目 录

1 Portal

1.1 Portal配置命令

1.1.1 captive-bypass enable

captive-bypass enable 命令用来开启 Portal 被动 Web 认证功能。

undo captive-bypass enable 命令用来关闭 Portal 被动 Web 认证功能。

【命令】

captive-bypass enable

undo captive-bypass enable

【缺省情况】

Portal 被动 Web 认证功能处于关闭状态，即 iOS 系统和部分 Android 系统的用户接入已开启 Portal 认证的网络后会自动弹出 Portal 认证页面。

【视图】

Portal Web 服务器视图

【缺省用户角色】

network-admin

【使用指导】

iOS 系统或者部分 Android 系统的用户接入已开启 Portal 认证的网络后，设备会主动向这类用户终端推送 Portal 认证页面。开启 Portal 被动 Web 认证功能后，仅在这类用户使用浏览器访问 Internet 时，设备才会为其推送 Portal 认证页面。

【举例】

开启 Portal 被动 Web 认证功能。

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] captive-bypass enable
```

【相关命令】

- **display portal web-server**

1.1.2 default-logon-page

default-logon-page 命令用来配置本地 Portal Web 服务提供的缺省认证页面文件。

undo default-logon-page 命令用来恢复缺省情况。

【命令】

default-logon-page *file-name*

undo default-logon-page

【缺省情况】

本地 Portal Web 服务未提供缺省认证页面文件。

【视图】

本地 Portal Web 服务视图

【缺省用户角色】

network-admin

【参数】

file-name：表示缺省认证页面文件名（不包括文件的保存路径），为 1～91 个字符的字符串，包括字母、数字、点和下划线。

【使用指导】

指定的缺省认证页面文件由用户编辑，并将其打包成 zip 格式文件后上传到设备存储介质的根目录下。配置 **default-logon-page** 命令后设备会将指定的压缩文件进行解压缩，并设置为本地 Portal Web 服务为用户进行 Portal 认证提供的缺省认证页面文件。如果没有配置 **default-logon-page** 命令，则设备中就不存在为用户进行 Portal 认证的缺省认证页面文件，进而，用户无法进行正常的本地 Portal 认证。

【举例】

配置本地 Portal Web 服务器提供的缺省认证页面文件为 pagefile1.zip。

```
<Sysname> system-view
[Sysname] portal local-web-server http
[Sysname-portal-local-websvr-http] default-logon-page pagefile1.zip
```

【相关命令】

- **portal local-web-server**

1.1.3 display portal

display portal 命令用来显示 Portal 配置信息和 Portal 运行状态信息。

【命令】

display portal interface *interface-type interface-number*

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

interface *interface-type interface-number*：表示接口类型和接口编号。

【举例】

显示接口 Vlan-interface2 的 Portal 配置信息和 Portal 运行状态信息。

```
<Sysname> display portal interface vlan-interface 2
```

```
Portal information of Vlan-interface2
    NAS-ID profile: aaa
    Authorization : Strict checking
    ACL           : Enabled
    User profile  : Disabled
IPv4:
    Portal status: Enabled
    Portal authentication method: Direct
    Portal web server: wbs
    Portal mac-trigger-server: Not configured
    Authentication domain: my-domain
    User-dhcp-only: Enabled
    Pre-auth IP pool: ab
    Max Portal users: Not configured
    Bas-ip: Not configured
    User detection: Type: ICMP  Interval: 300s  Attempts: 5   Idle time: 180s
    Action for server detection:
        Server type    Server name                      Action
        Web server     wbs                              fail-permit
        Portal server  pts                              fail-permit
    Layer3 source network:
        IP address              Mask
        1.1.1.1                 255.255.0.0

    Destination authentication subnet:
        IP address              Mask
        2.2.2.2                 255.255.255.0

IPv6:
    portal status: Disabled
    Portal authentication method: Disabled
    Portal web server: Not configured
    Portal mac-trigger-server: Not configured
    Authentication domain: Not configured
    User-dhcp-only: Disabled
    Pre-auth IP pool: Not configured
    Max Portal users: Not configured
    Bas-ipv6:Not configured
    User detection: Not configured
    Action for server detection:
        Server type    Server name                      Action
        --             --                               --
    Layer3 source network:
        IP address                                      Prefix length

    Destination authentication subnet:
        IP address                                      Prefix length
```

表1-1 display portal interface 命令显示信息描述表

字段	描述
Portal information of interface	接口上的Portal信息
NAS-ID profile	接口上引用的NAS-ID profile
Authorization	服务器下发给Portal用户的授权信息类型，包括ACL和User profile
Strict checking	Portal授权信息的严格检查模式是否开启
IPv4	IPv4 Portal的相关信息
IPv6	IPv6 Portal的相关信息
Portal status	接口上Portal认证的运行状态，包括以下取值： • Disabled：Portal 认证未开启 • Enabled：Portal 认证已开启 • Authorized：Portal 认证服务器或者 Portal Web 服务器不可达，端口自动开放
Portal authentication method	接口上配置的认证方式，包括以下取值： • Direct：直接认证方式 • Redhcp：二次地址分配认证方式 • Layer3：可跨三层认证方式
Portal Web server	接口上配置的Portal Web服务器的名称
Portal mac-trigger-server	（暂不支持）接口上配置MAC绑定服务器的名称
Authentication domain	接口上的Portal强制认证域
User-dhcp-only	仅允许通过DHCP方式获取IP地址的客户端上线功能 • Enabled：仅允许通过 DHCP 方式获取 IP 地址的客户端上线功能处于开启状态，表示仅允许通过 DHCP 方式获取 IP 地址的客户端上线 • Disabled：仅允许通过 DHCP 方式获取 IP 地址的客户端上线功能处于关闭状态，表示通过 DHCP 方式获取 IP 地址的客户端和静态配置 IP 地址的客户端都可以上线
Pre-auth ip-pool	为认证前的Portal用户指定的IP地址池名称
Max Portal users	接口上配置的最大用户数
Bas-ip	发送给Portal认证服务器的Portal报文的BAS-IP属性
Bas-ipv6	发送给Portal认证服务器的Portal报文的BAS-IPv6属性
User detection	接口上配置的用户在线状态探测配置，包括探测的方法（ARP、ICMP、ND、ICMPv6），探测周期和探测尝试次数，用户闲置的时间
Action for server detection	服务器可达性探测功能对应的端口控制配置： • Server type：服务器类型，包括 Portal server 和 Web server，分别表示 Portal 认证服务器和 Portal Web 服务器 • Server name：服务器名称 • Action：对应的接口根据服务器探测结果所采取的动作，为不需要认证（fail-permit）

字段	描述
Layer3 source subnet	Portal源认证网段信息
Destination authentication subnet	Portal目的认证网段认证信息
IP address	Portal认证网段的IP地址
Mask	Portal认证网段的子网掩码
Prefix length	Portal IPv6认证网段的地址前缀长度

【相关命令】

- **portal domain**
- **portal enable**
- **portal free-all except destination**
- **portal ipv6 free-all except destination**
- **portal ipv6 layer3 source**
- **portal layer3 source**
- **portal web-server**

1.1.4 display portal packet statistics

display portal packet statistics 命令用来显示 Portal 认证服务器的报文统计信息。

【命令】

display portal packet statistics [**server** *server-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

server *server-name*：Portal 认证服务器的名称，为 1～32 个字符的字符串，区分大小写。

【使用指导】

执行此命令后，显示的报文统计信息包括设备接收到 Portal 认证服务器发送的报文以及设备发送给该 Portal 认证服务器的报文的信息。

若不指定参数 **server**，则依次显示所有 Portal 认证服务器的报文统计信息。

【举例】

显示名称为 pts 的 Portal 认证服务器的报文统计信息。

```
<Sysname> display portal packet statistics server pts
 Portal server :  pts
 Invalid packets: 0
```

```
Pkt-Type                        Total    Drops    Errors
REQ_CHALLENGE                   3        0        0
ACK_CHALLENGE                   3        0        0
REQ_AUTH                        3        0        0
ACK_AUTH                        3        0        0
REQ_LOGOUT                      1        0        0
ACK_LOGOUT                      1        0        0
AFF_ACK_AUTH                    3        0        0
NTF_LOGOUT                      1        0        0
REQ_INFO                        6        0        0
ACK_INFO                        6        0        0
NTF_USERDISCOVER                0        0        0
NTF_USERIPCHANGE                0        0        0
AFF_NTF_USERIPCHAN              0        0        0
ACK_NTF_LOGOUT                  1        0        0
NTF_HEARTBEAT                   0        0        0
NTF_USER_HEARTBEAT              2        0        0
ACK_NTF_USER_HEARTBEAT          0        0        0
NTF_CHALLENGE                   0        0        0
NTF_USER_NOTIFY                 0        0        0
AFF_NTF_USER_NOTIFY             0        0        0
```

表1-2 display portal server statistics 命令显示信息描述表

字段	描述
Portal server	Portal认证服务器名称
Invalid packets	无效报文的数目
Pkt-Type	报文的名称
Total	报文的总数
Drops	丢弃报文数
Errors	携带错误信息的报文数
REQ_CHALLENGE	Portal认证服务器向接入设备发送的challenge请求报文
ACK_CHALLENGE	接入设备对Portal认证服务器challenge请求的响应报文
REQ_AUTH	Portal认证服务器向接入设备发送的请求认证报文
ACK_AUTH	接入设备对Portal认证服务器认证请求的响应报文
REQ_LOGOUT	Portal认证服务器向接入设备发送的下线请求报文
ACK_LOGOUT	接入设备对Portal认证服务器下线请求的响应报文
AFF_ACK_AUTH	Portal认证服务器收到认证成功响应报文后向接入设备发送的确认报文
NTF_LOGOUT	接入设备发送给Portal认证服务器，用户被强制下线的通知报文
REQ_INFO	信息询问报文
ACK_INFO	信息询问的响应报文
NTF_USERDISCOVER	Portal认证服务器向接入设备发送的发现新用户要求上线的通知报文

字段	描述
NTF_USERIPCHANGE	接入设备向Portal认证服务器发送的通知更改某个用户IP地址的通知报文
AFF_NTF_USERIPCHAN	Portal认证服务器通知接入设备对用户表项的IP切换已成功报文
ACK_NTF_LOGOUT	Portal认证服务器对强制下线通知的响应报文
NTF_HEARTBEAT	Portal认证服务器周期性向接入设备发送的服务器心跳报文
NTF_USER_HEARTBEAT	接入设备收到的从Portal认证服务器发送的用户同步报文
ACK_NTF_USER_HEARTBEAT	接入设备向Portal认证服务器回应的用户同步响应报文
NTF_CHALLENGE	接入设备向Portal认证服务器发送的challenge请求报文
NTF_USER_NOTIFY	接入设备向Portal认证服务器发送的用户消息通知报文
AFF_NTF_USER_NOTIFY	Portal认证服务器向接入设备发送的对NTF_USER_NOTIFY的确认报文

【相关命令】

- **reset portal packet statistics**

1.1.5 display portal rule

display portal rule 命令用来显示用于报文匹配的 Portal 过滤规则信息。

【命令】

display portal rule { **all** | **dynamic** | **static** } **interface** *interface-type interface-number* [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

all：显示所有 Portal 规则信息，包括动态 Portal 规则和静态 Portal 规则。

dynamic：显示动态 Portal 规则信息，即用户通过 Portal 认证后设备上产生的 Portal 规则，这类规则定义了允许指定源 IP 地址的报文通过接口。

static：显示静态 Portal 规则信息，即开启 Portal 后产生的 Portal 规则，这类规则定义了在 Portal 功能开启后对接口上收到的报文的过滤动作。

interface *interface-type interface-number*：显示指定接口的 Portal 规则信息。*interface-type interface-number* 为接口类型和接口编号。

slot *slot-number*：显示指定成员设备上的 Portal 规则信息。*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则表示所有成员设备上的 Portal 过滤规则信息。

【举例】

显示接口 Vlan-interface100 上所有 Portal 过滤规则的信息。

```
<Sysname> display portal rule all interface vlan-interface 100 slot 1
Slot 1:
IPv4 portal rules on Vlan-interface100:
Rule 1
 Type                : Static
 Action              : Permit
 Protocol            : Any
 Status              : Active
 Source:
    IP             : 0.0.0.0
    Mask           : 0.0.0.0
    Port           : Any
    MAC            : 0000-0000-0000
    Interface      : Vlan-interface100
    VLAN           : 100
 Destination:
    IP             : 192.168.0.111
    Mask           : 255.255.255.255
    Port           : Any

Rule 2
 Type                : Dynamic
 Action              : Permit
 Status              : Active
 Source:
    IP             : 2.2.2.2
    MAC            : 000d-88f8-0eab
    Interface      : Vlan-interface100
    VLAN           : 100
 Author ACL:
    Number         : 3001

Rule 3
 Type                : Static
 Action              : Redirect
 Status              : Active
 Source:
    IP             : 0.0.0.0
    Mask           : 0.0.0.0
    Interface      : Vlan-interface100
    VLAN           : 100
    Protocol       : TCP
 Destination:
    IP             : 0.0.0.0
    Mask           : 0.0.0.0
    Port           : 80

Rule 4:
```

```
 Type                : Static
 Action              : Deny
 Status              : Active
 Source:
    IP             : 0.0.0.0
    Mask           : 0.0.0.0
    Interface      : Vlan-interface100
    VLAN           : Any
 Destination:
    IP             : 0.0.0.0
    Mask           : 0.0.0.0

IPv6 portal rules on Vlan-interface100:
Rule 1
 Type                : Static
 Action              : Permit
 Protocol            : Any
 Status              : Active
 Source:
    IP              : ::
    Prefix length   : 0
    Port            : Any
    MAC             : 0000-0000-0000
    Interface       : Vlan-interface100
    VLAN            : 100
 Destination:
    IP               : 3000::1
    Prefix length    : 64
    Port             : Any

