目 录

1 网络配置

1.1 漫游

1.1.1 WLAN漫游简介

在 ESS（Extended Service Set，拓展服务集）区域中，WLAN 客户端从一个 AP 上接入转移到另一个 AP 上接入的过程叫做漫游。在漫游过程中，客户端需要维持原有的 IP 地址、授权信息等，确保已有业务不中断。

为了提高用户体验，缩短客户端漫游时间，AC 支持快速漫游，即使用 RSN+802.1X 认证接入的客户端在漫游到新 AP 时不再需要进行 802.1X 认证。

1.1.2 漫游基本概念

- IACTP（Inter Access Controller Tunneling Protocol，接入控制器间隧道协议）：H3C 公司自主研发的隧道协议，该协议提供了 AC 间报文的通用封装和传输机制。提供漫游服务的 AC 之间会建立 IACTP 隧道，用于保证 AC 间控制报文以及客户端漫游信息的安全传输。
- HA（Home Agent，本地代理）：客户端跨 AC 漫游后，与该客户端初始上线 AP 相连接的 AC 即为 HA。
- FA（Foreign Agent，外地代理）：客户端跨 AC 漫游后，客户端与某个不是 HA 的 AC 进行关联，该 AC 即为 FA。

1.1.3 漫游组网方式

1. AC内漫游

如 图 1-1 所示，当前网络中只有一台AC，客户端可以从同一AC内的一个AP漫游到另一个AP上接入，称为AC内漫游（Intra-AC roaming）。

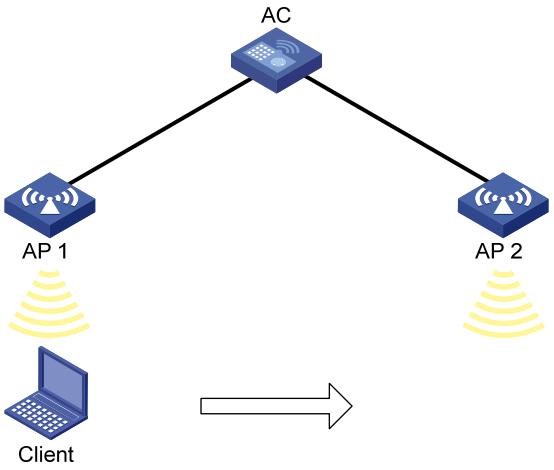
客户端完成 AC 内漫游的过程如下：

(1) 客户端在 AP 1 上初始上线，在 AC 上会创建该客户端的漫游表项信息；

(2) 客户端漫游到 AP 2，AC 查找该客户端的漫游表项，并根据是否是 RSN+802.1X 认证方式决定是否对其进行快速漫游；

(3) 如果进行快速漫游，客户端不需要再次认证，即可在 AP 2 上成功上线；否则需要重新认证。

图1-1 AC 内漫游



2. AC间漫游

如 图 1-2 所示，当前网络中存在多台AC，客户端除了在AC内漫游，还可能从一个AC内的AP漫游到另一个AC内的AP上接入，称为AC间漫游（Inter-AC roaming）。该组网方式下，通过创建漫游组，统一管理参与漫游的AC，没有加入漫游组的AC将不参与漫游。

客户端完成 AC 间漫游的过程如下：

(1) 客户端在 AP 2 上初始上线，在 AC 1 上会创建该客户端的漫游表项，并通过 IACTP 隧道将漫游表项同步到漫游组成员 AC 2 上；

(2) 客户端漫游到 AP 3，AC 2 查找该客户端的漫游表项，根据是否是 RSN+802.1X 认证方式决定是否对其进行快速漫游；

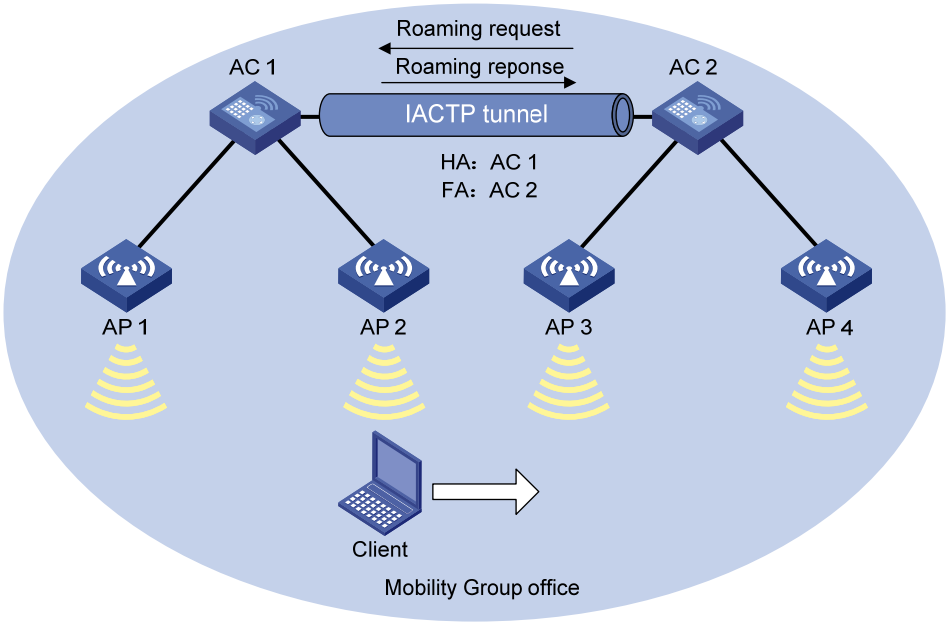
(3) 如果进行快速漫游，客户端不需要再次认证，即可在 AP 3 上成功上线；否则需要重新认证；

(4) 客户端在 AP 3 上线，AC 2 会给 AC 1 发送漫游请求消息；

(5) AC 1 收到漫游请求消息，并校验漫游信息是否正确。如果校验失败，则给 AC 2 回复漫游失败的漫游响应消息。如果校验成功，AC 1 添加该客户端的漫游轨迹和漫出信息，并给 AC 2 回复漫游成功的漫游响应信息；

(6) AC 2 收到 AC 1 回复的漫游响应信息。如果漫游失败，AC 2 将通知客户端下线；如果漫游成功，AC 2 添加该客户端的漫入信息。

图1-2 AC 间漫游



1.2 链路聚合

以太网链路聚合通过将多条以太网物理链路捆绑在一起形成一条以太网逻辑链路，实现增加链路带宽的目的，同时这些捆绑在一起的链路通过相互动态备份，可以有效地提高链路的可靠性。

1.2.1 聚合组

链路捆绑是通过接口捆绑实现的，多个以太网接口捆绑在一起后形成一个聚合组，而这些被捆绑在一起的以太网接口就称为该聚合组的成员端口。每个聚合组唯一对应着一个逻辑接口，称为聚合接口。聚合组与聚合接口的编号是相同的，例如聚合组 1 对应于聚合接口 1。

二层聚合组/二层聚合接口：二层聚合组的成员端口全部为二层以太网接口，其对应的聚合接口称为二层聚合接口。

聚合接口的速率和双工模式取决于对应聚合组内的选中端口：聚合接口的速率等于所有选中端口的速率之和，聚合接口的双工模式则与选中端口的双工模式相同。

1.2.2 选中/非选中状态

聚合组内的成员端口具有以下两种状态：

- 选中（Selected）状态：此状态下的成员端口可以参与数据的转发，处于此状态的成员端口称为“选中端口”。
- 非选中（Unselected）状态：此状态下的成员端口不能参与数据的转发，处于此状态的成员端口称为“非选中端口”。

1.2.3 操作Key

操作 Key 是系统在进行链路聚合时用来表征成员端口聚合能力的一个数值，它是根据成员端口上的一些信息（包括该端口的速率、双工模式等）的组合自动计算生成的，这个信息组合中任何一项的变化都会引起操作 Key 的重新计算。在同一聚合组中，所有的选中端口都必须具有相同的操作 Key。

1.2.4 属性类配置

属性类配置：包含的配置内容如 表 1-1 所示。在聚合组中，只有与对应聚合接口的属性类配置完全相同的成员端口才能够成为选中端口。

表1-1 属性类配置

配置项	内容
VLAN配置	端口上允许通过的VLAN、端口缺省VLAN、VLAN报文是否带Tag配置

1.2.5 聚合模式

链路聚合分为静态聚合和动态聚合两种模式，处于静态聚合模式下的聚合组称为静态聚合组，处于动态聚合模式下的聚合组称为动态聚合组。

静态聚合和动态聚合工作时首先要选取参考端口，之后再确定成员端口的状态。

1. 静态聚合

(1) 选择参考端口

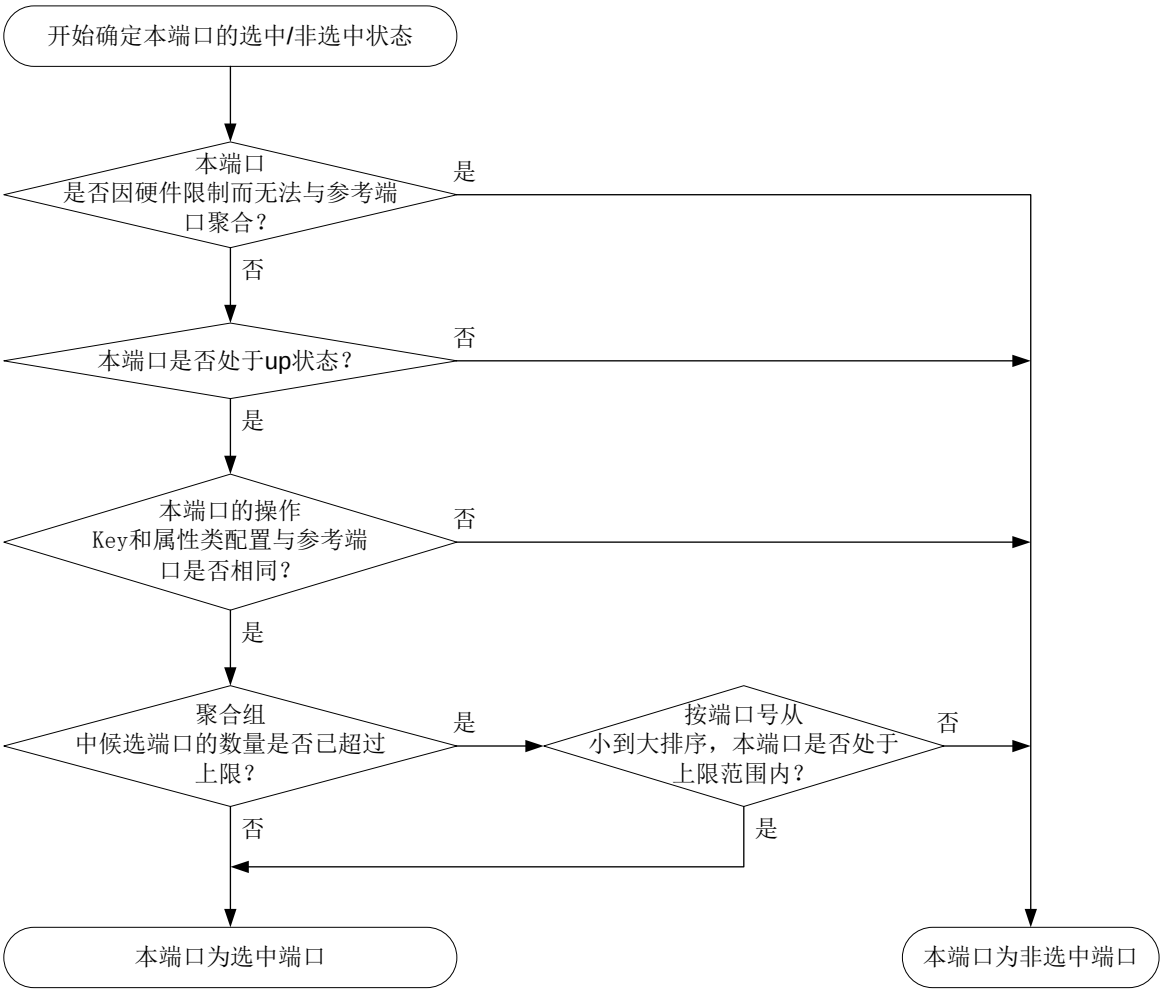
参考端口从本端的成员端口中选出，其操作 Key 和属性类配置将作为同一聚合组内的其他成员端口的参照，只有操作 Key 和属性类配置与参考端口一致的成员端口才能被选中。

对于聚合组内处于 up 状态的端口，按照端口的高端口优先级->全双工/高速率->全双工/低速率->半双工/高速率->半双工/低速率的优先次序，选择优先次序最高、且属性类配置与对应聚合接口相同的端口作为参考端口；如果多个端口优先次序相同，首先选择原来的选中端口作为参考端口；如果此时多个优先次序相同的端口都是原来的选中端口，则选择其中端口号最小的端口作为参考端口；如果多个端口优先次序相同，且都不是原来的选中端口，则选择其中端口号最小的端口作为参考端口。

(2) 确定成员端口状态

静态聚合组内成员端口状态的确定流程如 图 1-3 所示。

图1-3 静态聚合组内成员端口状态的确定流程



2. 动态聚合

动态聚合模式通过 LACP（Link Aggregation Control Protocol，链路聚合控制协议）协议实现，动态聚合组内的成员端口可以收发 LACPDU（Link Aggregation Control Protocol Data Unit，链路聚合控制协议数据单元），本端通过向对端发送 LACPDU 通告本端的信息。当对端收到该 LACPDU 后，将其中的信息与所在端其他成员端口收到的信息进行比较，以选择能够处于选中状态的成员端口，使双方可以对各自接口的选中/非选中状态达成一致。

(1) 选择参考端口

参考端口从聚合链路两端处于 up 状态的成员端口中选出，其操作 Key 和属性类配置将作为同一聚合组内的其他成员端口的参照，只有操作 Key 和属性类配置与参考端口一致的成员端口才能被选中。

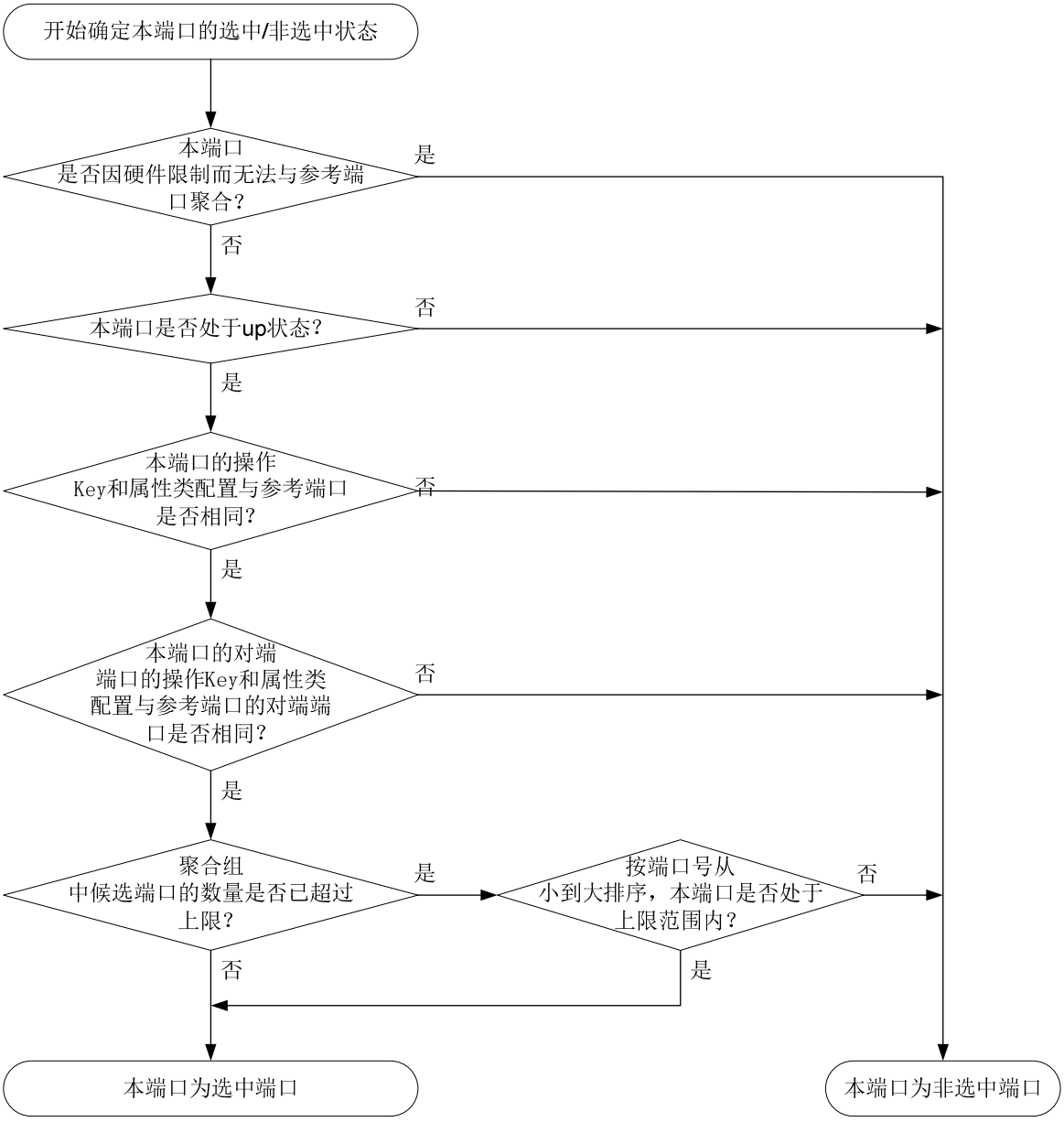
- 首先，从聚合链路的两端选出设备 ID（由系统的 LACP 优先级和系统的 MAC 地址共同构成）较小的一端：先比较两端的系统 LACP 优先级，优先级数值越小其设备 ID 越小；如果优先级相同再比较其系统 MAC 地址，MAC 地址越小其设备 ID 越小。
- 其次，对于设备 ID 较小的一端，再比较其聚合组内各成员端口的端口 ID（由端口优先级和端口的编号共同构成）：先比较端口优先级，优先级数值越小其端口 ID 越小；如果优先级相同再

比较其端口号，端口号越小其端口 ID 越小。端口 ID 最小、且属性类配置与对应聚合接口相同的端口作为参考端口。

(2) 确定成员端口的状态

在设备ID较小的一端，动态聚合组内成员端口状态的确定流程如 图 1-4 所示。

图1-4 动态聚合组内成员端口状态的确定流程



与此同时，设备 ID 较大的一端也会随着对端成员端口状态的变化，随时调整本端各成员端口的状态，以确保聚合链路两端成员端口状态的一致。

3. 静态聚合和动态聚合的优点

静态聚合和动态聚合的优点分别为：

- 静态聚合模式：一旦配置好后，端口的转发流量的状态就不会受网络环境的影响，比较稳定。
- 动态聚合模式：能够根据对端和本端的信息调整端口的转发流量的状态，比较灵活。

1.3 PPPoE

PPPoE（Point-to-Point Protocol over Ethernet，在以太网上承载 PPP 协议）的提出，解决了 PPP 无法应用于以太网的问题，是对 PPP 协议的扩展。

1.3.1 PPPoE概述

PPPoE 描述了在以太网上建立 PPPoE 会话及封装 PPP 报文的方法。要求通信双方建立的是点到点关系，而不是在以太网中所出现的点到多点关系。

PPPoE 利用以太网将大量主机组成网络，然后通过一个远端接入设备为以太网上的主机提供互联网接入服务，并对接入的每台主机实现控制、认证、计费功能。由于很好地结合了以太网的经济性及 PPP 良好的可扩展性与管理控制功能，PPPoE 被广泛应用于小区接入组网等环境中。

