神州云科 Yunke China | DCN

DCFW-1800E-X 系列下一代防火墙

命令手册

---201902

目录

第 1 章 系统管理 1-15
1.1 系统概述 1-15
1.1.1 命令行特性 1-15
1.1.2 语法帮助 1-15
1.1.3 使用语法帮助补齐命令 1-16
1.1.4 命令简写 1-16
1.1.5 命令模式 1-16
1.1.6 常用命令介绍 1-17
1.2 实现系统配置的途径 1-17
1.2.1 通过串口实现系统配置 1-17
1.2.2 通过 Telnet 实现系统配置 1-18
1.2.3 通过 SSH 方式实现系统配置 1-18
1.3 系统文件管理 1-18
1.3.1 copy 命令使用 1-18
1.3.2 保存配置文件 1-19
1.3.3 多配置文件 1-19
1.3.4 配置文件的上传与下载 1-19
1.3.5 系统升级 1-20
1.4 常用系统管理命令 1-20
1.4.1 开启、关闭 Telnet 服务 1-20
1.4.2 开启、关闭 SSH 服务 1-20
1.4.3 查看谁在系统上 1-20
1.4.4 清除登录用户 1-20
1.4.5 查看系统的版本 1-20
第 2 章 配置接口 2-22
2.1 配置以太网端口 2-22
2.1.1 以太网端口概述 2-22
2.1.2 配置以太网端口 2-22
2.1.3 配置案例 2-27
2.1.4 以太网端口监控与维护 2-27
2.1.5 故障分析 2-28
2.2 配置 VLAN 接口 2-28
2.2.1 VLAN 概述 2-29
2.2.2 配置接口封装的链路层协议为 VLAN 2-29
2.2.3 配置信息的显示 2-29
VLAN 配置信息显示命令: 2-29
2.2.4 配置案例 2-29
2.2.5 故障分析 2-30
2.3 配置透明网桥（vlan 透传） 2-30
2.3.1 透明网桥概述 2-30
2.3.2 配置透明网桥 2-31
2.3.3 配置网桥 STP 2-31

2.3.4 配置案例 2-32
2.3.5 透明网桥监控与维护 2-33
2.3.6 常见故障分析 2-34
2.4 配置链路聚合 Trunk 接口 2-34
2.4.1 链路聚合 Trunk 概述 2-34
2.4.2 配置链路聚合 Trunk 接口 2-34
2.4.3 配置案例 2-36
2.4.4 常见故障分析 2-37
2.5 配置 PPPoE 接口 2-37
2.5.1 PPPoE 概述 2-37
2.5.2 配置 PPPoE 接口 2-37
2.5.3 配置案例 2-38
2.6 配置 DHCP 接口 2-38
2.6.1 DHCP 概述 2-38
2.6.2 配置 DHCP 接口 2-38
2.6.3 配置案例 2-38
2.7 配置旁路接口 2-39
2.7.1 旁路工作模式概述 2-39
2.7.2 配置旁路接口 2-39
2.8 配置 gre 接口 2-40
2.8.1 gre 接口概述 2-40
2.8.2 配置 gre 接口 2-40
2.8.3 配置案例 2-40
第 3 章 配置安全域 3-42
3.1 安全域概述 3-42
3.2 配置向域中添加接口 3-42
3.3 配置区域内接口互访 3-42
3.4 配置案例 3-42
3.4.1 配置案例: 添加接口到域中 3-42
3.5 安全域监控与维护 3-43
3.5.1 查看域信息 3-43
3.6 常见故障分析 3-43
3.6.1 故障现象： 3-43
第 4 章 配置 IPv6 4-44
4.1 IPv6 概述 4-44
4.1.1 IPv6 协议特点 4-44
4.1.2 IPv6 地址介绍 4-45
IPv6 地址表示方式 4-45
IPv6 的地址分类 4-46
FF02:0:0:0:0:1:FFXX:XXXX 4-47
IEEE EUI-64 格式的接口标识符 4-47
图 4-2 MAC 地址到 EUI-64 格式的接口标识符的转换过程 4-47
4.1.3 IPv6 邻居发现协议介绍 4-47
4.1.4 IPv6PMTU 发现 4-50
图 4-5 PMTU 发现的工作过程 4-50

4.1.5 IPv6 过渡技术简介 4-51
4.1.6 IPv6 隧道技术简介 4-52
IPv6 in iPv4 隧道原理 4-52
IPv6 in IPv4 隧道模式 4-53
ISATAP 隧道 4-53
4.2 配置 IPv6 4-54
4.2.1 配置 IPv6 单播地址 4-54
4.2.2 配置 IPv6 邻居发现协议 4-55
4.2.3 配置 IPv6 静态路由 58
4.2.4 配置 IPv6 策略路由 58
4.2.5 配置 IPv6 管理设备 59
4.2.6 配置 IPv6 包过滤 59
4.2.7 配置 IPv6 扩展头过滤 60
4.2.8 配置 IPv6-MAC 绑定 60
4.2.9 配置 DNSv6 服务器 61
4.2.10 配置 DHCPv6 服务器 61
4.2.11 配置 IPv4/IPv6 双协议栈 62
4.2.12 配置 IPv6 手动隧道 62
4.2.13 配置 IPv6 6to4 隧道 63
4.2.14 配置 IPv6 ISATAP 隧道 63
4.3 配置案例 64
4.3.1 配置案例 1：基本 IPv6 手动隧道 64
4.4 IPv6 监控与维护 66
4.4.1 查看 IPv6 隧道 66
4.4.2 常见故障分析 66
第 5 章 配置 IPSec VPN 68
5.1 IPSec VPN 概述 68
5.2 配置 IPSec VPN 69
5.2.1 缺省配置信息 69
5.2.2 配置 IKE 阶段 1 70
5.2.3 配置 IKE 阶段 2 74
5.2.4 手工配置 IPsec 安全策略 76
5.3 配置案例 77
5.3.1 配置案例： 77
5.4 IPSec VPN 监控与维护 78
5.4.1 显示一阶段 SA 78
5.4.2 显示二阶段 SA 78
5.4.3 清除一阶段 SA 79
5.4.4 清除二阶段 SA 79
5.4.5 常见故障分析 79
第 6 章 配置 NAT 80
6.1 NAT 概述 80
6.2 配置 NAT 81
6.2.1 配置地址池(NAT POOL) 81
6.2.2 配置 static NAT 81

6.2.3 配置 source NAT 82
6.2.4 配置 destination NAT.....82
6.2.5 配置 destination NAT 自动映射 83
6.3 端口管理 84
6.3.1 设置服务端口号 84
第 7 章 配置 DHCP 服务器.....86
7.1 DHCP 服务概述.....86
7.1.1 DHCP 服务器概述 86
7.1.2 DHCP Relay 概述.....86
7.2 配置 DHCP Server.....87
7.2.1 在接口上指定 DHCP Server 服务.....87
7.2.2 配置 DHCP Server 服务子网 87
7.2.3 配置 DHCP Server 地址池及其租约 87
7.2.4 配置 DHCP 子网缺省网关 88
7.2.5 配置 DHCP 子网 DNS 服务器.....88
7.2.6 配置 DHCP 子网 WINS 服务器.....88
7.2.7 配置 DHCP 子网域名.....88
7.2.8 配置 DHCP 地址绑定.....88
7.2.9 配置 DHCP 地址排除.....89
7.3 DHCP 服务监控.....89
7.3.1 DHCP Debug 89
7.3.2 显示 DHCP Server 配置信息.....89
7.3.3 显示 DHCP Server 地址分配信息.....90
7.4 配置案例 91
第 8 章 配置对象 93
8.1 配置绝对时间和周期时间.....93
8.1.1 绝对时间和周期时间概述.....93
8.1.2 配置在绝对时间中配置有效时间范围 93
8.1.3 配置在周期时间中配置有效时间范围 94
8.1.4 配置在周期时间中配置有效时间段.....94
8.1.5 配置案例 96
8.1.6 配置案例:配置时间表.....96
8.1.7 绝对时间与周期时间监控与维护.....96
8.1.8 查看周期表与绝对时间 96
8.1.9 常见故障分析.....97
8.1.10 故障现象 1： 97
8.2 配置服务对象和服务对象组 97
8.2.1 服务对象和服务对象组概述.....97
8.2.2 配置服务对象和服务对象组.....97
8.2.3 配置向服务对象中添加 TCP|UDP 服务 97
8.2.4 配置向服务对象中添加 ICMP 服务 98
8.2.5 配置向服务对象组中添加服务对象 99
8.2.6 配置案例 99
8.2.7 配置案例 1: 添加服务对象与服务对象组.....99
8.2.8 配置案例 2:配置服务对象 100

8.2.9 服务对象与服务对象组监控与维护 101
8.2.10 查看服务对象 101
8.2.11 查看服务对象组 101
8.2.12 常见故障分析 101
8.2.13 故障现象 1： 101
8.3 配置地址对象和地址对象组 102
8.3.1 地址对象和地址对象组概述 102
8.3.2 配置地址对象和地址对象组 102
8.3.3 配置向地址对象中添加单个地址 102
8.3.4 配置向地址对象中添加网络掩码 103
8.3.5 配置向对象地址中添加地址范围 103
8.3.6 配置向地址对象组中添加地址对象 104
8.3.7 配置案例 104
8.3.8 配置案例：添加地址对象与地址对象组 104
8.3.9 地址对象与地址对象组监控与维护 105
8.3.10 查看地址对象 105
8.3.11 查看地址对象组 106
8.3.12 常见故障分析 106
8.3.13 故障现象 1： 106
8.4 配置应用对象和应用对象组 106
8.4.1 应用对象、应用分类、应用对象组概述 106
8.4.2 配置应用对象组 106
8.4.3 配置案例 107
8.5 配置关键字对象 108
8.5.1 关键字对象概述 108
8.5.2 配置关键字对象组 108
8.5.3 配置案例 108
8.6 配置健康检查对象 109
8.6.1 健康检查概述 109
8.6.2 配置健康检查对象 109
8.6.3 配置健康检查组 110
第 9 章 配置静态路由 112
9.1 静态路由概述 112
9.2 配置静态路由 112
9.3 配置缺省路由 112
9.4 多路径选择 113
9.5 配置信息显示命令 113
9.6 配置案例 113
9.6.1 配置缺省路由 113
9.7 常见故障 114
9.7.1 数据包转发不正常 114
第 10 章 配置策略路由 115
10.1 策略路由概述 115
10.2 配置策略路由 115
10.2.1 策略路由配置 115

10.2.2 调整策略路由的顺序 115
10.2.3 多路径选择 116
10.3 常见故障分析 116
10.3.1 故障现象： 116
第 11 章 配置 RIP 117
11.1 RIP 协议概述 117
11.2 配置 RIP 117
11.2.1 缺省配置信息 117
11.2.2 配置启用 RIP 路由协议功能 118
11.2.3 配置 RIP 版本 118
11.2.4 配置 RIP 发布的网络 119
11.2.5 配置 RIP 发布缺省路由 119
11.2.6 配置 RIP 默认的重发布度量 120
11.2.7 配置 RIP 定时器触发时间 120
11.2.8 配置 RIP 定时器触发时间 121
11.2.9 配置 RIP 接口收发报文版本 122
11.2.10 配置 RIP 接口的认证类型 122
11.3 RIP 监控与维护 123
11.3.1 查看 RIP 路由表 123
11.3.2 查看 RIP 配置 123
11.3.3 查看调试信息 124
11.4 常见故障分析 125
11.4.1 故障现象：两台设备不能正常通信 125
第 12 章 配置 OSPF 126
12.1 OSPF 协议概述 126
12.2 配置 OSPF 126
12.2.1 缺省配置信息 126
12.2.2 配置启用 OSPF 路由协议功能 127
12.2.3 配置 OSPF 路由器 Router-ID 128
12.2.4 配置运行 OSPF 的接口 128
12.2.5 配置 OSPF 区域认证方式 129
12.2.6 配置 OSPF NSSA 130
12.2.7 配置 OSPF 区域间路由聚合 131
12.2.8 配置 OSPF 路由重分布 132
12.2.9 配置 OSPF 重发布路由缺省 Metric 133
12.2.10 配置 OSPF 重发布默认路由 134
12.2.11 配置 OSPF 协议优先级 135
12.2.12 配置 OSPF 兼容 RFC1583 136
12.2.13 配置 OSPF 路由计算定时器 136
12.2.14 配置 OSPF 接口认证方式 137
12.2.15 配置 OSPF 接口明文认证密钥 137
12.2.16 配置 OSPF 接口密文认证密钥 138
12.2.17 配置 OSPF 接口的优先级 139
12.2.18 配置 OSPF 接口发送报文的开销 139
12.2.19 配置 OSPF 接口 LSA 重传间隔 140

12.2.20 配置 OSPF 接口 LSA 发送延迟 141
12.2.21 配置 OSPF 接口 Hello 报文定时器 141
12.2.22 配置 OSPF 接口邻居失效定时器 142
12.2.23 配置接口的 OSPF 网络类型 142
12.3 常见故障分析 143
12.3.1 故障现象 1：两台设备不能建立邻接关系 143
第 13 章 配置 BGP 145
13.1 BGP 协议概述 145
13.2 配置 BGP 146
13.2.1 缺省配置信息 146
13.2.2 配置启用 BGP 路由协议功能 147
13.2.3 配置 BGP 路由器 Router-ID 148
13.2.4 配置指定 BGP 对等体 148
13.2.5 配置 BGP 对等体组 149
13.2.6 配置回环接口作为 BGP 邻居 150
13.2.7 EBGP 多跳配置 150
13.2.8 配置删除私有 AS 号 151
13.2.9 配置允许发送团体属性 151
13.2.10 配置限制接收的路由数量 152
13.2.11 配置保留对等体路由信息 153
13.2.12 配置关闭对等体 153
13.2.13 配置 IGP 和 BGP 路由交互 154
13.2.14 配置重发布 IGP 路由到 BGP 155
13.2.15 配置 BGP 的定时器 155
13.2.16 配置 MED 属性 156
13.2.17 配置 LOCAL_PREF 属性 158
13.2.18 配置比较 router-id 158
13.2.19 配置 BGP 聚合路由 159
13.3 常见故障分析 160
13.3.1 故障现象 1：两台设备不能建立邻接关系 160
第 14 章 配置防火墙策略 161
14.1 防火墙策略概述 161
14.2 配置防火墙策略 161
14.2.1 防火墙策略添加和删除 161
14.2.2 防火墙策略添加 161
14.2.3 防火墙策略删除 162
14.2.4 基于策略的老化时间的修改 162
14.2.5 流镜像功能 163
14.2.6 使能和禁用 163
14.3 配置案例 163
第 15 章 配置用户策略 165
15.1 用户策略概述 165
15.2 配置用户策略 165
15.3 配置案例 166
第 16 章 配置 Web 访问策略 167

16.1 Web 访问策略概述.....167
16.2 配置 Web 访问策略.....167
16.3 配置自定义 URL 类.....168
16.4 配置案例.....168
第 17 章 配置应用审计策略.....170
17.1 应用审计策略概述.....170
17.2 配置应用审计策略.....170
17.3 配置案例.....171
第 18 章 配置控制策略.....172
18.1 控制策略概述.....172
18.2 配置控制策略.....172
18.3 配置案例.....173
第 19 章 应用策略白名单.....175
19.1 白名单概述.....175
19.2 配置白名单.....175
19.3 配置案例.....175
第 20 章 配置入侵防护策略.....177
20.1 入侵防御策略概述.....177
20.2 配置入侵防御策略.....177
20.2.1 配置入侵防护事件集.....177
20.2.2 入侵防护策略.....178
20.2.3 设备联动.....178
20.2.4 日志合并.....179
20.3 配置案例.....179
第 21 章 配置防病毒策略.....181
21.1 防病毒策略概述.....181
21.2 配置防病毒策略.....181
21.2.1 防病毒策略添加.....181
21.2.2 防病毒策略修改.....182
21.2.3 防病毒策略删除.....182
21.3 配置案例.....183
第 22 章 协议管理.....184
22.1 协议管理概述.....184
22.2 配置协议管理.....184
22.3 配置案例.....184
第 23 章 配置流量控制策略.....185
23.1 流量管理概述.....185
23.2 配置流量管理.....185
23.2.1 配置线路绑定接口.....185
23.2.2 配置通道关联线路.....186
23.2.3 配置排除策略.....187
23.2.4 显示 qos 配置及限速状态.....187
23.3 配置案例.....187
第 24 章 配置认证用户.....189
24.1 认证用户设置概述.....189

24.2 配置认证用户 189
24.2.1 配置本地管理员用户 190
24.2.2 配置 RADIUS 管理员用户 190
24.2.3 配置 LDAP 管理员用户 191
24.2.4 配置本地接入用户 191
24.3 配置 RADIUS 服务器支持 192
24.3.1 配置 RADIUS 服务器 192
24.4 配置 LDAP 服务器支持 192
24.4.1 配置 LDAP 服务器 192
24.5 配置 portal server 支持 193
24.5.1 配置 Portal Server 193
24.6 配置用户组 193
24.6.1 配置用户组 193
24.6.2 配置用户加入用户组 194
24.7 配置案例 194
24.7.1 配置案例 1：本地用户认证 194
24.8 认证用户监控与维护 195
24.8.1 查看接入用户信息 195
24.8.2 查看用户组信息 195
24.8.3 查看 RADIUS 服务器信息 196
24.8.4 查看 LDAP 服务器信息 196
24.8.5 查看用户验证和登陆的过程 196
24.9 常见故障分析 197
24.9.1 故障现象 1：认证用户认证失败 197
第 25 章 配置防 DOS 攻击 198
25.1 防 DOS 攻击概述 198
25.2 配置防 DOS 攻击 198
25.2.1 缺省配置 198
25.2.2 配置防 ping-of-death 攻击功能 198
25.2.3 配置防 tear-drop 攻击功能 199
25.2.4 配置防 jolt2 攻击功能 199
25.2.5 配置防 land-base 攻击功能 199
25.2.6 配置防 winnuke 攻击功能 200
25.2.7 配置防 syn-flag 攻击功能 200
25.2.8 配置防 smurf 攻击 200
25.2.9 配 Flood 防御 201
Ipv4 flood 防御配置步骤 201
Ipv6 flood 防御配置步骤 201
25.2.10 配置智能 TCP Flood 防御 202
25.3 防 DOS 攻击的监控与维护 202
25.3.1 查看配置信息 202
25.3.2 查看系统当前的 TCP 半连接数 203
25.3.3 查看防 DOS 攻击的 debug 信息 204
25.4 常见故障分析 204
25.4.1 TCP Flood 攻击防御失效 204

第 26 章 配置防扫描.....205
26.1 防扫描概述.....205
26.2 配置防扫描.....205
26.2.1 缺省配置信息.....205
26.2.2 配置防 TCP Scan.....205
26.2.3 配置防 UDP Scan.....206
26.2.4 配置防 Ping sweep.....206
26.2.5 配置扫描识别门限.....207
26.2.6 配置对源主机的阻断时间.....207
26.3 配置案例.....207
26.3.1 配置防扫描.....208
26.4 防扫描监控与维护.....208
26.4.1 查看防扫描配置.....208
26.5 常见故障分析.....209
26.5.1 配置防扫描后没有报警，没有拒包.....209
第 27 章 配置 IP-MAC 绑定.....210
27.1 IP-MAC 绑定概述.....210
27.2 配置 IP-MAC 绑定.....210
27.2.1 配置 IP-MAC 绑定.....210
27.2.2 查看 ARP 列表.....210
27.2.3 清除 ARP 列表.....211
27.3 配置案例.....211
第 28 章 配置 PKI.....212
28.1 PKI 协议概述.....212
28.2 配置 PKI.....212
28.2.1 本地证书的导出.....212
28.2.2 本地生成证书请求的证书导入.....213
28.2.3 PKCS12 格式证书的导入.....213
28.2.4 证书私钥文件的导入.....214
28.2.5 CA 证书的导出.....214
28.2.6 CA 证书的导入.....215
28.2.7 CRL 的导出.....215
28.2.8 CRL 导入.....216
第 29 章 配置 PKI CA.....217
29.1 PKI 协议概述.....217
29.2 配置 PKI CA.....217
29.2.1 生成 CA 证书.....217
29.2.2 配置证书请求信息－位置.....217
29.2.3 配置证书请求信息－国家或地区.....218
29.2.4 配置证书请求信息－组织.....218
29.2.5 配置证书请求信息－州/省.....219
29.2.6 配置证书请求信息－部门.....219
29.2.7 配置证书请求信息－EMAIL.....219
29.2.8 配置证书请求信息－密钥长度.....220
29.2.9 配置证书请求信息－有效期.....220

29.2.10 CA 证书的导出 220
29.2.11 CA 证书导入 221
29.2.12 CRL 的更新 222
29.2.13 CRL 的导出 222
29.2.14 生成用户证书请求信息 223
29.2.15 签发用户证书请求 223
29.2.16 导出用户证书 224
29.3 常见故障分析 224
第 30 章 配置高可用性（HA） 225
30.1 HA 概述 225
30.2 配置 HA 225
30.2.1 HA 配置 225
30.2.2 配置同步配置 226
30.2.3 连接同步配置 226
30.2.4 接口联动配置 227
30.2.5 配置故障检测 227
30.3 配置案例 228
第 31 章 配置 VRRP 229
31.1 VRRP 概述 229
31.2 配置 VRRP 229
31.3 配置案例 236
31.4 监控与维护 236
31.4.1 查看 VRRP 配置 236
31.5 故障分析 237
31.5.1 故障现象 1： 237
第 32 章 配置系统日志 238
32.1 配置系统日志概述 238
32.2 配置系统日志 238
32.2.1 缺省配置信息 238
32.2.2 配置本地日志 238
32.2.3 配置模块发送日志到本地日志 238
32.2.4 配置在线用户查询、冻结 239
32.2.5 清除本地日志 240
32.2.6 配置模块发送日志到 E-mail 240
32.2.7 配置使能 SYSLOG 日志服务器 240
32.2.8 配置 SYSLOG 服务器地址 241
32.2.9 配置 SYSLOG 服务器的端口 241
32.2.10 配置模块发送日志到 SYSLOG 服务器 241
32.2.11 配置使能集中管理中心服务器 242
32.2.12 配置集中管理中心服务器地址 242
32.2.13 配置集中管理中心服务器的端口 242
32.2.14 配置硬盘存储阈值 243
32.3 配置案例 243
32.3.1 配置案例 1: 配置本地日志 243
32.4 常见故障分析 243

32.4.1 故障现象 1：SYLOG 日志失效。 243
32.4.2 故障现象 2：E-mail 日志失效。 244
第 33 章 系统维护 245
33.1 系统时间设置 245
33.1.1 查看系统连续运行的时间 245
33.1.2 查看系统当前的日期和时间 245
33.1.3 配置系统当前的时区 246
33.1.4 手动设置系统当前的日期和时间 248
33.1.5 使用 ntp 设置系统当前的时间 248
33.1.6 使用 ntp 立即更新系统时间 249
33.2 系统升级和相关配置备份恢复 249
33.2.1 手动升级及配置恢复 249
33.2.2 自动升级 250
33.3 系统诊断 250
33.3.1 Ping 命令的使用 250
33.3.2 Traceroute 命令的使用 251
33.3.3 TCPSYN 命令的使用 252
33.4 E-mail 设置 253
33.4.1 配置 SMTP 服务器名称或者地址 253
33.4.2 配置邮件发送者邮件地址 254
33.4.3 配置邮件接收者邮件地址 254
33.4.4 配置发送邮件时是否需要认证 254
33.4.5 配置发送邮件时认证使用的用户名 255
33.4.6 配置发送邮件时认证使用的密码 255
33.4.7 配置 SSL 加密 255
33.5 配置系统监控 256
33.5.1 配置 CPU 占用率 256
33.5.2 配置内存占用率 256
33.5.3 配置流量 256
33.5.4 配置连接数 257
33.5.5 配置报文大小 257
第 34 章 配置 DNS 258
34.1 DNS 概述 258
34.2 配置 DNS 258
34.2.1 缺省配置信息 258
34.2.2 配置主 DNS 服务器 258
34.2.3 配置从 DNS 服务器 258
34.2.4 DNS 查询 259
34.3 配置案例 259
34.3.1 配置案例 259
34.4 常见故障分析 259
34.4.1 故障现象 1：DNS 解析失败 259
第 35 章 配置管理员用户 260
35.1 配置管理员 260
35.1.1 配置用户权限表 260

35.1.2 配置本地用户.....260
35.1.3 配置 RADIUS 管理员用户.....261
35.1.4 配置 LDAP 管理员用户.....261
35.1.5 配置管理员用户的管理地址.....261
35.1.6 配置管理员最短口令长度.....261
35.2 配置信息显示命令.....262
35.3 配置案例.....262
35.3.1 配置管理员用户的权限表功能.....262
35.4 故障分析.....264
35.4.1 用户无法登录.....264
35.4.2 命令无法执行.....264
第 36 章 配置 SNMP.....265
36.1 SNMP 协议概述.....265
36.2 配置 SNMP.....265
36.2.1 缺省配置信息.....265
36.2.2 配置启用 SNMP 代理.....266
36.2.3 配置设备物理地址.....266
36.2.4 配置 trap 地址.....266
36.2.5 配置 community.....267
36.2.6 配置 SNMP 版本.....267
36.2.7 配置 SNMP USM 用户.....268
36.3 配置案例.....269
36.3.1 配置案例 1：通过 MIB Browser 访问设备 MIB 库.....269
36.4 监控与维护.....270
36.4.1 查看 usm 用户.....270
36.5 常见故障分析.....271
36.5.1 故障现象 1：管理站不能访问代理站 MIB 库.....271
第 37 章 配置云平台.....272
37.1 云平台概述.....272
37.2 云平台配置.....272
第 38 章 配置 SSL VPN.....273
38.1 SSL VPN 概述.....273
38.2 配置 SSL VPN.....273
38.3 配置 dns&wins.....274
38.4 配置下发路由.....275
38.5 配置客户端下载链接.....275
38.6 查看 SSL VPN 监控.....275
第 39 章 配置 VRF.....277
39.1 VRF 功能概述.....277
39.2 配置 VRF.....277
第 40 章 配置沙箱.....278
40.1 沙箱概述.....278
40.2 沙箱配置.....278
第 41 章 配置镜像功能.....279
41.1 镜像功能概述.....279

41.2 配置端口镜像功能.....279
41.2.1 配置启用端口镜像.....279
第 42 章 配置源进源出功能.....280
42.1 源进源出功能概述.....280
42.2 配置源进源出功能.....280
42.2.1 源进源出功能启用.....280

第1章 系统管理

系统管理是对系统进行管理维护的一种重要手段，通过系统管理可以了解设备的基本用法，比如怎样对设备进行管理，如何上传下载配置文件，如何升级系统，以及如何获得帮助等。

1.1 系统概述

下一代防火墙使用的操作系统，可以通过命令行配置，也可以通过图形界面进行配置。其中命令行配置除了可以通过 console 口连接，也可以通过 SSH，Telnet 客户端连接，图形界面采用的 B/S 模式，可以通过 HTTPS 和 HTTP 进行连接。本手册只介绍通过命令行的方式进行配置管理。

1.1.1 命令行特性

这一节主要讲述当您进入命令行进行配置时所要进行的步骤。请仔细阅读本节以及后边几节中关于使用命令行接口的详细信息。

使用命令行接口（CLI），请按照以下步骤：

第 1 步：当进入命令行接口出现命令提示符后，请确认您有相应的权限。大多数配置命令都需要用户您有管理员权限。

第 2 步：键入命令名称。

注意：

设备命令行中的所有命令和关键字都是小写。

如果命令不含需要用户输入的参数，那么请直接跳到第 3 步。如果命令含需要用户输入的参数，那么继续以下步骤：

1） 如果命令需要一个参数值，请输入一个参数值。在输入参数值时，可能要输入关键字。

2） 命令的参数值部分一般指定了您应该输入什么样的参数，是某范围内的数值，或者字符串或者 IP 地址。关键字是指命令中要操作的对象。

3） 如果命令需要多个参数值，请按命令的提示依次输入关键字和每个参数值。直到提示信息中出现让您按回车键信息为止。

第 3 步：输入完整的命令后，请按回车键。

例如：“exit”是一个不含参数和关键字的命令。命令名称为 exit；“ip address A.B.C.D/M”是一个含有参数和关键字的命令。其中命令名称为 ip，关键字为 address，参数值为 A.B.C.D/M。

1.1.2 语法帮助

命令行接口内置有语法帮助。如果您对某个命令的语法不是很确定，请输入该命令中您所知道的部分，然后输入“?”或“空格加？”。命令行会提示您已经输入的部分命令后剩余部分的可能的命令清单。

1.1.3 使用语法帮助补齐命令

用户输入“Tab”键后，对命令进行补齐的功能。当您输入了一部分命令后，再输入“Tab”键，如果匹配的命令有多个，则列出可能的命令清单，如果匹配的命令只有一个，那么命令行会自动把用户输入的那部分命令补齐，并把光标移至最后。

命令中的符号

您可能会在命令语法中看到各种符号，这些符号只是说明您该如何输入该命令，但是不是命令本身的一个部分。下表对这些符号进行了概要说明。

表1-1命令行中的符号

符号	描述
大写字母	大写字母表示该命令的该部分必须输入一个字符串参数。例如命令： User-group NAME firewall 中您必须在NAME那个位置输入一个合法的用户组的名字作为您所创建的用户组的名字。
A.B.C.D和A.B.C.D/M	A.B.C.D表示IP地址，M表示掩码。例如命令： ip route A.B.C.D/M (A.B.C.D|INTERFACE)
圆括号 ( )和竖直线 |	圆括号一般和竖直线配合使用。圆括号括起来的部分表示这部分命令有几个用竖直线分隔开的可选项，您必须选择输入其中一项。 例如命令： timezone (utc|cst) 中圆括号内包含由竖直线分隔的两个可选项，您必须输入utc 和cst其中的一个。
中括号 [ ]	中括号表示里面的参数可输入或可不输入。 例如命令： show user [USERNAME] 中第二个参数如果输入表示有要显示指定用户名称的接入用户信息，如果不输入表示显示所有接入用户的信息
尖括号和数值范围	尖括号和数值范围表示输入的参数的取值范围在那两个数值之间的某个数。 例如命令：policy <1-5000> 中配置到设备上的策略ID可以是1至5000中的任何一个。

1.1.4 命令简写

命令简写是指您可以只输入命令单词或关键字的前边部分字母，只要那部分字母不会造成歧义，就可以直接回车执行该命令。但需要用户输入的参数如 PPPoE 模板的名字等，要完整输入。例如：ip address 192.168.1.1/16 可以简写成：ip add 192.168.1.1/16

注意：

当使用命令简写时，您必须输入足够多的字母，以确保在众多命令中不会造成歧义。

1.1.5 命令模式

设备支持丰富的命令模式，下表列出了所有的命令模式。

表1-2设备支持的所有命令模式

命令模式	提示符	进入方法
普通模式	DCFW-1800>	系统引导起来后，输入密码

特权模式	DCFW-1800 #	在普通模式下输入enable
全局配置模式	DCFW-1800 (config)#	在特权模式下输入 configure terminal
以太网接口配置模式	DCFW-1800 (config-ge0/0)#	在全局配置模式下输入interface IFNAME，例如：interface ge0/0
VLAN配置模式	DCFW-1800 (config-vlan12)#	在配置模式下输入 interface vlan+VID

1.1.6 常用命令介绍

表1-3普通模式下的常用命令介绍

命令	描述
enable	进入特权模式，可以对设备进行配置和写操作
exit	退出当前模式，返回到上一级模式。
ping -c <1-10000> -s <0-65507> -w <0-10> WORD	网络连通性基本检测工具，WORD为对方主机地址。-c表示ping包的个数，-s表示包的大小，-w是等待相应的时间。
list	显示当前模式下可用的命令
show running-config	显示当前的配置信息（可以是没有保存的）
show startup-config	显示已经保存的启动配置信息
show version	显示版本信息

1.2 实现系统配置的途径

您可以通过以下途径对设备进行管理：

- 使用终端（或者仿终端软件）连接到设备的串口（Console）从而访问设备的命令行接口（CLI）
- 使用 Telnet 管理设备
- 使用 SSH 管理设备
- 通过 Web 进行管理

1.2.1 通过串口实现系统配置

- 波特率：9600
- 数据位：8
- 奇偶校验：无
- 停止位：1
- 流量控制：无

正确设置完 Console 的参数并将设备加电，可以看到设备的登录提示信息。

1.2.2 通过 Telnet 实现系统配置

任何一个有 Telnet 功能的工作站都能通过 TCP/IP 网络连接到设备。可以通过以下步骤 Telnet 登录到设备：

通过 Console 口用管理员用户的帐号登录到设备。进入接口配置模式。

然后给设备某个接口配置 IP 地址。给接口配置 IP 地址可以使用以下命令：

ip address A.B.C.D/M

配置接口允许 Telnet 登录，可以使用下面的命令：

allow telnet

此后可以从该接口上以该接口的 IP 地址 Telnet 登录到设备命令行接口。

注意：

默认情况下接口是不允许 Telnet 登录的。

1.2.3 通过 SSH 方式实现系统配置

网络被攻击，很多情况是由于服务器提供了 Telnet 服务引起的。Telnet 服务有一个致命的弱点——它以明文的方式传输用户名及口令，所以，很容易被别有用心的人窃取口令。目前，一种有效代替 Telnet 服务的有用工具就是 SSH 服务。SSH 客户端与服务器端通讯时，用户名及口令均进行了加密，有效防止了对口令的窃听。设备支持以 SSH 的方式对设备的管理。

任何一个有 SSH 功能的工作站都能通过 TCP/IP 网络连接到设备。可以通过以下步骤登录到设备：

通过 Console 口用管理员用户的帐号登录到设备。进入接口配置模式。

然后给设备某个接口配置 IP 地址。给接口配置 IP 地址可以使用以下命令：

ip address A.B.C.D/M

配置接口允许 SSH 登录，可以使用下面的命令：

allow ssh

此后可以从该接口上以该接口的 IP 地址通过 SSH 命令登录到设备命令行接口。

注意：

默认情况下接口的 SSH 功能是关闭的，如果你需要启用该功能，必须使用 allow ssh 命令打开。

1.3 系统文件管理

系统文件的管理是指对于配置文件、系统应用程序文件的维护和管理。对于系统文件的管理，在没有特别指明的时候，都是在特权模式下操作。

1.3.1 copy 命令使用

copy 命令的格式如下：

copy ftp user password A.B.C.D RemoteFile (version|config)

具体参数解释如下

version ： 表示更新版本文件

config ： 表示配置文件

copy tftp A.B.C.D RemoteFile (version|config)
具体参数解释如下
version ： 表示更新版本文件
config ： 表示配置文件

1.3.2 保存配置文件

注意：
每一次修改了设备的配置后，必须将配置保存到设备中，重新启动后，配置才能保持不变。

配置文件保存的步骤如下所述：

方法 1：

步骤1	write memory	将配置文件保存到系统中

方法 2：

步骤1	write file	将配置文件保存到系统中

注意：
1）以上两个命令作用相同，都实现保存配置文件的功能。
2）startup-config 表示系统启动时的配置项，而 running-config 表示系统启动后当前的配置项，操作员更改后的配置项反映在 running-config 中，系统刚启动时，running-config 就是 startup-config。

1.3.3 多配置文件

多配置文件备份步骤如下所述：

步骤1	copy (running-config|startup-config) backup-config [<0-9>]	将运行配置或者启动配置备份

为配置文件添加描述信息：

步骤1	write (startup-config|backup-config) (default|<0-9>) description .DESCRIPTION	为配置文件添加描述信息

将某一个配置文件作为下次启动的配置:

步骤1	copy backup-config (default|<0-9>) startup-config	将某一个配置文件作为下次启动的配置:

1.3.4 配置文件的上传与下载

用户还可以把一份好的配置文件保存到文本文件中，在需要的时候（例如不小心把设备配置搞乱了，不知道怎样把配置恢复到以前的状态时）再把配置文件下载到设备中。通过使用下面的命令完成配置文件的下载：
copy tftp A.B.C.D RemoteFile config

配置导出的命令：
copy (running-config|startup-config) tftp A.B.C.D RemoteFile

1.3.5 系统升级

用户还可以把一份版本文件下载到设备中。通过使用下面的命令完成系统文件的下载：
copy tftp A.B.C.D RemoteFile version

1.4 常用系统管理命令

1.4.1 开启、关闭 Telnet 服务

关闭 Telnet 服务的步骤：

步骤1	(no) allow telnet	关闭Telnet服务，执行该命令后将禁止其他机器Telnet到设备

1.4.2 开启、关闭 SSH 服务

关闭 SSH 服务的步骤：

步骤1	(no) allow ssh	关闭SSH服务，执行该命令后将禁止其他机器SSH到设备

1.4.3 查看谁在系统上

who 命令显示当前有哪些操作员登录进系统。

1.4.4 清除登录用户

如果有多个操作员登录进系统，而有些操作员出现了异常，某个管理员可以把其他管理员踢出系统，可以通过 clear user 命令完成这个功能。
清除管理员用户
操作步骤：

步骤1	clear user USERNAME addr A.B.C.D time .TIME	根据输入的用户名，地址，时间清除对应的用户。

1.4.5 查看系统的版本

show version 命令可以查看系统的版本信息，包括所有物理接口，以及接口的 MAC 地址，系统的版本信息。例如：

```
DCFW-1800# show version
Model Name          : DCFW-1800E-X7160
Serial Number       : 5000T-0F189-1000T-0OR0L-019QF
DCFOS               : DCFOS-5.5-2-20190221
App Signature       : 20190129
```

IPS Signature : 20190129
AV Signature : 20190129
Compile time : Feb 21 2019 17:12:36

mgt: e1000e v2.1.4-NAPI MAC address: 44:8a:5b:38:7e:76
ge0/0: e1000e v2.1.4-NAPI MAC address: 44:8a:5b:38:7e:77
ge0/1: e1000e v2.1.4-NAPI MAC address: 44:8a:5b:38:7e:78
ge0/2: e1000e v2.1.4-NAPI MAC address: 44:8a:5b:38:7e:79
ge0/3: e1000e v2.1.4-NAPI MAC address: 44:8a:5b:38:7e:7a
ge0/4: e1000e v2.1.4-NAPI MAC address: 44:8a:5b:38:7e:7b

第2章 配置接口

2.1 配置以太网端口

2.1.1 以太网端口概述

通过配置以太网端口可以实现更改端口的带宽设置、双工模式以及端口速率等设置功能。对于端口的命名，如果是 10000M 网卡，则名称前缀为 Xge，比如 Xge0，Xge1 等等；如果是 1000M 网卡，则名称前缀为 ge，比如 ge0，ge1 等等。设备的所有端口缺省状态下是打开的。

2.1.2 配置以太网端口

缺省配置

表2-1端口缺省设置信息

内容	缺省设置	备注
端口自协商配置（auto-negotiate on/off）	on	可以更改设置
端口MTU(mtu)	1500	可以更改设置
端口管理状态(shutdown/no shutdown)	no shutdown	可以更改设置

启用自协商功能

默认情况下，端口参数是自协商的，在自协商模式下，端口的所有参数都是自动协商出来的，不能设置端口的参数。

启用端口自协商功能的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	auto-negotiate on	启用端口的自协商功能
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

禁用自协商功能

默认情况下，端口参数是自协商的。禁用自协商功能后，可以对端口参数进行配置。

禁用端口自协商功能的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	auto-negotiate off	禁用端口的自协商功能
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

注意：

缺省情况下端口的自协商功能是打开的，用户必须关闭端口的自协商功能后才能对端口的其他参数进行配置。

双工设置

双工就是在相对的方向上可以同时传输信息。半双工可以实现双向的通信，但不能在两个方向上同时进行，必须轮流交替地进行。与共享式 HUB 相连时，应置以太网口为半双工方式；与交换式 LAN SWITCH 相连时，一般置以太网口为全双工方式。

配置端口双工模式的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	duplex (full|half)	配置端口的双工模式
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

参数说明：duplex (full\|half)

参数	说明	缺省配置
full	全双工	
half	半双工	

速率设置

端口速率表示了端口收发数据包的速率，通常为 10M 和 100M，千兆设备端口速率为 10M 、100M 和 1000M。要使网络互联设备可以正常工作，必须保证相互连接的两个端口配置有相同的速率。

端口速率设置的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	speed (10|100|1000)	配置端口的速率
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

注意：

百兆端口不能设置 1000M 速率。

关闭端口

端口关闭后将不再收发数据，主要用于系统故障的发现和诊断，但是通常情况下不需要这样做。

关闭端口的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	shutdown	关闭端口

步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

配置接口 IP 地址

端口的 IP 地址可以通过三种方式配置：

- ✧ 静态配置：静态指定 IP 地址
- ✧ PPPoE 方式获取：通过 PPPoE 从 PPPoE 服务器获取 IP 地址，同时也能取到网关和 DNS 设置。适用于设备通过 ADSL 接入 internet
- ✧ DHCP 方式获取：通过 DHCP 方式从 DHCP 服务器获取 IP 地址，同时也能取到网关和 DNS 设置

每个端口都能分别配置不同的 IP 地址方式，但每次只能配置一种方式。下面分别介绍这三种不同：

配置端口静态 IP 的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	ip address A.B.C.D/M	静态指定接口IP地址，A.B.C.D/M为接口IP地址和掩码长度
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

配置端口通过 PPPoE 方式获取地址的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	ip address pppoe [A.B.C.D]	配置接口通过PPPoE方式获取地址，同时接口也可以自己指定IP地址，A.B.C.D为接口指定IP地址
步骤4	pppoe username USERNAME	配置PPPoE认证的用户名
步骤5	pppoe password PASSWORD	配置PPPoE认证的密码
步骤6	pppoe default_gateway	配置接口使用PPPoE网关为缺省网关
步骤7	pppoe dns	配置使用PPPoE服务器的DNS设置
步骤8	pppoe distance<1-255>	配置通过PPPoE获取缺省网关的权重
步骤9	end	退回到特权模式下
步骤10	write terminal	显示配置

配置端口通过 DHCP 方式获取地址的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	ip address dhcp metric <1-255> gw (reset|default) dns (reset|default)	配置接口通过DHCP获取IP地址
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

参数说明： ip address dhcp：

参数	说明	缺省配置
metric <1-255>	配置通过DHCP获取地址的权重，范围<1-255>	
gw (reset|default)	配置网关的获取方式，reset为使用DHCP服务器指定的网关，default为使用系统原有的网关	
dns (reset|default)	配置DNS的获取方式，reset为使用DHCP服务器指定的DNS，default为使用系统原有的DNS	

使用 no ip address 可以删除当前接口的 IP 地址设置；
使用 no ip address dhcp 可以取消接口的 dhcp client 设置；
使用 no ip address pppoe 可以取消接口的 PPPoE 设置。

注意：
DHCP Client 允许在物理接口,VLAN 接口上启用，但不能在加入 VLAN 的物理接口启用。

配置接口 MTU

接口的 MTU 用于控制接口的最大报文发送长度。

关闭端口的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	mtu <1280-1500>	设置端口最大发送报文长度，缺省为1500
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

配置内外网接口

内外网接口用于用户识别和统计集。

配置内外网接口的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	traffic-mode external/internal	配置接口是内网接口或外网接口
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

配置端口管理访问

端口的管理访问是用来控制通过该端口访问和管理设备的权限。通过配置端口的管理访问可以限制对端口的某类访问，保护设备的安全运行。

配置端口管理访问的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface

步骤3	allow (|http|https|ping|telnet|ssh|bgp |dns|ospf|rip|tcontrol)	配置端口管理访问
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

参数说明：allow access：

参数	说明	缺省配置
tcontrol	允许或者禁止监控中心管理设备	
http	允许或者禁止通过HTTP方式管理设备	
https	允许或者禁止通过HTTPs方式管理设备	
telnet	允许或者禁止通过Telnet方式管理设备	
ssh	允许或者禁止通过ssh方式管理设备	
ping	允许或者禁止外面设备Ping 设备	
bgp	允许或者禁止外面设备使用bgp	
dns	允许或者禁止外面设备使用设备的dns服务器功能	
ospf	允许或者禁止外面设备使用ospf	
rip	允许或者禁止外面设备使用rip	

以上这些权限在同一个端口上可以同时打开多个，可以组合使用。

配置端口接入访问

端口的接入访问是用来控制通过该端口接入的用户访问 Internet 或者服务器的权限。通过配置管理的接入访问可以限制端口的某些接入，保护服务器的安全。

配置端口接入访问的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	allow (webauth)	配置端口接入访问
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

参数说明：allow access

参数	说明	缺省配置
webauth	允许或者禁止该端口接入Web认证用户	

以上这些权限在同一个端口上可以同时打开多个，可以组合使用。

配置端口别名

设备在出厂的时候每个端口的名字和设备面板上的名字是一致的，在设备的使用过程中，为了便于理解和记住端口的用处，需要把接口改成比较直观的名字。通过 aliasname 命令可以给每个端口取一个个直观的别名。

修改端口别名的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	aliasname NAME	配置端口别名，NAME为端口的别名
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

2.1.3 配置案例

案例描述

将端口 ge0 的速率设置为 100Mbps，双工模式设置为全双工，关闭端口 ge0。

配置步骤：

步骤1	进入以太网端口配置模式
	DCFW-1800(config)# interface ge0
步骤2	关闭自协商
	DCFW-1800(config-if)# no auto
步骤3	配置端口ge0的带宽为100Mbps
	DCFW-1800(config-if)# speed 100
步骤4	配置端口ge0为全双工工作模式
	DCFW-1800(config-if)# duplex full
步骤5	关闭端口ge0
	DCFW-1800(config-if)# shutdown

2.1.4 以太网端口监控与维护

4.1.4.1 显示端口的信息

显示某个端口信息的步骤：

步骤1	显示某个端口的信息
	DCFW-1800_A# show interface ge0 ge0 Link status is up,Admin status is up aliasname eth0 mtu 1500 HWaddr: 00:92:25:26:00:08 auto negotiate: ON speed: 100 duplex: UFLL inet addr: 192.168.0.10 Bcast: 192.168.0.255 Mask:255.255.255.0 UP BROADCAST PHYUP RUNNING MULTICAST MTU:1500 Metric:1

	RX packets:8738 errors:0 dropped:0 overruns:0 frame:0 TX packets:6556 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 RX rate: 2 packets/s 370 bytes/s TX rate: 0 packets/s 0 bytes/s

Show interface 命令不指定具体端口则显示所有端口的信息。

2.1.5 故障分析

用如下方法测试以太网端口是否正常工作：

- 在网络负载小时，从 PC 机（PC 机与设备位于同一局域网内）Ping 设备的以太网口，观察是否能正确返回全部报文；
- 在网络负载大时，查看连接双方(如设备和交换机)的端口统计信息，观察接收到错帧的统计数量是否快速增加。
- 如果这两项测试中有任何一项不能通过，则可以断定设备的以太网口工作不正常。
- 在确认以太网有故障之后可按如下步骤进行排错：
- 查看物理设备连接是否正常
- 在物理设备连接正常的情况下，网线两端端口对应的 Link 指示灯应点亮。
- 查看连接双方速率设置是否一致
- 如果一方工作于 100Mbps 模式，而另一方工作于 10Mbps 模式时，端口也不会正常工作。故障表现为：配置为 100Mbps 模式的一方显示为端口 down；配置为 10Mbps 模式的一方则显示为端口 UP。对于这种故障，只要使用 speed 命令把连接双方的速率配成一致即可。
- 查看连接双方是否处于同一网络
- 连接双方必须处于同一网络，即二者的网络地址一样而主机地址不同，如果二者网络地址不一样，请用 ip address 命令正确设置 IP 地址。
- 查看连接双方的双工模式是否一致（其中一方为设备）
- 当双工模式不一致，即一方工作于全双工模式，而另一方工作于半双工模式，故障表现为：

