

(12) 发明专利

(10) 授权公告号 CN 101009560 B

(45) 授权公告日 2013. 02. 13

(21) 申请号 200710007272. 4

US 2003/0055962 A1, 2003. 03. 20, 说明书第

(22) 申请日 2007. 01. 25

[0039]-[0042], [0071], [0074]-[0095], [0110],
[0113]-[0116], [0122], [0125], [0127], [0134],
[0151] 段及附图 3 和 9.

(30) 优先权数据

2006-015749 2006. 01. 25 JP

WO 2006/003914 A1, 2006. 01. 12, 全文.

(73) 专利权人 日本电气株式会社

CN 1665238 A, 2005. 09. 07, 全文.

地址 日本东京

审查员 杨颖

(72) 发明人 北村浩

(74) 专利代理机构 中原信达知识产权代理有限公司
责任公司 11219

代理人 钟强 谷惠敏

(51) Int. Cl.

H04L 9/32(2006. 01)

H04L 29/06(2006. 01)

(56) 对比文件

CN 2528167 Y, 2002. 12. 25, 全文.

US 2003/0055962 A1, 2003. 03. 20, 同上.

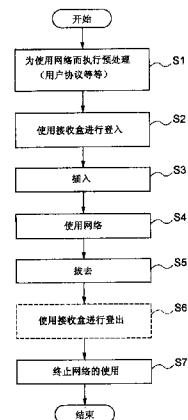
权利要求书 6 页 说明书 18 页 附图 20 页

(54) 发明名称

通信系统、用于资格审查 / 设置的网络、通信设备和网络连接方法

(57) 摘要

B 本发明提供一种网络连接方法，该方法能够预防受病毒感染的通信设备或想要未授权接入的通信设备与网络的连接，并能够以简单的方式实现与网络的连接。请求者通信设备的用户通过将通信设备的电缆插入网络设备的端口，而连接到主网络。当请求者通信设备通过网络设备内的登入网络被一对一的连接到接收盒时，就使用接收盒执行登入。当接收盒通过登入处理确定请求者通信设备满足了连接资格时，接收盒将该请求者通信设备将要连接的网络从登入网络转换到主网络。然后，请求者通信设备执行对主网络实际使用的切换。



1. 一种在通信系统中使用的网络连接设备,所述通信系统包括提供各种服务的 VLAN 或 VPN 的主网络、与主网络独立提供的 VLAN 或 VPN 的用于资格审查 / 设置的网络、接收控制部分,该接收控制部分被连接到主网络和用于资格审查 / 设置的网络,所述网络连接设备包括:

当通信设备请求与主网络的连接时,经用于资格审查 / 设置的网络来在一一对的基础上执行通信设备与接收控制部分的隔离连接的装置;

使接收控制部分在一一对的基础上获取隔离连接的通信设备的状态信息,用于执行资格审查,以便确定该状态是否满足了预置的资格条件的装置;

当确定满足了资格条件时,通过转换通信设备所连接的端口,将通信设备所连接的网络连接到主网络的装置,

其中,在低于 OSI 模型的网络层的层中链路发生状态变化时,在 VLAN 或 VPN 中执行资格审查 / 设置。

2. 一种在通信系统中使用的网络连接设备,所述通信系统包括提供各种服务的 VLAN 或 VPN 的多个主网络、与多个主网络独立提供的 VLAN 或 VPN 的用于资格审查 / 设置的网络、接收控制部分,该接收控制部分被连接到多个主网络和用于资格审查 / 设置的网络,所述网络连接设备包括:

当通信设备请求与多个主网络的连接时,经用于资格审查 / 设置的网络来在一一对的基础上执行通信设备与接收控制部分的隔离连接的装置;

使接收控制部分在一一对的基础上获取隔离连接的通信设备的状态信息,用于执行资格审查,以便确定该状态是否满足了预置的资格条件的装置;

当确定满足了资格条件时,通过转换通信设备所连接的端口,根据资格条件,将通信设备所连接的网络连接到一个主网络的装置,

其中,在低于 OSI 模型的网络层的层中链路发生状态变化时,在 VLAN 或 VPN 中执行资格审查 / 设置。

3. 根据权利要求 1 的网络连接设备,其中接收控制部分预先向隔离连接的通信设备提供密钥信息,通过使用电子签名功能来验证从主网络获取的信息是否为正确信息。

4. 根据权利要求 1 的网络连接设备,其中通信设备预先向隔离连接的接收控制部分提供密钥信息,通过使用电子签名功能来验证从设备自身发送到主网络的信息是否为正确信息。

