentiality

Non-repudiation

- To resolve the security issues on the network, Open System Interconnect (OSI) security architecture (international standard number: ISO 7498-2) proposes that the design of a secure information system infrastructure should contain five types of security services (security functions), eight security mechanisms and general security mechanisms to support the five types of security services, and five OSI security management modes. One security service can be provided by one or more security mechanisms and one security mechanism can provide one or more security services.
  - 5 security services are: authentication service, access control, data integrity, data confidentiality, and non-repudiation.
  - 8 security mechanisms are: encryption, digital signature, access control, data integrity, data exchange, service flow filling, routing, and authentication.
- Security service: indicates security safeguards provided by the computer network. International Organization for Standardization (ISO) defines several basic security services as follows: certification service, access control, data confidentiality, data integrity, and non-repudiation.
  - Certification service: is to validate the reliability of certain entity's identification, which can be divided into two types. One is called entity authentication, which is to validate the authenticity of an entity's ID. The ID of an entity that has been authenticated can connect to entity rights in the ACL to determine whether it has permission to access. Password authentication is the most common method of entity authentication. Another authentication is called data source authentication, which is used to prove whether certain information comes from a certain entity. Data signature serves as an example.
  - Access control: the objective of access control is to prevent unauthorized access to any source and to ensure that only authorized entities can access protected resources.

  - Data confidentiality service: is to ensure that only authorized entities can understand the protected resources, and it has two types of service in information security: data confidentiality service and traffic flow confidentiality service. Data confidentiality service mainly adopts encryption methods. Attackers can hardly presume any useful information even though they steal the encrypted data; traffic flow confidentiality service is to prevent eavesdroppers from presuming sensitive information through changes of the network traffic.

  - Data integrity service: is used to prevent unauthorized modification and damage of data. The service can prompt the message receiver to find whether the message is modified or replaced by a dummy message by an attacker.

  - Non-repudiation service: the service prevents the denial of data source and data submission according to ISO standard. It has two possibilities: the non-repudiation of data sending and the non-repudiation of data acceptance. Two services need complicated infrastructure's support, such as digital signature.

- Security mechanism is used to implement security service. It can be concrete, specific and universal. Main security mechanisms include: encryption, digital signature, access control, data integrity, authentication exchange, traffic filling, route control and notarization.

  - Encryption mechanism is used to protect data confidentiality. It depends on modern cryptology theory and its encryption/decryption algorithms are open generally. The security of encryption mainly depends on key security and strength. There are two types of encryption mechanism: symmetric one and asymmetric one.

  - Digital signature mechanism is an important method to protect data integrity and non-repudiation. It plays an increasingly important role in network application. It can be generated by specific digital signature mechanism or by a certain encryption mechanism.

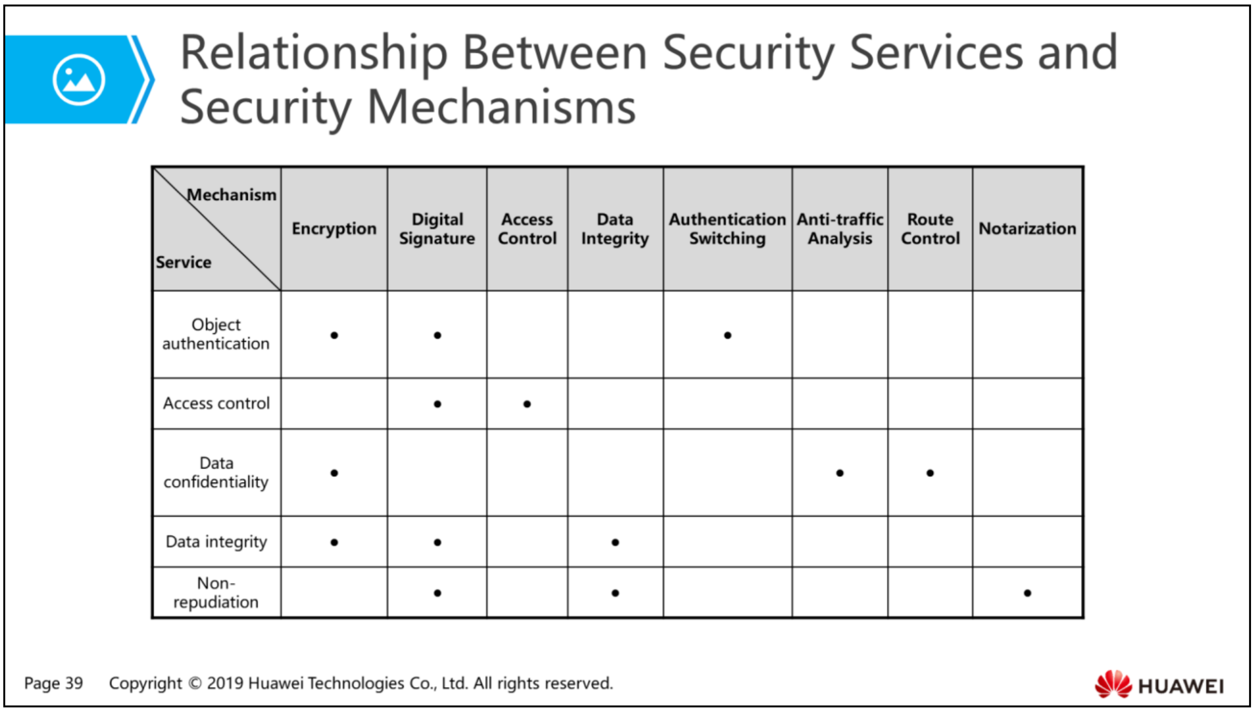
  - Access control mechanism is closely related to entity authentication. Firstly, access to a resource entity should pass the authentication, and then access control mechanism processes the entity access request to query that if the entity has the right to access the requested resource and respond to it.

  - Data integrity mechanism is used to protect data from unauthorized modification. The mechanism can use a unidirectional and irreversible function--hash function to calculate message digest and implement digital signature on the message digest.

  - Traffic filling mechanism is targeted at attacks that analyses network traffic. Sometimes the attacker deduces some useful information or clues according to traffic change between the two communication parties.

  - Routing control mechanism can specify the path of data across the network. In this way, we can choose a path on which the nodes are reliable, which ensures that the sent message will not be attacked due to passing insecure nodes.

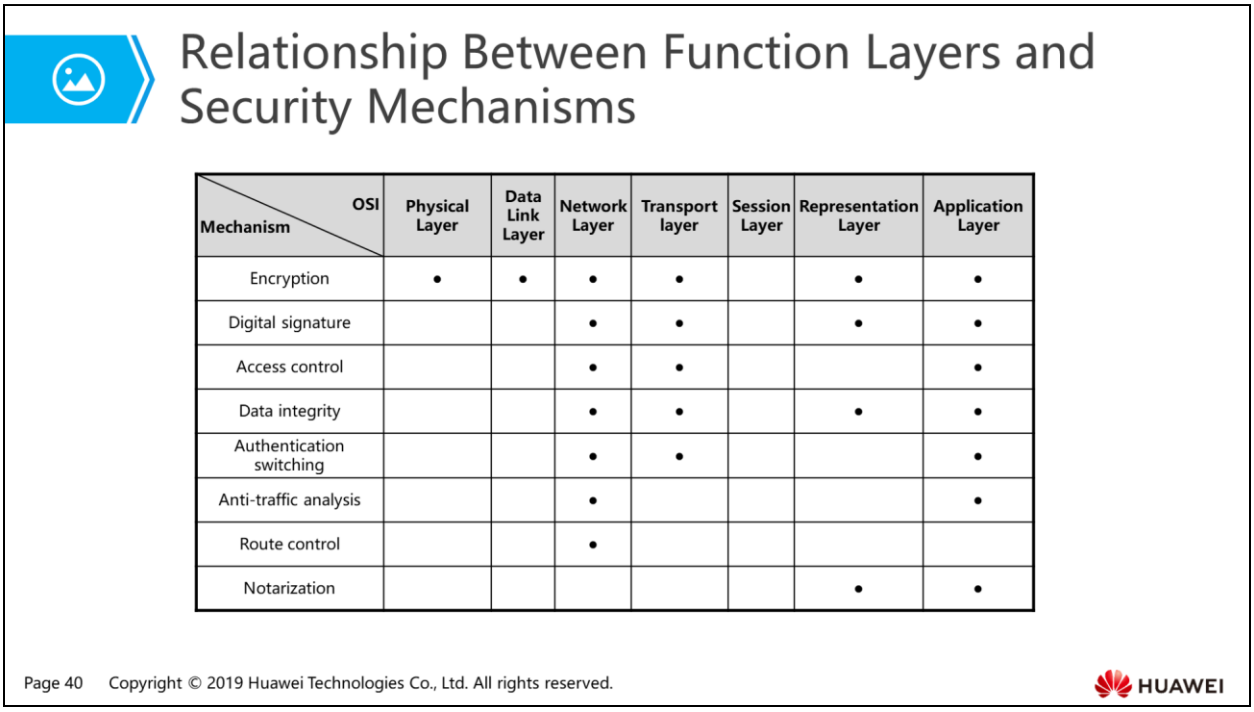
  - Notarization mechanism is provided by a third party, which is trusted by all communication parties. The third party ensures data integrity and the correctness of data source, time and destination.



Relationship Between Security Services and Security Mechanisms

Mechanism / Service	Encryption	Digital Signature	Access Control	Data Integrity	Authentication Switching	Anti-traffic Analysis	Route Control	Notarization
Object authentication	●	●			●			
Access control		●	●					
Data confidentiality	●					●	●	
Data integrity	●	●		●				
Non-repudiation		●		●				●

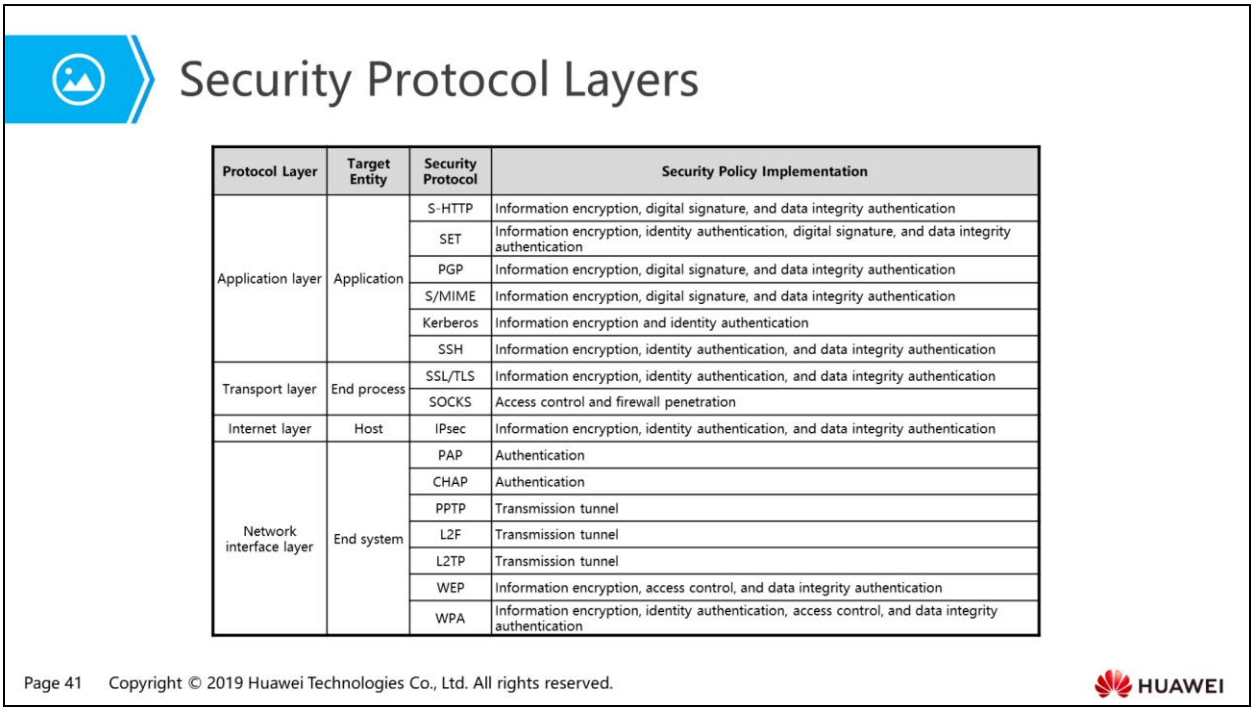
- As shown in the table, the provision of each service is sometimes considered appropriate by some mechanisms. It is provided by one mechanism or several mechanisms. The table shows a general relationship which is changeable.
- For example, object authentication service can be implemented by encryption, digital signature, and authentication switching mechanism; access control service can be implemented by digital signature and access control mechanism.



Relationship Between Function Layers and Security Mechanisms

OSI Mechanism	Physical Layer	Data Link Layer	Network Layer	Transport layer	Session Layer	Representation Layer	Application Layer
Encryption	●	●	●	●		●	●
Digital signature			●	●		●	●
Access control			●	●			●
Data integrity			●	●		●	●
Authentication switching			●	●			●
Anti-traffic analysis			●				●
Route control			●				
Notarization						●	●

- As shown in the table, each layer of the reference model can provide certain types of security service. A certain type of security service is provided by a specific layer. The security service is supported by the security mechanism on this layer unless otherwise specified. Several layers can provide specific security services. These security services are not always provided by such layers but can be offered by lower layers. Even though a layer does not provide security services, the definition of services on this layer requires modification in order to send the request of security services to lower layers.
- For example, security services that can be provided by the network layer includes encryption, digital signature, access control, data integrity, authentication switching, anti-traffic analysis and route control.



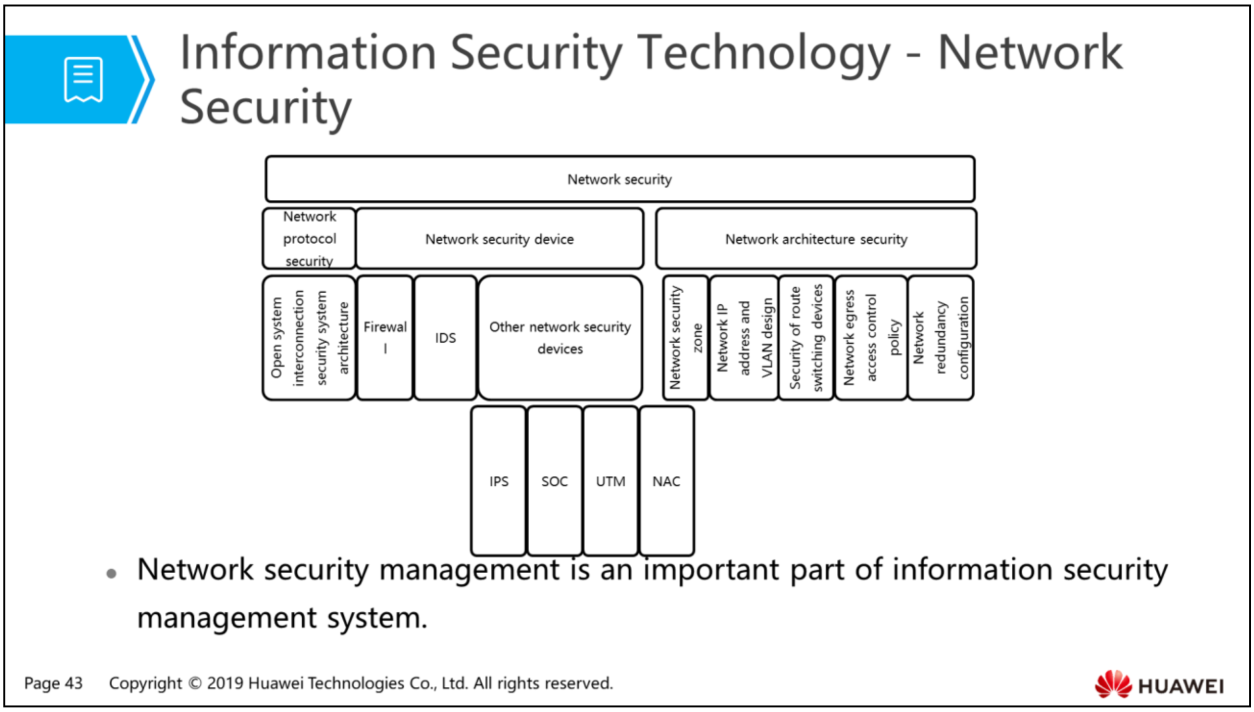
Security Protocol Layers

Protocol Layer	Target Entity	Security Protocol	Security Policy Implementation
Application layer	Application	S-HTTP	Information encryption, digital signature, and data integrity authentication
		SET	Information encryption, identity authentication, digital signature, and data integrity authentication
		PGP	Information encryption, digital signature, and data integrity authentication
		S/MIME	Information encryption, digital signature, and data integrity authentication
		Kerberos	Information encryption and identity authentication
		SSH	Information encryption, identity authentication, and data integrity authentication
Transport layer	End process	SSL/TLS	Information encryption, identity authentication, and data integrity authentication
		SOCKS	Access control and firewall penetration
Internet layer	Host	IPsec	Information encryption, identity authentication, and data integrity authentication
Network interface layer	End system	PAP	Authentication
		CHAP	Authentication
		PPTP	Transmission tunnel
		L2F	Transmission tunnel
		L2TP	Transmission tunnel
		WEP	Information encryption, access control, and data integrity authentication
		WPA	Information encryption, identity authentication, access control, and data integrity authentication

Page 41

- Now we have learned about how to ensure network security with an emphasis on the security principles; next we will introduce some specific security protocols on each layer of TCP/IP stack to implement our network security ideas or policies. Only after these security devices that can implement these security protocols are deployed and configured on the network can we implement these security policies.
- As shown in the table, there are end-to-end security protocols on the network interface layer, such as PAP (the security policy for identity authentication), PPTP (the security policy for transmission tunnels); there are security protocols between hosts on the Internet layer, such as IPSec (can implement information encryption, identity authentication and data integrity verification security policy). The others follow the same rule. Security protocols and policies of each layer are as follows:
- Network interface layer:
  - Password Authentication Protocol (PAP)
  - Challenge Handshake Authentication Protocol (CHAP)
  - Point-to-Point Tunneling Protocol (PPTP)
  - Level 2 Forwarding protocol (L2F)
  - Layer 2 Tunneling Protocol (L2TP)
  - Wired Equivalent Privacy (WEP)
  - Wi-Fi Protected Access (WPA)

- Internet layer:
  - IP Security (IPsec)
- Transport layer:
  - Secure Socket Layer (SSL)
  - Transport Layer Security (TLS)
  - Protocol for session traversal across firewall securely (SOCKS)
- Application layer:
  - Secure Shell Protocol (SSH)
  - Kerberos
  - Pretty Good Privacy (PGP)
  - Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - Secure Hyper Text Transfer Protocol (S-HTTP)
  - Secure Electronic Transaction (SET)

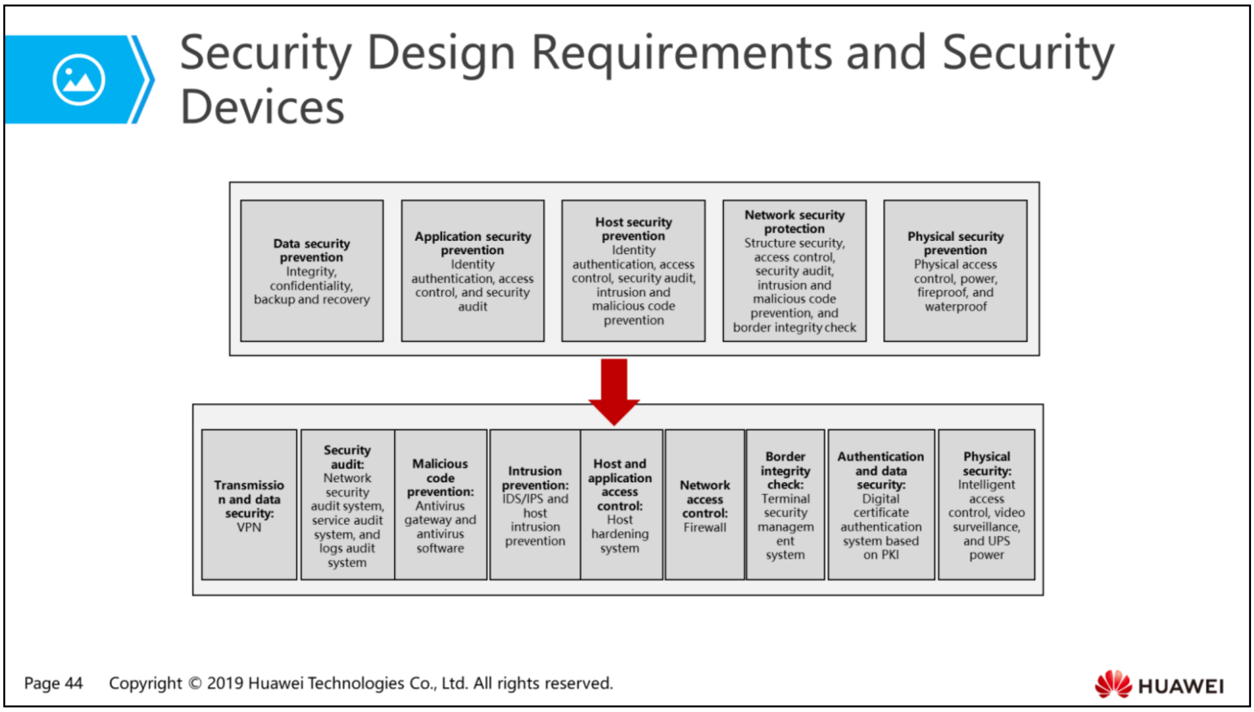


Information Security Technology - Network Security

- Network security
  - Network protocol security
    - Open system interconnection security system architecture
  - Network security device
    - Firewall
    - IDS
    - Other network security devices
      - IPS
      - SOC
      - UTM
      - NAC
  - Network architecture security
    - Network security zone
    - Network IP address and VLAN design
    - Security of route switching devices
    - Network egress access control policy
    - Network redundancy configuration

- Network security management is an important part of information security management system.

- The assurance of network security plays an important role in the information security management. It is generally acknowledged that network security only means to add a firewall device in the network structure, which is far from enough. The figure indicates that, apart from firewalls, other security devices or control measures such as intrusion detection system (IDS), access control solution and network redundancy configuration are required to safeguard network security.



Security Design Requirements and Security Devices

Data security prevention Integrity, confidentiality, backup and recovery

Application security prevention Identity authentication, access control, and security audit

Host security prevention Identity authentication, access control, security audit, intrusion and malicious code prevention

Network security protection Structure security, access control, security audit, intrusion and malicious code prevention, and border integrity check

Physical security prevention Physical access control, power, fireproof, and waterproof

Transmission and data security: VPN

Security audit: Network security audit system, service audit system, and logs audit system

Malicious code prevention: Antivirus gateway and antivirus software

Intrusion prevention: IDS/IPS and host intrusion prevention

Host and application access control: Host hardening system

Network access control: Firewall

Border integrity check: Terminal security management system

Authentication and data security: Digital certificate authentication system based on PKI

Physical security: Intelligent access control, video surveillance, and UPS power

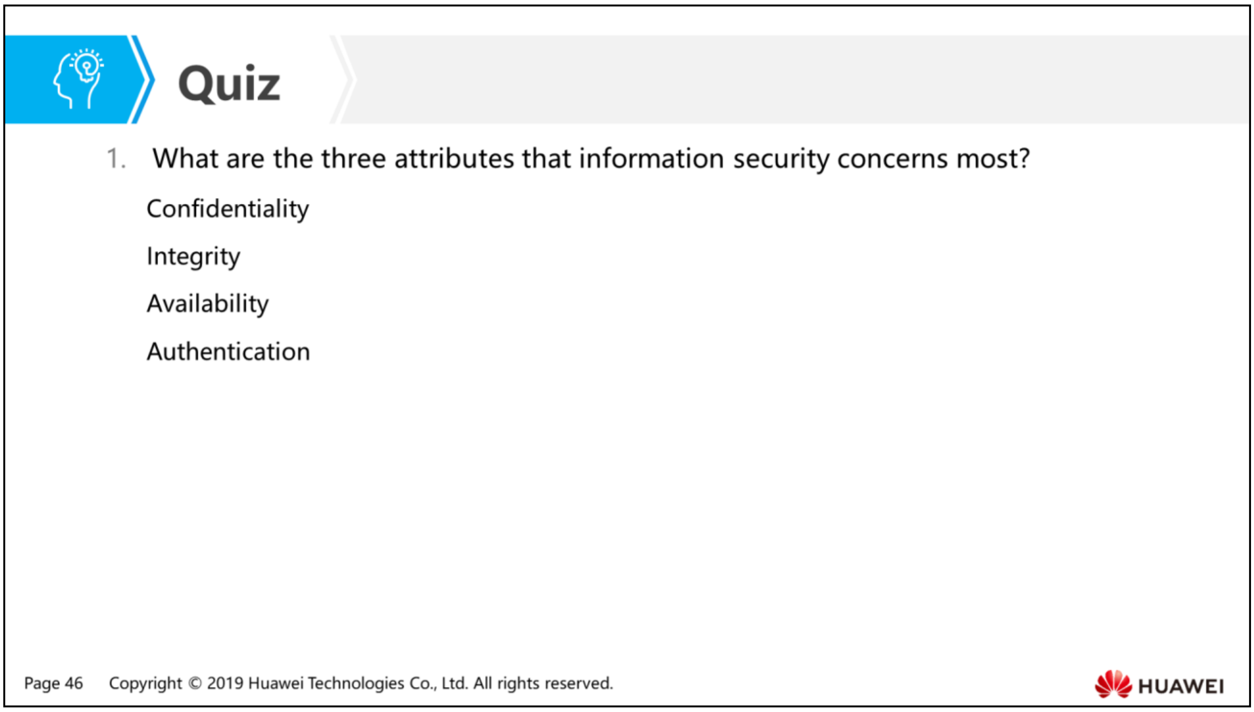
Page 44

HUAWEI

- As mentioned above, only after security devices that can implement security protocols are deployed and configured on the network can we implement these security policies. How to deploy the devices?
- To make the security design of information system, define the security demands of the system at first, make comprehensive analysis on the architecture and carried services of the information system, determine the system security risks and protection requirements, balance the relationship among security, cost and efficiency, and determine the security protection measures. With the development of the information system and services, the security assurance system should be continuously improved.
  - Physical security: includes the selection of physical location, physical access control, anti-theft, fire-proof, water-proof, lightning protection, temperature and humidity control, power supply, anti-static and electromagnetic shielding. For example, important zones should be equipped with an electronic access control system and the equipment room should be equipped with the anti-theft alarm system and automatic fire-fighting system.
  - Network security: includes structure security, security auditing, access control, border integrity check, malicious code protection, intrusion prevention and network device protection.
  - Host security: includes identity authentication, access control, security auditing, intrusion prevention, malicious code protection and resource control.
  - The application security: includes identity authentication, access control, security auditing, communication integrity and confidentiality, anti-repudiation, software fault-tolerance and resource control.

    - Data security: includes data integrity and confidentiality, data backup and recovery.

- The following security devices can be deployed:
    - The border isolation devices such as firewalls can be installed on the network exit, server area and other important network segment to logically isolate the network border or areas and implement access control for the network layer.
    - Deploy anti-virus gateway on the network border and the network anti-virus system on the server and terminals.
    - The intrusion detection system (IDS) or intrusion prevention system (IPS) can be installed on key network points to monitor and analyze network data flow or network behaviors in real time. After detecting malicious or suspicious behaviors, the system provides prompt alarms and responses.
    - The comprehensive security auditing system can be deployed to perform the function of network security auditing, service auditing and log auditing.
    - The terminal security management system or host monitoring and auditing system can implement the border integrity check and terminal security management.
- In addition, other optional security deployment according to system service characteristics and security requirements include:
    - Deploy VPN gateway to ensure data integrity and confidentiality during transmission.
    - Deploy vulnerability scanning system to scan vulnerabilities of all devices that support TCP/IP protocols and fix vulnerabilities in operating systems and application systems through patch distribution system.
    - Deploy application layer firewall or website anti-tampering system on systems that provide public services through website to protect WEB server.



Quiz

1. What are the three attributes that information security concerns most?

Confidentiality

Integrity

Availability

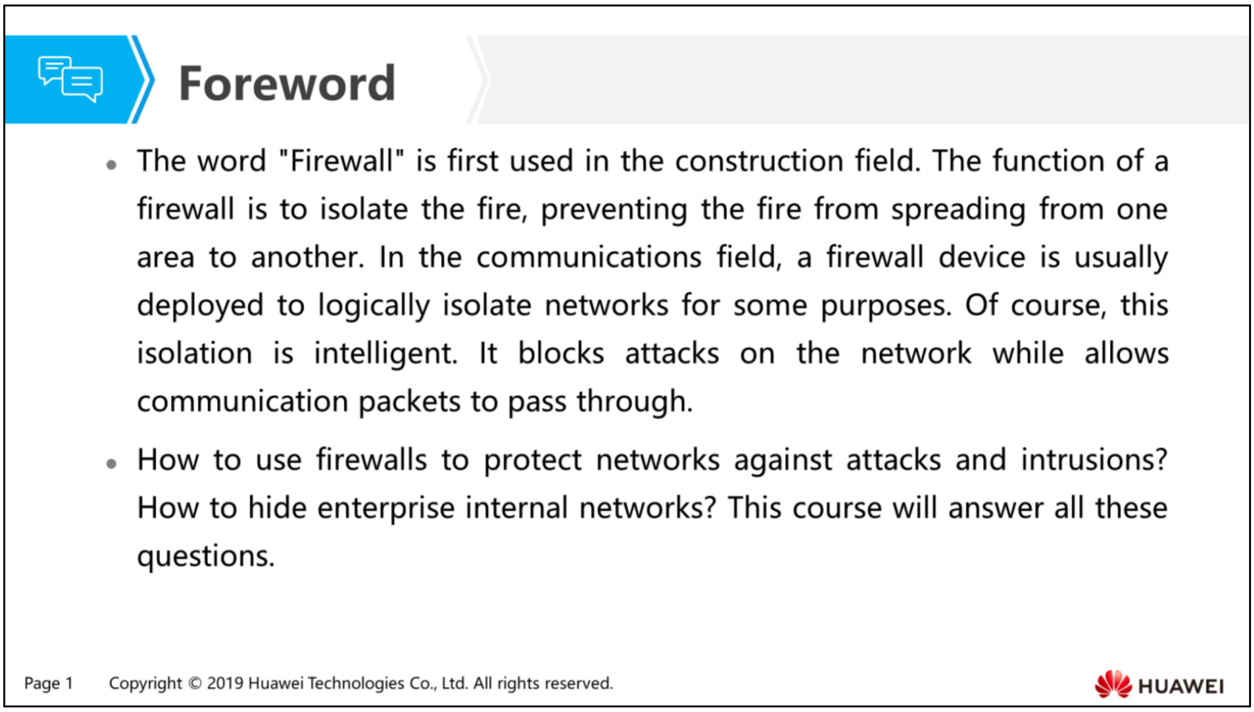
Authentication

- Answer: ABC.

Thank You

www.huawei.com

Huawei Firewall Technology Basis



Foreword

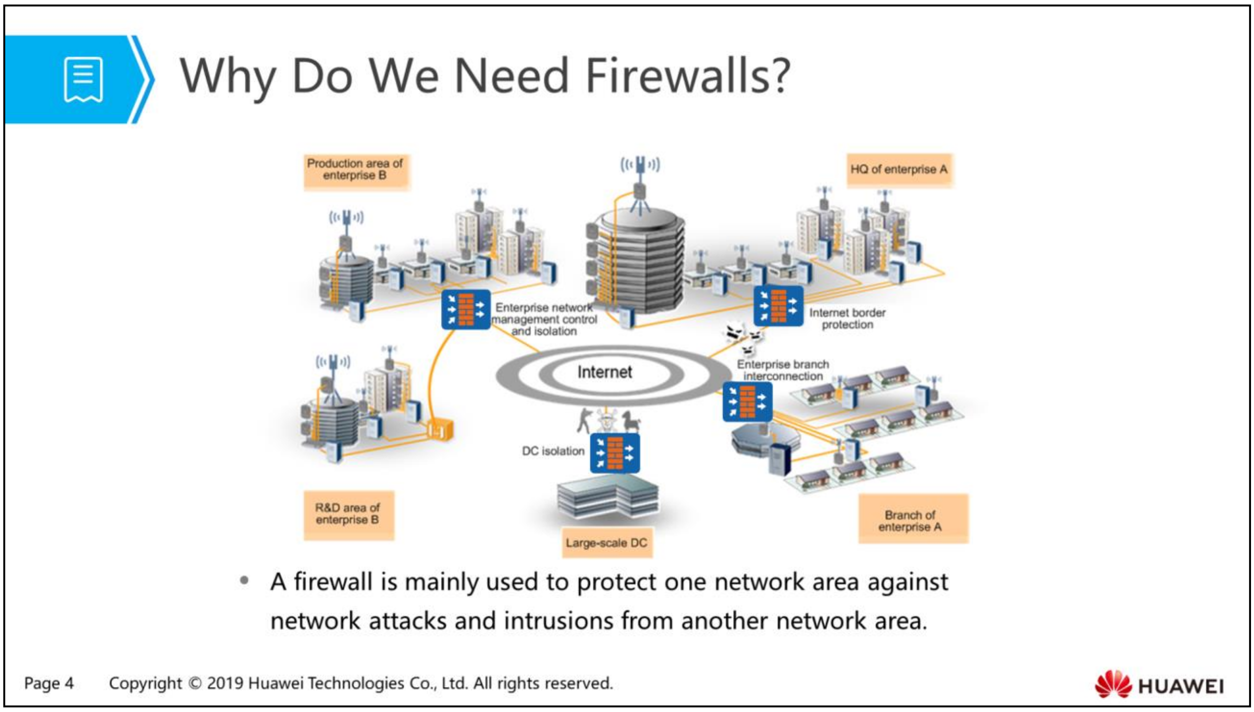
- The word "Firewall" is first used in the construction field. The function of a firewall is to isolate the fire, preventing the fire from spreading from one area to another. In the communications field, a firewall device is usually deployed to logically isolate networks for some purposes. Of course, this isolation is intelligent. It blocks attacks on the network while allows communication packets to pass through.
- How to use firewalls to protect networks against attacks and intrusions? How to hide enterprise internal networks? This course will answer all these questions.

Objectives

- Upon completion of this section, you will be able to:
  - Master firewall basic knowledge and security policy configuration
  - Master NAT principle and configuration
  - Understand attack defense principle and configuration

Contents

1. **Firewall Basic Knowledge**
   - Why Do We Need Firewalls?
   - Firewall Development History
   - Huawei Firewall Products
   - Security Zone
   - Security Policy
2. NAT
3. Attack Defense

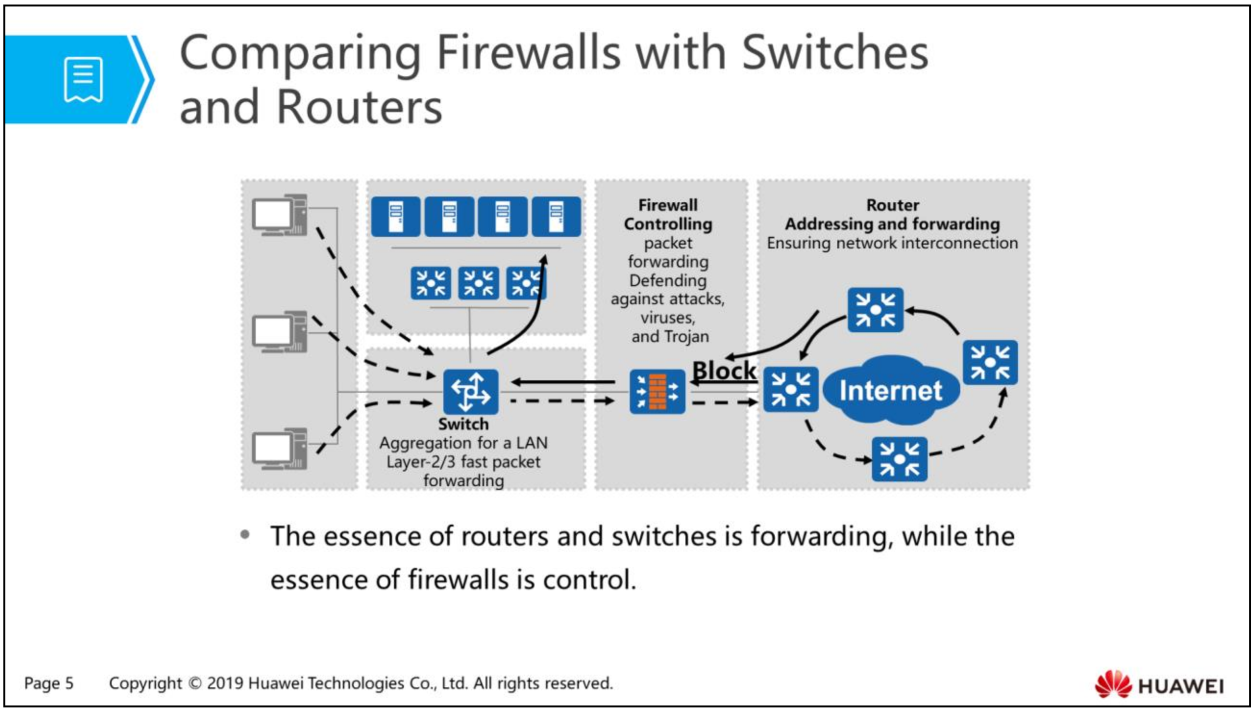


Why Do We Need Firewalls?

Production area of enterprise B
HQ of enterprise A
Enterprise network management control and isolation
Internet border protection
Internet
Enterprise branch interconnection
DC isolation
R&D area of enterprise B
Large-scale DC
Branch of enterprise A

- A firewall is mainly used to protect one network area against network attacks and intrusions from another network area.

- The word "Firewall" is first used in the construction field. The function of a firewall is to isolate the fire, preventing the fire from spreading from one area to another. In the communications field, a firewall device is usually deployed to logically isolate networks for some purposes. Of course, this isolation is intelligent. It blocks attacks on the network while allows communication packets to pass through.
- A firewall is mainly used to protect one network area against network attacks and intrusions from another network area. Thanks to its isolation and defense nature, the firewall can be flexibly deployed at a network border or between two subnets, such as the egress of an enterprise network or the border of a DC.



Comparing Firewalls with Switches and Routers

Firewall
Controlling packet forwarding
Defending against attacks, viruses, and Trojan

Router
Addressing and forwarding
Ensuring network interconnection

Block

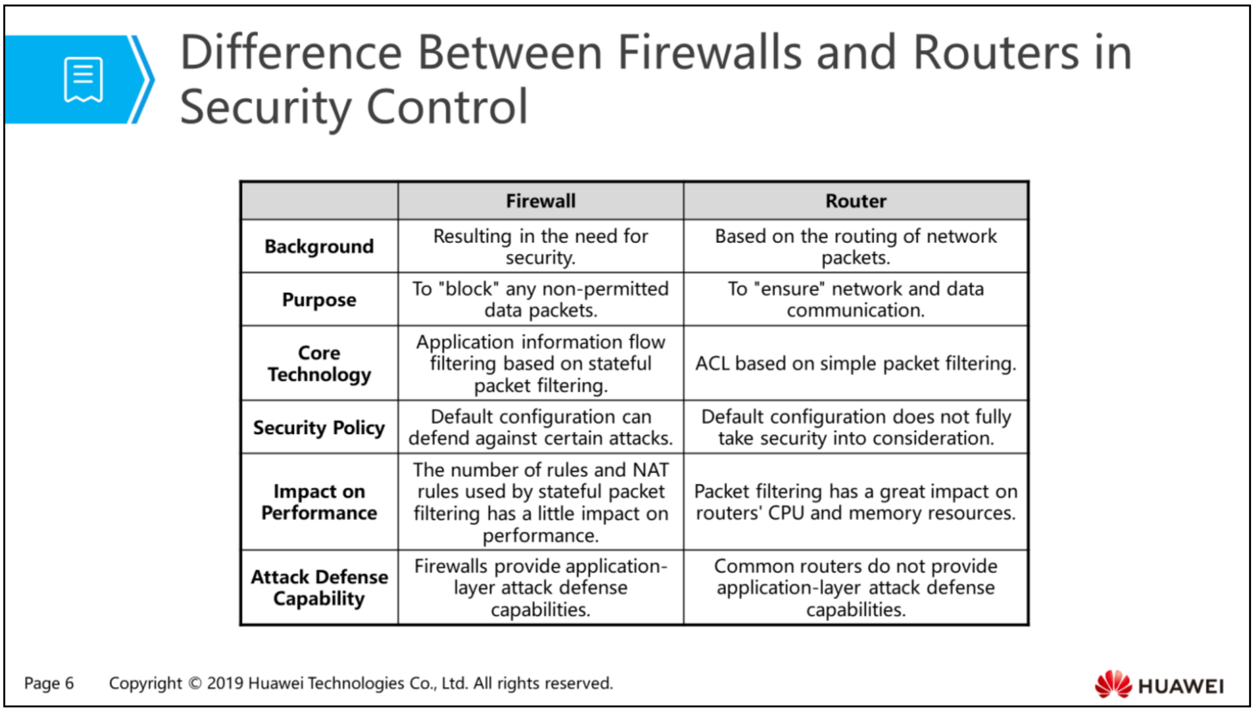
Internet

Switch
Aggregation for a LAN
Layer-2/3 fast packet forwarding

- The essence of routers and switches is forwarding, while the essence of firewalls is control.

HUAWEI

- Firewalls are different from routers and switches. Routers interconnect networks and use routing protocols for interconnection and forward packets to destinations. Switches are usually used to build LANs. As important hubs for LAN communications, switches use Layer 2/3 switching to rapidly forward packets. Firewalls are mainly deployed on network borders to control incoming and outgoing packets. That is, security protection is the core feature of firewalls. The essence of routers and switches is forwarding, while the essence of firewalls is control.
- Currently, there is a trend for mid-range and low-end routers and firewalls to integrate for function complementary. Huawei has released a series of such all-in-one devices.



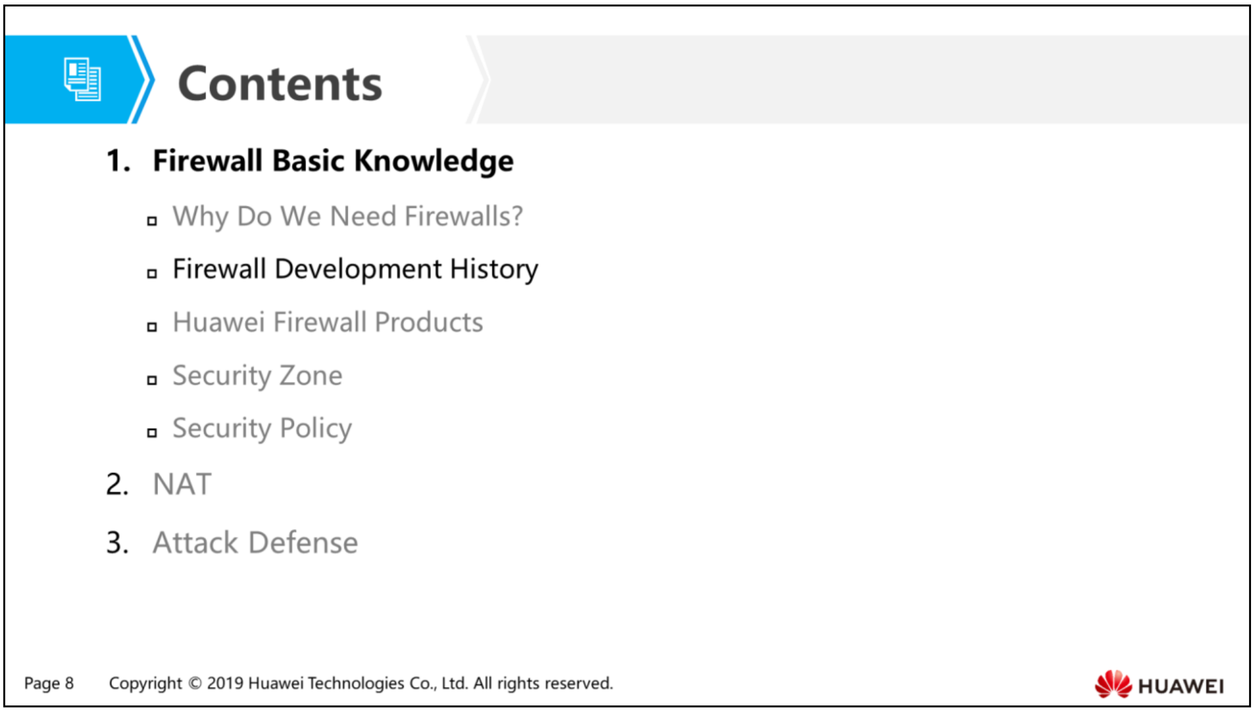
Difference Between Firewalls and Routers in Security Control

	Firewall	Router
Background	Resulting in the need for security.	Based on the routing of network packets.
Purpose	To "block" any non-permitted data packets.	To "ensure" network and data communication.
Core Technology	Application information flow filtering based on stateful packet filtering.	ACL based on simple packet filtering.
Security Policy	Default configuration can defend against certain attacks.	Default configuration does not fully take security into consideration.
Impact on Performance	The number of rules and NAT rules used by stateful packet filtering has a little impact on performance.	Packet filtering has a great impact on routers' CPU and memory resources.
Attack Defense Capability	Firewalls provide application-layer attack defense capabilities.	Common routers do not provide application-layer attack defense capabilities.

- Currently, most routers (at both consumer and enterprise levels) on the market provide simple firewall functions, such as packet filtering and IP address filtering. Why do we still need hardware firewalls? Differences between firewalls and routers are as follows:
- Background:
  - Routers are designed for the routing of network data packets. Routers take charge of route management for data packets in different network segments. The concern of routers is the routing of data packets in different network segments for communication.
  - Firewalls are designed to meet the need for security. Whether data packets can correctly reach destinations, when they arrive, and where they go are not major concerns of firewalls. Instead, their concerns are whether a data packet can pass through and what damage the packet may bring to the network.
- Objective:
  - The purpose of routers is to interconnect networks and exchange data.
  - The purpose of firewalls is to block any non-permitted data packets.
- Core Technology: The core ACL of routers is based on simple packet filtering, belonging to OSI Layer 3 filtering. Technically speaking, firewalls filter application information based on stateful packet filtering.
- Security Policy:
  - The default configuration of routers does not fully take security into consideration. Advanced configuration is required for attack defense. As security rules designed for routers are complicated, there is a high probability of configuration errors.

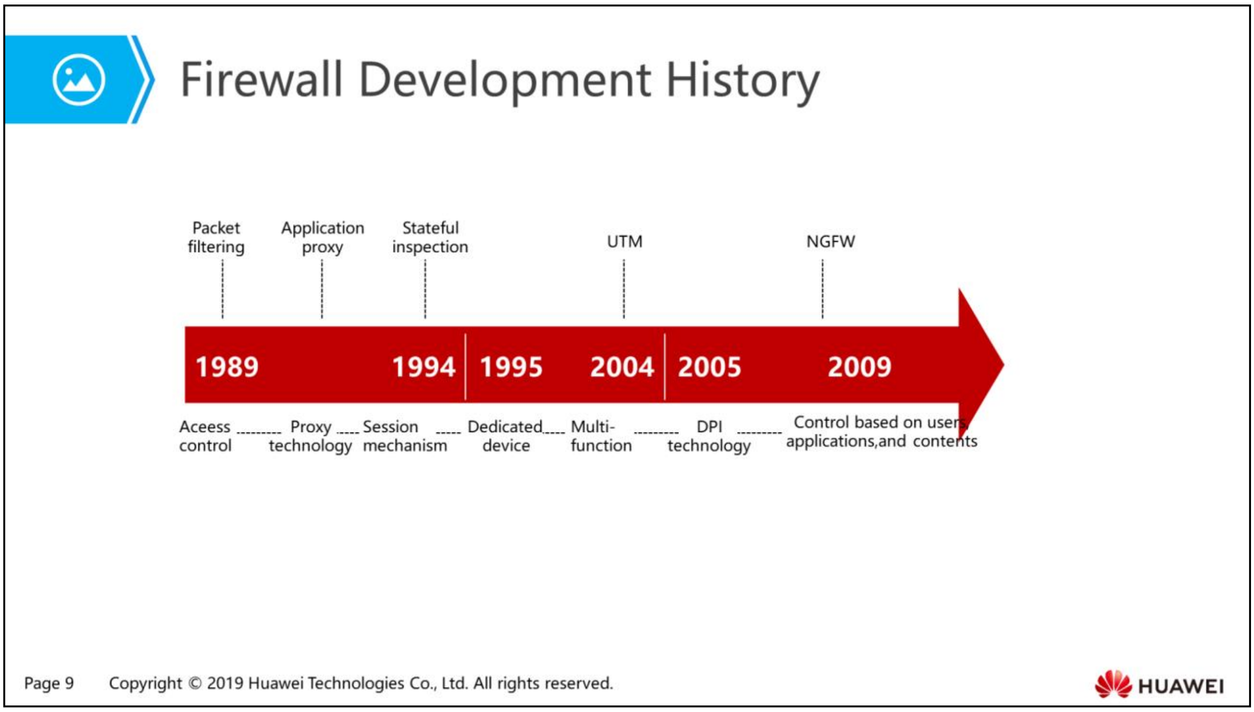
    - The default configuration of certain firewalls can defend against various attacks. More human-friendly firewalls provide graphical UIs to simplify configuration and reduce configuration error rate.

- Impact on Performance:
    - Routers are designed to forward data packets, not to act as a full-feature firewall. Therefore, the computation amount is very large during data forwarding. Packet filtering will exert great impact on routers' CPU and memory usage. That is why data forwarding rate decreases after the firewall function is enabled on routers. As router hardware costs are high, their high-performance hardware is costly.
    - Firewalls are not designed to forward data. Instead, they are designed to check whether packets meet requirements. If yes, they allow the packets to pass. Otherwise, they reject the packets. Firewall software is optimized for data packet filtering, and major modules are running in the kernel mode of the operating system. The design is taken security into consideration to offer very high data packet filtering performance.
    - As routers deliver simple packet filtering, adding packet filtering rules or NAT rules increases the burden on router performance. While firewalls use stateful packet filtering, adding rules increases little burden on performance.
- Attack Defense Capability:
    - Generally, ordinary routers cannot defend against application-layer attacks or detect intrusions in real time. To obtain such functions, router system software must be upgraded. In addition to the software upgrade, the hardware may need to be upgraded to afford increasing computation workloads.
- Therefore, a root condition for whether to use firewalls is to the requirements for network security, not whether the network topology is simple or complex or whether applications are easy or difficult to use. Even if the network topology and applications are simple, it is necessary to use firewalls. If the environment and applications are complicated, using firewalls can bring more benefits. For most networks, routers are the first gate, and firewalls are the second and also the most strict one.



Contents

1. **Firewall Basic Knowledge**
   - Why Do We Need Firewalls?
   - Firewall Development History
   - Huawei Firewall Products
   - Security Zone
   - Security Policy
2. NAT
3. Attack Defense



Firewall Development History

Packet filtering

Application proxy

Stateful inspection

UTM

NGFW

1989

1994

1995

2004

2005

2009

Aceess control

Proxy technology

Session mechanism

Dedicated device

Multi-function

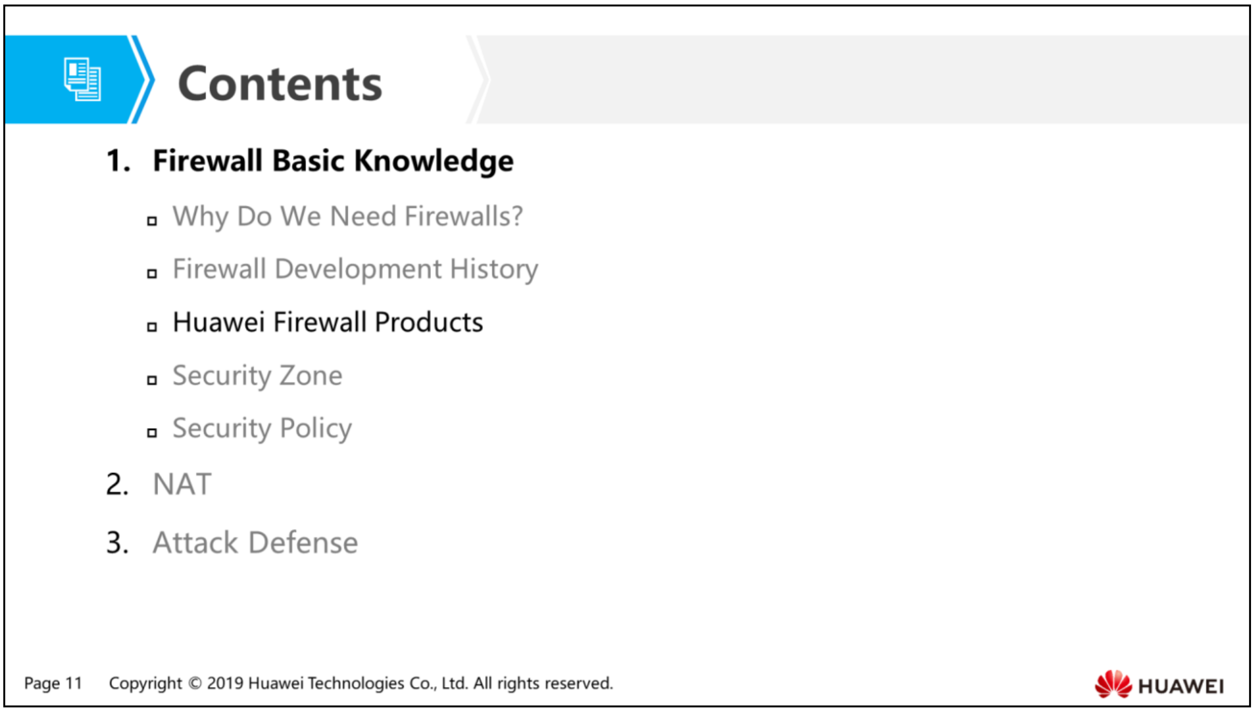
DPI technology

Control based on users applications,and contents

- The earliest firewall can be traced back to the late 80s of last century. In the two decades, firewall development can be divided into the following phases:
  - 1989-1994:
    - The packet filtering firewall was generated in 1989 for simple access control, which is called the first-generation firewall.
    - Then, the proxy firewall appeared, which acted as a proxy for communication between the intranet and extranet at the application layer. The proxy firewall belongs to the second-generation firewall. The proxy firewall is high in security but low in processing, and it is difficult to develop a proxy service for each type of application. Therefore, it provides proxy only for a few applications.
    - In 1994, the industry released the first stateful inspection firewall, which determined the action to be taken by dynamically analyzing packet status. As it does not need to proxy each application, its processing speeds up and is of high security. The stateful inspection firewall is called the third-generation firewall.
  - 1995-2004:
    - In this period, stateful inspection firewalls have become a trend. In addition to access control, firewalls have other functions, such as VPN.
    - Meanwhile, special devices started to appear, for example, Web Application Firewalls (WAFs) that protect web servers.

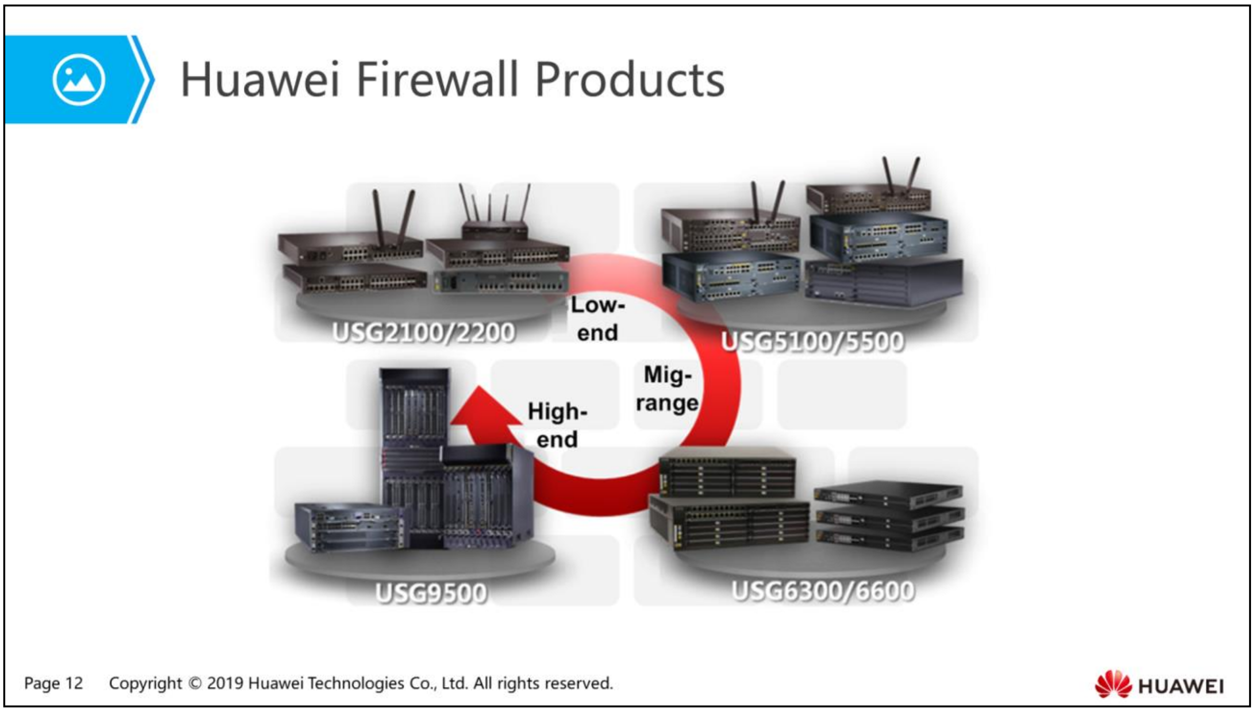
    - In 2004, the industry proposed the concept of United Threat Management (UTM). That is, integrating the conventional firewall, intrusion detection, antivirus, URL filtering, application control, and mail control into one firewall for all-round security protection.

- 2005- :
    - Since 2004, the UTM market has rapidly developed. UTM products merged one after another, but they are faced with new challenges. First, the detection degree on application-layer information is limited. More advanced detection means are required. Therefore, the Deep Packet Inspection (DPI) technology is widely used. Second, firewall performance is greatly challenged. Concurrent running of multiple functions greatly deteriorates the processing performance of UTM devices.
    - In 2008, next-generation firewalls (NGFWs) were released in the industry to resolve the performance deterioration problem. Furthermore, NGFWs can manage traffic based on users, applications, and content.
    - In 2009, the industry defines NGFWs to clarify the functions that NGFWs should have. Then, security vendors released their NGFWs. Firewalls have entered a new era.



Contents

1. **Firewall Basic Knowledge**
   - Why Do We Need Firewalls?
   - Firewall Development History
   - Huawei Firewall Products
   - Security Zone
   - Security Policy
2. NAT
3. Attack Defense

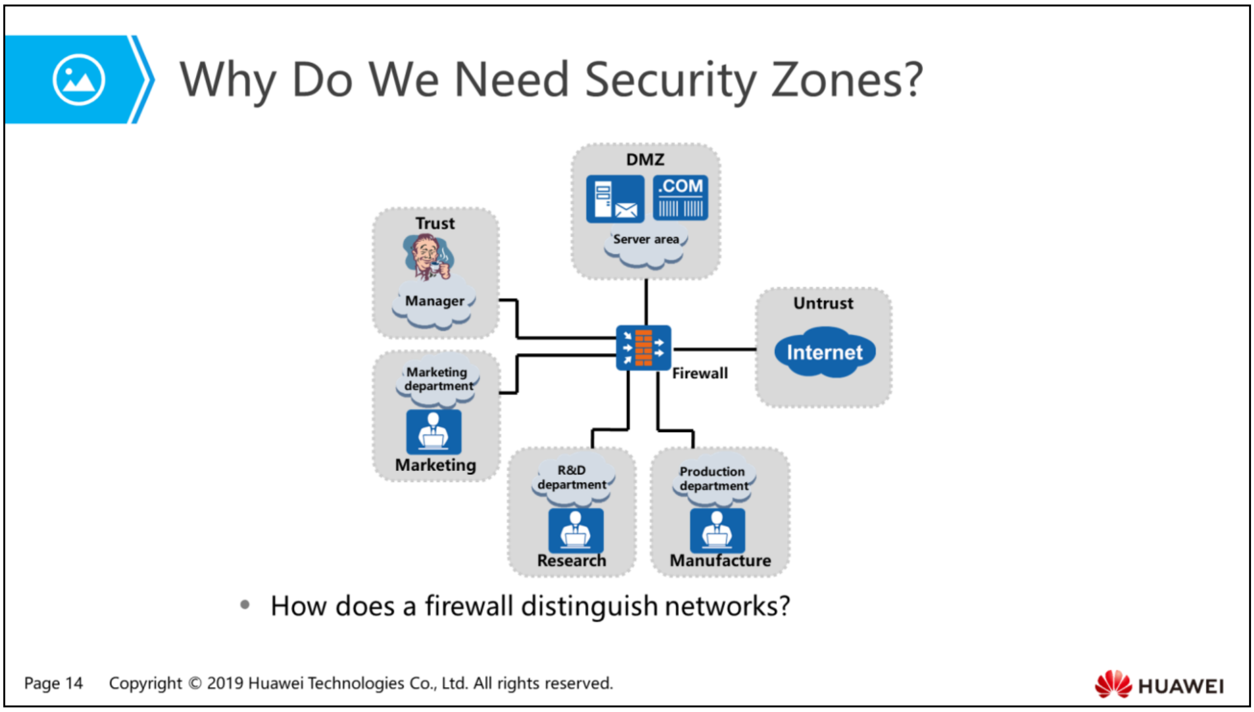


Huawei Firewall Products

- Huawei firewall products include the USG2000, USG5000, USG6000, and USG9500 series, covering low-end, mid-range, and high-end models with various functions, meeting security requirements of different network environments. Among them, the USG2000 and USG5000 series are UTM products, the USG6000 series are NGFWs, and the USG9500 series are high-end firewalls.
- The USG2100 has the firewall, UTM, VPN, routing, and wireless (Wi-Fi/3G) functions integrated. It is plug-and-play and easy to configure, able to provide a secure, flexible, and convenient integrated networking and access solution.
- As firewall products facing next-generation network environments, the USG6000 series provides application-layer-centric next-generation network security, allowing network administrators to control networks in a more clear, refined, and easy way. The USG6000 series provides accurate application access control, identification of over 6000 applications, multiple user authentication techniques, comprehensive unknown threat defense, simple security management, and high full-service performance.
- The USG9500 series is the first terabit-level DC firewall in the industry. It has passed the test of NSS Labs, a US-based authoritative third-party security evaluation agency in the industry. It adopts distributed hardware and software design, provides industry-leading security technologies, and integrates switching, routing, and security services. It is widely applied in large-scale DC, education, government networks.

Contents

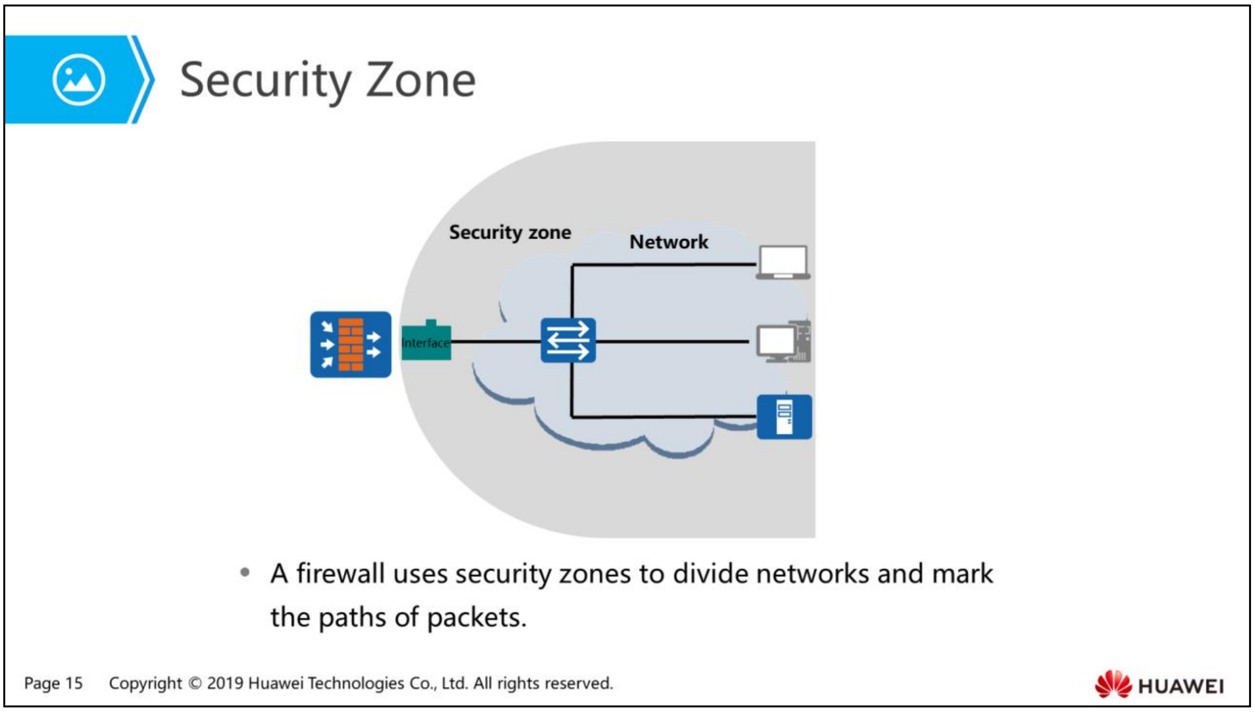
1. **Firewall Basic Knowledge**
   - Why Do We Need Firewalls?
   - Firewall Development History
   - Huawei Firewall Products
   - Security Zone
   - Security Policy
2. NAT
3. Attack Defense



Why Do We Need Security Zones?

