

## 第一阶段-RS 评分标准

1. DCRS 开启 telnet 登录功能，用户名 dcn01，密码 dcn01，配置使用 telnet 方式登录终端界面前显示如下授权信息：“WARNING!!!  
Authorised access only, all of your done will be recorded!  
Disconnected IMMEDIATELY if you are not an authorised user!  
Otherwise, we retain the right to pursue the legal  
responsibility”。

共 8 分，telnet 登录提示 banner 且登录成功得分。

```
DCRS#telnet 127.0.0.1
Connecting Host 127.0.0.1 Port 23...
Service port is 23
Connected to 127.0.0.1
WARNING!!! Authorised access only, all of your done will be recorded! Disconnected IMMEDIATELY if you are not an authorised user! Otherwise, we re
tain the right to pursue the legal responsibility
login:dcn01
Password:*****Jun 12 10:22:58:000 2021 DCRS MODULE_UTILS_TELNET/5/:Telnet: User dcn01 login successfully from 127.0.0.1:32884.
```

2. 总部部署了一套网管系统实现对核心 DCRS 进行管理，网管系统 IP 为：10.52.0.100，读团体值为：DCN2021，版本为 V2C，DCRS Trap 信息实时上报网管，当 MAC 地址发生变化时，也要立即通知网管发生的变化，每 35s 发送一次；DCRS 出口往返流量发送给 DCBI，由 DCBI 对收到的数据进行用户所要求的分析；
- 共 8 分，共 3 处。

1. 3 分，完全一致得分，否则不得分

```
DCRS#show snmp status
System Name : DC YunKe Networks Co.,Ltd.
System Contact : 400-810-9119
System Location : China
Trap enable
RMON enable
Community Information:
V1/V2c Trap Host Information:
    Trap-rec-address: 10.52.0.100
    Host Version:V2
    Community string: DCN2021
V3 Trap Host Information:
Security IP is Enabled.
```

2. 3 分，完全一致得分，否则不得分

```
DCRS#show mac-notification summary
MAC address notification:enabled
MAC address snmp traps:enabled
MAC address notification interval = 35
MAC address notification history log size = 10
MAC address added = 0
MAC address removed = 0
MAC address moved = 0
MAC address snmp traps generated = 0
DCRS#
```

3. 2 分，完全一致得分，否则不得分

```
DCWS#show monitor
monitor session 1:
source ports:
RX port: 20
TX port: 20
Flow monitor source:
Destination Ethernet1/0/10, tunnel VID 0 desMAC 00-00-00-00-00-00 desIP 0.0.0.0 srcIP 0.0.0.0
-----
No monitor in session 2
-----
No monitor in session 3
-----
No monitor in session 4
-----
```

3. 对 DCRS 上 VLAN40 开启以下安全机制：

业务内部终端相互二层隔离，启用环路检测，环路检测的时间间隔为 10s，发现环路以后关闭该端口，恢复时间为 30 分钟；如发现私设 DHCP 服务器则关闭该端口，配置防止 ARP 欺骗攻击；  
共 8 分，共 3 处。

1.2 分，完全一致得分，否则不得分

```
DCRS#show isolate-port group
vlan 40 :Isolate-port group vlan40
The isolate-port Ethernet1/0/8
The isolate-port Ethernet1/0/7
The isolate-port Ethernet1/0/6
The isolate-port Ethernet1/0/5
The isolate-port Ethernet1/0/4
```

