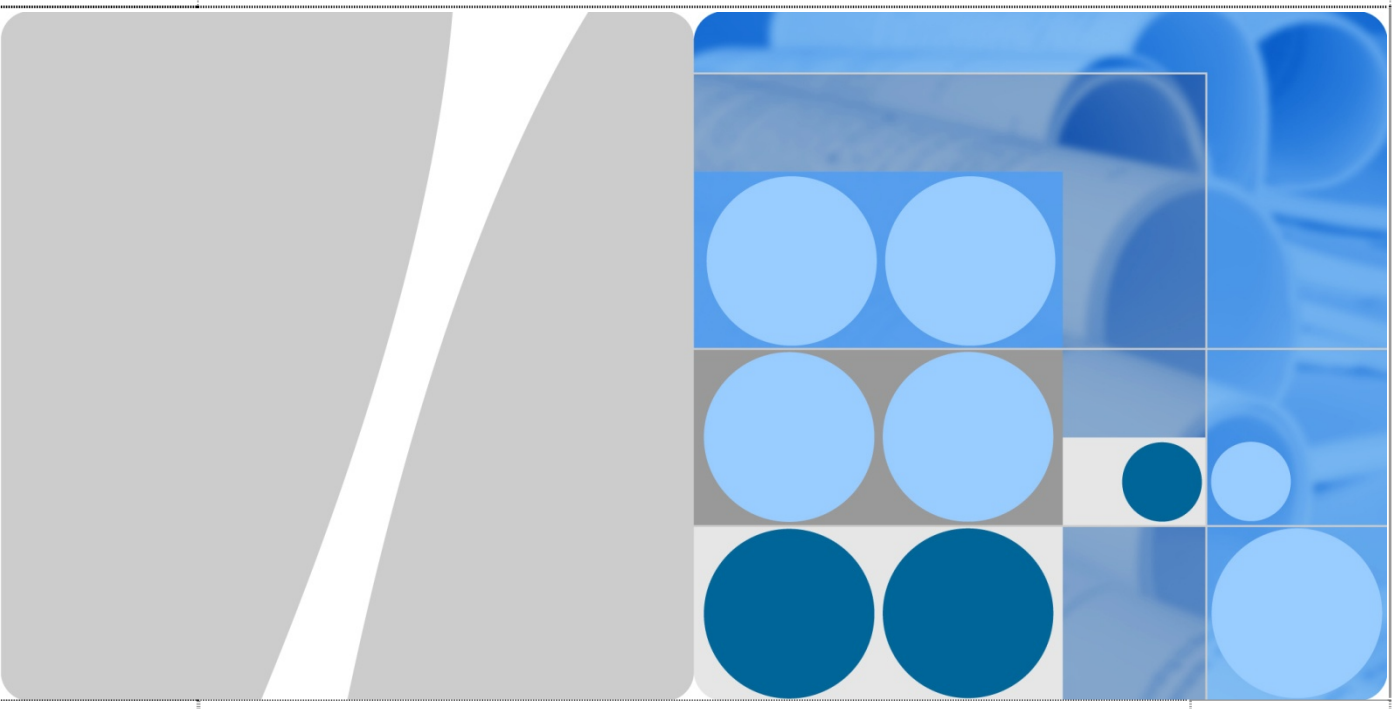


数据中心解决方案
V100R001C01
部署指南

文档版本	01
发布日期	2011-07-22

华为技术有限公司

华为技术有限公司

地址：	深圳市龙岗区坂田华为总部办公楼　　邮编：518129
网址：	http://www.huawei.com
客户服务邮箱：	support@huawei.com
客户服务电话：	4008302118

目 录

插图目录

表格目录

1 数据中心解决方案概述

1.1 方案简介

当今社会的竞争是信息化的竞争，企业信息化程度越高，竞争力就越大。随着网络技术、通信技术的发展，数据中心已经成为企业信息化的核心，数据中心的建设好坏直接影响企业的效率和发展。

企业建设数据中心：

- 一方面通过将企业的各种业务系统集中部署到数据中心，完成业务系统的整合，进一步支撑业务分析、决策支持，最大化地提升信息的生产力。
- 另一方面，通过 WEB 提供信息门户，建立和客户沟通的渠道，提供企业宣传、产品推广、客户服务，进一步支撑电子商务，完成基于互联网的业务运营。
- 另外，数据中心还能够提供高性能计算的业务，如：3D 渲染、药物研究、基因分析、WEB 搜索业务。

在一个企业的数据中心中，可能同时有这三种典型业务，这些业务可能相对独立，也可能融合在大的业务系统中。

对于企业来讲，随着“数据大集中”的进展，越来越多的业务和数据都集中到若干个数据中心。数据中心承载网络的高性能和高可靠性成为企业业务开展的核心问题。

华为数据中心解决方案主要侧重于对建设数据中心的网络部分提出整体建议，保证数据中心的高性能、安全、可靠，从而使数据中心能承载更多高品质的业务。

1.2 典型组网

图1-1 数据中心典型组网图

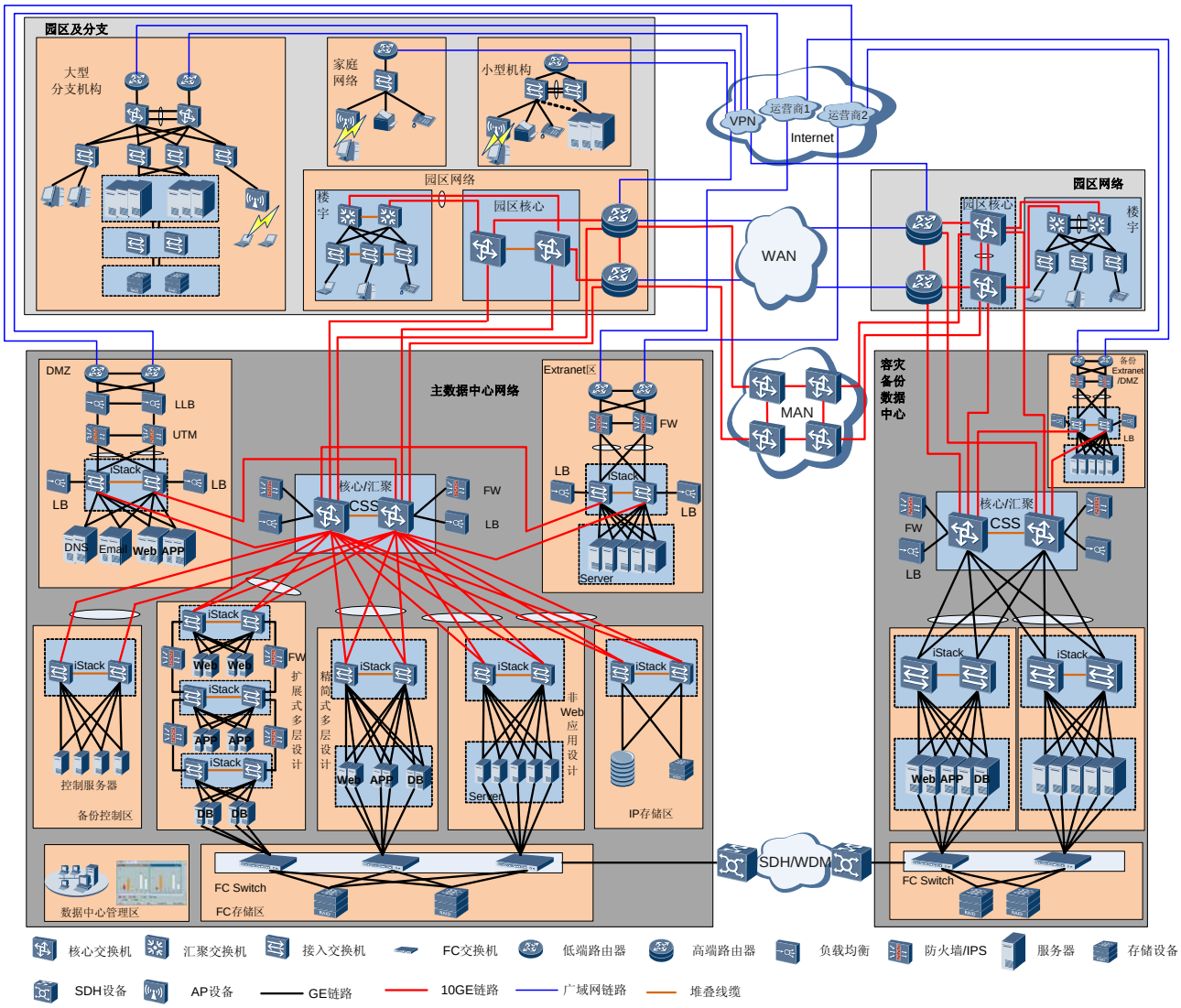


图 1-1 是数据中心的典型组网图，该数据中心遵循了分区的设计原则。根据企业自身特点，依据业务系统的相关性、数据流的访问要求和系统安全控制的要求等，把数据中心的服务器与业务系统分成内网区（Intranet）、外联区（Extranet 区）和互联网区（DMZ 区）、数据中心管理区。

- Intranet 区

  企业内部访问的数据中心区域，通常称为内网区，对外部网络不可见。主要为企业内部用户和企业分支用户提供服务。

- Extranet 区

  企业提供给合作伙伴访问的数据中心区域，通常称为外联区。通过 VPN 接入实现对服务器群的访问和不同企业的隔离。

- DMZ 区

  企业提供给 Internet 用户访问的数据中心区域，外部用户通过公网访问，一般放的是企业门户网站的服务器群、内外部用户常用的服务器（如 DNS、Email 等）。

- 数据中心管理区

  该区域实现对数据中心中网络设备的管理和维护。

说明

本配置举例主要介绍主数据中心中 Intranet 区业务网络（不含 DMZ 区和 Extranet 区）、数据中心管理网络、DMZ 区业务网络和 Extranet 区业务网络的配置，对于服务器、存储设备、LLB、UTM、FW 本身的配置，请参考相关厂家的用户手册。

另外，因容灾备份数据中心中 Intranet 区业务网络、DMZ 区、Extranet 区的配置跟主数据中心中的基本一致，所以此处不再单独介绍。

1.3 配套产品和版本

表1-1 数据中心解决方案配套产品和版本

部件	产品	版本
DMZ 和 Extranet 区的出口路由器	AR 路由器	V200R001C00 版本及以上
核心/汇聚交换机	S9300	V100R006C00 版本及以上
接入交换机	S6700/S5700/S3700	V100R006C00 版本及以上
网管系统	eSight	V200R001C00

2 数据中心网络配置

2.1 数据中心基础网络配置

说明

本节介绍数据中心四个区（Intranet 区、DMZ 区、Extranet 区和维护管理区）之间以及四个区内部的网络连通性配置，不管从业务上来讲是否允许互通。基础网络之外的不同类型用户接入数据中心时对网络的要求，在 2.2 不同用户接入数据中心时对网络的要求中进行介绍。

