SD-WAN Solution Technology

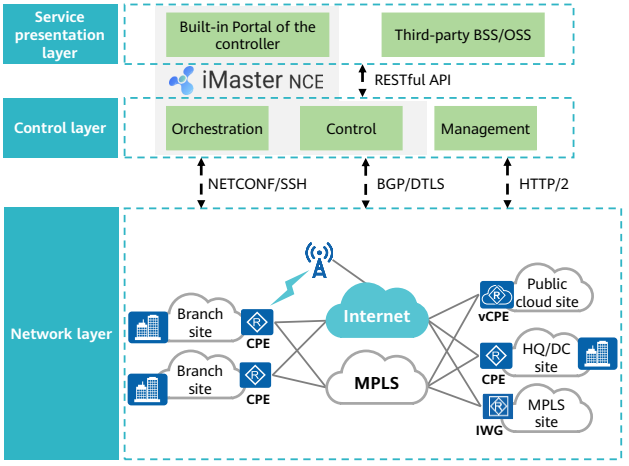
Foreword

- As digital transformation of enterprises steps into the cloud era and the software-defined networking (SDN) era is coming, software-defined WAN (SD-WAN) has become a next-generation solution for enterprise branch interconnection. It is widely deployed by enterprises due to its key features such as network-agnostic, intelligent traffic steering, zero touch provisioning (ZTP), and visualization.
- There are many vendors in the SD-WAN field. According to statistics of Gartner, more than 60 vendors in the world have provided multi-layer SD-WAN solutions that support multiple business models by the end of 2019.
- SD-WAN is deemed to be a next-generation enterprise branch interconnection solution by industry analysts, which has profound impact on and preliminarily replace existing traditional MPLS VPN services. In the future, SD-WAN will continue to develop and evolve rapidly oriented to emerging technologies and solutions such as cloud, 5G, XGSPON, artificial intelligence (AI), and blockchain.

Objectives

- On completion of this course, you will be able to:
  - Describe the architecture and components of SD-WAN Solution.
  - Describe the basic implementation of SD-WAN Solution.
  - Describe the functions and features of the customer-premises equipment (CPE).

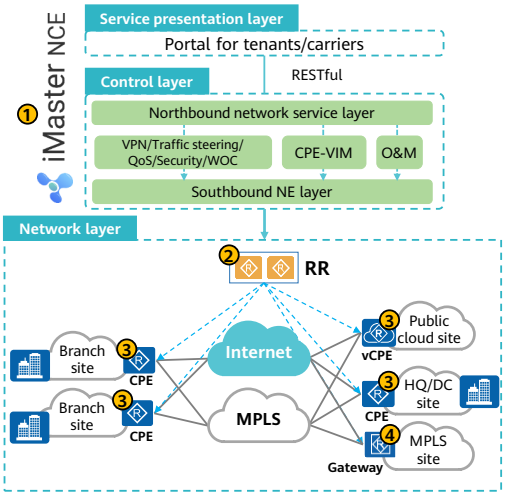
Architecture of SD-WAN Solution



- **Service presentation layer**: presents the SD-WAN service logic.
  - Provides portal pages for carriers, MSPs, and large enterprises, on which SD-WAN services can be processed and enabled in an end-to-end manner.
  - Allows customers to customize portal pages as needed through northbound open APIs of the SD-WAN controller (iMaster NCE-WAN).
- **Control layer**: controls network layer devices. Typically, iMaster NCE-WAN is used to abstract the network model of an SD-WAN network, and pre-configure and automatically provision network services based on service templates.
- **Network layer**: is the basic physical network of an enterprise WAN, which consists of physical and virtual devices including CPEs, virtual CPEs (vCPEs).

- From the perspective of functions, the overall architecture of the SD-WAN Solution consists of the network layer, control layer, and service presentation layer. These layers are associated with each other through standard interfaces and communication protocols.
- iMaster NCE-WAN is SD-WAN controller, and consists of the service layer (built-in Portal) and control layer.
- The enterprise HQ, branches, DCs, and IT infrastructures deployed on the cloud are referred to as enterprise sites.