- How does a firewall distinguish networks?

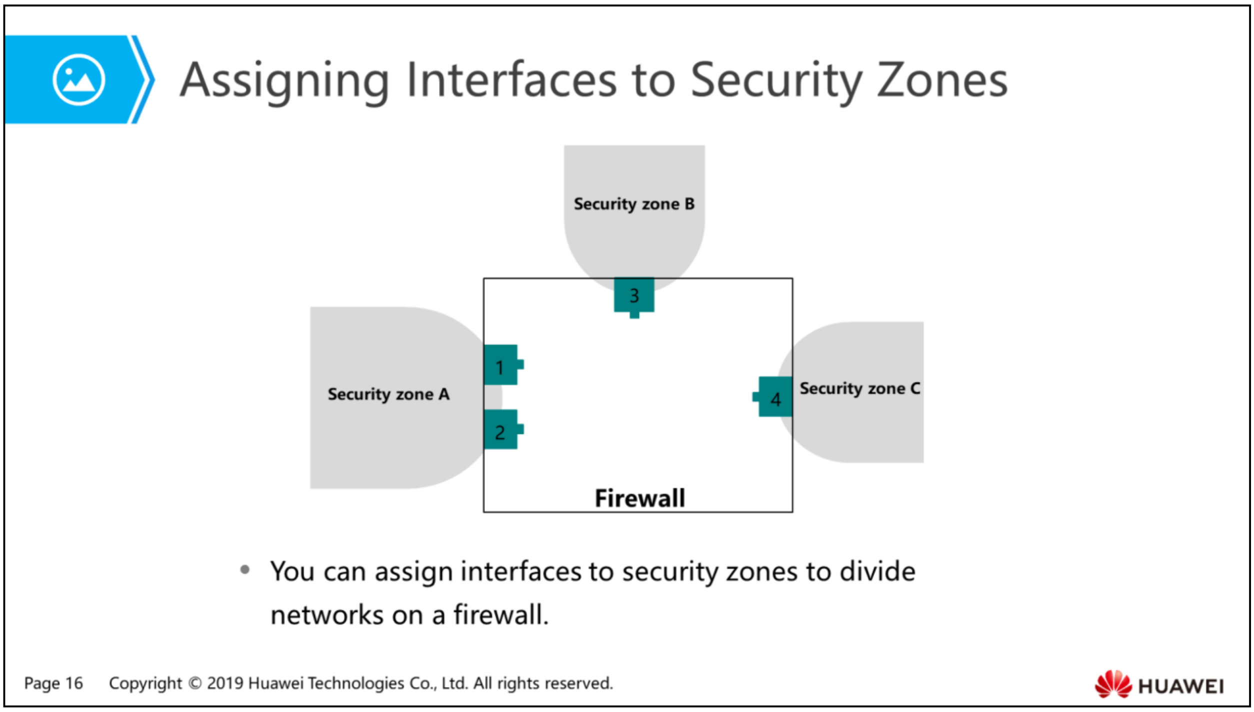
- A firewall is deployed on the network border for isolation. Well, how does the firewall distinguish networks?



Security Zone

- A firewall uses security zones to divide networks and mark the paths of packets.

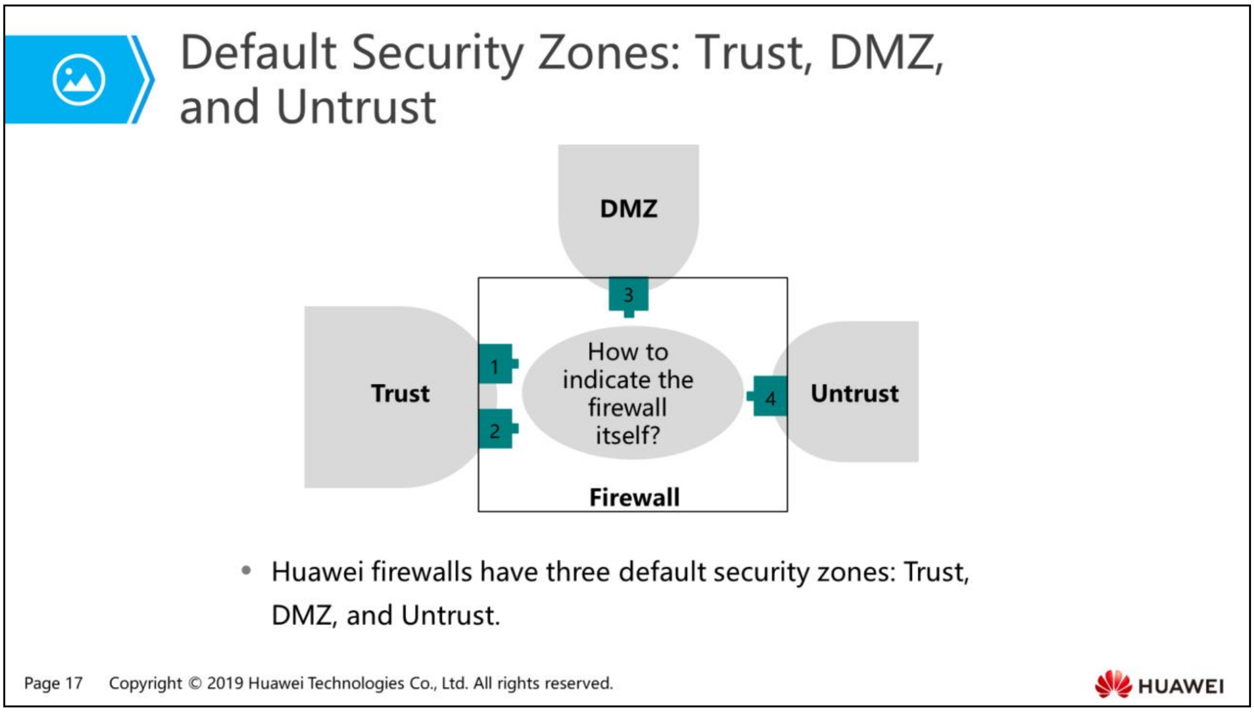
- To distinguish networks on firewalls, we bring an important concept to the firewalls: security zone, which is also called zone. A security zone contains one or multiple interfaces. Security zones are a major difference between firewalls and routers. Firewalls use security zones to divide networks and mark the paths of packets. Generally speaking, packets are controlled only when they travel between security zones.
- As we all know, firewalls use interfaces to connect to networks. After interfaces are assigned to security zones, security zones are associated with networks. When we mention a security zone, we refer to the network connected to the security zone. The figure shows the relationship of interface, network, and security zone.



Assigning Interfaces to Security Zones

- You can assign interfaces to security zones to divide networks on a firewall.

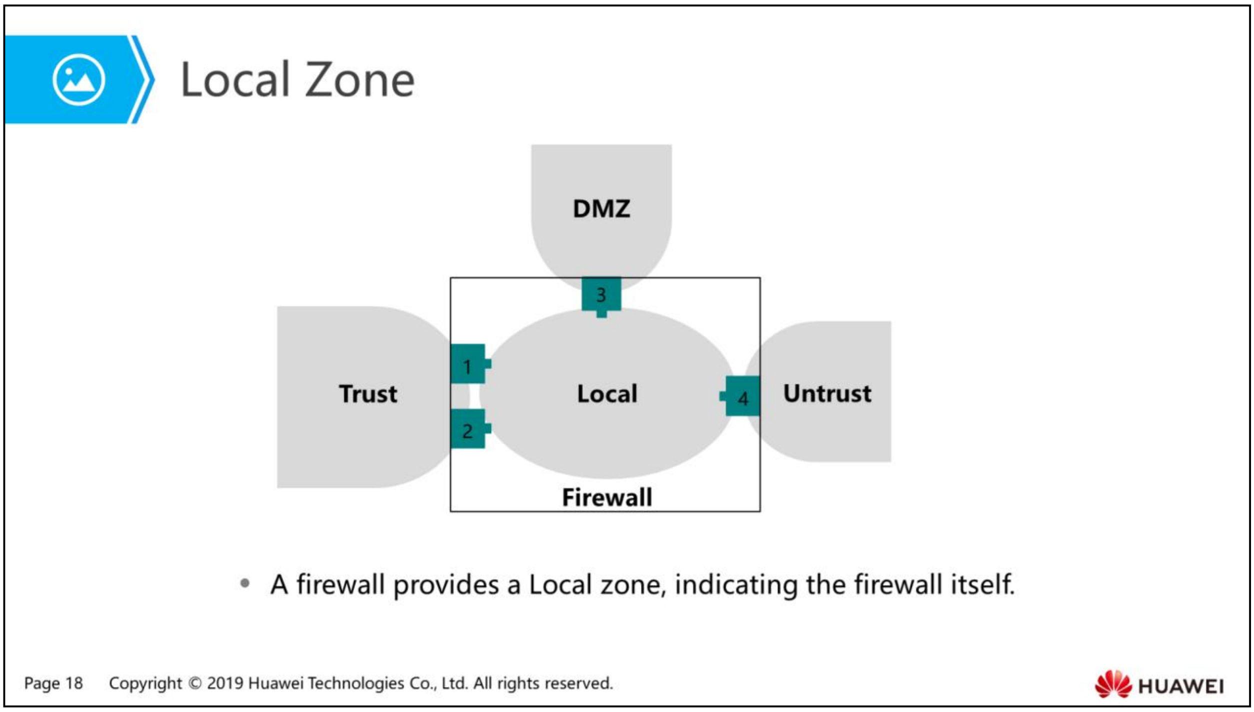
- You can assign interfaces to security zones to divide networks on a firewall. As shown in the figure, interfaces 1 and 2 are assigned to security zone A, interface 3 to security zone B, and interface 4 to security zone C. Then, the firewall has three security zones, corresponding to three networks.
- On a Huawei firewall, one interface can be assigned to only one security zone.



Default Security Zones: Trust, DMZ, and Untrust

- Huawei firewalls have three default security zones: Trust, DMZ, and Untrust.

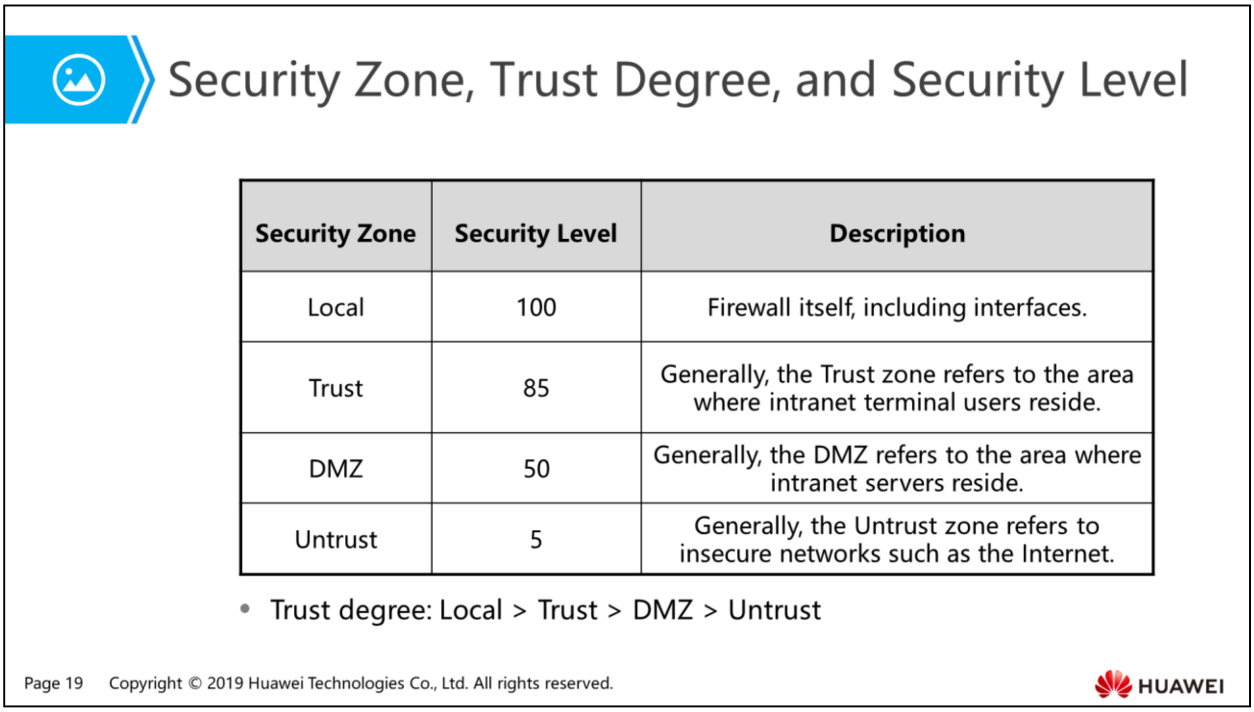
- Huawei firewalls have three default security zones: Trust, DMZ, and Untrust.
  - The Trust zone usually refers to the network of internal users. This network is highly trusted.
  - The DMZ usually refers to the network of internal servers. The trust level of this network is medium.
  - The Untrust zone usually refers to insecure networks, such as the Internet. The network is untrusted.
- If there are a few networks and the network environment is simple, using default security zones can meet network division requirements. If there are many networks, you can create more security zones as required.
- As shown in the figure, if interfaces 1 and 2 connect to internal users, assign the interfaces to the Trust zone; if interface 3 connects to internal servers, assign it to the DMZ; if interface 4 connects to the Internet, assign it to the Untrust zone.
- When an internal user accesses the Internet, the packet travels from the Trust zone to the Untrust zone. When an Internet user accesses an internal server, the packet travels from the Untrust zone to the DMZ.
- Note that the Demilitarized Zone (DMZ) is originally a military term, referring to a partially controlled area between a strict military control area and a loose public area. Firewalls reference this term to refer to a security zone separate from both the internal and external networks.
- In addition to packets flowing between networks, there are packets destined for the firewall itself (for example, firewall login and configuration packets) and packets sent from the firewall. How to mark the routes of such packets on firewalls?



Local Zone

- A firewall provides a Local zone, indicating the firewall itself.

- A firewall provides a Local zone, indicating the firewall itself. All packets originated from the firewall are regarded from the Local zone; those to be responded and processed by the firewall (not the packets to be forwarded) are regarded to the Local zone.
- No interface can be assigned to the Local zone. All interfaces on the firewall are already in the Local zone. That is, for a packet destined for a network, the destination security zone is the zone where the interface resides; for a packet destined for the firewall, the destination security zone is the Local zone.

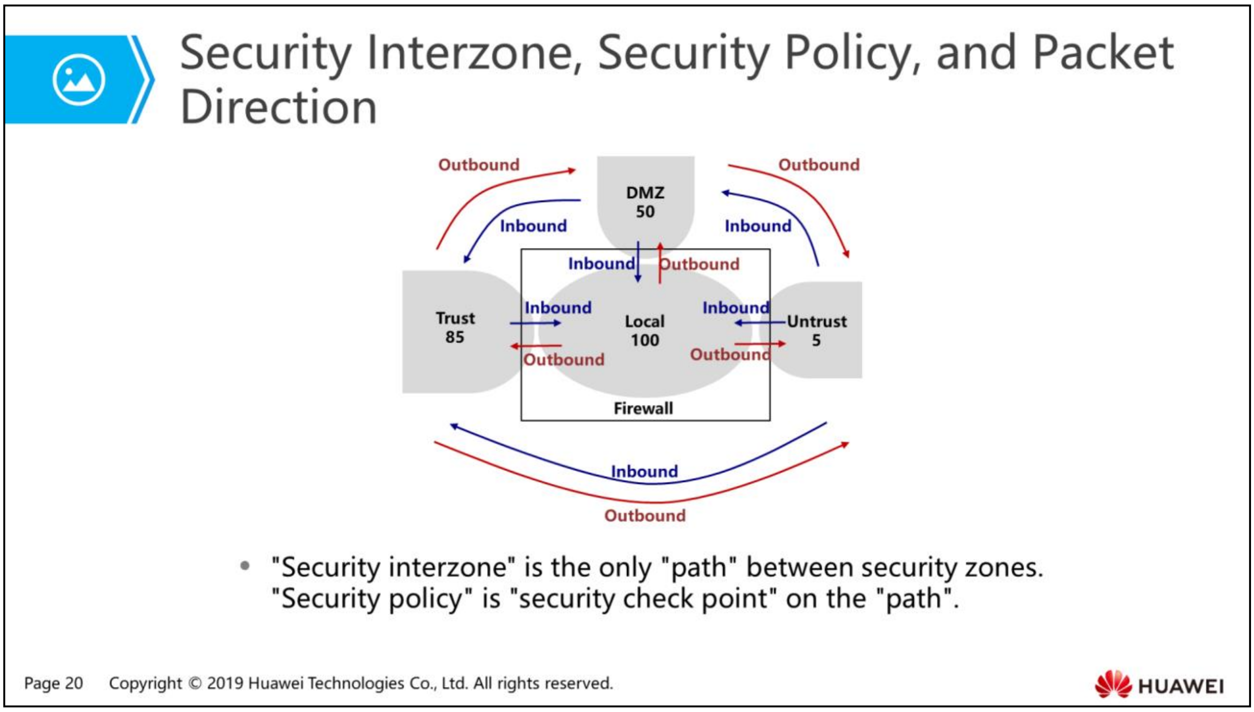


Security Zone, Trust Degree, and Security Level

Security Zone	Security Level	Description
Local	100	Firewall itself, including interfaces.
Trust	85	Generally, the Trust zone refers to the area where intranet terminal users reside.
DMZ	50	Generally, the DMZ refers to the area where intranet servers reside.
Untrust	5	Generally, the Untrust zone refers to insecure networks such as the Internet.

- Trust degree: Local > Trust > DMZ > Untrust

- The trust degree varies with networks. As security zones indicate networks on firewalls, how to determine the trust degree of a security zone? On a Huawei firewall, each security zone has a unique security level, indicated by a number ranging from 1 to 100. A greater number indicates a more trusted network. For default security zones, their security levels are fixed: 100 for the Local zone, 85 for the Trust zone, 50 for the DMZ, and 5 for the Untrust zone.



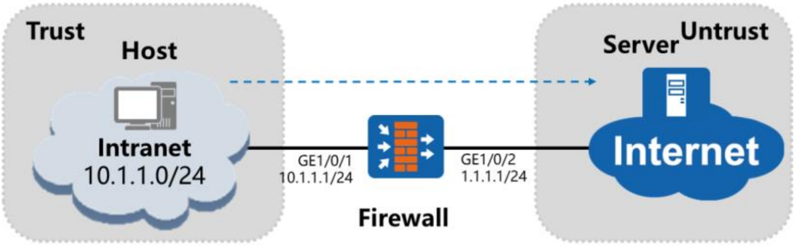
Security Interzone, Security Policy, and Packet Direction

- "Security interzone" is the only "path" between security zones. "Security policy" is "security check point" on the "path".

Page 20 Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

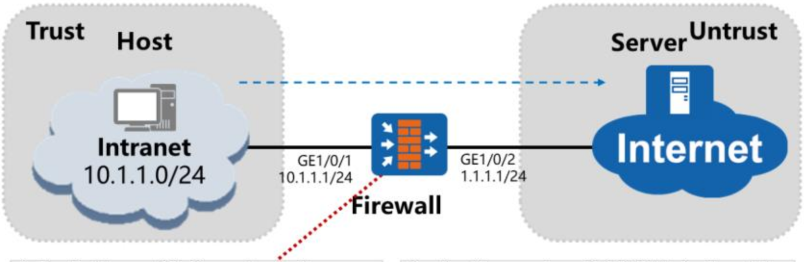
- An interzone refers to a zone between two security zones. Each interzone has its own view, where most firewall configurations are performed.
  - The concept, security interzone, describes traffic transmission paths. An interzone is the unique "path" between "zones". To control traffic traveling through the path, you must set "check points" (security policies). When packets travel between security zones, we define the Inbound direction if the packets flow from a lower-level security zone to a higher-level security zone and the Outbound direction if the packets flow from a higher-level security zone to a lower-level security zone. The two directions trigger different security checks. In the figure, the traffic directions are marked among the four security zones: Local, Trust, DMZ, and Untrust.
- Generally, communication parties exchange packets. That is, packets are transmitted in both directions in an interzone. The first packet in a flow is used to determine the direction of the flow.
- By setting security zones, they have clear interzone relationships. Each security zone indicates a network, and a firewall interconnects networks. On this basis, the firewall can control packets traveling among the networks.

Security Zone Configuration Example



- On a testing network shown in the figure, an NGFW serves as a security gateway. To allow users in 10.1.1.0/24 to access the server at 1.1.1.10, we must configure security zones on the NGFW.

Security Zone Configuration Commands



Set the IP addresses of interfaces and assign the interfaces to security zones.

```
interface GigabitEthernet1/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet1/0/1
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet1/0/2
```

Question: Why cannot users in 10.1.1.0/24 ping through the server?

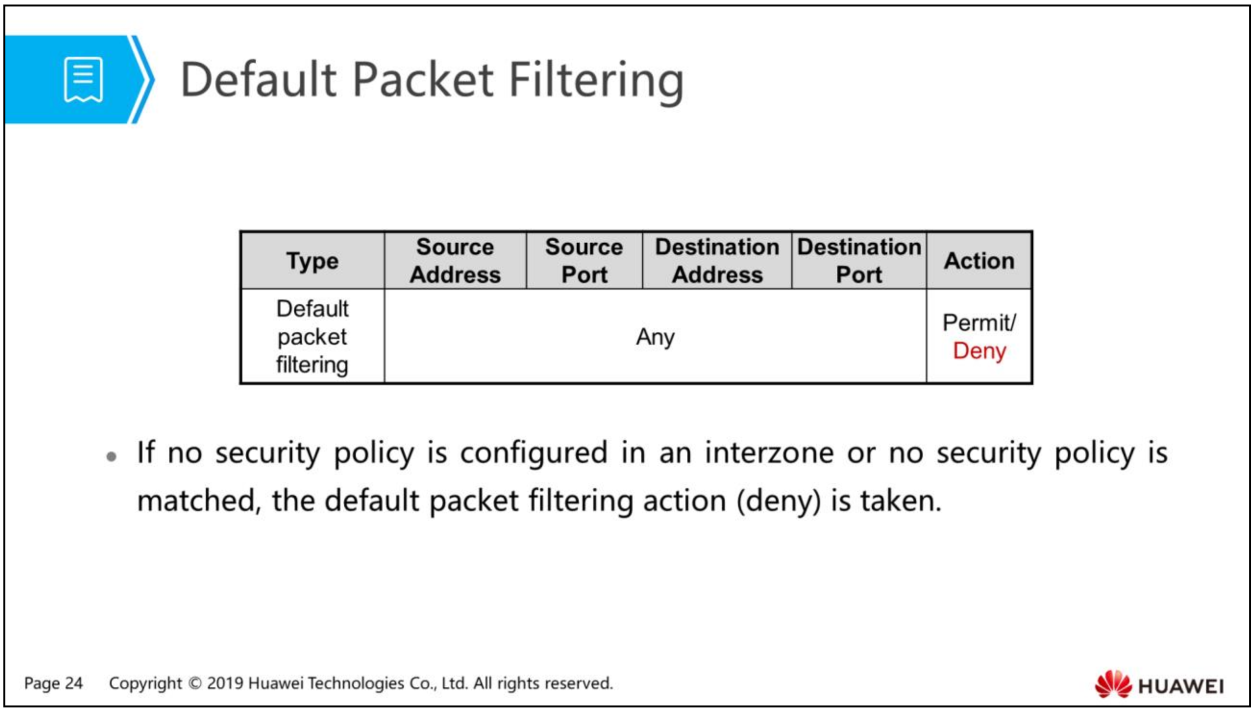
```
PC>ping 1.1.1.10

Ping 1.1.1.10: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!

--- 1.1.1.10 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
  100.00% packet loss
```

Contents

1. **Firewall Basic Knowledge**
   - Why Do We Need Firewalls?
   - Firewall Development History
   - Huawei Firewall Products
   - Security Zone
   - Security Policy
2. NAT
3. Attack Defense



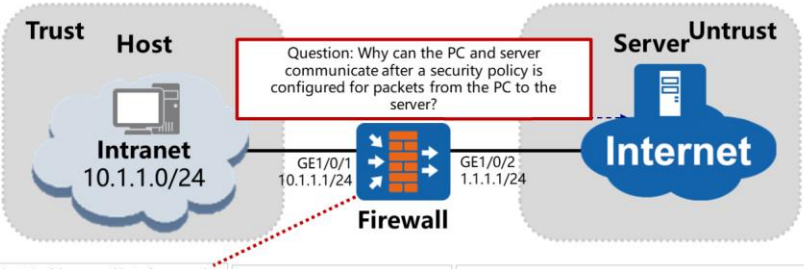
Default Packet Filtering

Type	Source Address	Source Port	Destination Address	Destination Port	Action
Default packet filtering	Any				Permit/ Deny

- If no security policy is configured in an interzone or no security policy is matched, the default packet filtering action (deny) is taken.

- If no security policy is configured, the firewall does not allow packet transmission between security zones.
- Default packet filtering is the default security policy that takes effect on all packets. Without configuration, the default packet filtering action is **deny**.

Security Policy Configuration Commands



Question: Why can the PC and server communicate after a security policy is configured for packets from the PC to the server?

1. Set the IP addresses of interfaces and assign the interfaces to security zones.

```
interface GigabitEthernet1/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet1/0/1
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet1/0/2
```

2. Configure a security policy.

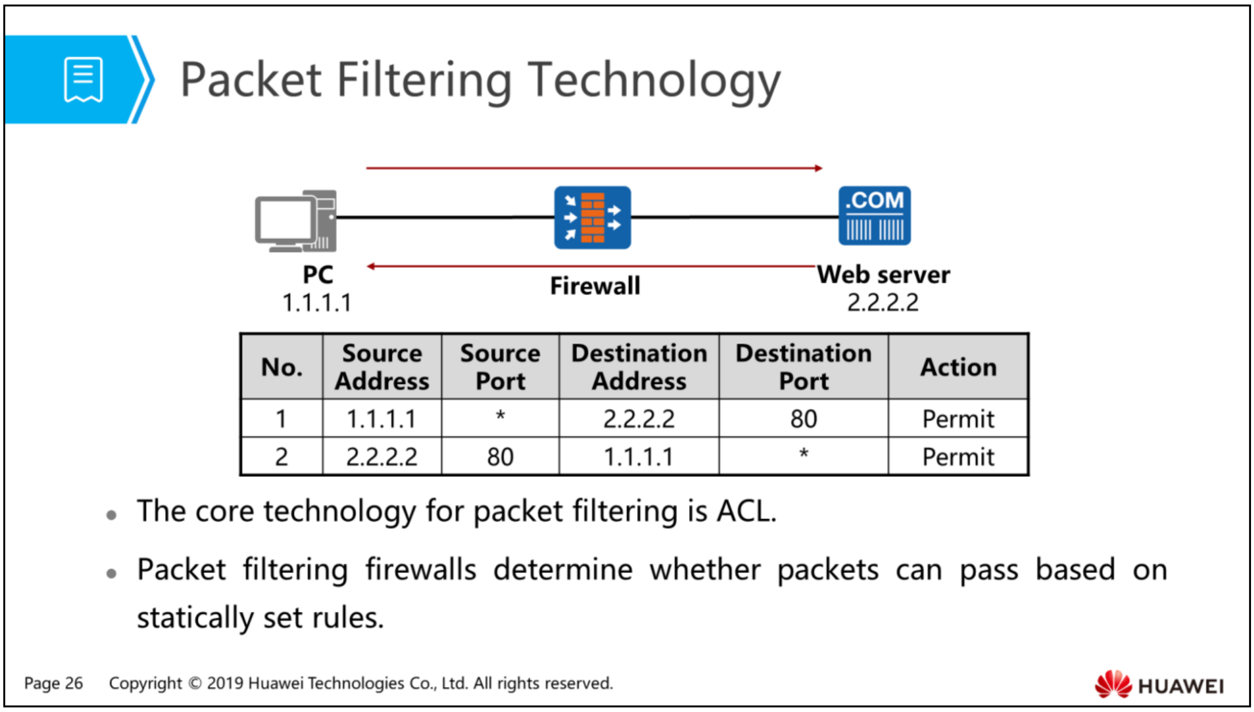
```
security-policy
  rule name policy_sec_1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0
24
    action permit
```

Users in 10.1.1.0/24 can ping through the server.

```
PC>ping 1.1.1.10

Ping 1.1.1.10: 32 data bytes, Press Ctrl_C to break
From 1.1.1.10: bytes=32 seq=1 ttl=127 time<1 ms
From 1.1.1.10: bytes=32 seq=2 ttl=127 time=15 ms
From 1.1.1.10: bytes=32 seq=3 ttl=127 time=15 ms
From 1.1.1.10: bytes=32 seq=4 ttl=127 time<1 ms
From 1.1.1.10: bytes=32 seq=5 ttl=127 time<1 ms

--- 1.1.1.10 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 0/6/15 ms
```

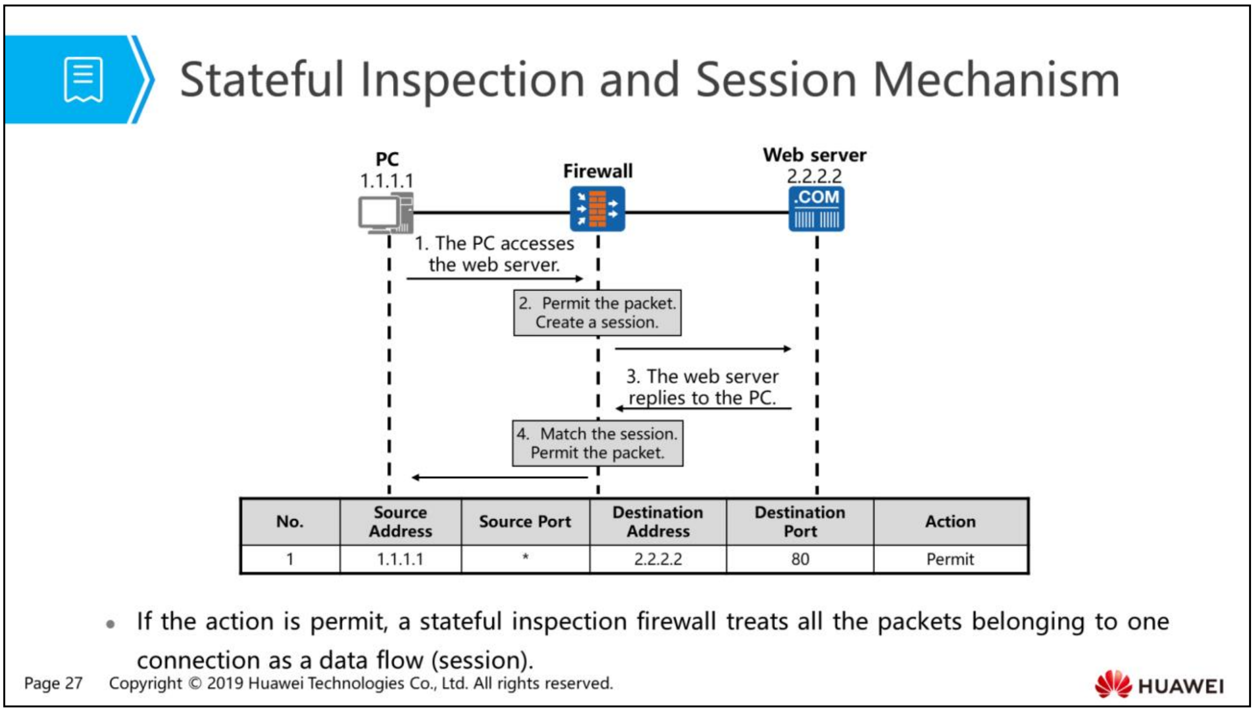


Packet Filtering Technology

No.	Source Address	Source Port	Destination Address	Destination Port	Action
1	1.1.1.1	*	2.2.2.2	80	Permit
2	2.2.2.2	80	1.1.1.1	*	Permit

- The core technology for packet filtering is ACL.
- Packet filtering firewalls determine whether packets can pass based on statically set rules.

- Packet filtering firewalls determine whether packets can pass based on statically set rules. Such a firewall considers packets are stateless and isolated entities and does not care the cause and consequence of packets.
- As shown in the figure, the PC and server are in different networks, and both connect to a firewall. Communication between the PC and server is controlled by the firewall. When the PC accesses the web server to browse a web page:
    - Rule 1 must be set on the firewall to allow the packets from the PC to the web server to pass.
        - In rule 1, * at the source port indicates any port. This is because the PC's operating system determines the source port when it accesses the web server. For example, in the Windows system, the port number ranges from 1024 to 65535. As the port number is not fixed, the source port is set to any. After the rule is set, packets from the PC can pass through the firewall and reach the web server.
    - The web server will reply a packet to the PC. This packet must pass through the firewall to the PC. Before the generation of stateful inspection firewalls, packet filtering firewalls require rule 2 to allow the reverse packet to pass.
        - In rule 2, the destination port is set to any because we are uncertain about the source port used by the PC to access the web server.
- If the PC is in a protected network, such settings bring great security risks. As rule 2 allows packets with any destination ports to pass, attackers may disguise as web servers to pass through the firewall, bringing about huge security risks to the PC.
- "Per-packet inspection" affects forwarding efficiency and makes the firewall a bottleneck for packet forwarding on the network.



Stateful Inspection and Session Mechanism

1. The PC accesses the web server.

2. Permit the packet. Create a session.

3. The web server replies to the PC.

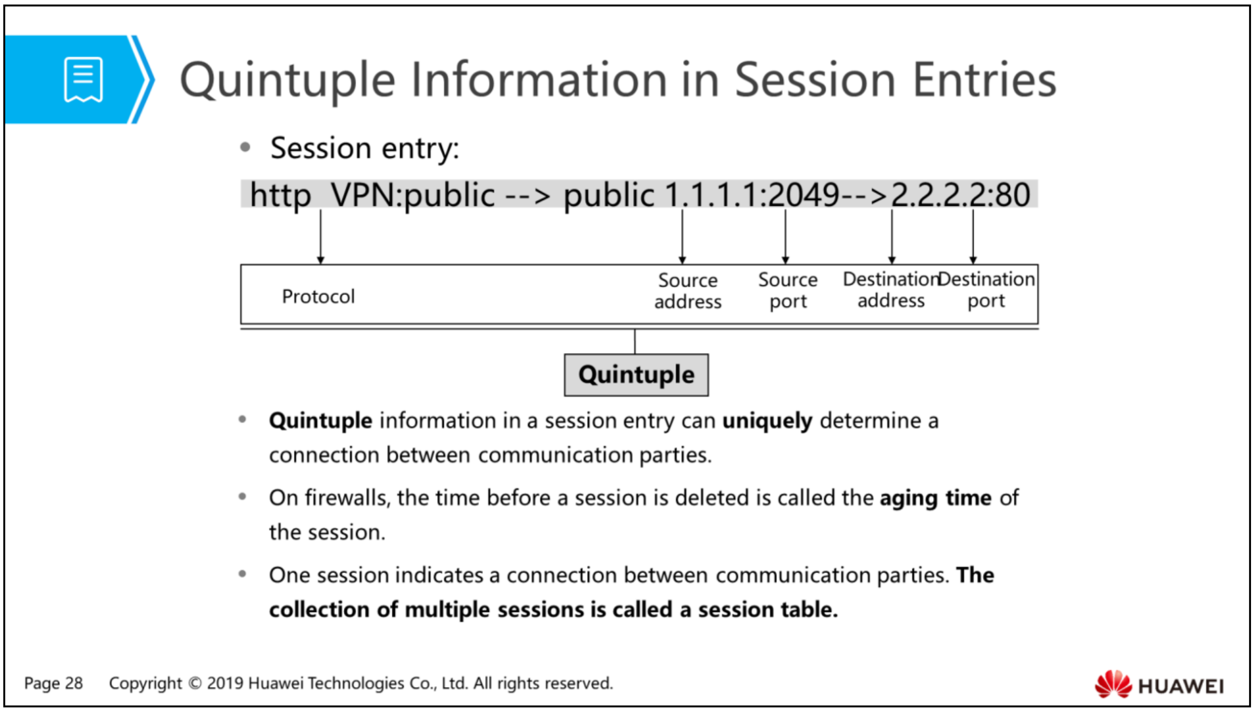
4. Match the session. Permit the packet.

No.	Source Address	Source Port	Destination Address	Destination Port	Action
1	1.1.1.1	*	2.2.2.2	80	Permit

- If the action is permit, a stateful inspection firewall treats all the packets belonging to one connection as a data flow (session).

- A stateful inspection firewall uses a detection mechanism based on the connection status and treats all the packets belonging to one connection as a data flow. From the view of a stateful inspection firewall, packets in a data flow are not isolated entities. Instead, they are related. The firewall creates a session for the first packet in the data flow and directly forwards subsequent packets in the data flow based on the session, improving forwarding efficiency.

- As shown in the figure, the stateful inspection firewall makes up the disadvantages of packet filtering technologies:
  - First, we still need to set rule 1 on the firewall to allow packets from the PC to the web server to pass.
  - After the first packet arrives at the firewall, the firewall allows the packet to pass and creates a session for the access from the PC to the web server. The session contains information about the packet from the PC, including the address and port.
  - When the packet replied by the web server to the PC arrives at the firewall, the firewall compares packet information with session information. If the packet matches the session and complies with the subsequent packet definition in the related protocol standard, the firewall considers the packet as the reply packet from the web server to the PC and directly permits the packet.



Quintuple Information in Session Entries

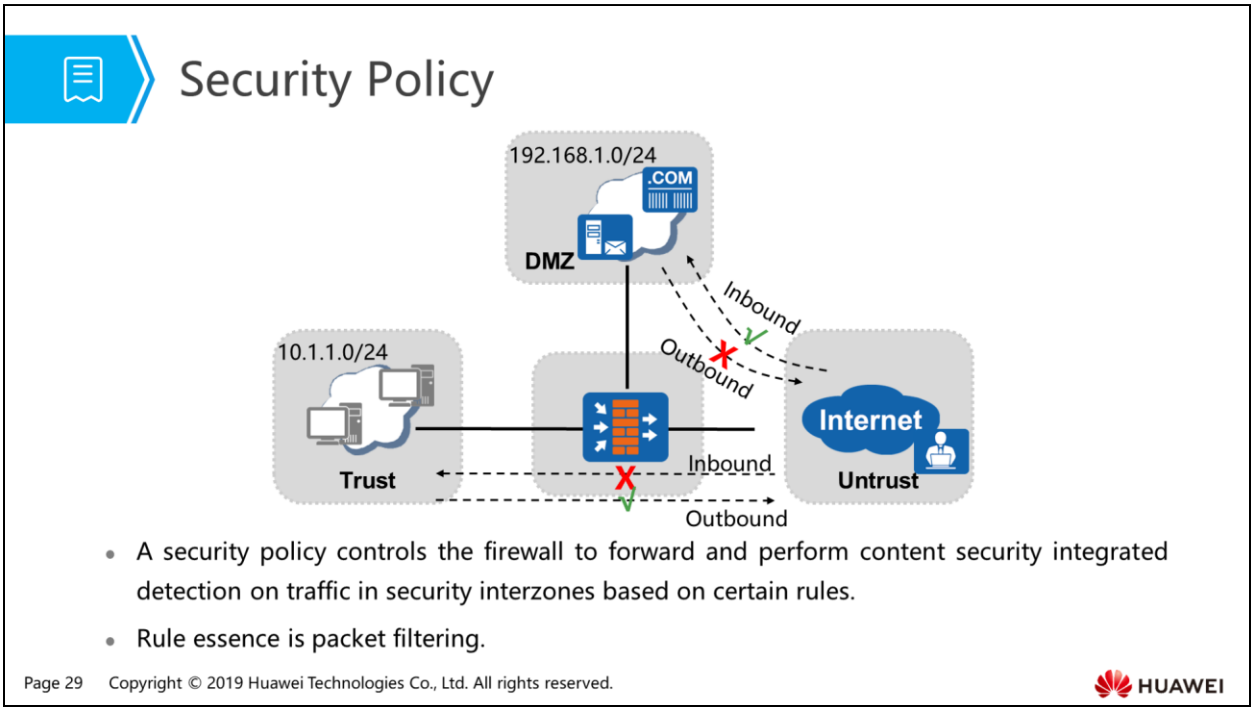
- Session entry:

```
http  VPN:public --> public 1.1.1.1:2049-->2.2.2.2:80
```

Protocol
Source address
Source port
Destination address
Destination port
Quintuple

- **Quintuple** information in a session entry can **uniquely** determine a connection between communication parties.
- On firewalls, the time before a session is deleted is called the **aging time** of the session.
- One session indicates a connection between communication parties. **The collection of multiple sessions is called a session table.**

- A session represents a connection between communication parties and indicates the connection status. The collection of multiple sessions on a firewall is called a session table.
- In the session entry shown on the figure:
  - http indicates the protocol, 1.1.1.1 indicates the source address, 2049 indicates the source port, 2.2.2.2 indicates the destination port, and the value of 80 indicates the destination port.
  - The source address, source port, destination address, destination port, and protocol are important information of sessions. We call them quintuple. Packets with the same quintuple are considered to belong to one flow. On a firewall, the five elements identify a connection.
- Sessions are dynamically generated but not permanently existent. If no packet matches a session for a long time, it indicates that the connection has been torn down, and the session is unnecessary. To save system resources, the firewall deletes the session after a period of time. This period of time is call the aging time of the session.



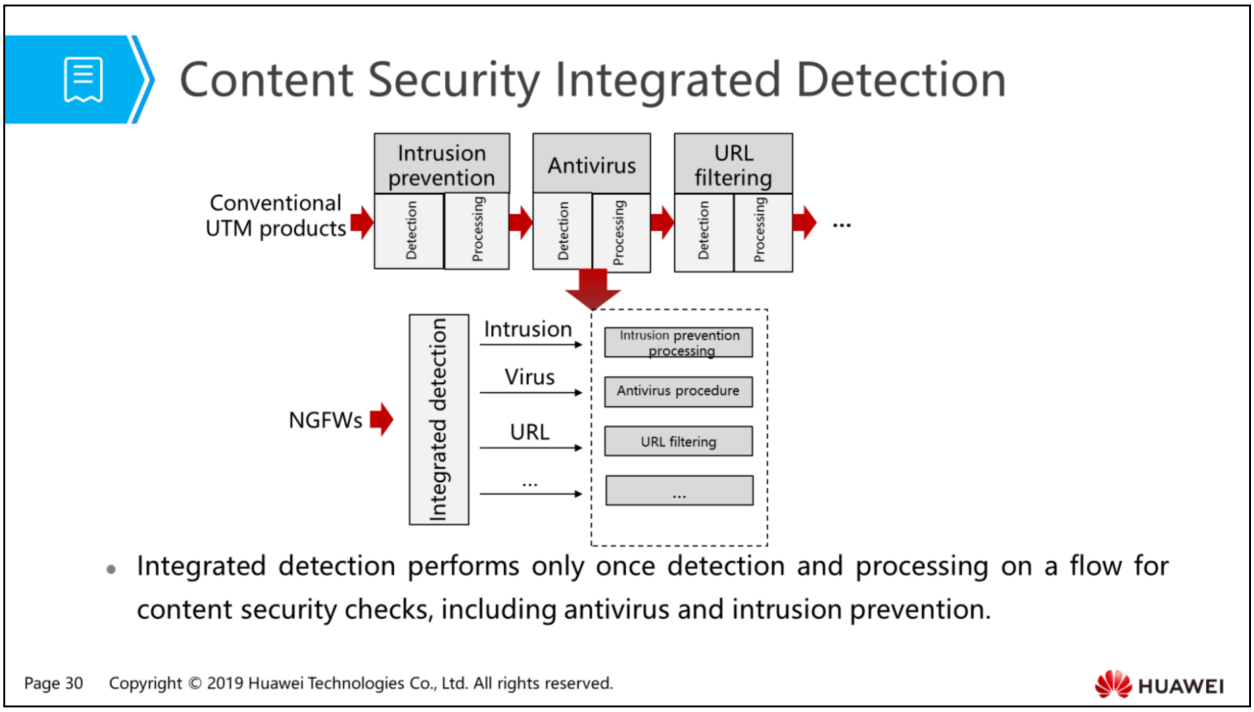
Security Policy

- A security policy controls the firewall to forward and perform content security integrated detection on traffic in security interzones based on certain rules.
- Rule essence is packet filtering.

Page 29 Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

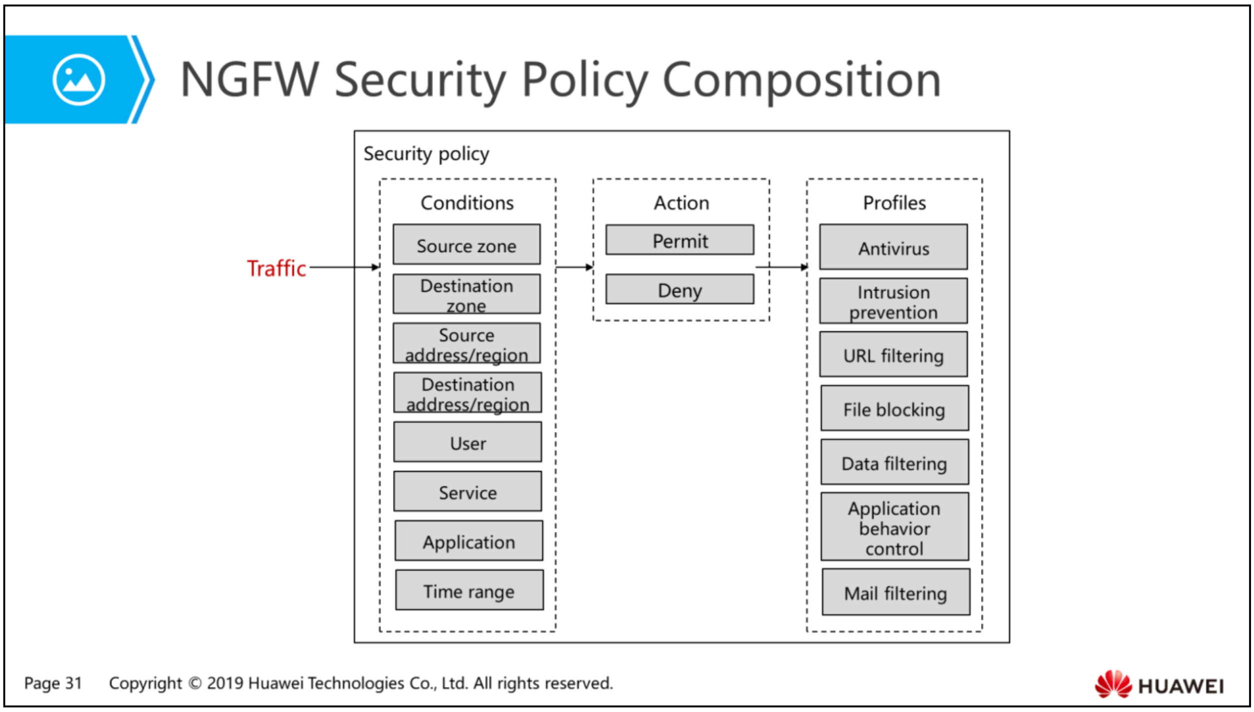
- A firewall protects a network from being attacked by any untrust network while permitting legitimate communication between the two networks.
- A security policy controls the firewall to forward and perform content security integrated detection on traffic in security interzones based on certain rules. The security interzone is the unique path between two security zones. Security policies are like check points on the path.
- Security policies check passing data flows. Only the data flows that match the security policies are allowed to pass through firewalls.
- An interzone refers to a path between two security zones. Each interzone has its own view, where most security policies are configured.
- The security policy configured in the figure does the following things:
  - Allow the Internet to access servers in 192.168.1.0/24 but prevent the servers from accessing the Internet.
  - Allow data packets from 10.1.1.0/24 to access the Internet but prevent the Internet from accessing the intranet.



Content Security Integrated Detection

- Integrated detection performs only once detection and processing on a flow for content security checks, including antivirus and intrusion prevention.

- Firewalls can identify traffic attributes and match them with security policy conditions. If all the conditions are met, the traffic matches the policy. The device implements the matched security policy.
    - If the action is **permit**, the firewall checks the traffic content. If the traffic passes the security detection, the traffic is allowed through. If not, the traffic is denied.
    - If the action is **Deny**, the traffic is denied.
- Content security integrated detection uses the Intelligence Awareness Engine (IAE) to perform only once detection and processing on a flow to obtain all needed data for subsequent content security checks, including antivirus and intrusion prevention. This implementation greatly improves processing performance.
- Thanks to efficient integrated detection, we can configure loose security policy conditions to match a class of traffic and use content security functions to protect the network.



NGFW Security Policy Composition

Security policy

Traffic

Conditions

- Source zone
- Destination zone
- Source address/region
- Destination address/region
- User
- Service
- Application
- Time range

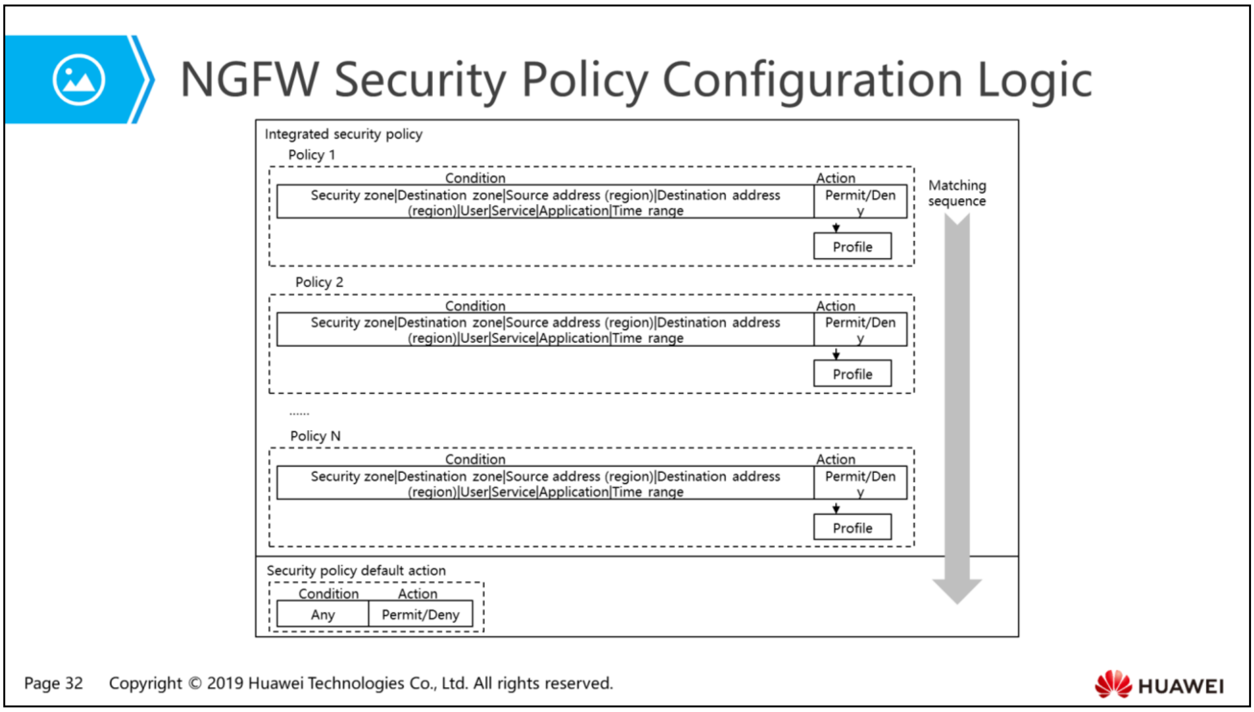
Action

- Permit
- Deny

Profiles

- Antivirus
- Intrusion prevention
- URL filtering
- File blocking
- Data filtering
- Application behavior control
- Mail filtering

- When traffic passes through an NGFW, the security policy works as follows:
  - The firewall analyzes traffic and retrieves the attributes, including the source security zone, destination security zone, source IP address, source region, destination IP address, destination region, user, service (source port, destination port, and protocol type), application and time range.
  - Then the NGFW compares traffic attributes with the conditions defined in security policies. If all the conditions of a policy are met, the traffic matches the policy. If one or more conditions are not met, the firewall compares the traffic attributes using the conditions in the next policy. If none of the policies is met, the firewall denies the traffic by default.
  - If the traffic matches a security policy, the NGFW performs the action defined in the policy on the traffic. If the action is **deny**, the NGFW blocks the traffic. If the action is **permit**, the NGFW checks whether the policy references a profile. If so, go to the next step. If not, the NGFW permits the traffic.
  - If the action defined in the policy is **permit** and certain profiles are referenced in the policy, the firewall performs integrated checks on the content carried over the traffic.
  - The integrated check inspects the content carried over the traffic based on the conditions defined in the referenced profiles and implements appropriate actions based on the check result. If one profile blocks the traffic, the NGFW blocks the traffic. If all profiles permit the traffic, the firewall allows the traffic through.



NGFW Security Policy Configuration Logic

Integrated security policy

Policy 1

Condition	Action
Security zone|Destination zone|Source address (region)|Destination address (region)|User|Service|Application|Time range	Permit/Deny → Profile

Policy 2

Condition	Action
Security zone|Destination zone|Source address (region)|Destination address (region)|User|Service|Application|Time range	Permit/Deny → Profile

......

Policy N

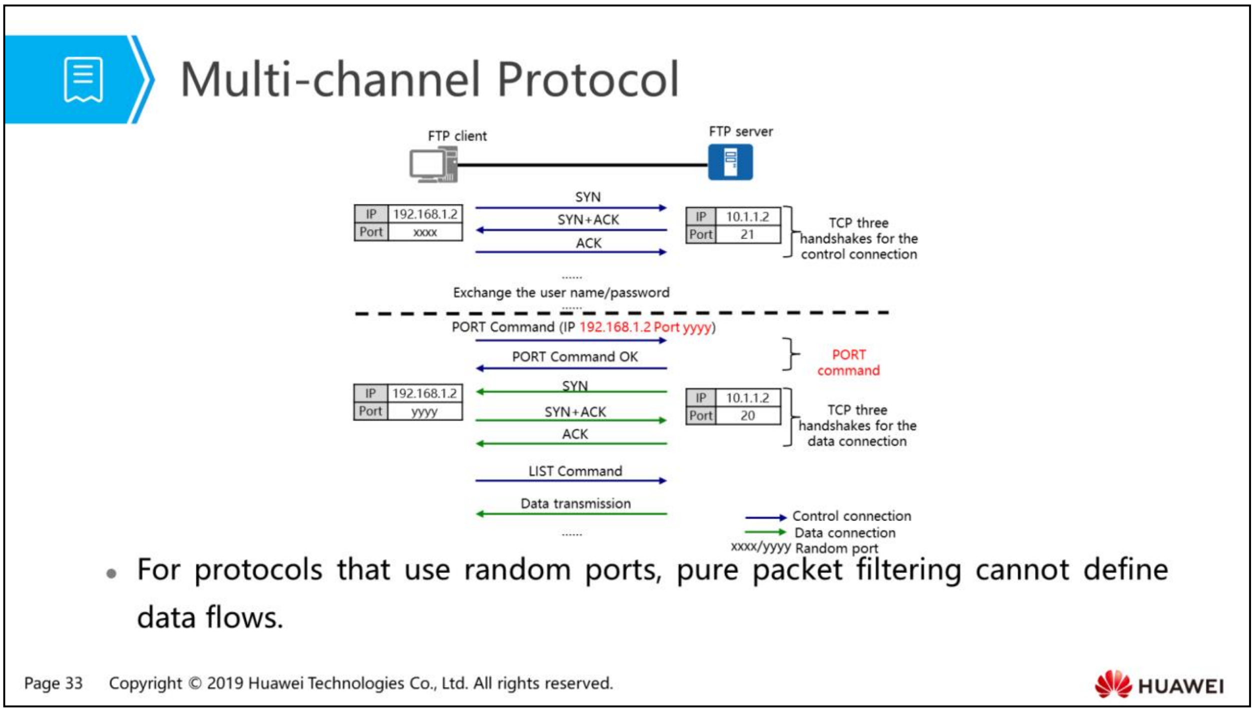
Condition	Action
Security zone|Destination zone|Source address (region)|Destination address (region)|User|Service|Application|Time range	Permit/Deny → Profile

Matching sequence

Security policy default action

Condition	Action
Any	Permit/Deny

- NGFW security policies are applied globally. Security zones, IP addresses, and other matching conditions are optional. In addition, multiple security zones can be selected.
- If multiple security policies are configured, the policies are matched top down. If traffic matches a security policy, the following policies are ignored. Therefore, you must place the policies from the most specific to the least specific.
- The system has an implicit deny any policy. Traffic that does not match any security policy is discarded.
- A policy has multiple match conditions, such as security zone, user, and application. A packet matches a policy if the packet matches all the conditions of the policy. The default conditions of a policy are all any, which means that all packets match the policy.
- If a condition has multiple values, the values are logically ORed, meaning that a packet matches the condition if the packet matches any value of the condition.



Multi-channel Protocol

- For protocols that use random ports, pure packet filtering cannot define data flows.

Page 33 Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved. HUAWEI

- Most multimedia application protocols (such as H.323 and SIP), FTP, and NetMeeting use prescribed ports to initialize a control connection and then dynamically select a port for data transmission. Port selection is unpredictable. An application may use more than one port at a time. Packet filtering firewalls can use ACLs to match applications of single-channel protocols to prevent network attacks. However, ACLs can block only applications using fixed ports. Multi-channel protocol applications that use random ports bring security risks.

- Single-channel protocol: uses only one port during communication. For example, WWW uses only port 80.

- Multi-channel protocol: uses two or more ports for communication. For example, FTP passive mode uses port 21 and a random port.

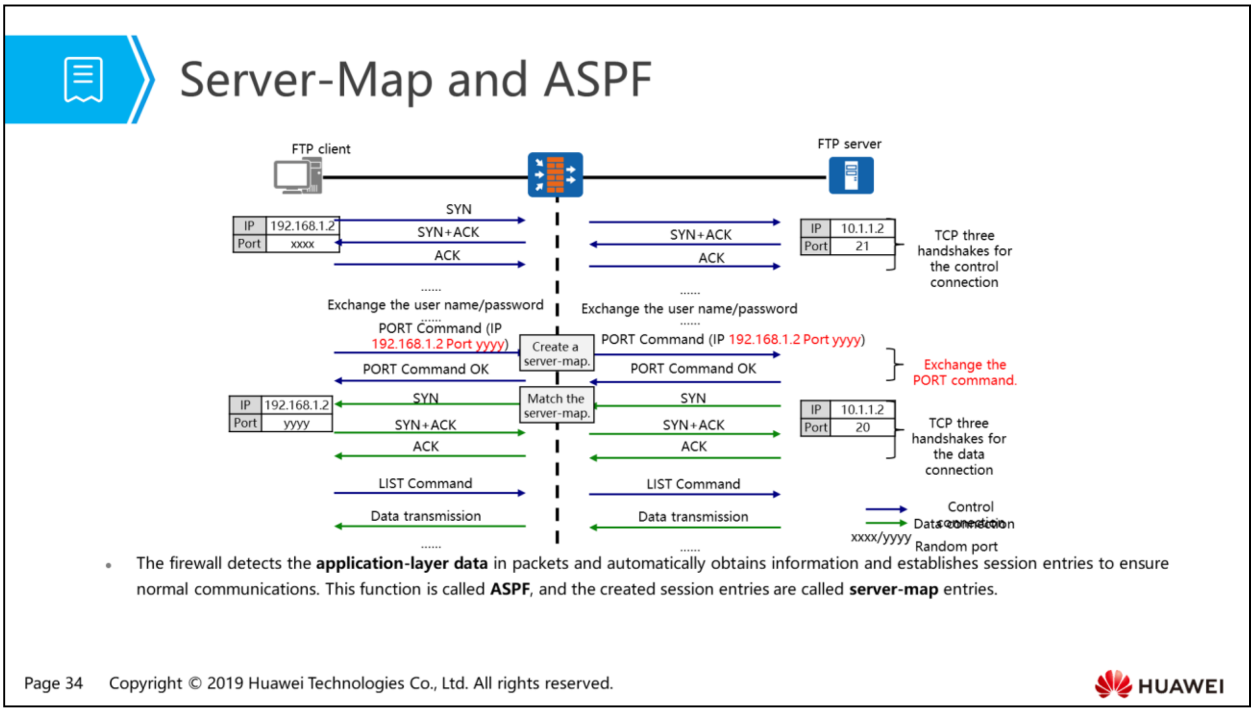
- FTP is a typical multi-channel protocol. Two connections are set up between the FTP client and server. They are the control connection and data connection. The control connection communicates FTP commands and parameters including information necessary for setting up the data connection. The data connection obtains directories and transfers data. The port number used for the data connection is negotiated during the control connection. FTP works in either active (PORT) or passive (PASV) mode, determined by the data connection initiation mode. In active mode, the FTP server initiates the data connection to the FTP client; in passive mode, the FTP server accepts the data connection initiated by the FTP client. The mode can be set on the FTP client. Here, the active mode is used as an example.

    - The FTP client initiates a control connection to port 21 of the FTP server and then use the PORT command to negotiate the port number used for data transmission. If the negotiation succeeds, the server initiates a data connection to the port number. A port number is negotiated for each time of data transmission.

    - The configured security policy allows only FTP, that is, port 21. When the FTP client initiates a control connection to the server, a session is created.

    - The source port of the data connection that the server initiates to the client is 20, and the destination port is negotiated port yyyy. The firewall does not consider the packets as subsequent packets of the session. Therefore, the user name and password are authenticated, but the directory listing cannot be obtained.

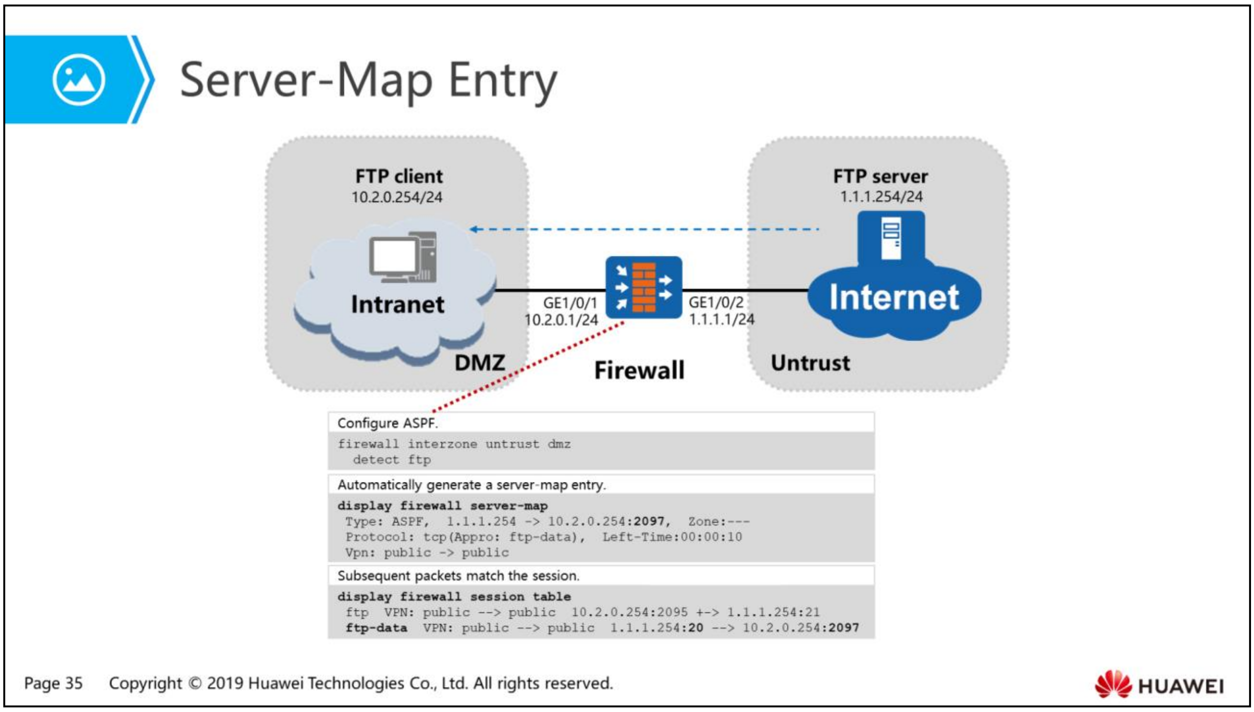
    - If a security policy is configured in the direction from the server to the client, all ports of the clients must be allowed, bringing about security risks.



Server-Map and ASPF

- The firewall detects the **application-layer data** in packets and automatically obtains information and establishes session entries to ensure normal communications. This function is called **ASPF**, and the created session entries are called **server-map** entries.

- Some special applications negotiate port numbers during communication. Therefore, the firewall needs to check the application-layer data of packets to obtain related information and create session entries for normal communication. This function is called Application Specific Packet Filter (ASPF), and the created session entries are called server-map entries.
    - For multi-channel protocols such as FTP, you can use the ASPF function to check the establishment process of control and data connections. By generating server-map entries, the ASPF function ensures that FTP traverses the firewall without affecting the security check function.
    - Server-map entries are like "hidden channels" on the firewall, so that the firewall can properly forward special application packets, such as FTP packets. Of course, this channel is not arbitrarily enabled. Instead, the firewall allows the existence of such a channel only after analyzing the application-layer information of packets to predict the behavior of subsequent packets.
    - A server-map is used only for checking the first packet. After a connection is established, packets are forwarded based on the session table.
    - The server-map table is very important for data forwarding on firewalls. In addition to ASPF, NAT Server and other features can generate server-map entries.
- As shown in the figure:
    - The server-map entry records the data connection initiated from the FTP server to port 2071 of the client. The data connection from the server to the client will match this server-map entry, without the need of a reverse security policy.
    - After the first packet in the data connection matches the server-map entry, the firewall forwards the packet and creates a session for the data connection. Subsequent packets of the data connection will match the session, not the server-map entry.
    - If the server-map entry is not matched by any packet, it will be deleted after the aging timer expires. This mechanism ensures that the server-map entry is deleted in a timely manner to safeguard the network. Subsequent data connections will trigger the re-establishment of server-map entries.



