园区网典型技术应用概述

一、什么是园区网络
1、园区网络一般是指企业或者机构的内部网络
2、园区网络的主要目的是使企业或者机构的各项业务运作更有效率
3、按规模可以将园区网络划分成：
3.1、大型园区网络：终端用户数量/个 > 2000；网元数量/个 > 100
3.2、中型园区网络：2000 > 终端用户数量/个 > 200；100 >网元数量/个 > 25
3.3、小型园区网络：终端用户数量/个 < 200；网元数量/个 < 25
4、有些企业还存在不同地域的办公分支机构，每个分支机构网络可看做一个单园区网络

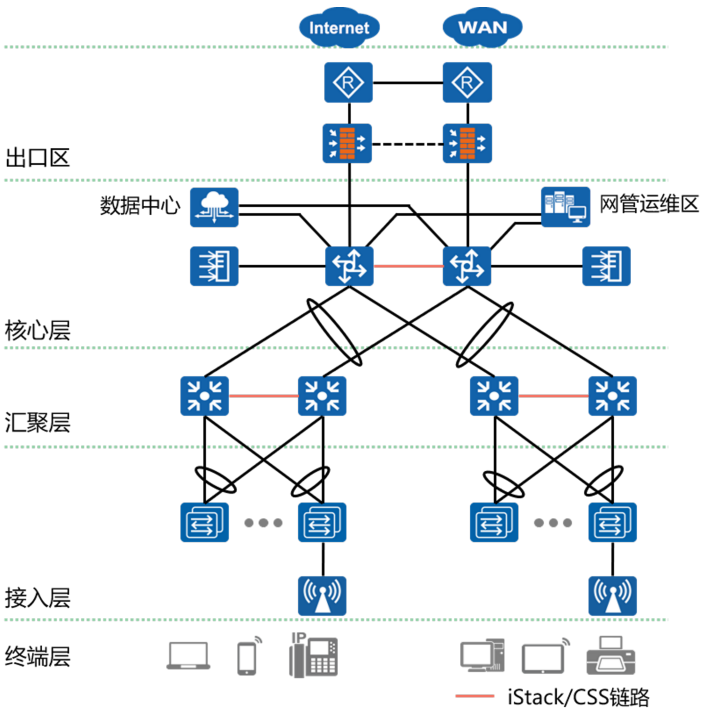
二、常见的行业园区网
1、企业园区网络
关注网络可靠性、先进性，持续提升员工的办公体验，保障运营生产的效率和质量

2、校园网络
2.1、分为普教园区和高教园区
2.2、高教园区相对复杂，通常存在教研网、学生网，还可能有运营性的宿舍网络
2.3、网络可管理性、安全性要求高；对网络先进性亦有要求

3、政务园区网络
3.1、通常指政府机构的内部网络
3.2、安全要求极高，通常采用内网和外网隔离的措施保障涉密信息的绝对安全

4、商业园区网络
4.1、商场、超市、酒店、公园等
4.2、网络主要用于服务消费者，此外还包含服务内部办公的子网
4.3、提供上网服务，并构建商业智能化系统提升用户体验，降低运维成本，提升商业效率，实现价值转移
注：为了满足不同行业园区的需求，园区网络架构会根据其服务的行业特点进行设计， 最终打造的是带有行业属性的园区网络方案

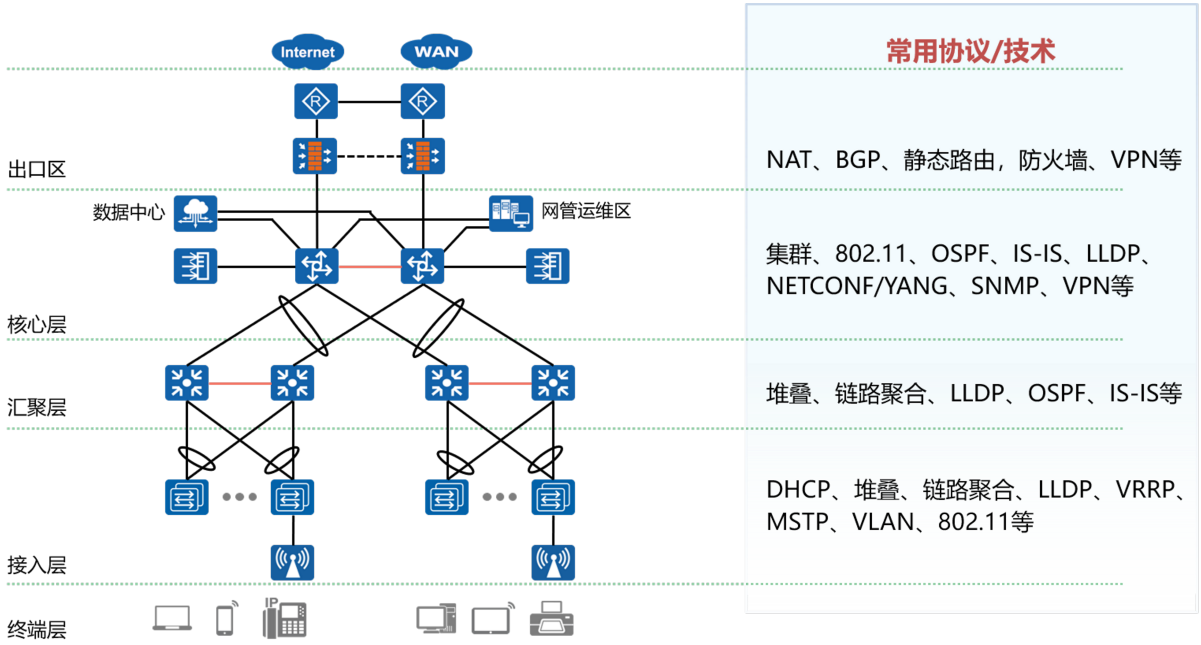
三、园区网络典型架构



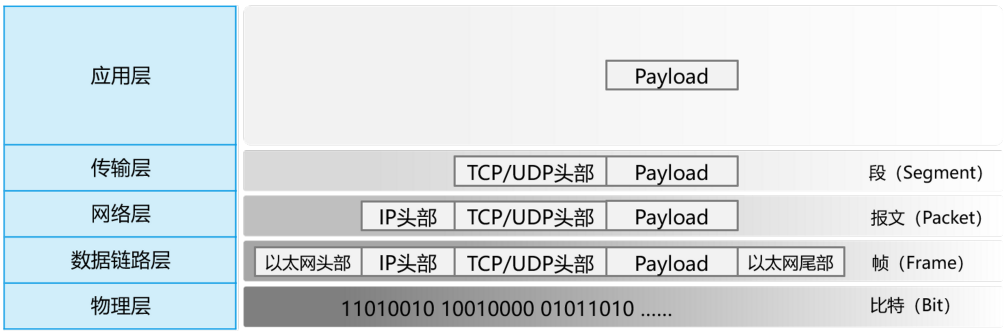
核心层：是园区网骨干，是园区数据交换的核心，联接园区网的各个组成部分，如数据中心、管理中心、园区出口等
汇聚层：处于园区网的中间层次，完成数据汇聚或交换的功能，可以提供一些关键的网络基本功能，如路由、安全等

接入层：为终端用户提供园区网接入功能，是园区网的边界
出口区：园区内部网络到外部网络的边界，用于实现内部用户接入到公网，外部用户（包括客户、合作伙伴、分支机构、远程用户等）接入到内部网络
数据中心区：部署服务器和应用系统的区域，为企业内部和外部用户提供数据和应用服务

