

[19] 中华人民共和国国家知识产权局



[12] 发明专利申请公布说明书

[21] 申请号 200910023078.4

[43] 公开日 2009 年 11 月 18 日

[51] Int. Cl.

H04L 12/24 (2006.01)

H04L 29/06 (2006.01)

[11] 公开号 CN 101582794A

[22] 申请日 2009.6.26

[21] 申请号 200910023078.4

[71] 申请人 西安电子科技大学

地址 710071 陕西省西安市太白路 2 号

[72] 发明人 朱 辉 李 晖 尹 铛 刘 欢
段海生

[74] 专利代理机构 陕西电子工业专利中心

代理人 王品华 朱红星

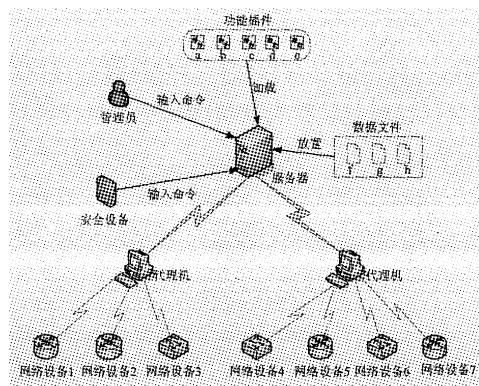
权利要求书 3 页 说明书 8 页 附图 3 页

[54] 发明名称

网络设备统一配置系统及其配置方法

[57] 摘要

本发明公开了一种网络设备统一配置系统及其配置方法，主要解决现有的配置方法对网络设备的配置工作量大和缺乏安全功能的问题。它使用一套自行设计的命令集来统一配置不同厂家、不同型号的网络设备，其主要组成部分有服务器、代理机和网络设备，服务器中加载有命令事件采集插件、回复事件采集插件、事件格式扩展插件、场景分析插件、事件响应插件和设备信息文件、命令转换信息文件、命令转换规则文件。自设计命令在服务器上转换为能够在目标网络设备中执行的特定命令后经由代理机转发给网络设备执行，待执行完毕其输出信息被发送给代理机进行处理并返回给服务器。本发明具有方便集中、统一配置网络设备的优点，能够被广泛应用于计算机网络管理领域。



1、一种网络设备统一配置系统，包括网络设备和服务器，其特征在于：

网络设备的输入端连接有代理机，用于转发来自服务器的命令至网络设备、接收、处理网络设备中命令执行后的输出信息，并将处理结果返回给服务器；

服务器内加载有功能插件和数据文件，用于接受用户输入的命令和转换命令，并发送至代理机、接收回复输出到终端；

所述的功能插件包括：

A. 接受输入命令、判断命令格式正误、封装并生成命令事件的命令事件采集插件；

B. 接收回信息、生成回复事件的回复事件采集插件；

C. 定义命令、命令事件和回复事件格式的事件格式扩展插件；

D. 判断命令是否能被转换、触发响应插件转换命令、由回复事件到达或计时器超时结束命令转换执行状态变迁的场景分析插件；

E. 转换输入命令为能在目标设备执行的命令、并发送至代理机的事件响应插件；

所述的数据文件包括：

a. 存储设备 ID、设备型号、代理机 IP、代理机端口的设备信息文件；

b. 存储设备型号、各型号对应的转换规则文件名的命令转换信息文件；

c. 存储统一命令、对应具体型号的命令信息的命令转换规则文件。

2. 根据权利要求 1 所述的网络设备统一配置系统，其特征在于：所述网络设备包括交换机、路由器。

3. 根据权利要求 1 所述的网络设备统一配置系统，其特征在于：所述代理机包括接收命令模块和发送回复模块，接收命令模块用于接收来自服务器的命令，转发命令给网络设备；发送回复模块用于接收并处理网络设备中命令执行后的输出信息，将处理后的信息返回给服务器。

4. 一种网络设备统一配置方法，包括如下步骤：

(1) 设计一套可用于配置不同厂家、不同型号网络设备的统一命令集，将设备信息文件、命令转换信息文件、命令转换规则文件放置于服务器中；

(2) 在服务器中加载命令事件采集插件、命令事件格式扩展插件、场景分析插件、事件响应插件、回复事件采集插件；

(3) 用户从终端输入需要配置的目标网络设备号和统一命令集中的一条命令，命令事件采集插件获得该命令后对其格式进行判断，若格式正确，则根据命令事件格式扩展插件中定义的事件格式生成命令事件，若格式错误，则结束该条命令的执行；

