

AAA



## Foreword

AAA defines a security architecture that is comprised of three functions referred to as Authentication, Authorization and Accounting. Each of these functions represents a modular component which can be applied as components of the security framework implemented by an enterprise, and often managed through the use of client/server based protocols such as RADIUS and HWTACACS. Implementation of the AAA architecture as a solution for enhanced functionality is introduced to reinforce the overall security framework of the enterprise network.

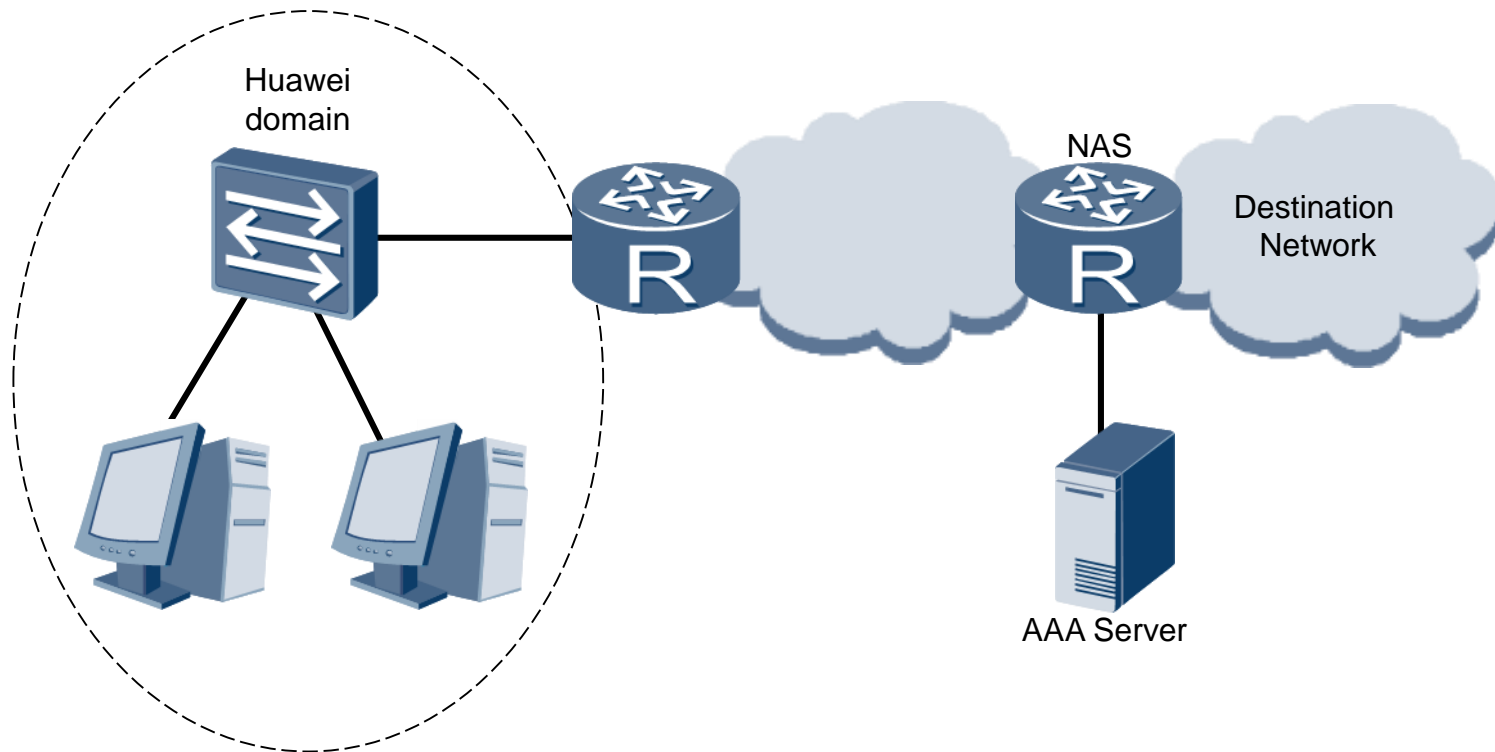


## Objectives

Upon completion of this section, trainees will be able to:

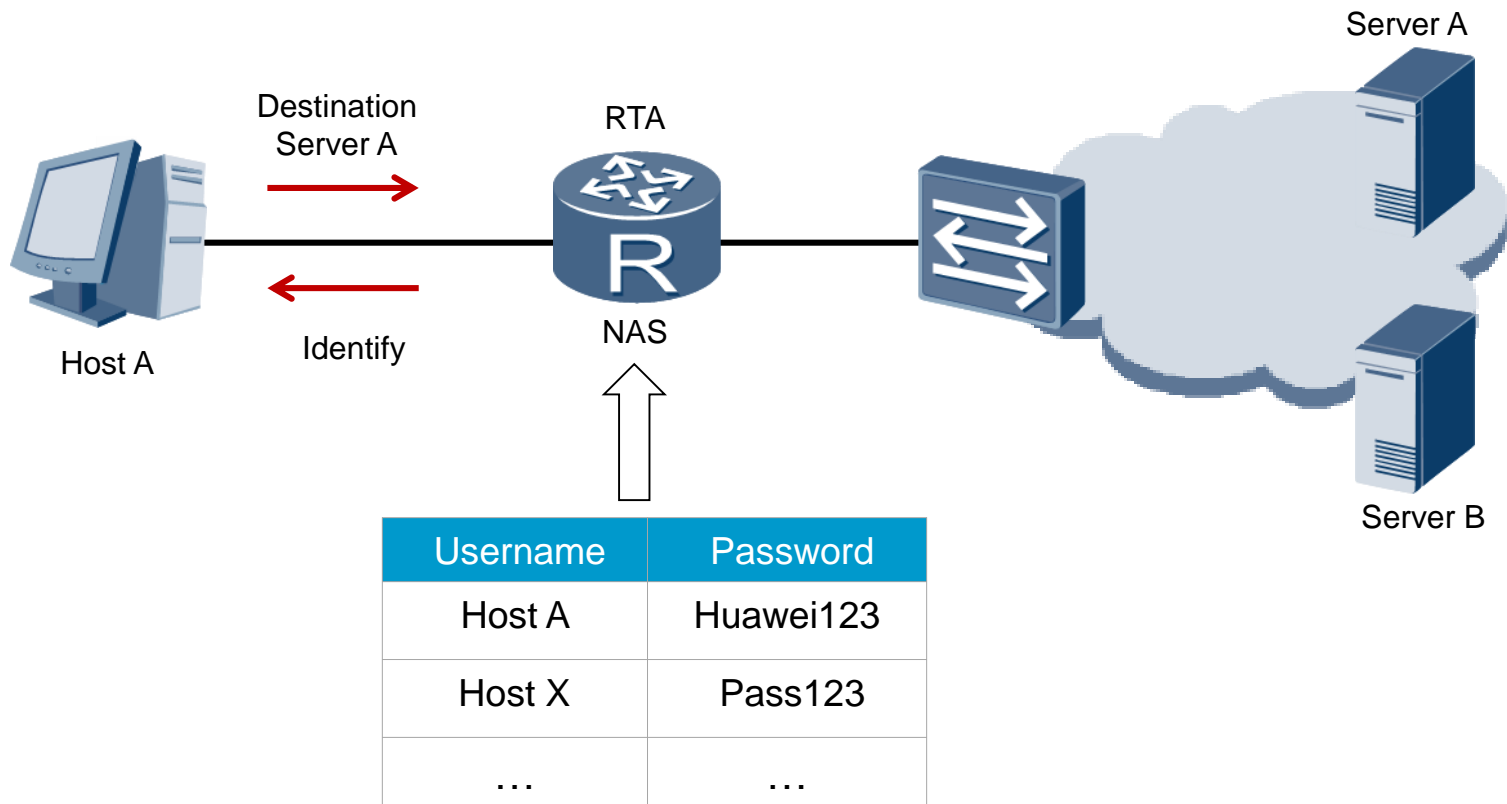
- Describe the schemes of the AAA security architecture.
- Successfully configure Authentication and Authorization schemes.

# AAA Application



- AAA enables the authentication, authorization and accounting of users attempting to access destination network resources.

# Authentication



- User access is managed based on an authentication scheme.