  网络流量增大时，配置为半双工模式的一方显示冲突频繁（如连接共享式 Hub 则整个网络段上所有其它机器都显示冲突严重），配置为全双工模式的一方则显示接收到大量错包，同时，双方丢包严重。

  可用 show interface [IFNAME]命令查看以太网收发包的错误率，冲突现象一般可以通过网口状态指示灯观察到；

  在连接共享式 Hub 时，应该以半双工模式工作；在连接 Lanswitch 时，一般使用全双工模式工作。

2.2 配置VLAN接口

本节涉及设备 VLAN 的配置，内容主要包括：

- VLAN 概述
- 配置接口封装的链路层协议为 VLAN

2.2.1 VLAN 概述

在一个物理局域网内，通过对端口的划分，将局域网内的设备分割为几个各自独立的群组，群组内部的设备之间可以自由地通讯，而当分属不同群组的设备要进行通讯时，必须进行三层的路由转发；通过这种方式，一个物理局域网就如同被划分为几个相互隔离的局域网，这些不同的群组就称为虚拟局域网（VLAN）。

2.2.2 配置接口封装的链路层协议为 VLAN

如果要让设备识别带 VLAN 标识的包，需要创建一个 vlan，然后将以太网接口加入该 vlan，则可以通过该子接口接收/转发带 VLAN 标识的包。

VLAN ID 值的说明：

设备的 VLAN ID 值的范围是 1-4094，这个值是通过使用 vlan ID 指令创建，例如，如果创建了一个 vlan 10 需要将 ge0 加入 vlan 10 且为 untag 方式，则命令为 untag vlan 10。

配置接口封装的链路层协议为 VLAN 的步骤:

步骤1	DCFW-1800(config)#vlan <1-4094>	用于创建VLAN，<1-4094>为VLAN ID。
	DCFW-1800(config)#interface ge0	进入接口视图
	DCFW-1800(config-ge0)#tag vlan ID	指定接口的vlan tag ID，一个接口可以有多个tag ID
	DCFW-1800(config)#interface vlan<1-4094>	用于创建VLAN接口，<1-4094>为VLAN ID。
步骤2	ip address A.B.C.D/M	设置 vlan的IP地址

注意：

当该以太网接口已配置 IP 地址，则加入 VLAN 后会自动删除 IP 地址。

2.2.3 配置信息的显示

VLAN 配置信息显示命令:

步骤1	show interface	显示VLAN接口信息
步骤2	Show vlan	显示VLAN 信息

2.2.4 配置案例

在两个 VLAN 之间做路由连接

案例描述

交换机与设备相连。

在该交换机上划分两个 VLAN：VLAN 10 和 VLAN 20。

VLAN 10 的 VLAN ID 为 10，包含端口 1、2、3，端口 1 为 Taged 端口，连接的 ge0 接口，端口 2、3 为 Untaged 端口，下接 192.168.10.0/24 网段。

VLAN 20 的 VLAN ID 为 20，包含端口 1、4、5，端口 1 为 Taged 端口，连接的 ge0 接口，端口 4、5 为 Untaged 端口，下接 192.168. 20.0/24 网段；

在设备的 ge0 接口上也划分两个 VLAN，vlan10 和 vlan20，VLAN ID 分别为 10 和 20。

vlan10 的 IP 地址为 192.168.10.1/24。

vlan20 的 IP 地址为 192.168. 20.1/24。

配置步骤

步骤**1**	创建vlan 10，并指定IP地址。
	DCFW-1800# configure terminal DCFW-1800(config)# vlan 10 DCFW-1800(config-vlan)# exit DCFW-1800(config)# interface vlan10 DCFW-1800(config-vlan10)#ip address 192.168.10.1/24 DCFW-1800(config-vlan10)#allow all DCFW-1800(config-vlan10)#exit
步骤**2**	创建vlan 20，并指定IP地址
	DCFW-1800# configure terminal DCFW-1800(config)# vlan 20 DCFW-1800(config-vlan)# exit DCFW-1800(config)# interface vlan20 DCFW-1800(config-vlan20)#ip address 192.168.20.1/24 DCFW-1800(config-vlan20)#allow all DCFW-1800(config-vlan20)#exit
步骤**3**	创建接口间互访的安全策略
	DCFW-1800# configure terminal DCFW-1800(config)# policy 1 any any any any any any any always permit DCFW-1800(config-policy)# enable DCFW-1800(config-policy)# exit
步骤**3**	保存配置
	DCFW-1800 (config)# write memory

2.2.5 故障分析

VLAN 无法正常工作

故障现象	VLAN无法正常工作
分析与解决	1.请检查配置，是否是您需要配置的VLAN ID，您的配置是否正确 2.网络拓扑是否正确 3.线路是否正常 4.VLAN状态是否正确

2.3 配置透明网桥（vlan 透传）

2.3.1 透明网桥概述

透明网桥功能：最初是由 DEC 公司提出，并被 802.1 委员会采纳并标准化，透明网桥使用最方便，易于安装。当桥接入互连的局域网内，就能运行。它不会影响现存的局域网，原有的软硬件无须改变，也不要设置地址开关和加载路径选择表参数。对于用户来说，该网桥是透明的，即该网桥进入或离开整个网络，用户感觉不到。

2.3.2 配置透明网桥

创建透明网桥

创建透明网桥的步骤：

步骤1	VLAN ID	创建一个VLAN

使用 no VLAN 可以删除一个 VLAN。

配置网桥组端口

配置透明网桥后，需要将实际物理接口或聚合接口加入网桥中，这些接口被称为网桥组端口。

配置网桥组端口的步骤：

步骤1	interface NAME	进入一个端口
步骤2	Tag/untag<1-4094>	将多个接口加入同一个vlan，同一个vlan的接口及视为一个透明网桥

2.3.3 配置网桥 STP

STP（Spanning Tree Protocol）是生成树协议的英文缩写。该协议可应用于环路网络，通过一定的算法实现路径冗余，同时将环路网络修剪成无环路的树型网络，从而避免报文在环路网络中的增生和无限循环。

创建新的桥接口，开启关闭 STP 功能

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	VLAN ID	进入VLAN
步骤3	bridge stp (enable|disable)	选择开启货关闭STP功能

配置网桥优先级

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	VLAN ID	进入VLAN
步骤3	bridge priority <0-61440>	配置桥接口优先级

参数说明：

参数	说明	缺省配置
priority	桥接口优先级值，范围0-61440	32768

配置网桥发送 bpdu hello 时间

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	VLAN ID	进入VLAN
步骤3	bridge hello-time <1-10>	配置发送bpdu hello时间

参数说明：

参数	说明	缺省配置
hello-time	发送hello bpdu时间间隔，范围1-10	2

配置网桥 STP 最大老化时间

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	VLAN ID	进入VLAN
步骤3	bridge max-age <6-40>	配置STP最大老化时间

参数说明：

参数	说明	缺省配置
max-age	STP最大老化时间，范围6-40	20

配置网桥端口状态转换时延

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	VLAN ID	进入VLAN
步骤3	bridge forward-delay <4-30>	配置端口状态转换时延

参数说明：

参数	说明	缺省配置
forward-delay	端口状态转换时延，范围4-30	15

注意：

要选择性能较高、位置较靠中心的桥的优先级最高。

提示：

端口转换时间是指：开启 STP 后，端口从 listening 到 learning 到 forwarding 变化的时间间隔。

2.3.4 配置案例

配置透明网桥

案例描述

将设备插入一个原有的网络结构中，不改变原有拓扑和配置，将设备的 ge0 和 ge1 两个端口加入网桥组（vlan 10）中。ge0 口连接 Router（192.168.0.1），ge1 口连接 192.168.0.0/16 网段其余机器。

配置步骤：

步骤**1**	创建透明网桥（vlan 10）
	DCFW-1800# configure terminal DCFW-1800(config)# vlan 10 DCFW-1800(config-vlan)# exit
步骤**2**	将端口ge0加入透明网桥(vlan 10)
	DCFW-1800(config)# interface ge0 DCFW-1800(config-ge0)# untag vlan 10 DCFW-1800(config-ge0)# exit
步骤**3**	将端口ge1加入透明网桥(vlan 10)
	DCFW-1800(config)# interface ge1 DCFW-1800(config-ge1)# untag vlan 10 DCFW-1800(config-ge1)# exit

2.3.5 透明网桥监控与维护

查看桥组信息

步骤**1**	查看桥组信息
	DCFW-1800# show vlan 10 stp vlan:vlan10 STP: enabled bridge id : 32768.d43d7e900ab0 designated root : 32768.d43d7e900ab0 Ageing time: 300 Hello time: 2 Max age: 20 Forward delay: 15 vlan ports: ge0 <forwarding><untagged> ge1 <forwarding><untagged> 分别显示了桥组名、STP启用状态、桥ID、指定的根、FDB老化时间及该桥组所包含的端口及端口的状态

查看 FDB 信息

步骤**1**	
	DCFW-1800# show vlan10 fdb vlan:vlan10 Address State Ageing Interface 00:10:f3:0e:56:b8 forwarding 87 ge0 00:16:41:59:3e:9c forwarding 31 ge0 00:16:76:65:3c:b7 forwarding 201 ge0

	00:16:76:6b:15:9b	forwarding	18	ge0
	00:16:41:59:57:ca	forwarding	151	ge0
	00:16:17:96:c5:71	forwarding	110	ge0
	00:10:f3:0d:1a:04	forwarding	static	ge0
	00:16:76:80:ab:84	forwarding	89	ge0
	00:16:76:6b:16:d9	forwarding	63	ge0
	00:16:76:65:3e:3c	forwarding	90	ge0
	00:16:17:ed:ff:5f	forwarding	125	ge0
	00:15:e9:b0:4f:42	forwarding	1	ge0
	00:16:17:96:c5:6f	forwarding	49	ge0
	00:17:df:ba:4c:00	forwarding	0	ge0
	00:16:76:6b:9d:98	forwarding	262	ge0
	00:19:aa:15:6f:03	forwarding	0	ge0
	00:16:76:80:ab:94	forwarding	12	ge0
	00:10:f3:0d:1a:05	forwarding	static	ge1
	其中本地端口的MAC地址显示为static，不会老化。			

查看透明网桥的 debug 信息

步骤**1**	查看桥组报文处理信息
	DCFW-1800#debug vlan

2.3.6 常见故障分析

透明网桥无法正常工作

故障现象	在网桥的两个端口之间数据无法转发
分析与解决	1）是否将正确的端口加入网桥 2）链路是否正常 3）端口状态是否正常（该端口Admin状态是否是up）

2.4 配置链路聚合Trunk接口

2.4.1 链路聚合 Trunk 概述

链路聚合 Trunk 是通过组合多个链路成为一个逻辑的网络链路，用于提高带宽。在使用快速以太网和千兆以太网技术，通过链路聚合提高了设备之间通讯通道的容量和可用性。两个或多个百兆或千兆以太网连接捆绑在一起来提高带宽的容量和连接的冗余性。链路聚合也提供了负载均衡的方式来处理通讯负荷，使得通讯负荷均分在几个链路中，不会有单独一个链路超负载。通过链路聚合，用户可以在许多应用中得到实际的益处：更高的可靠性、更高的带宽，使用现有的设备，节约成本（不需要更新设备来获取更高的带宽）

2.4.2 配置链路聚合 Trunk 接口

创建新的 Trunk 接口，将物理接口加入 Trunk 中

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	Interface tvi0	创建Trunk接口tvi0
步骤3	Interface ge0 trunk-group 0 Interface ge1 trunk-group 0	物理口ge0、ge1加入到trunk 0组

参数说明：

参数	说明	缺省配置
Trunk组号	0-255	

配置 Trunk 的聚合模式

配置步骤

步骤1	configure terminal	进入配置模式
步骤2	Interface tvi0	进入Trunk接口tvi0
步骤3	trunk lacp	配置Trunk接口tvi0聚合模式为LACP协议聚合模式

参数说明：

参数	说明	缺省配置
LACP聚合模式	所有加入到Trunk的物理子接口上都开启LACP协议，将与对端的物理接口进行LACP协商，符合聚合条件者可以聚合在一起	

配置 Trunk 发送负载均衡

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	Interface tvi0	创建Trunk接口tvi0
步骤3	trunk hash dst-mac	配置Trunk负载均衡根据目的MAC哈希
步骤4	trunk hash src-dst-ip	配置Trunk负载均衡根据源/目的IP哈希
步骤5	trunk hash polling	配置Trunk负载均衡根据轮询
步骤6	trunk hash dst-ip	配置Trunk负载均衡根据目的IP哈希
步骤7	trunk hash src-dst-mac	配置Trunk负载均衡根据源/目的MAC哈希
步骤8	trunk hash src-ip	配置Trunk负载均衡根据源IP哈希
步骤9	trunk hash src-mac	配置Trunk负载均衡根据源MAC哈希

参数说明：

参数	说明	缺省配置
dst-mac	src-dst-ip是根据待发报文的目的MAC做hash，选择发送端口	

src-dst-ip	src-dst-ip是根据待发报文的源IP、目的IP及端口（如果是TCP或UDP报文）来做hash选择发送端口	
polling	polling是根据轮询做hash选择发送端口	
dst-ip	dst-ip是根据待发报文的目的ip来做hash选择发送端口	
src-dst-mac	src-dst-mac是根据待发报文的源/目的mac做hash选择发送端口	
src-ip	src-ip是根据待发报文的源ip做hash选择发送端口	
src-mac	src-mac是根据待发报文的源mac做hash选择发送端口	

配置 Trunk 接口作为桥接口的一个端口

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	Vlan 10	配置一个透明桥
步骤3	Interface tvi0	进入Trunk接口配置
步骤4	Untag vlan10	配置为桥端口

配置 Trunk 接口配置为 vlan 口

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	Interface tvi0	进入Trunk接口配置
步骤3	Tag vlan 10	配置Trunk接口为vlan口

参数说明：

参数	说明	缺省配置
Trunk的vlan ID	vlan ID与物理接口vlan ID相同	

2.4.3 配置案例

案例描述

某公司两个子网 LAN1、LAN2，分别连接两台设备，接口为百兆。两个 LAN 分别连接设备的 3 个接口，LAN1 与 LAN2 之间交互网络流量很大，需要 300M 带宽，而且需要做链路备份，防止某条链路故障而导致两个 LAN 不通。

这种情况，可以在两台设备上分别配置两个 Trunk 接口，并且物理口直连，分别将 3 个物理口加入到 Trunk 中去，使之聚合，从而增加带宽并做链路备份。

配置步骤

步骤	1.进入设备配置模式 DCFW-1800 #config terminal

	2.新建Trunk接口tvi0，trunk组号为0 DCFW-1800(config)#intface tvi0 3.配置trunk接口模式为LACP模式 DCFW-1800(config-tvi0)#trunk lacp 4.配置trunk负载均衡为3层模式 DCFW-1800(config-tvi0)#trunk hash src-dst-ip 5.返回上级接口节点 DCFW-1800(config-tvi0)#exit 6.将eth0 eth1 eth2加入到tvi0中去 DCFW-1800(config)#interface eth0 DCFW-1800(config-eth0)#trunk-group 0 DCFW-1800(config-eth0)#interface eth1 DCFW-1800(config-eth1)# trunk-group 0 DCFW-1800(config-eth1)#interface eth2 DCFW-1800(config-eth2)#i trunk-group 0 7.退出，配置完成 DCFW-1800(config-eth2)#end DCFW-1800 #
说明	两台设备分别作上述配置后，两台设备的3个端口间相互聚合，在上层看来是一个接口，这样带宽增加了3倍。 同时，3个接口可以相互做备份，某个接口因故障down掉，两台设备之间照样可以连通。

2.4.4 常见故障分析

故障现象 1：Trunk 接口不收发报文

现象	Trunk接口不能接收报文也不能发送报文
分析	可能是Trunk链路聚合协商不成功，导致其下端口inactive
解决	检查对端设备trunk口配置，使Trunk两端聚合协商成功

2.5 配置PPPoE接口

2.5.1 PPPoE 概述

pppoe 是 point-to-point protocol over ethernet 的简称，可以使以太网的主机通过一个简单的桥接设备连到一个远端的接入集中器上。通过 pppoe 协议，远端接入设备能够实现对每个接入用户的控制和计费。

2.5.2 配置 PPPoE 接口

配置 PPPoE 接口，在物理口上配置 PPPoE

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	Interface ge0	进入到物理口
步骤3	ip address pppoe pppoe username xxx	配置接口pppoe模式，添加pppoe用户名/密码

	pppoe password secret xxx

2.5.3 配置案例

案例描述：

某公司使用 pppoe 拨号方式转发内网用户数据。用户名 xsa112233、密码 111222333。

配置步骤

步骤1	1.进入设备配置模式 DCFW-1800 #config terminal 2.进入到拨号接口 DCFW-1800(config)#interface ge0/0 3.配置接口获取IP方式 DCFW-1800(config-ge0/0)# ip address pppoe 4.配置用户名、密码 DCFW-1800(config-ge0/0)# pppoe username xsa112233 DCFW-1800(config-ge0/0)#pppoe password secret 111222333 5.退出，配置完成 DCFW-1800(config-eth2)#end DCFW-1800 #

2.6 配置DHCP接口

2.6.1 DHCP 概述

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是一个局域网的网络协议，使用 UDP 协议工作，主要有两个用途：给内部网络或网络服务供应商自动分配 IP 地址，给用户或者内部网络管理员作为对所有计算机作中央管理的手段。DHCP 有 3 个端口，其中 UDP67 和 UDP68 为正常的 DHCP 服务端口，分别作为 DHCP Server 和 DHCP Client 的服务端口。

2.6.2 配置 DHCP 接口

配置 DHCP 接口，在物理口上配置 DHCP

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	Interface ge0	进入到物理口
步骤3	ip address dhcp metric METRIC gw （default|reset） dns （default|reset）	配置接口dhcp方式获取IP地址，并设置路由权值、全局dns。

2.6.3 配置案例

案例描述：

某公司把设备接入到 dhcp 环境中，通过 dhcp 获取接口 IP 地址。

配置步骤

步骤**1**	1.进入设备配置模式 DCFW-1800 #config terminal 2.进入到拨号接口 DCFW-1800(config)#intface ge0/0 3.配置接口获取IP方式 DCFW-1800(config-ge0/0)# ip address dhcp metric 10 gw reset dns default 4.退出，配置完成 DCFW-1800(config-eth2)#end DCFW-1800 #

2.7 配置旁路接口

2.7.1 旁路工作模式概述

在此工作模式中，网络的流量不会流经设备，而是由其它网络设备把需要检测的流量镜像一份给设备。在这种部署模式下，设备不会影响网络流量的正常转发；发现攻击时，可以通过与防火墙联动等手段来阻断攻击。

2.7.2 配置旁路接口

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	Interface ge0	进入到物理口
步骤**3**	listen-mode	配置接口监听

2.8 配置gre接口

2.8.1 gre 接口概述

GRE 是对某些网络层协议（如：IP，IPX，AppleTalk 等）的数据报文进行封装，使这些被封装的数据报文能够在另一个网络层协议（如 IP）中传输。这是 GRE 最初的定义，最新的 GRE 封装规范，已经可以封装二层数据帧了，如 PPP 帧、MPLS 等。在 RFC2784 中，GRE 的定义是“X over Y”，X 和 Y 可以是任意的协议。GRE 真的变成了“通用路由封装”了。

GRE 协议实际上是一种封装协议，它提供了将一种协议的报文封装在另一种协议报文中的机制，使报文能够在异种网络中传输。异种报文传输的通道称为 tunnel（隧道）。

GRE 隧道不能配置二层信息，但可以配置 IP 地址。GRE 利用为隧道指定的实际物理接口完成转发，转发过程如下：

（1）所有发往远端 VPN 的原始报文，首先被发送到隧道源端

（2）原始报文在隧道源端进行 GRE 封装，填写隧道建立时确定的隧道源地址和目的地址，然后再通过公共 IP 网络转发到远端 VPN 网络

2.8.2 配置 gre 接口

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface gre<0-2047>	新建gre接口
步骤3	aliasname NAME	设置接口名称
步骤4	ip address A.B.C.D/M	设置ip地址
步骤5	source(A.B.C.D |INTERFACE_NAME)	设置隧道源地址
步骤6	destination (A.B.C.D | dynamic)	设置隧道对端地址
步骤7	key <1-9999>	设置隧道标示
步骤8	keepalive [<1-86400>] [<1-1000>]	设置保活时间，默认为10s，设置重试次数，默认3次
步骤9	ttl <1-255>	设置ttl，默认为0

以上命令均可使用 no 命令取消对各个命令的设置，使其恢复到缺省配置。

参数说明：interface gre<0-2047>

参数	说明	缺省配置
gre<0-2047>	gre组号	无

2.8.3 配置案例

配置步骤：

步骤1	配置gre接口
	1.进入gre接口 DCFW-1800(config)# interface gre10 2.给接口命名

	DCFW-1800(config-gre10)#aliasname 10 3.配置源地址 DCFW-1800(config-gre10)#source 172.16.2.2 4.配置对端地址 DCFW-1800(config-gre10)#destination 172.16.2.1 5.配置组号 DCFW-1800(config-gre10)#key 10 6.配置保活时间 DCFW-1800(config-gre10)#keepalive 2 3 7.配置ttl DCFW-1800(config-gre10)# ttl 2 8.配置ip地址 DCFW-1800(config-gre10)#ip address 10.1.1.2/24 9.配置完成，退出 DCFW-1800(config-gre10)#exit
步骤**2**	添加静态路由
	DCFW-1800(config)#ip route 172.16.1.0/24 gre10

第3章 配置安全域

3.1 安全域概述

域就是接口组，可以在一个域中加入多个接口，但是一个接口只能属于一个域。如果一个接口被包含在某个域中，就不能单独对该接口进行配置。

3.2 配置向域中添加接口

可以用 include 命令向域中添加一个接口。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	zone NAME	进入名为NAME的域模式
步骤3	include interface IF_NAME	将名为IF_NAME的接口加入该域中
步骤4	show zone NAME	显示域配置信息

使用 no include interface IF_NAME 可以删除接口组中通过 include interface 命令添加的接口。

参数说明：

命令（1）：zone NAME

参数	说明	缺省配置
<NAME>	域名称	无

命令（2）：include interface IF_NAME

参数	说明	缺省配置
<IF_NAME>	接口名称	无

3.3 配置区域内接口互访

可以用 allow intrazone 命令来配置区域内接口互访

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	zone NAME	进入名为NAME的域模式
步骤3	allow intrazone	允许区域内接口互访

3.4 配置案例

3.4.1 配置案例：添加接口到域中

案例描述

配置一个接口到指定的域中。

配置步骤：

步骤**1**	创建一个域
	DCFW-1800_A(config)# zone all
步骤**2**	在这个域中添加一个接口
	DCFW-1800_A(config-addr)# include interface ge0
	DCFW-1800_A(config-addrgrp)# address-object dev

配置结果：

```
DCFW-1800# show running-config
!
zone all
    include interface ge0
!
```

3.5 安全域监控与维护

3.5.1 查看域信息

查看某个域的步骤：

步骤**1**	显示某个域信息
	DCFW-1800_A# show zone all ! zone all include interface ge0 DCFW-1800_A# all是域名称; ge0是被加到域中的接口名称。

3.6 常见故障分析

3.6.1 故障现象：

现象	执行no zone NAME以后，该域仍然存在。
分析	当一个域正在被引用时，就不能通过no命令删除。
解决	可以先撤销其它配置对该域的引用，确定其没有被引用之后再用no命令删除该节点。

第4章 配置 IPv6

4.1 IPv6概述

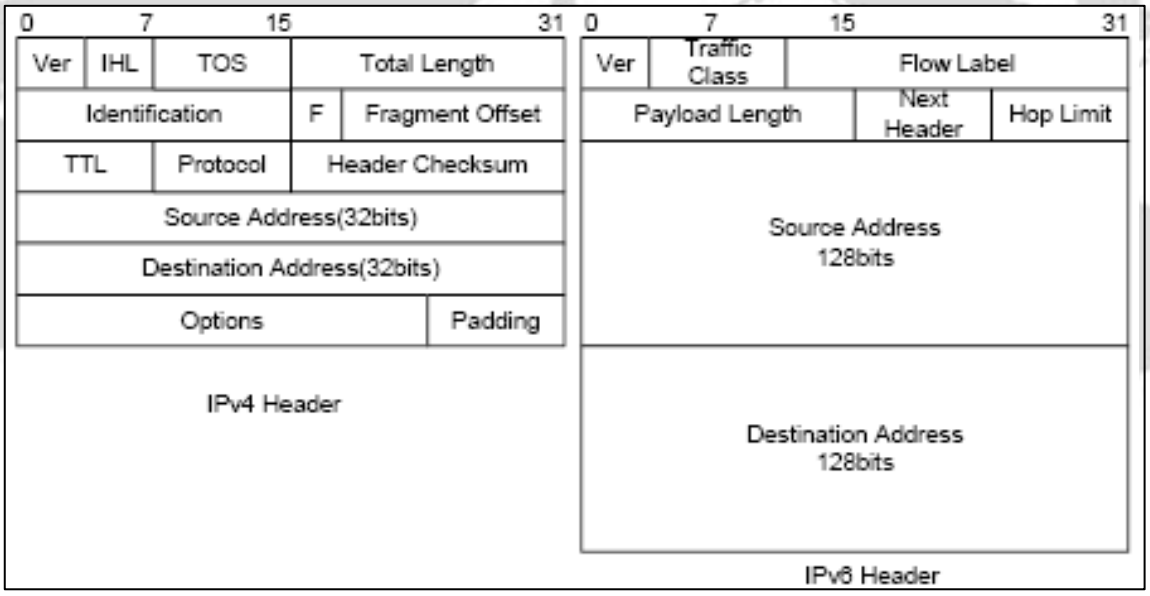
IPv6（InternetProtocolVersion6，因特网协议版本 6）是网络层协议的第二代标准协议，也被称为 IPng（IPNextGeneration，下一代因特网），它是 IETF（Internet EngineeringTaskForce，Internet 工程任务组）设计的一套规范，是 IPv4 的升级版本。IPv6 和 IPv4 之间最显著的区别为：IP 地址的长度从 32 比特增加到 128 比特。

4.1.1 IPv6 协议特点

简化的报文头格式

通过将 IPv4 报文头中的某些字段裁减或移入到扩展报文头，减小了 IPv6 基本报文头的负载，从而简化了转发设备对 IPv6 报文的处理，提高了转发效率。尽管 IPv6 地址长度是 IPv4 地址长度的四倍，但 IPv6 基本报文头的长度只有 40 字节，为 IPv4 报文头长度（不包括选项字段）的两倍。

图4-1 IPv4 报文头和 IPv6 基本报文头格式比较



充足的地址空间

IPv6 的源地址与目的地址长度都是 128 比特（16 字节）。它可以提供超过 3.4×10^{38} 种可能的地址空间，完全可以满足多层次的地址划分需要，以及公有网络和机构内部私有网络的地址分配。

层次化的地址结构

IPv6 的地址空间采用了层次化的地址结构，有利于路由快速查找，同时可以借助路由聚合，有效减少 IPv6 路由表占用的系统资源。

地址自动配置

为了简化主机配置，IPv6 支持有状态地址配置和无状态地址配置：

- ✧ 有状态地址配置是指从服务器（如 DHCP 服务器）获取 IPv6 地址及相关信息；

- 无状态地址配置是指主机根据自己的链路层地址及路由器发布的前缀信息自动配置 IPv6 地址及相关信息。
- 同时，主机也可根据自己的链路层地址及默认前缀（FE80::/64）形成链路本地地址，实现与本链路上其他主机的通信。

内置安全性

IPv6 将 IPSec 作为它的标准扩展头，可以提供端到端的安全特性。这一特性也为解决网络安全问题提供了标准，并提高了不同 IPv6 应用之间的互操作性。

支持 QoS

IPv6 报文头的流标签（FlowLabel）字段实现流量的标识，允许设备对某一流中的报文进行识别并提供特殊处理。

增强的邻居发现机制

IPv6 的邻居发现协议就是一组 ICMPv6（InternetControlMessageProtocolfor IPv6，IPv6 的因特网控制报文协议）消息，管理着邻居节点间（即同一链路上的节点）信息的交互。它代替了 ARP（AddressResolutionProtocol，地址解析协议）、ICMPv4 路由器发现和 ICMPv4 重定向消息，并提供了一系列其他功能。

灵活的扩展报文头

IPv6 取消了 IPv4 报文头中的选项字段，并引入了多种扩展报文头，在提高处理效率的同时还大大增强了 IPv6 的灵活性，为 IP 协议提供了良好的扩展能力。IPv4 报文头中的选项字段最多只有 40 字节,而 IPv6 扩展报文头的大小只受到 IPv6 报文大小的限制。

4.1.2 IPv6 地址介绍

IPv6 地址表示方式

IPv6 地址被表示为以冒号(:)分隔的一连串 16 比特的十六进制数。每个 IPv6 地址被分为 8 组，每组的 16 比特用 4 个十六进制数来表示，组和组之间用冒号隔开，比如：2001:0000:130F:0000:0000:09C0:876A:130B。

为了简化 IPv6 地址的表示，对于 IPv6 地址中的“0”可以有下面的处理方式：

- 每组中的前导“0 ”可以省略，即上述地址可写为

  2001:0:130F:0:0:9C0:876A:130B。
- 如果地址中包含连续两个或多个均为 0 的组，则可以用双冒号“::”来代替，即上述地址可写为 2001:0:130F::9C0:876A:130B。

注意：

在一个 IPv6 地址中只能使用一次双冒号“::”，否则当设备将“::”解析为 0 以恢复 128 位地址时，就无法确定“::”所代表的 0 的个数。

IPv6 地址由两部分组成：地址前缀与接口标识。其中，地址前缀相当于 IPv4 地址中的网络号码字段部分，接口标识相当于 IPv4 地址中的主机号码部分。地址前缀的表示方式为：IPv6 地址/前缀长度。其中，IPv6 地址是前面所列出的任一形式，而前缀长度是一个十进制数，表示 IPv6 地址最左边多少位为地址前缀。

IPv6 的地址分类

Pv6 主要有三种类型的地址：单播地址、组播地址和任播地址。

- 单播地址：用来唯一标识一个接口，类似于 IPv4 的单播地址。发送到单播地址的数据报文将被传送给此地址所标识的接口。
- 组播地址：用来标识一组接口（通常这组接口属于不同的节点），类似于 IPv4
- 的组播地址。发送到组播地址的数据报文被传送给此地址所标识的所有接口。
- 任播地址：用来标识一组接口（通常这组接口属于不同的节点）。发送到任播地址的数据报文被传送给此地址所标识的一组接口中距离源节点最近（根据使用的路由协议进行度量）的一个接口。

提示：

IPv6 中没有广播地址，广播地址的功能通过组播地址来实现。

IPv6 地址类型是由地址前面几位（称为格式前缀）来指定的，主要地址类型与格式前缀的对应关系如表 1-1 所示。

表4-1地址类型与格式前缀的对应关系

地址类型		格式前缀（二进制）	IPv6 前缀标识
单播地址	未指定地址	00...0 (128 bits)	::/128
	环回地址	00...1 (128 bits)	::1/128
	链路本地地址	1111111010	FE80::/10
	站点本地地址	1111111011	FEC0::/10
	全球单播地址	其他形式	-
组播地址		11111111	FF00::/8
任播地址		从单播地址空间中进行分配，使用单播地址的格式	

单播地址的类型

IPv6 单播地址的类型可有多种，包括全球单播地址、链路本地地址和站点本地地址等。

- 全球单播地址等同于 IPv4 公网地址，提供给网络服务提供商。这种地址类型的结构允许路由前缀的聚合，从而限制了全球路由表项的数量。
- 链路本地地址用于邻居发现协议和无状态自动配置中本地链路上节点之间的通信。使用链路本地地址作为源或目的地址的数据报文不会被转发到其他链路上。
- 站点本地地址与 IPv4 中的私有地址类似。使用站点本地地址作为源或目的地址的数据报文不会被转发到本站点（相当于一个私有网络）外的其它站点。
- 环回地址：单播地址 0:0:0:0:0:0:0:1（简化表示为::1）称为环回地址，不能分配给任何物理接口。它的作用与在 IPv4 中的环回地址相同，即节点用来给自己发送 IPv6 报文。
- 未指定地址：地址::称为未指定地址，不能分配给任何节点。在节点获得有效的 IPv6 地址之前，可在发送的 IPv6 报文的源地址字段填入该地址，但不能作为 IPv6 报文中的目的地址。

组播地址

下表所示的组播地址，是预留的特殊用途的组播地址。

表4-2预留的 IPv6 组播地址列表

地址	应用
FF01::1	节点本地范围所有节点组播地址
FF02::1	链路本地范围所有节点组播地址
FF01::2	节点本地范围所有路由器组播地址
FF02::2	链路本地范围所有路由器组播地址
FF05::2	站点本地范围所有路由器组播地址

另外，还有一类组播地址：被请求节点（Solicited-Node）地址。该地址主要用于获取同一链路上邻居节点的链路层地址及实现重复地址检测。每一个单播或任播 IPv6 地址都有一个对应的被请求节点地址。其格式为：

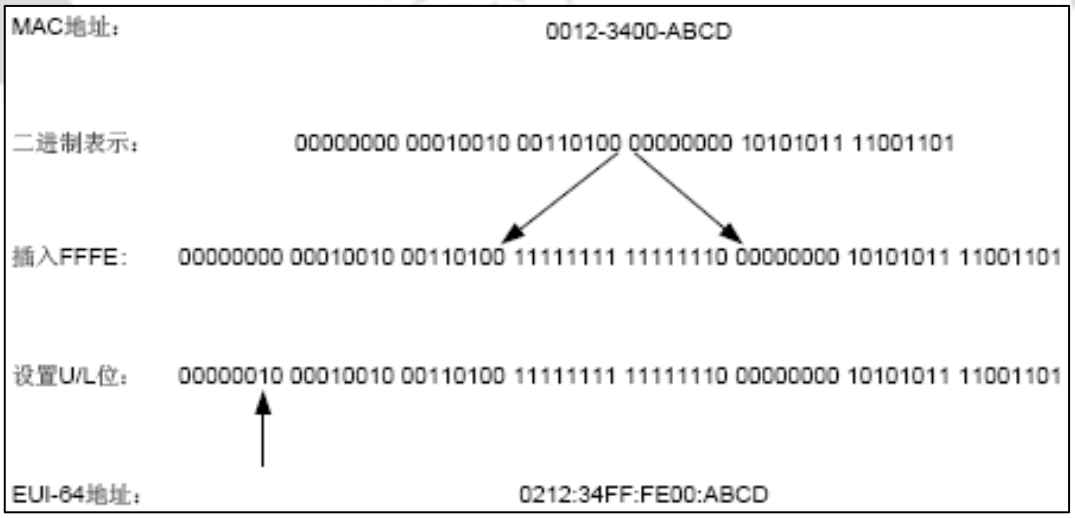
FF02:0:0:0:0:1:FFXX:XXXX

其中，FF02:0:0:0:0:1:FF 为 104 位固定格式；XX:XXXX 为单播或任播 IPv6 地址的后 24 位。

IEEE EUI-64 格式的接口标识符

IPv6 单播地址中的接口标识符用来标识链路上的一个唯一的接口。目前 IPv6 单播地址基本上都要求接口标识符为 64 位。IEEEEUI-64 格式的接口标识符是从接口的链路层地址（MAC 地址）变化而来的。IPv6 地址中的接口标识符是 64 位，而 MAC 地址是 48 位，因此需要在 MAC 地址的中间位置（从高位开始的第 24 位后）插入十六进制数 FFFE（1111111111111110）。为了确保这个从 MAC 地址得到的接口标识符是唯一的，还要将 Universal/Local(U/L)位从高位开始的第 7 位设置为1”。最后得到的这组数就作为 EUI-64 格式的接口标识符。

图4-2 MAC 地址到 EUI-64 格式的接口标识符的转换过程



4.1.3 IPv6 邻居发现协议介绍

IPv6 邻居发现协议使用五种类型的 ICMPv6 消息，实现下面一些功能：地址解析、验证邻居是否可达、重复地址检测、路由器发现/前缀发现及地址自动配置、重定向等功能。

邻居发现协议使用的 ICMPv6 消息的类型及作用如表 1-3 所示。

表4-3邻居发现协议使用的 ICMPv6 消息类型及作用

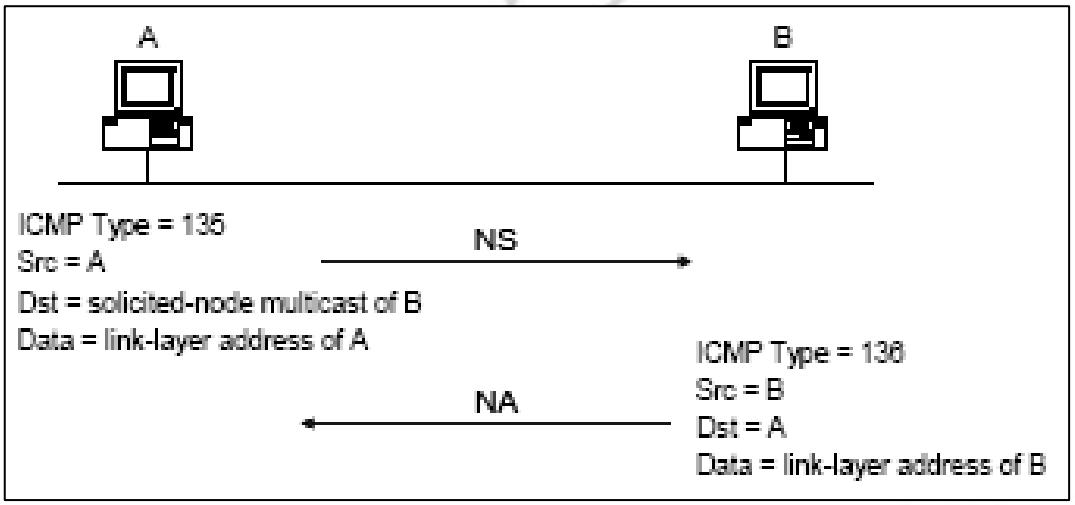
ICMPv6 消息	作用
邻居请求消息 NS（Neighbor Solicitation）	获取邻居的链路层地址
	验证邻居是否可达
	进行重复地址检测
邻居通告消息 NA（NeighborAdvertisement）	对 NS 消息进行响应
	节点在链路层变化时主动发送 NA 消息，向邻居节点通告本节点的变化信息
地路由器请求消息 RS（RouterSolicitation）	主机启动后，通过 RS 消息向路由器发出请求，请求前缀和其他配置信息，用于主机的自动配置
路由器通告消息 RA（RouterAdvertisement）	对 RS 消息进行响应
	在没有抑制 RA 消息发布的条件下，路由器会周期性地发布 RA 消息，其中包括前缀和一些标志位的信息
重定向消息（Redirect）	当满足一定的条件时，缺省网关通过向源主机发送重定向消息，使主机重新选择正确的下一跳地址进行后续报文的发送

邻居发现协议提供的主要功能如下：

地址解析

获取同一链路上邻居节点的链路层地址（与 IPv4 的 ARP 功能相同），通过邻居请求消息 NS 和邻居通告消息 NA 实现。如图 1-3 所示，节点 A 要获取节点 B 的链路层地址。

图4-3 地址解析示意图



- 节点 A 以组播方式发送 NS 消息。NS 消息的源地址是发送 NS 消息的节点 A 的接口 IPv6 地址，目的地址是节点 B 的被请求节点组播地址，消息内容中包含了节点 A 的链路层地址。
- 节点 B 收到 NS 消息后，判断报文的目的地址是否为自己的 IPv6 地址对应的被请求节点组播地址。如果是，则以单播方式返回 NA 消息，其中包含了自己的链路层地址。
- 节点 A 从收到的 NA 消息中就可获取到节点 B 的链路层地址之后双方即可通信。

验证邻居是否可达

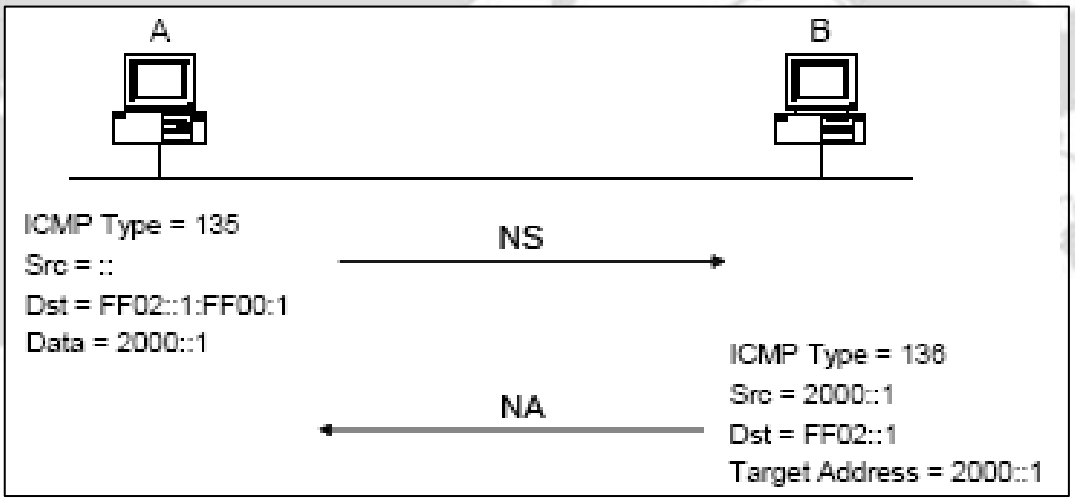
在获取到邻居节点的链路层地址后，通过邻居请求消息 NS 和邻居通告消息 NA 可以验证邻居节点是否可达。

- 节点发送 NS 消息，其中目的地址是邻居节点的 IPv6 地址。
- 如果收到邻居的确认报文，则认为邻居可达；否则，认为邻居不可达。

重复地址检测

当节点获取到一个 IPv6 地址后，需要使用重复地址检测功能确定该地址是否已被其他节点使用（与 IPv4 的免费 ARP 功能相似）。通过邻居请求消息 NS 和邻居通告消息 NA 实现，如下图所示。

图4-4 重复地址检测示意图



- 节点 A 发送 NS 消息，NS 消息的源地址是未指定地址::，目的地址是想要检测的 IPv6 地址对应的被请求节点组播地址，消息内容中包含了想要检测的 IPv6 地址。
- 如果节点 B 已经使用这个 IPv6 地址，则会返回 NA 消息。其中包含了自己的 IPv6 地址。
- 节点 A 收到节点 B 发来的 NA 消息，就知道该 IPv6 地址已被使用。反之，则说明该地址未被使用，节点 A 就可使用此 IPv6 地址。

路由器发现/前缀发现及地址自动配置

路由器发现及前缀发现是指主机从收到的 RA 消息中获取邻居路由器及所在网络的前缀，以及其他配置参数。

地址无状态自动配置是指主机根据路由器发现/前缀发现所获取的信息，自动配置 IPv6 地址。

路由器发现/前缀发现通过路由器请求消息 RS 和路由器通告消息 RA 来实现，具体过程如下：

- 主机启动时，通过 RS 消息向路由器发出请求，请求前缀和其他配置信息，以便用于主机的配置。
- 路由器返回 RA 消息，其中包括前缀和一些标志位的信息（路由器也会周期性地发布 RA 消息）。
- 主机利用路由器返回的 RA 消息中的地址前缀及其他配置参数，自动配置接口的 IPv6 地址及其他信息。

重定向功能

当主机启动时，它的路由表中可能只有一条到缺省网关的缺省路由。当满足一定的条件时，缺省网关会向源主机发送 ICMPv6 重定向消息，通知主机选择更好的下一跳进行后续报文的发送（与 IPv4 的 ICMP 重定向消息的功能相同）。

设备在满足下列条件时会发送对主机重定向的 ICMPv6 重定向报文：

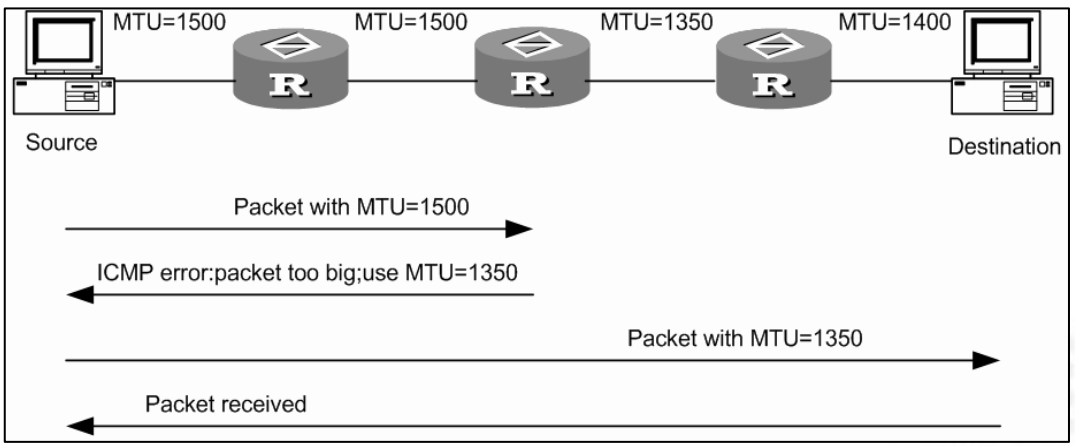
- 接收和转发数据报文的接口是同一接口；
- 被选择的路由本身没有被 ICMPv6 重定向报文创建或修改过；
- 被选择的路由不是缺省路由；
- 被转发的 IPv6 数据报文中不包含路由扩展头；

4.1.4 IPv6PMTU 发现

报文从源端到目的端的传输路径中所经过的链路可能具有不同的 MTU。在 IPv6 中，当报文的长度大于链路的 MTU 时，报文的分片将在源端进行，从而减轻中间转发设备的处理压力，合理利用网络资源。

PMTU（PathMTU，路径 MTU）发现机制的目的就是要找到从源端到目的端的路径上最小的 MTU。PMTU 发现的工作过程如下图所示。

图4-5 PMTU 发现的工作过程



- 源端主机使用自己的 MTU 对报文进行分片，之后向目的主机发送报文。
- 中间转发设备接收到该报文进行转发时，如果发现转发报文的接口支持的 MTU 值小于报文长度，则会丢弃报文，并给源端返回一个 ICMPv6 差错报文，其中包含了转发失败的接口的 MTU。
- 源主机收到该差错报文后，将使用报文中所携带的 MTU 重新对报文进行分片并发送。
- 如此反复，直到目的端主机收到这个报文，从而确定报文从源端到目的端路径中的最小 MTU。

4.1.5 IPv6 过渡技术简介

随着 Internet 的日益膨胀，现有的 IPv4 地址已经十分紧缺，虽然使用分配临时 IPv4 地址或 NAT（NetworkAddressTranslator，网络地址转换）等技术，在一定程度上缓解了 IPv4 地址不足的状况，但也增加了地址解析和处理方面的开销，同时导致某些高层应用失效，而且仍然无法回避 IPv4 地址即将被分配殆尽这个问题。采用 128 位地址长度的 IPv6 协议，彻底解决了 IPv4 地址不足的难题，并且在地址容量、安全性、网络管理、移动性以及服务质量等方面有明显的改进，是下一代互联网络协议采用的核心标准之一。IPv6 与 IPv4 不兼容，但它同所有的 TCP / IP 协议族中的其他协议兼容，即 IPv6 完全可以取代 IPv4。