5. 根据权利要求 1 的网络连接设备,其中当检测到与用于资格审查 / 设置连接的网络的连接时,该检测是通过设备自身与用于资格审查 / 设置连接的网络的连接来触发,该通信设备确认在用于资格审查 / 设置的网络中的连接目标,并执行对确认连接目标的接收控制部分的所需信息的自动发现配置。

6. 根据权利要求 1 的网络连接设备,其中当通信设备从主网络断开时,
接收控制部分将通信设备返回到隔离连接设置。

7. 根据权利要求 1 的网络连接设备,当通信设备连接到用于资格审查 / 设置的网络,而没有加载用于资格审查的工具时,接收控制部分引导从通信设备到用于资格审查的工具的下载网站的 Web 接入,

通信设备从下载站点中下载和安装用于资格审查的工具。

8. 根据权利要求 7 的网络连接设备, 其中在连接到用于资格审查 / 设置的网络时, 如果在下载站点上存在用于资格审查的新工具, 该通信设备就下载和执行用于资格审查的新工具。

9. 根据权利要求 7 的网络连接设备, 其中当通信设备连接到用于资格审查 / 设置的网络时, 用于资格审查的工具确认在下载网站上更新信息的存在, 如果存在这种信息, 就下载更新信息。

10. 根据权利要求 1 的网络连接设备, 其中当从外部预先设置关于主网络匹配条件的事件时, 接收控制部分将所有的通信设备连接到用于资格审查 / 设置的网络。

11. 根据权利要求 7 的网络连接设备, 其中该通信设备是可以加载用于资格审查的工具的通信设备。

12. 根据权利要求 1 的网络连接设备, 其中当这种设备不能够加载用于资格审查的工具时, 接收控制部分包括确认通信设备类型的装置, 和根据确认结果在通信设备上设置信息的装置。

13. 根据权利要求 12 的网络连接设备, 其中在通信设备上设置的信息是能够使通信设备在主网络上操作的信息。

14. 根据权利要求 1 的网络连接设备, 其中主网络和用于资格审查 / 设置的网络分别至少是 VLAN(虚拟 LAN[局域网]) 或 VPN(虚拟专用网) 。

15. 一种 VLAN 或 VPN 的用于资格审查 / 设置的网络, 该用于资格审查 / 设置的网络与提供各种服务的 VLAN 或 VPN 的主网络独立地提供, 并和主网络一起被连接到接收控制部分, 该用于资格审查 / 设置的网络包括 :

当通信设备请求连接到主网络时, 在一对一的基础上执行通信设备与接收控制部分的隔离连接的装置 ;

当确定通信设备的状态信息满足了预置的资格条件时, 通过转换通信设备所连接的端口, 将与接收控制部分隔离连接的通信设备连接到主网络的设备,

其中, 在低于 OSI 模型的网络层的层中链路发生状态变化时, 在 VLAN 或 VPN 中执行资格审查 / 设置。

16. 一种 VLAN 或 VPN 的用于资格审查 / 设置的网络, 该用于资格审查 / 设置的网络与提供各种服务的 VLAN 或 VPN 的多个主网络独立地提供, 并和主网络一起被连接到接收控制部分, 该用于资格审查 / 设置的网络包括 :

当通信设备请求连接到主网络时, 在一对一的基础上执行通信设备与接收控制部分的隔离连接的装置 ;

当确定通信设备的状态信息满足了预置的资格条件时, 通过转换通信设备所连接的端口, 根据资格条件选择地将与接收控制部分隔离连接的通信设备, 连接到多个主网络中的一个主网络的装置,

其中, 在低于 OSI 模型的网络层的层中链路发生状态变化时, 在 VLAN 或 VPN 中执行资格审查 / 设置。

17. 根据权利要求 15 的用于资格审查 / 设置的网络, 其中接收控制部分预先向隔离连接的通信设备提供密钥信息, 通过使用电子签名功能来验证从主网络获取的信息是否为正确信息。

18. 根据权利要求 15 的用于资格审查 / 设置的网络, 其中通信设备预先向隔离连接的接收控制部分提供密钥信息, 通过使用电子签名功能来验证从通信设备发送到主网络的信息是否为正确信息。