(4) 命令事件生成后，场景分析插件根据命令转换信息文件和目标网络设备对应的命令转换规则文件，对命令状态转移条件进行匹配，判断终端输入的命令是否符合转换规则，若不符合转换规则，变迁命令状态，结束该条命令的执行，若符合转换规则，亦变迁命令状态，触发事件响应插件转换并发送命令，同时开启计时器为接收回复消息计时；

(5) 事件响应插件由场景分析插件触发后，根据目标网络设备对应的命令转换规则，先将终端输入的命令转换为能在目标网络设备上执行的若干条命令，再通过查询设备信息文件获得目标网络设备相连的代理机 IP，最后将目标网络设备号、命令 ID 和转换后的命令信息一起发送到该代理机；

(6) 代理机接收到来自服务器的信息后，根据目标网络设备号，查找到该目标网络设备的 IP，然后把命令转发给目标网络设备执行，同时将命令 ID 存储于本地；

(7) 目标网络设备执行来自代理机转发的命令后，将终端输出信息回复给代理机进行处理，处理后的回复信息和保存的命令 ID 被代理机一并发回给服务器；

(8) 服务器中的回复事件采集插件将接受到的回复信息生成回复事件后，场景分析插件通过匹配状态转移条件，分析回复中所带的命令 ID 与发送命令的 ID 是否相同，若相同，变迁命令状态，打印回复信息到终端，并结束该条命令的执行，若不相同或始终未接受到回复信息，则下一条命令输入时，计时器超时，匹配该条命令的状态转移条件，变迁命令状态，结束该条命令的执行。

5. 根据权利要求 4 所述的网络设备统一配置方法，其中步骤 4 所述命令状态转移条件

包括：

1) IncorrectCmd 条件：若命令不符合转换规则，则匹配该条件，使命令从状态 s0 变迁到状态 final；

2) CorrectCmd 条件：若命令符合转换规则，则匹配该条件，使命令从状态 s0 变迁到状态 send；

3) Reply 条件：若接收到的回复中所带命令 ID 与发送命令的 ID 相同，则匹配该条件，使命令从状态 send 变迁到状态 final；

4) TimerExpiry 条件：若计时器超时，则匹配该条件，使命令从状态 send 变迁到状态 final。

6. 根据权利要求 4 所述的网络设备统一配置方法，其中步骤 4 所述的命令状态包括：

- a) 初始状态 s0: 命令一开始所处的状态;
- b) 发送状态 send: 用于触发事件响应插件转换并发送命令, 同时开启计时器为接收到回复消息计时;
- c) 终止状态 final: 用于结束命令的执行。

网络设备统一配置系统及其配置方法

技术领域

本发明属于计算机网络管理领域，涉及网络设备的配置，可用于对不同厂家、不同型号的网络设备进行集中化和统一化管理。

背景技术

自网络设备诞生之初，人们就开始在配置和管理它们，用以维护一个个计算机网络，事实上，配置网络设备并非难事，以下即是几种简单可行的方案：

1、telnet——这是最常用的配置网络设备的方案，几乎所有厂家的网络设备都支持这个协议。用户只需要在本地终端键入 telnet 命令，输入用户名和口令，就可以登陆网络设备进行操作和管理。这些在本地输入的发送给设备执行的命令就像是直接在设备的控制台上输入一样，操作十分简单。它的优点是普遍性，为 Internet 远程登陆服务的标准协议和主要方式。

2、安全 shell 连接 SSH——这是安全性极高的一种配置方案，它可以对所有的传输数据进行加密，能防止“中间人”攻击、DNS 和 IP 欺骗，另外，还有一个额外的优点就是传输的数据是经过压缩的，可以加快传输的速度。在安全性要求比较高的场合完全可以代替 telnet，只是有些网络设备若要支持此协议，必须另外进行配置。