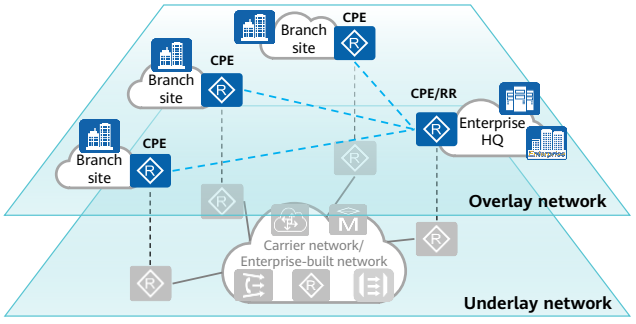
Key Components of the SD-WAN Solution



No.	Component	Functions
1	iMaster NCE-WAN	1. Network service orchestration 2. NE control 3. Basic network O&M 4. CPE orchestration and management 5. Basic performance monitoring (providing link quality information, application quality information, traffic information, as well as statistics from dimensions such as intra-site and inter-site)
2	RR	Distributes information about inter-CPE VPN routes and tunnels based on VPN topology policies.
3	CPE	Functions as the egress device of a site, which can be a traditional CPE or Network Functions Virtualization (NFV) vCPE.
4	Gateway	Connects an SD-WAN network to a non-SD-WAN network.

Network Layer Overview

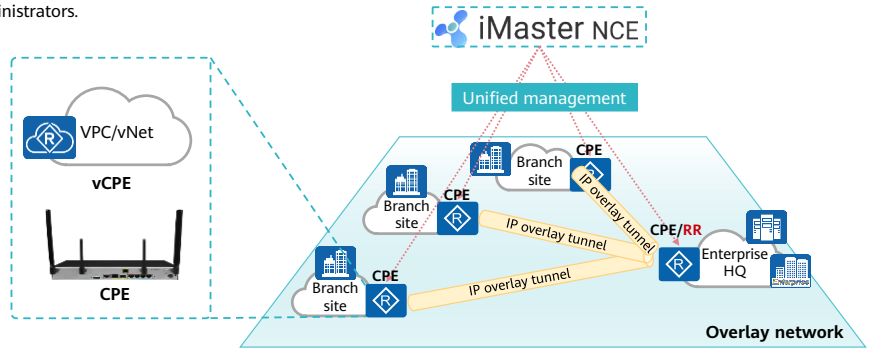
- The SD-WAN network of an enterprise consists of two layers: physical network (underlay) and virtual network (overlay), which are completely decoupled from each other.
  - Physical network: refers to the underlay WAN provided by a carrier or built by the enterprise itself, including private lines and MPLS networks.
  - Virtual network: is also called an overlay network. Huawei SD-WAN Solution introduces IP overlay virtualization technology to construct one or more virtual overlay networks on a physical network. Service policies are deployed on virtual networks and decoupled from the physical network, so that service forwarding is independent of WAN interconnection.



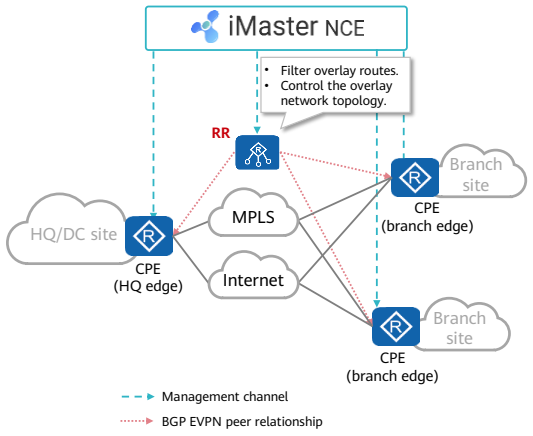
- Multiple overlay networks can be deployed to provide different services under the same tenant (for example, services of multiple departments) or provide different services for different tenants.
- From the perspective of network device functions, the SD-WAN network layer consists of two types of NEs: CPE and gateway.

CPE Overview

- A CPE is an edge node of an SD-WAN network and also called an edge CPE. CPEs are interconnected with each other through IP overlay tunnels.
- CPEs are classified into traditional physical CPEs and vCPEs that are deployed at public cloud sites.
- All SD-WAN CPEs of an enterprise are centrally managed by iMaster NCE-WAN, and are managed and maintained by tenant administrators.