19. 根据权利要求 15 的用于资格审查 / 设置的网络, 其中当通信设备从主网络断开时, 接收控制部分将通信设备返回到隔离连接设置。

20. 根据权利要求 15 的用于资格审查 / 设置的网络, 其中当通信设备被隔离连接到用于资格审查 / 设置的网络, 而没有加载用于资格审查的工具时, 接收控制部分引导从通信设备到用于资格审查的工具的下载站点的 Web 接入,

通信设备从下载站点中下载和安装用于资格审查的工具。

21. 根据权利要求 20 的用于资格审查 / 设置的网络, 其中当通信设备被隔离连接到接收控制部分时, 如果在下载站点上存在用于资格审查的新工具, 该通信设备就下载和执行用于资格审查的新工具。

22. 根据权利要求 20 的用于资格审查 / 设置的网络, 其中当连接到网络自身时, 用于资格审查的工具就使通信设备确认在下载站点上更新信息的存在, 如果存在这种信息, 就使通信设备下载更新信息。

23. 根据权利要求 15 的用于资格审查 / 设置的网络, 其中当从外部预先设置关于主网络匹配条件的事件时, 接收控制部分就使所有的通信设备连接到该网络自身。

24. 根据权利要求 20 的用于资格审查 / 设置的网络, 其中该通信设备是可以加载工具的通信设备。

25. 根据权利要求 15 的用于资格审查 / 设置的网络, 其中当这种设备不能加载用于资格审查的工具时, 接收控制部分确认通信设备类型, 并根据确认结果在通信设备上设置信息。

26. 根据权利要求 25 的用于资格审查 / 设置的网络, 其中在通信设备上设置的信息是能够使通信设备在主网络上操作的信息。

27. 根据权利要求 15 的用于资格审查 / 设置的网络, 其中主网络至少是 VLAN(虚拟 LAN[局域网]) 或 VPN(虚拟专用网)。

28. 根据权利要求 27 的用于资格审查 / 设置的网络, 其中该网络自身至少是 VLAN(虚拟 LAN[局域网]) 或 VPN(虚拟专用网)。

29. 一种通信设备, 该通信设备请求与通信系统中主网络的连接, 该通信系统包括提供各种服务的 VLAN 或 VPN 的主网络、与主网络独立提供的 VLAN 或 VPN 的用于资格审查 / 设置的网络、和接收控制部分, 该接收控制部分被连接到主网络和用于资格审查 / 设置的网络, 其中

该设备自身经用于资格审查 / 设置的网络在一一对的基础上被隔离连接到接收控制部分, 以便执行该设备自身是否满足了预置的资格条件的资格审查, 并当确定满足了资格条件时, 通过转换通信设备所连接的端口, 将该设备自身所连接的网络连接到主网络,

其中, 在低于 OSI 模型的网络层的层中链路发生状态变化时, 在 VLAN 或 VPN 中执行资格审查 / 设置。

30. 一种通信设备, 该通信设备请求与通信系统中多个主网络的连接, 该通信系统包括提供各种服务的 VLAN 或 VPN 的主网络、与主网络独立提供的 VLAN 或 VPN 的用于资格审查

/ 设置的网络、和接收控制部分,该接收控制部分被连接到主网络和用于资格审查 / 设置的网络,其中

该设备自身经用于资格审查 / 设置的网络在一对一的基础上被隔离连接到接收控制部分,以便执行该设备自身是否满足了预置的资格条件的资格审查,当确定满足了资格条件时,通过转换通信设备所连接的端口,根据资格条件,将该设备自身所连接的网络选择地连接到多个主网络中的一个主网络,

其中,在低于 OSI 模型的网络层的层中链路发生状态变化时,在 VLAN 或 VPN 中执行资格审查 / 设置。

31. 根据权利要求 29 的通信设备,其中在经用于资格审查 / 设置的网络与接收控制部分隔离连接的状态中,从接收控制部分预先提供密钥信息,通过使用电子签名功能来验证从主网络获取的信息是否为正确信息。

32. 根据权利要求 29 的通信设备,其中该设备自身预先向接收控制部分提供密钥信息,通过使用电子签名功能来验证从该设备自身发送到主网络的信息是否为正确信息。

33. 根据权利要求 29 的通信设备,其中当检测到与用于资格审查 / 设置连接的网络的连接时,该检测是由设备自身与用于资格审查 / 设置连接的网络的连接来触发,该设备自身确认在用于资格审查 / 设置的网络中的连接目标,并执行对确认连接目标的接收控制部分的所需信息的自动发现配置。

