目 录

1 Password Control ····· 1-1
1.1 Password Control简介 ····· 1-1
1.2 Password Control配置任务简介 ····· 1-4
1.3 配置Password Control ····· 1-4
1.3.1 使能密码管理 ····· 1-4
1.3.2 配置全局密码管理 ····· 1-5
1.3.3 配置用户组密码管理 ····· 1-7
1.3.4 配置本地用户密码管理 ····· 1-7
1.3.5 配置super密码管理 ····· 1-9
1.3.6 以交互式方式设置本地用户密码 ····· 1-10
1.4 Password Control显示和维护 ····· 1-10
1.5 Password Control典型配置举例 ····· 1-10

1 Password Control

1.1 Password Control简介

Password Control（密码管理）是本地认证服务器提供的密码安全功能，它根据管理员设置的安全策略对用户的登录密码、super 密码和用户的登录状态进行控制。密码管理功能实现的密码安全策略包括：

1. 密码最小长度限制

根据系统安全需求不同，管理员可以设置用户密码的最小长度。当用户设置用户密码时，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，此时将显示出错信息，提醒用户重新输入密码。

2. 密码更新间隔时间管理

管理员可以根据系统安全需求，设置用户登录设备后修改自身密码的最小间隔时间。当非管理级别的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。这样可以有效防止登录用户频繁进行修改密码的操作。

说明

- 非 FIPS 模式下，该功能对管理级别的用户不生效。FIPS 模式下，该功能对管理级别的用户同样生效。关于用户级别的详细介绍请参见“基础配置指导”中的“CLI”。
- 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。

---

3. 密码老化管理

密码老化时间用来限制用户密码的使用时间。当密码的使用时间超过老化时间超时后，需要用户更换密码。

当用户登录时，如果用户输入已经过期的密码，系统将提示该密码已经过期，需要重新设置密码。如果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。

4. 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。

说明

在密码老化管理和密码过期提醒这两项功能中，不允许 FTP 用户更改密码，只能通过管理员修改 FTP 用户的密码；允许 Telnet、SSH、Terminal（通过 Console 或 AUX 登录设备）用户自行修改密码。

5. 密码老化后允许登录管理

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。这样允许密码过期的用户登录设备时不需要立即更新密码。

6. 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，旧的密码将被记录下来，形成该用户的密码历史记录。如果用户新设置的密码以前被使用过，系统将给出错误提示，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历史密码相比较，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。

7. 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。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，通过设置可以有三种选择：

- 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。
- 不对该用户做禁止，允许其继续登录。在该用户登录成功或者密码管理黑名单的老化时间（系统规定为 1 分钟）超时后，该用户会从该黑名单中被删除。
- 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。

说明

- 密码管理的黑名单的最大条数为 1024。不存在的用户进行登录认证时将失败，但不将该用户加入黑名单中。
- FTP 用户和通过 VTY 方式访问设备的用户在认证失败后，会被加入密码管理的黑名单。
- Web 用户认证失败不会加入密码管理黑名单。另外，通过 Console 或 AUX 连接到设备的用户，由于系统无法获得其 IP 地址，且通过这两种方式访问设备的用户已经具备了一定的权限和安全性，所以认证失败后也不会被加入密码管理的黑名单。

8. 密码的组合检测功能

根据系统安全需求不同，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：

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

密码元素的组合级别为 1～4 级，级别表示设置密码时至少要包含的密码元素种类数目：

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

当用户设定或修改密码时，系统检查设定的密码是否符合配置要求。如果不符合，将给出错误提示。

在 FIPS 模式下，密码元素的组合级别必须为 4。

MSR 系列路由器各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR 900	FIPS配置	不支持
MSR 930		不支持
MSR 20-1X		不支持
MSR 20		支持
MSR 30		支持，仅MSR 3016不支持
MSR 50		支持
MSR 2600		支持

9. 密码的复杂度检测功能

密码的复杂度越低，其被破解的可能性就越大，比如包含用户名、使用重复字符等。出于安全性考虑，管理员可以设置用户密码的复杂度检测功能，确保用户的密码具有较高的复杂度。具体实现是：配置本地用户密码时，系统检测输入的密码是否符合一定的复杂度要求，如果不符合复杂度要求，则提示密码配置失败。目前，复杂度检测功能对密码的复杂度要求包括：

- 密码中不能包含用户名或者颠倒的用户名。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。
- 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。

10. 密码回显为“*”