PPPoE 协议将 PPP 报文封装在以太网帧之内，在以太网上提供点对点的连接。关于 PPPoE 的详细介绍，可以参考 RFC 2516。

1.3.2 PPPoE组网结构

说明

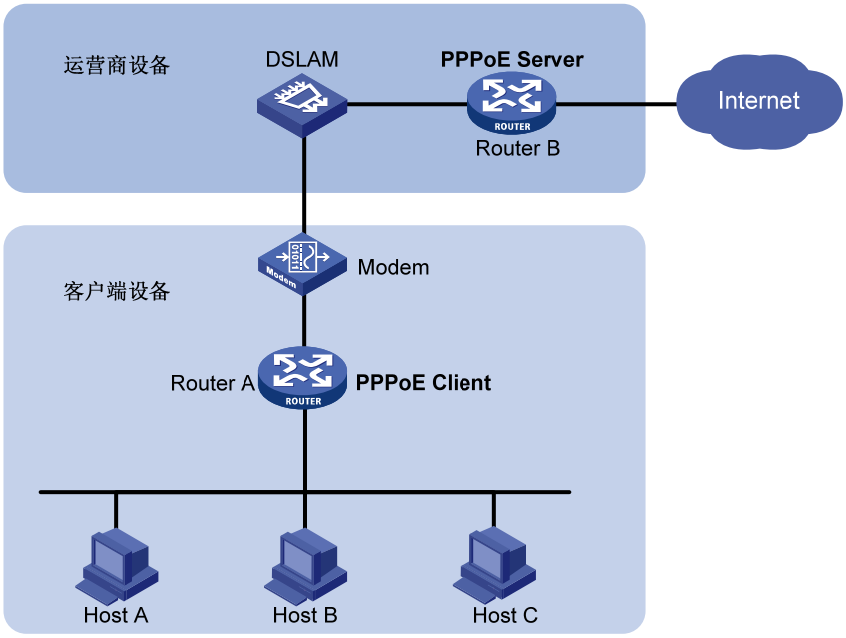
目前设备作为 PPPoE Client 接入网络。

PPPoE 使用 Client/Server 模型。PPPoE Client 向 PPPoE Server 发起连接请求，两者之间会话协商通过后，就建立 PPPoE 会话，此后 PPPoE Server 向 PPPoE Client 提供接入控制、认证、计费等功能。

常见组网如下：

在两台路由器之间建立 PPPoE 会话，所有主机通过同一个 PPPoE 会话传送数据，主机上不用安装 PPPoE 客户端拨号软件，一般是一个企业共用一个账号接入网络（图中 PPPoE Client 位于企业/公司内部，PPPoE Server 是运营商的设备）。

图1-5 PPPoE 组网结构图



1.4 VLAN

VLAN（Virtual Local Area Network，虚拟局域网）技术可以把一个物理 LAN 划分成多个逻辑的 LAN——VLAN，每个 VLAN 是一个广播域。处于同一 VLAN 的主机能够直接互通，而处于不同 VLAN 的主机不能够直接互通。

1.4.1 基于端口划分VLAN

VLAN 可以基于端口进行划分。它按照设备端口来定义 VLAN 成员，将指定端口加入到指定 VLAN 中之后，端口就可以转发该 VLAN 的报文。

在某 VLAN 内，可根据需要配置端口加入 Untagged 端口列表或 Tagged 端口列表（即配置端口为 Untagged 端口或 Tagged 端口），从 Untagged 端口发出的该 VLAN 报文不带 VLAN Tag，从 Tagged 端口发出的该 VLAN 报文带 VLAN Tag。

端口的链路类型分为三种。在端口加入某 VLAN 时，对不同链路类型的端口加入的端口列表要求不同：

- Access：端口只能发送一个 VLAN 的报文，发出去的报文不带 VLAN Tag。该端口只能加入一个 VLAN 的 Untagged 端口列表。
- Trunk：端口能发送多个 VLAN 的报文，发出去的端口缺省 VLAN 的报文不带 VLAN Tag，其他 VLAN 的报文都必须带 VLAN Tag。在端口缺省 VLAN 中，该端口只能加入 Untagged 端口列表；在其他 VLAN 中，该端口只能加入 Tagged 端口列表。
- Hybrid：端口能发送多个 VLAN 的报文，端口发出去的报文可根据需要配置某些 VLAN 的报文带 VLAN Tag，某些 VLAN 的报文不带 VLAN Tag。在不同 VLAN 中，该端口可以根据需要加入 Untagged 端口列表或 Tagged 端口列表。

1.4.2 VLAN接口

不同VLAN间的主机不能直接通信，通过设备上的VLAN接口，可以实现VLAN间的三层互通。VLAN接口是一种三层的虚拟接口，它不作为物理实体存在于设备上。每个 VLAN 对应一个 VLAN 接口，VLAN 接口的 IP 地址可作为本 VLAN 内网络设备的网关地址，对需要跨网段的报文进行基于 IP 地址的三层转发。

1.5 MAC

MAC（Media Access Control，媒体访问控制）地址表记录了 MAC 地址与接口的对应关系，以及接口所属的 VLAN 等信息。设备在转发报文时，根据报文的目的 MAC 地址查询 MAC 地址表，如果MAC地址表中包含与报文目的MAC地址对应的表项，则直接通过该表项中的出接口转发该报文；如果 MAC 地址表中没有包含报文目的 MAC 地址对应的表项时，设备将采取广播的方式通过对应 VLAN 内除接收接口外的所有接口转发该报文。

1.5.1 MAC地址表分类

MAC 地址表项分为以下几种：

- 动态 MAC 地址表项：可以由用户手工配置，也可以由设备通过源 MAC 地址学习自动生成，用于目的是某个 MAC 地址的报文从对应接口转发出去，表项有老化时间。手工配置的动态 MAC 地址表项优先级等于自动生成的 MAC 地址表项。
- 静态 MAC 地址表项：由用户手工配置，用于目的是某个 MAC 地址的报文从对应接口转发出去，表项不老化。静态 MAC 地址表项优先级高于自动生成的 MAC 地址表项。

1.5.2 MAC地址表项老化时间

MAC 地址表中自动生成的表项并非永远有效，每一条表项都有一个生存周期，这个生存周期被称作老化时间。配置动态 MAC 地址表项的老化时间后，超过老化时间的动态 MAC 地址表项会被自动删除，设备将重新进行 MAC 地址学习，构建新的动态 MAC 地址表项。如果在到达生存周期前某表项被刷新，则重新计算该表项的老化时间。

用户配置的老化时间过长或者过短，都可能影响设备的运行性能：

- 如果用户配置的老化时间过长，设备可能会保存许多过时的 MAC 地址表项，从而耗尽 MAC 地址表资源，导致设备无法根据网络的变化更新 MAC 地址表。
- 如果用户配置的老化时间太短，设备可能会删除有效的 MAC 地址表项，导致设备广播大量的数据报文，增加网络的负担。

用户需要根据实际情况，配置合适的老化时间。如果网络比较稳定，可以将老化时间配置得长一些或者配置为不老化；否则，可以将老化时间配置得短一些。比如在一个比较稳定的网络，如果长时间没有流量，动态 MAC 地址表项会被全部删除，可能导致设备突然广播大量的数据报文，造成安全隐患，此时可将动态 MAC 地址表项的老化时间设得长一些或不老化，以减少广播，增加网络稳定性和安全性。动态 MAC 地址表项的老化时间作用于全部接口上。

1.5.3 接口MAC地址学习

缺省情况下，MAC 地址学习功能处于开启状态。有时为了保证设备的安全，需要关闭 MAC 地址学习功能。常见的危及设备安全的情况是：非法用户使用大量源 MAC 地址不同的报文攻击设备，导致设备 MAC 地址表资源耗尽，造成设备无法根据网络的变化更新 MAC 地址表。关闭 MAC 地址学习功能可以有效防止这种攻击。在开启全局的 MAC 地址学习功能的前提下，用户可以关闭单个接口的 MAC 地址的学习功能。

如果MAC地址表过于庞大，可能导致设备的转发性能下降。通过配置接口的MAC地址数学习上限，用户可以控制设备维护的 MAC 地址表的表项数量。当接口学习到的 MAC 地址数达到上限时，该接口将不再对 MAC 地址进行学习，同时，用户还可以根据需要选择是否允许系统转发源 MAC 不在 MAC 地址表里的报文。

1.6 STP

生成树协议运行于二层网络中，通过阻塞冗余链路构建出无数据环路的树型网络拓扑，并在设备或数据链路故障时，重新计算出新的树型拓扑。

生成树协议包括 STP、RSTP、PVST 和 MSTP。

- STP：由 IEEE 制定的 802.1D 标准定义，是狭义的生成树协议。
- RSTP：由 IEEE 制定的 802.1w 标准定义，它在 STP 基础上进行了改进，实现了网络拓扑的快速收敛。其“快速”体现在，当一个端口被选为根端口和指定端口后，其进入转发状态的延时将大大缩短，从而缩短了网络最终达到拓扑稳定所需要的时间。
- PVST：PVST 为每个 VLAN 维护一个单独的生成树实例。每个 VLAN 都将运行单个生成树，允许以每个 VLAN 为基础开启或关闭生成树。每个 VLAN 内的生成树实例都有单独的网络拓扑结构，相互之间没有影响。
- MSTP：由 IEEE 制定的 802.1s 标准定义，它可以弥补 STP 和 RSTP 的缺陷，既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径转发，从而为冗余链路提供了更好的负载分担机制。

1.6.1 生成树工作模式

生成树的工作模式有以下几种：

- STP 模式：设备的所有端口都将向外发送 STP BPDU。如果端口的对端设备只支持 STP，可选择此模式。
- RSTP 模式：设备的所有端口都向外发送 RSTP BPDU。当端口收到对端设备发来的 STP BPDU 时，会自动迁移到 STP 模式；如果收到的是 MSTP BPDU，则不会进行迁移。
- PVST 模式：对于 Access 端口，PVST 将根据该 VLAN 的状态发送 RSTP 格式的 BPDU。对于 Trunk 端口和 Hybrid 端口，PVST 将在缺省 VLAN 内根据该 VLAN 的状态发送 RSTP 格式的 BPDU，而对于其他本端口允许通过的 VLAN，则发送 PVST 格式的 BPDU。
- MSTP 模式：设备的所有端口都向外发送 MSTP BPDU。当端口收到对端设备发来的 STP BPDU 时，会自动迁移到 STP 模式；如果收到的是 RSTP BPDU，则不会进行迁移。

1.6.2 MSTP基本概念

MSTP 把一个交换网络划分成多个域，这些域称为 MST（Multiple Spanning Tree Regions，多生成树域）域。每个域内形成多棵生成树，各生成树之间彼此独立并分别与相应的 VLAN 对应，每棵生成树都称为一个 MSTI（Multiple Spanning Tree Instance，多生成树实例）。CST（Common Spanning Tree，公共生成树）是一棵连接交换网络中所有 MST 域的单生成树。IST（Internal Spanning Tree，内部生成树）是 MST 域内的一棵生成树，它是一个特殊的 MSTI，通常也称为 MSTI 0，所有 VLAN 缺省都映射到 MSTI 0 上。CIST（Common and Internal Spanning Tree，公共和内部生成树）是一棵连接交换网络内所有设备的单生成树，所有 MST 域的 IST 再加上 CST 就共同构成了整个交换网络的一棵完整的单生成树。

其中，对于属于同一 MST 域的设备具有下列特点：

- 都使能了生成树协议。
- 域名相同。
- VLAN 与 MSTI 间映射关系的配置相同。
- MSTP 修订级别的配置相同。
- 这些设备之间有物理链路连通。

1.6.3 生成树端口角色

生成树可能涉及到的端口角色有以下几种：

- 根端口（Root Port）：在非根桥上负责向根桥方向转发数据的端口就称为根端口，根桥上没有根端口。
- 指定端口（Designated Port）：负责向下游网段或设备转发数据的端口就称为指定端口。
- 替换端口（Alternate Port）：是根端口或主端口的备份端口。当根端口或主端口被阻塞后，替换端口将成为新的根端口或主端口。
- 备份端口（Backup Port）：是指定端口的备份端口。当指定端口失效后，备份端口将转换为新的指定端口。当使能了生成树协议的同一台设备上的两个端口互相连接而形成环路时，设备会将其中一个端口阻塞，该端口就是备份端口。
- 主端口（Master Port）：是将 MST 域连接到总根的端口（主端口不一定在域根上），位于整个域到总根的最短路径上。主端口是 MST 域中的报文去往总根的必经之路。主端口在 IST/CIST 上的角色是根端口，而在其他 MSTI 上的角色则是主端口。

STP 只涉及根端口、指定端口和替换端口三种端口角色，RSTP 的端口角色中新增了备份端口，MSTP 涉及所有的端口角色。

1.6.4 生成树端口状态

RSTP和MSTP中的端口状态可分为三种，如 表 1-2 所示。

表1-2 RSTP 和 MSTP 中的端口状态

状态	描述
Forwarding	该状态下的端口可以接收和发送BPDU，也转发用户流量
Learning	是一种过渡状态，该状态下的端口可以接收和发送BPDU，但不转发用户流量

状态	描述
Discarding	该状态下的端口可以接收和发送BPDU，但不转发用户流量

STP 定义了五种端口状态：Disabled、Blocking、Listening、Learning 和 Forwarding。其中 Disabled、Blocking 和 Listening 状态都对应 RSTP/MSTP 中的 Discarding 状态。

1.7 路由表

实现了对路由表的查看，包括路由表的概要信息和统计信息。

1.8 静态路由

静态路由是一种特殊的路由，由管理员手工配置。当网络结构比较简单时，只需配置静态路由就可以使网络正常工作。静态路由不能自动适应网络拓扑结构的变化，当网络发生故障或者拓扑发生变化后，必须由管理员手工修改配置。

缺省路由是在没有找到匹配的路由表项时使用的路由。配置 IPv4 缺省路由时，指定目的地址为 0.0.0.0/0；配置 IPv6 缺省路由时，指定目的地址为::/0。

1.9 IP

1.9.1 IP地址分类和表示

IP 地址是每个连接到 IPv4 网络上的设备的唯一标识。IP 地址长度为 32 比特，通常采用点分十进制方式表示，即每个 IP 地址被表示为以小数点隔开的 4 个十进制整数，每个整数对应一个字节，如 10.1.1.1。

IP 地址由两部分组成：

- 网络号码字段（Net-id）：用于区分不同的网络。网络号码字段的前几位称为类别字段（又称为类别比特），用来区分 IP 地址的类型。
- 主机号码字段（Host-id）：用于区分一个网络内的不同主机。

IP地址分为 5 类，每一类地址范围如 表 1-3 所示。目前大量使用的IP地址属于A、B、C三类。

表1-3 IP 地址分类

地址类型	地址范围	说明
A	0.0.0.0～127.255.255.255	IP地址0.0.0.0仅用于主机在系统启动时进行临时通信，并且永远不是有效目的地址 127.0.0.0网段的地址都保留作环回测试，发送到这个地址的分组不会输出到链路上，它们被当作输入分组在内部进行处理
B	128.0.0.0～191.255.255.255	-
C	192.0.0.0～223.255.255.255	-
D	224.0.0.0～239.255.255.255	组播地址
E	240.0.0.0～255.255.255.255	255.255.255.255用于广播地址，其它地址保留今后使

地址类型	地址范围	说明
		用

1.9.2 子网和掩码

随着 Internet 的快速发展，IP 地址已近枯竭。为了充分利用已有的 IP 地址，可以使用子网掩码将网络划分为更小的部分（即子网）。通过从主机号码字段部分划出一些比特位作为子网号码字段，能够将一个网络划分为多个子网。子网号码字段的长度由子网掩码确定。

子网掩码是一个长度为 32 比特的数字，由一串连续的“1”和一串连续的“0”组成。“1”对应于网络号码字段和子网号码字段，而“0”对应于主机号码字段。

多划分出一个子网号码字段会浪费一些 IP 地址。例如，一个 B 类地址可以容纳 65534（2^{16}-2，去掉主机号码字段全 1 的广播地址和主机号码字段全 0 的网段地址）个主机号码。但划分出 9 比特长的子网字段后，最多可有 512（2^9）个子网，每个子网有 7 比特的主机号码，即每个子网最多可有 126（2^7-2，去掉主机号码字段全 1 的广播地址和主机号码字段全 0 的网段地址）个主机号码。因此主机号码的总数是 512*126=64512 个，比不划分子网时要少 1022 个。

若不进行子网划分，则子网掩码为默认值，此时子网掩码中“1”的长度就是网络号码的长度，即 A、B、C 类 IP 地址对应的子网掩码默认值分别为 255.0.0.0、255.255.0.0 和 255.255.255.0。

1.9.3 IP地址的配置方式

接口获取 IP 地址有以下几种方式：

- 通过手动指定 IP 地址
- 通过 DHCP 分配得到 IP 地址

1.9.4 接口MTU

当设备收到一个报文后，如果发现报文长度比转发接口的 MTU 值大，则进行下列处理：

- 如果报文不允许分片，则将报文丢弃；
- 如果报文允许分片，则将报文进行分片转发。

为了减轻转发设备在传输过程中的分片和重组数据包的压力，更高效的利用网络资源，请根据实际组网环境设置合适的接口 MTU 值，以减少分片的发生。

1.10 IPv6

IPv6（Internet Protocol Version 6，互联网协议版本 6）是网络层协议的第二代标准协议，也被称为 IPng（IP Next Generation，下一代互联网协议），它是 IETF（Internet Engineering Task Force，互联网工程任务组）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：地址的长度从 32 比特增加到 128 比特。

1.10.1 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。
- 如果地址中包含一组或连续多组均为 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。

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，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。

1.10.2 IPv6 地址分类

IPv6 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。

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 1-4 所示。

表1-4 IPv6 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	简介
单播地址	未指定地址	00...0 (128 bits)	::/128	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

地址类型		格式前缀（二进制）	IPv6 前缀标识	简介
	环回地址	00...1 (128 bits)	::1/128	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
	链路本地地址	1111111010	FE80::/10	用于邻居发现协议和无状态自动配置中链路本地上节点之间的通信。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
	全球单播地址	其他形式	-	等同于IPv4公网地址，提供给网络服务提供商。这种类型的地址允许路由前缀的聚合，从而限制了全球路由表项的数量
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		-

1.10.3 IEEE EUI-64 生成接口标识

IPv6 单播地址中的接口标识符用来唯一标识链路上的一个接口。目前 IPv6 单播地址基本上都要求接口标识符为 64 位。

不同接口的 IEEE EUI-64 格式的接口标识符的生成方法不同，分别介绍如下：

- 所有 IEEE 802 接口类型（例如，以太网接口、VLAN 接口）：IEEE EUI-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）。为了使接口标识符的作用范围与原 MAC 地址一致，还要将 Universal/Local (U/L)位（从高位开始的第 7 位）进行取反操作。最后得到的这组数就作为 EUI-64 格式的接口标识符。
- Tunnel 接口：IEEE EUI-64 格式的接口标识符的低 32 位为 Tunnel 接口的源 IPv4 地址，ISATAP 隧道的接口标识符的高 32 位为 0000:5EFE，其他隧道的接口标识符的高 32 位为全 0。
- 其他接口类型（例如，Serial 接口）：IEEE EUI-64 格式的接口标识符由设备随机生成。

1.10.4 接口上全球单播地址的配置方法

IPv6 全球单播地址可以通过下面几种方式配置：

- 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 地址的前缀需要手工配置，而接口标识符则由接口自动生成。
- 手工配置：用户手工配置 IPv6 全球单播地址。
- 无状态自动配置：根据接收到的 RA 报文中携带的地址前缀信息及使用 EUI-64 功能生成的接口标识，自动为接口生成 IPv6 全球单播地址。
- 有状态获取地址：通过 DHCPv6 服务器自动获取 IPv6 地址。

一个接口上可以配置多个全球单播地址。

1.10.5 接口上链路本地地址的配置方法

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::/10）及使用 EUI-64 功能生成的接口标识，自动为接口生成链路本地地址。
- 手工指定：用户手工配置 IPv6 链路本地地址。

每个接口只能有一个链路本地地址，为了避免链路本地地址冲突，推荐使用链路本地地址的自动生成方式。

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，如果删除手工指定的地址，则自动生成的链路本地地址会生效。

1.11 NAT

NAT（Network Address Translation，网络地址转换）是将 IP 数据报文头中的 IP 地址转换为另一个 IP 地址的过程。在实际应用中，NAT 主要应用在连接两个网络的边缘设备上，用于实现允许内部网络用户访问外部公共网络以及允许外部公共网络访问部分内部网络资源（例如内部服务器）的目的。NAT 最初的设计目的是实现私有网络访问公共网络的功能，后扩展为实现任意两个网络间进行访问时的地址转换应用。