Rule 2
 Type                : Dynamic
 Action              : Permit
 Status              : Active
 Source:
    IP              : 3000::1
    MAC             : 0015-e9a6-7cfe
    Interface       : Vlan-interface100
    VLAN            : 100
 Author ACL:
    Number          : 3001

Rule 3
 Type                : Static
 Action              : Redirect
 Status              : Active
 Source:
    IP              : ::
```

```
    Prefix length   : 0
    Interface       : Vlan-interface100
    VLAN            : 100
    Protocol        : TCP
 Destination:
    IP              : ::
    Prefix length   : 0
    Port            : 80

Rule 4:
 Type               : Static
 Action             : Deny
 Status             : Active
 Source:
    IP             : ::
    Prefix length  : 0
    Interface      : Vlan-interface100
    VLAN           : 100
 Destination:
    IP             : ::
    Prefix length  : 0
Author ACL:
    Number          : 3001
```

表1-3 display portal rule 命令显示信息描述表

字段	描述
Rule	Portal过滤规则编号。IPv4过滤规则和IPv6过滤规则分别编号
Type	Portal过滤规则的类型，包括以下取值： • Static：静态类型 • Dynamic：动态类型
Action	Portal过滤规则的匹配动作，包括以下取值： • Permit：允许报文通过 • Redirect：重定向报文 • Deny：拒绝报文通过
Protocol	Portal免认证规则中使用的传输层协议，包括以下取值： • Any：不限制传输层协议类型 • TCP：TCP 传输类型 • UDP：UDP 传输类型
Status	Portal过滤规则下发的状态，包括以下取值： • Active：表示规则已生效 • Unactuated：表示规则未生效
Source	Portal过滤规则的源信息
IP	源IP地址

字段	描述
Mask	源IPv4地址子网掩码
Prefix length	源IPv6地址前缀
Port	源传输层端口号
MAC	源MAC地址
Interface	Portal过滤规则应用的二层或三层接口
VLAN	源VLAN
Protocol	Portal重定向规则中使用的传输层协议类型，取值只能为TCP
Destination	Portal规则的目的信息
IP	目的IP地址
Port	目的传输层端口号
Mask	目的IPv4地址子网掩码
Prefix length	目的IPv6地址前缀
Author ACL	Portal用户认证后的授权ACL，即AAA授权给用户的ACL，该字段仅在Type为Dynamic时才显示
Number	授权ACL编号，N/A表示AAA未授权ACL

1.1.6 display portal server

display portal server 命令用来显示 Portal 认证服务器信息。

【命令】

display portal server [*server-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

server-name：Portal 认证服务器的名称，为 1～32 个字符的字符串，区分大小写。

【使用指导】

若不指定参数 *server-name*，则显示所有 Portal 认证服务器信息。

【举例】

显示 Portal 认证服务器 pts 的信息。

```
<Sysname> display portal server pts
Portal server: pts
```

```
Type                  : IMC
IP                    : 192.168.0.111
VPN instance          : Not configured
Port                  : 50100
Server detection      : Timeout 60s  Action: log
User synchronization  : Timeout 200s
Status                : Up
```

表1-4 display portal server 命令显示信息描述表

字段	描述
Type	Portal认证服务器类型，其取值如下： • CMCC：符合中国移动标准规范的服务器 • iMC：符合 iMC 标准规范的服务器
Portal server	Portal认证服务器名称
IP	Portal认证服务器的IP地址
VPN instance	Portal认证服务器所属的MPLS L3VPN实例
Port	Portal认证服务器的监听端口
Server detection	Portal认证服务器可达性探测功能的参数，包括超时时间（单位：秒），以及探测到服务器状态变化后触发的动作（log）
User synchronization	Portal用户用户信息同步功能的参数，包括超时时间（单位：秒）
Status	Portal认证服务器当前状态，其取值如下： • Up：服务器可达性探测功能未开启，或服务器可达性探测功能开启且探测结果为该服务器当前可达 • Down：服务器可达性探测功能已开启，探测结果为该服务器当前不可达

【相关命令】

- **portal enable**
- **portal server**
- **server-detect** (portal authentication server view)
- **user-sync**

1.1.7 display portal user

display portal user 命令用来显示 Portal 用户的信息。

【命令】

display portal user { **all** | **interface** *interface-type interface-number* | **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

all：显示所有 Portal 用户的信息。

interface *interface-type interface-number*：显示指定接口上的 Portal 用户信息。*interface-type interface-number* 为接口类型和接口编号。

ip *ipv4-address*：显示指定 IPv4 地址的 Portal 用户信息。

ipv6 *ipv6-address*：显示指定 IPv6 地址的 Portal 用户信息。

verbose：显示指定 Portal 用户的详细信息。

【举例】

显示所有 Portal 用户的信息。

```
<Sysname> display portal user all
Total portal users: 2
Username: abc
  Portal server: pts
  State: Online
  VPN instance: N/A
  MAC                IP                VLAN   Interface
  000d-88f8-0eab     2.2.2.2           100    Vlan-interface100
  Authorization information:
    DHCP IP pool: N/A
    User profile: abc （active）
    Session group profile: N/A
    ACL number: N/A
    Inbound CAR: N/A
    Outbound CAR: N/A

Username: def
  Portal server: pts
  State: Online
  VPN instance: N/A
  MAC                IP                VLAN   Interface
  000d-88f8-0eac     3.3.3.3           200    Vlan-interface200
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
    ACL number: 3001
    Inbound CAR: CIR    3072 bps        PIR     3072 bps (inactive)
    Outbound CAR: CIR    3072 bps        PIR     3072 bps (inactive)
```

表1-5 display portal user 命令显示信息描述表

字段	描述
Total portal users	总计的Portal用户数目
Username	用户名
Portal server	用户认证所使用的Portal认证服务器的名称
State	Portal用户的当前状态，包括以下取值： • Initialized：初始化完成后的待认证状态 • Authenticating：正在认证状态 • Waiting_SetRule：等待下发用户授权信息 • Authorizing：正在授权状态 • Online：在线状态 • Waiting_Traffic：等待获取用户最后一次流量 • Stop Accounting：停止计费 • Done：下线结束
VPN instance	Portal用户所属的MPLS L3VPN实例。若用户属于公网，则显示为N/A
MAC	Portal用户的MAC地址
IP	Portal用户的IP地址
VLAN	Portal用户所在的VLAN
Interface	Portal用户接入的接口
Authorization information	Portal用户的授权信息
DHCP IP pool	Portal用户的授权地址池名称。若无授权地址池，则显示为N/A
User profile	Portal用户的授权User Profile名称。若未授权User Profile，则显示为N/A。授权状态包括如下： • active：AAA 授权 User profile 成功 • inactive：AAA 授权 User profile 失败或者设备上不存在该 User profile
Session group profile	（暂不支持）Portal用户的授权Session Group Profile名称。若未授权Session Group Profile，则显示为N/A。
ACL number	Portal用户的授权ACL编号。若未授权ACL，则显示为N/A。授权状态包括如下： • active：AAA 授权 ACL 成功 • inactive：AAA 授权 ACL 失败或者设备上不存在该 ACL
Inbound CAR	授权的入方向CAR（CIR：平均速率，单位为bps；PIR：峰值速率，单位为bps）。若未授权入方向CAR，则显示为N/A
Outbound CAR	授权的出方向CAR（CIR：平均速率，单位为bps；PIR：峰值速率，单位为bps）。若未授权出方向CAR，则显示为N/A

显示 IP 地址为 50.50.50.3 的 Portal 用户的详细信息。

```
<Sysname> display portal user ip 50.50.50.3 verbose
```

```
Basic:
  Current IP address: 50.50.50.3
  Original IP address: 30.30.30.2
  Username: user1@hrss
  User ID: 0x28000002
  Access interface: Vlan-interface20
  Service-VLAN/Customer-VLAN: -/-
  MAC address: 0000-0000-0001
  Domain: hrss
  VPN instance: N/A
  Status: Online
  Portal server: test
  Portal authentication method: Direct
AAA:
  Realtime accounting interval: 60s, retry times: 3
  Idle cut: 180 sec, 10240 bytes, direction: Inbound
  Session duration: 500 sec, remaining: 300 sec
  Remaining traffic: 10240000 bytes
  Login time: 2014-01-19  2:42:3 UTC
  ITA policy name: N/A
  DHCP IP pool: abc
ACL&QoS&Multicast:
  Inbound CAR: CIR 64000bps PIR 640000bps
  Outbound CAR: CIR 64000bps PIR 640000bps
  ACL number: 3000（inactive）
  User profile: portal (active)
  Session group profile: N/A
  Max multicast addresses: 4
  Multicast address list: 1.2.3.1, 1.34.33.1, 3.123.123.3, 4.5.6.7
                          2.2.2.2, 3.3.3.3, 4.4.4.4
  User group: 1 (Id=1)
Flow statistic:
  Uplink   packets/bytes: 7/546
  Downlink packets/bytes: 0/0
ITA:
  level-1 uplink   packets/bytes: 0/0
          downlink packets/bytes: 0/0
  level-2 uplink   packets/bytes: 0/0
          downlink packets/bytes: 0/0
```

表1-6 display portal user verbose 命令显示信息描述表

字段	描述
Current IP address	Portal用户当前的IP地址
Original IP address	Portal用户认证时的IP地址
Username	Portal用户上线时使用的用户名
User ID	Portal用户ID

字段	描述
Access interface	Portal用户接入的接口
Service-VLAN/Customer-VLAN	Portal用户所在的公网VLAN/私网VLAN（“-”表示没有VLAN信息）
MAC address	用户的MAC地址
Domain	用户认证时使用的ISP域名
VPN instance	用户所属的MPLS L3VPN实例，N/A表示用户属于公网
Status	Portal用户的当前状态，包括以下取值： • Authenticating：正在认证状态 • Authorizing：正在授权状态 • Waiting_SetRule：正在下发 Portal 规则状态 • Online：在线状态 • Waiting_Traffic：正在等待用户流量状态 • Stop Accounting：正在停止计费状态 • Done：用户下线完成状态
Portal server	Portal服务器名称
Portal authentication method	接入接口上的Portal认证方式，包括如下取值： • Direct：直接认证方式 • Redhcp：二次地址分配认证方式 • Layer3：可跨三层认证方式
AAA	Portal用户的AAA授权信息
Realtime accounting interval	授权的实时计费间隔和重传次数。若未授权，则显示为N/A
Idle cut	授权的闲置切断时长和流量。若未授权，则显示为N/A
direction	用户数据流量的统计方向，包括以下取值： • Both：表示用户双向数据流量 • Inbound：表示用户上行数据流量 • Outbound：表示用户下行数据流量
Session duration	授权的会话时长以及剩余的会话时长。若未授权，则显示为N/A
Remaining traffic	授权的剩余流量。若未授权，则显示为N/A
Login time	用户登录时间，即用户授权成功的时间，格式为设备时间，如：2023-1-19 2:42:30 UTC
ITA policy name	（暂不支持）授权的ITA（Intelligent Target Accounting，智能靶向计费）策略名称
DHCP IP pool	授权的DHCP地址池名称。若未授权DHCP地址池，则显示为N/A
Inbound CAR	授权的入方向CAR（CIR：平均速率，单位为bps；PIR：峰值速率，单位为bps）。若未授权入方向CAR，则显示为N/A。如果下发成功，显示为active，否则为inactive

字段	描述
Outbound CAR	授权的出方向CAR（CIR：平均速率，单位为bps；PIR：峰值速率，单位为bps）。若未授权出方向CAR，则显示为N/A。如果下发成功，显示为active，否则为inactive
ACL number	授权的ACL编号。若未授权ACL，则显示为N/A。授权状态包括如下： • active：AAA 授权 ACL 成功 • inactive：AAA 授权 ACL 失败或者设备上不存在该 ACL
User profile	授权的User profile名称。若未授权User profile，则显示为N/A。授权状态包括如下： • active：AAA 授权 User profile 成功 • inactive：AAA 授权 User profile 失败或者设备上不存在该 User profile
Session group profile	（暂不支持）授权的Session group profile名称。若未授权Session group profile，则显示为N/A。
Max multicast addresses	授权Portal用户可加入的组播组的最大数目
Multicast address list	授权Portal用户可加入的组播组列表。若未授权组播组列表，则显示为N/A
User group	Portal用户所属的用户组的名称。当用户组的ID取值为0xffffffff时无效。
Flow statistic	Portal用户流量统计信息
Uplink packets/bytes	上行流量报文数/字节数
Downlink packets/bytes	下行流量报文数/字节数
ITA	（暂不支持）Portal用户的ITA业务流量统计信息
level-*n* uplink packets/bytes	（暂不支持）计费等级为*n*的上行流量报文数/字节数，*n*的取值范围为1～8
level-n downlink packets/bytes	（暂不支持）计费等级为*n*的下行流量报文数/字节数，*n*的取值范围为1～8

【相关命令】

- **portal enable**

1.1.8 display portal web-server

display portal web-server 命令用来显示 Portal Web 服务器信息。

【命令】

display portal web-server [*server-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

server-name：Portal Web 服务器的名称，为 1～32 个字符的字符串，区分大小写。

【使用指导】

若不指定参数 *server-name*，则显示所有 Portal Web 服务器信息。

【举例】

显示 Portal Web 服务器 wbs 的信息。