2.1.1 Intranet 区配置

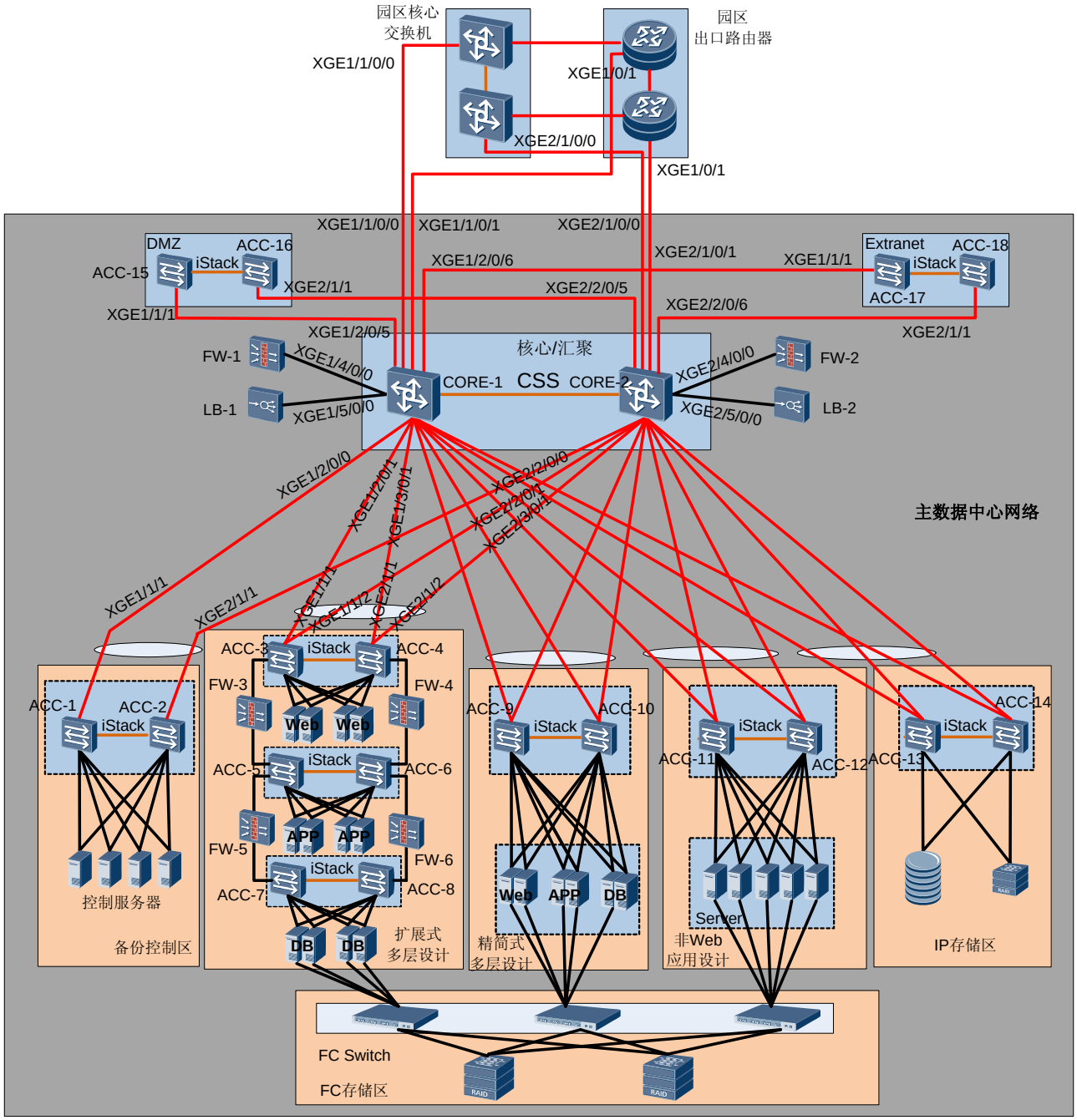
典型组网

图 2-1 为数据中心 Intranet 区的典型组网图。

- 主数据中心 Intranet 区核心/汇聚交换机和园区核心交换机、园区出口路由器、容灾备份数据中心核心交换机、小型园区中的核心交换机和出口路由器之间通过配置 OSPF 路由协议，实现路由全网可达，这些设备划分到同一个 Area0 中。
- Intranet 区与 DMZ、Extranet 区通过配置 OSPF 路由协议，实现各区路由互通。
- Intranet 区核心/汇聚交换机之间配置堆叠，与备份控制区、扩展式多层设计区、精简式多层设计区、非 Web 应用设计区和 IP 存储区之间以 Eth-Trunk 方式连接。接入交换机之间也配置堆叠，从而形成集群+堆叠的扁平化化无环网络。
- Intranet 区核心/汇聚交换机集成防火墙和负载均衡器：
  - 对于需要负载均衡服务的服务器，网关设置在负载均衡器上，服务器通过负载均衡器对外提供企业内网地址，本身与负载均衡器通信采用 172.16.0.0/16 网段的私网地址。
  - 其他服务器网关设置在防火墙上。
  - 防火墙和负载均衡器采用双机热备方式，提高可靠性保护。
- 对于控制备份区，接入交换机配置堆叠后，只需要配置 VLAN。
- 对于扩展式多层设计区，Web、App、DB 服务器需要分配不同的 IP 地址网段，并且网关配置在其接入交换机上。整区的交换机连同防火墙需要配置 OSPF 路由协议，跟 DMZ 区、Internet 区、Extranet 区在同一个 Area 里。

- 对于精简式多层设计区，Web、App、Db 服务器需要分配不同的 IP 地址网段，并且其接入交换机需要为各类服务器划分不同的 VLAN。网关根据需要可以配置在防火墙上或者负载均衡器上。
- 对非 Web 应用设计区，接入交换机配置堆叠后，只需要配置 VLAN。该区内的服务器网关根据是否需要负载分担服务，将网关配置在 LB 上或者 FW 上。
- 对于 IP 存储区，接入交换机配置堆叠后，只需要配置 VLAN。

图2-1 数据中心 Intranet 区典型组网图



物理连接

设备名称	接口编号	对接设备名称	接口编号
CORE-1	XGE1/0/0	园区核心交换机-1	XGE1/1/0/0
	XGE1/0/1	园区出口路由器-1	XGE1/0/1
	XGE2/0/0	ACC-1	XGE0/1/1
	XGE2/0/1	ACC-3	XGE0/1/1
	XGE3/0/1	ACC-4	XGE0/1/1
	XGE2/0/2	ACC-9	XGE0/1/1
	XGE3/0/2	ACC-10	XGE0/1/1
	XGE2/0/3	ACC-11	XGE0/1/1
	XGE3/0/3	ACC-12	XGE0/1/1
	XGE2/0/4	ACC-13	XGE0/1/1
	XGE3/0/4	ACC-14	XGE0/1/1
	XGE2/0/5	ACC-15	XGE0/1/1
	XGE2/0/6	ACC-17	XGE0/1/1
	XGE4/0/0	FW-1	XGE0/1/1
	XGE4/0/1	FW-1	XGE0/1/2
	XGE5/0/0	LB-1	XGE0/1/1
	XGE5/0/1	LB-1	XGE0/1/2
CORE-2	XGE1/0/0	园区核心交换机-1	XGE2/1/0/0
	XGE1/0/1	园区出口路由器-2	XGE1/0/1
	XGE2/0/0	ACC-2	XGE0/1/1
	XGE2/0/1	ACC-3	XGE0/1/2
	XGE3/0/1	ACC-4	XGE0/1/2
	XGE2/0/2	ACC-9	XGE0/1/2
	XGE3/0/2	ACC-10	XGE0/1/2
	XGE2/0/3	ACC-11	XGE0/1/2
	XGE3/0/3	ACC-12	XGE0/1/2
	XGE2/0/4	ACC-13	XGE0/1/2
	XGE3/0/4	ACC-14	XGE0/1/2
	XGE2/0/5	ACC-16	XGE0/1/1
	XGE2/0/6	ACC-18	XGE0/1/1

设备名称	接口编号	对接设备名称	接口编号
	XGE4/0/0	FW-1	XGE0/1/1
	XGE4/0/1	FW-1	XGE0/1/2
	XGE5/0/0	LB-1	XGE0/1/1
	XGE5/0/1	LB-1	XGE0/1/2
ACC-1 ~ ACC-14	GE 端口 其中 CE-3 ~ CE-8 一些 GE 端口跟 FW 相连	服务器	服务器网卡接口
ACC-3	GE0/0/0	FW-3	Interface 1
ACC-4	GE0/0/0	FW-4	Interface 2
ACC-5	GE0/0/0	FW-3	Interface 3
	GE0/0/1	FW-5	Interface 4
ACC-6	GE0/0/0	FW-4	Interface 5
	GE0/0/1	FW-6	Interface 6
ACC-7	GE0/0/0	FW-5	Interface 7
ACC-8	GE0/0/0	FW-6	Interface 8

配置思路

采用如下思路完成此配置举例：

- 因堆叠使能后，会影响端口编号，所以先把扁平化无环网络配置完成
- 配置端口描述信息
- 配置核心汇聚交换机
  - 服务器网关在 FW 上：配置 VLAN，相应接口加入 VLAN，使服务器和 FW 在相同 VLAN 内可以互通
  - 服务器网关在 LB 上：配置 VLAN，相应接口加入 VLAN, 使服务器和 LB 在相同 VLAN 内可以互通
  - 配置接口 IP 地址及 OSPF 路由协议，实现核心汇聚交换机可以跟旁挂的 FW、LB、DMZ 区、Internet 区、控制备份区服务器、扩展式多层设计区服务器、精简式多层设计区服务器、非 Web 应用设计区服务器、IP 存储区服务器路由互通
- 配置防火墙设备
  - 登录防火墙设备，配置 VRRP，VIP 作为服务器、LB 网关地址
  - 配置防火墙 IP 和 OSPF 路由协议，实现路由可达
  - 配置防火墙热备功能

  - 配置防火墙防攻击和过滤功能
- 配置负载均衡设备
  - 登录负载均衡设备，配置 VRRP，VIP 作为服务器
  - 配置负载均衡功能，实现服务器负载均衡
  - 配置静态路由，实现下一条路由可达 FW 上
  - 配置负载均衡器热备功能
- 配置备份控制区接入交换机
  - 配置 VLAN，接口加入 VLAN
- 配置扩展式多层设计区接入交换机
  - 配置接口 IP、路由 OSPF，实现路由可达
  - 配置防火墙功能
- 配置精简式多层设计区接入交换机
  - 配置 VLAN，接口加入 VLAN
- 配置非 Web 应用设计区接入交换机
  - 配置 VLAN，接口加入 VLAN
- 配置 IP 存储区接入交换机
  - 配置 VLAN，接口加入 VLAN

操作步骤

1. 配置扁平化无环网络

   a. 在核心交换机上使能堆叠功能

   - 配置 CORE-1

```
sysname CORE-1
set css id 1     //如果没有修改过缺省值，该步骤可以省略
css enable
```