出于安全考虑，用户输入的密码中的每个字符均以“*”显示。

11. 认证超时管理

认证超时管理只针对 Telnet 用户和 Terminal 用户。

认证过程的时间为：从服务器获得用户名到该用户的密码验证结束的时间。用户如果在规定时间内没有完成认证，则认证失败，用户连接将被断开。

12. 用户帐号闲置时间管理

根据系统安全需求，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账号立即失效，系统不再允许使用该用户账号登录。例如，管理员配置用户帐号的闲置时间为 60 天，如果用户名为 test 的用户自最后一次成功登录之后的 60 天内，都未成功登录过设备，那么该用户帐号 test 就会失效。

13. 日志功能

系统对用户成功修改密码事件和用户登录失败加入密码管理黑名单事件有相应的日志记录。

1.2 Password Control配置任务简介

本特性的各功能可支持在多个视图下配置，各视图可支持的功能不同。而且，相同功能的命令在不同视图下或针对不同密码时有效范围有所不同，具体情况如下：

- 系统视图下的全局配置对所有本地用户密码和 super 密码都有效；
- 用户组视图下的配置只对当前用户组内的所有本地用户密码有效；
- 本地用户视图下的配置只对当前的本地用户密码有效；
- 为 super 密码的各管理参数所作的配置只对 super 密码有效。

上述四者之间的优先级关系如下：

- 对于本地用户密码的各管理参数来说，其生效的优先级顺序由高到底依次为本地用户视图、用户组视图、系统视图。
- 对于 super 密码的各管理参数来说，系统优先采用单独为 super 密码所作的单独配置；如果没有为 super 密码进行单独配置时，采用全局配置。

表1-1 Password Control 配置任务简介

配置任务	说明	详细配置
使能密码管理	必选	1.3.1
配置全局密码管理	可选	1.3.2
配置用户组密码管理	可选	1.3.3
配置本地用户密码管理	可选	1.3.4
配置super密码管理	可选	1.3.5
以交互式方式设置本地用户密码	可选	1.3.6

1.3 配置Password Control

1.3.1 使能密码管理

使能密码管理功能包括两个部分：

(1) 使能全局密码管理功能。只有使能全局密码管理功能后，密码管理相关的配置才能生效。

(2) 使能指定的密码管理功能。某些密码安全策略在使能全局密码管理功能后，还需要单独使能指定的密码管理功能才能生效。这些密码管理功能包括：

- 密码老化管理
- 密码最小长度管理
- 密码历史记录管理
- 密码组合检测管理功能

表1-2 使能密码管理

操作	命令	说明
进入系统视图	**system-view**	-
使能全局密码管理功能	**password-control enable**	必选 缺省情况下，全局密码管理功能处于未使能状态
使能指定的密码管理功能	**password-control** { **aging** | **composition** | **history** | **length** } **enable**	可选 缺省情况下，各密码管理功能均处于使能状态

说明

使能了全局密码管理功能后，设备上已配置的本地用户密码将不被显示，即无法通过相应的 **display** 命令查看本地用户密码。

1.3.2 配置全局密码管理

表1-3 配置全局密码管理

操作	命令	说明
进入系统视图	**system-view**	-
配置密码的老化时间	**password-control aging** *aging-time*	可选 缺省情况下，密码的老化时间为90天
配置密码更新的最小时间间隔	**password-control password update interval** *interval*	可选 缺省情况下，密码更新的最小时间间隔为24小时
配置密码的最小长度	**password-control length** *length*	可选 缺省情况下，密码的最小长度为10个字符
配置用户密码的组合策略	**password-control composition type-number** *type-number* [**type-length** *type-length*]	可选 缺省情况下，密码元素的组合类型至少为1种，至少要包含每种元素的个数为1个

操作	命令	说明
		在FIPS模式下，*type-number*取值必须为4
配置用户密码的复杂度检查策略	**password-control complexity** { **same-character** | **user-name** } **check**	可选 缺省情况下，不对用户密码进行复杂度检查
配置每个用户密码历史记录的最大条数	**password-control history** *max-record-num*	可选 缺省情况下，每个用户密码历史记录的最大条数为4条
配置用户登录尝试次数以及登录尝试失败后的行为	**password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	可选 缺省情况下，用户登录尝试次数为3次；如果用户登录失败，则1分钟后再允许该用户重新登录
配置密码老化前的提醒时间	**password-control alert-before-expire** *alert-time*	可选 缺省情况下，密码老化前的提醒时间为7天
配置密码过期后允许用户登录的时间和次数	**password-control expired-user-login delay** *delay* **times** *times*	可选 缺省情况下，密码过期后的30天内允许用户登录3次
配置用户认证的超时时间	**password-control authentication-timeout** *authentication-timeout*	可选 缺省情况下，用户认证的超时时间为60秒
配置用户帐号的闲置时间	**password-control login idle-time** *idle-time*	可选 缺省情况下，用户帐号的闲置时间为90天