# Authentication

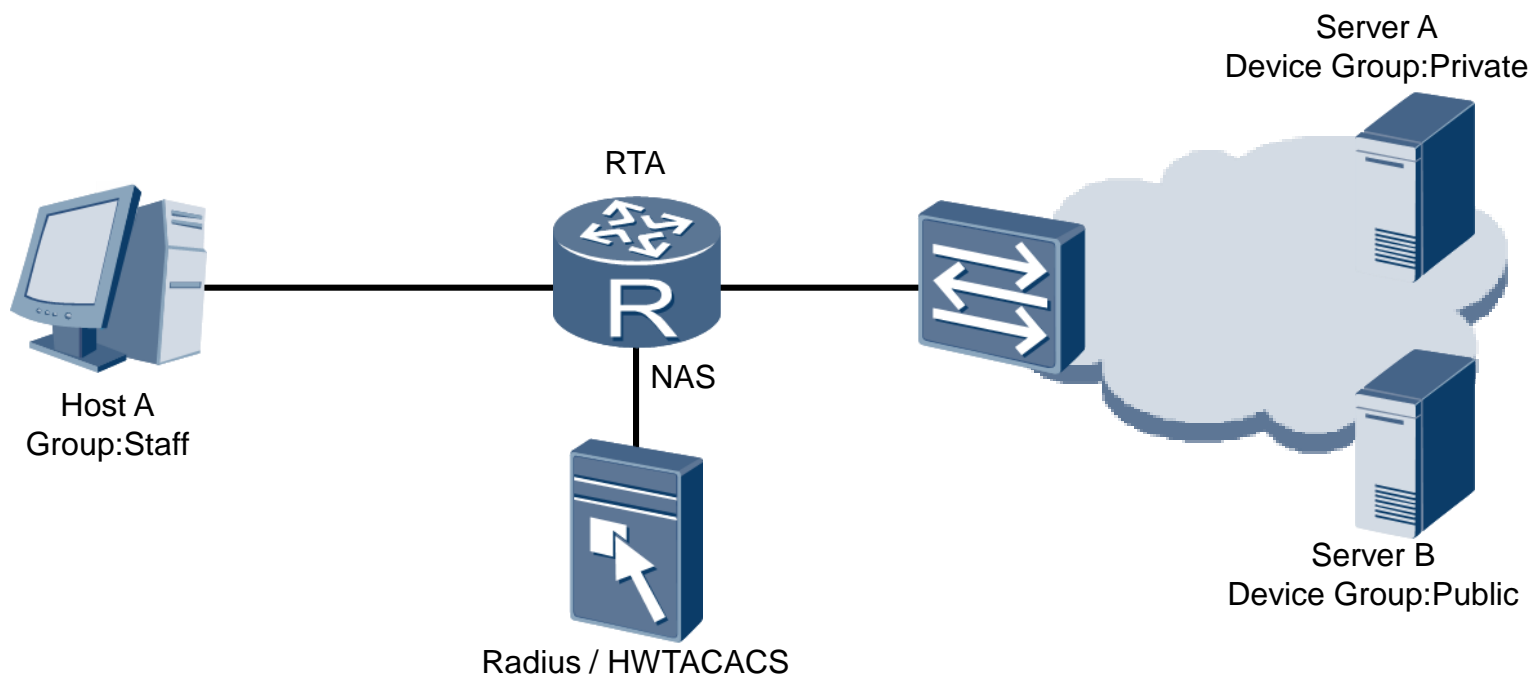
Se ci sono più metodi di autenticazione definiti, attenzione al loro ordine:

- è stata configurata prima la autenticazione remota e poi quella locale;
- l'account esiste localmente ma non sul server remoto;
- AR2200 considera l'autenticazione fallita e non prova l'autenticazione locale.

Autenticazione locale è usata solo se il server remoto **NON RISPONDE**.

La clausola di “non-authentication” deve essere l'ultima opzione disponibile.

# Authorization



Device Group	User Group	Time	Privilege
Private	Admin	09:00-12:00	15
Public	Admin	09:00-18:00	15
Public	Staff	09:00-18:00	2

