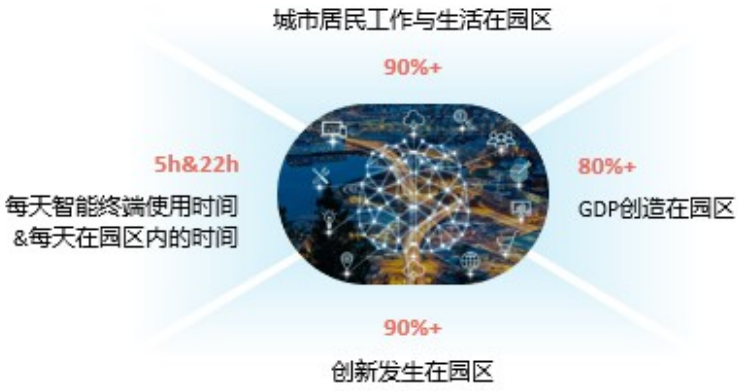
园区网典型技术应用概述

- 工厂、政府机关、商场、写字楼、校园、公园等，这些场所内为了实现数据互通而搭建的网络都可以称之为园区网。园区有大有小，有行业属性的不同，相应地，园区网络也变化多样。但是，无论如何变化，园区网络一般划分为出口层、核心层、汇聚层及接入层。
- 本课程主要介绍园区网络的总体架构、网络各层次中所使用的常用技术及协议、典型的组网场景。

“城市，除了马路，都是园区”



什么是园区网络?

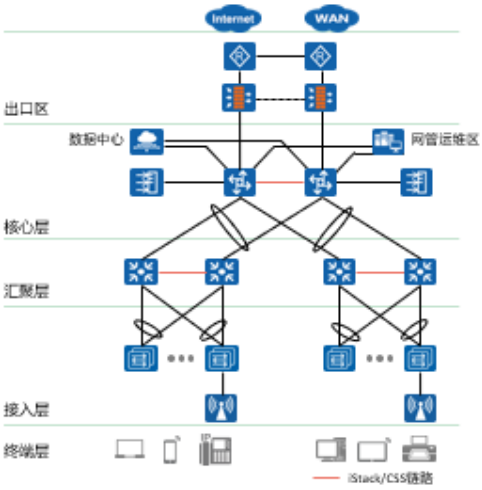
- 园区网络一般是指企业或者机构的内部网络。
- 园区网络的主要目的是使企业或者机构的各项业务运作更有效率。
- 按规模可以将园区网络划分成：
  - 大型园区网络：终端用户数量/个 > 2000；网元数量/个 > 100。
  - 中型园区网络：2000 > 终端用户数量/个 > 200；100 >网元数量/个 > 25。
  - 小型园区网络：终端用户数量/个 < 200；网元数量/个 < 25。
- 有些企业还存在不同地域的办公分支机构，每个分支机构网络可看做一个单园区网络。

常见的行业园区网

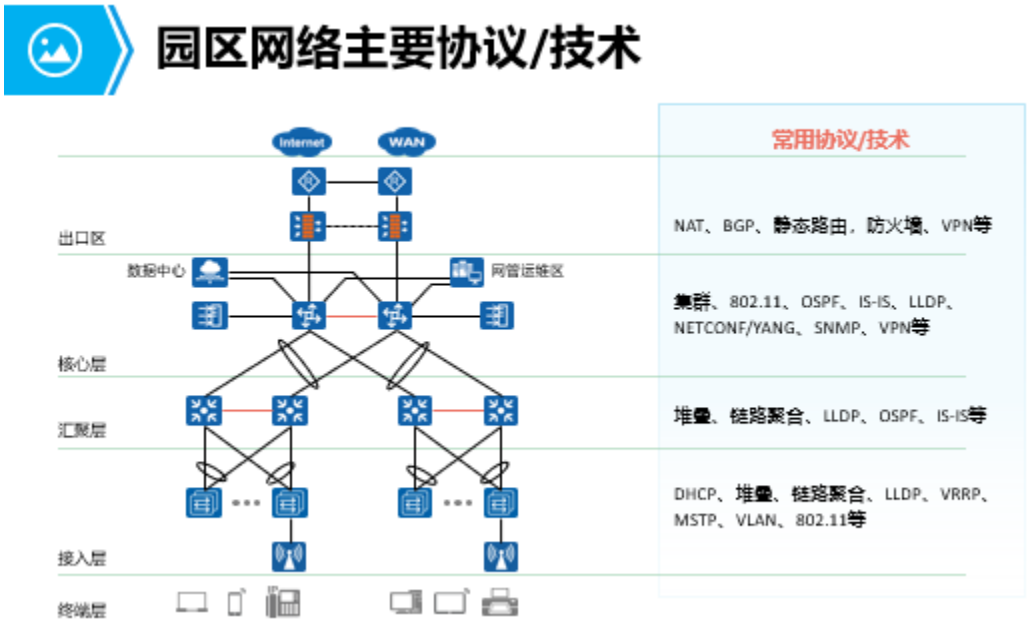
- 企业园区网络
  - 关注网络可靠性、先进性，持续提升员工的办公体验，保障运营生产的效率和质量。
- 校园网络
  - 分为普教园区和高教园区。
  - 高教园区相对复杂，通常存在教研网、学生网，还可能有运营性的宿舍网络。
  - 网络可管理性、安全性要求高；对网络先进性亦有要求。
- 政务园区网络
  - 通常指政府机构的内部网络。
  - 安全要求极高，通常采用内网和外网隔离的措施保障涉密信息的绝对安全。
- 商业园区网络
  - 商场、超市、酒店、公园等。
  - 网络主要用于服务消费者，此外还包含服务内部办公的子网。
  - 提供上网服务，并构建商业智能化系统提升用户体验，降低运维成本，提升商业效率，实现价值转移。

- 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。

园区网络典型架构

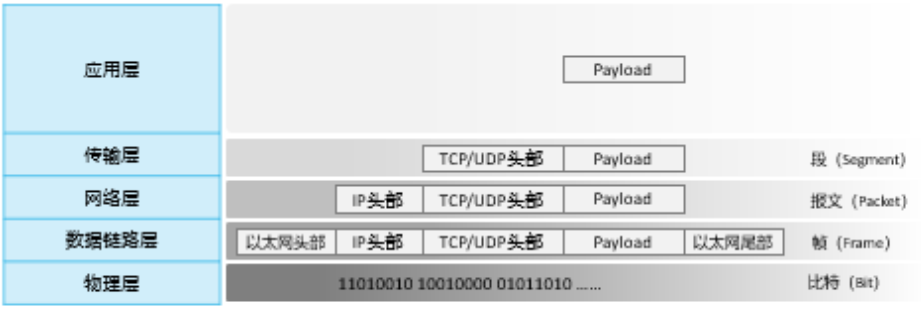


- **核心层**：是园区网骨干，是园区数据交换的核心，联接园区网的各个组成部分，如数据中心、管理中心、园区出口等。
- **汇聚层**：处于园区网的中间层次，完成数据汇聚或交换的功能，可以提供一些关键的网络基本功能，如路由、安全等。
- **接入层**：为终端用户提供园区网接入功能，是园区网的边界。
- **出口区**：园区内部网络到外部网络的边界，用于实现内部用户接入到公网，外部用户（包括客户、合作伙伴、分支机构、远程用户等）接入到内部网络。
- **数据中心区**：部署服务器和应用系统的区域，为企业内部和外部用户提供数据和应用服务。



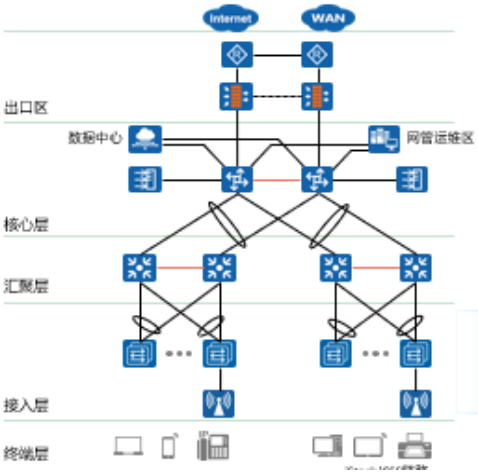
- NAT：Network Address Translation，网络地址转换。
- LLDP：Link Layer Discovery Protocol，链路层发现协议。链路层发现协议是 IEEE 802.1ab 中定义的第二层发现协议。通过采用 LLDP 技术，在网络规模迅速扩大时，网管系统可以快速掌握二层网络拓扑信息、拓扑变化信息。
- NETCONF：Network Configuration Protocol，网络配置协议。NETCONF 是一种提供网络设备配置管理的协议，采用基于数据编码的可扩展标记语言配置数据以及协议信息，提供了安装、操作和删除网元配置的机制。
- YANG：Yet Another Next Generation，通过 NETCONF 网络配置协议发送的数据的数据建模语言，可以用来建模网元的配置数据和状态数据。
- SNMP：Simple Network Management Protocol，简单网络管理协议。
- VRRP：Virtual Router Redundancy Protocol，虚拟路由冗余协议。
- MSTP：Multiple Spanning Tree Protocol，多生成树协议。