RR Overview

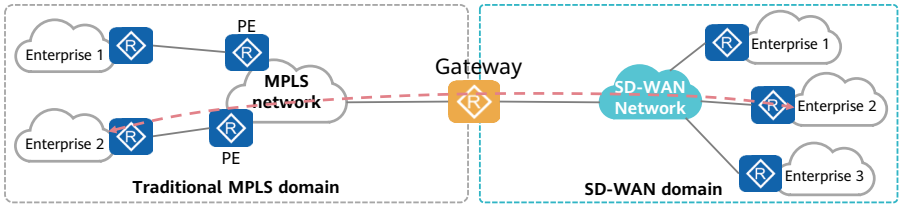


- A router reflector (RR) transfers BGP routes and reduces the number of BGP peers.
- In Huawei SD-WAN Solution, an RR also controls routes and the network topology. Therefore, an RR is also called an area controller on SD-WAN networks.
- Both CPEs at edge sites and RRs are managed by iMaster NCE-WAN.
- Control channels are established between RRs and between RRs and edge sites.
- RRs are managed by iMaster NCE-WAN, and control route sending and receiving at edge sites based on the overlay network topology model. In this manner, sites can communicate with each other based on the designed overlay topology model.

- RR site: A CPE functions as an RR and distributes EVPN routes between CPE gateways at edge sites based on the VPN topology policy.
- If an egress CPE at a site is configured as both the gateway and RR, this site is an RR site. If no device takes the role of the gateway or RR at a site, the site is an edge site.
- One edge site can establish IBGP peer relationships with two RRs simultaneously, and the two RRs back up each other.
- Multiple RRs can be deployed for a tenant. All RRs are connected in full-mesh mode on the control plane.

Gateway Overview

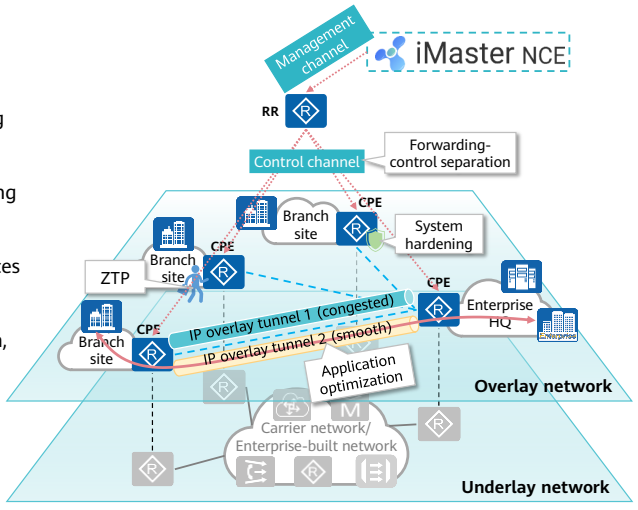
- New SD-WAN sites of an enterprise often need to communicate with the enterprise's legacy sites or third-party services. Because some legacy sites are interconnected through MPLS VPN, while SD-WAN sites are interconnected through IP overlay tunnels, SD-WAN sites cannot directly communicate with legacy sites.
- An **SD-WAN gateway** can connect to both SD-WAN and traditional MPLS networks, achieving interconnection between the SD-WAN and traditional MPLS networks.



- A gateway's role name varies depending on the service scenario. For example, a gateway connecting SD-WAN sites to legacy sites is an interworking gateway (IWG), as shown in the above figure. A gateway connecting SD-WAN sites to a cloud is called a cloud gateway. In addition, functions of a gateway can be extended. A gateway that connects Point of Presence (POP) sites for building a POP network is referred to as a POP gateway.

Main Functions of SD-WAN Solution

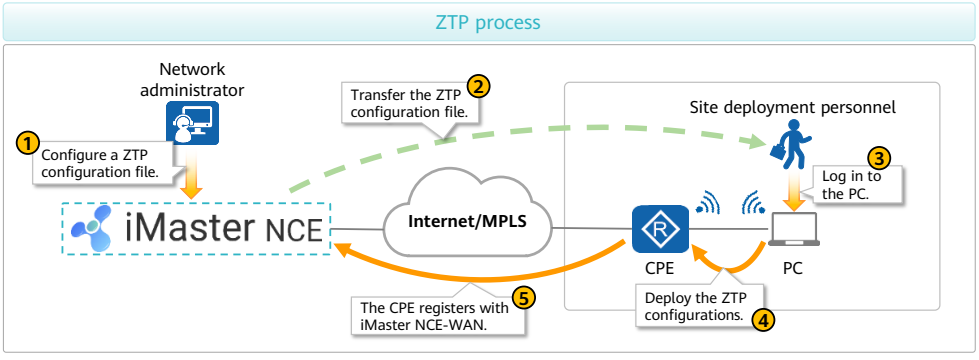
- SD-WAN Solution provides the following functions:
  - Zero touch provisioning (ZTP), enabling service provisioning within 1 hour
  - Forwarding-control separation, achieving flexible networking
  - Application optimization, making services controllable and visible
  - Comprehensive security defense system, ensuring service security