```
<Sysname> display portal web-server wbs
Portal Web server: wbs
    Type             : IMC
    URL              : http://www.test.com/portal
    URL parameters   : userurl=http://www.test.com/welcome
                       userip=source-address
    VPN instance     : Not configured
    Server detection : Interval: 120s  Attempts: 5  Action: log
    IPv4 status      : Up
    IPv6 status      : Up
    Captive-bypass   : Disabled
    If-match         : original-url http://2.2.2.2 redirect-url http://192.168.56.2
```

表1-7 display portal web-server 命令显示信息描述表

字段	描述
Type	Portal Web服务器类型，其取值如下： • CMCC：符合中国移动标准规范的服务器 • iMC：符合 iMC 标准规范的服务器
Portal Web server	Portal Web服务器名称
URL	Portal Web服务器的URL地址以及携带的参数
URL parameters	Portal Web服务器的URL携带的参数信息
VPN instance	Portal Web服务器所属的MPLS L3VPN实例名称
Server detection	Portal Web服务器可达性探测功能的参数，包括探测间隔时间（单位：秒），探测尝试次数以及探测到服务器状态变化后的动作（log）
IPv4 status	IPv4 Portal Web服务器当前状态，其取值如下： • Up：服务器可达性探测功能未开启，或服务器可达性探测功能开启且探测结果为该服务器当前可达 • Down：服务器可达性探测功能已开启，且探测结果为该服务器当前不可达
IPv6 status	IPv6 Portal Web服务器当前状态，其取值如下： • Up：服务器可达性探测功能未开启，或服务器可达性探测功能开启且探测结果为该服务器当前可达 • Down：服务器可达性探测功能已开启，且探测结果为该服务器当前不可达
Captive-bypass	Portal被动Web认证功能状态，其取值如下： • Disabled：未开启 • Enabled：已开启
If-match	配置的URL重定向匹配规则，未配置时，显示Not configured

【相关命令】

- **portal enable**
- **portal web-server**
- **server-detect** (portal web-server view)

1.1.9 display web-redirect rule

display web-redirect rule 命令用来显示指定接口上的 Web 重定向过滤规则信息。

【命令】

display web-redirect rule interface *interface-type interface-number* [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

interface *interface-type interface-number*：显示指定接口的 Web 重定向过滤规则信息。*interface-type interface-number* 为接口类型和接口编号。

slot *slot-number*：显示指定成员设备上指定接口的 Web 重定向过滤规则信息。*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则显示主用设备上的 Web 重定向过滤规则信息。

【举例】

显示接口 Vlan-interface100 上的所有 Web 重定向过滤规则。

```
<Sysname> display web-redirect rule interface vlan-interface 100
IPv4 web-redirect rules on vlan-interface 100:
Rule 1:
 Type                : Dynamic
 Action              : Permit
 Status              : Active
 Source:
    IP               : 192.168.2.114
    VLAN             : Any

Rule 2:
 Type                : Static
 Action              : Redirect
 Status              : Active
 Source:
    VLAN             : Any
    Protocol         : TCP
 Destination:
    Port             : 80
```

```
IPv6 web-redirect rules on vlan-interface 100:
Rule 1:
 Type                : Static
 Action              : Redirect
 Status              : Active
 Source:
    VLAN             : Any
    Protocol         : TCP
 Destination:
    Port             : 80
```

表1-8 display web-redirect rule 命令显示信息描述表

字段	描述
Rule	Web重定向规则编号
Type	Web重定向规则的类型，包括以下取值： • Static：静态类型。该类型的规则在 Web 重定向功能生效时生成 • Dynamic：动态类型。该类型的规则在用户访问重定向页面时生成
Action	Web重定向规则的匹配动作，包括以下取值： • Permit：允许报文通过 • Redirect：重定向报文
Status	Web重定向规则下发的状态，包括以下取值： • Active：表示规则已生效 • Inactive：表示规则未生效
Source	Web重定向规则的源信息
IP	源IP地址
Mask	源IPv4地址子网掩码
Prefix length	源IPv6地址前缀
VLAN	源VLAN，如果未指定，显示为Any
Protocol	Web重定向规则中使用的传输层协议类型，取值只能为TCP
Destination	Web重定向规则的目的信息
Port	目的传输层端口号，默认为80

1.1.10 if-match

if-match 命令用来配置重定向 URL 的匹配规则。

undo if-match 命令用来删除配置的重定向 URL 匹配规则。

【命令】

if-match { **original-url** *url-string* **redirect-url** *url-string* [**url-param-encryption** { **aes** | **des** } **key** { **cipher** | **simple** } *string*] | **user-agent** *string* **redirect-url** *url-string* }

undo if-match { **original-url** *url-string* | **user-agent** *user-agent* }

【缺省情况】

不存在重定向 URL 的匹配规则。

【视图】

Portal Web 服务器视图

【缺省用户角色】

network-admin

【参数】

original-url *url-string*：根据用户 Web 访问请求的 URL 地址进行匹配，其中 *url-string* 是用户 Web 访问请求的 URL 地址，为 1～256 个字符的字符串，区分大小写。该 URL 地址必须是以 http://或者 https://开头的完整 URL 路径。

redirect-url *url-string*：Web 访问请求被重定向后的地址，为 1～256 个字符的字符串，区分大小写。该 URL 地址必须是以 http://或者 https://开头的完整 URL 路径。

url-param-encryption：对设备重定向给用户的 Portal Web 服务器 URL 中携带的所有参数信息进行加密。如果未指定本参数，则表示不对携带的所有参数信息进行加密。

aes：加密算法为 AES 算法。

des：加密算法为 DES 算法。

key：设置密钥。

cipher：以密文方式设置密钥。

simple：以明文方式设置密钥，该密钥将以密文形式存储。

string：密钥字符串，区分大小写。密钥的长度范围和选择的加密方式有关。具体关系如下：

- 对于 **des** 加密方式，明文密钥为 8 个字符的字符串，密文密钥为 41 个字符的字符串。
- 对于 **aes** 加密方式，明文密钥为 1～31 个字符的字符串，密文密钥为 1～73 个字符的字符串。

user-agent *user-agent*：根据用户 HTTP/HTTPS 请求报文中的 User Agent 信息进行匹配，其中 *user-agent* 是 HTTP User Agent 信息内容，为 1～255 个字符的字符串，区分大小写。HTTP User Agent 信息包括硬件厂商信息、软件操作系统信息、浏览器信息、搜索引擎信息等内容。

【使用指导】

重定向 URL 匹配规则用于控制重定向用户的 HTTP 或 HTTPS 请求，该匹配规则可匹配用户的 Web 请求地址或者用户的终端信息。为了让用户能够成功访问重定向后的地址，需要通过 **portal free-rule** 命令配置免认证规则，放行去往该地址的 HTTP 或 HTTPS 请求报文。与 **url** 命令不同的是，重定向匹配规则可以灵活的进行地址的重定向，而 **url** 命令一般只用于将用户的 HTTP 或 HTTPS 请求重定向到 Portal Web 服务器进行 Portal 认证。在二者同时存在时，**if-match** 命令优先进行地址的重定向。

【举例】

配置 URL 地址为 http://www.abc.com.cn 的匹配规则，访问此地址的报文被重定向到 http://192.168.0.1，对重定向 URL 中携带的参数进行加密。

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] if-match original-url http://www.abc.com.cn redirect-url
http://192.168.0.1 url-param-encryption des key simple 12345678
```

配置用户代理信息为 5.0(WindowsNT6.1)AppleWebKit/537.36(KHTML,likeGecko)Chrome/36.0.1985.125Safari/537.36 的匹配规则，访问此地址的报文被重定向到 http://192.168.0.1。

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] if-match user-agent
5.0(WindowsNT6.1)AppleWebKit/537.36(KHTML,likeGecko)Chrome/36.0.1985.125Safari/537.36
redirect-url http://192.168.0.1
```

【相关命令】

- **display portal web-server**
- **portal free-rule**
- **url**
- **url-parameter**

1.1.11 ip (portal authentication server view)

ip 命令用来指定 Portal 认证服务器的 IPv4 地址。

undo ip 命令用来恢复缺省情况。

【命令】

ip *ipv4-address* [**vpn-instance** *vpn-instance-name*] [**key** { **cipher** | **simple** } *string*]

undo ip

【缺省情况】

未指定 Portal 认证服务器的 IPv4 地址。

【视图】

Portal 认证服务器视图

【缺省用户角色】

network-admin

【参数】

ipv4-address：Portal 认证服务器的 IPv4 地址。

vpn-instance *vpn-instance-name*：Portal 认证服务器所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示 Portal 认证服务器位于公网中。

key：与 Portal 认证服务器通信时使用的共享密钥。设备与 Portal 认证服务器交互的 Portal 报文中会携带一个在该共享密钥参与下生成的验证字，该验证字用于接受方校验收到的 Portal 报文的正确性。

cipher：以密文方式设置密钥。

simple：以明文方式设置密钥，该密钥将以密文形式存储。

string：密码字符串，区分大小写。明文密钥为 1～64 个字符的字符串，密文密钥为 1～117 个字符的字符串。

【使用指导】

一个 Portal 认证服务器对应一个 IPv4 地址，因此一个 Portal 认证服务器视图下只允许存在一个 IPv4 地址。多次执行本命令，最后一次执行的命令生效。

不同的 Portal 认证服务器不允许 IPv4 地址和 VPN 的配置都相同。

【举例】

指定 Portal 认证服务器 pts 的 IPv4 地址为 192.168.0.111、共享密钥为明文 portal。

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] ip 192.168.0.111 key simple portal
```

【相关命令】

- **portal server**
- **display portal server**

1.1.12 ipv6

ipv6 命令用来指定 Portal 认证服务器的 IPv6 地址。

undo ipv6 命令用来恢复缺省情况。

【命令】

ipv6 *ipv6-address* [**vpn-instance** *vpn-instance-name*] [**key** { **cipher** | **simple** } *string*]

undo ipv6

【缺省情况】

未指定 Portal 认证服务器的 IPv6 地址。

【视图】

Portal 认证服务器视图

【缺省用户角色】

network-admin

【参数】

ipv6-address：Portal 认证服务器的 IPv6 地址。

vpn-instance *vpn-instance-name*：Portal 认证服务器所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示 Portal 认证服务器位于公网中。

key：与 Portal 认证服务器通信需要的共享密钥。设备与 Portal 认证服务器交互的 Portal 报文中会携带一个在该共享密钥参与下生成的验证字，该验证字用于接受方校验收到的 Portal 报文的正确性。

cipher：以密文方式设置密钥。

simple：以明文方式设置密钥，该密钥将以密文形式存储。

string：密码字符串，区分大小写。明文密钥为 1～64 个字符的字符串，密文密钥为 1～117 个字符的字符串。

【使用指导】

一个 Portal 认证服务器对应一个 IPv6 地址，因此一个 Portal 认证服务器视图下只允许存在一个 IPv6 地址。多次执行本命令，最后一次执行的命令生效。

不同的 Portal 认证服务器不允许 IPv6 地址和 VPN 实例的配置都相同。

【举例】

指定 Portal 认证服务器 pts 的 IPv6 地址为 2000::1、共享密钥为明文 portal。

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] ipv6 2000::1 key simple portal
```

【相关命令】

- **display portal server**
- **portal server**

1.1.13 port (portal authentication server view)

port 命令用来配置设备主动向 Portal 认证服务器发送 Portal 报文时使用的 UDP 端口号。

undo port 命令用来恢复缺省情况。

【命令】

port *port-number*

undo port

【缺省情况】

设备主动发送 Portal 报文时使用的 UDP 端口号为 50100。

【视图】

Portal 认证服务器视图

【缺省用户角色】

network-admin

【参数】

port-number：设备向 Portal 认证服务器主动发送 Portal 报文时使用的目的 UDP 端口号，取值范围为 1～65534。

【使用指导】

本命令配置的端口号要和 Portal 认证服务器上配置的监听 Portal 报文的端口号保持一致。

【举例】

配置设备向 Portal 认证服务器 pts 主动发送 Portal 报文时使用的目的 UDP 端口号为 50000。

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] port 50000
```

【相关命令】

- **portal server**

1.1.14 portal { bas-ip | bas-ipv6 } (interface view)

portal { bas-ip | bas-ipv6 }命令用来设置发送给 Portal 认证服务器的 Portal 报文中的 BAS-IP 或 BAS-IPv6 属性。

undo portal { bas-ip | bas-ipv6 }命令用来恢复缺省情况。

【命令】

portal { **bas-ip** *ipv4-address* | **bas-ipv6** *ipv6-address* }

undo portal { **bas-ip** | **bas-ipv6** }

【缺省情况】

对于响应类报文 IPv4 Portal 报文中的 BAS-IP 属性为报文的源 IPv4 地址，IPv6 Portal 报文中的 BAS-IPv6 属性为报文源 IPv6 地址。

对于通知类报文 IPv4 Portal 报文中的 BAS-IP 属性为出接口的 IPv4 地址，IPv6 Portal 报文中的 BAS-IPv6 属性为出接口的 IPv6 地址。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv4-address：接口发送 Portal 报文的 BAS-IP 属性值，应该为本机的地址，不能为全 0 地址、全 1 地址、D 类地址、E 类地址和环回地址。

ipv6-address：接口发送 Portal 报文的 BAS-IPv6 属性值，应该为本机的地址，不能为多播地址、全 0 地址、本地链路地址。

【使用指导】

设备上运行 Portal 协议 2.0 版本时，主动发送给 Portal 认证服务器的报文（例如强制用户下线报文）中必须携带 BAS-IP 属性。设备上运行 Portal 协议 3.0 版本时，主动发送给 Portal 认证服务器必须携带 BAS-IP 或者 BAS-IPv6 属性。

配置此命令后，设备主动发送的通知类 Portal 报文，其源 IP 地址为配置的 BAS-IP，否则为 Portal 报文出接口 IP 地址。

接口上开启了二次地址分配认证方式的 Portal 认证时，如果 Portal 认证服务器上指定的设备 IP 不是 Portal 报文出接口 IP 地址，则必须通过本命令配置相应的 BAS-IP 或 BAS-IPv6 属性，使其值与 Portal 认证服务器上指定的设备 IP 一致，否则 Portal 用户无法认证成功。