从TCP/IP对等模型说起



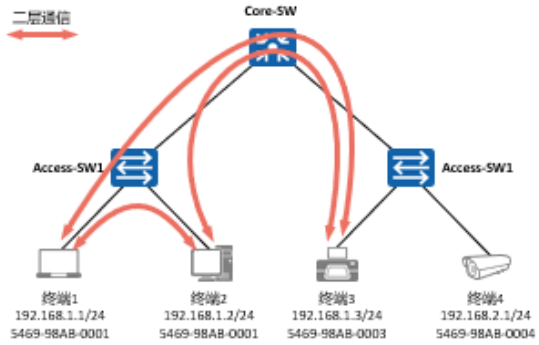
- 将网络的通信过程划分为小一些、简单一些的部件，有助于各个部件的开发、设计和故障排除。
- 通过网络组件的标准化，允许多个供应商进行开发。
- 通过定义在模型的每一层实现什么功能，鼓励产业的标准化。
- 允许各种类型的网络硬件和软件相互通信。

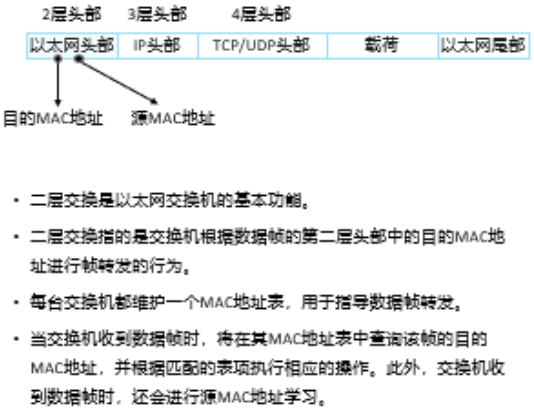
从园区网络到以太网二层交换



- 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。
- 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。
- 如果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。

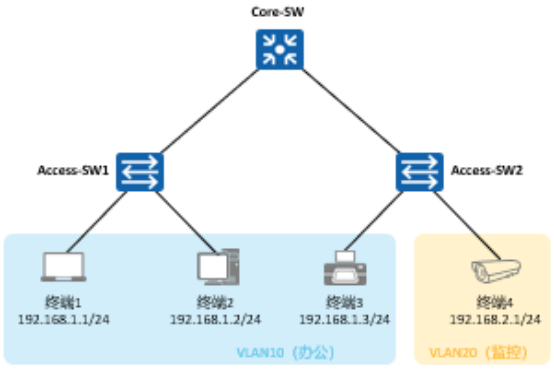
什么是二层交换





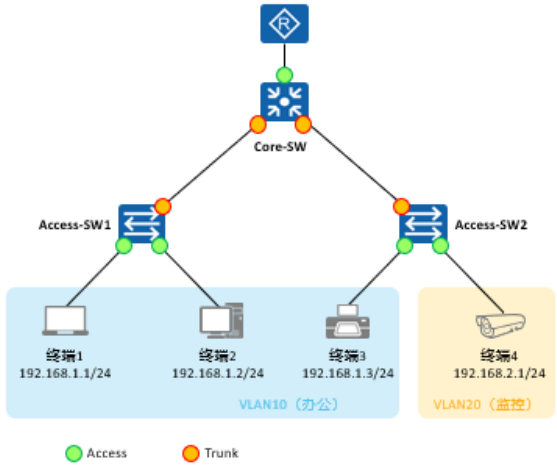
- 二层交换设备工作在 OSI 模型的第二层，即数据链路层，它对数据包的转发是建立在 MAC（Media Access Control ）地址基础之上的。
- 二层交换设备通过解析和学习以太网帧的源 MAC 来维护 MAC 地址与接口的对应关系（保存 MAC 与接口对应关系的表称为 MAC 表），通过其目的 MAC 来查找 MAC 表决定向哪个接口转发。
- 二层交换设备不同的接口发送和接收数据独立，各接口属于不同的冲突域，因此有效地隔离了网络中物理层冲突域，使得通过它互连的主机（或网络）之间不必再担心流量大小对于数据发送冲突的影响。

VLAN



- 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。
- 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。
- VLAN内的设备间可以直接通信，而VLAN间不能直接互通。
- VLAN之间互相隔离，不同VLAN间需通过三层设备实现相互通信。
- 一个VLAN一般为一个逻辑子网。
- 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。

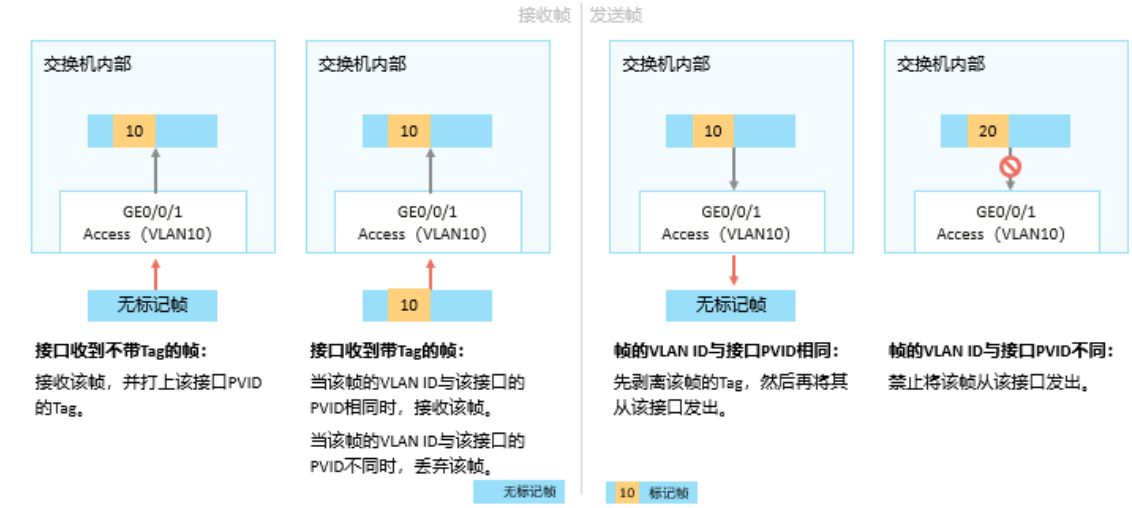
以太网二层接口类型概述



交换机的以太网二层接口主要存在以下三种类型：

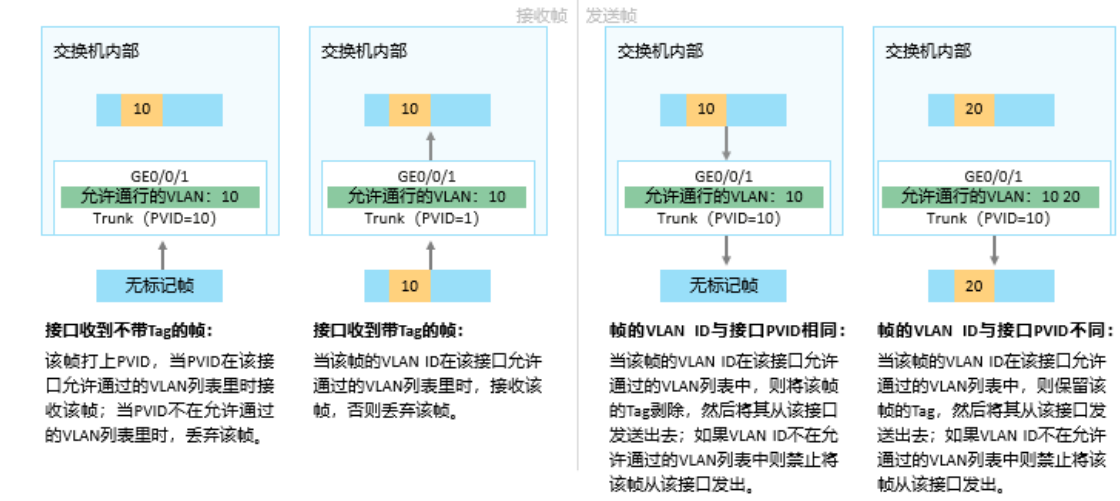
- **Access**：常用来连接用户PC、服务器等终端设备的接口。Access接口所连接的这些设备的网卡往往只收发无标记帧。Access接口只能加入一个VLAN。
- **Trunk**：Trunk接口允许多个VLAN的数据帧通过，这些数据帧通过802.1Q Tag实现区分。Trunk接口常用于交换机之间的互联，也用于连接路由器、防火墙等设备的子接口。
- **Hybrid**：Hybrid接口与Trunk接口类似，也允许多个VLAN的数据帧通过，这些数据帧通过802.1Tag实现区分。用户可以灵活指定Hybrid接口在发送某个（或某些）VLAN的数据帧时是否携带Tag。