四、园区网络主要协议/技术

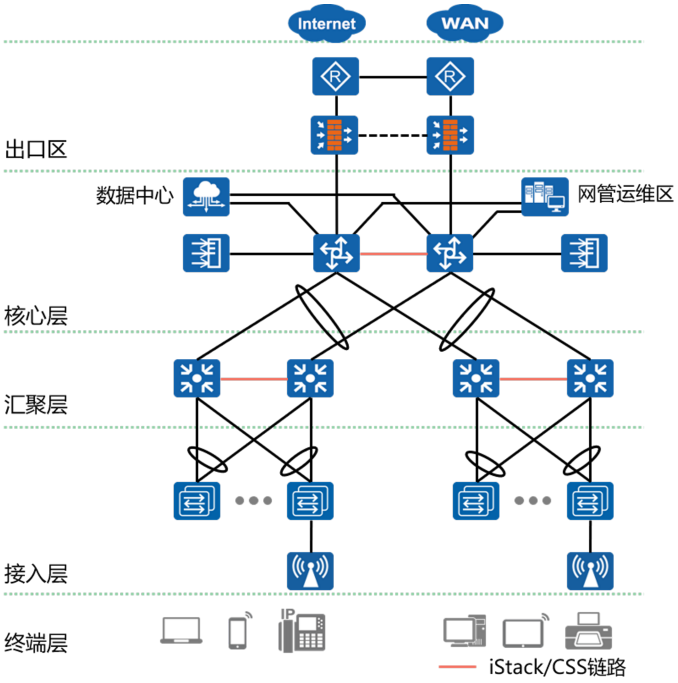


五、从TCP/IP对等模型说起



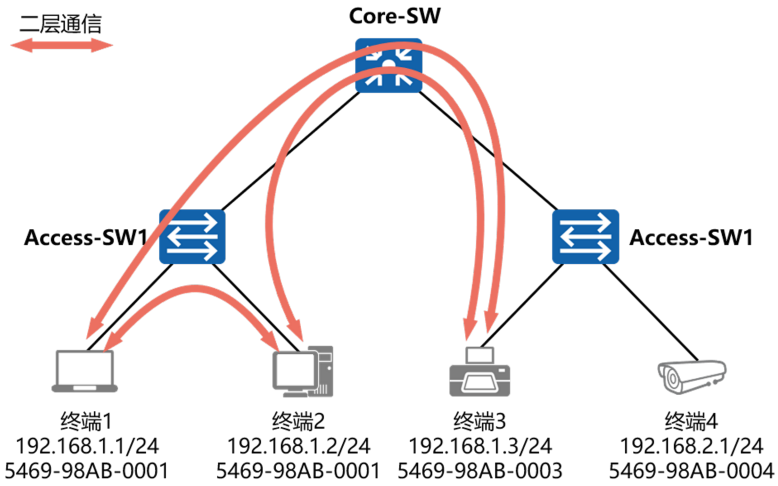
1、将网络的通信过程划分为小一些、简单一些的部件，有助于各个部件的开发、设计和故障排除
2、通过网络组件的标准化，允许多个供应商进行开发
3、通过定义在模型的每一层实现什么功能，鼓励产业的标准化
4、允许各种类型的网络硬件和软件相互通信

六、从园区网络到以太网二层交换

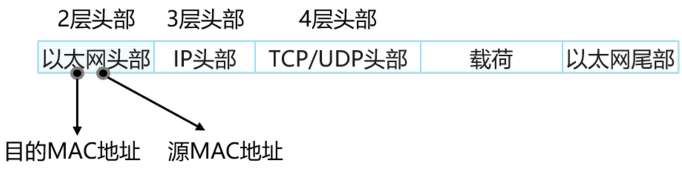


1、接入层为用户提供各种接入方式，是终端接入网络的第一层
2、接入层通常由接入交换机组成，接入层交换机在网络中数量众多，安装位置分散，通常是简单的二层交换机
3、若终端层存在无线终端设备，接入层需要无线接入点AP设备，AP设备通过接入交换机接入网络

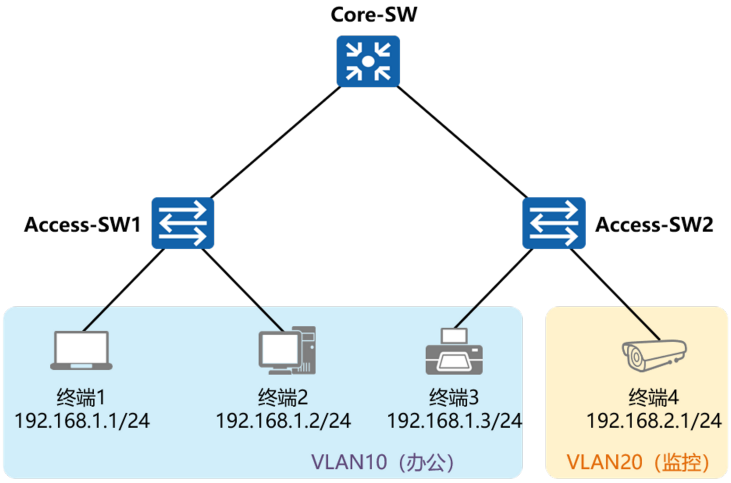
七、什么是二层交换



1、二层交换是以太网交换机的基本功能
2、二层交换指的是交换机根据数据帧的第二层头部中的目的MAC地址进行帧转发的行为
3、每台交换机都维护一个MAC地址表，用于指导数据帧转发
4、当交换机收到数据帧时，将在其MAC地址表中查询该帧的目的MAC地址，并根据匹配的表项执行相应的操作。此外，交换机收到数据帧时，还会进行源MAC地址学习

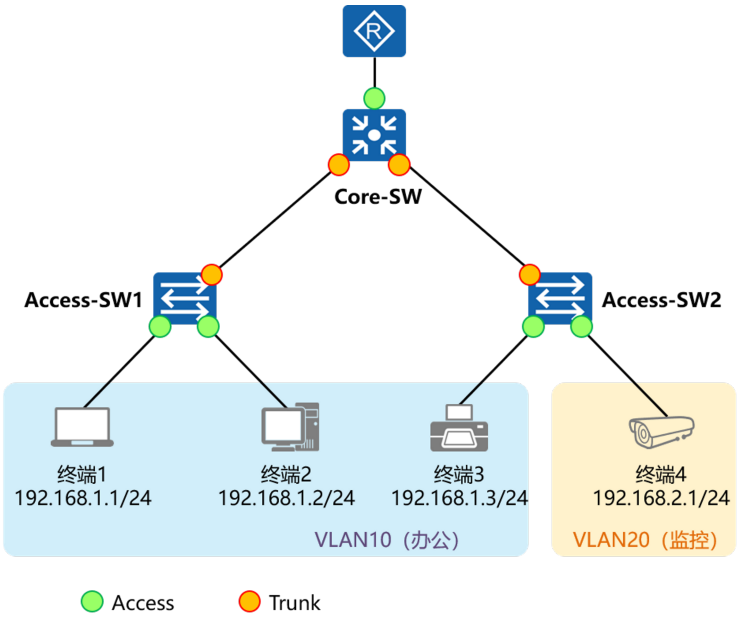


八、VLAN

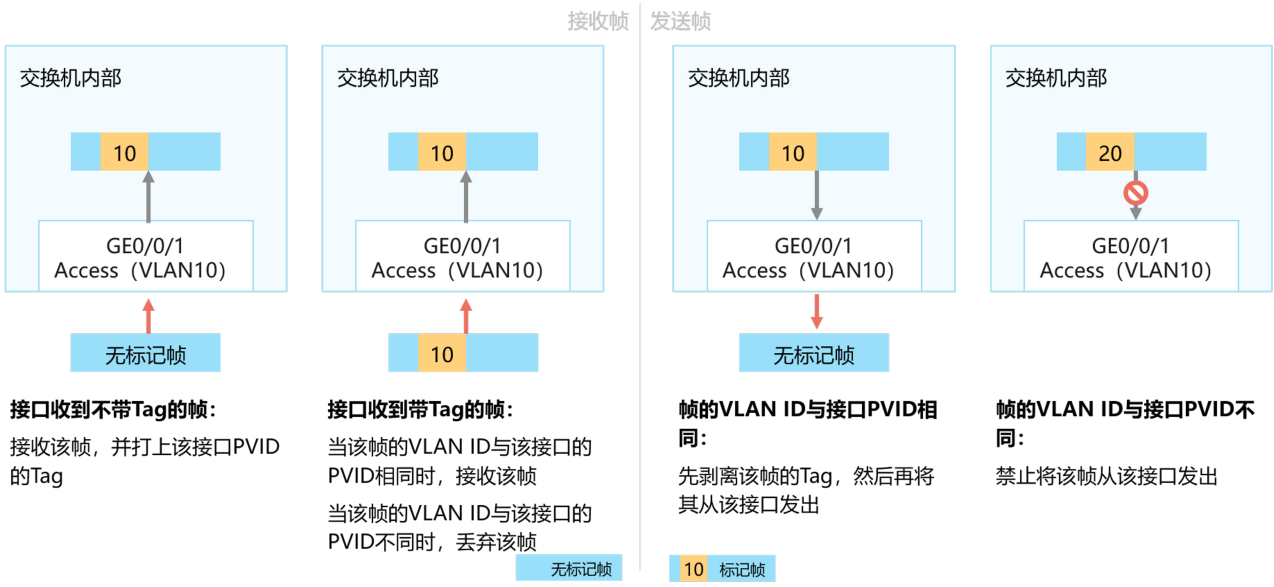


1、VLAN（Virtual Local Area Network）即虚拟局域网，是将一个物理的LAN在逻辑上划分成多个广播域的通信技术
2、一个VLAN中所有设备都是在同一广播域内，不同的VLAN为不同的广播域
3、VLAN内的设备间可以直接通信，而VLAN间不能直接互通
4、VLAN之间互相隔离，不同VLAN间需通过三层设备实现相互通信
5、一个VLAN一般为一个逻辑子网
6、VLAN中成员多基于交换机的端口分配，所谓的VLAN划分，通常指的是将交换机的接口添加到特定的VLAN中，从而该接口所连接的设备也加入到了该VLAN