在 IPv6 成为主流协议之前，首先使用 IPv6 协议栈的网络希望能与当前仍被 IPv4 支撑着的 Internet 进行正常通信，因此必须开发出 IPv4 和 IPv6 互通技术以保证 IPv4 能够平稳过渡到 IPv6。此外，互通技术应该对信息传递做到高效无缝。国际上 IETF 组建了专门的 NGTRANS 工作组，开展对 IPv4 和 IPv6 过渡问题和高效无缝互通问题的研究。目前已经出现了多种过渡技术和互通方案，这些技术各有特点，用于解决不同过渡时期、不同环境的通信问题。

目前解决过渡问题的基本技术主要有 3 种：双协议栈（RFC2893），隧道技术（RFC2893）和 NAT-PT(RFC2766)。

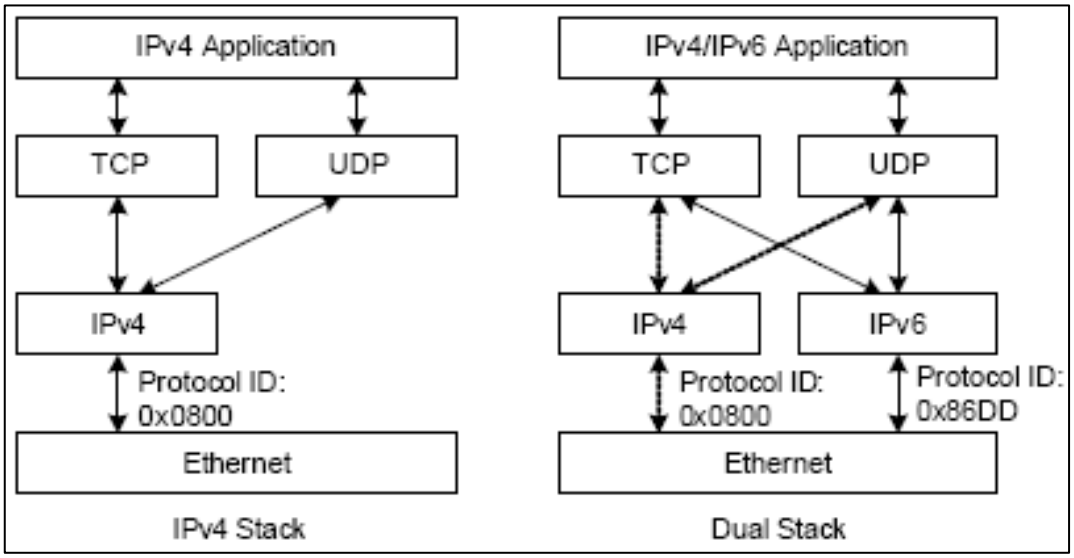
提示：

本设备支持双协议栈和隧道技术。

对于 IPv6 节点来说，兼容 IPv4 的最直接有效的办法就是保留一个完整的 IPv4 协议栈。同时支持 IPv4 协议和 IPv6 协议的网络节点即成为双协议栈节点。当双协议栈节点配置 IPv4 地址和 IPv6 地址后，就可以在相应接口上转发 IPv4 和 IPv6 报文。

当一个上层的应用支持 IPv4 和 IPv6 协议时，根据协议要求可以选用 TCP 或 UDP 作为传输层的协议，但在选择网络层协议时，它会优先选择 IPv6 协议栈。

图4-6 IPv4 单协议栈和 IPv4/IPv6 双协议栈的结构图



4.1.6 IPv6 隧道技术简介

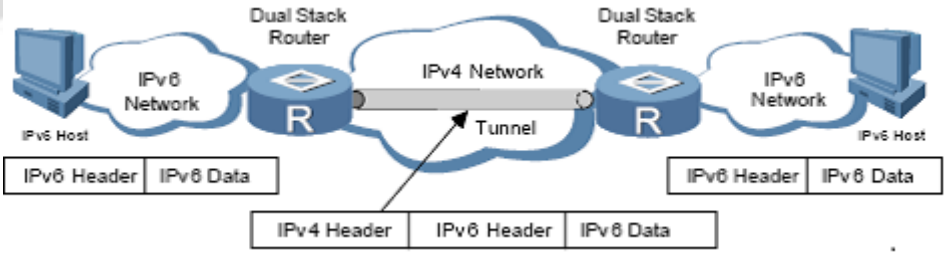
Tunnel（隧道）技术是 VPN（VirtualPrivateNetwork）中广泛采用的一种第三层隧道协议。Tunnel 是一个虚拟的点对点的连接，在实际应用中仅支持点对点连接的虚拟接口为 Tunnel 接口。一个 Tunnel 提供了一条使封装的数据报文能够传输的通路，并且在一个 Tunnel 的两端可以分别对数据报进行封装及解封装。

本设备支持配置 IPv6 in IPv4 隧道。

IPv6 in iPv4 隧道原理

IPv6inIPv4 隧道机制是将 IPv6 数据报文封装上 IPv4 的报文头,通过隧道 Tunnel）使 IPv6 报文穿越 IPv4 网络，实现隔离的 IPv6 网络的互通，如下图所示。

图4-7 IPv6 in IPv4 隧道原理图



注意：

IPv6 in IPv4 隧道两端的设备必须支持 IPv4/IPv6 双协议栈。

IPv6 inIPv4 隧道对报文的处理过程如下：

- IPv6 网络中的设备发送 IPv6 报文，到达隧道的源端设备；
- 隧道的源端设备根据路由表判定该报文要通过隧道进行转发，将会在 IPv6 报文前封装上 IPv4 的报文头，通过隧道的实际物理接口将报文转发出去；

- 封装报文通过隧道到达隧道目的端设备,目的端设备判断该封装报文的目的地是本设备后，将对报文进行解封装。
- 目的端设备根据解封装后的 IPv6 报文的目的地址将报文进行转发；如果目的地就是本设备，则将 IPv6 报文转给上层协议处理。

IPv6 in IPv4 隧道模式

IPv6iniPv4 隧道可以建立在主机-主机、主机-设备、设备-主机、设备-设备之间。隧道的终点可能是 IPv6 报文的最终目的地，也可能需要进一步转发。

根据隧道终点的 IPv4 地址的获取方式不同，隧道分为“配置隧道”及“自动隧道”。

- 如果隧道的终点不是IPv6报文的最终目的地,当IPv6报文通过隧道到达隧道终点后，隧道终点设备（通常为路由器）会对封装的 IPv6 报文进行解封装，并转发 IPv6 报文到最终目的地。在这种情况下，不能从 IPv6 报文的目的地址中自动获取到隧道终点的 IPv4 地址,需要进行手工配置。这样的隧道即为“配置隧道”。
- 如果隧道的终点就是 IPv6 报文的最终目的地,则可以采用内嵌 IPv4 地址的特殊 IPv6 地址形式，实现从 IPv6 报文的目的地址中自动获取隧道终点的 IPv4 地址。这样的隧道即为“自动隧道”。

根据对 IPv6 报文的封装方式的不同，IPv6 inIPv4 隧道分为以下几种模式：

- 手动隧道
- 6to4 隧道
- ISATAP（Intra-SiteAutomaticTunnelAddressingProtocol，站点内自动隧道寻址协议）隧道

在上面列出的隧道模式中，手动隧道为配置隧道；IPv4 兼容 IPv6 自动隧道、6to4 隧道及 ISATAP 隧道为自动隧道。

手动隧道

手动隧道是点到点之间的链路，一条链路就是一个单独的隧道。主要用于边缘路由器-边缘路由器或主机-边缘路由器之间定期安全通信的稳定连接，可实现与远端 IPv6 网络的连接。

6to4 隧道

6to4 隧道是点到多点的自动隧道,主要用于将多个 IPv6 孤岛通过 IPv4 网络连接到 IPv6 网络。6to4 隧道通过 IPv6 报文的目的地址中嵌入的 IPv4 地址，可以自动获取隧道的终点。6to4 隧道采用特殊的地址：6to4 地址，其格式为：2002:abcd:efgh: 子网号::接口 ID/64，其中 abcd:efgh 表示该 6to4 隧道对应的 32 位 IPv4 源地址，用

16 进制表示（如 1.1.1.1 可以表示为 0101:0101）。通过这个嵌入的 IPv4 地址可以自动确定隧道的终点，使隧道的建立非常方便。

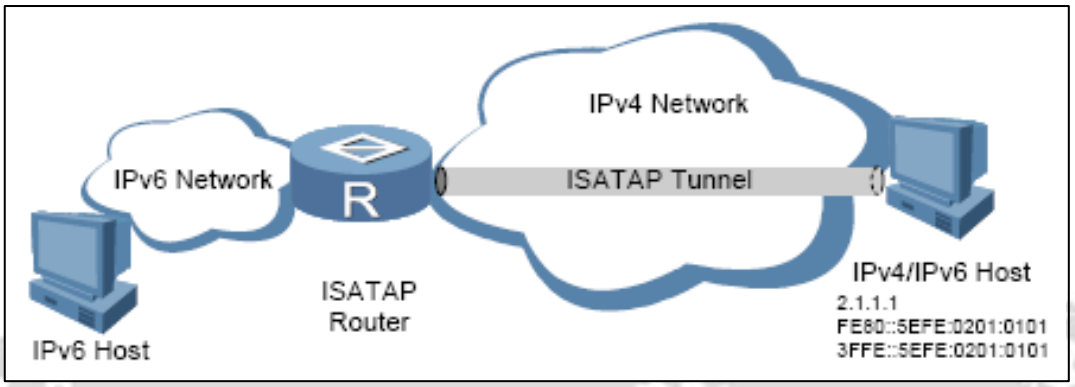
由于 6to4 地址的 64 位地址前缀中的 16 位子网号可以由用户自定义，前缀中的前

48 位已由固定数值、隧道起点或终点设备的 IPv4 地址确定，使 IPv6 报文通过隧道进行转发成为可能。6to4 隧道可以实现 IPv6 网络的互连，克服了 IPv4 兼容 IPv6 自动隧道使用的局限性。

ISATAP 隧道

随着 IPv6 技术的推广现有的 IPv4 网络中将会出现越来越多的 IPv6 主机ISATAP 隧道技术为这种应用提供了一个较好的解决方案。ISATAP 隧道是点到点的自动隧道技术，通过在 IPv6 报文的目的地址中嵌入的 IPv4 地址，可以自动获取隧道的终点。使用 ISATAP 隧道时，IPv6 报文的目的地址和隧道接口的 IPv6 地址都要采用特殊的地址:ISATAP 地址。ISATAP 地址格式为:Prefix(64bit):0:5EFE:ip-address。 ip-address 形式为 a.b.c.d 或者 abcd:efgh,其中 abcd:efgh 表示 32 位 IPv4 源地址。通过这个嵌入的 IPv4 地址就可以自动建立隧道，完成 IPv6 报文的传送。ISATAP 隧道主要用于在 IPv4 网络中 IPv6 路由器-IPv6 路由器、主机-路由器的连接。

图4-8 ISATAP 隧道



4.2 配置IPv6

4.2.1 配置 IPv6 单播地址

IPv6 站点本地地址和全球单播地址可以通过下面两种方式配置：

- 采用 EUI-64 格式形成:当配置采用 EUI-64 格式形成 IPv6 地址时接口的 IPv6 地址的前缀是所配置的前缀，而接口标识符则由接口的链路层地址转化而来。
- 手工配置：用户手工配置 IPv6 站点本地地址或全球单播地址。

IPv6 的链路本地地址可以通过两种方式获得：

- 自动生成：设备根据链路本地地址前缀（FE80::/64）及接口的链路层地址，自动为接口生成链路本地地址；
- 手动指定：用户手工配置 IPv6 链路本地地址。

提示：

1）当接口配置了 IPv6 站点本地地址或全球单播地址后，同时会自动生成链路本地地址。且与采用 ipv6 address auto link-local 命令生成的链路本地地址相同。此时如果手工指定接口的链路本地地址，则手工指定的有效。如果删除手工指定的链路本地地址，则接口的链路本地地址恢复为系统自动生成的地址。

2）配置链路本地地址时，手工指定方式的优先级高于自动生成方式。即如果先采用自动生成方式，之后手工指定，则手工指定的地址会覆盖自动生成的地址；如果先手工指定，之后采用自动生成的方式，则自动配置不生效，接口的链路本地地址仍是手工指定的。

此时如果想要改为自动配置，则必须先删除手工指定的地址，再配置采用自动生成的方式。

3）在 LoopBack 接口视图下配置 IPv6 站点本地地址或全球单播地址时，只能配置 128 位的前缀长度

注意：

1）本设备只支持手动配置 IPv6 全球单播地址或站点本地地址 IPv6 地址；

2）本设备自动生成接口的 IPv6 链路本地地址，无需配置。

配置 IPv6 单播地址

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	interface IFNAME	进入接口模式
步骤**3**	pv6 address ipv6-address/prefix-length	配置IPv6全球单播地址或站点本地地址 手工指定 IPv6地址

4.2.2 配置 IPv6 邻居发现协议

用户可以根据实际情况，配置接口是否发送 RA 消息及发送 RA 消息的时间间隔，同时可以配置 RA 消息中的相关参数以通告给主机。当主机接收到 RA 消息后，就可以采用这些参数进行相应操作。可以配置的 RA 消息中的参数及含义如表 1-8 所示。

表 1-6RA 消息中的参数及描述

参数	描述
前缀信息（Prefix Information）	在同一链路上的主机收到设备发布的前缀信息后，可以进行无状态自动配置等操作
被管理地址配置标志位（M flag）	用于确定主机是否采用有状态自动配置获取IPv6地址如果设置该标志位为1，主机将通过有状态自动配置（例如DHCP 服务器）来获取IPv6地址；否则，将通过无状态自动配置获取IPv6 地址，即根据自己的链路层地址及路由器发布的前缀信息生成IPv6 地址
其他配置标志位（O flag）	用于确定主机是否采用有状态自动配置获取除IPv6地址外的其他信息 如果设置其他配置标志位为1，主机将通过有状态自动配置（例如 DHCP服务器）来获取除IPv6地址外的其他信息；否则，将通过无状态自动配置获取其他信息
路由器生存时间ra-lifetime）	用于设置发布RA消息的路由器作为主机的默认路由器的时间，主机根据接收到的RA消息中的路由器生存时间参数值，就可以确定是否将发布该RA消息的路由器作为默认路由器
邻居请求消息重传时间间隔（**ra-interval**）	设备发送NS消息后，如果未在指定的时间间隔内收到响应，则会重新发送NS消息

保持邻居可达状态的时间（**reachable-time**）	当通过邻居可达性检测确认邻居可达后，在所设置的可达时间内，设备认为邻居可达；超过设置的时间后，如果需要向邻居发送报文，会重新确认邻居是否可达

提示：

在接口上配置的邻居请求消息重传时间间隔及保持邻居可达状态的时间，既可作为 RA 消息中的信息发布给主机，也可作为本接口发送邻居请求消息的时间间隔及保持邻居可达状态的时间。

注意：

RA 消息发布的最大间隔时间应该小于或等于 RA 消息中路由器的生存时间

配置 RA 消息的相关参数。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	interface IFNAME	进入接口模式
步骤**3**	ipv6 nd send-ra	取消对RA消息发布的抑制 必选 缺省情况下，抑制发布RA消息
步骤**4**	ipv6 nd ra-interval SECONDS	配置RA消息发布的时间间隔 缺省情况下，RA消息发布最大时间间隔为600秒，最小时间间隔为200秒 RA 消息周期性发布时，相邻两次的时间间隔是在最大时间间隔与最小时间间隔之间随机选取一个值作为周期性发布RA消息的时间间隔 配置的最小时间间隔应该小于等于最大时间间隔的 0.75 倍；RA消息发布的最大实际间隔应该小于或等于 RA消息中路由器的生存时间
步骤**5**	ipv6 nd prefix-advertisement IPV6PREFIX VALID PREFERRED [onlink] [autoconfig]	配置RA消息中的前缀信息 缺省情况下，没有配置 RA 消息中的前缀信息，此时将使用发送 RA 消息的接口 IPv6 地址作为 RA 消息中的前缀信息
步骤**6**	ipv6 nd managed-config-flag	配置被管理地址配置标志位为1 缺省情况下，被管理地址标志位为0，即主机通过无状态自动配置获取 IPv6 地址
步骤**7**	ipv6 nd other-config-flag	配置其他配置标志位为1 可选缺省情况下，其他配置标志位为 0，即主机通过无状态自动配置获 取其他信息
步骤**8**	ipv6 nd ra-lifetime SECONDS	配置RA消息中路由器的生存时间 缺省情况下，RA 消息中路由器的生存时间为 1800 秒 RA 消息中路由器的生存时间应该大于或等于 RA 消息的发布时间间隔
步骤**9**	ipv6 nd ra-interval SECONDS	配置邻居请求消息重传时间间隔 缺省情况下，接口发送 NS 消息的间间隔为 1000 毫

		秒，接口发布的RA消息中Retrans Timer字段的值为0
步骤10	ipv6 nd reachable-time MILLISECONDS	配置保持邻居可达状态的时间 可选缺省情况下接口保持邻居可达状 态的时间为30000毫秒，接口发 布的RA消息中ReachableTimer 字段的值为0

4.2.3 配置 IPv6 静态路由

配置 IPv6 静态路由

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	ipv6 route X:X::X:X/M (X:X::X:X |INTERFACE_NAME) [<1-255><1-100>]	配置IPv6静态路由
步骤3	no ipv6 route X:X::X:X/M (X:X::X:X |INTERFACE_NAME)	取消IPv6静态路由配置
步骤4	show ipv6 route	显示IPv6路由表

4.2.4 配置 IPv6 策略路由

配置 IPv6 策略路由

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	proute6 *(IF_IN|**any**) (SIP|**any**) (DIP|**any**) (SEV|**any**) (USER|**any**) (APP|**any**) (SCHEDULE|**always**) (blackhole|throw|unicast)* [**ID***<1-65535>*]	配置路由策略的匹配条件，将满足策略的数据包路由至下一跳，此命令可配置多条。匹配的顺序按显示的先后顺序来匹配
步骤3	*nexthopinterface (OUT_IN) gateway (IPv6 address)*[**weight***<1-255>*]	配置策略路由的下一跳，此命令可以配置多条。按照weight的分配流量。
步骤4	exit	返回特权模式

调整策略路由的顺序

用 move 命令可以调整策略路由的顺序，从而使位置在前的策略优先匹配。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	proute6 move <*1-65535*>[before | after] <*1-65535*>	移动一条策略路由到指定的策略路由之前

4.2.5 配置 IPv6 管理设备

配置 IPv6 管理设备。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	interface IFNAME	进入接口模式
步骤**3**	allow ping	配置允许ping
步骤**4**	allow http	配置允许http管理
步骤**5**	allow https	配置允许https管理
步骤**6**	allow telnet	配置允许telnet管理
步骤**7**	allow ssh	配置允许ssh管理

4.2.6 配置 IPv6 包过滤

配置 IPv6 包过滤。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	policy-v6 <1-9999> (*IF_IN*|any) (*IF_OUT*|any) (*SIP*|any) (*DIP*|any) *CMD_GROUP_SERVICE* (*USER*|any)(*APP*any) (*TR*|always)(permit|deny)	添加防火墙策略
步骤**3**	show policy	查看防火墙策略

参数说明： **policy-v6 <1-9999> *(IF_IN|any) (IF_OUT|any) (SIP|any) (DIP|any) CMD_GROUP_SERVICE (USER|any)(APP|any) (TR|always)(permit|deny)***

参数	说明	缺省配置
<1-9999>	策略ID	
IF_IN	策略匹配的入接口	无
IF_OUT	策略匹配的出接口	无
SIP	策略匹配的源IP	无
DIP	策略匹配的目的IP	无
CMD_GROUP_SERVICE	策略匹配的服务	无
USER	策略匹配的用户名	无
APP	策略匹配的应用	无
TR	策略生效的时间	无
PERMIT|DENY	策略动作	无

4.2.7 配置 IPv6 扩展头过滤

配置 IPv6 扩展头过滤。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	ipv6 ext-hdr filter (exthdr_auth | exthdr_dest | exthdr_esp | exthdr_fragment | exthdr_hop | exthdr_routing)	配置扩展头过滤，可选身份验证头、目的地选项头、封装安全性净荷头、分段头、逐跳选项头、选路头

4.2.8 配置 IPv6-MAC 绑定

添加一项 IP-MAC 绑定，需要输入 IP 地址、MAC 地址。

配置步骤：

步骤**1**	config terminal	进入配置模式
步骤**2**	ipv6 mac bind X:X::X:X FF-FF-FF-FF-FF-FF	配置一条IP-MAC绑定

config 模式下使用 no ipv6 mac bind X:X::X:X 清除一条绑定项。

4.2.9 配置 DNSv6 服务器

配置 DNSv6 服务器。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	dns listener6X:X::X:X	配置ipv6监听地址
步骤3	dns server	进入dns服务器配置
步骤4	zone ZONE_NAME	配置名称
步骤5	primiry-server HOST-NAME	配置主服务器
步骤6	e-mailEMAIL_ADDRESS	配置邮件地址
步骤7	default-ttl<0-214748364>	配置ttl，默认86400
步骤8	refresh <0-214748364>	配置刷新时间，默认10800
步骤9	retry<0-214748364>	配置重试时间，默认3600
步骤10	espire <0-214748364>	配置到期时间，默认604800
步骤11	negative-ttl<0-214748364>	配置错误缓存时间，默认3600
步骤12	rr type-aaaa DOMAIN_NAMEX:X::X:X [<0-2147483647>]	配置NS记录信息
步骤13	rr type-nsDOMAIN_NAMESERVER_NAME[<0-2147483647>]	配置dns记录
步骤13	exit	退出配置
步骤14	add zone ZONE_NAME	添加zone

4.2.10 配置 DHCPv6 服务器

配置 DHCPv6。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	dhcp	进入DHCP配置模式
步骤3	poolv6 IFNAME	增加子网的地址池,其租约为所配置的时间

	X:X::X:XX:X::X:X<300-2592000>

4.2.11 配置 IPv4/IPv6 双协议栈

为了实现双协议栈功能，必须先使能 IPv6 功能。否则即使配置了接口的 IPv6 地址，仍无法转发 IPv6 的报文。

配置双协议栈。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	interface IFNAME	进入接口模式
步骤3	ip addressA.B.C.D/M	配置接口的IPV4地址
步骤4	ipv6 addressX:X::X:X/M	配置接口的IPV6地址

4.2.12 配置 IPv6 手动隧道

配置手动隧道。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	interface tunnel <*number*> mode ipv6-ipv4 manual	创建Tunnel接口（手动隧道）并进入Tunnel接口模式
步骤3	ipv6 addressX:X::X:X/M	配置Tunnel接口的IPv6地址
步骤4	tunnel-source *ip-address*	配置Tunnel接口的源端地址 缺省情况下，Tunnel接口上没有配置源端地址
步骤5	tunnel-destination *ip-address*	配置Tunnel接口的目的端地址 缺省情况下，Tunnel接口上没有配置目的端地址

注意：

1）以上各项 Tunnel 接口下进行的功能特性配置，在删除 Tunnel 接口后，该接口上的所有配置也将被删除。

2）如果隧道两端 Tunnel 接口的地址不在同一个网段，则必须配置通过隧道到达对端的转发路由，以便需要进行封装的报文能正常转发。

3）配置静态路由时，需要手动配置到达目的地址（不是隧道的终点 IPv4 地址，而是封装前报文的目的 IPv6 地址）的路由，并将下一跳配置为隧道本端的 Tunnel 接口号或者网络地址。在隧道的两端都要进行此项配置。

4）配置动态路由时，需要在隧道两端的 Tunnel 接口使能动态路由协议。在隧道的两端都要进行此项配置。

4.2.13 配置 IPv6 6to4 隧道

配置 6to4 隧道。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	interface tunnel <*number*>mode ipv6-ipv4 6to4	创建Tunnel接口(6to4隧道)并进入Tunnel接口模式
步骤**3**	ipv6 addressX:X::X:X/M	配置Tunnel接口的IPv6地址
步骤**4**	tunnel-source *ip-address*	配置Tunnel接口的源端地址 缺省情况下，Tunnel接口上没有配置源端地址

注意：

1）同一隧道起点只能创建一条自动隧道。

2）自动隧道不需要配置目的地址，因为自动隧道的目的地址可以通过 IPv4 兼容 IPv6 地址中嵌入的 IPv4 地址自动获得。

3）如果隧道两端 Tunnel 接口的地址不在同一个网段，则必须配置通过隧道到达对端的转发路由，以便需要进行封装的报文能正常转发。

4）配置静态路由时，需要手动配置到达目的地址（不是隧道的终点 IPv4 地址，而是封装前报文的目的 IPv6 地址）的路由，并将下一跳配置为隧道本端的 Tunnel 接口号或者网络地址。在隧道的两端都要进行此项配置。

4.2.14 配置 IPv6 ISATAP 隧道

配置 ISATAP 隧道

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	interface tunnel <*number*>mode ipv6-ipv4 isatap	创建Tunnel接口（ISATAP隧道模式）并进入Tunnel接口模式
步骤**3**	ipv6 addressX:X::X:X/M	配置Tunnel接口的IPv6地址
步骤**4**	tunnel-source *ip-address*	配置Tunnel接口的源端地址 缺省情况下，Tunnel接口上没有配置源端地址

注意：

如果隧道两端 Tunnel 接口的地址不在同一个网段，则必须配置通过隧道到达对端的转发路由，以便需要进行封装的报文能正常转发。

配置静态路由时，需要手动配置到达目的地址（不是隧道的终点 IPv4 地址，而是封装前报文的目的 IPv6 地址）的路由，并将下一跳配置为隧道本端的 Tunnel 接口号或者网络地址。在隧道的两端都要进行此项配置。

4.3 配置案例

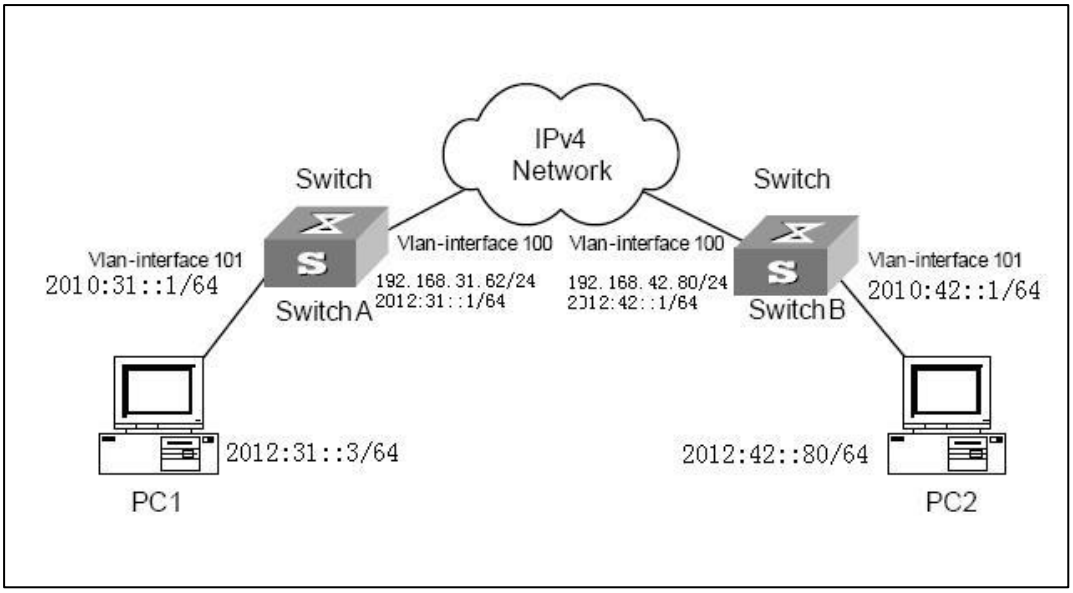
4.3.1 配置案例 1：基本 IPv6 手动隧道

案例描述

假定网络环境如下图所示，PC1 和 PC2 分属两个遥远的不同网段的 IPv6 网络，两者之间已有 IPv4 网络可以互访。

可以在设备 A 和设备 B 上配置 IPv6 手动隧道，实现 PC1 和 PC2 之间的 IPv6 数据相互访问。

图4-9 案例组网图



配置步骤：

设备 A 的配置：

步骤**1**	进入配置模式
	DCFW-1800_A#configure terminal
步骤**2**	配置接口IPv4地址和IPv6地址
	DCFW-1800_A(config)# interface ge0/0 DCFW-1800_A(config- ge0/0)# ip address 192.168.31.62/24 DCFW-1800_A(config- ge0/0)# ipv6 address 2012:31::1/64 DCFW-1800_A(config- ge0/0)# exit
步骤**3**	创建ipv6手动隧道，并配置源和对端地址
	DCFW-1800_A(config)# interface tunnel 101 mode ipv6-ipv4 manual DCFW-1800_A(config-tunnel101)# ipv6 address 2010:31::1/64 DCFW-1800_A(config-tunnel101)# tunnel -source192.168.31.62 DCFW-1800_A(config-tunnel101)# tunnel -destination 192.168.42.80 DCFW-1800_A(config-tunnel101)# exit
步骤**4**	配置ipv6路由
	DCFW-1800_A(config)# ipv6 route 2012:42::0/64 tunnel101 DCFW-1800_A(config)# ipv6 route 2010:42::0/64 tunnel101

设备 B 的配置：

步骤**1**	启用ipv6
	DCFW-1800_B#configure terminal DCFW-1800_B(config)# ipv6 enable
步骤**2**	配置接口IPv4地址和IPv6地址
	DCFW-1800_B(config)# interface ge0/0 DCFW-1800_B(config- ge0/0)# ip address 192.168.42.80/24 DCFW-1800_B(config- ge0/0)# ipv6 address 2012:42::1/64 DCFW-1800_B(config- ge0/0)# exit
步骤**3**	创建ipv6手动隧道，并配置源和对端地址
	DCFW-1800_B(config)# interface tunnel 101 mode ipv6-ipv4 manual DCFW-1800_B(config-tunnel101)# ipv6 address 2010:42::1/64 DCFW-1800_B(config-tunnel101)# tunnel-source192.168.42.80 DCFW-1800_B(config-tunnel101)# tunnel -destination 192.168.31.62.80 DCFW-1800_B(config-tunnel101)# exit
步骤**4**	配置ipv6路由
	DCFW-1800_B(config)# ipv6 route 2012:31::0/64 tunnel101 DCFW-1800_B(config)# ipv6 route 2010:41::0/64 tunnel101

4.4 IPv6监控与维护

4.4.1 查看 IPv6 隧道

完成 IPv6 隧道配置后，在任意模式下执行 show 命令，可以显示配置 IPv6 隧道后的运行情况。通过查看显示信息，用户可以验证配置的效果。

配置步骤：

步骤**1**	showinterface ***tunl<number>***	显示指定Tunnel接口的相关信息
步骤**2**	showiptunnel***[IFNAME]***	显示指定Tunnel接口的IPv6相关

4.4.2 常见故障分析

故障现象：在 Tunnel 接口上配置了相关的参数后（例如隧道的起点、终点地址和隧道模式）仍未处于 Up 状态。

分析	Tunnel接口未处于Up状态的最常见原因是隧道起点的物理接口没有处于Up 状态。使用show interfacetunnel和showiptunnel命令查看隧道起点的物理接口状态为Up还是Down。
解决	Tunnel接口未处于Up状态的另一个可能的原因是隧道的终点地址不可达.使用showipv6route和showiproute命令查看是否终点 地址通过路由可达。如果路由表中没有保证隧道通讯的路由项，请配置相关路由。

第5章 配置 IPSec VPN

5.1 IPSec VPN概述

IPSec 使用加密和认证机制，为数据在公共网络环境中的传输提供安全保障。它能够为数据传输提供了以下安全服务：

- 数据的机密性——IPSec 使用 ESP 安全协议为数据传输提供加密保护。
- 数据的完整性——IPSec 使用 ESP 或 AH 安全协议为数据的传输提供完整性保护。这使得数据接收方可以及时地发现数据是否在传输的过程中被修改过。
- 数据源的认证——IPSec 接收方验证数据的来源。
- 抗重播——IPSec 的接收方可以检测到重播的 IP 包并丢弃。

通常，一个 IPSec 系统实现主要由以下部分组成：

- 安全协议——包括“封装安全载荷协议（以下简称 ESP）”和“认证头协议（以下简称 AH）”协议。ESP 可以提供数据的完整性、机密性和抗重播服务；AH 协议可以提供数据源认证、完整性和抗重播保护。
- 安全策略库（以下简称 SPDB）和安全关联库（以下简称 SADB）——安全策略库决定了对哪些 IP 报文进行处理，如何进行处理（丢弃、绕过、IPSec 处理）；安全关联库决定了对那些需要进行 IPSec 处理的 IP 报文的处理细节，如使用什么安全协议，加密算法，认证算法等。
- 密钥管理协议——用于协商建立、更新、删除 SA，包括 ISAKMP SA 和 IPSec SA。通常 IPSec 系统实现使用 IKE 密钥管理协议协商建立 SA。

相关术语解释：

- 认证头协议（AH）：用于验证数据包的安全协议。
- 封装安全载荷协议（ESP）：用于加密和验证数据包的安全协议；可与 AH 配合工作可也以单独工作。
- 加密算法：ESP 所使用的加密算法
- 验证算法：AH 或 ESP 用来验证对方的验证算法
- 密钥管理协议：用于完成共享密钥的建立、更新和删除。其中，IKE（Internet 密钥交换协议）是 IPSec 默认使用的密钥交换协议

构建 VPN 是 IPSec 的典型应用。本章主要详细介绍使用 IPSec 构建 VPN 的过程，并给出典型案例。单独使用设备集成的 IPSec VPN 子系统可以为网关之间、使用 VPN 客户端的主机和网关之间的数据传输提供安全保障。设备集成的 IPSec VPN 子系统具有以下功能：

- 支持路由模式和桥模式使用 IPSec。

- 支持隧道模式和传输模式。
- 使用 IKE 协议建立、更新、删除 SA。
- IKE 阶段 1 协商支持预共享密钥认证方法、RSA 签名认证方法、数字信封（国密）认证方法。
- 主模式协商和野蛮模式协商。
- 使用预共享密钥认证方法时，支持使用 IPv4 地址、FQDN、USER_FQDN 类型的 ID。使用 RSA 签名认证方法或数字信封（国密）认证方法时，使用证书的主题作为 ID。
- 支持静态接入（通过指定对端网关为静态 IP 或域名的方式）和动态接入（通过指定对端网关为动态 IP 的方式）。
- 支持双网关。当设定对端网关为静态 IP 时，允许设置冗余网关，这使得当本方与对端网关的主 IP 协商失败时，可以继续与对端网关的另一个 IP 协商。
- 支持丰富的加密算法和认证算法。
- 支持 DH 组 1、组 2、组 5。
- 支持 DPD 探测。
- 支持 NAT 穿越。
- 支持路由注入。通常，在多链路环境中使用 IPSec 时，启用路由注入功能后，可以在 IPSec SA 协商成功后，自动添加一条合适的路由。删除 IPSec SA 后，该路由会被清除。
- 支持扩展认证。
- 支持使用模式配置方式，为 VPN 客户端下发内部 IP、DNS 和 WINS。
- 支持单独或组合使用 ESP 协议和 AH 协议。
- 支持 PFS。
- 支持手工建立 IPSec SA。
- 提供 IPSec 配置向导快速建立配置。
- 符合国家密码管理局制定的《IPSec VPN 技术规范》。

5.2 配置IPSec VPN

5.2.1 缺省配置信息

表5-1表 IPSec VPN 缺省配置信息

内容	缺省设置	备注
密钥协商时协商双方的身份标识	预共享密钥方式默认为IKE协商使用的接口的IP地址；RSA签名和数字信封（国密）方式默认为证书的主题	采用预共享密钥认证方式时，可更改为FQDN、

		USER_FQDN
密钥协商验证对方的方式	预共享密钥(pre-shared)	可更改为RSA签名或数字信封（国密）
ISAKMP SA的生存期	86400秒	可更改设置
IPSec SA的生存期（时间方式）	3600秒	可更改设置
IPSec SA的生存期（流量方式）	0Kb	可更改设置
安全协议的工作方式	通道模式	可更改为传输模式
加密算法	3DES	可更改设置
验证算法	MD5	可更改设置
密钥协商模式	主模式	可更改野蛮模式
DPD对等体检测功能	不启用	可更改为启用
扩展认证	不启用	可更改设置
模式配置	不启用	可更改设置

5.2.2 配置 IKE 阶段 1

在全局配置模式下配置 IKE（Internet Key Exchange）阶段 1 的相关参数。IKE 协商发起方利用这些参数发起协商，通过与对对端协商建立 ISAKMP SA，从而为 IPSec SA 的协商建立安全环境。

配置步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	vpn ipsec phase1	进入阶段1的配置
步骤**3**	edit gateway NAME	编辑一个阶段1的名称,进入下一层结点
步骤**4**	authentication (pre-share|rsa-sig)	设置认证方法，密钥认证、数字认证
步骤**5**	set mode {main | aggressive}	设置阶段1的协商模式（数字信封（国密）认证方式不支持野蛮模式）
步骤**6**	set remotegw A.B.C.D|DOMAIN-NAME|dynamic	设置对端网关的地址
步骤**6.1**	set nat <10-900> no set nat	设置NAT保活报文发送间隔
步骤**7**	set localid (fqdn *ID_NAME*|user-fqdn	设置本地ID类型

	ID_NAME) no set localid [address]	
步骤8	set peerid(address *A.B.C.D*|fqdn *ID_NAME*|user-fqdn *ID_NAME)* no set peerid	设置对端ID类型
步骤8	authentication (pre-share|rsa-rig) no authentication	预共享秘钥认证 RSA数字证书认证
步骤9	dpd (enable|disable) no dpd	开启或禁用dpd功能
步骤10	set policy <*1-3*> no set policy <*1-3*>	添加、删除或修改一个加密提案
步骤11	encrypt (3des|des|aes128|aes192|aes256) hash (md5|sha)	设置加密算法；缺省为3des 设置HASH认证算法；缺省为md5
步骤12	group (1|2|5) no group	设置DH组
步骤13	lifetime <120-86400> no lifetime	设置一阶段sa的生命周期
步骤14	xauth-server (enable|disable) no xauth-server	开启或禁用扩展认证
步骤15	set modecfg-server no set modecfg-server	开启模式配置
步骤19	exit	退出当前设置

以上命令均可使用 no 命令取消对各个命令的设置，使其恢复到缺省配置。

参数说明：edit gateway NAME

参数	说明	缺省配置
NAME	阶段1的名称	缺省无设置

参数说明：set mode {main\|aggressive}

参数	说明	缺省配置
{main|aggressive}	设置阶段1的协商方式	缺省是主模式

参数说明：set remotegw A.B.C.D|DOMAIN-NAME dynamic

参数	说明	缺省配置
{A.B.C.D|DOMAIN-NAME dynamic}	设置对端网关的方式	缺省是IP地址

参数说明：set preshared-key KEY

参数	说明	缺省配置
KEY	密钥值。在设置认证方式为预共享密钥时有效。	无

参数说明：set local-cert NAME

参数	说明	缺省配置
NAME	本地证书名称。在设置认证方式为rsa签名或国密时有效。	无

参数说明：group (1\|2\|5)

参数	说明	缺省配置
(1|2|5)	在设置为预共享密钥或rsa签名方式时可配置密钥交换所采用的Diff-Hellmen数组	默认group2

参数说明：lifetime TIME

参数	说明	缺省配置
TIME	配置isakmp sa的生存期	默认是86400秒

参数说明：set policy <1-3>

参数	说明	缺省配置
<1-3>	配置IKE 策略，最多可以配置三组算法组合	缺省是policy1

参数说明：encrypt (des|3des|aes128|aes192|aes256|scb128)

参数	说明	缺省配置
(des|3des|aes128|aes192|aes256|scb128)	设置加密算法	预共享密钥和rsa签名默认是3DES加密。国密方式默认是SM1(对应于scb128)加密

参数说明：hash (md5|sha)

参数	说明	缺省配置
(md5|sha)	设置HASH认证算法	预共享密钥和rsa签名默认是默认是MD5认证。国密方式默认是SHA1认证

参数说明：set dpd <30-120>

参数	说明	缺省配置
<30-120>	设置对等体检测	缺省是0

参数说明：set nat <10-900>

参数	说明	缺省配置
<10-900>	设置NAT穿越的保活时间	缺省是0

参数说明：setid (local|peer)ID

参数	说明	缺省配置
ID	设置本地|对端ID值	缺省无设置

参数说明：set nexthop (primary|secondary) A.B.C.D/M

参数	说明	缺省配置
A.B.C.D/M	启用路由注入时，可设置下一跳为IP地址。通常在多链路的环境下使用。	缺省无设置

参数说明：set xauth-server USERGROUP

参数	说明	缺省配置
USERGROUP	扩展认证服务器指定的用户组	缺省无设置

参数说明：ip-range A.B.C.D A.B.C.D

参数	说明	缺省配置
A.B.C.D	模式配置地址池起始和结束地址	缺省无设置

参数说明：dnsA.B.C.D

参数	说明	缺省配置
A.B.C.D	配置服务器分配给客户端的dns	缺省无设置

参数说明：winsA.B.C.D

参数	说明	缺省配置
A.B.C.D	配置服务器分配给客户端的wins	缺省无设置

注意：

用户可以配置多条 IKE 策略，当设备进行 IKE 协商时试图协商到两端设备相同的 IKE 策略。

5.2.3 配置 IKE 阶段 2

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	vpn ipsec phase2	进入阶段2的配置
步骤3	edit tunnel*NAME* no edit tunnel*NAME*	添加、删除或编辑IPSEC
步骤4	set peer GATEWAY-NAME no set peer	为IPSEC指定一个一阶段（IKE）协商策略
步骤5	mode (tunnel|) no mode	指定IPSEC的封装模式
步骤6	pfs (1|2|5) no pfs	指定完美向前保密组
步骤7	set lifetime kilobytes<*2560-536870912*> set lifetime seconds<*120-86400*> no set lifetime kilobytes no set lifetime seconds	设置Ipsec sa生命周期

步骤8	auto-connect (enable|disable) no auto-connect	开启或禁用自动连接
步骤9	set (proposal1|proposal2|proposal3|proposal4)(esp-3des-md5|esp-aes128-sha1|esp-aes256-null|esp-null-md5|esp-3des-null|esp-aes192-md5|esp-aes256-sha1|esp-null-null|esp-3des-sha1|esp-aes192-null|esp-des-md5|esp-null-sha1|esp-aes128-md5|esp-aes192-sha1|esp-des-null|esp-aes128-null|esp-aes256-md5|esp-des-sha1)(ah-md5-hmac|ah-null|ah-sha-hmac) noset(proposal1|proposal2|proposal3|proposal4)	设置IPSEC加密提案
步骤10	exit	退出IPSec策略配置模式

以上命令均可使用 no 命令取消对各个命令的设置，使其恢复到缺省配置。

参数说明：edit tunnel NAME

参数	说明	缺省配置
NAME	编辑阶段2的名称	

参数说明：set peer GATEWAY

参数	说明	缺省配置
GATEWAY	阶段1的名称	

参数说明：set（propasal1\|propasal2\|propasal3）(esp-3des-md5\|esp-3des-null\|esp-3des-sha1\|esp-aes128-md5\|esp-aes128-null\|esp-aes128-sha1\|esp-aes192-md5\|esp-aes192-null\|esp-aes192-sha1\|esp-aes256-md5\|esp-aes256-null\|esp-aes256-sha1\|esp-des-md5\|esp-des-null\|esp-des-sha1\|esp-null-md5\|esp-null-null\|esp-null-sha1\|esp-scb128-null\|esp-scb128-md5\|esp-scb128-sha1)(ah-null\|ah-md5-hmac\|ah-sha-hmac)

参数	说明	缺省配置
(esp-3des-md5|esp-3des-null|esp-3des-sha1|esp-aes128-md5|esp-aes128-null|esp-aes128-sha1|esp-aes192-md5|esp-aes192-null|esp-aes192-sha1|esp-aes256-md5|esp-aes256-null|esp-ae	设置ESP封装算法	预共享密钥和rsa方式下，缺省是esp-3des-md5。国密方式缺省是esp-scb128-sha1

s256-sha1|esp-des-md5|esp-des-null|esp-des-sha1|esp-null-md5|esp-null-null|esp-null-sha1|esp-scb128-null|esp-scb128-md5|esp-scb128-sha1)		
(ah-null|ah-md5-hmac|ah-sha-hmac)	设置AH封装算法	预共享密钥和rsa方式下，缺省是ah-md5-hmac。国密方式缺省是ah-null

参数说明：pfs (1\|2\|5)

参数	说明	缺省配置
(1|2|5)	配置pfs所使用的Diffle-Hellmen数组	缺省无设置

参数说明：set lifetime seconds <600-86400>

参数	说明	缺省配置
<600-86400>	配置IPSec SA时间的生存期	缺省是3600秒

参数说明：set lifetimekilobytes <10-524288>

参数	说明	缺省配置
<10-524288>	配置IPSec SA流量的生存期	缺省是0KB

5.2.4 手工配置 IPsec 安全策略

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	policy (IF_IN|any) (IF_OUT|any) (SIP|any) (DIP|any) ("CMD_GROUP_SERVICE")(USER|any)(APPLICATION|any)(SCHEDULE|always) (permit|deny|ipsec) [ID]	配置IPSsec安全策略
步骤3	exit	退出IPSec策略配置模式

5.3 配置案例

5.3.1 配置案例：

配置步骤：

步骤1	配置一阶段
	DCFW-1800(config)# vpn ipsec phase1 DCFW-1800(config-phase1)# edit gateway ike_test DCFW-1800(config-phase1-ike_test)# set mode main DCFW-1800(config-phase1-ike_test)# set remotegw 192.168.1.97 DCFW-1800(config-phase1-ike_test)# lifetime 6000 DCFW-1800(config-phase1-ike_test)# set dpd 30 DCFW-1800(config-phase1-ike_test)# dpd enable DCFW-1800(config-phase1-ike_test)# authentication pre-share DCFW-1800(config-phase1-ike_test)# set preshared-key 111111 DCFW-1800(config-phase1-ike_test)# set nat 10 DCFW-1800(config-phase1-ike_test)# set policy 1 DCFW-1800(config-phase1-ike_test-policy1)# encrypt 3des DCFW-1800(config-phase1-ike_test-policy1)# hash md5 DCFW-1800(config-phase1-ike_test-policy1)# exit
步骤2	配置二阶段
	DCFW-1800(config)# vpn ipsec phase2 DCFW-1800(config-phase2)# edit tunnel ipsec_test DCFW-1800(config-phase2-ipsec_test)# set peer ike_test DCFW-1800(config-phase2-ipsec_test)# mode tunnel DCFW-1800(config-phase2-ipsec_test)# set lifetime seconds 3600 DCFW-1800(config-phase2-ipsec_test)# pfs 2 DCFW-1800(config-phase2-ipsec_test)# set proposal1 esp-3des-md5 ah-null DCFW-1800(config-phase2-ipsec_test)#exit
步骤3	配置地址对象
	DCFW-1800(config)# address 2_24 DCFW-1800(config-address)# net-address 2.2.2.0/24 DCFW-1800(config-address)# exit DCFW-1800(config)# address 1_24

	DCFW-1800(config-address)#net-address 1.1.1.0/24 DCFW-1800(config-address)# exit
步骤4	配置tunnel接口
	DCFW-1800(config)# interface tunnel 10 mode ipsec DCFW-1800(config-tunnel10)#tunnel-ipsec ipsec_test DCFW-1800(config-tunnel10)#tunnel-ipsec interested-subnet 2_24 1_24
步骤5	添加静态路由
	DCFW-1800(config)#ip route 1.1.1.0/24 tunnel10

5.4 IPSec VPN监控与维护

5.4.1 显示一阶段 SA

步骤1	DCFW-1800# show ike sa
	Name: ike_test id: 895 local_addr: 192.168.1.61 peer_addr: 192.168.1.65 stat: establish life time: 5996 Data: ike sa Total count: 1.