使用 H3C iMC 的 Portal 认证服务器的情况下，如果 Portal 服务器上指定的设备 IP 不是设备上 Portal 报文出接口的 IP 地址，则开启了 Portal 认证的接口上必须配置 BAS-IP 或者 BAS-IPv6 属性。

【举例】

配置接口 Vlan-interface100 发送 Portal 报文的 BAS-IP 属性值为 2.2.2.2。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal bas-ip 2.2.2.2
```

【相关命令】

- **display portal**

1.1.15 portal { ipv4-max-user | ipv6-max-user } (interface view)

portal { **ipv4-max-user** | **ipv6-max-user** }命令用来配置接口上的 Portal 最大用户数。

undo portal { **ipv4-max-user** | **ipv6-max-user** }命令用来恢复缺省情况。

【命令】

portal { **ipv4-max-user** | **ipv6-max-user** } *max-number*

undo portal { **ipv4-max-user** | **ipv6-max-user** }

【缺省情况】

接口上的 Portal 最大用户数不受限制。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

max-number：接口上允许的最大 IPv4 或 IPv6 Portal 用户数，取值范围为 1～4294967295。

【使用指导】

如果接口上配置的 Portal 最大用户数小于当前接口上已经在线的 Portal 用户数，则该配置可以执行成功，且在线 Portal 用户不受影响，但系统将不允许新的 Portal 用户从该接口接入。

【举例】

在接口 Vlan-interface100 上配置 IPv4 Portal 最大用户数为 100。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal ipv4-max-user 100
```

【相关命令】

- **display portal**
- **portal max-user**

1.1.16 portal apply web-server (interface view)

portal [**ipv6**] **apply web-server** 命令用来引用 Portal Web 服务器，设备会将 Portal 用户的 HTTP 请求报文重定向到该 Web 服务器。

undo portal [**ipv6**] **apply web-server** 命令用来取消恢复缺省情况。

【命令】

portal [**ipv6**] **apply web-server** *server-name* [**fail-permit**]

undo portal [**ipv6**] **apply web-server**

【缺省情况】

未引用 Portal Web 服务器。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6：表示 IPv6 Portal Web 服务器。若不指定该参数，则表示 IPv4 Portal Web 服务器。

server-name：被引用的 Portal Web 服务器的名称，为 1～32 个字符的字符串，区分大小写，且必须已经存在。

fail-permit：开启 Portal Web 服务器不可达时的 Portal 用户逃生功能，即设备探测到 Portal Web 服务器不可达时取消接口上的 Portal 认证功能，允许用户不经过 Portal 认证即可自由访问网络。

【使用指导】

一个接口上可以同时开启 IPv4 Portal 认证和 IPv6 Portal 认证，因此也可以同时引用一个 IPv4 Portal Web 服务器和一个 IPv6 Portal Web 认证服务器。

如果接口上同时开启了 Portal 认证服务器逃生功能和 Portal Web 服务器逃生功能，则当任意一个服务器不可达时，即取消接口 Portal 认证功能，当两个服务器均恢复正常通信后，再重新启动 Portal 认证功能。

【举例】

在接口 Vlan-interface100 上引用名称为 wbs 的 Portal Web 服务器作为用户认证时使用的 Web 服务器。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal apply web-server wbs
```

【相关命令】

- **display portal**
- **portal fail-permit server**
- **portal web-server**

1.1.17 portal authorization strict-checking

portal authorization strict-checking 命令用来开启 Portal 授权信息的严格检查模式。

undo portal authorization strict-checking 命令用来关闭 Portal 授权信息的严格检查模式。

【命令】

portal authorization { **acl** | **user-profile** } **strict-checking**

undo portal authorization { **acl** | **user-profile** } **strict-checking**

【缺省情况】

缺省为非严格检查授权信息模式，当服务器下发的授权 ACL、User Profile 在设备上不存在或者设备下发 ACL、User Profile 失败时，用户保持在线。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

acl：表示开启对授权 ACL 的严格检查。

user-profile：表示开启对授权 User Profile 的严格检查。

【使用指导】

接口上开启 Portal 授权信息的严格检查模式后，当服务器给用户下发的授权 ACL、User Profile 在设备上不存在或者设备下发 ACL、User Profile 失败时，设备将强制该用户下线。

可同时开启对授权 ACL 和授权 User Profile 的严格检查模式。若同时开启了对授权 ACL 和对授权 User Profile 的严格检查模式，则只要其中任意一个授权属性未通过严格授权检查，则用户就会下线。

【举例】

在接口 Vlan-interface100 上开启对授权 ACL 的严格检查模式。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal authorization acl strict-checking
```

【相关命令】

- **display portal**

1.1.18 portal delete-user

portal delete-user 命令用来强制在线 Portal 用户下线。

【命令】

portal delete-user { *ipv4-address* | **all** | **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv4-address：在线 Portal 用户的 IPv4 地址。

all：所有接口下的在线 IPv4 Portal 用户和 IPv6 Portal 用户。

interface *interface-type interface-number*：指定接口下的所有在线 Portal 用户，包括 IPv4 Portal 用户和 IPv6 Portal 用户。*interface-type interface-number* 为接口类型和接口编号。

ipv6 *ipv6-address*：指定在线 IPv6 Portal 用户的地址。

【举例】

强制 IP 地址为 1.1.1.1 的在线 Portal 用户下线。

```
<Sysname> system-view
[Sysname] portal delete-user 1.1.1.1
```

【相关命令】

- **display portal user**

1.1.19 portal device-id

portal device-id 命令用来配置设备 ID。

undo portal device-id 命令用来恢复缺省情况。

【命令】

portal device-id *device-id*

undo portal device-id

【缺省情况】

未配置任何设备 ID。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

device-id：设备 ID，为 1～63 个字符的字符串，区分大小写。

【使用指导】

通过配置设备 ID，使得设备向 Portal 服务器发送的协议报文中携带一个属性，此属性用于向 Portal 服务器标识发送协议报文的接入设备。

不同设备的设备 ID 不能相同。

【举例】

配置设备的 ID 名为 0002.0010.100.00。

```
<Sysname> system-view
[Sysname] portal device-id 0002.0010.100.00
```

1.1.20 portal domain (interface view)

portal [**ipv6**] **domain** 命令用于指定 Portal 用户使用的认证域，使得所有从该接口接入的 Portal 用户强制使用该认证域。

undo portal [**ipv6**] **domain** 命令用来删除 Portal 用户使用的认证域。

【命令】

portal [**ipv6**] **domain** *domain-name*

undo portal [**ipv6**] **domain**

【缺省情况】

未指定 Portal 用户使用的认证域。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6：指定 IPv6 Portal 用户使用的认证域。若不指定本参数，则表示指定 IPv4 Portal 用户使用的认证域。

domain-name：ISP 认证域名，为 1～255 个字符的字符串，不区分大小写。

【使用指导】

接口上可以同时指定 IPv4 Portal 用户和 IPv6 Portal 用户的认证域。

如果不指定 **ipv6** 参数，则表示配置或者删除 IPv4 Portal 用户使用的认证域。

【举例】

指定从接口 Vlan-interface100 上接入的 IPv4 Portal 用户使用认证域为 my-domain。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal domain my-domain
```

【相关命令】

- **display portal**

1.1.21 portal enable (interface view)

portal [**ipv6**] **enable** 命令用来开启 Portal 认证功能，并指定认证方式。

undo portal [**ipv6**] **enable** 命令用来关闭 Portal 认证功能。

【命令】

portal enable method { **direct** | **layer3** | **redhcp** }

portal ipv6 enable method { **direct** | **layer3** }

undo portal [**ipv6**] **enable**

【缺省情况】

Portal 认证功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6：表示 IPv6 Portal 认证。若不指定该参数，则表示 IPv4 Portal 认证。

method：认证方式。

- **direct**：直接认证方式。
- **layer3**：可跨三层认证方式。
- **redhcp**：二次地址分配认证方式。

【使用指导】

不能通过重复执行本命令来修改 Portal 认证方式。如需修改 Portal 的认证方式，请先通过 **undo portal** [**ipv6**] **enable** 命令取消 Portal 认证功能，再执行 **portal** [**ipv6**] **enable** 命令。

开启 IPv6 Portal 认证功能之前，需要保证设备支持 IPv6 ACL 和 IPv6 转发功能。

IPv6 Portal 认证不支持二次地址分配方式。

允许在接口上同时开启 IPv4 Portal 认证和 IPv6 Portal 认证功能。

【举例】

在接口 Vlan-interface100 上开启 IPv4 Portal 认证，且指定为直接认证方式。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal enable method direct
```

【相关命令】

- **display portal**

1.1.22 portal fail-permit server

portal [**ipv6**] **fail-permit server** 命令用来开启 Portal 认证服务器不可达时的 Portal 用户逃生功能。

undo portal [**ipv6**] **fail-permit server** 命令用来关闭 Portal 认证服务器不可达时的 Portal 用户逃生功能。

【命令】

portal [**ipv6**] **fail-permit server** *server-name*

undo portal [**ipv6**] **fail-permit server**

【缺省情况】

Portal 认证服务器不可达时的 Portal 用户逃生功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6：表示 IPv6 Portal 认证服务器。若不指定该参数，则表示 IPv4 Portal 认证服务器。

server-name：Portal 认证服务器名称，为 1～32 个字符的字符串，区分大小写。

【使用指导】

如果接口上同时开启了 Portal 认证服务器不可达时的 Portal 用户逃生功能和 Portal Web 服务器不可达时的 Portal 用户逃生功能，则当任意一个服务器不可达时，立即放开接口控制，允许用户不经过 Portal 认证即可自由访问网络；当两个服务器均恢复可达后，再重新启动接口的 Portal 认证功能。重新启动接口的 Portal 认证功能之后，未通过认证的用户需要通过认证之后才能访问网络资源，已通过认证的用户可继续访问网络资源。

一个接口上，最多同时可以开启一个 Portal 认证服务器不可达时的 Portal 用户逃生功能和一个 Portal Web 服务器不可达时的 Portal 用户逃生功能。

多次执行本命令，最后一次执行的命令生效。

【举例】

在接口 Vlan-interface100 上启用 Portal 认证服务器 pts1 不可达时的 Portal 用户逃生功能。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal fail-permit server pts1
```

【相关命令】

- **display portal**

1.1.23 portal free-all except destination

portal free-all except destination 命令用来配置 IPv4 Portal 目的认证网段。

undo portal free-all except destination 命令用来删除 IPv4 Portal 目的认证网段。

【命令】

portal free-all except destination *ipv4-network-address* { *mask-length* | *mask* }

undo portal free-all except destination [*ipv4-network-address*]

【缺省情况】

未配置 IPv4 Portal 目的网段认证，表示对访问任意目的网段的用户都进行 Portal 认证。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv4-network-address：IPv4 Portal 认证网段地址。

mask-length：子网掩码长度，取值范围为 0～32。

mask：子网掩码，点分十进制格式。

【使用指导】

接口上仅要求 Portal 用户访问指定目的认证网段（除免认证规则中指定的目的 IP 地址或网段）时才需要进行 Portal 认证，访问其它网段访问时不需要进行 Portal 认证。

可以通过多次执行本命令，配置多条目的认证网段。

如果 **undo** 命令中不携带 IP 地址参数，则表示删除所有的 IPv4 Portal 目的认证网段。

目的网段认证对二次地址分配认证方式的 Portal 认证不生效。

如果接口上同时配置了源认证网段和目的认证网段，则源认证网段配置不会生效。

【举例】

在接口 Vlan-interface2 上配置 IPv4 Portal 目的认证网段为 11.11.11.0/24，仅允许访问 11.11.11.0/24 网段的用户触发 Portal 认证，其它目的网段可以直接访问。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname–Vlan-interface2] portal free-all except destination 11.11.11.0 24
```

【相关命令】

- **display portal**

1.1.24 portal free-rule

portal free-rule 命令用来配置基于 IP 地址的 Portal 免认证规则。

undo portal free-rule 命令用来删除指定的或所有 Portal 免认证规则。

【命令】

portal free-rule *rule-number* { **destination ip** { *ipv4-address* { *mask-length* | *mask* } | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] | **source ip** { *ipv4-address* { *mask-length* | *mask* } | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] } * [**interface** *interface-type interface-number*]

portal free-rule *rule-number* { **destination ipv6** { *ipv6-address prefix-length* | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] | **source ipv6** { *ipv6-address prefix-length* | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] } * [**interface** *interface-type interface-number*]

undo portal free-rule { *rule-number* | **all** }

【缺省情况】

不存在基于 IP 地址的 Portal 免认证规则。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

rule-number：免认证规则编号。取值范围为 0～4294967295。

destination：指定目的信息。

source：指定源信息。

ip *ipv4-address*：免认证规则的 IPv4 地址。

{ *mask-length* | *mask* }：免认证规则的 IP 地址掩码。其中，*mask-length* 为子网掩码长度，取值范围为 0～32；*mask* 为子网掩码，点分十进制格式。

ipv6 *ipv6-address*：免认证规则的 IPv6 地址。

prefix-length：免认证规则的 IPv6 地址前缀长度，取值范围为 0～128。

ip any：任意 IPv4 地址。

ipv6 any：任意 IPv6 地址。

tcp *tcp-port-number*：免认证规则的 TCP 端口号，取值范围为 0～65535。

udp *udp-port-number*：免认证规则的 UDP 端口号，取值范围为 0～65535。

all：所有免认证规则。

interface *interface-type interface-number*：免认证规则生效的三层接口。

【使用指导】

可以同时指定源和目的参数，或者仅指定其中一个参数，后者表示另外一个地址不受限制。

如果免认证规则中同时配置了源端口号和目的端口号，则要求源和目的端口号所属的传输层协议类型保持一致。

未指定三层接口的情况下，免认证规则对所有开启 Portal 的接口生效；指定三层接口的情况下，免认证规则只对指定的三层接口生效。

相同内容的免认证规则不能重复配置，否则提示免认证规则已存在或重复。

【举例】

配置一条基于 IPv4 地址的 Portal 免认证规则：编号为 1、源地址为 10.10.10.1/24、目的地址为 20.20.20.1、目的 TCP 端口号为 23、生效接口为 Vlan-interface1。该规则表示在 Vlan-interface1 接口上，10.10.10.1/24 网段地址的用户不需要经过 Portal 认证即可以访问地址为 20.20.20.1 的主机在 TCP 端口 23 上提供的服务。

```
<Sysname> system-view
[Sysname] portal free-rule 1 destination ip 20.20.20.1 32 tcp 23 source ip 10.10.10.1 24
interface vlan-interface 1
```