Server-Map Entry

Configure ASPF.

```
firewall interzone untrust dmz
  detect ftp
```

Automatically generate a server-map entry.

```
display firewall server-map
 Type: ASPF,  1.1.1.254 -> 10.2.0.254:2097,  Zone:---
 Protocol: tcp(Appro: ftp-data),  Left-Time:00:00:10
 Vpn: public -> public
```

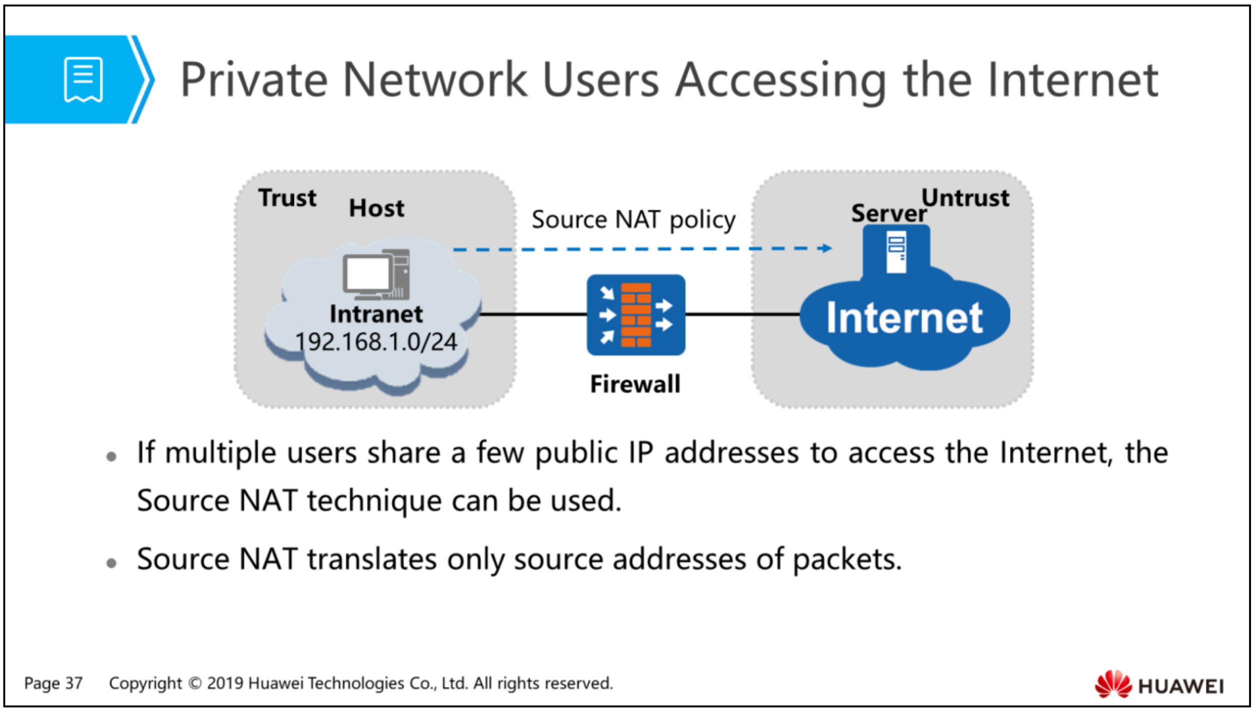
Subsequent packets match the session.

```
display firewall session table
 ftp  VPN: public --> public  10.2.0.254:2095 +-> 1.1.1.254:21
 ftp-data  VPN: public --> public  1.1.1.254:20 --> 10.2.0.254:2097
```

- The relationship between server-map and session:
  - A server-map entry records key information about the application-layer data. If a packet matches the entry, it is not controlled by security policies.
  - A session entry indicates the connection status of two communication parties.
  - The server-map entry does not represent the current connection status. It is a prediction of incoming packets based on the analysis of an existing connection.
  - After receiving a packet, the firewall first checks whether it matches the session table.
  - If not, the firewall checks whether the packet matches a server-map entry.
  - The packets matching server-map entries are not controlled by security policies.
  - Then, the firewall creates sessions for the packets that match server-map entries.

Contents

1. Firewall Basic Knowledge
2. NAT
   - Private Network Users Accessing the Internet
   - Internet Users Accessing Intranet Servers
3. Attack Defense



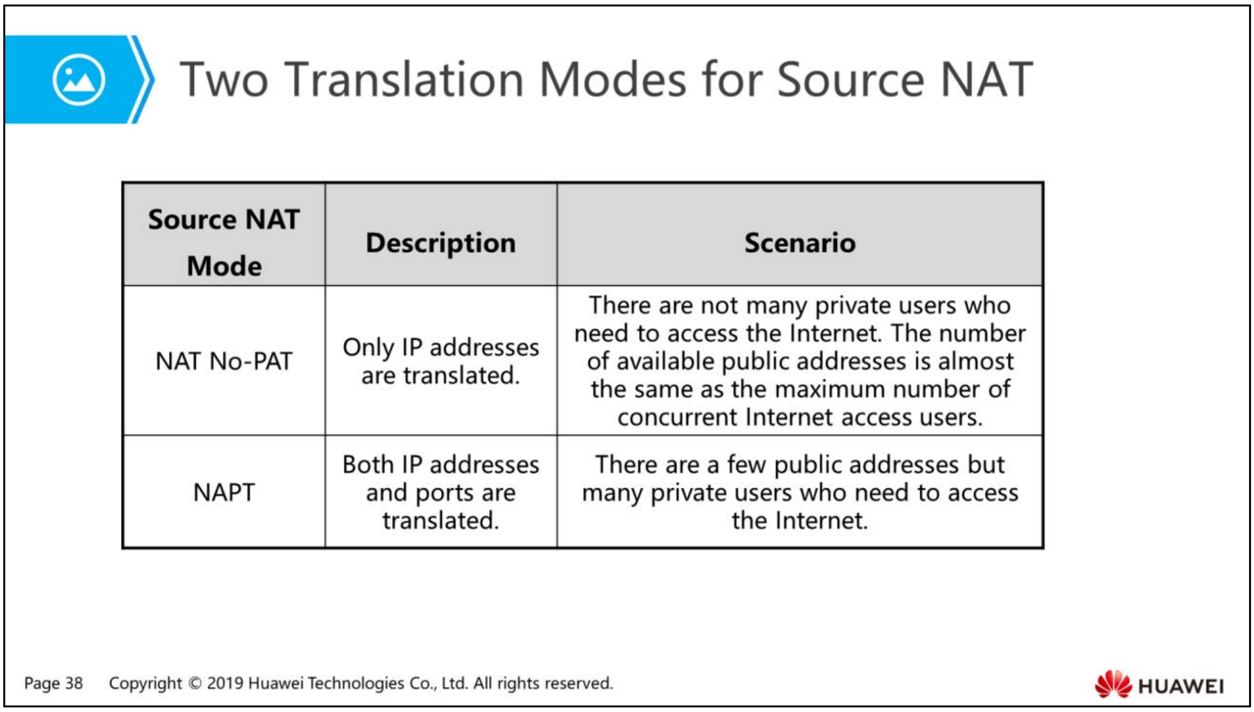
Private Network Users Accessing the Internet

- If multiple users share a few public IP addresses to access the Internet, the Source NAT technique can be used.
- Source NAT translates only source addresses of packets.

Page 37 Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

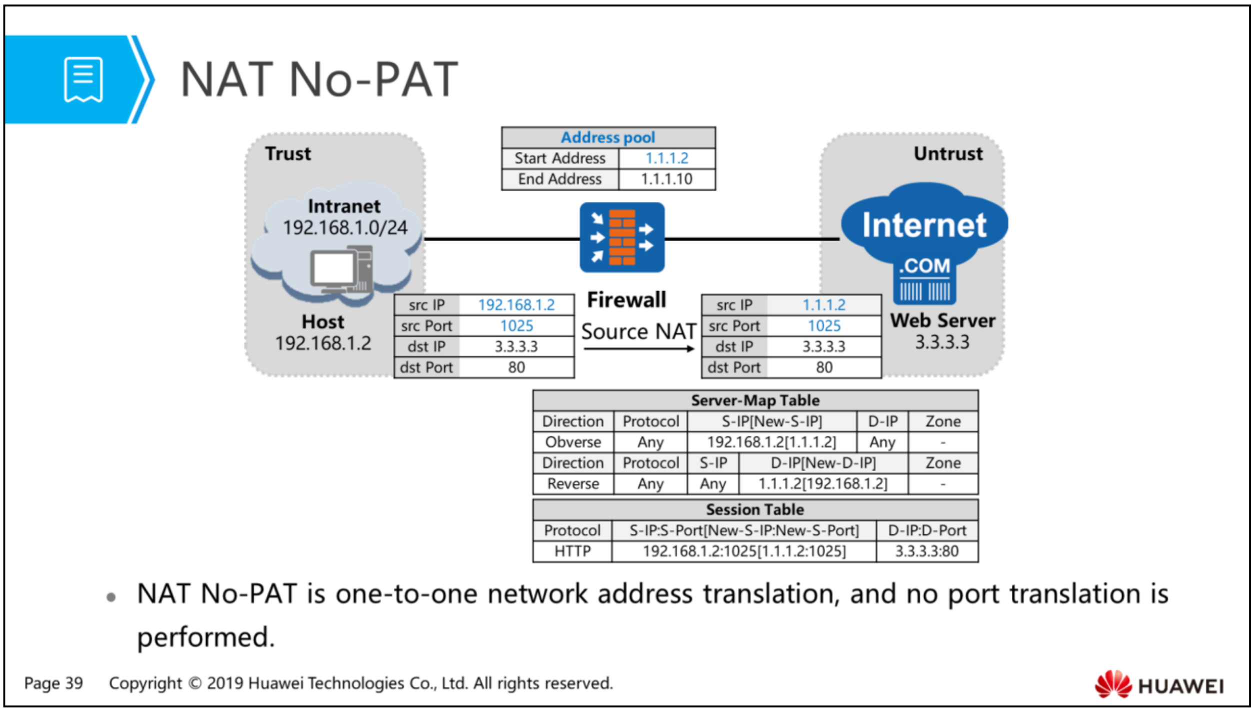
- NAT is an address translation technology that translates the IP address in an IPv4 header to another IP address. Generally, NAT is used to translate private addresses in IPv4 headers to public addresses, so that users in a private network can use a few public addresses to access the Internet. In this manner, NAT resolves public IPv4 address shortage.
- On campus and enterprise networks, it is usually expected to enable multiple users to access the Internet using fewer public IP addresses. Source NAT meets this requirement. Source NAT translates only source addresses of packets. In this manner, users in a private network can access the Internet.
- As shown in the figure, the firewall is deployed at the network border. Source NAT is configured on the firewall to translate the source addresses in packets sent from users in a private network to the Internet into public addresses, so that the users can access the Internet.



Two Translation Modes for Source NAT

Source NAT Mode	Description	Scenario
NAT No-PAT	Only IP addresses are translated.	There are not many private users who need to access the Internet. The number of available public addresses is almost the same as the maximum number of concurrent Internet access users.
NAPT	Both IP addresses and ports are translated.	There are a few public addresses but many private users who need to access the Internet.

- There are multiple Source NAT modes. Here we introduce two of them.
- Address pool mode without port translation (No-PAT):
  - Private users share IP addresses in the address pool. The firewall translates one private address into one public address. Ports are not translated. So the number of IP addresses in the address pool restricts the maximum number of concurrent Internet access users. This mode applies to services that require specific source ports. That is, source port translation is prohibited.
- Address pool mode with port translation (NAPT):
  - This mode applies to mid-range and large-scale networks with many private users. Multiple users share one public address and are distinguished based on ports. Therefore, this mode supports more concurrent Internet access users.



NAT No-PAT

Address pool	
Start Address	1.1.1.2
End Address	1.1.1.10

src IP	192.168.1.2
src Port	1025
dst IP	3.3.3.3
dst Port	80

src IP	1.1.1.2
src Port	1025
dst IP	3.3.3.3
dst Port	80

Server-Map Table

Direction	Protocol	S-IP[New-S-IP]	D-IP	Zone
Obverse	Any	192.168.1.2[1.1.1.2]	Any	-
Direction	Protocol	S-IP	D-IP[New-D-IP]	Zone
Reverse	Any	Any	1.1.1.2[192.168.1.2]	-

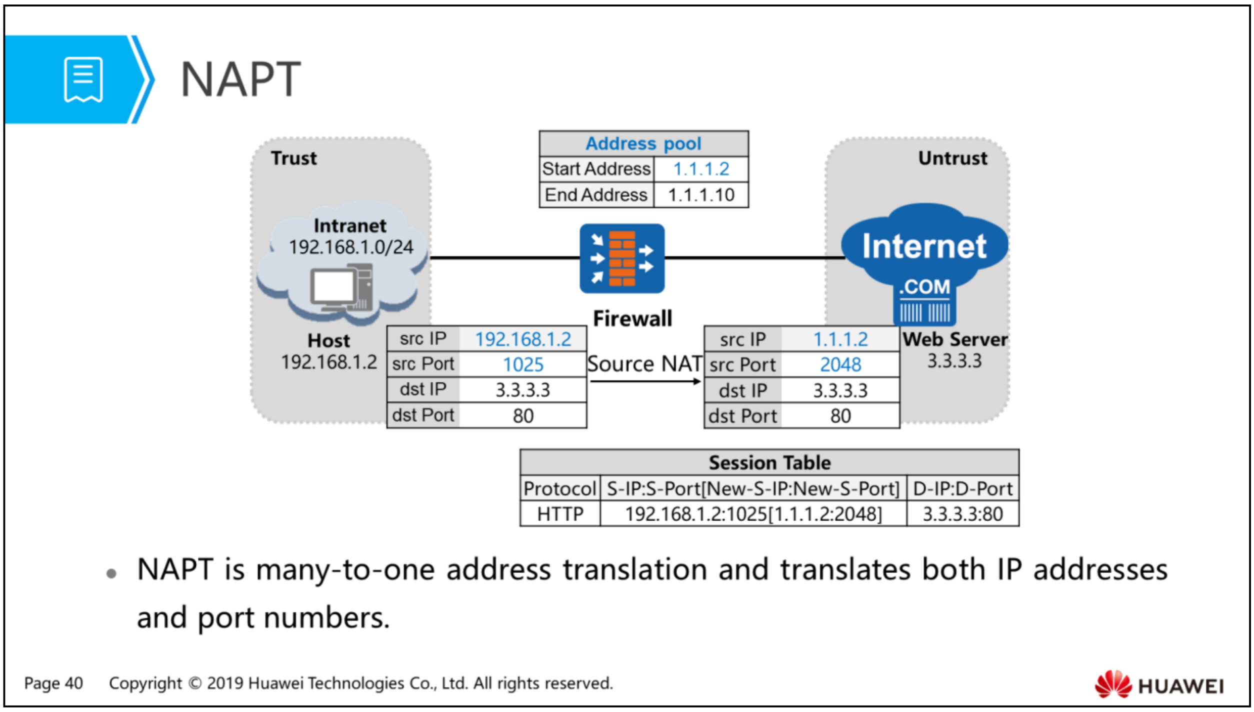
Session Table

Protocol	S-IP:S-Port[New-S-IP:New-S-Port]	D-IP:D-Port
HTTP	192.168.1.2:1025[1.1.1.2:1025]	3.3.3.3:80

- NAT No-PAT is one-to-one network address translation, and no port translation is performed.

HUAWEI

- NAT No-PAT is one-to-one network address translation, and no port translation is performed.
- NAT No-PAT is implemented by configuring a NAT address pool, which contains multiple public addresses. Source NAT translates only IP addresses and maps one private address to a single public address.
- After NAT No-PAT is configured, the firewall creates server-map entries for data flows to maintain mappings between private and public IP addresses. Then the firewall translates IP addresses and forwards packets according to the mappings.
- As shown in the figure, when the host accesses the web server, the firewall does the following processing:
  - Upon receiving a packet from host, the firewall first checks the destination IP address, identifying that the packet needs to be transmitted between Trust and Untrust zones. If the packet is permitted by an interzone security policy, the firewall searches for a matching NAT policy and then finds out that address translation is required.
  - The firewall replaces the source IP address of the packet with an idle public IP address picked from the NAT address pool (a pool of IP addresses for NAT), and then forwards the packet to the Internet. At the same time, the firewall adds an entry to the server-map and session tables.
  - Upon receiving the packet that the web server replies, the firewall searches the session table and the entry created in the previous step is matched. Accordingly, the firewall changes the destination address of the packet to the IP address of the host, and then forwards the packet to the intranet.
- In this manner, the private and public IP addresses are translated. If all addresses in the address pool are allocated, NAT cannot be performed for the rest intranet hosts until the address pool has available addresses.



NAPT

Address pool	
Start Address	1.1.1.2
End Address	1.1.1.10

src IP	192.168.1.2
src Port	1025
dst IP	3.3.3.3
dst Port	80

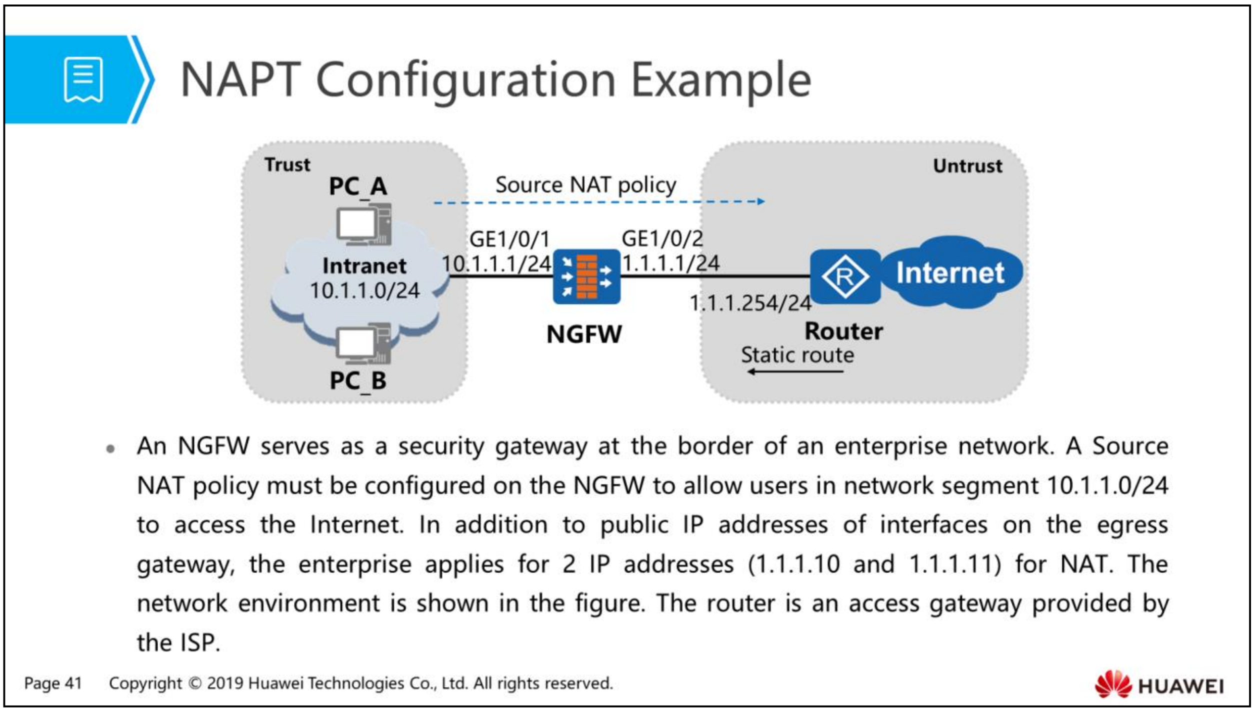
src IP	1.1.1.2
src Port	2048
dst IP	3.3.3.3
dst Port	80

Session Table

Protocol	S-IP:S-Port[New-S-IP:New-S-Port]	D-IP:D-Port
HTTP	192.168.1.2:1025[1.1.1.2:2048]	3.3.3.3:80

- NAPT is many-to-one address translation and translates both IP addresses and port numbers.

- NAPT is many-to-one address translation and translates both IP addresses and port numbers.
- NAPT is implemented by configuring a NAT address pool, which contains one or multiple public addresses. Addresses and ports are both translated, so that private addresses share one or multiple public addresses.
- As shown in the figure, when the host accesses the web server, the firewall does the following processing:
    - Upon receiving a packet from host, the firewall first checks the destination IP address, identifying that the packet needs to be transmitted between Trust and Untrust zones. If the packet is permitted by an interzone security policy, the firewall searches for a matching NAT policy and then finds out that address translation is required.
    - The firewall replaces the source IP address of the packet with a public IP address picked from the NAT address pool and the source port with a new port, and then forwards the packet to the Internet. At the same time, the firewall adds an entry to the session table.
    - Upon receiving the packet that the server replies to the host, the firewall searches the session table, and the entry created in the previous step is matched. Accordingly, the firewall changes the destination address of the packet to the IP address of the host and the destination port to the original port of the inbound packet. Then the firewall forwards the packet to the intranet.
- As both addresses and ports are translated, multiple private users can share one public address to access the Internet. The firewall can distinguish users based on ports, so more users can access the Internet at the same time.



NAPT Configuration Example

Trust

PC_A

Intranet 10.1.1.0/24

PC_B

Source NAT policy

GE1/0/1 10.1.1.1/24

NGFW

GE1/0/2 1.1.1.1/24

Untrust

1.1.1.254/24

Router

Static route

Internet

- An NGFW serves as a security gateway at the border of an enterprise network. A Source NAT policy must be configured on the NGFW to allow users in network segment 10.1.1.0/24 to access the Internet. In addition to public IP addresses of interfaces on the egress gateway, the enterprise applies for 2 IP addresses (1.1.1.10 and 1.1.1.11) for NAT. The network environment is shown in the figure. The router is an access gateway provided by the ISP.

- Configuration roadmap:

1. Set interface IP addresses and assign the interfaces to security zones.

2. Configure security policies to allow packet transmission between a specified private network and the Internet.

3. Configure a NAT address pool.

4. Configure a Source NAT policy for source address translation when users in the specified network access the Internet.

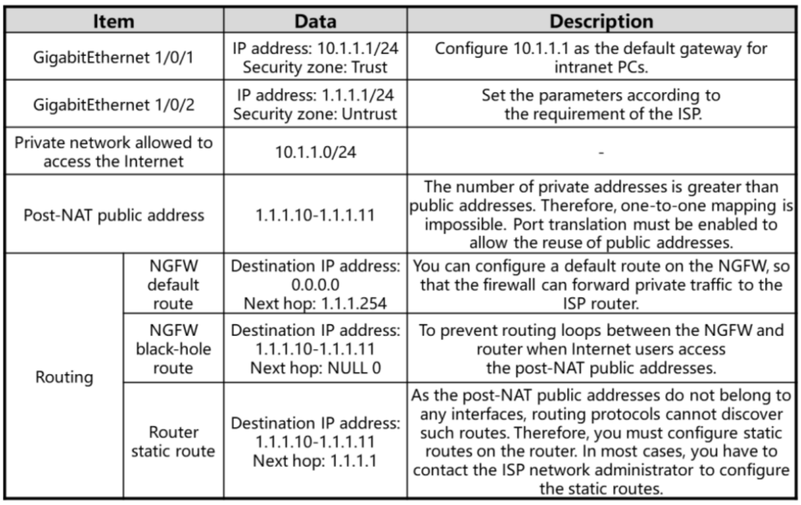
5. Configure default routes on the NGFW, so that the NGFW can forward private traffic to the ISP router.

6. Configure a black-hole route on the NGFW to prevent routing loops between the NGFW and router.

7. Configure the default gateway on each PC in the private network, so that the PCs send traffic to the NGFW when they access the Internet.

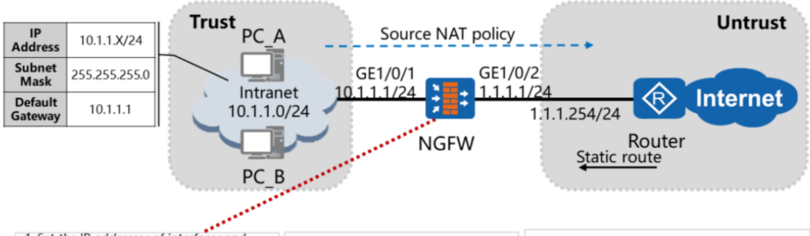
8. Configure static routes on the router, so that the router can forward return traffic from the Internet to the NGFW.

Data Planning



Item		Data	Description
GigabitEthernet 1/0/1		IP address: 10.1.1.1/24 Security zone: Trust	Configure 10.1.1.1 as the default gateway for intranet PCs.
GigabitEthernet 1/0/2		IP address: 1.1.1.1/24 Security zone: Untrust	Set the parameters according to the requirement of the ISP.
Private network allowed to access the Internet		10.1.1.0/24	-
Post-NAT public address		1.1.1.10-1.1.1.11	The number of private addresses is greater than public addresses. Therefore, one-to-one mapping is impossible. Port translation must be enabled to allow the reuse of public addresses.
Routing	NGFW default route	Destination IP address: 0.0.0.0 Next hop: 1.1.1.254	You can configure a default route on the NGFW, so that the firewall can forward private traffic to the ISP router.
	NGFW black-hole route	Destination IP address: 1.1.1.10-1.1.1.11 Next hop: NULL 0	To prevent routing loops between the NGFW and router when Internet users access the post-NAT public addresses.
	Router static route	Destination IP address: 1.1.1.10-1.1.1.11 Next hop: 1.1.1.1	As the post-NAT public addresses do not belong to any interfaces, routing protocols cannot discover such routes. Therefore, you must configure static routes on the router. In most cases, you have to contact the ISP network administrator to configure the static routes.

NAPT Configuration Command



IP Address	10.1.1.X/24
Subnet Mask	255.255.255.0
Default Gateway	10.1.1.1

1. Set the IP addresses of interfaces and assign the interfaces to security zones.

```
interface GigabitEthernet1/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 1.1.1.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet1/0/1
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet1/0/2
```

2. Configure a security policy.

```
security-policy
  rule name policy_sec_1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action permit
```

3. Configure a NAT address pool.

```
nat address-group addressgroup1
 section 0 1.1.1.10 1.1.1.11
```

4. Configure a source NAT policy.

```
nat-policy
  rule name policy_nat_1
    source-zone trust
    destination-zone untrust
    source-address 10.1.1.0 24
    action nat address-group
addressgroup1
```

5. Configure the default route.

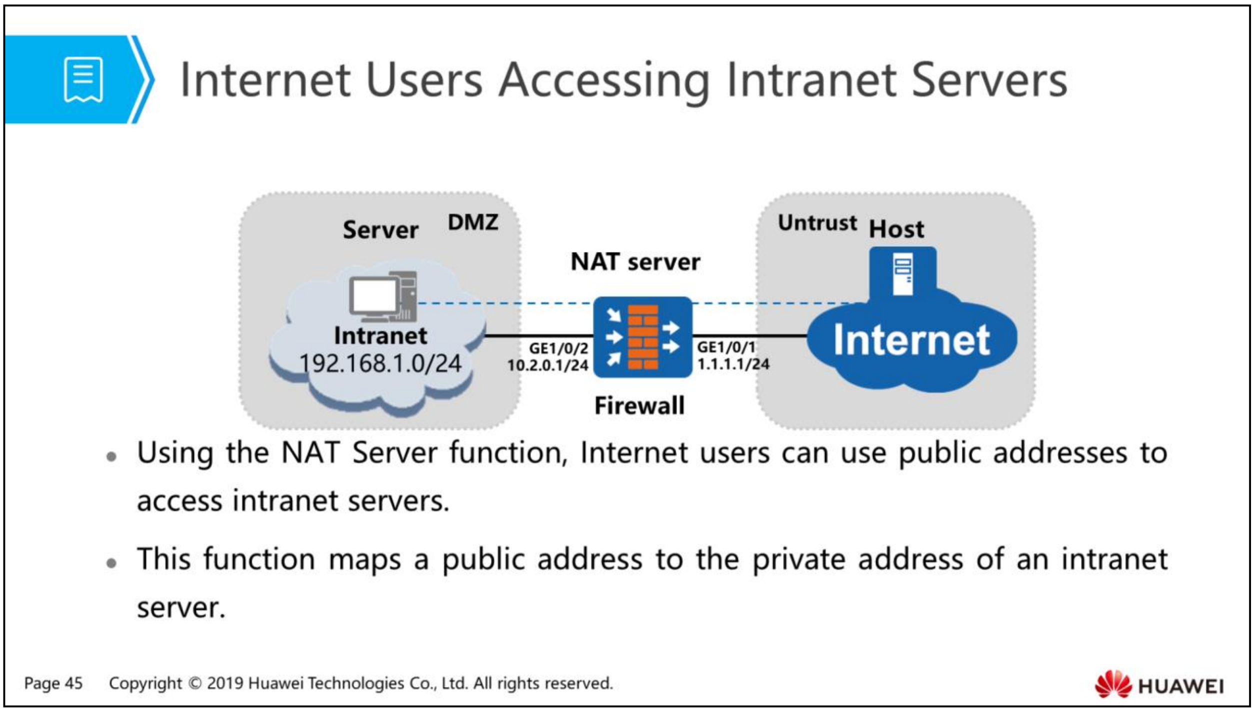
```
ip route-static 0.0.0.0 0.0.0.0
1.1.1.254
```

6. Configure black-hole routes.

```
ip route-static 1.1.1.10
255.255.255.255 NULL0 ip route-static
1.1.1.11 255.255.255.255 NULL0
```

Contents

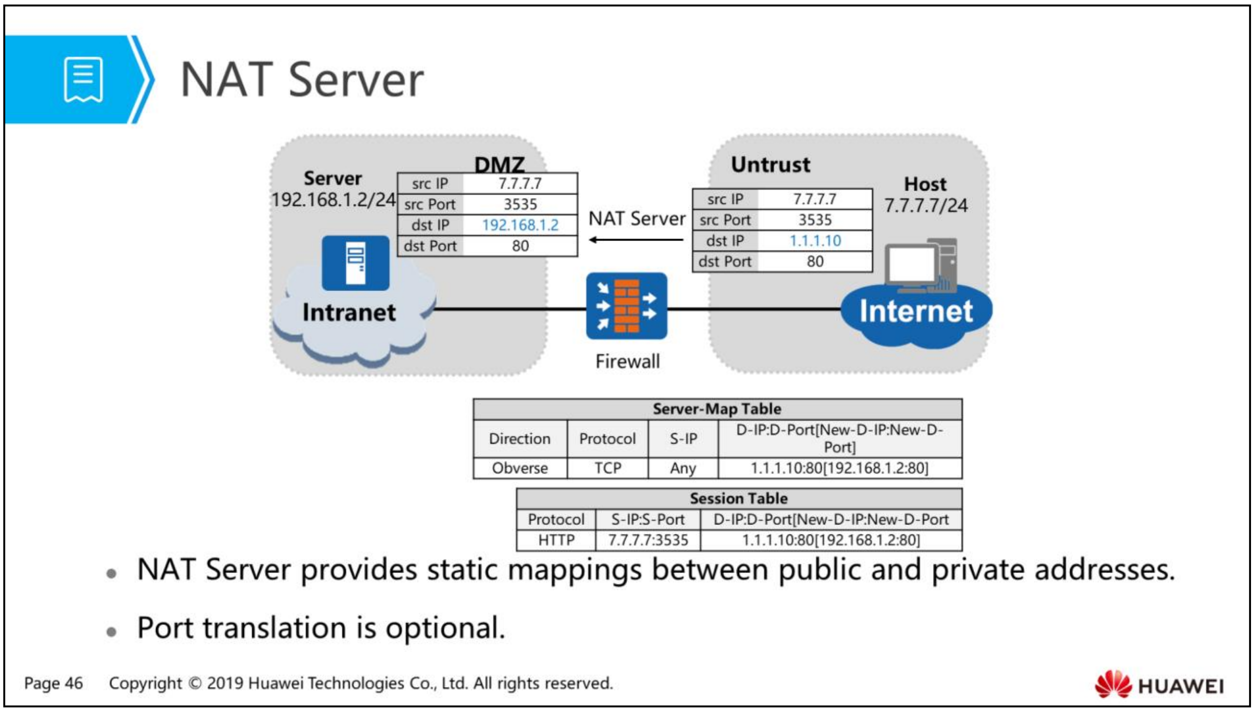
1. Firewall Basic Knowledge
2. **NAT**
   - Private Network Users Accessing the Internet
   - Internet Users Accessing Intranet Servers
3. Attack Defense



Internet Users Accessing Intranet Servers

- Using the NAT Server function, Internet users can use public addresses to access intranet servers.
- This function maps a public address to the private address of an intranet server.

- Using the NAT Server function, Internet users can use public addresses to access intranet servers.
- Some customers, like schools and enterprises, need to provide servers such as web and FTP servers for extranet users to access. Such servers usually reside on private networks. The NAT Server function enables extranet users to access intranet servers.
- As shown in the figure, the firewall provides the NAT Server function, which maps a public IP address to the private IP address of an internal server. The public IP address is an entrance for extranet users to access the internal server.



NAT Server

src IP	7.7.7.7
src Port	3535
dst IP	192.168.1.2
dst Port	80

src IP	7.7.7.7
src Port	3535
dst IP	1.1.1.10
dst Port	80

Server-Map Table

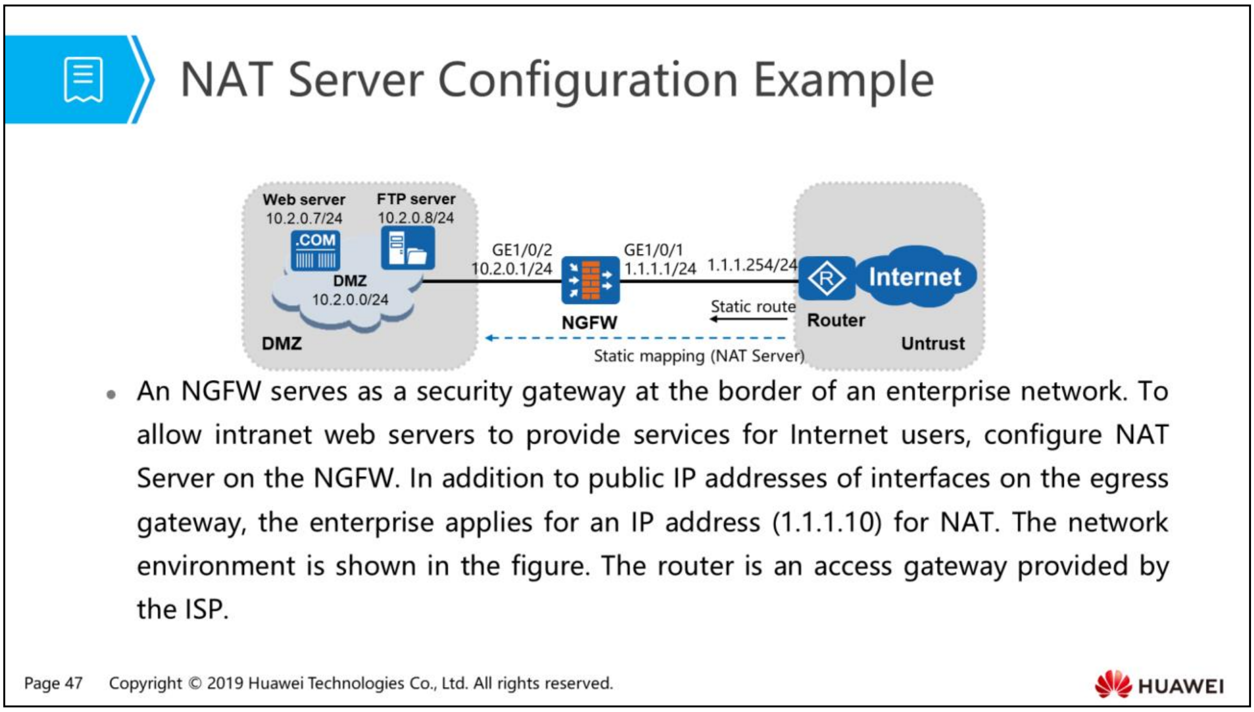
Direction	Protocol	S-IP	D-IP:D-Port[New-D-IP:New-D-Port]
Obverse	TCP	Any	1.1.1.10:80[192.168.1.2:80]

Session Table

Protocol	S-IP:S-Port	D-IP:D-Port[New-D-IP:New-D-Port
HTTP	7.7.7.7:3535	1.1.1.10:80[192.168.1.2:80]

- NAT Server provides static mappings between public and private addresses.
- Port translation is optional.

- For the sake of security, external networks are generally prohibited from proactively accessing internal networks. However, occasionally, a method is expected to permit access from extranets. For example, a company intends to provide resources for customers and employees on business trips. The NAT Server function translates the destination IP addresses in packets. It maps public IP addresses to private ones, and translates public addresses into private ones based on the mappings.
- After the NAT server is configured, Internet users can initiate access requests to the intranet server. The IP addresses and ports of the users are unknown, but the IP address of the intranet server and the port are known. Therefore, after NAT Server is successfully configured, the device automatically generates the server-map entry to save the mapping relationship between the public and private IP addresses. The device translates the IP address of the packet and forwards the packet according to the mapping relationship. A pair of forward and return static server-map entries is generated for each valid NAT Server configuration. The entries exist until static mapping configuration is deleted.
- By configuring NAT Server on the firewall, mappings are established between public and private addresses. After the configuration, the firewall automatically generates server-map entries, indicating the mappings between public and private addresses.
- As shown in the figure, when the host accesses the server, the firewall does the following processing:
  - When receiving a packet destined for 1.1.1.10 from an Internet user, the firewall searches the server-map table and finds a match, and then translates the destination IP address to 192.168.1.2.
  - The firewall checks the destination IP address, identifying that the packet is destined for the DMZ from the Untrust zone. If the packet matches and is permitted by an interzone security policy, the firewall searches for a matching NAT policy and then finds out that address translation is required.
  - Upon receiving the packet that the server replies to the host, the firewall searches the session table, and the entry created in the previous step is matched. Accordingly, the firewall changes the source address in the packet to 1.1.1.10, and then forwards the packet to the Internet.
  - When receiving subsequent packets sent from the host to the server, the firewall directly translates them according to session entries, instead of searching for server-map entries.
- In addition, the firewall can determine whether to translate ports during address translation and whether to allow servers to use public addresses to access the Internet, to meet the requirements of different scenarios.

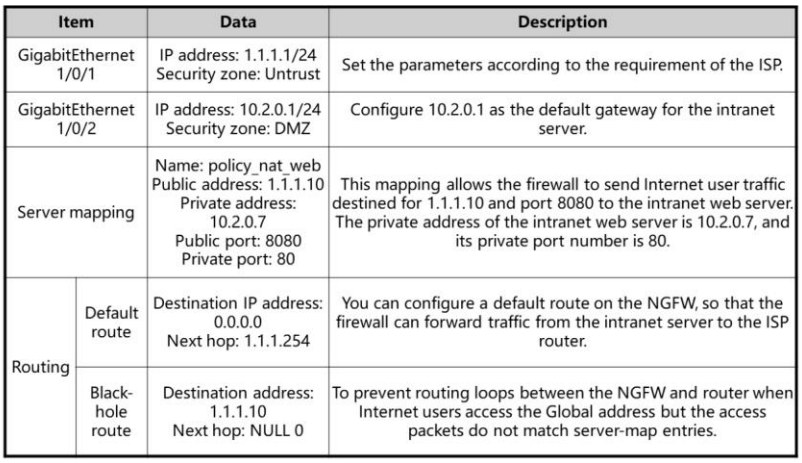


NAT Server Configuration Example

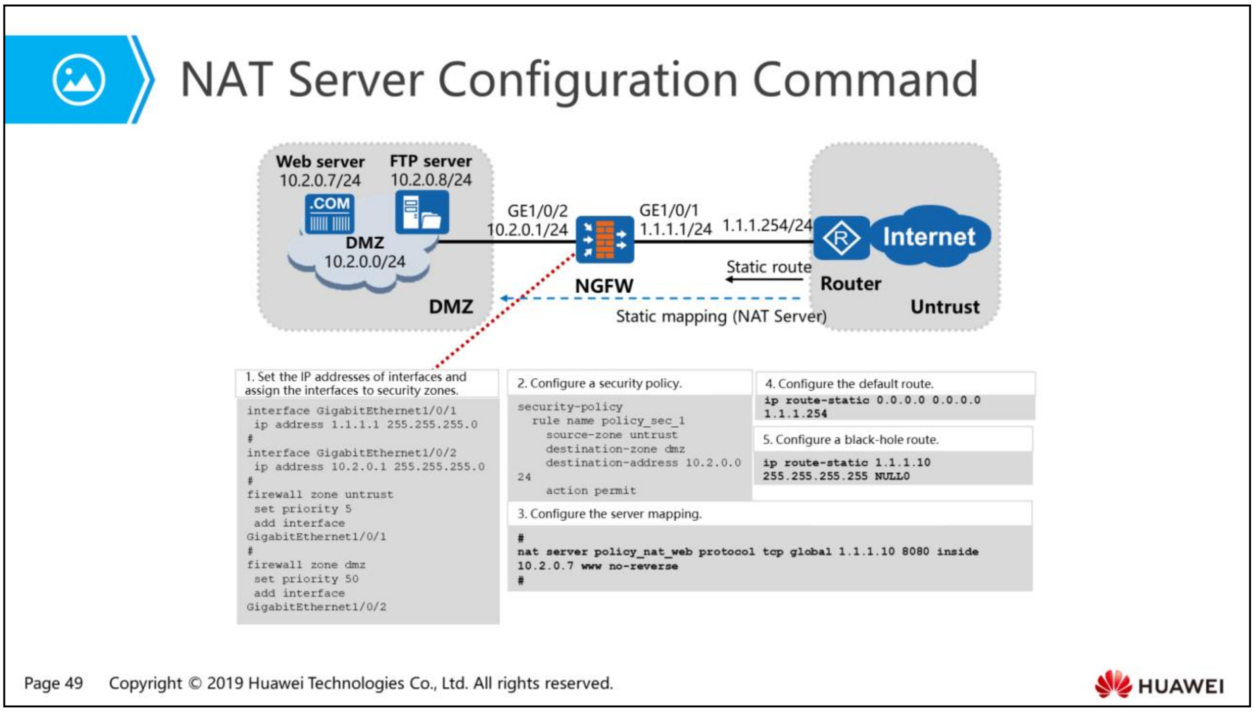
- An NGFW serves as a security gateway at the border of an enterprise network. To allow intranet web servers to provide services for Internet users, configure NAT Server on the NGFW. In addition to public IP addresses of interfaces on the egress gateway, the enterprise applies for an IP address (1.1.1.10) for NAT. The network environment is shown in the figure. The router is an access gateway provided by the ISP.

- Configuration roadmap:
  - 1. Set interface IP addresses and assign the interfaces to security zones.
  - 2. Configure security policies to allow external users to access internal servers.
  - 3. Configure NAT Server. Create static mapping to map the intranet web server.
  - 4. Configure default routes on the NGFW, so that the NGFW can forward private traffic to the ISP router.
  - 5. Configure a black-hole route on the NGFW to prevent routing loops between the NGFW and router.
  - 6. Configure a static route to the public address mapped to the server on the router.

Data Planning



Item		Data	Description
GigabitEthernet 1/0/1		IP address: 1.1.1.1/24 Security zone: Untrust	Set the parameters according to the requirement of the ISP.
GigabitEthernet 1/0/2		IP address: 10.2.0.1/24 Security zone: DMZ	Configure 10.2.0.1 as the default gateway for the intranet server.
Server mapping		Name: policy_nat_web Public address: 1.1.1.10 Private address: 10.2.0.7 Public port: 8080 Private port: 80	This mapping allows the firewall to send Internet user traffic destined for 1.1.1.10 and port 8080 to the intranet web server. The private address of the intranet web server is 10.2.0.7, and its private port number is 80.
Routing	Default route	Destination IP address: 0.0.0.0 Next hop: 1.1.1.254	You can configure a default route on the NGFW, so that the firewall can forward traffic from the intranet server to the ISP router.
	Black-hole route	Destination address: 1.1.1.10 Next hop: NULL 0	To prevent routing loops between the NGFW and router when Internet users access the Global address but the access packets do not match server-map entries.



NAT Server Configuration Command

1. Set the IP addresses of interfaces and assign the interfaces to security zones.

```
interface GigabitEthernet1/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 10.2.0.1 255.255.255.0
#
firewall zone untrust
 set priority 5
 add interface
GigabitEthernet1/0/1
#
firewall zone dmz
 set priority 50
 add interface
GigabitEthernet1/0/2
```

2. Configure a security policy.

```
security-policy
  rule name policy_sec_1
    source-zone untrust
    destination-zone dmz
    destination-address 10.2.0.0
24
    action permit
```

3. Configure the server mapping.

```
#
nat server policy_nat_web protocol tcp global 1.1.1.10 8080 inside
10.2.0.7 www no-reverse
#
```

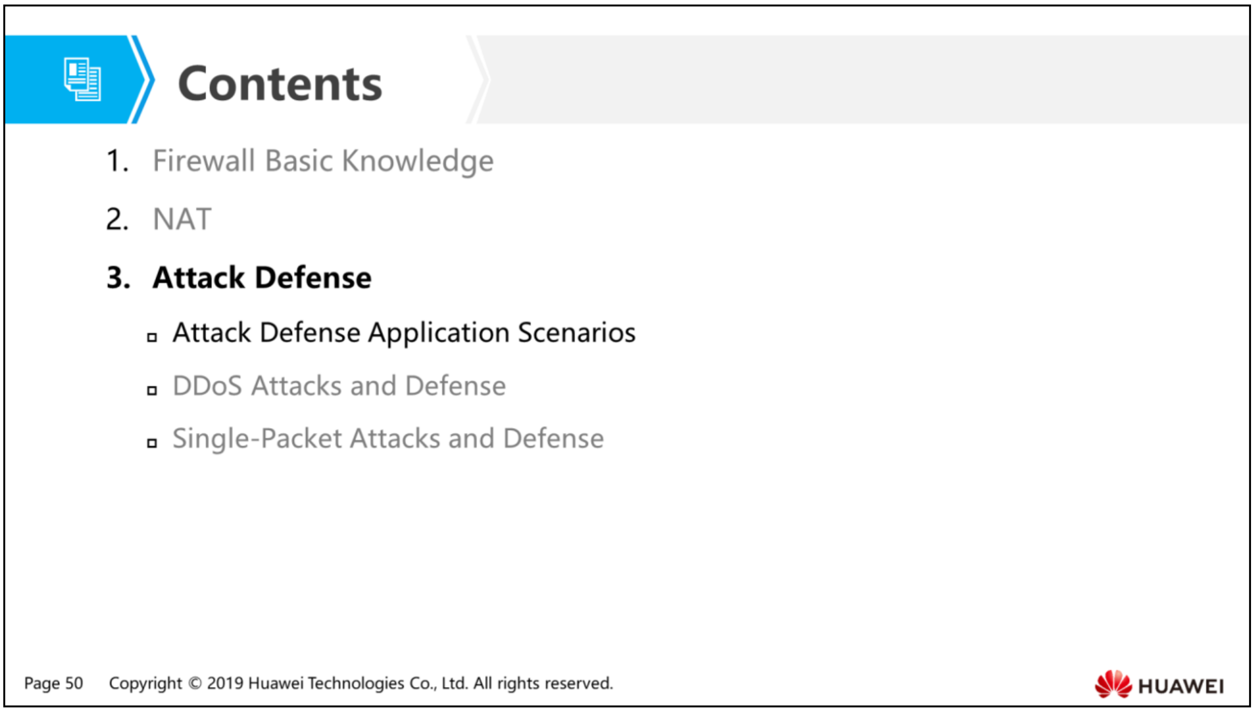
4. Configure the default route.

```
ip route-static 0.0.0.0 0.0.0.0
1.1.1.254
```

5. Configure a black-hole route.

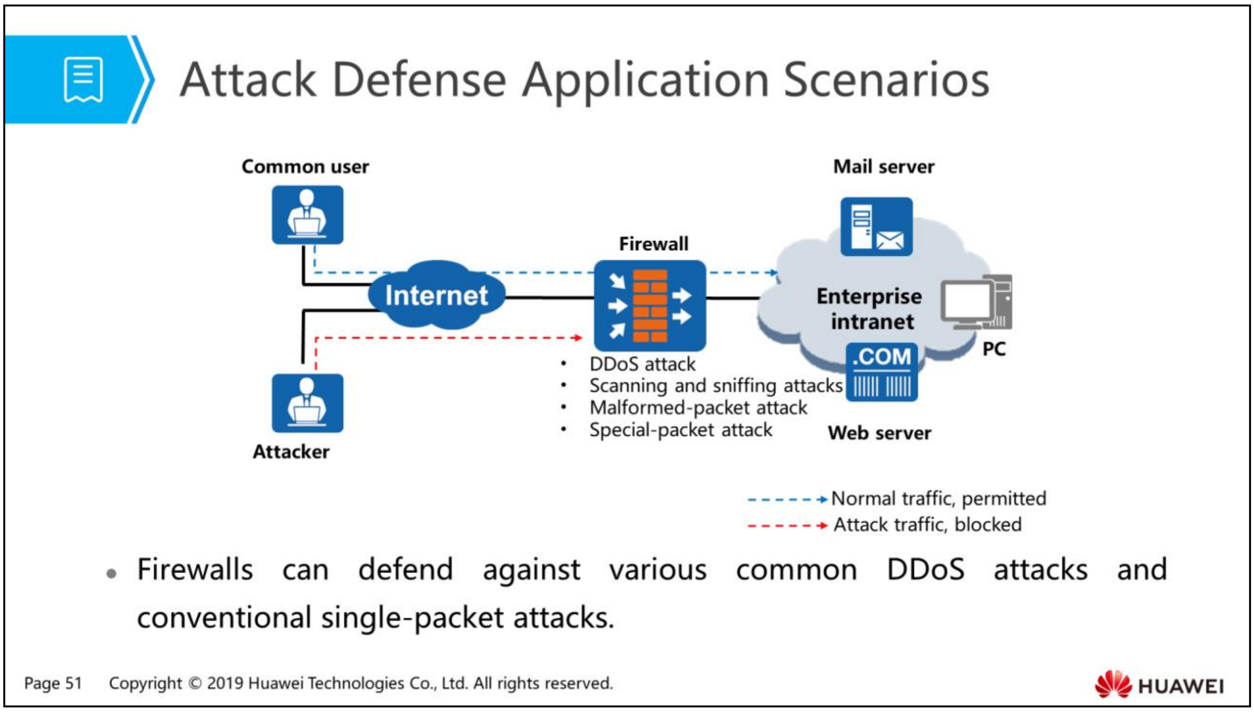
```
ip route-static 1.1.1.10
255.255.255.255 NULL0
```

- In the scenario in which an intranet server advertises multiple public IP addresses for Internet users, if the interfaces with the multiple IP addresses reside in different security zones, you can configure NAT Server to advertise different public IP addresses based on the security zones. If the interfaces with these IP addresses reside in the same security zones, you can configure NAT Server with parameter no-reverse. After you specify the no-reverse parameter, you can map multiple global IP addresses with one inside IP address.
- In addition, after you specify the no-reverse parameter, the server-map table generated by the firewall applies only to the forward direction. When the intranet server proactively accesses the Internet, the firewall cannot translate the private IP address of the intranet server to a public IP address. Therefore, the intranet server fails to initiate access to the Internet. Therefore, you can specify the no-reverse parameter to prevent intranet servers from initiating access to the Internet.



Contents

1. Firewall Basic Knowledge
2. NAT
3. **Attack Defense**
   - Attack Defense Application Scenarios
   - DDoS Attacks and Defense
   - Single-Packet Attacks and Defense



Attack Defense Application Scenarios

- DDoS attack
- Scanning and sniffing attacks
- Malformed-packet attack
- Special-packet attack

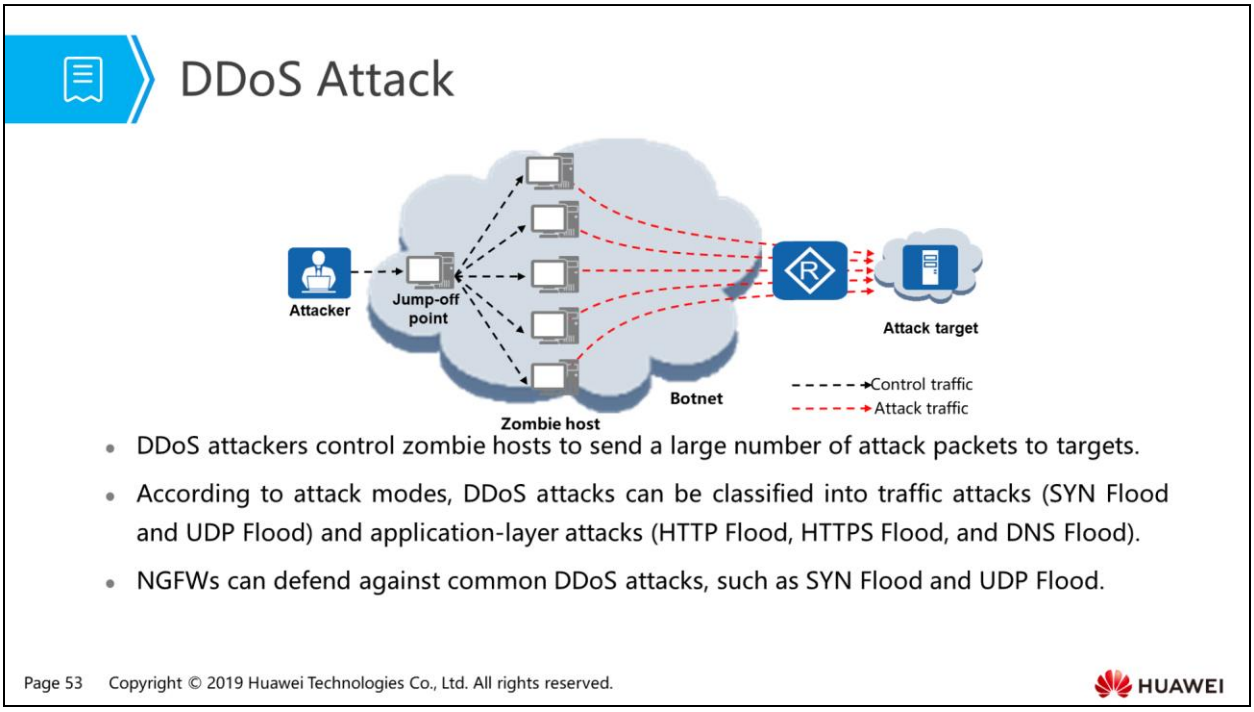
- Firewalls can defend against various common DDoS attacks and conventional single-packet attacks.

Page 51

- Servers are deployed in most large and medium-sized enterprises and data centers, and the servers (such as mail and web servers) are probably attacked. Currently, most targeted attacks are DDoS attacks, such as SYN flood, UDP flood, ICMP flood, HTTP flood, HTTPS flood, DNS flood, and SIP flood. These DDoS attacks cause network congestions and severely threaten servers, causing the servers unable to provide services or even broken down.
- Deploying firewalls on the egresses of previous networks can effectively defend against common DDoS attacks and conventional single-packet attacks.
- After being deployed at the enterprise network egress and enabled with the attack defense function, a firewall permits service traffic and blocks attack traffic. The attack defense function protects intranet servers and PCs. Here, we mainly describe the configuration for defending against common single-packet attacks.

Contents

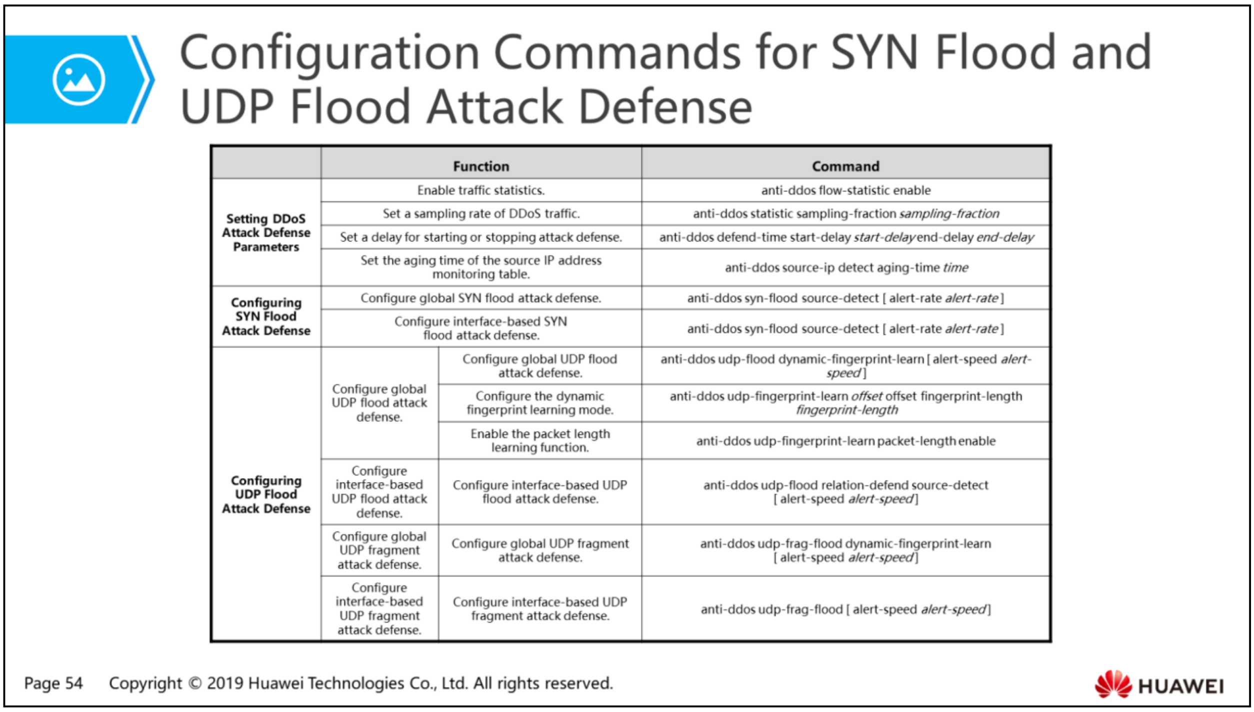
1. Firewall Basic Knowledge
2. NAT
3. **Attack Defense**
   - Attack Defense Application Scenarios
   - DDoS Attacks and Defense
   - Single-Packet Attacks and Defense



DDoS Attack

- DDoS attackers control zombie hosts to send a large number of attack packets to targets.
- According to attack modes, DDoS attacks can be classified into traffic attacks (SYN Flood and UDP Flood) and application-layer attacks (HTTP Flood, HTTPS Flood, and DNS Flood).
- NGFWs can defend against common DDoS attacks, such as SYN Flood and UDP Flood.

- An attacker launches Distributed Denial of Service (DDoS) attacks by controlling many zombie hosts to send a large number of attack packets to the attack target. As a result, links are congested, and system resources are exhausted on the attacked network. In this case, the attack target fails to provide services for legitimate users.
- As shown in the figure, the attacker resorts to every possible means to control a large number of online hosts. These controlled hosts are called zombie hosts, and the network consisting of the attacker and zombie hosts is called a botnet. After locking a target, the attacker controls zombie hosts to send a large number of attack packets to the target, congesting the target network and exhausting system resources.
- Currently, the Internet has many zombie hosts and botnets. Driven by profits, DDoS attacks become a major security threat to the Internet.
- There are multiple types of DDoS attacks. NGFWs can defend against common DDoS attacks: SYN Flood, UDP Flood, ICMP Flood, HTTP Flood, HTTPS Flood, DNS Flood, and SIP Flood.



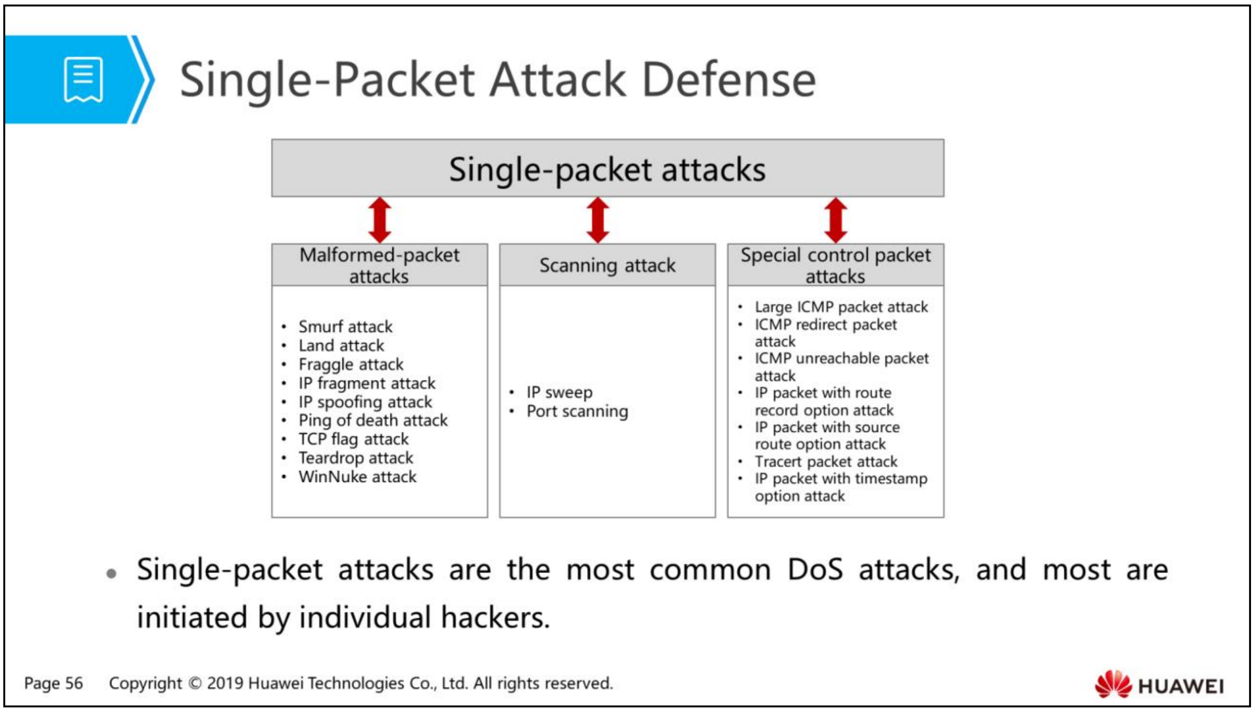
Configuration Commands for SYN Flood and UDP Flood Attack Defense

	Function		Command
Setting DDoS Attack Defense Parameters	Enable traffic statistics.		anti-ddos flow-statistic enable
	Set a sampling rate of DDoS traffic.		anti-ddos statistic sampling-fraction *sampling-fraction*
	Set a delay for starting or stopping attack defense.		anti-ddos defend-time start-delay *start-delay*end-delay *end-delay*
	Set the aging time of the source IP address monitoring table.		anti-ddos source-ip detect aging-time *time*
Configuring SYN Flood Attack Defense	Configure global SYN flood attack defense.		anti-ddos syn-flood source-detect [alert-rate *alert-rate*]
	Configure interface-based SYN flood attack defense.		anti-ddos syn-flood source-detect [alert-rate *alert-rate*]
Configuring UDP Flood Attack Defense	Configure global UDP flood attack defense.	Configure global UDP flood attack defense.	anti-ddos udp-flood dynamic-fingerprint-learn [alert-speed *alert-speed*]
		Configure the dynamic fingerprint learning mode.	anti-ddos udp-fingerprint-learn *offset* offset fingerprint-length *fingerprint-length*
		Enable the packet length learning function.	anti-ddos udp-fingerprint-learn packet-length enable
	Configure interface-based UDP flood attack defense.	Configure interface-based UDP flood attack defense.	anti-ddos udp-flood relation-defend source-detect [alert-speed *alert-speed*]
	Configure global UDP fragment attack defense.	Configure global UDP fragment attack defense.	anti-ddos udp-frag-flood dynamic-fingerprint-learn [alert-speed *alert-speed*]
	Configure interface-based UDP fragment attack defense.	Configure interface-based UDP fragment attack defense.	anti-ddos udp-frag-flood [alert-speed *alert-speed*]

- Set DDoS attack defense parameters before enabling DDoS attack defense.
- Here provides only configuration commands for defending against SYN flood and UDP flood attacks. For configuration commands and precautions against other DDoS attacks, see the product documentation of the corresponding firewall model.