九、以太网二层接口类型概述
1、交换机的以太网二层接口主要存在以下三种类型：



1.1、Access：常用来连接用户PC、服务器等终端设备的接口。Access接口所连接的这些设备的网卡往往只收发无标记帧。Access接口只能加入一个VLAN



接口收到不带Tag的帧：

接收该帧，并打上该接口PVID的Tag

接口收到带Tag的帧：

当该帧的VLAN ID与该接口的PVID相同时，接收该帧

当该帧的VLAN ID与该接口的PVID不同时，丢弃该帧

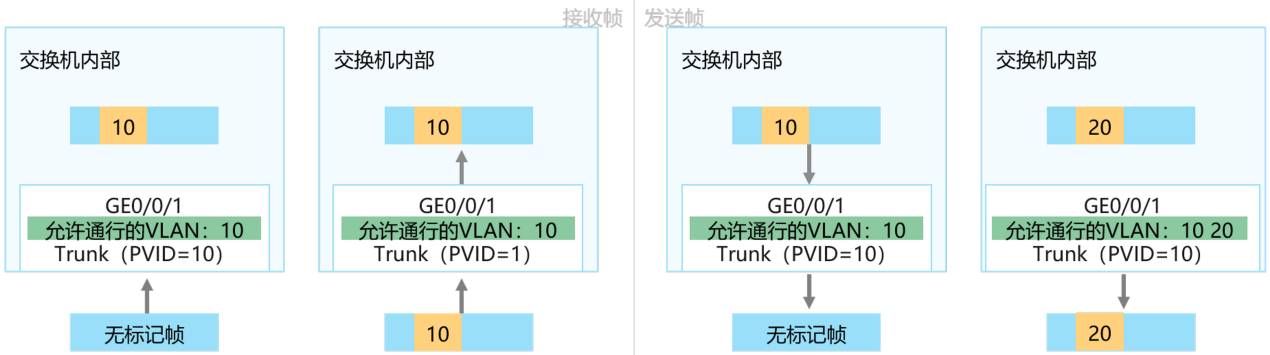
帧的VLAN ID与接口PVID相同：

先剥离该帧的Tag，然后再将其从该接口发出

帧的VLAN ID与接口PVID不同：

禁止将该帧从该接口发出

1.2、Trunk：Trunk接口允许多个VLAN的数据帧通过，这些数据帧通过802.1Q Tag实现区分。Trunk接口常用于交换机之间的互联，也用于连接路由器、防火墙等设备的子接口



接口收到不带Tag的帧：

该帧打上PVID，当PVID在该接口允许通过的VLAN列表里时接收该帧；当PVID不在允许通过的VLAN列表里时，丢弃该帧

接口收到带Tag的帧：

当该帧的VLAN ID在该接口允许通过的VLAN列表里时，接收该帧，否则丢弃该帧

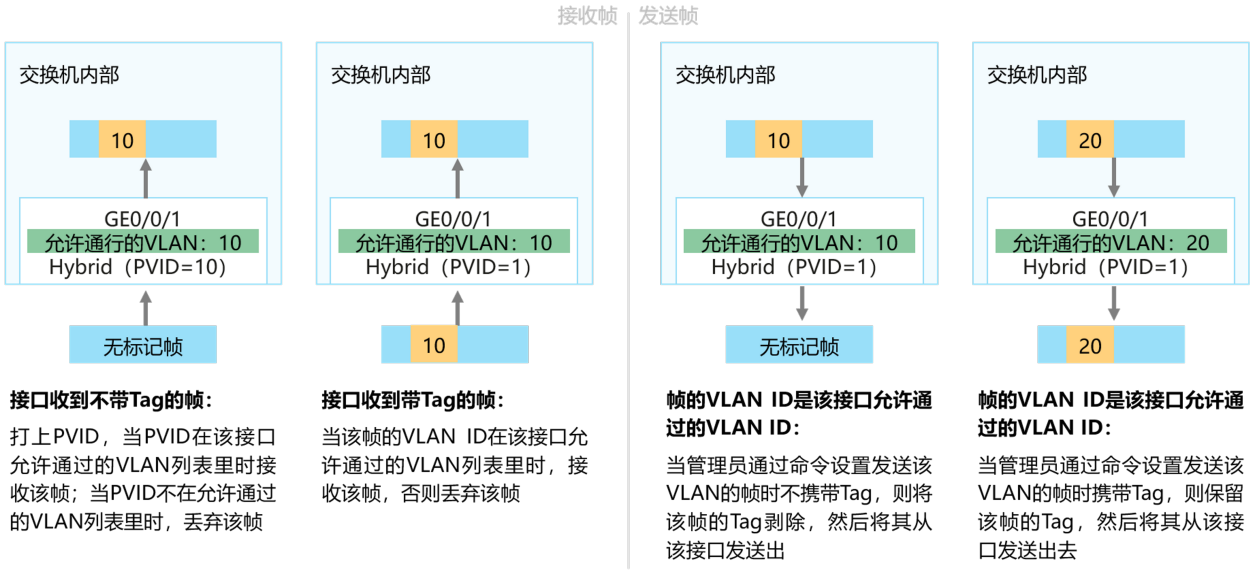
帧的VLAN ID与接口PVID相同：

当该帧的VLAN ID在该接口允许通过的VLAN列表中，则将该帧的Tag剥除，然后将其从该接口发送出去；如果VLAN ID不在允许通过的VLAN列表中则禁止将该帧从该接口发出

帧的VLAN ID与接口PVID不同：

当该帧的VLAN ID在该接口允许通过的VLAN列表中，则保留该帧的Tag，然后将其从该接口发送出去；如果VLAN ID不在允许通过的VLAN列表中则禁止将该帧从该接口发出

1.3、Hybrid：Hybrid接口与Trunk接口类似，也允许多个VLAN的数据帧通过，这些数据帧通过802.1Tag实现区分。用户可以灵活指定Hybrid接口在发送某个（或某些）VLAN的数据帧时是否携带Tag



接口收到不带Tag的帧：

打上PVID，当PVID在该接口允许通过的VLAN列表里时接收该帧；当PVID不在允许通过的VLAN列表里时，丢弃该帧

接口收到带Tag的帧：

当该帧的VLAN ID在该接口允许通过的VLAN列表里时，接收该帧，否则丢弃该帧

帧的VLAN ID是该接口允许通过的VLAN ID：

当管理员通过命令设置发送该VLAN的帧时不携带Tag，则将该帧的Tag剥除，然后将其从该接口发送出

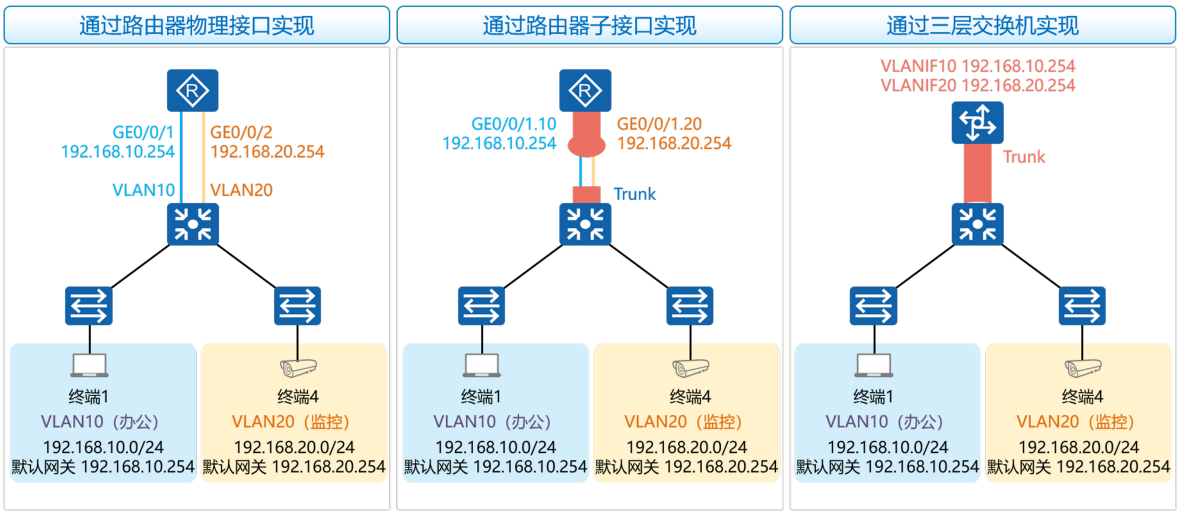
帧的VLAN ID是该接口允许通过的VLAN ID：

当管理员通过命令设置发送该VLAN的帧时携带Tag，则保留该帧的Tag，然后将其从该接口发送出去

2、VLAN划分方式总览

VLAN划分方式	原理
基于接口	根据交换机的接口来划分VLAN
基于MAC地址	根据数据帧的源MAC地址来划分VLAN
基于子网划分	根据数据帧中的源IP地址来划分VLAN
基于协议划分	根据数据帧所属的协议（族）类型及封装格式来划分VLAN
基于策略（MAC地址、IP地址、接口）划分	根据配置的策略划分VLAN，能实现多种组合的划分方式，包括接口、MAC地址、IP地址等