   - 配置 CORE-2

```
sysname CORE-2
set css id 2
css enable
```

   b. 在接入交换机上使能堆叠功能

   说明

   因为 S5700 默认就处于堆叠状态，所以如果没有修改默认状态，只需要连接好堆叠线缆，交换机就会自动选举主、备、从堆叠设备。如果当前交换机处于非堆叠状态，可以执行如下步骤使能交换机的堆叠功能。

   以 ACC-1 为例，其他接入交换机的配置相同。

```
sysname ACC-1
stack slot 1 priority 255  //优先级越高，堆叠成功后就成为 Master
stack enable
```

说明
在堆叠生效后，配置新系统名字为编号比较小的设备名，如 COER-1 和 CORE-2 堆叠，堆叠完成后配置新系统名字为 CORE-1。ACC-1 和 ACC-2 堆叠，堆叠完成后配置新系统名字为 ACC-1。Intranet 各区接口服务器命名类同。DMZ 区接入交换机堆叠完成后配置新系统名字为 DMZ，Extranet 区接口交换机堆叠完成后配置新系统名字为 Extranet。

c. 堆叠设备之间配置 Eth-Trunk

以 CORE-1 跟 ACC-1 之间配置 Eth-trunk 为例，其他接入交换机的配置相同。

```
CORE-1 配置
#
interface eth-trunk 1
                    #
                    interface xgigabitethernet 1/2/0/0
                        eth-trunk 1
                    #
interface xgigabitethernet 1/2/0/0
                        eth-trunk 1
                    #
ACC-1 配置
#
interface eth-trunk 1
mode lacp-static
                    #
                    interface xgigabitethernet 1/1/1
                        eth-trunk 1
                    #
interface xgigabitethernet 2/1/1
                        eth-trunk 1
                    #
```

请参考上述配置，配置下面表格关设备的 Eth-Trunk。

本端设备	Eth-trunk 配置	对端设备	Eth-trunk 配置	备注
CORE-1	Eth-trunk 1	ACC-1	Eth-trunk 1	CORE-1 跟备份控制区 ACC-1 的 eth-trunk 连接
	Eth-trunk 2	ACC-3	Eth-trunk 2	CORE-1 跟扩展式多层设计区 ACC-3 的 eth-trunk 连接
	Eth-trunk 3	ACC-9	Eth-trunk 3	CORE-1 跟精简式多层设计区 ACC-9 的 eth-trunk 连接
	Eth-trunk 4	ACC-11	Eth-trunk 4	CORE-1 跟非 Web 应用设计区 ACC-11 的 eth-trunk 连接
	Eth-trunk 5	ACC-13	Eth-trunk 5	CORE-1 跟 IP 存储区 ACC-13 的 eth-trunk 连接
	Eth-trunk 6	FW-1	Eth-trunk 6	CORE-1 跟 FW-1 的 eth-trunk 连接
	Eth-trunk 7	FW-2	Eth-trunk 7	CORE-1 跟 FW-2 的 eth-trunk 连接
	Eth-trunk 8	LB-1	Eth-trunk 8	CORE-1 跟 LB-1 的 eth-trunk 连接

本端设备	Eth-trunk 配置	对端设备	Eth-trunk 配置	备注
	Eth-trunk 9	LB-2	Eth-trunk 9	CORE-1 跟 LB-2 的 eth-trunk 连接
	Eth-trunk 10	ACC-15	Eth-trunk 10	CORE-1 跟 DMZ 区的 eth-trunk 连接
	Eth-trunk 11	ACC-17	Eth-trunk 11	CORE-1 跟 Extranet 区的 eth-trunk 连接
	Eth-trunk 12	园区核心交换机	Eth-trunk 12	CORE-1 跟园区核心交换 eth-trunk 连接

2. 配置接口描述信息

   以在 CORE-1 上配置为例，其他接口的配置相同。

```
interface xgigabitethernet 1/2/0/0
description To-[CE-1]XGE-1/1/1
```

3. 配置核心汇聚交换机

   a. 服务器网关在 FW-1/FW-2 上，配置 VLAN，相应接口加入 VLAN，使服务器/LB 和 FW 在相同 VLAN 内可以互通。

   假设备份控制区里面的控制服务器网关配置在 FW 上，则核心汇聚交换机需要配置 VLAN，将连接备份控制区和 FW-1、FW-2 的接口加入此 VLAN。实现服务器跟 FW 同一网段互通。

   数据规划如下表所示。

服务器 IP 地址	VLAN 划分	网关设备	网关 IP	备注
10.100.20.x/24	200	FW	FW 之间 VRRP 的 VIP： 10.100.20.254	FW-1 接口 IP 地址为 10.100.20.1 FW-2 接口 IP 地址为 10.100.20.2

```
#
vlan 200   //假定备份控制区所有服务器在同一个网段地址，只需要配置一个 VLAN。
#
 interface eth-trunk 1  //CORE-1 跟 ACC-1 的逻辑接口容许 VLAN200 通过
   port link-type trunk
   undo port trunk allow-pass vlan 1
    port trunk allow-pass vlan 200
#
 interface eth-trunk 6   //CORE-1 跟 FW-1 的逻辑接口容许 VLAN200 通过
   port link-type trunk
   undo port trunk allow-pass vlan 1
   port trunk allow-pass vlan 200
#
interface eth-trunk 7   //CORE-1 跟 FW-1 的逻辑接口容许 VLAN200 通过
```

```
   port link-type trunk
   undo port trunk allow-pass vlan 1
   port trunk allow-pass vlan 200
#
```

说明

上述配置只是针对一个 VLAN 的情况，如果服务器存在多个网段地址，每个网段地址对应一个 VLAN 一个网关，请对照上述配置举例进行相关配置。

b. 服务器网关在 LB 上，配置 VLAN，相应接口加入 VLAN，使服务器和 LB 在相同 VLAN 内可以互通。

假设非 Web 应用设计区里面的服务器需要负载均衡服务，则服务器网关地址需要配置在 LB 上。核心/汇聚交换机需要配置 VLAN，将连接该区和 LB-1、LB-2 的接口加入此 VLAN。实现服务器跟 LB 同一网段互通，并且服务器采用私网地址如 172.16.0.0/16 网段的地址，通过 LB 对外体现为企业内网地址。

服务器 IP 地址	VLAN 划分	网关设备	网关 IP	备注
172.16.1.x/24	400	LB	LB 之间 VRRP 的 VIP： 172.16.1.254	服务器通过 LB 对外体现为企业内网地址 10.100.40.x/24

```
#
 vlan 400   //假定非 Web 应用区所有服务器在同一个网段地址，只需要配置一个 VLAN
#
 interface eth-trunk 4  //CORE-1 跟 ACC-11 的逻辑接口容许 VLAN400 通过
   port link-type trunk
   undo port trunk allow-pass vlan 1
   port trunk allow-pass vlan 400
#
 interface eth-trunk 8   //CORE-1 跟 LB-1 的逻辑接口容许 VLAN400 通过
   port link-type trunk
   undo port trunk allow-pass vlan 1
   port trunk allow-pass vlan 400
#
interface eth-trunk 9   //CORE-1 跟 LB-1 的逻辑接口容许 VLAN400 通过
   port link-type trunk
   undo port trunk allow-pass vlan 1
   port trunk allow-pass vlan 400
#
```

说明

上述配置只是针对一个 VLAN 的情况，如果服务器存在多个网段地址，每个网段地址对应一个 VLAN 一个网关，请对照上述配置举例进行相关配置。另外 LB 下一跳为 FW，在核心/汇聚交换机上需要配置 VLAN，将 FW 跟 LB 相关接口加入到此 VLAN 内。

```
#
 vlan 100   //此 VLAN 用于 FW 跟 LB 同网段互通
#
 interface eth-trunk 6
   port link-type trunk
   undo port trunk allow-pass vlan 1
   port trunk allow-pass vlan 100
#
```

```
 interface eth-trunk 7
    port link-type trunk
    undo port trunk allow-pass vlan 1
    port trunk allow-pass vlan 100
#
interface eth-trunk 8
    port link-type trunk
    undo port trunk allow-pass vlan 1
    port trunk allow-pass vlan 100
#
interface eth-trunk 9
    port link-type trunk
    undo port trunk allow-pass vlan 1
    port trunk allow-pass vlan 100
#
```

c. 配置接口 IP 地址及 OSPF 路由协议，实现网络各节点的网际层互通

核心/汇聚交换机需要创建多个 VLANIF 三层接口，分别跟 FW-1/FW-2、DMZ 区、Extranet 区、扩展式多层设计区接入交换机、出口路由器建立三层互通。并且配置路由协议 OSPF，发布网络路由。其他区域同样需要配置相关 IP 地址和路由协议。

按照下面表格配置 VLANIF 接口及其 IP 地址。

本端接口	本端 IP 地址	对端设备	对端 IP 地址	备注
VLANIF 10	10.10.10.1/24	FW-1 、FW-2	10.10.1.2/24 10.10.1.3/24	跟 FW-1、FW-2 相连网段
VLANIF 11	10.10.11.1/24	ACC-11	10.10.11.2/24	跟扩展式多层设计接入服务器 ACC-11
VLANIF 20	10.10.20.1/24	DMZ	10.10.20.2/24	跟 DMZ 区相连的网段
VLANIF 30	10.10.30.1/24	Extranet	10.10.30.2/24	跟 Extranet 区相连的网段
VLANIF 40	10.10.40.1/24	园区核心交换机	10.10.40.2/24	跟园区核心交换机相连的网段
VLANIF 50	10.10.50.1/24	出口路由器-1	10.10.50.2/24	跟出口路由器-1 相连的网段
VLANIF 60	10.10.60.1/24	出口路由器-2	10.10.60.2/24	跟出口路由器-2 相连的网段

以配置接口 VLANIF10 及其 IP 地址为例进行配置，其他配置类似。

```
#
 vlan 10
#
 interface eth-trunk 6
```

```
   port link-type trunk
   undo port trunk allow-pass vlan 1
   port trunk allow-pass vlan 10
#
interface eth-trunk 7
   port link-type trunk
   undo port trunk allow-pass vlan 1
   port trunk allow-pass vlan 10
#
interface vlanif 10
  ip address 10.10.10.1 24
#
```

配置 OSPF，发布路由，包括直连路由。

```
#
 ospf 1
   import-route direct
   area 0.0.0.0
     network 10.10.10.1 0.0.0.255
     network 10.10.11.1 0.0.0.255
     network 10.10.20.1 0.0.0.255
     network 10.10.30.1 0.0.0.255
     network 10.10.40.1 0.0.0.255
     network 10.10.50.1 0.0.0.255
     network 10.10.60.1 0.0.0.255
#
```