Contents

1. Firewall Basic Knowledge
2. NAT
3. **Attack Defense**
   - Attack Defense Application Scenarios
   - DDoS Attacks and Defense
   - Single-Packet Attacks and Defense



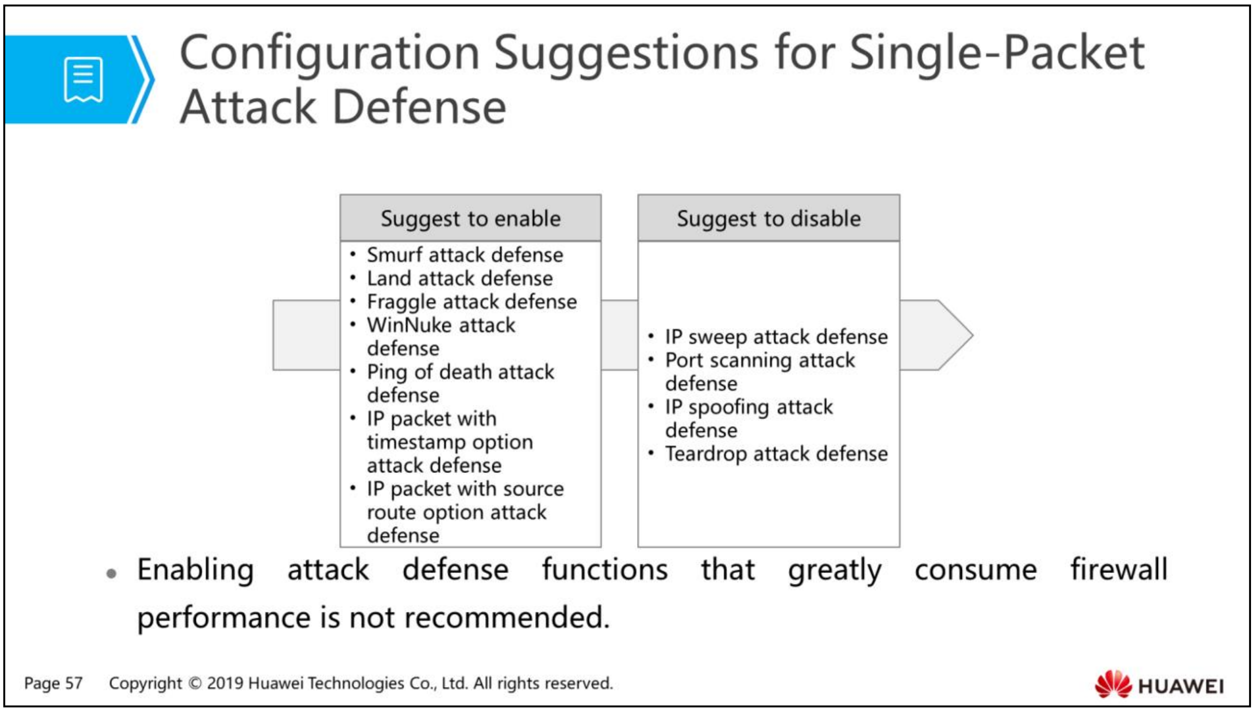
Single-Packet Attack Defense

Single-packet attacks

Malformed-packet attacks	Scanning attack	Special control packet attacks
• Smurf attack • Land attack • Fraggle attack • IP fragment attack • IP spoofing attack • Ping of death attack • TCP flag attack • Teardrop attack • WinNuke attack	• IP sweep • Port scanning	• Large ICMP packet attack • ICMP redirect packet attack • ICMP unreachable packet attack • IP packet with route record option attack • IP packet with source route option attack • Tracert packet attack • IP packet with timestamp option attack

- Single-packet attacks are the most common DoS attacks, and most are initiated by individual hackers.

- The most common DoS attacks are single-packet attacks. Such attacks are often initiated by individual hackers. As attack packets are simplex, it is easy to defend against such attacks once grasping attack characteristics.
- Single-packet attacks include scanning, malformed-packet, and special packet attacks.
  - Scanning attacks mainly include IP sweep and port scanning. In an IP sweep attack, the attacker sends IP packets such as TCP, UDP, and ICMP packets whose destination addresses change instantly, to find existing hosts and networks. In this manner, the potential attack targets can be detected accurately. Port scanning: An attacker scans TCP and UDP ports to detect the operating system and potential services of the target. Through scanning and sniffing, attackers can roughly understand the types of services that the target provides and potential vulnerabilities for further intrusions.
  - In malformed-packet attacks, the attacker sends defective IP packets to the target system. The target system may encounter errors or crash when handling such packets. Such malformed packet attacks mainly include Ping-of-Death attacks and Teardrop attacks.
  - The attacker of special packet attacks uses legitimate packets to probe network environment. Special packets are legitimate but rarely used on networks. Typical special packet attacks include large ICMP packet control and tracert and timestamp option IP packet control.
- Defense against single-packet attacks is a basic defense function of firewalls. Huawei full-series firewalls can defend against single-packet attacks.

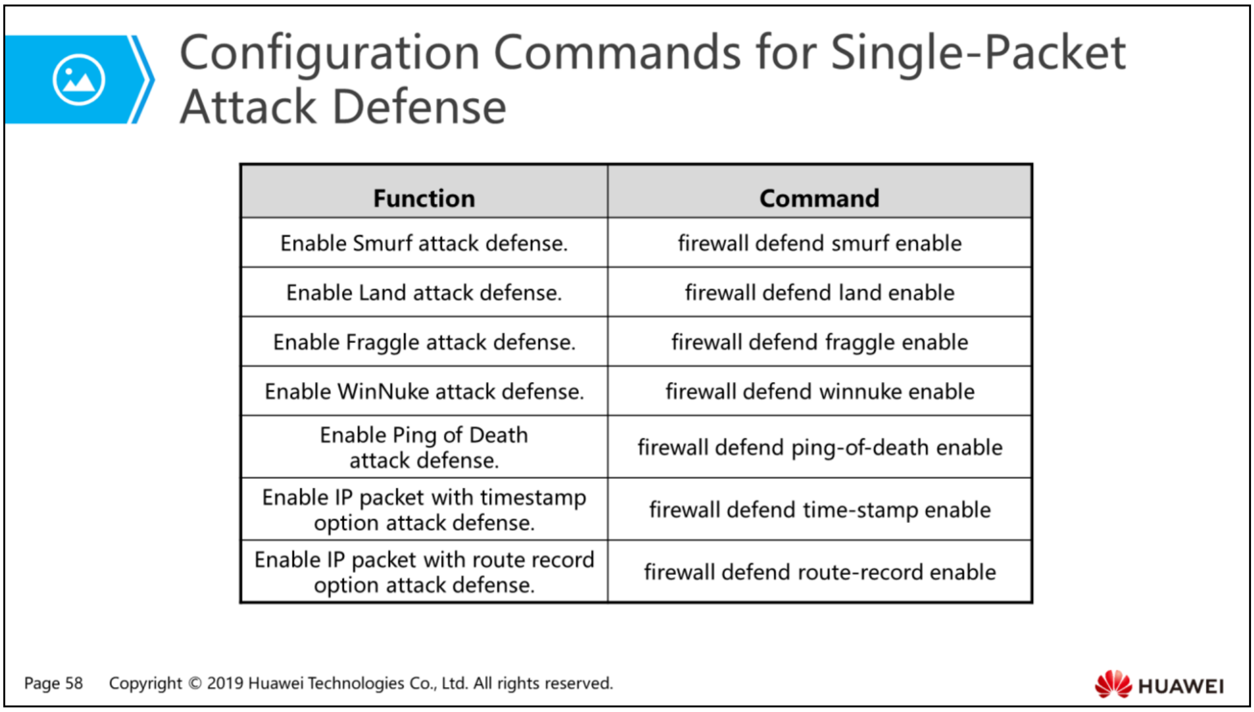


Configuration Suggestions for Single-Packet Attack Defense

Suggest to enable	Suggest to disable
• Smurf attack defense • Land attack defense • Fraggle attack defense • WinNuke attack defense • Ping of death attack defense • IP packet with timestamp option attack defense • IP packet with source route option attack defense	• IP sweep attack defense • Port scanning attack defense • IP spoofing attack defense • Teardrop attack defense

- Enabling attack defense functions that greatly consume firewall performance is not recommended.

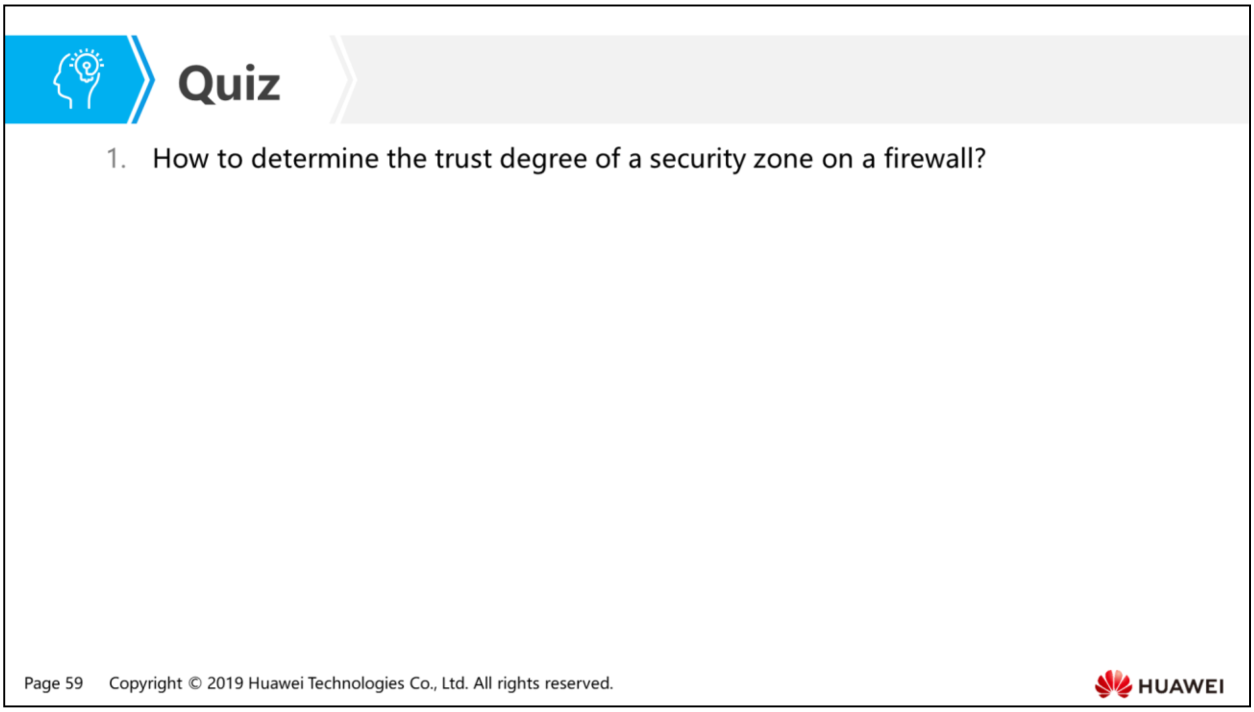
- Single-packet attack defense functions that are recommended to enable are against common attacks. After such defense functions are enabled, firewalls can effectively defend against attacks, and firewall performance is not greatly affected. Scanning attack defense greatly consumes firewall performance. Therefore, enabling this function is not recommended.



Configuration Commands for Single-Packet Attack Defense

Function	Command
Enable Smurf attack defense.	firewall defend smurf enable
Enable Land attack defense.	firewall defend land enable
Enable Fraggle attack defense.	firewall defend fraggle enable
Enable WinNuke attack defense.	firewall defend winnuke enable
Enable Ping of Death attack defense.	firewall defend ping-of-death enable
Enable IP packet with timestamp option attack defense.	firewall defend time-stamp enable
Enable IP packet with route record option attack defense.	firewall defend route-record enable

- Only configuration commands are provided here. For detailed configuration precautions, see the product documentation of the corresponding firewall model.



Quiz

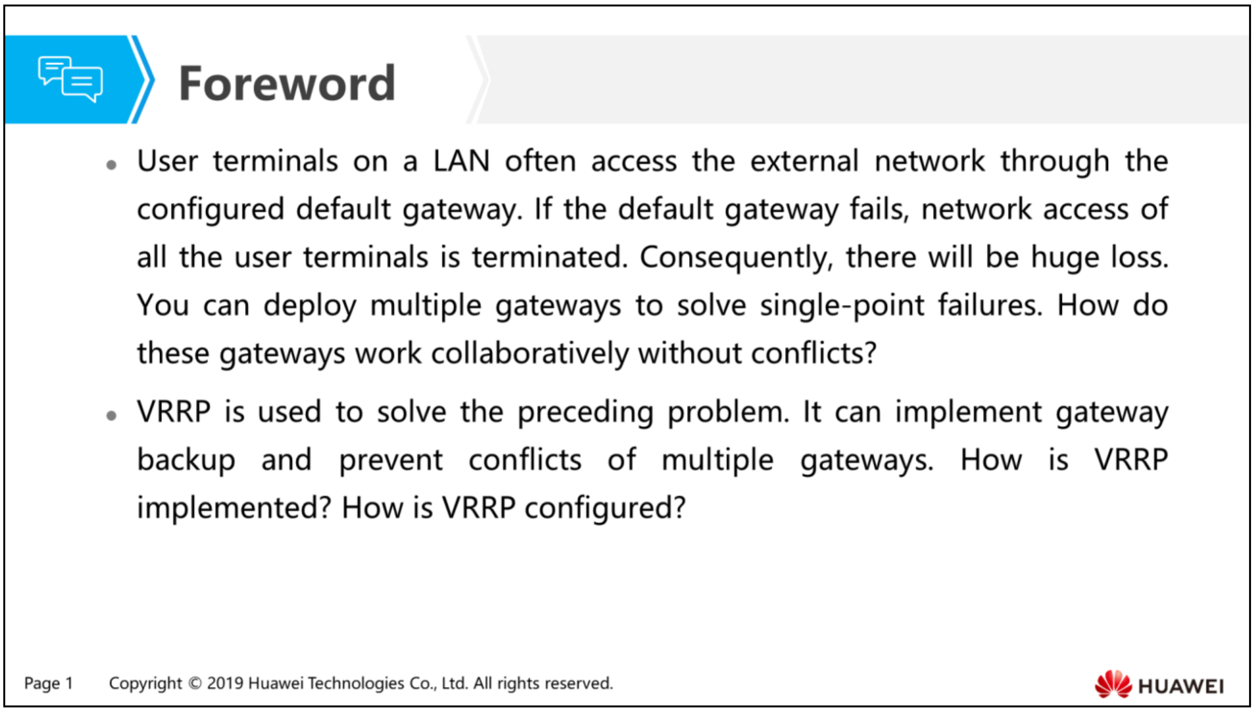
1. How to determine the trust degree of a security zone on a firewall?

- Answer: On a Huawei firewall, each security zone has a unique security level, indicated by a number ranging from 1 to 100. A greater number indicates a more trusted security zone. For default security zones, their security levels are fixed: 100 for the Local zone, 85 for the Trust zone, 50 for the DMZ, and 5 for the Untrust zone.

Thank You

www.huawei.com

VRRP Principles and Configurations



Foreword

- User terminals on a LAN often access the external network through the configured default gateway. If the default gateway fails, network access of all the user terminals is terminated. Consequently, there will be huge loss. You can deploy multiple gateways to solve single-point failures. How do these gateways work collaboratively without conflicts?
- VRRP is used to solve the preceding problem. It can implement gateway backup and prevent conflicts of multiple gateways. How is VRRP implemented? How is VRRP configured?

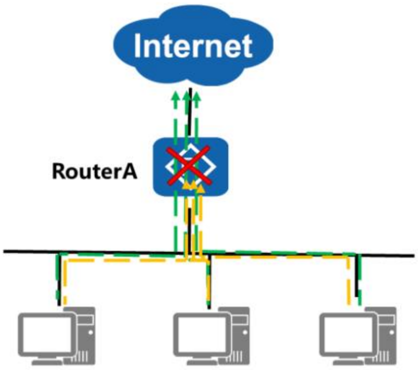
Objectives

- Upon completion of this section, you will be able to:
  - Master VRRP principles
  - Understand the VRRP active/standby switchover
  - Master VRRP configurations

Contents

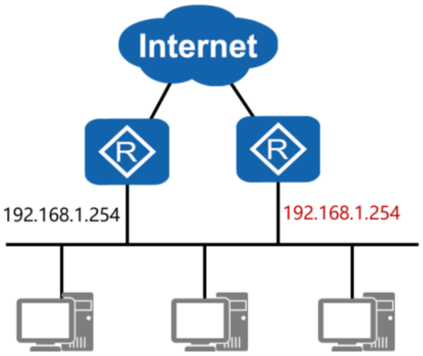
1. **VRRP Background and Overview**
2. VRRP Active/Standby Switchover
3. VRRP Load Balancing
4. Basic VRRP Configuration

Limitations of a Single Gateway

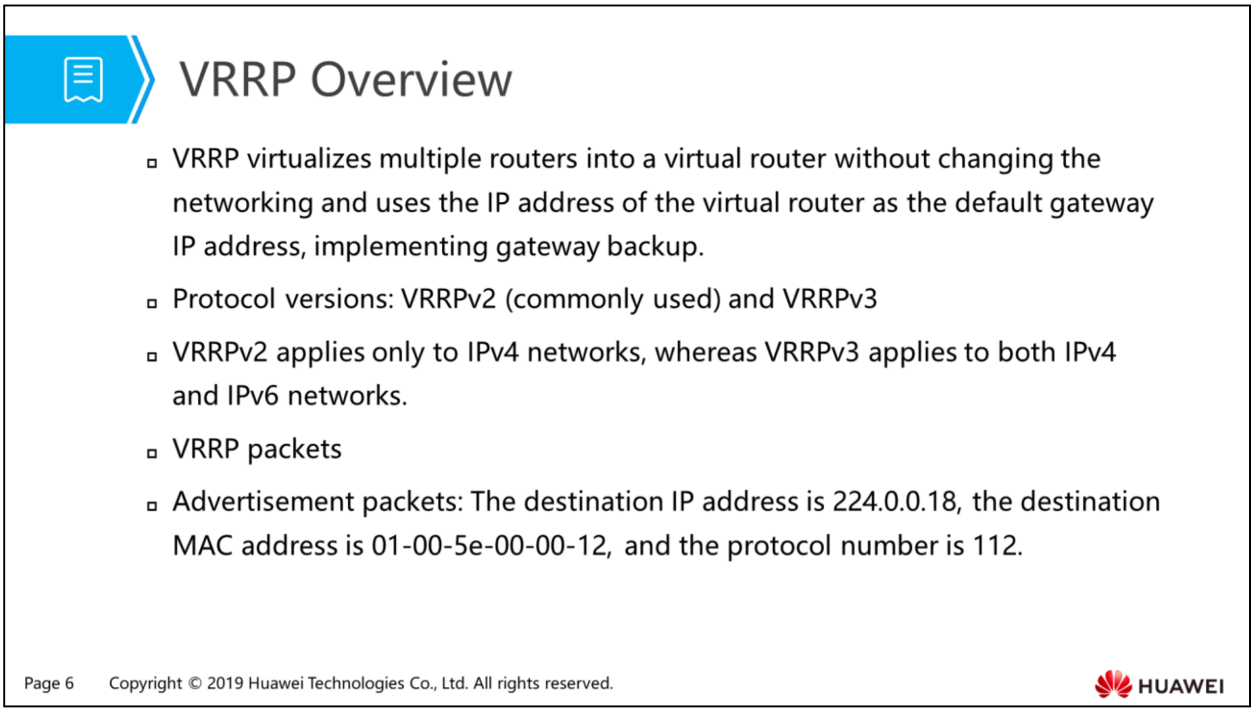


- When RouterA fails, the devices that use RouterA as the gateway cannot communicate with the Internet.

Problems of Multiple Gateways

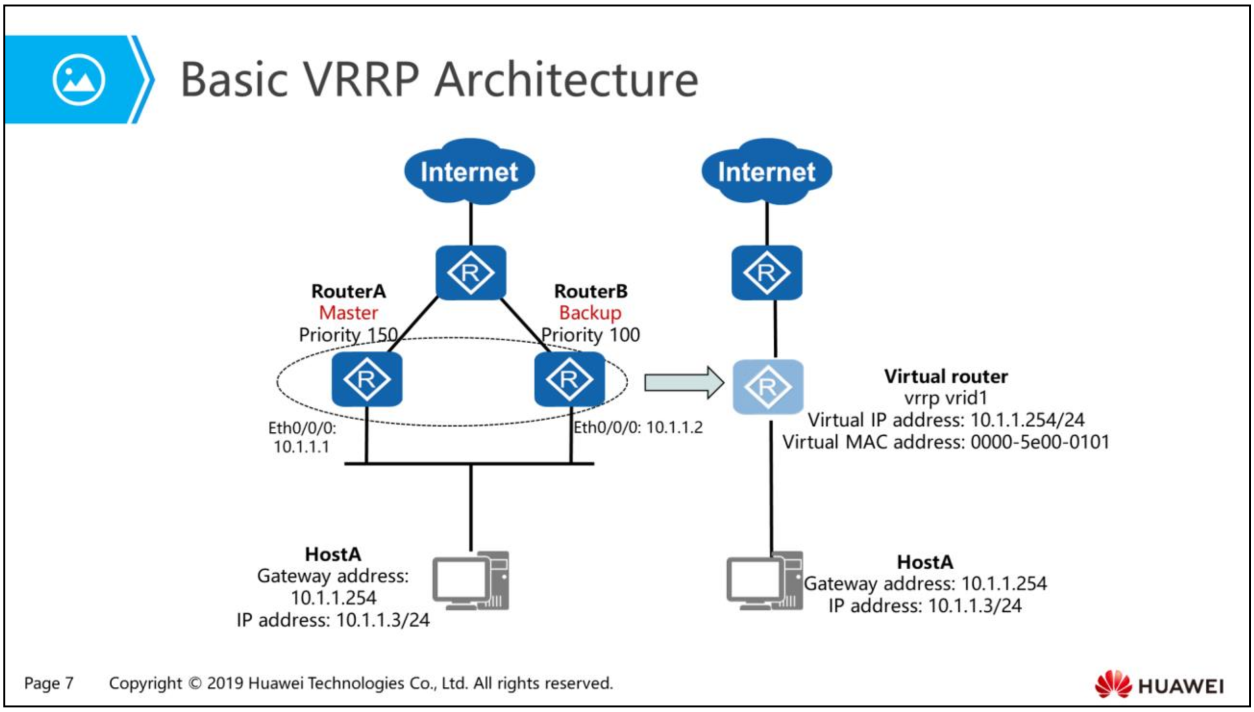


- Multiple gateways can be deployed to implement gateway backup.
- However, many problems may occur. IP addresses of gateways conflict, and hosts frequently use different egresses.



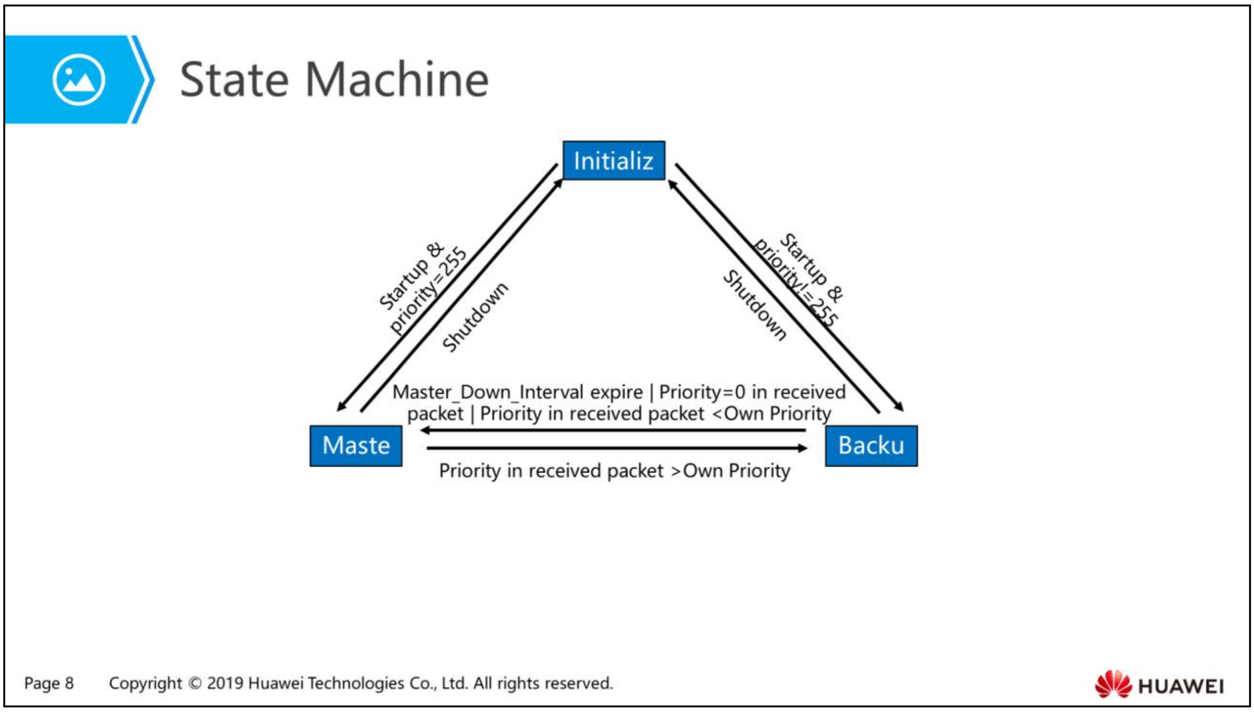
VRRP Overview

- VRRP virtualizes multiple routers into a virtual router without changing the networking and uses the IP address of the virtual router as the default gateway IP address, implementing gateway backup.
- Protocol versions: VRRPv2 (commonly used) and VRRPv3
- VRRPv2 applies only to IPv4 networks, whereas VRRPv3 applies to both IPv4 and IPv6 networks.
- VRRP packets
- Advertisement packets: The destination IP address is 224.0.0.18, the destination MAC address is 01-00-5e-00-00-12, and the protocol number is 112.



Basic VRRP Architecture

- Basic concepts of VRRP:
  - VRRP router: device running VRRP. For example, RouterA and RouterB are VRRP routers.
  - Virtual router: VRRP group consisting of one master and multiple backups. The VRRP group's virtual IP address is used as the default gateway address on a LAN. For example, RouterA and RouterB form a virtual router.
  - Virtual router master: VRRP device that forwards packets. RouterA is the virtual router master.
  - Virtual router backup: a group of VRRP devices that do not forward packets. When the master is faulty, a backup with the highest priority becomes the master. RouterB is the virtual router backup.
  - Priority: priority of a device in a VRRP group. The value ranges from 0 to 255.The value 0 indicates that a device does not join a VRRP group and is used to enable the backup to immediately become the master without waiting for the timeout. The value 255 is reserved for the IP address owner and cannot be manually configured. The default value is 100.
  - VRID: virtual router ID. The VRID of the virtual router composed of RouterA and RouterB is 1. The value is manually configured and ranges from 1 to 255.
  - Virtual IP address: IP address of a virtual router. A virtual router can be assigned one or more virtual IP addresses. Virtual IP addresses are configurable. The virtual IP address of the virtual router composed of RouterA and RouterB is 10.1.1.254/24.
  - IP address owner: VRRP device that uses an IP address of a virtual router as the actual interface address. If an IP address owner is available, it always functions as the virtual router master.
  - Virtual MAC address: MAC address that is generated by the virtual router based on the VRID. A virtual router has one virtual MAC address and is in the format of 00-00-5E-00-01-{vrid}.The virtual router sends ARP Reply packets carrying the virtual MAC address but not the interface MAC address. The VRID of the virtual router composed of RouterA and RouterB is 1, so the MAC address of the VRRP group is 00-00-5E-00-01-01.



State Machine

Initializ

Startup & priority=255

Shutdown

Startup & priority!=255

Shutdown

Master_Down_Interval expire | Priority=0 in received packet | Priority in received packet <Own Priority

Maste

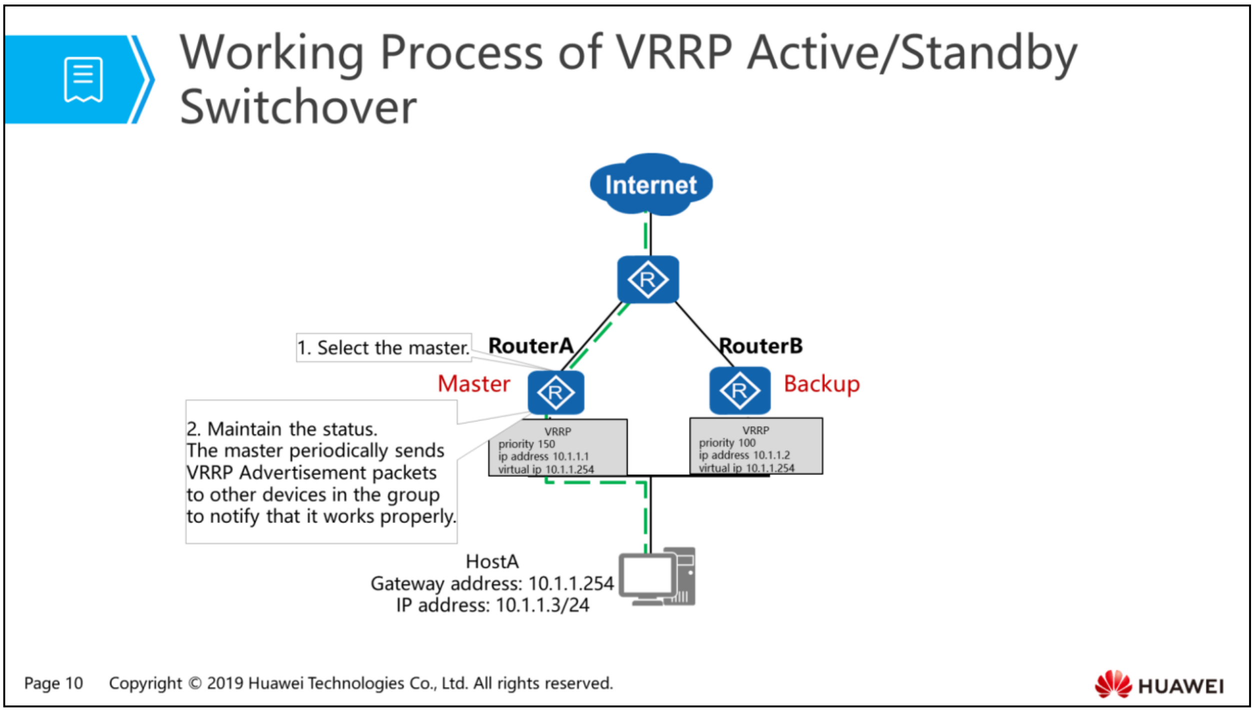
Backu

Priority in received packet >Own Priority

- VRRP defines three statuses: Initialize, Master, and Backup.
- The conditions for state transition are as follows:
  - Initialize->Master: Startup priority=255
  - Initialize->Backup: Startup priority！ =255
  - Master->Initialize: The device is powered off.
  - Master->Backup: The device receives packets with a higher priority than its priority.
  - Backup->Initialize: The device is powered off.
  - Backup->Master: The device does not receive VRRP Advertisement packets within the timeout interval; the priority of the master in the received Advertisement packet is 0; the priority of the master in the received Advertisement packet is lower than its own priority.

Contents

1. VRRP Background and Overview
2. **VRRP Active/Standby Switchover**
3. VRRP Load Balancing
4. Basic VRRP Configuration

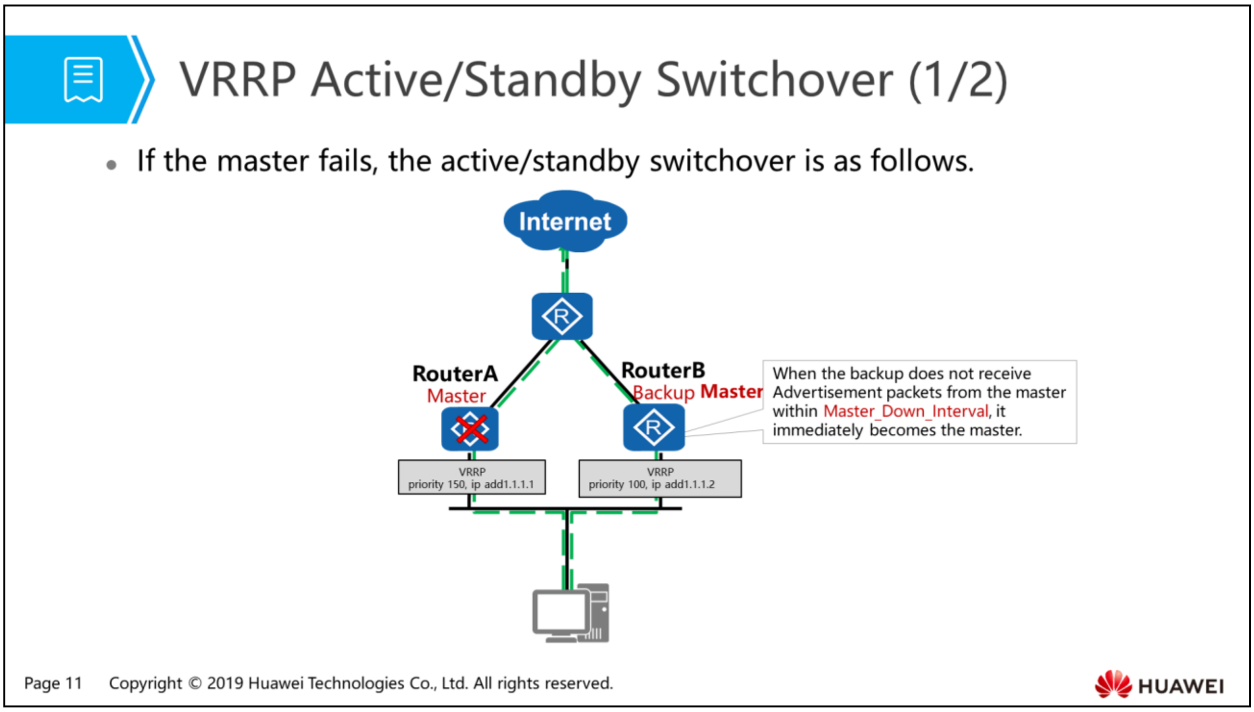


Working Process of VRRP Active/Standby Switchover

1. Select the master.

2. Maintain the status.
The master periodically sends VRRP Advertisement packets to other devices in the group to notify that it works properly.

- The VRRP working process is as follows:
  - Selecting the master
    - VRRP determines the master based on device priorities. The master sends gratuitous ARP packets to notify the connected network devices or hosts of the virtual MAC address of the VRRP group, and forwards packets.
    - Election rule: The device with the highest priority becomes the master. When two devices have the same priority and the master already exists, the master retains its status. If there is no master, the IP addresses are compared. The device with a larger interface IP address becomes the master.
  - Advertising the master status (maintaining the VRRP group status)
    - The master periodically sends VRRP Advertisement packets to advertise its configuration (for example, priority) and running status. The backup determines whether the master works properly based on the received VRRP packets. When the master abandons its role (for example, the master is deleted from the VRRP group), it sends Advertisement packets with the priority of 0. In this case, the backup can rapidly switch to be the master, without waiting for Master_Down_Interval timer. This switching time is called Skew_Time and is calculated as follows:
    - Skew_Time = (256 – Priority of the backup)/256
    - The unit is second.
    - When the master fails and cannot send VRRP Advertisement packets, the backup cannot immediately lean the working status of the master. After Master_Down_Interval expires, the backup considers that the master fails and switches to be the master.
    - Master_Down_Interval = 3 x Advertisement_Interval + Skew_time
    - The unit is second.



VRRP Active/Standby Switchover (1/2)

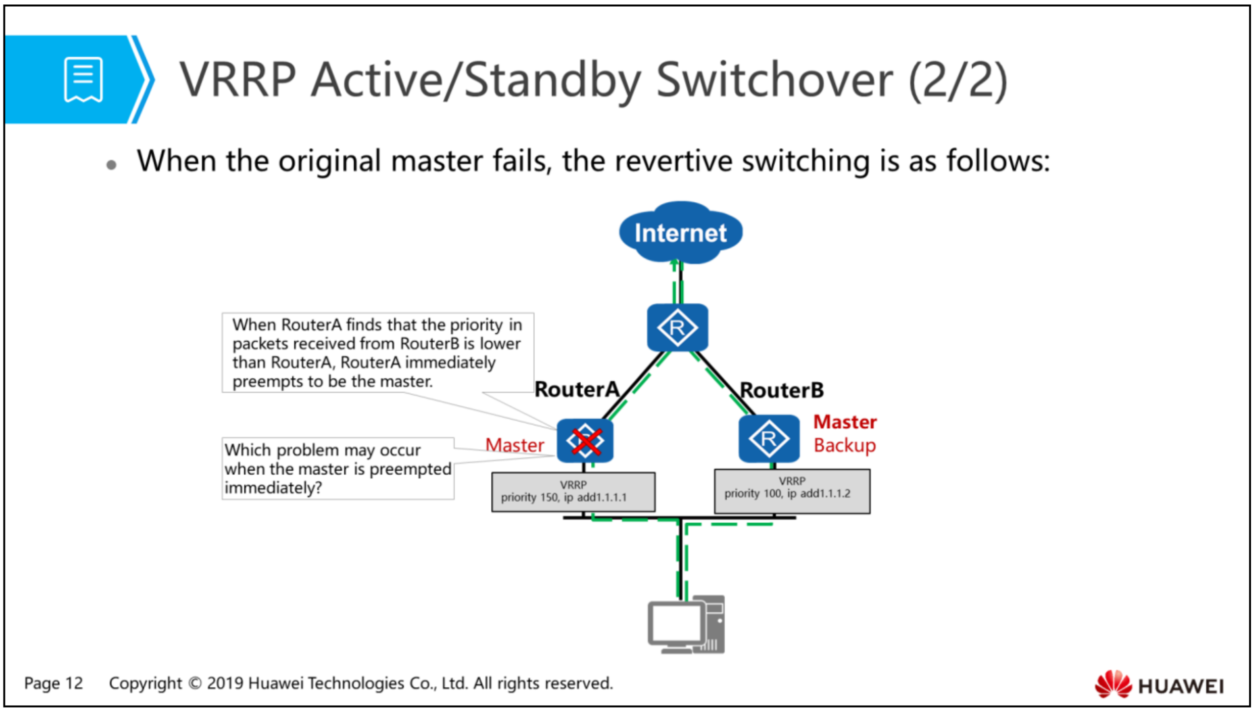
- If the master fails, the active/standby switchover is as follows.

When the backup does not receive Advertisement packets from the master within Master_Down_Interval, it immediately becomes the master.

- The process is as follows when the master fails:
  - If the backup does not receive Advertisement packets after the timer (Master_Down_Interval) expires, the backup becomes the master. The calculation formula is as follows:

    Master_Down_Interval = 3 x Advertisement_Interval + Skew_time

  - When there are multiple backups in a VRRP group, multiple master devices may occur in a short period of time. In this case, the device compares the priority in the received VRRP packets with the local priority and the device with the highest priority becomes the master.
  - After the device becomes the master, it immediately sends gratuitous ARP packets to update MAC address entries so that user traffic is diverted to itself. The process is transparent for users.



VRRP Active/Standby Switchover (2/2)

- When the original master fails, the revertive switching is as follows:

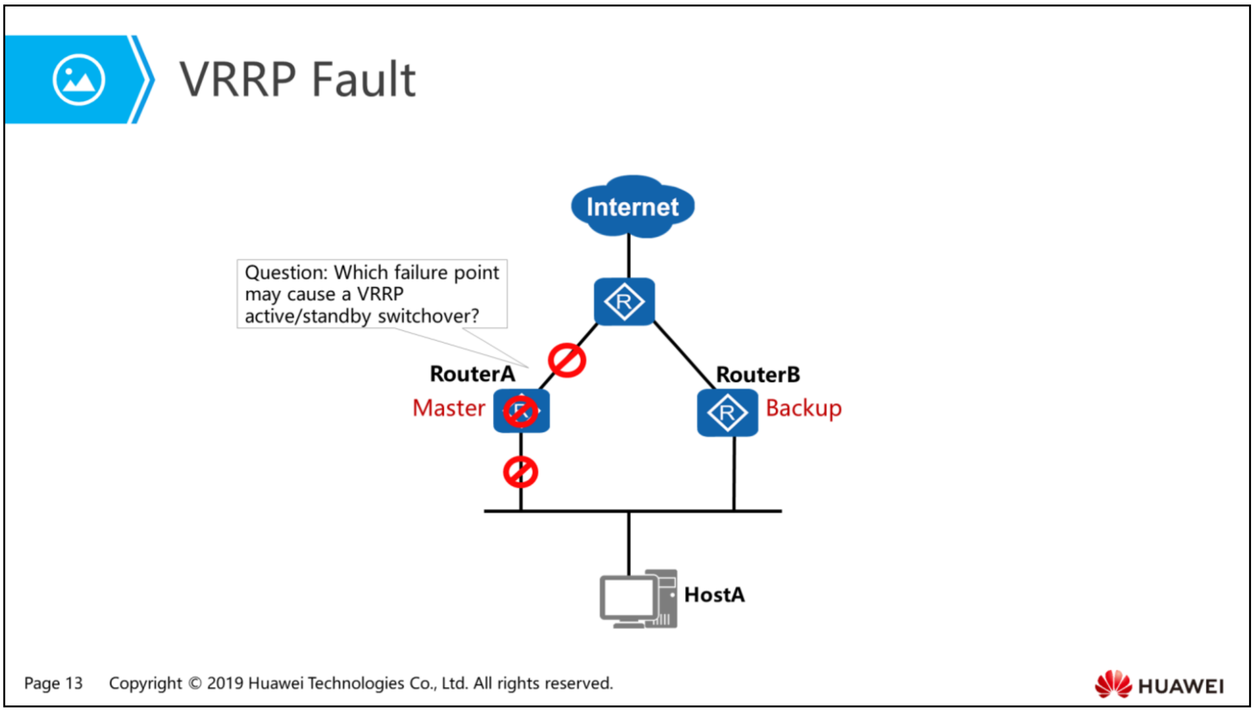
When RouterA finds that the priority in packets received from RouterB is lower than RouterA, RouterA immediately preempts to be the master.

Which problem may occur when the master is preempted immediately?

Page 12

HUAWEI

- Preemption mode:
  - If the priority of a virtual router backup is higher than the priority of the current virtual router master, the virtual router backup automatically becomes the virtual router master. By default, a device works in preemption mode.
  - If the IP address owner is available, it always works in preemption mode and becomes the master.
- Preemption delay:
  - By default, the preemption delay is 0 seconds, indicating immediate preemption.
  - If RouterA immediately preempts to be the master after recovery, traffic may be interrupted. This is because convergence of a routing protocol on the uplink of RouterA is not completed. In this case, the preemption delay needs to be configured.
  - on an unstable network, the backup may not receive packets from the master within Master_Down_Interval due to congestion. The backup switches to be the master. When packets from the original master reach the new master, the new master switches to be the backup. Consequently, members of the VRRP group frequently switch their statuses. To resolve this issue, you can configure the preemption delay so that the backup waits for Master_Down_Interval and preemption delay. If the backup does not receive VRRP Advertisement packets during this period, the backup switches to be the master.

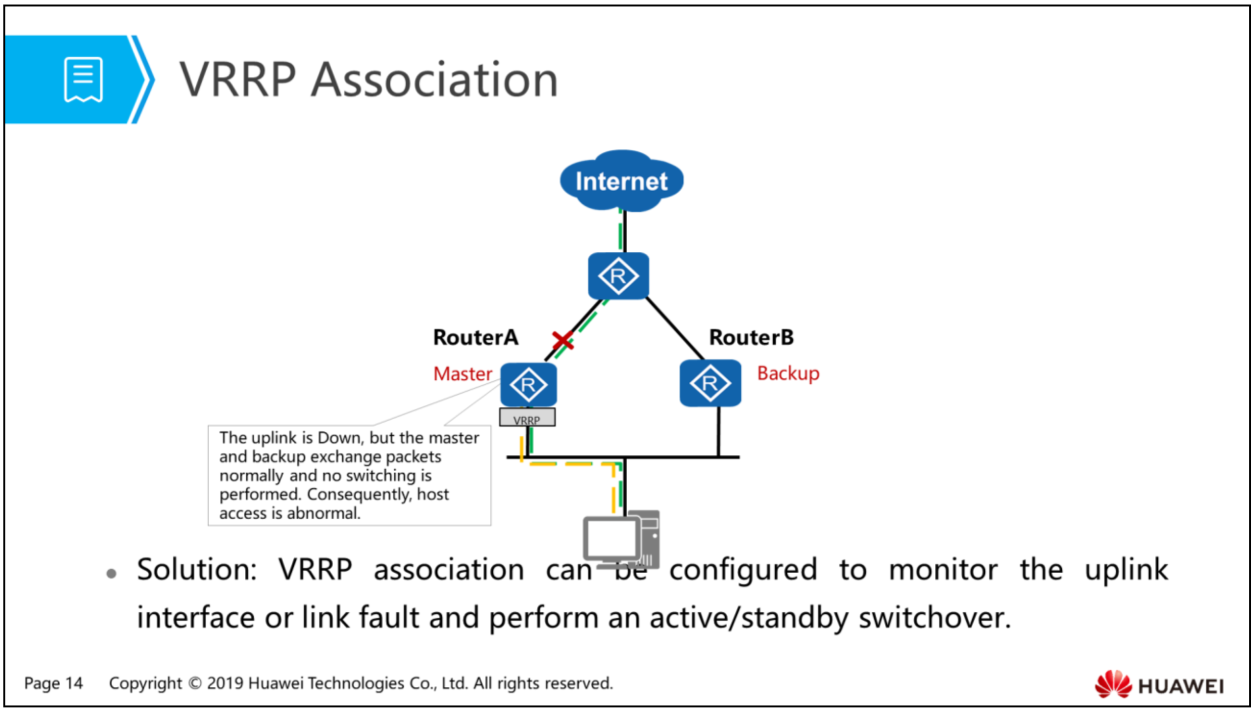


VRRP Fault

Question: Which failure point may cause a VRRP active/standby switchover?

Page 13

- The uplink fault on RouterA does not trigger a VRRP active/standby switchover. As a result, HostA's Internet access traffic is discarded at the RouterA. VRRP needs to detect the uplink fault and a VRRP active/standby switchover can be performed in a timely manner.
- When RouterA or the interface of RouterA connected to RouterB fails, a VRRP active/standby switchover is triggered. This is because the backup cannot receive protocol packets sent by the master within Master_Down_Interval.



VRRP Association

The uplink is Down, but the master and backup exchange packets normally and no switching is performed. Consequently, host access is abnormal.

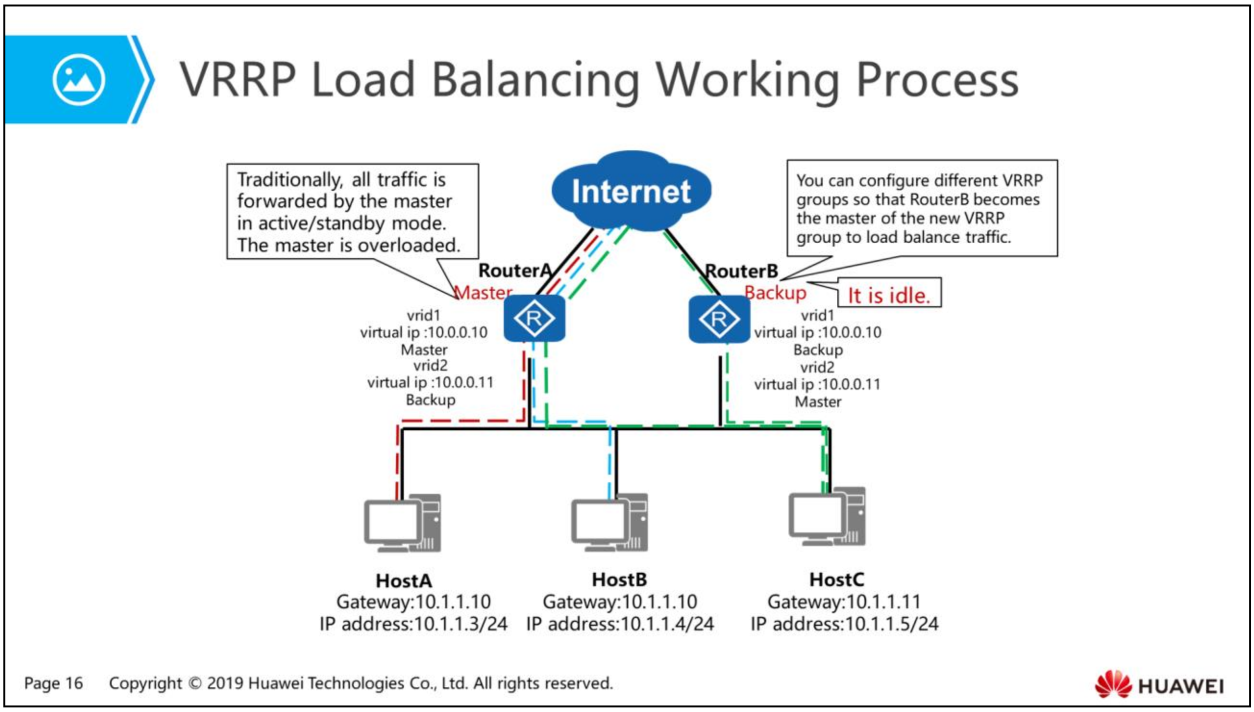
- Solution: VRRP association can be configured to monitor the uplink interface or link fault and perform an active/standby switchover.

Page 14

- Problem: VRRP cannot detect the status change of the interface that is not enabled with VRRP. When the uplink fails, VRRP cannot detect the fault and an active/standby switchover is not performed, causing service interruption.
- Solution: VRRP association can be configured to monitor the uplink interface or link fault and perform an active/standby switchover.

Contents

1. VRRP Background and Overview
2. VRRP Active/Standby Switchover
3. VRRP Load Balancing
4. Basic VRRP Configuration



VRRP Load Balancing Working Process

Traditionally, all traffic is forwarded by the master in active/standby mode. The master is overloaded.

You can configure different VRRP groups so that RouterB becomes the master of the new VRRP group to load balance traffic.

It is idle.

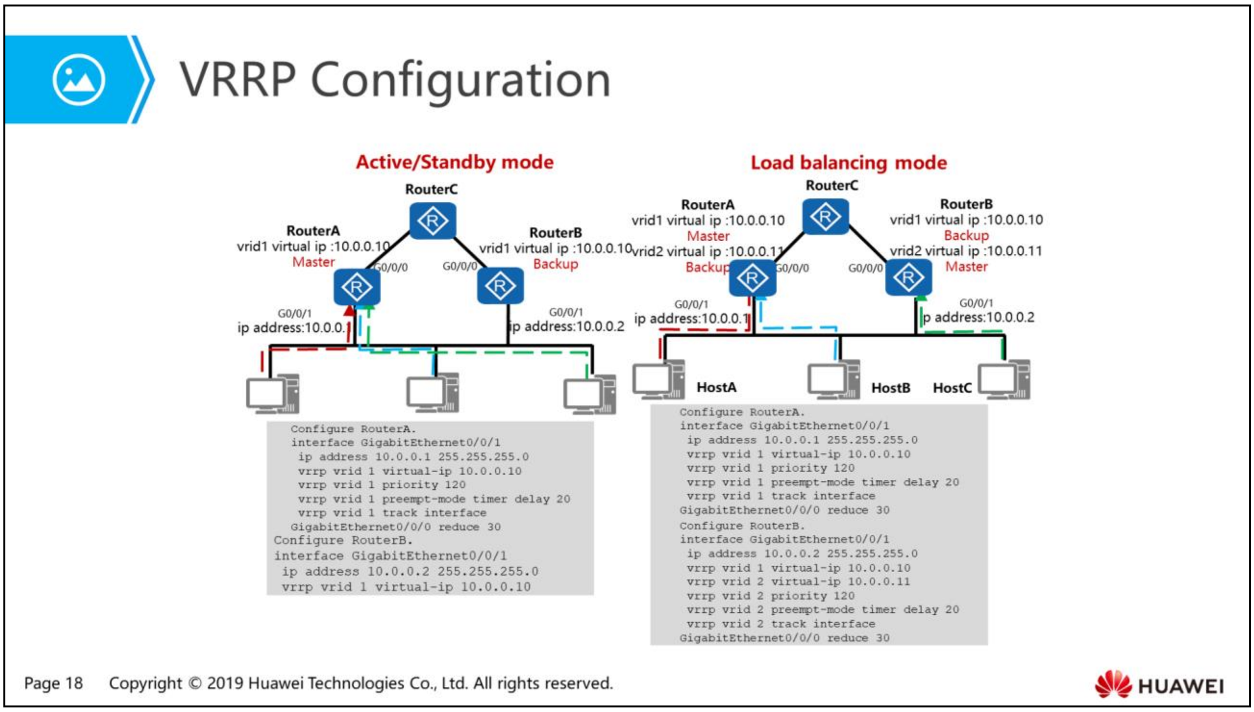
Page 16 Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- In load balancing mode, multiple VRRP groups forward service traffic. The principles and negotiation process of the VRRP load balancing mode and VRRP active/standby mode are the same. Each VRRP group consists of one master and multiple backups.
- Unlike the active/standby mode, the load balancing mode requires establishment of multiple VRRP groups. Different devices are used as masters for the VRRP group. A device can play different roles in multiple VRRP groups.

Contents

1. VRRP Background and Overview
2. VRRP Active/Standby Switchover
3. VRRP Load Balancing
4. Basic VRRP Configuration

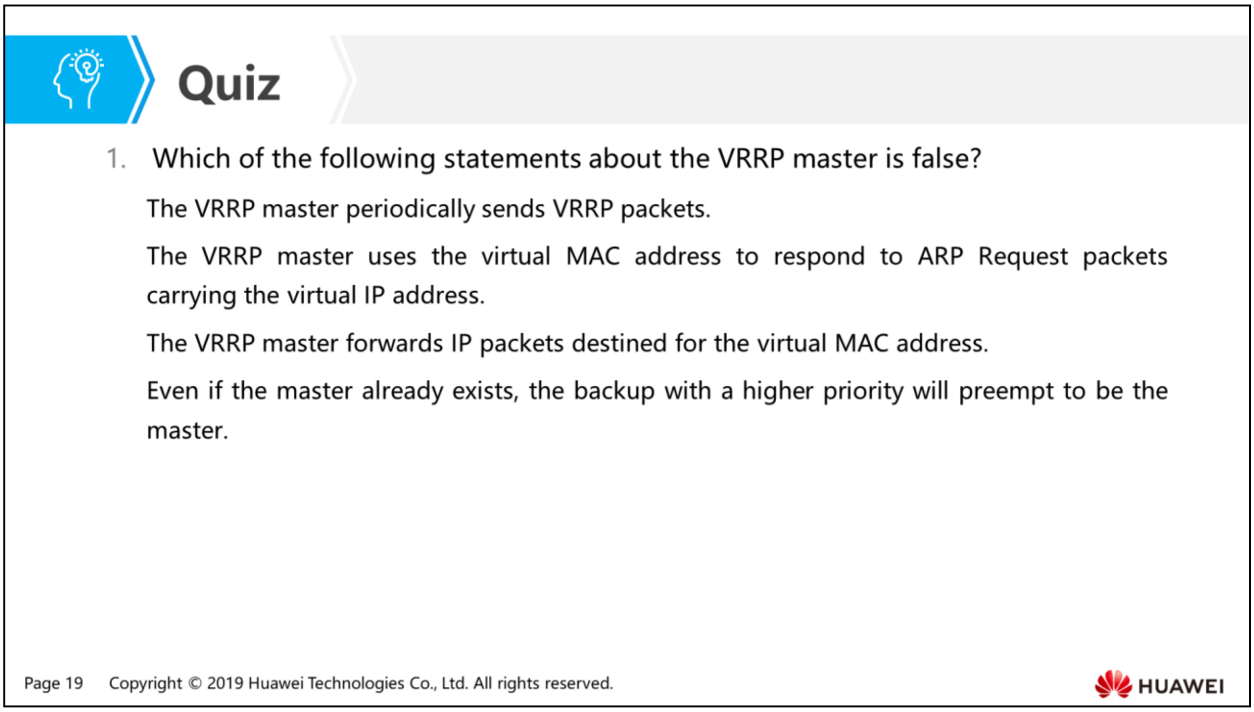


VRRP Configuration

```
  Configure RouterA.
  interface GigabitEthernet0/0/1
   ip address 10.0.0.1 255.255.255.0
   vrrp vrid 1 virtual-ip 10.0.0.10
   vrrp vrid 1 priority 120
   vrrp vrid 1 preempt-mode timer delay 20
   vrrp vrid 1 track interface
  GigabitEthernet0/0/0 reduce 30
Configure RouterB.
interface GigabitEthernet0/0/1
 ip address 10.0.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.0.10
```

```
Configure RouterA.
interface GigabitEthernet0/0/1
 ip address 10.0.0.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.0.10
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode timer delay 20
 vrrp vrid 1 track interface
GigabitEthernet0/0/0 reduce 30
Configure RouterB.
interface GigabitEthernet0/0/1
 ip address 10.0.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.0.10
 vrrp vrid 2 virtual-ip 10.0.0.11
 vrrp vrid 2 priority 120
 vrrp vrid 2 preempt-mode timer delay 20
 vrrp vrid 2 track interface
GigabitEthernet0/0/0 reduce 30
```

- The configuration roadmap in load balancing mode is similar to that in active/standby mode. A VRRP group is used as an example. The configuration of the master is as follows:
  - vrrp vrid 1 virtual-ip 10.0.0.10 //Configure the virtual IP address of VRRP group 1.
  - vrrp vrid 1 priority 120 //Set the device priority in VRRP group 1 to 120. The priorities of other devices are not specified manually, so the default value of 100 is used. The local device is the master.
  - vrrp vrid 1 preempt-mode timer delay 20 //Set the preemption delay of the master to 20s.
  - vrrp vrid 1 track interface GigabitEthernet0/0/0 reduce 30 //Associate VRRP with the uplink interface G0/0/0. When G0/0/0 fails, the VRRP priority of the master is reduced by 30.
- Configuration of the backup:
  - vrrp vrid 1 virtual-ip 10.0.0.10 //Configure the virtual IP address of VRRP group 1.



Quiz

1. Which of the following statements about the VRRP master is false?

The VRRP master periodically sends VRRP packets.

The VRRP master uses the virtual MAC address to respond to ARP Request packets carrying the virtual IP address.

The VRRP master forwards IP packets destined for the virtual MAC address.

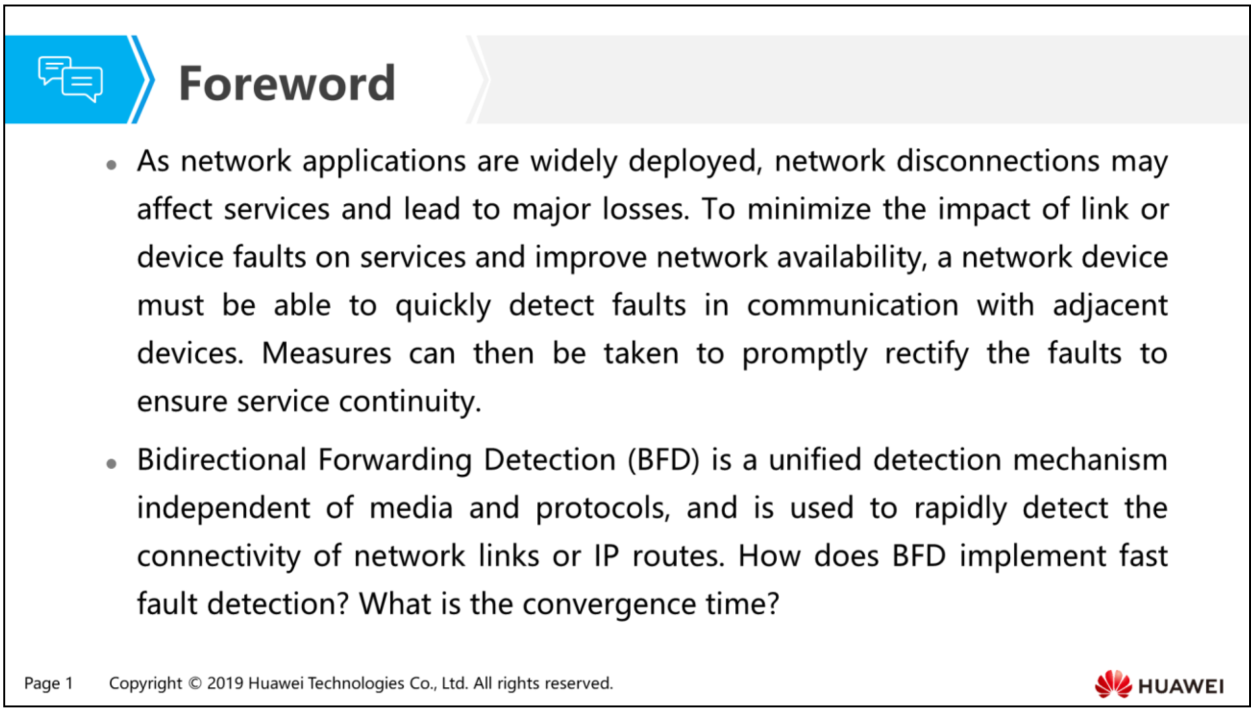
Even if the master already exists, the backup with a higher priority will preempt to be the master.

- Answer: D.

Thank You

www.huawei.com

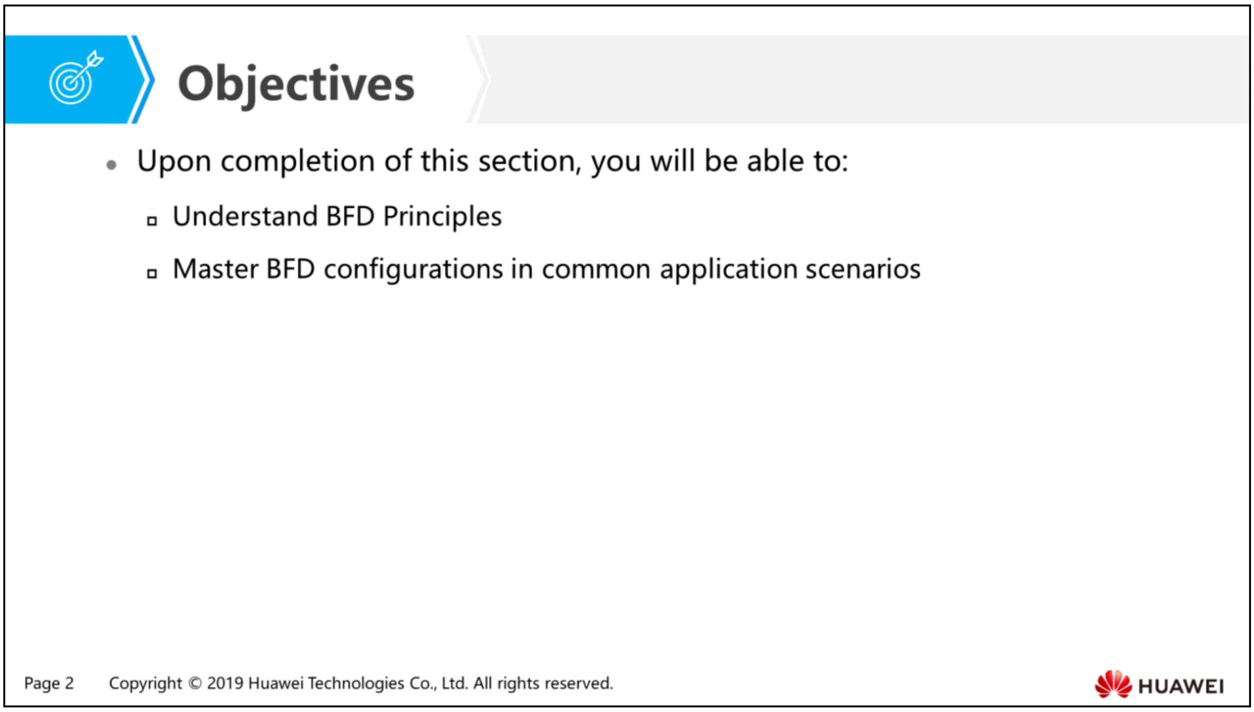
BFD Principles and Configurations



Foreword

- As network applications are widely deployed, network disconnections may affect services and lead to major losses. To minimize the impact of link or device faults on services and improve network availability, a network device must be able to quickly detect faults in communication with adjacent devices. Measures can then be taken to promptly rectify the faults to ensure service continuity.
- Bidirectional Forwarding Detection (BFD) is a unified detection mechanism independent of media and protocols, and is used to rapidly detect the connectivity of network links or IP routes. How does BFD implement fast fault detection? What is the convergence time?

- To minimize the impact of device faults on services and improve network availability, a network device must be able to quickly detect faults in communication with adjacent devices. Measures can then be taken to promptly rectify the faults to ensure service continuity. In practice, hardware detection is used to detect link faults. For example, Synchronous Digital Hierarchy (SDH) alarms are used to report link faults. However, not all media can provide the hardware detection mechanism. Applications use the Hello mechanism of the upper-layer routing protocol to detect faults. The detection duration is more than 1 second, which is too long for some applications. If no routing protocol is deployed on a small-scale Layer 3 network, the Hello mechanism cannot be used.
- BFD addresses these issues and provides fast fault detection independent of media and routing protocols. BFD is useful because it can:
  - Quickly detect link faults between neighboring network devices. The detected faults may occur on interfaces, data links, or forwarding engines.
  - Provide uniform detection for all media and protocol layers in real time.
- With BFD, you can improve network performance and adjacent systems can quickly detect communication faults so that a standby channel can be created immediately to restore communications and ensure network reliability.