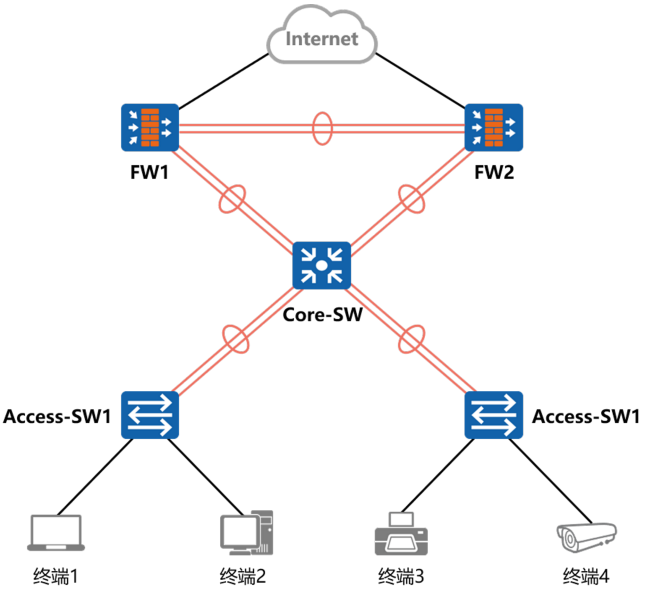
3、实现VLAN之间的IP可达性



十、以太网链路聚合

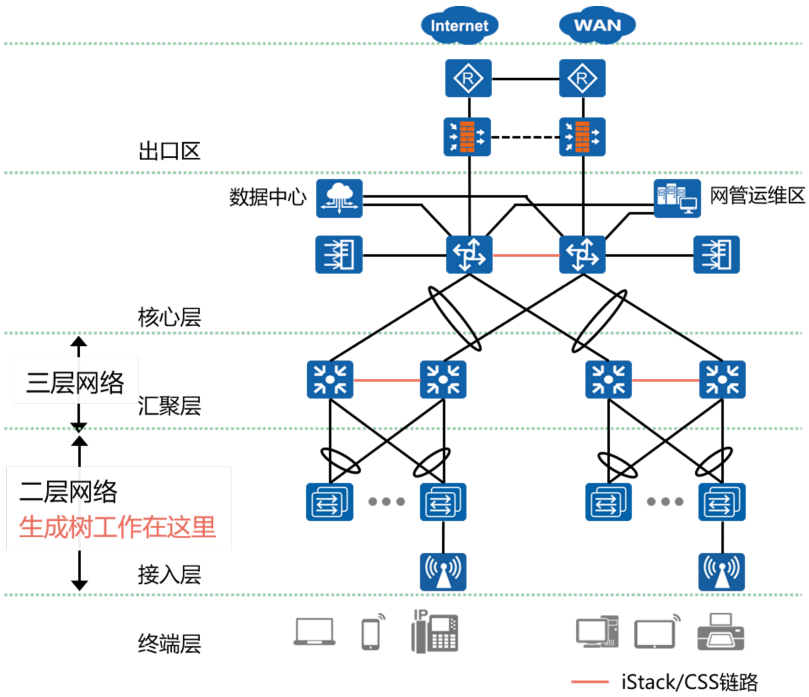
1、链路聚合（Link Aggregation，LAG）是将多条物理链路捆绑在一起成为一条逻辑链路，从而增加链路带宽的技术

2、完成聚合后的链路称为以太网聚合链路



3、链路聚合的优势：
3.1、增加可用带宽
3.2、提供负载均衡
3.3、提供网络冗余性
3.4、提高网络的可靠性
3.5、降低转发延迟
3.6、缩小转发所需时间
4、链路聚合的2种模式：手工聚合、LACP
5、链路聚合既可以配置在交换机上，也可以配置在路由器

十一、生成树技术 —— 防环+保证二层网络可靠性

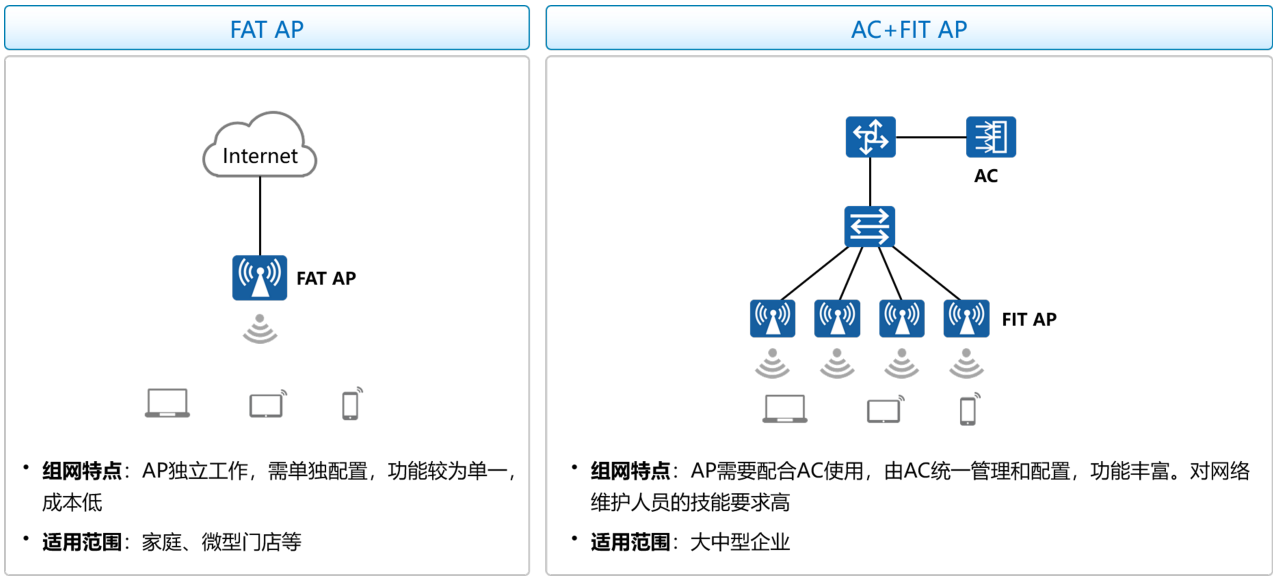


1、生成树的作用及特点：
1.1、解决交换网络中的环路问题
1.2、动态地适应根据网络拓扑变更
1.3、配合冗余链路，保证二层网络可靠性

2、生成树有3种模式：
2.1、STP【802.1D】
2.2、RSTP【802.1W】
2.3、MSTP【802.1S】

十二、WLAN与主要网元
1、WLAN（Wireless Local Area Network，无线局域网）广义上是指以无线电波、激光、红外线等来代替有线局域网中的部分或全部传输介质所构成的网络
2、802.11是IEEE在1997年为WLAN定义的一个无线网络通信的工业标准
3、此后这一标准又不断得到补充和完善，形成802.11的标准系列，例如
802.11、802.11a、802.11b、802.11g、802.11n、802.11ac、802.11ac-II、802.11ax等

4、WLAN组网架构综述



5、AC+FIT AP架构
1、AC (Access Controller，无线控制器)：在AC+FIT AP网络架构中，AC对无线局域网中的所有FIT AP进行控制和管理
2、AC负责WLAN的接入控制、转发和统计、AP的配置监控、漫游管理、AP的网管代理、安全控制
3、FIT AP（瘦AP）负责802.11报文的加解密、802.11的物理层功能、接受AC的管理、空口的统计等简单功能
4、AC和AP之间使用的通信协议是CAPWAP
5、相比于FAT AP架构，AC+FIT AP架构的优点如下：
5.1、配置与部署更容易
5.2、安全性更高

5.3、更新与扩展容易

6、CAPWAP

6.1、CAPWAP（Control And Provisioning of Wireless Access Points Protocol Specification，无线接入点控制和配置协议）定义了如何对AP进行管理、业务配置，即AC通过CAPWAP隧道来实现对AP的集中管理和控制

6.2、CAPWAP协议定义的主要内容有：AP自动发现AC，AC对AP进行安全认证，AP从AC获取软件，AP从AC获得初始和动态配置等。通过该协议，AP和AC之间建立起CAPWAP隧道