Access接口

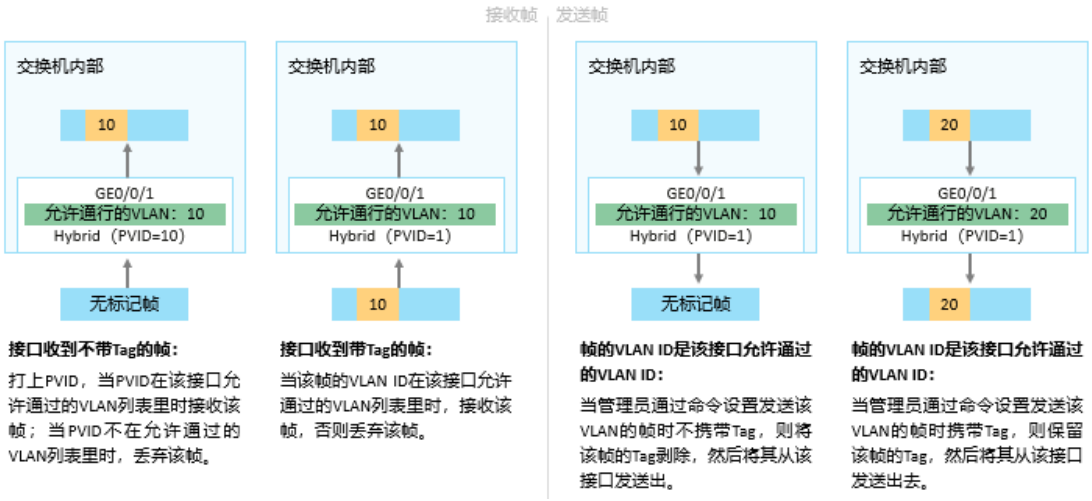


- 所有的二层接口无论其类型如何，都有一个缺省 VLAN ID，这个缺省 VLAN ID 被称为 PVID（Port Default VLAN ID），在华为的交换机上，PVID 缺省为 1。另外，出于提高数据帧处理效率的考虑，在交换机内部，数据帧一律携带 Tag。

Trunk接口



Hybrid接口

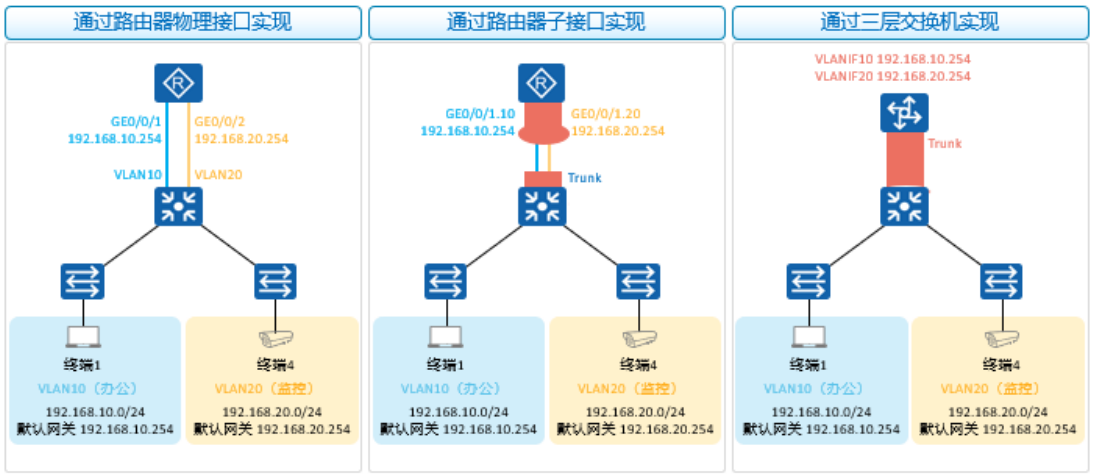


- Hybrid 接口也能承载多个 VLAN 的数据，它与 Trunk 接口在数据帧的接收行为上大体相同，这里不再赘述。Trunk 接口在发送数据帧时，仅当待发送的数据帧与发送接口的 PVID 相同时，数据帧的 Tag 才会被移除，除此之外，该接口发送出去的其他 VLAN 的数据帧都是携带 Tag 的。而 Hybrid 接口发送数据帧的行为则与 Trunk 接口不同。我们可以通过命令指定 Hybrid 接口在发送某个，或者某些 VLAN 的数据帧时不携带 Tag。

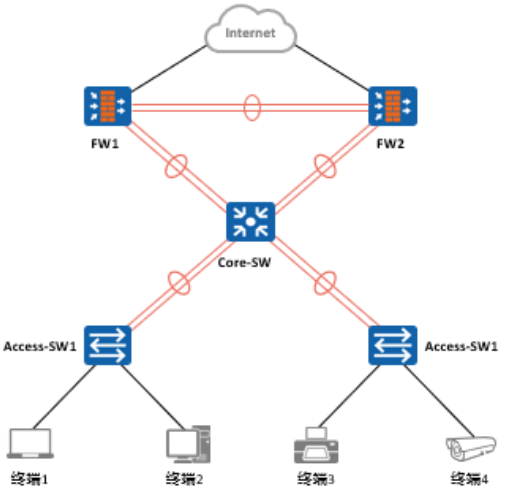
VLAN划分方式总览

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

实现VLAN之间的IP可达性

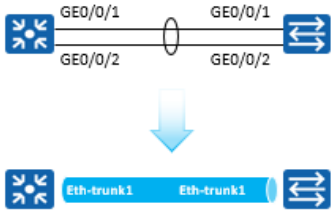


以太网链路聚合



- 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。
- 完成聚合后的链路称为以太网聚合链路。

增加带宽　提高可靠性　负载分担

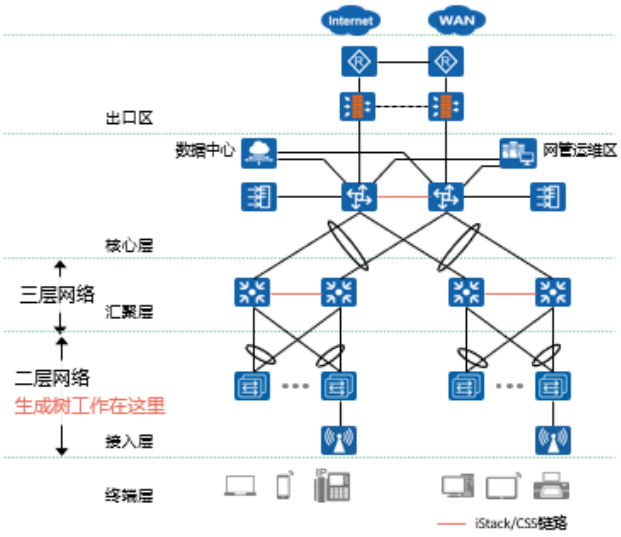


- 随着网络规模不断扩大，用户对骨干链路的带宽和可靠性提出越来越高的要求。在传统技术中，常用更换高速率的接口板或更换支持高速率接口板的设备的方式来增加带宽，但这种方案需要付出高额的费用，而且不够灵活。
- 采用链路聚合技术可以在不进行硬件升级的条件下，通过将多个物理接口捆绑为一个逻辑接口，达到增加链路带宽的目的。在实现增大带宽目的的同时，链路聚合采用备份链路的机制，可以有效的提高设备之间链路的可靠性。
- LAG 是指将若干条以太链路捆绑在一起所形成的逻辑链