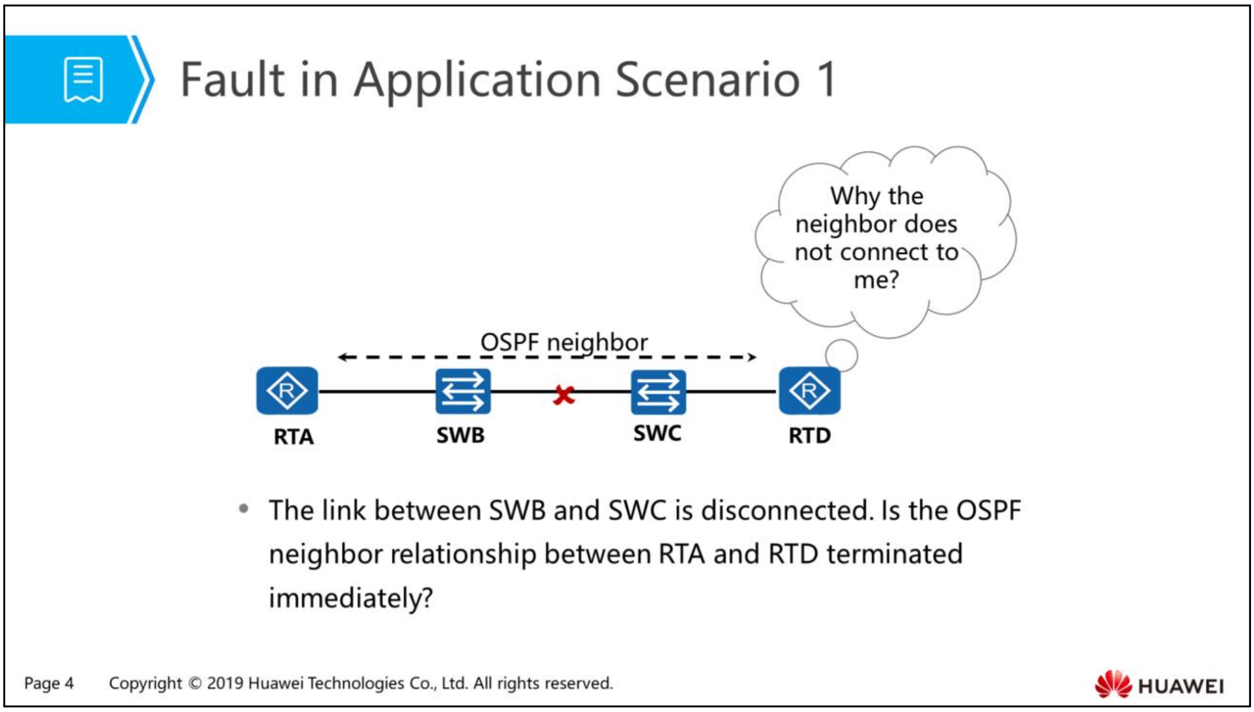


Objectives

- Upon completion of this section, you will be able to:
  - Understand BFD Principles
  - Master BFD configurations in common application scenarios

Contents

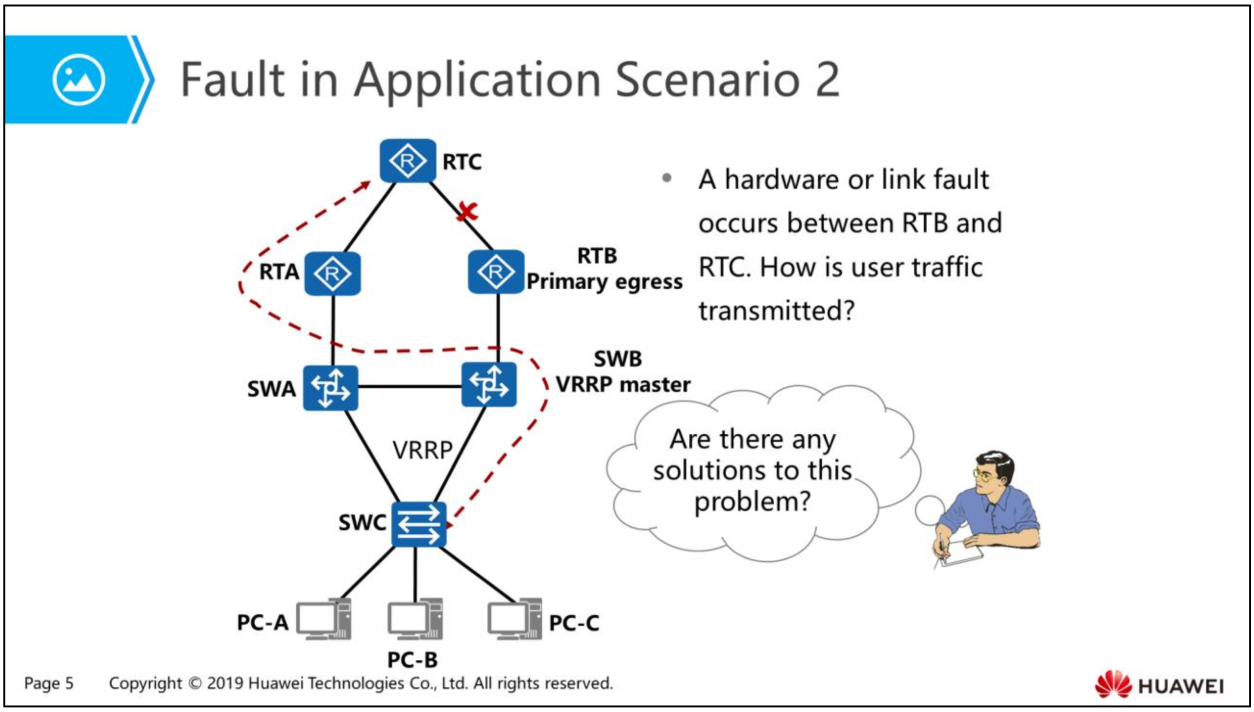
1. **BFD Principles**
2. BFD Application Scenarios



Fault in Application Scenario 1

- The link between SWB and SWC is disconnected. Is the OSPF neighbor relationship between RTA and RTD terminated immediately?

- Scenario description:
  - RTA and RTD establish an OSPF neighbor relationship. The interval for sending Hello packets is 10s. When the link between SWB and SWC is disconnected, RTA and RTD cannot detect the disconnection. The neighbor relationship is terminated when the dead interval is exceeded.

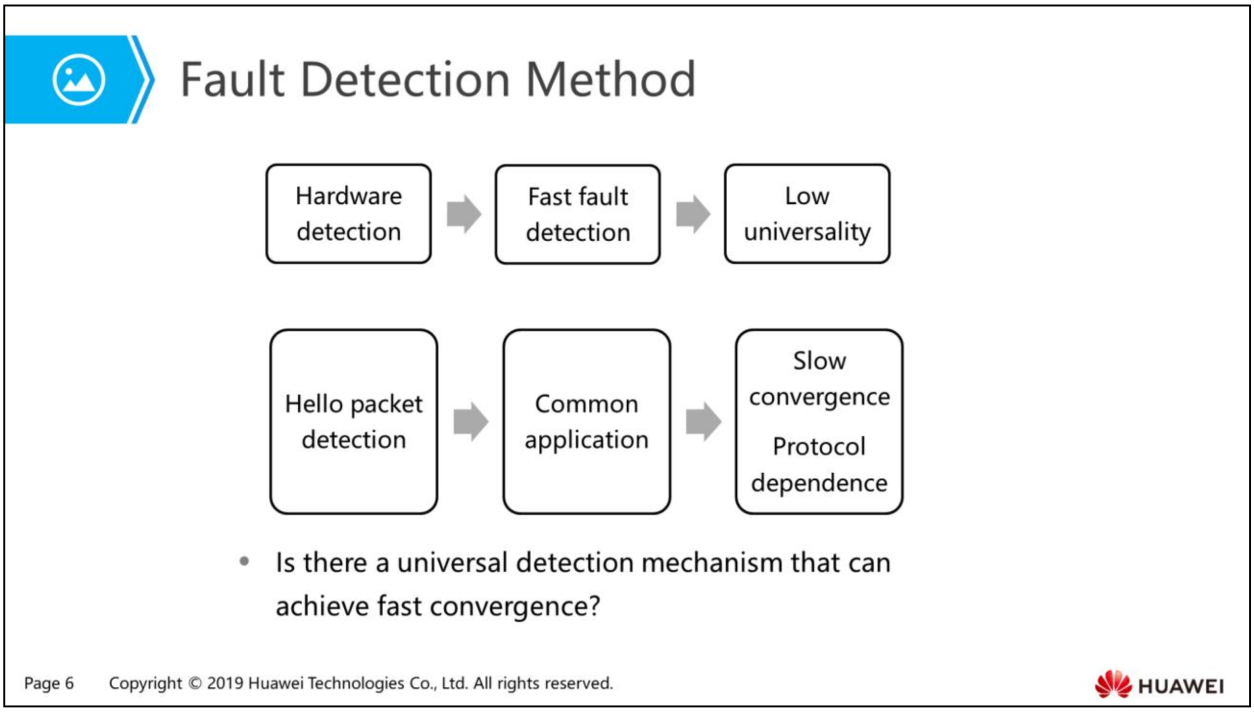


Fault in Application Scenario 2

- A hardware or link fault occurs between RTB and RTC. How is user traffic transmitted?

Are there any solutions to this problem?

- Scenario description:
  - SWA and SWB are enabled with VRRP to provide gateway backup. SWB is the master.
  - When the link between RTB and RTC is terminated, SWB can detect the disconnection through a dynamic routing protocol but cannot notify the interface on the downstream device of the detected link fault. In this case, SWB still functions as the master.
  - User data is still sent to SWB. SWB forwards user data to SWA based on a route, and then SWA sends it to RTA. Although services are not interrupted, but a sub-optimal path is generated.



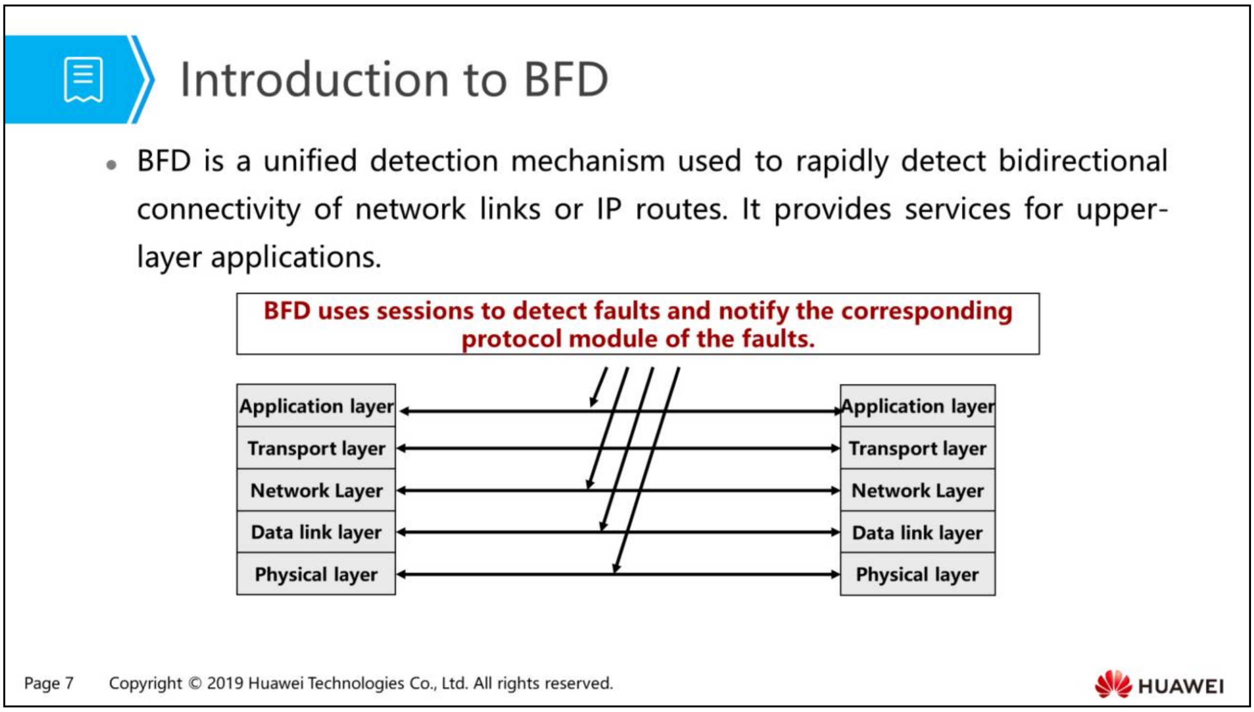
Fault Detection Method

Hardware detection → Fast fault detection → Low universality

Hello packet detection → Common application → Slow convergence Protocol dependence

- Is there a universal detection mechanism that can achieve fast convergence?

- Hardware detection:
  - For example, Synchronous Digital Hierarchy (SDH) alarms are used to report link faults. Hardware detection can quickly detect a fault; however, not all media can provide the hardware detection mechanism.
- Slow Hello mechanism:
  - It usually refers to the Hello mechanism offered by a routing protocol. This mechanism can detect a fault in seconds. In high-speed data transmission, for example, at gigabit rates, the detection time longer than 1s causes the loss of a large amount of data. For delay-sensitive services such as voice services, the delay longer than 1s is also unacceptable. In addition, this mechanism relies on routing protocols.
- Other detection mechanisms:
  - Different protocols or device manufacturers may provide proprietary detection mechanisms; however, it is difficult to deploy the proprietary detection mechanisms when systems are interconnected.

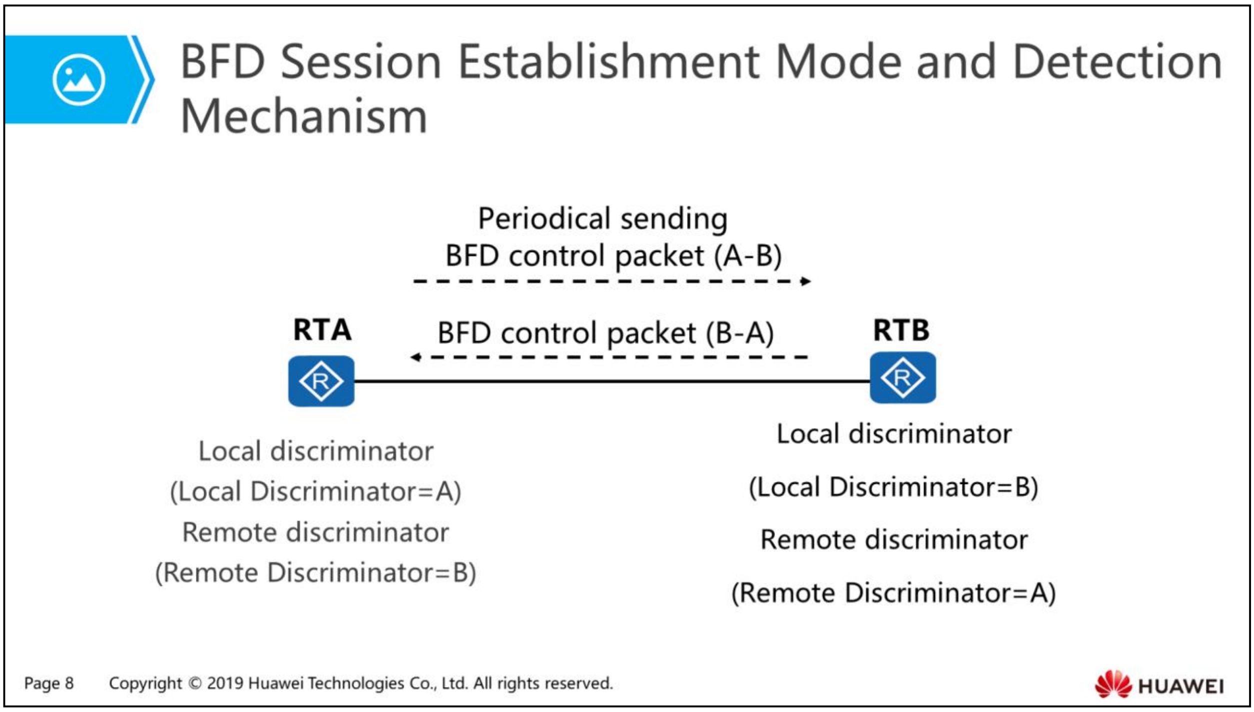


Introduction to BFD

- BFD is a unified detection mechanism used to rapidly detect bidirectional connectivity of network links or IP routes. It provides services for upper-layer applications.

BFD uses sessions to detect faults and notify the corresponding protocol module of the faults.

- After a BFD session is set up, the local device periodically sends BFD packets. If the local device does not receive a response from the remote device within the detection time, it considers the forwarding path faulty. BFD then notifies the upper-layer application for processing.
- BFD does not provide neighbor discovery. Instead, BFD obtains neighbor information from the upper-layer application BFD serves to establish a BFD session.
- BFD can detect the physical interface status, Layer 2 link status, network layer address reachability, transport layer connection status, and application layer protocol running status.



BFD Session Establishment Mode and Detection Mechanism

Periodical sending BFD control packet (A-B)

RTA

BFD control packet (B-A)

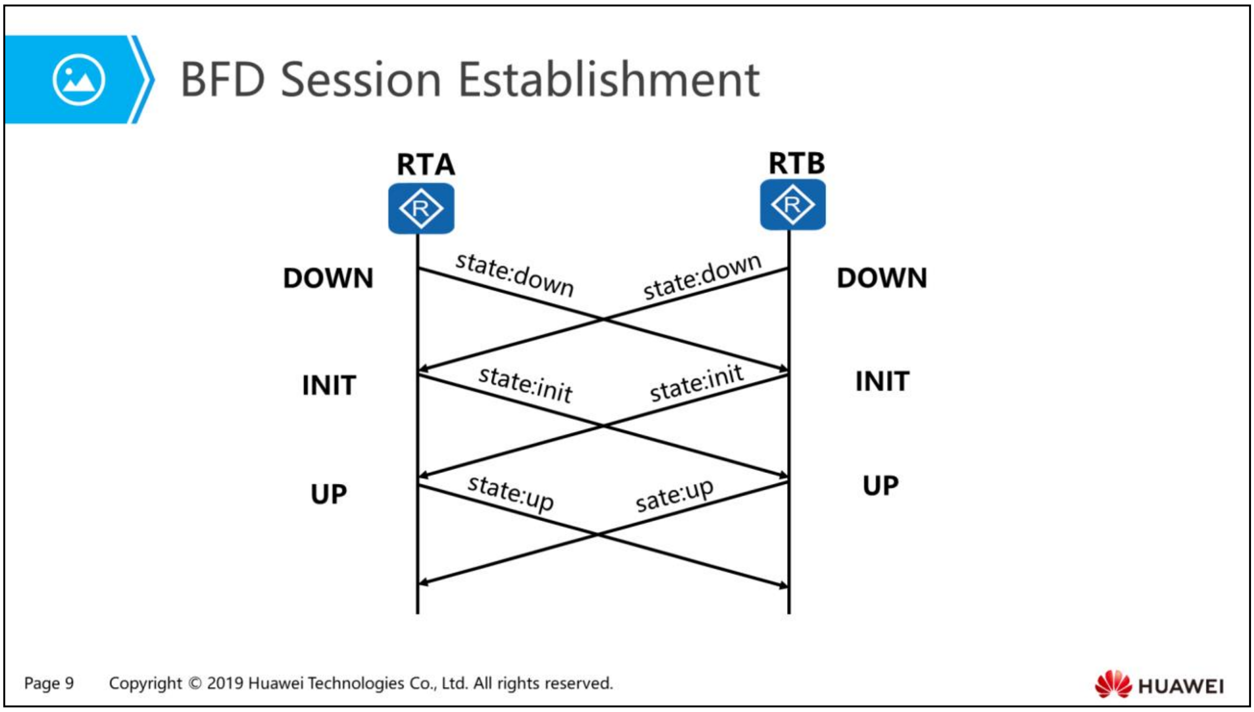
RTB

Local discriminator
(Local Discriminator=A)
Remote discriminator
(Remote Discriminator=B)

Local discriminator
(Local Discriminator=B)
Remote discriminator
(Remote Discriminator=A)

Page 8

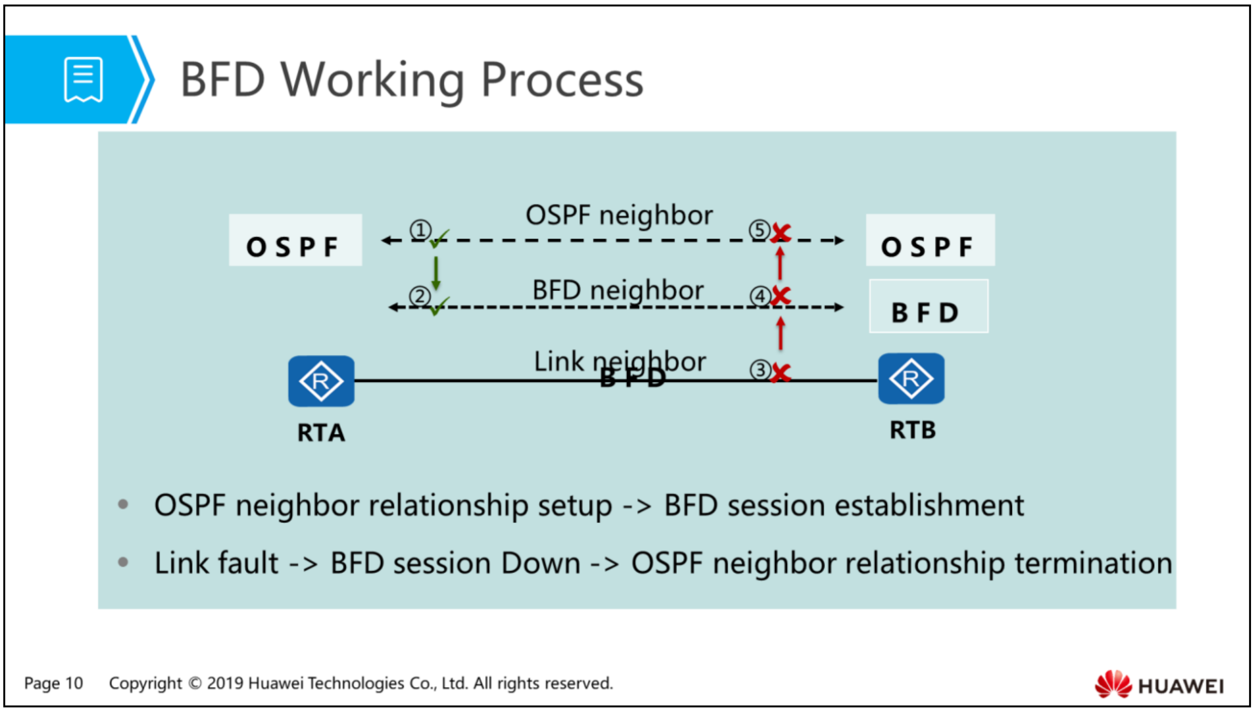
- BFD identifiers:
  - The BFD identifier is similar to the OSPF router ID.
  - Identifiers fall into local and remote discriminators. The local discriminator identifies the local device and the remote identifier identifies the remote device.
  - A static BFD session is set up by using commands to manually configure BFD session parameters, including the local discriminator and remote discriminator.
  - A dynamic BFD session is triggered by an application. When an application triggers dynamic setup of a BFD session, the system allocates the value that belongs to the dynamic session discriminator area as the local discriminator of the BFD session. Then the local system sends a BFD control packet with the remote discriminator of 0 to the remote system for BFD session negotiation. When one end of a BFD session receives a BFD control packet with the remote discriminator of 0, this end checks the BFD control packet. If the packet matches the local BFD session, this end learns the local discriminator in the received BFD control packet to obtain the remote discriminator.
- BFD detection mechanism:
  - Two systems set up a BFD session and periodically send BFD control packets along the path between them. If one system does not receive BFD control packet within a specified period, the system considers that a fault has occurred on the path. BFD control packets are UDP packets and the port number is 3784.
  - BFD provides the asynchronous mode. In asynchronous mode, two systems periodically send BFD control packets to each other. If one system does not receives three packets consecutively, the system considers the BFD session Down.



BFD Session Establishment

HUAWEI

- RTA and RTB each start BFD state machines. The initial status of BFD state machine is Down. RTA and RTB send BFD control packets with the State field set to Down. If BFD sessions are configured statically, the remote discriminator in BFD packets are specified. If BFD sessions are configured dynamically, the remote discriminator is 0.
- After receiving the BFD packet with the State field set to Down, RTB switches the session status to Init and sends a BFD packet with the State field set to Init.
- After the local BFD session status of RTB changes to Init, RTB no longer processes the received BFD packets with the State field set to Down.
- After receiving the BFD packet with the State field set to Init, RTB changes the local BFD session status to Up.
- The BFD session status change on RTA is similar to that on RTB.
- After the session is established successfully, RTA and RTB periodically send control packets with the State field set to Up.



BFD Working Process

OSPF

① OSPF neighbor ⑤

OSPF

② BFD neighbor ④

BFD

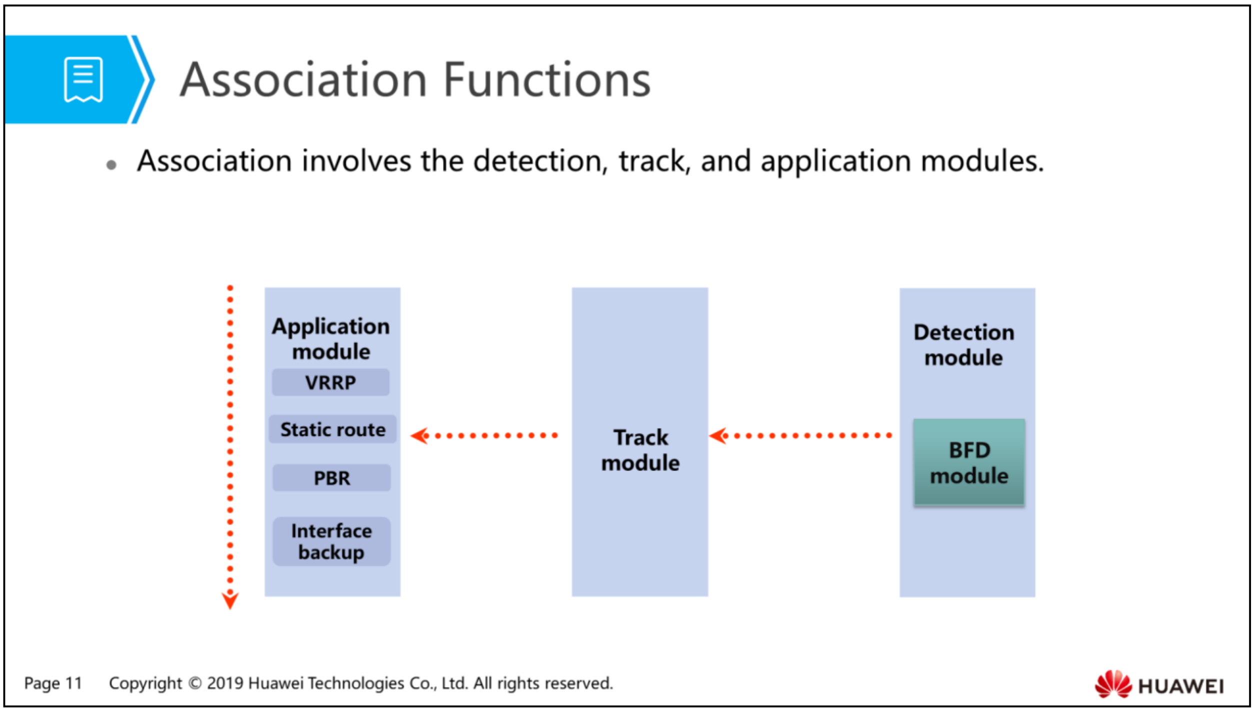
Link neighbor BFD ③

RTA

RTB

- OSPF neighbor relationship setup -> BFD session establishment
- Link fault -> BFD session Down -> OSPF neighbor relationship termination

- BFD for OSPF:
  - OSPF uses its own Hello mechanism to discover a neighbor and establishes a connection.
  - After the OSPF neighbor relationship is established, the neighbor information including source and destination IP addresses is advertised to BFD.
  - A BFD session is established based on the received neighbor information.
  - The detected link fails.
  - BFD quickly sends BFD packets to detect the link fault. If there is no response within the specified time, the BFD session becomes Down.
  - BFD notifies the local OSPF process of neighbor unreachability.
  - The local OSPF process terminates the OSPF neighbor relationship.



Association Functions

- Association involves the detection, track, and application modules.

Application module

VRRP

Static route

PBR

Interface backup

Track module

Detection module

BFD module

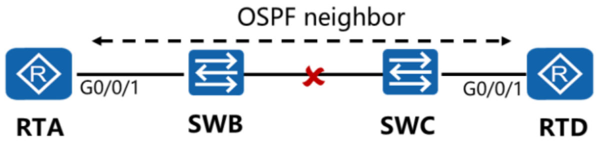
- The detection module is responsible for monitoring the link status and network performance, and notifies the track module of the detection result.
- After receiving the detection result of the detection module, the track module changes the status of the track item and notifies the application module.
- The application module takes an action based on the track item status.

Contents

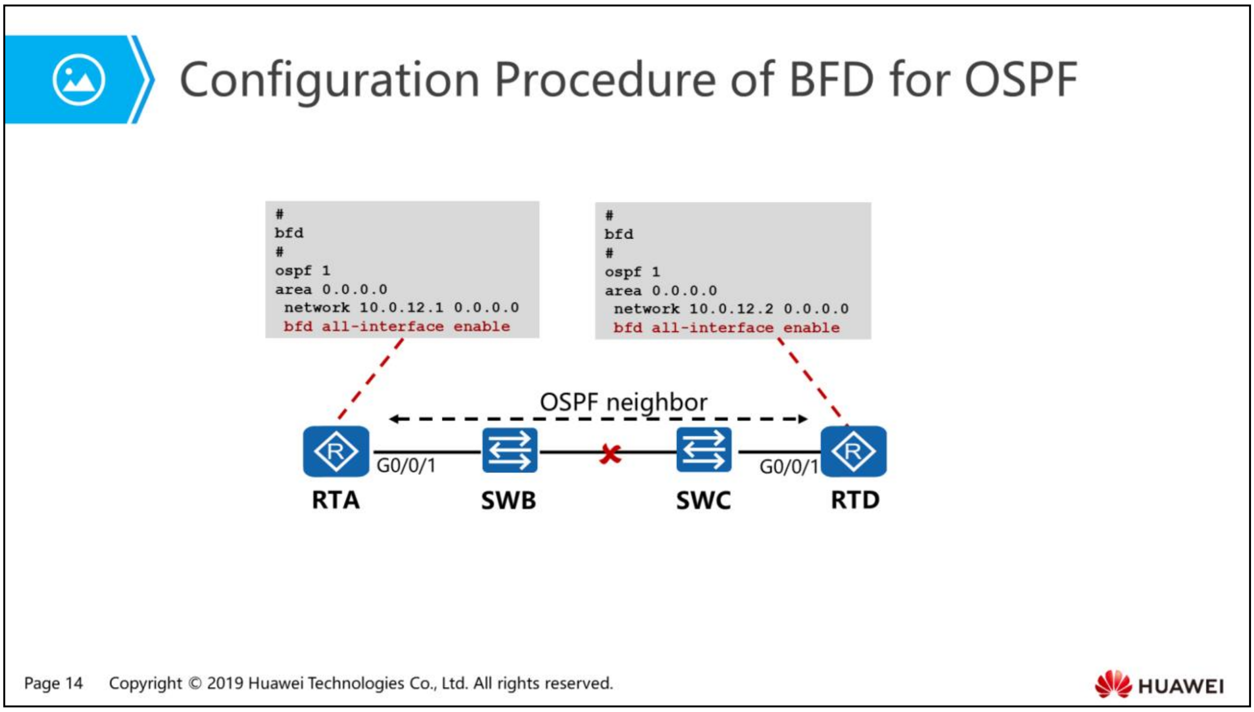
1. BFD Principles

2. **BFD Application Scenarios**

Configuration Requirements of BFD for OSPF



- A company uses two Layer 2 switches to connect two departments that are far from each other. RTA and RTD are enabled with OSPF and establish an OSPF neighbor relationship to ensure that they are reachable at the network layer.
- RTA and RTD support BFD. BFD for OSPF needs to be used. When a fault occurs on the link between RTA/RTD and a Layer 2 switch or between switches, for example, the link is Down, BFD can quickly detect the fault and notify OSPF.

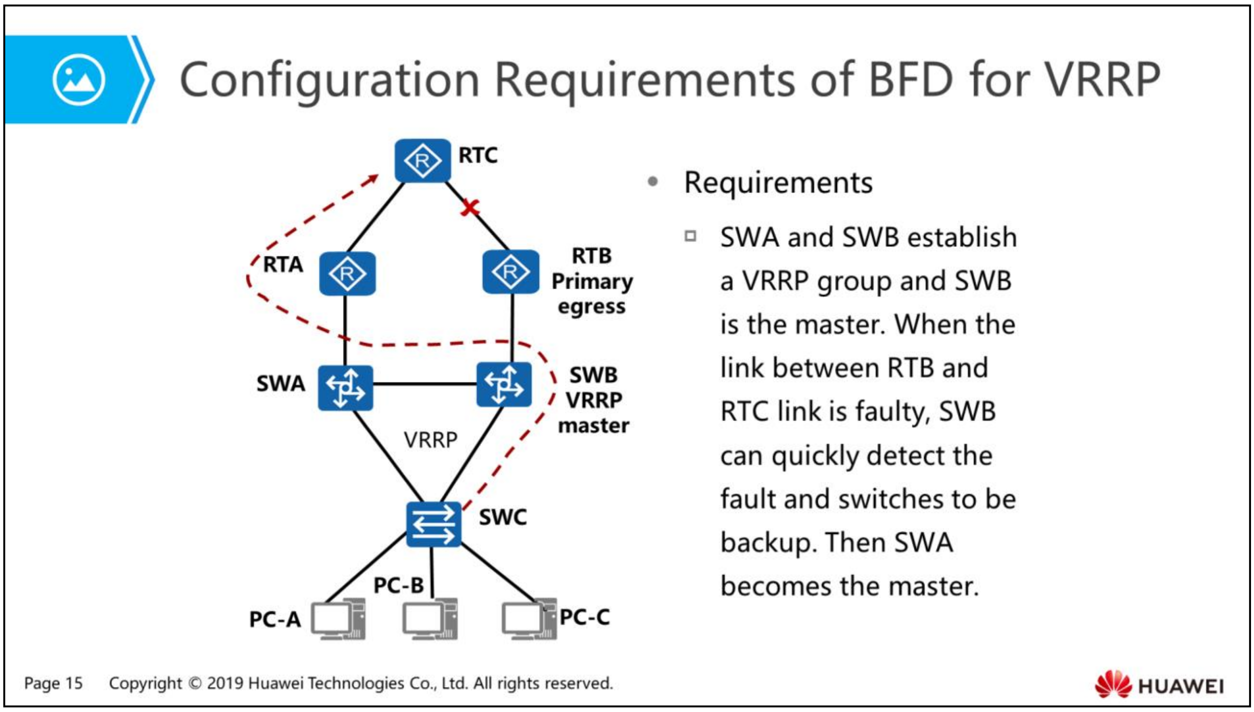


Configuration Procedure of BFD for OSPF

```
#
bfd
#
ospf 1
area 0.0.0.0
 network 10.0.12.1 0.0.0.0
 bfd all-interface enable
```

```
#
bfd
#
ospf 1
area 0.0.0.0
 network 10.0.12.2 0.0.0.0
 bfd all-interface enable
```

- The configuration roadmap is as follows:
  - Configure OSPF on RTA and RTD and establish an OSPF neighbor relationship.
  - Enable BFD globally.
  - Enable BFD in OSPF areas of RTA and RTD.

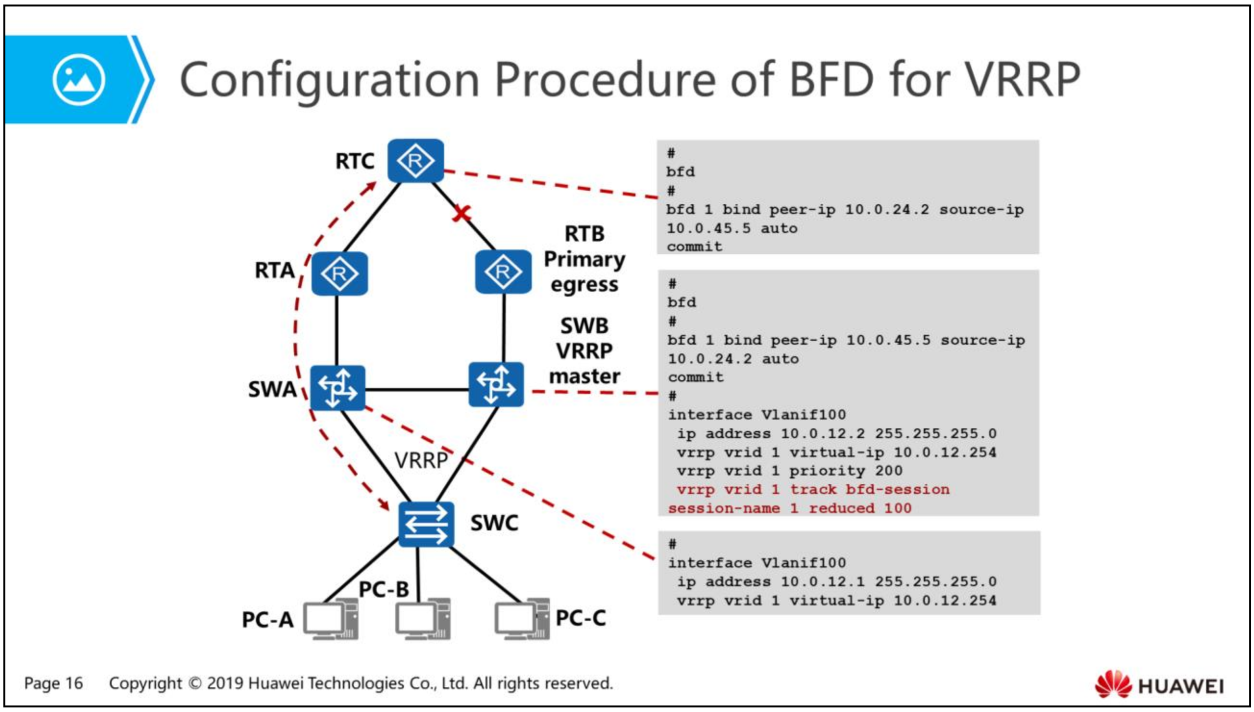


Configuration Requirements of BFD for VRRP

- Requirements
  - SWA and SWB establish a VRRP group and SWB is the master. When the link between RTB and RTC link is faulty, SWB can quickly detect the fault and switches to be backup. Then SWA becomes the master.

Page 15 Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved. HUAWEI

- Association with VRRP:
  - VRRP can only detect faults in VRRP groups. Association between a VRRP group and the interface status allows the device to detect faults on the uplink interface or direct uplink of the master. When an indirect uplink of the master fails, VRRP cannot detect the fault. You can deploy association between VRRP and BFD to detect the indirect uplink of the master. When the uplink of the master fails, BFD rapidly detects the fault and notifies the master of adjusting its priority. This triggers an active/standby switchover, ensuring proper traffic forwarding.



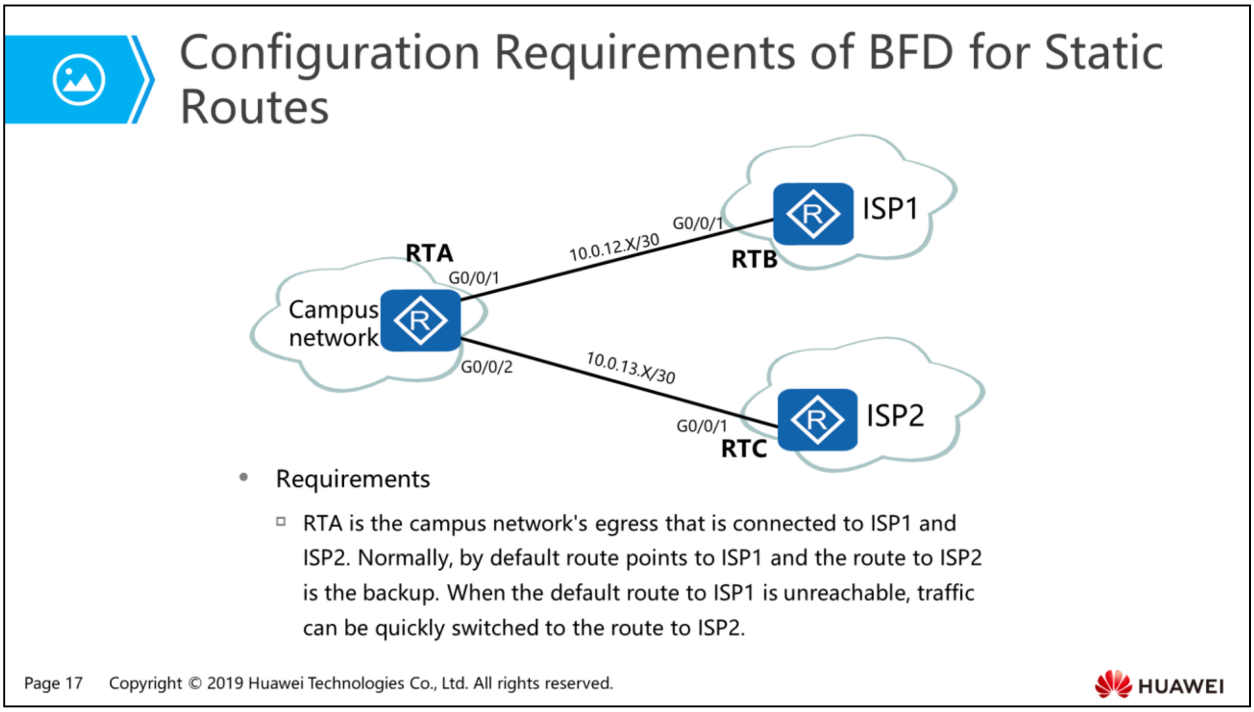
Configuration Procedure of BFD for VRRP

```
#
bfd
#
bfd 1 bind peer-ip 10.0.24.2 source-ip
10.0.45.5 auto
commit
```

```
#
bfd
#
bfd 1 bind peer-ip 10.0.45.5 source-ip
10.0.24.2 auto
commit
#
interface Vlanif100
 ip address 10.0.12.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.12.254
 vrrp vrid 1 priority 200
 vrrp vrid 1 track bfd-session
session-name 1 reduced 100
```

```
#
interface Vlanif100
 ip address 10.0.12.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.12.254
```

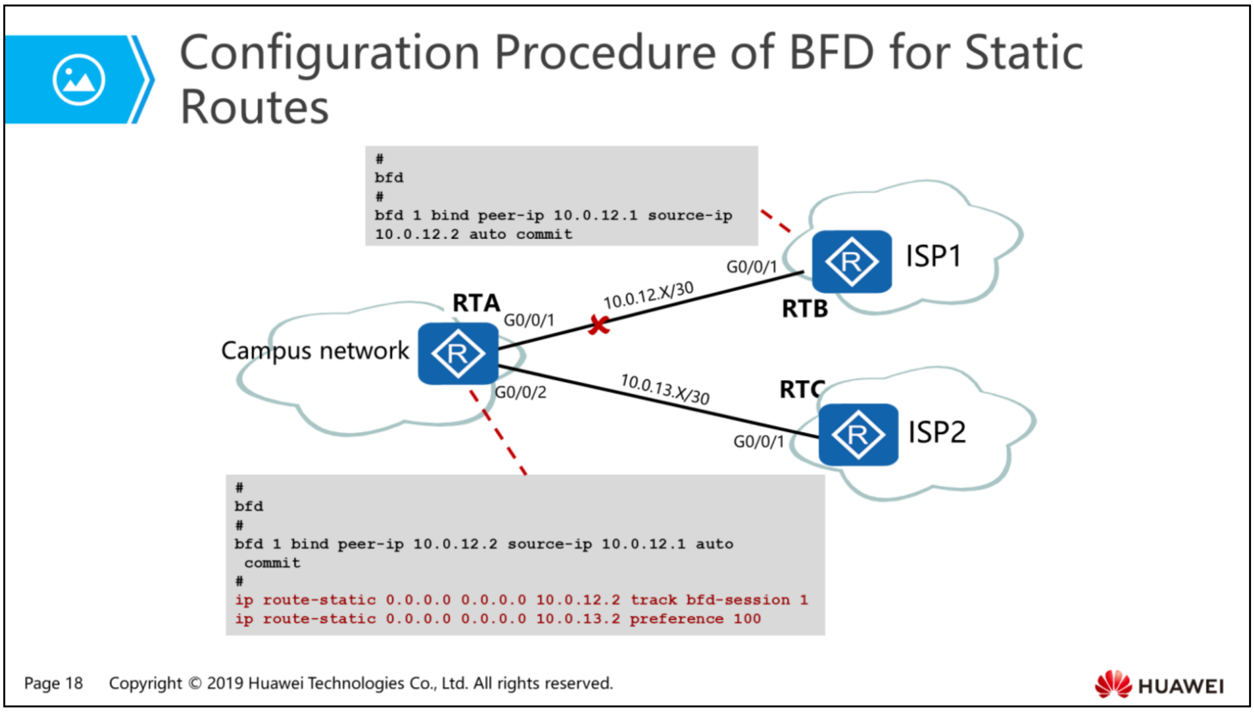
- The configuration roadmap is as follows:
  - Configure SWA and SWB to establish a VRRP group.
  - Configure a BFD session between SWB and RTC.
  - Associate the VRRP group on SWB with the BFD session. When the BFD session status changes, the priority of SWB is reduced, triggering an active/standby switchover.
  - SWA becomes the master in the VRRP group to forward user traffic.



Configuration Requirements of BFD for Static Routes

- Requirements
  - RTA is the campus network's egress that is connected to ISP1 and ISP2. Normally, by default route points to ISP1 and the route to ISP2 is the backup. When the default route to ISP1 is unreachable, traffic can be quickly switched to the route to ISP2.

- BFD for static routes:
  - Static routes do not have a detection mechanism. When a fault occurs on a network, an administrator needs to rectify the fault. BFD for static routes enables a BFD session to detect the status of the link of the static route on the public network.
  - Each static route can be bound to a BFD session. When a BFD session bound to a static route detects a fault (for example, the link changes from Up to Down) on a link, BFD reports the fault to the routing management module (RM). Then, the RM configures the route as inactive, indicating that the route is unavailable and deleted from the IP routing table. When the BFD session bound to the static route is successfully set up or the link of the static route is restored (that is, the link changes from Down to Up), BFD reports the event to the RM and the RM configures the static route as active, indicating that the route is available and added to the IP routing table.

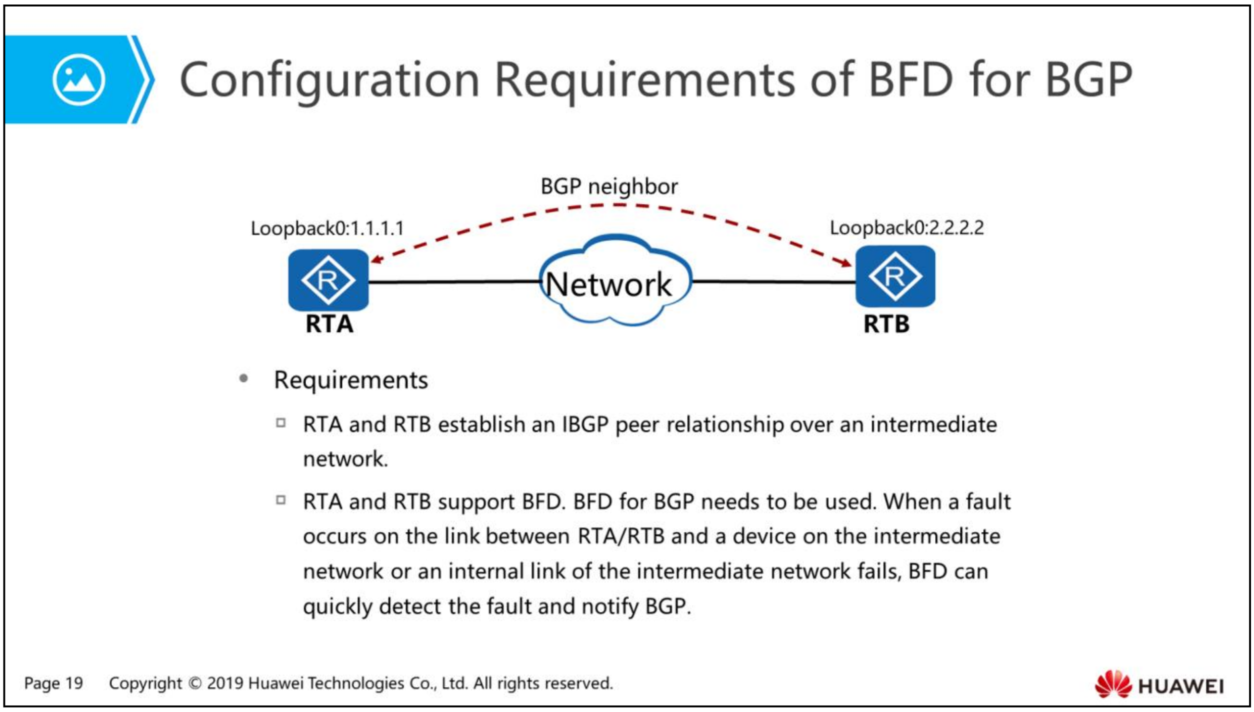


Configuration Procedure of BFD for Static Routes

```
#
bfd
#
bfd 1 bind peer-ip 10.0.12.1 source-ip
10.0.12.2 auto commit
```

```
#
bfd
#
bfd 1 bind peer-ip 10.0.12.2 source-ip 10.0.12.1 auto
 commit
#
ip route-static 0.0.0.0 0.0.0.0 10.0.12.2 track bfd-session 1
ip route-static 0.0.0.0 0.0.0.0 10.0.13.2 preference 100
```

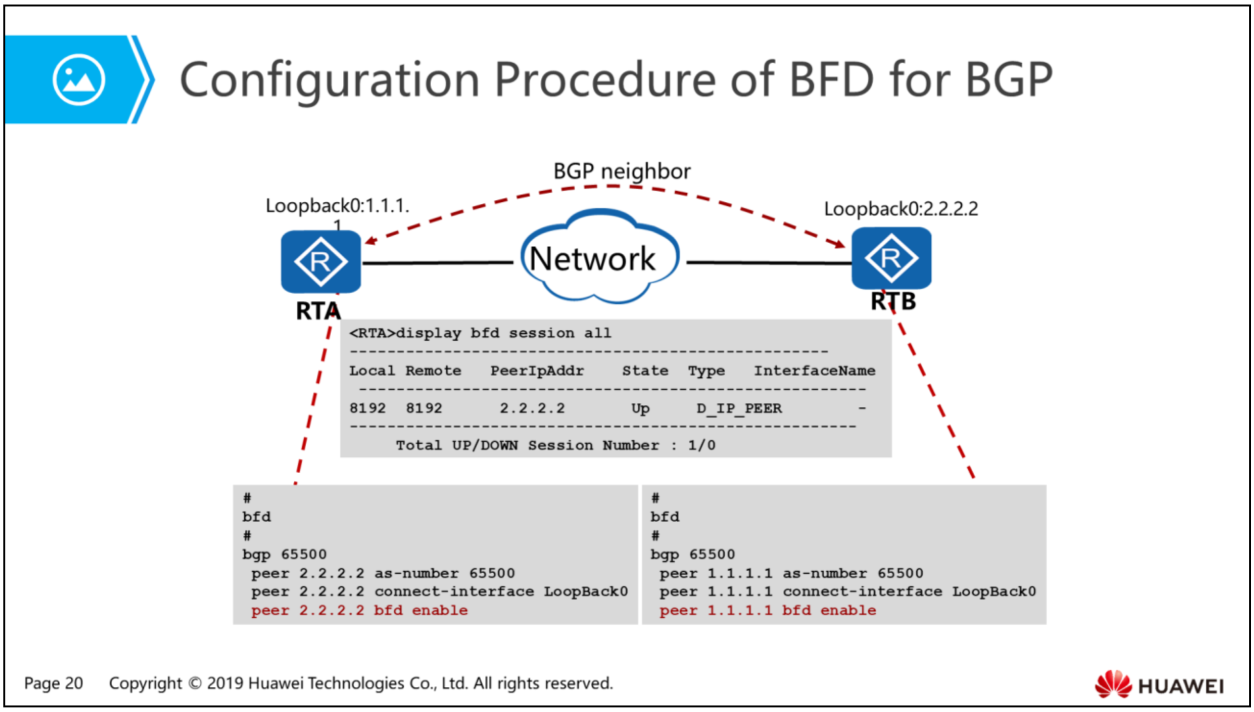
- The configuration roadmap is as follows:
  - Enable BFD globally on RTA and RTB.
  - Configure a BFD session between RTA and RTB.
  - On RTA, configure the default route to ISP1, retain the default priority of 60, and associate the route with the BFD session.
  - On RTA, configure the default route to ISP2 and set the priority of this route to be lower than that of the route to ISP1.



Configuration Requirements of BFD for BGP

- Requirements
  - RTA and RTB establish an IBGP peer relationship over an intermediate network.
  - RTA and RTB support BFD. BFD for BGP needs to be used. When a fault occurs on the link between RTA/RTB and a device on the intermediate network or an internal link of the intermediate network fails, BFD can quickly detect the fault and notify BGP.

- Association with BGP:
  - Association between BFD and BGP is similar to association between BFD and OSPF. The difference is that BFD notifies the BGP module of the TCP layer.



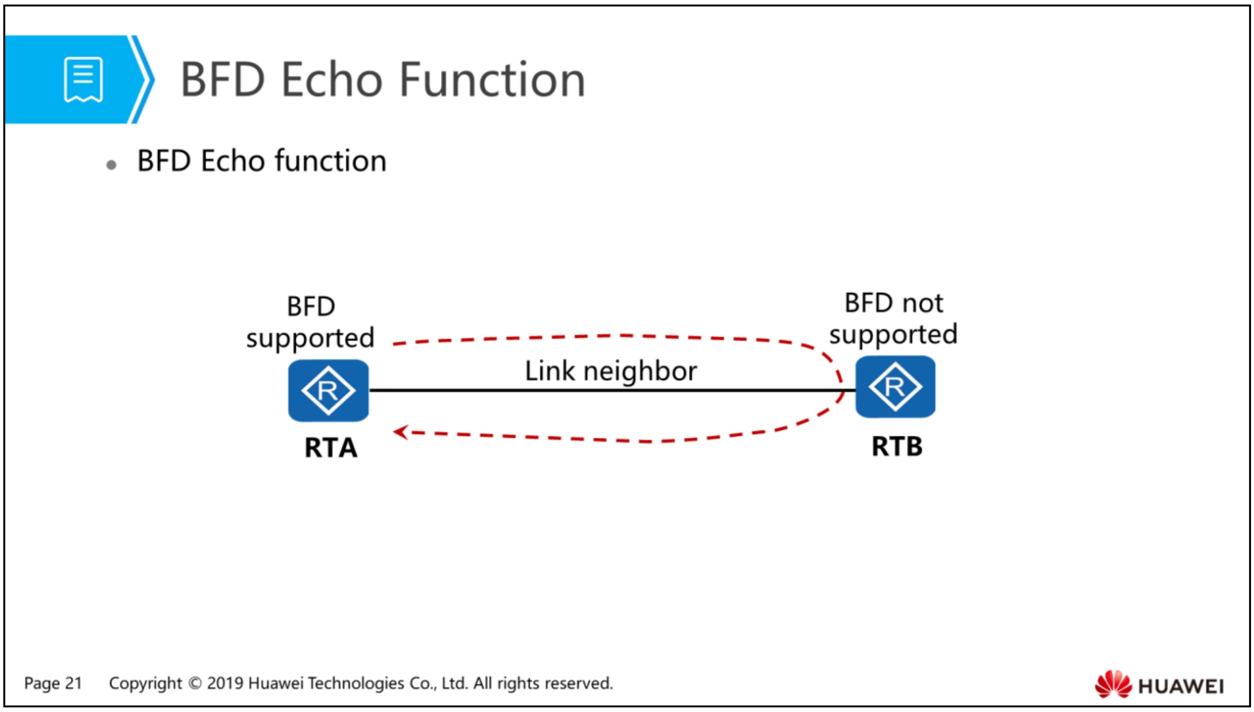
Configuration Procedure of BFD for BGP

```
<RTA>display bfd session all
----------------------------------------------------
Local Remote   PeerIpAddr    State  Type   InterfaceName
 -------------------------------------------------------
8192  8192       2.2.2.2       Up     D_IP_PEER        -
------------------------------------------------------
     Total UP/DOWN Session Number : 1/0
```

```
#
bfd
#
bgp 65500
 peer 2.2.2.2 as-number 65500
 peer 2.2.2.2 connect-interface LoopBack0
 peer 2.2.2.2 bfd enable
```

```
#
bfd
#
bgp 65500
 peer 1.1.1.1 as-number 65500
 peer 1.1.1.1 connect-interface LoopBack0
 peer 1.1.1.1 bfd enable
```

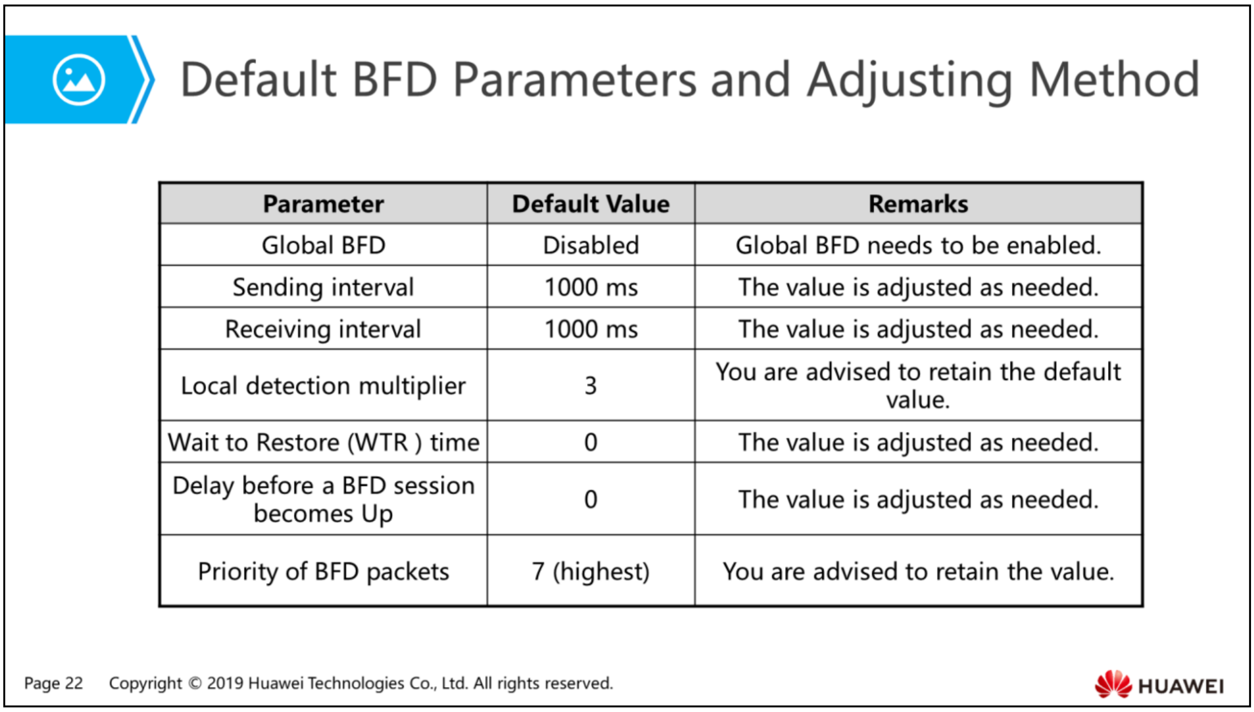
- The configuration roadmap is as follows:
  - Ensure that there are reachable routes between RTA and RTB.
  - Configure BGP neighbor parameters of RTA and RTB, and establish an IBGP peer relationship.
  - Enable BFD globally on RTA and RTB.
  - Enable BFD in BGP processes on RTA and RTB.



BFD Echo Function

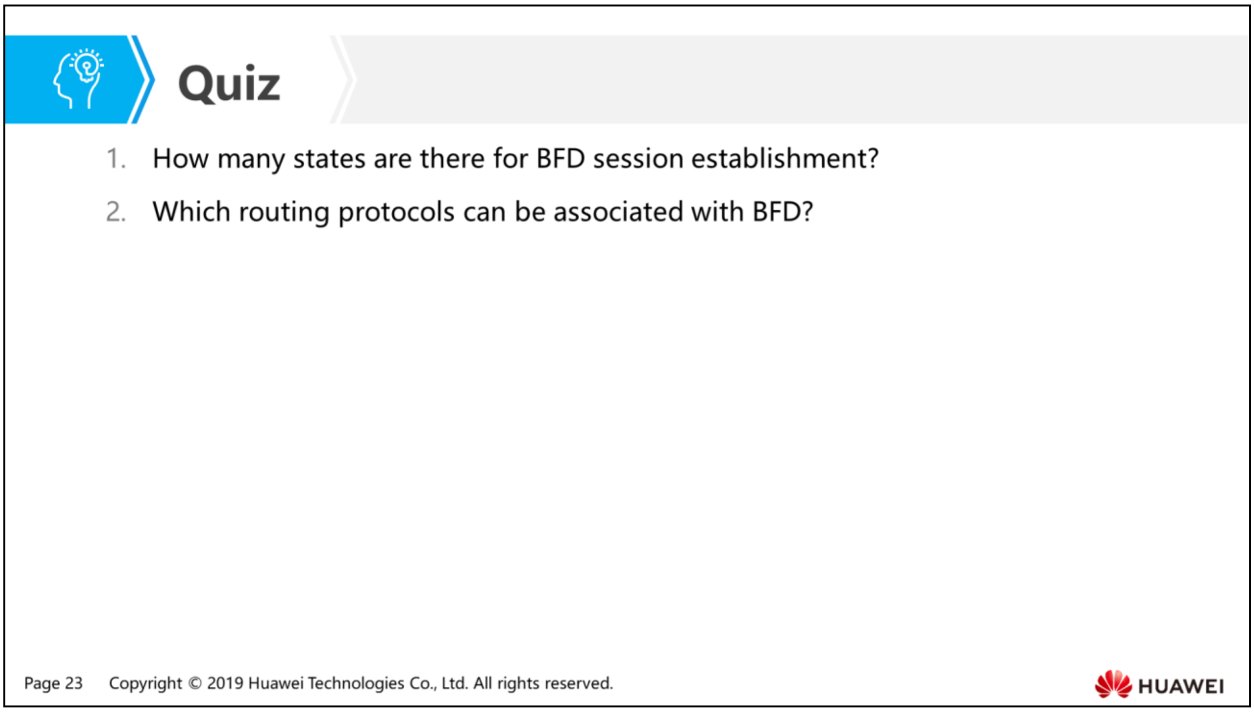
- BFD Echo function

- BFD Echo function:
  - The BFD Echo function checks the connectivity of the forwarding link by looping back packets.
  - RTA and RTB are directly connected. RTA supports BFD, and RTB supports only forwarding at the network layer and does not support BFD. To rapidly detect forwarding failures between the two devices, the BFD Echo function is configured on RTA. RTA sends an Echo Request packet to RTB. RTB then sends the Echo Request packet back along the same path to detect the connectivity of the forwarding link.
  - RTA sends BFD packets with source and destination addresses as RTA from the outbound interface. RTB directly sends the received BFD packets to RTA.



Default BFD Parameters and Adjusting Method

Parameter	Default Value	Remarks
Global BFD	Disabled	Global BFD needs to be enabled.
Sending interval	1000 ms	The value is adjusted as needed.
Receiving interval	1000 ms	The value is adjusted as needed.
Local detection multiplier	3	You are advised to retain the default value.
Wait to Restore (WTR) time	0	The value is adjusted as needed.
Delay before a BFD session becomes Up	0	The value is adjusted as needed.
Priority of BFD packets	7 (highest)	You are advised to retain the value.



Quiz

1. How many states are there for BFD session establishment?
2. Which routing protocols can be associated with BFD?

- Answer: BFD states include DOWN, INIT, and UP.
- Answer: BFD can be associated with the static route, OSPF, BGP, and so on.