1.11.1 动态转换

动态地址转换是指内部网络和外部网络之间的地址映射关系在建立连接的时候动态产生。该方式通常适用于内部网络有大量用户需要访问外部网络的组网环境。动态地址转换存在两种转换模式：

- NO-PAT 模式

  NO-PAT（Not Port Address Translation）模式下，一个外网地址同一时间只能分配给一个内网地址进行地址转换，不能同时被多个内网地址共用。当使用某外网地址的内网用户停止访问外网时，NAT 会将其占用的外网地址释放并分配给其他内网用户使用。

  该模式下，NAT 设备只对报文的 IP 地址进行 NAT 转换，同时会建立一个 NO-PAT 表项用于记录 IP 地址映射关系，并可支持所有 IP 协议的报文。

- PAT 模式

  PAT（Port Address Translation）模式下，一个 NAT 地址可以同时分配给多个内网地址共用。该模式下，NAT 设备需要对报文的 IP 地址和传输层端口同时进行转换，且只支持 TCP、UDP 和 ICMP（Internet Control Message Protocol，因特网控制消息协议）查询报文。

  采用 PAT 方式可以更加充分地利用 IP 地址资源，实现更多内部网络主机对外部网络的同时访问。

1.11.2 内部服务器

在实际应用中，内网中的服务器可能需要对外部网络提供一些服务，例如给外部网络提供 Web 服务，或是 FTP 服务。这种情况下，NAT 设备允许外网用户通过指定的 NAT 地址和端口访问这些内

部服务器，NAT 内部服务器的配置就定义了 NAT 地址和端口与内网服务器地址和端口的映射关系。NAT 内部服务器支持以下几种内网和外网的地址、端口映射关系。

表1-5 NAT 内部服务器的地址与端口映射关系

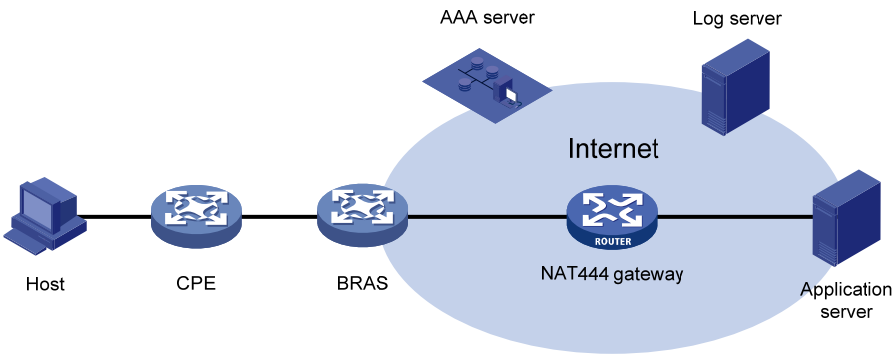
外网	内网
一个外网地址	一个内网地址
一个外网地址、一个端口号	一个内网地址、一个内网端口号
一个外网地址，N个连续的外网端口号	一个内网地址，一个内网端口
	N个连续的内网地址，一个内网端口号
	一个内网地址，N个连续的内网端口号
N个连续的外网地址	一个内网地址
	N个连续的内网地址
N个连续的外网地址连续，一个外网端口号	一个内网地址，一个内网端口号
	N个连续的内网地址，一个内网端口号
	一个内网地址，N个连续的内网端口号
一个外网地址，一个外网端口号	一个内部服务器组
一个外网地址，N个连续的外网端口号	
N个连续的外网地址，一个外网端口号	

1.11.3 NAT 444 地址转换

NAT444 是运营商网络部署 NAT 的整体解决方案，它基于 NAT444 网关，结合 AAA 服务器、日志服务器等配套系统，提供运营商级的 NAT，并支持用户溯源等功能。在众多 IPv4 向 IPv6 网络过渡的技术中，NAT444 仅需在运营商侧引入二次 NAT，对终端和应用服务器端的更改较小，并且 NAT444 通过端口块分配方式解决用户溯源等问题，因此成为了运营商的首选 IPv6 过渡方案。

NAT444 解决方案的架构如 图 1-6 所示。

图1-6 NAT444 解决方案架构



- CPE：实现用户侧地址转换。

- BRAS：负责接入终端，并配合 AAA 完成用户认证、授权和计费。
- NAT444 网关：实现运营商级地址转换。
- AAA 服务器：负责用户认证、授权和计费等。
- 日志服务器：接受和记录用户访问信息，响应用户访问信息查询。

NAT444 网关设备进行的地址转换（以下称为“NAT444 地址转换”）是一种 PAT 方式的动态地址转换，但与普通 PAT 方式动态地址转换不同的是，NAT444 地址转换是基于端口块（即一个端口范围）的方式来复用公网 IP 地址的，即一个私网 IP 地址在一个时间段内独占一个公网 IP 地址的某个端口块。例如：假设私网 IP 地址 10.1.1.1 独占公网 IP 地址 202.1.1.1 的一个端口块 10001～10256，则该私网 IP 向公网发起的所有连接，源 IP 地址都将被转换为同一个公网 IP 地址 202.1.1.1，而源端口将被转换为端口块 10001～10256 之内的一个端口。

1. NAT444 静态转换

NAT444 静态地址转换是指，NAT 网关设备根据配置自动计算私网 IP 地址到公网 IP 地址、端口块的静态映射关系，并创建静态端口块表项。当私网 IP 地址成员中的某个私网 IP 地址向公网发起新建连接时，根据私网 IP 地址匹配静态端口块表项，获取对应的公网 IP 地址和端口块，并从端口块中动态为其分配一个公网端口，对报文进行地址转换。

配置 NAT444 静态地址转换时，需要创建一个端口块组，并在端口块组中配置私网 IP 地址成员、公网 IP 地址成员、端口范围和端口块大小。假设端口块组中每个公网 IP 地址的可用端口块数为 m（即端口范围除以端口块大小），则端口块静态映射的算法如下：按照从小到大的顺序对私网 IP 地址成员中的所有 IP 地址进行排列，最小的 m 个私网 IP 地址对应最小的公网 IP 地址及其端口块，端口块按照起始端口号从小到大的顺序分配；次小的 m 个私网 IP 地址对应次小的公网 IP 地址及其端口块，端口块的分配顺序相同；依次类推。

2. NAT444 动态转换

NAT444 动态地址转换融合了普通 NAT 动态地址转换和 NAT444 静态地址转换的特点。当内网用户向公网发起连接时，首先根据动态地址转换中的 ACL 规则进行过滤，决定是否需要进行源地址转换。对于需要进行源地址转换的连接，当该连接为该用户的首次连接时，从所匹配的动态地址转换配置引用的 NAT 地址组中获取一个公网 IP 地址，从该公网 IP 地址中动态分配一个端口块，创建动态端口块表项，然后从端口块表项中动态分配一个公网端口，进行地址转换。对该用户后续连接的转换，均从生成的动态端口块表项中分配公网端口。当该用户的所有连接都断开时，回收为其分配的端口块资源，删除相应的动态端口块表项。

NAT444 动态地址转换支持增量端口块分配。当为某私网 IP 地址分配的端口块资源耗尽（端口块中的所有端口都被使用）时，如果该私网 IP 地址向公网发起新的连接，则无法再从端口块中获取端口，无法进行地址转换。此时，如果预先在相应的 NAT 地址组中配置了增量端口块数，则可以为该私网 IP 地址分配额外的端口块，进行地址转换。

1.11.4 高级设置

1. NAT地址组

一个 NAT 地址组是多个地址组成员的集合。当需要对到达外部网络的数据报文进行地址转换时，报文的源地址将被转换为地址组成员中的某个地址。

2. NAT444 地址组

NAT444 地址组与 NAT 地址组的配置基本相同，所不同的是，NAT444 地址组必须配置端口块参数（端口范围、端口块大小和增量端口块数）以实现基于端口块的 NAT444 地址转换。

3. 端口块组

配置 NAT444 端口块静态映射需要创建一个端口块组，并在接口的出方向上应用该端口块组。端口块组中需要配置私网 IP 地址成员、公网 IP 地址成员、端口范围和端口块大小，系统会根据端口块组中的配置自动计算私网 IP 地址到公网 IP 地址、端口块的静态映射关系，创建静态端口块表项，并根据表项进行 NAT444 地址转换。

4. 服务器组

在配置内部服务器时，将内部服务器的内网信息指定为一个内部服务器组，组内的多台主机可以共同对外提供某种服务。外网用户向内部服务器指定的外网地址发起应用请求时，NAT 设备可根据内网服务器的权重和当前连接数，选择其中一台内网服务器作为目的服务器，实现内网服务器负载分担。

5. PAT方式地址转换模式

目前，PAT 支持两种不同的地址转换模式：

- Endpoint-Independent Mapping（不关心对端地址和端口转换模式）：只要是来自相同源地址和源端口号的报文，不论其目的地址是否相同，通过 PAT 映射后，其源地址和源端口号都被转换为同一个外部地址和端口号，该映射关系会被记录下来并生成一个 EIM 表项；并且 NAT 设备允许所有外部网络的主机通过该转换后的地址和端口来访问这些内部网络的主机。这种模式可以很好的支持位于不同 NAT 网关之后的主机进行互访。
- Address and Port-Dependent Mapping（关心对端地址和端口转换模式）：对于来自相同源地址和源端口号的报文，相同的源地址和源端口号并不要求被转换为相同的外部地址和端口号，若其目的地址或目的端口号不同，通过 PAT 映射后，相同的源地址和源端口号通常会被转换成不同的外部地址和端口号。与 Endpoint-Independent Mapping 模式不同的是，NAT 设备只允许这些目的地址对应的外部网络的主机可以通过该转换后的地址和端口来访问这些内部网络的主机。这种模式安全性好，但由于同一个内网主机地址转换后的外部地址不唯一，因此不便于位于不同 NAT 网关之后的主机使用内网主机转换后的地址进行互访。

6. DNS映射

通过配置 DNS 映射，可以在 DNS 服务器位于外网的情况下，实现内网用户可通过域名访问位于同一内网的内部服务器的功能。DNS 映射功能需要和内部服务器配合使用，由内部服务器对外提供服务的外网 IP 地址和端口号，由 DNS 映射建立“内部服务器域名<-->外网 IP 地址+外网端口号+协议类型”的映射关系。

NAT 设备对来自外网的 DNS 响应报文进行 DNS ALG 处理时，由于载荷中只包含域名和应用服务器的外网 IP 地址（不包含传输协议类型和端口号），当接口上存在多条 NAT 服务器配置且使用相同的外网地址而内网地址不同时，DNS ALG 仅使用 IP 地址来匹配内部服务器可能会得到错误的匹配结果。因此需要借助 DNS 映射的配置，指定域名与应用服务器的外网 IP 地址、端口和协议的映射关系，由域名获取应用服务器的外网 IP 地址、端口和协议，进而（在当前 NAT 接口上）精确匹配内部服务器配置获取应用服务器的内网 IP 地址。

7. NAT Hairpin

通过在内网侧接口上使能 NAT hairpin 功能，可以实现内网用户使用 NAT 地址访问内网服务器或内网其它用户。NAT hairpin 功能需要与内部服务器、出方向动态地址转换或出方向静态地址转换配合工作，且这些配置所在的接口必须在同一个接口板，否则 NAT hairpin 功能无法正常工作。

该功能在不同工作方式下的具体转换过程如下：

- C/S 方式：NAT 在内网接口上同时转换访问内网服务器的报文的源和目的 IP 地址，其中，目的 IP 地址转换通过匹配某外网接口上的内部服务器配置来完成，源地址转换通过匹配内部服务器所在接口上的出方向动态地址转换或出方向静态地址转换来完成。
- P2P 方式：内网各主机首先向外网服务器注册自己的内网地址信息，该地址信息为外网侧出方向地址转换的 NAT 地址，然后内网主机之间通过使用彼此向外网服务器注册的外网地址进行互访。该方式下，外网侧的出方向地址转换必须配置为 PAT 转换方式，并使能 EIM 模式。

8. 开启NAT ALG功能

通过开启指定应用协议类型的 ALG 功能，实现对应用层报文数据载荷字段的分析和 NAT 处理。

9. NAT日志

(1) NAT 会话日志

NAT 会话日志是为了满足网络管理员安全审计的需要，对 NAT 会话（报文经过设备时，源或目的信息被 NAT 进行过转换的连接）信息进行的记录，包括 IP 地址及端口的转换信息、用户的访问信息以及用户的网络流量信息。

有三种情况可以触发设备生成 NAT 会话日志：

- 新建 NAT 会话。
- 删除 NAT 会话。新增高优先级的配置、删除配置、报文匹配规则变更、NAT 会话老化以及执行删除 NAT 会话的命令时，都可能导致 NAT 会话被删除。
- 存在 NAT 活跃流。NAT 活跃流是指在一定时间内存在的 NAT 会话。当设置的生成活跃流日志的时间间隔到达时，当前存在的 NAT 会话信息就被记录并生成日志。

(2) NAT444 日志

NAT444 日志分为 NAT444 用户日志和 NAT444 告警信息日志。

NAT444 用户日志是为了满足互联网用户溯源的需要，在 NAT444 地址转换中，对每个用户的私网 IP 地址进行端口块分配或回收时，都会输出一条基于用户的日志，记录私网 IP 地址和端口块的映射关系。在进行用户溯源时，只需根据报文的公网 IP 地址和端口找到对应的端口块分配日志信息，即可确定私网 IP 地址。

有两种情况可以触发设备输出 NAT444 用户日志：

- 端口块分配：端口块静态映射方式下，在某私网 IP 地址的第一个新建连接通过端口块进行地址转换时输出日志；端口块动态映射方式下，在为某私网 IP 地址分配端口块或增量端口块时输出日志。
- 端口块回收：端口块静态映射方式下，在某私网 IP 地址的最后一个连接拆除时输出日志；端口块动态映射方式下，在释放端口块资源（并删除端口块表项）时输出日志。

在 NAT444 地址转换中，如果可为用户分配的公网 IP 地址、端口块或端口块中的端口都被占用，则该用户的后续连接由于没有可用的资源无法对其进行地址转换，相应的报文将被丢弃。为了监控公网 IP 地址和端口块资源的使用情况，可以对端口用满和资源用满两种情况记录告警信息日志。

- 端口用满告警：在私网 IP 地址对应的端口块中的所有端口都被占用的情况下，输出告警信息日志。对于端口块动态映射方式，如果配置了增量端口块分配，则当首次分配的端口块中的端口都被占用时，并不输出日志；只有当增量端口块中的端口也都被占用时，才会输出日志。
- 资源用满告警：在 NAT444 端口块动态映射中，如果所有资源（公网 IP 地址、端口块）都被占用，则输出日志。

1.11.5 注意事项

- 入方向的静态地址转换通常用于与接口上的出方向动态地址转换、内部服务器或出方向静态地址转换配合以实现双向 NAT，不建议单独配置。
- 若接口上同时存在普通 NAT 静态地址转换、普通 NAT 动态地址转换、NAT444 端口块静态映射、NAT444 端口块动态映射和内部服务器的配置，则在地址转换过程中，它们的优先级从高到低依次为：内部服务器；普通 NAT 静态地址转换；NAT444 端口块静态映射；NAT444 动态转换和普通 NAT 动态地址转换，系统对二者不做区分，统一按照 ACL 编号由大到小的顺序匹配。
- 各地址组成员的 IP 地址段不能互相重叠。
- 配置的所有地址组成员包含的地址总数不能少于安全引擎（或安全插卡）的数量。
- 内部服务器组成员按照权重比例对外提供服务，权重值越大的内部服务器组成员对外提供服务的比重越大。
- 在配置 NAT444 日志功能前，必须先配置将用户定制日志发送到日志主机的功能，否则无法产生 NAT444 告警信息日志。

1.12 DHCP

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）用来为网络设备动态地分配 IP 地址等网络配置参数。

DHCP 采用客户端/服务器通信模式，由客户端向服务器提出请求分配网络配置参数的申请，服务器返回为客户端分配的 IP 地址等配置信息，以实现 IP 地址等信息的动态配置。

在 DHCP 的典型应用中，一般包含一台 DHCP 服务器和多台客户端（如 PC 和便携机）。如果 DHCP 客户端和 DHCP 服务器处于不同物理网段时，客户端可以通过 DHCP 中继与服务器通信，获取 IP 地址及其他配置信息。

1.12.1 DHCP服务器

在以下场合通常利用 DHCP 服务器来完成 IP 地址分配：

- 网络规模较大，手工配置需要很大的工作量，并难以对整个网络进行集中管理。
- 网络中主机数目大于该网络支持的 IP 地址数量，无法给每个主机分配一个固定的 IP 地址。例如，Internet 接入服务提供商限制同时接入网络的用户数目，用户必须动态获得自己的 IP 地址。
- 网络中只有少数主机需要固定的 IP 地址，大多数主机没有固定的 IP 地址需求。

DHCP 服务器通过地址池来保存为客户端分配的 IP 地址、租约时长、网关信息、域名后缀、DNS 服务器地址、WINS 服务器地址、NetBIOS 节点类型和 DHCP 选项信息。服务器接收到客户端发送的请求后，选择合适的地址池，并将该地址池中的信息分配给客户端。

DHCP 服务器在将 IP 地址分配给客户端之前，还需要进行 IP 地址冲突检测。

1. DHCP地址池

地址池的地址管理方式有以下几种：

- 静态绑定 IP 地址，即通过将客户端的硬件地址或客户端 ID 与 IP 地址绑定的方式，实现为特定的客户端分配特定的 IP 地址。
- 动态选择 IP 地址，即在地址池中指定可供分配的 IP 地址范围，当收到客户端的 IP 地址申请时，从该地址范围中动态选择 IP 地址，分配给该客户端。

在 DHCP 地址池中还可以指定这两种类型地址的租约时长。

DHCP 服务器为客户端分配 IP 地址时，地址池的选择原则如下：

(1) 如果存在将客户端 MAC 地址或客户端 ID 与 IP 地址静态绑定的地址池，则选择该地址池，并将静态绑定的 IP 地址和其他网络参数分配给客户端。

(2) 如果不存在静态绑定的地址池，则按照以下方法选择地址池：

- 如果客户端与服务器在同一网段，则将 DHCP 请求报文接收接口的 IP 地址与所有地址池配置的网段进行匹配，并选择最长匹配的网段所对应的地址池。
- 如果客户端与服务器不在同一网段，即客户端通过 DHCP 中继获取 IP 地址，则将 DHCP 请求报文中 giaddr 字段指定的 IP 地址与所有地址池配置的网段进行匹配，并选择最长匹配的网段所对应的地址池。

2. DHCP服务器分配IP地址的次序

DHCP 服务器为客户端分配 IP 地址的优先次序如下：

(1) 与客户端 MAC 地址或客户端 ID 静态绑定的 IP 地址。

(2) DHCP 服务器记录的曾经分配给客户端的 IP 地址。

(3) 客户端发送的 DHCP-DISCOVER 报文中 Option 50 字段指定的 IP 地址。Option 50 为客户端请求的 IP 地址选项（Requested IP Address），客户端通过在 DHCP-DISCOVER 报文中添加该选项来指明客户端希望获取的 IP 地址。该选项的内容由客户端决定。

(4) 按照动态分配地址选择原则，顺序查找可供分配的 IP 地址，选择最先找到的 IP 地址。

(5) 如果未找到可用的 IP 地址，则从当前匹配地址池中依次查询租约过期、曾经发生过冲突的 IP 地址，如果找到则进行分配，否则将不予处理。

3. DHCP选项

DHCP 利用选项字段传递控制信息和网络配置参数，实现地址动态分配的同时，为客户端提供更加丰富的网络配置信息。

Web 页面为 DHCP 服务器提供了灵活的选项配置方式，在以下情况下，可以使用 Web 页面 DHCP 选项功能：

- 随着 DHCP 的不断发展，新的 DHCP 选项会陆续出现。通过该功能，可以方便地添加新的 DHCP 选项。
- 有些选项的内容，RFC 中没有统一规定。厂商可以根据需要定义选项的内容，如 Option 43。通过 DHCP 选项功能，可以为 DHCP 客户端提供厂商指定的信息。
- Web 页面只提供了有限的配置功能，其他功能可以通过 DHCP 选项来配置。例如，可以通过 Option 4，IP 地址 1.1.1.1 来指定为 DHCP 客户端分配的时间服务器地址为 1.1.1.1。