- ZTP: Multiple ZTP modes are available to enable CPEs to quickly register with iMaster NCE-WAN.
- Forwarding-control separation, achieving flexible networking: CPEs establish management channels with iMaster NCE-WAN through NETCONF, and iMaster NCE-WAN delivers configurations to CPEs to establish IP overlay tunnels.
- Application optimization, making services controllable and visible: Service awareness (SA) technology is used to identify applications. TCP Flow Performance Monitor (FPM) and IP FPM technologies are used to implement application quality detection, and IP FPM technology is used to implement link quality measurement. Smart Policy Routing (SPR) technology implements intelligent link switching based on the application quality.
- Comprehensive security defense system, ensuring service security: Multiple VPN technologies, such as IPsec and MPLS, are used to provide E2E security protection. The firewall function provides comprehensive security assurance at the hardware, pipe, and application levels.

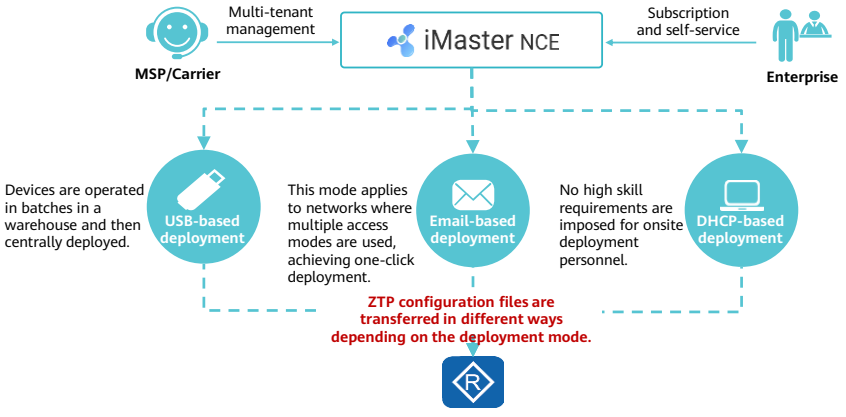
ZTP Zero Touch Provisioning Overview

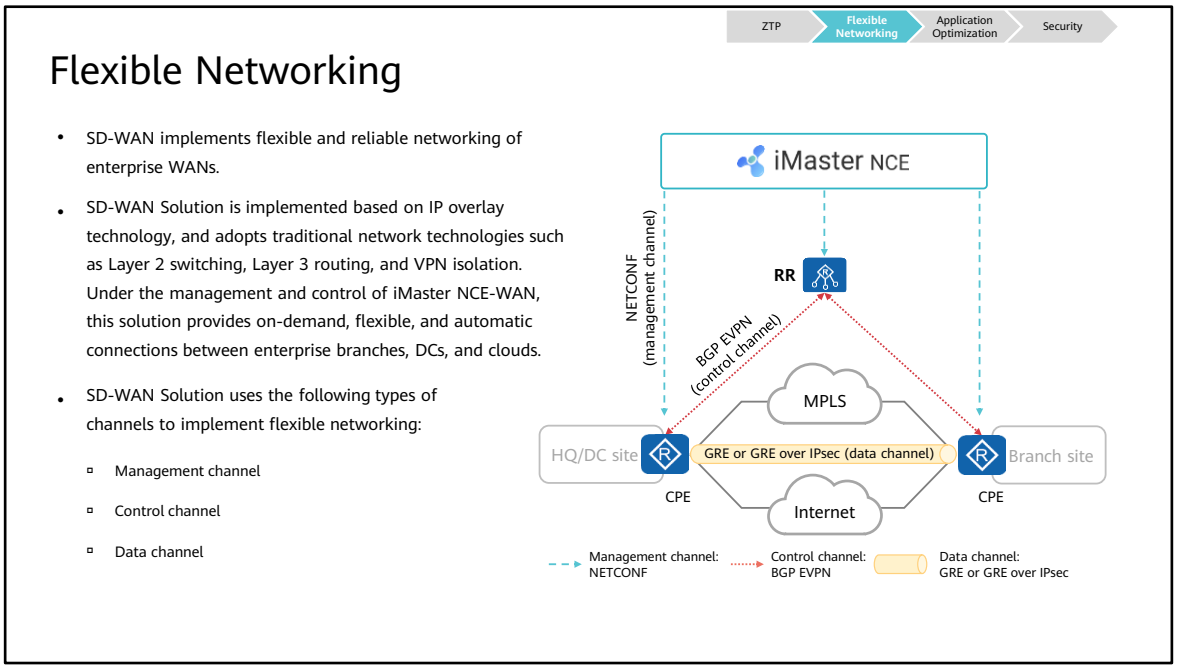
- With the development of network technologies such as SDN and cloud computing, an increasing number of enterprise networks adopt cloud-based management. However, most sites still need to be deployed by technical engineers onsite, leading to high deployment costs and long deployment period. Huawei offers ZTP to enable quick deployment.