5.4.2 显示二阶段 SA

步骤1	DCFW-1800# show ipsec sa
	Name: ipsec_test id: 1786 local_addr: 192.168.1.61 peer_addr: 192.168.1.65 esp: yes mode: tunnel enc_algo/auth_algo: 3des/md5 inbound_spi/outbound_spi: 131155688/170802143 ah: no stat: establish life time/cur_life_time: 3600/3553 inbound/outbound: 0/0 kbytes

	local_net: 2.2.2.0/24 peer_net: 1.1.1.1/32 Data: ipsec sa Total count: 1.

5.4.3 清除一阶段 SA

步骤1	clear ike sa all
步骤2	clear ike sa id <1-2000000000>根据ID删除指定SA clear ike sa name NAME根据名字清除指定SA

5.4.4 清除二阶段 SA

步骤1	clear ipsec sa all
步骤2	clear ipsec sa id <1-2000000000>根据ID删除指定SA clear ipsec sa name NAME根据名字清除指定SA

5.4.5 常见故障分析

故障现象：不能建立隧道

现象	安全联盟协商不成功，不能建立SA，在命令show crypto ipsec sa中看不到相关信息
分析	1）查看两端设备的相应的安全策略配置是否对称 2）阶段1的协商策略、验证密钥是否一致 3）阶段2的转换集是否一致
解决	1）如果安全策略配置不对称，则修改成对称 2）阶段1或者阶段2的协商策略不一致，则修改成一致

第6章 配置 NAT

6.1 NAT概述

NAT 即网络地址转换，最初是由 RFC1631(目前已由 RFC3022 替代)定义，用于私有地址向公有地址的转换，以解决公有 IP 地址短缺的问题。后来随着 NAT 技术的发展及应用的不断深入，NAT 更被证明是一项非常有用的技术，可用于多种用途，如：提供了单向隔离，具有很好的安全特性；可用于目标地址的映射，使公有地址可访问配置私有地址的服务器；另外还可用于服务器的负载均衡和地址复用等。

NAT 分为源 NAT 和目的 NAT。源 NAT 是基于源地址的 NAT，可细分为动态 NAT、PAT 和静态 NAT。动态 NAT 和 PAT 是一种单向的针对源地址的映射，主要用于内网访问外网，减少公有地址的数目，隐藏内部地址。动态 NAT 指动态地将源地址转换映射到一个相对较小的地址池中，对于同一个源 IP，不同的连接可能映射到地址池中不同的地址；PAT 是指将所有源地址都映射到同一个地址上，通过端口的映射实现不同连接的区分，实现公网地址的共享。静态 NAT 是一种一对一的双向地址映射，主要用于内部服务器向外提供服务的情况。在这种情况下，内部服务器可以主动访问外部，外部也可以主动访问这台服务器，相当于在内、外网之间建立了一条双向通道。

基于目标地址的 NAT，我们称为目的 NAT，可分为目标地址映射、目标端口映射、服务器负载均衡等。基于目标地址的 NAT 也称为反向 NAT 或地址映射。目的 NAT 是一种单向的针对目标地址的映射，主要用于内部服务器向外部提供服务的情况，它与静态 NAT 的区别在于它是单向的。外部可以主动访问内部，内部却不可以主动访问外部。另外，可使用目的 NAT 实现负载均衡的功能，即可以将一个目标地址转换为多个内部服务器地址。也可以通过端口的映射将不同的端口映射到不同的机器上。

另外，掌握 NAT 的基本原理之后，NAT 不仅仅可用于公有地址和私有地址之间的转换，还可用于公有地址与公有地址之间、私有地址与私有地址之间的转换。

本设备还支持 NAT ALG，普通 NAT 实现了对 UDP 或 TCP 报文头中的的 IP 地址及端口转换功能，但对应用层数据载荷中的字段无能为力，在许多应用层协议中，比如多媒体协议（H.323、SIP 等）、FTP、SQLNET 等，TCP/UDP 载荷中带有地址或者端口信息，这些内容不能被 NAT 进行有效的转换，就可能导致问题。而 NAT ALG（Application Level Gateway，应用层网关）技术能对多通道协议进行应用层报文信息的解析和地址转换，将载荷中需要进行地址转换的 IP 地址和端口或者需特殊处理的字段进行相应的转换和处理，从而保证应用层通信的正确性。

例如，FTP 应用就由数据连接和控制连接共同完成，而且数据连接的建立动态地由控制连接中的载荷字段信息决定，这就需要 ALG 来完成载荷字段信息的转换，以保证后续数据连接的正确建立。

本设备支持的 NAT ALG 应用协议有 FTP、TFTP、H.323、SQLNET

注意：

NAT 的负载均衡功能只是将一个目标地址均衡转换到不同的内部主机地址上，它并不检测内部主机是否运行正常。它仅仅是一种特殊的地址转换功能，并不是真正意义上的负载均衡。

6.2 配置NAT

系统中把 NAT 的配置分为：Static、Source、Destination 三种类型。

每条 NAT 规则都是和某个特定的接口相关联的，需要注意的是，Source NAT 是在离开接口时进行转换的，Destination NAT 是在进入接口时进行转换的，所以配置 Source NAT 的时候必须和对应的出接口关联，而配置 Destination NAT 的时候需要和对应的入接口关联。

6.2.1 配置地址池(NAT POOL)

地址池中存放供动态 NAT 使用的地址范围的集合。地址池的使用支持轮转方式和非轮转方式，同时支持地址池分段。

在进行地址转换后，报文的真实地址将被转换为地址池中的地址。

配置地址池的步骤:

步骤1	configure terminal	进入配置模式
步骤2	ip nat pool POOLNAME	进入地址池节点
步骤3	ip address A.B.C.D A.B.C.D	配置一段地址池
步骤4	rotary	轮询

使用 no ip nat pool POOLNAME 命令可以删除一个地址池。

使用 no rotary 命令可以禁用轮询。

注意：

不能删除正被 NAT 规则引用的地址池；结束地址不能小于起始地址；池段范围不能出现重叠现象。

6.2.2 配置 static NAT

静态 NAT 是一对一的双向地址映射。在这种情况下，被映射的内部主机可以主动访问外部，外部也可以主动访问这台内部主机，相当于在内、外网之间建立了一条双向通道。

配置 static NAT 的步骤:

步骤1	configure terminal	进入配置模式
步骤2	ip nat static IFNAME A.B.C.D A.B.C.D [ID]	配置一条静态NAT规则

使用 no ip nat ID 命令可以删除一条静态 NAT 规则。

注意：

建议在配置 NAT 规则时不指定 ID，系统会自动进行选择。

6.2.3 配置 source NAT

源 NAT 是一种单向的针对源地址的映射，主要用于内网访问外网，减少公有地址的数目，隐藏内部地址。

配置 source NAT 的步骤:

步骤1	configure terminal	进入配置模式
步骤2	ip nat source IFNAME (ADDR_OBJ | any) (ADDR_OBJ | any) (SRV_OBJ|any) (POOL|interface) [ID]	配置一条源NAT规则。可以指定已经定义的地址池，也可以用interface关键字，表明使用出接口的接口地址

使用 no ip nat ID 命令可以删除一条源 NAT 规则。

注意：

建议在配置 NAT 规则时不指定 ID，系统会自动进行选择。

6.2.4 配置 destination NAT

目的 NAT 根据应用场合不同，可以分为以下三种：

服务器地址、端口映射：实现外网地址和内部地址的单向映射或同时实现转换端口；

服务器业务分流：根据访问的业务不同，系统把目的地址转换为内部不同的服务器地址；

服务器负载分担：把一个外部 IP 映射到内部的一个地址池中，即一到多的映射功能；

接口映射：根据外网出接口的 IP 自动更改目的 NAT 规则，主要用于 PPPoE 等拨号上网获得动态 IP 的情况。

配置 destination NAT 的步骤:

步骤1	configure terminal	进入配置模式
步骤2	ip nat destination IFNAME (ADDR_OBJ | any) (ADDR_OBJ | any | interface) (SRV_OBJ|any) POOL [service <1-65535>] [ID]	配置一条目的NAT规则。

使用 no ip nat ID 命令可以删除一条目的 NAT 规则。

注意：

建议在配置 NAT 规则时不指定 ID，系统会自动进行选择。

6.2.5 配置 destination NAT 自动映射

目的 NAT 自动映射会自动将用户输入的目的地址对象中的地址，和地址池中包含的地址建立对应关系，自动生成多条目的 NAT 规则。在自动生成的这些目的 NAT 规则中，目的地址对象都为主机地址，而转换后的地址是地址池中的地址范围所包含的主机地址。

注意：

若目的地址对象中包含的主机地址个数为 M，地址池中的主机地址个数为 N，则经过自动映射：

M > N 时，自动生成 M 条目的 NAT 规则，其中的前 N-1 条 NAT 使用地址池中的前 N-1 个主机地址，其余 NAT 规则都使用地址池中的最后一个主机地址。

M = N 时，自动生成 M 条目的 NAT 规则，每条 NAT 中的目的地址和地址池中的地址是一一对应的。

M < N 时，自动生成 M 条目的 NAT 规则，仅使用地址池中的前 M 条主机地址，每条 NAT 中的目的地址和转换后的地址是一一对应的

配置 destination NAT 自动映射的步骤:

步骤1	configure terminal	进入配置模式
步骤2	ip nat auto-destination IFNAME (ADDR_OBJ | any) (ADDR_OBJ | any) (SRV_OBJ|any) POOL [log]	配置一条目的NAT自动映射。
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

由于会生成多条目的 NAT 规则，需使用 no ip nat ID 命令删除生成的每一条目的 NAT 规则。

参数说明：ip nat auto-destination IFNAME (ADDR_OBJ | any) (ADDR_OBJ | any) (SRV_OBJ|any) POOL [log]：

参数	说明	缺省配置
IFNAME	要进行目的NAT的报文进入设备的接口名称	无
(ADDR_OBJ | any)	要进行目的NAT的报文的源地址对象名称	无
(ADDR_OBJ | any)	要进行目的NAT的报文的目的地址对象名称	无
(SRV_OBJ|any)	要进行目的NAT的报文的服务类型	无
POOL	地址池名称，存放目的NAT使用的地址范围的集合	无
[log]	进行日志记录	无

注意：

优化的目的 NAT 仅能针对目的地址进行展开，若目的地址包含的地址过多，则可读性降低，不建议包含过多目的地址的地址对象使用优化的目的 NAT。若目的地址为“any”，则无法使用优化的目的 NAT。

6.3 端口管理

6.3.1 设置服务端口号

针对服务器有时会改变或者添加所提供服务对应的监听端口号的情况，设备需要改变或添加预置的服务端口号，使设备能正确识别报文中端口号所对应的服务类型。

例如，某个 FTP 服务器除了开放 21 端口监听请求之外，也开放了 1000 端口监听 FTP 请求；当设备接收到一个报文的目的端口号为 1000 时，要识别出该报文为一个 FTP 相关报文，这样就需要设备对服务的端口进行一定的处理。

提示：

协议对应的默认端口号无法改变或删除。

配置步骤：

步骤1	configure terminal	进入全局配置模式

步骤2	ip nat service (ftp|tftp) <1-65535>	添加协议对应的端口号(目前仅支持ftp和tftp协议)
步骤3	end	退到特权模式下
步骤4	write terminal	显示配置

提示：

每个协议，除了默认端口，最多可以添加 7 个端口号。

第7章 配置 DHCP 服务器

7.1 DHCP服务概述

本设备提供两种 DHCP 服务功能：DHCP 服务器和 DHCP Relay。

7.1.1 DHCP 服务器概述

DHCP 的全称是动态主机配置协议（Dynamic Host Configuration Protocol）。设备可以作为 DHCP Server，用于实现对网络中 IP 地址的动态分配和集中管理。动态分配是指当 DHCP 客户端第一次从 DHCP Server 租用到 IP 地址后，并非永久的使用该地址，只要租约到期，客户端就要释放(Release)这个 IP 地址以给其它工作站使用。为了实现 IP 地址的动态分配，必须设置 DHCP Server 拥有一个 IP 地址范围，用来分配给用户，这个用来分配给客户端的地址范围也叫 IP 地址池（IP Pool）。

主机（客户端）先广播 DHCPDISCOVER 包寻找网络上的 DHCP 服务器，DHCP 服务器向客户端单播包含配置参数的 DHCPOFFER 消息。

- 当客户端第一次登录到网络时，它会向网络广播一个 DHCPDISCOVER 消息，此时由于客户端还不知道自己属于哪一个网路，所以封包的来源地址为 0.0.0.0，目的地址则为 255.255.255.255。
- 由于网络上可能不止一个 DHCP 服务器，凡是具有有效 IP 地址信息的 DHCP 服务器均从各自还没有租出的地址中选择一个空闲 IP，然后将该提议回应给客户端。
- 客户端从接收到的第一个提议中选定 IP 地址信息，并广播一条租用地址的消息请求。由发出该提议的 DHCP 服务器响应该消息，确认已接受请求并开始租用。
- 客户端收到确认后开始使用此地址

注意：

DHCP 客户端可以接收多个 DHCP 服务器的消息，自己从中选一个 DHCP 服务器，同时也暗示它拒绝了其它 DHCP 服务器应答的配置参数。

7.1.2 DHCP Relay 概述

DHCP Relay 是用来将一个网段的 DHCP 请求转发给其它网段的 DHCP Server，由其它网段的 DHCP Server 分配 IP 地址。DHCP Relay 存在的原因是因为 DHCP 客户端还没有 IP 环境设定，这时由 DHCP Relay 来接管客户的 DHCP 请求然后将 DHCP 消息传递给 DHCP Server，再将 DHCP 服务器的应答消息传给客户端，客户端获得 IP 地址。当然也可以在每一个网段之中安装 DHCP Server 但这样的话设备成本会增加而且管理上面也比较分散。

7.2 配置DHCP Server

7.2.1 在接口上指定 DHCP Server 服务

配置步骤

步骤1	(config)# interface IFNAME	进入相应接口
步骤2	(config-if)# dhcpserver enable	在该接口上指定DHCP Server
步骤3	(config-if)# no dhcpserver enable	在该接口上取消DHCP Server

注意：

只有在该接口上指定了 DHCPServer 服务，DHCP Server 才会处理该接口的 DHCP 请求。系统初始时 DHCP Server 不处理所有接口的 DHCP 请求。

DHCP SERVER 支持物理接口和 VLAN 接口。

7.2.2 配置 DHCP Server 服务子网

配置步骤

步骤1	(config)# dhcp	进入DHCP配置模式
步骤2	(config-dhcp)# share-net NAME subnet A.B.C.D/M	增加子网及其SUBNET
步骤3	(config-dhcp)# no share-net NAME subnet	删除子网SUBNET
步骤4	(config-dhcp)# no share-net NAME	删除子网所有配置

7.2.3 配置 DHCP Server 地址池及其租约

配置步骤

步骤1	(config-dhcp)# share-net NAME A.B.C.D E.F.G.H infinite	增加子网的地址池,其租约为无限
步骤2	(config-dhcp)# share-net NAME A.B.C.D A.B.C.D <0-100> days <0-23> hours <0-59> mins	增加子网的地址池,其租约为所配置的时间
步骤3	(config-dhcp)#no share-net NAMEA.B.C.D E.F.G.H	删除子网的地址池

注意：

每个子网只可以有 1 个地址池。 infinite 意味租约期为无限。若租约不为 infinte，则其取值范围为 5 分钟至 100 天。

7.2.4 配置 DHCP 子网缺省网关

配置步骤

步骤1	(config-dhcp)#share-net NAME router A.B.C.D	配置子网的缺省网关
步骤2	(config-dhcp)#no share-net NAME router	取消子网的缺省网关

7.2.5 配置 DHCP 子网 DNS 服务器

配置步骤

步骤1	(config-dhcp)# share-net NAME dns A.B.C.D [E.F.G.H]	配置子网的DNS服务器
步骤2	(config-dhcp)# no share-net NAMEdns	取消子网的DNS服务器

7.2.6 配置 DHCP 子网 WINS 服务器

配置步骤

步骤1	(config-dhcp)# share-net NAME wins A.B.C.D [E.F.G.H]	配置子网的WINS服务器
步骤2	(config-dhcp)# no share-net NAME wins	取消子网的WINS服务器

7.2.7 配置 DHCP 子网域名

配置步骤

步骤1	(config-dhcp)# share-net NAME domain NAME	配置子网的域名
步骤2	(config-dhcp)# no share-net NAMEdomain	取消子网的域名

7.2.8 配置 DHCP 地址绑定

DHCP Server 可以设置指定的 IP 地址与指定的 MAC 地址捆绑，指定的 MAC 地址与 IP 地址一一对应，每条绑定项都有指定的绑定名称。

配置步骤

步骤1	(config-dhcp)# bind NAME HH-HH-HH-HH-HH-HH A.B.C.D	设置地址绑定
步骤2	(config-dhcp)# no bind NAME	取消地址绑定

7.2.9 配置 DHCP 地址排除

DHCP Server 可以设置保留的地址范围,这些保留的地址将不会分配给 DHCP 客户端。

配置步骤

步骤1	(config-dhcp)# exclude 10.0.0.0 10.0.0.11	设置地址排除
步骤2	(config-dhcp)# no exclude 10.0.0.0 10.0.0.11	取消地址排除

7.3 DHCP服务监控

7.3.1 DHCP Debug

步骤1	显示当前DHCP的debug情况
	DCFW-1800# show dhcp debug
步骤2	打开 DHCP debug开关
	DCFW-1800#debug dhcp event DCFW-1800# debug dhcp packet detail DCFW-1800# show debug DHCP debugging status: DHCP event debugging is on DHCP packet debugging is on
步骤3	关闭no debug dhcp event/no debug dhcp packet detail
	DCFW-1800#no debug dhcp packet detail DCFW-1800# show dhcp debug

7.3.2 显示 DHCP Server 配置信息

步骤1	显示当前DHCP的配置及开关情况
	DCFW-1800#show dhcp config

```
dhcp
exclude 10.0.0.2 10.0.0.3
exclude 10.0.0.5 10.0.0.10
bind aaa 11:22:33:44:55:66 1.1.1.1
bind bindtable 00:16:76:65:30:9c 192.168.6.169
share-net aaa subnet 10.0.0.0/24
share-net aaa 10.0.0.3 10.0.0.10 7 days 3 hours 5 mins
share-net aaa router 10.0.0.1
share-net aaa dns 203.196.0.3
share-net aaa wins 10.0.0.1
share-net aaa domain zte.com
share-net bbb subnet 192.168.6.1/24
share-net bbb 192.168.6.171 192.168.6.173 infinite
share-net bbb router 192.168.6.1
share-net bbb dns 203.196.0.3
share-net bbb wins 192.168.0.1
share-net bbb domain zte.com
```

7.3.3 显示 DHCP Server 地址分配信息

步骤1	显示当前的地址租约以及客户端信息

```
DCFW-1800# show dhcp ip active
------------------------------
ipaddr:            192.168.2.4
macaddr:           00-0d-60-78-81-75
start_time:      2007-01-01 05:22:43
end_time:          2007-01-01 05:27:43
interface:       bvi2
DCFW-1800# show dhcp ip free
------------------------------
ipaddr:            192.168.2.3
macaddr:           00-16-76-65-3b-3c
start_time:      2007-01-01 05:17:49
end_time:          2007-01-01 05:22:49
```

	interface: bvi2 DCFW-1800# show dhcp ip summary General Statistics Active IP : 1 Abandoned IP : 0 Expired Leases : 1 Usage by Network : Network Netmask Active Abandoned Expired 192.168.2.1 255.255.255.0 1 0 1

7.4 配置案例

案例描述：

配置设备（DHCP Server）给两个子网分配 IP 地址，如下图所示，172.16.1.0/16 为直接相连的子网，172.16.2.0/16 为通过另一台设备（DHCP Relay）连接的子网。

配置步骤：

步骤**1**	配置图中DHCP SERVER所在的设备上接口IP地址
	DCFW-1800_A(config) interface ge0 DCFW-1800_A (config- ge0) ip address 192.168.0.1/24 DCFW-1800_A (config- ge0) dhcpserver enable DCFW-1800_A (config) interface ge1 DCFW-1800_A (config- ge1) ip address 172.16.1.1/24 DCFW-1800_A (config- ge1) dhcpserver enable DCFW-1800_A (config) exit DCFW-1800_A(config) ip route 172.16.2.0/24 192.168.0.2 DCFW-1800_A (config) exit
步骤**2**	配DHCP相关参数
	DCFW-1800_A (config)dhcp DCFW-1800_A (config-dhcp)share-net ge1 subnet 172.16.1.0/24 DCFW-1800_A(config-dhcp)share-net ge1 router 172.16.1.1 DCFW-1800_A (config-dhcp)share-net ge1 dns 202.99.16.1

	DCFW-1800_A (config-dhcp)share-net ge1 172.16.1.10 172.16.1.250 infinite DCFW-1800_A (config-dhcp)share-net ForRelay subnet 172.16.2.0/24 DCFW-1800_A (config-dhcp)share-net ForRelay 172.16.2.10 172.16.2.254 infinite DCFW-1800_A (config-dhcp)exit
步骤3	配置dhcp relay
	DCFW-1800_A (config)# interface ge1 DCFW-1800_A (config-ge1)# dhcprelay 192.168.0.1 DCFW-1800_A (config-ge1)# exit DCFW-1800_A(config)# policy 1 any any any any any always permit DCFW-1800_A(config-policy)# enable DCFW-1800_A(config-policy)# exit

第8章 配置对象

8.1 配置绝对时间和周期时间

8.1.1 绝对时间和周期时间概述

为了方便用户配置和管理，下一代防火墙设备中引入了时间对象概念，时间对象分为绝对时间和周期时间。在其它功能的配置中，可以引用时间对象来定义配置生效的条件。

绝对时间：配置服务在指定的时间内生效。

周期时间：配置服务在指定的时间范围内在指定的周期（星期一~星期日）执行。

8.1.2 配置在绝对时间中配置有效时间范围

绝对时间中只能配置一个有效时间范围

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	schedule onetimeNAME	进入名为NAME的绝对时间模式，如果不存在就创建新的时间对象。
步骤3	absolute YY-MM-DD HH:NN:SS YY-MM-DD HH:NN:SS	配置有效时间范围。年、月、日、小时、分钟、秒为一个时间单位，设置时间表的起始和终止时间。

使用 no absolute 删除绝对时间中的有效时间范围。

参数说明： schedule onetime NAME

参数	说明	缺省配置
<NAME>	时间对象的名称	无

参数说明：absolute YY-MM-DD HH:NN:SS YY-MM-DD HH:NN:SS

参数	说明	缺省配置
<YY-MM-DD>	时间表起止日期（年，月，日）	无
<HH:NN:SS>	时间表起止时间（时，分，秒）	无
<YY-MM-DD>	时间表终止日期（年，月，日）	无

<HH:NN:SS>	时间表终止时间（时，分，秒）	无

8.1.3 配置在周期时间中配置有效时间范围

周期时间中可以定义有效时间范围和有效时间段。有效时间范围只能有一个，而有效时间段可以有多个。有效时间段之间是或的关系，满足其中一个即可；有效时间范围和有效时间段之间是与的关系，都满足才生效。

可以用 absolute 命令向周期时间中添加一个有效时间范围。

配置步骤：

步骤1	Configure terminal	进入配置模式
步骤2	schedulerecurringNAME	进入名为NAME的周期时间模式，如果不存在就创建新的时间对象。
步骤3	absolute YY-MM-DD HH:NN:SS YY-MM-DD HH:NN:SS	配置有效时间范围。年、月、日、小时、分钟、秒为一个时间单位，设置时间表的起始和终止时间。
步骤4	show running-config	查看当前配置

参数说明： schedulerecurringNAME

参数	说明	缺省配置
<NAME>	循环时间表名称	无

参数说明： absolute YY-MM-DD HH:NN:SS YY-MM-DD HH:NN:SS

参数	说明	缺省配置
<YY-MM-DD>	周期表起止日期（年，月，日）	无
<HH:NN:SS>	周期表起止时间（时，分，秒）	无
<YY-MM-DD>	周期表终止日期（年，月，日）	无
<HH:NN:SS>	周期表终止时间（时，分，秒）	无

8.1.4 配置在周期时间中配置有效时间段

可以用 periodic 命令向周期时间中添加多个有效时间段。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	schedulerecurringNAME	进入名为NAME的时间对象模式，如果不存在就创建新的时间对象。
步骤**3**	periodic HH:NN:SS HH:NN:SS (monday|null)…(sunday|null)	配置周期时间段。可配置每天的时间范围，支持离散的星期配置。
步骤**4**	show running-config	查看当前配置

参数说明： schedulerecurringNAME

参数	说明	缺省配置
<NAME>	周期表名称	无

参数说明： periodic HH:NN:SS HH:NN:SS (monday\|null)…(sunday\|null)

参数	说明	缺省配置
<HH:NN:SS >	周期表起止时间（时，分，秒）	无
<HH:NN:SS>	周期表终止时间（时，分，秒）	无
<monday|null>	星期一或者null	无
<tuesday|null>	星期二或者null	无
<wednesday|null>	星期三或者null	无
<.thursday|null>	星期四或者null	无
<friday|null>	星期五或者null	无
<saturday|null>	星期六或者null	无
<sunday|null>	星期日或者null	无

注意：

Periodic HH:NN:SS HH:NN:SS (nmonday|null)…(Sunday|null)命令中星期一到星期日必须要填写如果不要设置可以用 null 代替

8.1.5 配置案例

8.1.6 配置案例:配置时间表

案例描述

配置一个时间对象，其中绝对时间范围从 2007 年 1 月 1 日 0 点到 2007 年 2 月 2 日 0 点，周期时间段是每周六和周日早上 8 点半到下午 5 点半。

配置步骤：

步骤1	创建一个时间表
	DCFW-1800_A(config)# schedulerecurring backup
步骤2	在时间对象中配置有效时间范围
	DCFW-1800_A(config-tr-obj)#absolute 07-01-0100:00:00 07-02-02 00:00:00
步骤3	在时间对象中配置绝对时间
	periodic 08:30:00 17:30:00 null null null null null saturday sunday

配置结果：

```
DCFW-1800# show running-config
schedule recurring backup
    absolute 07-01-01 00:00:00 07-02-02 00:00:00
    periodic 08:30:00 17:30:00 null null null null null saturday sunday
!
```

8.1.7 绝对时间与周期时间监控与维护

8.1.8 查看周期表与绝对时间

配置步骤：

步骤1	显示某个周期时间表
	DCFW-1800_A# show schedule recurring backup schedule recurring backup

	absolute 07-01-01 00:00:00 07-02-02 00:00:00 periodic 08:30:00 17:30:00 null null null null null saturday sunday DCFW-1800_A# backup是时间表名称;。07-01-01 00:00:00 07-02-02 00:00:00是绝对时间 08:30:00 17:30:00 null null null null null saturday sunday是周期时间

8.1.9 常见故障分析

8.1.10 故障现象 1：

现象	执行no schedule recurring NAME以后，该时间表仍然存在。
分析	当一个对象或对象组正在被引用时，就不能通过no命令删除。
解决	可以先撤销其它配置对时间表的引用，确定其没有被引用之后再用no命令删除该节点。

8.2 配置服务对象和服务对象组

8.2.1 服务对象和服务对象组概述

为了方便用户配置和管理，下一代防火墙设备中引入了服务对象的概念。在其它功能的配置中，可以引用服务对象来定义配置生效的条件。

8.2.2 配置服务对象和服务对象组

服务对象中包含了协议和协议属性。

8.2.3 配置向服务对象中添加 TCP|UDP 服务

可以用 tcp|udp 命令向 Service 中添加 tcp|udp 服务。对于 TCP 和 UDP 来讲，服务对象包含协议、源端口和目标端口信息。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	service NAME	进入名为NAME的服务对象模式
步骤**3**	(tcp|udp) dest <1-65535> [<1-65535>] [source <1-65535> [<1-65535>]]	添加一个tcp|udp服务，需要指定目标端口或范围，也可以指定源端口或范围
步骤**4**	show service NAME	显示服务对象NAME的配置信息

使用 no dest <1-65535> [<1-65535>] [source <1-65535> [<1-65535>]]可以取消对服务对象的设置。

参数说明： service NAME

参数	说明	缺省配置
<NAME>	服务对象的名称	无

参数说明：(tcp\|udp) dest <1-65535> [<1-65535>] [source <1-65535> [<1-65535>]]

参数	说明	缺省配置
<dest>	目标端口	无
<1-65535>	目标起止端口	无
<1-65535>	目标终止端口	无
<source>	源端口	无
<1-65535>	源起止端口	无
<1-65535>	源终止端口	无

8.2.4 配置向服务对象中添加 ICMP 服务

可以用 icmp 命令向 Service 中添加 icmp 服务。对于 ICMP，服务对象包含协议、type、code 信息。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	service NAME	进入名为NAME的服务对象模式
步骤3	icmp <0-255> [<0-255>]	添加一个icmp服务，需要指定type，可以指定code
步骤4	show service NAME	显示服务对象NAME的配置信息

参数说明： icmp <0-255> [<0-255>]

参数	说明	缺省配置
<0-225>	ICMP type	无
<0-225>	ICMP code	无

8.2.5 配置向服务对象组中添加服务对象

服务对象组是服务对象的集合，一个服务对象组中可以包括多个服务对象。

可以用 service-object 命令向服务对象组中添加一个服务对象,可以是系统预定义服务，也可以是用户自定义的服务。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	service-group NAME	进入名为NAME的服务对象组模式
步骤3	service-object ("CMD_GROUP_SERVICEX "|SERVICE)	将指定的预定义服务或自定义服务添加到该服务对象组中
步骤4	show service-group NAME	显示服务对象NAME的配置信息

参数说明： service-object (" CMD_GROUP_SERVICEX "\|SERVICE)

参数	说明	缺省配置
<"CMD_GROUP_SERVICEX" | SERVICE>	系统支持的服务与自定义服务	无

使用 no service-object ("CMD_GROUP_SERVICEX"|SERVICE)命令可以删除服务对象组中通过 service-object 命令添加的服务对象。

8.2.6 配置案例

8.2.7 配置案例 1: 添加服务对象与服务对象组

案例描述

配置一个服务对象和一个服务对象组并且将这个服务对象放入服务对象组里。

配置步骤：

步骤**1**	创建一个服务对象
	DCFW-1800_A(config)# service svc
步骤**2**	在这个地址对象中添加TCP服务
	DCFW-1800_A(config-sev)# tcp dest 80
步骤**3**	创建一个服务对象组
	DCFW-1800_A(config)# service-group svc-group
步骤**4**	将服务对象(svc)添加到这个服务对象组里
	DCFW-1800_A(config-sevgrp)# service-object svc
步骤**5**	显示添加信息
	DCFW-1800_A(config)# show service-group ! service-group svc-group service-object svc DCFW-1800_A(config)#

配置结果：

```
DCFW-1800_A# show running-config
service svc
    tcp dest 80
!
!
service-group svc-group
    service-object svc
```

8.2.8 配置案例 2:配置服务对象

案例描述

配置一个服务对象，其中包含 tcp 协议，目标端口分别为 23，源端口的范围是 1~65535。

配置步骤：

步骤**1**	创建一个服务对象
	DCFW-1800_A(config)# service telnet2
步骤**2**	向服务对象中添加端口范围

	DCFW-1800_A(config-sev)# tcp dest 23 source 1 65535

8.2.9 服务对象与服务对象组监控与维护

8.2.10 查看服务对象

查看某个地址对象的步骤：

步骤**1**	显示某个地址对象信息
	DCFW-1800_A# show service svc ! service svc tcp dest 80 DCFW-1800_A# svc是服务对象名称; 80是目标端口。

8.2.11 查看服务对象组

查看某个地址对象组的步骤：

步骤**1**	显示某个地址对象组信息
	DCFW-1800_A # show service-groupsvc-group ! service-groupsvc-group service-object svc DCFW-1800_A # svc-group是服务对象组名称; svc是服务对象名称。

8.2.12 常见故障分析

8.2.13 故障现象 1：

现象	执行no service|service-group NAME以后，该对象或对象组仍然存在。
分析	当一个对象或对象组正在被引用时，就不能通过no命令删除。

解决	可以先撤销其它配置对该对象或对象组的引用，确定其没有被引用之后再用no命令删除该节点。

8.3 配置地址对象和地址对象组

8.3.1 地址对象和地址对象组概述

为了方便用户配置和管理，下一代防火墙设备中引入了地址对象的概念。地址对象分为地址节点和地址组，地址组是地址节点的集合。在其它功能的配置中，可以引用地址对象来定义配置生效的条件。

8.3.2 配置地址对象和地址对象组

地址对象中可以指定一个确定的 IP 地址，也可以用网络掩码的形式指定一个 IP 范围，还可以通过起止 IP 地址的形式确定一个 IP 范围。一个地址对象中可以添加多种类型的多个地址。

8.3.3 配置向地址对象中添加单个地址

可以用 host-address 命令向地址对象中添加单个 IP 地址。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	address NAME	进入名为NAME的地址对象模式
步骤3	host-address A.B.C.D	将指定的IP地址加入该地址对象中
步骤4	show address NAME	显示地址对象的配置信息

使用 no host-address 可以取消对地址对象的设置，使其恢复到缺省配置。

参数说明： address NAME

参数	说明	缺省配置
<NAME>	地址对象的名称	无

参数说明： host-address A.B.C.D

参数	说明	缺省配置
<A.B.C.D>	IP地址	无

8.3.4 配置向地址对象中添加网络掩码

可以用 net-address 命令向地址对象中添加一个网络掩码，用网络掩码表示一个网段的所有 IP 地址。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	address NAME	进入名为NAME的地址对象模式
步骤3	net－address A.B.C.D/M	将一个网络掩码加入该地址对象中
步骤4	show address NAME	显示地址对象的配置信息

参数说明： net-address A.B.C.D/M

参数	说明	缺省配置
<A.B.C.D/M>	网络地址及掩码	无

8.3.5 配置向对象地址中添加地址范围

可以用 range-address 命令向地址对象中添加一个网络地址范围，这种情况下要确定范围的起止 IP 地址。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	address NAME	进入名为NAME的地址对象模式
步骤3	range-address A.B.C.D E.F.G.H	用起止与终止IP地址表示范围，并添加到该地址对象中
步骤4	show address NAME	显示地址对象的配置信息

参数说明： rang-address A.B.C.D E.F.G.H

参数	说明	缺省配置
<A.B.C.D E.F.G.H>	起止与终止IP地址	无

8.3.6 配置向地址对象组中添加地址对象

地址对象组是地址对象的集合，一个地址对象组中可以包括多个地址对象。
可以用 address-object 命令向地址对象组中添加一个地址对象。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	address-group NAME	进入名为NAME的地址对象组模式
步骤3	address-object ADDRESS	将指定的地址对象添加到该地址对象组中
步骤4	show address-group NAME	显示地址对象组的配置信息

使用 no address-objectADDRESS 命令可以删除地址对象组中通过 address-object 命令添加的地址对象。

参数说明： address-group NAME

参数	说明	缺省配置
<NAME>	地址对象组名称	无
<ADDRESS>	地址对象名称	无

8.3.7 配置案例

8.3.8 配置案例: 添加地址对象与地址对象组

案例描述

配置一个地址对象和一个地址对象组并且将这个地址对象放入地址对象组里。

配置步骤：

步骤1	创建一个地址对象
	DCFW-1800_A(config)# address dev
步骤2	在这个地址对象中添加一个主机地址
	DCFW-1800_A(config-addr)# host-address 192.168.10.100
步骤3	创建一个地址对象组

	DCFW-1800_A(config)# address-group dev-group
步骤4	将地址对象(dev)添加到这个地址对象组里
	DCFW-1800_A(config-addrgrp)# address-object dev
步骤5	显示添加信息
	DCFW-1800_A(config)# show address-group ! address-group dev-group address-object dev

配置结果：

```
DCFW-1800_A# show running-config
address dev
    host-address 192.168.10.100
!
!
address-group dev-group
    address-object dev
!
```

8.3.9 地址对象与地址对象组监控与维护

8.3.10 查看地址对象

查看某个地址对象的步骤：

步骤1	显示某个地址对象信息
	DCFW-1800_A# show address dev ! address dev host-address 192.168.10.100 DCFW-1800_A# dev是地址对象名称; 192.168.10.100是主机IP地址。

8.3.11 查看地址对象组

查看某个地址对象组的步骤：

步骤**1**	显示某个地址对象组信息
	DCFW-1800_A# show address-groupdev-group ! Address-group dev-group address-object dev DCFW-1800_A# dev-group是地址对象组名称; dev是地址对象。

8.3.12 常见故障分析

8.3.13 故障现象 1：

现象	执行no address|address-group NAME以后，该对象或对象组仍然存在。
分析	当一个对象或对象组正在被引用时，就不能通过no命令删除。
解决	可以先撤销其它配置对该对象或对象组的引用，确定其没有被引用之后再用no命令删除该节点。

8.4 配置应用对象和应用对象组

8.4.1 应用对象、应用分类、应用对象组概述

为了方便用户配置和管理，下一代防火墙设备中引入了应用对象的概念。应用对象即应用程序对象。应用分类即按照程序的功能给引用分类。应用对象组即应用对象或/和应用分类的集合。在其它功能的配置中，可以引用应用对象来定义配置生效的条件。设备中的 1000 多种应用会定期更新。

8.4.2 配置应用对象组

应用对象和应用分类是系统内置的，无法配置和修改。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	app-group NAME	进入名为NAME的应用对象组模式

步骤3	member app APP	将指定的应用对象、应用分类加入到应用对象组中
步骤4	show app-group	显示应用对象组的配置信息

使用 no member app APP 可以删除应用对象组的引用。

参数说明： app-group NAME

参数	说明	缺省配置
<NAME>	应用对象组的名称	无

参数说明：member app APP

参数	说明	缺省配置
<APP>	应用对象或应用分类名称	无

8.4.3 配置案例

案例描述

配置一个应用对象组。

配置步骤：

步骤1	创建一个应用对象组
	DCFW-1800_A(config)# app-group apptest
步骤2	在应用对象组中添加应用对象http
	DCFW-1800_A(config-addr)# member app http
步骤3	在应用对象组中添加应用分类p2p-software
	DCFW-1800_A(config)# member app p2p-software
步骤4	显示添加信息
	DCFW-1800# show app-group app-group apptest member app p2p-software

	member app http

8.5 配置关键字对象

8.5.1 关键字对象概述

为了方便用户配置和管理，下一代防火墙设备中引入了关键字对象的概念。在其它功能的配置中，可以引用关键字对象来定义配置生效的条件。

8.5.2 配置关键字对象组

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	keyword NAME	进入名为NAME的关键字对象模式
步骤3	contentCONTENT	配置关键字
步骤4	show keyword（NAME）	显示关键字对象的配置信息

使用 no content CONTENT 可以删除应用对象组的引用。

参数说明： keyword NAME

参数	说明	缺省配置
<NAME>	*关键字对象的名称*	*无*

参数说明： content CONTENT

参数	说明	缺省配置
<CONTENT>	关键字内容	无

8.5.3 配置案例

案例描述

配置一个关键字对象。

配置步骤：

步骤**1**	创建一个关键字对象
	DCFW-1800_A(config)# keyword testkey
步骤**2**	在关键字对象中添加关键字
	DCFW-1800_A(config-addr)#content baidu.com
步骤**3**	显示添加信息
	DCFW-1800# show keyword ========== Keyword Name : testkey Description : 1 items : baidu.com ==========

8.6 配置健康检查对象

8.6.1 健康检查概述

健康检查的功能是对目标地址是否可达进行检测。

8.6.2 配置健康检查对象

配置步骤

步骤**1**	configure terminal	进入配置模式
步骤**2**	healthcheck NAME [TYPE]	设置健康检查
步骤**3**	real ip A.B.C.D	添加健康检查目的ip
步骤**4**	timeout <1-86400>	设置超时时间
步骤**5**	interval<1-86400>	设置间隔时间
步骤**6**	Maxretrys<1-10>	设置最大尝试次数
步骤**7**	avg-delay<0-60000>	设置平均延迟
步骤**8**	loss-rate<0-100>	设置丢包率
步骤**9**	sample-times<10-50>	设置质量采样范围

参数说明

参数	说明	缺省配置
NAME	地址监控对象名称	无
[TYPE]	健康检查类型（dns | icmp| tcphalfopen | udp）	无
A.B.C.D	健康检查的目标地址	无
<1-86400>	超时时间	5
<1-86400>	间隔时间	16
<1-10>	最大尝试次数	3
<0-60000>	平均延迟	无
<0-100>	丢包率	无
<10-50>	质量采样范围	10

8.6.3 配置健康检查组

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	healthcheck-group NAME [Type]	设置健康检查组名和类型
步骤3	include hm NAME	加入健康检查对象
步骤4	pass hm <0-5>	设置至少通过的健康检查方法数

参数说明：

参数	说明	缺省配置
NAME	地址监控对象组名	无
[Type]	健康检查类型（ipv4/ipv6）	无
NAME	健康检查对象名	无

<0-5>	至少通过的健康检查方法数（0：所有）	0

第9章 配置静态路由

9.1 静态路由概述

在 IP 设备中，单播路由的获得通常有两种途径：静态配置和动态路由获取。静态配置就是由网络管理员通过终端命令行等手段明确定义，被称为静态路由。

9.2 配置静态路由

静态路由是由用户配置的路由。当用户确信到达某个网段应该先转发到某个地址时，可以通过 ip route 命令配置这个静态路由，同时可以配置该静态路由的权重(1-100)，用于负载分担。静态路由支持地址监控对象的联动。当地址监控对象失效以后，使对应的静态路由无效，并增加地址监控对象中的地址的 32 位掩码的路由，下一跳和对应的静态路由的下一跳相同。

配置静态路由的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	ip route A.B.C.D/M (A.B.C.D|INTERFACE) [monitor MONITOR] [<distance><weight>]	配置静态路由
步骤3	exit	退出配置模式
步骤4	show ip route	显示静态路由信息

参数说明：ip route：

参数	说明	缺省配置
A.B.C.D/M	目的地址	
(A.B.C.D|INTERFACE)	路由网关地址或者出接口	
MONITOR	监控地址组名称	
<distance>	路由优先级，范围<1-255>	
<weight>	路由权重，范围1-100	

9.3 配置缺省路由

有一类特殊的路由称为默认路由（或缺省路由），即目的地址和掩码为

0.0.0.0/0 的路由。它可以匹配任何目的地址，所以每个找不到对应路由的报文都将按默认路由转发。通常默认路由都是在用户认为有必要时通过静态路由配置的。在网络有一个唯一出口连接到其他网络时，配置默认路由是很有用的，它可以使设备所需要的路由数量大大降低。

配置缺省路由的步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	ip route0.0.0.0/0 (A.B.C.D|INTERFACE)	配置缺省路由
步骤**3**	end	退出配置模式

9.4 多路径选择

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	default static route (per-ip-connection | per-source-address)	选择根据连接或者根据源ip，进行负载

9.5 配置信息显示命令

显示静态路由信息

命令	解释
show ip route	显示静态路由信息

9.6 配置案例

9.6.1 配置缺省路由

案例描述：

配置缺省路由，把每个没有对应路由的报文转发到公网地址 202.118.3.2

配置步骤：

步骤**1**	配置缺省路由
	DCFW-1800_A(config)# ip route 0.0.0.0/0 202.118.3.2
步骤**2**	配置接口参数

	DCFW-1800_A(config)# interface ge0/0 DCFW-1800_A(config-ge0/0)#ip address 202.118.3.1/24 DCFW-1800_A(config)# interface ge0/1 DCFW-1800_A(config-ge0/1)#ip address 192.168.0.1/24
步骤3	查看路由表
	DCFW-1800_A# show ip route Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, D - DHCP, P - PPPOE, > - selected route, * - FIB route C>* 127.0.0.0/8 is directly connected, lo weight: 0 K>* 127.0.0.1/32 is directly connected, lo weight: 0 C>* 192.168.0.0/24 is directly connected, ge0/1 weight: 0 K>* 192.168.0.1/32 is directly connected, ge0/1 weight: 0 C>* 202.118.3.0/24 is directly connected, ge0/0 weight: 0 K>* 202.118.3.1/32 is directly connected, ge0/0 weight: 0

9.7 常见故障

9.7.1 数据包转发不正常

故障现象：数据包转发不正常

分析与解决：有可能是以下几种情况导致数据包转发不正常

- 没有配置正确的静态路由
- 对于没有对应静态路由项的数据包没有配置缺省路由
- 静态路由指定的下一跳地址不可达

第10章 配置策略路由

10.1 策略路由概述

所谓策略路由，顾名思义，即是根据一定的策略进行报文转发，因此策略路由是一种比目的路由更灵活的路由机制。在设备转发一个数据报文时，首先根据配置的规则对报文进行过滤，匹配成功则按照一定的转发策略进行报文转发。这种规则可以是基于标准和扩展访问控制列表；而转发策略则是控制报文按照指定的策略路由表进行转发。因此，策略路由是对传统 IP 路由机制的有效增强。

设备支持按照策略进行路由。数据包首先由策略进行匹配，匹配成功后路由至设定的主机。策略路由支持根据 PPPOE 动态指定下一跳。

10.2 配置策略路由

10.2.1 策略路由配置

配置策略路由的步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	proute *(IF_IN*|**any**) *(SIP*|**any**) *(DIP*|**any**) *(SEV*|**any**) *(USER*|**any**) *(APP*|**any**) *(SCHEDULE*|**always**) *(blackhole|throw|unicast)*	配置路由策略的匹配条件，将满足策略的数据包路由至下一跳，此命令可配置多条。匹配的顺序按显示的先后顺序来匹配
步骤**3**	*nexthop (gateway|interface) (IF_IN|IP)* [**weight***<1-255>*]	配置策略路由的下一跳，此命令可以配置多条。按照weight的分配流量。
步骤**4**	multipath-algorithm *(per-ip-connection|per-source-address)*	选择多路径算法，可选根据源IP或根据连接
步骤**5**	exit	返回特权模式

注意：

策略路由只在流量进入设备的时候生效，对于设备本身发起的流量，不起作用。

10.2.2 调整策略路由的顺序

用 move 命令可以调整策略路由的顺序，从而使位置在前的策略优先匹配。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	proute move <*1-65535*>[before | after] <*1-65535*>	移动一条策略路由到指定的策略路由之前

10.2.3 多路径选择

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	proute<*1-65535*>	进入需要修改的策略路由
步骤**3**	multipath-algorithm (per-ip-connection | per-source-address)	选择根据连接或者根据源ip，进行负载