- 扩展已有的 DHCP 选项。当前已提供的方式无法满足用户需求时（比如通过 Web 页面最多只能配置 8 个 DNS 服务器地址，如果用户需要配置的 DNS 服务器地址数目大于 8，则 Web 页面无法满足需求），可以通过 DHCP 选项功能进行扩展。

常用的DHCP选项配置如 表 1-6 所示。

表1-6 常用 DHCP 选项配置

选项编号	选项名称	推荐的选项填充类型
3	Router Option	IP地址
6	Domain Name Server Option	IP地址
15	Domain Name	ASCII字符串
44	NetBIOS over TCP/IP Name Server Option	IP地址
46	NetBIOS over TCP/IP Node Type Option	十六进制数串
66	TFTP server name	ASCII字符串
67	Bootfile name	ASCII字符串
43	Vendor Specific Information	十六进制数串

4. DHCP服务器的IP地址冲突检测功能

为防止 IP 地址重复分配导致地址冲突，DHCP 服务器为客户端分配地址前，需要先对该地址进行探测。

DHCP 服务器的地址探测是通过 ping 功能实现的，通过检测是否能在指定时间内得到 ping 响应来判断是否存在地址冲突。DHCP 服务器发送目的地址为待分配地址的 ICMP 回显请求报文。如果在指定时间内收到回显响应报文，则认为存在地址冲突。DHCP 服务器从地址池中选择新的 IP 地址，并重复上述操作。如果在指定时间内没有收到回显响应报文，则继续发送 ICMP 回显请求报文，直到发送的回显显示报文数目达到最大值。如果仍然没有收到回显响应报文，则将地址分配给客户端，从而确保客户端获得的 IP 地址唯一。

1.12.2 DHCP中继

由于在 IP 地址动态获取过程中采用广播方式发送请求报文，因此 DHCP 只适用于 DHCP 客户端和服务器处于同一个子网内的情况。为进行动态主机配置，需要在所有网段上都设置一个 DHCP 服务器，这显然是很不经济的。

DHCP 中继功能的引入解决了这一难题：客户端可以通过 DHCP 中继与其他网段的 DHCP 服务器通信，最终获取到 IP 地址。这样，多个网络上的 DHCP 客户端可以使用同一个 DHCP 服务器，既节省了成本，又便于进行集中管理。

1. DHCP中继用户地址表项记录功能

为了防止非法主机静态配置一个 IP 地址并访问外部网络，设备支持 DHCP 中继用户地址表项记录功能。

启用该功能后，当客户端通过 DHCP 中继从 DHCP 服务器获取到 IP 地址时，DHCP 中继可以自动记录客户端 IP 地址与硬件地址的绑定关系，生成 DHCP 中继的用户地址表项。

本功能与其他 IP 地址安全功能（如 ARP 地址检查和授权 ARP）配合，可以实现只允许匹配用户地址表项中绑定关系的报文通过 DHCP 中继。从而，保证非法主机不能通过 DHCP 中继与外部网络通信。

2. DHCP中继动态用户地址表项定时刷新功能

DHCP 客户端释放动态获取的 IP 地址时，会向 DHCP 服务器单播发送 DHCP-RELEASE 报文，DHCP 中继不会处理该报文的内容。如果此时 DHCP 中继上记录了该 IP 地址与 MAC 地址的绑定关系，则会造成 DHCP 中继的用户地址表项无法实时刷新。为了解决这个问题，DHCP 中继支持动态用户地址表项的定时刷新功能。

DHCP 中继动态用户地址表项定时刷新功能开启时，DHCP 中继每隔指定时间采用客户端获取到的 IP 地址和 DHCP 中继接口的 MAC 地址向 DHCP 服务器发送 DHCP-REQUEST 报文：

- 如果 DHCP 中继接收到 DHCP 服务器响应的 DHCP-ACK 报文或在指定时间内没有接收到 DHCP 服务器的响应报文，则表明这个 IP 地址已经可以进行分配，DHCP 中继会删除动态用户地址表中对应的表项。为了避免地址浪费，DHCP 中继收到 DHCP-ACK 报文后，会发送 DHCP-RELEASE 报文释放申请到的 IP 地址。
- 如果 DHCP 中继接收到 DHCP 服务器响应的 DHCP-NAK 报文，则表示该 IP 地址的租约仍然存在，DHCP 中继不会删除该 IP 地址对应的表项。

1.13 DHCP Snooping

DHCP Snooping 是 DHCP 的一种安全特性，具有如下功能：

1. 保证客户端从合法的服务器获取IP地址

网络中如果存在私自架设的非法 DHCP 服务器，则可能导致 DHCP 客户端获取到错误的 IP 地址和网络配置参数，从而无法正常通信。为了使 DHCP 客户端能通过合法的 DHCP 服务器获取 IP 地址，DHCP Snooping 安全机制允许将端口设置为信任端口和不信任端口：

- 信任端口正常转发接收到的 DHCP 报文。
- 不信任端口接收到 DHCP 服务器响应的 DHCP-ACK 和 DHCP-OFFER 报文后，丢弃该报文。

在 DHCP Snooping 设备上指向 DHCP 服务器方向的端口需要设置为信任端口，其他端口设置为不信任端口，从而保证 DHCP 客户端只能从合法的 DHCP 服务器获取 IP 地址，私自架设的伪 DHCP 服务器无法为 DHCP 客户端分配 IP 地址。

2. 记录DHCP Snooping表项

DHCP Snooping 通过监听 DHCP-REQUEST 报文和信任端口收到的 DHCP-ACK 报文，记录 DHCP Snooping 表项，其中包括客户端的 MAC 地址、DHCP 服务器为 DHCP 客户端分配的 IP 地址、与 DHCP 客户端连接的端口及 VLAN 等信息。利用这些信息可以实现 ARP Detection 功能，即根据 DHCP Snooping 表项来判断发送 ARP 报文的用户是否合法，从而防止非法用户的 ARP 攻击。

3. 备份DHCP Snooping表项

DHCP Snooping 设备重启后，设备上记录的 DHCP Snooping 表项将丢失。如果 DHCP Snooping 与其他模块配合使用，则表项丢失会导致这些模块无法通过 DHCP Snooping 获取到相应的表项，进而导致 DHCP 客户端不能顺利通过安全检查、正常访问网络。

DHCP Snooping 表项备份功能将 DHCP Snooping 表项保存到指定的文件中，DHCP Snooping 设备重启后，自动根据该文件恢复 DHCP Snooping 表项，从而保证 DHCP Snooping 表项不会丢失。

4. 支持Option 82 功能

Option 82 记录了 DHCP 客户端的位置信息。管理员可以利用该选项定位 DHCP 客户端，实现对客户端的安全和计费等控制。Option 82 包含两个子选项：Circuit ID 和 Remote ID。

支持 Option 82 功能是指设备接收到 DHCP 请求报文后，根据报文中是否包含 Option 82 以及用户配置的处理策略及填充模式等对报文进行相应的处理，并将处理后的报文转发给 DHCP 服务器。当设备接收到 DHCP 服务器的响应报文时，如果报文中含有 Option 82，则删除 Option 82，并转发给 DHCP 客户端；如果报文中不含有 Option 82，则直接转发。

具体的处理方式见 表 1-7。

表1-7 Option 82 处理方式

收到 DHCP 请求报文	处理策略	DHCP Snooping 对报文的处理
收到的报文中带有Option 82	Drop	丢弃报文
	Keep	保持报文中的Option 82不变并进行转发
	Replace	根据DHCP Snooping上配置的填充模式、内容、格式等填充Option 82，替换报文中原有的Option 82并进行转发
收到的报文中不带有Option 82	-	根据DHCP Snooping上配置的填充模式、内容、格式等填充Option 82，添加到报文中并进行转发

1.14 DNS

DNS（Domain Name System，域名系统）是一种用于 TCP/IP 应用程序的分布式数据库，提供域名与地址之间的转换。IPv4 DNS 提供域名和 IPv4 地址之间的转换，IPv6 DNS 提供域名和 IPv6 地址之间的转换。

设备作为 DNS 客户端，当用户在设备上进行某些应用（如 Telnet 到一台设备或主机）时，可以直接使用便于记忆的、有意义的域名，通过域名系统将域名解析为正确的地址。

域名解析分为动态域名解析和静态域名解析两种。动态域名解析和静态域名解析可以配合使用。在解析域名时，首先采用静态域名解析（查找静态域名解析表），如果静态域名解析不成功，再采用动态域名解析。由于动态域名解析需要域名服务器的配合，会花费一定的时间，因而可以将一些常用的域名放入静态域名解析表中，这样可以大大提高域名解析效率。

1.14.1 动态域名解析

使用动态域名解析时，需要手工指定域名服务器的地址。

动态域名解析通过向域名服务器查询域名和地址之间的对应关系来实现将域名解析为地址。

动态域名解析支持域名后缀列表功能。用户可以预先设置一些域名后缀，在域名解析的时候，用户只需要输入域名的部分字段，系统会自动将输入的域名加上不同的后缀进行解析。例如，用户想查询域名 aabbcc.com，那么可以先在后缀列表中配置 com，然后输入 aabbcc 进行查询，系统会自动将输入的域名与后缀连接成 aabbcc.com 进行查询。

使用域名后缀的时候，根据用户输入域名方式的不同，查询方式分成以下几种情况：

- 如果用户输入的域名中没有“.”，比如 aabbcc，系统认为这是一个主机名，会首先加上域名后缀进行查询，如果所有加后缀的域名查询都失败，将使用最初输入的域名（如 aabbcc）进行查询。
- 如果用户输入的域名中间有“.”，比如 www.aabbcc，系统直接用它进行查询，如果查询失败，再依次加上各个域名后缀进行查询。
- 如果用户输入的域名最后有“.”，比如 aabbcc.com.，表示不需要进行域名后缀添加，系统直接用输入的域名进行查询，不论成功与否都直接返回结果。就是说，如果用户输入的字符中最后一个字符为“.”，就只根据用户输入的字符进行查找，而不会去匹配用户预先设置的域名后缀，因此最后这个“.”，也被称为查询终止符。带有查询终止符的域名，称为 FQDN（Fully Qualified Domain Name，完全合格域名）。

1.14.2 静态域名解析

手工建立域名和地址之间的对应关系。当用户使用域名进行某些应用时，系统查找静态域名解析表，从中获取指定域名对应的地址。

1.14.3 DNS代理

DNS 代理（DNS proxy）用来在 DNS client 和 DNS server 之间转发 DNS 请求和应答报文。局域网内的 DNS client 把 DNS proxy 当作 DNS server，将 DNS 请求报文发送给 DNS proxy。DNS proxy 将该请求报文转发到真正的 DNS server，并将 DNS server 的应答报文返回给 DNS client，从而实现域名解析。

使用 DNS proxy 功能后，当 DNS server 的地址发生变化时，只需改变 DNS proxy 上的配置，无需改变局域网内每个 DNS client 的配置，从而简化了网络管理。

1.15 动态DNS

DNS 仅仅提供了域名和地址之间的静态对应关系，当节点的地址发生变化时，DNS 无法动态地更新域名和地址的对应关系。此时，如果仍然使用域名访问该节点，通过域名解析得到的地址是错误的，从而导致访问失败。

DDNS（Dynamic Domain Name System，动态域名系统）用来动态更新 DNS 服务器上域名和地址之间的对应关系，保证通过域名解析到正确的地址。

使用 DDNS 服务前，用户需要先登录 DDNS 服务器，注册账户。设备作为 DDNS 客户端，在地址变化时，向 DDNS 服务器发送更新域名和地址对应关系的 DDNS 更新请求，更新请求中携带用户的账户信息（用户名和密码）。DDNS 服务器对账户信息认证通过后，通知 DNS 服务器动态更新域名和地址之间的对应关系。

目前，只有 IPv4 域名解析支持 DDNS，IPv6 域名解析不支持 DDNS，即只能通过 DDNS 动态更新域名和 IPv4 地址之间的对应关系。

为了简化配置，设备通过 DDNS 策略来管理和维护 DDNS 客户端的参数，如 DDNS 服务提供商信息（即 DDNS 服务器信息）、用户的账户信息（用户名和密码）、更新时间间隔、关联的 SSL 客户端策略等。创建 DDNS 策略后，可以在不同的接口上应用相同的 DDNS 策略，从而简化 DDNS 的配置。

1.16 IPv6 DNS

DNS（Domain Name System，域名系统）是一种用于 TCP/IP 应用程序的分布式数据库，提供域名与地址之间的转换。IPv4 DNS 提供域名和 IPv4 地址之间的转换，IPv6 DNS 提供域名和 IPv6 地址之间的转换。

设备作为 DNS 客户端，当用户在设备上进行某些应用（如 Telnet 到一台设备或主机）时，可以直接使用便于记忆的、有意义的域名，通过域名系统将域名解析为正确的地址。

域名解析分为动态域名解析和静态域名解析两种。动态域名解析和静态域名解析可以配合使用。在解析域名时，首先采用静态域名解析（查找静态域名解析表），如果静态域名解析不成功，再采用动态域名解析。由于动态域名解析需要域名服务器的配合，会花费一定的时间，因而可以将一些常用的域名放入静态域名解析表中，这样可以大大提高域名解析效率。

1.16.1 动态域名解析

使用动态域名解析时，需要手工指定域名服务器的地址。

动态域名解析通过向域名服务器查询域名和地址之间的对应关系来实现将域名解析为地址。

动态域名解析支持域名后缀列表功能。用户可以预先设置一些域名后缀，在域名解析的时候，用户只需要输入域名的部分字段，系统会自动将输入的域名加上不同的后缀进行解析。例如，用户想查询域名 aabbcc.com，那么可以先在后缀列表中配置 com，然后输入 aabbcc 进行查询，系统会自动将输入的域名与后缀连接成 aabbcc.com 进行查询。

使用域名后缀的时候，根据用户输入域名方式的不同，查询方式分成以下几种情况：

- 如果用户输入的域名中没有“.”，比如 aabbcc，系统认为这是一个主机名，会首先加上域名后缀进行查询，如果所有加后缀的域名查询都失败，将使用最初输入的域名（如 aabbcc）进行查询。
- 如果用户输入的域名中间有“.”，比如 www.aabbcc，系统直接用它进行查询，如果查询失败，再依次加上各个域名后缀进行查询。
- 如果用户输入的域名最后有“.”，比如 aabbcc.com.，表示不需要进行域名后缀添加，系统直接用输入的域名进行查询，不论成功与否都直接返回结果。就是说，如果用户输入的字符中最后一个字符为“.”，就只根据用户输入的字符进行查找，而不会去匹配用户预先设置的域名后缀，因此最后这个“.”，也被称为查询终止符。带有查询终止符的域名，称为 FQDN（Fully Qualified Domain Name，完全合格域名）。

1.16.2 静态域名解析

手工建立域名和地址之间的对应关系。当用户使用域名进行某些应用时，系统查找静态域名解析表，从中获取指定域名对应的地址。

1.16.3 DNS代理

DNS 代理（DNS proxy）用来在 DNS client 和 DNS server 之间转发 DNS 请求和应答报文。局域网内的 DNS client 把 DNS proxy 当作 DNS server，将 DNS 请求报文发送给 DNS proxy。DNS proxy 将该请求报文转发到真正的 DNS server，并将 DNS server 的应答报文返回给 DNS client，从而实现域名解析。

使用 DNS proxy 功能后，当 DNS server 的地址发生变化时，只需改变 DNS proxy 上的配置，无需改变局域网内每个 DNS client 的配置，从而简化了网络管理。

1.17 IGMP Snooping

IGMP snooping（Internet Group Management Protocol snooping，互联网组管理协议窥探）运行在二层设备上，通过侦听三层设备与接收者主机间的 IGMP 报文建立 IGMP snooping 转发表，并根据该表指导组播数据的转发。

IGMP snooping 转发表的表项由 VLAN、组播组地址、组播源地址和成员端口四个元素构成，其中成员端口是指二层设备上朝向组播组成员的端口。

1.18 MLD Snooping

MLD snooping（Multicast Listener Discovery snooping，组播侦听者发现协议窥探）运行在二层设备上，通过侦听三层设备与接收者主机间的 MLD 报文建立 MLD snooping 转发表，并根据该表指导 IPv6 组播数据的转发。

MLD snooping 转发表的表项由 VLAN、IPv6 组播组地址、IPv6 组播源地址和成员端口四个元素构成，其中成员端口是指二层设备上朝向 IPv6 组播组成员的端口。

1.19 ARP

ARP（Address Resolution Protocol，地址解析协议）是将 IP 地址解析为以太网 MAC 地址（或称物理地址）的协议。

设备通过 ARP 协议解析到目的 MAC 地址后，将会在自己的 ARP 表中增加 IP 地址和 MAC 地址映射关系的表项，以用于后续到同一目的地报文的转发。

ARP 表项分为两种：动态 ARP 表项、静态 ARP 表项。

1.19.1 动态ARP表项

动态 ARP 表项由 ARP 协议通过 ARP 报文自动生成和维护，可以被老化，可以被新的 ARP 报文更新，可以被静态 ARP 表项覆盖。当到达老化时间、接口状态 down 时，系统会删除相应的动态 ARP 表项。

动态 ARP 表项可以固化为静态 ARP 表项，但被固化后无法再恢复为动态 ARP 表项。

为了防止部分接口下的用户占用过多的 ARP 资源，可以通过设置接口学习动态 ARP 表项的最大个数来进行限制。

1.19.2 静态ARP表项

静态 ARP 表项通过手工创建或由动态 ARP 表项固化而来，不会被老化，不会被动态 ARP 表项覆盖。

配置静态 ARP 表项可以增加通信的安全性。静态 ARP 表项可以限制和指定 IP 地址的设备通信时只使用指定的 MAC 地址，此时攻击报文无法修改此表项的 IP 地址和 MAC 地址的映射关系，从而保护了本设备和指定设备间的正常通信。

在配置静态 ARP 表项时，如果管理员希望用户使用某个固定的 IP 地址和 MAC 地址通信，可以将该 IP 地址与 MAC 地址绑定；如果进一步希望限定用户只在指定 VLAN 的特定接口上连接，则需要进一步指定报文转发的 VLAN 和出接口。

一般情况下，ARP 动态执行并自动寻求 IP 地址到以太网 MAC 地址的解析，无需管理员的介入。

说明

当静态 ARP 表项中的 IP 地址与 VLAN 虚接口的 IP 地址属于同一网段时，该静态 ARP 表项才能正常指导转发。

1.19.3 代理ARP

如果 ARP 请求是从一个网络的主机发往同一网段却不在同一物理网络上的另一台主机，那么连接它们的具有代理 ARP 功能的设备就可以回答该请求，这个过程称作代理 ARP。

代理 ARP 功能屏蔽了分离的物理网络这一事实，使用户使用起来，好像在同一个物理网络上。

代理 ARP 分为普通代理 ARP 和本地代理 ARP，二者的应用场景有所区别：

- 普通代理 ARP：想要互通的主机分别连接到设备的不同三层接口上，且这些主机不在同一个广播域中。
- 本地代理 ARP：想要互通的主机连接到设备的同一个三层接口上，且这些主机不在同一个广播域中。

在配置本地代理 ARP 时，用户也可以指定进行 ARP 代理的 IP 地址范围。

1.19.4 免费ARP

免费 ARP 报文是一种特殊的 ARP 报文，该报文中携带的发送端 IP 地址和目标 IP 地址都是本机 IP 地址。

设备通过对外发送免费 ARP 报文来实现以下功能：

- 确定其它设备的 IP 地址是否与本机的 IP 地址冲突。当其它设备收到免费 ARP 报文后，如果发现报文中的 IP 地址和自己的 IP 地址相同，则给发送免费 ARP 报文的设备返回一个 ARP 应答，告知该设备 IP 地址冲突。
- 设备改变了硬件地址，通过发送免费 ARP 报文通知其它设备更新 ARP 表项。