配置一条基于 IPv6 地址的 Portal 免认证规则：编号为 2、源地址为 2000::1/64、目的地址为 2001::1、目的 TCP 端口号为 23、生效接口为 Vlan-interface1。该规则表示在 Vlan-interface1 接口上，

2000::1/64 网段地址的用户不需要经过 Portal 认证即可以访问目的地址为 2001::1 的主机在 TCP 端口 23 上提供的服务。

```
<Sysname> system-view
[Sysname] portal free-rule 2 destination ipv6 2001::1 128 tcp 23 source ip 2000::1 64 interface vlan-interface 1
```

【相关命令】

- **display portal rule**

1.1.25 portal free-rule destination

portal free-rule destination 命令用来配置基于目的的 Portal 免认证规则，这里的目的指的是主机名。

undo portal free-rule 命令用来删除指定的或所有 Portal 免认证规则。

【命令】

portal free-rule *rule-number* **destination** *host-name*

undo portal free-rule { *rule-number* | **all** }

【缺省情况】

不存在基于目的的 Portal 免认证规则。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

rule-number：免认证规则编号。取值范围为 0～4294967295。

destination：指定目的信息。

host-name：主机名，为 1～253 个字符的字符串，不区分大小写，字符串中可以包含字母、数字、“-”、“_”、“.”和通配符“*”，且不能为“i”、“ip”、“ipv”或“ipv6”。

all：所有免认证规则。

【使用指导】

基于目的 Portal 免认证规则支持如下两种配置方式：

- 精确匹配：即完整匹配主机名。例如配置的主机名为 abc.com.cn，其含义为只匹配 abc.com.cn 的主机名，如果报文中携带的主机名为 dfabc.com.cn，则匹配失败。
- 模糊匹配：即使用通配符配置主机名，通配符只能位于主机名字符串之首或末尾，例如配置的主机名为*abc.com.cn、abc*和*abc*，其含义分别为匹配所有以 abc.com.cn 结尾的主机名、匹配所有以 abc 开头的主机名和匹配所有含有 abc 字符串的主机名。

配置基于目的 Portal 免认证规则时，需要注意的是：

- 通配符“*”表示任意个数字符，设备会将已配置的多个连续的通配符识别为一个通配符。
- 配置的主机名不能只有通配符。
- 相同内容的免认证规则不能重复配置，否则提示免认证规则已存在或重复。

- 目前，只有用户浏览器发起的 HTTP/HTTPS 请求报文，支持模糊匹配的免认证规则。

【举例】

配置一条基于目的的 Portal 免认证规则：编号为 4、主机名为 www.h3c.com。该规则表示用户的 HTTP/HTTPS 请求报文中的主机名必须是 www.h3c.com 时，该用户才可以不需要经过 Portal 认证即可以访问网络资源。

```
<Sysname> system-view
[Sysname] portal free-rule 4 destination www.h3c.com
```

【相关命令】

- **display portal rule**

1.1.26 portal free-rule source

portal free-rule source 命令用来配置基于源的 Portal 免认证规则，这里的源可以是源 MAC 地址、源接口或者源 VLAN。

undo portal free-rule 命令用来删除指定的或所有 Portal 免认证规则。

【命令】

portal free-rule *rule-number* **source** { **interface** *interface-type interface-number* | **mac** *mac-address* | **vlan** *vlan-id* } *

undo portal free-rule { *rule-number* | **all** }

【缺省情况】

未配置基于源的 Portal 免认证规则。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

rule-number：免认证规则编号。取值范围为 0～4294967295。

interface *interface-type interface-number*：免认证规则的源接口。*interface-type interface-number* 为接口类型和接口编号。

mac *mac-address*：免认证规则的源 MAC 地址，为 H-H-H 的形式。

vlan *vlan-id*：免认证规则的源 VLAN 编号。配置本关键字仅对通过 VLAN 接口接入的 Portal 用户生效。

all：所有免认证规则。

【使用指导】

如果免认证规则中同时指定了源 VLAN 和二层源接口，则要求该接口属于对应的 VLAN，否则该规则无效。

【举例】

配置一条 Portal 免认证规则：编号为 3、源 MAC 地址为 1-1-1、源 VLAN 为 VLAN 10。该规则表示 MAC 地址为 1-1-1，属于 VLAN 10 的用户不需要经过 Portal 认证即可以访问网络资源。

```
<Sysname> system-view
[Sysname] portal free-rule 3 source mac 1-1-1 vlan 10
```

【相关命令】

- **display portal rule**

1.1.27 portal ipv6 free-all except destination

portal ipv6 free-all except destination 命令用来配置 IPv6 Portal 目的网段认证。

undo portal ipv6 free-all except destination 命令用来删除 IPv6 Portal 目的认证网段。

【命令】

portal ipv6 free-all except destination *ipv6-network-address prefix-length*

undo portal ipv6 free-all except destination [*ipv6-network-address*]

【缺省情况】

未配置 IPv6 Portal 目的网段认证，表示对访问任意 IPv6 目的网段的用户都进行 Portal 认证。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6-network-address：IPv6 Portal 认证网段地址。

prefix-length：IPv6 地址前缀长度，取值范围为 0～128。

【使用指导】

接口上仅要求在 Portal 用户访问指定目的认证网段（除免认证规则中指定的目的 IP 地址或网段）时才需要进行 Portal 认证，访问其它网段访问时不需要进行 Portal 认证。

可以通过多次执行本命令，配置多条目的认证网段。

如果 **undo** 命令中不携带 IP 地址参数，则表示删除所有的 IPv6 Portal 目的认证网段。

目的网段认证对二次地址分配认证方式的 Portal 认证不生效。

如果接口上同时配置了源认证网段和目的认证网段，则源认证网段配置不会生效。

【举例】

在接口 Vlan-interface2 上配置 IPv6 Portal 目的认证网段为 1::2/16，仅要求访问 1::2/16 网段的用户必须进行 Portal 认证。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] portal ipv6 free-all except destination 1::2 16
```

【相关命令】

- **display portal**

1.1.28 portal ipv6 layer3 source

portal ipv6 layer3 source 命令用来配置 IPv6 Portal 源认证网段。

undo portal ipv6 layer3 source 命令用来删除 IPv6 Portal 源认证网段。

【命令】

portal ipv6 layer3 source *ipv6-network-address prefix-length*

undo portal ipv6 layer3 source [*ipv6-network-address*]

【缺省情况】

未配置 IPv6 Portal 源认证网段，表示对来自任意网段的 IPv6 用户都进行 Portal 认证。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6-network-address：IPv6 Portal 源认证网段地址。

prefix-length：IPv6 地址前缀长度，取值范围为 0～128。

【使用指导】

配置此功能后，接口上只允许在源认证网段范围内的 IPv6 用户报文才能触发 Portal 认证，否则丢弃。

如果 **undo** 命令中不携带 IP 地址参数，则表示删除所有的 IPv6 Portal 源认证网段。

源认证网段仅对 Portal 的可跨三层认证方式（**layer3**）生效。

如果接口上同时配置了源认证网段和目的网段认证，则源认证网段配置不会生效。

【举例】

在接口 Vlan-interface2 上配置一条 IPv6 Portal 源认证网段为 1::1/16，仅允许来自 1::1/16 网段的用户触发 Portal 认证。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] portal ipv6 layer3 source 1::1 16
```

【相关命令】

- **display portal**
- **portal ipv6 free-all except destination**

1.1.29 portal ipv6 user-detect

portal ipv6 user-detect 命令用来开启 IPv6 Portal 用户在线探测功能。

undo portal user-detect 命令用来关闭 IPv6 Portal 用户在线探测功能。

【命令】

portal ipv6 user-detect type { **icmpv6** | **nd** } [**retry** *retries*] [**interval** *interval*] [**idle** *time*]

undo portal ipv6 user-detect

【缺省情况】

IPv6 Portal 用户在线探测功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

type：指定探测类型。

- **icmpv6**：表示探测类型为 ICMPv6。
- **nd**：表示探测类型为 ND。

retry *retries*：探测次数，取值范围为 1～10，缺省值为 3。

interval *interval*：探测间隔，取值范围为 1～1200，单位为秒，缺省值为 3。

idle *time*：用户在线探测闲置时长，即闲置多长时间后发起探测，取值范围为 60～3600，单位为秒，缺省值为 180。

【使用指导】

根据探测类型的不同，设备有以下两种探测机制：

- 当探测类型为 ICMPv6 时，若设备发现一定时间（**idle** *time*）内接口上未收到某 Portal 用户的报文，则会向该用户定期（**interval** *interval*）发送探测报文。如果在指定探测次数（**retry** *retries*）之内，设备收到了该用户的响应报文，则认为用户在线，且停止发送探测报文，重复这个过程，否则，强制其下线。
- 当探测类型为 ND 时，若设备发现一定时间（**idle** *time*）内接口上未收到某 Portal 用户的报文，则会向该用户发送 ND 请求报文。设备定期（**interval** *interval*）检测用户 ND 表项是否被刷新过，如果在指定探测次数（**retry** *retries*）内用户 ND 表项被刷新过，则认为用户在线，且停止检测用户 ND 表项，重复这个过程，否则，强制其下线。

请根据配置的认证方式选择合适的探测方法，如果配置了直接方式或者二次地址分配方式，则可以使用 ND 或 ICMPv6 探测方式，如果配置了可跨三层认证方式，则可以使用 ICMPv6 探测方式，若配置了 ND 探测方式，则探测功能不生效。

如果用户接入设备上配置了阻止 ICMPv6 报文的防火墙策略，则接口上的 ICMPv6 探测方式可能会失败，从而导致接口上的 Portal 用户非正常下线。因此，若接口上需要使用 ICMPv6 探测方式，请保证用户接入设备不会过滤掉 ICMPv6 报文。

【举例】

在接口 Vlan-interface100 上开启 IPv6 Portal 用户在线探测功能：探测类型为 ND，检测用户 ND 表项的探测次数为 5 次，探测间隔为 10 秒，闲置时间为 300 秒。

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal ipv6 user-detect type nd retry 5 interval 10 idle 300
```

【相关命令】

- **display portal**

1.1.30 portal layer3 source

portal layer3 source 命令用来配置 IPv4 Portal 源认证网段。

undo portal layer3 source 命令用来删除 IPv4 Portal 源认证网段。

【命令】

portal layer3 source *ipv4-network-address* { *mask-length* | *mask* }

undo portal layer3 source [*ipv4-network-address*]

【缺省情况】

未配置 IPv4 Portal 源认证网段，表示对来自任意网段的 IPv4 用户都进行 Portal 认证。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv4-network-address：IPv4 Portal 认证网段地址。

mask-length：子网掩码长度，取值范围为 0～32。

mask：子网掩码，点分十进制格式。

【使用指导】

配置此功能后，接口上只允许在源认证网段范围内的 IPv4 用户报文才能触发 Portal 认证，否则丢弃

如果 **undo** 命令中不携带 IP 地址参数，则表示删除所有的 IPv4 Portal 源认证网段。

源认证网段仅对 Portal 的可跨三层认证方式（**layer3**）生效。

如果接口上同时配置了源认证网段和目的网段认证，则源认证网段配置不会生效。

【举例】

在接口 Vlan-interface2 上配置一条 IPv4 Portal 源认证网段为 10.10.10.0/24，仅允许来自 10.10.10.0/24 网段的用户触发 Portal 认证。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] portal layer3 source 10.10.10.0 24
```

【相关命令】

- **display portal**
- **portal free-all except destination**

1.1.31 portal local-web-server

portal local-web-server 命令用来开启本地 Portal 服务，并进入基于 HTTP/HTTPS 协议的本地 Portal Web 服务视图。

undo portal local-web-server 命令用来关闭本地 Portal 服务功能。

【命令】

portal local-web-server { **http** | **https ssl-server-policy** *policy-name* [**tcp-port** *port-number*] }

undo portal local-web-server { **http** | **https** }

【缺省情况】

本地 Portal 服务功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

http：指定本地 Portal Web 服务使用 HTTP 协议和客户端交互认证信息。

https：指定本地 Portal Web 服务使用 HTTPS 协议和客户端交互认证信息。

ssl-server-policy *policy-name*：指定 HTTPS 服务关联的 SSL 服务器端策略。*policy-name* 为 SSL 服务器端策略的名称，为 1～31 个字符的字符串，不区分大小写，且必须已经存在。

tcp-port *port-number*：指定本地 Portal Web 服务的 HTTPS 服务侦听的 TCP 端口号，取值范围为 1～65535，缺省值为 443。

【使用指导】

本地 Portal 服务功能是指，Portal 认证系统中不采用外部独立的 Portal Web 服务器和 Portal 认证服务器，而由接入设备实现 Portal Web 服务器和 Portal 认证服务器功能。

只有接口上引用的 Portal Web 服务器中的 URL 同时满足以下两个条件时，接口上才会使用本地 Portal Web 服务功能。条件如下：

- 该 URL 中的 IP 地址是设备本机上的 IP 地址（除 127.0.0.1 以外）。
- 该 URL 以/portal/结尾，例如：http://1.1.1.1/portal/。