10.3 常见故障分析

10.3.1 故障现象：

现象	配置了策略路由后，还是无法Ping通
分析	原因可能是地址对象配置错误和下一跳配置错误
解决	分清入口和报文源地址对象，并配置正确下一跳地址

第11章 配置 RIP

11.1 RIP协议概述

RIP 协议是基于 D-V 算法（又称为 Bellman-Ford 算法）的内部动态路由协议，简称 IGP（Interior Gateway Protocol）,它通过 UDP 数据报交换路由信息。D-V 算法又称为距离向量算法,这种算法在 ARPARNET 早期就用于计算机网络的路由的计算。RIP 协议在目前已成为路由器、主机路由信息传递的标准之一，是最广泛使用的 IGP 之一，被大多数 IP 路由器商业卖主广泛使用。 RIP 协议被设计用于使用同种技术的中型网络，因此适应于大多数的校园网和使用速率变化不是很大的连续线的地区性网络。对于更复杂的环境，一般不使用 RIP 协议。

RIP 协议使用跳数来衡量到达信宿机的距离称为路由权， RIP 协议使用两种形式的报文：路径信息请求报文和路径信息响应报文。在路由器端口第一次启动时，将会发送请求报文。路径信息响应报文包含了实际的路由信息，以每 30 秒的间隔发送给相邻端口。在 RIP 协议中，还使用了水平分割、毒性逆转机制来防止路由环的形成，并且使用触发更新和路由超时机制确保路由的正确性。

11.2 配置RIP

11.2.1 缺省配置信息

设备关于 RIP 的缺省设置信息如以下表格所示：

表 11-1 RIP 缺省配置信息

内容	缺省设置	备注
使能/禁止状态（enable/disable）	disable	可更改设置
接口认证类型（none/text/md5）	none	可更改设置
版本	2	可更改设置
定时更新时间	30秒	建议采用缺省设置
超时时间	180秒	建议采用缺省设置
垃圾收集时间	120秒	建议采用缺省设置

11.2.2 配置启用 RIP 路由协议功能

启用 rip 路由协议，在此基础上才能对 rip 路由功能作进一步配置

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router rip	启用rip功能并进入rip配置节点

在配置模式下使用 no router rip 可以取消对 rip 的设置，使其恢复到缺省配置。

参数说明： router NAME

参数	说明	缺省配置
NAME	*路由协议类型*	*无*

提示：

只有在启用 rip 以后才能对 rip 其他功能作进一步配置。

11.2.3 配置 RIP 版本

RIP 的版本配置，在接口没有做出版本配置的情况下控制 RIP 协议收发报文的版本信息。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router rip	启用rip功能并进入rip配置模式
步骤3	version 1	配置收发报文版本为1
步骤4	end	回到enable模式
步骤5	show running-config	show命令

使用 no version 可以取消对 version 的设置，使其恢复到缺省配置 2。

参数说明： version <1-2>

参数	说明	缺省配置
<1-2>	Rip版本	2

11.2.4 配置 RIP 发布的网络

把系统所在的直连网络发布出去，使其他路由器能够学到到达本地网络的路由。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router rip	启用rip功能并进入rip配置模式
步骤3	network 202.38.168.1/24	配置向外发布网络202.38.168.1/24
步骤4	end	回到enable模式
步骤5	show ip rip	show命令

使用 no network 202.38.168.1/24 可以取消对 202.38.168.1/24 的设置，使其不发布 202.38.168.1/24 的路由。

参数说明： network <A.B.C.D/M>

参数	说明	缺省配置
<A.B.C.D/M>	*需要发布的网络*	*无*

11.2.5 配置 RIP 发布缺省路由

配置一条 0.0.0.0/0 的路由发布出去。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router rip	启用rip功能并进入rip配置模式
步骤3	default-information originate	配置发布缺省路由
步骤4	end	回到enable模式

步骤5	show ip rip	show命令

使用 no default-information originate 可以取消发布缺省路由的设置。

11.2.6 配置 RIP 默认的重发布度量

重发布某种类型时如果没有配置本身的重发布度量，就是用默认的度量值。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router rip	启用rip功能并进入rip配置模式
步骤3	default-metric 3	配置默认的重发布度量为3
步骤4	end	回到enable模式
步骤5	show ip rip	show命令

使用 no default-metri 可以取消对默认度量的设置，使其恢复到默认值 1。

参数说明： default-metric <1-16>

参数	说明	缺省配置
<1-16>	默认的重发布度量值	1

11.2.7 配置 RIP 定时器触发时间

RIP 会根据定时更新时间周期的向外发布整个路由表，如果超时时间到达时还没有收到某条路由的更新，就把这条路由从内核路由表中删除，并把 metric 置为 16 向外发布，并设置垃圾收集定时器；垃圾收集时间到达时，把这条路由在 rip 路由表中删除。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router rip	启用rip功能并进入rip配置模式
步骤3	timers basic 5 30 20	配置定时器触发时间为5 30 20秒
步骤4	end	回到enable模式

步骤5	show ip rip	show命令

使用 no timers basic 可以取消对定时器触发时间的设置，使其恢复到默认值 30 秒 180 秒 120 秒。

参数说明： timers basic<5- 2147483647><5- 2147483647><5- 2147483647>

参数	说明	缺省配置
<5- 2147483647>	定时更新时间	30秒
<5- 2147483647>	超时时间	180秒
<5- 2147483647>	垃圾收集时间	120秒

11.2.8 配置 RIP 定时器触发时间

重发布路由可以把例如静态、直连、ospf 的路由引入到 rip 中向外发布。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router rip	启用rip功能并进入rip配置模式
步骤3	redistribute connected metric 3	配置重发布直连路由，度量为3
步骤4	end	回到enable模式
步骤5	show ip rip	show命令

使用 no redistribute connected 可以取消直连路由的重发布。

参数说明： redistribute （connected|static|ospf）[metric <1-16>]

参数	说明	缺省配置
（connected|static|ospf）	路由类型	无
<1-16>	重发布度量	1

11.2.9 配置 RIP 接口收发报文版本

对每个接口设置特有的收发报文版本。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router rip	启用rip功能并进入rip配置模式
步骤3	ip rip ge0/1 send version 1	配置接口ge0/1的发送版本为1
步骤4	end	回到enable模式
步骤5	show ip rip	show命令

使用 no ip rip ge0/1 send version 可以取消对接口 ge0/1 发送版本的配置，使其恢复到默认值。

参数说明： ip rip NAME(send|receive) version <1-2>

参数	说明	缺省配置
NAME	接口名	无
(send|receive)	动作类型	无
<1-2>	版本	2

11.2.10 配置 RIP 接口的认证类型

对每个接口设置特有的收发报文版本。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router rip	启用rip功能并进入rip配置模式
步骤3	ip rip ge0/1 authentication md5 12345	配置接口ge0/1为md5认证，认证密码为12345
步骤4	end	回到enable模式
步骤5	show running-config	show命令

使用 no ip rip ge0/1 authentication 可以取消对接口 ge0/1 认证的配置，使其恢复到默认值无认证。

参数说明： ip rip NAME authentication (md5|text)NAME

参数	说明	缺省配置
NAME	接口名	无
(md5|text)	认证类型	无
NAME	认证密码	无

11.3 RIP监控与维护

11.3.1 查看 RIP 路由表

查看 RIP 路由表的步骤：

步骤1	显示rip路由表

```
DCFW-1800# show ip route rip
Codes: R - RIP, C - connected, O - OSPF, B - BGP
       (n) - normal, (s) - static, (d) - default, (r) - redistribute,
       (i) - interface
    Network          Next Hop        Metric From          Time
R(s) 0.0.0.0/0       0.0.0.0           1 self
C(r) 192.168.31.0/24 0.0.0.0           1 self
C(i) 202.38.168.0/24 0.0.0.0           1 self
DCFW-1800#
```

可以看出RIP路由表中有三条路由，两个直连路由192.168.31.0/24和192.168.31.0/24，度量为1，还有一个默认路由。

11.3.2 查看 RIP 配置

查看 RIP 配置的步骤：

步骤1	察看RIP的配置

Routing Protocol is "rip"

Sending updates every 5 seconds with +/-50%, next due in 2 seconds

Timeout after 30 seconds, garbage collect after 20 seconds

Default redistribution metric is 1

Redistributing: connected

Default version control: send version 2, receive version 2

Interface	Send	Recv
ge0/2	2	2

Routing for Networks:

202.38.168.1/24

Routing Information Sources:

Gateway	BadPackets	BadRoutes	Distance	Last Update

Distance: (default is 120)

DCFW-1800#

可以看出定时器时间设置为5秒30秒和20秒，默认重发布路由度量为1，重发布了直连路由，接口2的收发版本都为2，配置网络202.38.168.1/24向外发布。

11.3.3 查看调试信息

应用环境

debug rip events 可以查看 RIP 运行时各个事件

debug rip packet 可以查看 RIP 收发报文的信息

debug rip zebra 可以查看陆由变更时发生的事件

调试实例

DCFW-1800# debug rip packet

DCFW-1800# debug rip events

update timer fire!

SEND UPDATE to ge0/2 ifindex 3

multicast announce on ge0/2

update routes on interface ge0/2 ifindex 3

SEND to socket 11 port 520 addr 224.0.0.9

SEND RESPONSE version 2 packet size 44

```
  0.0.0.0/0 -> 0.0.0.0 family 2 tag 0 metric 1
  192.168.31.0/24 -> 0.0.0.0 family 2 tag 0 metric 3

Rip_read!
ignore packet comes from myself, 202.38.168.1
update timer fire!
SEND UPDATE to ge0/2 ifindex 3
multicast announce on ge0/2
update routes on interface ge0/2 ifindex 3
SEND to socket 11 port 520 addr 224.0.0.9
SEND RESPONSE version 2 packet size 44
  0.0.0.0/0 -> 0.0.0.0 family 2 tag 0 metric 1
  192.168.31.0/24 -> 0.0.0.0 family 2 tag 0 metric 3

Rip_read!
ignore packet comes from myself, 202.38.168.1
```

结果分析

对以上调试实例进行必要的分析，当出现不是预期情况的处理方法。

- RIP 会定时在各个接口发布更新报文，也会收到其他设备发送来的更新报文。

注意：

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug rip (events|packet|zebra)命令禁用此功能。

11.4 常见故障分析

11.4.1 故障现象：两台设备不能正常通信

现象	两台设备不能正常通信
分析	互连接口收发版本不匹配，认证类型不匹配，接口配置是否正确
解决	检查接口配置，修改接口配置

第12章 配置 OSPF

12.1 OSPF协议概述

OSPF(Open Shortest Path First)是动态路由协议,其功能是实现网际间的路由。

OSPF 是一个自治系统内部路由协议，用于在单一自治系统(autonomous system,AS)内计算产生路由。与 RIP 等距离向量路由协议不同的是，OSPF 是基于链路状态的路由协议。它能够在网络链路变化时快速产生新路由，并能够管理比 RIP 范围更大的网络自治系统。

OSPF 是自治系统内部使用的链路状态路由协议，OSPF 通过路由器之间通告链路状态信息（LSA），来建立链路状态数据库，然后就可以根据 SPF 算法计算出到每个结点的最短路径树了,进而可计算出路由。它的工作方式与我们熟悉的 RIP 和 IGRP 协议不同，OSPF 只须发送当前结点到相邻结点的路由结构信息，而 RIP 和 IGRP 需要结点把自己保留的路由表或路由表的一部分全部发送到相邻结点，相邻结点根据这些信息更新自己的路由表，显然 OSPF 协议发送的信息量少，而 RIP 发送的信息量较多。在通告的链路状态结构中，OSPF 协议支持 IP 子网结构。

OSPF 向相邻的路由器定期发送一个 hello 报文，并接收邻居路由器发来的 hello 报文。这个 hello 报文不但可以帮助路由器在初始工作时了解相邻结构，而且可以在运行中了解相邻路由器的工作情况，如果相邻的路由器关机了，或链路不通了，就不会从相应邻居那里收到 hello 报文了, 从而能够很快知道哪些路由器不能工作了，能够对网络拓扑结构的变化做到快速反应。

如果网络支持多个路由器，可以实现在一个网段的诸多 OSPF 路由器中选择一个指定路由器 DR 和一个备份指定路由器 BDR，在进行链路数据库同步时，由指定路由器向整个网络发送 LSA, 以减少流量开销。

12.2 配置OSPF

12.2.1 缺省配置信息

设备关于 OSPF 的缺省设置信息如以下表格所示：

表 12-1 OSPF 缺省配置信息

内容	缺省设置	备注
使能/禁止状态（enable/disable）	disable	可更改设置
OSPF区域认证类型（none/text/md5）	不认证	可更改设置
接口认证类型（none/text/md5）	不认证	可更改设置

发布缺省路由	不发布	可更改设置
OSPF路由的优先级	110	可更改设置
spf-delay值和spf-holdtime值	spf-delay：5秒 spf-holdtime：10秒	建议采用缺省设置
兼容rfc1583	不兼容	可更改设置
LSA重传时间	5秒	建议采用缺省设置
LSA发送延迟	1秒	建议采用缺省设置
Hello-interval值	10秒	可更改设置
Dead-interval值	4 * Hello-interval	可更改设置
接口选举DR的优先级	1	可更改设置
OSPF区域路由聚合	不聚合	可更改设置
重发布其他路由协议路由的路由类型	第2类外部路由	可更改设置

12.2.2 配置启用 OSPF 路由协议功能

启用 OSPF 路由协议，在此基础上才能对 OSPF 路由功能作进一步配置。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	router ospf	启用OSPF功能并进入OSPF配置节点

在配置模式下使用 no router OSPF 可以取消对 OSPF 的设置，使其恢复到缺省配置。

参数说明： router NAME

参数	说明	缺省配置
NAME	路由协议类型	无

提示：

只有在启用 OSPF 以后才能对 OSPF 其他功能作进一步配置。

12.2.3 配置 OSPF 路由器 Router-ID

OSPF 协议需要路由器的 Router-ID，作为本路由器在自治系统中的唯一标识。一般在协议任务启动后，会自动选出一个 Router-ID。通常路由器先挑选 IP 地址最大的环回地址。若无环回地址，则选择状态 up 的接口地址大的作为本路由器的 Router-ID.也可以指定一个 Router-ID。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	router ospf	启用OSPF功能并进入OSPF配置模式
步骤**3**	router-id 1.1.1.1	配置路由器Router-ID
步骤**4**	end	回到enable模式
步骤**5**	show ip ospf	show命令

使用 no router-id 可以取消对 router-id 的设置， router-id 将会重新自动选举。

参数说明： router-id A.B.C.D

参数	说明	缺省配置
A.B.C.D	OSPF Router-ID	

12.2.4 配置运行 OSPF 的接口

配置运行 OSPF 的接口以及其所属的区域。

配置步骤：

*步骤**1***	*configure terminal*	*进入配置模式*
*步骤**2***	*router ospf*	*启用OSPF功能并进入OSPF配置模式*
*步骤**3***	*network 10.0.1.0/24 area 0*	*从属于10.0.1.0/24接口上启用OSPF,其所属的区域为0*

步骤4	*end*	*回到enable模式*
步骤5	*show ip ospf*	*show命令*

使用 no network 10.0.1.0/24 area 0 可以取消设置。

参数说明： network A.B.C.D/M area (A.B.C.D|<0-4294967295>)

参数	说明	缺省配置
<A.B.C.D/M>	接口所属的网段	无
(A.B.C.D|<0-4294967295>)	区域ID	无

12.2.5 配置 OSPF 区域认证方式

OSPF 支持在同一区域内进行认证。一个区域中所有的路由器的认证类型必须一致（不认证、明文认证、MD5 密文认证）。认证提供基于密码的保护，防止未经授权对区域进行的访问。在配置区域认证时，必须对区域的所有接口单独配置认证密码。当接口的认证方式和接口所在区域的认证不一致时，优先考虑接口配置的认证方式。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router ospf	启用OSPF功能并进入OSPF配置模式
步骤3	area 0 authentication	配置区域0的认证方式为明文认证。
步骤4	end	回到enable模式
步骤5	show ip ospf	show命令

使用 no area (A.B.C.D|<0-4294967295>) authentication 可以取消区域认证的设置，恢复为默认值不认证。

参数说明： area (A.B.C.D|<0-4294967295>) authentication [message-digest]

参数	说明	缺省配置
(A.B.C.D|<0-4294967295>)	区域ID	无
message-digest	密文认证方式	没有这个参数表示明文

		认证

12.2.6 配置 OSPF NSSA

自治系统外的 ASE 路由不可以进入到 NSSA 区域中，但是 NSSA 区域内的路由器引入的 ASE 路由可以在 NSSA 中传播并发送到区域之外。由于是作为 OSPF 标准协议的一种扩展属性，应尽量减少与不支持该属性的路由器协调工作时的冲突和兼容性问题。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	router ospf	启用OSPF功能并进入OSPF配置模式
步骤**3**	area 1 nssa translate-candidate	配置区域1为nssa区域，并且该设备参与是否将7类lsa转为5类的选举。
步骤**4**	end	回到enable模式
步骤**5**	show ip ospf	show命令

使用 no area 1 nssa 可以取消该区域的 nssa 属性设置。

参数说明：area (A.B.C.D|<0-4294967295>) nssa (translate-candidate|translate-never|translate-always) [no-summary]

参数	说明	缺省配置
(A.B.C.D|<0-4294967295>)	区域ID	无
(translate-candidate|translate-never|translate-always)	NSSA区域的ABR是否进行7转5操作。非ABR该参数无意义。	缺省为translate-candidate，表示从ABR中选出一个来进行7转5操作。
[no-summary]	配置该参数的话，ABR会将3类LSA也过滤掉不传入NSSA区域	可选配置。

注意：

a)如果某个区域内的路由器配置了该属性，该区域内的所有路由器都要配置该属性。

b)在改变该属性时，需要重新启动 ospf。

12.2.7 配置 OSPF 区域间路由聚合

区域间的路由聚合是为了减少区域间路由数量，它使 ABR 通告一条聚合的域间路由到其他区域，而被聚合的路由不被宣告出去。在 OSPF 中，ABR 向其他区域发送路由信息时，以网段为单位生成 Type 3 LSA。如果该区域中存在一些连续的网段，则可以配置 ABR 将这些连续的网段聚合成一个网段。这样 ABR 只发送一条聚合后的 LSA，所有落入本命令指定的聚合网段范围的 LSA 将不再会被单独发送出去，这样可减少其他区域中链路状态数据库（LSDB）的规模。如果该网段范围用关键字 not-advertise 限定，则到这一个网段路由的聚合路由将不会被广播出去。这个网段是由 IP 地址/掩码的方式说明的。接收聚合网段和对网段的限定，可减少区域间路由信息的交流量。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router ospf	启用OSPF功能并进入OSPF配置模式
步骤3	area 0 range 10.0.0.0/16	设置聚合路由通告的区域和地址范围
步骤4	end	回到enable模式
步骤5	show running-config ospf	show命令

使用 no area (A.B.C.D|<0-4294967295>) range A.B.C.D/M.可以设置。

参数说明： area (A.B.C.D|<0-4294967295>) range A.B.C.D/M [not-advertise]

参数	说明	缺省配置
(A.B.C.D|<0-4294967295>)	进行聚合的区域ID	
A.B.C.D/M	地址范围	
[not-advertise]	不宣告聚合后的路由	

参数说明： area (A.B.C.D|<0-4294967295>) range A.B.C.D/M advertise cost <0-16777215>

参数	说明	缺省配置
(A.B.C.D|<0-4294967295>)	进行聚合的区域ID	
A.B.C.D/M	地址范围	
<0-16777215>	聚合路由的宣告Metric	

参数说明： area (A.B.C.D|<0-4294967295>) range A.B.C.D/M substitute A.B.C.D/M

参数	说明	缺省配置
(A.B.C.D|<0-4294967295>)	进行聚合的区域ID	1
A.B.C.D/M	地址范围	
A.B.C.D/M	将地址范围替换成该地址宣告	

提示：

可以使用 no area (A.B.C.D|<0-4294967295>) range A.B.C.D/M advertise cost 取消路由聚合宣告的 cost。

12.2.8 配置 OSPF 路由重分布

为了能够使得多个路由协议同时运作，可以将一种路由协议的信息引入到另一种路由协议中，这个过程可以称为路由重分布。运行 OSPF 的自治系统可以引入自治系统外部的其他路由协议的路由或者静态路由以达到路由信息共享。当路由器运行 OSPF 且还运行其他路由协议，若要引入外部路由信息，需要配置路由重分布。

OSPF 使用 4 类不同的路由，按优先级由高到低排列如下：

- 区域内路由
- 区域间路由
- 第一类外部路由
- 第二类外部路由

区域内和区域间路由描述自治系统内部的网络结构；外部路由则描述了如何选择到自治系统以为的路由。第一类外部路由是指接收的是 IGP 路由（例如 RIP、STATIC），由于这类路由的可信程度较高，所以，计算出的外部路由的花费与自治系统内部的路由花费的数量级相同，并且与 OSPF 自身路由的花费具有可比性，即到第一类外部路由的花费

值＝本路由器到相应的 ASBR 的花费值＋ASBR 到该路由目的地址的花费值。第二类外部路由器是指接收的是 EGP 路由，由于这类路由的可信度比较低，所以 OSPF 协议认为，从 ASBR 到自治系统之外的花费远远大于在自治系统之内到达 ASBR 的花费，计算路由花费时主要考虑前者。即第二类外部路由的花费值＝ASBR 到该路由目的地址的花费值。如果该值相等，再考虑本路由器到相应的 ASBR 的花费值。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	router ospf	启用OSPF功能并进入OSPF配置模式
步骤**3**	redistribute connected metric 11 metric-type 1	配置重发布直连路由，Metric为11，第一类外部路由
步骤**4**	end	回到enable模式
步骤**5**	show running-config ospf	show命令

使用 no redistribute (connected|static|rip)可以取消路由重发布的设置。

参 数 说 明： redistribute (connected|static|rip) metric <1-16777214> metric-type (1|2)

参数	说明	缺省配置
(connected|static|rip)	重发布路由的类型	无
<1-16777214>	重发布的路由的Metric	无
(1|2)	重发布路由的类型	第二类外部路由

12.2.9 配置 OSPF 重发布路由缺省 Metric

配置 OSPF 重发布外部路由时的缺省 Metric。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	router ospf	启用OSPF功能并进入OSPF配置模式
步骤**3**	default-metric 100	配置重发布路由的缺省Metric为100
步骤**4**	end	回到enable模式

步骤5	show running-config ospf	show命令

使用 no default-metric 可以取消该设置。

参数说明： default-metric <1-16777214>

参数	说明	缺省配置
<1-16777214>	*重发布路由的默认Metric*	*无*

12.2.10 配置 OSPF 重发布默认路由

一旦配置了路由重分布，路由器就自动成为自治系统边界路由器。但是缺省情况下，不会发布缺省路由，可以强制自治系统边界路由器发布缺省路由。但这时路由器表中必须包含缺省路由。如果路由表中没有缺省路由，而要强制自治系统边界路由器产生缺省路由，使用 always 参数。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router ospf	启用OSPF功能并进入OSPF配置模式
步骤3	default-information originate metric 100 metric-type 1	配置重发布默认路由，Metric为100，类型为第一类外部路由。
步骤4	end	回到enable模式
步骤5	show running-config ospf	show命令

使用 no default-information originate 可以取消该项配置，使其恢复到默认值。

参数说明： default-information originate metric <1-16777214> metric-type (1|2)

参数	说明	缺省配置
<1-16777214>	重发布默认路由的Metric。	无
(1|2)	重发布默认路由的类型	第二类外部路由

参数说明： default-information originate always metric <1-16777214> roumetric-type (1|2)

参数	说明	缺省配置
always	强制发布默认路由，即使路由表中没有默认路由。	无
<1-16777214>	重发布默认路由的Metric。	无
(1|2)	重发布默认路由的类型	第二类外部路由

12.2.11 配置 OSPF 协议优先级

一个协议的优先级指的是一个路由信息来源的可信度等级。优先级是一个 1 到 255 的整数，通常情况下，值越高可信度越低。值为 255 就意味着路由信息源根本不可信，应该被忽略。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	router ospf	启用OSPF功能并进入OSPF配置模式
步骤**3**	distance <1-255>	配置OSPF的管理距离（协议优先级）
步骤**4**	end	回到enable模式
步骤**5**	show running-config ospf	show命令

使用 no distance 可以取消配置，使其恢复到默认值 110。

参数说明： distance <1-255>

参数	说明	缺省配置
<1-255>	接口名	无

参数说明： distance ospf intra-area <1-255> inter-area <1-255> external <1-255>

参数	说明	缺省配置
<1-255>	域内路由的OSPF优先级	110
<1-255>	域间路由的OSPF优先级	110

<1-255>	AS外部路由的OSPF优先级	110

12.2.12 配置 OSPF 兼容 RFC1583

配置路由器计算外部到ASBR的路径时是否兼容RFC1583的规定，当有多条到达ASBR的AS内部路径时：

兼容RFC1583，直接判断多条路由的距离值

不兼容RFC1583，始终优先选择非骨干区域的区域内路径。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router ospf	启用OSPF功能并进入OSPF配置模式
步骤3	compatible rfc1583	设置兼容rfc1583
步骤4	end	回到enable模式
步骤5	show ip ospf	show命令

使用 no compatible rfc1583 可以取消兼容 rfc1583 的配置，使其恢复到默认值不兼容rfc1583。

12.2.13 配置 OSPF 路由计算定时器

配置 ospf 接收拓扑结构改变之后和启动最短路径优先（OSPF）之间的延迟时间和配置连续两次 SPF 计算之间的时间。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router ospf	启用OSPF功能并进入OSPF配置模式
步骤3	timers spf 1020	设置spf-delay为10秒，设置spf-holdtime为20秒
步骤4	end	回到enable模式
步骤5	show ip ospf	show命令

使用 no timers spf 可以取消该配置，使其恢复到默认值 spf-delay 为 5 秒，spf-holdtime 为 10 秒。

参数说明： timers spf <0-4294967295><0-4294967295>

参数	说明	缺省配置
<0-4294967295>	spf-delay值	5秒
<0-4294967295>	spf-holdtime值	10秒

12.2.14 配置 OSPF 接口认证方式

OSPF 支持接口间的邻居在建立邻居关系的时候进行认证，防止非法设备接入网络。OSPF 支持两种认证模式：明文认证和 MD5 认证。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	interface ge0/0	进入接口ge0/0进行OSPF配置
步骤3	ip ospf authentication	设置接口认证方式为明文认证
步骤4	end	回到enable模式
步骤5	show running-config	show命令

使用 no ip ospf authentication 可以取消该配置，使其恢复到默认值不认证。

参数说明： ip ospf authentication [message-digest]

参数	说明	缺省配置
[message-digest]	不用该参数表示明文认证，使用该参数表示密文认证	不认证

12.2.15 配置 OSPF 接口明文认证密钥

配置 OSPF 接口上用于明文认证的密钥。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	interface ge0/0	进入接口ge0/0进行OSPF配置

步骤3	ip ospf authentication-key aaa	设置接口明文认证密钥
步骤4	end	回到enable模式
步骤5	show running-config	show命令

使用 no ip ospf authentication-key 可以取消该配置，删除该认证密钥。

参数说明： ip ospf authentication-key AUTH_KEY

参数	说明	缺省配置
AUTH_KEY	配置用于明文认证的密钥	不认证

12.2.16 配置 OSPF 接口密文认证密钥

配置 OSPF 接口上用于密文认证的密钥。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	interface ge0/0	进入接口ge0/0进行OSPF配置
步骤3	ip ospf message-digest-key 1 md5 aaa	设置接口认证方式为明文认证
步骤4	end	回到enable模式
步骤5	show running-config	show命令

使用 no ip ospf message-digest-key<1-255>可以取消该配置，删除该认证密钥。

参数说明： ip ospf message-digest-key <1-255> md5 KEY

参数	说明	缺省配置
<1-255>	配置key-ID	无
KEY	密文认证的密钥	无

12.2.17 配置 OSPF 接口的优先级

网络支持多个路由器，可以实现在一个网段的诸多 OSPF 路由器中选择一个指定路由器 DR 和一个备份指定路由器 BDR，在进行链路数据库同步时，由指定路由器向整个网络发送 LSA, 以减少流量开销。

路由器接口的优先级决定了该接口在选举 DR 时所具有的资格，优先级高的在选举权发生冲突时首先考虑。DR 不是人为指定的，而是由本网段中所有的路由器共同选举出来的。本网段内优先级大于 0 的路由器都可以作为“候选人”。在所有自称是 DR 的路由器中选取优先级最大的；若两台路由器的优先级相等，则选 Router ID 最大的为 DR。在选举 DR 的同时也选举出 BDR，BDR 也和本网段内的所有路由器建立邻接关系并交换路由信息。当 DR 失效后，BDR 会立即成为 DR，由于不需要重新选举，并且邻接关系事先已经建立，所以这个过程是非常短暂的。这个时候还需要再重新选举出一个新的 BDR，虽然一样需要较长的时间，但并不会影响路由的计算。网段中的 DR 并不一定是 priority 最大的路由器；同理，BDR 也并不一定就是 priority 第二大的路由器。

DR 是指某个网段中的概念，是针对路由器的接口而言的。某台路由器在一个接口上可能是 DR，在另一个接口上可能是 BDR，或者是 DRother。

只有在广播或者 NBMA 类型接口时才会选举 DR，在点到点或者点到多点类型的接口上不需要选举 DR。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	interface ge0/0	进入接口ge0/0进行OSPF配置
步骤3	ip ospf priority <0-255>	设置接口的优先级
步骤4	end	回到enable模式
步骤5	show running-config ospf	show命令

使用 no ip ospfpriority 可以取消该配置，使其恢复到默认值不认证。

参数说明： ip ospf priority <0-255>

参数	说明	缺省配置
<0-255>	接口优先级	无

12.2.18 配置 OSPF 接口发送报文的开销

用户可以指定接口发送报文的开销，否则 OSPF 会根据当前的接口自动计算开销。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	interface ge0/0	进入接口ge0/0进行OSPF配置
步骤**3**	ip ospf cost <1-65535>	设置接口发送报文开销
步骤**4**	end	回到enable模式
步骤**5**	show ip ospf interface	show命令

使用 no ip ospf cost 可以取消该配置。

参数说明： ip ospf cost <1-65535>

参数	说明	缺省配置
<1-65535>	接口发送报文的开销	无

12.2.19 配置 OSPF 接口 LSA 重传间隔

当一台路由器向他的邻居发送一条 LSA 后，需要等待对方的确认报文。若在规定的时间内没有收到对方的确认报文，就会重传这条 LSA。用户可以对 retransmit-internal 的值进行配置。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	interface ge0/0	进入接口ge0/0进行OSPF配置
步骤**3**	ip ospf retransmit-interval <3-65535>	设置接口LSA重传间隔
步骤**4**	end	回到enable模式
步骤**5**	show ip ospf interface	show命令

使用 no ip ospf retransmit-interval 可以取消该配置，使其恢复到默认值 5 秒。

参数说明： ip ospf retransmit-interval <3-65535>

参数	说明	缺省配置
<3-65535>	LSA重传间隔时间	5秒

12.2.20 配置 OSPF 接口 LSA 发送延迟

在发送链路状态更新报文（LSU）时，对报文中 LSA 的老化时间增加 transmit-delay 秒。该参数的配置主要考虑到接口上发送报文的所需的时间。LSA 在本路由器的“链路状态数据库”（LSDB）中会随着时间老化（age 每秒钟加 1），但在网络的传输过程中却不会。所以有必要在发送之前将老化时间增加 transmit-delay 秒，这一点对于低速网络更为重要。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	interface ge0/0	进入接口ge0/0进行OSPF配置
步骤3	ip ospf transmit-delay <1-65535>	设置接口LSA发送延迟
步骤4	end	回到enable模式
步骤5	show ip ospf interface	show命令

使用 no ip ospf transmit-delay 可以取消该配置，使其恢复到默认值不认证。

参数说明： ip ospf transmit-delay <1-65535>

参数	说明	缺省配置
<1-65535>	接口LSA发送延迟	1秒

12.2.21 配置 OSPF 接口 Hello 报文定时器

Hello 报文是最常用的一种报文，它周期性地被发送至邻居路由器，用于发现与维护邻居关系，选举 DR 与 BDR。用户可以对发送 Hello 报文的时间间隔 Hello-interval 的值进行配置。值越小，网络的变化将被越快的发现，但将花费更多的网络的传输。同一网段的路由其的 Hello-interval 必须相同。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	interface ge0/0	进入接口ge0/0进行OSPF配置
步骤3	ip ospf hello-interval <1-65535>	设置接口Hello报文发送定时器
步骤4	end	回到enable模式
步骤5	show ip ospf interface	show命令

使用 no ip ospf hello-interval 可以取消该配置，使其恢复到默认值 10 秒。

参数说明： ip ospf hello-interval <1-65535>

参数	说明	缺省配置
<1-65535>	Hello报文发送间隔时间	10秒

12.2.22 配置 OSPF 接口邻居失效定时器

相邻路由器间的失效时间时指在该时间间隔内若未收到对方的 hello 报文，则认为对端路由器失效。用户可以对邻居路由器的失效时间 Dead-interval 的值进行配置。Dead-interval 的值至少是 Hello-interval 值的 4 倍，同一网段的路由器的 Dead-interval 也必须相同。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	interface ge0/0	进入接口ge0/0进行OSPF配置
步骤**3**	ip ospf dead-interval <1-65535>	设置接口邻居失效间隔时间
步骤**4**	end	回到enable模式
步骤**5**	show ip ospf interface	show命令

使用 no ip ospf dead-interval 可以取消该配置，使其恢复到默认值 40 秒。

参数说明： ip ospf dead-interval <1-65535>

参数	说明	缺省配置
<1-65535>	*邻居失效间隔时间*	*40秒*

12.2.23 配置接口的 OSPF 网络类型

缺省情况下，按不同介质可划分成下列三种网络：广播网络（以太网，令牌环网、FDDI），非广播多路访问网络（帧中继、X.25），点到点网络（HDLC、PPP）。对以上任一类网络都可以进行 OSPF 配置。可以不考虑缺省的介质类型，选择配置 OSPF 网络类型。利用这一点，可将非广播多路访问网络配置为广播网络，如 X.25 和帧中继允许 OSPF 在其上以广播型运行，这就不用再去配置邻居。可将广播网络配置为非广播多路访问网络，

例如当网络中有不支持组播传送地址的路由器时。对于不具有广播和组播能力的网络，必须配置对端邻居来指定发送 hello 报文，并可以指定邻居的优先级和轮询时间间隔。

点到多点时具有一个或者多个邻居的编号的点到点接口，它建立多主机路由。与非广播多路访问和点到点网络相比，点到多点网络具有以下优点：一到多接口更易于配置，因为它不需要配置邻居命令，只需要一个 IP 子网，所以不必分配路由选择。不需要全网络拓扑结构，开销较小。

设备支持 OSPF 网络类型有广播型和点对点型。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	interface ge0/0	进入接口ge0/0进行OSPF配置
步骤**3**	ipospf network (broadcast|point-to-point)	设置接口OSPF网络类型
步骤**4**	end	回到enable模式
步骤**5**	show ip ospf interface	show命令

使用 no ipospf network 可以取消该配置。

参数说明： ipospf network (broadcast\|point-to-point)

参数	说明	缺省配置
broadcast	设置接口OSPF网络类型为广播型网络。	
point-to-point	设置接口OSPF网络类型为点对点型网络。	

12.3 常见故障分析

12.3.1 故障现象 1：两台设备不能建立邻接关系

现象	两台设备不能建立邻接关系
分析	区域ID不匹配 认证类型不匹配 密钥不匹配 网段（网络掩码匹配）

	Hello-interval不匹配 Dead-interval不匹配 两台设备间是否需要建立邻接关系？
解决	检查接口上OSPF参数的配置 是否应该和邻居路由器建立一个邻接关系，满足下列条件中的一个或者多个，那么将建立邻接关系： 网络类型是点对点的 网络类型是点到多点的 网络类型是虚链路 本地路由器是邻接路由器所在网络的DR 本地路由器是邻接路由器所在网络的BDR 邻居路由器是DR 邻居路由器是BDR

第13章 配置 BGP

13.1 BGP协议概述

BGP（Border Gateway Protocol）是一种不同自治系统的路由器之间进行通信的外部网关协议(Exterior Gateway Protocol，EGP)，其主要功能是在不同的自治系统(Autonomous Systems，AS)之间交换网络可达信息，并通过协议自身机制来消除路由环路。

BGP 使用 TCP 协议作为传输协议，通过 TCP 协议的可靠传输机制保证 BGP 的传输可靠性。

运行 BGP 协议的 Router 称为 BGP Speaker，建立了 BGP 会话连接(BGP Session)的 BGP Speakers 之间被称作对等体(BGP Peers)。 BGP speaker 之间建立对等体的模式有两种： IBGP(Internal BGP) 和 EBGP(External BGP)。IBGP 是指在相同 AS 内建立的 BGP 连接，EBGP 是指在不同 AS 之间建立的 BGP 连接。二者的作用简而言之就是：EBGP 是完成不同 AS 之间路由信息的交换，IBGP 是完成路由信息在本 AS 内的过渡。

本产品支持的是版本是 BGP-4，具有如下特点：

- 支持配置 router-id
- 支持手动指定 BGP 对等体
- 支持 BGP 对等体组
- 支持使用 Loopback 接口
- 支持多跳跃 EBGP 连接
- 支持接收路由数量限制
- 支持过滤私有 AS 号
- 支持定时器设置
- 支持 BGP 和 IGP 交互
- 支持 BGP 路由聚合
- 支持 BGP 路由衰减
- 支持 BGP 路由反射器
- 支持 AS 联盟
- 支持管理距离配置
- 支持 BGP 软复位
- 支持 BGP 的监控和维护

支持的路由属性主要有以下十种：

- ORIGN

- AS_PATH
- NEXT_HOP
- MULTI_EXIT_DISC
- LOCAL-PREFERENCE
- ATOMIC_AGGREGATE
- AGGREGATOR
- COMMUNITY
- ORIGINATOR_ID
- CLUSTER_LIST

除此而外，还支持对接收和发布的路由实施策略，支持 AS 路径列表过滤，访问列表(access list)、前缀列表(prifex list)、分发控制列表(distribute-list)和路由映射(Route map)过滤器。

13.2 配置BGP

13.2.1 缺省配置信息

关于 BGP 的缺省设置信息如以下表格所示：

表13-1 BGP 缺省配置信息

内容	缺省设置	备注
路由器ID	如果配置了lookback接口，就从lookback接口中选择最大的，否则就从物理接口中选择最大的。	可更改设置
缺省路由生成	不生成	可更改设置
EBGP多跳	关闭/2555	可更改设置
发布缺省路由	不发布	可更改设置
TCP MD5认证	不认证	不可更改设置
Keepalive Time值	60秒	建议采用缺省设置
Holdtime 值	180秒	可更改设置
ConnectRetry time	120秒	不可更改设置
AdvIntelval（IBGP）	15秒	建议采用缺省设置
Advintelval(EBGP)	30秒	建议采用缺省设置

Bgp scan time	60秒	可更改设置
MED值	0	可更改设置
Local_pref值	100	可更改设置
路由聚合	关闭	可更改设置
路由衰减	关闭	可更改设置
Suppress limit	2000	可更改设置
Half-life-time	15minutes	可更改设置
Reuse limit	750	可更改设置
Max-suppress time	4*half-life-time	可更改设置
管理距离	EBGP 20 IBGP 200 Local 200	
IGP 路由检查	不检查	可更改设置

13.2.2 配置启用 BGP 路由协议功能

启用 BGP 路由协议，在此基础上才能对 BGP 路由功能作进一步配置。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	router bgp <1-4294967295>	启用bgp功能并进入bgp配置节点

在配置模式下使用 no router bgp<1-4294967295>可以取消对 bgp 的设置，使其恢复到缺省配置。

参数说明： router NAME

参数	说明	缺省配置
NAME	路由协议类型	无

提示：

只有在启用 bgp 以后才能对 bgp 其他功能作进一步配置。每一台设备同时只能配置一个 bgp 实例。

自治系统：AS 是拥有同一选路策略，在同一技术管理部门下运行的一组路由器。它的范围是<1-4294967295>。

13.2.3 配置 BGP 路由器 Router-ID

BGP 协议需要路由器的 Router-ID，作为本路由器在自治系统中的唯一标识。一般在协议任务启动后，会自动选出一个 Router-ID。通常路由器先挑选 IP 地址最大的环回地址。若无环回地址，则选择状态 up 的接口地址大的作为本路由器的 Router-ID.也可以指定一个 Router-ID。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用BGP功能并进入BGP配置模式
步骤3	bgp router-id 1.1.1.1	配置路由器Router-ID
步骤4	end	回到enable模式
步骤5	show ip bgp	show命令

使用 no bgp router-id 可以取消对 router-id 的设置， router-id 将会重新自动选举。

参数说明： bgp router-id A.B.C.D

参数	说明	缺省配置
A.B.C.D	bgp Router-ID	

13.2.4 配置指定 BGP 对等体

BGP 的运行需要手动指定对等体。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor 1.1.1.1 remote-as 100	指定对等体的ip地址为1.1.1.1 所属AS 为AS100

步骤4	end	回到enable模式
步骤5	show run bgp	show命令

使用 no neighbor 1.1.1.1 remote-as 100 可以取消设置。

参数说明： neighbor A.B.C.D remote-as <1-4294967295>

参数	说明	缺省配置
A.B.C.D	对等体的地址	无
<1-4294967295>	对等体所属自治系统的自治系统号	无

13.2.5 配置 BGP 对等体组

对 BGP Speaker 来说，许多对等体的配置信息(包括执行的路由策略等)都相同，为了简化配置，提高效率，推荐使用 BGP 对等体组。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor WORD peer-group	创建对等体组。
步骤4	neighbor A.B.C.D peer-group WORD	向对等体组中添加成员
步骤5	end	回到enable模式
步骤6	show run bgp	show命令

使用 no neighbor peer-group WORD 可以取消对等体组设置，恢复为默认值不认证。

参数说明： neighbor A.B.C.D peer-group WORD

参数	说明	缺省配置
A.B.C.D	对等体组的地址	无
WORD	对等体组的名字	

13.2.6 配置回环接口作为 BGP 邻居

BGP 使用到达一个邻居的最优本地地址作为发送更新报文的源。该地址通常是具有到邻居的最佳路径的接口的 IP 地址。当有多条链路可用于连接到一个邻居时，这通常在 IBGP 拓扑中出现，通常使用一个环回接口作为本地路由器的 BGP 邻居，并且可用性很强。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor 1.1.1.1 remote-as 100	指定对等体的ip地址为1.1.1.1 所属AS 为AS100
步骤4	neighbor 1.1.1.1 update-source lo1	配置lo1作为作为邻居的源端口
步骤5	end	回到enable模式

使用 no neighbor A.B.C.D update-source lo1 可以撤销设置。

参数说明： neighbor A.B.C.D update-source lo<1-255>

参数	说明	缺省配置
A.B.C.D	对等体IP地址	无
lo<1-255>	Lookback接口地址	无

13.2.7 EBGP 多跳配置

EBGP 缺省的 TTL 值是 1 跳，要求是直连的。如果不是直连的，就需要配置 EBGP 多跳并配置跳数<1-255>。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor A.B.C.D ebgp-multihop<1-255>	配置EBGP多跳并配置跳数
步骤4	End	回到enable模式
步骤5	show running-config bgp	show命令

使用 no neighbor1.1.1.1 ebgp-multihop<1-255>取消设置。

参数说明： neighbor A.B.C.D ebgp-multihop<1-255>

参数	说明	缺省配置
A.B.C.D	邻居IP地址	无
<1-255>	跳数	1

13.2.8 配置删除私有 AS 号

在 RFC4271 中规定 AS 号的 64512 到 65535 为私有 AS 号不能在公网上传播。所以有的时候需要向对等体宣告路由的时候去掉私有的 AS 号。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor{A.B.C.D | peer-group-name}remove-private-AS	删除私有AS号
步骤4	end	回到enable模式
步骤5	show ip bgp	show命令

使用 no neighbor{A.B.C.D | peer-group-name}remove-private-AS，可以取消该配置。

参数说明： neighbor{A.B.C.D \| peer-group-name}remove-private-AS

参数	说明——Table Heading	缺省配置
A.B.C.D	邻居IP地址	无
peer-group-name	组名	无

13.2.9 配置允许发送团体属性

BGP 默认是不向对等体发送团体属性的，有的时候采用团体属性做路由过滤的时候，需要开启向邻居发送团体属性。

配置步骤：

步骤1	configure terminal	进入配置模式

步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor{A.B.C.D | peer-group-name}send-community	开启发送团体属性
步骤4	end	回到enable模式
步骤5	show running-config	show命令

使用 no neighbor{A.B.C.D | peer-group-name}send-community 可以取消该配置.