1. 学习免费ARP报文功能

启用了学习免费 ARP 报文功能后，设备会根据收到的免费 ARP 报文中携带的信息（发送端 IP 地址、发送端 MAC 地址）对自身维护的 ARP 表进行修改。设备先判断 ARP 表中是否存在与此免费 ARP 报文中的发送端 IP 地址对应的 ARP 表项：

- 如果没有对应的 ARP 表项，设备会根据该免费 ARP 报文中携带的信息新建 ARP 表项。
- 如果存在对应的 ARP 表项，设备会根据该免费 ARP 报文中携带的信息更新对应的 ARP 表项。

关闭学习免费 ARP 报文功能后，设备不会根据收到的免费 ARP 报文来新建 ARP 表项，但是会更新已存在的对应 ARP 表项。如果用户不希望通过免费 ARP 报文来新建 ARP 表项，可以关闭学习免费 ARP 报文功能，以节省 ARP 表项资源。

2. 回复免费ARP报文功能

开启回复免费 ARP 报文功能后，当设备收到非同一网段的 ARP 请求时发送免费 ARP 报文。关闭该功能后，设备收到非同一网段的 ARP 请求时不发送免费 ARP 报文。

3. 接口定时发送免费ARP报文功能

用户可以配置某些接口定时发送免费 ARP 报文，以便及时通知下行设备更新 ARP 表项或者 MAC 地址表项，主要应用场景如下：

- 防止仿冒网关的 ARP 攻击

如果攻击者仿冒网关发送免费 ARP 报文，就可以欺骗同网段内的其它主机，使得被欺骗的主机访问网关的流量被重定向到一个错误的 MAC 地址，导致其它主机用户无法正常访问网络。

为了降低这种仿冒网关的 ARP 攻击所带来的影响，可以在网关的接口上启用定时发送免费 ARP 功能。启用该功能后，网关接口上将按照配置的时间间隔周期性发送接口主 IP 地址和手工配置的从 IP 地址的免费 ARP 报文。这样，每台主机都可以学习到正确的网关，从而正常访问网络。

- 防止主机 ARP 表项老化

在实际环境中，当网络负载较大或接收端主机的 CPU 占用率较高时，可能存在 ARP 报文被丢弃或主机无法及时处理接收到的 ARP 报文等现象。这种情况下，接收端主机的动态 ARP 表项会因超时而老化，在其重新学习到发送设备的 ARP 表项之前，二者之间的流量就会发生中断。

为了解决上述问题，可以在网关的接口上启用定时发送免费 ARP 功能。启用该功能后，网关接口上将按照配置的时间间隔周期性发送接口主 IP 地址和手工配置的从 IP 地址的免费 ARP 报文。这样，接收端主机可以及时更新 ARP 映射表，从而防止了上述流量中断现象。

1.19.5 ARP攻击防御

ARP 协议有简单、易用的优点，但是也因为其没有任何安全机制而容易被攻击发起者利用。目前 ARP 攻击和 ARP 病毒已经成为局域网安全的一大威胁，为了避免各种攻击带来的危害，设备提供了多种技术对攻击进行防范、检测和解决。

不同设备支持配置的 ARP 攻击防御功能如下：

- 网关设备支持配置的功能包括：ARP 黑洞路由、ARP 源抑制、源 MAC 地址一致性检查、ARP 主动确认、源 MAC 地址固定的 ARP 攻击检测、授权 ARP 和 ARP 扫描；
- 接入设备支持配置的功能包括：ARP 网关保护、ARP 过滤保护和 ARP Detection。

1. ARP防止IP报文攻击功能

如果网络中有主机通过向设备发送大量目标 IP 地址不能解析的 IP 报文来攻击设备，则会造成下面的危害：

- 设备向目的网段发送大量 ARP 请求报文，加重目的网段的负载。
- 设备会试图反复地对目标 IP 地址进行解析，增加了 CPU 的负担。

为避免这种 IP 报文攻击所带来的危害，设备提供了下列两个功能：

- ARP 黑洞路由功能：开启该功能后，一旦接收到目标 IP 地址不能解析的 IP 报文，设备立即产生一个黑洞路由，使得设备在一段时间内将去往该地址的报文直接丢弃。等待黑洞路由老化时间过后，如有报文触发则再次发起解析，如果解析成功则进行转发，否则仍然产生一个黑洞路由将去往该地址的报文丢弃。这种方式能够有效地防止 IP 报文的攻击，减轻 CPU 的负担。

- ARP 源抑制功能：如果发送攻击报文的源是固定的，可以采用 ARP 源抑制功能。开启该功能后，如果网络中每 5 秒内从某 IP 地址向设备某接口发送目的 IP 地址不能解析的 IP 报文超过了设置的阈值，则设备将不再处理由此 IP 地址发出的 IP 报文直至该 5 秒结束，从而避免了恶意攻击所造成的危害。

2. ARP报文源MAC地址一致性检查功能

ARP 报文源 MAC 地址一致性检查功能主要应用于网关设备上，防御以太网数据帧首部中的源 MAC 地址和 ARP 报文中的源 MAC 地址不同的 ARP 攻击。

配置本特性后，网关设备在进行 ARP 学习前将对 ARP 报文进行检查。如果以太网数据帧首部中的源 MAC 地址和 ARP 报文中的源 MAC 地址不同，则认为是攻击报文，将其丢弃；否则，继续进行 ARP 学习。

3. ARP主动确认功能

ARP 的主动确认功能主要应用于网关设备上，防止攻击者仿冒用户欺骗网关设备。

启用 ARP 主动确认功能后，设备在新建或更新 ARP 表项前需进行主动确认，防止产生错误的 ARP 表项。

使能严格模式后，新建 ARP 表项前，ARP 主动确认功能会执行更严格的检查：

- 收到目标 IP 地址为自己的 ARP 请求报文时，设备会发送 ARP 应答报文，但不建立 ARP 表项；
- 收到 ARP 应答报文时，需要确认本设备是否对该报文中的源 IP 地址发起过 ARP 解析：若发起过解析，解析成功后则设备启动主动确认功能，主动确认流程成功完成后，设备可以建立该表项；若未发起过解析，则设备丢弃该报文。

4. 源MAC地址固定的ARP攻击检测功能

本特性根据 ARP 报文的源 MAC 地址对上送 CPU 的 ARP 报文进行统计，在 5 秒内，如果收到同一源 MAC 地址（源 MAC 地址固定）的 ARP 报文超过一定的阈值，则认为存在攻击，系统会将此 MAC 地址添加到攻击检测表项中。在该攻击检测表项老化之前，如果设置的检查模式为过滤模式，则会打印日志信息并且将该源 MAC 地址发送的 ARP 报文过滤掉；如果设置的检查模式为监控模式，则只打印日志信息，不会将该源 MAC 地址发送的 ARP 报文过滤掉。

对于网关或一些重要的服务器，可能会发送大量 ARP 报文，为了使这些 ARP 报文不被过滤掉，可以将这类设备的 MAC 地址配置成保护 MAC 地址，这样，即使该设备存在攻击也不会被检测、过滤。

5. 授权ARP功能

所谓授权 ARP，就是动态学习 ARP 的过程中，只有和 DHCP 服务器生成的租约或 DHCP 中继生成的安全表项一致的 ARP 报文才能够被学习。

使能接口的授权 ARP 功能后，系统会禁止该接口学习动态 ARP 表项，可以防止用户仿冒其他用户的 IP 地址或 MAC 地址对网络进行攻击，保证只有合法的用户才能使用网络资源，增加了网络的安全性。

6. ARP扫描功能

启用 ARP 扫描功能后，设备会对局域网内的邻居自动进行扫描（向邻居发送 ARP 请求报文，获取邻居的 MAC 地址，从而建立动态 ARP 表项）。

ARP 扫描功能一般与 ARP 固化功能配合使用。ARP 固化功能用来将当前的 ARP 动态表项（包括 ARP 扫描生成的动态 ARP 表项）转换为静态 ARP 表项。通过对动态 ARP 表项的固化，可以有效防止攻击者修改 ARP 表项。

建议在网吧这种环境稳定的小型网络中使用这两个功能。

7. ARP网关保护功能

在设备上不与网关相连的接口上配置此功能，可以防止伪造网关攻击。

在接口上配置此功能后，当接口收到 ARP 报文时，将检查 ARP 报文的源 IP 地址是否和配置的被保护网关的 IP 地址相同。如果相同，则认为此报文非法，将其丢弃；否则，认为此报文合法，继续进行后续处理。

8. ARP过滤保护功能

ARP 过滤保护功能用来限制接口下允许通过的 ARP 报文，可以防止仿冒网关和仿冒用户的攻击。

在接口上配置此功能后，当接口收到 ARP 报文时，将检查 ARP 报文的源 IP 地址和源 MAC 地址是否和允许通过的 IP 地址和 MAC 地址相同：

- 如果相同，则认为此报文合法，继续进行后续处理；
- 如果不相同，则认为此报文非法，将其丢弃。

9. ARP Detection功能

ARP Detection 功能主要应用于接入设备上，对于合法用户的 ARP 报文进行正常转发，否则直接丢弃，从而防止仿冒用户、仿冒网关的攻击。

ARP Detection 包含三个功能：用户合法性检查、ARP 报文有效性检查、ARP 报文强制转发。

(1) 用户合法性检查

如果仅在 VLAN 上开启 ARP Detection 功能，则仅进行用户合法性检查。

对于 ARP 信任接口，不进行用户合法性检查；对于 ARP 非信任接口，需要进行用户合法性检查，以防止仿冒用户的攻击。

用户合法性检查是根据 ARP 报文中源 IP 地址和源 MAC 地址检查用户是否是所属 VLAN 所在接口上的合法用户，包括基于 IP Source Guard 静态绑定表项的检查、基于 DHCP Snooping 表项的检查。只要符合任何一个，就认为该 ARP 报文合法，进行转发。如果所有检查都没有找到匹配的表项，则认为是非法报文，直接丢弃。

(2) ARP 报文有效性检查

对于 ARP 信任接口，不进行报文有效性检查；对于 ARP 非信任接口，需要根据配置对 MAC 地址和 IP 地址不合法的报文进行过滤。可以选择配置源 MAC 地址、目的 MAC 地址或 IP 地址检查模式。

- 源 MAC 地址的检查模式：会检查 ARP 报文中的源 MAC 地址和以太网报文头中的源 MAC 地址是否一致，一致则认为有效，否则丢弃报文。
- 目的 MAC 地址的检查模式（只针对 ARP 应答报文）：会检查 ARP 应答报文中的目的 MAC 地址是否为全 0 或者全 1，是否和以太网报文头中的目的 MAC 地址一致。全 0、全 1、不一致的报文都是无效的，需要被丢弃。
- IP 地址检查模式：会检查 ARP 报文中的源 IP 或目的 IP 地址，如全 1、或者组播 IP 地址都是不合法的，需要被丢弃。对于 ARP 应答报文，源 IP 和目的 IP 地址都进行检查；对于 ARP 请求报文，只检查源 IP 地址。

(3) ARP 报文强制转发

对于从 ARP 信任接口接收到的 ARP 报文不受此功能影响，按照正常流程进行转发；对于从 ARP 非信任接口接收到的并且已经通过用户合法性检查的 ARP 报文的处理过程如下：

- 对于 ARP 请求报文，通过信任接口进行转发。

- 对于 ARP 应答报文，首先按照报文中的以太网目的 MAC 地址进行转发，若在 MAC 地址表中没有查到目的 MAC 地址对应的表项，则将此 ARP 应答报文通过信任接口进行转发。

1.20 ND

IPv6 邻居发现（Neighbor Discovery，ND）协议使用五种类型的ICMPv6 消息（如 表 1-8 所示），实现地址解析、验证邻居是否可达、重复地址检测、路由器发现/前缀发现、地址自动配置和重定向等功能。

表1-8 ND 使用的 ICMPv6 消息

ICMPv6 消息	类型号	作用
邻居请求消息NS（Neighbor Solicitation）	135	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（Neighbor Advertisement）	136	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
路由器请求消息RS（Router Solicitation）	133	节点启动后，通过RS消息向路由器发出请求，请求前缀和其他配置信息，用于节点的自动配置
路由器通告消息RA（Router Advertisement）	134	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，其中包括前缀信息选项和一些标志位的信息
重定向消息（Redirect）	137	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

1.20.1 邻居表项

邻居表项保存的是设备在链路范围内的邻居信息，设备邻居表项可以通过邻居请求消息 NS 及邻居通告消息 NA 来动态创建，也可以通过手工配置来静态创建。

目前，静态邻居表项有两种配置方式：

- 配置本节点的三层接口相连的邻居节点的 IPv6 地址和链路层地址。
- 配置本节点 VLAN 中的二层端口相连的邻居节点的 IPv6 地址和链路层地址。

对于 VLAN 接口，可以采用上述两种方式来配置静态邻居表项：

- 采用第一种方式配置静态邻居表项后，设备还需要解析该 VLAN 下的二层端口信息。
- 采用第二种方式配置静态邻居表项后，需要保证该二层端口属于指定的 VLAN，且该 VLAN 已经创建了 VLAN 接口。

1.20.2 RA报文

设备为同一链路上的主机发布 RA 报文，主机可以根据 RA 报文中的信息进行无状态自动配置等操作。设备可以抑制 RA 报文的发送，也可以周期性发送 RA 报文，相邻两次 RA 报文发送时间间隔

是在最大时间间隔与最小时间间隔之间随机选取的一个值。最小时间间隔应该小于等于最大时间间隔的 0.75 倍。

RA报文中的参数和参数描述如 表 1-9 所示。

表1-9 RA 报文中的参数

参数	描述
地址前缀/前缀长度	主机根据该地址前缀/前缀长度生成对应的IPv6地址，完成无状态自动配置操作
有效生命期	表示前缀有效期。在有效生命期内，通过该前缀自动生成的地址可以正常使用；有效生命期过期后，通过该前缀自动生成的地址变为无效，将被删除
首选生命期	表示首选通过该前缀无状态自动配置地址的时间。首选生命期过期后，节点通过该前缀自动配置的地址将被废止。节点不能使用被废止的地址建立新的连接，但是仍可以接收目的地址为被废止地址的报文。首选生命期必须小于或等于有效生命期
不用于无状态配置标识	选择了该标识，则指定前缀不用于无状态地址配置
不是直连可达标识	选择了该标识，则表示该前缀不是当前链路上直连可达的
MTU	发布链路的MTU，可以用于确保同一链路上的所有节点采用相同的MTU值
不指定跳数限制标识	选择了该标识，则表示RA消息中不带有本设备的跳数限制
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 如果选择了该标志位，主机将通过有状态自动配置（例如DHCPv6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
其他信息配置标志位（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 如果选择了其他信息配置标志位，主机将通过有状态自动配置（例如DHCPv6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（Router 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。发布RA消息中路由器生存时间为0的路由器不能作为默认路由器
邻居请求重传间隔（Retrans Timer）	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
配置路由优先级 (Router Preference)	用于设置发布RA消息的路由器的路由器优先级，主机根据接收到的RA消息中的路由器优先级，可以选择优先级最高的路由器作为默认网关。在路由器的优先级相同的情况下，遵循“先来先用”的原则，优先选择先接收到的RA消息对应的发送路由器作为默认网关
保持邻居可达时间（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

1.20.3 ND代理功能

如果 NS 请求是从一个网络的主机发往同一网段却不在同一物理网络上的另一台主机，那么连接它们的具有代理功能的设备就可以代答该请求，回应 NA 报文，这个过程称作 ND 代理（ND Proxy）。

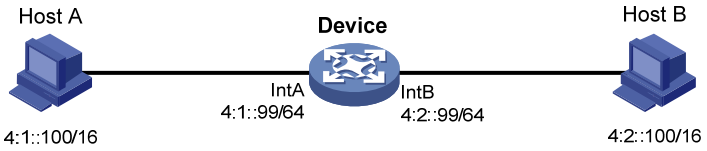
ND Proxy 功能屏蔽了分离的物理网络这一事实，使用户使用起来，好像在同一个物理网络上。

ND Proxy 功能根据应用场景不同分为普通 ND Proxy 和本地 ND Proxy。

1. 普通ND Proxy

普通ND Proxy的典型应用环境如 图 1-7 所示。Device通过两个三层接口Int A和Int B连接两个网络，两个三层接口的IPv6 地址不在同一个网段，接口地址分别为 4:1::99/64、4:2::99/64。但是两个网络内的主机Host A和Host B的地址通过掩码的控制，既与相连设备的接口地址在同一网段，同时二者也处于同一个网段。

图1-7 普通 ND 代理的典型应用环境



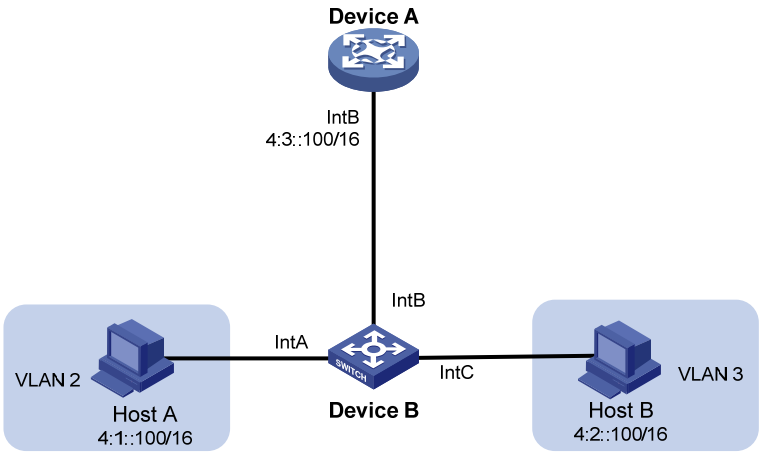
在这种组网情况下，当 Host A 需要与 Host B 通信时，由于目的 IPv6 地址与本机的 IPv6 地址为同一网段，因此 Host A 会直接发出请求 Host B 硬件地址的 NS 请求。但是，此时的两台主机处于不同的广播域中，Host B 无法收到 Host A 的 NS 请求报文，当然也就无法应答。

通过在 Device 上启用普通 ND Proxy 功能，可以解决此问题。在接口 Int A 和 Int B 上启用普通 ND Proxy 后，Router 可以应答 Host A 的 NS 请求。同时，Device 作为 Host B 的代理，把其它主机发送过来的报文转发给 Host B。这样，实现 Host A 与 Host B 之间的通信。

2. 本地ND Proxy

本地ND Proxy的应用场景如 图 1-8 所示。Host A属于VLAN 2，Host B属于VLAN 3，它们分别连接到端口Int A和Int C上。

图1-8 本地 ND 代理的应用场景



在这种组网情况下，当 Host A 需要与 Host B 通信时，由于目的 IPv6 地址与本机的 IPv6 地址为同一网段，因此 Host A 会直接发出请求 Host B 硬件地址的 NS 请求。但是，因为连接两台主机处于不同的 VLAN 中，Host B 无法收到 Host A 的 NS 请求报文。

通过在 Device A 上启用本地 ND Proxy 功能，可以解决此问题。在接口 Int B 上启用本地 ND Proxy 后，Device A 会代替 Host B 回应 NA，Host A 发给 Host B 的报文就会通过 Device A 进行转发，从而实现 Host A 与 Host B 之间的通信。

1.21 HTTP/HTTPS

为了方便用户对网络设备进行配置和维护，设备提供了 Web 登录功能。用户可以通过 PC 登录到设备上，使用 Web 界面直观地配置和维护设备。

设备支持的 Web 登录方式有以下两种：

- HTTP 登录方式：HTTP（Hypertext Transfer Protocol，超文本传输协议）用来在 Internet 上传递 Web 页面信息。目前，设备支持的 HTTP 协议版本为 HTTP/1.0。
- HTTPS 登录方式：HTTPS（Hypertext Transfer Protocol Secure，超文本传输协议的安全版本）是支持 SSL（Secure Sockets Layer，安全套接字层）协议的 HTTP 协议。HTTPS 通过 SSL 协议，能对客户端与设备之间交互的数据进行加密，能为设备制定基于证书属性的访问控制策略，提高了数据传输的安全性和完整性，保证合法客户端可以安全地访问设备，禁止非法客户端访问设备，从而实现了对设备的安全管理。