配置本地 Portal Web 服务功能时，需要注意的是：

- 已经被 HTTPS 服务关联的 SSL 服务器端策略不能被删除。
- 不能通过重复执行本命令来修改 HTTPS 服务关联的 SSL 服务器端策略，如需修改，请先通过 **undo portal local-web-server https** 命令删除已创建的本地 Portal Web 服务，再执行 **portal local-web-server https ssl-server-policy** 命令。

配置本地 Portal Web 服务参数时，需要注意的是：

- 如果本地 Portal Web 服务引用的 SSL 服务器端策略与 HTTPS 服务引用的 SSL 服务器端策略相同，则本地 Portal Web 服务使用的 TCP 端口号可以与 HTTPS 服务器使用的 TCP 端口号相同，否则不能使用相同的 TCP 端口号。
- 除了 HTTPS 协议默认的端口号，本地 Portal Web 服务的 TCP 端口号不能与知名协议使用的端口号或者设备上其它服务已使用的 TCP 端口号配置一致，如 HTTP 的端口号 80；Telnet 的端口号 23，否则会造成本地 Portal Web 服务无法向 Portal 用户推送认证页面。
- 使用 HTTP 协议和 HTTPS 协议的本地 Portal Web 服务侦听的 TCP 端口号不能配置一致，比如不能都配置为 8080，否则会导致本地 Web 服务无法正常使用。

【举例】

开启本地 Portal 服务，并进入基于 HTTP 协议的本地 Portal Web 服务视图。

```
<Sysname> system-view
[Sysname] portal local-web-server http
[Sysname-portal-local-websvr-http] quit
```

开启本地 Portal 服务，并进入基于 HTTP 协议的本地 Portal Web 服务视图，引用的 SSL 服务器端策略为 policy1。

```
<Sysname> system-view
[Sysname] portal local-web-server https ssl-server-policy policy1
[Sysname-portal-local-websvr-https] quit
```

更改引用的 SSL 服务器端策略为 policy2。

```
[Sysname] undo portal local-web-server https
[Sysname] portal local-web-server https ssl-server-policy policy2
[Sysname-portal-local-websvr-https] quit
```

使用 HTTPS 协议和客户端交互认证信息的方式创建本地 Portal Web 服务，引用的 SSL 服务器端策略为 policy1，指定侦听的端口号为 442。

```
<Sysname> system-view
[Sysname] portal local-web-server https ssl-server-policy policy1 tcp-port 442
[Sysname-portal-local-websvr-https] quit
```

【相关命令】

- **default-logon-page**
- **portal local-web-server**
- **ssl server-policy**（安全命令参考/SSL）

1.1.32 portal log enable

portal log enable 命令用来开启 Portal 用户上/下线日志功能。

undo portal log enable 命令用来关闭 Portal 用户上/下线日志功能。

【命令】

portal log enable

undo portal log enable

【缺省情况】

Portal 用户上/下线日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启本功能后，设备会对用户上线和下线时的信息进行记录，包括用户名、IP 地址、接口名称、VLAN、用户 MAC 地址、上线失败原因等。生成的日志信息将被发送到设备的信息中心，通过设置信息中心的参数，决定日志信息的输出规则（即是否允许输出以及输出方向）。有关信息中心参数的配置请参见“网络管理和监控配置指导”中的“信息中心”。

【举例】

开启 Portal 用户上/下线日志功能。

```
<Sysname> system-view
[Sysname] portal log enable
```

1.1.33 portal max-user

portal max-user 命令用来配置全局 Portal 最大用户数。

undo portal max-user 命令用来恢复缺省情况。

【命令】

portal max-user *max-number*

undo portal max-user

【缺省情况】

全局 Portal 最大用户数不受限制。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

max-number：系统中允许同时在线的最大 Portal 用户数。取值范围为 1～4294967295。

【使用指导】

如果配置的全局 Portal 最大用户数小于当前已经在线的 Portal 用户数，则该命令可以执行成功，且在线 Portal 用户不受影响，但系统将不允许新的 Portal 用户接入。

该命令指定的最大用户数是指 IPv4 Portal 和 IPv6 Portal 用户的总数。

建议所有开启 Portal 的接口上的最大 IPv4 Portal 用户数和最大 IPv6 Portal 用户数之和不超过配置的全局最大 Portal 用户数，否则会有部分 Portal 用户因为全局最大用户数已达到上限而无法上线。

【举例】

配置全局 Portal 最大用户数为 100。

```
<Sysname> system-view
```

```
[Sysname] portal max-user 100
```

【相关命令】

- **display portal user**
- **portal** { **ipv4-max-user** | **ipv6-max-user** }

1.1.34 portal nas-id-profile

portal nas-id-profile 命令用来指定接口引用的 NAS-ID Profile。

undo portal nas-id-profile 命令用来恢复缺省情况。

【命令】

portal nas-id-profile *profile-name*

undo portal nas-id-profile

【缺省情况】

未指定引用的 NAS-ID Profile。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

profile-name：标识指定 VLAN 和 NAS-ID 绑定关系的 Profile 名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

本命令引用的 NAS-ID Profile 由命令 **aaa nas-id profile** 配置，具体情况请参考“安全命令参考”中的“AAA”。

对于 QinQ 报文，Portal 接入只能匹配内层 VLAN。有关 QinQ 的详细介绍，请参见“二层技术-以太网交换配置指导”中的“QinQ”。

如果接口上指定了 NAS-ID Profile，则此 Profile 中定义的绑定关系优先使用；如果接口上未指定 NAS-ID Profile 或指定的 Profile 中没有找到匹配的绑定关系，则使用设备名作为 NAS-ID。

【举例】

在接口 Vlan-interface 2 上指定名为 aaa 的 NAS-ID Profile。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] portal nas-id-profile aaa
```

【相关命令】

- **aaa nas-id profile**（安全命令参考/AAA）

1.1.35 portal nas-port-id format

portal nas-port-id format 命令用来配置 NAS-Port-ID 属性的格式。

undo portal nas-port-id format 命令用来恢复缺省情况。

【命令】

portal nas-port-id format { 1 | 2 | 3 | 4 }

undo portal nas-port-id format

【缺省情况】

NAS-Port-ID 的消息格式为格式 2。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

1：表示格式 1，具体为 {atm | eth | trunk} NAS_slot/NAS_subslot/NAS_port:XPI.XCI AccessNodeIdentifier/ANI_rack/ANI_frame/ANI_slot/ANI_subslot/ANI_port[:ANI_XPI.ANI_XCI]。

2：表示格式 2，具体为 SlotID00IfNOVlanID。

3：表示格式 3，具体为在格式 2 的内容后面添加 Option82 或者 Option18。

4：表示格式 4，具体为 slot=**;subslot=**;port=**;vlanid=**;vlanid2=**。

【使用指导】

可通过本命令修改设备为 Portal 用户发送的 RADIUS 报文中填充的 NAS-Port-ID 属性的格式。

不同厂商的 RADIUS 服务器要求不同的格式，通常中国电信的 RADIUS 服务器要求采用格式 1。

1. 格式 1

{atm | eth | trunk} NAS_slot/NAS_subslot/NAS_port:XPI.XCI AccessNodeIdentifier/ANI_rack/ANI_frame/ANI_slot/ANI_subslot/ANI_port[:ANI_XPI.ANI_XCI]

各项含义如下：

- {atm | eth | trunk}：BRAS 端口类型，包括 ATM 接口、以太接口或 trunk 类型的以太网接口。
- NAS_slot：BRAS 槽号，取值为 0～31。
- NAS_subslot：BRAS 子槽号，取值为 0～31。
- NAS_Port：BRAS 端口号，取值为 0～63。
- XPI：如果接口类型为 atm，则 XPI 对应 VPI，取值为 0～255；如果接口类型为 eth 或 trunk，则 XPI 对应 PVLAN，XPI 取值为 0～4095。
- XCI：如果接口类型为 atm，则 XCI 对应 VCI，取值为 0～65535；如果接口类型为 eth 或 trunk，XCI 对应于 CVLAN，XCI 取值为 0～4095。
- AccessNodeIdentifier：接入节点标识（例如 DSLAM 设备），为不超过 50 个字符的字符串，字符串中不能包括空格。
- ANI_rack：接入节点机架号（如支持紧耦合的 DSLAM 设备），取值为 0～15。
- ANI_frame：接入节点机框号，取值为 0～31。
- ANI_slot：接入节点槽号，取值为 0～127。
- ANI_subslot：接入节点子槽号，取值为 0～31。

- ANI_port：接入节点端口号，取值为 0～255。
- ANI_XPI.ANI_XCI：可选项，主要用于携带 CPE 侧的业务信息，可用于标识未来的业务类型需求，如在多 PVC 应用场合下可标识具体的业务。其中，如果接口类型为 atm，则 ANI_XPI 对应 VPI，取值为 0～255，ANI_XCII 对应 VCI，取值为 0～65535；如果接口类型为 eth 或 trunk，则 ANI_XPI 对应 PVLAN，取值为 0～4095，则 ANI_XCI 对应 CVLAN，取值为 0～4095。

字符串之间用一个空格隔开，要求字符串中间不能有空格。花括号中的内容是必选的，|表示并列的关系，多选一。[ ]表示可选项。对于某些设备没有机架、框、子槽的概念，相应位置应统一填 0，对于无效的 VLAN ID 值都填 4096。

如接口类型为 ATM，则 AccessNodeIdentifier、ANI_rack、ANI_frame、ANI_slot、ANI_subslot、ANI_port 域可统一填 0。

如运营商未使用 SVLAN 技术，则 XPI=4096，XCI=VLAN，取值为 0～4095。

如运营商未使用 VLAN 技术区分用户（用户 PC 直连 BAS 端口），则 XPI=4096，XCI=4096。

对于接入节点设备（如 DSLAM），按如上格式上报本接入节点的接入线路信息，对于与 BRAS 设备相关的接入线路信息可统一填 0，如：“0 0/0/0:4096.1234 guangzhou001/0/31/63/31/127”

其含义是 DSLAM 节点标识为 guangzhou001、DSLAM 的机架号为 0（没有机架）、DSLAM 的框号为 31、DSLAM 的槽号为 63、DSLAM 的子槽号为 31、DSLAM 的端口号为 127、VLAN ID 号为 1234，BRAS 接入线路信息为未知。

对于 BRAS 设备，在获取接入节点设备（如 DSLAM）的接入线路信息后，根据 BRAS 的配置可透传接入线路信息，也可修改添加接入线路信息中与 BRAS 设备相关的线路信息，形成完整的接入线路信息，如：“eth 31/31/7:4096.1234 guangzhou001/0/31/63/31/127”。

格式 1 的解释示例如下：

- 例 1：NAS_PORT_ID =“atm 31/31/7:255.65535 0/0/0/0/0/0”

含义：BRAS 设备的用户接口类型为 ATM 接口，BRAS 槽号为 31，BRAS 子槽号为 31，BRAS 端口号为 7，VPI 为 255，VCI 为 65535。

- 例 2：NAS_PORT_ID =“eth 31/31/7:1234.2345 0/0/0/0/0/0”

含义：BRAS 设备的用户接口类型为以太接口，BRAS 槽号为 31，BRAS 子槽号为 31，BRAS 端口号为 7，PVLAN ID 为 1234，CVLAN ID 为 2345。

- 例 3：NAS_PORT_ID =“eth 31/31/7:4096.2345 0/0/0/0/0/0”

含义：BRAS 设备的用户接口类型为以太接口，BRAS 槽号为 31，BRAS 子槽号为 31，BRAS 端口号为 7，VLAN ID 为 2345。

- 例 4：NAS_PORT_ID =“eth 31/31/7:4096.2345 guangzhou001/1/31/63/31/127”

含义：BRAS 设备的用户接口类型为以太接口，BRAS 槽号为 31，BRAS 子槽号为 31, BRAS 端口号为 7，VLAN ID 为 2345,接入节点 DSLAM 的标识为 guangzhou001，DSLAM 的机架号为 1，DSLAM 的框号为 31，DSLAM 的槽号为 63，DSLAM 的子槽号为 31，DSLAM 的端口号为 127。

2. 格式 2

SlotID00IfNOVlanID

各项含义如下：

- SlotID：用户接入的槽位号，为两个字符的字符串。
- IfNO：用户接入的接口编号，为 3 个字符的字符串。
- VlanID：用户接入的 VLAN ID，为 9 个字符的字符串。

3. 格式 3

其格式为在格式 2 的 NAS-Port-ID 内容后面添加用户 DHCP 报文中指定 Option 的内容：对于 IPv4 用户，此处添加的是 DHCP Option82 的内容。对于 IPv6 用户，此处添加的是 DHCP Option18 的内容。

4. 格式 4

其格式为 slot=**;subslot=**;port=**;vlanid=**;vlanid2=**，具体情况如下：

- 对于非 VLAN 接口，其格式为 slot=**;subslot=**;port=**;vlanid=0。
- 对于只终结了一层 VLAN Tag 的接口，其格式为 slot=**;subslot=**;port=**;vlanid=**。

【举例】

配置 NAS-Port-ID 属性的格式为 format 1。