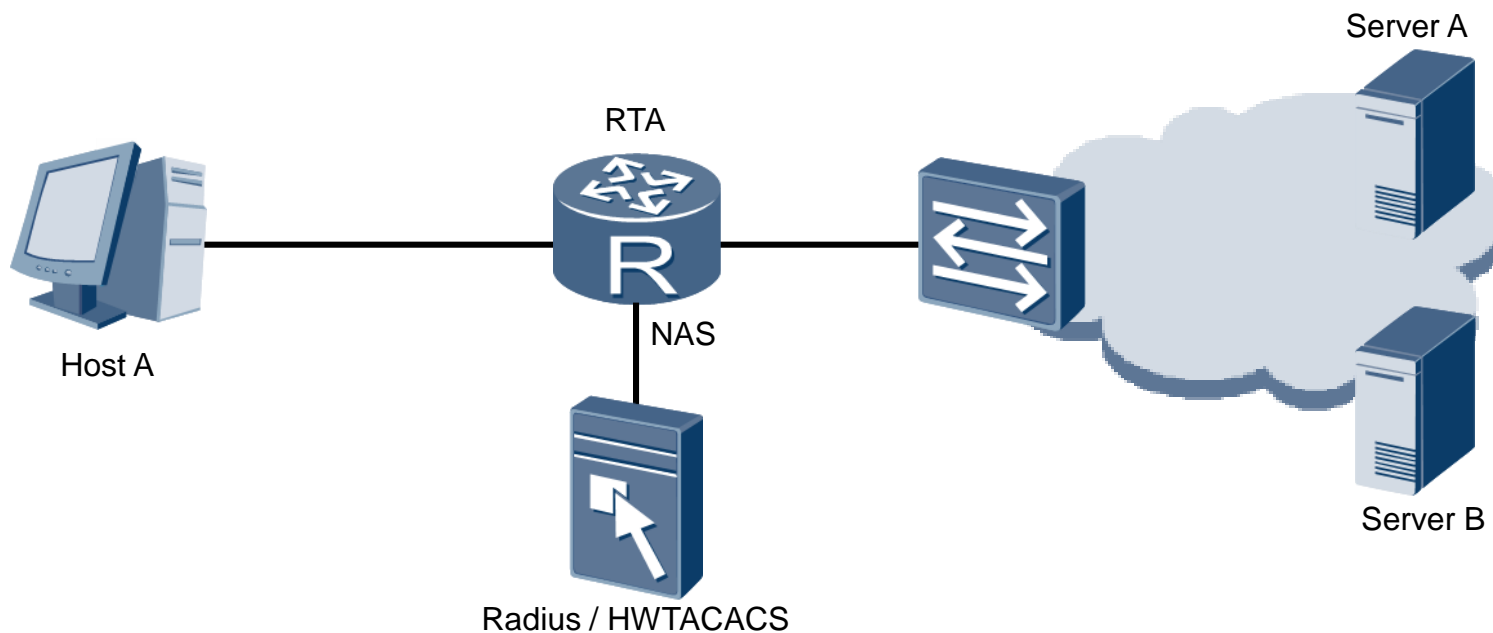
# Authorization

Radius non può essere configurato per effettuare solo autorizzazione.

Se sono configurati più metodi di autorizzazione, questi sono eseguiti nell'ordine in cui sono stati impostati.