  采用 HTTPS 登录时，设备上只需使能 HTTPS 服务，用户即可通过 HTTPS 登录设备。此时，设备使用的证书为自签名证书，使用的 SSL 参数为各个参数的缺省值。（自签名证书指的是服务器自己生成的证书，无需从 CA 获取）

通过引用 ACL（Access Control List，访问控制列表），可以对访问设备的登录用户进行控制：

- 当未引用 ACL、引用的 ACL 不存在或者引用的 ACL 为空时，允许所有登录用户访问设备；
- 当引用的 ACL 非空时，则只有 ACL 中 permit 的用户才能访问设备，其它用户不允许访问设备，可以避免非法用户使用 Web 页面登录设备。

1.22 FTP

FTP 用于在 FTP 服务器和 FTP 客户端之间传输文件，是 IP 网络上传输文件的通用协议。本设备可作为 FTP 服务器，使用 20 端口传输数据，使用 21 端口传输控制消息。

1.23 Telnet

设备可以开启 Telnet 服务器功能，以便用户能够通过 Telnet 登录到设备进行远程管理和监控。

通过引用 ACL（Access Control List，访问控制列表），可以对访问设备的登录用户进行控制：

- 当未引用 ACL、引用的 ACL 不存在或者引用的 ACL 为空时，允许所有登录用户访问设备。
- 当引用的 ACL 非空时，则只有 ACL 中 permit 的用户才能访问设备，其它用户不允许访问设备，可以避免非法用户通过 Telnet 访问设备。

1.24 NTP

NTP（Network Time Protocol，网络时间协议）可以用来在分布式时间服务器和客户端之间进行时间同步，使网络内所有设备的时间保持一致，从而使设备能够提供基于统一时间的多种应用。

NTP 通过时钟层数来定义时钟的准确度。时钟层数的取值范围为 1～15，取值越小，时钟准确度越高。

在某些网络中，例如无法与外界通信的孤立网络，网络中的设备无法与权威时钟进行时间同步。此时，可以从该网络中选择一台时钟较为准确的设备，指定该设备与本地时钟进行时间同步，即采用本地时钟作为参考时钟，使得该设备的时钟处于同步状态。该设备作为时间服务器为网络中的其他设备提供时间同步，从而实现整个网络的时间同步。

通过 Web 页面可以配置本地时钟作为参考时钟。

1.25 LLDP

LLDP（Link Layer Discovery Protocol，链路层发现协议）提供了一种标准的链路层发现方式，可以将本端设备的信息（包括主要能力、管理地址、设备标识、接口标识等）组织成不同的 TLV（Type/Length/Value，类型/长度/值），并封装在 LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元）中发布给与自己直连的邻居，邻居收到这些信息后将其以标准 MIB（Management Information Base，管理信息库）的形式保存起来，以供网络管理系统查询及判断链路的通信状况。

1.25.1 LLDP代理

LLDP 代理是 LLDP 协议运行实体的一个抽象映射。一个接口下，可以运行多个 LLDP 代理。目前 LLDP 定义的代理类型包括：最近桥代理、最近非 TPMR 桥代理和最近客户桥代理。LLDP 在相邻的代理之间进行协议报文交互，并基于代理创建及维护邻居信息。

1.25.2 LLDP报文的发送机制

在指定类型 LLDP 代理下，当端口工作在 TxRx 或 Tx 模式时，设备会以报文发送时间间隔为周期，向邻居设备发送 LLDP 报文。如果设备的本地配置发生变化则立即发送 LLDP 报文，以将本地信息的变化情况尽快通知给邻居设备。但为了防止本地信息的频繁变化而引起 LLDP 报文的大量发送，可以配置限制发送报文速率的令牌桶大小来作限速处理。

当设备的工作模式由 Disable/Rx 切换为 TxRx/Tx，或者发现了新的邻居设备（即收到一个新的 LLDP 报文且本地尚未保存发送该报文设备的信息）时，该设备将自动启用快速发送机制，即将 LLDP 报文的发送周期设置为快速发送周期，并连续发送指定数量（快速发送 LLDP 报文的个数）的 LLDP 报文后再恢复为正常的发送周期。

1.25.3 LLDP报文的接收机制

当端口工作在 TxRx 或 Rx 模式时，设备会对收到的 LLDP 报文及其携带的 TLV 进行有效性检查，通过检查后再将邻居信息保存到本地，并根据 Time To Live TLV 中 TTL（Time To Live，生存时间）的值来设置邻居信息在本地设备上的老化时间，若该值为零，则立刻老化该邻居信息。

由于 TTL＝Min（65535，（TTL 乘数×LLDP 报文的发送间隔＋1）），即取 65535 与（TTL 乘数×LLDP 报文的发送间隔＋1）中的最小值，因此通过调整 TTL 乘数可以控制本设备信息在邻居设备上的老化时间。

1.25.4 端口初始化时间

当端口的 LLDP 工作模式发生变化时，端口将对协议状态机进行初始化操作。为了避免端口工作模式频繁改变而导致端口不断执行初始化操作，可配置端口初始化延迟时间，当端口工作模式改变时延迟一段时间再执行初始化操作。

1.25.5 LLDP Trap功能

如果开启了发送 LLDP Trap 功能，设备可以通过向网管系统发送 Trap 信息以通告如发现新的 LLDP 邻居、与原来邻居的通信链路发生故障等重要事件。

1.25.6 LLDP TLV

TLV 是组成 LLDP 报文的单元，每个 TLV 都代表一个信息。LLDP 可以封装的 TLV 包括基本 TLV、802.1 TLV、802.3 TLV 和 LLDP-MED（Link Layer Discovery Protocol Media Endpoint Discovery，链路层发现协议媒体终端发现） TLV。

基本 TLV 是网络设备管理基础的一组 TLV，802.1 TLV、802.3 TLV 和 LLDP-MED TLV 则是由标准组织或其他机构定义的 TLV，用于增强对网络设备的管理，可根据实际需要选择是否在 LLDPDU 中发送。

1.26 设置

1.26.1 日志信息等级

设备产生的日志信息按严重性可划分为如 表 1-10 所示的八个等级，各等级的严重性依照数值从 0～7 依次降低。

表1-10 日志信息等级列表

数值	信息等级	描述
0	emergency	表示设备不可用的信息，如系统授权已到期
1	alert	表示设备出现重大故障，需要立刻做出反应的信息，如流量超出接口上限
2	critical	表示严重信息，如设备温度已经超过预警值，设备电源、风扇出现故障等
3	error	表示错误信息，如接口链路状态变化等
4	warning	表示警告信息，如接口连接断开，内存耗尽告警等
5	notification	表示正常出现但是重要的信息，如通过终端登录设备，设备重启等
6	informational	表示需要记录的通知信息，如通过命令行输入命令的记录信息，执行**ping**命令的日志信息等
7	debugging	表示调试过程产生的信息

1.26.2 日志信息输出方向

系统可以向日志缓冲区（logbuffer）、日志主机（loghost）等方向发送日志信息。日志信息的各个输出方向相互独立，可在页面中分别设置。

2 网络安全

2.1 包过滤

包过滤是指采用 ACL 规则对接口、VLAN 或全局入方向或出方向的报文进行过滤，即对匹配上 ACL 规则的报文按照其中定义的匹配动作允许或拒绝通过，对未匹配上任何 ACL 规则的报文则按照指定的缺省动作进行处理。

2.2 QoS策略

QoS 即服务质量。对于网络业务，影响服务质量的因素包括传输的带宽、传送的时延、数据的丢包率等。在网络中可以通过保证传输的带宽、降低传送的时延、降低数据的丢包率以及时延抖动等措施来提高服务质量。

QoS 策略包含了三个要素：类、流行为、策略。用户可以通过 QoS 策略将指定的类和流行为绑定起来，灵活地进行 QoS 配置。

2.2.1 类

类用来定义一系列的规则来对报文进行分类。

2.2.2 流行为

流行为用来定义针对报文所做的 QoS 动作。

2.2.3 策略

策略用来将指定的类和流行为绑定起来，对符合分类条件的报文执行流行为中定义的动作。

2.2.4 应用策略

QoS 策略支持以下应用方式：

- 基于接口应用 QoS 策略：QoS 策略对通过接口接收或发送的流量生效。接口的每个方向（出和入两个方向）只能应用一个策略。如果 QoS 策略应用在接口的出方向，则 QoS 策略对本地协议报文不起作用。一些常见的本地协议报文如下：链路维护报文等。
- 基于全局应用 QoS 策略：QoS 策略对所有流量生效。

2.3 优先级映射

报文在进入设备以后，设备会根据映射规则分配或修改报文的各种优先级的值，为队列调度和拥塞控制服务。

优先级映射功能通过报文所携带的优先级字段来映射其他优先级字段值，就可以获得决定报文调度能力的各种优先级字段，从而为全面有效的控制报文的转发调度等级提供依据。

2.3.1 端口优先级

如果配置了优先级信任模式，即表示设备信任所接收报文的优先级，会自动解析报文的优先级或者标志位，然后按照映射表映射到报文的优先级参数。

如果没有配置优先级信任模式，并且配置了端口优先级值，则表明设备不信任所接收报文的优先级，而是使用端口优先级，按照映射表映射到报文的优先级参数。

1. 配置端口优先级

按照接收端口的端口优先级，设备通过一一映射为报文分配优先级。

2. 配置优先级信任模式

根据报文自身的优先级，查找优先级映射表，为报文分配优先级参数，可以通过配置优先级信任模式的方式来实现。

在配置接口上的优先级模式时，用户可以选择下列信任模式：

- Untrust：不信任任何优先级。
- Dot1p：信任报文自带的 802.1p 优先级，以此优先级进行优先级映射。
- DSCP：信任 IP 报文自带的 DSCP 优先级，以此优先级进行优先级映射。

2.3.2 优先级映射表

报文在进入设备以后，设备会根据映射规则分配或修改报文的各种优先级的值，为队列调度和拥塞控制服务。

优先级映射功能通过报文所携带的优先级字段来映射其他优先级字段值，就可以获得决定报文调度能力的各种优先级字段，从而为全面有效的控制报文的转发调度等级提供依据。

设备中提供了三张优先级映射表，分别 802.1p 优先级到本地优先级映射表、DSCP 到 802.1p 优先级映射表和 DSCP 到 DSCP 映射表。如果缺省优先级映射表无法满足用户需求，可以根据实际情况对映射表进行修改。

2.4 802.1X

802.1X 协议是一种基于端口的网络接入控制协议，即在局域网接入设备的端口上对所接入的用户和设备进行认证，以便控制用户设备对网络资源的访问。

2.4.1 802.1X的体系结构

802.1X 系统中包括三个实体：

- 客户端：请求接入局域网的用户终端，由局域网中的设备端对其进行认证。客户端上必须安装支持 802.1X 认证的客户端软件。
- 设备端：局域网中控制客户端接入的网络设备，位于客户端和认证服务器之间，为客户端提供接入局域网的端口，并通过与认证服务器的交互来对所连接的客户端进行认证。
- 认证服务器端：用于对客户端进行认证、授权和计费，通常为 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器。认证服务器根据设备端发送来的客户端认证信息来验证客户端的合法性，并将验证结果通知给设备端，由设备端决定是否允许客户端接入。

2.4.2 802.1X的认证方法

在接入设备上，802.1X 认证方法有三种方式：

- CHAP 或 PAP 认证方法。在这种方式下，设备对 EAP 认证过程进行终结，将收到的 EAP 报文中的客户端认证信息封装在标准的 RADIUS 报文中，与服务器之间采用 PAP 或 CHAP 方法进行认证。CHAP 以密文的方式传送密码，而 PAP 是以明文的方式传送密码。
- EAP 认证方法。在这种方式下，设备端对收到的 EAP 报文进行中继，使用 EAPOR（EAP over RADIUS）封装格式将其承载于 RADIUS 报文中发送给 RADIUS 服务器。

2.4.3 接入控制方式

端口支持以下两种接入控制方式：

- 基于端口认证：只要该端口下的第一个用户认证成功后，其它接入用户无须认证就可使用网络资源，但是当第一个用户下线后，其它用户也会被拒绝使用网络。
- 基于 MAC 认证：该端口下的所有接入用户均需要单独认证，当某个用户下线后，也只有该用户无法使用网络。

2.4.4 授权状态

端口支持以下三种授权状态：

- 强制授权：表示端口始终处于授权状态，允许用户不经认证即可访问网络资源。
- 强制非授权：表示端口始终处于非授权状态。设备端不为通过该端口接入的客户端提供认证服务。
- 自动识别：表示端口初始状态为非授权状态，仅允许 EAPOL 报文收发，不允许用户访问网络资源；如果用户通过认证，则端口切换到授权状态，允许用户访问网络资源。

2.4.5 周期性重认证

该功能开启后，设备会根据周期性重认证时间间隔定期向该端口在线 802.1X 用户发起重认证，以检测用户连接状态的变化、确保用户的正常在线，并及时更新服务器下发的授权属性（例如 ACL、VLAN、User Profile）。

2.4.6 在线用户握手

该功能开启后，设备会根据周期发送握手请求报文时间间隔定期向通过 802.1X 认证的在线用户发送握手报文，以定期检测用户的在线情况。如果设备连续多次没有收到客户端的响应报文，则会将用户置为下线状态。

2.4.7 安全握手

在线用户握手功能处于开启状态的前提下，还可以通过开启在线用户握手安全功能，来防止在线的 802.1X 认证用户使用非法的客户端与设备进行握手报文的交互，而逃过代理检测、双网卡检测等 iNode 客户端的安全检查功能。

2.4.8 认证触发

设备端主动触发方式用于支持不能主动发送 EAPOL-Start 报文的客户端，例如 Windows XP 自带的 802.1X 客户端。设备主动触发认证的方式分为以下两种：

- 单播触发：当设备收到源 MAC 地址未知的报文时，主动向该 MAC 地址单播发送 Identity 类型的 EAP-Request 帧来触发认证。若设备端在设置的时长内没有收到客户端的响应，则重发该报文。
- 组播触发：设备每隔一定时间（缺省为 30 秒）主动向客户端组播发送 Identity 类型的 EAP-Request 帧来触发认证。

2.4.9 Auth-Fail VLAN

802.1X Auth-Fail VLAN 功能允许用户在认证失败的情况下访问某一特定 VLAN 中的资源。需要注意的是，这里的认证失败是认证服务器因某种原因明确拒绝用户认证通过，比如用户密码错误，而不是认证超时或网络连接等原因造成的认证失败。

1. 基于端口认证

在接入控制方式为基于端口认证的端口上配置 Auth-Fail VLAN 后，若该端口上有用户认证失败，则该端口会离开当前的 VLAN 被加入到 Auth-Fail VLAN，所有在该端口接入的用户将被授权访问 Auth-Fail VLAN 里的资源。

当加入 Auth-Fail VLAN 的端口上有用户发起认证并失败，则该端口将会仍然处于 Auth-Fail VLAN 内；如果认证成功，则该端口会离开 Auth-Fail VLAN，之后端口加入 VLAN 情况与认证服务器是否下发授权 VLAN 有关，具体如下：

- 若认证服务器下发了授权 VLAN，则端口加入下发的授权 VLAN 中。用户下线后，端口会离开下发的授权 VLAN，若端口上配置了 Guest VLAN，则加入 Guest VLAN，否则加入缺省 VLAN。
- 若认证服务器未下发授权 VLAN，则端口回到缺省 VLAN 中。用户下线后，端口仍在缺省 VLAN 中。

2. 基于MAC认证

在接入控制方式为基于 MAC 认证的端口上配置 Auth-Fail VLAN 后，该端口上认证失败的用户将被授权访问 Auth-Fail VLAN 里的资源。

当 Auth-Fail VLAN 中的用户再次发起认证时，如果认证成功，则设备会根据认证服务器是否下发 VLAN 决定将该用户加入到下发的授权 VLAN 中，或使其回到端口的缺省 VLAN 中；如果认证失败，则该用户仍然留在该 Auth-Fail VLAN 中。

2.4.10 Guest VLAN

802.1X Guest VLAN 功能允许用户在未认证的情况下，访问某一特定 VLAN 中的资源。

当端口上处于 Guest VLAN 中的用户发起认证且失败时：如果端口配置了 Auth-Fail VLAN，则该端口会被加入 Auth-Fail VLAN；如果端口未配置 Auth-Fail VLAN，则该端口仍然处于 Guest VLAN 内。

当端口上处于 Guest VLAN 中的用户发起认证且成功时，端口会离开 Guest VLAN，之后端口加入 VLAN 情况与认证服务器是否下发 VLAN 有关，具体如下：

若认证服务器下发 VLAN，则端口加入下发的 VLAN 中。用户下线后，端口离开下发的 VLAN 回到初始 VLAN 中，该初始 VLAN 为端口加入 Guest VLAN 之前所在的 VLAN。

若认证服务器未下发 VLAN，则端口回到初始 VLAN 中。用户下线后，端口仍在该初始 VLAN 中。

根据端口的接入控制方式不同，Guest VLAN 的生效情况有所不同。

1. 基于端口认证

在接入控制方式为基于端口认证的端口上配置 Guest VLAN 后，若全局和端口上都使能了 802.1X，端口授权状态为 auto，且端口处于激活状态，则该端口就被立即加入 Guest VLAN，所有在该端口接入的用户将被授权访问 Guest VLAN 里的资源。

2. 基于MAC认证

在接入控制方式为基于 MAC 认证的端口上配置 Guest VLAN 后，端口上未认证的用户将被授权访问 Guest VLAN 里的资源。

2.4.11 Critical VLAN

802.1X Critical VLAN 功能允许用户在认证时，当所有认证服务器都不可达的情况下访问某一特定 VLAN 中的资源。目前，只采用 RADIUS 认证方式的情况下，在所有 RADIUS 认证服务器都不可达后，端口才会加入 Critical VLAN。若采用了其它认证方式，则端口不会加入 Critical VLAN。

根据端口的接入控制方式不同，Critical VLAN 的生效情况有所不同。

1. 基于端口认证

在接入控制方式为基于端口认证的端口上配置 Critical VLAN 后，若该端口上有用户认证时，所有认证服务器都不可达，则该端口会被加入到 Critical VLAN，之后所有在该端口接入的用户将被授权访问 Critical VLAN 里的资源。在用户进行重认证时，若所有认证服务器都不可达，且端口指定在此情况下强制用户下线，则该端口也会被加入到 Critical VLAN。

已经加入 Critical VLAN 的端口上有用户发起认证时，如果所有认证服务器不可达，则端口仍然在 Critical VLAN 内；如果服务器可达且认证失败，且端口配置了 Auth-Fail VLAN，则该端口将会加入 Auth-Fail VLAN，否则回到端口的缺省 VLAN 中；如果服务器可达且认证成功，则该端口加入 VLAN 的情况与认证服务器是否下发 VLAN 有关，具体如下：

若认证服务器下发了授权 VLAN，则端口加入下发的授权 VLAN 中。用户下线后，端口会离开下发的授权 VLAN，若端口上配置了 Guest VLAN，则加入 Guest VLAN，否则加入缺省 VLAN。

若认证服务器未下发授权 VLAN，则端口回缺省 VLAN 中。用户下线后，端口仍在缺省 VLAN 中。

2. 基于MAC认证

在接入控制方式为基于 MAC 认证的端口上配置 Critical VLAN 后，若该端口上有用户认证时，所有认证服务器都不可达，则端口将允许 Critical VLAN 通过，用户将被授权访问 Critical VLAN 里的资源。

当 Critical VLAN 中的用户再次发起认证时，如果所有认证服务器不可达，则用户仍然在 Critical VLAN 中；如果服务器可达且认证失败，且端口配置了 Auth-Fail VLAN，则该用户将会加入 Auth-Fail VLAN，否则回到端口的缺省 VLAN 中；如果服务器可达且认证成功，则设备会根据认证服务器是否下发授权 VLAN 决定将该用户加入下发的授权 VLAN 中，或使其回到端口的缺省 VLAN 中。