```
<Sysname> system-view
[Sysname] portal nas-port-id format 1
```

1.1.36 portal pre-auth ip-pool

portal [**ipv6**] **pre-auth ip-pool** 命令用来配置 Portal 认证前用户使用的地址池。

undo portal [**ipv6**] **pre-auth ip-pool** 命令用来恢复缺省情况。

【命令】

portal [**ipv6**] **pre-auth ip-pool** *pool-name*

undo portal [**ipv6**] **pre-auth ip-pool**

【缺省情况】

未配置 Portal 认证前用户使用的地址池。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6：表示 IPv6 Portal 用户。若不指定该参数，则表示 IPv4 Portal 用户。

pool-name：表示 IP 地址池的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

在 Portal 用户通过设备的子接口接入网络的组网环境中，当子接口上未配置 IP 地址，且用户需要通过 DHCP 获取地址时，就必须通过本命令指定一个地址池，并在用户进行 Portal 认证之前为其分配一个 IP 地址使其可以进行 Portal 认证。

仅当接口使用直接认证方式的情况下，接口上为认证前的 Portal 用户指定的 IP 地址池才能生效。

当使用接口上指定的 IP 地址池为认证前的 Portal 用户分配 IP 地址时，该指定的 IP 地址池必须存在且配置完整，否则无法为 Portal 用户分配 IP 地址，并导致用户无法进行 Portal 认证。

【举例】

在接口 Vlan-interface100 上为认证前的 Portal 用户指定 IPv4 地址池为 abc。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal pre-auth ip-pool abc
```

【相关命令】

- **dhcp server ip-pool**（三层技术-IP 业务命令参考/DHCP）
- **display portal**
- **ipv6 dhcp pool**（三层技术-IP 业务命令参考/DHCP）

1.1.37 portal refresh enable

portal refresh { **arp** | **nd** } **enable** 命令用来开启 Portal 客户端 Rule ARP/ND 表项生成功能。

undo portal refresh { **arp** | **nd** } **enable** 命令用来关闭 Portal 客户端 Rule ARP/ND 表项生成功能。

【命令】

portal refresh { **arp** | **nd** } **enable**

undo portal refresh { **arp** | **nd** } **enable**

【缺省情况】

Portal 客户端 Rule ARP 表项、ND 表项生成功能均处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

arp：表示 ARP 表项。

nd：表示 ND 表项。

【使用指导】

Portal 客户端的 Rule ARP/ND 表项生成功能处于开启状态时，Portal 客户端上线后，其 ARP/ND 表项为 Rule 表项，在 Portal 客户端下线后会被立即删除，导致 Portal 客户端在短时间内再上线时会因 ARP/ND 表项还未学习到而认证失败。此情况下，需要关闭本功能，使得 Portal 客户端上线后其 ARP/ND 表项仍为动态表项，在 Portal 客户端下线后按老化时间正常老化。

此功能的开启和关闭不影响已经在线的 Portal 客户端的 ARP/ND 表项类型。

【举例】

关闭 Portal 客户端 Rule ARP 表项生成功能。

```
<Sysname> system-view
[Sysname] undo portal refresh arp enable
```

1.1.38 portal roaming enable

portal roaming enable 命令用来开启 Portal 用户漫游功能。

undo portal roaming enable 命令用来关闭 Portal 用户漫游功能。

【命令】

portal roaming enable

undo portal roaming enable

【缺省情况】

Portal 用户漫游功能处于关闭状态，即 Portal 用户上线后不能在所在的 VLAN 内漫游。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

Portal 用户漫游功能只对通过 VLAN 接口上线的 Portal 用户有效。

设备上有用户在线的情况下，不能配置此命令。

如果开启了 Portal 用户漫游功能，则 Portal 用户上线后可以在开启 Portal 的 VLAN 内漫游，即用户通过 VLAN 内的任何二层端口都可以访问网络资源；否则用户只能通过认证成功的二层端口访问网络资源。

Portal 用户漫游功能需要在关闭 Portal 客户端 Rule ARP/ND 表项生成功能（通过命令 **undo portal refresh { arp | nd } enable**）的情况下才能生效。

【举例】

开启 Portal 用户漫游功能。

```
<Sysname> system-view
[Sysname] portal roaming enable
```

1.1.39 portal server

portal server 命令用来创建 Portal 认证服务器，并进入 Portal 认证服务器视图。如果指定的 Portal 认证服务器已经存在，则直接进入 Portal 认证服务器视图。

undo portal server 命令用来删除指定的 Portal 认证服务器。

【命令】

portal server *server-name*

undo portal server *server-name*

【缺省情况】

不存在 Portal 认证服务器。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

server-name：Portal 认证服务器的名称，为 1～32 个字符的字符串，区分大小写。

【使用指导】

Portal 认证服务器视图用于配置 Portal 认证服务器的相关参数，包括服务器的 IP 地址、端口号，服务器所在的 VPN 实例，设备和服务器间通信的预共享密钥，服务器探测功能等。

可以配置多个 Portal 认证服务器。

【举例】

创建名称为 pts 的 Portal 认证服务器，并进入 Portal 认证服务器视图。

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts]
```

【相关命令】

- **display portal server**

1.1.40 portal user-detect

portal user-detect 命令用来开启 IPv4 Portal 用户在线探测功能。

undo portal user-detect 命令用来关闭 IPv4 Portal 用户在线探测功能。

【命令】

portal user-detect type { **arp** | **icmp** } [**retry** *retries*] [**interval** *interval*] [**idle** *time*]

undo portal user-detect

【缺省情况】

IPv4 Portal 用户在线探测功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

type：指定探测类型。

- **arp**：表示探测类型为 ARP。
- **icmp**：表示探测类型为 ICMP。

retry *retries*：探测次数，取值范围为 1～10，缺省值为 3。

interval *interval*：探测间隔，取值范围为 1～1200，单位为秒，缺省值为 3。

idle *time*：用户在线探测闲置时长，即闲置多长时间后发起探测，取值范围为 60～3600，单位为秒，缺省值为 180。

【使用指导】

根据探测类型的不同，设备有以下两种探测机制：

- 当探测类型为 ICMP 时，若设备发现一定时间（**idle** *time*）内接口上未收到某 Portal 用户的报文，则会向该用户定期（**interval** *interval*）发送探测报文。如果在指定探测次数（**retry** *retries*）之内，设备收到了该用户的响应报文，则认为用户在线，且停止发送探测报文，重复这个过程，否则，强制其下线。
- 当探测类型为 ARP 时，若设备发现一定时间（**idle** *time*）内接口上未收到某 Portal 用户的报文，则会向该用户发送 ARP 请求报文。设备定期（**interval** *interval*）检测用户 ARP 表项是否被刷新过，如果在指定探测次数（**retry** *retries*）内用户 ARP 表项被刷新过，则认为用户在线，且停止检测用户 ARP 表项，重复这个过程，否则，强制其下线。

请根据配置的认证方式选择合适的探测方法，如果配置了直接方式或者二次地址分配方式，则可以使用 ARP 或 ICMP 探测方式，如果配置了可跨三层认证方式，则仅可以使用 ICMP 探测方式，若配置了 ARP 探测方式，则探测功能不生效。

如果用户接入设备上配置了阻止 ICMP 报文的防火墙策略，则接口上的 ICMP 探测方式可能会失败，从而导致接口上的 Portal 用户非正常下线。因此，若接口上需要使用 ICMP 探测方式，请保证用户接入设备不会过滤掉 ICMP 报文。

【举例】

在接口 Vlan-interface100 上开启 Portal 用户在线探测功能：探测类型为 ARP，检测用户 ARP 表项的探测次数为 5 次，探测间隔为 10 秒，闲置时间为 300 秒。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal user-detect type arp retry 5 interval 10 idle 300
```

【相关命令】

- **display portal**

1.1.41 portal user-dhcp-only (interface view)

portal user-dhcp-only 命令用来开启仅允许通过 DHCP 方式获取 IP 地址的客户端上线的功能。

undo portal user-dhcp-only 命令用来关闭仅允许通过 DHCP 方式获取 IP 地址的客户端上线的功能。

【命令】

portal [**ipv6**] **user-dhcp-only**

undo portal [**ipv6**] **user-dhcp-only**

【缺省情况】

仅允许通过 DHCP 方式获取 IP 地址的客户端上线的功能处于关闭状态，通过 DHCP 方式获取 IP 地址的客户端和配置静态 IP 地址的客户端都可以上线。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6：表示允许上线的客户端的 IP 地址为 IPv6 地址，如果不指定本参数，则表示允许上线的客户端的 IP 地址为 IPv4 地址。

【使用指导】

配置本命令后，配置静态 IP 地址的 Portal 认证用户不能上线。

在 IPv6 网络中，配置本命令后，终端仍会使用临时 IPv6 地址进行 Portal 认证，从而导致认证失败，所以终端必须关闭临时 IPv6 地址。

【举例】

在接口 Vlan-interface100 上配置仅允许通过 DHCP 获取 IP 地址的客户端上线功能。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal user-dhcp-only
```

【相关命令】

- **display portal**

1.1.42 portal web-server

portal web-server 命令用来创建 Portal Web 服务器，并进入 Portal Web 服务器视图。如果指定的 Portal Web 服务器已经存在，则直接进入 Portal Web 服务器视图。

undo portal web-server 命令用来删除 Portal Web 服务器。

【命令】

portal web-server *server-name*

undo portal web-server *server-name*

【缺省情况】

不存在 Portal Web 服务器。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

server-name：Portal Web 服务器的名称，为 1～32 个字符的字符串，区分大小写。

【使用指导】

Portal Web 服务器是指 Portal 认证过程中向用户推送认证页面的 Web 服务器，也是设备强制重定向用户 HTTP 请求报文时所指的 Web 服务器。Portal Web 服务器视图用于配置该 Web 服务器的 URL 地址及配置设备重定向该 URL 地址给用户时 URL 地址所携带的参数，同时该视图还用于配置 Portal Web 服务器探测等功能。

【举例】

创建名称为 wbs 的 Portal Web 服务器，并进入 Portal Web 服务器视图。

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs]
```

【相关命令】

- **display portal web-server**
- **portal apply web-server**

1.1.43 reset portal packet statistics

reset portal packet statistics 命令用来清除 Portal 报文的统计信息。

【命令】

reset portal packet statistics [**server** *server-name*]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

server-name：Portal 认证服务器的名称，为 1～32 个字符的字符串，区分大小写。

【使用指导】

若不指定参数 **server**，则清除所有 Portal 认证服务器的报文统计信息。

【举例】

清除名称为 st 上的 Portal 认证服务器的统计信息。

```
<Sysname> reset portal packet statistics server pts
```

【相关命令】

- **display portal packet statistics**

1.1.44 server-detect (portal authentication server view)

server-detect 命令用来开启 Portal 认证服务器的可达性探测功能。开启 Portal 认证服务器的可达性探测功能后，设备会定期检测 Portal 认证服务器发送的 Portal 报文来判断服务器的可达状态。

undo server-detect 命令用来关闭 Portal 认证服务器的可达性探测功能。

【命令】

server-detect [**timeout** *timeout*] **log**

undo server-detect

【缺省情况】

Portal 认证服务器的可达性探测功能处于关闭状态。

【视图】

Portal 认证服务器视图

【缺省用户角色】

network-admin

【参数】

timeout *timeout*：探测超时时间，取值范围为 10～3600，单位为秒，缺省值为 60。

log：Portal 认证服务器可达或者不可达的状态改变时，发送日志信息。日志信息中记录了 Portal 认证服务器名以及该服务器状态改变前后的状态。

【使用指导】

只有当设备上存在开启 Portal 认证的接口时，Portal 认证服务器的可达性探测功能才生效。

只有在支持 Portal 服务器心跳功能（目前仅 iMC 的 Portal 认证服务器支持）的 Portal 认证服务器的配合下，本功能才有效。

若设备在指定的探测超时时间（**timeout** *timeout*）内收到 Portal 报文，且验证其正确，则认为此次探测成功且服务器可达，否则认为此次服务器不可达。

设备配置的探测超时时间（**timeout** *timeout*）必须大于服务器上配置的逃生心跳间隔时间。

【举例】

开启对 Portal 认证服务器 pts 的探测功能，探测超时时间为 600 秒，若服务器状态改变，则发送日志信息。

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] server-detect timeout 600 log
```

【相关命令】

- **portal server**

1.1.45 server-detect (portal web server view)

server-detect 命令用来开启 Portal Web 服务器的可达性探测功能。

undo server-detect 命令用来关闭 Portal Web 服务器的可达性探测功能。

【命令】

server-detect [**interval** *interval*] [**retry** *retries*] **log**

undo server-detect

【缺省情况】

Portal Web 服务器的可达性探测功能处于关闭状态。

【视图】

Portal Web 服务器视图

【缺省用户角色】

network-admin

【参数】

interval *interval*：进行探测尝试的时间间隔，取值范围为 10～1200，单位为秒，缺省值为 20。

retry *retries*：连续探测失败的最大次数，取值范围为 1～10，缺省值为 3。若连续探测失败数目达到此值，则认为服务器不可达。

log：Portal Web 服务器可达或者不可达的状态改变时，发送日志信息。日志信息中记录了 Portal Web 服务器名以及该服务器状态改变前后的状态。

【使用指导】

该探测方法可由设备独立完成，不需要 Portal Web 服务器端的任何配置来配合。

只有当配置了 Portal Web 服务器的 URL 地址，且设备上存在开启 Portal 认证接口时，该 Portal Web 服务器的可达性探测功能才生效。

【举例】

配置对 Portal Web 服务器 wbs 的探测功能，每次探测间隔时间为 600 秒，若连续二次探测均失败，则发送服务器不可达的日志信息。

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] server-detect interval 600 retry 2 log
```

【相关命令】

- **portal web-server**

1.1.46 server-register

server-register 命令用来配置设备定期向 Portal 认证服务器发送注册报文。

undo server-register 命令用来恢复缺省情况。

【命令】

server-register [**interval** *interval-value*]

undo server-register

【缺省情况】

设备不会定期向 Portal 认证服务器发送注册报文。

【视图】

Portal 认证服务器视图

【缺省用户角色】

network-admin

【参数】

interval *interval-value*：设备定期向 Portal 认证服务器发送注册报文的时间间隔，取值范围为 1～3600，单位为秒，缺省值为 600。