4. 配置防火墙防设备

   a. 在进行 FW 相关配置前，需要先配置 SPU 为 FW 类型

   set service-type firewall

   b. 配置 VRRP，VIP 作为服务器、LB 网关地址

```
#
 sysname FW-1
#
 interface Eth-trunk6
#
 interface Eth-trunk6.200
   control-vid 200 dot1q-termination
   dot1q termination vid 200
   dot1q vrrp vid 200
   ip address 10.100.20.1 24
   vrrp vrid 20 virtual-ip 10.100.20.254  //此 IP 为备份控制区服务器网关地址
   vrrp vrid 20 priority 120              //此 VRRP 作为 Master
   arp broadcast enable
#
 interface Eth-trunk6.100                 //此子接口用于跟 LB 进行通信
   control-vid 100 dot1q-termination
   dot1q termination vid 100
   dot1q vrrp vid 100
   ip address 10.100.10.1 24
   vrrp vrid 10 virtual-ip 10.100.10.254   //此 IP 为 LB 下一跳网关
   vrrp vrid 10 priority 120
   arp broadcast enable
```

```
#
```

说明

FW-2 的 VRRP 配置跟 FW-1 相同，在配置 VRRP 优先级时要小于 FW-1。

c. 配置防火墙 IP 和路由，实现跟各区路由可达

```
#
 interface Eth-trunk6.10          //此子接口用于跟核心汇聚交换机进行通信
    control-vid 10 dot1q-termination
    dot1q termination vid 10
    dot1q vrrp vid 10
    ip address 10.10.10.2 24    //FW-2 对应子接口为 10.10.10.3/24
    arp broadcast enable
#
ospf 1
   import-route direct         //通过 OSPF 发布直连路由
   area 0.0.0.0
     network 10.10.10.2 0.0.0.255
#
```

d. 配置防火墙热备功能

```
FW-1 配置
#
hot-standby-group local 10.100.20.1 peer 10.100.20.2 src-data-port 3001 dst-data-
port 4001
hot-standby enable
FW-2 配置
#
hot-standby-group local 10.100.20.1 peer 10.100.20.2 src-data-port 4001 dst-data-
port 3001
hot-standby enable
```

e. 配置防火墙防攻击、过滤功能

FW-1 和 FW-2 为核心汇聚交换机 S93 内置防火墙，支持如下功能：

- 配置安全区域
- 支持 ACL 包过滤防火墙
- 支持 ASPF 针对应用层的包过滤
- 支持黑白名单根据报文的源 IP 地址进行过滤
- 支持端口映射
- 支持虚拟防火墙
- 支持日志功能，流量统计和监控
- 支持如下攻击防范：
  - 拒绝服务型攻击
  - 扫描窥探攻击
  - 畸形报文攻击
  - Land 攻击
  - Smurf 攻击
  - WinNuke 攻击
  - SYN Flood 攻击

- ICMP 和 UDP Flood 攻击
- Ping of Death 攻击
- 地址扫描与端口扫描攻击
- Ping of Death 攻击
- ICMP-Redirect 和 ICMP-Unreachable
- 攻击 Teardrop 攻击
- Fraggle 攻击
- IP-Fragment 攻击
- Tracert 攻击

具体过滤和防攻击请根据实际需求参考《Quidway S9300 多业务接入交换机 配置指南-SPU》的“防火墙配置”。

5. 配置负载均衡业务

a. 在进行 LB 相关配置前，需要先配置 SPU 为 Load Balance 类型

```
set service-type load-balance
```

b. 配置 VRRP，VIP 作为服务器网关地址

```
#
sysname LB-1
#
interface Eth-trunk8
#
interface Eth-trunk8.200
control-vid 200 dot1q-termination
dot1q termination vid 200
dot1q vrrp vid 200
ip address 172.16.1.1 16
vrrp vrid 20 virtual-ip 172.16.1.254  //此 IP 为非 Web 应用设计区服务器网关地址
vrrp vrid 20 priority 120             //此 VRRP 作为 Master
arp broadcast enable
#
interface Eth-trunk8.100                 //此子接口用于跟 FW 进行通信
control-vid 100 dot1q-termination
dot1q termination vid 100
ip address 10.100.10.3 24
arp broadcast enable
#
```

说明

LB 接口配置和 VRRP 配置跟 FW 类似。负载均衡器跟服务器采用私网地址 172.16/16，负载均衡器对外表现为企业内网地址 10.100.10/24。

c. 配置服务器负载均衡业务功能

LB-1 和 LB-2 为核心汇聚交换机 S93 内置负载均衡器，支持服务器负载均衡。

负载均衡的相关配置具体请参考《Quidway S9300 多业务接入交换机 配置指南-SPU》的“负载均衡配置”。

d. 配置静态路由，实现下一条路由可达 FW 上

```
ip route-static 0.0.0.0 0.0.0.0 10.100.10.254
```

LB-2 需要相同的配置。

e. 配置负载均衡器热备功能

LB-1 配置

```
#
hot-standby-group local 172.16.1.1 peer 172.16.1.2 src-data-port 3001 dst-data-port
4001
hot-standby enable
```

FW-2 配置

```
#
hot-standby-group local 172.16.1.2 peer 172.16.1.1 src-data-port 4001 dst-data-port
3001
hot-standby enable
#
```

6. 配置备份控制区接入交换机

a. 上行配置 eth-trunk，跟核心汇聚交换机对接

备份控制区接入交换机上行跟核心汇聚交换机配置 Eth-trunk，具体配置可以参考核心汇聚交换机的配置。

b. 划分 VLAN，同网段服务器加入到同一 VLAN 内。

划分 VLAN，服务器接入端口 default 方式加入 VLAN，实现服务器二层互通。

```
#
 vlan 100
#
 interface gigabitEthernet1/0/0
    port link-type access
    port default vlan 100
#
```

多个端口需要加入 VLAN，请参考上述配置。如果该区存在多个网段，则不同网段分布在不同的 VLAN 内。

7. 配置扩展式多层设计区接入交换机

扩展式多层设计区 Web、APP、DB 服务器网关配置在其接入交换机上，各接入交换机之间需要配置路由协议实现该区网络可达。同时该区路由需要跟核心汇聚交换机旁的 FW 进行路由交互，以实现网络层可达。串行的防火墙可以配置二层防火墙或者三层防火墙，如果配置三层防火墙则同样需要配置路由协议。

a. Web、APP、DB 服务器各接入交换机配置 VLAN，配置 VLANIF 接口作为其网关

VLAN 划分，服务器端口加入 VLAN 请参考备份控制区接入交换机的配置。VLANIF 接口及其 IP 地址的配置请参考核心汇聚交换机的配置。

b. Web、APP、DB 服务器各接入交换机配置 OSPF、实现区域内路由可达

本区跟核心汇聚交换机、FW、DMZ 区接入交换机、Extranet 区接入交换机配置同进程的 OSPF，所有网段地址都规划在 Area 0 即可。OSPF 的配置请参考核心汇聚交换机的配置。

c. 配置串行防火墙防攻击过滤功能

如果防火墙工作在二层，则不需要配置 IP 地址和路由协议。如果防火墙工作在三层，则需要配置 IP 和 OSPF 路由协议。相关配置和该防火墙防攻击过滤功能请参看该设备的用户手册。

8. 配置精简式多层设计区接入交换机

该区 Web、App、Db 服务器配置不同的私网网段地址。需要在接入服务器上根据不同的网段地址划分不同的 VLAN。具体可以参考备份控制区接入服务器的配置。

9. 非 Web 应用设计区

该区接入交换机配置跟备份控制区接入交换机类似，具体配置请参考备份控制区接入交换机。

10. IP 存储区

该区接入交换机配置跟备份控制区接入交换机类似，具体配置请参考备份控制区接入交换机。

----结束

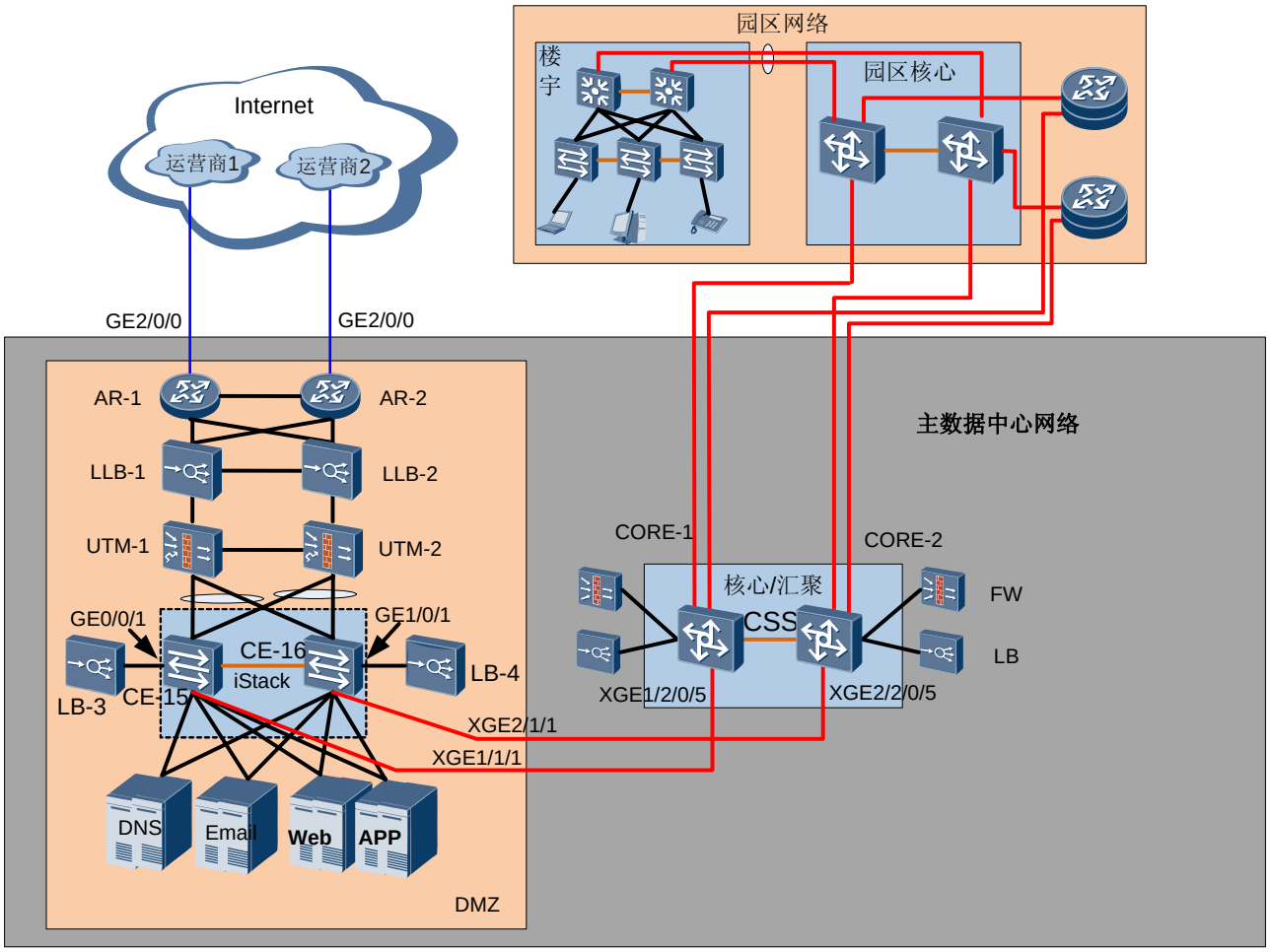
2.1.2 DMZ 区配置

典型组网

图 2-1 为数据中心 DMZ 区的典型组网图。

- DMZ 区采用不同链路接入两家运营商网络，并且通过 LLB 实现智能判断，将不同来源的 Internet 用户返程数据返回到不同的接入运营商网络。实现两家运营商接入链路负载分担。
- UTM 设备集成 IPS 和防火墙功能，对 Internet 用户数据报文进行分析过滤和病毒防范。
- DMZ 区接入交换机跟核心汇聚交换机配置 OSPF 路由协议 ，且在同一个 area 0 里面，实现路由可达。
- DMZ 区的服务器如果需要负载均衡业务，则网关配置在 LB 上，否则配置在堆叠交换机上。
- DMZ 区接入交换机和 LB 上需要配置默认路由，到 Internet 的下一跳为 UTM。