2.4.12 端口的强制认证ISP域

在端口上指定强制认证域为 802.1X 接入提供了一种安全控制策略。所有从该端口接入的 802.1X 用户将被强制使用指定的认证域来进行认证、授权和计费，从而防止用户通过恶意假冒其它域账号从本端口接入网络。另外，管理员也可以通过配置强制认证域对不同端口接入的用户指定不同的认证域，从而增加了管理员部署 802.1X 接入策略的灵活性。

2.4.13 EAD快速部署

EAD（Endpoint Admission Defense，端点准入防御）作为一个网络端点接入控制方案，它通过安全客户端、安全策略服务器、接入设备以及第三方服务器的联动，加强了对用户的集中管理，提升了网络的整体防御能力。但是在实际的应用过程中 EAD 客户端的部署工作量很大，例如，需要网络管理员手动为每一个 EAD 客户端下载、升级客户端软件，这在 EAD 客户端数目较多的情况下给管理员带来了操作上的不便。

802.1X 认证支持的 EAD 快速部署功能就可以解决以上问题，它允许未通过认证的 802.1X 用户访问一个指定的 IP 地址段（称为 Free IP），并可以将用户发起的 HTTP 访问请求重定向到该 IP 地址段中的一个指定的 URL，实现用户自动下载并安装 EAD 客户端的目的。

2.4.14 配置 802.1X SmartOn功能

开启了 SmartOn 功能的端口上收到 802.1X 客户端发送的 EAPOL-Start 报文后，将向其回复单播的 EAP-Request/Notification 报文，并开启 SmartOn 通知请求超时定时器定时器等待客户端响应的 EAP-Response/Notification 报文。若 SmartOn 通知请求超时定时器超时后客户端仍未回复，则设备会重发 EAP-Request/Notification 报文，并重新启动该定时器。当重发次数达到规定的最大次数后，会停止对该客户端的 802.1X 认证；若在重发次数达到最大次数之前收到了该 Notification 报文的回复报文，则获取该报文中携带的 Switch ID 和 SmartOn 密码的 MD5 摘要，并与设备本地配置的 SmartOn 的 Switch ID 以及 SmartOn 密码的 MD5 摘要值比较，若相同，则继续客户端的 802.1X 认证，否则中止客户端的 802.1X 认证。

802.1X SmartOn 功能与在线用户握手功能互斥，建议两个功能不要同时开启。

2.5 ISP域

设备对用户的管理是基于 ISP（Internet Service Provider，互联网服务提供者）域的，一个 ISP 域对应着一套实现 AAA（Authentication、Authorization、Accounting，认证、授权、计费）的配置策略，它们是管理员针对该域用户制定的一套认证、授权、计费方法，可根据用户的接入特征以及不同的安全需求组合使用。

设备支持的认证方法包括：

- 不认证：对用户非常信任，不对其进行合法性检查，一般情况下不采用这种方法。
- 本地认证：认证过程在接入设备上完成，用户信息（包括用户名、密码和各种属性）配置在接入设备上。优点是速度快，可以降低运营成本；缺点是存储信息量受设备硬件条件限制。
- 远端认证（RADIUS）：认证过程在接入设备和远端的服务器之间完成，接入设备和远端服务器之间通过 RADIUS 协议通信。优点是用户信息集中在服务器上统一管理，可实现大容量、

高可靠性、支持多设备的集中式统一认证。当远端服务器无效时，可配置备选认证方式完成认证。

设备支持的授权方法包括：

- 不授权：接入设备不请求授权信息，不对用户可以使用的操作以及用户允许使用的网络服务进行授权。此时，认证通过的 login 用户只有系统所给予的缺省用户角色，其中 FTP/SFTP/SCP 用户的工作目录是设备的根目录，但并无访问权限；认证通过的非 login 用户，可直接访问网络。
- 本地授权：授权过程在接入设备上进行，根据接入设备上为本地用户配置的相关属性进行授权。
- 远端授权（RADIUS）：授权过程在接入设备和远端服务器之间完成。RADIUS 协议的认证和授权是绑定在一起的，不能单独使用 RADIUS 进行授权。RADIUS 认证成功后，才能进行授权，RADIUS 授权信息携带在认证回应报文中下发给用户。当远端服务器无效时，可配置备选授权方式完成授权。

设备支持的计费方法包括：

- 不计费：不对用户计费。
- 本地计费：计费过程在接入设备上完成，实现了本地用户连接数的统计和限制，并没有实际的费用统计功能。
- 远端计费（RADIUS）：计费过程在接入设备和远端的服务器之间完成。当远端服务器无效时，可配置备选计费方式完成计费。

每个用户都属于一个 ISP 域。为便于对不同接入方式的用户进行区分管理，提供更为精细且有差异化的认证、授权、计费服务，设备将用户划分为以下几个类型：

- LAN 接入用户：例如 802.1X 认证用户。
- 登录用户：例如 Telnet、FTP、终端接入用户（即从 Console、AUX 等接口登录的用户）。
- Portal 用户。

在多 ISP 的应用环境中，不同 ISP 域的用户有可能接入同一台设备，因此系统中可以存在多个 ISP 域，其中包括一个缺省存在的名称为 system 的 ISP 域。如果某个用户在登录时没有提供 ISP 域名，系统将把它归于缺省的 ISP 域。系统缺省的 ISP 域可以手工修改为一个指定的 ISP 域。

用户认证时，设备将按照如下先后顺序为其选择认证域：接入模块指定的认证域-->用户名中指定的 ISP 域-->系统缺省的 ISP 域。其中，仅部分接入模块支持指定认证域，例如 802.1X 认证。

2.6 RADIUS

2.6.1 RADIUS协议简介

RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）是一种分布式的、客户端/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰，常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中。

- RADIUS 客户端：一般位于接入设备上，可以遍布整个网络，负责将用户信息传输到指定的 RADIUS 服务器，然后根据服务器返回的信息进行相应处理（如接受/拒绝用户接入）。
- RADIUS 服务器：一般运行在中心计算机或工作站上，维护用户的身份信息和与其相关的网络服务信息，负责接收接入设备发送的认证、授权、计费请求并进行相应的处理，然后给接入设备返回处理结果（如接受/拒绝认证请求）。

RADIUS 协议使用 UDP 作为封装 RADIUS 报文的传输层协议，通过使用共享密钥机制来保证客户端和 RADIUS 服务器之间消息交互的安全性。

当接入设备对用户提供 AAA（Authentication、Authorization、Accounting，认证、授权、计费）服务时，若要对用户采用 RADIUS 服务器进行认证、授权、计费，则作为 RADIUS 客户端的接入设备上需要配置相应的 RADIUS 服务器参数。

2.6.2 RADIUS增强功能

1. Accounting-on功能

设备重启后，重启前的原在线用户可能会被 RADIUS 服务器认为仍然在线而短时间内无法再次登录。为了解决这个问题，需要开启 Accounting-on 功能。

开启了 Accounting-on 功能后，设备会在重启后主动向 RADIUS 服务器发送 Accounting-on 报文来告知自己已经重启，并要求 RADIUS 服务器停止计费且强制通过本设备上线的用户下线。若设备发送 Accounting-on 报文后 RADIUS 服务器无响应，则会在按照一定的时间间隔尝试重发几次。

2. Session control功能

H3C 的 IMC RADIUS 服务器使用 session control 报文向设备发送授权信息的动态修改请求以及断开连接请求。设备上开启接收 session control 报文的开关后，会打开知名 UDP 端口 1812 来监听并接收 RADIUS 服务器发送的 session control 报文。

需要注意的是，该功能仅能和 H3C 的 IMC RADIUS 服务器配合使用。

2.7 本地认证

本地认证泛指由接入设备对用户进行认证、授权和计费，进行本地认证的用户的信息（包括用户名、密码和各种属性）配置在接入设备上。

为使某个请求网络服务的用户可以通过本地认证，需要在设备上添加相应的用户条目。所谓用户，是指在设备上设置的一组用户属性的集合，该集合以用户名唯一标识。

为了简化用户的配置，增强用户的可管理性，引入了用户组的概念。用户组是一系列公共用户属性的集合，某些需要集中管理的公共属性可在用户组中统一配置和管理，属于该用户组的所有用户都可以继承这些属性。

3 系统

3.1 ACL

ACL（Access Control List，访问控制列表）是一或多条规则的集合，用于识别报文流。这里的规则是指描述报文匹配条件的判断语句，匹配条件可以是报文的源地址、目的地址、端口号等。设备依照这些规则识别出特定的报文，并根据预先设定的策略对其进行处理。

3.1.1 ACL分类

ACL包括 表 3-1 所列的几种类型，它们的主要区别在于规则制订依据不同：

表3-1 ACL 分类

ACL 分类		规则制定依据
IPv4 ACL	基本ACL	依据报文的源IPv4地址制订规则
	高级ACL	依据报文的源/目的IPv4地址、源/目的端口号、优先级、承载的IPv4协议类型等三、四层信息制订规则
IPv6 ACL	基本ACL	依据报文的源IPv6地址制订规则
	高级ACL	依据报文的源/目的IPv6地址、源/目的端口号、优先级、承载的IPv6协议类型等三、四层信息制订规则
二层ACL		依据报文的源/目的MAC地址、802.1p优先级、链路层协议类型等二层信息
自定义ACL		以报文头为基准，指定从报文的第几个字节开始与掩码进行“与”操作，并将提取出的字符串与用户定义的字符串进行比较，从而找出相匹配的报文

3.1.2 ACL规则匹配顺序

一个 ACL 中可以包含多条规则，设备将报文按照一定顺序与这些规则进行匹配，一旦匹配上某条规则便结束匹配过程。规则匹配顺序有两种：

- 配置顺序：按照规则编号由小到大进行匹配。
- 自动排序：按照“深度优先”原则由深到浅进行匹配，见 表 3-2（自定义ACL不支持自动排序）：

表3-2 各类型 ACL 的“深度优先”排序法则

ACL 分类		规则制定依据
IPv4 ACL	基本ACL	1. 先比较源 IPv4 地址的范围，较小者（即通配符掩码中“0”位较多者）优先 2. 如果源 IPv4 地址范围相同，再比较配置的先后次序，先配置者优先
	高级ACL	1. 先比较协议范围，指定有 IPv4 承载的协议类型者优先 2. 如果协议范围相同，再比较源 IPv4 地址范围，较小者优先 3. 如果源 IPv4 地址范围也相同，再比较目的 IPv4 地址范围，较小者优先

ACL 分类		规则制定依据
		4. 如果目的 IPv4 地址范围也相同，再比较 TCP/UDP 端口号的覆盖范围，较小者优先 **5.** 如果 TCP/UDP 端口号的覆盖范围无法比较，则比较配置的先后次序，先配置者优先
IPv6 ACL	基本ACL	**1.** 先比较源 IPv6 地址的范围，较小者（即前缀较长者）优先 **2.** 如果源 IPv6 地址范围相同，再比较配置的先后次序，先配置者优先
	高级ACL	**1.** 先比较协议范围，指定有 IPv6 承载的协议类型者优先 **2.** 如果协议范围相同，再比较源 IPv6 地址范围，较小者优先 **3.** 如果源 IPv6 地址范围也相同，再比较目的 IPv6 地址范围，较小者优先 **4.** 如果目的 IPv6 地址范围也相同，再比较 TCP/UDP 端口号的覆盖范围，较小者优先 **5.** 如果 TCP/UDP 端口号的覆盖范围无法比较，则比较配置的先后次序，先配置者优先
二层ACL		**1.** 先比较源 MAC 地址范围，较小者（即掩码中“1”位较多者）优先 **2.** 如果源 MAC 地址范围相同，再比较目的 MAC 地址范围，较小者优先 **3.** 如果目的 MAC 地址范围也相同，再比较配置的先后次序，先配置者优先

说明

- 比较 IPv4 地址范围的大小，就是比较 IPv4 地址通配符掩码中“0”位的多少。
- 比较 IPv6 地址范围的大小，就是比较 IPv6 地址前缀的长短：前缀越长，范围越小。
- 比较 MAC 地址范围的大小，就是比较 MAC 地址掩码中“1”位的多少：“1”位越多，范围越小。

3.1.3 ACL规则编号

每条规则都有自己的编号，这个编号可由手工指定或由系统自动分配。由于规则编号可能影响规则的匹配顺序，因此当系统自动分配编号时，为方便后续在已有规则之间插入新规则，通常在相邻编号之间留有一定空间，这就是规则编号的步长。系统自动分配编号的方式为：从 0 开始，按照步长分配一个大于现有最大编号的最小编号。比如原有编号为 0、5、9、10 和 12 的五条规则，步长为 5，则系统将自动为下一条规则分配编号 15。如果步长发生了改变，则原有全部规则的编号都将自动从 0 开始按新步长重新排列。比如原有编号为 0、5、9、10 和 15 的五条规则，当步长变为 2 后，这些规则的编号将依次变为 0、2、4、6 和 8。

3.2 时间段

时间段（Time Range）定义了一个时间范围。用户通过创建一个时间段并在某业务中将其引用，就可使该业务在此时间段定义的时间范围内生效。但如果一个业务所引用的时间段尚未配置或已被删除，该业务将不会生效。

譬如，当一个 ACL 规则只需在某个特定时间范围内生效时，就可以先配置好这个时间段，然后在配置该 ACL 规则时引用此时间段，这样该 ACL 规则就只能在该时间段定义的时间范围内生效。

时间段可分为以下两种类型：

- 周期时间段：表示以一周为周期（如每周一的 8 至 12 点）循环生效的时间段。
- 绝对时间段：表示在指定时间范围内（如 2011 年 1 月 1 日 8 点至 2011 年 1 月 3 日 18 点）生效时间段。

每个时间段都以一个名称来标识，一个时间段内可包含一或多个周期时间段和绝对时间段。当一个时间段内包含有多个周期时间段和绝对时间段时，系统将先分别取各周期时间段的并集和各绝对时间段的并集，再取这两个并集的交集作为该时间段最终生效的时间范围。

3.3 文件管理

3.3.1 文件系统

设备上的一个存储介质即称为一个文件系统。

1. 文件系统的命名

本设备除了固定存储介质外还支持可插拔存储介质 U 盘，可插拔存储介质的文件系统名称由存储介质的位置、存储介质类型、存储介质编号和冒号组成：

- 存储介质的位置：请参见本文档的 2. 存储介质位置。
- 存储介质类型：U 盘的类型名称为“usb”。
- 存储介质编号：同类型的存储介质以英文小写字母 a 开始进行排序，例如“usba”表示第一个 U 盘。
- 冒号：作为存储介质名称的结束符，例如第一个 U 盘的完整名称为“usba:”

2. 存储介质位置


说明

文件系统名称中的所有英文字符输入时不区分大小写。

3. 缺省文件系统

缺省文件系统是指用户登录设备后默认工作在的文件系统。用户在对文件或者文件夹进行操作时，如果不指定文件系统，则表示对设备的缺省文件系统进行操作。例如，在保存当前配置时，如果不输入任何保存位置信息，则下次启动配置文件将保存在缺省文件系统的根目录下。

4. 目录

本设备的文件系统采用树形目录结构。

根目录

根目录用“/”来表示。

(1) 工作目录

工作目录也被称为当前工作目录。

用户登录设备后，缺省的工作目录为设备 Flash 的根目录。

(2) 文件夹的命名

文件夹名称中可以包含数字、字母或特殊字符（除了*|\/?<>":）。给文件夹命名时，首字母请不要使用“.”。因为系统会把名称首字母为“.”的文件夹当成隐藏文件夹。

(3) 常用文件夹

设备出厂时会携带一些文件夹，在运行过程中可能会自动产生一些文件夹，这些文件夹包括：

- diagfile：用于存放诊断信息文件的文件夹
- logfile：用于存放日志文件的文件夹
- seclog：用于存放安全日志文件的文件夹
- versionInfo：用于存放版本信息文件的文件夹
- 其它名称的文件夹

5. 文件

(1) 文件的命名

文件名中可以输入以数字、字母、特殊字符为组合的字符串（除了*|\/?<>":）。给文件命名时，首字母请不要使用“.”。因为系统会把名称首字母为“.”的文件当成隐藏文件。

(2) 常见文件类型

设备出厂时会携带一些文件，在运行过程中可能会自动产生一些文件，这些文件包括：

- xx.ipe（复合软件包套件，是启动软件包的集合）
- xx.bin（启动软件包）
- xx.cfg（配置文件）
- xx.mdb（二进制格式的配置文件）
- xx.log（用于存放日志的文件）
- 其它后缀的文件

(3) 隐藏文件和文件夹

文件/文件夹分为隐藏的、非隐藏的。因为有些系统文件/文件夹是隐藏文件/文件夹，所以对于隐藏文件/文件夹，请不要修改或删除，以免影响对应功能；对于非隐藏的文件/文件夹，请完全了解它的作用后再执行文件/文件夹操作，以免误删重要文件/文件夹。

3.3.2 使用限制和注意事项

- 设备在执行文件系统操作过程中，禁止对存储介质进行插拔操作。否则，可能会引起文件系统的损坏。
- 当用户占用可插拔存储介质的资源（如用户正在访问某个目录）时，存储介质被强制拔出。此时，请先释放占用的存储介质的资源，再插入存储介质。否则，存储介质被插入后可能不能被识别。
- 当需要对 U 盘进行写文件系统操作，请确保没有将 U 盘写保护。如果 U 盘写保护了，这些操作将执行失败。其它文件系统操作不受写保护开关影响。

3.3.3 文件操作

文件操作是指对指定的文件路径下的文件进行相应操作，目前文件操作分为以下三类：

- 上传：设备支持上传版本文件、配置文件、证书、本地 Portal 页面、map 文件、特殊 AP 版本文件等。
- 下载：设备支持下载版本文件、配置文件、一键诊断信息及之前上传的信息文件等。
- 删除：设备支持选择删除设备上的非隐性文件。

说明

目前删除之后的文件无法恢复，请确保删除文件准确无误。

3.4 管理员

管理员通过 HTTP、HTTPS、SSH、Telnet、FTP、PAD、终端接入（即从 Console 口接入）方式登录到设备上之后，可以对设备进行配置和管理。对登录用户的管理和维护主要涉及以下几个部分：

- 帐户管理：对用户的基本信息（用户名、密码）以及相关属性的管理。
- 角色管理：对用户可执行的系统功能以及可操作的系统资源权限的管理。
- 密码管理：对用户登录密码的设置、老化、更新以及用户登录状态等方面的管理。

3.4.1 帐户管理

为使请求某种服务的用户可以成功登录设备，需要在设备上添加相应的帐户。所谓用户，是指在设备上设置的一组用户属性的集合，该集合以用户名唯一标识。一个有效的用户条目中可包括用户名、密码、角色、可用服务、密码管理等属性。

3.4.2 角色管理

对登录用户权限的控制，是通过为用户赋予一定的角色来实现。一个角色中定义了允许用户执行的系统功能以及可操作的系统资源，具体实现如下：

- 通过角色规则实现对系统功能的操作权限的控制。例如，定义用户角色规则允许用户配置 A 功能，或禁止用户配置 B 功能。
- 通过资源控制策略实现对系统资源（接口、VLAN）的操作权限的控制。例如，定义资源控制策略允许用户操作 VLAN 10，禁止用户操作接口 GigabitEthernet1/0/1。

1. 角色规则

一个角色中可以包含多条规则，规则定义了允许/禁止用户操作某类实体的权限。

系统支持的实体类型包括：

- 命令行：控制用户权限的最小单元，具体可分为读、写、执行类型的命令行。
- 特性：与一个功能相关的所有命令的集合。系统中的所有特性及其包含的命令都是系统预定义的，不允许用户自定义。
- 特性组：一个或者多个特性的集合。系统预定义了两个特性组 L2 和 L3。L2 中包含了所有的二层协议相关功能的命令，L3 中包含了所有三层协议相关功能的命令。管理员可以根据需要自定义特性组，但不能修改和删除系统预定义的特性组 L2 和 L3。各个特性组之间包含的特性允许重叠。

- Web 菜单：通过 Web 对设备进行配置时，各配置页面以 Web 菜单的形式组织，按照层次关系，形成多级菜单的树形结构。
- XML 元素：与 Web 菜单类似，XML 对于配置对象的组织也呈现树状结构，每一个 XML 元素代表 XML 配置中的一个 XML 节点。
- SNMP OID：对象标识符，SNMP 协议通过 OID 唯一标识一个被管理对象。