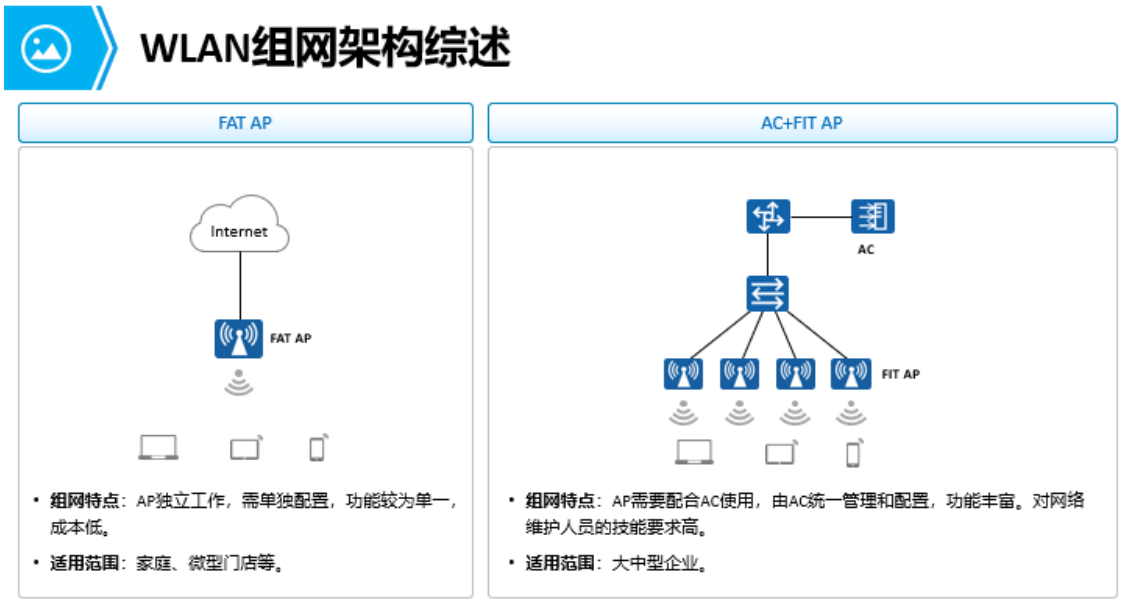
路，简写为 Eth-Trunk。每个聚合组唯一对应着一个逻辑接口，这个逻辑接口称之为聚合接口或 Eth-Trunk 接口。

- 链路聚合技术主要有以下三个优势：
- 增加带宽：链路聚合接口的最大带宽可以达到各成员接口带宽之和。
- 提高可靠性：当某条活动链路出现故障时，流量可以切换到其他可用的成员链路上。
- 负载分担：在一个链路聚合组内，可以实现在各成员活动链路上的负载分担。

生成树技术：防环+保证二层网络可靠性



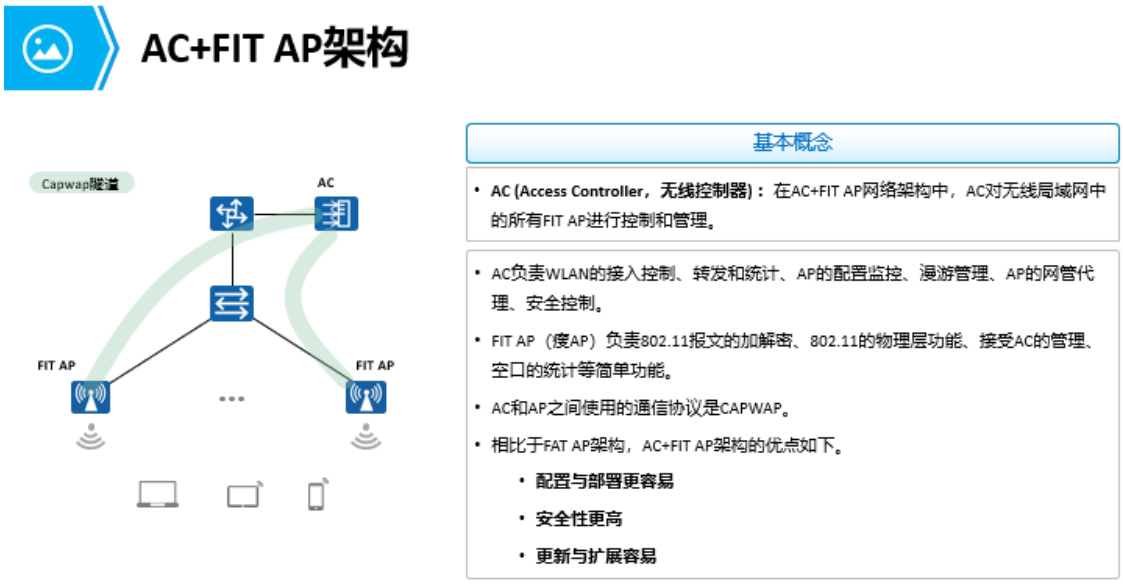
- 解决交换网络中的环路问题
- 动态地适应根据网络拓扑变更
- 配合冗余链路，保证二层网络可靠性



- 无线接入点 (AP, Access Point)
- 一般支持 FAT AP（胖 AP）、FIT AP（瘦 AP）和云管理 AP 三种工作模式，根据网络规划的需求，可以灵活地在多种模式下切换。
- FAT AP：适用于家庭，独立工作，需单独配置，功能较为单一，成本低。独立完成用户接入、认证、数据安全、业务转发和 QoS 等功能。
- FIT AP：适用于大中型企业，需要配合 AC 使用，由 AC

统一管理和配置，功能丰富，对网络维护人员的技能要求高。用户接入、AP 上线、认证、路由、AP 管理、安全协议、QoS 等功能需要同 AC 配合完成。

- 云管理：适用于中小型企业，需要配合云管理平台使用，由云管理平台统一管理和配置，功能丰富，即插即用，对网络维护人员的技能要求低。
- 无线接入控制器 (AC, Access Controller)
- 一般位于整个网络的汇聚层，提供高速、安全、可靠的 WLAN 业务。
- 提供大容量、高性能、高可靠性、易安装、易维护的无线数据控制业务，具有组网灵活、绿色节能等优势。

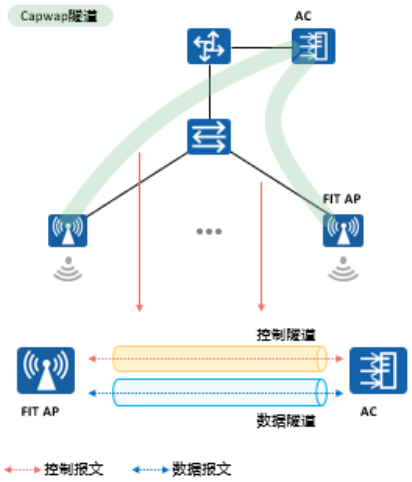


- AC 和 AP 之间使用的通信协议是无线接入点控制和配置（Control And Provisioning of Wireless Access Points，CAPWAP）。CAPWAP 协议定义的主要内容有：AP 自动发现 AC，AC 对 AP 进行安全认证，AP 从 AC 获取软件，AP 从 AC 获得初始和动态配置等。通过该协议，AP 和 AC 之间建立起 CAPWAP 隧道。CAPWAP 隧道有两种：控制隧道和数据隧道。

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）；数据隧道主要传输数据报文。CAPWAP 隧道可以进行数据传输层安全（Datagram Transport Layer Security，DTLS）加密，因此传输的报文更加安全。

- 相比于 FAT AP 架构，AC+FIT AP 架构的优点如下。
- 配置与部署：通过 AC 进行集中地网络配置和管理，不再需要对每个 AP 进行单独配置操作，同时对整网 AP 进行信道、功率的自动调整，免去了烦琐的人工调整过程。
- 安全性：由于 FAT AP 无法进行统一的升级操作，无法保证所有 AP 版本都有最新的安全补丁，而 AC+FIT AP 架构主要的安全能力是在 AC 上的，软件更新和安全配置仅需在 AC 上进行，从而可以快速进行全局安全设置；同时，为了防止加载恶意代码，设备会对软件进行数字签名认证，增强了更新过程的安全性。AC 也实现了 FAT AP 架构无法支持的一些安全功能，包括病毒检测、统一资源定位地址（Uniform Resource Locater，URL）过滤、状态检测防火墙等高级安全特性。
- 更新与扩展：架构的集中管理模式使得同一 AC 下的 AP 有着相同的软件版本。当需要更新时，先由 AC 获取更新包或补丁，然后由 AC 统一更新 AP 版本。AP 和 AC 的功能拆分也减少了对 AP 版本的频繁更新，有关用户认证、网管和安全等功能的更新只需在 AC 上进行。