图2-2 DMZ 区典型组网



设备名称	接口编号	对接设备名称	接口编号
ACC-15	XGE0/1/1	PE-1	XGE2/0/5
	GE0/0/1	LB-3	Interface1
	GE0/0/2	UTM-1	Interface2
	GE0/0/3	UTM-2	Interface3
	GE0/0/4	DNS 服务器 1	Interface4
	GE0/0/5	DNS 服务器 2	Interface5
	GE0/0/6	Email 服务器	Interface6
	GE0/0/7	Web 服务器	Interface7
	GE0/0/8	APP 服务器	Interface8
ACC-16	XGE0/1/1	PE-2	XGE2/0/5
	GE1/0/1	LB-4	Interface9

设备名称	接口编号	对接设备名称	接口编号
	GE1/0/2	UTM-2	Interface10
	GE1/0/3	UTM-1	Interface11
	GE1/0/4	DNS 服务器 1	Interface12
	GE1/0/5	DNS 服务器 2	Interface13
	GE1/0/6	Email 服务器	Interface14
	GE1/0/7	Web 服务器	Interface15
	GE1/0/8	APP 服务器	Interface16
AR-1	GE2/0/0	运营商网络 1	-
AR-2	GE2/0/0	运营商网络 2	-

配置思路

- 配置配置各设备接口描述、IP 地址，配置路由协议 OSPF，实现该区域路由整网可达
- 配置 UTM、LLB、LB

说明
因 UTM、LLB、LB 不是华为公司设备，相关配置请参考对应设备的用户手册。

操作步骤

1. 配置各设备接口描述、IP 地址，配置路由协议 OSPF，实现该区域路由整网可达

   在 Intranet 区配置中提及 DMZ 区的 ACC-15 和 ACC-16 配置为堆叠设备，需要跟核心汇聚交换机配置 OSPF，实现路由可达，相关配置如下：

   配置三层接口

```
#
 vlan 20
#
 interface eth-trunk 10
    port link-type trunk
    undo port trunk allow-pass vlan 1
    port trunk allow-pass vlan 20
#
interface vlanif 20
    ip address 10.10.2.2 24
#
```

   配置 OSPF，发布路由

```
#
 ospf 1
    import-route direct
```

```
   area 0.0.0.0
   network 10.10.2.1 0.0.0.255
#
```

配置静态路由指向 UTM

```
ip route-static 0.0.0.0 0.0.0.0 x.x.x.x
```

2. 服务器接入交换机划分 VLAN，不同网段服务器接入同一个 VLAN

   如果服务器网关配置在 LB 上，则接入服务器需要划分 VLAN，将 LB 和相关服务器配置在同一网段上。VLAN 的划分及服务器端口加入 VLAN 请参看 Intranet 区备份控制区接入服务器的配置。

3. LB 负载均衡业务配置

   LB 不是华为公司设备，请参考其配置指南。

4. 在服务器接入交换机上配置网关

   根据需要，接入交换机上可以配置多个 VLANIF 接口作为服务器的网关地址。

```
#
 vlan batch 700 701
#
 interface gigabitEthernet1/0/5
   port link-type access
   port default vlan 700
#
 interface gigabitEthernet1/0/6
    port link-type access
    port default vlan 700
#
 interface gigabitEthernet1/0/7
   port link-type access
   port default vlan 701
#
 interface gigabitEthernet1/0/8
    port link-type access
    port default vlan 701
#
 interface vlanif 700
    ip address 10.200.1.254 24
#
 interface vlanif 701
    ip address 10.201.1.254 24
 #
```

----结束

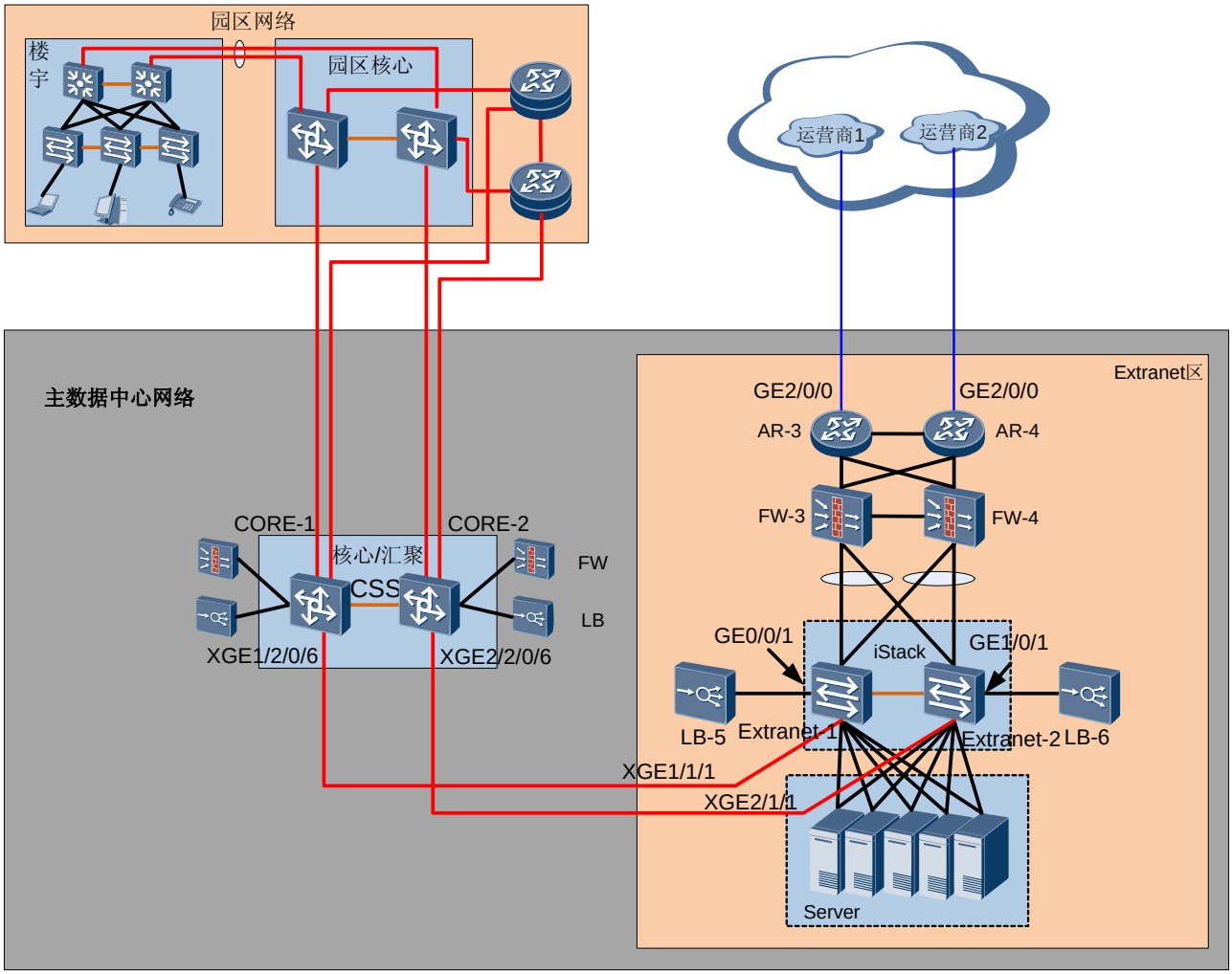
2.1.3 Extranet 区配置

典型组网

如图 2-3 所示是 Extranet 区的典型组网图。

- 区域内部服务器建议采用二层方式接入
- FW 建议采用三层路由模式串接单独对外提供服务，LB 采用旁挂接入
- FW 对外提供的 NAT 后的 IP 地址用于隐藏内部拓扑

图2-3 Extranet 区典型配置



设备名称	接口编号	对接设备名称	接口编号
Extranet-1	XGE1/1/1	CORE-1	XGE1/2/0/6
	GE0/0/1	LB-5	Interface1
	GE0/0/2	FW-3	Interface2

设备名称	接口编号	对接设备名称	接口编号
	GE0/0/3	FW-4	Interface3
	GE0/0/4 及以后的端口，根据服务器数量决定	服务器	服务器网卡接口
Extranet-2	XGE2/1/1	CORE-2	XGE2/2/0/6
	GE1/0/1	LB-6	Interface4
	GE1/0/3	FW-4	Interface5
	GE1/0/4	FW-3	Interface6
	GE1/0/5 及以后的端口，根据服务器数量决定	服务器	服务器网卡接口
AR-3	GE2/0/0	运营商网络 1	-
AR-4	GE2/0/0	运营商网络 2	-

配置思路

- 配置 Extranet 区接入交换机与数据中心核心交换机的互通
- 配置 Extranet 区接入交换机与 Extranet 区其他设备的网络互通
- 出口路由器 AR 与 Internet、AR 与下行设备之间的网络互通配置

操作步骤

1. 配置 Extranet 区接入交换机与数据中心核心交换机之间的互通

   具体配置请参见 2.1.1 Intranet 区配置。

2. 配置汇聚交换机各网段网关 IP

```
#
interface vlanif 2500
  ip address 10.254.0.1 12  //Vlan 3000 网关地址，其他接入接口配置相同
```

3. 配置区域接入交换机

   a. 配置接口允许通过的 VLAN

```
#
interface GigabitEthernet  1/0/0
    port link-type access
     port defaut vlan 2500 //Extranet 所属 vlan
其他接入接口配置相同，
```

   b. 配置接入交换机端口描述信息

```
#
```

```
interface xgigabitethernet 0/1/1
   description To Server A //根据实际客户要求格式配所联设备的设备名称及 IP 地址作为描述信息
```