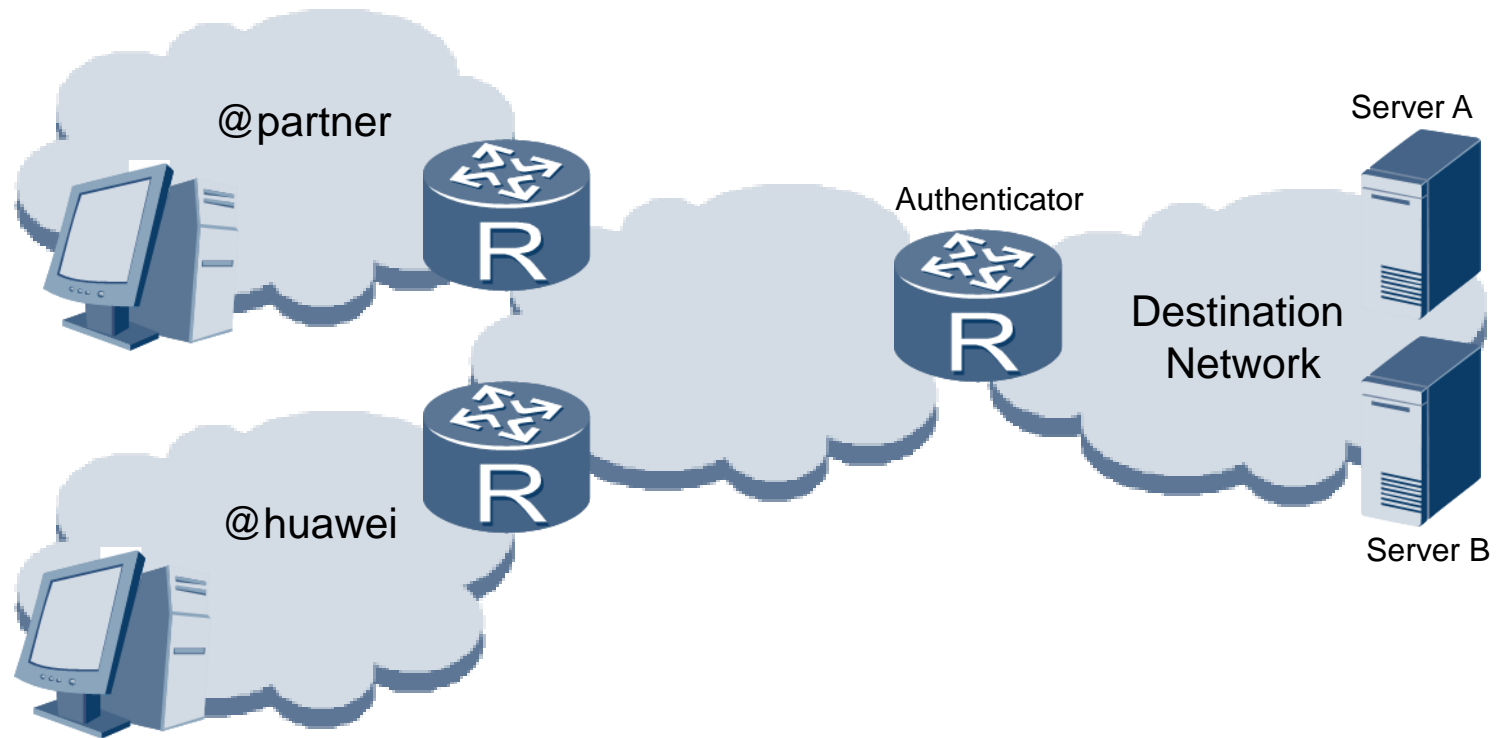


# Accounting



Login Time	Username	Uptime	Bandwidth Up/Down
May/01/2013 03:20:55	Host A	01:22:15	496.2KB / 21MB
Apr/16/2013 12:40:51	Host X	00:30:12	123KB / 1MB

# AAA Domains



- Different schemes can be applied to users in different domains.

# Dominio

Se il nome utente non contiene un delimitatore ( @ | % ) allora si considera facente parte del dominio locale di default: “default”.

Viene effettuata local authentication.

Sono disponibili due domini di default:

**default** – global default domain for common access users;

**default\_admin** – global default domain for administrators.

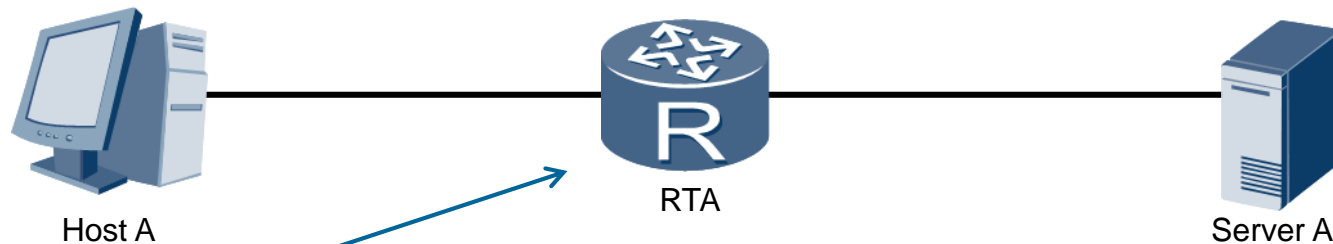
utilizzato per gli amministratori che accedono con

HTTP,SSH,TELNET,TERMINAL.

Autenticazione predefinita: locale.

Massimo 32 domini, inclusi i due locali.

# AAA Local Configuration



```
[RTA]aaa
[RTA-aaa]local-user huawei password cipher hello123
[RTA-aaa]authentication-scheme auth1
[RTA-aaa-authen-auth1]authentication-mode local
[RTA-aaa-authen-auth1]quit
[RTA-aaa] authorization-scheme auth2
[RTA-aaa-author-auth2]authorization-mode local
[RTA-aaa-author-auth2]quit
[RTA-aaa]domain huawei
[RTA-aaa-domain-huawei]authentication-scheme auth1
[RTA-aaa-domain-huawei]authorization-scheme auth2
```

- Authentication and authorization can be applied on the AR2200E.

# AAA Local Configuration Verification

```
[Huawei]display domain name huawei
Domain-name                : huawei
Domain-state                : Active
Authentication-scheme-name  : auth1
Accounting-scheme-name     : default
Authorization-scheme-name   : auth2
Service-scheme-name        : -
RADIUS-server-template     : -
HWTACACS-server-template   : -
User-group                  : -
```

- Local AAA schemes are associated with individual domains.



## Summary

- Which two AAA schemes are supported when configuring VRP to support the local mode?
- If no domain is defined for users, what action is taken?



**Thank you**  
[www.huawei.com](http://www.huawei.com)