3、远程桌面——这是微软公司为了方便网络管理员管理维护服务器而推出的一项服务。从 windows 2000 server 版本开始引入，网络管理员使用远程桌面连接程序连接到网络任意一台开启了远程桌面控制功能的计算机上，就如同自己操作该计算机一样，运行程序，维护数据库等。远程桌面从某种意义上类似于早期的 telnet，它可以将程序运行等工作交给服务器，而返回给远程控制计算机的仅仅是图象，鼠标键盘的运动变化轨迹。

4、简单网络管理协议 SNMP——是一种简单网络管理协议，其前身是简单网关监控协议 SGMP，用来对通信线路进行管理。随后，人们对 SGMP 进行了很大的修改，特别是加入了符合Internet定义的 SMI 和MIB体系结构，改进后的协议就是著名的 SNMP。SNMP 的目标是管理互联网 Internet 上众多厂家生产的软硬件平台，因此 SNMP 受 Internet 标准网络管理框架的影响也很大。现在 SNMP 已经出到第三个版本的协议，其功能较以前已经大大地加强和改进了。SNMP 的体系结构是围绕着以下四个概念和目标进行设计的：保持管理代理的软件成本尽可能低；最大限度地保持远程管理的功能，以便充分利用 Internet 的网络资源；体系结构必须有扩充的余地；保持 SNMP 的独立性，不依赖于

具体的计算机、网关和网络传输协议。在最近的改进中，又加入了保证 SNMP 体系本身安全性的目标。

上述这些配置方案虽然已为用户所普遍使用，但是存在以下不足：

1) 统一化管理程度低。现有的配置方案往往只适用于同时配置一台或几台机器，当网络中的设备数量增加时，用户需要频繁地切换、登陆不同的设备终端上，而不能在同一平台上对所有控制的设备进行配置和管理，所以集中、统一管理网络设备的问题有待解决。

2) 配置工作量大。由于各个网络设备生产厂家出于对自身利益的考虑，都会为自家的设备配备特有的配置命令集，而且，对不同型号的设备所配备的命令集大小还不尽相同。这种维权主义的直接后果是增添了网络管理人员的烦恼，例如要对不同厂家、不同型号的设备配置同一属性，则需要输入不同的命令。如今网络设备的厂商、型号何其之多，生成的命令简直多如牛毛，且不论能否记住，哪怕是翻手册查询也实属一项痛苦的差事。

3) 缺乏安全功能。管理一个网络，除了对网络中的设备进行配置管理以外，还应该慎重考虑的一个问题就是网络的安全问题，对于网络管理人员来说，在忙于配置管理设备的同时还必须时刻关注网络中的安全事件，否则一旦有安全事件发生，网络将变得岌岌可危，这无形中增加了网络管理人员的工作量，而且容易造成对安全问题的疏忽，如果能够将配置网络设备和保障网络安全两者结合在一起，由一套配置系统来实现，那就可以减轻网络管理人员的负担，同时提高网络的安全性，但是现有的配置方案往往只能用于配置网络设备，而缺乏保障网络安全的功能，无法满足网络管理人员的需求。

发明内容

本发明的目的在于克服上述已有技术的缺点，提供一种网络设备统一配置系统及其配置方法，以使用一套命令集实现对所有的网络设备进行配置，并同时联动安全设备处理安全事件。

为实现上述目的，本发明的统一配置系统包括：

网络设备的输入端连接有代理机，用于转发来自服务器的命令至网络设备、接收、处理网络设备中命令执行后的输出信息，并将处理结果返回给服务器；

服务器内加载有功能插件和数据文件，用于接受用户或安全设备输入的命令和转换命令，并发送至代理机、接收回复输出到终端；

该功能插件包括：

A. 接受输入命令、判断命令格式正误、封装并生成命令事件的命令事件采集插件

-
- B. 接收回信息、生成回事件的回事件采集插件；
 - C. 定义命令、命令事件和回事件格式的事件格式扩展插件；
 - D. 判断命令是否能被转换、触发响应插件转换命令、由回事件到达或计时器超时结束命令转换执行状态变迁的场景分析插件；
 - E. 转换输入命令为能在目标设备执行的命令、并发送至代理机的事件响应插件；
- 该数据文件包括：
- a. 存储设备 ID、设备型号、代理机 IP、代理机端口的设备信息文件；
 - b. 存储设备型号、各型号对应的转换规则文件名的命令转换信息文件；
 - c. 存储统一命令、对应具体型号的命令信息的命令转换规则文件。