ZTP Modes

- SD-WAN Solution supports the following ZTP modes:

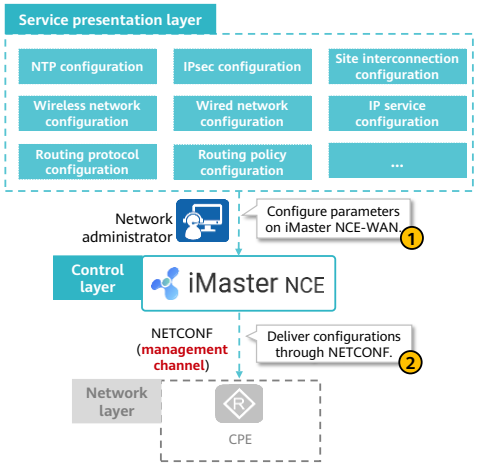




- Management channel:
  - iMaster NCE-WAN establishes management channels with all managed devices through NETCONF for network-wide device management and service orchestration.
- Control channel:
  - Control channels are established between CPEs and RRs.
  - RRs centrally control and distribute service routes between branch sites.
  - The enhanced BGP EVPN protocol is used to implement separate transmission of tenants' VPN routes and next-hop information, and implement IPsec SA negotiation.
- Data channel:
  - Data channels are established between CPEs.
  - Data is forwarded over GRE or GRE over IPsec data tunnels. The extended GRE header carries VN IDs to differentiate tenants or departments, thereby transmitting data of multiple VNs over the same data tunnel.

Management Channel

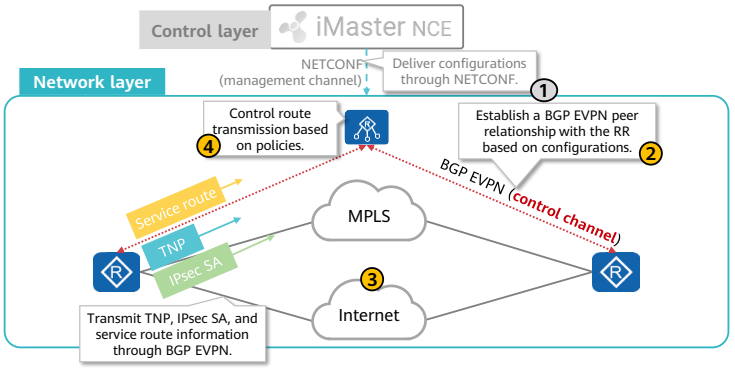
- iMaster NCE-WAN establishes management channels with CPEs through NETCONF.
- iMaster NCE-WAN delivers configurations through control channels to achieve the following functions:
  - Unified management of CPEs, automatic service delivery, and unified control of overlay networks
  - Application visualization and automatic application optimization
  - Network security services