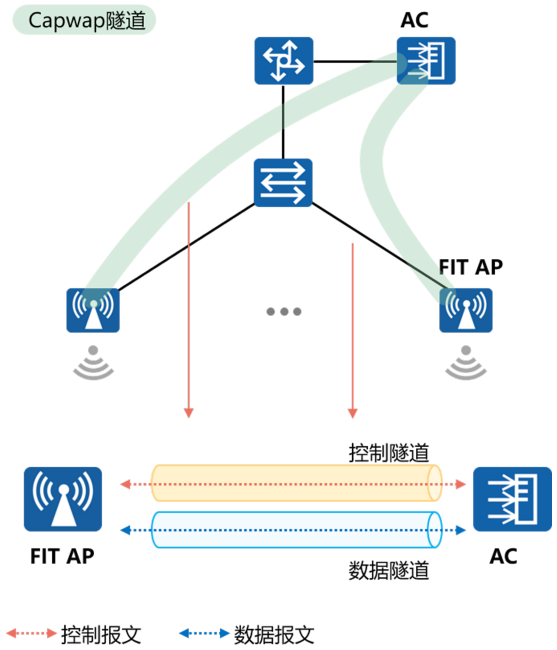
7、CAPWAP隧道的功能

7.1、CAPWAP隧道有两种：控制隧道和数据隧道

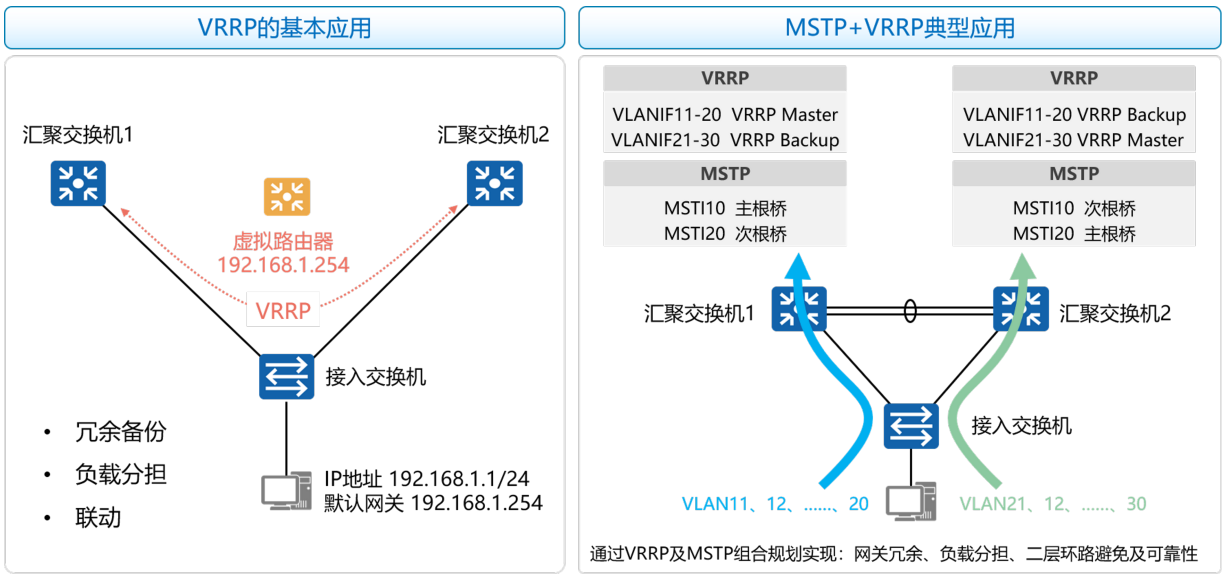
7.1.1、控制隧道主要传输控制报文（也称管理报文，是AC管理控制AP的报文）

7.2.1、数据隧道主要传输数据报文

7.2、CAPWAP隧道可以进行数据传输层安全加密，因此传输的报文更加安全。当采用隧道转发模式时，AP将STA发出的数据通过CAPWAP隧道实现与AC之间的交互



十三、VRRP【虚拟路由冗余协议】



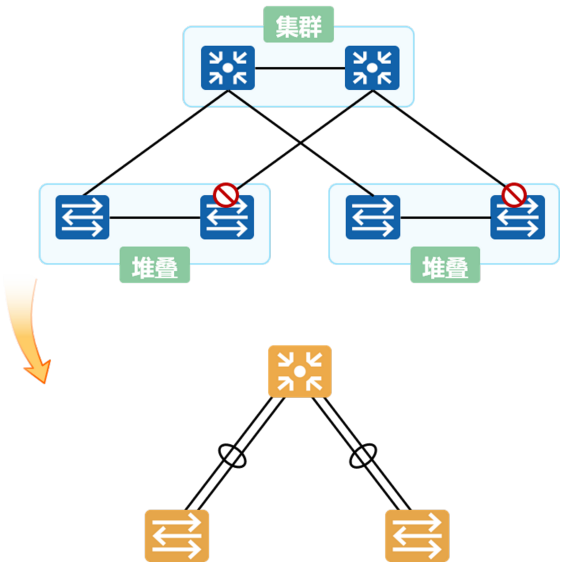
1、通过VRRP可以实现对于用户而言的网络无缝切换

2、VRRP可以令多台主设备共同虚拟出一台虚拟设备，为该虚拟设备分配一个IP地址与MAC地址

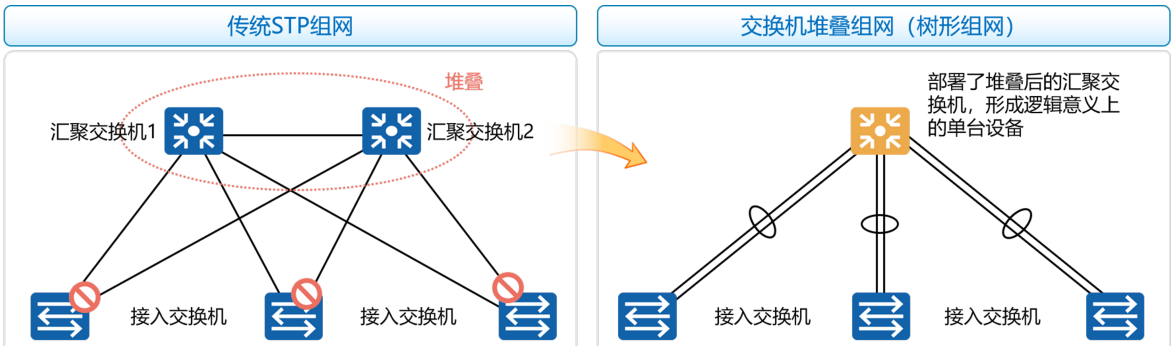
3、将虚拟设备的IP地址当作用户的网关地址

4、在主设备（master）正常工作时，用户数据由master设备负责转发；当master设备失效时，用户数据由backup设备负责转发，而对于用户完全透明
5、由于华为的设备在VRRP下默认开启占先权，因此在主设备恢复后，会立即从backup设备抢回转发权
6、VRRP也可以与MSTP共同作用，令不同的设备成为不同生成树实例的主设备，且在不同的实例之间配置互为备份

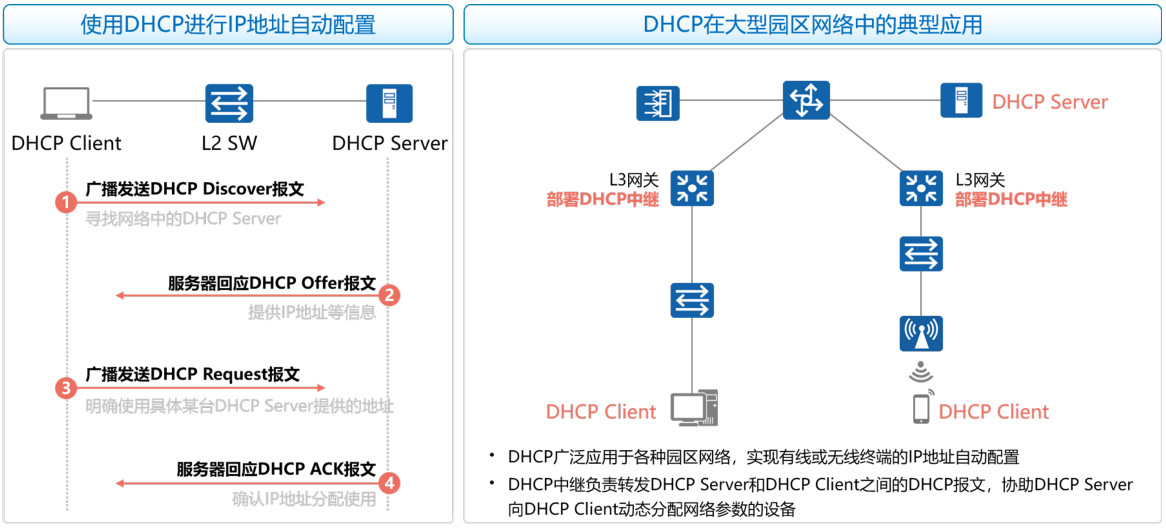
十四、集群/堆叠
1、iStack（Intelligent Stack，智能堆叠），简称堆叠，是指将多台支持堆叠特性的交换机设备组合在一起，从逻辑上组合成一台交换设备。iStack针对华为盒式交换机
2、CSS（Cluster Switch System，集群交换机系统），又称为集群，是指将两台支持集群特性的交换机设备组合在一起，从逻辑上组合成一台交换设备。CSS针对华为框式交换机



3、堆叠与园区网络树形结构组网形态



十五、DHCP【动态主机配置协议】
1、DHCP用来动态的分客户端分配IP地址
2、DHCP究竟使用广播还是单播，关注客户端发送的第一个DHCP Discover包；若客户端发送的该报文使用的是广播的方式，则后续的Offer、Request、ACK均为广播；若客户端发送的DHCP Discover包为单播发送，则后续报文也使用单播的方式
3、若在DHCP Server与DHCP Client之间经过了3层设备，则3层设备必须要开启DHCP中继代理的功能，用来帮助传递DHCP报文