Thank You

www.huawei.com

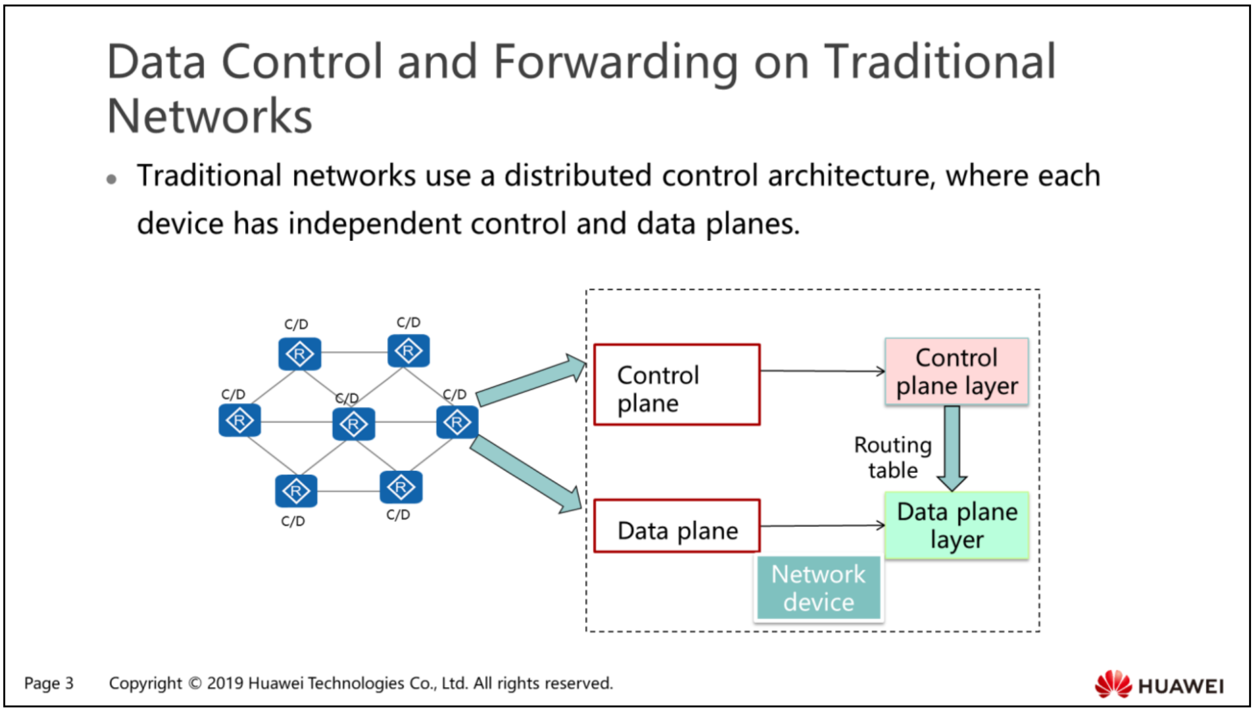
SDN Overview

Objectives

- Upon completion of this section, you will be able to:
  - Be familiar with the benefits of SDN
  - Master the SDN concept and architecture
  - Understand ways of SDN evolution for traditional networks

Contents

1. **SDN Concept and Architecture**
2. Benefits of SDN
3. Ways of SDN Evolution

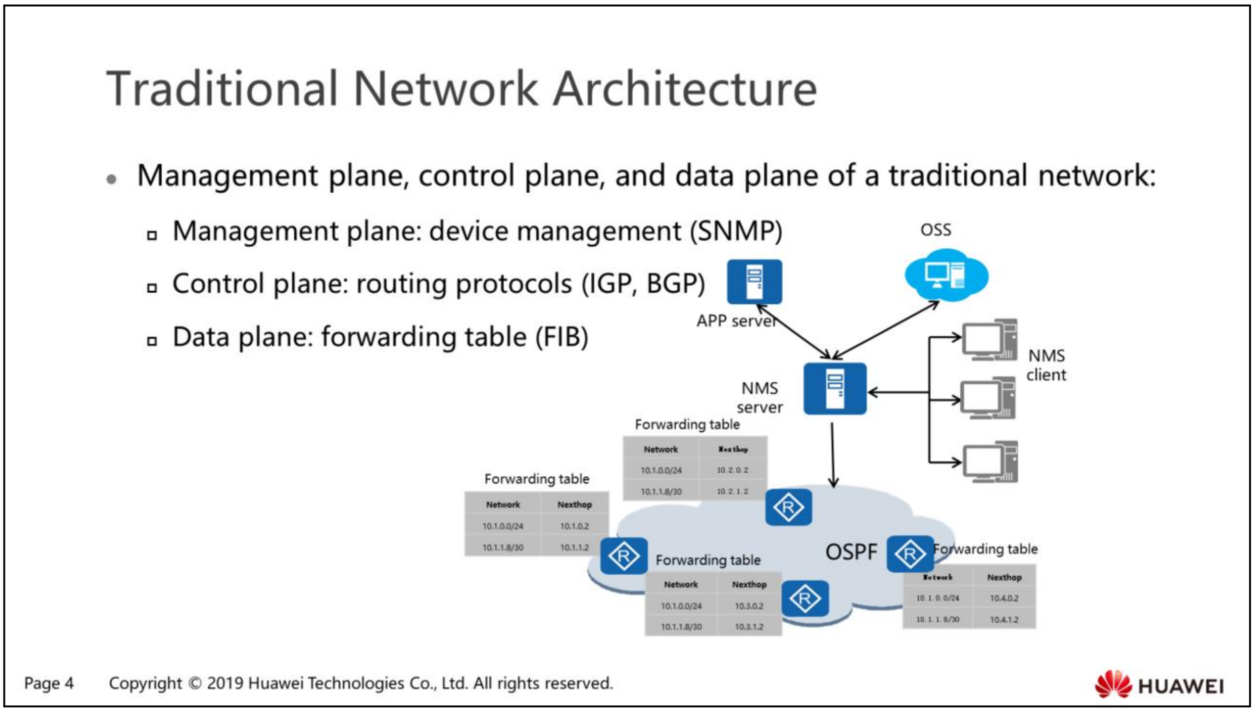


Data Control and Forwarding on Traditional Networks

- Traditional networks use a distributed control architecture, where each device has independent control and data planes.

Page 3

- Traditional networks use a distributed control architecture.
  - In the distributed control architecture of a traditional IP network, the control plane responsible for protocol computing and the data plane responsible for packet forwarding are located on the same device.
  - After routes and topologies on the network change, all network devices must re-calculate routes. This is a distributed control process.
  - On a traditional IP network, each device independently collects network information and calculates its own routes.
  - A disadvantage of this model is that routes cannot be calculated on all devices from a global perspective.



Traditional Network Architecture

- Management plane, control plane, and data plane of a traditional network:
  - Management plane: device management (SNMP)
  - Control plane: routing protocols (IGP, BGP)
  - Data plane: forwarding table (FIB)

Forwarding table

Network	Nexthop
10.1.0.0/24	10.2.0.2
10.1.1.8/30	10.2.1.2

Forwarding table

Network	Nexthop
10.1.0.0/24	10.1.0.2
10.1.1.8/30	10.1.1.2

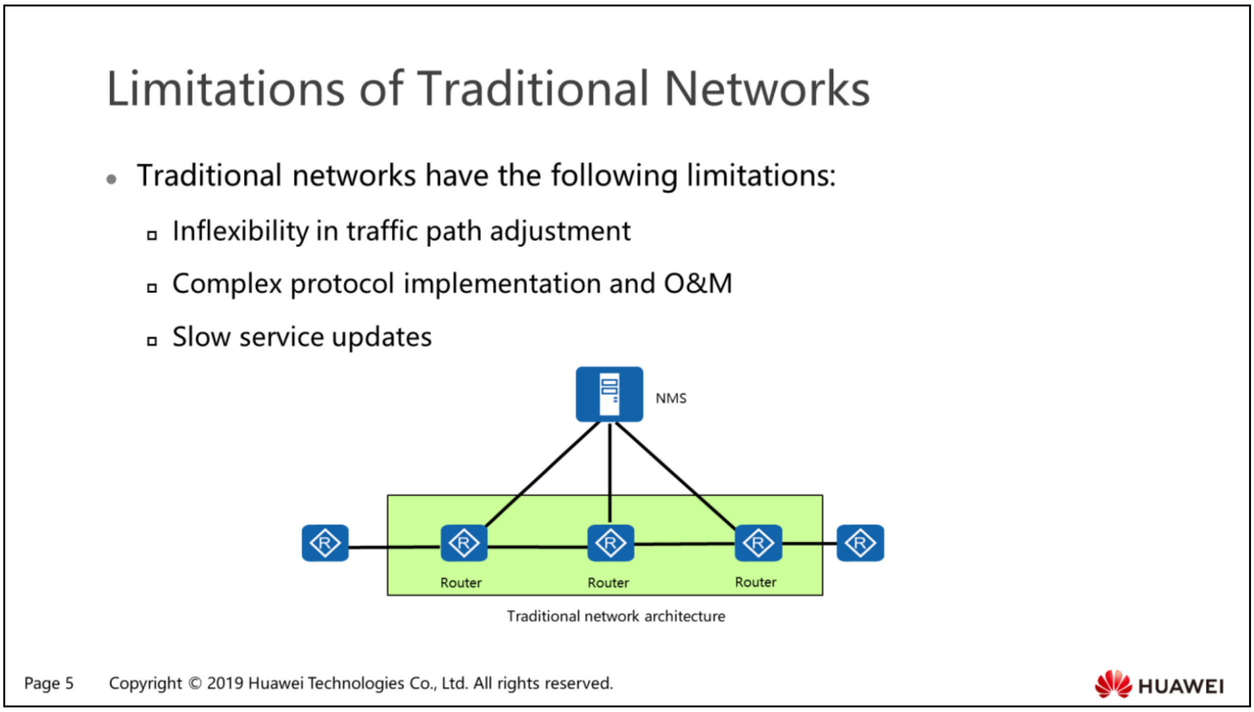
Forwarding table

Network	Nexthop
10.1.0.0/24	10.3.0.2
10.1.1.8/30	10.3.1.2

Forwarding table

Network	Nexthop
10.1.0.0/24	10.4.0.2
10.1.1.8/30	10.4.1.2

- OSS: Operation Support System
- NMS: Network Management Server
- In the traditional network architecture:
  - A network has a management plane, a control plane, and a data plane.
  - The management plane consists of device management and service management systems. The device management system manages network topologies, device interfaces, and device features, and can deliver configuration scripts to devices. The service management system provides functions such as service performance monitoring and service alarm management.
  - The control plane is responsible for protocol processing and calculation. For example, routing protocols are used to calculate routes and create routing tables.
  - The data plane processes and forwards service packets according to instructions from the control plane. For example, routers forward received data packets through corresponding outbound interfaces according to routing tables generated by routing protocols.

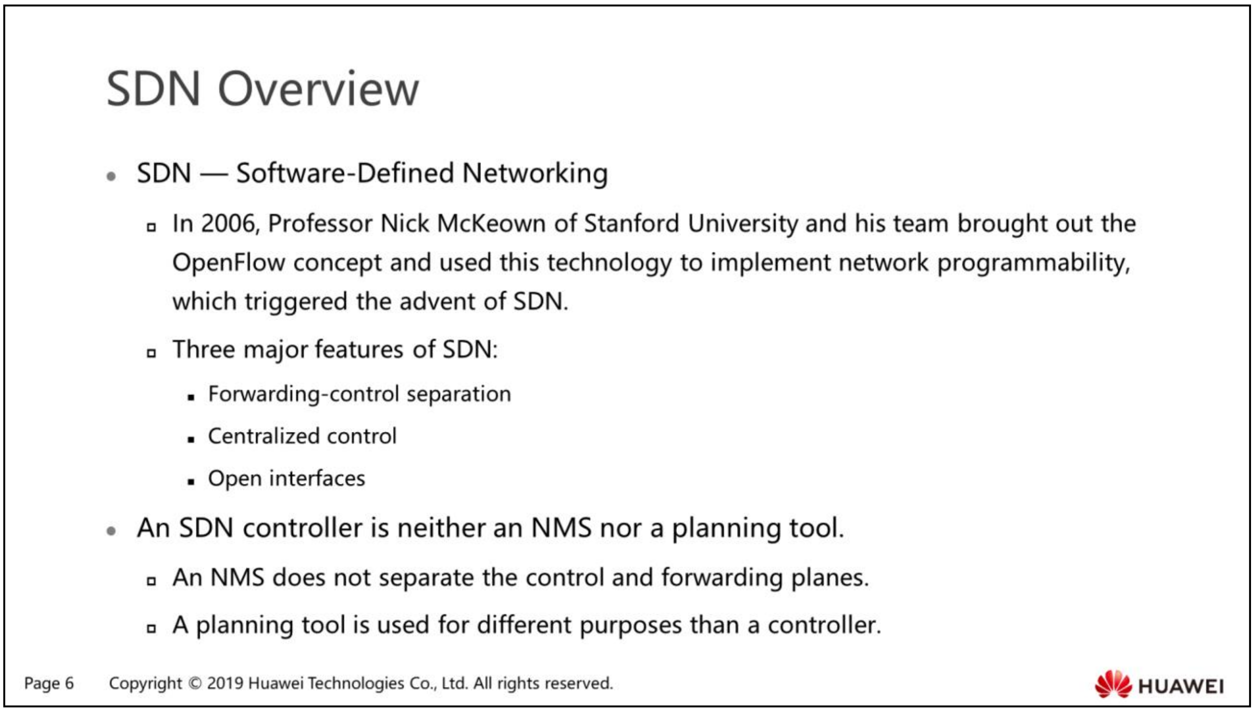


Limitations of Traditional Networks

- Traditional networks have the following limitations:
  - Inflexibility in traffic path adjustment
  - Complex protocol implementation and O&M
  - Slow service updates

Traditional network architecture

- Limitations of traditional networks:
  - On a traditional network, a network management system is usually deployed as the management plane, whereas the control plane and data plane are distributed on each network device.
  - To change traffic paths, new traffic policies need to be configured on network elements. This method, however, is time-consuming and prone to errors, especially on a large-scale network. Traffic paths can also be adjusted by configuring TE tunnels, but the complex TE tunnel configuration requires high technical skills of maintenance personnel.
  - Traditional networks use complex protocols, such as IGP, BGP, MPLS, and multicast protocols, and more protocols are continuously introduced into the networks.
  - Equipment vendors also develop their proprietary protocols. Network devices have large numbers of commands, and operation interfaces of devices from different vendors vary greatly, making network operation and maintenance complex.
  - It may take a long time to deploy a new function on a traditional network, because the control planes of network devices are closed, and devices from different vendors may use different control mechanisms. Additionally, software upgrades need to be performed on every device, which greatly reduces the work efficiency.

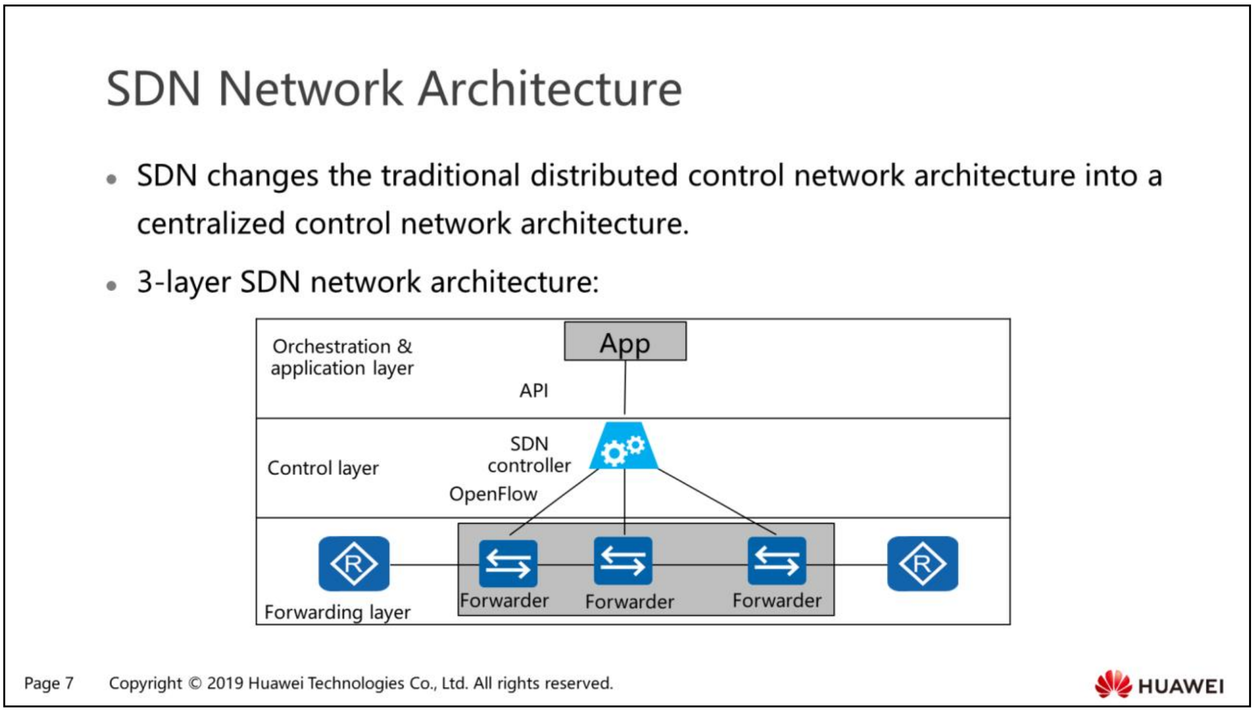


SDN Overview

- SDN — Software-Defined Networking
  - In 2006, Professor Nick McKeown of Stanford University and his team brought out the OpenFlow concept and used this technology to implement network programmability, which triggered the advent of SDN.
  - Three major features of SDN:
    - Forwarding-control separation
    - Centralized control
    - Open interfaces
- An SDN controller is neither an NMS nor a planning tool.
  - An NMS does not separate the control and forwarding planes.
  - A planning tool is used for different purposes than a controller.

HUAWEI

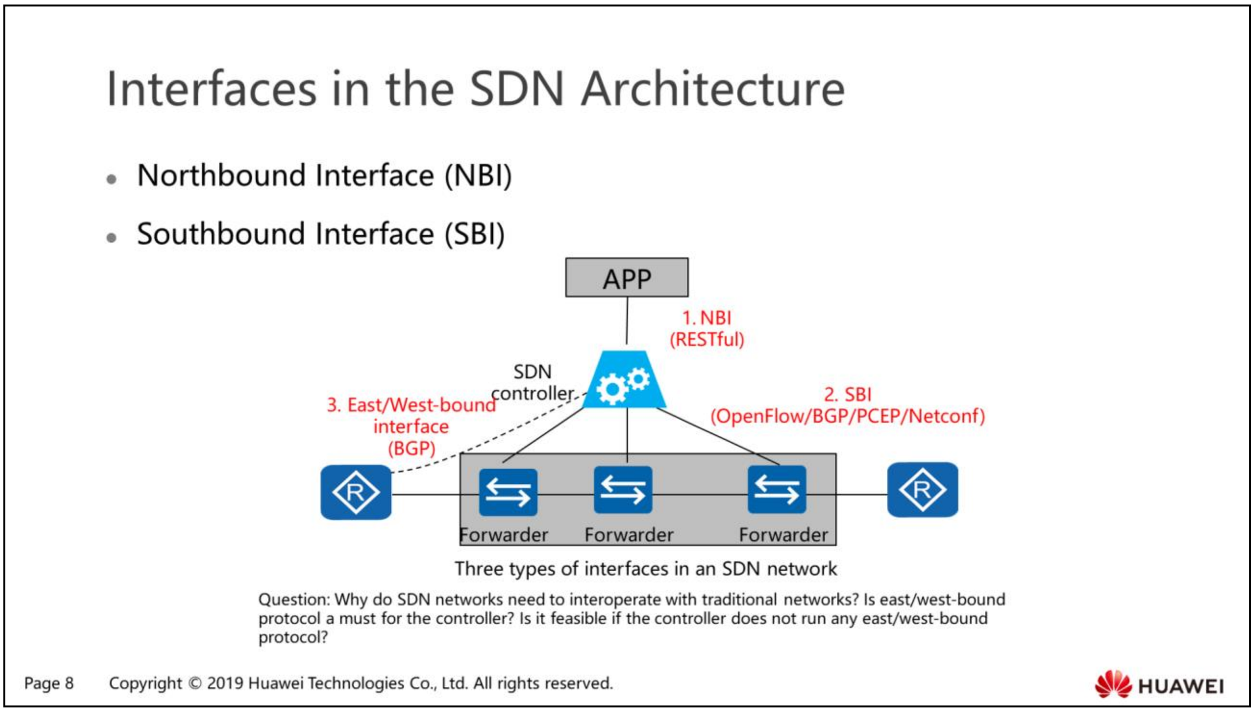
- SDN has three major features:
  - Forwarding-control separation: The control plane of network elements is moved to a controller, which completes protocol calculation and creates flow tables. The forwarding plane is located on network devices.
  - Centralized control: A controller centrally manages network elements and delivers flow tables. You only need to configure the controller and do not need to perform the configuration on network devices.
  - Open interfaces: To deploy third-party applications, you only need to program new network functions using the open interfaces provided by the controller and run the functions on the controller.
- An SDN controller is neither a network management system nor a planning tool.
  - A network management system does not separate the control and forwarding planes. It only performs management operations, for example, manages network topologies, monitors device alarms and performance, and delivers configuration scripts. Forwarding entries still need to be generated on control planes of network devices.
  - A planning tool is used for different purposes than a controller. A planning tool delivers parameters for control planes of network elements, such as IP addresses and VLAN IDs, but not forwarding entries. A controller delivers flow table entries for data packet forwarding.



SDN Network Architecture

- SDN changes the traditional distributed control network architecture into a centralized control network architecture.
- 3-layer SDN network architecture:

- Orchestration and application layer: This layer consists of application programs meeting service requirements of users, including OSS and OpenStack. Same as a traditional IP network, an SDN network also has a forwarding plane, a control plane, and a management plane. The difference is that the traditional IP network architecture uses a distributed control model, whereas the SDN architecture uses a centralized control model.
- Control layer: The control layer is the control center of the network system. It generates internal switching paths and cross-border service routes, and processes network state change events.
- Forwarding layer: This layer is the basic network consisting of forwarders and connectors and implements data forwarding. The forwarding entries are generated by the control layer.



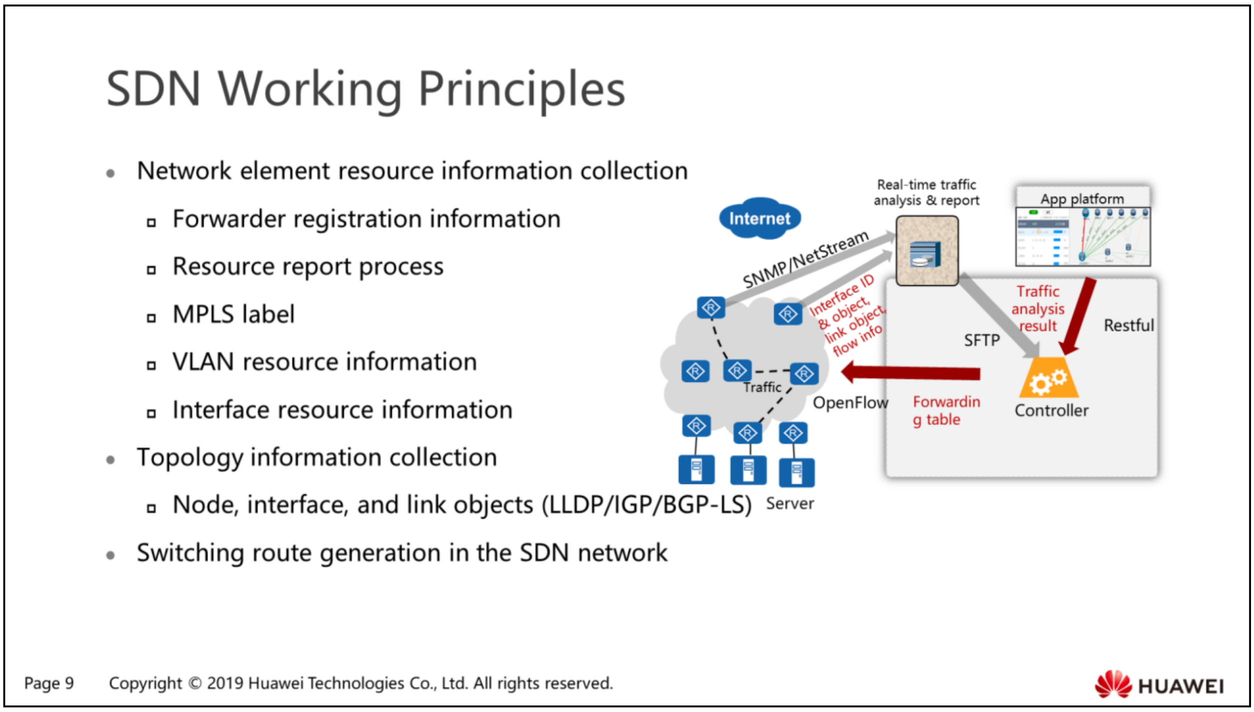
Interfaces in the SDN Architecture

- Northbound Interface (NBI)
- Southbound Interface (SBI)

Three types of interfaces in an SDN network

Question: Why do SDN networks need to interoperate with traditional networks? Is east/west-bound protocol a must for the controller? Is it feasible if the controller does not run any east/west-bound protocol?

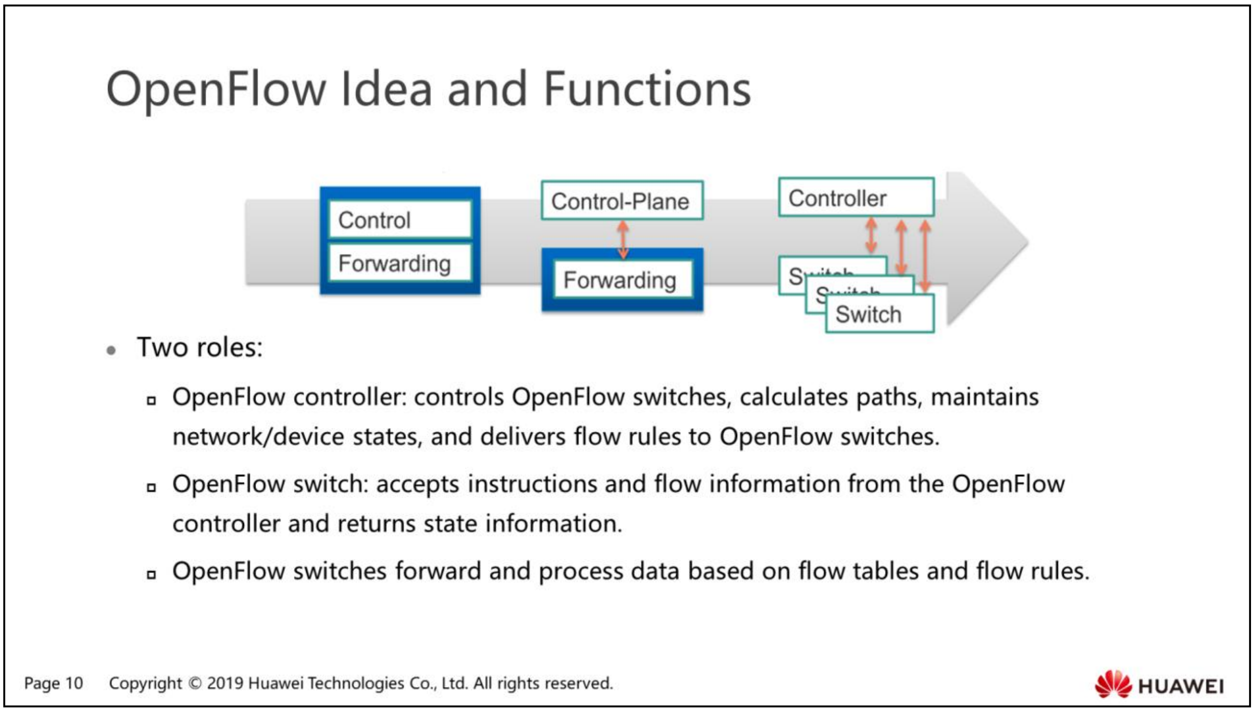
- RESTful interface:
  - RESTful interfaces are northbound interfaces between a controller and upper-layer applications. Open APIs, proprietary interfaces of network devices, and all the Internet software architectures complying with the Representational State Transfer (REST) standard are RESTful.
  - REST means that an accessed resource (text, image, audio, or video) transitions from one state to another state. It is essentially an Internet resource access protocol.
- OpenFlow interface:
  - The OpenFlow interface is a chip-based interface protocol used between a controller and downstream forwarders. The OpenFlow protocol implements communication between the controller and forwarders based on TCP/IP.
- BGP interface:
  - The BGP interface adds some BGP route attributes (such as the Additional Path and BGP Flow Specification attributes) to the BGP protocol. These BGP route attributes are used to deliver BGP route features, based on which egress routers of an IDC can optimize traffic paths.
- PCE interface:
  - The Path Computation Element (PCE) interface enables a controller to calculate traffic engineering paths based on available network bandwidth, so that TE tunnels can be established within ASs of a data center.
- Carriers have deployed large-scale distributed networks and will not upgrade their traditional networks to SDN networks in a short period of time. Therefore, interoperability with traditional networks is necessary for SDN networks. An SDN controller must support various traditional inter-domain routing protocols to enable interoperation with traditional networks.
- East/West-bound protocol is a must for an SDN controller. An east/west-bound protocol enables the SDN controller to provide new services through simple modification or upgrade of controller programs. East/West-bound protocols also provide interfaces for cross-regional SDN controller interconnection and hierarchical controller deployment.



SDN Working Principles

- Network element resource information collection
  - Forwarder registration information
  - Resource report process
  - MPLS label
  - VLAN resource information
  - Interface resource information
- Topology information collection
  - Node, interface, and link objects (LLDP/IGP/BGP-LS)
- Switching route generation in the SDN network

- Generally, the controller acts as a server, and forwarders initiate control connection setup with it. After the forwarders are successfully authenticated, control connections can be set up between the controller and forwarders.
- Register messages sent from a device carry resource information (such as interface, label, and VLAN resources) and vendor-defined information (including device type, version number, and device ID). The controller collects such information for local search and driver program loading.
- Network topology information describes network nodes, links, and connections between network nodes.
- The controller collects topology information so that it can calculate proper paths based on network resources and deliver flow tables with path information to forwarders.



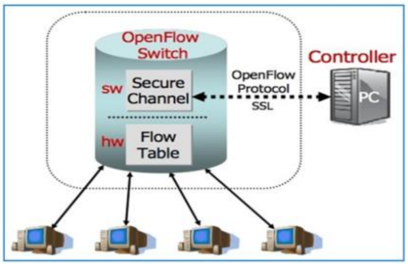
OpenFlow Idea and Functions

- Two roles:
  - OpenFlow controller: controls OpenFlow switches, calculates paths, maintains network/device states, and delivers flow rules to OpenFlow switches.
  - OpenFlow switch: accepts instructions and flow information from the OpenFlow controller and returns state information.
  - OpenFlow switches forward and process data based on flow tables and flow rules.

- A flow is a group of data packets with the same properties, such as 5-tuple information (source IP address, destination IP address, source port, destination port, and protocol).
- The OpenFlow protocol is a control protocol used between the controller and forwarders.
- Switches can communicate with the controller using encrypted OpenFlow protocol.
- OpenFlow switches provide the data plane. They forward data traffic based on flow tables and enforce network policies.
- The OpenFlow controller provides the control plane. It creates, updates, and maintains flow tables for OpenFlow switches.
- An OpenFlow switch has the following basic elements:
  - Flow table: saves the properties and behavior defined for each flow.
  - Secure network channel: connects the switch and controller and transfers control messages. When a new data packet arrives at the switch for the first time, the switch sends the packet to the controller through the channel for route resolution.
  - OpenFlow protocol: a set of open standard interfaces used to read and write flow tables.

OpenFlow Network Switching Model

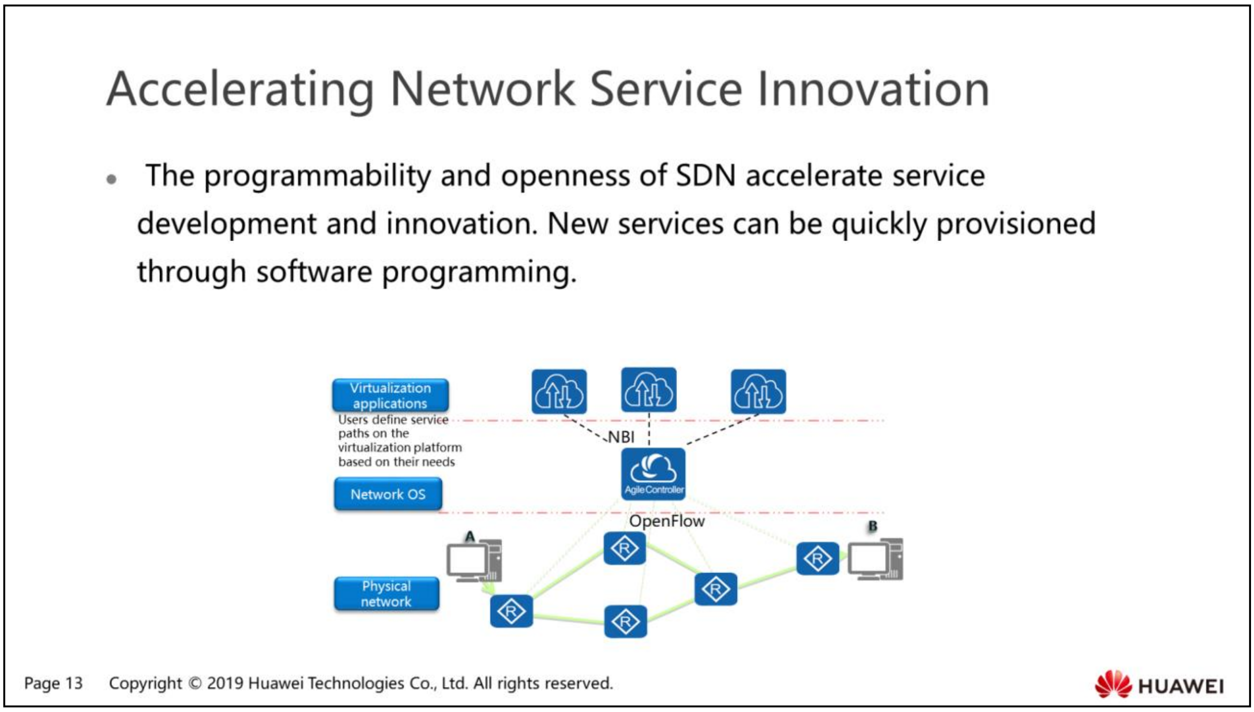
- This model simplifies underlying data communication (switches and routers), defines an open public application programming interface (API) for flow tables, and uses a controller to control the entire network.



OpenFlow system architecture

Contents

1. SDN Concept and Architecture
2. **Benefits of SDN**
3. Ways of SDN Evolution



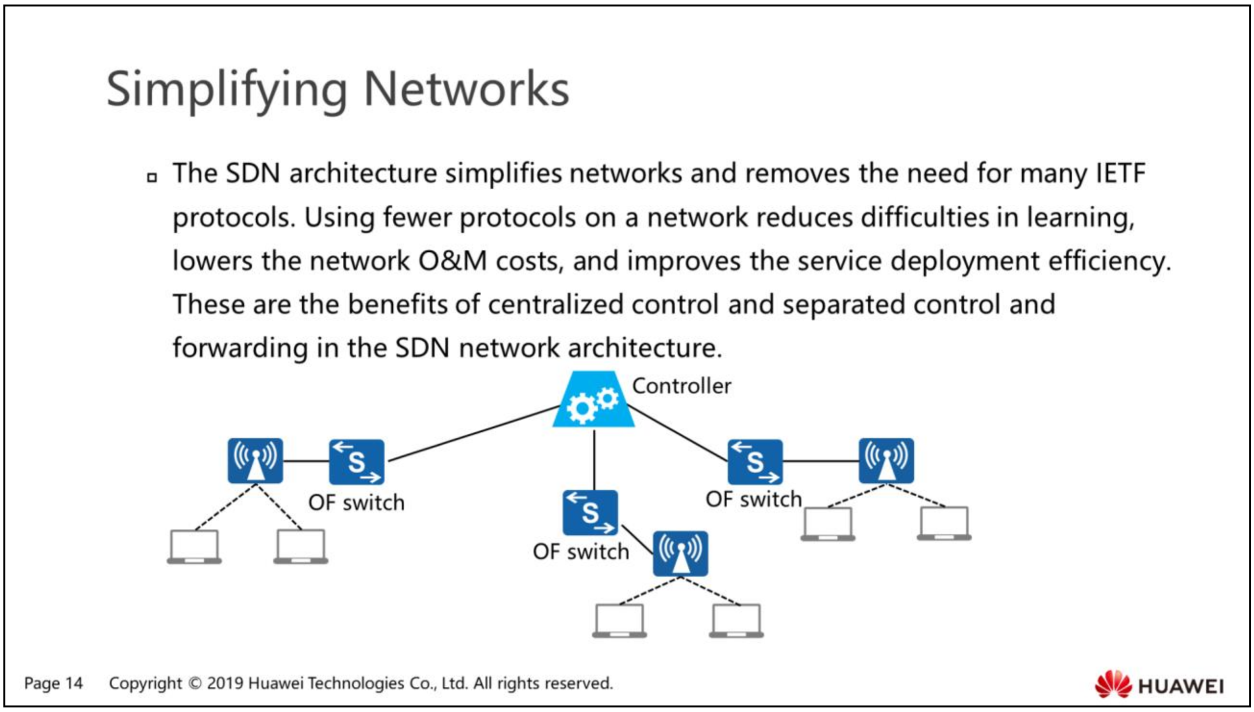
Accelerating Network Service Innovation

- The programmability and openness of SDN accelerate service development and innovation. New services can be quickly provisioned through software programming.

Virtualization applications
Users define service paths on the virtualization platform based on their needs
NBI
Network OS
AgileController
OpenFlow
A
B
Physical network

Page 13 HUAWEI

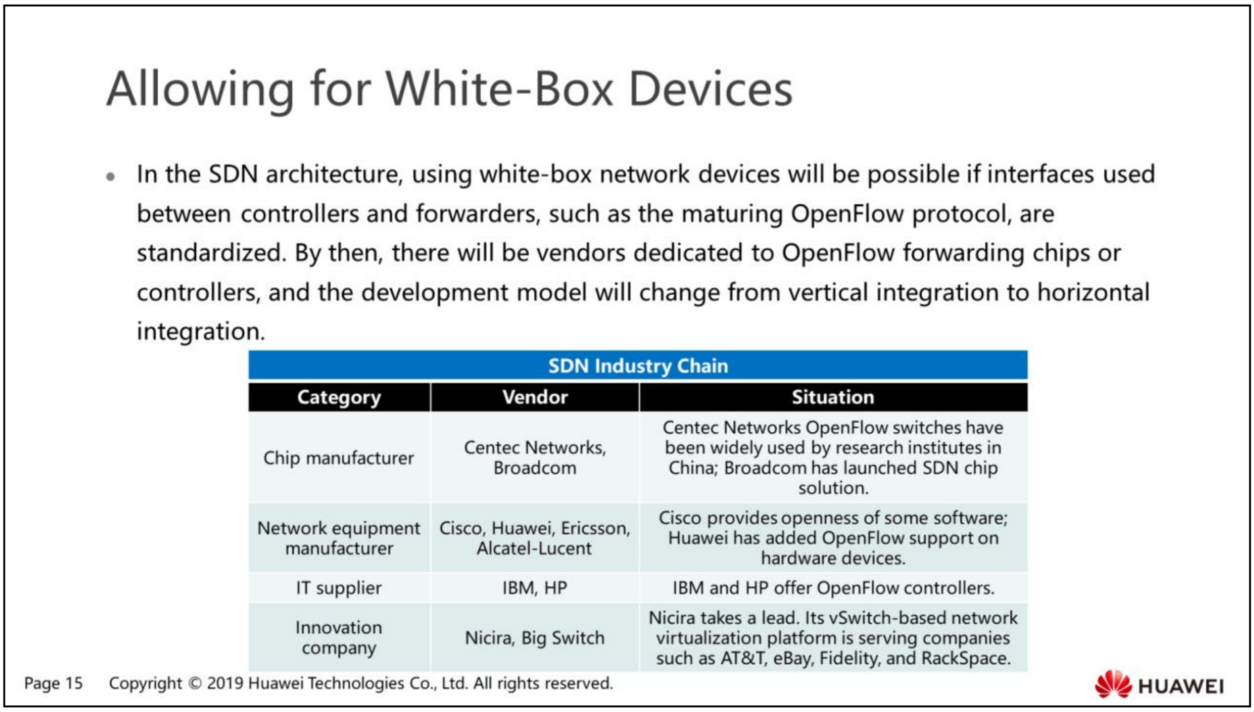
- SDN introduces an SDN controller to the network architecture so that the control plane is concentrated on the SDN controller, unlike the distributed control planes in the traditional network architecture. The SDN controller provides centralized network control. The SDN network architecture has three major features: forwarding-control separation, centralized control, and open interfaces.
- The centralized SDN controller simplifies the network and accelerates service innovation. Essentially, SDN improves network programmability by using the SDN controller to define network functions based on software. The SDN network architecture still has the management plane, control plane, and data plane. It just reallocates functions of these planes. In the traditional network architecture, the control plane is distributed on every forwarding device. In the SDN network architecture, the control plane is concentrated on an SDN controller, whereas the management plane and data plane are basically the same as those in the traditional network architecture.
- An SDN network provides fast innovation capability. Valuable services can be retained, and valueless services can be quickly withdrawn. On traditional networks, it usually takes several years to deploy a new service, because people need to propose, discuss about, and define the new service, then develop a standard protocol, and finally upgrade all network devices. SDN shortens the new service provisioning time from several years to several months or even shorter.



Simplifying Networks

- The SDN architecture simplifies networks and removes the need for many IETF protocols. Using fewer protocols on a network reduces difficulties in learning, lowers the network O&M costs, and improves the service deployment efficiency. These are the benefits of centralized control and separated control and forwarding in the SDN network architecture.

- Centralized control in the SDN network architecture removes the need for many protocols, such as RSVP, LDP, MBGP, and PIM. Because the controller calculates paths, creates flow tables, and delivers flow tables to forwarders, forwarders do not need to run these protocols for path calculation. In the future, many east/west-bound protocols will be removed from networks, whereas north/south-bound protocols such as OpenFlow will evolve continuously to meet requirements of the SDN network architecture.



Allowing for White-Box Devices

- In the SDN architecture, using white-box network devices will be possible if interfaces used between controllers and forwarders, such as the maturing OpenFlow protocol, are standardized. By then, there will be vendors dedicated to OpenFlow forwarding chips or controllers, and the development model will change from vertical integration to horizontal integration.

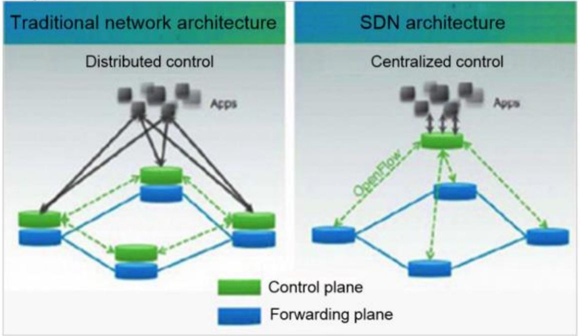
SDN Industry Chain

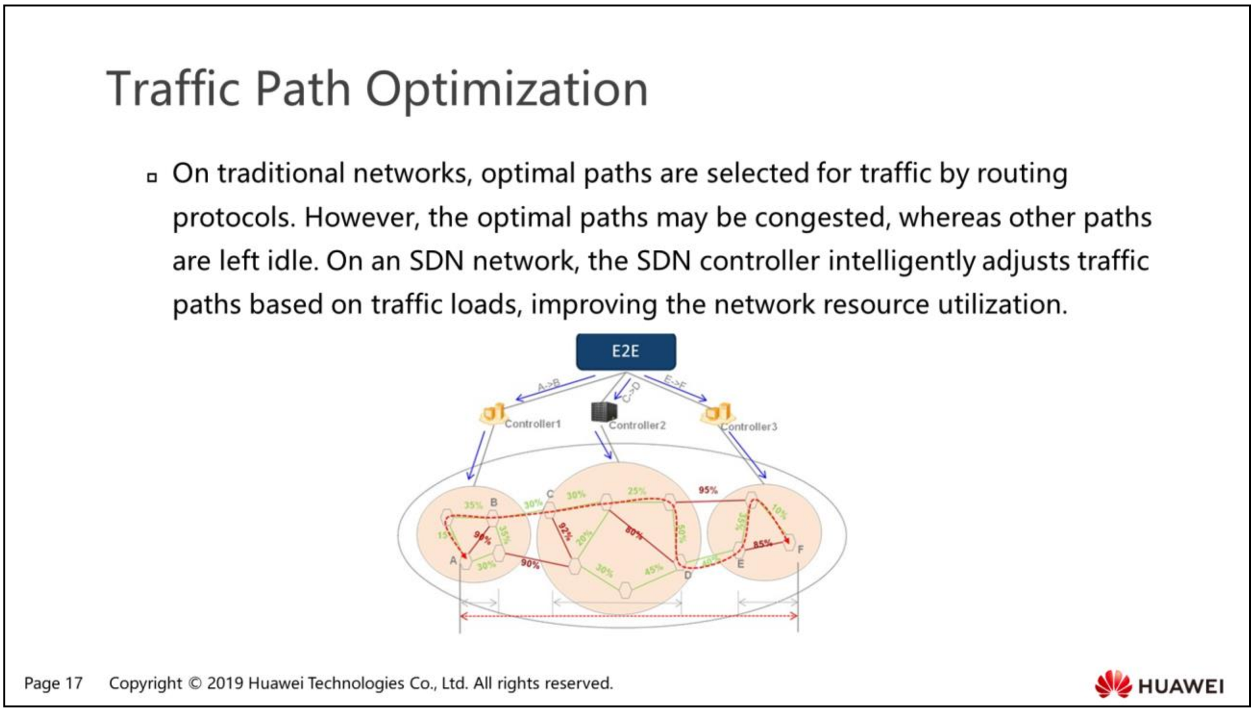
Category	Vendor	Situation
Chip manufacturer	Centec Networks, Broadcom	Centec Networks OpenFlow switches have been widely used by research institutes in China; Broadcom has launched SDN chip solution.
Network equipment manufacturer	Cisco, Huawei, Ericsson, Alcatel-Lucent	Cisco provides openness of some software; Huawei has added OpenFlow support on hardware devices.
IT supplier	IBM, HP	IBM and HP offer OpenFlow controllers.
Innovation company	Nicira, Big Switch	Nicira takes a lead. Its vSwitch-based network virtualization platform is serving companies such as AT&T, eBay, Fidelity, and RackSpace.

- Vertical integration is a model where one vendor provides software, hardware, and services. Horizontal integration is a model where each vendor provides a component of a product and an integrator integrates all components and sells the product. This horizontal division facilitates independent evolution and update of each component, accelerates product evolution, promotes competition, and helps to lower the purchase prices of components.

Service Automation

- In the SDN architecture, a controller controls the entire network. The SDN controller automatically completes deployment of network services, such as L2VPN and L3VPN, and shields specific internal implementations, enabling network service automation without the need for any other systems.





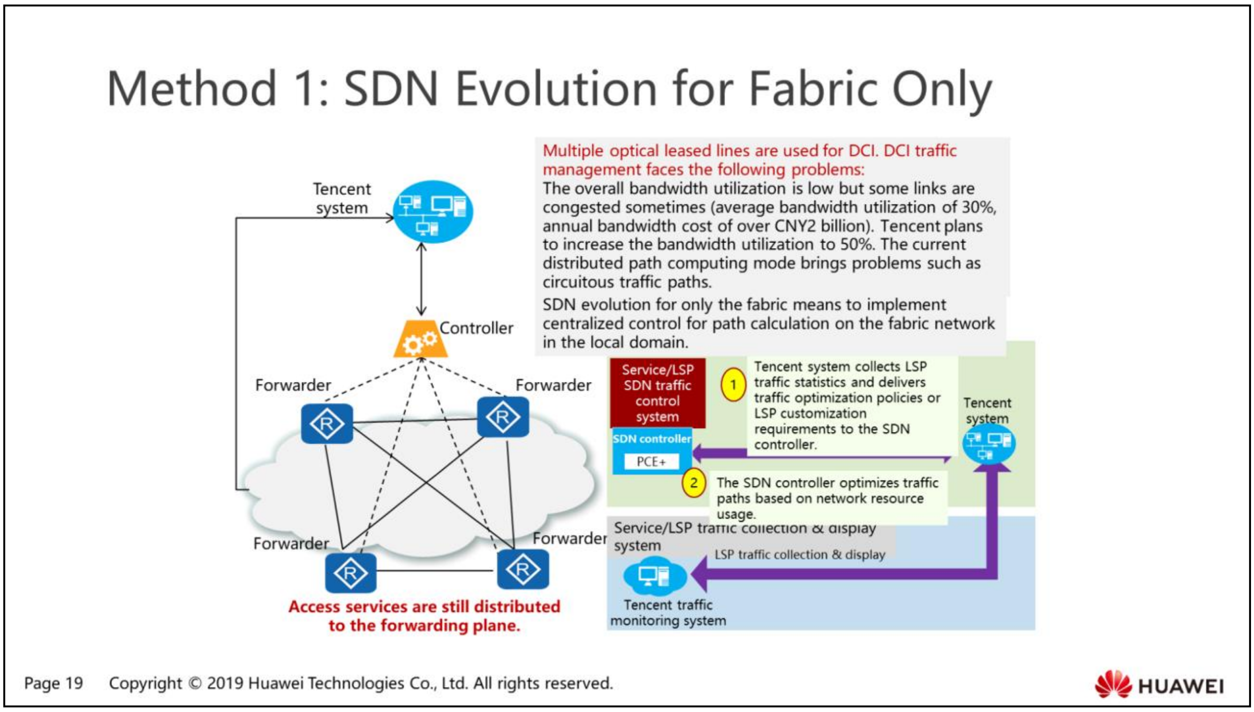
Traffic Path Optimization

- On traditional networks, optimal paths are selected for traffic by routing protocols. However, the optimal paths may be congested, whereas other paths are left idle. On an SDN network, the SDN controller intelligently adjusts traffic paths based on traffic loads, improving the network resource utilization.

- Actually, traditional networks also have some traffic engineering technologies to cope with congestion of optimal paths. MPLS TE is such a traffic engineering technology. Like other traditional protocols, MPLS TE uses the distributed model, so path selection depends on the service processing sequence. Another traffic engineering protocol, RSVP, cannot be deployed on a large-scale network because of its soft state mechanism. In the SDN architecture, path calculation and tunnel setup are completed by a centralized controller, without the need for the RSVP protocol. This architecture implements dynamic path adjustment and removes the dependency on the service processing sequence.

Contents

1. SDN Concept and Architecture
2. Benefits of SDN
3. **Ways of SDN Evolution**



Method 1: SDN Evolution for Fabric Only

Multiple optical leased lines are used for DCI. DCI traffic management faces the following problems:
The overall bandwidth utilization is low but some links are congested sometimes (average bandwidth utilization of 30%, annual bandwidth cost of over CNY2 billion). Tencent plans to increase the bandwidth utilization to 50%. The current distributed path computing mode brings problems such as circuitous traffic paths.

SDN evolution for only the fabric means to implement centralized control for path calculation on the fabric network in the local domain.

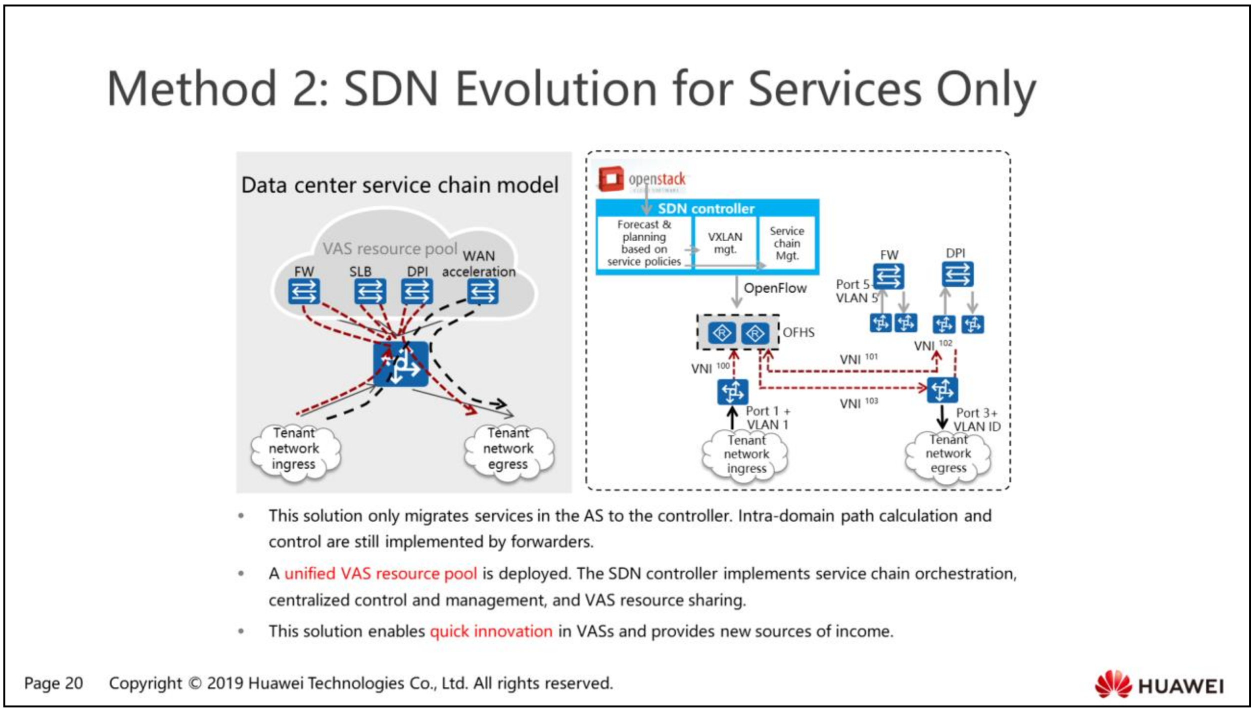
Tencent system
Controller
Forwarder
Forwarder
Forwarder
Forwarder
Service/LSP SDN traffic control system
SDN controller
PCE+
Tencent system
Service/LSP traffic collection & display system
LSP traffic collection & display
Tencent traffic monitoring system

1 Tencent system collects LSP traffic statistics and delivers traffic optimization policies or LSP customization requirements to the SDN controller.

2 The SDN controller optimizes traffic paths based on network resource usage.

Access services are still distributed to the forwarding plane.

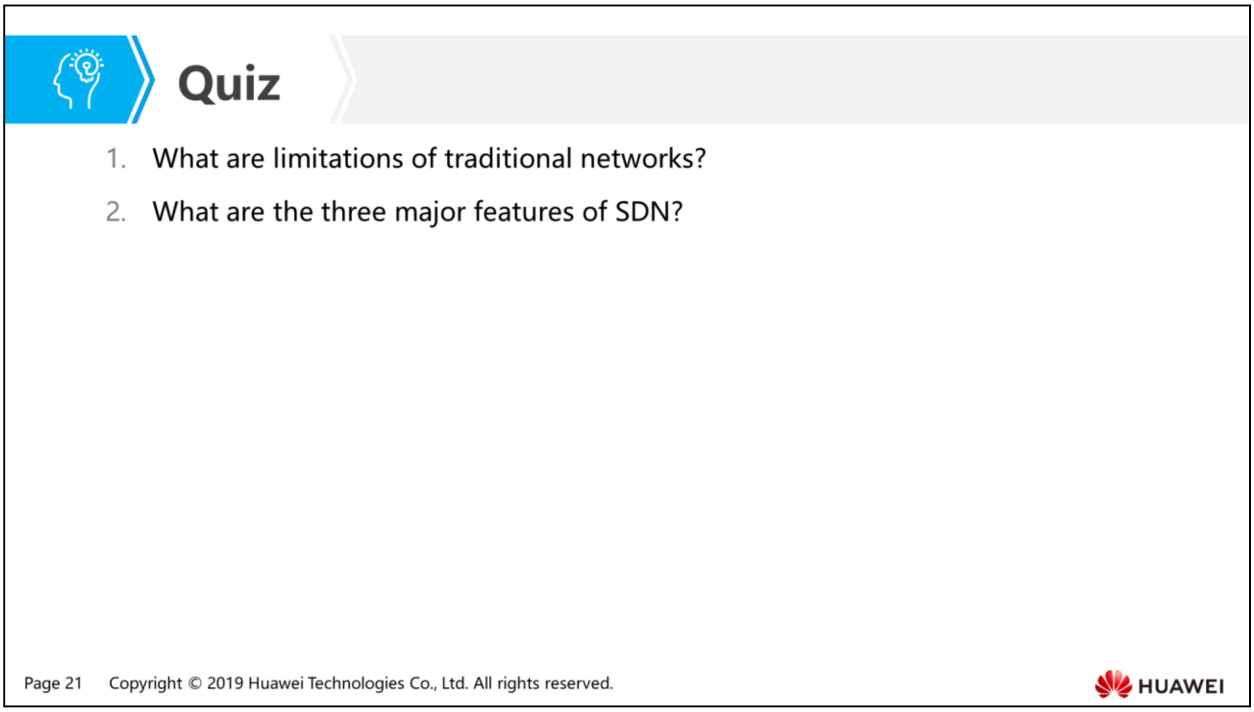
- This solution implements centralized control for path calculation on the fabric network in the local domain.
- The controller only provides intra-domain path calculation and control.



Method 2: SDN Evolution for Services Only

- This solution only migrates services in the AS to the controller. Intra-domain path calculation and control are still implemented by forwarders.
- A unified VAS resource pool is deployed. The SDN controller implements service chain orchestration, centralized control and management, and VAS resource sharing.
- This solution enables quick innovation in VASs and provides new sources of income.

- This solution only migrates services in the autonomous system to the controller. Intra-domain path calculation and control are still implemented by forwarders.



Quiz

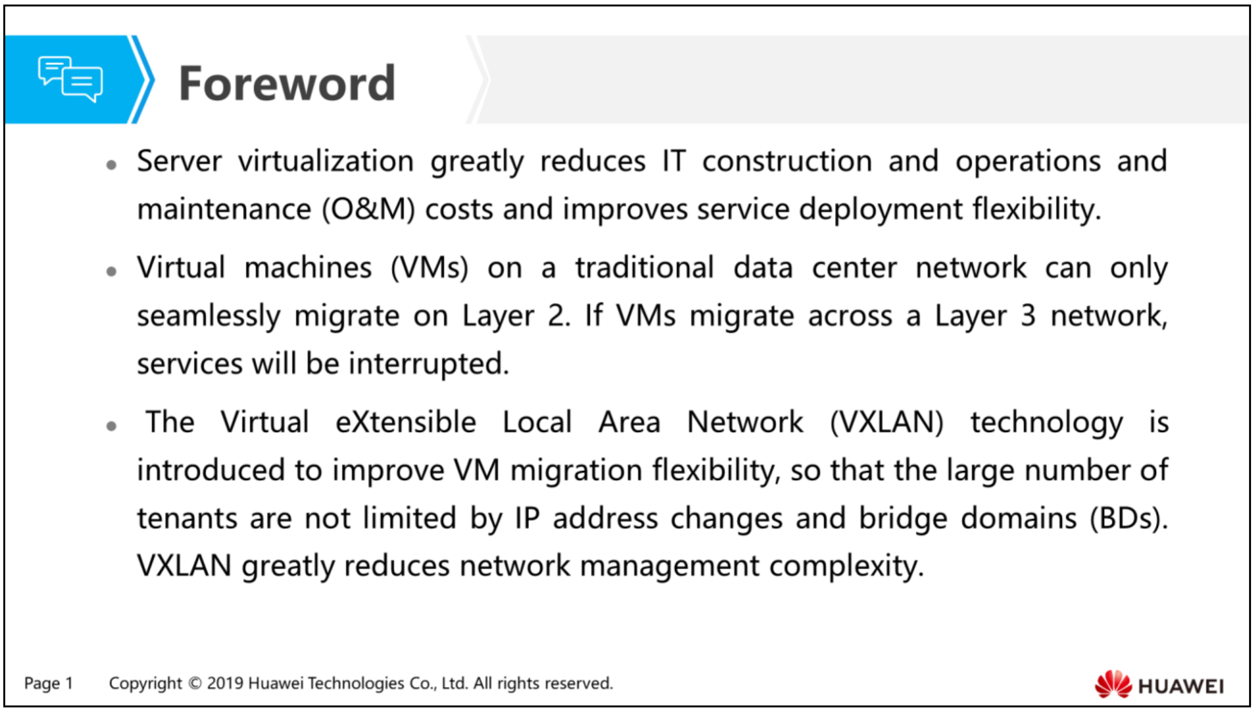
1. What are limitations of traditional networks?
2. What are the three major features of SDN?

- Answer: Major limitations include insufficient capability to flexibly adjust traffic paths, complex network protocol implementation and O&M, and slow update of services.
- Answer: Forwarding-control separation, centralized control, and open interfaces.

Thank You

www.huawei.com

VXLAN Overview



Foreword

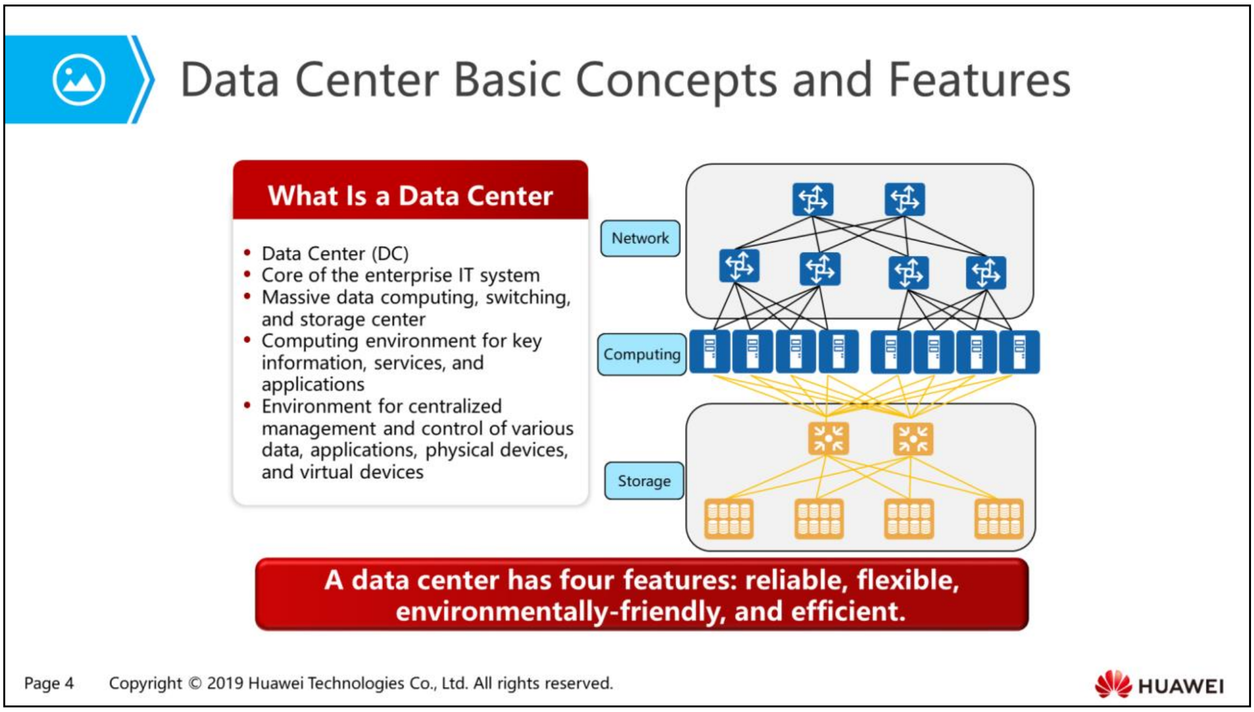
- Server virtualization greatly reduces IT construction and operations and maintenance (O&M) costs and improves service deployment flexibility.
- Virtual machines (VMs) on a traditional data center network can only seamlessly migrate on Layer 2. If VMs migrate across a Layer 3 network, services will be interrupted.
- The Virtual eXtensible Local Area Network (VXLAN) technology is introduced to improve VM migration flexibility, so that the large number of tenants are not limited by IP address changes and bridge domains (BDs). VXLAN greatly reduces network management complexity.

Objectives

- Upon completion of this section, you will be able to:
  - Understand challenges facing data center network
  - Be familiar with the basic principles of VXLAN
  - Master basic configurations of SDN-based VXLAN

Contents

1. **Challenges Facing Data Center Networks**
2. Basic VXLAN Principles
3. Basic VXLAN Configurations



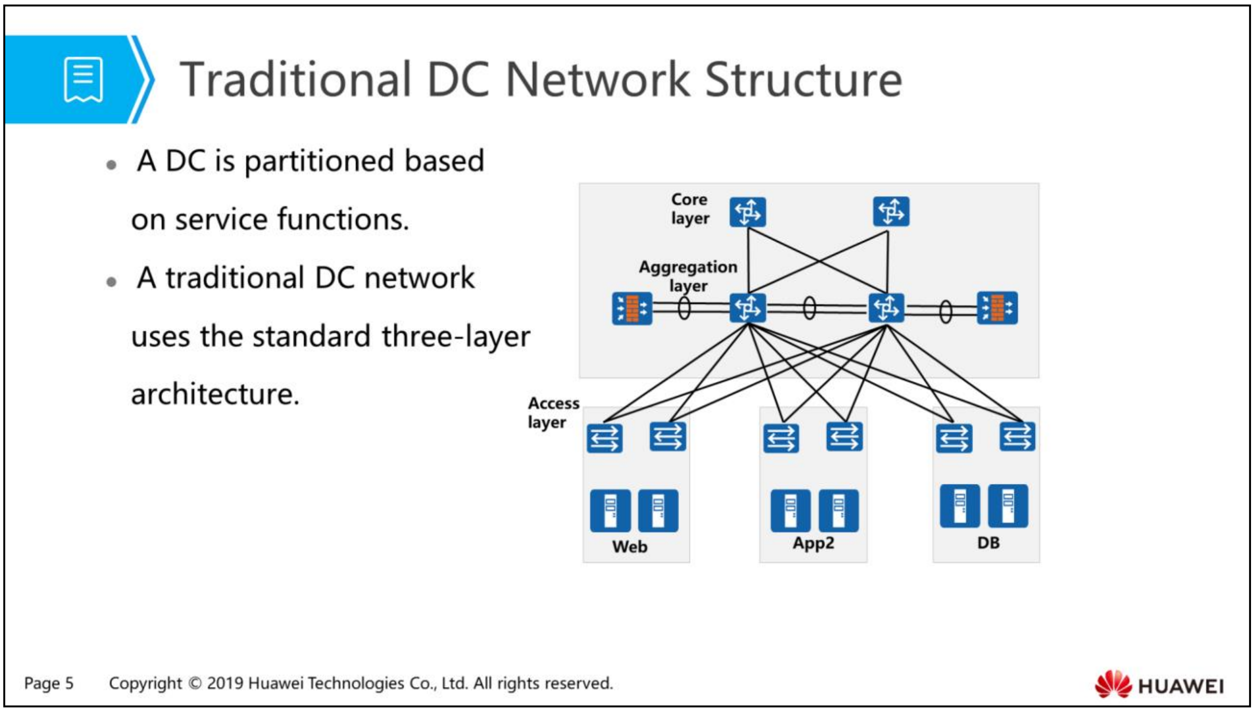
Data Center Basic Concepts and Features

What Is a Data Center

- Data Center (DC)
- Core of the enterprise IT system
- Massive data computing, switching, and storage center
- Computing environment for key information, services, and applications
- Environment for centralized management and control of various data, applications, physical devices, and virtual devices

A data center has four features: reliable, flexible, environmentally-friendly, and efficient.

- A Data Center (DC) is a collection of complete and complex systems consisting of the computing system, auxiliary devices (such as the communications and storage system), data communication system, environment control devices, monitoring devices, and various security devices.
- A data center stores, processes, transmits, switches, and manages information in a centralized mode within a physical space.
- Key devices in a data center include servers, network devices, and storage devices.
- Power supply system, air conditioning system, cabinets, fire protection system, monitoring system, and other systems that affect operating environment of the key devices are key physical facilities.
- An Internet Data Center (IDC) is a center for data storage and processing on the Internet that involves the most intensive data exchange.