ZTP | Flexible Networking | Application Optimization | Security

Control Channel

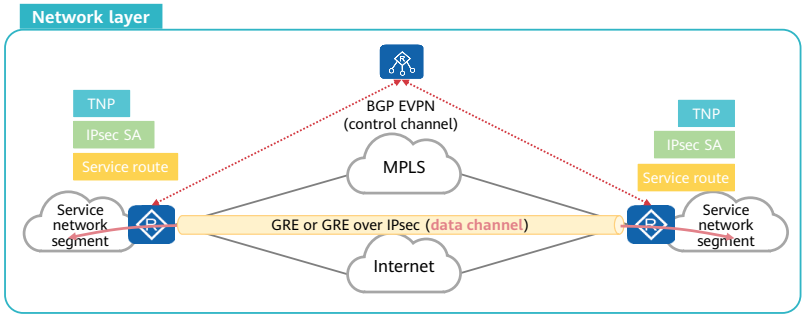
- After iMaster NCE-WAN delivers configurations to a CPE through the management channel, the CPE establishes a control channel with an RR through BGP EVPN.
- The control channel is used to transmit transport network port (TNP) information, IPsec SA information, and service routes.
- After the control channel is established, iMaster NCE-WAN controls route transmission and overlay topology establishment by deploying policies on the RR.



- A TNP is a WAN port on a CPE used for connecting to a transport network. The key TNP information includes the site ID, CPE router ID, transport network ID, public IP address, private IP address, and tunnel encapsulation mode.

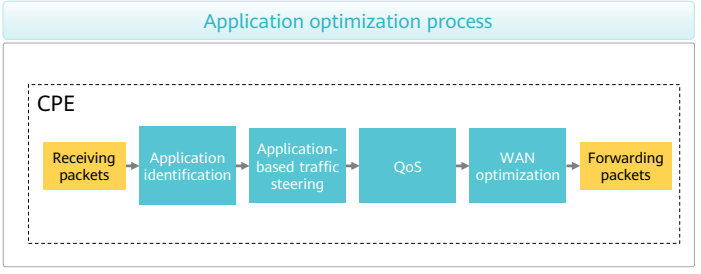
Data Channel

- SD-WAN Solution uses GRE or GRE over IPsec to establish data channels.
- CPEs establish GRE or GRE over IPsec tunnels based on the TNP and IPsec SA information transferred through BGP EVPN.
- CPEs forward data based on the service routes transferred through BGP EVPN.



Application Optimization

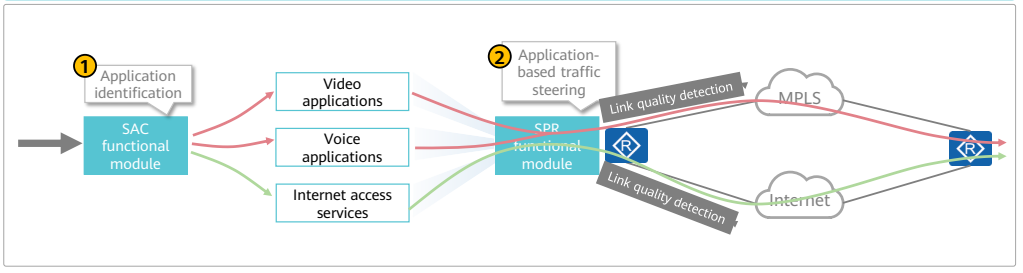
- To meet diversified requirements of enterprise applications, traditional WANs have the following issues to resolve:
  - Applications of different values are carried on the same link.
  - When link quality deteriorates, dynamic routing cannot be implemented.
  - No effective measure is available when link quality deteriorates.
- To resolve these issues, Huawei SD-WAN Solution offers enterprise experience optimization functions, including:
  - Application identification
  - Application-based traffic steering
  - QoS
  - WAN optimization