34. 根据权利要求 29 的通信设备,其中,当设备自身连接到用于资格审查 / 设置的网络,而没有加载用于资格审查的工具时,接收控制部分就引导从设备自身到用于资格审查的工具的下载站点的 Web 接入,该设备自身就从下载站点中下载和安装用于资格审查的工具。

35. 根据权利要求 34 的通信设备,其中,当连接到用于资格审查 / 设置的网络时,如果在下载站点上存在用于资格审查的工具,该设备自身就下载和执行用于资格审查的新工具。

36. 根据权利要求 34 的通信设备,其中当设备自身连接到用于资格审查 / 设置的网络时,用于资格审查的工具就确认在下载站点上更新信息的存在,如果存在这种信息,就下载更新信息。

37. 根据权利要求 34 的通信设备,其中该设备自身是可以加载工具的设备。

38. 根据权利要求 29 的通信设备,其中如果设备自身不能够加载用于资格审查的工具,接收控制部分就确认该设备自身的类型,并根据确认结果在设备自身上设置信息。

39. 根据权利要求 38 的通信设备,其中在设备自身上设置的信息是能够使该设备自身在主网络上操作的信息。

40. 根据权利要求 29 的通信设备,其中该主网络和用于资格审查 / 设置的网络至少分别是 VLAN(虚拟 LAN[局域网]) 或 VPN(虚拟专用网)。

41. 一种在通信系统中使用的网络连接方法,该通信系统包括提供各种服务的 VLAN 或 VPN 的主网络、与主网络独立提供的 VLAN 或 VPN 的用于资格审查 / 设置的网络、接收控制部分,该接收控制部分被连接到主网络和用于资格审查 / 设置的网络,该方法包括步骤:

当通信设备请求与主网络的连接时,经用于资格审查 / 设置的网络来在一对一的基础上执行通信设备与接收控制部分的隔离连接;

使接收控制部分在一对一的基础上获取隔离连接的通信设备的状态信息,用于执行资格审查,以便确定该状态是否满足了预置的资格条件;

当确定满足了资格条件时,通过转换通信设备所连接的端口,将通信设备所连接的网络连接到主网络,

其中,在低于 OSI 模型的网络层的层中链路发生状态变化时,在 VLAN 或 VPN 中执行资格审查 / 设置。

42. 一种在通信系统中使用的网络连接方法,该通信系统包括提供各种服务的 VLAN 或 VPN 的多个主网络、与多个主网络独立提供的 VLAN 或 VPN 的用于资格审查 / 设置的网络、接收控制部分,该接收控制部分被连接到多个主网络和用于资格审查 / 设置的网络,该方法包括步骤:

当通信设备请求与多个主网络的连接时,经用于资格审查 / 设置的网络来在一对一的基础上执行通信设备与接收控制部分的隔离连接;

使接收控制部分在一对一的基础上获取隔离连接的通信设备的状态信息,用于执行资格审查,以便确定该状态是否满足了预置的资格条件;

当确定满足了资格条件时,通过转换通信设备所连接的端口,根据资格条件,将通信设备所连接的网络连接到一个主网络,

其中,在低于 OSI 模型的网络层的层中链路发生状态变化时,在 VLAN 或 VPN 中执行资格审查 / 设置。

43. 根据权利要求 41 的网络连接方法,其中接收控制部分预先向隔离连接的通信设备提供密钥信息,通过使用电子签名功能来验证从主网络获取的信息是否为正确信息。

44. 根据权利要求 41 的网络连接方法,其中该通信设备预先向隔离连接的接收控制部分提供密钥信息,通过使用电子签名功能来验证从该设备自身发送到主网络的信息是否为正确信息。

45. 根据权利要求 41 的网络连接方法,其中当检测到与用于资格审查 / 设置连接的网络的连接时,该检测是由设备自身与用于资格审查 / 设置连接的网络的连接来触发,该通信设备确认在用于资格审查 / 设置的网络中的连接目标,并执行对确认连接目标的接收控制部分的获取信息的自动发现配置。

46. 根据权利要求 41 的网络连接方法,其中当通信设备从主网络断开时,接收控制部分将通信设备返回到隔离连接设置。

47. 根据权利要求 41 的网络连接方法,其中当通信设备连接到用于资格审查 / 设置的网络,而没有加载用于资格审查的工具时,接收控制部分就引导从通信设备到用于资格审查工具的下载站点的 Web 接入,通信设备从下载站点中下载和安装用于资格审查的工具。