AC+FIT AP架构



什么是CAPWAP

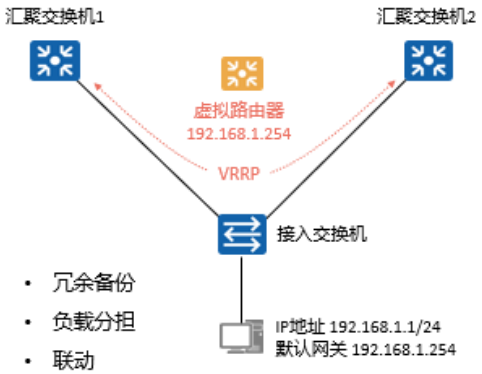
- **CAPWAP（Control And Provisioning of Wireless Access Points Protocol Specification，无线接入点控制和配置协议）**定义了如何对AP进行管理、业务配置，即AC通过CAPWAP隧道来实现对AP的集中管理和控制。
- CAPWAP协议定义的主要内容有：AP自动发现AC，AC对AP进行安全认证，AP从AC获取软件，AP从AC获得初始和动态配置等。通过该协议，AP和AC之间建立起CAPWAP隧道。

CAPWAP隧道的功能

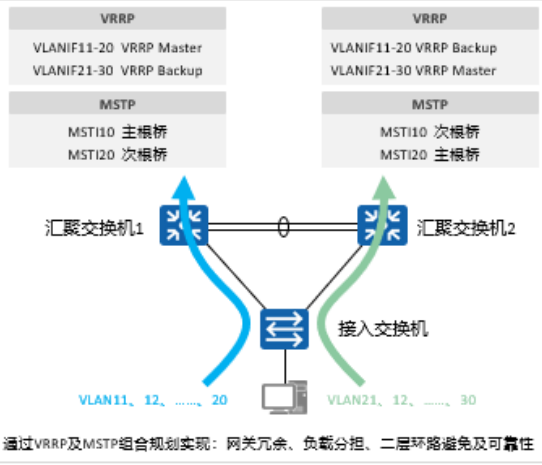
- CAPWAP隧道有两种：控制隧道和数据隧道。
- 控制隧道主要传输控制报文（也称管理报文，是AC管理控制AP的报文）；数据隧道主要传输数据报文。CAPWAP隧道可以进行数据传输层安全加密，因此传输的报文更加安全。当采用隧道转发模式时，AP将STA发出的数据通过CAPWAP隧道实现与AC之间的交互。

使用VRRP实现网关冗余

VRRP的基本应用



MSTP+VRRP典型应用

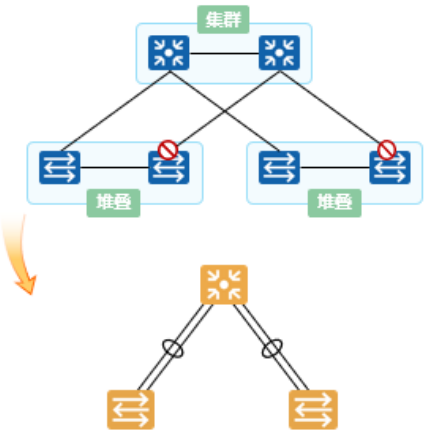


- 虚拟路由冗余协议 VRRP（Virtual Router Redundancy Protocol）通过把几台路由设备联合组成一台虚拟的路由设备，将虚拟路由设备的 IP 地址作为用户的默认网关实现与外部网络通信。当网关设备发生故障时，VRRP 机制能够选举新的网关设备承担数据流量，从而保障网络的可靠通信。
- 通常，同一网段内的所有主机上都设置一条相同的、以网关为下一跳的缺省路由。主机发往其他网段的报文将通过缺省路由发往网关，再由网关进行转发，从而实现主机与外部网

络的通信。当网关发生故障时，本网段内所有以网关为缺省路由的主机将无法与外部网络通信。增加出口网关是提高系统可靠性的常见方法，此时如何在多个出口之间进行选路就成为需要解决的问题。

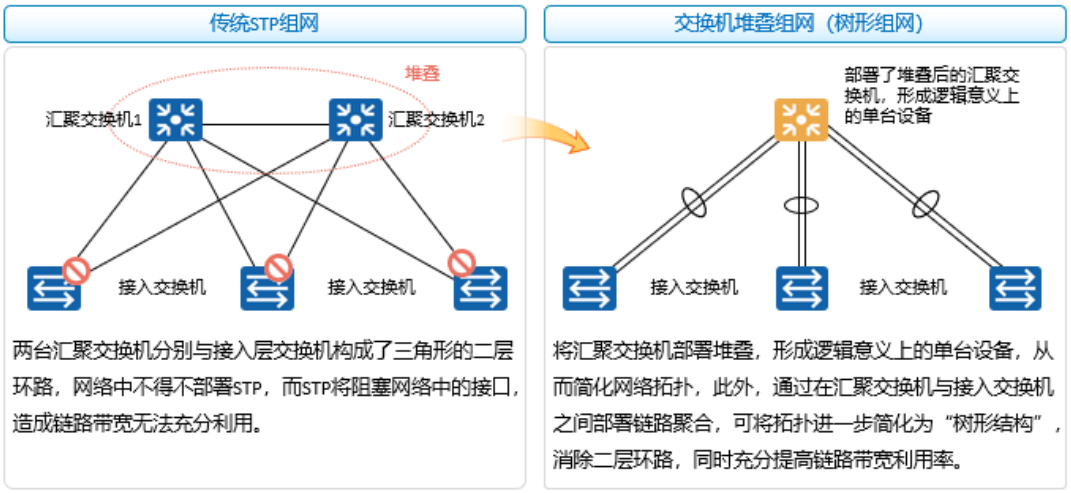
- VRRP 的出现很好的解决了这个问题。VRRP 能够在不改变组网的情况下，将多台路由设备组成一个虚拟路由器，通过配置虚拟路由器的 IP 地址为默认网关，实现默认网关的备份。
- **冗余备份**：VRRP 可以将多台路由设备配置为缺省网关路由器，当出现单点故障的时候通过备份链路进行业务传输，从而降低网络故障的可能性，保证用户的各种业务不中断传输。
- **负载分担**：VRRP 可以实现多台设备同时承担业务流量，从而减轻主用设备上数据流量的承载压力，在路由设备之间更均衡地分担流量。
- **联动功能**：VRRP 联动可以监视上行链路的故障。当上行接口或链路故障时，VRRP 备份组的 Master 设备降低优先级，重新进行选举，确保 Master 路由器为最佳的 VRRP 路由设备，保证流量的正常转发。VRRP 与 BFD 联动可以提高 VRRP 备份组中主备设备的切换速度。利用 BFD 检测速度快的特点，在 Master 设备和 Backup 设备之间建立 BFD 会话并与 VRRP 备份组进行绑定，实现 Master 设备和 Backup 设备之间的链路出现故障时，Backup 设备迅速切换为 Master，承担网络流量。