4. 配置 LB 设备
   - Extranet 区域内服务器处在同一网段情况下，无特殊要求的情况下，服务器、交换机和 LB 之间可以进行二层互通。需要将服务器网关指向 LB 设备。
   - 若负载均衡的服务器不在同一网段，则服务器、交换机和 LB 之间需三层互通，将需要负载均衡的路由下一跳指向负载均衡设备。
5. 配置 FW 设备
   - 建议 FW 使用路由模式对外提供服务，通过启用 NAT 功能将内网地址转化为对提供服务器的私网地址
   - 建议 NAT 在防火墙出端口使能
6. AR 互通配置
   a. 配置与 FW 接口允许通过的 VLAN

```
#
interface Ethernet 0/0/1
 port link-type access
 port defaut vlan 2900 //Extrannet 所属 vlan，其他接入接口配置相同。注：AR 使用下行口与 FW 相连
#
interface vlanif 2900
 ip address 192.168.0.2 24//Vlan 2900 网关地址，其他配置类似
```

   b. 配置与运营商接口允许通过的 IP 及路由

说明

注：由于运营商提供的网络类型及 IP 等信息与实际组网有关，根据实际情况参考 AR 产品手册进行配置。

----结束

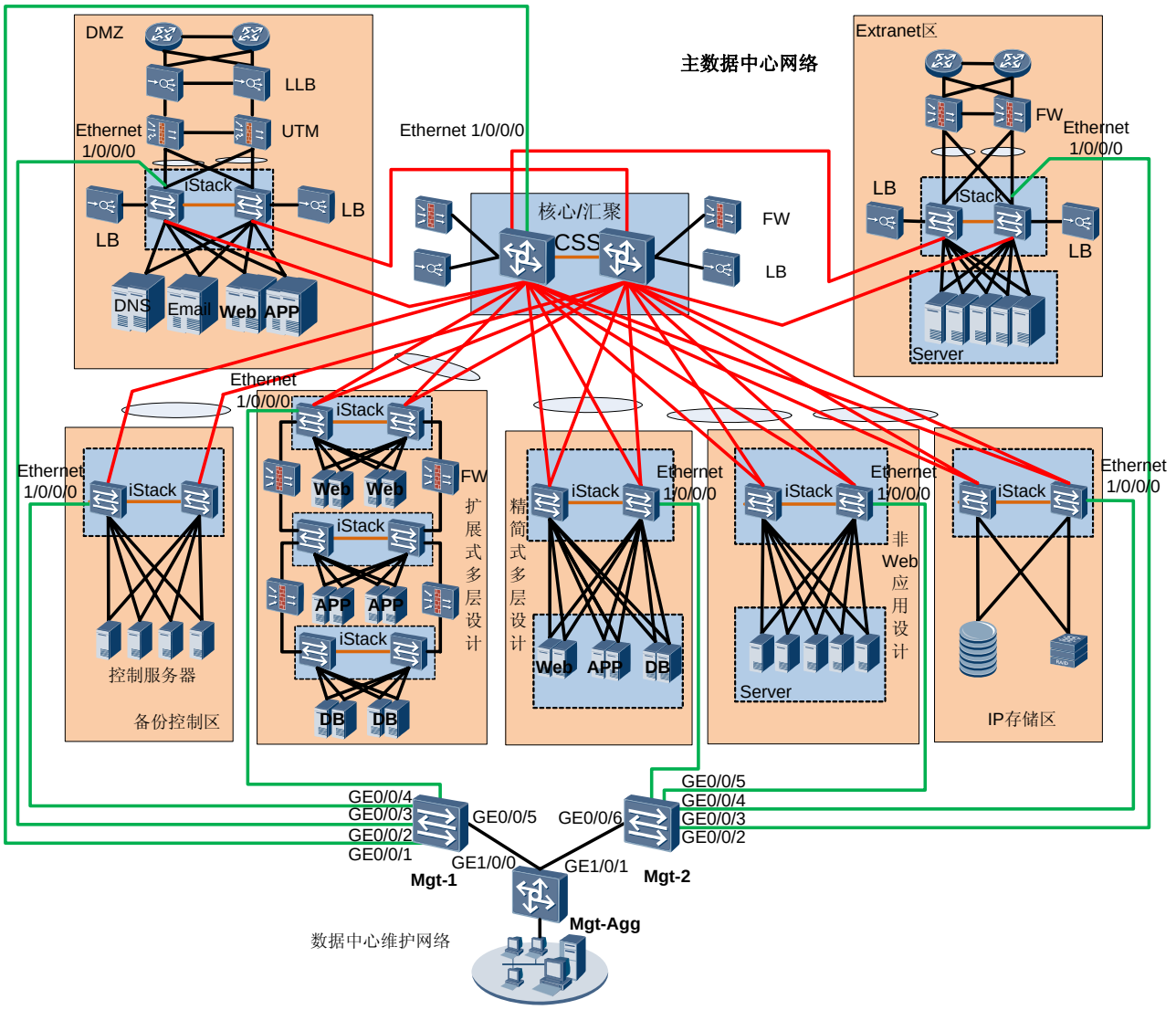
2.1.4 维护网络配置

典型组网

如图 2-4 所示是维护网络的典型配置组网图。

- 整个区域内部网络建议采用独立 IP 地址段且不对外发布路由
- 区域内部建议采用全二层组网

图2-4 维护网络典型配置组网



设备名称	接口编号	对接设备名称	接口编号
Mgt-Agg	GE1/0/0	Mgt-1	GE0/0/5
	GE1/0/1	Mgt-2	GE0/0/6
Mgt-1	GE0/0/1~GE0/0/5	被管理设备	网管接口
Mgt-2	GE0/0/1~GE0/0/6	被管理设备	网管接口

配置思路

- 维护网络接入交换机、核心/汇聚交换机的互联互通配置
  配置区域核心交换机

- 配置 VLAN 并将对应的接口加入 VLAN
- 配置接口 IP 地址及路由协议，实现维护管理网络内各节点的网络层互通
- 配置接口 IP 地址及路由协议，实现维护管理网络与外部网络互通，须根据实际情况按照规定的安全访问规则与配置最小的访问权限。

配置接入交换机

- 配置 VLAN 并将对应的接口加入 VLAN

- 在数据中心被管理网元设备，如接入交换机、核心/汇聚交换机配置管理 IP 及 SNMP 等网管参数
- 在网管设备上添加被管理网元设备

操作步骤

1. 配置区域核心交换机

   a. 配置互联接口允许通过的 VLAN

```
#
vlan batch 3000 3001 3099
#
interface GigabitEthernet  1/0/0
  port link-type trunk
  port trunk allow-pass vlan 3000 3001 3099 //允许维护区域不同设备的 VLAN 通过
```

   b. 配置汇聚交换机描述信息

   以 switch-1 上配置为例，其他互联端口接口的配置相同。

```
#
interface xgigabitethernet 0/1/1
  description To switch-2 GE-1/0/5 //根据实际客户要求格式配置，其他互联接口配置同上
```

   c. 配置汇聚交换机各网段网关 IP

```
#
interface vlanif 3000
  ip address 172.16.0.1 12  //Vlan 3000 网关地址
#
interface vlanif 3001
  ip address 172.17.0.1 12//Vlan 3001 网关地址，其他网段地址配置同上
```

2. 配置区域接入交换机

   a. 配置互联接口允许通过的 VLAN（配置同核心交换机）

   同步骤一中第一步配置

   b. 配置普通接口允许通过的 VLAN

```
#
interface GigabitEthernet  1/0/0
  port link-type access
  port defaut vlan 3000  //被管理设备所属 vlan，其他接入交换机普通接口配置相同
```

   c. 配置接入交换机端口描述信息

同步骤一中第二步配置，如所联的设备是非互联接口直接联被管理设备建议建议采用所联设备设备名称及 IP 地址作为描述信息。

3. 配置被管理设备的网元管理地址及 SNMP 网管参数

   a. 配置被管理设备的网元管理地址，

```
#
interface Ethernet1/0/0/0
 ip address 172.16.0.2 255.240.0.0
```

   说明
   S9300 堆叠管理网口主控为默认为 Eth1/0/0/0。华为公司其他设备类型配置类似。其他厂商的设备地址配置过程请以其厂商提供的配置为准。

   b. 配置被管理设备的网元管理 SNMP 参数

```
#
snmp-agent
  snmp-agent community read public
  snmp-agent community write private
  snmp-agent sys-info version all
```