Traditional DC Network Structure

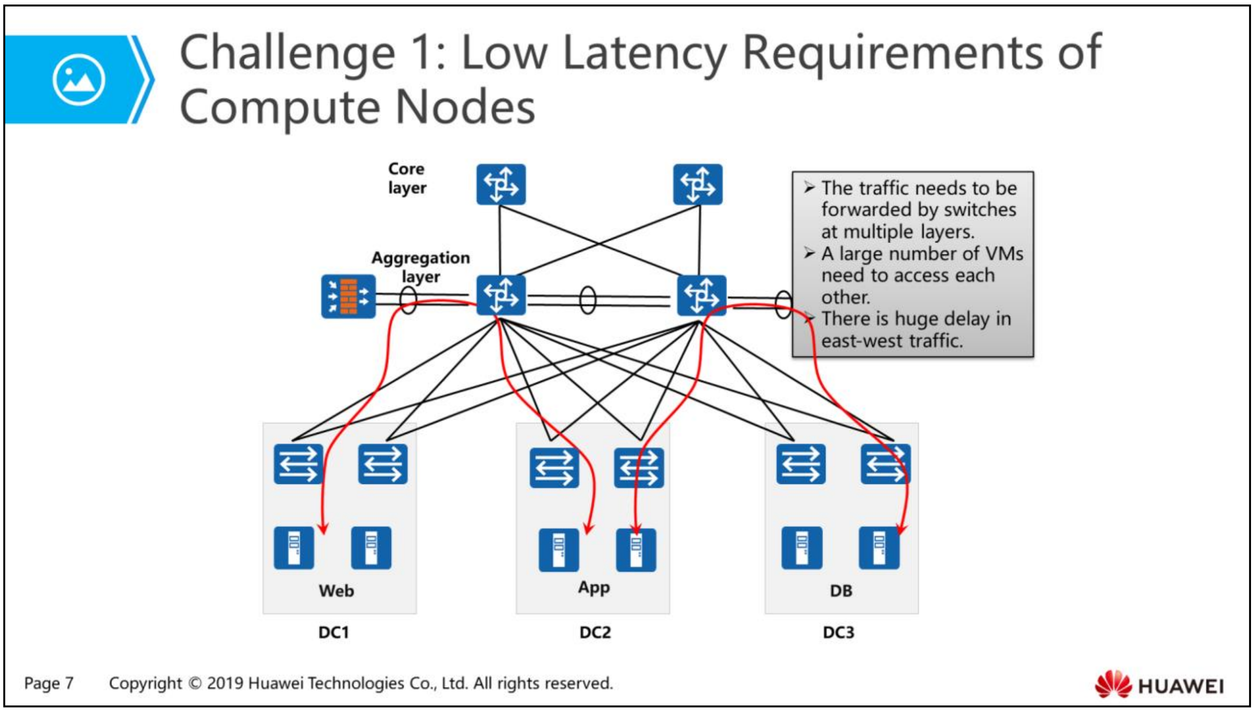
- A DC is partitioned based on service functions.
- A traditional DC network uses the standard three-layer architecture.

Page 5 HUAWEI

- The traditional network model supports DCs of various types in a long period of time.
- Based on functional modules, a traditional DC is divided into the core area, public server area, intranet server area, Internet server area, DC management area, data exchange and test server area, data storage area, and data disaster recovery (DR) area.
- According to the application types, the server area is divided into different layers, such as the database layer, application server layer, and web server layer.
- Typically, a traditional data center has three layers: access layer, aggregation layer, and core layer.

Contents

1. **Challenges Facing Data Center Networks**
   - Low Latency Requirements of Compute Nodes
   - Wide Application of Virtualization Technology
   - Network and Service Maintenance Automation
2. Basic VXLAN Principles
3. Basic VXLAN Configurations



Challenge 1: Low Latency Requirements of Compute Nodes

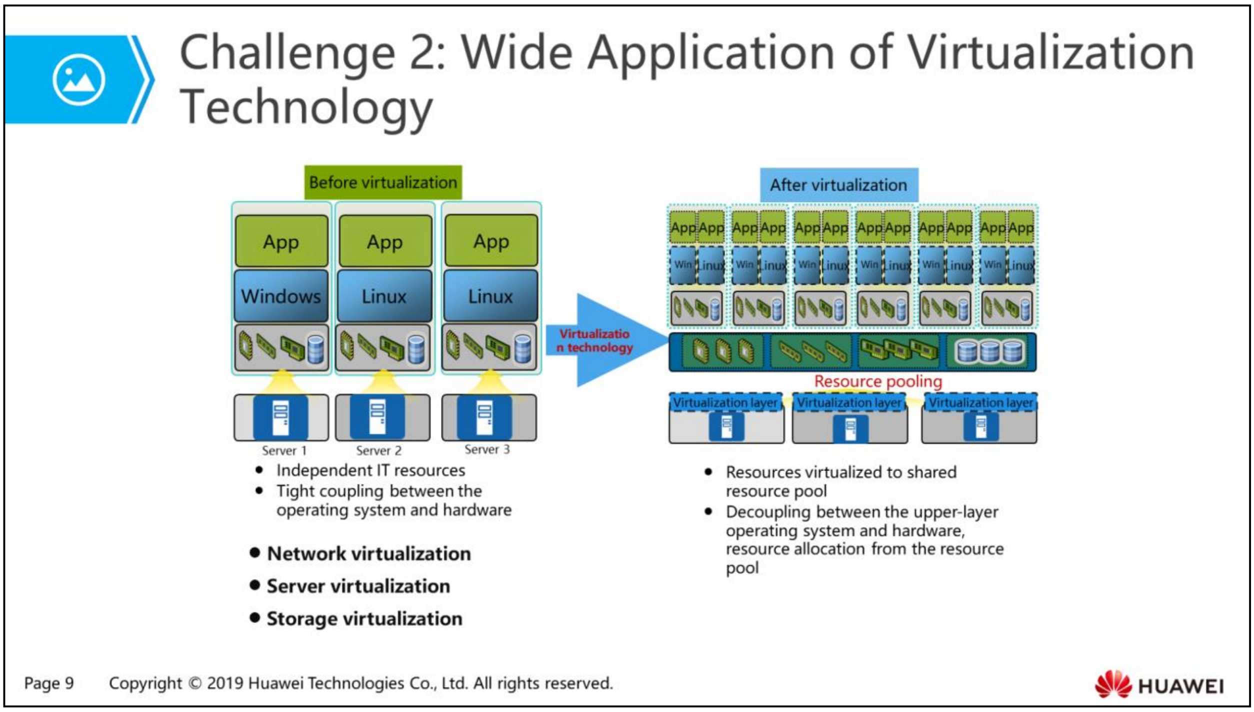
- The traffic needs to be forwarded by switches at multiple layers.
- A large number of VMs need to access each other.
- There is huge delay in east-west traffic.

HUAWEI

- A large number of VMs are deployed on a physical server, causing huge traffic concurrency.
- The data traffic model is converted from the traditional north-south traffic to east-west traffic.
- A large amount of many-to-one and many-to-many east-west traffic exists on the network.
- The devices on the access and aggregation layers need to provide high processing capabilities.

Contents

1. **Challenges Facing Data Center Networks**
   - Low Latency Requirements of Compute Nodes
   - Wide Application of Virtualization Technology
   - Network and Service Maintenance Automation
2. Basic VXLAN Principles
3. Basic VXLAN Configurations



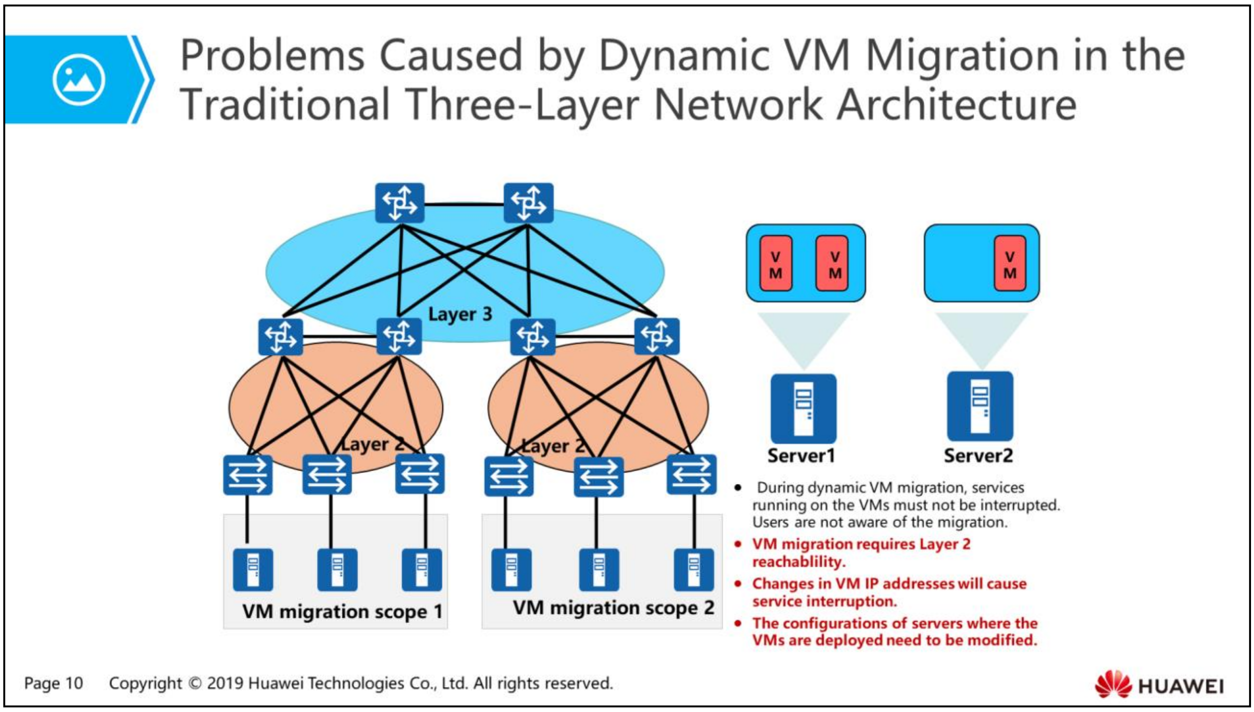
Challenge 2: Wide Application of Virtualization Technology

- Independent IT resources
- Tight coupling between the operating system and hardware

- Resources virtualized to shared resource pool
- Decoupling between the upper-layer operating system and hardware, resource allocation from the resource pool

- **Network virtualization**
- **Server virtualization**
- **Storage virtualization**

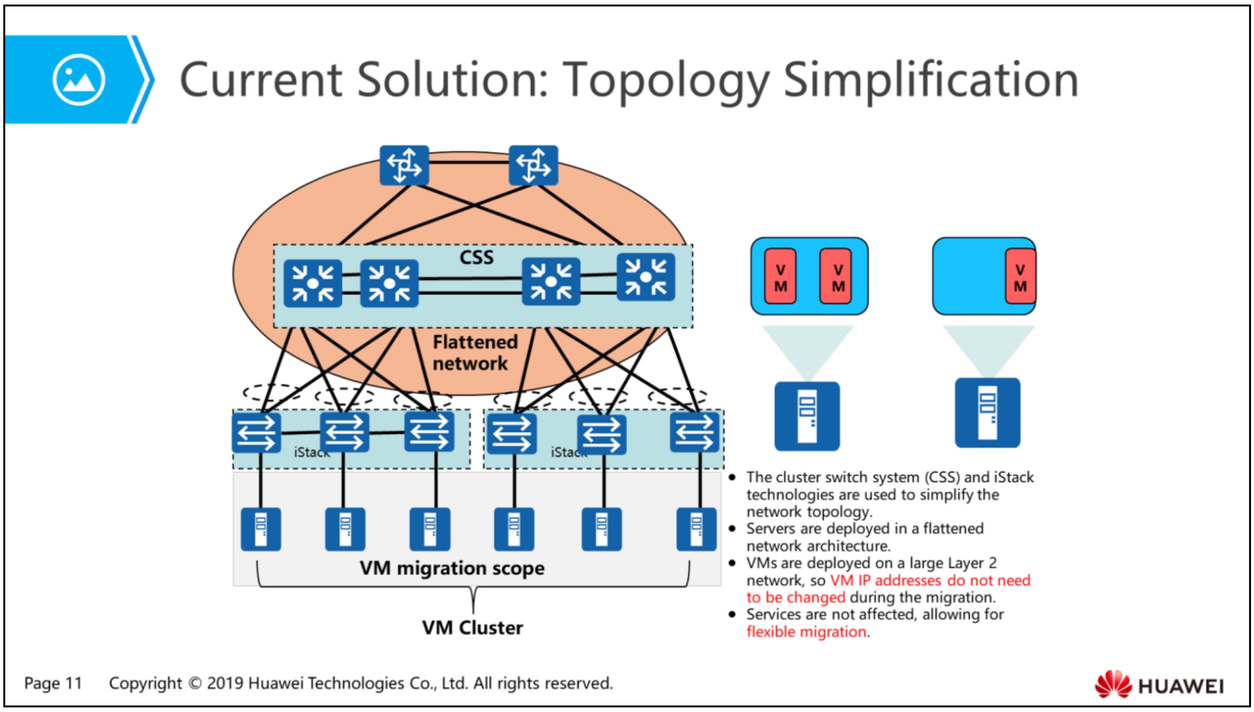
- In a traditional DC, servers are mainly used to provide services externally. Service areas can be isolated by security zone or VLAN.
- Generally, the computing, network, and storage resources required by a service are deployed centrally in one area. Access between different areas is prohibited or enabled through a Layer 3 network. Most network traffic in a DC is south-north traffic. In this design mode, computing resources cannot be shared among different areas, resulting in low resource utilization.
- By using the virtualization and cloud computing management technologies, resources in different areas form a resource pool, effectively improving the DC resource utilization.
- With the emergence of new technologies and applications, new services such as VM migration, data synchronization, data backup, and collaborative computing are deployed in DCs, greatly increasing internal east-west traffic.
- Dynamic VM migration is commonly used in actual applications. For example, before a user upgrades and maintains a server, the user can migrate VMs on the server to another server to ensure service continuity during the period. After the server upgrade and maintenance, the user can migrate VMs back to the original server.
- Dynamic VM migration technology can fully use computing resources. For example, an online shopping platform of a company provides promotion activities in one area during a specific period. The service volume greatly increases during this period. To effectively use resources, VMs in other areas with small service volume can be migrated to this area temporarily, providing that services in those areas are not interrupted. After the promotion activities, VMs can be migrated back to the original areas.



Problems Caused by Dynamic VM Migration in the Traditional Three-Layer Network Architecture

- During dynamic VM migration, services running on the VMs must not be interrupted. Users are not aware of the migration.
- **VM migration requires Layer 2 reachablility.**
- **Changes in VM IP addresses will cause service interruption.**
- **The configurations of servers where the VMs are deployed need to be modified.**

- Dynamic VM migration is the process of moving VMs from one physical server to another physical server, while ensuring continuity of services deployed on the VMs.
- End users are unaware of the dynamic VM migration process, so that the administrators can flexibly allocate server resources or maintain and upgrade the physical servers, without affecting normal server use by end users.
- If a VM migrates over a Layer 2 network, the VM IP address needs to be changed, causing interruption of services deployed on the original server. Besides, the configurations of other servers also need to be changed, leading to huge workload.



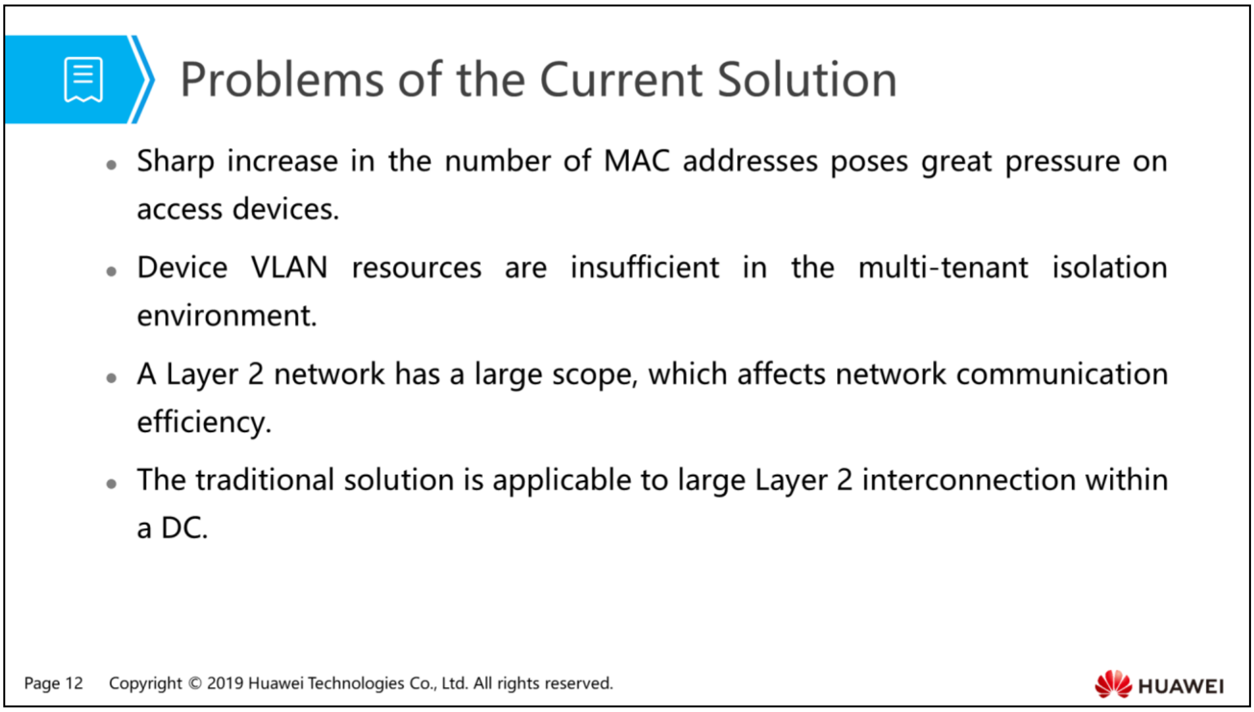
Current Solution: Topology Simplification

- The cluster switch system (CSS) and iStack technologies are used to simplify the network topology.
- Servers are deployed in a flattened network architecture.
- VMs are deployed on a large Layer 2 network, so VM IP addresses do not need to be changed during the migration.
- Services are not affected, allowing for flexible migration.

Page 11

HUAWEI

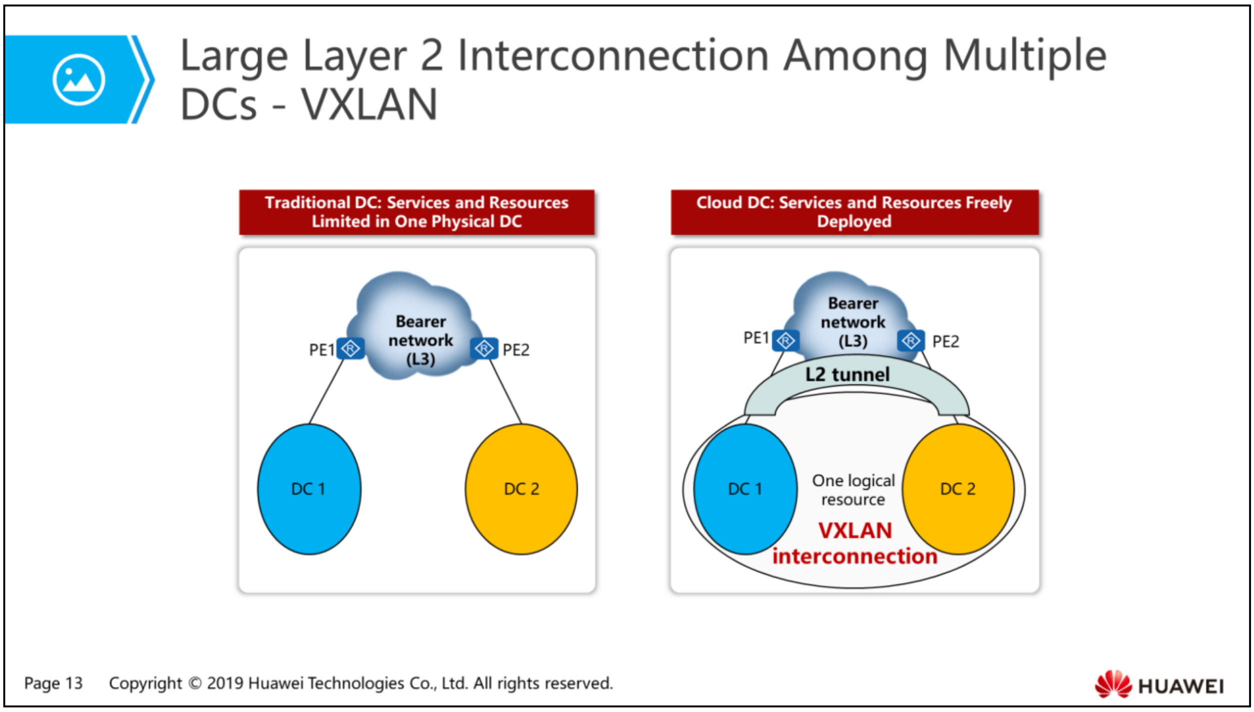
- To enable flexible VM migration in a large scope or even across regions, involved servers must be deployed on a large Layer 2 network to break through restrictions on VM migration across a Layer 3 network.
- CSS can be deployed on the core/aggregation layer and iStack can be deployed on the access layer to simplify the network topology.
- There is no need to enable Layer 2 loop prevention mechanisms such as Spanning Tree Protocol (STP) on devices. This effectively improves the link resource utilization.
- However, devices still have performance issues.
- This solution is suitable for VM migration within a DC.



Problems of the Current Solution

- Sharp increase in the number of MAC addresses poses great pressure on access devices.
- Device VLAN resources are insufficient in the multi-tenant isolation environment.
- A Layer 2 network has a large scope, which affects network communication efficiency.
- The traditional solution is applicable to large Layer 2 interconnection within a DC.

- Traditional Layer 2 technologies STP or CSS+iStack are not suitable for building large Layer 2 networks.
- VXLAN can construct a large Layer 2 network to improve the link bandwidth utilization.



Large Layer 2 Interconnection Among Multiple DCs - VXLAN

- In this early stage, VM management and migration are completed on physical networks. Therefore, the east-west traffic in a DC is mainly Layer 2 traffic.

- To extend the scale of a Layer 2 physical network and improve link utilization, large Layer 2 technologies, such as Transparent Interconnection of Lots of Links (TRILL) and Shortest Path Bridging (SPB) are developed.

- As the virtualized DC scale expands and cloud-based management becomes popular, VM management and migration on physical networks can no longer meet virtualization requirements. As a result, overlay technologies such as VXLAN and Network Virtualization using Generic Routing Encapsulation (NVGRE) are developed.

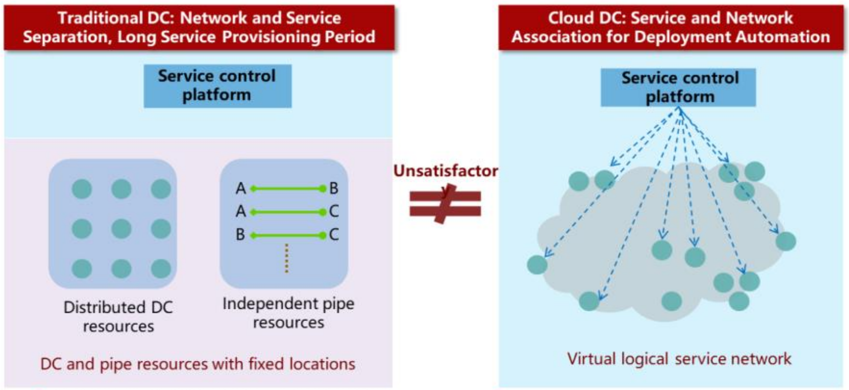
- In the overlay solution, east-west traffic on a physical network is gradually changed from Layer 2 traffic to Layer 3 traffic. In addition, the overlay solution changes the network topology from physical Layer 2 to logical Layer 2 and provides the logical Layer 2 division and management functions, better matching requirements of multiple tenants.

- Overlay technologies such as VXLAN and NVGRE use MAC-in-IP encapsulation to solve limitations of physical networks, including the limit on the number of VLANs and MAC address entries supported by access switches. These technologies also provide a unified logical network management tool to enable policy migration during VM migration, greatly reducing network dependency during virtualization. These technologies attract major concern in network virtualization.

Contents

1. **Challenges Facing Data Center Networks**
   - Low Latency Requirements of Compute Nodes
   - Wide Application of Virtualization Technology
   - Network and Service Maintenance Automation
2. Basic VXLAN Principles
3. Basic VXLAN Configurations

Challenge 3: Quick Service Innovation, Automatic Service Provisioning



Traditional DC: Network and Service Separation, Long Service Provisioning Period

Service control platform

Distributed DC resources

Independent pipe resources

DC and pipe resources with fixed locations

Unsatisfactory

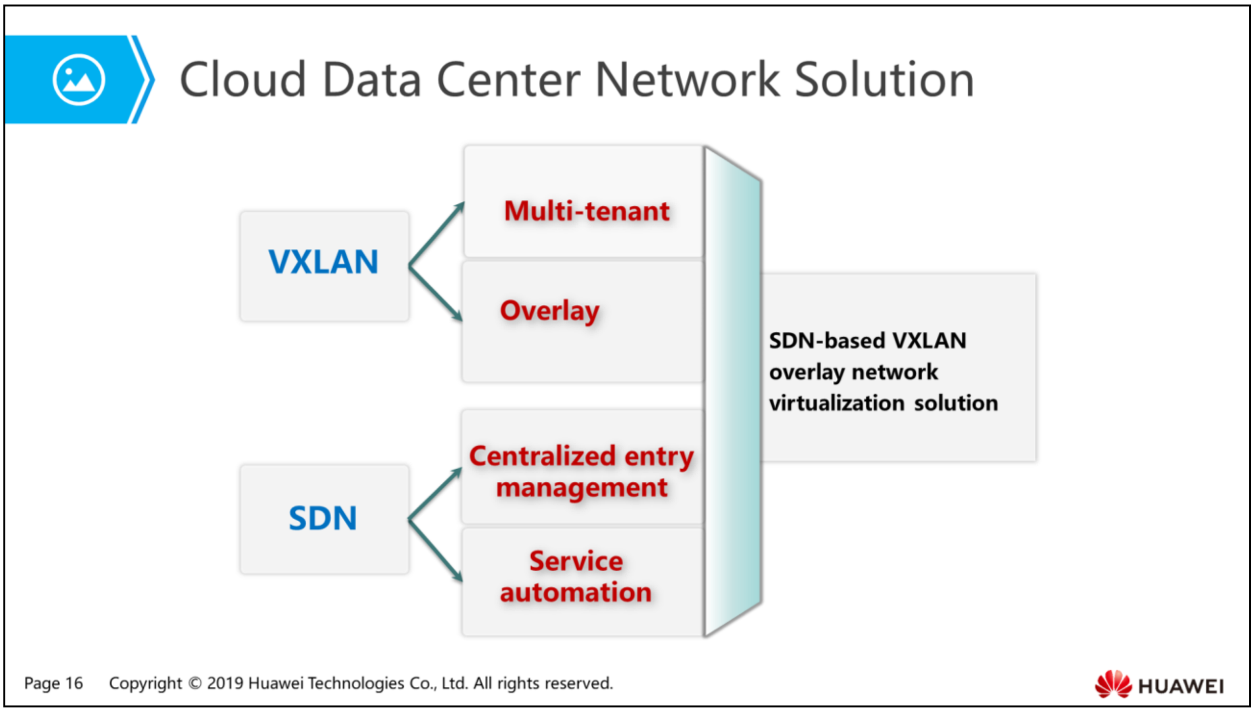
Cloud DC: Service and Network Association for Deployment Automation

Service control platform

Virtual logical service network

- Distributed, isolated DC and network resources: Quick service customization and rollout requirements cannot be met.
- Inefficient service deployment: The service customization capability is weak and service provisioning period is long.

- Quick service customization and deployment automation: Networks provide open APIs.
- Service-based on-demand allocation of network resources: A unified service control platform is used to implement collaboration between network resources and services.



Cloud Data Center Network Solution

VXLAN

Multi-tenant

Overlay

SDN

Centralized entry management

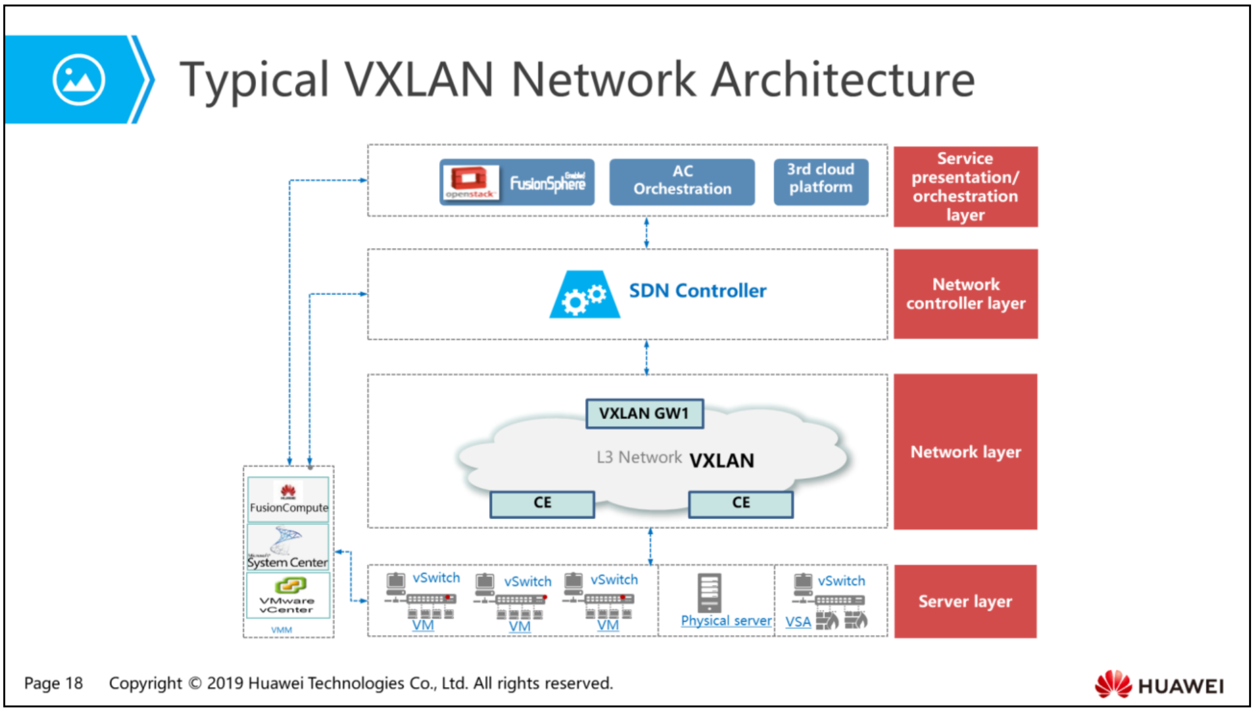
Service automation

SDN-based VXLAN overlay network virtualization solution

- The VXLAN technology enables multiple tenants to interconnect at Layer 2.
- VXLAN uses the tunneling technology to build a logical Layer 2 network across data centers, without changing the Layer 3 network topology.
- The VXLAN technology effectively resolves limitations on the number of VLANs.
- The VXLAN technology optimizes the Layer 2 network to prevent broadcast storms.
- SDN technologies are mainly used to simplify network deployment, O&M, and adjustment.

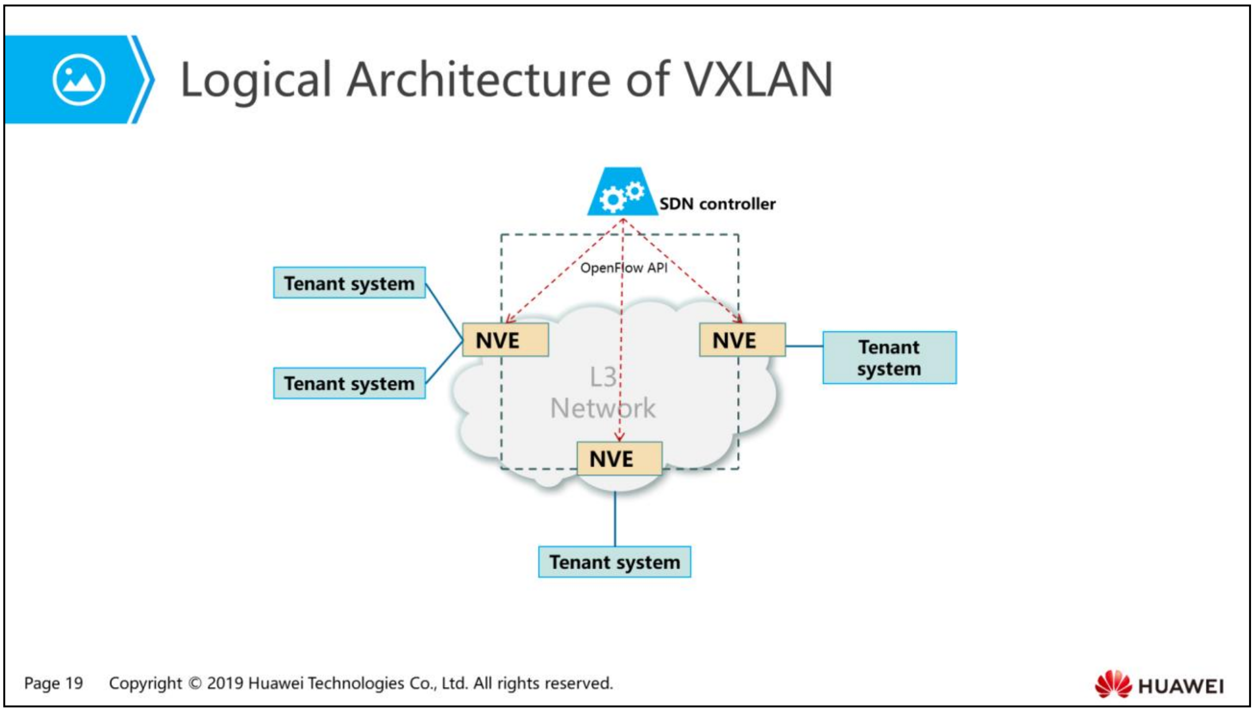
Contents

1. Challenges Facing Data Center Networks
2. **Basic VXLAN Principles**
3. Basic VXLAN Configurations



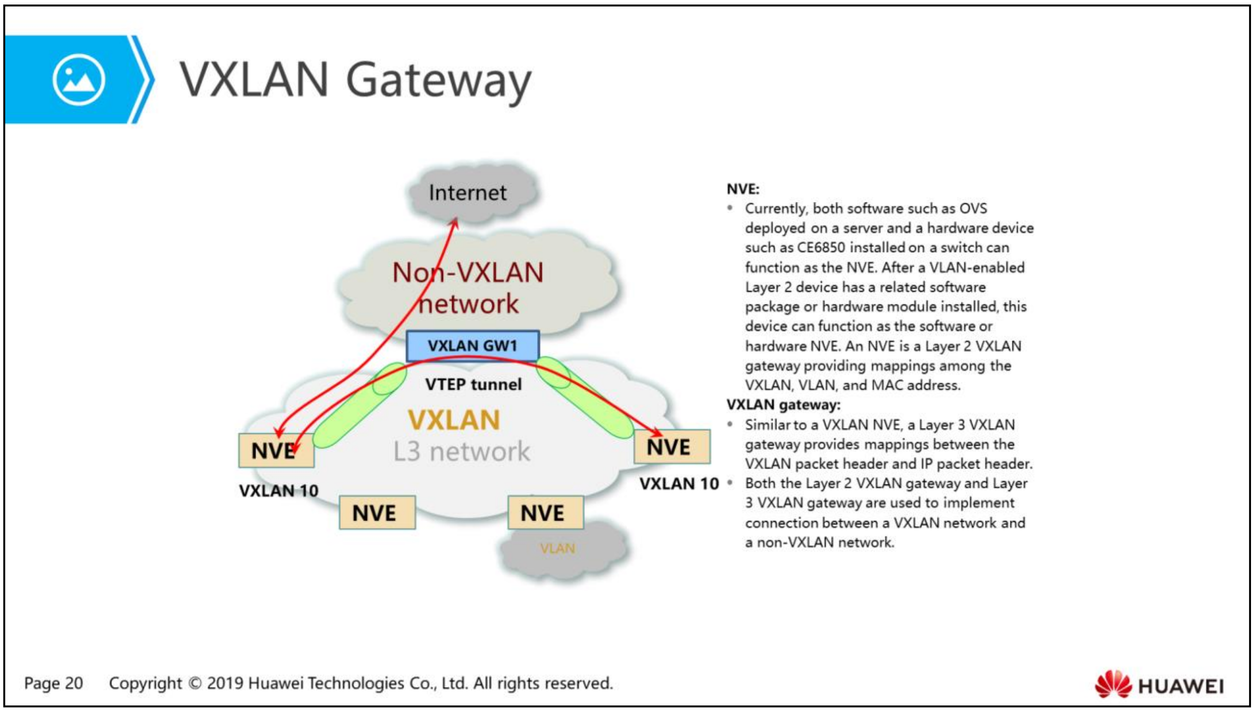
Typical VXLAN Network Architecture

- VXLAN, NVGRE, and STT are three typical NVO3 technologies.
- These technologies use MAC-in-IP encapsulation to build a logical Layer 2 network over an IP network.
- VMs of the same tenant can communicate at Layer 2 and migrate across a Layer 3 physical network.
- Compared with overlay technologies such as the traditional L2VPN, NVO3 enables virtual or physical hosts but not network sites to connect to CE devices.
- In addition, the hosts are movable.
- Currently, IT vendors dominate overlay network construction by virtualizing servers using the hypervisor.



Logical Architecture of VXLAN

- VXLAN (Virtual eXtensible Local Area Network, RFC7348) is a standard NVO3 technology defined by the IETF. It uses MAC-in-UDP encapsulation to enable Layer 2 forwarding over a Layer 3 network. VXLAN uses 24-bit VNI to support 16 million tenants, allowing VMs to migrate over a large Layer 2 network and meeting multi-tenant requirements.
- In the VXLAN NVO3 network model, a device deployed at the VXLAN network edge is called VXLAN NVE and is responsible for encapsulation and decapsulation between VLAN and VXLAN networks. After encapsulation, packets can be transmitted between NVEs over a virtual Layer 2 overlay network established on Layer 3 networks.
- VXLAN has the following characteristics:
  - Location independence: Services can be flexibly deployed in any location, enabling network expansion in server virtualization environment.
  - Scalability: New overlay network is planned based on the traditional network architecture. This facilitates deployment, avoids large Layer 2 broadcast storms, and has strong scalability.
  - Simple deployment: The reliable SDN controller completes configuration and management of the control plane, which avoids large-scale distributed deployment. In addition, the centralized deployment mode accelerates configuration of network and security infrastructure and improves scalability.
  - Applicable to cloud service: This technology can isolate ten millions of tenants, applicable for large-scale deployment of cloud services.
  - Technical advantage: VXLAN uses the widely used UDP to transmit packets, having high maturity.



VXLAN Gateway

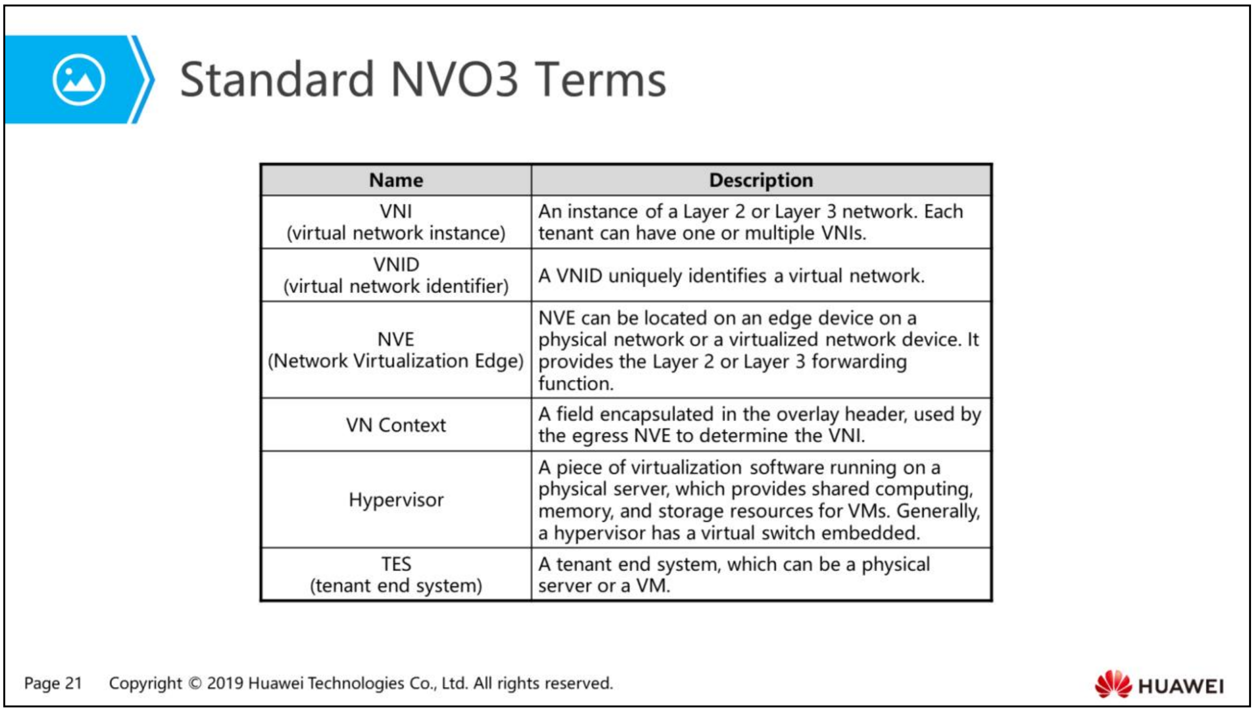
NVE:

- Currently, both software such as OVS deployed on a server and a hardware device such as CE6850 installed on a switch can function as the NVE. After a VLAN-enabled Layer 2 device has a related software package or hardware module installed, this device can function as the software or hardware NVE. An NVE is a Layer 2 VXLAN gateway providing mappings among the VXLAN, VLAN, and MAC address.

VXLAN gateway:

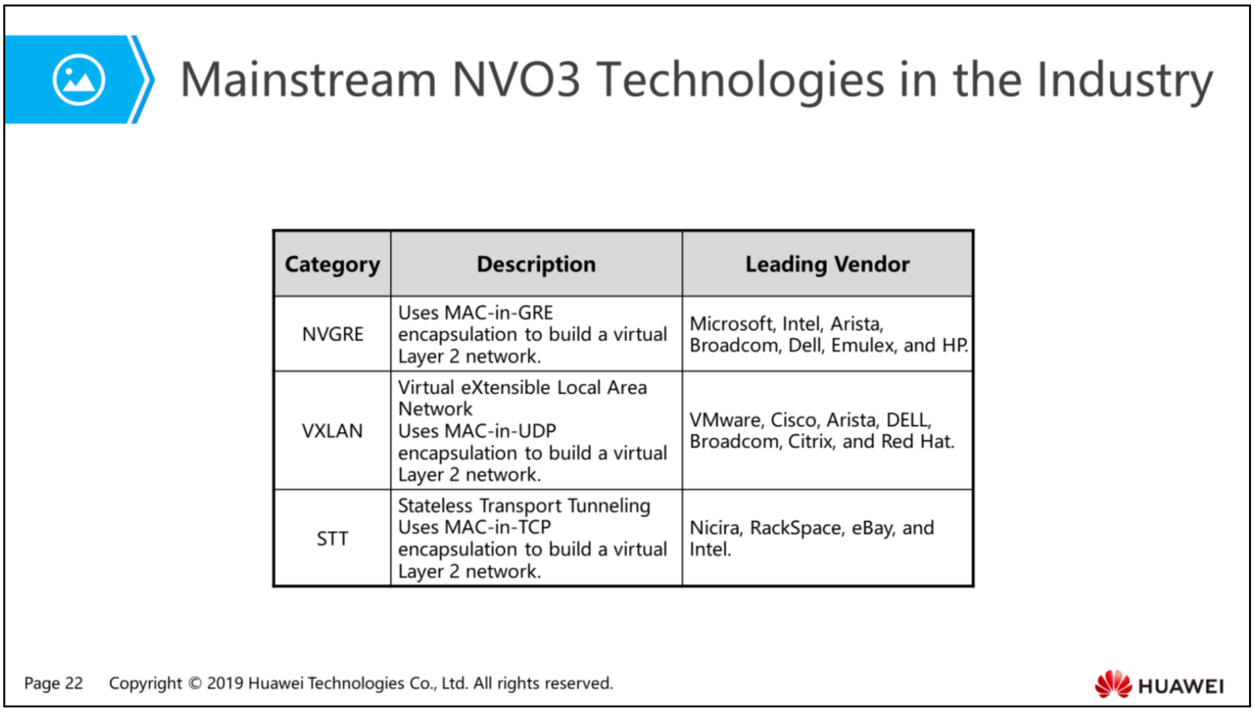
- Similar to a VXLAN NVE, a Layer 3 VXLAN gateway provides mappings between the VXLAN packet header and IP packet header.
- Both the Layer 2 VXLAN gateway and Layer 3 VXLAN gateway are used to implement connection between a VXLAN network and a non-VXLAN network.

- An NVE is a functional module at the server virtualization layer, enabling VMs to use virtualization software to establish VTEP tunnels.
- An NVE can also be a VXLAN-capable access switch that provides the VXLAN gateway service to multiple tenants in a centralized manner.
- A VXLAN gateway can implement communication between tenants on different VXLANs, as well as between VXLAN users and non-VXLAN users. This function is similar to that of a VLANIF interface.



Standard NVO3 Terms

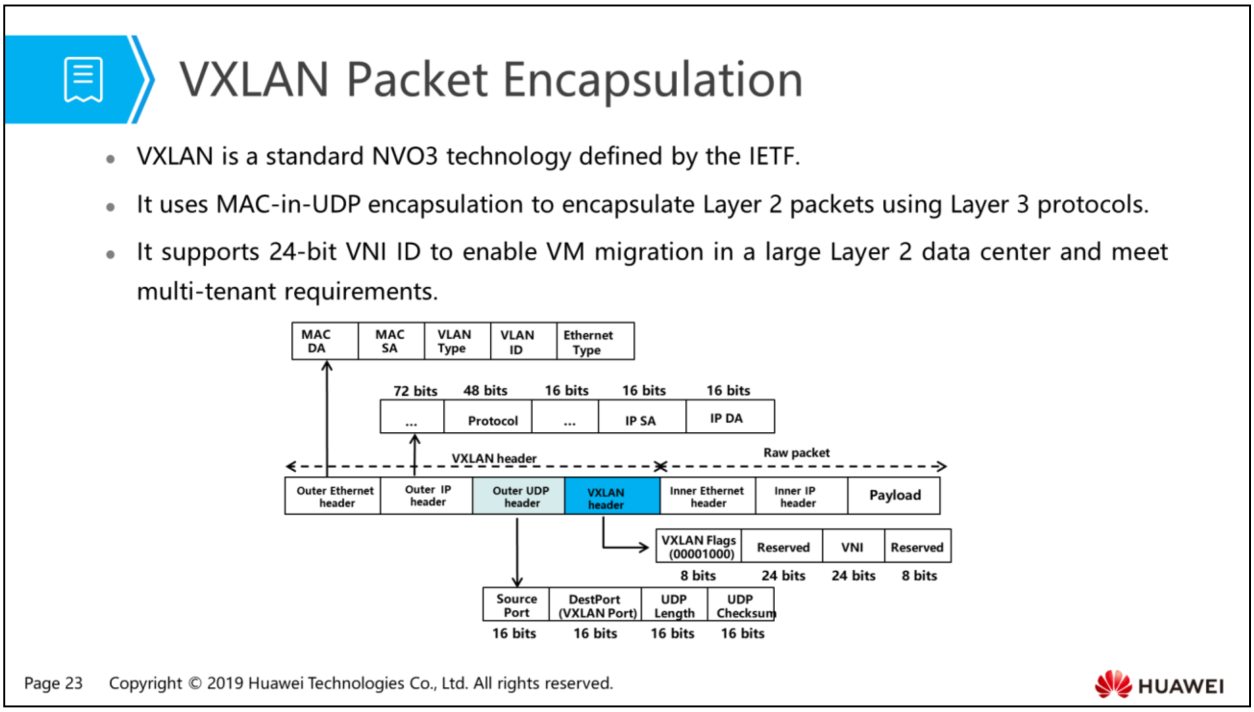
Name	Description
VNI (virtual network instance)	An instance of a Layer 2 or Layer 3 network. Each tenant can have one or multiple VNIs.
VNID (virtual network identifier)	A VNID uniquely identifies a virtual network.
NVE (Network Virtualization Edge)	NVE can be located on an edge device on a physical network or a virtualized network device. It provides the Layer 2 or Layer 3 forwarding function.
VN Context	A field encapsulated in the overlay header, used by the egress NVE to determine the VNI.
Hypervisor	A piece of virtualization software running on a physical server, which provides shared computing, memory, and storage resources for VMs. Generally, a hypervisor has a virtual switch embedded.
TES (tenant end system)	A tenant end system, which can be a physical server or a VM.



Mainstream NVO3 Technologies in the Industry

Category	Description	Leading Vendor
NVGRE	Uses MAC-in-GRE encapsulation to build a virtual Layer 2 network.	Microsoft, Intel, Arista, Broadcom, Dell, Emulex, and HP.
VXLAN	Virtual eXtensible Local Area Network Uses MAC-in-UDP encapsulation to build a virtual Layer 2 network.	VMware, Cisco, Arista, DELL, Broadcom, Citrix, and Red Hat.
STT	Stateless Transport Tunneling Uses MAC-in-TCP encapsulation to build a virtual Layer 2 network.	Nicira, RackSpace, eBay, and Intel.

- VXLAN, NVGRE, and STT are three typical NVO3 technologies that use MAC-in-IP encapsulation to build a Layer 2 network over an IP network, enabling VMs of the same tenant to communicate at Layer 2 and migrate over a Layer 3 physical network. Compared with overlay technologies such as the traditional L2VPN, NVO3 enables virtual or physical hosts but not network sites to connect to CE devices. In addition, the hosts are movable. Currently, IT vendors dominate overlay network construction by virtualizing servers using the hypervisor.
- A leading vendor that supports NVGRE is Microsoft.   Different from VXLAN, NVGRE encapsulates packets using GRE rather than TCP/IP. NVGRE uses the rightmost 24 bits in the GRE packet header as the tenant network identifier.
- VXLAN is an overlay network technology that uses MAC-in-UDP encapsulation. We will introduce the VXLAN technology in details in later slides.
- STT is a MAC-over-IP protocol. Similar to VXLAN and NVGRE that encapsulate Layer 2 frames to the payload of IP packets, STT also adds a TCP header and an STT header at the front of the payload of IP packets.



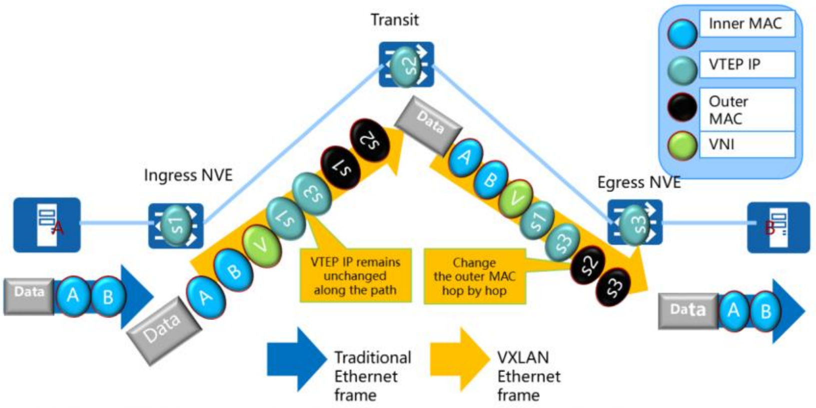
VXLAN Packet Encapsulation

- VXLAN is a standard NVO3 technology defined by the IETF.
- It uses MAC-in-UDP encapsulation to encapsulate Layer 2 packets using Layer 3 protocols.
- It supports 24-bit VNI ID to enable VM migration in a large Layer 2 data center and meet multi-tenant requirements.

Page 23

- VXLAN header:
  - VNI (24 bits): used to identify a VXLAN segment.
  - Reserved fields (24 bits and 8 bits): must be set to 0.
- Outer UDP header:
  - The destination UDP port number is 4789. The source port number is the hash value calculated using parameters in the inner Ethernet frame header.
- Outer IP header:
  - In the outer IP header, the source IP address is the IP address of the VTEP where the sender VM resides; the destination IP address is the IP address of the VTEP where the destination VM resides.
- Outer Ethernet header:
  - SA: specifies the MAC address of the VTEP where the sender VM resides.
  - DA: specifies the next-hop MAC address in the routing table of the VTEP where the destination VM resides.
  - VLAN Type: This field is optional. The value of this field is 0x8100 when the packet has a VLAN tag.
  - Ethernet Type: specifies the type of the Ethernet frame. The value of this field is 0x0800 when the packet type is IP.

VXLAN Data Encapsulation Process



Inner MAC

VTEP IP

Outer MAC

VNI

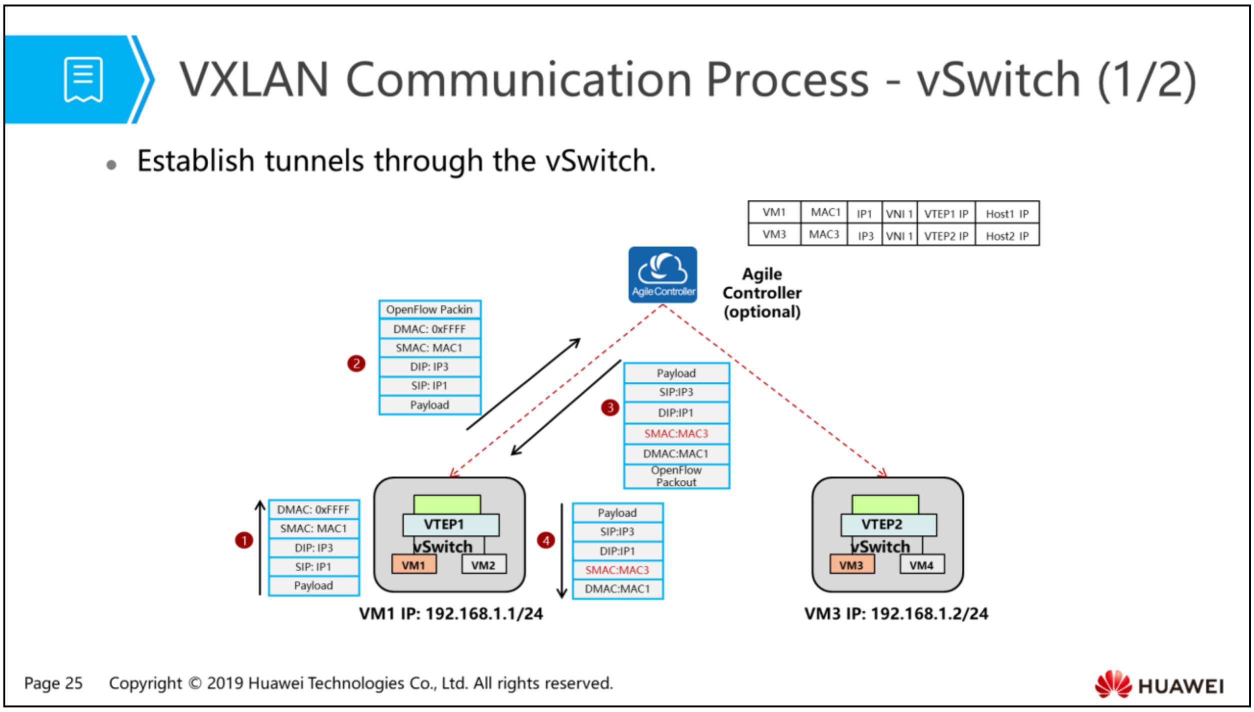
VTEP IP remains unchanged along the path

Change the outer MAC hop by hop

Traditional Ethernet frame

VXLAN Ethernet frame

- The original Layer 2 packets from the source end arrive at the destination over the IP network. The servers consider the VXLAN network as a bridge fabric.

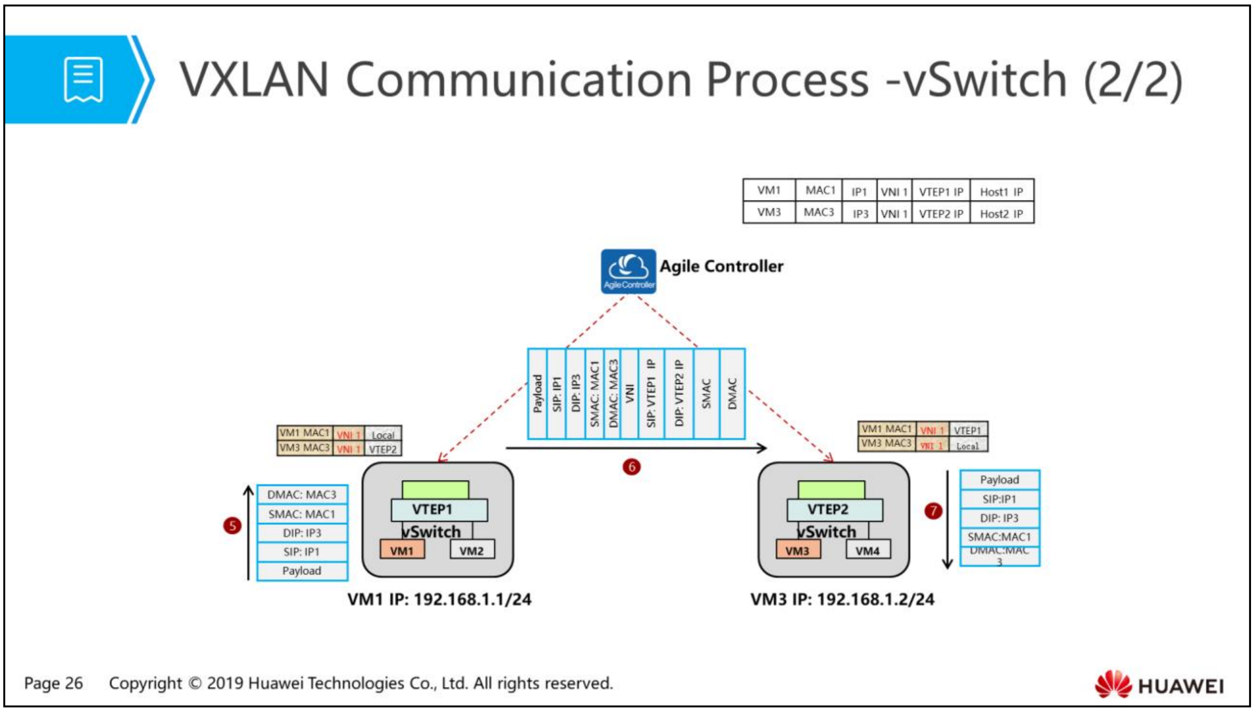


VXLAN Communication Process - vSwitch (1/2)

- Establish tunnels through the vSwitch.

VM1	MAC1	IP1	VNI 1	VTEP1 IP	Host1 IP
VM3	MAC3	IP3	VNI 1	VTEP2 IP	Host2 IP

- A vSwitch is a virtual switch that is integrated in the VM tool hypervisor.
- Using the vSwitch, a VTEP tunnel is established between servers Hypervisor where VMs reside.
- The Agile Controller is optional.
- VTEP is short for virtual tunnel end point, and is the ingress or egress of a VXLAN tunnel. The VM traffic passes through the vSwitch and is imported by the ingress VTEP to a VXLAN tunnel.
- VNI is short for virtual network instance. One VNI ID uniquely identifies a virtual network. In this example, VM1 and VM2 are on the same virtual network, and their VNI ID is 1.
- The IP addresses of VM1 and VM3 are IP1 and IP3. VM1 and VM3 are in the same subnet.
- The ARP exchange process is as follows:
    - VM1 sends an ARP packet to request the MAC address of VM3.
    - The ARP packet is encapsulated and forwarded through the OpenFlow channel to the Agile Controller, which has ARP proxy enabled.
    - The Agile Controller finds MAC3 based on IP3 and sends an ARP response packet, with IP3 and MAC3 as the SIP and SMAC.
    - The vSwitch sends the ARP response packet to VM1.

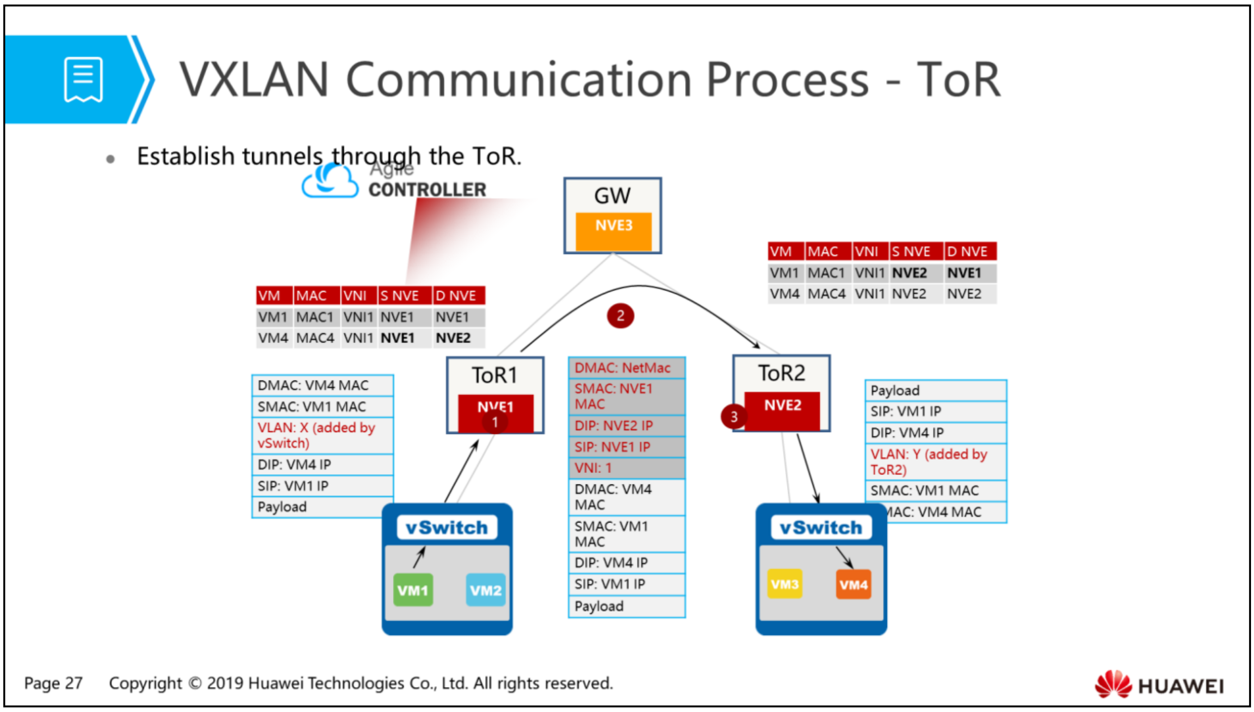


VXLAN Communication Process -vSwitch (2/2)

VM1	MAC1	IP1	VNI 1	VTEP1 IP	Host1 IP
VM3	MAC3	IP3	VNI 1	VTEP2 IP	Host2 IP

Page 26 HUAWEI

- The packet forwarding process is as follows:
  - VM1 sends a data packet, in which SIP, DIP, SMAC, and DMAC are IP1, IP3, MAC1, and MAC3.
  - VTEP1 performs VXLAN encapsulation, after which the inner SIP and DIP are IP1 and IP3, and the outer SIP and DIP are VTEP1 IP and VTEP2 IP.
  - VTEP2 decapsulates the VXLAN packet and sends it to VM3.



VXLAN Communication Process - ToR

- Establish tunnels through the ToR.