集群/堆叠简介



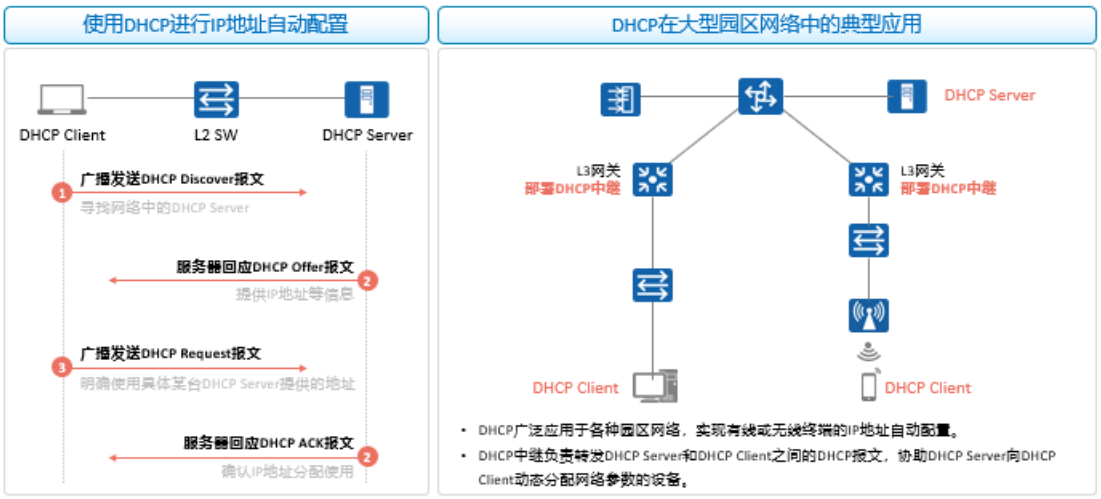
- iStack（Intelligent Stack，智能堆叠），简称堆叠，是指将多台支持堆叠特性的交换机设备组合在一起，从逻辑上组合成一台交换设备。iStack针对华为盒式交换机。
- CSS（Cluster Switch System，集群交换机系统），又称为集群，是指将两台支持集群特性的交换机设备组合在一起，从逻辑上组合成一台交换设备。CSS针对华为框式交换机。

堆叠与园区网络树形结构组网形态



- 堆叠 iStack（Intelligent Stack），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整体交换设备。
- 堆叠系统建立之前，每台交换机都是单独的实体，有自己独立的 IP 地址和 MAC 地址，对外体现为多台交换机，用户需要独立的管理所有的交换机；堆叠建立后堆叠成员对外体现为一个统一的逻辑实体，用户使用一个 IP 地址对堆叠中的所有交换机进行管理和维护，如图所示。通过交换机堆叠，可以实现网络大数据量转发和网络高可靠性，同时简化网络管理。

DHCP

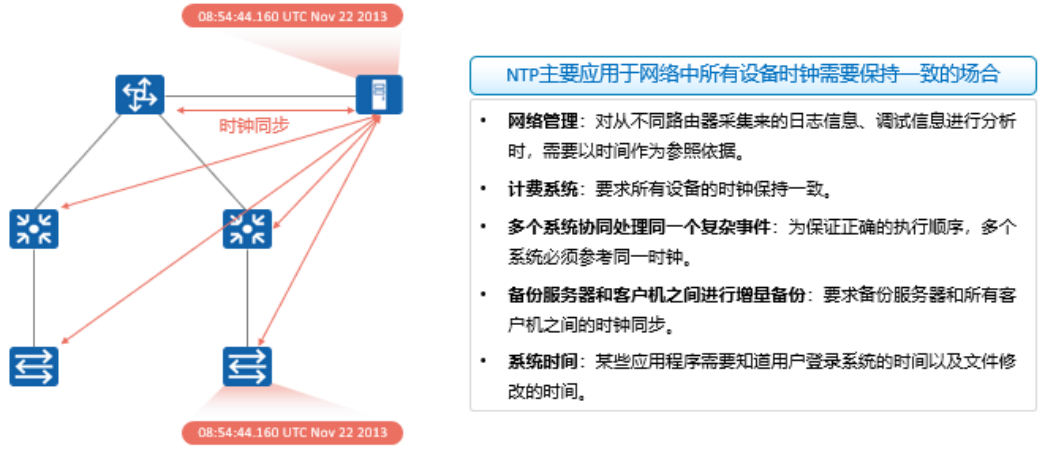


- 动态主机配置协议 DHCP（Dynamic Host Configuration Protocol）是一种用于集中对用户 IP 地址进行动态管理和配置的技术。即使规模较小的网络，通过 DHCP 也可以使后续增加网络设备变得简单快捷。
- DHCP 允许计算机动态地获取 IP 地址，而不是静态为每台主机指定地址。
- DHCP 能够分配其他配置参数，例如客户端的启动配置文件，使客户端仅用一个消息就获取它所需要的所有配置信息。
- DHCP 协议由 RFC 2131 定义，采用客户端/服务器通信模式，由客户端（DHCP Client）向服务器（DHCP Server）提出配置申请，服务器返回为客户端分配的配置信息。
- DHCP 可以提供两种地址分配机制，网络管理员可以根据网络需求为不同的主机选择不同的分配策略。
- 动态分配机制：通过 DHCP 为主机分配一个有使用期限（这个使用期限通常叫做租期）的 IP 地址。这种分配机制适用于主机需要临时接入网络或者空闲地址数小于网络主机总数且主机不需要永久连接网络的场景。
- 静态分配机制：网络管理员通过 DHCP 为指定的主机分

配固定的 IP 地址。相比手工静态配置 IP 地址，通过 DHCP 方式静态分配机制避免人工配置发生错误，方便管理员统一维护管理。

- DHCP 受益主要有以下两点：
- 降低客户端的配置和维护成本
- 集中管理

NTP



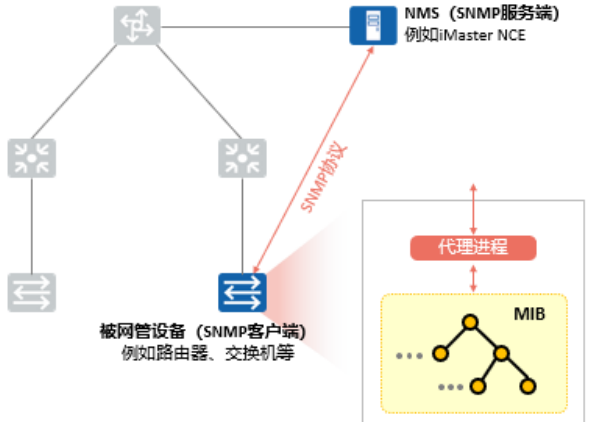
- 网络时间协议 NTP（Network Time Protocol）是 TCP/IP 协议族里面的一个应用层协议。NTP 用于在一系列分布式时间服务器与客户端之间同步时钟。NTP 的实现基于 IP 和 UDP。NTP 报文通过 UDP 传输，端口号是 123。
- 随着网络拓扑的日益复杂，整个网络内设备的时钟同步将变得十分重要。如果依靠管理员手工修改系统时钟，不仅工作量巨大，而且时钟的准确性也无法得到保证。NTP 的出现就是为了解决网络内设备系统时钟的同步问题。
- NTP 主要应用于网络中所有设备时钟需要保持一致的场合，比如：网络管理：对从不同路由器采集来的日志信息、调试信息进行分析时，需要以时间作为参照依据。
- 计费系统：要求所有设备的时钟保持一致。
- 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。

- 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。
- 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。
- 交换机既可以作为 NTP 的服务器，也可以作为 NTP 的客户端。

- LLDP（Link Layer Discovery Protocol）是 IEEE 802.1ab 中定义的链路层发现协议。LLDP 是一种标准的二层发现方式，可以将本端设备的管理地址、设备标识、接口标识等信息组织起来，并发布给自己的邻居设备，邻居设备收到这些信息后将其以标准的管理信息库 MIB（Management Information Base）的形式保存起来，以供网络管理系统查询及判断链路的通信状况。
- 随着网络规模越来越大，网络设备种类繁多，并且各自的配置错综复杂，对网络管理能力的要求也越来越高。传统网络管理系统多数只能分析到三层网络拓扑结构，无法确定网络设备的详细拓扑信息、是否存在配置冲突等。因此需要有一个标准的二层信息交流协议。
- LLDP 提供了一种标准的链路层发现方式。通过 LLDP 获

取的设备二层信息能够快速获取相连设备的拓扑状态；显示出客户端、交换机、路由器、应用服务器以及网络服务器之间的路径；检测设备间的配置冲突、查询网络失败的原因。企业网用户可以通过使用网管系统，对支持运行 LLDP 协议的设备进行链路状态监控，在网络发生故障的时候快速进行故障定位。

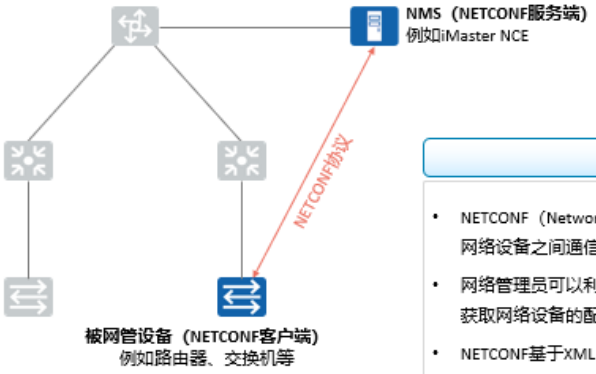
SNMP



SNMP简介

- 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。
- 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。
- 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。