Application Identification and Traffic Steering

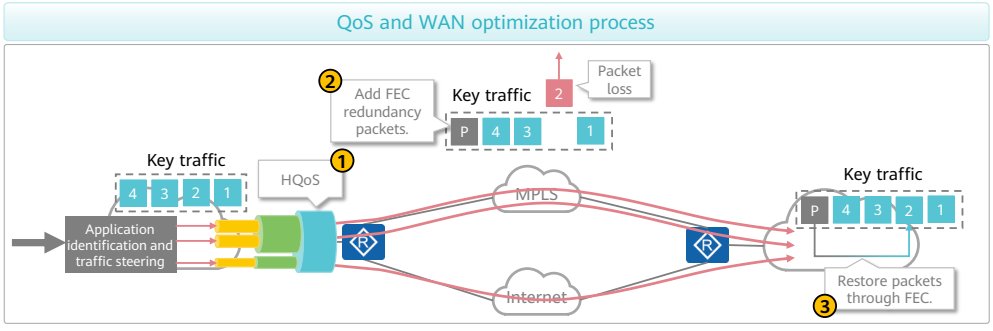
- SD-WAN Solution uses Smart Application Control (SAC) to identify applications and uses SPR to implement application-based traffic steering.
  - SAC enables a device to identify applications and groups application traffic through SA and first-packet identification (FPI).
  - SPR enables a device to measure the link quality based on link quality detection packets and determine forwarding paths for traffic.

Application identification and traffic steering processes



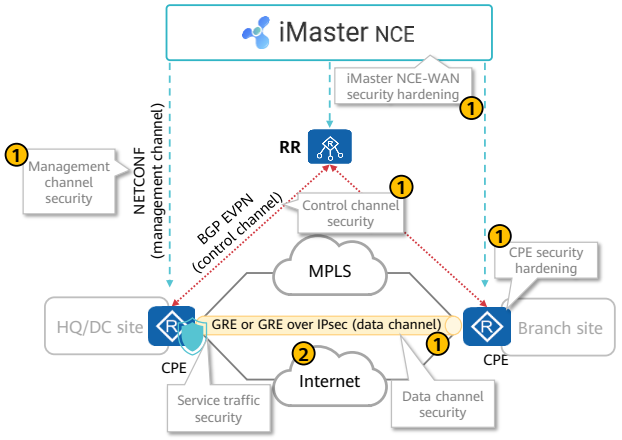
QoS and WAN Optimization

- SD-WAN Solution uses HQoS for bandwidth control and scheduling, and uses Forward Error Correction (FEC) or Adaptive FEC (A-FEC) for WAN traffic optimization.
  - HQoS implements hierarchical scheduling based on multi-level queues and differentiates services and users, implementing refined QoS.
  - FEC or A-FEC optimization enables the local device to adjust related parameters based on packet loss on the network to generate redundant packets. The peer device then verifies and reassembles the packets.



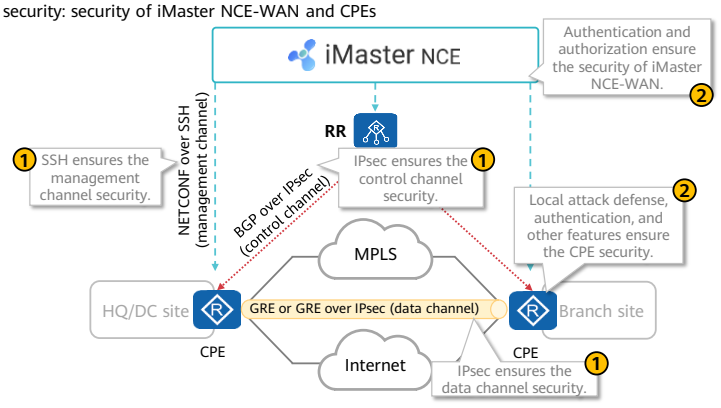
Security Overview

- With the emergence of SD-WAN, the traditional closed architecture of enterprise WANs is transformed into an open architecture, which enlarges the attack range and brings new security challenges, including unauthorized access, data leakage, and network attacks.
- SD-WAN Solution provides high security from two perspectives:
  - System security: component security and inter-component security
  - Service security: firewall, IPS, and URL filtering



SD-WAN System Security Hardening

- SD-WAN system security includes:
  - Inter-component security: security of management, control, and forwarding channels
  - Component security: security of iMaster NCE-WAN and CPEs



SD-WAN Service Security

- From the perspective of traffic, SD-WAN services are classified into the following types:
  - Site-to-site access service
    - IPsec ensures security of site-to-site access services.
  - Site-to-Internet access service
    - The built-in firewall, IPS, and URL filtering functions of CPEs ensure the security of site-to-Internet access services.
  - Site-to-cloud access service
    - iMaster NCE-WAN is interconnected with a third-party security gateway and controls this gateway to provide security services.