参数说明： neighbor{A.B.C.D | peer-group-name}send-community

参数	说明	缺省配置
A.B.C.D	邻居IP地址	无
peer-group-name	组名	无

13.2.10 配置限制接收的路由数量

不同的设备性能是不一样的，有的时候为了保护设备，就需要限制接收路由的数量。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor{A.B.C.D | peer-group-name}maximum-prefix<1-4294967295>	配置限制接收路由的数量
步骤4	end	回到enable模式
步骤5	show running-config	show命令

使用 no neighbor{A.B.C.D | peer-group-name}maximum-prefix<1-4294967295>可以取消该配置。

参数说明：neighbor{A.B.C.D | peer-group-name}maximum-prefix<1-4294967295>

参数	说明	缺省配置
A.B.C.D	邻居IP地址	无

peer-group-name	组名	无
<1-4294967295>	路由数量	无

13.2.11 配置保留对等体路由信息

保存邻居发来的路由信息，当 bgp 重新建立对等体时，不需要要邻居直接发送路由信息，这样对内存要求比较高，一般情况下不建议这样配置。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor{A.B.C.D | peer-group-name} soft-reconfiguration inbound	配置保留对等体路由信息
步骤4	end	回到enable模式
步骤5	show running-config	show命令

使用 no neighbor{A.B.C.D | peer-group-name} soft-reconfiguration inbound 可以取消该配置。

参数说明： neighbor{A.B.C.D \| peer-group-name} soft-reconfiguration inbound

参数	说明	缺省配置
A.B.C.D	邻居IP地址	无
peer-group-name	组名	无

注意：

一般情况下不需要这样配置对内存要求很高的。

13.2.12 配置关闭对等体

有的时候配置一些路由策略而需要临时关闭 BGP 对等体。

配置步骤：

步骤1	configure terminal	进入配置模式

步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor{A.B.C.D | peer-group-name} shutdown	关闭BGP对等体
步骤4	end	回到enable模式
步骤5	show running-config bgp	show命令

使用 no neighbor{A.B.C.D | peer-group-name} shutdown 可以取消该配置。

参数说明： neighbor{A.B.C.D | peer-group-name} shutdown

参数	说明	缺省配置
A.B.C.D	邻居IP地址	无
peer-group-name	组名	无

13.2.13 配置 IGP 和 BGP 路由交互

通过和 IGP 协议的交互，从 IGP 注入路由信息。BGP 将注入的路由发布给自己的邻居。要通过 Network 命令手工注入 BGP Speaker 要向其 BGP Speaker 公告的网络信息。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	network A.B.C.D/M [backdoor]	宣告路由
步骤4	end	回到enable模式
步骤5	show ip bgp	show命令

使用 no network A.B.C.D/M 可以取消该配置。

参数说明： network A.B.C.D/M [backdoor]

参数	说明	缺省配置
A.B.C.D/M	路由/掩码	无

注意：

1）如果不加掩码，就按默认的 A、B、C 类

2）如果要确保通告的路由为本地存在的路由，还需要配置 bgp network import-check 坚持这条路由是否在当前的 IP 路由表中，如果不在的话就不把这条路由作为 BGP 路由

13.2.14 配置重发布 IGP 路由到 BGP

将 IGP 产生的路由重发布到 BGP 的路由中，重发布的路由可以是直连路由、静态路由和动态路由协议产生的路由。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤**3**	redistribute [connected | ospf | rip | static]	重发布路由
步骤**4**	end	回到enable模式
步骤**5**	show ip bgp	show命令

使用 no redistribute [connected | ospf | rip | static]可以取消该配置，使其恢复到默认值 5 秒。

参数说明： redistribute [connected | ospf | rip | static]

参数	说明	缺省配置
Connected	直连路由	无
Ospf	Ospf产生的路由	无
Rip	Rip产生的路由	无
Static	静态路由	无

13.2.15 配置 BGP 的定时器

BGP 使用 Kepalive 定时器来维持和对等体的有效连接，使用 Holdtime 定时器来判断对等体是否有效。缺省情况下，Kepalive 定时器的值为 60 S，Holdtime 定时器的值 180S。当 BGP Speakers 之间建立 BGP 连接时，双方将对 Holdtime 进行协商，值更小的 Holdtime 将被选择，而 Keepalive 定时器值的选择将基于协商后的 Holdtime 的 1/3 和配置的 Keepalive 的值得较小者。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	timers bgp<0-65535><0-65535>	设置Holdtime、keepalive定时器
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

使用 no timers bgp<0-65535><0-65535>可以取消该配置。

参数说明： timers bgp<0-65535><0-65535>

参数	说明	缺省配置
<0-65535>	Keepalive	60秒
<0-65535>	Holdtime	180秒

注意：

设置了定时器后必须执行 clear 命令，有关 clear 命令下面会讲到使用。

13.2.16 配置 MED 属性

BGP 使用 MED 值作为从 EBGP Peers 学习到的路径进行优先级比较的依据之一，MED 值越小，路径优先级越高。

缺省情况下，选举最优路径时，只对来自同一 AS 的对等体的路径才比较 MED 值，如果您希望允许比较来自不同 AS 的对等体的路径的 MED 值，在 BGP 配置模式下执行：

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	bgp always-compare-med	允许来自不同 AS 的路径的MED值能进行比较。
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

缺省情况下，选举最优路径时，对来自 AS 联盟内部其他子 AS 的对等体的路径是不进行 MED 比较的，如果您希望来自 AS 联盟内部对等体的路径允许比较 MED 值，在 BGP 配置模式下执行：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	bgp bestpath med confed	允许来自联盟内部其他子AS 的对等体的路径的 MED 值能进行比较。
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

缺省情况下，如果接收到未设置 MED 属性的路径，该路径的 MED 值被认为是 0 根据 MED 值越小，路径优先级越高，所以该路径的 MED 达到了最高的优先级。
如果您希望未设置 MED 属性的路径的 MED 属性优先级为最低，在 BGP 配置模式下执行：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	bgp bestpath med missing-as-worst	将未设置MED属性的路径的优先级设置为最低。
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

缺省情况下，选举最优路径时，将根据接收到的路径的顺序进行比来自相同 AS 的对等体的路径先比较，在 BGP 配置模式下执行：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	bgp deterministic-med	允许来自相同AS的对等体的路径先比较，缺省情况下将按照路径接收顺序比较，后接收的路径先比较。
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

提示：

除此之外也可以通过 route-map 修改 AS-PATH 属性。

13.2.17 配置 LOCAL_PREF 属性

BGP 使用 LOCAL_PREF 作为从 IBGP Peers 学习到的路径进行优先级比较的依据之一，LOCAL_PREF 值越大优先级越高。

BGP Speaker 将接收到的外部路由发送给 IBGP Peers 时添加本地优先级属性，如果需要修改本地优先级属性，在 BGP 配置模式下执行：

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	bgp default local-preference<0-4294967295>	修改localpref的值
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

使用 no bgp default local-preference<0-4294967295>可以取消该配置，恢复到默认的 100.

参数说明： bgp default local-preference <0-4294967295>

参数	说明——Table Heading	缺省配置
<0-4294967295>	Local_pref值	100

提示：

除此之外也可以通 route-map 进行修改。

13.2.18 配置比较 router-id

缺省情况下，在选举最优路径过程中，如果接收到两条从不同 EBGP Peers 接收来的所有路径属性都相同的路径，我们是根据接收的顺序选举最优路径。您可以通过配置如下命令，选举 Router ID 更小的路径为最优路径。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	bgp bestpath compare-routerid	允许BGP进行最优路径选择时比较 router ID。
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

使用 no bgp bestpath compare-routerid 可以取消该配置。

13.2.19 配置 BGP 聚合路由

BGP-4 支持 CIDR，所以允许创建聚合表项，以减小 BGP 路由表的大小。当然，只有当聚合范围内存在有效的路径时，才将 BGP 聚合表项添加到 BGP 路由表中。本产品支持手动聚合和自动聚合。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	aggregate-addressA.B.C.D/M	配置聚合路由
步骤4	aggregate-addressA.B.C.D/Mas-set	添加AS号
步骤5	aggregate-addressA.B.C.D/Msummary-only	不发送聚合精细路由
步骤6	end	回到enable模式
步骤5	show run bgp	show命令

参数说明： aggregate-addressA.B.C.D/M [as-setsummary-only]

参数	说明	缺省配置
A.B.C.D/M	聚合路由	

参数说明： aggregate-addressA.B.C.DAggregate maskA.B.C.D [as-setsummary-only]

参数	说明	缺省配置
A.B.C.D	聚合地址	

A.B.C.D	聚合掩码	

注意：

路由聚合对设备的性能要求很高的，应在充分考虑设备性能后再考虑使用。

13.3 常见故障分析

13.3.1 故障现象 1：两台设备不能建立邻接关系

现象	两台设备不能建立邻接关系
分析	两边peer地址路由不可达 对等体IP地址或者AS号配置错误 Open报文协商不成功 配置lookback接口路由不可达 Igp之间网络不通 Router-id冲突
解决	检查接口配置 打开debug开关 通过抓包分析

第14章 配置防火墙策略

14.1 防火墙策略概述

防火墙策略对通过设备的源接口/源域、目的接口/目的域、源 ip、目的 IP、服务、用户、应用、时间进行访问控制

14.2 配置防火墙策略

14.2.1 防火墙策略添加和删除

14.2.2 防火墙策略添加

配置步骤:

步骤1	configure terminal	进入配置模式
步骤2	**policy** (*IF_IN*|any) (*IF_OUT*|any) (*SIP*|any) (*DIP*|any) *CMD_GROUP_SERVICE* (*USER*|any)(*APP*any) (*TR*|always)(permit|deny)	添加防火墙策略
步骤3	show policy	查看防火墙策略

参数说明：policy (IF_IN\|any) (IF_OUT\|any) (SIP\|any) (DIP\|any) CMD_GROUP_SERVICE (USER\|any)(APP\|any) (TR\|always)(permit\|deny)

参数	说明	缺省配置
IF_IN	策略匹配的入接口	无
IF_OUT	策略匹配的出接口	无
SIP	策略匹配的源IP	无
DIP	策略匹配的目的IP	无
CMD_GROUP_SERVICE	策略匹配的服务	无
USER	策略匹配的用户名	无
APP	策略匹配的应用	无
TR	策略生效的时间	无
PERMIT|DENY	策略动作	无

14.2.3 防火墙策略删除

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	no policy PolicyID	删除防火墙策略

参数说明：no policy PolicyID

参数	说明	缺省配置
<PolicyID>	防火墙策略ID	无

14.2.4 基于策略的老化时间的修改

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	protocol manage NAME	进入到名称为NATM的协议管理模式
步骤3	protocal（tcp|udp）	配置协议类型
步骤4	port PORT_NUMBER	配置协议端口号
步骤5	timeout TIMEOUT	配置超时时间，单位分钟

防火墙的服务和协议管理相同即可自动关联。

参数说明：protocol manage NAME

参数	说明	缺省配置
< NAME>	协议管理名称	无

参数说明：port PORT_NUMBER

参数	说明	缺省配置
<PORT_NUMBER >	协议端口	无

参数说明：timeout TIMEOUT

参数	说明	缺省配置
<TIMEOUT >	超时时间	无

14.2.5 流镜像功能

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	policy PolicyID	进入到防火墙策略配置模式
步骤3	mirror IFNAME	设置将匹配策略的流量镜像到物理接口

参数说明： policy PolicyID

参数	说明	缺省配置
<PolicyID>	防火墙策略ID	无

参数说明：mirror IFNAME

参数	说明	缺省配置
<IFNAME>	匹配策略的流量镜像到的接口名称	无

14.2.6 使能和禁用

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	policy PolicyID	进入到防火墙策略配置模式
步骤3	enable|disable	启用/禁用防火墙策略

参数说明：policy PolicyID

参数	说明	缺省配置
<PolicyID>	防火墙策略ID	无

14.3 配置案例

案例描述

配置防火墙策划，入接口 ge0/0，出接口 ge0/1，用户 lili 的数据阻断。

配置步骤：

步骤**1**	进入congfig模式
	DCFW-1800#configure terminal
步骤**2**	添加防火墙策略
	DCFW-1800(config)# policy 1 ge0/0 ge0/1 any any any lili any always deny
步骤**3**	启用策略
	DCFW-1800(config-policy)# enable

第15章 配置用户策略

15.1 用户策略概述

为了方便用户配置和管理，下一代防火墙设备中引入了认证策略的概念。认证策略用来控制用户上网的认证方式。

15.2 配置用户策略

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	user-policy (IF_IN|any) （IF_OUT|any）（SIP|any）（DIP|any）（TR|always）（local-webauth|permit）	添加用户认证策略
步骤3	showuser-policy	查看用户认证策略
步骤4	no user-policy USER_POLICY_ID	删除用户认证策略

参数说明：user-policy (IF_IN\|any)（IF_OUT\|any）(SIP\|any）(DIP\|any）(TR\|always）（local-webauth\|permit）

参数	说明	缺省配置
IF_IN	策略匹配的入接口	无
IF_OUT	策略匹配的出接口	无
SIP	策略匹配的源IP	无
DIP	策略匹配的目的IP	无
TR	策略生效时间	无
local-webauth|permit	策略动作类型，本地web认证、允许通过	无

参数说明： no user-policy USER_POLICY_ID

参数	说明	缺省配置
USER_POLICY_ID	用户认证策略ID	无

15.3 配置案例

案例描述

配置 ge0/1 接口的用户 web 认证。

配置步骤：

步骤1	进入congfig模式
	DCFW-1800#configure terminal
步骤2	添加防火墙策略并启用
	DCFW-1800(config)# user-policy ge0/1 any any any always local-webauth

第16章 配置 Web 访问策略

16.1 Web访问策略概述

通过 Web 访问策略，管理员可以：

- 通过配置，禁止用户访问特定的主机或者 URL 分类。
- 对用户的 Web 访问进行记录。

16.2 配置Web访问策略

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	web-policy <1-32> (USER|any) (ADDR|any) (enable|disable)	添加web访问策略
步骤3	rule <1-32> (CATEGORY|any) (FILE|any) (KEYWORD|any) (permit|deny) (emergencies|alerts|critical|errors|warnings|notifications|information|ignore) (SCHEDULE|always) (enable|disable)	向web访问策略里面添加规则
步骤4	web-policy forbidden-page [enable |disable]	启用/禁用阻断提示页面
步骤5	no rule <1-32>	从web访问策略里删除规则
步骤6	exit	退出配置模式
步骤7	show web-policy	显示当前配置的web访问策略
步骤8	web-policy <1-32>	修改web访问策略
步骤9	no web-policy <1-32>	删除web访问策略

***参数说明：*web-policy <1-32> (USER|any) (ADDR|any) (enable|disable)**

参数	说明	缺省配置
<1-32>	Web访问策略ID	无
USER|any	用户对象或用户对象组	无
ADDR|any	地址对象或地址对象组	无

enable|disable	启用或禁用web访问策略	无

参数说明： rule <1-32> (CATEGORY|any) (KEYWORD|any) (permit|deny) (emergencies|alerts|critical|errors|warnings|notifications|information|ignore) (SCHEDULE|always) (enable|disable)

参数	说明	缺省配置
<1-32>	Web访问策略ID	无
CATEGORY|any	URL分类名称，可以是自定义的或者预定义的	
FILE|any	文件类型	
KEYWORD|any	关键字对象名称	
SCHEDULE|always	规则生效时间	
permit|deny	规则禁用|启用	
emergencies|alerts|critical|errors|warnings|notifications|information|ignore	日志级别	

16.3 配置自定义URL类

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	url-category CATEGORY_NAME	添加自定义URL类，或者配置已经存在的URL类
步骤3	description CONTENT	添加该自定义URL类的描述信息
步骤4	url URL	向该自定义URL类中添加URL
步骤5	no url URL	从该自定义URL类中删除某条URL

16.4 配置案例

案例描述

配置 web 访问策略，阻止访问搜索引擎，并记录日志。

配置步骤：

步骤**1**	进入congfig模式
	DCFW-1800#configure terminal
步骤**2**	添加web访问策略
	DCFW-1800(config)# web-policy 1 user 192.168.1.41 enable
步骤**3**	添加规则，阻止访问搜索引擎
	DCFW-1800 (config-app-policy)# rule 1 searchengine any deny information always enable

第17章 配置应用审计策略

17.1 应用审计策略概述

企业环境中，为了提高员工的工作效率，通过应用审计功能，可以记录用户在网络中的行为，帮忙管理员更好的管理网络。

应用审计功能可以对如下几类应用审计出行为和内容：

- 即时通讯
- 搜索引擎
- 社交网络
- 电子邮件
- 文件共享
- 在线购物

17.2 配置应用审计策略

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	audit-policy <1-32> (USER|any) (ADDR|any) (enable|disable)	添加应用审计策略
步骤3	audit (instant-message|search-engine|social-network|email|file-transfer|online-shopping|other)	向应用审计策略中添加要审计的行为和内容
步骤4	no audit (instant-message|search-engine|social-network|email|file-transfer|online-shopping|other)	从应用审计策略里删除要审计的行为和内容
步骤5	exit	退出配置模式
步骤6	show audit-policy	显示当前配置的应用审计策略
步骤7	audit-policy <1-32>	修改应用审计策略
步骤8	no audit-policy <1-32>	删除应用审计策略

*参数说明：***audit-policy <1-32> (USER|any) (ADDR|any) (enable|disable)**

参数	说明	缺省配置
<1-32>	应用审计策略ID	无
USER|any	用户对象或用户对象组	无
ADDR|any	地址对象或地址对象组	无
enable|disable	启用或禁用应用审计策略	无

*参数说明：*audit (instant-message|search-engine|social-network|email|file-transfer|online-shopping|other)

参数	说明	缺省配置
instant-message|search-engine|social-network|email|file-transfer|online-shopping|other	审计的行为和内容，分别对应： 即时通讯|搜索引擎|社交网络|电子邮件|文件共享|在线购物。other对应于除了上述几类行为之外的其它类。	

17.3 配置案例

案例描述

配置应用审计策略，审计即时通讯及电子邮件，并记录日志。

配置步骤：

步骤1	进入congfig模式
	DCFW-1800#configure terminal
步骤2	添加应用审计策略
	DCFW-1800(config)# audit-policy 1 any any enable
步骤3	审计即时通讯及电子邮件
	DCFW-1800 (config-app-policy)# audit instant-message DCFW-1800 (config-app-policy)# audit email

第18章 配置控制策略

18.1 控制策略概述

随着宽带网络的不断普及，IM(即时聊天软件，如 MSN、QQ)，P2P(点到点传输软件，如 BitTorrent、eMule)，流媒体（视频点播软件，如 PPLive、QQLive），网络游戏（如搜狐游戏大厅、快乐西游）和股票软件（如大智慧、万点理财）在人们的工作、生活中也扮演了越来越重要的角色。

IM、P2P、流媒体、网络游戏和股票软件在给人们带来便利的同时，也给网络管理带来了新的挑战。一方面，这些软件随意滥用导致的网络拥堵、内部网络信息泄露、病毒传播等情况时有发生；另一方面，由于应用协议的复杂性，传统的防火墙对这些常用外联软件又无能为力，所以迫切需要针对外联软件进行有效管理的手段。

应用主要有以下类别：

- 即时通讯：MSN、QQ、雅虎通、Gtalk、Skype 等。
- P2P 软件：迅雷、QQ 旋风、BitTorrent 等。
- 流媒体：优酷、土豆、新浪视频等。
- 网络社区：新浪微博、腾讯微博、猫扑论坛、百度贴吧等。
- 网络游戏：魔兽世界、英雄联盟、刀塔等。
- 搜索引擎：百度、谷歌、雅虎、搜狗等。
- 电子商务：淘宝、京东、一号店、亚马逊等。
- 其他类别如股票软件、文件传输、电子邮件、远程控制、生活服务等。

应用只有在应用策略中引用，才能对相关的用户进行应用的控制和审计。应用对象随着应用特征库的更新而更新，用户不能手动创建新的应用对象，也不能删除已有的应用对象。

18.2 配置控制策略

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	app-policy ID(any|USER)(any|ADDRESS)	添加控制策略
步骤3	rule ID APP (ACTION|any) (CONTENT|any) (exclude|include) KEYWORD (SCHEDULE|always) (deny|permit) (alerts|critical|emergencies|errors|ignore|information|notifications|warnings)	向控制策略里面添加规则
步骤4	rule ID （enable|disable）	规则启用禁用

步骤5	（enable|disable）	策略启用禁用

参数说明： app-policy ID(any\|USER)(any\|ADDRESS)

参数	说明	缺省配置
ID	控制策略ID	无
any|USER	用户对象或用户对象组	无
any|ADDRESS	地址对象或地址对象组	无

参数说明：rule ID APP (ACTION|any) (CONTENT|any) (exclude|include) KEYWORD (SCHEDULE|always) (deny|permit) (alerts|critical|emergencies|errors|ignore|information|notifications|warnings)

参数	说明	缺省配置
ID	控制策略ID	无
APP	应用名称	
ACTION|any	应用行为	
CONTENT|any	应用行为内容	
exclude|include	关键字包含关系	
KEYWORD	关键字对象名称	
SCHEDULE|always	规则生效时间	
deny|permit	规则禁用|启用	
alerts|critical|emergencies|errors|ignore|information|notifications|warnings	日志级别	

18.3 配置案例

案例描述

配置控制策略，阻断 qq 的登录动作，并记录日志。

配置步骤：

步骤**1**	进入congfig模式
	DCFW-1800#configure terminal
步骤**2**	添加上网行为管理策略
	DCFW-1800(config)# app-policy 1 any any
步骤**3**	添加规则，阻断qq的登录动作
	DCFW-1800 (config-app-policy)# rule 1 qq Login any include any always deny notifications

第19章 应用策略白名单

19.1 白名单概述

白名单的概念与“黑名单”相对应。如果设立了白名单，则在白名单中的用户（或 IP 地址）会优先通过，安全性和快捷性都大大提高。应用控制策略、Web 访问策略、应用审计对白名单匹配的用户和地址不生效。

19.2 配置白名单

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	app-policy white-list (user | addr)	添加需要设置白名单的用户及地址

***参数说明：*app-policy white-list [user | addr]**

参数	说明	缺省配置
USER|any	用户对象或用户对象组	无
ADDR|any	地址对象或地址对象组	无

19.3 配置案例

案例描述

配置白名单，使 ip 为 2.2.2.2 的用户不被审计。

配置步骤：

步骤**1**	进入congfig模式
	DCFW-1800#configure terminal
步骤**2**	添加用户
	DCFW-1800(config)#user-local user_test DCFW-1800(config-user)#enable bind DCFW-1800(config-user)#bind ip address 2.2.2.2 DCFW-1800(config-user)#exit
步骤**3**	添加地址

	DCFW-1800(config)#address addr_test DCFW-1800(config-addr)# host-address 2.2.2.2 DCFW-1800(config-addr)#exit
步骤4	配置白名单
	DCFW-1800(config)# app-policy white-list user_test addr_test

第20章 配置入侵防护策略

20.1 入侵防御策略概述

随着互联网的飞速发展，网络环境也变得越来越复杂，恶意攻击、木马、蠕虫病毒等混合威胁不断增大，单一的防护措施已经无能为力，企业需要对网络进行多层、深层的防护来有效保证其网络安全，而入侵防御系统则是提供深层防护体系的保障。

入侵防护事件库支持在线更新和手动更新。

20.2 配置入侵防御策略

20.2.1 配置入侵防护事件集

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	ips set SETNAME	添加入侵防护时间
步骤**3**	member event ID level （alert|info|notice|warninig） action (block_source|drop|drop_session|pass|reset) log (off|on) (enable|disable)	向入侵防护事件集添加防护事件。
步骤**4**	level （high|low|middle）	配置防护级别
步骤**5**	description LINE	添加事件集的描述

参数说明： member event ID level （alert\|info\|notice\|warninig） action (block_source\|drop\|drop_session\|pass\|reset) log (off\|on) (enable\|disable)

参数	说明	缺省配置
ID	事件ID	无
alert|info|notice|warninig	事件报警等级	无
block_source|drop|drop_session|pass|reset	事件动作	无
off|on	日志开关	无
enable|disable	策略匹配的目的IP	无

参数说明：level （high|low|middle）

参数	说明	缺省配置
high|low|middle	事件集防护级别	无

参数说明： description LINE

参数	说明	缺省配置
LINE	事件集描述	无

20.2.2 入侵防护策略

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	ips rule IDRULE_NAME(any|IF_IN)(any|IF_OUT)(any|SIP)(any|DIP)IPS_SET [log]	添加入侵防护规则

参数说明： ips rule IDRULE_NAME(any|IF_IN) (any|IF_OUT)(any|SIP)(any|DIP) IPS_SET [log]

参数	说明	缺省配置
ID	规则ID	无
RULE_NAME	规则名称	无
IF_IN|any	策略匹配的入接口	any
IF_OUT|any	策略匹配的出接口	any
SIP|any	策略匹配的源IP	any
DIP|any	策略匹配的目的IP	any
IPS_SET	入侵防护事件集名称	无
[log]	规则日志记录	无

20.2.3 设备联动

配置步骤：

步骤1	configure terminal	进入配置模式

步骤2	ips interaction IPPORTUSERPASSWORD	配置入侵防护设备联动

参数说明： ips interaction IPPORTUSERPASSWORD

参数	说明	缺省配置
IP	联动设备IP	无
PORT	联动设备端口	无
USER	联动设备用户名	无
PASSWORD	联动设备密码	无

20.2.4 日志合并

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	ips log_merge both|dst_ip|src_ip five_minute|one_minute|thirty_second	配置日志合并条件和合并间隔

参数说明：ips log_merge both|dst_ip|src_ip five_minutes|one_minutes|thirty_second

参数	说明	缺省配置
both|dst_ip|src_ip	合并条件为根据源/目的ip|目的ip|源ip	无
five_minutes|one_minutes|thirty_second	合并间隔为5min|1min|30s	无

20.3 配置案例

案例描述

配置入侵防护时间集并添加入侵防护策略。

配置步骤：

步骤1	进入congfig模式
	DCFW-1800#configure terminal
步骤2	添加入侵防护事件集

	DCFW-1800(config)# ips set ipstest DCFW-1800 (config-ips-set)# member event 91438af level warning action pass log on enable
步骤3	添加入侵防护策略
	DCFW-1800(config)#ips rule 1 ipsrule any any any any ipstest log

第21章 配置防病毒策略

21.1 防病毒策略概述

设备可以针对外网入口处，进行实时的病毒扫描，将外来病毒隔离在内网之外，实现工作站被动防御病毒之外的主动病毒防护，我们可以在诸如 HTTP、FTP、IMAP、POP3、SMTP 等应用协议时进行文件扫描。

21.2 配置防病毒策略

21.2.1 防病毒策略添加

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	av rule NAME(IF_IN|any)(IF_OUT|any)(SIP|any)（DIP|any） protocol （http|smtp|imap|ftp|pop3 ） action （log|prev）（enable|disable）	添加防病毒策略
步骤**3**	show av rule	查看防病毒策略

参数说明：av rule NAME (IF_IN\|any)(IF_OUT\|any)(SIP\|any)（DIP\|any） protocol （http\|smtp\|imap\|ftp\|pop3 ）action （log\|prev）（enable\|disable）

参数	说明	缺省配置
NAME	防病毒策略名称	无
IF_IN	策略匹配的入接口	无
IF_OUT	策略匹配的出接口	无
SIP	策略匹配的源IP	无
DIP	策略匹配的目的IP	无
http|smtp|imap|ftp|pop3	防病毒协议	无
log|prev	策略动作类型	无
enable|disable	启用禁用	无

21.2.2 防病毒策略修改

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	av rule NAMEmod (IF_IN|any)(IF_OUT|any)(SIP|any)（DIP|any） protocol （http|smtp|imap|ftp|pop3 ）action （log|prev）（enable|disable）	修改防病毒策略

参数说明：av rule NAME mode (IF_IN\|any)(IF_OUT\|any)(SIP\|any)（DIP\|any）protocol （http\|smtp\|imap\|ftp\|pop3 ）action （log\|prev）（enable\|disable）

参数	说明	缺省配置
NAME	防病毒策略名称	无
IF_IN	策略匹配的入接口	无
IF_OUT	策略匹配的出接口	无
SIP	策略匹配的源IP	无
DIP	策略匹配的目的IP	无
http|smtp|imap|ftp|pop3	防病毒协议	无
log|prev	策略动作类型	无
enable|disable	启用禁用	无

21.2.3 防病毒策略删除

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	no av rule NAME	删除防火墙策略

参数说明：no av rule NAME

参数	说明	缺省配置
< NAME >	防病毒策略名称	无

21.3 配置案例

案例描述

配置防病毒策略，入接口 ge0/0，出接口 ge0/1，协议 http，动作阻断。

配置步骤：

步骤1	进入congfig模式
	DCFW-1800#configure terminal
步骤2	添加防火墙策略并启用
	DCFW-1800(config)#av rule avtest any any any any protocol http action prev enable

第22章 协议管理

22.1 协议管理概述

基于协议的长连接管理功能用于设置特定数据流的超长保持时间，让数据流的会话连接保持时间不受全局老化时间限制。

22.2 配置协议管理

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	protocol manage NAME	添加协议管理
步骤3	protocol (UDP | TCP)	选择协议
步骤4	port <1-65535>	设置端口
步骤4	timeout <1-65535>	设置超时时间

22.3 配置案例

案例描述

配置防病毒策略，入接口 ge0/0，出接口 ge0/1，协议 http，动作阻断。

配置步骤：

步骤1	进入congfig模式
	DCFW-1800#configure terminal
步骤2	添加防火墙策略并启用
	DCFW-1800(config)#av rule avtest any any any any protocol http action prev enable

第23章 配置流量控制策略

23.1 流量管理概述

QoS 为英文 Quality of Service 缩写，即服务质量。简单地说，QoS 能够对穿过设备的数据包进行合理的排队，对其中特定的数据包赋以较高的优先级，从而加速传输的过程，以实现实时交互。

由于每种应用系统对网络的要求有所不同，这使得带宽本身并不能解决网络拥塞的问题。QoS 所追求的传输质量在于：数据包不仅要到达其欲传输的目的地址，而且要保证数据包的顺序性、完整性和实时性。通过 QoS，网络可以按照业务的类型或级别加以区分，并能够依次对各级别进行处理。并支持流量整形，让突发流量平滑转发。

23.2 配置流量管理

23.2.1 配置线路绑定接口

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	qos-profile line NAME	添加名称NAME的线路
步骤3	bind interface IF_NAME	把线路绑定到指定的接口上
步骤4	maxbandwidth egress KBPS	配置线路的出方向最大带宽
步骤5	maxbandwidth ingress KBPS	配置线路的入方向最大带宽
步骤6	limit (bath|egress|ingress)	配置线路生效的方向
步骤7	enable|disable	线路启用禁用
步骤7	clear qos-profile statistics	清除线路计数状态

参数说明：qos-profile line NAME

参数	说明	缺省配置
NAME	线路名称	无

参数说明：bind interface IF_NAME

参数	说明	缺省配置
IF_NAME	接口名称、区域名称	无

参数说明：maxbandwidth egress KBPS

参数	说明	缺省配置
KBPS	限制速率，单位kbps	无

23.2.2 配置通道关联线路

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	qos-profile channel C_NAME　parent L_NAME	添加通道名称C_NAME，关联线路L_NAME
步骤3	bandwidth (egress|ingress) KBPS	配置通道的出入保证带宽
步骤4	maxbandwidth (egress|ingress) KBPS	配置通道的出入最大带宽
步骤5	perip （egress|ingress） KBPS	配置每IP限速带宽
步骤6	priority（high+|high|high-|low+|low|low-|medium+|medium|medium-）	配置通道优先级
步骤7	match (address|application|service|user) NAME	通道匹配条件
步骤8	schedule SCHE	通道生效时间
步骤9	move （bottom|down|top|up）	移动通道
步骤10	clear qos-profile statistics	清除通道计数状态

参数说明：qos-profile channel C_NAME　parentL_NAME

参数	说明	缺省配置
C_NAME	通道名称	无
L_NAME	线路名称	

参数说明：bandwidth (egress\|ingress) KBPS

参数	说明	缺省配置
egress	出方向	无
ingress	入方向	无
KBPS	限制速率，单位kbps	1G

参数说明：match (address\|application\|service\|user) NAME

参数	说明	缺省配置
NAME	对象或对象组名称	无

参数说明：schedule SCHE

参数	说明	缺省配置
SCHE	时间对象或时间对象组名称	无

23.2.3 配置排除策略

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	qos-profile white-list ADDRESS USER	添加qos排除策略
步骤3	no qos-profile white-list ADDRESS USER	删除排除策略

参数说明：qos-profile white-list ADDRESS USER

参数	说明	缺省配置
ADDRESS	地址对象或地址对象组名称	无
USER	用户对象或用户对象组名称	

23.2.4 显示 qos 配置及限速状态

配置步骤：

步骤1	show qos-profile	查看qos配置
步骤2	show qos-profile statistics	查看qos计数状态

23.3 配置案例

案例描述

配置 ge0/1 接口入方向限速保证带宽 2Mbps、最大带宽 10Mbps。

配置步骤：

步骤1	进入congfig模式

	DCFW-1800#configure terminal
步骤2	添加线路
	DCFW-1800(config)#qos-profile line qostest DCFW-1800 (config-qos-qostest)#limit ingress DCFW-1800 (config-qos-qostest)#maxbandwidth ingress 1000000 DCFW-1800 (config-qos-qostest)#bind interface ge01
步骤3	添加通道
	DCFW-1800 (config)# qos-profile channel qoschannel parent qostest DCFW-1800 (config-qos-qoschannel)# bandwidth ingress 2000 DCFW-1800 (config-qos-qoschannel)#maxbandwidth ingress 10000 DCFW-1800 (config-qos-qoschannel)#schedule always DCFW-1800 (config-qos-qoschannel)#match user any DCFW-1800 (config-qos-qoschannel)#match application any DCFW-1800 (config-qos-qoschannel)#match service any DCFW-1800 (config-qos-qoschannel)#match address any

第24章 配置认证用户

24.1 认证用户设置概述

设备支持使用本地用户数据库、RADIUS 服务器、LDAP 服务器的用户认证。

1）可以把用户名添加到设备用户数据库中，然后为用户设置一个密码以允许用户使用这个内部数据库进行认证。

2）可以添加一个 RADIUS 服务器并且选择 RADIUS，以允许用户使用选定的 RADIUS 服务器进行认证。

3）可以添加一个 LDAP 服务器并且选择 LDAP，以允许用户使用选定的 LDAP 服务器进行认证。

您还可以禁用某些用户使他们无法通过设备进行认证。或者选择临时帐户，使用户在一定时间段内为合法帐户。

要启用认证，您必须在一个或者多个用户组中添加用户名，也可以把 RADIUS 服务器或 LDAP 服务器添加到用户组中。然后当您需要认证的时候，可以选择相应的用户组。

可以在以下操作中要求认证：

- 管理员身份认证
- 任何动作被设置为认证的用户策略（web 认证等）
- IPsecVPN

当一个用户输入用户名和密码时，设备在内部用户数据库上搜索匹配的用户名。如果这个用户名被设置成了禁用，那么这个用户就无法取得认证，连接将被放弃。如果这个用户设置了密码并且密码匹配，那么就允许连接。如果密码不匹配，连接同样会被放弃。

如果选择的是 RADIUS，而且配置了 RADIUS 支持，用户名和密码与 RADIUS 服务器中的用户名和密码相匹配，则允许连接。如果用户名和密码不同于 RADIUS 服务器中的用户名和密码，连接将被放弃。

如果选择的是 LDAP，而且配置了 LDAP 支持，用户名和密码与 LDAP 服务器中的用户名和密码相匹配，则允许连接。如果用户名和密码不同于 LDAP 服务器中的用户名和密码，连接将被放弃。

24.2 配置认证用户

设备用户按用户权限分为：

- 管理员用户：用户对设备管理员身份的认证与授权。
- 接入用户：用户防火墙策略，或 vpn 的用户接入认证。

按验证方式分为：

- 本地验证用户：本地用户数据库保存用户名和密码。

- RADIUS 验证管理员用户：本地只保存用户名，通过 RADIUS 服务器验证用户身份。
- RADIUS 验证用户：本地不保存用户名，通过 RADIUS 服务器验证用户身份。
- LDAP 验证管理员用户：本地只保存用户名，通过 LDAP 服务器验证用户身份。
- LDAP 验证用户：本地不保存用户名，通过 LDAP 服务器验证用户身份。

24.2.1 配置本地管理员用户

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	user administrator USER local PASSWORD authorized-table NAME [disable]	配置本地验证管理员用户： USER：用户名 PASSWORD：密码 NAME：权限表 disable：禁用该用户，默认enable
步骤3	user administrator test description DESC	DESC 用户的描述
步骤4	user administrator test authorized-address (first|second|third) (A.B.C.D/M | X:X::X:X/M)	配置用户的管理地址，可以配置三个
步骤5	user administrator USER (enable|disable)	禁用或者解禁该管理员
步骤6	show admin-user [USERNAME]	显示管理员的信息

使用 no user administrator USER authorized-address (first|second|third)删除用户的管理地址。

使用 no user administrator USER description 删除该管理员的描述。

使用 no user administrator USER 删除该管理员。

24.2.2 配置 RADIUS 管理员用户

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	user administrator USER radius SERVER authorized-table NAME [enable | disable]	配置radius验证管理员用户： USER：用户名 SERVER：Radius 服务器名称 NAME：权限表 disable：禁用该用户，默认enable

步骤3	user administrator USER (enable|disable)	禁用或者解禁该管理员
步骤4	show admin-user [USERNAME]	显示管理员的信息

24.2.3 配置 LDAP 管理员用户

配置步骤：

步骤1	DCFW-1800# con t	进入配置模式
步骤2	DCFW-1800(config)# user administrator adm1 ldap ldap1 authorized-table admin	配置ldap类型管理员用户
步骤3	DCFW-1800(config)#exit	回到enable模式

使用 no user administrator USER authorized-address (first|second|third)删除用户的管理地址。

使用 no user administrator USER description 删除该管理员的描述。

使用 no user administrator USER 删除该管理员。

24.2.4 配置本地接入用户

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	user-local USER enable authenticate authenticate local PASSWORD	配置本地验证接入用户，用户类型access为接入用户： USER：用户名 PASSWORD：密码 disable：禁用该用户，默认为enable
步骤3	Config模式： show user [USERNAME]	显示接入用户信息
步骤4	user-local USER enable bind bind ip address A.B.C.D 或者 bind ip address range A.B.C.D E.F.G.H	为用户绑定ip或ip段

使用 no bind ip address A.B.C.D 删除为用户绑定的 ip。

config 模式下使用 no user-local USER 删除用户。

24.3 配置RADIUS服务器支持

如果您配置了 RADIUS 支持，当管理员用户被配置为要求使用 RADIUS 服务器认证的时候，设备将连接 RADIUS 服务器以获得认证。

24.3.1 配置 RADIUS 服务器

配置步骤:

步骤1	configure terminal	进入全局配置模式
步骤2	radius-server NAME A.B.C.D SECRET[PORT]	NAME：radius服务器名称 A.B.C.D：radisu服务器ip地址SECRET：radisu服务器密码 PORT：可选，radisu服务器端口 默认为：1812
步骤3	show radius-server [SERVERNAME]	显示radius server信息

使用 no radius-server NAME 删除 radius 服务器。

24.4 配置LDAP服务器支持

如果您配置了 RADIUS 支持，当管理员用户被配置为要求使用 RADIUS 服务器认证的时候，设备将连接 RADIUS 服务器以获得认证。

24.4.1 配置 LDAP 服务器

配置步骤:

步骤1	DCFW-1800#configure terminal	进入配置模式
步骤2	DCFW-1800(config)# ldap ldap1	进入模板ldap1
步骤3	DCFW-1800(config-ldap)# ldap 192.168.31.32 389	配置ip 端口号
步骤4	DCFW-1800(config-ldap)# cnid cn	配置通用名id
步骤5	DCFW-1800(config-ldap)# dn dc=zte,dc=com	配置区别名
步骤6	DCFW-1800(config-ldap)# bindtype simple	配置绑定方式
步骤7	en	回到enable模式

使用 no ldap NAME 服务器模板名称可以删除模板。

enable 模式下：

使用 show ldapserver 可以查看 LDAP 服务器的配置信息。

24.5 配置portal server支持

24.5.1 配置 Portal Server

配置步骤:

步骤1	configure terminal	进入全局配置模式
步骤2	user-portal radiusSERVER_NAME	SERVER_ NAME：radius服务对象名称
步骤3	user-portal serverA.B.C.D	A.B.C.D：portal server的IP地址
步骤4	user-portal timeout<1-144000>	<1-144000>：用户认证后无流量超时时间
步骤5	user-portal-server portal-url URL	URL：重定向的用户认证页面

使用 no user-portal server 删除 portal server。

24.6 配置用户组

24.6.1 配置用户组

配置步骤:

步骤1	configure terminal	进入全局配置模式
步骤2	user-group NAME	NAME：用户组名称
步骤3	show usergroup [GROUPNAME]	显示用户组信息。

使用 no usergroup NAME 删除用户组。

注意：

show usergroup [GROUPNAME]命令中有一栏是 Refer_Count，表示用户组的引用计数，即有多少个策略引用该用户组。当用户组的引用计数大于 0 时，用户组不能被删除。

24.6.2 配置用户加入用户组

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	user-group GROUPNAME	USERNAME：用户名称
	member USERNAME	GROUPNAME：用户组名称

使用 no member USERNAME 将用户从用户组中删除（不会删除此用户）。

24.7 配置案例

24.7.1 配置案例 1：本地用户认证

案例描述

本地保存用户名和密码的认证用户通过设备用户认证后，访问外网资源。

配置步骤：

步骤1	配置前准备
	DCFW-1800_A(config)# interface ge0/0
	DCFW-1800_A(config- ge0/0)# ip address 200.0.0.1/24
	DCFW-1800_A(config- ge0/0)# exit
	DCFW-1800_A(config)# interface ge0/1
	DCFW-1800_A(config- ge0/1)# ip address 10.0.0.1/16
	DCFW-1800_A(config- ge0/1)# allow access https
	DCFW-1800_A(config- ge0/1)# allow access http
	DCFW-1800_A(config- ge0/1)# allow access webauth
	DCFW-1800_A(config- ge0/1)# exit
	DCFW-1800_A(config)# interface ge0/2
	DCFW-1800_A(config- ge0/2)# ip address 192.168.0.1/24
	DCFW-1800_A(config-ge)# exit
步骤2	配置超时时间
	DCFW-1800_A(config)# user-webauth keepalive-timeout 3600
步骤3	配置用户唯一性限制
	DCFW-1800_A(config)# user-webauth login-single mode forbid-new
步骤4	配置认证页面地址

	DCFW-1800_A(config)# user-webauth hello-url https://10.0.0.1:1443/
步骤5	配置用户组
	DCFW-1800_A(config)# user-local user1 DCFW-1800_A(config-user)#quit DCFW-1800_A(config)# user-group firewall DCFW-1800_A(config-group)# member user1
步骤6	配置安全策略
	DCFW-1800_A(config)# policy 1 ge0/0 ge0/1 any any any any any always permit DCFW-1800_A(config-policy)# user-policy any any any any always local-webauth DCFW-1800_A(config-policy)# end DCFW-1800_A#
步骤7	登陆用户认证的portal页面，进行用户认证。
	https://10.0.0.1:1443/
步骤8	访问外网资源

24.8 认证用户监控与维护

24.8.1 查看接入用户信息

查看接入用户信息：

步骤1	查看用户信息
	DCFW-1800_A# show user NAME

24.8.2 查看用户组信息

查看用户组信息:

步骤1	查看用户组信息
	DCFW-1800_A# show user-group NAME

24.8.3 查看 RADIUS 服务器信息

查看 RADIUS 服务器信息：

步骤1	查看RADIUS服务器信息
	DCFW-1800_A# show radius-server ras1

24.8.4 查看 LDAP 服务器信息

查看 RADIUS 服务器信息：

步骤1	查看LDAP服务器信息
	DCFW-1800_A# show ldapserver

24.8.5 查看用户验证和登陆的过程

应用环境

无论用户是本地用户、本地有用户名的 RADIUS/LDAP 验证用户、或者本地没有存放用户名的 RADIUS/LDAP 用户，用户登陆失败时。为了在终端显示该调试信息，需要执行命令 terminal monitor。

调试实例

```
DCFW-1800_A# debug aaa events
AAA: receive AAA request:
    Type = 4
    Usergroup : zte
    Username : test
    Password : 123456
    Address : 10.0.0.22
AAA: send AAA response:
    Type = 4
    Result : Failed
    Reason : Password wrong
```

结果分析

这时您需要确认：

- 用户密码是否正确。

注意：

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源，因此强烈建议用户，当调试结束时，一定要用 no debug aaa events 命令禁用此功能。

24.9 常见故障分析

24.9.1 故障现象 1：认证用户认证失败

现象	认证用户进行认证时失败。
分析	密码错误 用户已经禁用 本地不保存用户名的认证用户认证时所在的组没有加入RADIUS服务器或LDAP服务器。 RADIUS/LDAP服务器配置错误 RADIUS/LDAP服务器连接不上（比如：ping不通） RADIUS/LDAP服务器上没有这个用户 确定用户是否为临时帐户且已经过期。
解决	检查用户密码，输入正确的用户名和密码 解禁用户 为该用户认证时所在的组添加RADIUS服务器/LDAP服务器。 修改该RADIUS/LDAP服务器的配置 首先确保设备和RADIUS/LDAP服务器能通讯，能ping通 为该RADIUS//LDAP服务器添加该用户 重新设置用户的有效期。

第25章 配置防 DOS 攻击

25.1 防DOS攻击概述

作为一款设备产品，需要同时具备防止攻击和保证正常数据通过的功能。当设备遇到大量攻击时，如果所有的连接资源都被攻击所占用，则正常数据就无法通过设备。

防 DOS(Denial of Service)攻击设计的目标就是要使设备能够阻止外部的恶意攻击，同时还能使内网正常地与外界通信。不仅保护设备，更要保护内网。当遭受到攻击时，向用户进行报警提示。

常见的 DOS 攻击主要包括 ping-of-death、tear-drop、jolt2、syn-flag、land-base、winnuke、smurf 等。

25.2 配置防DOS攻击

25.2.1 缺省配置

内容	缺省设置	备注
防ping of death攻击	disable	可更改设置
防tear drop攻击	disable	可更改设置
防jolt2攻击	disable	可更改设置
防land-based攻击	disable	可更改设置
防winnuke攻击	disable	可更改设置
防syn flag攻击	disable	可更改设置
防smurf攻击	disable	可更改设置

25.2.2 配置防 ping-of-death 攻击功能

ping-of-death 攻击是通过向目的主机发送长度超过 65535 的 icmp 报文，使目的主机发生处理异常而崩溃。

配置了防 ping-of-death 攻击功能后，设备可以检测出 ping-of-death 攻击，丢弃攻击报文并输出告警日志信息。

配置步骤

步骤**1**	configure terminal	进入配置模式

步骤2	ip defend attack ping-of-death	打开防ping-of-death攻击

使用 no 命令可以关闭该功能。

25.2.3 配置防 tear-drop 攻击功能

tear-drop 攻击通过向目的主机发送报文偏移重叠的分片报文，使目的主机发生处理异常而崩溃。

配置了防 tear-drop 攻击功能后，设备可以检测出 tear-drop 攻击，并输出告警日志信息。因为正常报文传送也有可能出现报文重叠，因此设备不会丢弃该报文，而是采取裁减、重新组装报文的方式，发送出正常的报文。

配置步骤

步骤1	configure terminal	进入配置模式
步骤2	ip defend attack tear-drop	打开防tear-drop攻击

使用 no ip defend attack tear-drop 命令可以关闭该功能。

25.2.4 配置防 jolt2 攻击功能

jolt2 攻击通过向目的主机发送报文偏移加上报文长度超过 65535 的报文，使目的主机处理异常而崩溃。

配置了防 jolt2 攻击功能后，设备可以检测出 jolt2 攻击，丢弃攻击报文并输出告警日志信息。

配置步骤

步骤1	configure terminal	进入配置模式
步骤2	ip defend attack jolt2	打开防jolt2攻击

使用 no ip defend attack jolt2 命令可以关闭该功能。

25.2.5 配置防 land-base 攻击功能

land-base 攻击通过向目的主机发送目的地址和源地址相同的报文，使目的主机消耗大量的系统资源，从而造成系统崩溃或死机。

配置了防 land-base 攻击功能后，设备可以检测出 land-base 攻击，丢弃攻击报文并输出告警日志信息。

配置步骤

步骤1	configure terminal	进入配置模式
步骤2	ip defend attack land-base	打开防land-base攻击

使用 no ip defend land-base 命令可以关闭该功能。

25.2.6 配置防 winnuke 攻击功能

winnuke 攻击通过向目的主机的 139、138、137、113、53 端口发送 TCP 紧急标识位 urg 为 1 的带外数据报文，使系统处理异常而崩溃。

配置了防 winnuke 攻击功能后，设备可以检测出 winnuke 攻击报文，将报文中的 TCP 紧急标志位为 0 后转发报文，并可以输出告警日志信息。

配置步骤

步骤1	configure terminal	进入配置模式
步骤2	ip defend attack winnuke	打开防winnuke攻击

使用 no ip defend attack winnuke 命令可以关闭该功能。

25.2.7 配置防 syn-flag 攻击功能

syn-flag 攻击通过向目的主机发送错误的 tcp 标识组合报文，浪费目的主机资源。

配置了防 syn-flag 攻击功能后，设备可以检测出 syn-flag 攻击，丢弃攻击报文并输出告警日志信息。

配置步骤

步骤1	configure terminal	进入配置模式
步骤2	ip defend attack syn-flag	打开防syn-flag攻击

使用 no 命令可以关闭该功能。

25.2.8 配置防 smurf 攻击

Smurf 攻击结合使用了 IP 欺骗和 ICMP 回复方法使大量网络传输充斥目标系统，引起目标系统拒绝为正常系统进行服务。Smurf 攻击通过使用将回复地址设置成受害网络的广播地址的 ICMP 应答请求(ping)数据包，来淹没受害主机，最终导致该网络的所有主机都对此 ICMP 应答请求做出答复，导致网络阻塞。