   说明
   此处为华为公司设备 SNMP 简单配置，其他厂商的设备的配置过程请参考设备的用户手册。

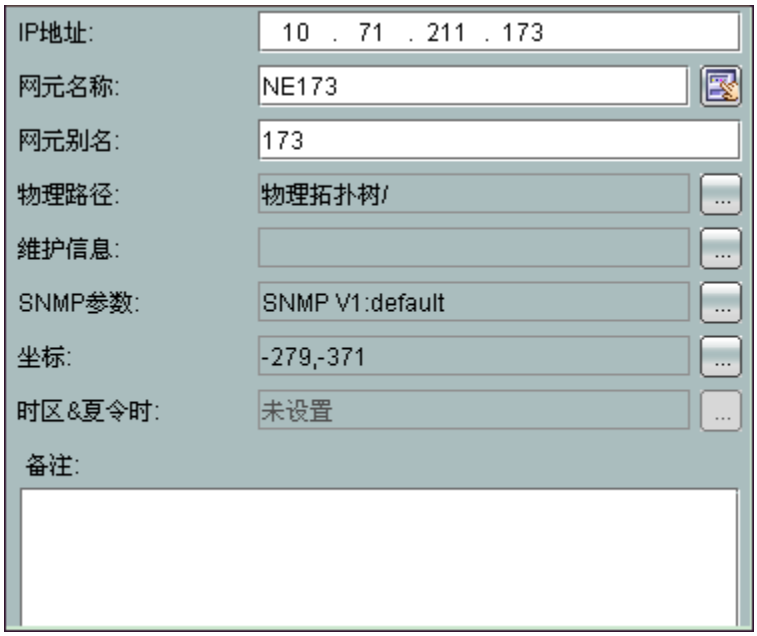
4. 添加被管理网元设备

   a. 在主拓扑图中单击右键，选择“新建 > 网元”。

   b. 在弹出的对话框左侧对象类型树中选择待创建网元的网元类型。

   c. 输入网元属性的取值信息。

   例如：增加 UPE-1，网元属性信息如下图所示。



单击“确定”。

----结束

2.2 不同用户接入数据中心时对网络的要求

说明

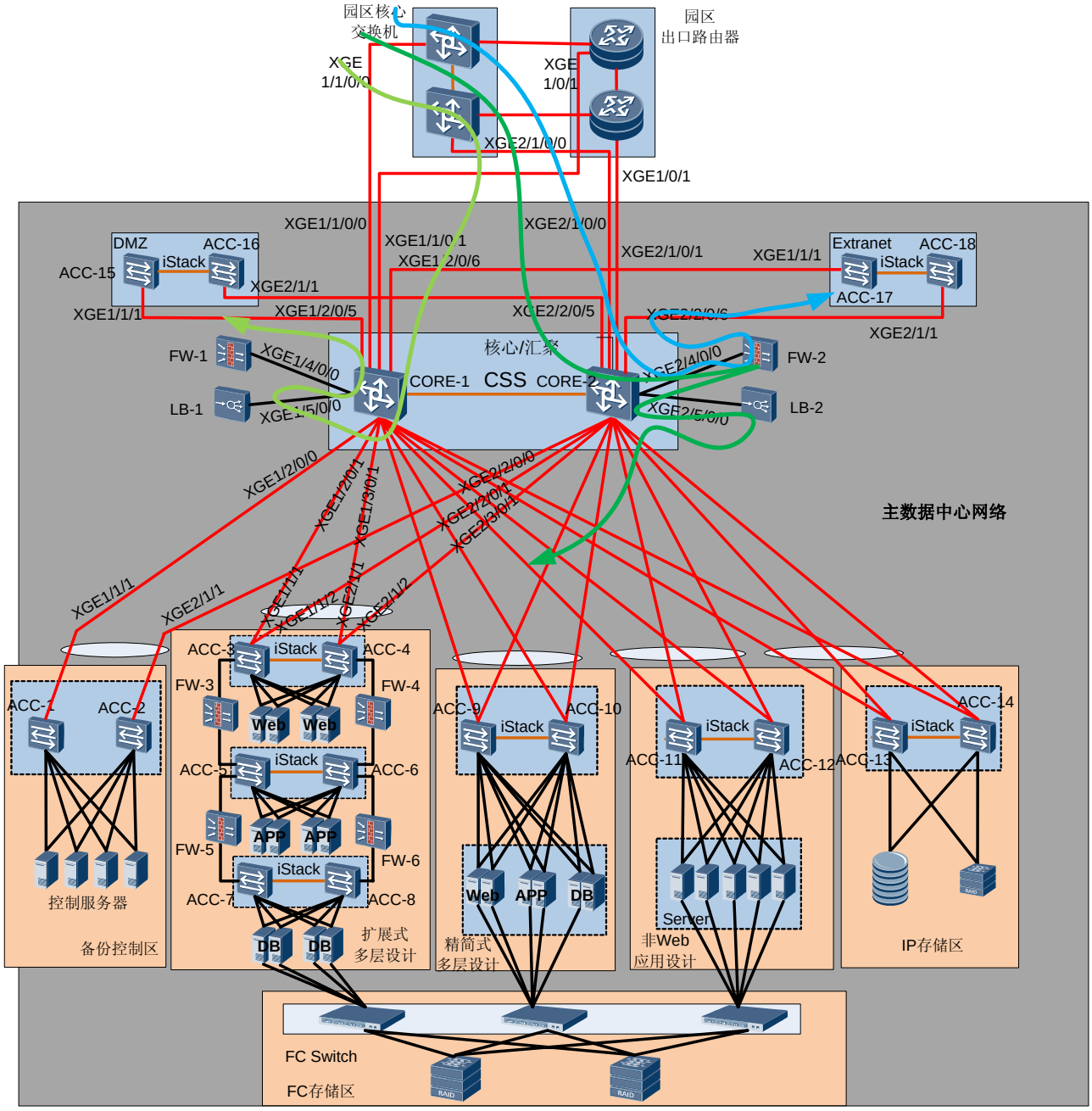
在基础网络配置完成以后，不同的用户接入到数据中心网络时对网络设备有不同的要求，本节主要介绍这些不同要求相关的配置。

2.2.1 企业内部园区用户接入数据中心对网络的要求

用户接入流程

- 企业内部用户园区用户通过企业园区核心交换机接入数据中心。
- 企业内部用户接入数据中心后，FW 根据用户不同权限授予必要的业务资源访问的权限。
- 企业内部用户接入数据中心后，在合理授权的情况下，可以访问如 Extranet 和 DMZ 区域服务器。

图2-5 企业内部园区用户接入数据中心网络示意图



对网络的要求

- 企业内部园区通过园区核心交换机访问数据中心。
- 在数据中心核心/汇聚交换机旁挂的防火墙上配置防火墙策略、在负载均衡设备上配置负载均衡策略，以提高对用户的业务交付能力。
  - 防火墙旁挂在核心/汇聚交换机上保证数据中心提供业务的能力，防止由于防火墙故障导致整个数据中心不能提供服务。
  - 防火墙对不同的用户提供不同权限，以访问不同的业务。

- 核心/汇聚交换机旁挂负载均衡设备，对海量用户访问的服务器进行负载均衡。

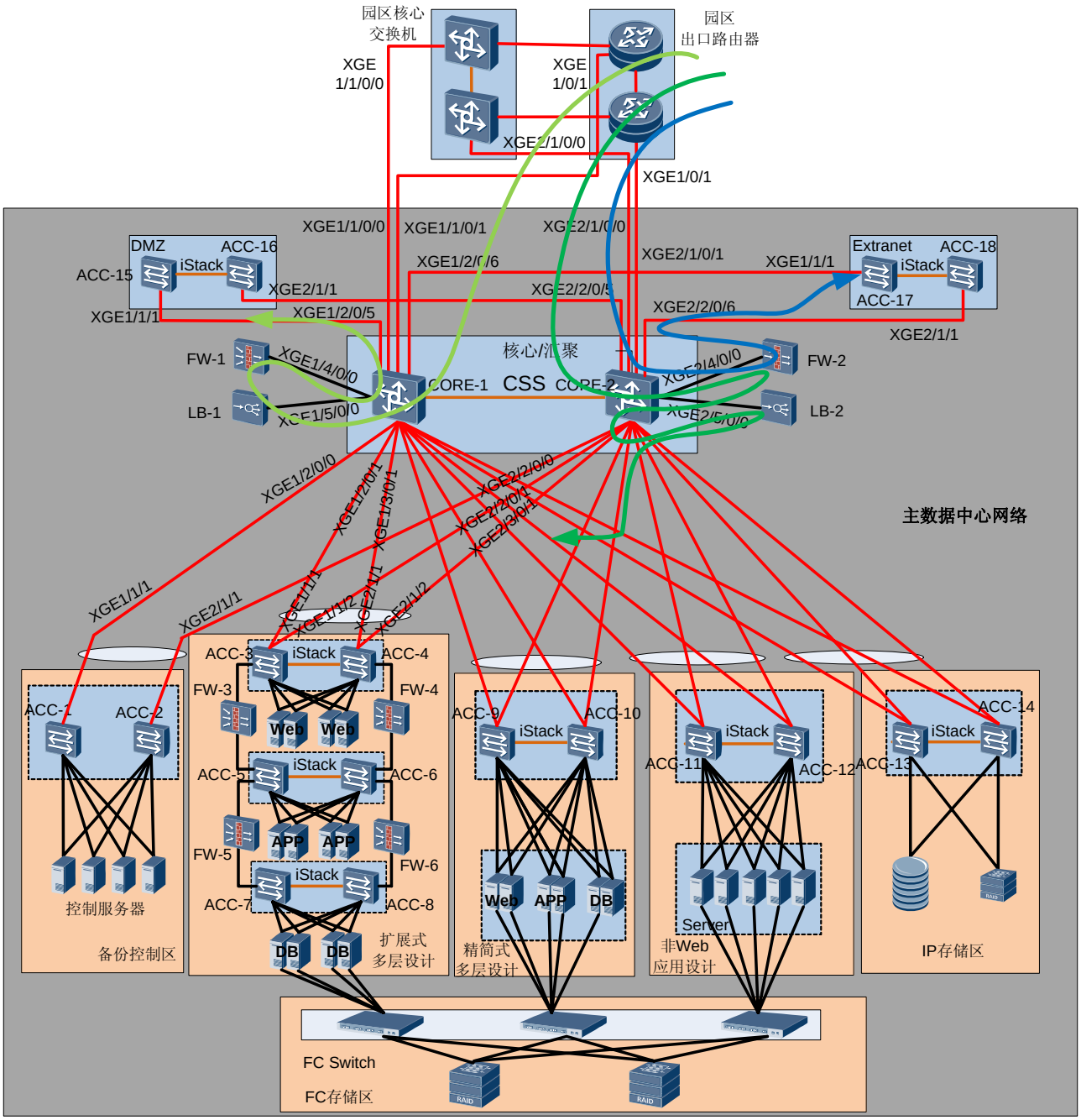
- 用户应只能访问 Intranet 区域内部对外提供资源的区域，不能访问后台资源。
- 用户如果需要访问 Internet 区域及企业合作伙伴资源应在合理授权的情况下，通过 DMZ 区域或 Extranet 区域访问。

2.2.2 企业网分支用户接入数据中心对网络的要求

用户接入流程

- 企业分支用户用户通过企业园区出口路由器接入数据中心。
- 企业分支用户接入数据中心后，FW 根据用户不同权限授予必要的业务资源访问的权限。
- 企业分支用户接入数据中心后，在合理授权的情况下，可以访问如 Extranet 和 DMZ 区域服务器。

图2-6 企业内部园区用户接入数据中心网络示意图



对网络的要求

- 企业分支用户通过园区出口路由器通过三层访问数据中心。
- 在数据中心核心/汇聚交换机旁挂的防火墙上配置防火墙策略、在负载均衡设备上配置负载均衡策略，以提高对用户的业务交付能力。
  - 防火墙旁挂在核心/汇聚交换机上保证数据中心提供业务的能力，防止由于防火墙故障导致整个数据中心不能提供服务。
  - 防火墙对不同的用户提供不同权限，以访问不同的业务。