2.3 分，完全一致得分，否则不得分

```
DCRS#show loopback-detection
Loopback Detection Global Information
Transmit Interval : 10s(loopback mode), 10s(no loopback mode)
Control Recover Time : 1800
Loopback Detection Port Information
PortName      Loopback Detection      Control Mode      Is Controlled      Happen times
Ethernet1/0/1  Disable                 No                No                0
Ethernet1/0/2  Disable                 No                No                0
Ethernet1/0/3  Disable                 No                No                0
Ethernet1/0/4  Enable                  Shutdown          No                0
Ethernet1/0/5  Enable                  Shutdown          No                0
Ethernet1/0/6  Enable                  Shutdown          No                0
Ethernet1/0/7  Enable                  Shutdown          No                0
Ethernet1/0/8  Enable                  Shutdown          No                0
Ethernet1/0/9  Disable                 No                No                0
Ethernet1/0/10 Disable                 No                No                0
Ethernet1/0/11 Disable                 No                No                0
Ethernet1/0/12 Disable                 No                No                0
Ethernet1/0/13 Disable                 No                No                0
Ethernet1/0/14 Disable                 No                No                0
Ethernet1/0/15 Disable                 No                No                0
Ethernet1/0/16 Disable                 No                No                0
Ethernet1/0/17 Disable                 No                No                0
Ethernet1/0/18 Disable                 No                No                0
Ethernet1/0/19 Disable                 No                No                0
Ethernet1/0/20 Disable                 No                No                0
Ethernet1/0/21 Disable                 No                No                0
Ethernet1/0/22 Disable                 No                No                0
Ethernet1/0/23 Disable                 No                No                0
Ethernet1/0/24 Disable                 No                No                0
Ethernet1/0/25 Disable                 No                No                0
Ethernet1/0/26 Disable                 No                No                0
Ethernet1/0/27 Disable                 No                No                0
Ethernet1/0/28 Disable                 No                No                0
```

3.3 分, 完全一致得分, 否则不得分

```
DCRS#show ip dhcp snooping
```

DHCP Snooping is enabled

DHCP Snooping binding arp: disabled  
DHCP Snooping maxnum of action info:10  
DHCP Snooping switch ID 00-03-0f-dc-fe-78  
DHCP Snooping dropped packets 0, discarded packets 0  
DHCP Snooping alarm count 0, binding count 0,  
static binding count 0, from shell 0, from server 0  
expired binding 0, request binding 0

| interface      | trust   | action   | recovery | alarm num | bind num |
|----------------|---------|----------|----------|-----------|----------|
| Ethernet1/0/1  | untrust | none     | 0        | 0         | 0        |
| Ethernet1/0/2  | untrust | none     | 0        | 0         | 0        |
| Ethernet1/0/3  | untrust | none     | 0        | 0         | 0        |
| Ethernet1/0/4  | untrust | shutdown | 0        | 0         | 0        |
| Ethernet1/0/5  | untrust | shutdown | 0        | 0         | 0        |
| Ethernet1/0/6  | untrust | shutdown | 0        | 0         | 0        |
| Ethernet1/0/7  | untrust | shutdown | 0        | 0         | 0        |
| Ethernet1/0/8  | untrust | shutdown | 0        | 0         | 0        |
| Ethernet1/0/9  | untrust | none     | 0        | 0         | 0        |
| Ethernet1/0/10 | untrust | none     | 0        | 0         | 0        |
| Ethernet1/0/11 | untrust | none     | 0        | 0         | 0        |
| Ethernet1/0/12 | untrust | none     | 0        | 0         | 0        |
| Ethernet1/0/13 | untrust | none     | 0        | 0         | 0        |
| Ethernet1/0/14 | untrust | none     | 0        | 0         | 0        |
| Ethernet1/0/15 | untrust | none     | 0        | 0         | 0        |
| Ethernet1/0/16 | untrust | none     | 0        | 0         | 0        |
| Ethernet1/0/17 | untrust | none     | 0        | 0         | 0        |
| Ethernet1/0/18 | untrust | none     | 0        | 0         | 0        |
| Ethernet1/0/19 | untrust | none     | 0        | 0         | 0        |
| Ethernet1/0/20 | trust   | none     | 0        | 0         | 0        |
| Ethernet1/0/21 | untrust | none     | 0        | 0         | 0        |
| Ethernet1/0/22 | untrust | none     | 0        | 0         | 0        |
| Ethernet1/0/23 | untrust | none     | 0        | 0         | 0        |
| Ethernet1/0/24 | untrust | none     | 0        | 0         | 0        |
| Ethernet1/0/25 | untrust | none     | 0        | 0         | 0        |