NETCONF/YANG



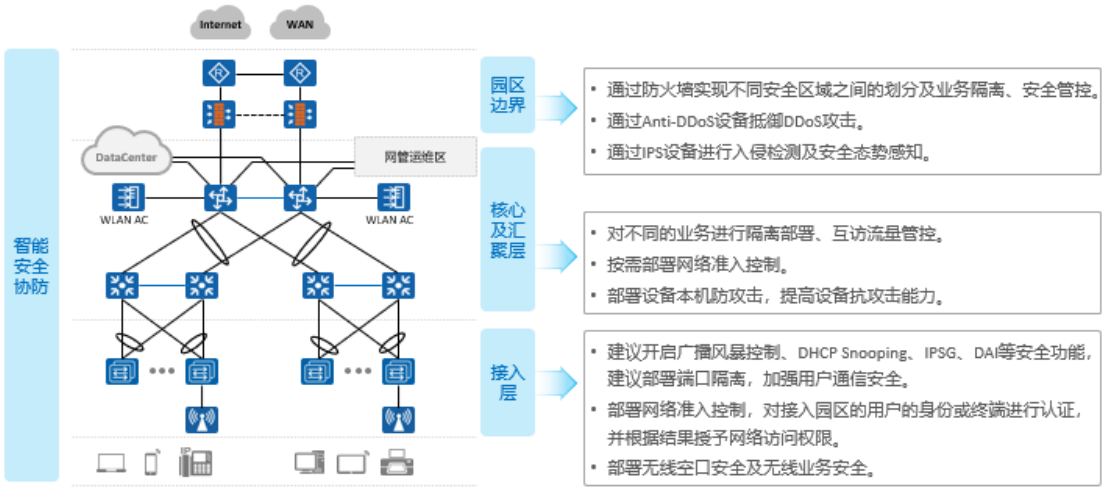
SNMP的短板

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。

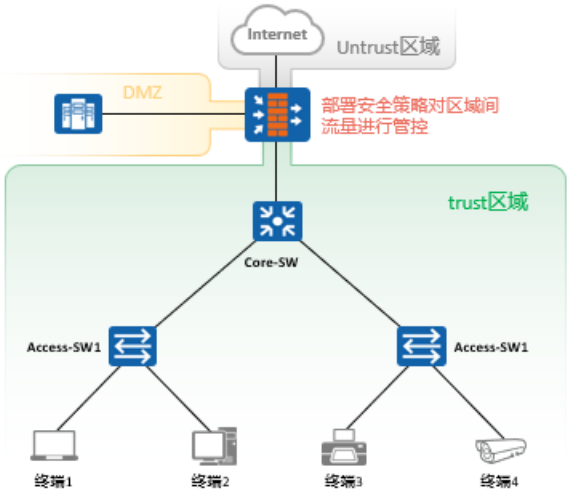
NETCONF

- 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。
- 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。
- NETCONF基于XML（Extensible Markup Language，可扩展标记语言）。

园区网络安全概述



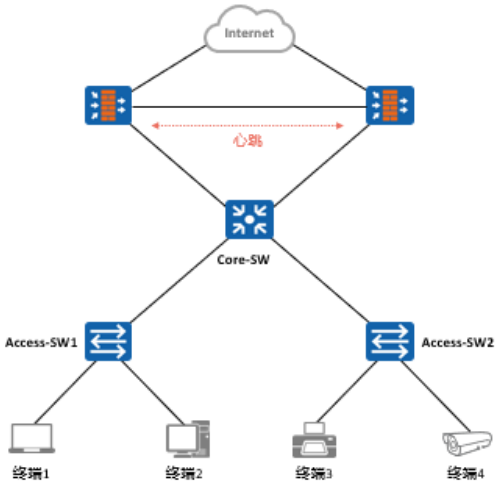
基于防火墙的安全区域划分及安全策略



- 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。
- 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。
- 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。

- 在一台防火墙上不允许创建两个相同安全级别（Priority）的安全区域；
- 防火墙的接口必须加入一个安全区域，否则不能正常转发流量。
- 防火墙的一个接口只能属于一个安全区域。
- 防火墙的一个安全区域可以拥有多个接口。
- 系统自带的缺省安全区域不能删除，用户可以根据实际需求创建自定义的安全区域。

防火墙双机热备概述



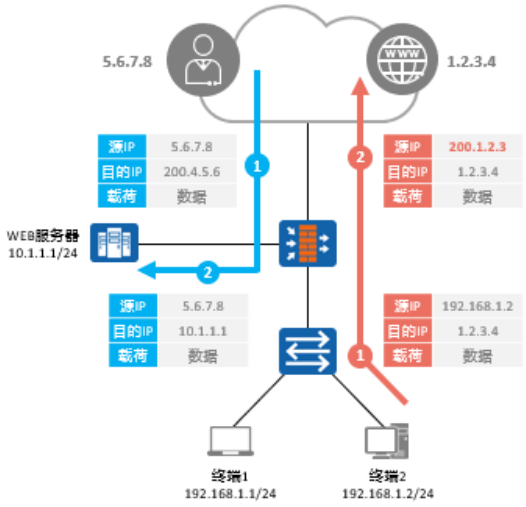
需求

- 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。
- 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。

方案

- 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。
- 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）。
- 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。

NAT



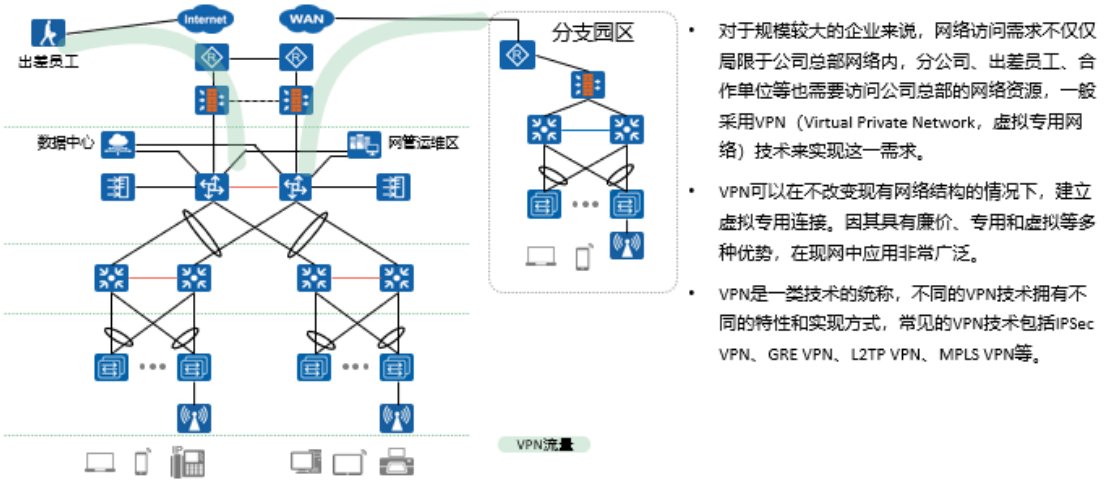
需求

- 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。
- 外网用户需访问采用私网IP地址的服务器（例如WEB服务器）。

NAT（Network Address Translation）

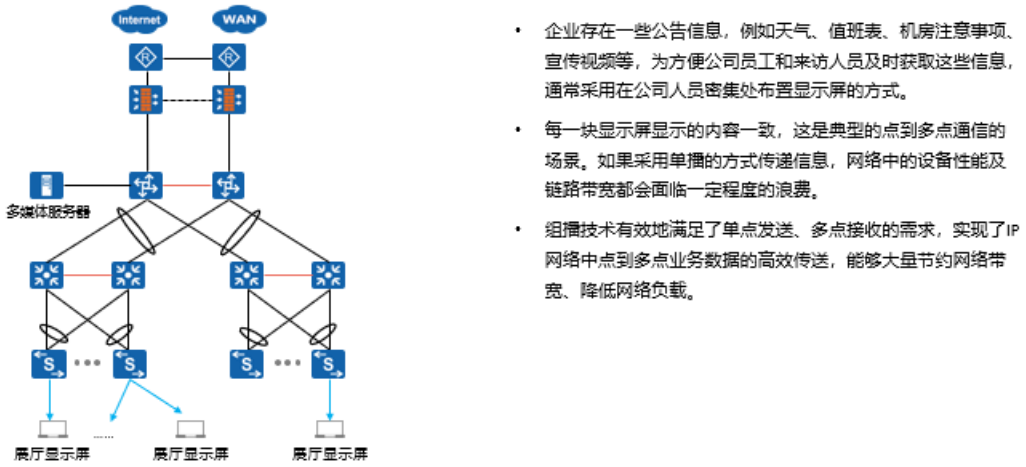
- NAT是将IP数据报文头中的IP地址转换为另一个IP地址的过程。
- 常用NAT：
  - 源IP地址转换（Source IP address-based NAT）：
    - No-Port 地址转换（No-PAT）
    - 网络地址及端口转换（NAPT）
  - 目的IP地址转换（Destination IP address-based NAT）：
    - NAT Server