注意

用户登录尝试失败后的行为的配置属于即时生效的配置，会在配置生效后立即影响密码管理黑名单中当前用户的锁定状态以及这些用户后续的登录，而其它配置生效后仅对后续登录的用户以及后续设置的用户密码有效，不影响当前用户。

MSR 系列路由器各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR 900	FIPS模式	不支持
MSR 930		不支持
MSR 20-1X		不支持
MSR 20		支持
MSR 30		支持，仅MSR 3016不支持
MSR 50		支持

型号	特性	描述
MSR 2600		支持

1.3.3 配置用户组密码管理

表1-4 配置用户组密码管理

操作	命令	说明
进入系统视图	**system-view**	-
创建用户组，并进入用户组视图	**user-group** *group-name*	-
配置用户组的密码老化时间	**password-control aging** *aging-time*	可选 缺省情况下，采用全局密码老化时间
配置用户组的密码最小长度	**password-control length** *length*	可选 缺省情况下，采用全局密码最小长度 在FIPS模式下，密码长度至少为8位 非FIPS模式下，密码长度至少为4位
配置用户组的密码组合策略	**password-control composition type-number** *type-number* [**type-length** *type-length*]	可选 缺省情况下，采用全局密码组合策略 在FIPS模式下，*type-number*取值必须为4

MSR 系列路由器各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR 900	FIPS模式	不支持
MSR 930		不支持
MSR 20-1X		不支持
MSR 20		支持
MSR 30		支持，仅MSR 3016不支持
MSR 50		支持
MSR 2600		支持

1.3.4 配置本地用户密码管理

表1-5 配置本地用户密码管理

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
创建本地用户，并进入本地用户视图	**local-user** *user-name*	-
配置本地用户的密码老化时间	**password-control aging** *aging-time*	可选 缺省情况下，采用本地用户所属用户组的密码老化时间，若用户组未配置该值，则采用全局配置
配置本地用户的密码最小长度	**password-control length** *length*	可选 缺省情况下，采用本地用户所属用户组的密码最小长度，若用户组未配置该值，则采用全局配置 在FIPS模式下，密码长度至少为8位 非FIPS模式下，密码长度至少为4位
配置本地用户的密码组合策略	**password-control composition type-number** *type-number* [**type-length** *type-length*]	可选 缺省情况下，采用本地用户所属用户组的密码组合策略，若用户组未配置该值，则采用全局配置 在FIPS模式下，*type-number*取值必须为4

MSR 系列路由器各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR 900	FIPS模式	不支持
MSR 930		不支持
MSR 20-1X		不支持
MSR 20		支持
MSR 30		支持，仅MSR 3016不支持
MSR 50		支持
MSR 2600		支持

1.3.5 配置super密码管理

说明

- 系统命令行采用分级保护方式：命令行级别由低到高被划分为访问级、监控级、系统级、管理级 4 个级别。同时对登录用户划分等级，分为 4 级，分别与上述的命令行级别对应，即不同级别的用户登录后，只能使用等于或低于自己级别的命令。
- 为了防止未授权用户的非法侵入，在从低级别用户切换到高级别用户时，要进行用户身份验证，即需要输入高级别用户密码，这个高级别的密码就被称为 super 密码。关于 super 密码的详细介绍，请参见“基础配置指导”中的“CLI”。

表1-6 配置 super Password Control

操作	命令	说明
进入系统视图	**system-view**	-
配置super密码的老化时间	**password-control super aging** *aging-time*	可选 缺省情况下，super密码的老化时间为全局密码老化时间
配置super密码的最小长度	**password-control super length** *length*	可选 缺省情况下，super密码的最小长度为全局密码最小长度 在FIPS模式下，密码长度至少为8位 非FIPS模式下，密码长度至少为4位
配置super密码的组合策略	**password-control super composition type-number** *type-number* [**type-length** *type-length*]	可选 缺省情况下，super密码组合策略为全局密码组合策略 在FIPS模式下，*type-number*取值必须为4

MSR 系列路由器各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR 900	FIPS模式	不支持
MSR 930		不支持
MSR 20-1X		不支持
MSR 20		支持
MSR 30		支持，仅MSR 3016不支持
MSR 50		支持
MSR 2600		支持

1.3.6 以交互式方式设置本地用户密码

以交互方式设置本地用户密码时会要求用户在输入本地密码后进行密码确认。

表1-7 以交互式方式设置本地用户密码

操作	命令	说明
进入系统视图	**system-view**	-
创建本地用户，并进入本地用户视图	**local-user** *user-name*	-
以交互式方式设置本地用户密码	**password**	必选

1.4 Password Control显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 Password Control 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 Password Control 统计信息。