4. DCWS 配置 IPv6 地址，使用相关特性实现 VLAN50 的 IPv6 终端可自动从网关处获得 IPv6 有状态地址。

DCRS 配置 IPv6 地址，开启路由公告功能，路由器公告的生存期为 2 小时，确保 VLAN30 的 IPv6 终端可以获得 IPv6 无状态地址。DCWS 与 DCRS 之间配置 RIPng，使 PC1 与 PC3 可以通过 IPv6 通信共 12 分，共 4 处。

1. 3 分，ipv6 地址和默认网关 2001:50:: 开头可得分

PC3:

```
以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . : 
    IPv6 地址 . . . . . : 2001:50::1
    本地链接 IPv6 地址 . . . . . : fe80::35b6:af10:ae1e:bf91%11
    自动配置 IPv4 地址 . . . . . : 169.254.191.145
    子网掩码 . . . . . : 255.255.0.0
    默认网关. . . . . : 2001:50::254
```

2. 3 分

PC1: ipv6 地址为 2001:30::+EUI64，默认网关以 FE80 本地链路地址开头，可得分。

```
以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . : 
    IPv6 地址 . . . . . : 2001:30::89a5:9b76:f3a7:be01
    临时 IPv6 地址 . . . . . : 2001:30::6dde:de90:e93:ad2f
    本地链接 IPv6 地址 . . . . . : fe80::89a5:9b76:f3a7:be01%11
    IPv4 地址 . . . . . : 172.16.40.1
    子网掩码 . . . . . : 255.255.255.192
    默认网关. . . . . : fe80::203:fff:fe90:23b7%11
                        172.16.40.62

隧道适配器 isatap.{543C27D0-FFA8-4F61-9345-D361EA52E268}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :
```

3.3分，显示R和ipv6网段可得分，网段可以不一致

```
DCRS#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - IS-IS, B - BGP
Timers: Uptime
C   ::1/128 via ::, Loopback, 01:13:00 tag:0
C   2001:30::/64 via ::, Vlan30, 00:24:02 tag:0
R   2001:50::/64 [120/2] via fe80::203:fff:fe90:14a1, Vlan100, 00:04:17 tag:0
C   2001:100::/64 via ::, Vlan100, 00:24:02 tag:0
```

4.3分

PC1 ping PC3: ping 通可得分，地址参考 1，2ipv6 地址

```
C:\Users\Administrator>ping 2001:50::1

正在 Ping 2001:50::1 具有 32 字节的数据:
来自 2001:50::1 的回复: 时间<1ms
来自 2001:50::1 的回复: 时间<1ms
来自 2001:50::1 的回复: 时间<1ms
来自 2001:50::1 的回复: 时间<1ms

2001:50::1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间<以毫秒为单位>:
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

5. 尽可能加大 DCWS 与防火墙 DCFW 之间的带宽;

配置使总部 VLAN40 业务的用户访问 IDC SERVER 的数据流经过 DCFW 10.1.0.254, IDC SERVER 返回数据流经过 DCFW10.2.0.254, 且对双向数据流开启所有安全防护, 参数和行为为默认;  
共 12 分, 共 3 处。

1.5 分, 完全一致得分, 否则不得分