VPN技术应用场景



- IPSec：IP Security， 因特网协议安全协议。
- GRE：Generic Routing Encapsulation， 通用路由封装协议。
- L2TP：Layer 2 Tunneling Protocol， 二层隧道协议。
- MPLS：Multiprotocol Label Switching，多协议标签交换协议。

组播应用场景



- 单播（Unicast）是在一台源 IP 主机和一台目的 IP 主机之间进行。网络上绝大部分的数据都是以单播的形式传输的，

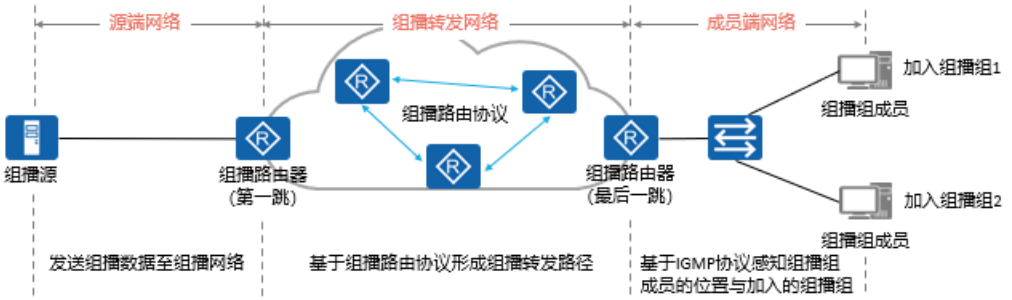
例如电子邮件收发、网上银行都是采用单播实现的。

- 在单播通信中每一个数据包都有确切的目的 IP 地址；对于同一份数据，如果存在多个接收者，Server 需发送与接收者数目相同的单播数据包；当接收者增加到成百上千时，将极大加重 Server 创建相同数据和发送多份相同拷贝后所产生的消耗，网络中的设备性能及链路带宽都会面临一定程度的浪费；单播方式较适合用户稀少的网络，当用户量较大时很难保证网络传输质量。
- 广播（Broadcast）是在一台源 IP 主机和网络中所有其它的 IP 主机之间进行，属于一对所有的通讯方式，所有主机都可以接收到（不管是否需要）。
- 广播数据包被限制在广播域中；一旦有设备发送广播数据，则广播域内所有设备都会收到这个数据包，并且不得不耗费资源去处理，大量的广播数据包将消耗网络的带宽及设备资源；广播方式只适合共享网段，且信息安全性和有偿服务得不到保障。
- 组播（Multicast）是在一台源 IP 主机和多台（一组）IP 主机之间进行，中间的网络设备根据接收者的需要，有选择性地对数据进行复制和转发。

组播网络基本架构

组播网络大体可以分为三个部分：

- 源端网络：将组播源产生的组播数据发送至组播网络。
- 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）。
- 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。

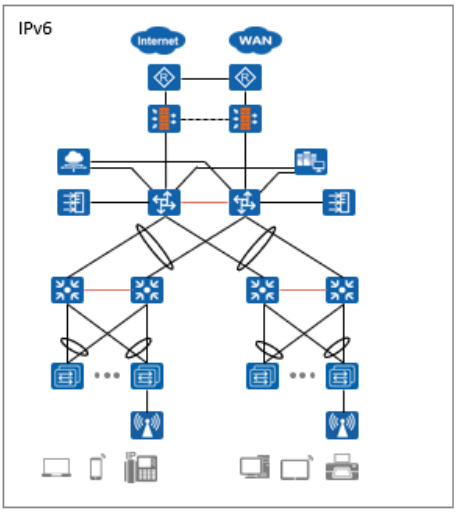


- 组播源（Source）：组播流量的发送者，例如多媒体服务器。组播源无需运行任何组播协议，只需简单 地将组播数据发送出来即可。
- 组播接收者（Receiver）：也被称为组播组成员，是期望接收特定组播组流量的设备，例如运行多媒体直播客户端软件的 PC。
- 组播组（Multicast Group）：用 IP 组播地址进行标识的一个集合。任何用户主机（或其他接收设备），加入一个组播组，就成为了该组成员，可以识别并接收发往该组播组的组播数据。
- 组播路由器（Multicast Router）：支持组播、运行组播协议的网络设备，实际上不仅仅路由器能够支持 组播，交换机、防火墙等设备也能够支持组播（取决于设备型号），路由器仅是一个代表。
- 第一跳路由器（First-Hop Router）：组播转发路径上，与组播源相连且负责转发该组播源发出的组播数据的 PIM 路由器。
- 最后一跳路由器（Last-Hop Router）：组播转发路径上，与组播组成员相连且负责向该组成员转发组播数据的 PIM 路

由器。

- IGMP（Internet Group Management Protocol，因特网组管理协议），是 TCP/IP 协议族中负责 IP 组播成员管理的协议，它用来在接收者和与其直接相邻的组播路由器之间建立、维护组播组成员关系。

IPv6概述



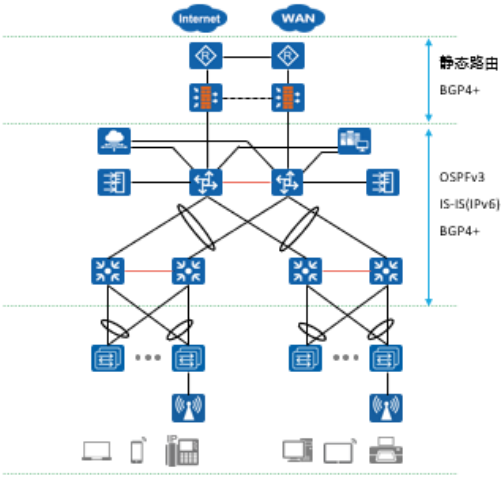
- IPv4协议是目前广泛部署的因特网协议。在因特网发展初期，IPv4以其协议简单、易于实现、互操作性好的优势而得到快速发展。但随着因特网的迅猛发展，IPv4地址空间不足的问题日趋明显，IPv6取代IPv4势在必行。
- IPv6（Internet Protocol Version 6）是网络层协议的第二代标准协议，也被称为IPng（IP Next Generation）。它是Internet工程任务组IETF（Internet Engineering Task Force）设计的一套规范，是IPv4（Internet Protocol Version 4）的升级版本。
- IPv6地址长度为128 bit，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。

ICMPv6

- ICMPv6 （Internet Control Message Protocol for IPv6）是IPv6的基础协议之一。
- ICMPv6报文被广泛应用于其它协议中，包括NDP、PathMTU发现机制等。
- 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。

- NDP：Neighbor Discovery Protocol，邻居发现协议。

IPv6路由



IPv6网络支持静态路由和动态路由协议：

- 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。
- 动态路由协议：
  - OSPFv3
  - IS-IS
  - BGP4+

思考题：

- （多选题）以下关于交换机二层接口的描述，正确的是？(　　)
- 交换机的二层接口类型有 Access、Trunk、Hybrid。
- Access 接口只能加入一个 VLAN。
- 缺省情况下，Trunk 接口允许 VLAN1 的流量通过，而且在发送时不携带 VLAN Tag。
- 在 Hybrid 接口上可通过命令指定接口在发送特定 VLAN 的流量时，是否携带 VLAN Tag。
- （多选题）以太网链路聚合技术有哪些优势？(　　)
- 增加带宽：链路聚合接口的最大带宽可以达到各成员接口带宽之和。
- 提高可靠性：当某条活动链路出现故障时，流量可以切换到其他可用的成员链路上。
- 负载分担：在一个链路聚合组内，可以实现在各成员活动链路上的负载分担。
- 智能调优：可根据流量大小自动调整活动接口数量。

答案：

- ABCD
- ABC
-