十六、NTP

NTP主要应用于网络中所有设备时钟需要保持一致的场合，在以下场景下需要时钟同步：

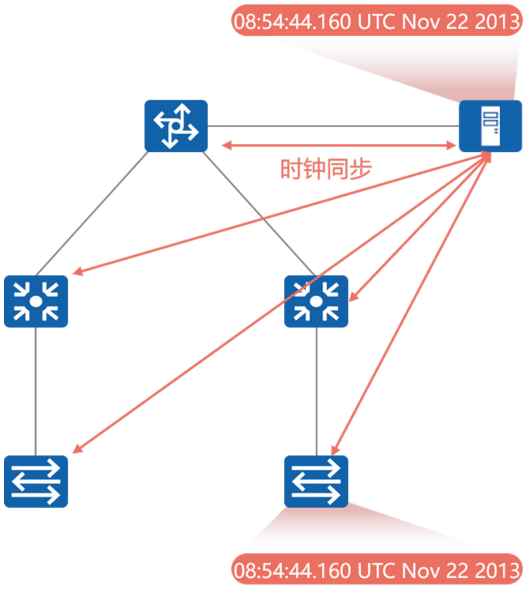
1、网络管理：对从不同路由器采集来的日志信息、调试信息进行分析时，需要以时间作为参照依据

2、计费系统：要求所有设备的时钟保持一致

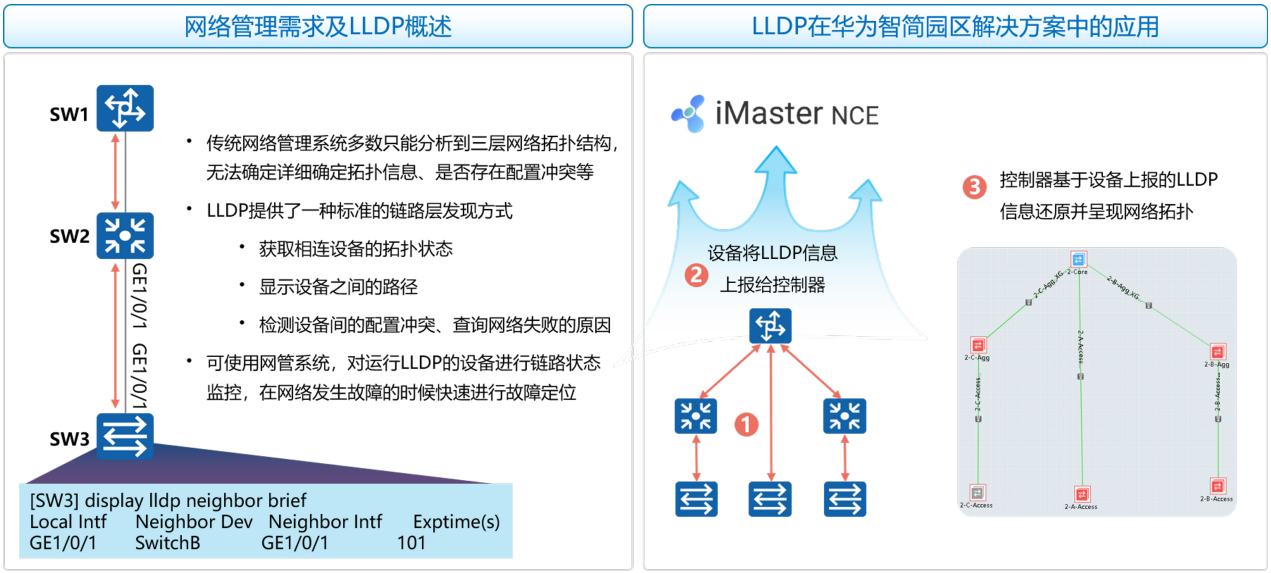
3、多个系统协同处理同一个复杂事件：为保证正确的执行顺序，多个系统必须参考同一时钟

4、备份服务器和客户机之间进行增量备份：要求备份服务器和所有客户机之间的时钟同步

5、系统时间：某些应用程序需要知道用户登录系统的时间以及文件修改的时间



十七、LLDP【链路层发现协议】

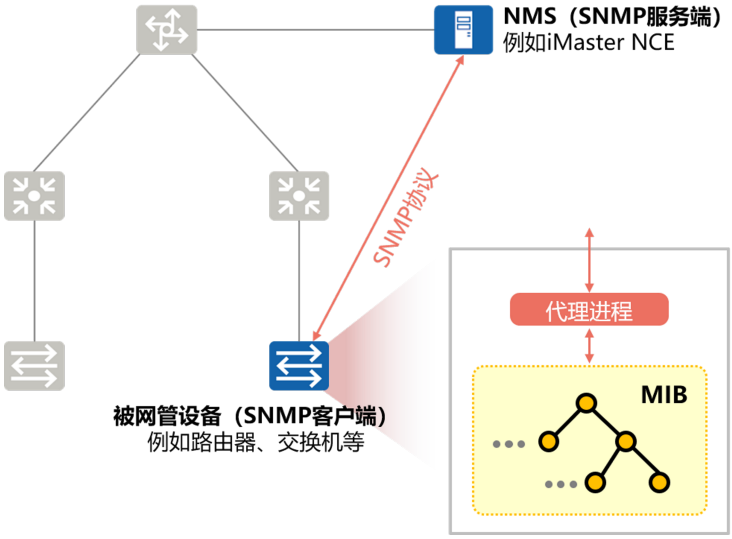


十八、SNMP【简单网络管理协议】

1、SNMP（Simple Network Management Protocol，简单网络管理协议）是广泛应用于TCP/IP网络的网络管理标准协议

2、SNMP提供了一种通过运行网络管理软件的中心计算机（即网络管理工作站NMS）来管理设备的方法

3、通过“利用网络管理网络”的方式，SNMP实现了对网络设备的高效和批量的管理；同时，SNMP协议也屏蔽了不同产品之间的差异，实现了不同种类和厂商的网络设备之间的统一管理



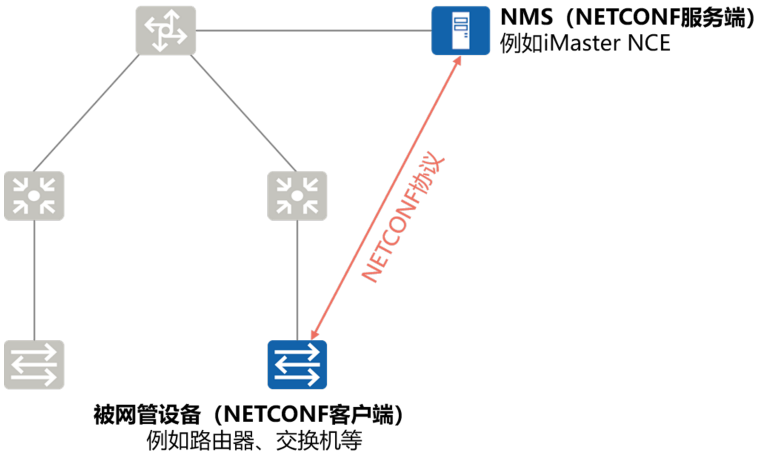
十九、NETCONF/YANG

1、SNMP的短板：SNMP并不是面向配置的协议，随着网络规模的增大、复杂性的增加，SNMP已经不能适应当前复杂网络的管理，特别是不能满足配置管理的需求

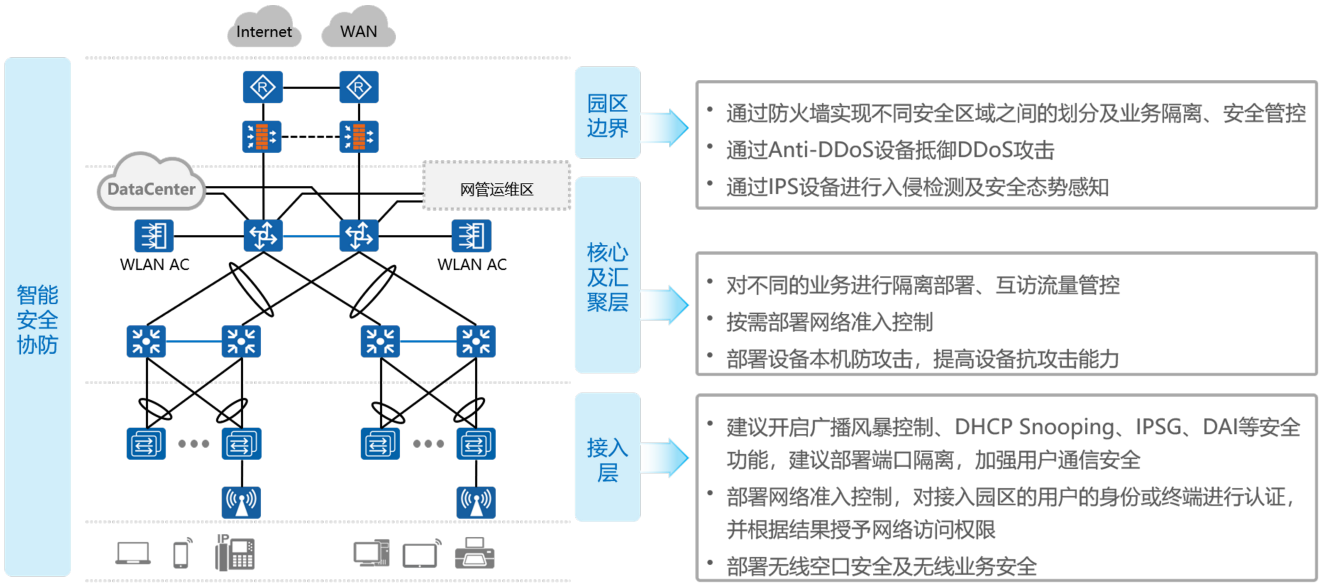
2、NETCONF（Network Configuration Protocol，网络配置协议）提供了一种网管和网络设备之间通信的机制