设备的防 smurf 攻击可以检测出 smurf 攻击，可以有效地丢弃攻击保温并输出高精日志信息。

配置步骤

步骤**1**	configure terminal	进入配置模式
步骤**2**	ip defend attack smurf	打开防smurf攻击

使用 no ip defend smurf 命令可以关闭该功能。

25.2.9 配 Flood 防御

Flood 攻击，是众多 DOS 攻击形式的一种方式。又分为 SYN Flood、UDP Flood、ICMP Flood。

SYN Flood 利用 TCP 协议的缺陷，向服务器端发送大量伪造的 TCP 连接请求之后，自身不再做出应答，使得服务器端的资源迅速耗尽，从而无法及时处理其它正常的服务请求，严重的时候甚至会导致服务器系统的崩溃。

UDP Flood 利用大量 UDP 小包冲击 DNS 服务器或 Radius 认证服务器、流媒体视频服务器。100k pps 的 UDPFlood 经常将线路上的骨干设备例如防火墙打瘫，造成整个网段的瘫痪。由于 UDP 协议是一种无连接的服务，在 UDPFLOOD 攻击中，攻击者可发送大量伪造源 IP 地址的小 UDP 包。

ICMP Flood 是通过对其目标发送超过 65535 字节的数据包，就可以令目标主机瘫痪，如果大量发送就成了洪水攻击。

设备的防 Flood 攻击采用了业界最新的 syncookie 技术，在很少占用系统资源的情况下，可以有效地抵御 Flood 对受保护服务器的攻击。

Ipv4 flood 防御配置步骤

步骤**1**	configure terminal	进入配置模式
步骤**2**	ip defend flood startIp STARTIP endIp ENDIP tcp (enable|disable)THRESHOLD udp （enable|disable）THRESHOLD icmp （enable|disable）THRESHOLD dns （enable|disable）THRESHOLD	配置flood防护的服务器IP、防护类型及阈值。

配置中使用 disable 命令可以关闭对应的 flood 功能。

Ipv6 flood 防御配置步骤

步骤**1**	configure terminal	进入配置模式
步骤**2**	ipv6 defend flood startIp STARTIP endIp ENDIP tcp (enable|disable)THRESHOLD udp （enable|disable）THRESHOLD icmp （enable|disable）THRESHOLD dns （enable|disable）THRESHOLD	配置flood防护的服务器IP、防护类型及阈值。

配置中使用 disable 命令可以关闭对应的 flood 功能。

25.2.10 配置智能 TCP Flood 防御

智能 TCP Flood，即 SYN Flood 攻击，是众多 DOS 攻击形式的一种方式。SYN Flood 利用 TCP 协议的缺陷，向服务器端发送大量伪造的 TCP 连接请求之后，自身不再做出应答，使得服务器端的资源迅速耗尽，从而无法及时处理其它正常的服务请求，严重的时候甚至会导致服务器系统的崩溃。

设备的防 syn flood 攻击采用了业界最新的 syncookie 技术，在很少占用系统资源的情况下，可以有效地抵御 SYN Flood 对受保护服务器的攻击。

配置步骤

步骤1	configure terminal	进入配置模式
步骤2	ip defend syn-cookie<100-10000>	打开防syn flood攻击，抵御syn flood对受保护服务器的攻击

使用 no ip defend syn-cookie 命令可以关闭该功能。

25.3 防DOS攻击的监控与维护

25.3.1 查看配置信息

步骤1	Show ip defend attack
	DCFW-1800# show ip defend attack ip defend attack informations: ip defend attack ping-of-death:disable ip defend attack tear-drop:disable ip defend attack jolt2:disable ip defend attack land-base:disable ip defend attack winnuke:disable ip defend attack syn-flag:disable ip defend syn-cookie:disable syn-cookie threshold:100 syn-cookie state:not booted ip defend arp:enable arp threshold:300

	arp block-time:60

25.3.2 查看系统当前的 TCP 半连接数

步骤1	show ip inspect count
	DCFW-1800# show ip inspect count System: Connect sum count: 3 Halfopen connect count: 0 Halfopen connect rate count: 0 TCP: Connect sum count: 3 Halfopen connect count: 0 Halfopen connect rate count: 0 UDP: Connect sum count: 0 Halfopen connect count: 0 Halfopen connect rate count: 0 ICMP: Connect sum count: 0 Halfopen connect count: 0 Halfopen connect rate count: 0 Generic: Connect sum count: 0 Halfopen connect count: 0 Halfopen connect rate count: 0 观察TCP的Halfopen connect count数是否异常，当该值偏大时，建议开启防syn flood功能。

25.3.3 查看防 DOS 攻击的 debug 信息

步骤1	Debug ip defend attack
	DCFW-1800#debug ip defend attack 打开该命令时，系统会向控制台打印检测到的攻击信息。

25.4 常见故障分析

25.4.1 TCP Flood 攻击防御失效

现象	SYN Flood的攻击防御失效，SYN Flood报文穿过设备。
分析	SYN Flood攻击防御失效的原因可能有以下几个：防syn flood攻击的服务没有启动，攻击门限设置过高或者IP Inspect没有启动。
解决	查看系统中的TCP半连接数是否有显示，如果TCP半连接数为0，应该是IP Inspect模块没有启动； 防syn flood攻击服务是否启动，可以用show ip defend attack命令查看。如果未启动，启动防syn flood攻击服务。 3、查看攻击门限设置是否过高。如过高，可降低攻击门限。

第26章 配置防扫描

26.1 防扫描概述

扫描也是网络攻击的一种，攻击者在发起网络攻击之前，通常会试图确定目标上开放的TCP/UDP 端口，而一个开放的端口通常意味着某种应用。

常见的扫描主要有：

- 垂直（Vertical）扫描：针对相同主机的多个端口
- 水平（Horizontal）扫描：针对多个主机的相同端口
- ICMP (Ping) sweeps：针对某地址范围，通过 Ping 方式发现存活主机

设备可以有效防范以上几类扫描，从而阻止外部的恶意攻击，保护设备和内网。当检测到此类扫描探测时，向用户进行报警提示。

26.2 配置防扫描

26.2.1 缺省配置信息

设备关于防扫描的缺省设置信息如以下表格所示：

表26-1防扫描的缺省配置信息

内容	缺省设置	备注
防TCP Scan攻击	disable	可更改设置
防UDP Scan攻击	disable	可更改设置
防Ping sweep攻击	disable	可更改设置
扫描识别门限	1000	可更改设置
对源主机的阻断时间	20	可更改设置

26.2.2 配置防 TCP Scan

根据实际网络情况，当受到 tcp scan 扫描攻击时，可以配置防 tcp 扫描攻击。

当一个源 IP 地址在 1 秒内将含有 tcp Syn 片段的 IP 封包发送给位于相同目标 IP 地址的不同端口数量大于配置的门限值时，即认为其进行了端口扫描，系统将其标记为 tcp scan，并在配置的阻断时间内拒绝来自于该台源主机的所有其它 tcp Syn 包。

启用防 tcp scan 扫描攻击，可能会占用比较多的内存。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	ip defend scan tcp	配置防TCP Scan攻击
步骤3	end	返回特权模式
步骤4	show ip defend scan	显示防扫描配置

使用 no ip defend scan tcp 可以取消对防 TCP Scan 的设置，使其恢复到缺省配置。

26.2.3 配置防 UDP Scan

根据实际网络情况，当受到 udp scan 扫描攻击时，可以配置防 udp scan 扫描攻击。当一个源 IP 地址在 1 秒内将含有 udp 的 IP 封包发送给位于相同目标 IP 地址的不同端口数量大于配置的门限值时，即进行了一次端口扫描，系统将其标记为 udp scan，并在配置的阻断时间内拒绝来自于该台源主机的所有其它 udp 包。

启用防 UDP Scan 扫描攻击，可能会占用比较多的内存。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	ip defend scan udp	配置防UDP Scan攻击
步骤3	end	返回特权模式
步骤4	show ip defend scan	显示防扫描配置

使用 no ip defend scan udp 可以取消对防 UDP Scan 的设置，使其恢复到缺省配置。

26.2.4 配置防 Ping sweep

根据实际网络情况，当受到 Ping sweep 扫描攻击时，可以配置防 Ping sweep 扫描攻击。当一个源 IP 地址在 1 秒内发送给不同主机的 ICMP 封包超过门限值时，即进行了一次地址扫描。此方案的目的是将 ICMP 封包(通常是应答请求) 发送给各个主机，以期获得至少一个回复，从而查明目标地址。设备在内部记录从某一远程源地点发往不同地址的 ICMP 封包数目。当某个源 IP 被标记为地址扫描攻击，则系统在配置的阻断时间内拒绝来自该主机的其它更多 ICMP 封包。

启用防 Ping sweep 扫描攻击，可能会占用比较多的内存。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	ip defend scan ping-sweep	配置防Ping sweep攻击

步骤3	end	返回特权模式
步骤4	show ip defend scan	显示防扫描配置

使用 no ip defend scan Ping-sweep 可以取消对防 Ping sweep 的设置，使其恢复到缺省配置。

26.2.5 配置扫描识别门限

用 threshold 可以配置防扫描功能的扫描识别门限，超过门限值时，该源 IP 被标记为扫描攻击，来自于该台源主机的所有其它攻击包都被阻断。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	ip defend scan threshold <10-65535>	配置扫描识别门限
步骤3	end	返回特权模式
步骤4	show ip defend scan	显示防扫描配置

使用 no ip defend scan threshold 可以取消对扫描识别门限的设置，使其恢复到缺省配置。

26.2.6 配置对源主机的阻断时间

用 block-time 命令可以设置阻断时间，当系统检测到扫描攻击时，在配置的阻断时间内拒绝来自于该台源主机的所有其它攻击包。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	ip defend scan block-time<1-65535>	配置防扫描的阻断时间
步骤3	end	返回特权模式
步骤4	show ip defend scan	显示防扫描配置

使用 no ip defend scan block-time 可以取消对防扫描阻断时间的设置，使其恢复到缺省配置。

26.3 配置案例

26.3.1 配置防扫描

当网络上出现扫描攻击时，通过所收集的流信息我们可以看到当前设备上来自于某台主机的半连接信息，如果流信息中有大量源 ip，目的 ip 不变，而对应的目的端口变化的流，可以认为受到了扫描攻击，这时我们可以看一下是什么类型的扫描，然后通过配置对应的防扫描攻击以保护内网和设备。

配置步骤：

步骤1	查看网络数据分析结果，确定是否受到扫描攻击
	可以用NetFlow，或者通过主机抓包，确定是否受到扫描攻击。
步骤2	配置防tcp scan攻击以及攻击门限
	DCFW-1800_A(config)# ip defend scan tcp DCFW-1800_A(config)# ip defend scan threshold 1000 DCFW-1800_A(config)# end DCFW-1800_A #

配置结果：

!
ip defend scan tcp
ip defend scan threshold 1000
!

26.4 防扫描监控与维护

26.4.1 查看防扫描配置

介绍常用的 show 命令的使用

查看防扫描配置的步骤：

步骤1	查看启用的防扫描类型
	ip defend scan informations: ip defend scan tcp:enable ip defend scan udp:disable ip defend scan ping-sweep:disable ip defend scan block-time:20 ip defend scan threshold:1000 blocked source ip list:

	10.1.1.121 TCP 15 可以看到启用了防TCP Scan，没有启用防UDP Scan，没有启用防Ping sweep，对源主机的阻断时间为20秒，扫描识别门限设置为1000，即当一个源IP 地址在1秒内将含有tcp Syn 片段的IP 封包发送给位于相同目标IP地址的不同端口数量大于1000时，系统认为进行了端口扫描，阻断该IP继续发送的TCP包。 IP为10.1.1.121的源主机被阻断，扫描类型为TCP Scan，剩余阻断时间15秒。

26.5 常见故障分析

26.5.1 配置防扫描后没有报警，没有拒包

现象	通过抓包或流收集后，确定确实受到了扫描攻击，而此时设备没有报警，没有拒包。
分析	可能是以下几种情况导致： 扫描识别门限设置得太大，导致扫描计数还没有达到门限值。 同时配置了防扫描、防Syn Flood和会话管理中的TCP半连接数目限制，三者功能有重叠，可能导致防扫描功能未起作用
解决	检查配置，如果是因为门限值设置得太大，根据实际需求修改到合适的值。

第27章 配置 IP-MAC 绑定

27.1 IP-MAC绑定概述

Address Resolution Protocol (ARP)是寻找 IP 地址所对应的 MAC 地址的一种协议。

为什么需要寻找 IP 地址对应的 MAC 地址呢？我们知道，在以太网中，对于处于同一子网的两个通信实体来说，他们的一次 IP 通信过程大致如下：

当源端发送一个 IP 包之前，它必须知道目的端的以太网地址才可以完成封装，可是此时源端只能知道目的端的 IP 地址（通过用户的事先配置或者查路由表），这样就必须依靠 ARP 协议来完成目的端以太网地址的解析。因此源端发送一个包含目的 IP 地址的 ARP 请求，目的端收到后向源端返回 ARP 应答，通告自己的 MAC 地址，源端获得目的端 MAC 地址后才可以将 IP 包封装在以太网头中发送出去。

由于网络中可能存在一些攻击软件仿冒某台主机上网，逃过跟踪。为了避免这种情况，设备实现了 IP-MAC 绑定功能，把用户的 MAC 和 IP 绑定起来。配置了 IP-MAC 绑定后，通过设备的报文的 MAC 和 IP 必须严格一致，否则报文将被丢弃。

在实际应用时，通常来说是为指定 MAC 绑定指定 ip，即一个 MAC 可以有多个 ip，但是一个特定的 ip 只能被指定的 MAC 使用。

27.2 配置IP-MAC绑定

27.2.1 配置 IP-MAC 绑定

添加一项 IP-MAC 绑定，需要输入绑定名称、IP 地址、MAC 地址。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	ipmac NAME A.B.C.D FF-FF-FF-FF-FF-FF unique-ip	配置一条IP-MAC绑定，开启唯一性检查
步骤3	end	返回特权模式
步骤4	show ip defend scan	显示防扫描配置

config 模式下使用 no ipmac NAME 清除一条绑定项。

27.2.2 查看 ARP 列表

步骤1	show arp	显示当前ARP列表

27.2.3 清除 ARP 列表

步骤1	clear arp	清除ARP列表

27.3 配置案例

案例描述

把张三的主机 192.168.31.118 和 00-16-41-59-3E-AF 绑定起来，并且是唯一性的。

配置步骤：

步骤1	添加IP-MAC绑定
	configure terminal ipmac NAME192.168.31.118 00-16-41-59-3E-AF unique-ip

第28章 配置 PKI

28.1 PKI协议概述

PKI（公钥基础设施）技术采用证书管理公钥，通过第三方的可信任机构--认证中心CA(Certificate Authority)，把用户的公钥和用户的其他标识信息（如名称、e-mail、身份证号等）捆绑在一起，在 Internet 网上验证用户的身份。目前，通用的办法是采用建立在 PKI 基础之上的数字证书，通过把要传输的数字信息进行加密和签名，保证信息传输的机密性、真实性、完整性和不可否认性，从而保证信息的安全传输。

设备上的 PKI 本地证书功能是：当设备作为 PKI 客户端时，选择本地证书作为本设备的身份标识，并且验证从其他主机接收到的证书的合法性。这相当于 IE 浏览器中的证书项功能。主要包含三项配置：导入用户证书、导入第三方 CA 证书、导入第三方 CA 的 CRL。这三个功能是相对独立又相互联系，即可以根据具体需要，导入不同的本地证书、不同的 CA 证书、不同的 CRL，但要验证某个终端证书时，需要导入该终端证书的 CA 证书、CRL，以便对该终端证书进行验证。

28.2 配置PKI

对设备所要使用的客户端证书、第三方 CA 证书、第三方 CRL 进行导入导出配置，并且可以生成一个证书请求，向第三方 CA 申请签发。

28.2.1 本地证书的导出

配置本地证书的导出。本地证书根据状态分为两种：本地生成的证书请求和本地证书。导出本地生成的证书请求导出的是证书请求文件；本地证书导出的证书文件。本地证书根据存放位置又分为两种：本地存放和 KEY。两种证书都能导出。

配置步骤：

步骤**1**	由1.2.1所示命令进入PKI配置节点	进入PKI配置模式
步骤**2**	certificate local export tftp A.B.C.D CERTIFICATE_NAME	

参数说明：certificate local export tftp A.B.C.D CERTIFICATE_NAME

参数	说明	缺省配置
A.B.C.D	Tftp服务器地址	无
CERTIFICATE_NAME	证书名称	无

28.2.2 本地生成证书请求的证书导入

通过设备的证书请求生成的证书请求文件，经 CA 签名后，再导入设备。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	certificate local cert_key|cert_chain import tftp A.B.C.D CERTIFICATE_NAME	本地生成的证书请求经CA签名后的证书导入。
步骤3	show certificate local [CERTIFICATE_NAME]	显示证书信息

使用 no certificate local CERTIFICATE_NAME，删除由 CERTIFICATE_NAME 指定的证书。

参数说明：certificate local cert_key import tftp A.B.C.D CERTIFICATE_NAME

参数	说明	缺省配置
A.B.C.D	Tftp服务器地址。	无
CERTIFICATE_NAME	证书名称。	无

28.2.3 PKCS12 格式证书的导入

导入 PKCS12 格式的证书。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	certificate local pkcs12 import (local|usb) tftp A.B.C.D CERTIFICATE_NAME [PASSWORD]	导入PKCS12格式的证书。
步骤3	show certificate local [CERTIFICATE_NAME]	显示证书信息

使用 no certificate local CERTIFICATE_NAME，删除由 CERTIFICATE_NAME 指定的证书。

参数说明：certificate local pkcs12 import (local\|usb) tftp A.B.C.D CERTIFICATE_NAME [PASSWORD]

参数	说明	缺省配置
(local|usb)	证书存入的位置：local表示存放在设备	无

	中；usb表示证书存入USBKEY。	
A.B.C.D	Tftp服务器地址	无
CERTIFICATE_NAME	证书名称	无
PASSWORD	加密PKCS12文件的密钥	无

28.2.4 证书私钥文件的导入

证书和私钥文件的导入。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	certificate local cert_key import (local|usb) tftp A.B.C.D CERTIFICATE_NAME KEYFILE_NAME [PASSWORD]	导入证书和私钥文件。
步骤3	show certificate local [CERTIFICATE_NAME]	显示证书信息

使用 no certificate local CERTIFICATE_NAME，删除由 CERTIFICATE_NAME 指定的证书。

参数说明：certificate local cert_key import (local\|usb) tftp A.B.C.D CERTIFICATE_NAME KEYFILE_NAME [PASSWORD]

参数	说明	缺省配置
(local|usb)	证书存入的位置：local表示存放在设备中；usb表示证书存入USBKEY。	无
A.B.C.D	Tftp服务器地址	无
CERTIFICATE_NAME	证书文件名	无
KEYFILE_NAME	私钥文件名	无
PASSWORD	加密私钥文件的密钥	无

28.2.5 CA 证书的导出

CA 证书的导出。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	certificatecaexport tftp A.B.C.D CERTIFICATE_NAME	导出CA证书
步骤**3**	show certificate ca [CERTIFICATE_NAME]	显示证书信息

参数说明：certificate caexport tftp A.B.C.D CERTIFICATE_NAME

参数	说明	缺省配置
A.B.C.D	Tftp服务地址	无
CERTIFICATE_NAME	CA证书名称	无

28.2.6 CA 证书的导入

导入 CA 证书，作为验证从其他终端接收过来的用户证书进行签名验证的依据，该导入的 CA 证书是作为可信证书使用的，必须要保证该 CA 证书的安全性。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	certificate ca ca import tftp A.B.C.D CERTIFICATE_NAME	导入CA证书。
步骤**3**	show certificate ca [CERTIFICATE_NAME]	显示证书信息

使用 no certificateca CERTIFICATE_NAME 删除由 CERTIFICATE_NAME 指定的 CA 证书。

参数说明：certificate caimport tftp A.B.C.D CERTIFICATE_NAME

参数	说明	缺省配置
A.B.C.D	Tftp服务器地址	无
CERTIFICATE_NAME	证书文件名称	无

28.2.7 CRL 的导出

导出 CRL。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	certificate crlexport tftp A.B.C.D CERTIFICATE_NAME	导出CRL。
步骤**3**	show certificate crl [CERTIFICATE_NAME]	显示CRL信息

使用 no certificate crl CERTIFICATE_NAME 删除由 CERTIFICATE_NAME 指定的 CRL。

参数说明：certificate crlexport tftp A.B.C.D CERTIFICATE_NAME

参数	说明	缺省配置
A.B.C.D	Tftp服务器地址	无
CERTIFICATE_NAME	CRL名称	无

28.2.8 CRL 导入

导入第三方 CA 的 CRL，在对从其他终端接收过来的证书进行验证时，要查找导入的 CRL，从而确定该终端用户证书是否被撤销。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	certificate crlimport tftp A.B.C.D CERTIFICATE_NAME	
步骤**3**	show certificate crl [CERTIFICATE_NAME]	显示CRL信息

使用 nocertificate crl CERTIFICATE_NAME 删除由 CERTIFICATE_NAME 指定的 CRL。

参数说明：certificate crlimport tftp A.B.C.D CERTIFICATE_NAME

参数	说明	缺省配置
A.B.C.D	Tftp服务器地址	无
CERTIFICATE_NAME	CRL文件名称	无

第29章 配置 PKI CA

29.1 PKI协议概述

CA 即证书管理机构，受委托发放数字证书的第三方组织或公司。数字证书是用来建立数字签名和公-私(public-private)密钥对的。CA 在这个过程中所起的作用就是保证获得这一独特证书的人就是被授权者本人。在数据安全和电子商务中，CA 是一个非常重要的组成部分，因为它们确保信息交换各方的身份。

CA 中心提供管理 CA 证书、签发并管理用户证书、管理 CRL 三大功能。在使用时，首先生成 CA 证书（颁发机构证书），并用该 CA 证书的私钥来为用户证书签名。用户证书可以根据用户的信息（如国家、地区、单位等）生成一个用户证书请求，然后对此请求进行签发，生成一个具有公私钥对的证书，颁发给具体用户，作为该用户的身份标识使用。对有些已经不安全的用户证书可以进行撤销操作，并根据撤销理由生成 CRL，将 CRL 颁发给用户，来作为验证证书是否安全有效的一个依据。

CA 中心的主要用途在于：签发用户证书、签发 CRL，在签发用户证书与 CRL 前，首先要确定 CA 根证书。

29.2 配置PKI CA

配置设备 CA 中心，主要包括配置管理 CA 证书、配置管理用户证书、配置管理 CRL 三个方面。需要注意的是，用户证书与 CRL 都是由 CA 证书（根证书）来签发，因此确定好 CA 证书后，如果没有安全因患（如 CA 私钥泄露）不要轻易改变 CA 证书。

29.2.1 生成 CA 证书

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	ca ca cacert new CERTIFICATE_NAME	配置CA证书请求。
步骤3	show ca ca cacert	显示CA证书信息

参数说明：

参数	说明	缺省配置
CERTIFICATE_NAME	证书请求名称	无

29.2.2 配置证书请求信息－位置

配置证书请求的可选信息－位置（城市）。

配置步骤：

步骤**1**	由1.2.1所示命令进入PKI CA配置节点	进入PKI CA配置模式
步骤**2**	city CITY_NAME	配置位置（城市）

参数说明：city CITY_NAME

参数	说明	缺省配置
CITY_NAME	位置（城市）名称	无

29.2.3 配置证书请求信息－国家或地区

配置证书请求可选信息－国家或地区，使用 GB。

配置步骤：

步骤**1**	由1.2.1所示命令进入PKI CA配置节点	进入PKI CA配置模式
步骤**2**	country COUNTRY_NAME	配置国家代码

参数说明：country COUNTRY_NAME

参数	说明	缺省配置
COUNTRY_NAME	国家或地区名称的两位代码。	

29.2.4 配置证书请求信息－组织

配置运行 PKI 的接口以及其所属的区域。

配置步骤：

步骤**1**	由1.2.1所示命令进入PKI CA配置节点	进入PKI CA配置模式
步骤**2**	organization ORGANIZATION_NAME	配置证书请求信息组织名称。

参数说明：organization ORGANIZATION_NAME

参数	说明	缺省配置
ORGANIZATION_NAME	组织名称	无

29.2.5 配置证书请求信息－州/省

配置证书请求信息－州/省。

配置步骤：

步骤1	由1.2.1所示命令进入PKI CA配置节点	进入PKI CA配置模式
步骤2	state STATE_NAME	配置证书请求信息－州/省

参数说明：state STATE_NAME

参数	说明	缺省配置
STATE_NAME	州/省名称	无

29.2.6 配置证书请求信息－部门

配置证书请求信息－部门。

配置步骤：

步骤1	由1.2.1所示命令进入PKI CA配置节点	进入PKI CA配置模式
步骤2	unit UNIT_NAME	配置证书请求信息－部门

参数说明：unit UNIT_NAME

参数	说明	缺省配置
UNIT_NAME	部门名称。	

29.2.7 配置证书请求信息－EMAIL

配置证书请求信息－EMAIL。

配置步骤：

步骤1	由1.2.1所示命令进入PKI CA配置节点	进入PKI CA配置模式
步骤2	email EMAIL	启用PKI功能并进入PKI配置模式

参数说明：email EMAIL

参数	说明	缺省配置
EMAIL	EMAIL地址	无

29.2.8 配置证书请求信息－密钥长度

配置证书请求信息－密钥长度。

配置步骤：

步骤1	由1.2.1所示命令进入PKI CA配置节点	进入PKI CA配置模式
步骤2	keylength KEY_LENGTH	启用PKI功能并进入PKI配置模式

参数说明：keylength KEY_LENGTH

参数	说明	缺省配置
KEY_LENGTH	密钥长度	无

29.2.9 配置证书请求信息－有效期

配置证书请求信息－有效期。

配置步骤：

步骤1	由1.2.1所示命令进入PKI CA配置节点	进入PKI CA配置模式
步骤2	days DAYS	启用PKI功能并进入PKI配置模式

参数说明：days DAYS

参数	说明	缺省配置
DAYS	有效期天数	365

29.2.10 CA 证书的导出

导出 CA 证书也分为两种格式，一种是 pem 格式，单导出 CA 证书文件。另一种是 pkcs12 格式文件，是将证书与密钥打包在一起导出。需要注意的是，导出 CA 证书为 pkcs12 格式时，会将 CA 私钥一同导出，仅做对 CA 证书的备份功能使用，不能给用户使用。给用户使用的 CA 证书要导出为 PEM 格式。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	ca ca cacert export tftp A.B.C.D (pem|p12) [PASSWORD]	

参数说明： ca ca cacert export tftp A.B.C.D (pem|p12) [PASSWORD]

参数	说明	缺省配置
A.B.C.D	Tftp服务器地址	无
(pem|p12)	导出ca证书的格式	
PASSWORD	导出为p12格式时的密码	

29.2.11 CA 证书导入

导入 CA 证书功能，可以将上级 CA 所颁发的证书导入到设备中去，使设备的 CA 中心作为一个子 CA 来管理用户证书与 CRL。导入 CA 证书分为两种格式：一种是 CA 证书与 CA 私钥打包在一起的 pkcs12 格式的文件；一种是 CA 证书与私钥分开存储，都为 PEM 格式的证书。

从第三方 CA 签发的证书导入 pkcs12 格式：

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	ca ca cacert import pkcs12 tftp A.B.C.D CERTIFICATE_NAME [PASSWORD]	导入第三方CA所签发的pkcs12格式证书，包含了CA私钥
步骤**3**	show ca ca cacert	显示证书信息

参数说明： ca ca cacert import pkcs12 tftp A.B.C.D CERTIFICATE_NAME [PASSWORD]

参数	说明	缺省配置
A.B.C.D	Tftp服务器地址。	无
CERTIFICATE_NAME	证书名称。	无
PASSWORD	Pkcs12格式文件的密码	

从第三方 CA 签发的证书导入 pem 格式：

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	ca ca cacert import pem tftp A.B.C.D CERTIFICATE_NAME KEYFILE_NAME [PASSWORD]	导入第三方CA所签发的pem格式证书，证书文件与私钥文件分开
步骤**3**	show ca ca cacert	显示证书信息

参数说明： ca ca cacert import pem tftp A.B.C.D CERTIFICATE_NAME KEYFILE_NAME [PASSWORD]

参数	说明	缺省配置
A.B.C.D	Tftp服务器地址。	无
CERTIFICATE_NAME	证书名称。	无
KEYFILE_NAME	密钥名称	
PASSWORD	密钥文件的密码	

29.2.12 CRL 的更新

在当前时间更新 CRL 撤销证书列表，会将自上次创建 CRL 后所撤销的证书的序列号、撤销原因更新到 CRL 列表中。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	ca ca crl update	更新CRL

29.2.13 CRL 的导出

导出 CRL 文件，提供给 CA 的用户使用，判断所要验证证书是否已经被撤销。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	ca ca crl export tftp A.B.C.D	导出CRL

参数说明： ca ca crl export tftp A.B.C.D

参数	说明	缺省配置
A.B.C.D	Tftp服务地址	无

29.2.14 生成用户证书请求信息

在创建用户证书时，首先要创建一个用户证书请求（生成请求文件及公私密钥对），然后用 CA 证书对该用户请求签发，生成一个用户可用的证书。生成证书后，可以对证书进行撤销、删除、导出、查看操作。

生成的用户证书时要对其进行签名，签名所用的为 CA 私钥，因此在签发用户证书时，一定要确保 CA 证书与私钥已经存在。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	ca ca sign NAME days DAYS password PASSWORD	签发用户证书
步骤**3**	show certificate NAME	显示用户证书信息

参数说明：ca ca sign NAME days DAYS password PASSWORD

参数	说明	缺省配置
NAME	已经生成的请求的名字	无
DAYS	有效期天数	无
PASSWORD	打包成pkcs12文件的密码	

29.2.15 签发用户证书请求

在创建用户证书时，首先要创建一个用户证书请求（生成请求文件及公私密钥对），然后用 CA 证书对该用户请求签发，生成一个用户可用的证书。生成证书后，可以对证书进行撤销、删除、导出、查看操作。

生成的用户证书时要对其进行签名，签名所用的为 CA 私钥，因此在签发用户证书时，一定要确保 CA 证书与私钥已经存在。

配置步骤：

步骤**1**	configure terminal	进入配置模式

步骤2	ca ca sign NAME days DAYS password PASSWORD	签发用户证书
步骤3	show certificate NAME	显示用户证书信息

参数说明： Ca ca sign NAME days DAYS password PASSWORD

参数	说明	缺省配置
NAME	已经生成的请求的名字	无
DAYS	有效期天数	无
PASSWORD	打包成pkcs12文件的密码	

29.2.16 导出用户证书

导出用户证书，可以将导出的用户证书拷贝到用户终端，作为用户的身份标识。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	ca ca certificate export tftp A.B.C.D CERTIFICATE_NAME	

参数说明： ca ca certificate export tftp A.B.C.D CERTIFICATE_NAME

参数	说明	缺省配置
A.B.C.D	Tftp服务器地址	无
CERTIFICATE_NAME	用户证书名称	无

29.3 常见故障分析

现象	导入CA证书时，提示导入证书错误
分析	导致这种错误提示的原因是：证书密码错误、证书公私钥不配对
解决	输入证书的正确密码，并保证所导入证书的公私钥配对性

第30章 配置高可用性（HA）

30.1 HA概述

HA(High Availability)即高可用性，可防止网络中由于单个设备故障或网络故障导致网络中断，保证网络服务的连续性和安全强度。

两台设备组成一个 HA 冗余组，在启动 HA 后，设备自动根据选举算法协商出主设备和备设备。主设备负责进行报文转发、ARP 应答，并实时向备设备同步状态和配置信息。备设备只被动接受主设备的同步信息，不进行业务处理。

目前设备，可通过心跳信号丢失、链路断开等方式进行 HA 切换。

30.2 配置HA

30.2.1 HA 配置

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	ha-group	进入到ha配置模式
步骤3	enable （backup-master|master-master）	配置抢占模式，主备模式、主主模式
步骤4	primary-failoverself L_ADDRESS peer P_ADDRESS	配置首选通信地址
步骤5	second-failoverself L_ADDRESS peer P_ADDRESS	配置备选通信地址
步骤6	unitID UNIT_ID	配置单元ID
步骤7	ha-time TIME	配置心跳间隔
步骤8	grob-style （master|backup|diable）	配置抢占模式，抢占主、抢占备、不抢占
步骤9	swap	ha交换

参数说明：primary-failoverself L_ADDRESS peer P_ADDRESS

参数	说明	缺省配置
L_ADDRESS	本地接口IP	无
P_ADDRESS	同步对端IP	无

参数说明：unitID UNIT_ID

参数	说明	缺省配置
UNIT_ID	单元ID，范围1-2	无

参数说明：ha-time TIME

参数	说明	缺省配置
TIME	心跳间隔时间，范围1-3	无

30.2.2 配置同步配置

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	ha-group	进入到ha配置模式
步骤3	config-sync self L_ADDRESS peer P_ADDRESS	配置同步配置
步骤4	config detect	开启实时检测同步状态
步骤5	web-sync	开启WEB配置自动同步功能

参数说明：config-sync self L_ADDRESS peer P_ADDRESS

参数	说明	缺省配置
L_ADDRESS	本地接口IP	无
P_ADDRESS	同步对端IP	无

30.2.3 连接同步配置

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	ha-group	进入到ha配置模式
步骤3	sync connection	连接同步配置
步骤4	mirroring-address self L_ADDRESS peer P_ADDRESS	配置连接同步的首选通信地址
步骤5	mirroring-address self L_ADDRESS peer P_ADDRESS	配置连接同步的备选通信地址

参数说明：mirroring-address self L_ADDRESS peer P_ADDRESS

参数	说明	缺省配置
L_ADDRESS	本地接口IP	无
P_ADDRESS	同步对端IP	无

30.2.4 接口联动配置

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	interface sync-groupNAME	新建接口联动组
步骤3	exit	退出组
步骤4	interface IF_NAME	需要加入接口联动组的成员
步骤5	sync-group-member NAME	加入接口联动

30.2.5 配置故障检测

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	ha-group	进入到ha配置模式
步骤3	sysmon-interface IF_NAME timeout TIME	配置接口监控
步骤4	sysmon-trunk TRUNK_NAMEthreshold ACTIVE_MEMBER	配置连狙聚合监控
步骤5	sysmon-hm HM_NAME	配置健康检查监控

参数说明：sysmon-interface IF_NAME timeout TIME

参数	说明	缺省配置
IF_NAME	监控的接口	无
TIME	超时时间	无

参数说明：sysmon-trunk TRUNK_NAMEthreshold ACTIVE_MEMBER

参数	说明	缺省配置
TRUNK_NAME	聚合接口	无
ACTIVE_MEMBER	接口成员个数	无

参数说明：sysmon-hm HM_NAME

参数	说明	缺省配置
HM_NAME	健康检查对象或健康检查对象组	无

30.3 配置案例

案例描述

配置 ha 配置同步，本地地址 2.1.1.1，对端地址 2.1.1.2

配置步骤：

步骤1	进入congfig模式
	DCFW-1800#configure terminal
步骤2	配置HA配置
	DCFW-1800(config)# ha-group DCFW-1800 (ha-group)# enable backup-master DCFW-1800 (ha-group)# ha-time 3 DCFW-1800 (ha-group)# grob-style master DCFW-1800 (ha-group)# unitID 2 DCFW-1800 (ha-group)# primary-failover self 2.1.1.1 peer 2.1.1.2
步骤3	配置ha的配置同步
	DCFW-1800 (ha-group)# config detect DCFW-1800 (ha-group)# config-sync self 2.1.1.1 peer 2.1.1.2

第31章 配置 VRRP

31.1 VRRP概述

通常，同一网段内的所有主机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。

缺省路由为用户的配置操作提供了方便，但是对缺省网关设备提出了很高的稳定性要求。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（Virtual Router Redundancy Protocol，虚拟路由器冗余协议）将可以承担网关功能的路由器加入到备份组中，形成一台虚拟路由器，由 VRRP 的选举机制决定哪台路由器承担转发任务，局域网内的主机只需将虚拟路由器配置为缺省网关。

VRRP 是一种容错协议，在提高可靠性的同时，简化了主机的配置。在具有多播或广播能力的局域网（如以太网）中，借助 VRRP 能在某台设备出现故障时仍然提供高可靠的缺省链路，有效避免单一链路发生故障后网络中断的问题，而无需修改动态路由协议、路由发现协议等配置信息。

31.2 配置VRRP

11.2.1 设置 VRRP 备份组的描述

设置一个 VRRP 备份组的描述信息。

配置步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	interface ge0/0	进入接口配置模式
步骤**3**	vrrp 1 descriptiondescription	找到或创建组号为1的虚拟路由器，并设置描述信息

参数说明：

参数	说明	缺省配置
Group numbers	备份组号	无
description	描述信息	无

11.2.2 取消 VRRP 备份组的描述

将一个 VRRP 备份组的描述清空。

配置步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	interface ge0/0	进入接口配置模式
步骤**3**	no vrrp 1 description	找到组号为1的虚拟路由器，取消描述

参数说明：

参数	说明	缺省配置
vrid	备份组号	无

11.2.3 向 VRRP 备份组增加一个虚拟 IP

增加一个虚拟 IP 到 VRRP 备份组。

配置步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	interface ge0/0	进入接口配置模式
步骤**3**	vrrp 1 ip 192.168.31.1	找到或创建组号为1的虚拟路由器，将一个虚拟IP增加到备份组

参数说明：

参数	说明	缺省配置
Group numbers	备份组号	无
ip	虚拟IP地址	无

注意：

虚拟 IP 地址不能为全零地址(0.0.0.0)、广播地址(255.255.255.255)、环回地址、非 A/B/C 类地址和其它非法 IP 地址(如 0.0.0.1)。

11.2.4 从 VRRP 备份组删除一个虚拟 IP

删除一个备份组的虚拟 IP。

配置步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	interface ge0/0	进入接口配置模式
步骤**3**	no vrrp 1 ip 192.168.31.1	找到组号为1的虚拟路由器，删除一个ip

参数说明：

参数	说明	缺省配置
vrid	备份组号	无
ip	虚拟IP地址	无

11.2.5 设置 VRRP 备份组的优先级

设置一个 VRRP 备份组的优先级。

配置步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	interface ge0/0	进入接口配置模式
步骤**3**	vrrp 1 priority120	找到或创建组号为1的虚拟路由器，并设置优先级

参数说明：

参数	说明	缺省配置
vrid	备份组号	无
priority	优先级	100

11.2.6 恢复 VRRP 备份组的缺省优先级

恢复一个 VRRP 备份组的缺省优先级 100。

配置步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	interface ge0/0	进入接口配置模式
步骤**3**	no vrrp 1 priority	找到组号为1的虚拟路由器，并恢复优先级为100

参数说明：

参数	说明	缺省配置
vrid	备份组号	无

11.2.7 启用 VRRP 备份组的抢占模式

启用一个 VRRP 备份组的抢占模式。

配置步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	interface ge0/0	进入接口配置模式

步骤3	vrrp 1 preemptdelay 10	找到或创建组号为1的虚拟路由器，启用抢占模式并把延迟设置为10秒

参数说明：

参数	说明	缺省配置
vrid	备份组号	无
preemptdelay	抢占延迟	0

11.2.8 禁用 VRRP 备份组的抢占模式

禁用一个 VRRP 备份组的抢占模式。

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	no vrrp 1 preempt	找到为1的虚拟路由器，禁用抢占

参数说明：

参数	说明	缺省配置
vrid	备份组号	无

11.2.9 设置 VRRP 备份组的版本模式

设置一个 VRRP 备份组的版本模式。

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	vrrp 1 version v3	找到或创建组号为1的虚拟路由器，并设置版本模式

参数说明：

参数	说明	缺省配置
vrid	备份组号	无
version	版本模式	v2

11.2.10 恢复 VRRP 备份组的缺省版本模式

恢复一个 VRRP 备份组的缺省版本模式。

配置步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	interface ge0/0	进入接口配置模式
步骤**3**	no vrrp 1 version	找到组号为1的虚拟路由器，恢复版本呢模式为v2

参数说明：

参数	说明	缺省配置
vrid	备份组号	无

11.2.11 设置 VRRP 备份组的认证模式

设置一个 VRRP 备份组的认证模式。

配置步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	interface ge0/0	进入接口配置模式
步骤**3**	vrrp 1 authentication md5 KEY	找到或创建组号为1的虚拟路由器，并设置md5认证模式和认证字

参数说明：

参数	说明	缺省配置
vrid	备份组号	无
authentication	认证模式	无

18.2.12 取消 VRRP 备份组的认证

取消一个 VRRP 备份组的认证。

配置步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	interface ge0/0	进入接口配置模式
步骤**3**	no vrrp 1 authentication	找到组号为1的虚拟路由器，并取消认证

参数说明：

参数	说明	缺省配置
vrid	备份组号	无

11.2.13 设置 VRRP 备份组的通告时间间隔

设置一个 VRRP 备份组的通告时间间隔。

配置步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	interface ge0/0	进入接口配置模式
步骤**3**	vrrp 1 timers advertise 200	找到或创建组号为1的虚拟路由器，并设置通告时间间隔

参数说明：

参数	说明	缺省配置
vrid	备份组号	无
timers advertise	通告时间间隔	100

11.2.14 恢复 VRRP 备份组的缺省通告时间间隔

恢复一个 VRRP 备份组的通告时间间隔。

配置步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	interface ge0/0	进入接口配置模式
步骤**3**	no vrrp 1 timers advertise	找到组号为1的虚拟路由器，并恢复通告时间间隔为100

参数说明：

参数	说明	缺省配置
vrid	备份组号	无

11.2.15 启用 VRRP 备份组的虚拟 IP 可 Ping

启用一个 VRRP 备份组的虚拟 IP 可 Ping。

配置步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	interface ge0/0	进入接口配置模式
步骤**3**	vrrp 1 ping	找到或创建组号为1的虚拟路由器，并启用Ping

参数说明：

参数	说明	缺省配置
vrid	备份组号	无

11.2.16 禁用 VRRP 备份组的虚拟 IP 可 Ping

禁用一个 VRRP 备份组的虚拟 IP 可 Ping。

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	no vrrp 1 ping	找到组号为1的虚拟路由器，并禁用Ping

参数说明：

参数	说明	缺省配置
vrid	备份组号	无

11.2.17 启用 VRRP 备份组

启用一个 VRRP 备份组。

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	vrrp 1 enable	找到组号为1的虚拟路由器，并启用

参数说明：

参数	说明	缺省配置
vrid	备份组号	无

11.2.18 禁用 VRRP 备份组

禁用一个 VRRP 备份组。

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	no vrrp 1 enable	找到组号为1的虚拟路由器，并禁用

参数说明：

参数	说明	缺省配置
vrid	备份组号	无

31.3 配置案例

案例描述

在接口 ge0/0 下，建立一个组号为 1，虚拟 IP 为 192.168.31.1，简单字符串认证，通告时间间隔为 2 秒的备份组。

配置步骤：

步骤1	进入congfig模式
	DCFW-1800#configure terminal
步骤2	进入接口
	DCFW-1800(config)# interface ge0/0
步骤3	建立虚拟IP为192.168.31.1的备份组1
	DCFW-1800(config-ge0/0)#vrrp 1 ip 192.168.31.1
步骤4	配置备份组1为简单字符串认证模式，认证字为123
	DCFW-1800(config-ge0/0)# vrrp 1 authentication text 123
步骤5	修改备份组1的通告时间间隔为2秒
	DCFW-1800(config-ge0/0)# vrrp 1 timers advertise 2
步骤6	启用备份组1
	DCFW-1800(config-ge0/0)# vrrp 1 enable

31.4 监控与维护

31.4.1 查看 VRRP 配置

配置步骤：

步骤1	显示VRRP配置信息
	DCFW-1800_A# show vrrp ge0/0-Group 1 Enabled State is Master Using VRRP protocol is version 2 Virtual IP address is 192.168.31.1

	Virtual MAC address is 00:00:5E:00:01:01 Advertisement interval is 2.00 seconds Priority is 100 Preemption enabled Ping disabled Using TEXT authentication, password: 123 Master is 192.168.31.106, priority is 100

31.5 故障分析

31.5.1 故障现象 1：

现象	配置好了一个备份组，在启用后一直显示处于“Initialize”状态。
分析	备份组所属接口没有处于UP状态，或者网线没有插好。
解决	备份组所属接口必须满足： 1、 接口处于UP状态 2、 接口网线上能检测到载波信号 3、 接口上至少配置了一个真实IP 地址

第32章 配置系统日志

32.1 配置系统日志概述

系统日志是记录设备运行状况的一种方法。本设备支持标准的 SYSLOG 格式，包括本地日志，以及发送到 E-mail 日志，提供给用户掌握系统运行状况的途径。

本设备支持日志存储耗尽机制，即日志存储耗尽日志报警和删除百分比设置，CLI 可配置，同时邮件告警可发送该类日志。

32.2 配置系统日志

32.2.1 缺省配置信息

内容	缺省设置	备注
本地日志（memory）	关闭	不可更改
E-Mail日志（email）	关闭	可更改设置
SYSLOG服务器状态（enable/disable）	disable	可更改设置
SYSLOG服务端口（port）	514	可更改设置

32.2.2 配置本地日志

本地日志即内存日志，系统将各模块的日志信息按配置保存到内存中.

系统默认启用本地日志.