- 核心/汇聚交换机旁挂负载均衡设备，对海量用户访问的服务器进行负载均衡。

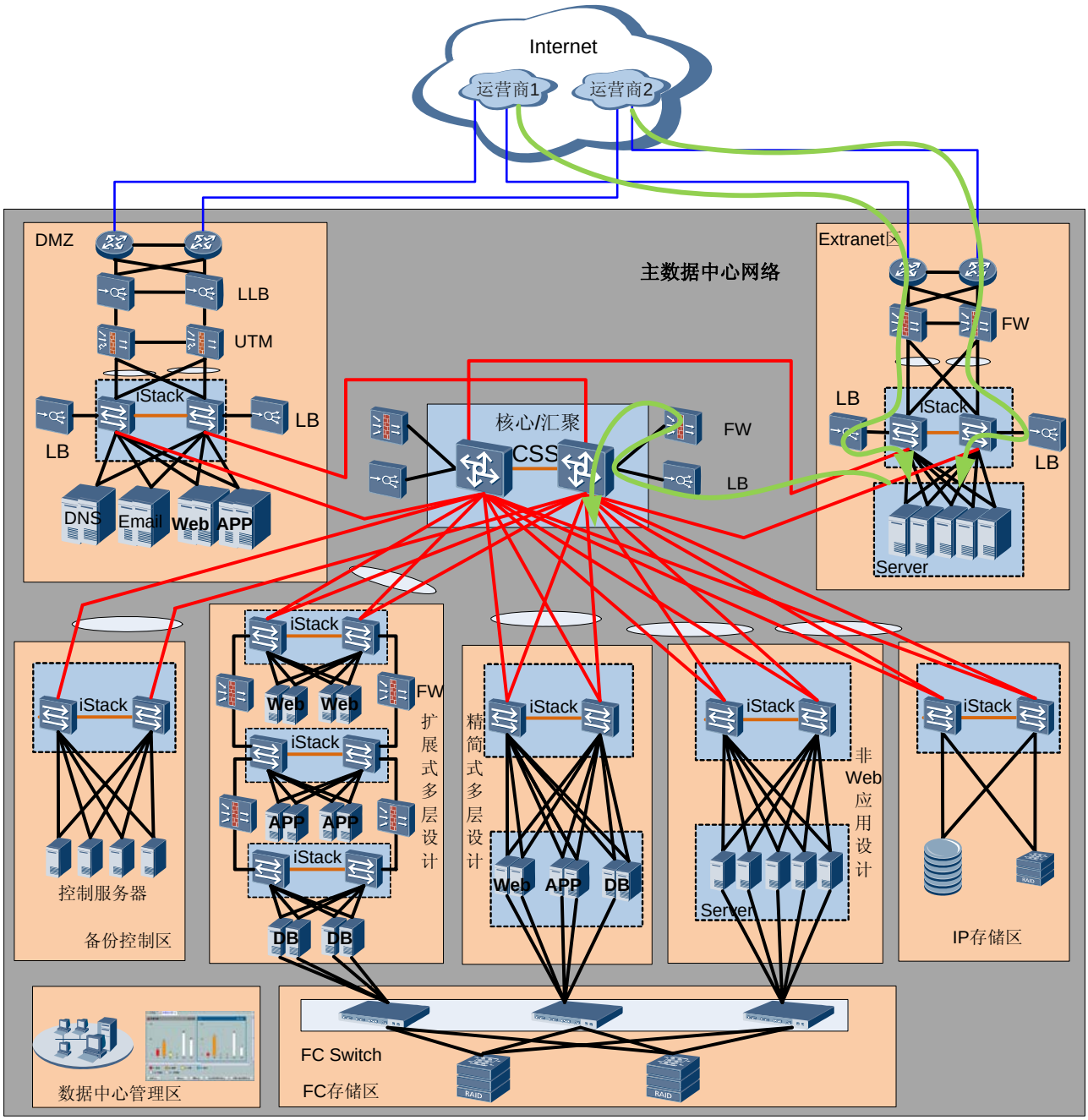
- 用户应只能访问 Intranet 区域内部对外提供资源的区域，不能访问后台资源。
- 用户如果需要访问 Internet 区域及企业合作伙伴资源应在合理授权的情况下，通过 DMZ 区域或 Extranet 区域访问。

2.2.3 企业合作伙伴接入数据中心对网络的要求

用户接入流程

- 企业合作伙伴由于业务需要通过 Extranet 区域以非 Internet 链路接入数据中心。
- 考虑到安全须在隐藏内网环境的情况下对企业合作伙伴提供服务。Extranet NAT 方隐藏己方网络资源，并应为每个用户授予最小的访问权限。
- 企业合作伙伴应被授予最小的访问权限且只能访问 Extranet 区域内资源。
- Extranet 服务器根据实际情况被授予最小的权限访问其他区域。

图2-7 企业合作伙伴接入数据中心网络示意图



对网络的要求

说明

因 LB 和防火墙不是华为公司设备，所以无法提供详细的配置脚本，请根据以下对这些网络设备的要求和具体产品的配置手册进行相关配置。

Extranet 区以及 Extranet 区与其他区域的网络连通性配置已经完成，具体配置请见 2.1.3 Extranet 区配置。

根据企业合作伙伴用户通过 Extranet 接入数据中心网络的方式，对数据中心网络设备的需求如下：

- 通过边缘路由器接入合作伙伴线路，根据实际链路类型及运营商提供的参数配置进行相关联通性配置。
- 为了保证 Extranet 互联区域的可靠性，所有设备均需要成对部署，即：两台路由器，两台链路负载均衡设备，两台防火墙。
- 主数据中心核心/汇聚交换机旁挂的防火墙配置策略以限制外部用户访问主数据中心网络。
- 在合理的授权的情况，允许合作伙伴用户访问主数据中心。
- 限制 Extranet 服务器有最小的授权权限访问其他数据中心数据。

2.2.4 企业外部用户通过 Internet 接入数据中心对网络的要求

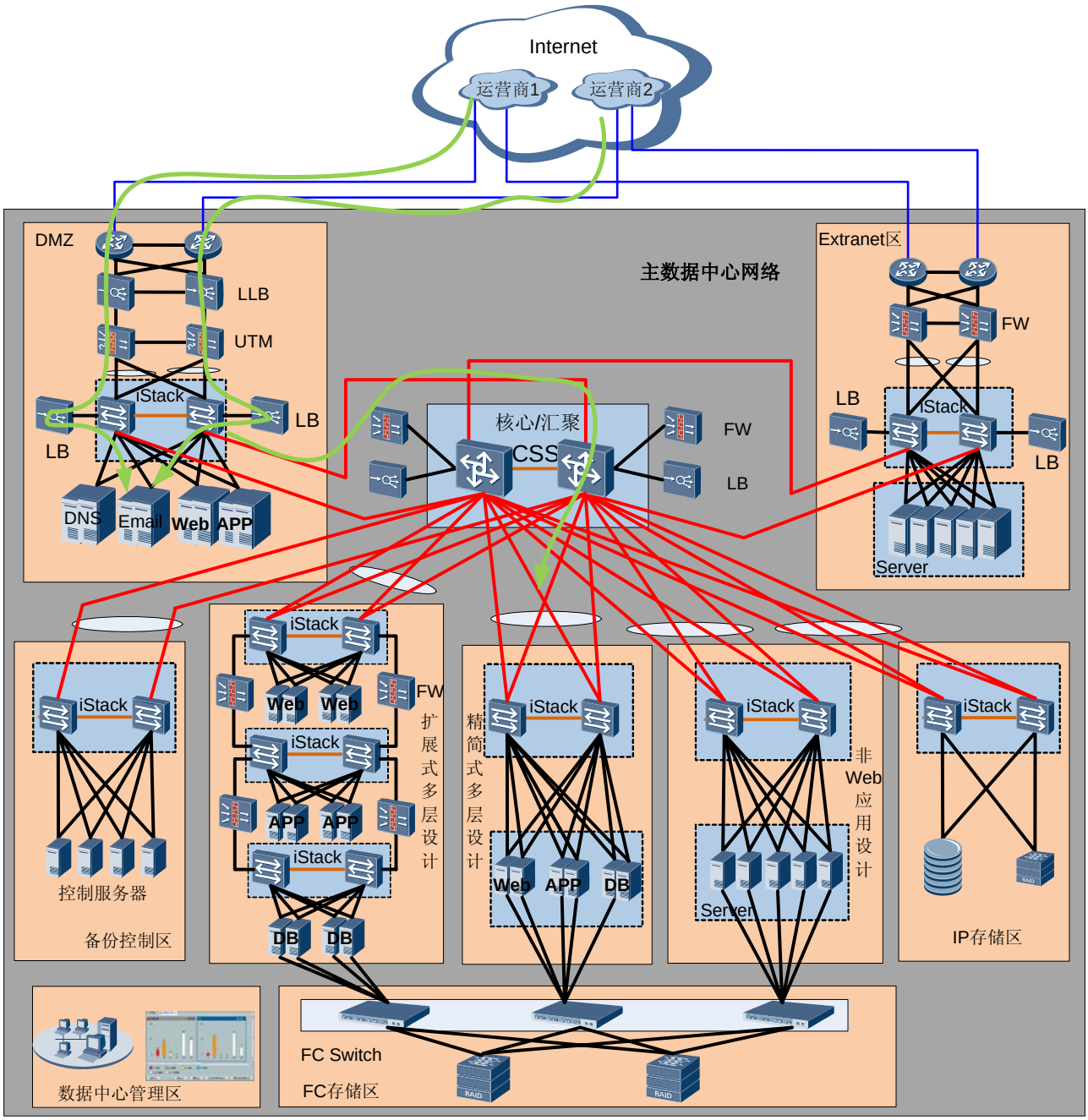
用户接入流程

如图 2-8 所示，企业外部用户分为本企业的出差员工、非本企业的外部用户，他们均通过 Internet 接入到数据中心的 DMZ 区：

- 本企业的出差员工以 SSL VPN 方式接入 DMZ 区，SSL 用户可以被授予独立 DMZ 网络 IP 或通过 NAT 方式访问授权的 DMZ 网络资源，并通过 DMZ 在被授权的情况下接入到主数据中心中。可以在服务器区部署单独的 SSL VPN 设备，也可以采用 UTM 设备统一接入。
- 非本企业的外部用户通过 Internet 接入 DMZ 区，使用 DMZ 区提供的服务，该部分用户不能访问主数据中心网络。

另外，有些企业的小型分支机构，在不租用 VPN 专线的情况下，可以用过 IPSec VPN 方式接入到 DMZ，使用 DMZ 区提供的服务，并通过 DMZ 接入到主数据中心中。可以在服务器区部署单独的 IPSec VPN 设备，也可以采用 UTM 设备统一接入。

图2-8 企业外部用户接入数据中心网络示意图



对网络的要求

说明

因 LLB、UTM 和防火墙不是华为公司设备，所以无法提供详细的配置脚本，请根据以下对这些网络设备的要求和具体产品的配置手册进行相关配置。

DMZ 区以及 DMZ 区与其他区域的网络连通性配置已经完成，具体配置请见 2.1.2 DMZ 区配置。

根据用户通过 Internet 接入数据中心网络的方式，对数据中心网络设备的需求如下：

- 当数据中心租用了两个运营商出口时，需要部署链路负载均衡 LLB 设备对来自不同运营商的请求从相应出口回应。在只有一个运营商出口时不需要部署。
- UTM 至少要包括防火墙和入侵检测系统 IPS（ Intrusion Detection System）两项功能。如果没有部署单独的 SSL VPN 和 IPSec VPN 设备，那么 UTM 还需要具有 SSL VPN 和 IPSec VPN 网关的功能。
  - IPS：对掺杂在应用数据流中的恶意代码、攻击行为、DDOS 攻击等进行侦测，并实时进行响应。
  - 防火墙：在网络层面，过滤非法流量，抵御外部的攻击，只允许合法的用户接入 DMZ。保护内部资源。
  - 防火墙和 IPS 本身都是重要的网络设备，而且其位置一般都是作为网络的出口。其位置和功能决定了防火墙和 IPS 设备应该具有非常高的可靠性。
- 为了保证 Internet 互联区域的可靠性，所有设备均需要成对部署，即：两台路由器，两台链路负载均衡设备，两台 UTM（至少含防火墙和 IPS）。
- 主数据中心核心/汇聚交换机旁挂的防火墙配置策略以限制非本企业的外部用户访问主数据中心网络。
- 本企业的内部用户在合理授权的情况下，可以访问主数据中心。
- 限制 DMZ 服务器有最小的授权权限访问其他数据中心数据。