所述的网络设备，包括交换机、路由器。

所述的代理机，包括接收命令模块和发送回复模块，接收命令模块用于接收来自服务器的命令，转发命令给网络设备；发送回复模块用于接收并处理网络设备中命令执行后的输出信息，将处理后的信息返回给服务器。

为实现上述目的，本发明的统一配置方法，包括如下步骤：

- (1) 设计一套可用于配置不同厂家、不同型号网络设备的统一命令集，将设备信息文件、命令转换信息文件、命令转换规则文件放置于服务器中；
- (2) 在服务器中加载命令事件采集插件、命令事件格式扩展插件、场景分析插件、事件响应插件、回事件采集插件；
- (3) 用户从终端输入需要配置的目标网络设备号和统一命令集中的一条命令，命令事件采集插件获得该命令后对其格式进行判断，若格式正确，则根据命令事件格式扩展插件中定义的事件格式生成命令事件，若格式错误，则结束该条命令的执行；
- (4) 命令事件生成后，场景分析插件根据命令转换信息文件和目标网络设备对应的命令转换规则文件，对命令状态转移条件进行匹配，判断终端输入的命令是否符合转换规则，若不符合转换规则，变迁命令状态，结束该条命令的执行，若符合转换规则，亦变迁命令状态，触发事件响应插件转换并发送命令，同时开启计时器为接收回消息计时；
- (5) 事件响应插件由场景分析插件触发后，根据目标网络设备对应的命令转换规则，先将终端输入的命令转换为能在目标网络设备上执行的若干条命令，再通过查询设备信息文件获得目标网络设备相连的代理机 IP，最后将目标网络设备号、命令 ID 和转换后的命令信息一起发送到该代理机；
- (6) 代理机接收到来自服务器的信息后，根据目标网络设备号，查找到该目标网

络设备的 IP，然后把命令转发给目标网络设备执行，同时将命令 ID 存储于本地；

(7) 目标网络设备执行来自代理机转发的命令后，将终端输出信息回复给代理机进行处理，处理后的回复信息和保存的命令 ID 被代理机一并发回给服务器；

(8) 服务器中的回复事件采集插件将接受到的回复信息生成回复事件后，场景分析插件通过匹配状态转移条件，分析回复中所带的命令 ID 与发送命令的 ID 是否相同，若相同，变迁命令状态，打印回复信息到终端，并结束该条命令的执行，若不相同或始终未接受到回复信息，则下一条命令输入时，计时器超时，匹配该条命令的状态转移条件，变迁命令状态，结束该条命令的执行。

本发明具有如下优点：

1) 网络设备配置工作量小。本发明由于自行设计了一套统一命令集，并且在服务器上加载有功能插件和设备信息文件、命令转换信息文件和命令转换规则文件，使得该套命令集里的任何一条命令都可以根据待配置网络设备的型号对应的命令转换规则，被转换为能够实际执行的若干条特定命令，即可以使用这套命令集里的命令对所有已知型号的网络设备进行配置，而无需输入设备生产厂家提供的特定命令进行配置。这在一定程度上减轻了网络管理人员的负担，网络管理人员只需要懂得统一命令集里的命令就可以对网络上不同设备进行配置，免去了其记忆和查询不同厂家大量命令的烦恼。

2) 方便大型网络的管理。本发明由于在服务器和网络设备之间添加了代理机，而且在服务器中加载的设备信息文件里存储着网络设备所连的代理机 IP 和端口信息，使得服务器能够通过代理机管理网络设备，而一台代理机可以同时连接几台网络设备，这样当连入被管理网络的设备数量较多时，代理机可以在很大程度上减少服务器对网络设备的管理任务，减轻服务器的工作负荷。

3) 易于在网络中添加新的设备。本发明由于在服务器上加载有命令转换信息文件和命令转换规则文件，使得添加新的设备到被管理网络时，只需知道其型号，就可以通过命令转换信息文件查询到对应的转换规则文件，获得命令转换规则，从而能够使用统一命令集中的命令对其进行配置。若新添加设备的型号未被记载，则只需为该新型号编写对应的转换规则文件，然后将型号名和转换规则文件名写入命令转换信息文件即可，这样可以很容易地增加任何型号的网络设备，便于扩展网络的规模。