```
DCFw# show lacp aggregate1
```

```
=====
Flags:  A -- LACP_ACTIVITY, B -- LACP_TIMEOUT, C -- AGGREGATION,
        D -- SYNCHRONIZATION, E -- COLLECTING, F -- DISTRIBUTING,
        G -- DEFAULTED, H -- EXPIRED
*****
state: lacp enable
port_num:2 active_num:2 select_num:2 min_bundle:1 max_bundle:16
load balance: flow
local --> system id:32768, 0003.0f80.c88d oper-key:0x11
remote --> system id:32768, 0003.0f90.14a2 oper-key:0x1
-----
member 1: ethernet0/1
speed:1000 duplex:full link state:up
status: active
send lacp packet:134 recv lacp packet:134
local --> id:38 priority:32768 oper-key:0x0011 Flags:ACDEF
remote --> id:1 priority:32768 oper-key:0x0001 Flags:ACDEF
-----
member 2: ethernet0/2
speed:1000 duplex:full link state:up
status: active
send lacp packet:134 recv lacp packet:135
local --> id:39 priority:32768 oper-key:0x0011 Flags:ACDEF
remote --> id:2 priority:32768 oper-key:0x0001 Flags:ACDEF
=====
```

2.2 分，完全一致得 2 分。

```
DCFw(config)# show ad zone trust configuration
```

The configuration on zone trust:  
ad enable

| Attack defense type   | threshold | action | status |
|-----------------------|-----------|--------|--------|
| Tear Drop             |           | drop   | on     |
| IP Spoofing           |           | drop   | on     |
| Land Attack           |           | drop   | on     |
| IP Option             |           | drop   | on     |
| IP Fragment           |           | drop   | on     |
| ip directed broadcast |           | drop   | on     |
| Winnuke               |           | drop   | on     |
| Port Scan             | 1         | drop   | on     |
| TCP Anomaly           |           | drop   | on     |
| ICMP Flood            | 1500      | drop   | on     |
| Address Sweep         | 1         | drop   | on     |
| Ping of Death         |           | drop   | on     |
| Huge ICMP Packet      | 1024      | drop   | on     |

|                     |   |      |  |  |    |
|---------------------|---|------|--|--|----|
| ARP spoofing        |   |      |  |  |    |
| reverse-query       |   |      |  |  | on |
| gratuitous arp rate | 0 |      |  |  | on |
| ip-number-per-mac   | 0 | drop |  |  | on |

|                           | src_thres | dst_thres | action | status |
|---------------------------|-----------|-----------|--------|--------|
| UDP Flood                 | 1500      | 1500      | drop   | on     |
| dns query flood           | 1500      | 1500      | drop   | on     |
| dns recursive query flood | 1000      | 1000      | drop   | on     |

| SYN Flood | src_thres | dst_thres_ip | dst_thres_port | action | status |
|-----------|-----------|--------------|----------------|--------|--------|
|           | 1500      | 1500         | 1500           | drop   | on     |

destination: ip-based

|            | min_rate | max_rate | timeout | action | status |
|------------|----------|----------|---------|--------|--------|
| SYN Proxy  | 1000     | 3000     | 30      | drop   | on     |
| SYN Cookie | 1000     | 3000     | 30      | drop   | on     |

3.5 分

用任意 PC 模拟 IDC SERVER, 使用 VLAN 40 PC2 tracert 10.100.18.2,

完全一致得分，否则不得分

```
C:\Users>tracert 10.100.18.2
```

通过最多 30 个跃点跟踪到 10.100.18.2 的路由

|   |       |       |       |              |
|---|-------|-------|-------|--------------|
| 1 | 1 ms  | <1 毫秒 | <1 毫秒 | 172.16.40.62 |
| 2 | <1 毫秒 | <1 毫秒 | <1 毫秒 | 10.2.0.254   |
| 3 | 1 ms  | 1 ms  | 1 ms  | 10.100.18.2  |



6. DCFW、DCRS、DCWS 之间配置 OSPF area 0 开启基于链路的 MD5 认证，密钥自定义，传播访问 INTERNET 默认路由；  
共 8 分，共 5 处。

1，2，3，4 处各 1 分；

```
DCWS#show run | begin interface Vlan113
interface Vlan113
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 0 test
ip address 10.3.0.253 255.255.255.252
!
interface Vlan114
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 0 test
ip address 10.4.0.253 255.255.255.252
!
interface Vlan115
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 0 test
ip address 10.5.0.254 255.255.255.252
!
interface Vlan116
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 0 test
ip address 10.6.0.254 255.255.255.252
```

6.4 分，完全一致得分，否则不得分