【使用指导】

Portal 服务器与接入设备认证交互时，如果二者之间有 NAT 设备，为了使 Portal 服务器能够访问该接入设备，在 NAT 设备上需配置静态 NAT 表项，该静态 NAT 表项中记录了接入设备的 IP 地址以及与 Portal 服务器交互时使用的转换后的 IP 地址。当有大量的接入设备需要与 Portal 服务器进行认证交互时，则需要在 NAT 设备上配置大量的静态 NAT 表项。开启本功能后，接入设备会主动向 Portal 服务器发送注册报文，该报文中携带了接入设备的名称。Portal 服务器收到该注册报文，记

录下接入设备的名称、地址转换后的 IP 地址以及端口号等信息后，后续这些信息用于与接入设备进行认证交互。接入设备通过定期发送注册报文更新 Portal 服务器上维护的注册信息。

需要注意的是，本功能仅用于和 CMCC 类型的 Portal 服务器配合使用。

【举例】

配置设备每隔 120 秒向 Portal 认证服务器发送注册报文。

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] server-register interval 120
```

【相关命令】

- **server-type**

1.1.47 server-type

server-type 命令用来配置 Portal 认证服务器或 Portal Web 服务器的类型。

undo server-type 命令用来恢复缺省情况。

【命令】

server-type { **cmcc** | **imc** }

undo server-type

【缺省情况】

Portal 认证服务器或 Portal Web 服务器的类型为 iMC 服务器。

【视图】

Portal 认证服务器视图

Portal Web 服务器视图

【缺省用户角色】

network-admin

【参数】

cmcc：表示 Portal 服务器类型为符合中国移动标准规范的服务器。

imc：表示 Portal 服务器类型为符合 iMC 标准规范的服务器。

【使用指导】

设备配置的 Portal 服务器类型必须保证与设备所使用的服务器类型保持一致。

【举例】

配置 Portal 认证服务器类型为 imc。

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] server-type imc
```

配置 Portal Web 服务器类型为 imc。

```
<Sysname> system-view
[Sysname] portal web-server pts
[Sysname-portal-websvr-pts] server-type imc
```

【相关命令】

- **display portal server**

1.1.48 tcp-port

tcp-port 命令用来配置本地 Portal Web 服务的 HTTP/HTTPS 服务侦听的 TCP 端口号。

undo tcp-port 命令用来恢复缺省情况。

【命令】

tcp-port *port-number*

undo tcp-port

【缺省情况】

HTTP 服务侦听的 TCP 端口号为 80，HTTPS 服务侦听的 TCP 端口号为 **portal local-web-serve** 命令指定的 TCP 端口号。

【视图】

本地 Portal Web 服务视图

【缺省用户角色】

network-admin

【参数】

port-number：表示侦听的 TCP 端口号，取值范围为 1～65535。

【使用指导】

接口上指定的 Portal Web 服务器的 URL 中配置的端口号，应该与本地 Portal Web 服务视图下指定的侦听端口号保持一致。

配置本地 Portal Web 服务的 HTTP/HTTPS 服务侦听的 TCP 端口号时，需要注意的是：

- 除了 HTTP 和 HTTPS 协议默认的端口号，本地 Portal Web 服务的 TCP 端口号不能与知名协议使用的端口号配置一致，如 FTP 的端口号 21；Telnet 的端口号 23，否则会造成本地 Web Server 无法收到用户的认证或下线请求数据。
- 不能把使用 HTTP 协议的本地 Portal Web 服务侦听的 TCP 端口号配置成 HTTPS 的默认端口号 443，反之亦然。
- 使用 HTTP 协议和 HTTPS 协议的本地 Portal Web 服务侦听的 TCP 端口号不能配置一致，比如不能都配置为 8080，否则会导致本地 Web 服务无法正常使用。
- 如果本地 Portal Web 服务引用的 SSL 服务器端策略与 HTTPS 服务引用的 SSL 服务器端策略相同，则本地 Portal Web 服务使用的 TCP 端口号可以与 HTTPS 服务器使用的 TCP 端口号相同；否则使用 TCP 端口号不能相同。

【举例】

配置本地 Portal Web 服务的 HTTP 服务侦听的 TCP 端口号为 2331。

```
<Sysname> system-view
[Sysname] portal local-web-server http
[Sysname-portal-local-websvr-http] tcp-port 2331
```

【相关命令】

- **portal local-web-server**

1.1.49 url

url 命令用来指定 Portal Web 服务器的 URL。

undo url 命令用来恢复缺省情况。

【命令】

url *url-string*

undo url

【缺省情况】

未指定 Portal Web 服务器的 URL。

【视图】

Portal Web 服务器视图

【缺省用户角色】

network-admin

【参数】

url-string：Portal Web 服务器的 URL，为 1～256 个字符的字符串，区分大小写。

【使用指导】

本命令指定的 URL 是可用标准 HTTP 或者 HTTPS 协议访问的 URL，它以 http://或者 https://开头。如果该 URL 未以 http://或者 https://开头，则缺省认为是以 http://开头。

若要对用户的 HTTPS 请求进行重定向，需要通过 **http-redirect https-port** 命令配置对 HTTPS 报文进行重定向的内部侦听端口号，具体介绍请参见“三层业务-IP 业务命令参考”中的“HTTP 重定向”。

【举例】

配置 Portal Web 服务器 wbs 的 URL 为 http://www.test.com/portal。

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] url http://www.test.com/portal
```

【相关命令】

- **display portal web-server**

1.1.50 url-parameter

url-parameter 命令用来配置设备重定向给用户的 Portal Web 服务器的 URL 中携带的参数信息。

undo url-parameter 命令用来删除配置的 Portal Web 服务器 URL 携带的参数信息。

【命令】

url-parameter *param-name* { **original-url** | **source-address** | **source-mac** [**encryption** { **aes** | **des** } **key** { **cipher** | **simple** } *string*] | **value** *expression* }

undo url-parameter *param-name*

【缺省情况】

未配置设备重定向给用户的 Portal Web 服务器的 URL 中携带的参数信息。

【视图】

Portal Web 服务器视图

【缺省用户角色】

network-admin

【参数】

param-name：URL 参数名，为 1～32 个字符的字符串，区分大小写。URL 参数名对应的参数内容由 *param-name* 后的参数指定。

original-url：用户初始访问的 Web 页面的 URL。

source-address：用户的 IP 地址。

source-mac：用户的 MAC 地址。

encryption：表示以密文的方式携带用户的 MAC 地址。

aes：指定加密算法为 AES 算法。

des：指定加密算法为 DES 算法。

cipher：以密文方式设置密钥。

key：指定加密密钥。

simple：以明文方式设置密钥，该密钥将以密文形式存储。

string：密钥字符串，区分大小写。密钥的长度范围和选择的加密方式有关。具体关系如下：

- 对于 **des cipher**，密钥为 41 个字符的字符串。
- 对于 **des simple**，密钥为 8 个字符的字符串。
- 对于 **aes cipher**，密钥为 1～73 个字符的字符串。
- 对于 **aes simple**，密钥为 1～31 个字符的字符串。

value *expression*：自定义字符串，为 1～256 个字符的字符串，区分大小写。

【使用指导】

可以通过多次执行本命令配置多条参数信息。

对于同一个参数名 *param-name* 后的参数设置，最后配置的生效。

该命令用于配置用户访问 Portal Web 服务器时，要求携带的一些参数，比较常用的是要求携带用户的 IP 地址、MAC 地址、用户原始访问的 URL 信息。用户也可以手工指定，携带一些特定的字符信息。配置完成后，在设备给用户强制重定向 URL 时会携带这些参数，例如配置 Portal Web 服务器的 URL 为：http://www.test.com/portal，若同时配置如下两个参数信息：**url-parameter** *userip* **source-address** 和 **url-parameter** *userurl* **value** *http://www.abc.com/welcome*，则设备给源 IP 为 1.1.1.1 的用户重定向时回应的 URL 格式即为：http://www.test.com/portal?userip=1.1.1.1&userurl=http://www.abc.com/welcome。

param-name 这个 URL 参数名必须与具体应用环境中的 Portal 服务器所支持的 URL 参数名保持一致，不同的 Portal 服务器支持 URL 参数名是不一样的，请根据具体情况配置 URL 参数名。例如 iMC 服务器支持的 URL 参数名如下：

- *userurl*：表示 **original-url**
- *userip*：表示 **source-address**
- *usermac*：表示 **source-mac**

在 Portal 服务器为 H3C 公司的 iMC 服务器的组网环境中，如果设备重定向给用户的 Portal Web 服务器的 URL 中需要携带用户的 IP 地址参数信息时，必须把 *param-name* 参数配置成 userip，否则，iMC 服务器不能识别用户的 IP 地址。

如果给某个参数配置了加密方式，则重定向 URL 中携带的将是其加密后的值。例如在上述配置的基础上，再配置 **url-parameter usermac source-mac encryption des key simple 12345678**，则设备给源 MAC 地址为 1111-1111-1111 的用户重定向时回应的 URL 格式即为：http://www.test.com/portal?usermac=xxxxxxxxx&userip=1.1.1.1&userurl=http://www.test.com/welcome，其中 xxxxxxxxx 为加密后的用户 mac 地址。

【举例】

为设备重定向给用户的 Portal Web 服务器 wbs 的 URL 中配置两个参数 userip 和 userurl，其值分别为用户 IP 地址和自定义字符串 http://www.abc.com/welcome。

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] url-parameter userip source-address
[Sysname-portal-websvr-wbs] url-parameter userurl value http://www.abc.com/welcome
```

为设备重定向给用户的 Portal Web 服务器 wbs 的 URL 中配置参数 usermac，其值为用户 mac 地址，并使用 des 算法进行加密。

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] url-parameter usermac source-mac encryption des key simple
12345678
```

【相关命令】

- **display portal web-server**
- **url**

1.1.51 user-sync

user-sync 命令用来配置开启 Portal 用户信息同步功能。

undo user-sync 命令用来关闭 Portal 用户信息同步功能。

【命令】

user-sync timeout *timeout*

undo user-sync

【缺省情况】

Portal 认证服务器的 Portal 用户信息同步功能处于关闭状态。

【视图】

Portal 认证服务器视图

【缺省用户角色】

network-admin

【参数】

timeout *timeout*：检测用户同步报文的时间间隔，取值范围为 60～18000，单位为秒。

【使用指导】

配置此功能后，设备会响应并周期性地检测指定的 Portal 认证服务器发来的用户同步报文，以保持设备与该服务器上在线用户信息的一致性。

只有在支持 Portal 用户心跳功能（目前仅 iMC 的 Portal 认证服务器支持）的 Portal 认证服务器的配合下，本功能才有效。为了实现该功能，还需要在 Portal 认证服务器上选择支持用户心跳功能，且服务器上配置的用户心跳间隔要小于等于设备上配置的检测超时时间。

在设备上删除 Portal 认证服务器时将会同时删除该服务器的用户信息同步功能配置。

对同一服务器多次执行本命令，最后一次执行的命令生效。

对于设备上多余的用户信息，即在检测用户同步报文的时间间隔 *timeout* 到达后被判定为 Portal 认证服务器上已不存在的用户信息，设备会在 *timeout* 后的某时刻将其删除掉。

如果服务器同步过来的用户信息在设备上不存在，则设备会将这些用户的 IP 地址封装在用户心跳回应报文中发送给服务器，由服务器删除多余的用户。

【举例】

配置对 Portal 认证服务器 pts 的 Portal 用户信息同步功能，检测用户同步报文的时间间隔为 600 秒，如果设备中的某用户信息在 600 秒内未在该 Portal 认证服务器发送的同步报文中出现，设备将强制该用户下线。

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] user-sync timeout 600
```

【相关命令】

- **portal server**

1.1.52 vpn-instance

vpn-instance 命令用来配置 Portal Web 服务器所属的 VPN 实例。

undo vpn-instance 命令用来恢复缺省情况。

【命令】

vpn-instance *vpn-instance-name*

undo vpn-instance

【缺省情况】

Portal Web 服务器位于公网中。

【视图】

Portal Web 服务器视图

【缺省用户角色】

network-admin

【参数】

v*pn-instance-name*：Portal Web 服务器所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。

【使用指导】

一个 Portal Web 服务器只能属于一个 VPN 实例。

【举例】

配置 Portal Web 服务器 wbs 所属的 VPN 实例为 abc。

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] vpn-instance abc
```

1.1.53 web-redirect url

web-redirect url 命令用来配置 Web 重定向功能。

undo web-redirect 命令用来关闭 Web 重定向功能。

【命令】

web-redirect [**ipv6**] **url** *url-string* [**interval** *interval*]

undo web-redirect [**ipv6**]

【缺省情况】

Web 重定功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6：表示 IPv6 Web 重定向功能。若不指定该参数，则表示 IPv4 Web 重定向功能。

url *url-string*：Web 重定向的地址，即用户的 Web 访问请求被重定向的 URL 地址，为 1～256 个字符的字符串，必须是以 http://或者 https://开头的完整 URL 路径。

interval *interval*：对用户访问的 Web 页面进行重定向的周期，取值范围为 60～86400，单位为秒，缺省值为 86400。

【使用指导】

接口上配置了 Web 重定向功能后，当该接口上接入的用户初次通过 Web 页面访问外网时，设备会将用户的初始访问页面重定向到指定的 URL 页面，之后用户才可以正常访问外网，经过一定时长（*interval*）后，设备又可以对用户要访问的网页或者正在访问的网页重定向到指定的 URL 页面。

不能同时开启 Web 重定向功能和 Portal 功能，否则 Web 重定向功能失效。

Web 重定向功能仅对使用默认端口号 80 的 HTTP 协议报文生效。

【举例】

在接口 Vlan-interface100 上配置 IPv4 Web 重定向功能：Web 重定向地址为 http://192.0.0.1，Web 重定向周期为 3600 秒。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] web-redirect url http://192.0.0.1 interval 3600
```

【相关命令】

- **display web-redirect rule**