表1-8 Password Control 显示和维护

操作	命令
显示密码管理的配置信息	**display password-control** [**super**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示用户认证失败后，被加入密码管理黑名单中的用户信息	**display password-control blacklist** [**user-name** *name* | **ip** *ipv4-address* | **ipv6** *ipv6-address*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除密码管理黑名单中的用户	**reset password-control blacklist** [**user-name** *name*]
清除用户的密码历史记录	**reset password-control history-record** [**user-name** *name* | **super** [**level** *level*]]

说明

当密码历史记录功能未启动时，**reset password-control history-record** 命令同样可以清除全部或者某个用户的密码历史记录。

1.5 Password Control典型配置举例

1. 组网需求

有以下密码管理需求：

- 全局密码管理策略：用户 2 次登录失败后就永久禁止登录；密码老化时间为 30 天；允许用户进行密码更新的最小时间间隔为 36 小时；密码过期后 60 天内允许登录 5 次；用户帐号的闲

置时间为 30 天；不允许密码中包含用户名或者颠倒用户名；不允许密码中包含连续三个或以上字符。

- super 密码管理策略：密码元素的最少组合类型为 3 种，至少要包含每种元素的个数为 5 个。
- 本地 Telnet 用户 test 的密码管理策略：最小密码长度为 12 个字符，密码元素的最少组合类型为 2 种，至少要包含每种元素的个数为 5 个，密码老化时间为 20 天。

2. 配置步骤

使能全局密码管理功能。

```
<Sysname> system-view
[Sysname] password-control enable
```

配置用户 2 次登录失败后就永久禁止该用户登录。

```
[Sysname] password-control login-attempt 2 exceed lock
```

配置全局的密码老化时间为 30 天。

```
[Sysname] password-control aging 30
```

配置密码更新的最小时间间隔为 36 小时。

```
[Sysname] password-control password update interval 36
```

配置用户密码过期后的 60 天内允许登录 5 次。

```
[Sysname] password-control expired-user-login delay 60 times 5
```

配置用户帐号的闲置时间为 30 天。

```
[Sysname] password-control login idle-time 30
```

使能在配置的密码中检查包含用户名或者颠倒的用户名的功能。

```
[Sysname] password-control complexity user-name check
```

使能在配置的密码中检查包含连续三个或以上相同字符的功能。

```
[Sysname] password-control complexity same-character check
```

配置 super 密码元素的最少组合类型为 3 种，至少要包含每种元素的个数为 5 个。

```
[Sysname] password-control super composition type-number 3 type-length 5
```

配置 super 密码。

```
[Sysname] super password level 3 simple 12345ABGFTweuix
```

添加本地用户 test。

```
[Sysname] local-user test
```

配置本地用户的服务类型为 Telnet。

```
[Sysname-luser-test] service-type telnet
```

配置本地用户的最小密码长度为 12 个字符。

```
[Sysname-luser-test] password-control length 12
```

配置本地用户的密码元素的最少组合类型为 2 种，至少要包含每种元素的个数为 5 个。

```
[Sysname-luser-test] password-control composition type-number 2 type-length 5
```

配置本地用户的密码老化时间为 20 天。

```
[Sysname-luser-test] password-control aging 20
```

以交互式方式配置本地用户密码。

```
[Sysname-luser-test] password
Password:***********
Confirm :***********
Updating user(s) information, please wait........
```

```
[Sysname-luser-test] quit
```

3. 验证配置结果

可通过如下命令查看全局密码管理的配置信息。

```
<Sysname> display password-control
Global password control configurations:
 Password control:                    Enabled
 Password aging:                      Enabled (30 days)
 Password length:                     Enabled (10 characters)
 Password composition:                Enabled (1 types,  1 characters per type)
 Password history:                    Enabled (max history record:4)
 Early notice on password expiration: 7 days
 User authentication timeout:         60 seconds
 Maximum failed login attempts:       2 times
 Login attempt-failed action:         Lock
 Minimum password update time:        36 hours
 User account idle-time:              30 days
 Login with aged password:            5 times in 60 day(s)
 Password complexity:                 Enabled (username checking)
                                      Enabled (repeated characters checking)
```

可通过如下命令查看 super 密码管理的配置信息。

```
<Sysname> display password-control super
 Super password control configurations:
 Password aging:                      Enabled (30 days)
 Password length:                     Enabled (10 characters)
 Password composition:                Enabled (3 types,  5 characters per type)
```

可通过如下命令查看到本地用户密码管理的配置信息。

```
<Sysname> display local-user user-name test
The contents of local user test:
 State:                    Active
 ServiceType:              telnet
 Access-limit:             Disable           Current AccessNum: 0
 User-group:               system
 Bind attributes:
 Authorization attributes:
 Password aging:                       Enabled (20 days)
 Password length:                      Enabled (12 characters)
 Password composition:                 Enabled (2 types,  5 characters per type)
Total 1 local user(s) matched.
```