2.1、网络管理员可以利用这套机制在网管上增加、修改、删除网络设备的配置，获取网络设备的配置和状态信息

2.2、NETCONF基于XML（Extensible Markup Language，可扩展标记语言）



二十、园区网络安全概述

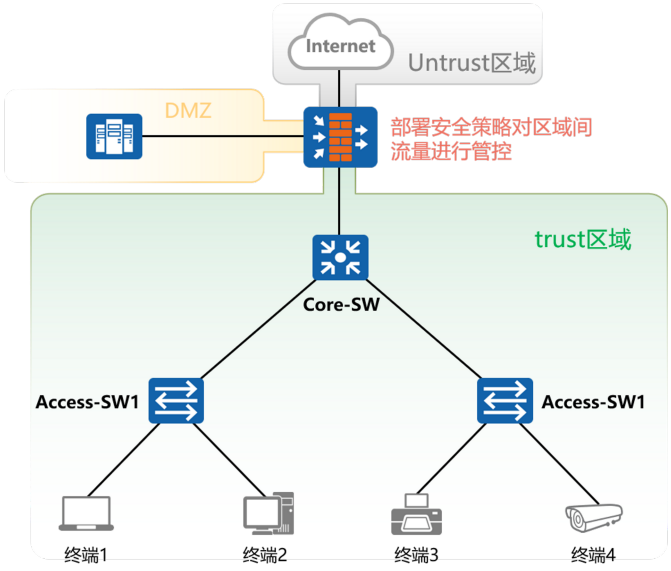


二十一、基于防火墙的安全区域划分及安全策略

1、安全区域（Security Zone），或者简称为区域（Zone），是一个安全的概念，大部分的安全策略都基于安全区域实施

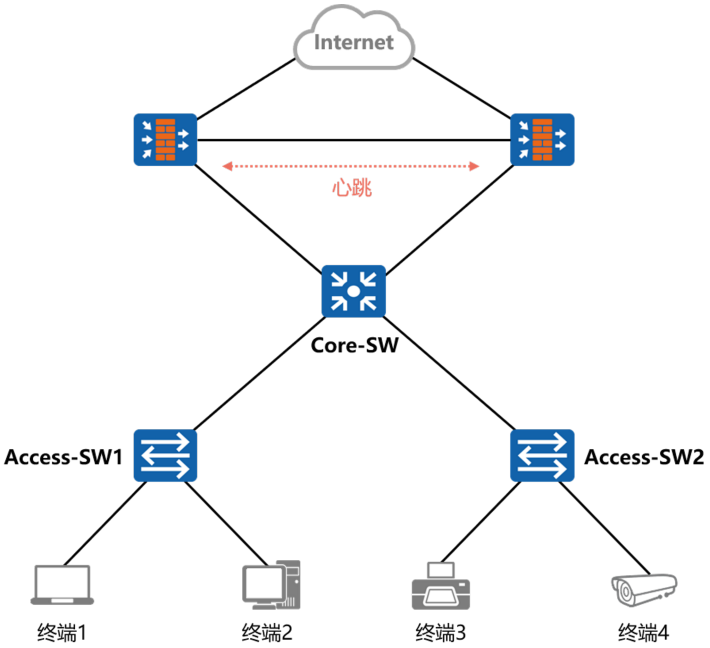
2、一个安全区域是防火墙若干接口所连网络的集合，这些网络中的用户具有相同的安全属性

3、将企业员工网络、公司服务器网络、外部网络划分到不同安全区域，对安全区域间的流量进行检测和保护

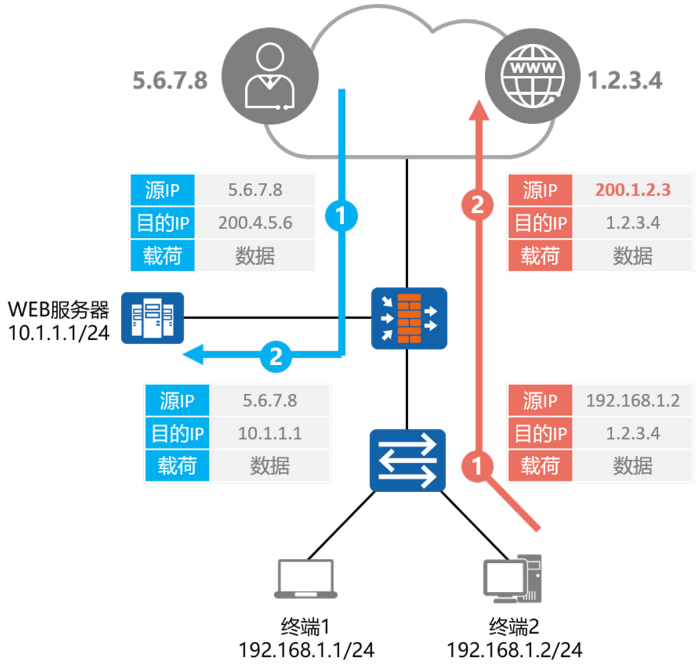


二十二、防火墙双机热备概述

1、防火墙部署在网络出口位置时，如果发生故障会影响到整网业务。需提升网络的可靠性
2、部署多台防火墙可提升可靠性，需保证设备切换过程中的业务连续性
3、部署两台FW并组成双机热备，双机热备需要两台硬件和软件配置均相同的FW
4、两台FW之间通过一条独立的链路连接，这条链路通常被称之为"心跳线"。两台FW通过心跳线了解对端的健康状况，向对端备份配置和表项（如会话表、IPSec SA等）
5、当一台FW出现故障时，业务流量能平滑地切换到另一台设备上处理，使业务不中断



二十三、源NAT
1、内网用户（采用私网IP地址）需访问Internet，需对其源IP地址进行转换，转换为公网IP地址
2、外网用户需访问采用私网IP地址的服务器（例如Web服务器）
3、NAT是将IP数据报文头中的IP地址转换为另一个IP地址的过程
4、常用NAT：
4.1、源IP地址转换（Source IP address-based NAT）：
4.1.1、No-Port 地址转换（No-PAT）
4.1.2、网络地址及端口转换（NAPT）
4.2、目的IP地址转换（Destination IP address-based NAT）：
NAT Server

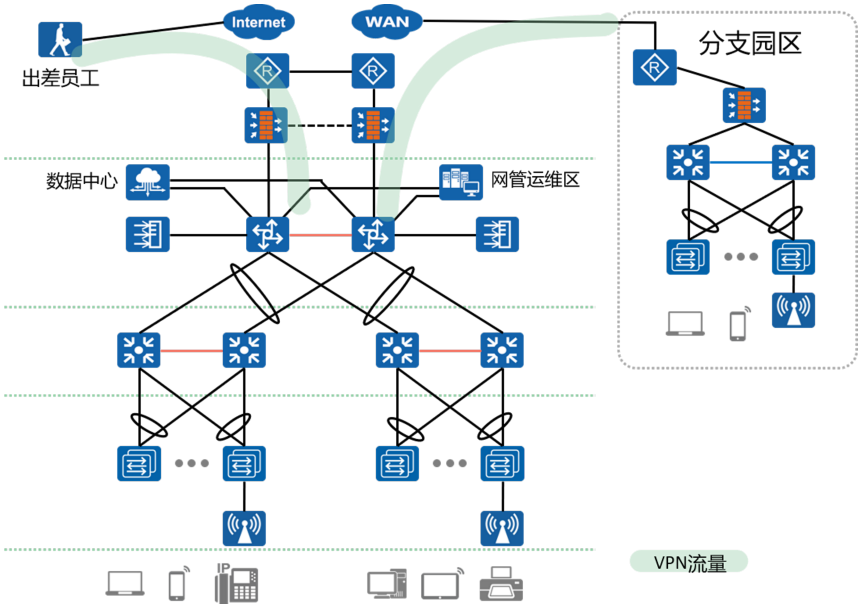


二十四、VPN

1、对于规模较大的企业来说，网络访问需求不仅仅局限于公司总部网络内，分公司、出差员工、合作单位等也需要访问公司总部的网络资源，一般采用VPN（Virtual Private Network，虚拟专用网络）技术来实现这一需求