32.2.3 配置模块发送日志到本地日志

配置步骤:

步骤1	configure terminal	进入全局配置模式
步骤2	log (ac|attack|ipsecvpn| av| bgp| config| early-warning| filter| flood| ha| hm|if-info| ips| nat| ospf| rip| qos| scan| systrm-info| server| vrrp) **memory** upto (alerts| emergencies| errors| critical| warnings)	每个模块，每个位置对应一个优先级。

32.2.4 配置在线用户查询、冻结

配置步骤：

步骤1	show user-recognition	查询当前在线用户
步骤2	show user-recognition user name NAME	显示用户名为NAME的当前在线用户
步骤3	show user-recognition address host ADDRESS	显示IP地址是ADDRESS的当前在线用户
步骤4	show user-recognition address name USER	显示用户名USER的当前在线用户
步骤5	show user-recognition address range ADDRESS1 ADDRESS2	显示地址IP在ADDRESS1和ADDRESS2范围内的当前在线用户
步骤6	show user-recognition authenticated	显示当前已认证的在线用户
步骤7	configure terminal	进入全局配置模式
步骤8	freeze ip IP TIME	冻结IP地址是IP的用户，冻结时间TIME
步骤9	freeze user NAME TIME	冻结用户名为NAME的用户，冻结时间TIME

参数说明： show user-recognition user name NAME

参数	说明	缺省配置
NAME	用户对象或用户对象组	无

参数说明： show user-recognition address DCFW-1800 ADDRESS

参数	说明	缺省配置
ADDRESS	主机IP地址	无

参数说明： show user-recognition address name USER

参数	说明	缺省配置
USER	用户对象或用户对象组	无

参数说明： show user-recognition address range ADDRESS1 ADDRESS2

参数	说明	缺省配置
ADDRESS1	地址范围的起始IP	无
ADDRESS2	地址范围的结束IP	无

参数说明：freeze ip IP TIME

参数	说明	缺省配置
IP	冻结的IP地址	无
TIME	冻结时间	无

参数说明：freeze user NAME TIME

参数	说明	缺省配置
NAME	冻结的用户名或用户组名	无
TIME	冻结时间	无

32.2.5 清除本地日志

该命令将清除本地所有日志信息。

配置步骤：

步骤1	clear log memory	清除本地日志

32.2.6 配置模块发送日志到 E-mail

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	log (ac|attack|ipsecvpn| av| bgp| config| early-warning| filter| flood| ha| hm|if-info| ips| nat| ospf| rip| qos| scan| systrm-info| server| vrrp) email upto (alerts| emergencies| errors| critical| warnings)	每个模块，每个位置对应一个优先级。

32.2.7 配置使能 SYSLOG 日志服务器

SYSLOG 日志，系统将各模块的日志信息按配置发送到 SYSLOG 服务器。

配置步骤：

步骤1	configure terminal	进入全局配置模式

步骤2	log server enable	启用SYSLOG日志

使用 nolog server enable 命令可以关闭 SYSLOG 日志。

32.2.8 配置 SYSLOG 服务器地址

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	log server address A.B.C.D	配置SYSLOG服务器地址为A.B.C.D
步骤3	Log server second address A.B.C.D	配置第二个日志服务器地址
步骤4	Log server third address A.B.C.D	配置第三个日志服务器地址

使用 nolog server address、no log second address 和 no log third address 命令可以取消 SYSLOG 的服务器地址。

32.2.9 配置 SYSLOG 服务器的端口

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	log server port <1-65535>	配置SYSLOG服务器的端口，范围为1-65535

使用 nolog server port 命令可以恢复 SYSLOG 的服务器端口为默认端口 514。

32.2.10 配置模块发送日志到 SYSLOG 服务器

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	log (ac|attack|ipsecvpn| av| bgp| config| early-warning| filter| flood| ha| hm|if-info| ips| nat| ospf| rip| qos| scan| systrm-info| server| vrrp) server upto (alerts| emergencies| errors| critical| warnings)	每个模块，每个位置对应一个优先级。 最低级别为informational

使用 no log (ac|attack|ipsecvpn| av| bgp| config| early-warning| filter| flood| ha| hm|if-info| ips| nat| ospf| rip| qos| scan| systrm-info| server| vrrp) "，删除对应模块的所有日志配置。

32.2.11 配置使能集中管理中心服务器

系统将当前的地址等信息发送到集中管理中心服务器。

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	state server enable	启用向集中管理中心服务器发送报告

使用 no state server enable 命令可以关闭向集中管理中心服务器发送报告。

32.2.12 配置集中管理中心服务器地址

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	state server addr A.B.C.D	配置集中管理中心服务器地址为A.B.C.D
步骤3	state server second addr A.B.C.D	配置第二个集中管理中心地址

使用 no state server addr 和 no state server second addr 命令可以取消集中管理中心服务器地址。

32.2.13 配置集中管理中心服务器的端口

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	log server state port <1-65535>	配置集中管理中心服务器的端口，范围为1-65535.
步骤3	log server second state port <1-65535>	配置第二个集中管理中心服务器的端口，范围为1-65535

32.2.14 配置硬盘存储阈值

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	disk-usage max <50-90>	配置硬盘存储阈值50%-90%

32.3 配置案例

32.3.1 配置案例 1: 配置本地日志

案例描述

配置接口模块通知级别日志到本地日志。

配置步骤：

步骤1	配置接口模块内存日志等级
	DCFW-1800#config terminal DCFW-1800(config)#log if-info memory upto notifications DCFW-1800(config)#exit
步骤2	查看配置
	DCFW-1800#show log-config log if-info memory upto notifications !

32.4 常见故障分析

32.4.1 故障现象 1：SYLOG 日志失效。

现象	在SYSLOG服务器上看不到对应模块日志
分析	1）是否正确配置SYLOG服务器的地址和端口号 2）是否指定模块的日志类别和等级到SYSLOG Server
解决	1）正确配置SYSLOG服务器的地址和端口号 2）指定模块的日志类别和等级到SYSLOG Server

32.4.2 故障现象 2：E-mail 日志失效。

现象	没有收到对应模块信息的邮件
分析	1）是否正确配置Email配置参数 2）是否指定模块的日志类别和等级到Email日志
解决	1）正确配置Email配置参数 2）指定模块的日志类别和等级到Email日志

第33章 系统维护

系统维护包括系统时间设置，E－mail 设置，系统相关配置的备份恢复，系统升级，诊断。

33.1 系统时间设置

33.1.1 查看系统连续运行的时间

查看步骤：

步骤1	查看系统连续运行的时间
	DCFW-1800# show system uptime current time : Sat Jul 25 23:17:30 2015 system runtime : 1 day 2 hours 3 minutes 表示当前时间是上午17:30，系统运行已经1 day 2 hours。

33.1.2 查看系统当前的日期和时间

查看步骤：

步骤1	查看系统当前的日期和时间
	DCFW-1800# show date ABS time :1437837427 UTC time :2015-07-25 15:17:07 Local time :2015-07-25 23:17:07 UTC time表示系统当前UTC时间, Local time表示系统当前本地时间

查看系统当前的时区

查看步骤：

步骤1	查看系统当前的时区
	DCFW-1800# show timezone timezone 57 表示当前时区为第57时区(即CST,中国时区)。

33.1.3 配置系统当前的时区

配置步骤：

步骤1	配置系统当前的时区
	DCFW-1800(config)# timezone 57 表示配置当前时区为第57时区(即CST,中国时区)。

时区参数对应如下：

1 zone1=GMT-12:00 日界线西
2 zone2=GMT-11:00 中途岛 萨摩亚群岛
3 zone3=GMT-10:00 夏威夷
4 zone4=GMT-09:00 阿拉斯加
5 zone5=GMT-08:00 太平洋时间(美国和加拿大) 蒂华纳
6 zone6=GMT-07:00 山地时间(美国和加拿大)
7 zone7=GMT-07:00 亚利桑那
8 zone8=GMT-07:00 齐瓦瓦拉巴斯马扎特兰
9 zone9=GMT-06:00 萨斯喀彻温
10 zone10=GMT-06:00 中部时间(美国和加拿大)
11 zone11=GMT-06:00 中美州
12 zone12=GMT-06:00 瓜达拉哈拉墨西哥城蒙特雷
13 zone13=GMT-05:00 波哥大 利马基多
14 zone14=GMT-05:00 东部时间(美国和加拿大)
15 zone15=GMT-05:00 印第安那州(东部)
16 zone16=GMT-04:00 大西洋时间(美国和加拿大)
17 zone17=GMT-04:00 加拉加斯 拉巴斯
18 zone18=GMT-04:00 圣地亚哥
19 zone19=GMT-03:30 纽芬兰
20 zone20=GMT-03:00 巴西利亚
21 zone21=GMT-03:00 布宜诺斯艾利斯 乔治敦
22 zone22=GMT-03:00 格陵兰
23 zone23=GMT-02:00 中大西洋
24 zone24=GMT-01:00 佛得角群岛
25 zone25=GMT-01:00 亚速尔群岛
26 zone26=GMT 格林威治都柏林爱丁堡伦敦里斯本
27 zone27=GMT 卡萨布兰卡蒙罗维亚
28 zone28=GMT+01:00 阿姆斯特丹柏林伯尔尼罗马斯德哥尔摩维也纳
29 zone29=GMT+01:00 贝尔格莱德布拉迪斯拉发布达佩斯卢布尔雅那
30 zone30=GMT+01:00 布鲁塞尔哥本哈根马德里巴黎

31 zone31=GMT+01:00 萨拉热窝斯科普里华沙萨格勒布
32 zone32=GMT+01:00 中非西部
33 zone33=GMT+02:00 布加勒斯特
34 zone34=GMT+02:00 哈拉雷比勒陀利亚
35 zone35=GMT+02:00 赫尔辛基基辅里加索非亚塔林维尔纽斯
36 zone36=GMT+02:00 开罗
37 zone37=GMT+02:00 雅典贝鲁特伊斯坦布尔明斯克
38 zone38=GMT+02:00 耶路撒冷
39 zone39=GMT+03:00 巴格达
40 zone40=GMT+03:00 科威特利雅得
41 zone41=GMT+03:00 莫斯科圣彼得堡伏尔加格勒
42 zone42=GMT+03:00 内罗毕
43 zone43=GMT+03:30 德黑兰
44 zone44=GMT+04:00 阿布扎比马斯喀特
45 zone45=GMT+04:00 巴库第比利斯埃里温
46 zone46=GMT+04:30 喀布尔
47 zone47=GMT+05:00 叶卡捷琳堡
48 zone48=GMT+05:00 伊斯兰堡卡拉奇塔什干
49 zone49=GMT+05:30 马德拉斯孟买加尔各答新德里
50 zone50=GMT+05:45 加德满都
51 zone51=GMT+06:00 阿拉木图新西伯利亚
52 zone52=GMT+06:00 阿斯塔纳达卡
53 zone53=GMT+06:00 斯里哈亚华登尼普拉
54 zone54=GMT+06:30 仰光
55 zone55=GMT+07:00 克拉斯诺亚尔斯克
56 zone56=GMT+07:00 曼谷河内雅加达
57 zone57=GMT+08:00 北京重庆乌鲁木齐香港特别行政区
58 zone58=GMT+08:00 吉隆坡新加坡
59 zone59=GMT+08:00 珀斯
60 zone60=GMT+08:00 台北
61 zone61=GMT+08:00 伊尔库茨克乌兰巴图
62 zone62=GMT+09:00 大阪东京札幌
63 zone63=GMT+09:00 汉城
64 zone64=GMT+09:00 雅库次克
65 zone65=GMT+09:30 阿德莱德
66 zone66=GMT+09:30 达尔文
67 zone67=GMT+10:00 布里斯班
68 zone68=GMT+10:00 符拉迪沃斯托克
69 zone69=GMT+10:00 关岛莫尔兹比港

70 zone70=GMT+10:00 霍巴特

71 zone71=GMT+10:00 堪培拉墨尔本悉尼

72 zone72=GMT+11:00 马加丹所罗门群岛新喀里多尼亚

73 zone73=GMT+12:00 奥克兰惠灵顿

74 zone74=GMT+12:00 斐济堪察加半岛马绍尔群岛

75 zone75=GMT+13:00 努库阿洛法

33.1.4 手动设置系统当前的日期和时间

命令说明：date <2006-2030><1-12><1-31><0-23><0-59><0-59>

关键字和参数	说明
<2006-2030>	配置年份
<1-12>	配置月份
<1-31>	配置日
<0-23>	配置小时
<0-59>	配置分钟
<0-59>	配置秒

配置步骤：

步骤**1**	设置系统当前的日期和时间
	DCFW-1800# date 2015 04 02 10 20 50 表示设置系统时间为20015年4月2日上午10点20分50秒

33.1.5 使用 ntp 设置系统当前的时间

配置步骤：

步骤**1**	配置ntp server地址及loop间隔
	DCFW-1800(config)# ntp 192.168.2.5760 [authentication-keyid 1 authentication-modemd5 123456 表示配置ntp server地址为192.168.2.57， ntp loop间隔为60秒，认证id为1，认证key为md5 123456

使用 no ntp 命令可以停止 ntp 配置。

查看步骤：

步骤**1**	显示ntp配置

	DCFW-1800# show ntp config timezone 57 ntp 192.168.2.57 60

33.1.6 使用 ntp 立即更新系统时间

步骤1	通过ntp立即更新系统时间
	DCFW-1800# ntpupdate time.windows.com time update success

33.2 系统升级和相关配置备份恢复

33.2.1 手动升级及配置恢复

命令说明：copy tftp A.B.C.D RemoteFile(version|config|applib |ipslib|avlib|urllib)

关键字和参数	说明
tftp	表示采用tftp协议传输文件
A.B.C.D	表示tftp server地址
RemoteFile	表示在tftp server上该文件名
(version |config |applib |ipslib |avlib |urllib)	version：表示更新软件版本 config：表示更新系统配置文件 applib：表示更新应用文件 ipslib：表示更新入侵防御软件 avlib：表示更新病毒文件 urllib ：表示更新url文件

命令说明：write (file|memory|terminal)

关键字和参数	说明
(file|memory|terminal)	File ：表示保存当前配置 Memory：表示缓存当前配置 Terminal：表示显示当前配置

33.2.2 自动升级

步骤1	进入自动升级配置模式
	DCFW-1800(config)# auto-update DCFW-1800(auto-update)#
步骤2	配置升级服务器
	DCFW-1800(auto-update)# server 192.168.31.155
步骤3	配置按星期几升级
	DCFW-1800(auto-update)# weekly sun mon null wed null fri null 表示每星期日/星期一/星期三/星期五升级
步骤4	或者配置按每月几号升级
	DCFW-1800(auto-update)# monthly 10,20,30 表示每月10号,20号,和30号升级
步骤5	配置升级时间
	DCFW-1800(auto-update)#time hour 3 minute 0 表示该天凌晨3点整升级
步骤6	启用自动升级配置
	DCFW-1800(auto-update)#update enable
步骤7	关闭自动升级配置
	DCFW-1800(auto-update)#update disable

33.3 系统诊断

33.3.1 Ping 命令的使用

设备提供了 Ping 命令用来检测网络的基本连接情况，Ping 命令发送 Internet Control Message Protocol (ICMP) 请求报文到网络中的某个 IP 设备。普通用户和管理员用户都可以使用 Ping 命令。

如果在设定时间内没有收到目的设备响应报文，则不输出任何信息，否则显示响应报文的字节数、报文序号、TTL 、响应时间。按 CTRL+C 可以结束 Ping 状态。

命令说明：ping -c <1-10000> -s <0-65507> -w <0-10> WORD

关键字和参数	说明
-I	表示源地址
-c <1-10000>	表示发送报文条数
-s <0-65507>	表示发送报文大小
-t<1-255>	表示TTL
-w <0-10>	表示接收报文等待时间
WORD	表示目的地址

检测步骤：

步骤**1**	测试设备到IP地址为10.13.2.14的设备的连通性。
	DCFW-1800# ping 10.13.2.14 如果设备连通，则出现以下信息： DCFW-1800# ping 10.13.2.14 PING10.13.2.14 (10.13.2.14): 56 data bytes 64 bytes from 10.13.2.14: icmp_seq=0 ttl=64 time=0.3 ms 64 bytes from 10.13.2.14: icmp_seq=1 ttl=64 time=0.0 ms 64 bytes from 10.13.2.14: icmp_seq=2 ttl=64 time=0.0 ms 64 bytes from 10.13.2.14: icmp_seq=3 ttl=64 time=0.0 ms 如果没有连通则出现以下信息： DCFW-1800# ping 1.1.1.1 PING1.1.1.1 (1.1.1.1): 56 data bytes

33.3.2 Traceroute 命令的使用

Traceroute 是另一种检测网络连接情况的命令，它与 Ping 命令不同的是：它不但可以测试网络是否连通，还可以获知在数据包的传输路径中哪一个地方出现问题。Traceroute 命令的输出信息包括到达目的地所经过的所有网关的 IP 地址和到此网关所用时间，如果某网关超时则显示“*”。

命令说明：traceroute [-s A.B.C.D][-u <0-65535] WORD

关键字和参数	说明
WORD	表示目的IP地址或域名

检测步骤：

步骤**1**	测试设备到IP地址为192.168.10.1的设备的连通性。
	DCFW-1800# traceroute 192.168.10.1 traceroute to 192.168.10.1 (192.168.10.1), 30 hops max, 38 byte packets 1 192.168.6.1 (192.168.6.1) 0.466 ms 1.287 ms 0.286 ms 2 192.168.10.1 (192.168.10.1) 2.092 ms 1.265 ms 2.134 ms 表示连通目的地

命令说明：traceroute –s A.B.C.D A.B.C.D

关键字和参数	说明
-s A.B.C.D	指定源ip地址
A.B.C.D	目标主机的ip地址

命令说明：traceroute –u <1-65535> A.B.C.D

关键字和参数	说明
<1-65535>	端口号
A.B.C.D	目标主机的ip地址

33.3.3 TCPSYN 命令的使用

TCPSYN 是一种检测对方设备端口打开情况的命令。TCPSYN 通过发送 TCP SYN 报文来检测对方对应端口是否打开。

命令说明：tcpsyn -c <1-1000> -w <1-1000>A.B.C.D <0-65535>

关键字和参数	说明
A.B.C.D	表示目的地地址
<0-65535>	表示目的地端口

-c <1-10000>	表示发送报文条数
-w <0-10>	表示接收报文等待时间

检测步骤：

步骤**1**	测试IP地址为192.168.31.155的设备其端口22的打开情况。
	DCFW-1800# tcpsyn 192.168.31.155 22 tcpsyn to 192.168.31.155:22 1 * TCP SYN timeout: reason=2. 2 * TCP SYN timeout: reason=2. 3 * TCP SYN timeout: reason=2. 4 * TCP SYN timeout: reason=2. 5 * TCP SYN timeout: reason=2. 说明对方22端口没有打开。
步骤**2**	测试IP地址为192.168.31.155的设备其端口21的打开情况。
	DCFW-1800# tcpsyn 192.168.31.155 21 tcpsyn to 192.168.31.155:21 1 TCP ACK form 192.168.31.155:21 2 TCP ACK form 192.168.31.155:21 3 TCP ACK form 192.168.31.155:21 4 TCP ACK form 192.168.31.155:21 5 TCP ACK form 192.168.31.155:21 说明对方21端口已经打开。

33.4 E-mail设置

33.4.1 配置 SMTP 服务器名称或者地址

配置步骤：

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	smtp-config	进入SMTP配置模式
3	server NAME	配置服务器的名字或者IP
4	server address	配置服务器的名字或者IP

5	server port	配置服务器端口

使用 no server 可以删除 SMTP 服务器配置。

33.4.2 配置邮件发送者邮件地址

配置步骤:

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	smtp-config	进入SMTP配置模式
3	sender NAME	配置邮件发送者的地址
4	Send-interval <1-60>	发送时间间隔

使用 no sender 取消配置。

33.4.3 配置邮件接收者邮件地址

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	smtp-config	进入SMTP配置模式
3	receiver1LONGSTRING	配置邮件接收者的地址。多个接收者地址需要使用分号“;”隔开，最多可以输入255的字符。

使用 no receiver1 取消配置。

33.4.4 配置发送邮件时是否需要认证

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	smtp-config	进入SMTP配置模式
3	auth enable	配置邮件发送时需要认证

使用 auth disable 取消发送邮件时需要认证的配置。

33.4.5 配置发送邮件时认证使用的用户名

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	smtp-config	进入SMTP配置模式
3	username NAME	配置邮件发送时认证使用的用户名

使用 no username 取消邮件发送时认证使用的用户名的配置。

33.4.6 配置发送邮件时认证使用的密码

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	smtp-config	进入SMTP配置模式
3	passwd PASSWORD	配置邮件发送时认证使用的密码

使用 no passwd 取消邮件发送时认证使用的密码。

33.4.7 配置 SSL 加密

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	smtp-config	进入SMTP配置模式
3	ssl enable	启用ssl加密

使用 ssl disable 取消 ssl 加密。

33.5 配置系统监控

33.5.1 配置 CPU 占用率

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	sysmon	进入sysmon配置模式
3	log cpu syslog	开启cpu使用率超过限制，发送日志到syslog服务器
4	log cpu local	开启cpu使用率超过限制，本地记录日志
5	log cpu email	开启cpu使用率超过限制，email发送日志
6	sysres cpu Usage	配置cpu使用率告警界限

33.5.2 配置内存占用率

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	sysmon	进入sysmon配置模式
3	log memory syslog	开启内存使用率超过限制，发送日志到syslog服务器
4	log memorylocal	开启内存使用率超过限制，本地记录日志
5	log memoryemail	开启内存使用率超过限制，email发送日志
6	sysres memory Usage	配置内存使用率告警界限

33.5.3 配置流量

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	sysmon	进入sysmon配置模式
3	log flow syslog	开启流量超过限制，发送日志到syslog服务器
4	log flowlocal	开启流量超过限制，本地记录日志
5	log flowemail	开启流量超过限制，email发送日志

6	sysres flow COUNT_OF_NET_FLOW	配置流量告警界限，COUNT_OF_NET_FLOW是界限值

33.5.4 配置连接数

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	sysmon	进入sysmon配置模式
3	log session syslog	开启会话数超过限制，发送日志到syslog服务器
4	log sessionlocal	开启会话数超过限制，本地记录日志
5	log sessionemail	开启会话数超过限制，email发送日志
6	sysres session COUNT_OF_NET_SESSION	配置会话数告警界限，COUNT_OF_NET_SESSION是界限值

33.5.5 配置报文大小

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	sysmon	进入sysmon配置模式
3	log packet syslog	开启包大小超过限制，发送日志到syslog服务器
4	log packetlocal	开启包大小超过限制，本地记录日志
5	log packetemail	开启包大小超过限制，email发送日志
6	sysres packet LENGTH_OF_THE_PACKET	配置包大小告警界限，LENGTH_OF_THE_PACKET是包大小界限值

第34章 配置 DNS

34.1 DNS概述

DNS 为其他需要域名解析的模块提供域名解析客户端功能：向配置的 DNS 服务器发送域名解析请求，并接受 DNS 服务器的响应，最后将解析后的地址发送给各个使用 DNS 的模块。

34.2 配置DNS

34.2.1 缺省配置信息

内容	缺省设置	备注
重试次数	2	不可更改设置
超时时间	5秒	不可更改设置

34.2.2 配置主 DNS 服务器

DNS 客户端首先向 DNS 主服务器请求域名解析。

配置步骤：

步骤1	configure terminal	进入全局配置模式。
步骤2	ip name-server master A.B.C.D	配置主DNS服务器。

使用 no ip name-server master 清除主 DNS 服务器。

34.2.3 配置从 DNS 服务器

如果 DNS 主服务器解析失败或超时，客户端首先向 DNS 从服务器请求域名解析。

配置步骤：

步骤1	configure terminal	进入全局配置模式。
步骤2	ip name-server backup A.B.C.D	配置从DNS服务器。

使用 no ip name-server backup 清除从 DNS 服务器。

34.2.4 DNS 查询

进行域名解析。

配置步骤：

步骤1	dns-lookup NAME	域名解析。

34.3 配置案例

34.3.1 配置案例

案例描述

DNS 服务器地址为 202.118.3.2，备份 DNS 服务器地址为 202.118.3.3。在设备上配置 DNS 服务后可以向配置的 DNS 服务器发送域名解析请求，并接受 DNS 服务器的响应，来进行域名解析。

配置步骤：

步骤1	创建一个域。
	DCFW-1800_A(config)# ip name-server master 202.118.3.2 DCFW-1800_A(config)# ip name-server backup 202.118.3.3
步骤2	查看配置信息。
	DCFW-1800# show running-config ! ip name-server master 202.118.3.2 ip name-server backup 202.118.3.3

34.4 常见故障分析

34.4.1 故障现象 1：DNS 解析失败

现象	DNS解析失败。
分析	DNS服务器配置错误，或没有到DNS服务器的路由。
解决	配置正确的DNS服务器地址或添加到DNS服务器网络的路由。

第35章 配置管理员用户

本章涉及管理员用户以及用户组的配置。叙述了怎样配置管理用户以及用户组的配置。

35.1 配置管理员

出厂的默认配置包括一个超级管理员用户 admin，使用这个帐号，可以登录设备对设备进行配置，包括配置其它的管理员。每个管理员都有它的管理地址，以及管理权限和描述，权限是通过权限表来限制的。下面一一列举怎样进行配置。下列各项配置，如未特别说明，均指特权模式下的操作。

35.1.1 配置用户权限表

权限表是在配置管理员用户的时候使用到的。每个管理员会对应一个管理员权限表，该管理员只具有管理员权限表中规定的权限。配置步骤如下

配置用户权限表的步骤:

步骤**1**	authorized-table NAME	如果不存在该权限表，创建一个，并进入权限表节点，如果存在，直接进入权限表节点
步骤**2**	Authorized (read|write) (all|system-config|log-config|log-read| admin-user||updata|reboot)	设置权限表的读写权限

参数说明:

参数	说明	缺省配置
read	表示后面的参数说明的是读权限。	无
write	表示后面的参数说明的是写权限。	无
all	表示所有功能都打开	无
system-config	具有系统配置的权限，系统配置具有下面六种权限规定以外的所有权限，且具有对象管理的权限。	无
log-config/log-read	具有日志，NetFlow操作的权限。	无
admin-user	具有管理员用户，授权表，在线信息的操作权限。	无
updata	具有升级的操作权限。	无

35.1.2 配置本地用户

本地管理员用户是指用户的信息保存在设备上。配置步骤如下

配置本地用户的步骤:

步骤**1**	user administrator USER local PASSWORD authorized-table NAME [disable]	创建或者修改本地管理员用户的密码以及管理权限表，并可以通过disable选项使该用户暂时无效。

35.1.3 配置 RADIUS 管理员用户

RADIUS 管理员用户是指用户的信息保存在 RADIUS 服务器上。用户认证需要通过 RADIUS 服务器认证。配置步骤如下

配置 RADIUS 管理员用户的步骤:

步骤**1**	user administrator USER radius SERVER authorized-table NAME [disable]	创建或者修改RADIUS管理员对应的RADIUS服务器以及管理权限表，并可以通过disable选项使该用户暂时无效。

35.1.4 配置 LDAP 管理员用户

LDAP 管理员用户是指用户的信息保存在 LDAP 服务器上。用户认证需要通过 LDAP 服务器认证。配置步骤如下

配置 RADIUS 管理员用户的步骤:

步骤**1**	user administrator USER ldap SERVER authorized-table NAME [disable]	创建或者修改RADIUS管理员对应的LDAP服务器以及管理权限表，并可以通过disable选项使该用户暂时无效。

35.1.5 配置管理员用户的管理地址

如果需要控制登录用户的地址，可以通过配置管理员用户的授权地址来控制用户登录的地址范围。如果没有配置该地址，那么可以通过任意的 IP 地址登录。配置步骤如下：

配置管理员用户的授权地址的步骤:

步骤**1**	user administrator USER authorized-address <1-16>(A.B.C.D/M|X:X::X:X/M)	可以配置三个授权地址段，该用户可以通过任意一个地址段内的地址登录

35.1.6 配置管理员最短口令长度

配置管理员用户的最短口令长度的步骤:

步骤**1**	admin password LENGTH	管理员用户的最短口令长度

参数说明：

参数	说明	缺省配置
LENGTH	最短口令长度	

35.2 配置信息显示命令

配置信息显示命令列表

命令	解释
show admin-user	显示当前已添加的管理员用户信息
show running-config	显示当前配置。

who 命令显示举例:

步骤**1**	在线管理员用户的显示举例:
	DCFW-1800# who Login style Username IP Console admin * Mon Apr 9 10:17:19 SSH admin 192.168.31.117 Mon Apr 9 10:21:17 Telnet admin 192.168.31.117 Mon Apr 9 10:21:32

35.3 配置案例

35.3.1 配置管理员用户的权限表功能

案例描述：

配置设备，添加两个管理员用户 check 和 admin，其中 check 的权限表是 show-config，admin 的权限表是 system-config。Show-config 具有显示功能的权限，而 admin 具有读写所有模块的权限。结果：

用户 check 只能使用 show 命令，不能进入 CONFIG 节点；

用户 admin 可以使用系统中所有命令。

配置步骤：

步骤**1**	添加授权表

	DCFW-1800# configure terminal DCFW-1800(config)# authorized-table reader DCFW-1800(authorized-table)# authorized read all DCFW-1800(authorized-table)# exit DCFW-1800(config)# DCFW-1800# configure terminal DCFW-1800(config)# authorized-table system-config DCFW-1800(authorized-table)# authorized read all DCFW-1800(authorized-table)# authorized write all DCFW-1800(authorized-table)# exit DCFW-1800(config)#
步骤2	添加管理员用户
	DCFW-1800# configure terminal DCFW-1800(config)# user administrator check local zte authorized-table reader DCFW-1800(config)# user administrator admin local zte authorized-table system-config
步骤3	设置用户管理地址
	DCFW-1800(config)# user administrator check authorized-address first 192.168.0.10
步骤4	保存配置
	DCFW-1800(config)# write memory

案例达到的效果如下：

以 check 用户登录

Username: check

Password:

DCFW-1800> en

DCFW-1800# show admin-user

Admin User Name	User Type	User Status
admin	local	enable
check	local	enable

Total users : 2

DCFW-1800# configure terminal

This user is not permited this operation

DCFW-1800#

以上可以看出，当我们以 check 用户登录时，只能查看信息，但是不能进入 config 节点进行配置。

如果用户不是通过 192.168.0.10 登录设备的，会提示非法地址的错误，不让登录。

以 admin 用户登录

```
Username: admin
Password:
DCFW-1800> en
DCFW-1800# show admin-user
Admin User Name                 User Type   User Status
admin                            local       enable
check                            local       enable
Total users : 2
DCFW-1800# configure terminal
DCFW-1800(config)#
```

以上可以看出，当我们以 admin 用户登录时，能够进入 config 节点进行配置。

35.4 故障分析

35.4.1 用户无法登录

故障现象	存在该用户，但使用这个用户名无法登录
分析与解决	1）该用户是否是管理员用户 2）是否对该用户名限制登录的IP地址范围 3）该用户是否处于封禁状态，如果是使用user administrator check local zte authorized-table Reader 类似的命令启用。 4）用户密码存在问题，请使用user administrator check local zte authorized-table Reader 指令重设一遍用户密码。

35.4.2 命令无法执行

故障现象	用户能够登录，但是不能执行命令
分析与解决	通过show running-config查看配置，查看用户对应的权限表中是否有对应的权限

第36章 配置 SNMP

36.1 SNMP协议概述

SNMP，Simple Network Management Protocol，即简单网络管理协议,，是有IETF(Internet Engineeriing Task Force，互联网工程任务组)定义的一套基于SGMP(Simple Gateway Monitor Protocol，简单网关监视协议)的网络管理协议。以SNMP 为技术的网络管理系统(NMS)中，管理工作站利用 SNMP 进行远程监控管理网络上的所有支持这种协议的设备(如计算机工作站、终端、路由器、Hub、网络打印机等)，主要负责监视设备状态、修改设备配置、接受事件警告等。

SNMPv3 保持了 SNMPv1 和 SNMPv2 易于理解和实现的特性，同时还增强了网络管理的安全性能，提供了前两个版本欠缺的保密、验证和访问控制等安全管理特性。SNMPv3 正在逐渐扩充和发展，新的管理信息库还在不断增加，能够支持更多的网络应用。所以，它是建立网络管理系统的有力工具，也将推动互联网不断发展。

根据需求增加了 snmpv3 特性，实现了 snmpv3 中的用户管理机制，还添加了公司的私有 mib 库。

36.2 配置SNMP

36.2.1 缺省配置信息

RIP 的缺省设置信息如以下表格所示：

表36-1SNMP 缺省配置信息

内容	缺省设置	备注
使能/禁止状态（enable/disable）	disable	可更改设置
版本v1	启用	可更改设置
版本v2c	启用	可更改设置
版本v3	启用	可更改设置
设备位置	空	可更改设置
trap地址	空	可更改设置
团体	public	可更改设置
Usm用户	空	可添加用户

36.2.2 配置启用 SNMP 代理

启用设备的 SNMP 代理，启用后客户端可以访问设备的 MIB 库信息

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	snmp	进入snmp配置节点
步骤3	snmp enable	启用snmp代理

在 snmp 节点下使用 snmp disable 可以关闭 snmp 代理。

参数说明： snmp NAME

参数	说明	缺省配置
enable	启用snmp代理	无
disable	关闭snmp代理	无

36.2.3 配置设备物理地址

配置设备物理地址的字符串信息。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	snmp	进入snmp配置节点
步骤3	syslocation abc	配置地址信息为abc
步骤4	end	回到enable模式

使用 no syslocation 可以取消对 syslocation 的设置，使其恢复到缺省配置空。

参数说明：syslocation NAME

参数	说明	缺省配置
NAME	设备地址信息	空

36.2.4 配置 trap 地址

配置 snmp 代理发送 trap 时 trap 信息发往的 IP 地址。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	snmp	进入snmp配置节点

步骤3	trap address 192.168.31.2	配置trap地址为192.168.31.2
步骤4	end	回到enable模式

使用 no trap address 可以取消 trap 地址的设置。

参数说明：trap address A.B.C.D

参数	说明	缺省配置
A.B.C.D	trap信息发送的IP地址	无

36.2.5 配置 community

配置 snmp 的团体字符串。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	snmp	进入snmp配置节点
步骤3	community abc	配置团体为abc
步骤4	end	回到enable模式

使用 no community 可以取消对团体的设置，使其恢复到默认值 public。

参数说明：community NAME

参数	说明	缺省配置
NAME	团体字符串信息	public

36.2.6 配置 SNMP 版本

配置 snmp 代理启用或关闭的版本。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	snmp	进入snmp配置节点
步骤3	version v1	启用snmp代理v1版本
步骤4	end	回到enable模式

使用 no version v1 可以关闭 snmp 代理 v1 版本。

参数说明：version (v1|v2c|v3)

参数	说明	缺省配置
(v1|v2c|v3)	启用snmp代理版本	启用

36.2.7 配置 SNMP USM 用户

配置 snmpv3 用户以及此用户对应的认证和加密算法。

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	snmp	进入snmp配置节点
步骤**3**	snmpv3 usm-user u1 auth-mode MD5 11111111 privacy DES 11111111	配置创建用户u1，采用MD5认证算法和DES加密算法，密钥均为11111111。
步骤**4**	end	回到enable模式

使用 no snmpv3 usm-user u1 可以删除用户 u1，使用 no snmpv2 usm-user 可以删除所有用户。

参数说明：snmpv3 usm-user NAME auth-mode (MD5|SHA) PASSWORD1 privacy (DES|AES)PASSWORD2

参数	说明	缺省配置
NAME	用户名	无
(MD5|SHA)	认证算法	无
PASSWORD1	认证算法密钥	无
(DES|AES)	加密算法	无
PASSWORD2	加密算法密钥	无

36.3 配置案例

36.3.1 配置案例 1：通过 MIB Browser 访问设备 MIB 库

案例描述

服务器为设备，实现了 snmp 代理，支持 v1、v2c、v3，计算机为 pc 机，安装了 iReasoning MIB Browser 软件作为管理站。

配置步骤：

步骤**1**	服务器的配置
	800C_3# configure terminal 800C_3(config)# snmp 800C_3(config-snmp)# snmp enable 800C_3(config-snmp)# syslocation abc 800C_3(config-snmp)# community public 800C_3(config-snmp)# trap address 192.168.31.2 800C_3(config-snmp)# snmpv3 usm-user u1 auth-mode MD5 11111111 privacy DES 11111111 800C_3(config-snmp)# end 800C_3#
步骤**2**	计算机上MIB Browser的配置

配置结果：

DUT 的 show running-config 信息

snmp

snmp enable

syslocation abc

trap address 192.168.31.2

snmpv3 usm-user u1 auth-mode MD5 secret XMrOjfrJUmSj5p7teDZnBoGy+MLHk26EnNTQfWyFPUmj2o7vvHJEaFzfpMlvuHx privacy DES secret XMrOjfrJUmSj5p7teDZnBoGy+MLHk2 6EnNTQfWyFPUmj2o7vvHJEaFzfpMlvuHx!

36.4 监控与维护

36.4.1 查看 usm 用户

介绍常用的 show 命令的使用

查看 usm user：

步骤**1**	显示usm用户的配置
	800C_3(config)# snmp 800C_3(config-snmp)# show snmpv3 usm-user

	usm-user authentication privacy u1 MD5 DES total usm-user number: 1 800C_3(config-snmp)# 可以看出snmp配置一个usm用户，使用MD5认证DES加密。

36.5 常见故障分析

36.5.1 故障现象 1：管理站不能访问代理站 MIB 库

现象	访问超时或提示认证失败
分析	团体字符串配置不正确或usm用户配置不正确
解决	检查并修改团体字符串和usm用户的配置

第37章 配置云平台

37.1 云平台概述

大规模网络、应用业务的巨幅增长，企业用户面临的安全威胁也与日俱增，威胁种类呈现出多样化的趋势。在企业网络安全建设方面，往往通过部署多台、多种类的安全设备，实现对信息网络的分级保护。传统的网管平台虽然可以集中式的进行安全检测和控制，但是管理性能低下，且接收数据存在各种性能瓶颈。在此背景下，我们推出了下一代数据驱动安全管理云中心，他不仅支持以往的硬件性能扩展，还支持基于软件的水平扩展，来满足大批量网络安全设备上报的数据元信息，通过大数据分析算法，安全资产管理，云计算等手段，以安全数据为核心，来驱动整个网络的安全能力的提升，是新一代的云安全界的顶尖产品。通过运行浏览器对云平台进行配置和管理。云平台安装之后默认开启了 web 服务。

37.2 云平台配置

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	cloud-agent enable|disable	启用/禁用云平台代理
步骤**3**	cloud-agent domain <HOST>	配置云平台地址
步骤**4**	cloud-agent port <1-65535>	配置云平台端口
步骤**5**	cloud-agent alive-cycle <1-600>	配置状态上报间隔
步骤**6**	cloud-agent bind-code <CODE>	配置用户绑定码

参数说明：

参数	说明	缺省配置
HOST	云平台地址	无
<1-65535>	云平台端口	9070
<1-600>	状态上报间隔	10
CODE	用户绑定码	无

第38章 配置 SSL VPN

38.1 SSL VPN概述

SSLVPN 指的是基于安全套接层协议(Security Socket Layer-SSL)建立远程安全访问通道的 VPN 技术。它是近年来兴起的 VPN 技术，其应用随着 Web 的普及和电子商务、远程办公的兴起而发展迅速。SSl 是一个不依赖于平台和运用程序的协议，保障 TCP-based 运用安全，有的说是会话层技术，这里说的是在应用层和 TCP 层之间的

SSL 加密知名协议：

- HTTP over SSL 加密网页流量是设计 SSL 初衷，也是第一个使用 SSL 保障安全的运用层协议，HTTPS 工作在 TCP443 端口;
- Emailover SSL 例如 SMTP over TLS，POP3 和 IMAP over TLS

38.2 配置SSL VPN

SSL VPN 功能使用隧道模式实现，因此需要配置隧道地址作为拨入用户网关。（需要用户拨入接口 sslvpn 功能启用）

配置 SSL VPN 的步骤：

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	sslvpn	进入sslvpn配置模式
步骤**3**	Address-pool ***A.B.C.D/M***	配置地址池网段(e.g. 8.8.0.0/16)
步骤**4**	Tunnel-address ***A.B.C.D/M***	配置隧道地址，必须是地址池内第一个地址(e.g. 8.8.0.1/16)
步骤**5**	enable	启用sslvpn功能
步骤**6**	exit	退出sslvpn配置模式
步骤**7**	show running-config sslvpn	查看sslvpn配置

可以使用 no address-pool x.x.x.x/x 和 no tunnel-address x.x.x.x/x 删除隧道地址和地址池，使用 disable 来禁用 sslvpn 功能。

38.3 用户中心自定义端口

步骤**1**	configure terminal	进入全局配置模式
步骤**2**	sslvpn	进入sslvpn配置模式

步骤3	user-center port <1024-65535>	自定义用户中心端口信息，默认端口8443
步骤4	exit	退出sslvpn配置模式

用户中心登陆方式 https://192.168.100.1:8443，IP 地址为系统物理接口地址，端口号为定义的端口号。

38.4 SSL多点登录

步骤1	configure terminal	进入全局配置模式
步骤2	sslvpn	进入sslvpn配置模式
步骤3	duplicate-cn enable/disable	用户多点登录启用/禁用
步骤4	exit	退出sslvpn配置模式

SSL VPN 启用多点登录后单个用户名使用多个 IP 进行登录，或多终端类型进行登录

38.5 SSL用户绑定

SSL 为安全性考虑，用户可绑定固定 IP 进行登录

步骤1	configure terminal	进入全局配置模式
步骤2	sslvpn	进入sslvpn配置模式
步骤3	user-bind *User A.B.C.D*	SSL用户绑定固定IP地址
步骤4	exit	退出sslvpn配置模式

参数说明：*User 为 ssl 用户名称，A.B.C.D 为绑定的 IP 地址*

38.6 配置dns&wins

DNS 和 WINS 将会下发给拨入的每一个用户，顺序先后有优先级区别。

配置 DNS&WINS 的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	sslvpn	进入sslvpn配置模式
步骤3	dns/wins ***A.B.C.D***	配置DNS&WINS地址(e.g.8.8.8.8)

步骤4	exit	退出sslvpn配置模式

可以使用 no dns 和 no wins 命令删除配置的 dns 和 wins 地址。

38.7 配置下发路由

为了 sslvpn 用户可以访问目标资源，需要将用户流量导入 sslvpn，实现办法是增加客户端本地路由条目达到更改网络连接的效果。

配置路由的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	sslvpn	进入sslvpn配置模式
步骤3	route ***A.B.C.D/M***	配置下发路由(e.g.3.3.0.0/16)
步骤4	exit	退出sslvpn配置模式

路由最多可配置 128 条，使用 no route ***A.B.C.D/M*** 来删除路由。

38.8 配置客户端下载链接

配置的下载链接会在 sslvpn 用户中心显示。

配置路由的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	sslvpn	进入sslvpn配置模式
步骤3	Client-link <android/ios/win32/win64>***LINK***	配置客户端下载链接
步骤4	exit	退出sslvpn配置模式

***参数说明：client-link* <android/ios/win32/win64>:**

参数	说明	缺省配置
LINK	下载链接	

下载链接必须为 http:// 或 https://头域名形式的地址。

38.9 查看SSL VPN监控

配置 sslvpn 监控

配置步骤：

步骤1	Show sslvpn tunnels	所有sslvpn在线用户

步骤2	Show sslvpn tunnels summary	在线用户总数
步骤3	Show sslvpn data	sslvpn最多允许在线数
步骤4	show running-config sslvpn	查看sslvpn配置

第39章 配置 VRF

39.1 VRF功能概述

虚拟系统通常仅限于一个设施使用，虚拟路由和转发技术能够从一台设备划分出多个虚拟系统，多个虚拟系统可视为多台独立的应用层转发设备。

39.2 配置VRF

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	vrf NAME	配置VRF的名字
步骤**3**	descriptionLINE	对VRF进行描述
步骤**4**	containINTERFACE	把对应名字的接口划分到VRF中
步骤**5**	exit	退出VRF配置模式
步骤**6**	no containINTERFACE	将某个接口从VRF中删除
步骤**7**	no description	删除VRF的描述
步骤**8**	no vrf NAME	配置模式下将VRF删除

参数说明：

参数	说明
NAME	VRF的地址名称
LINE	VRF描述的内容
INTERFACE	物理接口的名称

第40章 配置沙箱

40.1 沙箱概述

全系统模拟的沙箱(Sandbox)技术可以更为有效地帮助企业防御 APT 攻击, 为一些不可靠的程序提供试验而不影响系统运行的环境有时也被称作沙盒。

40.2 沙箱配置

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	av sandbox enable/ disable	配置沙箱的启用状态
步骤**3**	av sandbox server-master A.B.C.D <1-65535>	配置沙箱的主服务器地址和端口
步骤**4**	av sandbox server-backup A.B.C.D <1-65535>	配置沙箱的备服务器地址和端口
步骤**5**	show av sandbox check result [<1-1000>]	查看沙箱的结果
步骤**6**	exit	退出沙箱配置模式

注意：在配置沙箱之前，需要先配置病毒防护策略和文件类型。

参数说明：

参数	说明
A．B．C．D	服务器的IP地址
<1-65535>	服务器的端口号
[<1-1000>]	指定显示沙箱的条目数

第41章 配置镜像功能

41.1 镜像功能概述

镜像功能包括端口镜像功能、流镜像功能。

端口镜像功能是设备把某一个端口接收或发送的数据帧完全相同的复制给另一个端口；其中被复制的端口称为镜像源端口，复制的端口称为镜像目的端口。通常在镜像目的端口处连接一个协议分析仪（如 Sniffer 或其他抓包分析工具）或者旁挂设备，就可以监视和管理网络，并且能诊断网络故障。

41.2 配置端口镜像功能

41.2.1 配置启用端口镜像

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	monitor session NAME IFNAME to IFNAMEboth|rx|tx	指定端口镜像的源端口、目的端口以及镜像数据帧的范围(接收、发送或所有)

在 configure terminal 节点下使用 no monitor session NAME 可以删除某条端口镜像配置。

参数说明： **monitor session NAME IFNAME to IFNAMEboth|rx|tx**

参数	说明	缺省配置
NAME	端口镜像配置的名称	无
IFNAME	镜像源端口或目的端口的名称	无
both|rx|tx	镜像数据帧的范围(接收、发送或所有)	无

第42章 配置源进源出功能

42.1 源进源出功能概述

源进源出功能保证报文能够按原接口返回，即数据往返路径一致。

42.2 配置源进源出功能

42.2.1 源进源出功能启用

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	session_path consist	开启源进源出功能

在 configure terminal 节点下使用 no session_path consist 可关闭源进源出功能。

第43章 配置威胁情报

43.1 威胁情报概述

威胁情报也称协同防御，本质是安全共同体内成员共享一份黑名单，可以阻断恶意的 IP、域名和 URL，对比防火墙的黑名单功能，威胁情报着重检测对已知恶意目标的访问。相较于 WebUI，命令行支持根据关键字检索转发表、清除转发表，不支持配置威胁情报条目。

43.2 配置威胁情报功能

43.2.1 配置威胁情报功能

配置步骤

步骤**1**	configure terminal	进入配置模式
步骤**2**	cooperative defense （all | ip | domain | url ） (enable | disable)	全部或单独启用 | 禁用威胁情报功能
步骤**3**	cooperative defense reliable log (enable | disable) <1-100> deny (enable | disable) <1-100>	配置动作和阈值，可以启用|禁用记录日志并设置阈值，启用|禁用阻断功能并设置阈值
步骤**4**	cooperative defense level *CMD_GROUP_LEVEL* *CMD_GROUP_LEVEL* *CMD_GROUP_LEVEL*	设置威胁级别对应日志的三种级别，从前往后是高、中、低对应的日志级别,具体见参数说明
步骤**5**	show cooperative defense （<cr> | ip | domain | url | source）	展示威胁情报功能使能状态
步骤**6**	show cooperative (domain | ip | url) (<cr> | [NAME])	根据关键字检索转发表条目

参数说明：cooperative defense （all \| ip \| domain \| url ） (enable \| disable)

参数	说明	缺省配置
all | ip | domain | *url*	选择威胁情报功能	All
enable | disable	启用禁用	无

参数说明：cooperative defense reliable log (enable | disable) <1-100> deny (enable | disable) <1-100>

参数	说明	缺省配置
*enable	disable*	启用禁用记录日志	无
<1-100>	日志级阈值	无
enable	disable	启用禁用阻断功能	无
<1-100>	阻断级阈值	无

参数说明：cooperative defense level **CMD_GROUP_LEVEL CMD_GROUP_LEVEL CMD_GROUP_LEVEL**

参数	说明	缺省配置
CMD_GROUP_LEVEL *CMD_GROUP_LEVEL* *CMD_GROUP_LEVEL*	从前往后是高、中、低分别对应的日志等级 alerts 紧急 critical 告警 emergencies 严重 errors 错误 informational 警示 notifications 通知 warnings 信息	无

参数说明：show cooperative defense （<cr>|ip|domain|url|source）

参数	说明	缺省配置
<cr>|ip|domain|url|source	展示威胁情报使能状态，分别是 ： 所有、ip、域名、url、来源统计共五种。	所有

参数说明：show cooperative (domain | ip | url) (<cr> | [NAME])

参数	说明	缺省配置
domain	ip	url	选择检索类型	无
NAME	关键字	无关键字

43.3 配置案例

案例描述

启用所有威胁情报功能并查看状态，包括 IP、域名、url。

配置步骤

步骤1	进入congfig模式
	DCFW-1800#configure terminal
步骤2	启用所有威胁情报功能
	DCFW-1800(config)# cooperative defense all enable
步骤3	在特权模式Show 威胁情报功能状态
	DCFW-1800(config)#exit
	DCFW-1800# show cooperative defense