4) 功能插件的可扩展性强。本发明由于使用的各功能插件是通用的，只要在保持它们的接口不变的前提下改变内部实现，就可以用于实现其它的功能模块。例如用于分析系统日志中记录的事件时，可利用事件格式扩展插件定义日志事件的格式、事件采集插件获得日志事件、场景分析插件变迁日志事件的状态、和事件响应插件响应日志事件

中出现的属于网络安全范畴的事件。

5) 增强了网络的安全性能。本发明由于在服务器上加载的命令事件采集插件只负责从终端获取命令，而不管命令的输入者是什么，它可以是人当然也可以是安全设备，如防火墙、入侵检测系统、审计系统，只要它们可以输出统一命令集中的命令，就可以被命令事件采集插件获得，并被其它功能插件进行转换，达到配置目标网络设备的目的。安全设备作为命令输入者的情况经常出现在其对网络中的安全事件做出响应的场合，当网络上有某个安全事件发生并且被安全设备检测到时，可能需要对该安全事件相关联的某台网络设备的配置进行一定的改动，以响应该安全事件和保障网络的安全，这时就要求安全设备能够对网络设备输入配置命令，但是安全设备并不知道其所连网络设备的厂家、型号，也就无法获知网络设备上能够执行的特定命令，无法配置网络设备，这时候如果能够将其作为本发明的命令事件采集插件的命令输入者，就可以使用本发明中与具体设备无关的统一命令集对网络设备进行配置，因此，使用本发明配置网络设备可以克服以往安全设备对检测到的安全事件不能做出及时响应的弊端，实现网络的高安全性。

附图说明

图 1 为本发明网络设备统一配置系统的拓扑示意图；

图 2 为本发明系统中场景分析插件的命令转换状态变迁图；

图 3 为本发明网络设备统一配置方法流程图。

具体实施方式

参照图 1，本发明的网络设备统一配置系统，主要由服务器、代理机和网络设备三部分构成。其中：

服务器，设置在网络控制中心，接收并转换管理员或安全设备输入的统一命令集中的命令、将命令发送至代理机、接收并输出来自代理机的回复信息，该服务器中加载有功能插件和数据文件。功能插件包括有：(1) 接受输入命令、判断命令格式正误、封装并生成命令事件的命令事件采集插件 a；(2) 接收回复信息、生成回事件的回事件采集插件 b；(3) 定义命令、命令事件和回事件格式的事件格式扩展插件 c；(4) 判断命令是否能被转换、触发响应插件转换命令、由回事件到达或计时器超时结束命令转换执行状态变迁的场景分析插件 d；(5) 转换输入命令为能在目标设备执行的命令、并发送至代理机的事件响应插件 e，但不限于这些插件。数据文件包括有：1) 存储设备 ID、设备型号、代理机 IP、代理机端口的设备信息文件 f；2) 存储设备型号、各型号对应的转换规则文件名的命令转换信息文件 g；3) 存储统一命令、对应具体型号的命令信息的命令转换规则文件 h，但不限于这些文件。

代理机，可以选用一般的 PC 机，根据网络规模的大小和网络设备的数量多少，设定其数量，只要满足需求即可，具体数量不限，其主要用于转发来自服务器的命令至网络设备、接收、处理网络设备中命令执行后的输出信息、并将处理结果信息返回给服务器。

网络设备，包括路由器、交换机，其厂家、型号不限，主要用于执行代理机发送过来的命令，并将终端输出的信息发送给代理机。

在系统中各组成部分的连接关系为：服务器与若干台代理机相连，每台代理机又与若干台网络设备相连。它们之间传输着两种信息，一种是命令信息，即统一命令被服务器的功能插件依据数据文件转换后的命令，它经代理机传送给网络设备；另一种是回复信息，即网络设备执行命令后的输出信息，它经代理机处理后传回给服务器。服务器中的场景分析插件完成的命令转换状态变迁情况可参照图 2，它包含命令状态转移条件和命令状态两部分，其中命令状态转移条件为：