```
DCWS#sh ip route ospf
O*E2    0.0.0.0/0 [110/1] via 10.3.0.254, Vlan113, 00:00:20 tag:0
O       172.16.30.0/26 [110/2] via 10.5.0.253, Vlan115, 00:00:21 tag:0
O       172.16.40.0/26 [110/2] via 10.5.0.253, Vlan115, 00:00:21 tag:0
Total routes are : 3 item(s)
```

7. DCFW 与 DCRS 建立两对 IBGP 邻居关系，使用 AS 65500，DCFW 上 loopback1-4 为模拟 AS 65500 中网络，为保证数据通信的可靠性和负载，完成以下配置，要求如下：

- DCRS 通过 BGP 到达 loopback1, 2 网路下一跳为 10. 3. 0. 254;  
DCRS 通过 BGP 到达 loopback3, 4 网络下一跳为 10. 4. 0. 254;
- 通过 BGP 实现到达 loopback1, 2, 3, 4 的网络冗余;
- 使用 IP 前缀列表匹配上述业务数据流;
- 使用 LP 属性进行业务选路，只允许使用 route-map 来改变 LP 属性、实现路由控制，LP 属性可配置的参数数值为：200

共 12 分，路由全部正确得 12 分，完全一致得分，否则不得分

```
DCRS#sh ip bgp
BGP table version is 55, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop           Metric LocPrf Weight Path
* > i 10.11.0.0/24  10.3.0.254          0      100      0 i
* > i               10.4.0.254          0      100      0 i
* > i 10.12.0.0/24  10.3.0.254          0      100      0 i
* > i               10.4.0.254          0      100      0 i
* > i 10.13.0.0/24  10.3.0.254          0      100      0 i
* > i               10.4.0.254          0      200      0 i
* > i 10.14.0.0/24  10.3.0.254          0      100      0 i
* > i               10.4.0.254          0      200      0 i

Total number of prefixes 4
```

8. 如果 DCRS E0/3 端口的收包速率超过 30000 则关闭此端口，恢复时间 5 分钟，并每隔 10 分钟对端口的速率进行统计；为了更好地提高数据转发的性能，DCRS 交换中的数据包大小指定为 1600 字节；共 8 分，共 3 处。

1. 4 分，完全一致得分，否则不得分

```
DCRS#sh run int e1/0/3
!
Interface Ethernet1/0/3
rate-violation all 30000
rate-violation control shutdown
switchport access vlan 30
!
```

2, 3 处各 2 分，完全一致得分，否则不得分

```
DCRS(config)#show int e1/0/3
Interface brief:
 Ethernet1/0/3 is down, line protocol is down
 Ethernet1/0/3 is layer 2 port, alias name is (null), index is 3
 Hardware is Gigabit-TX, address is 00-03-0f-dc-ef-7b
 PVID is 30
 MTU 1600 bytes BW 10000 Kbit
 Time since last status change:0w-0d-6h-3m-44s (21824 seconds)
 Encapsulation ARPA, Loopback not set
 Auto-duplex, Auto-speed
 FlowControl is off, MDI type is auto
Statistics:
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 The last 5 second input rate 0 bits/sec, 0 packets/sec
 The last 5 second output rate 0 bits/sec, 0 packets/sec
 The last 600 second input rate 0 bits/sec, 0 packets/sec
 The last 600 second output rate 0 bits/sec, 0 packets/sec
Input packets statistics:
 0 input packets, 0 bytes, 0 no buffer
 0 unicast packets, 0 multicast packets, 0 broadcast packets
 0 input errors, 0 CRC, 0 frame alignment, 0 overrun, 0 ignored,
 0 abort, 0 length error, 0 undersize 0 jabber, 0 fragments, 0 pause frame
Output packets statistics:
```