VM	MAC	VNI	S NVE	D NVE
VM1	MAC1	VNI1	NVE1	NVE1
VM4	MAC4	VNI1	**NVE1**	**NVE2**

VM	MAC	VNI	S NVE	D NVE
VM1	MAC1	VNI1	**NVE2**	**NVE1**
VM4	MAC4	VNI1	NVE2	NVE2

DMAC: VM4 MAC
SMAC: VM1 MAC
VLAN: X (added by vSwitch)
DIP: VM4 IP
SIP: VM1 IP
Payload

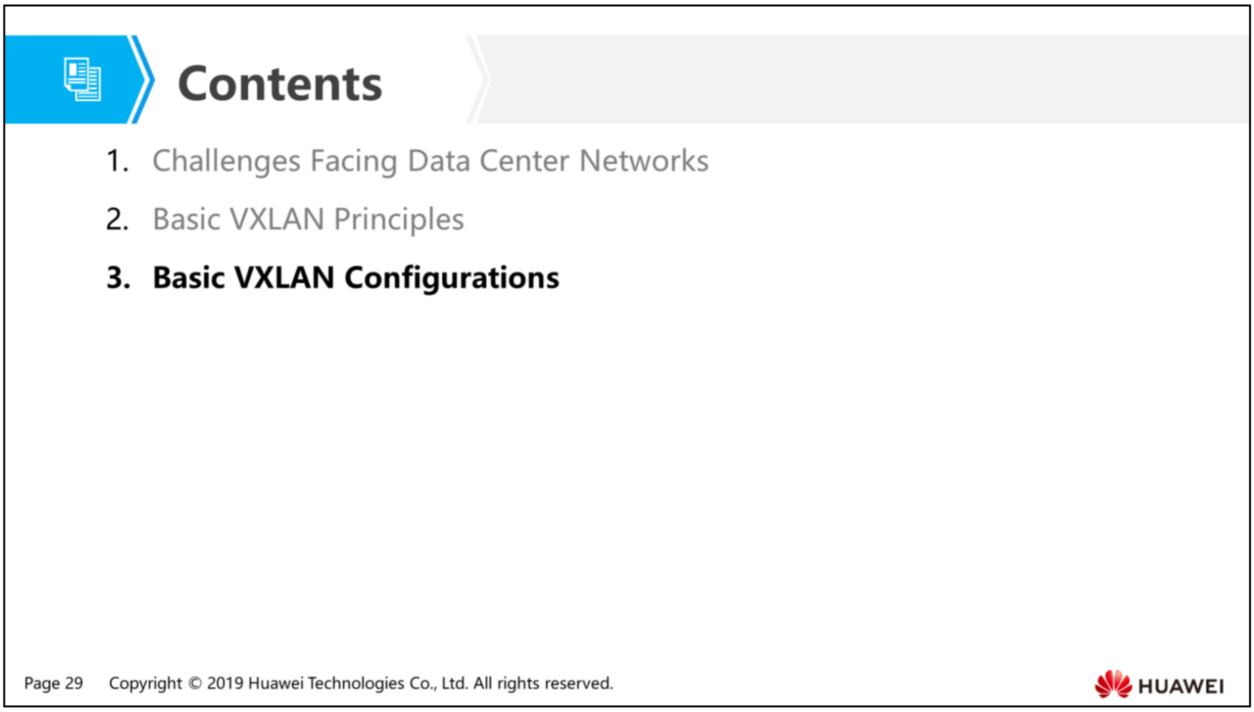
DMAC: NetMac
SMAC: NVE1 MAC
DIP: NVE2 IP
SIP: NVE1 IP
VNI: 1
DMAC: VM4 MAC
SMAC: VM1 MAC
DIP: VM4 IP
SIP: VM1 IP
Payload

Payload
SIP: VM1 IP
DIP: VM4 IP
VLAN: Y (added by ToR2)
SMAC: VM1 MAC
MAC: VM4 MAC

- Prerequisites
  - A dynamic routing protocol (OSPF is recommended) is running on the underlay network to ensure IP route reachability between NVE1, NVE2, and NVE3.
  - The Agile Controller has completed network service provisioning. vRouters have been created on the gateway, and specific networks have been created on the gateway and ToR switches. VLAN configuration has been delivered to vSwitches.
  - VM1 and VM4 map to VNI1 in BD1, whereas VM2 and VM3 map to VNI2 in BD2. Ingress replication tables have been created on ToR1 and ToR2. VMs 1 to 4 have been connected to the VXLAN network.
  - VM1 and VM4 have learned each other's ARP entry. ToR1 and ToR2 have learned MAC entries of VM1 and VM4 and associated the MAC addresses to the underlay tunnel (NVE1<->NVE2).
- Forwarding process
  - 1. VM1 sends data packets to VM4 on the same subnet. In the packets, SMAC and SIP are the MAC address and IP address of VM1, VLAN ID is X (local VLAN on ToR1, added by the vSwitch), and DMAC and DIP are the MAC address and IP address of VM4.

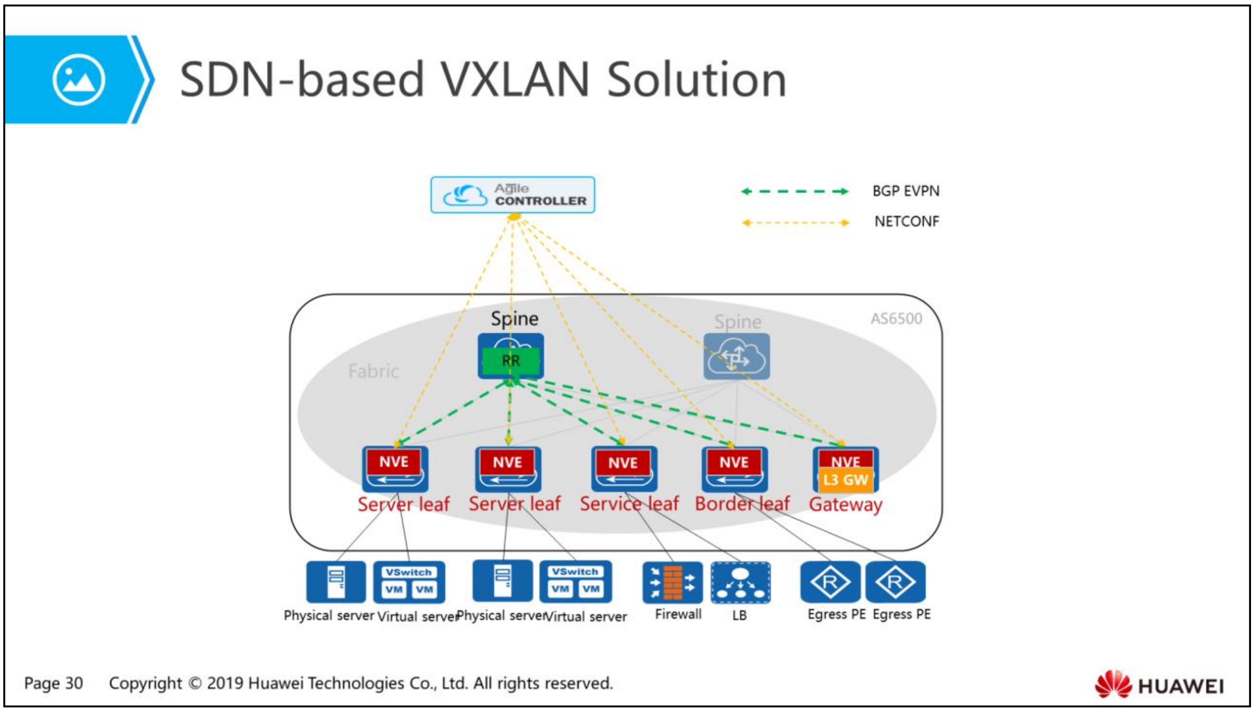
- When ToR1 receives the data packets, it finds the matching VNI1 based on the inbound interface and VLAN ID. ToR1 then searches the MAC table for VNI1 and VM4 MAC address, and finds that the outbound interface is the tunnel from NVE 1to NVE 2.
- 2. NVE1 encapsulates the data packets into VXLAN packets based on tunnel information, with the next-hop MAC address (NetMac) in the outer header. The VXLAN packets are forwarded hop by hop in the IP fabric network and finally arrive at NVE2.
- 3. NVE2 decapsulates the VXLAN packets and looks up the outbound interface in the MAC table based on VNI1 and DMAC of VM4 in the inner header. Then NVE2 adds VLAN Y to the packets and forwards them to VM4 through the outbound interface.
- The vSwitch deletes VLAN Y and forwards the packets to VM4.

- Remarks
    - L2 traffic forwarding does not depend on ARP entries learned by the Agile Controller or gateway. The ToR switches learn MAC addresses and associate them with corresponding tunnels.



Contents

1. Challenges Facing Data Center Networks
2. Basic VXLAN Principles
3. **Basic VXLAN Configurations**



SDN-based VXLAN Solution

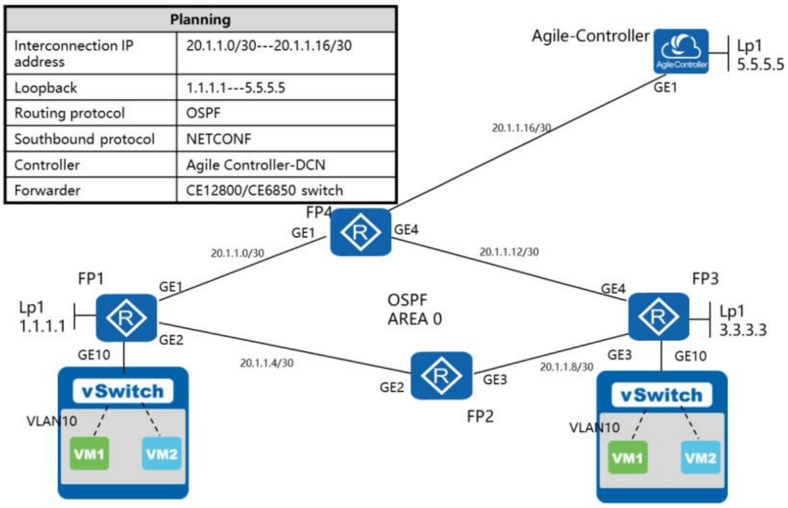
Page 30 Copyright © 2019 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

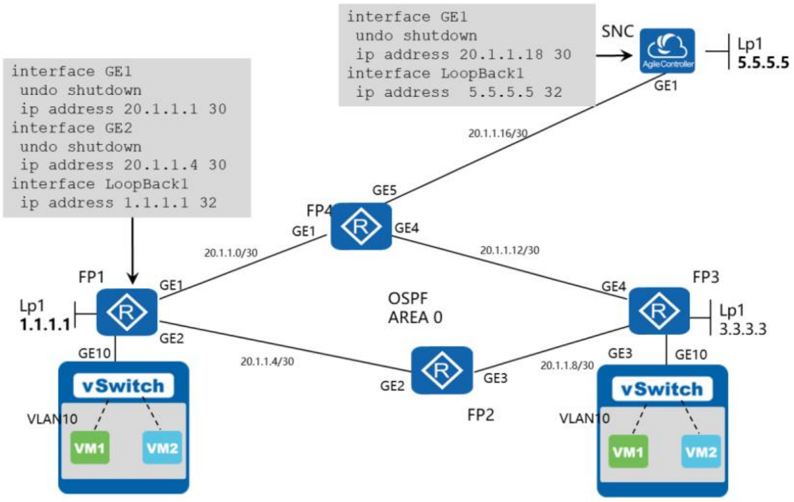
- Tunnel setup
  - The Agile Controller uses the NETCONF interface to deliver iBGP-EVPN configuration for the overlay network to leaf nodes.
  - The spine node functions as the route reflector (RR), and NVEs act as clients.
  - BGP-EVPN triggers automatic VXLAN tunnel setup between NVEs to remove the need for manual configuration of full-mesh tunnels.
- Entry synchronization on the control plane
  - NVEs learn MAC or ARP entries from data packets or ARP packets sent from VMs.
  - NVEs import learned forwarding entries to the EVPN instance to form MAC/IP routes.
  - NVEs use the BGP-EVPN protocol to advertise their MAC/IP routes to neighboring nodes.
  - BGP-EVPN neighbors (NVEs) create forwarding entries based on received MAC/IP route information.
- BGP-EVPN advertises MAC/IP routes and segment routes to establish L2/l3 forwarding paths.

SDN-based VXLAN Networking

Planning	
Interconnection IP address	20.1.1.0/30---20.1.1.16/30
Loopback	1.1.1.1---5.5.5.5
Routing protocol	OSPF
Southbound protocol	NETCONF
Controller	Agile Controller-DCN
Forwarder	CE12800/CE6850 switch

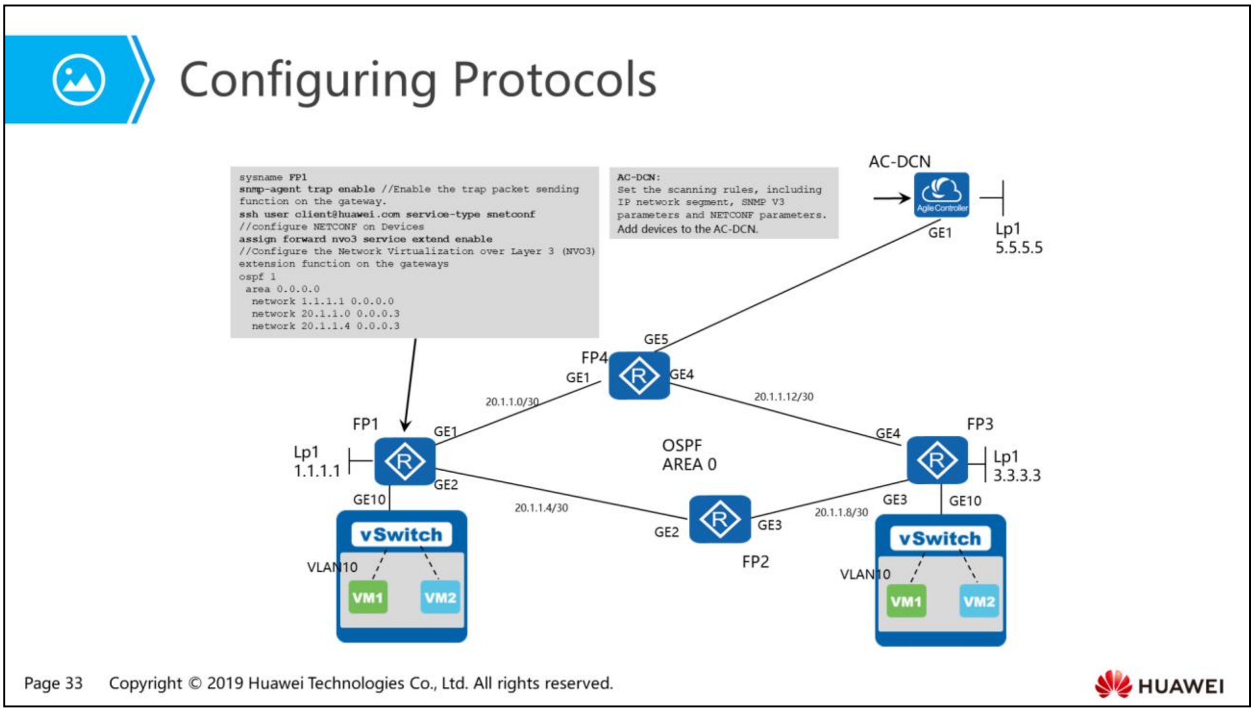


Configuring Interfaces



```
interface GE1
 undo shutdown
 ip address 20.1.1.18 30
interface LoopBack1
 ip address  5.5.5.5 32
```

```
interface GE1
 undo shutdown
 ip address 20.1.1.1 30
interface GE2
 undo shutdown
 ip address 20.1.1.4 30
interface LoopBack1
 ip address 1.1.1.1 32
```



Configuring Protocols

```
sysname FP1
snmp-agent trap enable //Enable the trap packet sending
function on the gateway.
ssh user client@huawei.com service-type snetconf
//configure NETCONF on Devices
assign forward nvo3 service extend enable
//Configure the Network Virtualization over Layer 3 (NVO3)
extension function on the gateways
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 20.1.1.0 0.0.0.3
  network 20.1.1.4 0.0.0.3
```

AC-DCN:
Set the scanning rules, including IP network segment, SNMP V3 parameters and NETCONF parameters.
Add devices to the AC-DCN.

- 1. configure SNMP parameters on devices so that the devices can be added to and discovered by the AC-DCN using SNMP
  - ▫ AC-DCN configuration on WEB portal
  - ▫ FP1configuration

  snmp-agent usm-user v3 admin group dc-admin

  snmp-agent usm-user v3 admin authentication-mode sha //Enter the authentication password, for example, Huawei@123.

  snmp-agent usm-user v3 admin privacy-mode aes128 //Enter the encryption password, for example, Huawei@1234.

  snmp-agent trap enable //Enable the trap packet sending function on the gateway.

- 2. configure NETCONF parameters on devices so that the AC-DCN can deliver service configurations to the devices and obtain information about the devices using NETCONF
  - ▫ Configure CE switch

  Configure SSH on the VTY CLI.

  local-user client@huawei.com password irreversible-cipher Huawei@123

  local-user client@huawei.com service-type ssh

  ssh user client@huawei.com authentication-type password

  ssh user client@huawei.com service-type snetconf

  snetconf server enable

- 3.Configure VXLAN
  - ▫ Configure the Network Virtualization over Layer 3 (NVO3) extension function on the gateways

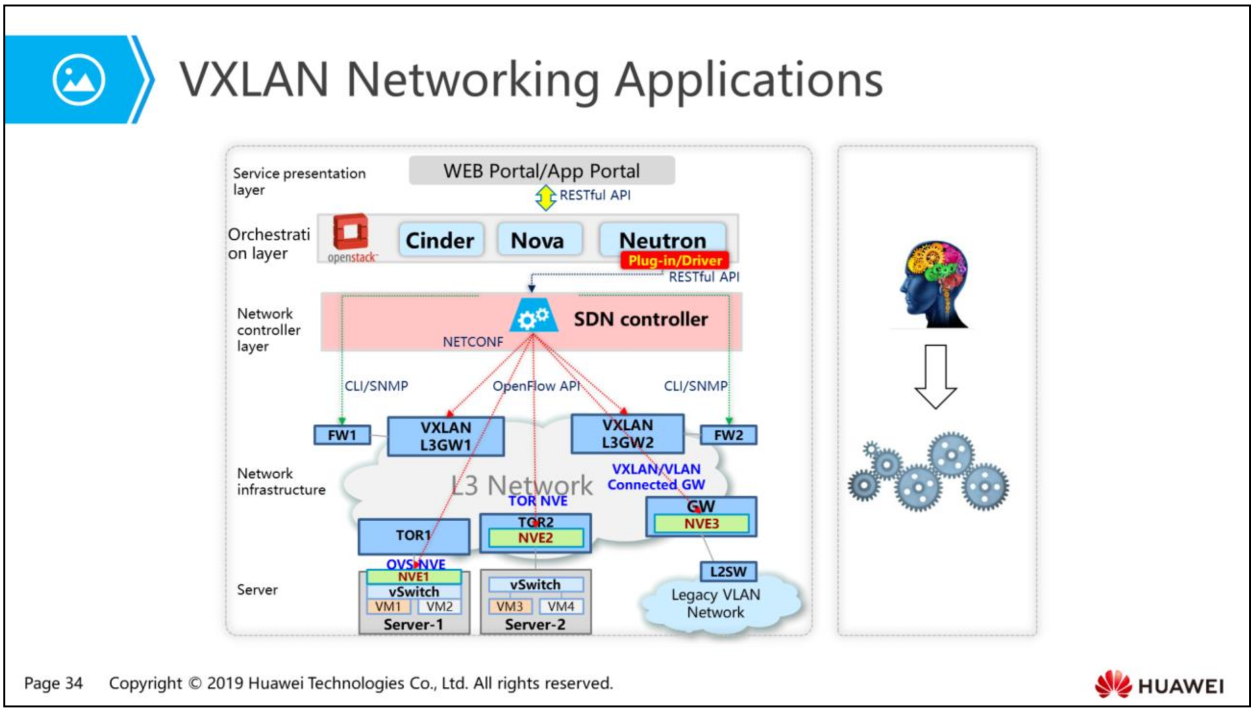
  assign forward nvo3 service extend enable

  assign forward nvo3 acl extend enable

  - ▫ Configure the enhanced mode for the NVO3 gateway

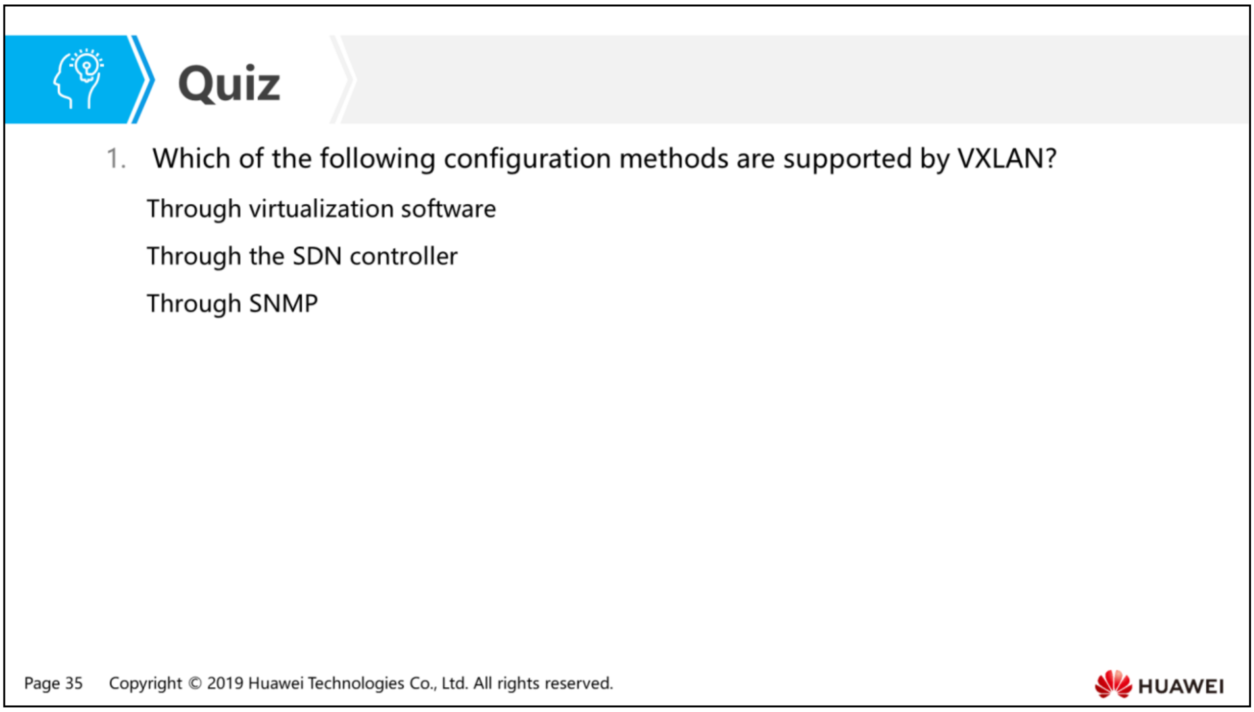
  assign forward nvo3-gateway enhanced l3

  - ▫ Other VXLAN functions are automatically delivered by the AC-DCN, but not manually configured



VXLAN Networking Applications

- Service presentation layer:
  - Provides portals for carriers, enterprises, tenants, and retail service providers (RSPs).
  - Provides flexible service customization pages.
- Orchestration layer:
  - Provides a standard and open OpenStack architecture compatible with multiple vendors.
  - Implements orchestration between computing, storage, and network resources.
- Network controller layer:
  - Consists of Agile Controller-DCN to complete network modeling and network instantiation.
  - Supports open APIs in the northbound direction for rapid customization and automatic provisioning of services.
  - Supports OpenFlow and NETCONF interfaces in the southbound direction to centrally manage and control physical and virtual networks.
- Network infrastructure:
  - VXLAN overlay networks with physical and virtual networks planned and designed in a unified manner reside in network infrastructure.
  - Improves service performance with the hardware VXLAN gateway.
  - Be compatible with traditional VLAN networks.



Quiz

1. Which of the following configuration methods are supported by VXLAN?

Through virtualization software

Through the SDN controller

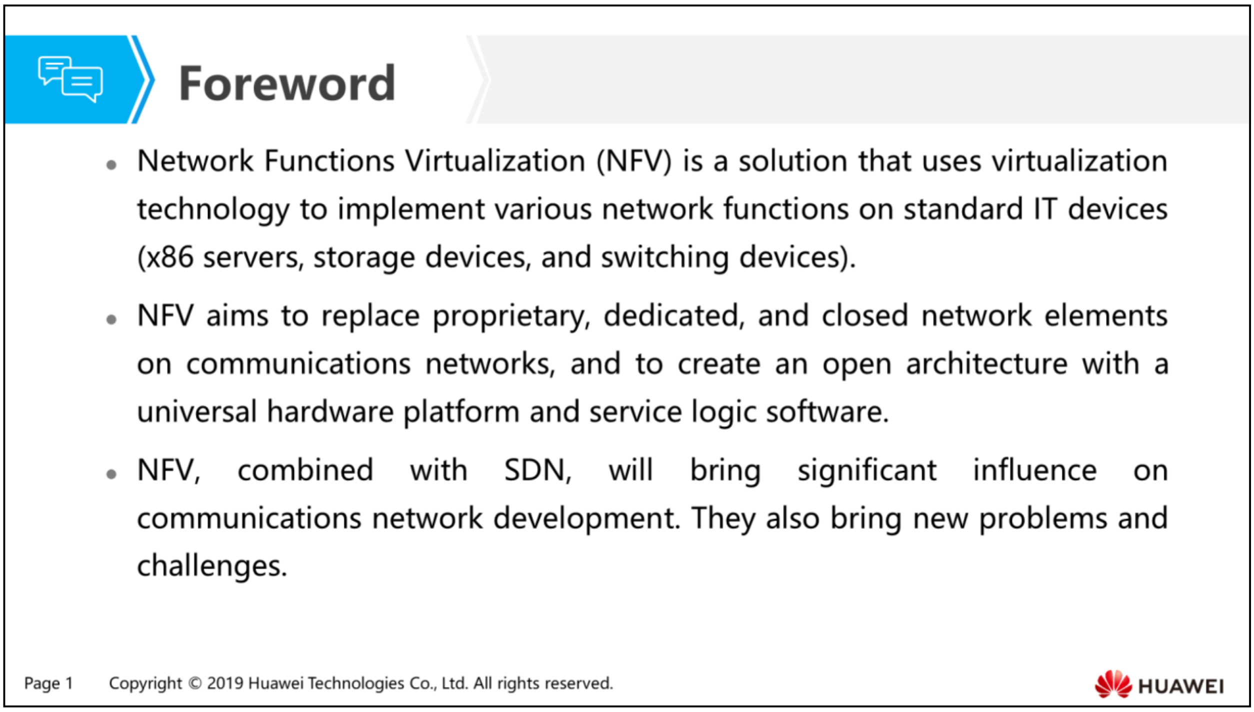
Through SNMP

- Answer: B.

Thank You

www.huawei.com

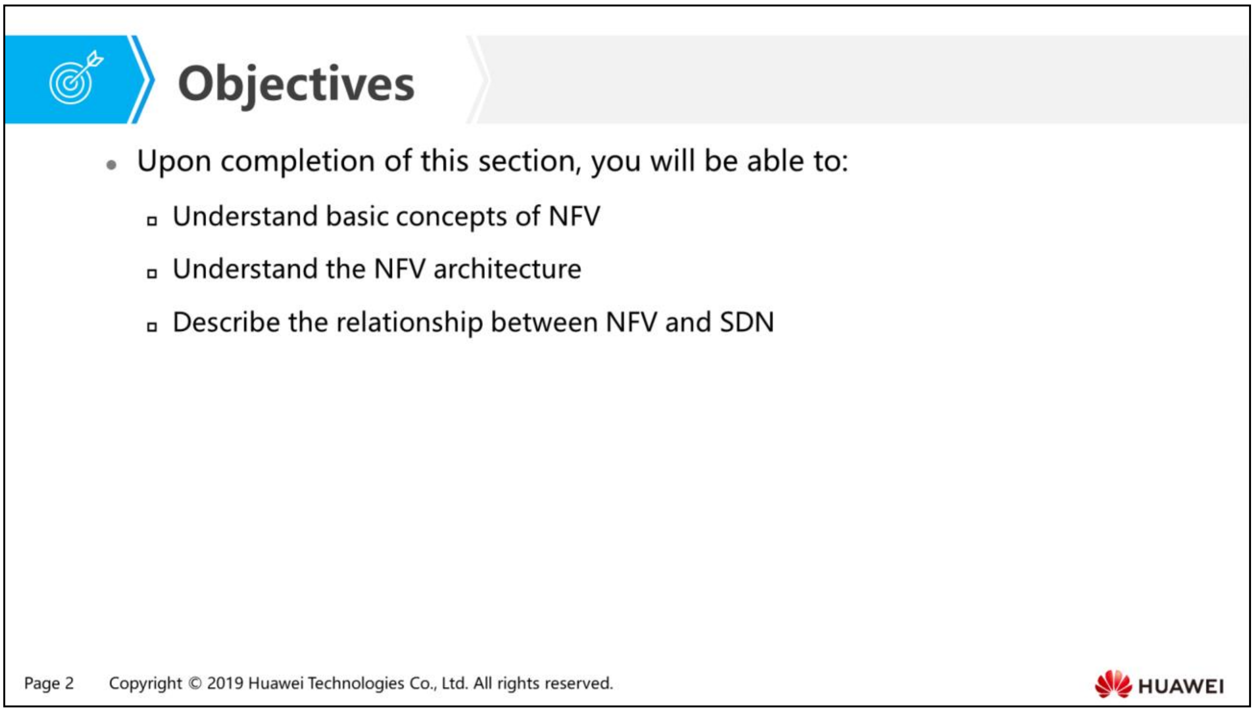
NFV Overview



Foreword

- Network Functions Virtualization (NFV) is a solution that uses virtualization technology to implement various network functions on standard IT devices (x86 servers, storage devices, and switching devices).
- NFV aims to replace proprietary, dedicated, and closed network elements on communications networks, and to create an open architecture with a universal hardware platform and service logic software.
- NFV, combined with SDN, will bring significant influence on communications network development. They also bring new problems and challenges.

- Carrier networks usually have a large number of hardware devices, while the number is increasing rapidly. New network services need to be supported by new devices. However, it becomes more and more difficult to reserve space and provide power supply for the new devices. Additionally, the increasing energy cost, required investment, and complexity of hardware devices impose great challenges to design, integration, and operation.
- A more serious problem is the short lifecycle of hardware devices. Carriers have to repeat the “design, integration, and deployment” process but obtain few benefits. On the contrary, service innovation is speeding up. Hardware devices slow down deployment of new value-added services and hinder innovation in network-centric fields.
- Network virtualization uses IT virtualization technology to incorporate various types of network devices, such as servers, switches, and storage devices, into industrial standards, enabling these devices to be deployed in data center networks, network sites, or users’ home. Network virtualization is applicable to packet processing on any data planes and control plane functions in fixed or mobile networks.

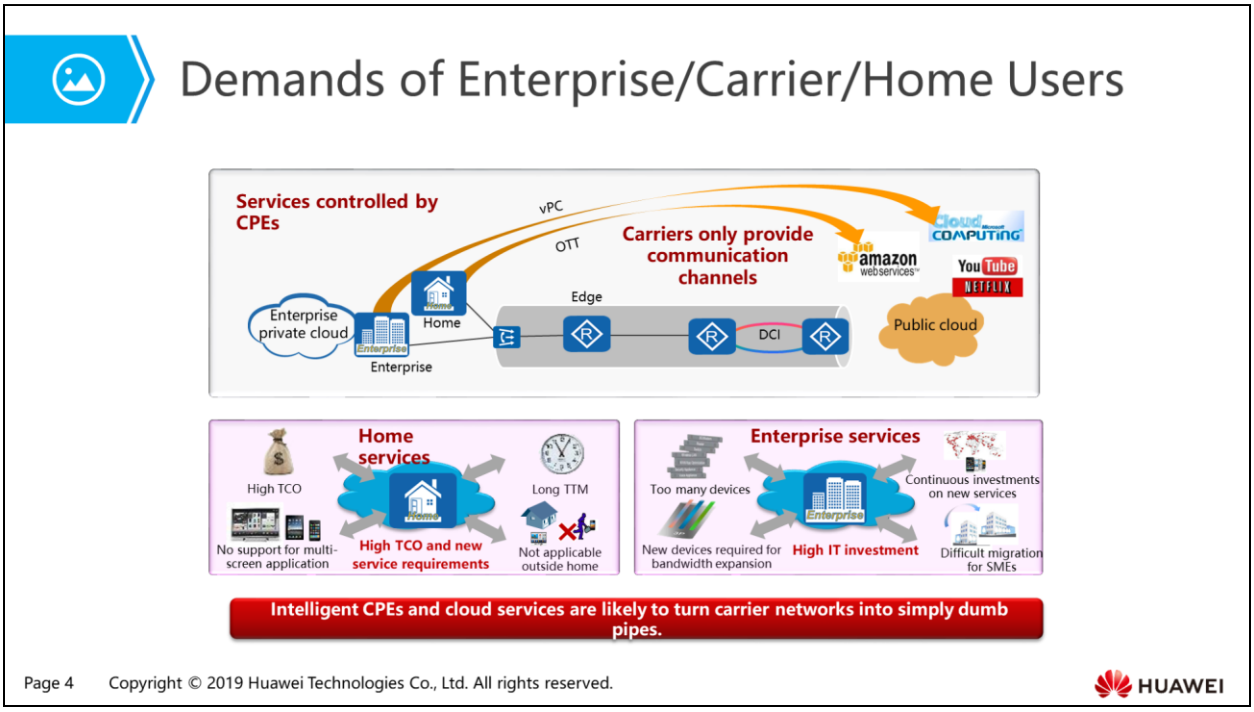


Objectives

- Upon completion of this section, you will be able to:
  - Understand basic concepts of NFV
  - Understand the NFV architecture
  - Describe the relationship between NFV and SDN

Contents

1. **Basic Concept of NFV**
2. NFV Architecture
3. Relationship Between NFV and SDN

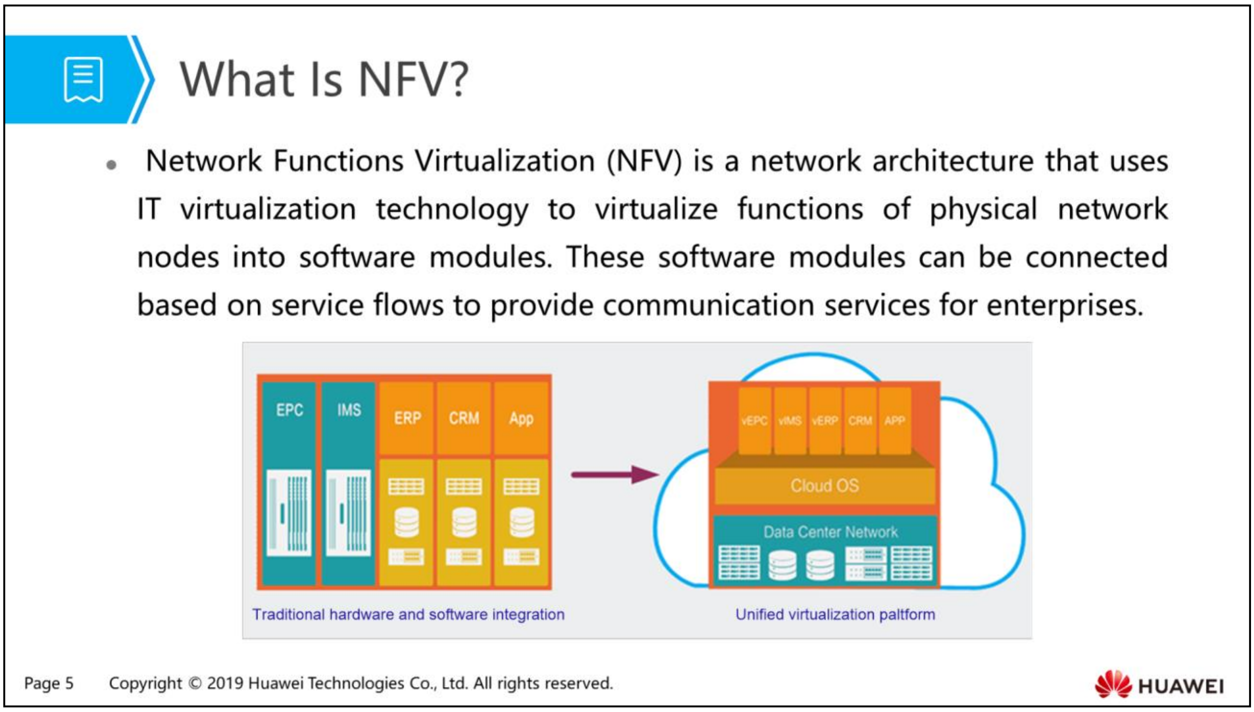


Demands of Enterprise/Carrier/Home Users

Services controlled by CPEs
vPC
OTT
Carriers only provide communication channels
Cloud COMPUTING
amazon webservices
YouTube
NETFLIX
Edge
Home
Enterprise private cloud
Enterprise
DCI
Public cloud
Home services
High TCO
Long TTM
No support for multi-screen application
High TCO and new service requirements
Not applicable outside home
Enterprise services
Too many devices
Continuous investments on new services
New devices required for bandwidth expansion
High IT investment
Difficult migration for SMEs

Intelligent CPEs and cloud services are likely to turn carrier networks into simply dumb pipes.

- As cloud services develop continuously and are required by more users, carriers only need to provide transmission pipes for private and public clouds. Therefore, carriers are facing the risk of becoming dumb pipes without obtaining benefits.
- Home users cannot enjoy applications on multiple screens or outside their home. In addition, service provisioning is time consuming and costly.
- Enterprise users need to invest heavily on communication devices (such as routers, switches, servers, and storage devices).
- New devices need to be purchased for system capacity expansion, which results in reinvestment.
- Customer premises equipment (CPE) is the gateway of an enterprise network and is connected to a PE router of a carrier.



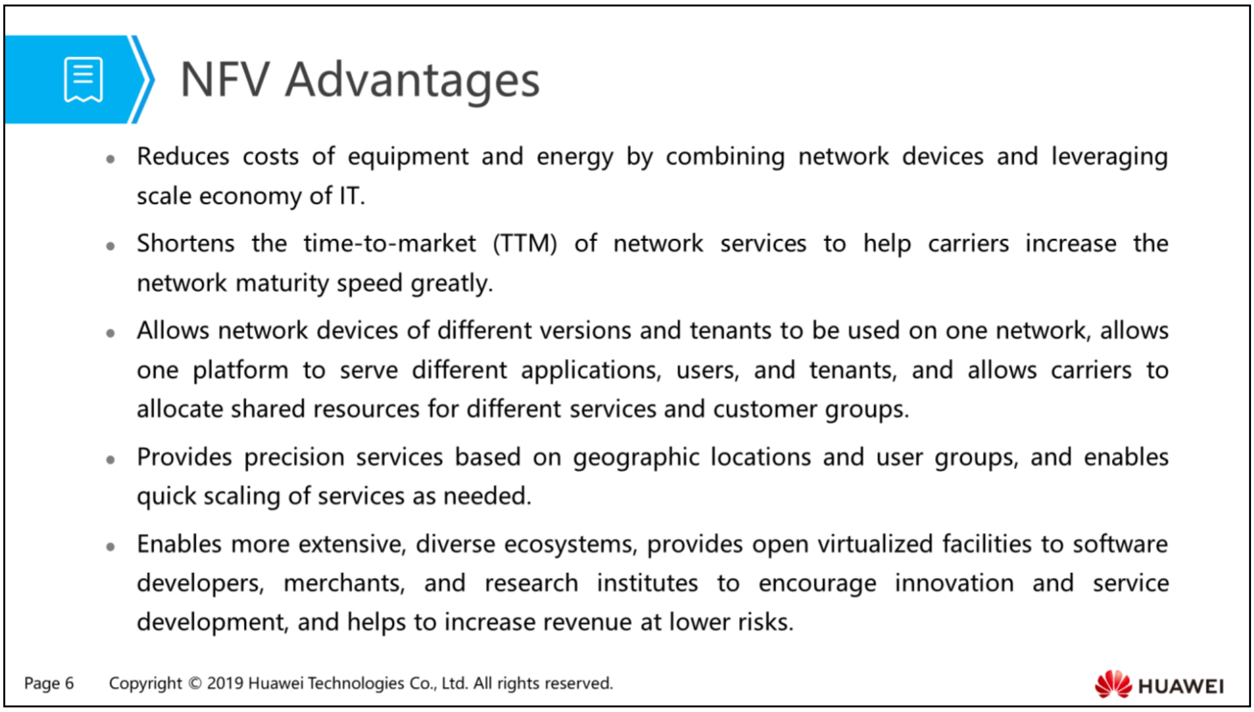
What Is NFV?

- Network Functions Virtualization (NFV) is a network architecture that uses IT virtualization technology to virtualize functions of physical network nodes into software modules. These software modules can be connected based on service flows to provide communication services for enterprises.

EPC
IMS
ERP
CRM
App
vEPC
vIMS
vERP
CRM
APP
Cloud OS
Data Center Network
Traditional hardware and software integration
Unified virtualization paltform

Page 5 HUAWEI

- NFV stands for Network Functions Virtualization. This technology builds a data center network with various network devices (such as servers, switches and storage devices). Using IT virtualization technology, NFV enables traditional CT services to be deployed on virtual machines (VMs).
- Before NFV is put into use, specific functions are implemented by dedicated devices. NFV separates the control plane from specific devices. Control planes of devices are deployed on VMs, while VMs run a cloud operating system. To deploy a new service, an enterprise only needs to create VMs on an open virtual machine management platform, and then install the corresponding software package on the VMs.



NFV Advantages

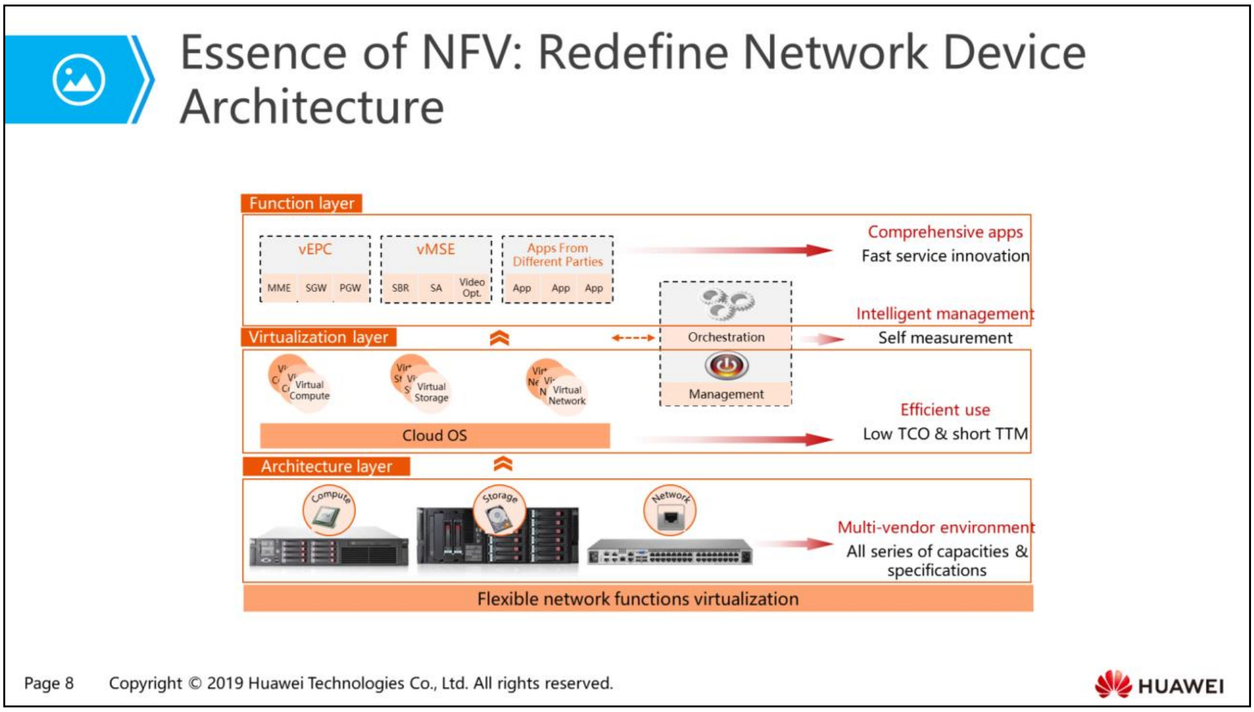
- Reduces costs of equipment and energy by combining network devices and leveraging scale economy of IT.
- Shortens the time-to-market (TTM) of network services to help carriers increase the network maturity speed greatly.
- Allows network devices of different versions and tenants to be used on one network, allows one platform to serve different applications, users, and tenants, and allows carriers to allocate shared resources for different services and customer groups.
- Provides precision services based on geographic locations and user groups, and enables quick scaling of services as needed.
- Enables more extensive, diverse ecosystems, provides open virtualized facilities to software developers, merchants, and research institutes to encourage innovation and service development, and helps to increase revenue at lower risks.

Page 6

- NFV also faces many technical challenges:
  - Virtual network appliances run on hardware devices from different vendors and different Hypervisor platforms. How to obtain higher performance is a challenge.
  - The hardware network platform needs to migrate to a virtual network platform. Hardware and virtual network platforms should be able to coexist to enable reuse of the current OSS/BSS systems of carriers.
  - Carriers need to manage and organize many virtual network appliances (especially management systems) and prevent attacks and incorrect configurations.
  - Hardware and software reliability must be ensured.
  - Virtual appliances (VAs) of different carriers need to be integrated. Network operators need to combine and match hardware devices, Hypervisors, and VAs from different vendors to prevent vendor lock-in without paying high integration cost.

Contents

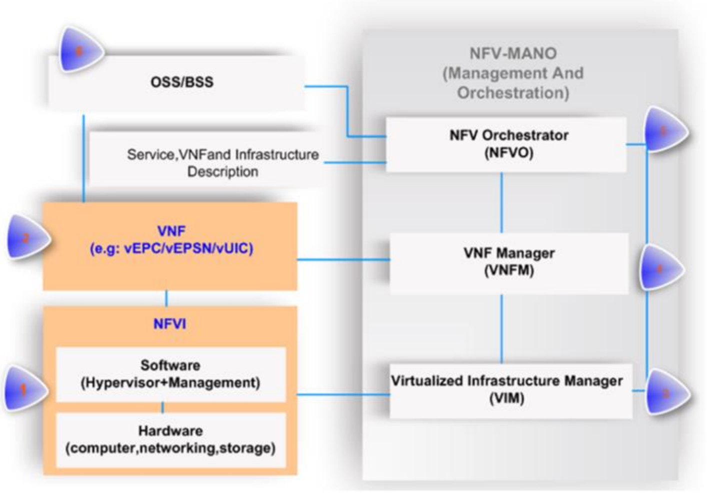
1. Basic Concept of NFV
2. **NFV Architecture**
3. Relationship Between NFV and SDN



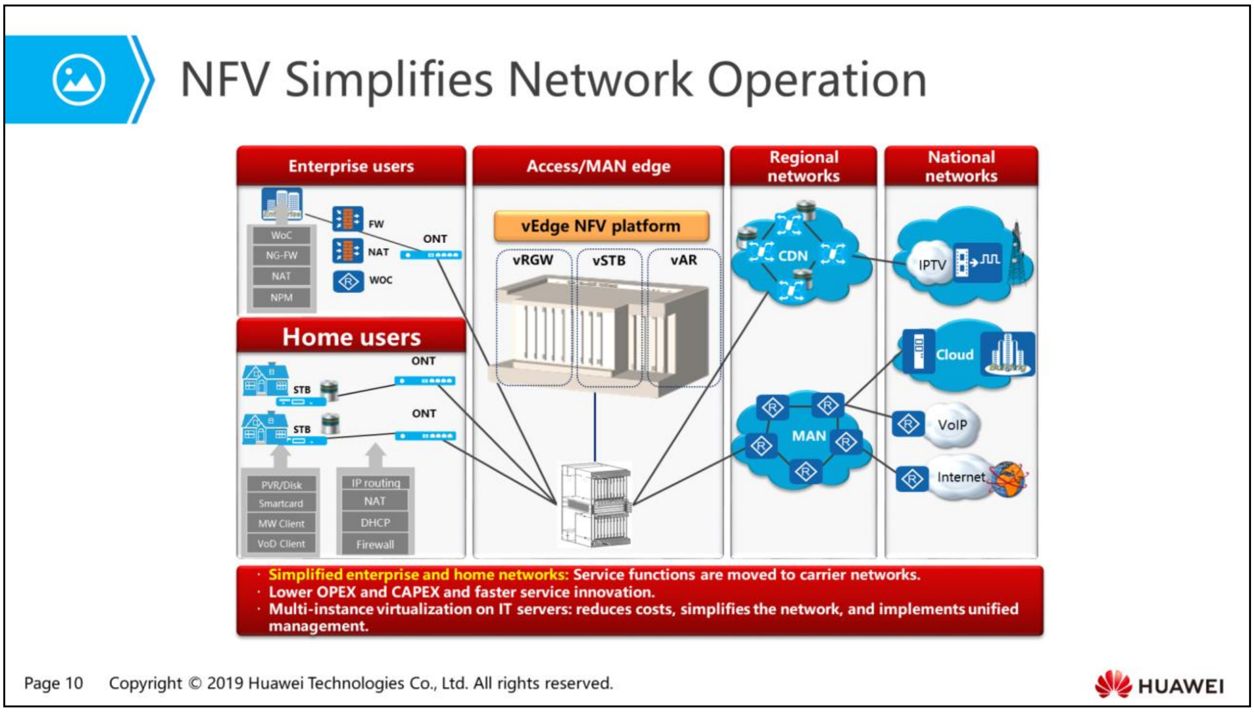
Essence of NFV: Redefine Network Device Architecture

- Huawei CloudEdge solution consists of four layers and has the following highlights:
  - Software application layer: Huawei provides extensive telecommunications applications and opens these applications to third parties for quick service innovation and deployment.
  - Cloud OS layer: This layer implements efficient use of resources and quick deployment of services.
  - Management and network orchestration (MANO) layer: This layer implements automatic network scaling and simplifies network management.
  - Hardware device layer: This layer has high-reliability, high-performance, commercial off-the-shelf (COTS) servers with various specifications to meet requirements for carrier-grade deployment. Multi-vendor COTS servers can be deployed at this layer.
- In the NFV architecture, the bottom layer is composed of physical devices, such as servers, storage devices, and network devices.
- Compute virtualization allows multiple virtual machines to be created on one server.
- Storage virtualization virtualizes multiple storage devices into one logical device.
- Network virtualization separates the control plane of network devices from the hardware by moving the control plane to virtual machines installed on servers.
- Various service software can be installed on the virtualized devices.

NFV Open Interfaces



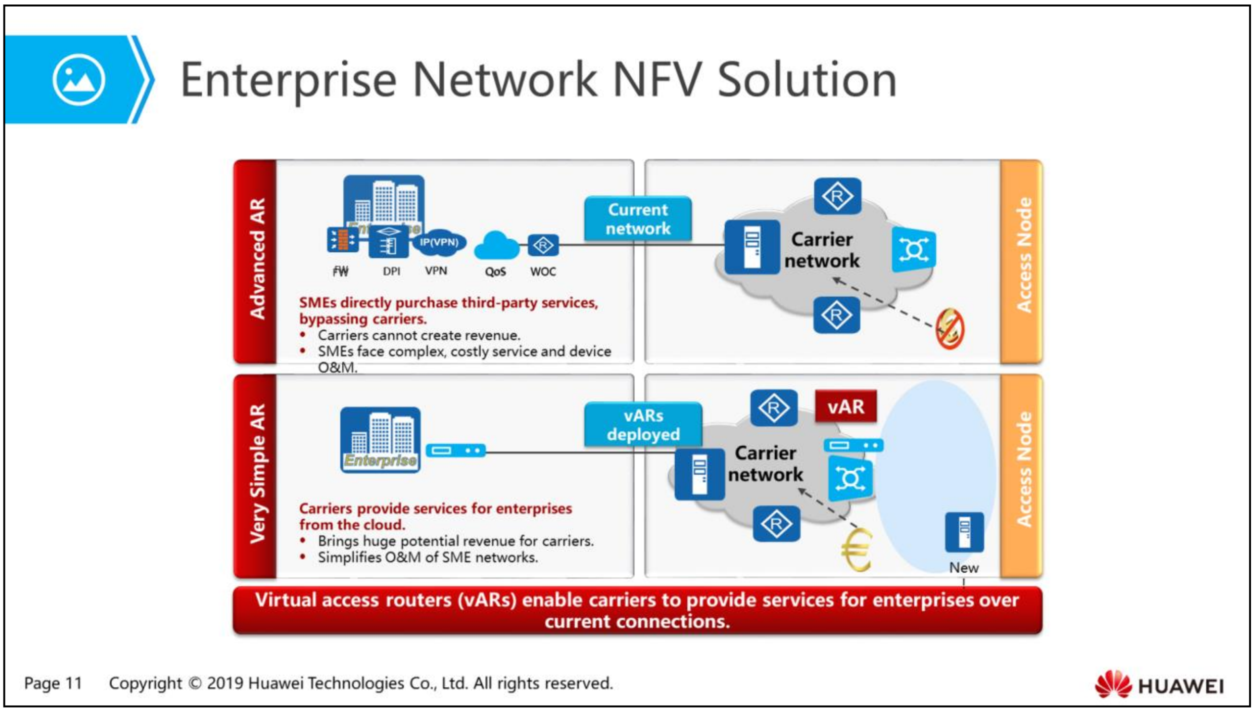
- Network Functions Virtualization Infrastructure (NFVI): provides the VNF running environment, including hardware and software components. Hardware components include computing, network, and storage resources. Software components include Hypervisor, network controller, and storage manager. The NFVI virtualizes physical resources into virtual resources for virtual network functions (VNFs).
- VNF: involves VNF and element management system (EMS). EMSs are used to configure and manage VNFs. Generally, one EMS manages one VNF.
- VIM: is the NFVI management module that provides functions such as resource discovery, virtual resource management, and fault handling to support running of VNFs.
- VNFM: is the VNF management module that controls the VNF lifecycle (including instantiation, configuration, and shutdown). Generally, each VNF has a VNFM.
- NFVO: is the network service (NS) lifecycle management module that controls and manages NSs, VNFs of NSs, and virtual resources for VNFs.
- OSS/BSS: is the management system for a service provider. It is not a functional component in the NFV architecture, but the NFVO must provide an interface for interoperation with the OSS/BSS.



NFV Simplifies Network Operation

- Simplified enterprise and home networks: Service functions are moved to carrier networks.
- Lower OPEX and CAPEX and faster service innovation.
- Multi-instance virtualization on IT servers: reduces costs, simplifies the network, and implements unified management.

- OPEX is the operating expense, which is the sum of the maintenance cost, marketing expense, labor cost, and depreciation.
- CAPEX is the capital expenditure, which is the sum of the strategic investment and rolling investment. CAPEX is the capital investment that is placed for infrastructure construction or expansion and needs to be shared in multiple fiscal years.
- Set top box (STB): is a device used to enhance or expand functions of televisions and is usually placed on the top of a TV set. It can receive programs broadcast by a satellite or transferred over a cable. Additionally, it can provide value-added services, such as online movie, video on demand (VoD), and e-commerce.
- Residential gateway (RGW): is an access gateway device that is directly connected to a CPE (such as a POTS machine, ISDN phone, or IP phone). It allows voice calls from a home user to be transmitted over a data network.



Enterprise Network NFV Solution

SMEs directly purchase third-party services, bypassing carriers.

- Carriers cannot create revenue.
- SMEs face complex, costly service and device O&M.

Carriers provide services for enterprises from the cloud.

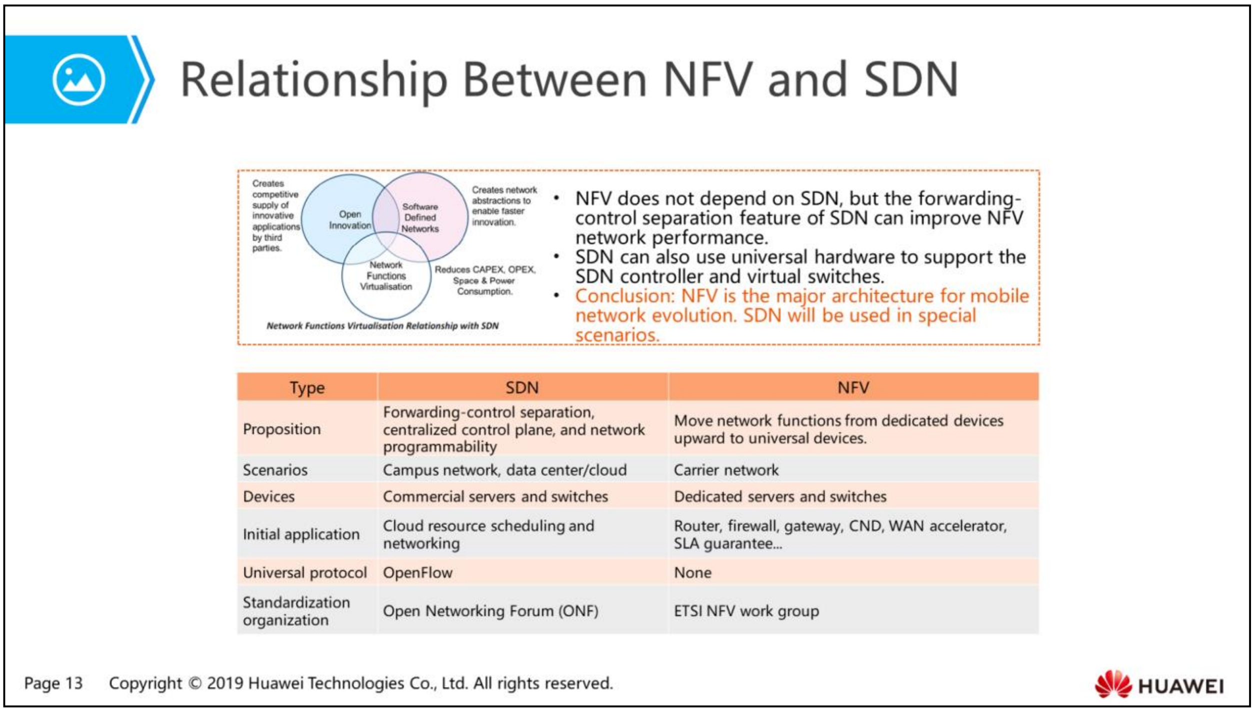
- Brings huge potential revenue for carriers.
- Simplifies O&M of SME networks.

Virtual access routers (vARs) enable carriers to provide services for enterprises over current connections.

- The vAR solution virtualizes advanced functions of AR routers, such as firewall, VoIP, and NAT, on servers. The servers can be located in a carrier’ s equipment room.
- The vAR solution simplifies CPE functions and features, and implements centralized management of advanced features. In actual project implementation, a VIP customer of a carrier may have thousands of CPEs distributed in different branches. The vAR solution can bring great convenience in this scenario.

Contents

1. Basic Concept of NFV
2. NFV Architecture
3. **Relationship Between NFV and SDN**



Relationship Between NFV and SDN

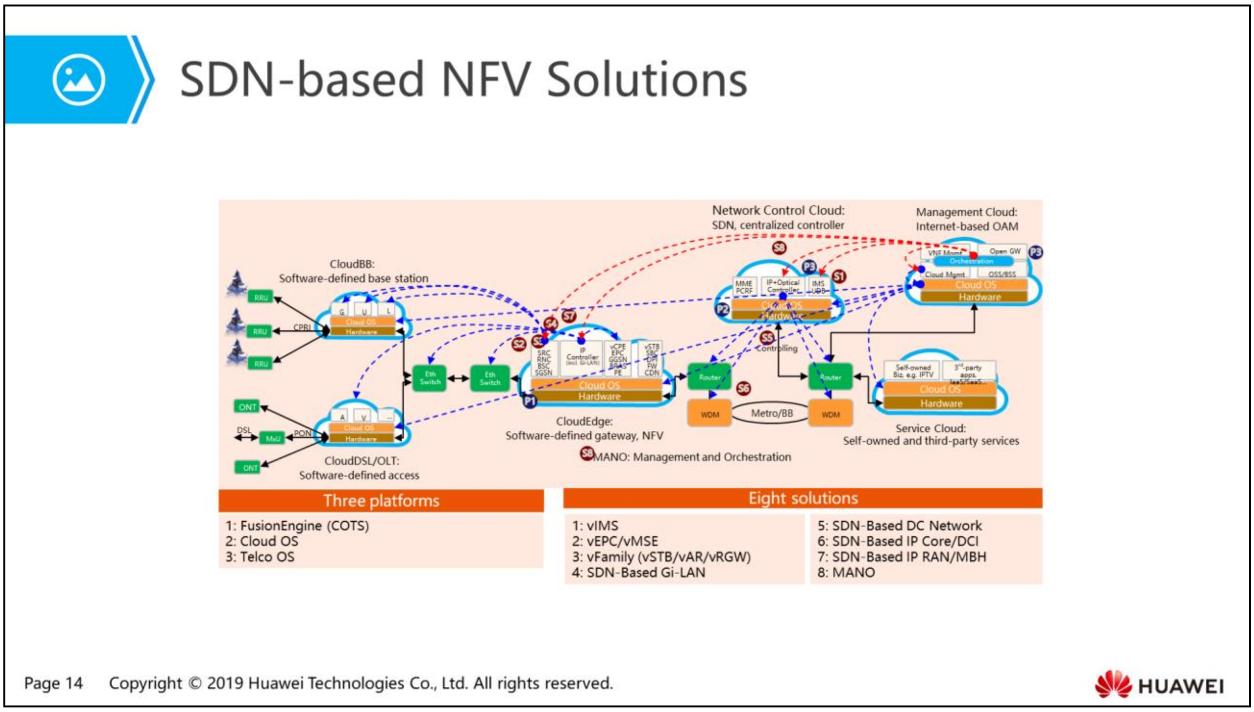
Creates competitive supply of innovative applications by third parties.
Open Innovation
Software Defined Networks
Creates network abstractions to enable faster innovation.
Network Functions Virtualisation
Reduces CAPEX, OPEX, Space & Power Consumption.

Network Functions Virtualisation Relationship with SDN

- NFV does not depend on SDN, but the forwarding-control separation feature of SDN can improve NFV network performance.
- SDN can also use universal hardware to support the SDN controller and virtual switches.
- Conclusion: NFV is the major architecture for mobile network evolution. SDN will be used in special scenarios.

Type	SDN	NFV
Proposition	Forwarding-control separation, centralized control plane, and network programmability	Move network functions from dedicated devices upward to universal devices.
Scenarios	Campus network, data center/cloud	Carrier network
Devices	Commercial servers and switches	Dedicated servers and switches
Initial application	Cloud resource scheduling and networking	Router, firewall, gateway, CND, WAN accelerator, SLA guarantee...
Universal protocol	OpenFlow	None
Standardization organization	Open Networking Forum (ONF)	ETSI NFV work group

- NFV is a device virtualization technology that runs control plane of devices on servers to make the devices open and compatible.
- SDN is a new network architecture that moves control plane of devices to a controller. The controller provides unified computing and delivers flow tables to devices.
- NFV and SDN are complementary to while independent from each other. Network functions can be virtualized and deployed without SDN, but combination of the two solutions can create more potential value.
- NFV aims to use current data center technologies to implement network function virtualization, without using SDN. However, NFV implementation depends on the control-forwarding separation concept of SDN, which can enhance device performance and simplify the processes of interoperation with existing devices, basic operations, and maintenance.
- NFV can provide infrastructure for SDN software running. Both NFV and SDN are implemented based on servers and switches.



SDN-based NFV Solutions

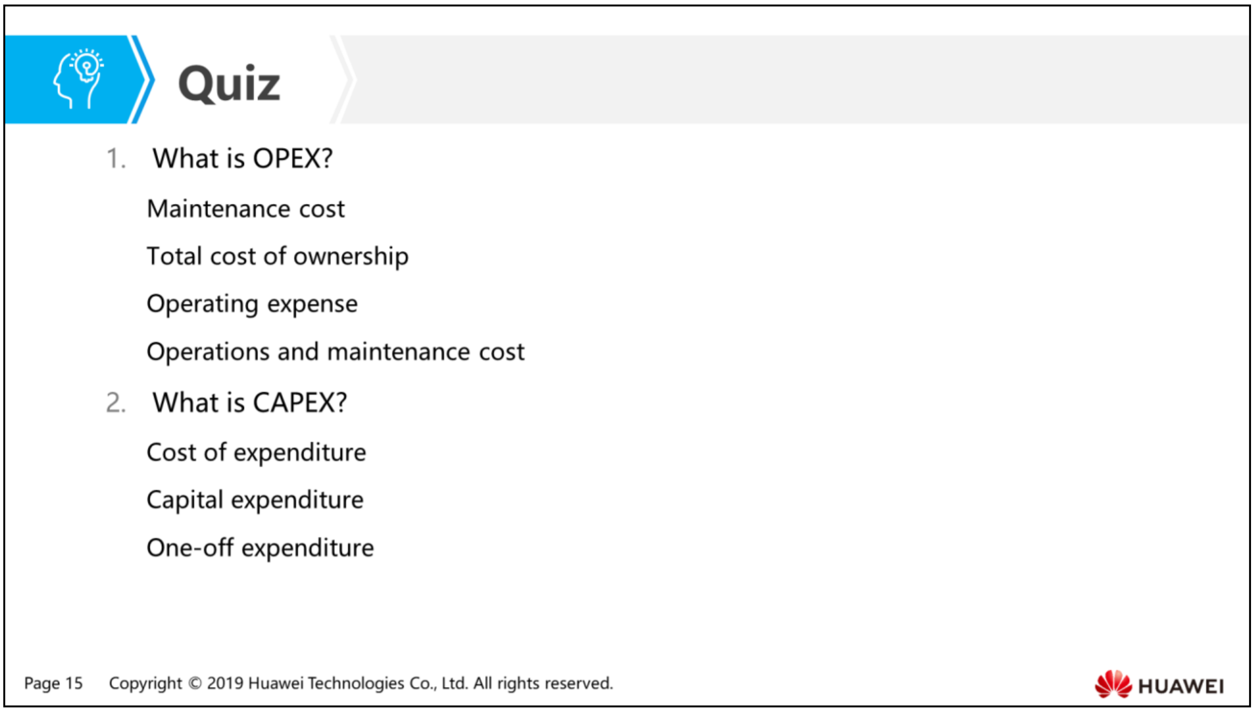
Three platforms

1: FusionEngine (COTS)
2: Cloud OS
3: Telco OS

Eight solutions

1: vIMS	5: SDN-Based DC Network
2: vEPC/vMSE	6: SDN-Based IP Core/DCI
3: vFamily (vSTB/vAR/vRGW)	7: SDN-Based IP RAN/MBH
4: SDN-Based Gi-LAN	8: MANO

- The SDN controller connects to a cloud platform through a northbound interface to receive configuration from the cloud platform. It calculates flow tables based on requirements received from the cloud platform and delivers flow tables to CE switches through a southbound interface.
- The SDN controller is implemented based on the NFV architecture, with E9000/RH2288s server at the bottom, SUSE Linux system as the software platform, and the Versatile Routing Platform (VRP) at the upper layer. The VRP platform is responsible for forwarding entry calculation.



Quiz

1. What is OPEX?

Maintenance cost

Total cost of ownership

Operating expense

Operations and maintenance cost

2. What is CAPEX?

Cost of expenditure

Capital expenditure

One-off expenditure

- Answer: C.
- Answer: B.

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