(1) IncorrectCmd 条件：若命令不符合转换规则，则匹配该条件，使命令从状态 s0 变迁到状态 final；

(2) CorrectCmd 条件：若命令符合转换规则，则匹配该条件，使命令从状态 s0 变迁到状态 send；

(3) Reply 条件：若接收到的回复中所带命令 ID 与发送命令的 ID 相同，则匹配该条件，使命令从状态 send 变迁到状态 final；

(4) TimerExpiry 条件：若计时器超时，则匹配该条件，使命令从状态 send 变迁到状态 final。

命令状态为：

1) 初始状态 s0：命令一开始所处的状态；

2) 发送状态 send：用于触发事件响应插件转换并发送命令，同时开启计时器为接收回复消息计时；

3) 终止状态 final：用于结束命令的执行。

参照图 3，本发明的配置方法包括如下步骤：

步骤 1，设计命令集，放置数据文件于服务器中。

设计一套与具体网络设备无关的统一命令集，为每种设备型号编写数据文件，数据文件包含：(1) 存储统一命令、对应具体型号的命令信息的命令转换规则文件；(2) 存储设备型号、各型号对应的转换规则文件名的命令转换信息文件；(3) 存储设备 ID、设备型号、代理机 IP、代理机端口的设备信息文件，然后将这些文件放置于服务器中。

步骤 2，服务器加载功能插件。

功能插件包含命令事件采集插件、命令事件格式扩展插件、场景分析插件、事件响应插件、和回复事件采集插件，将这些插件编译成动态链接库放入服务器中并修改插件对应的各配置文件即可成功加载插件于服务器上。

步骤 3，命令事件采集插件根据输入的统一命令生成命令事件。

用户从终端输入需要配置的目标网络设备号和统一命令集中的一条命令，命令事件采集插件获得该命令后对其格式进行判断，若格式正确，则根据命令事件格式扩展插件中定义的命令格式封装输入的命令，继而生成命令事件，若格式错误，则结束该条命令的执行。

步骤 4，场景分析插件完成命令转换状态变迁。

命令事件生成后，场景分析插件根据命令转换信息文件和目标网络设备对应的命令转换规则文件，对命令状态转移条件进行匹配，判断终端输入的命令是否符合转换规则，若不符合转换规则，则匹配 IncorrectCmd 条件，命令从状态 s0 变迁到状态 final，执行结束，若符合转换规则，则匹配 CorrectCmd 条件，命令从状态 s0 变迁到状态 send，触发事件响应插件的动作并开启计时器为接收回复消息计时。

步骤 5，事件响应插件转换并发送命令至代理机。

事件响应插件由场景分析插件中的状态 send 触发后，根据目标网络设备对应的命令转换规则，先将终端输入的命令转换为能在目标网络设备上执行的若干条命令，再通过查询设备信息文件获得目标网络设备相连的代理机 IP，最后将目标网络设备号、命令 ID 和转换后的命令信息一起发送到该代理机。

步骤 6，代理机转发命令至目标网络设备。

代理机接收到来自服务器的信息后，根据目标网络设备号，查找到该目标网络设备的 IP，然后把命令转发给目标网络设备执行，同时将命令 ID 存储于本地。

步骤 7，目标网络设备执行命令并发送输出信息给代理机。

目标网络设备执行来自代理机转发的命令后，将终端输出信息回复给代理机，代理机对这些信息进行集中处理，判断命令是否被成功执行，若执行成功，则将回复信息和保存的命令 ID 一起发回给服务器，若执行失败，则返回执行失败的标志性信息和命令 ID 给服务器。

步骤 8，回复事件采集插件接收并输出回复信息至服务器终端。

服务器中的回复事件采集插件总是在检测是否有回复信息的到来，一旦接收到回复信息，立即生成回复事件，继而刺激场景分析进行命令状态转移条件的匹配，分析回复

中所带的命令 ID 与发送命令的 ID 是否相同，若相同，则匹配 Reply 条件，命令从状态 send 变迁到状态 final，系统打印回复信息到终端，并结束该条命令的执行，若不相同或始终未接受到回复信息，则下一条命令输入时，计时器超时，匹配 TimerExpiry 条件，命令亦从状态 send 变迁到状态 final，结束它的执行过程。

