42 AAA and RADIUS Protocol Configuration

42.1 Overview of AAA and RADIUS

42.1.1 Overview of AAA

Authentication, Authorization and Accounting (AAA) integrates the three security functions of authentication, authorization and account into a tailorable module. It provides a unified configuration framework for management. AAA functions can be implemented with the RADIUS protocol.

The network security function of AAA mainly refers to access control, including:

- Which user can gain access to a network by means of our access equipment?
- What service can the users with access authority obtain?
- How to charge a user occupying network resource?

AAA implements the above-mentioned functions by means of the following services:

- Authentication: Authenticate a user's access right. AAA provides multiple authentication modes, including local authentication, RADIUS authentication and none, which can be simply selected as required.
- Authorization: Authorize a user with specified services and perform access control over the user.
- Accounting: Track the network resources used by a user and provides the settlement data.

Advantages of AAA:

- Flexible and easy to control
- Scalable
- Standardized authentication method, such as RADIUS
- Multiple standby systems

42.1.2 Overview of RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a distributed Client/Server system. It can protect a network against any interference resulting from unauthorized access. It can be used in various network environments requiring high security and remote user access maintenance (for example, it is used to manage a large number of scattered dial-in users using serial ports and modems). RADIUS Client runs on the DNOS platform of DER series routers. It sends an

42 AAA and RADIUS Protocol Configuration

42.1 Overview of AAA and RADIUS

42.1.1 Overview of AAA

Authentication, Authorization and Accounting (AAA) is the term used for a unified configuration framework for managing and controlling access to computer resources. The configuration, as spelled out in the term AAA, integrates the three security functions of authentication, authorization and accounting, into a customizable module. AAA functions can be implemented with the RADIUS protocol.

The network security function of AAA mainly refers to access control, including:

- Which user can gain access to a network by means of our access equipment?
- What service can the users with access authority obtain?
- How to charge a user occupying network resource?

AAA implements the above-mentioned functions by means of the following services:

- Authentication: Authenticate a user's access right. AAA provides multiple authentication modes, including local authentication, RADIUS authentication and none, which can be simply selected as required.
- Authorization: Authorize a user with specified services and perform access control over the user.
- Accounting: Track the network resources used by a user and provides the settlement data.

Advantages of AAA:

- Flexible and easy to control
- Scalable
- Standardized authentication method, such as RADIUS
- Multiple standby systems

42.1.2 Overview of RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a distributed Client/Server system. It can protect a network against any interference resulting from unauthorized access. It can be used in various network environments requiring high security and remote user access maintenance (for example, it is used to manage a large number of scattered dial-in

46 Configuring packet filtering

46.1 Overview of packet filtering

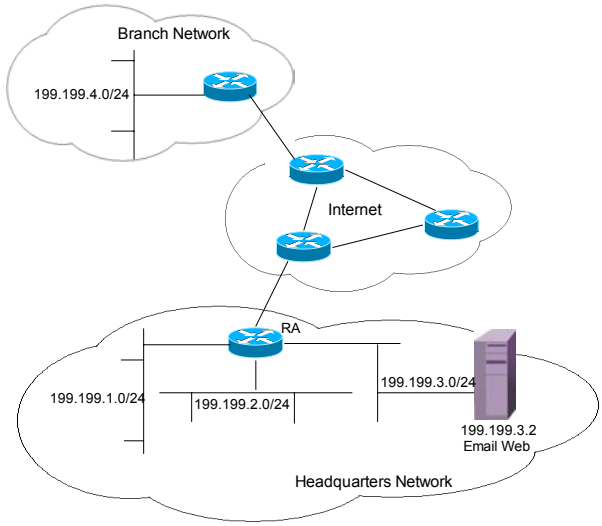
46.1.1 Introduction of packet filtering

There are two types of packet filtering: common packet filtering based on packets, and packet filtering based on status inspection.

The packet filtering based on status inspection greatly increases the flexibility and security of packet filtering, and keeps the advantages of common packet filtering by inspecting the connection status of application protocols above the network layer.

Take for example an actual network environment to illustrate the functions and principles of packet filtering.

Figure 46-1 Topology of packet filtering



The headquarters network and branch network of a company are connected via the Internet. In the headquarters, there is an e-mail and WEB server S1 to provide email services inside the company and the WEB service. A packet filtering is configured on the router RA in the headquarters to implement the following security strategies:

- Only the company employees can enjoy the service provided by the server S1.
- Only the employees in Department A1 can access the Internet without any restrictions.
- The employees in Department A2 can only access the branch network through the Internet.

The network administrator in the headquarters will configure the router RA with so-called filtering rules based on the

46 Configuring packet filtering

46.1 Overview of packet filtering

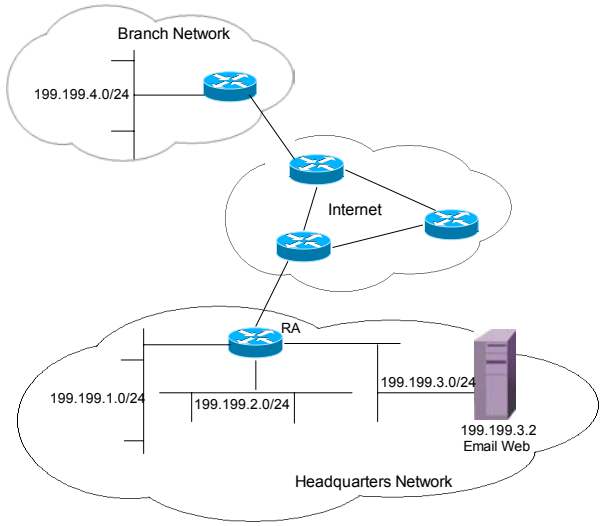
46.1.1 Introduction of packet filtering

There are two types of packet filtering: common packet filtering based on packets, and packet filtering based on status inspection.

The packet filtering based on status inspection greatly increases the flexibility and security of packet filtering, and keeps the advantages of common packet filtering by inspecting the connection status of application protocols above the network layer.

Take for example an actual network environment to illustrate the functions and principles of packet filtering.

Figure 46-1 Topology of packet filtering



The headquarters network and branch network of a company are connected via the Internet. In the headquarters, there is an e-mail and WEB server S1 to provide email services inside the company and the WEB service. A packet filtering is configured on the router RA in the headquarters to implement the following security strategies:

- Only the company employees can enjoy the service provided by the server S1.
- Only the employees in Department A1 can access the Internet without any restrictions.
- The employees in Department A2 can only access the branch network through the Internet.

The network administrator in the headquarters will configure the router RA with so-called filtering rules based on the