2、VPN可以在不改变现有网络结构的情况下，建立虚拟专用连接。因其具有廉价、专用和虚拟等多种优势，在现网中应用非常广泛

3、VPN是一类技术的统称，不同的VPN技术拥有不同的特性和实现方式，常见的VPN技术包括IPSec VPN、GRE VPN、L2TP VPN、MPLS VPN等

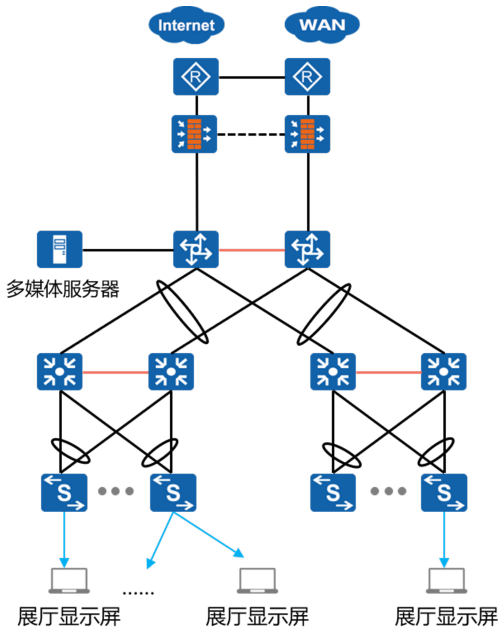


二十五、组播应用场景

1、企业存在一些公告信息，例如天气、值班表、机房注意事项、宣传视频等，为方便公司员工和来访人员及时获取这些信息，通常采用在公司人员密集处布置显示屏的方式

2、每一块显示屏显示的内容一致，这是典型的点到多点通信的场景。如果采用单播的方式传递信息，网络中的设备性能及链路带宽都会面临一定程度的浪费

3、组播技术有效地满足了单点发送、多点接收的需求，实现了IP网络中点到多点业务数据的高效传送，能够大量节约网络带宽、降低网络负载



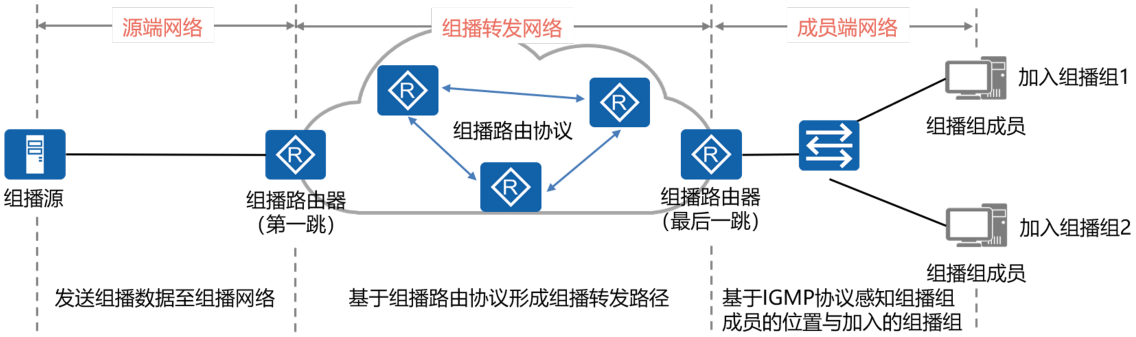
4、组播网络基本架构

组播网络大体可以分为三个部分：

4.1、源端网络：将组播源产生的组播数据发送至组播网络

4.2、组播转发网络：形成无环的组播转发路径，该转发路径也被称为组播分发树（Multicast Distribution Tree）

4.3、成员端网络：让组播网络感知组播组成员位置与加入的组播组

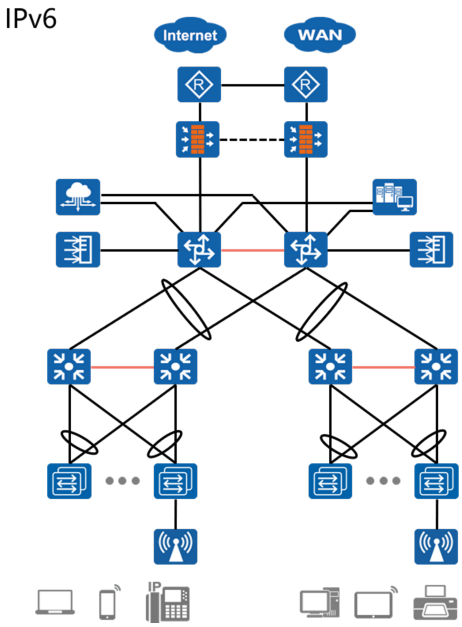


二十六、IPv6概述

1、IPv4协议是目前广泛部署的因特网协议。在因特网发展初期，IPv4以其协议简单、易于实现、互操作性好的优势而得到快速发展。但随着因特网的迅猛发展， IPv4地址空间不足的问题日趋明显，IPv6取代IPv4势在必行

2、IPv6（Internet Protocol Version 6）是网络层协议的第二代标准协议，也被称为IPng（IP Next Generation）。它是Internet工程任务组IETF（Internet Engineering Task Force）设计的一套规范，是IPv4（Internet Protocol Version 4）的升级版本

3、IPv6地址长度为128bit，海量的地址空间，满足物联网等新兴业务、有利于业务演进及扩展

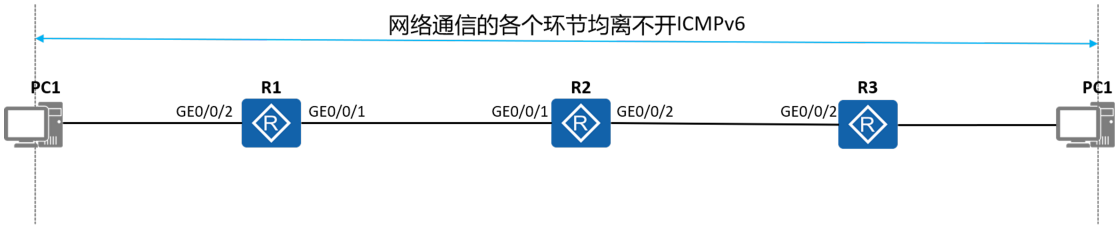


4、ICMPv6

4.1、ICMPv6 （Internet Control Message Protocol for IPv6）是IPv6的基础协议之一

4.2、ICMPv6报文被广泛应用于其它协议中，包括NDP、PathMTU发现机制等

4.3、ICMPv6控制着IPv6中的地址自动配置、地址解析、地址冲突检测、路由选择、以及差错控制等关键环节

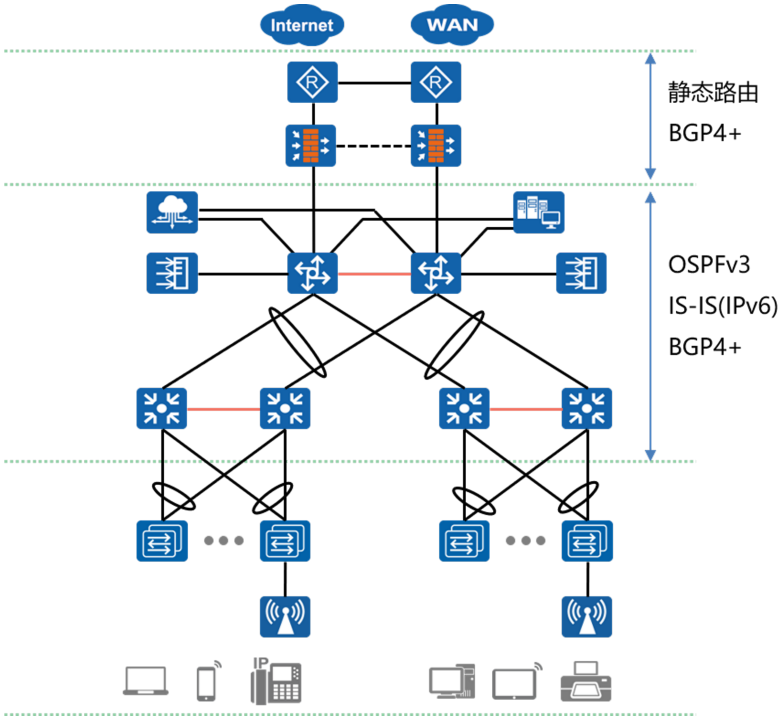


5、IPv6路由

IPv6网络支持静态路由和动态路由协议：

5.1、静态路由：IPv6静态路由的配置方式和IPv4静态路由的配置方式相同

5.2、动态路由协议：OSPFv3、RIPng、IS-IS、BGPv4+


Internet
WAN
静态路由
BGP4+
OSPFv3
IS-IS(IPv6)
BGP4+
IP