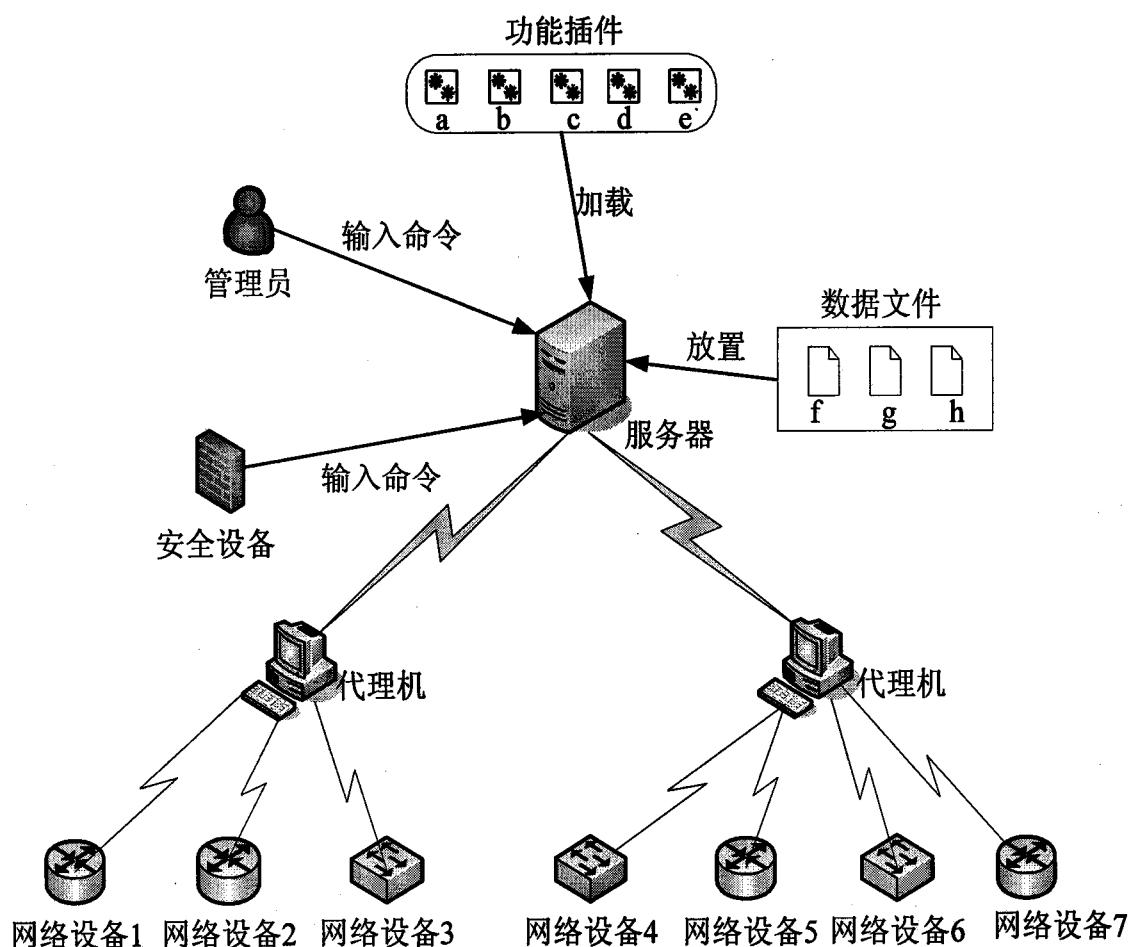


图 1

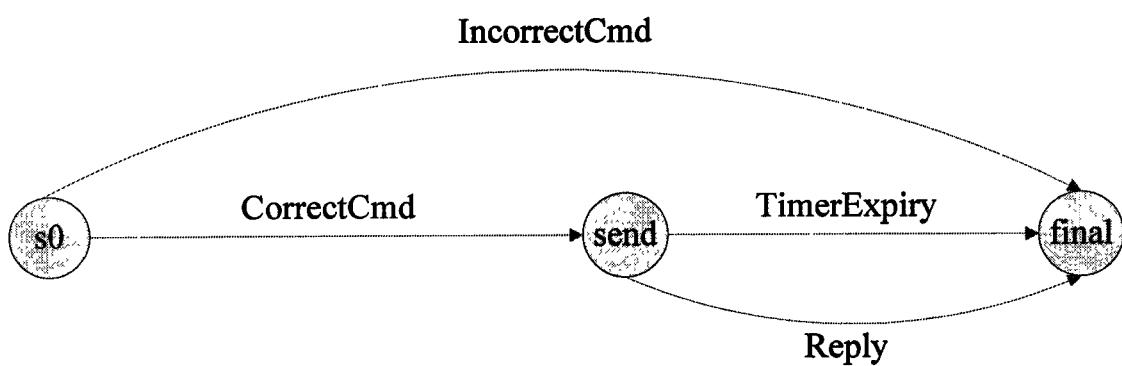