对实体的操作权限包括：

- 读权限：可查看指定实体的配置信息和维护信息。
- 写权限：可配置指定实体的相关功能和参数。
- 执行权限：可执行特定的功能，如与 FTP 服务器建立连接。

定义一个规则，就等于约定允许或禁止用户针对某类实体具有哪些操作权限，具体分为：

- 控制命令行的规则：用来控制一条命令或者与指定的命令特征字符串相匹配的一类命令是否允许被执行。
- 控制特性的规则：用来控制特性包含的命令是否允许被执行。因为特性中的每条命令都属于读类型、写类型或执行类型，所以在定义该类规则时，可以精细地控制特性所包含的读、写或执行类型的命令能否被执行。
- 控制特性组的规则：此规则和基于特性的规则类似，区别是一条基于特性组的规则中可同时对多个特性包含的命令进行控制。
- 控制 Web 菜单的规则：用来控制指定的 Web 菜单选项是否允许被操作。因为每个菜单项中的操作控件具有相应的读，写或执行属性，所以定义基于 Web 菜单的规则时，可以精细地控制菜单项中读、写或执行控件的操作。
- 控制 XML 元素的规则：用来控制指定的 XML 元素是否允许被执行。XML 元素也具有读，写或执行属性。
- 控制 OID 的规则：用来控制指定的 OID 是否允许被 SNMP 访问。OID 具有读，写和执行属性。

一个用户角色中可以定义多条规则，各规则以创建时指定的编号为唯一标识，被授权该角色的用户可以执行的命令为这些规则中定义的可执行命令的并集。若这些规则定义的权限内容有冲突，则规则编号大的有效。例如，规则 1 允许执行命令 A，规则 2 允许执行命令 B，规则 3 禁止执行命令 A，则最终规则 2 和规则 3 生效，即禁止执行命令 A，允许执行命令 B。

2. 资源控制策略

资源控制策略规定了用户对系统资源的操作权限。

- 对于登录命令行的用户而言，对接口/VLAN 的操作是指创建并进入接口视图/VLAN 视图、删除和应用接口/VLAN（在 **display** 命令中指定接口/VLAN 参数并不属于应用接口/VLAN 范畴）。
- 对于登录 Web 页面的用户而言，对接口/VLAN 的操作是指创建接口/VLAN、配置接口/VLAN 的属性、删除接口/VLAN 和应用接口/VLAN。

资源控制策略需要与角色规则相配合才能生效。在用户执行命令的过程中，系统对该命令涉及的系统资源使用权限进行动态检测，因此只有用户同时拥有执行该命令的权限和使用该资源的权限时，才能执行该命令。例如，若管理员为某用户角色定义了一条规则允许用户创建 VLAN，且同时指定用户具有操作 VLAN 10 的权限，则当用户被授权此角色并试图创建 VLAN 10 时，操作会被允许，但试图创建其它 VLAN 时，操作会被禁止。若管理员并没有为该角色定义允许用户创建 VLAN 的规则，则用户即便拥有该 VLAN 资源的操作权限，也无法执行相关的操作。

3. 缺省角色

系统预定义了多种角色，角色名和对应的权限如 表 3-3 所示。这些角色缺省均具有操作所有系统资源的权限，但具有不同的系统功能操作权限。如果系统预定义的用户角色无法满足权限管理需求，管理员还可以自定义用户角色来对用户权限做进一步控制。

表3-3 系统预定义的角色名和对应的权限

角色名	权限
network-admin	可操作系统所有功能和资源（除安全日志文件管理相关命令**display security-logfile summary**、**info-center security-logfile directory**、**security-logfile save**之外）
network-operator	• 可执行系统所有功能和资源的相关 **display** 命令（除 **display history-command all**、**display security-logfile summary** 等命令，具体请通过 **display role** 命令查看） • 如果用户采用本地认证方式登录系统并被授予该角色，则可以修改自己的密码 • 可执行进入 XML 视图的命令 • 可允许用户对所有 Web 菜单选项进行读操作 • 可允许用户对所有 XML 元素进行读操作 • 可允许用户对所有 SNMP OID 进行读操作
level-*n* (*n* = 0～15)	• level-0：可执行命令 **ping**、**tracert**、**ssh2**、**telnet** 和 **super**，且管理员可以为其配置权限 • level-1：具有 level-0 用户角色的权限，并且可执行系统所有功能和资源的相关 **display** 命令（除 **display history-command all** 之外），以及管理员可以为其配置权限 • level-2～level-8 和 level-10～level-14：无缺省权限，需要管理员为其配置权限 • level-9：可操作系统中绝大多数的功能和所有的资源，且管理员可以为其配置权限，但不能操作 **display history-command all** 命令、RBAC 的命令（Debug 命令除外）、文件管理、设备管理以及本地用户特性。对于本地用户，若用户登录系统并被授予该角色，可以修改自己的密码 • level-15：具有与 network-admin 角色相同的权限
security-audit	安全日志管理员，仅具有安全日志文件的读、写、执行权限，具体如下： • 可执行安全日志文件管理相关的命令（**display security-logfile summary**、**info-center security-logfile directory**、**security-logfile save**）。安全日志文件管理相关命令的介绍，请参见“网络管理与监控”中的“信息中心” • 可执行安全日志文件操作相关的命令，例如 **more** 显示安全日志文件内容；**dir**、**mkdir** 操作安全日志文件目录等，具体命令的介绍请参见“基础配置命令参考”中的“文件系统管理” 以上权限，仅安全日志管理员角色独有，其它任何角色均不具备
guest-manager	来宾用户管理员，只能查看和配置来宾用户管理相关Web页面，无命令行控制权限

说明

- 只有具有 network-admin 或者 level-15 用户角色的用户登录设备后才可以执行 RBAC 特性的所有命令、修改用户线视图下的相关配置（包括 **user-role**、**authentication-mode**、**protocol inbound** 和 **set authentication password**）以及执行创建/修改/删除本地用户和本地用户组；其它角色的用户，即使被授权对本地用户和本地用户组的操作权限，也仅仅具有修改自身密码的权限，没有除此之外的对本地用户和本地用户组的任何操作权限。
- 预定义的用户角色中，仅用户角色 level-0～level-14 可以通过自定义规则和资源控制策略调整自身的权限。需要注意的是，这种修改对于 **display history-command all** 命令不生效，即不能通过添加对应的规则来更改它的缺省执行权限。

4. 为用户赋予角色

根据用户登录方式的不同，为用户授权角色分为以下两类：

- 对于通过本地 AAA 认证登录设备的用户，由本地用户配置决定为其授权的用户角色。
- 对于通过 AAA 远程认证登录设备的用户，由 AAA 服务器的配置决定为其授权的用户角色。

将有效的角色成功授权给用户后，登录设备的用户才能以各角色所具有的权限来配置、管理或者监控设备。如果用户没有被授权任何角色，将无法成功登录设备。

一个用户可同时拥有多个角色。拥有多个角色的用户可获得这些角色中被允许执行的功能以及被允许操作的资源的集合。

5. 规则配置指导

定义控制命令行的规则时，通过输入命令特征字符串来指定要控制命令行的范围。特征字符串的输入需要遵循以下规则：

- 在输入命令特征字符串时必须指定该命令所在的视图，进入各视图的命令特征字符串由分号（;）分隔。分号将命令特征字符串分成多个段，每一个段代表一个或一系列命令，后一个段中的命令是执行前一个段中命令所进入视图下的命令。一个段中可以包含多个星号（*），每个星号（*）代表了 0 个或多个任意字符。例如：命令特征字符串“system ; interface * ; ip * ;” 代表从系统视图进入到任意接口视图后，以 **ip** 开头的所有命令。
- 当最后一个段中的最后一个可见字符为分号时，表示所指的命令范围不再扩展，否则将向子视图中的命令扩展。例如：命令特征字符串“system ; radius scheme * ;”代表系统视图下以 **radius scheme** 开头的所有命令；命令特征字符串“system ; radius scheme * ”代表系统视图下以 **radius scheme** 开头的所有命令，以及进入子视图（RADIUS 方案视图）下的所有命令。
- 当星号（*）出现在一个段的首部时，其后面不能再出现其它可打印字符，且该段必须是命令特征字符串的最后一个段。例如：命令特征字符串“system ; *”就代表了系统视图下的所有命令，以及所有子视图下的命令。
- 当星号（*）出现在一个段的中间时，该段必须是命令特征字符串的最后一个段。例如：命令特征字符串“debugging * event”就代表了用户视图下所有模块的事件调试信息开关命令。
- 一个段中必须至少出现一个可打印字符，不能全部为空格或 Tab。
- 对于能在任意视图下执行的命令（例如 **display** 命令）以及用户视图下的命令（例如 **dir** 命令），在配置包含此类命令的规则时，不需要在规则的命令匹配字符串中指定其所在的视图。

用户执行命令时，系统遵循以下匹配规则：

- 命令关键字与命令特征字符串是采用前缀匹配算法进行匹配的，即只要命令行中关键字的首部若干连续字符或全部字符与规则中定义的关键字相匹配，就认为该命令行与此规则匹配。因此，命令特征字符串中可以包括完整的或部分的命令关键字。例如，若规则“rule 1 deny command dis arp source *”生效，则命令 **display arp source-mac interface** 和命令 **display arp source-suppression** 都会被禁止执行。
- 基于命令的规则只对指定视图下的命令生效。若用户输入的命令在当前视图下不存在而在其父视图下被查找到时，用于控制当前视图下的命令的规则不会对其父视图下的命令执行权限进行控制。例如，定义一条规则“rule 1 deny command system ; interface * ; *”禁止用户执行接口视图下的任何命令。当用户在接口视图下输入命令 **acl basic** 3000 时，该命令仍然可以成功执行，因为系统在接口视图下搜索不到指定的 **acl** 命令时，会回溯到系统视图（父视图）下执行，此时该规则对此命令不生效。
- **display** 命令中的重定向符（“|”、“>”、“>>”）及其后面的关键字不被作为命令行关键字参与规则的匹配。例如，若规则“rule 1 permit command display debugging”生效，则命令 **display debugging > log** 是被允许执行的，其中的关键字**> log** 将被忽略，RBAC 只对重定向符前面的命令行 **display debugging** 进行匹配。但是，如果在规则中配置了重定向符，则 RBAC 会将其作为普通字符处理。例如，若规则“rule 1 permit command display debugging > log”生效，则命令 **display debugging > log** 将会匹配失败，因为其中的关键字**> log** 被 RBAC 忽略了，最终是命令 **display debugging** 与规则进行匹配。因此，配置规则时不要使用重定向符。

用户访问 SNMP OID 时，系统遵循以下匹配规则：

- 与用户访问的 OID 形成最长匹配的规则生效。例如用户访问的 OID 为 1.3.6.1.4.1.25506.141.3.0.1，角色中存在“rule 1 permit read write oid 1.3.6”，“rule 2 deny read write oid 1.3.6.1.4.1”和“rule 3 permit read write oid 1.3.6.1.4”，其中 rule 2 与用户访问的 OID 形成最长匹配，则认为 rule 2 与 OID 匹配，匹配的结果为用户的此访问请求被拒绝。
- 对于定义的 OID 长度相同的规则，规则编号大的生效。例如用户访问的 OID 为 1.3.6.1.4.1.25506.141.3.0.1，角色中存在“rule 1 permit read write oid 1.3.6”，“rule 2 deny read write oid 1.3.6.1.4.1”和“rule 3 permit read write oid 1.3.6.1.4.1”，其中 rule 2 和 rule 3 与访问的 OID 形成最长匹配，则 rule 3 生效，匹配的结果为用户的访问请求被允许。

3.4.3 密码管理

为了提高用户登录密码的安全性，可通过定义密码管理策略对用户的登录密码进行管理，并对用户的登录状态进行控制。

1. 密码长度检查

管理员可以限制用户密码的最小长度。当设置用户密码时，如果输入的密码长度小于设置的最小长度，系统将不允许设置该密码。

2. 密码组合检查

管理员可以设置用户密码的组成元素的组合类型，以及至少要包含每种元素的个数。密码的组成元素包括以下 4 种类型：

- [A～Z]

- [a～z]
- [0～9]
- 32 个特殊字符（空格~`!@#$%^&*()_+-={}|[]\:";'<>,./）

密码元素的组合类型有 4 种，具体涵义如下：

- 组合类型为 1 表示密码中至少包含 1 种元素；
- 组合类型为 2 表示密码中至少包含 2 种元素；
- 组合类型为 3 表示密码中至少包含 3 种元素；
- 组合类型为 4 表示密码中包含 4 种元素。

当用户设置密码时，系统会检查设定的密码是否符合配置要求，只有符合要求的密码才能设置成功。

3. 密码复杂度策略

为确保用户的登录密码具有较高的复杂度，要求管理员为其设置的密码必须符合一定的复杂度要求，只有符合要求的密码才能设置成功。目前，可配置的复杂度要求包括：

- 密码中不能包含连续三个或以上的相同字符。例如，密码“a111”就不符合复杂度要求。
- 密码中不能包含用户名或者字符顺序颠倒的用户名。例如，用户名为“abc”，那么“abc982”或者“2cba”之类的密码就不符合复杂度要求。

4. 密码更新管理

管理员可以设置用户登录设备后修改自身密码的最小间隔时间。当用户登录设备修改自身密码时，如果距离上次修改密码的时间间隔小于配置值，则系统不允许修改密码。例如，管理员配置用户密码更新间隔时间为 48 小时，那么用户在上次修改密码后的 48 小时之内都无法成功进行密码修改操作。

有两种情况下的密码更新并不受该功能的约束：用户首次登录设备时系统要求用户修改密码；密码老化后系统要求用户修改密码。

5. 密码老化管理

当用户登录密码的使用时间超过老化时间后，需要用户更换密码。如果用户输入的新密码不符合要求，或连续两次输入的新密码不一致，系统将要求用户重新输入。对于 FTP 用户，密码老化后，只能由管理员修改 FTP 用户的密码；对于 Telnet、SSH、Terminal（通过 Console 口或 AUX 口登录设备）用户可自行修改密码。

6. 密码过期提醒

在用户登录时，系统判断其密码距离过期的时间是否在设置的提醒时间范围内。如果在提醒时间范围内，系统会提示该密码还有多久过期，并询问用户是否修改密码。如果用户选择修改，则记录新的密码及其设定时间。如果用户选择不修改或者修改失败，则在密码未过期的情况下仍可以正常登录。对于 FTP 用户，只能由管理员修改 FTP 用户的密码；对于 Telnet、SSH、Terminal（通过 Console 口或 AUX 口登录设备）用户可自行修改密码。

7. 密码老化后允许登录

管理员可以设置用户密码过期后在指定的时间内还能登录设备指定的次数。这样，密码老化的用户不需要立即更新密码，依然可以登录设备。例如，管理员设置密码老化后允许用户登录的时间为 15 天、次数为 3 次，那么用户在密码老化后的 15 天内，还能继续成功登录 3 次。

8. 密码历史记录

系统保存用户密码历史记录。当用户修改密码时，系统会要求用户设置新的密码，如果新设置的密码以前使用过，且在当前用户密码历史记录中，系统将给出错误信息，提示用户密码更改失败。另外，用户更改密码时，系统会将新设置的密码逐一与所有记录的历史密码以及当前密码比较，要求新密码至少要与旧密码有 4 字符不同，且这 4 个字符必须互不相同，否则密码更改失败。

可以配置每个用户密码历史记录的最大条数，当密码历史记录的条数超过配置的最大历史记录条数时，新的密码历史记录将覆盖该用户最老的一条密码历史记录。

由于为用户配置的密码在哈希运算后以密文的方式保存，配置一旦生效后就无法还原为明文密码，因此，用户的当前登录密码，不会被记录到该用户的密码历史记录中。

9. 密码尝试次数限制

密码尝试次数限制可以用来防止恶意用户通过不断尝试来破解密码。

每次用户认证失败后，系统会将该用户加入密码管理的黑名单。可加入密码管理功能黑名单的用户包括：FTP 用户和通过 VTY 方式访问设备的用户。不会加入密码管理功能黑名单的用户包括：用户名不存在的用户、通过 Console 口或 AUX 口连接到设备的用户。

当用户连续尝试认证的失败累加次数达到设置的尝试次数时，系统对用户的后续登录行为有以下三种处理措施：

- 永久禁止该用户登录。只有管理员把该用户从密码管理的黑名单中删除后，该用户才能重新登录。
- 禁止该用户一段时间后，再允许其重新登录。当配置的禁止时间超时或者管理员将其从密码管理的黑名单中删除，该用户才可以重新登录。
- 不对该用户做禁止，允许其继续登录。在该用户登录成功后，该用户会从密码管理的黑名单中删除。

10. 用户帐号闲置时间管理

管理员可以限制用户帐号的闲置时间，禁止在闲置时间之内始终处于不活动状态的用户登录。若用户自从最后一次成功登录之后，在配置的闲置时间内再未成功登录过，那么该闲置时间到达之后此用户帐号立即失效，系统不再允许使用该帐号的用户登录。

3.5 系统设置

系统设置功能用来对设备的名称、位置等信息以及设备时间进行设置。

3.5.1 系统时间获取方式

为了便于管理，并保证与其它设备协调工作，设备需要准确的系统时间。系统时间由 GMT 时间、本地时区和夏令时运算之后联合决定。用户有两种方式获取 GMT 时间：

- 手工配置 GMT 时间。
- 通过 NTP/SNTP 协议获取 GMT 时间。

通过 NTP/SNTP 协议获取的 GMT 时间比命令行配置的 GMT 时间更精确。

3.5.2 NTP/SNTP简介

NTP（Network Time Protocol，网络时间协议）可以用来在分布式时间服务器和客户端之间进行时间同步，使网络内所有设备的时间保持一致，从而使设备能够提供基于统一时间的多种应用。

SNTP（Simple NTP，简单 NTP）采用与 NTP 相同的报文格式及交互过程，但简化了 NTP 的时间同步过程，以牺牲时间精度为代价实现了时间的快速同步，并减少了占用的系统资源。在时间精度要求不高的情况下，可以使用 SNTP 来实现时间同步。

3.5.3 NTP/SNTP时钟源工作模式

NTP支持服务器模式和对等体模式两种时钟源工作模式，如 表 3-4 所示。在服务器模式中，设备只能作为客户端；在对等体模式中，设备只能作为主动对等体。

SNTP 只支持服务器模式这一种时钟源工作模式。在该模式中，设备只能作为客户端，从 NTP 服务器获得时间同步，不能作为服务器为其他设备提供时间同步。

表3-4 NTP 时钟源工作模式

模式	工作过程	时间同步方向	应用场合
服务器模式	客户端上需要手工指定NTP服务器的地址。客户端向NTP服务器发送NTP时间同步报文。NTP服务器收到报文后会自动工作在服务器模式，并回复应答报文 一个客户端可以配置多个时间服务器，如果客户端从多个时间服务器获取时间同步，则客户端收到应答报文后，进行时钟过滤和选择，并与优选的时钟进行时间同步	客户端能够与NTP服务器的时间同步 NTP服务器无法与客户端的时间同步	该模式通常用于下级的设备从上级的时间服务器获取时间同步
对等体模式	主动对等体（Symmetric active peer）上需要手工指定被动对等体（Symmetric passive peer）的地址。主动对等体向被动对等体发送NTP时间同步报文。被动对等体收到报文后会自动工作在被动对等体模式，并回复应答报文 如果主动对等体可以从多个时间服务器获取时间同步，则主动对等体收到应答报文后，进行时钟过滤和选择，并与优选的时钟进行时间同步	主动对等体和被动对等体的时间可以互相同步 如果双方的时钟都处于同步状态，则层数大的时钟与层数小的时钟的时间同步	该模式通常用于同级的设备间互相同步，以便在同级的设备间形成备份。如果某台设备与所有上级时间服务器的通信出现故障，则该设备仍然可以从同级的时间服务器获得时间同步

3.5.4 NTP/SNTP时钟源身份验证

NTP/SNTP 时钟源身份验证功能可以用来验证接收到的 NTP 报文的合法性。只有报文通过验证后，设备才会接收该报文，并从中获取时间同步信息；否则，设备会丢弃该报文。从而，保证设备不会与非法的时间服务器进行时间同步，避免时间同步错误。