图 2

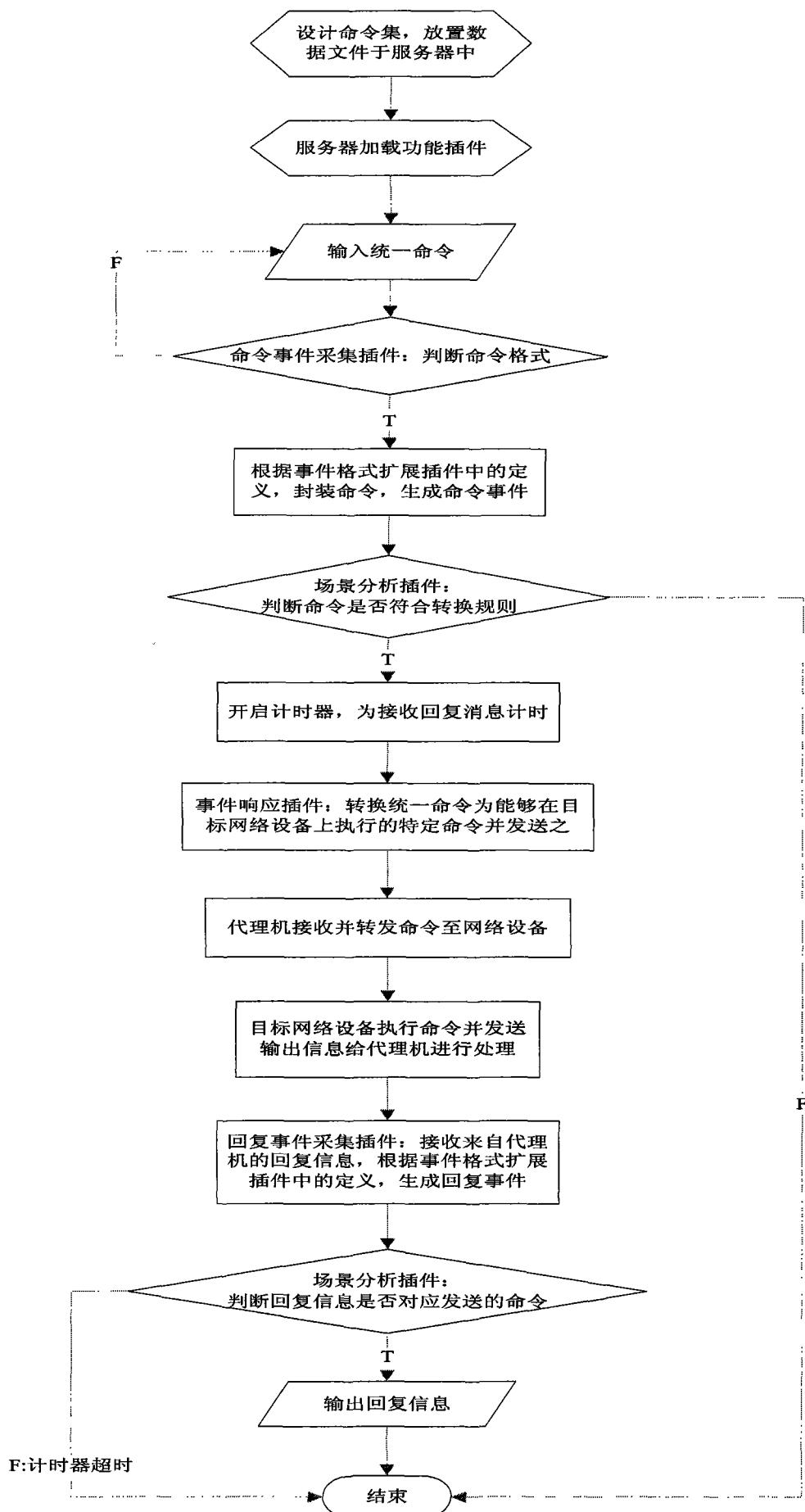


图 3