48. 根据权利要求 47 网络连接方法,其中当连接到用于资格审查 / 设置的网络时,如果在下载站点上存在用于资格审查的新工具,该通信设备就下载和执行用于资格审查的新工具。

49. 根据权利要求 47 的网络连接方法,其中当通信设备连接到用于资格审查 / 设置的网络时,用于资格审查的工具就确认在下载站点上更新信息的存在,如果存在这种信息,就下载更新信息。

50. 根据权利要求 41 的网络连接方法,其中当从外部预先设置关于主网络匹配条件的

事件时,接收控制部分就将所有的通信设备连接到用于资格审查 / 设置的网络。

51. 根据权利要求 41 的网络连接方法,其中通信设备是可以加载工具的通信设备。
52. 根据权利要求 41 的网络连接方法,其中当这种设备不能够加载用于资格审查的工具时,接收控制部分就确认通信设备的类型,并根据确认结果在通信设备上设置信息。
53. 根据权利要求 52 的网络连接方法,其中在通信设备上设置的信息是能够使通信设备在主网络上操作的信息。
54. 根据权利要求 41 的网络连接方法,其中该主网络和用于资格审查 / 设置的网络至少分别是 VLAN(虚拟 LAN[局域网]) 或 VPN(虚拟专用网)。

通信系统、用于资格审查 / 设置的网络、通信设备和网络连接方法

技术领域

[0001] 本发明涉及通信系统、用于资格审查 / 设置的网络、通信设备和网络连接方法、以及为此使用的资格审查工具程序。更具体而言，本发明涉及一种防止被病毒感染的通信设备、或者被用于尝试未授权接入的通信设备等等与网络连接的方法。

背景技术

[0002] 个人计算机（下文称为 PC）和因特网近来的普遍应用已经快速提高了网络作为社会经济和社会生产基础设施的重要性。遗憾地是，网络作为社会经济和社会生产技术设施的重要性不断增长导致网络受攻击的情况增加，比如以病毒的蓄意散布和未授权接入网络等形式。

[0003] 尽管，通常病毒是通过存储介质或电子邮件、或经由恶意网页或者已被未授权接入破坏的网页而被传播到 PC 等装置，然而近来已经迅速传播了仅仅通过连接因特网就会扩散的网络病毒。

[0004] 因此，已经报告了在以下情形时引起的损坏：例如网络 PC 在网络外部携带、并在连接到因特网时感染了病毒，一旦该网络 PC 返回并重新连接到网络而忘记了它已受感染，则该网络 PC 将病毒传播到整个网络。

[0005] 在这种环境下，当建立网络时，为了保护网络不仅免受外部攻击，而且还免受网络内部的感染，已经提出了一种隔离（quarantine）网络或系统，其涉及通过如下方式对从外部带入网络的 PC 等设备执行检查（下文称为隔离处理）：将 PC 等设备连接到隔离网络，以确定可能的病毒感染和是否对诸如 OS（操作系统）等软件添加了最新的补丁程序，当确定 PC 为安全时，就解除对连接网络的限制（例如，参考专利文献 1（日本专利公开号 2005-216253））。

发明内容

[0006] 然而，在上述的隔离网络或系统中，由于从外部带入网络的 PC 等设备被原样连接到隔离网络，因此万一将受病毒感染的设备连接到隔离网络时，那么同时连接到该隔离网络的设备就存在可能受到病毒感染的危险。

[0007] 另外，还存在这样的问题：当将诸如 PC 等设备连接到网络时，需要输入用于身份验证的 ID（识别信息）或密码等，这会给这种网络连接带来麻烦。由于这种连接需要输入用于连接网络的设置（诸如上述 ID 或密码的设置，或网络设备的设置），因此 PC 初学者会发现连接网络特别的困难。

[0008] 在考虑上面因素的情况下，本发明的目的是为了解决上述的问题，提供了一种通信系统、用于资格审查 / 设置的网络、通信设备和为此使用的网络连接方法，该网络连接方法能够以简单方式实现与主网络的连接，同时防止病毒传播到其它设备，并增加在隔离期间的业务量。

[0009] 根据本发明的通信系统包括提供各种服务的主网络、与主网络独立提供的用于资格审查 / 设置的网络、接收控制部分，该接收控制部分被连接到主网络和用于资格审查 / 设置的网络，该通信系统包括：

[0010] 在通信设备请求与主网络的连接时，经用于资格审查 / 设置的网络执行通信设备与接收控制部分的隔离连接的装置；

[0011] 在接收控制部分提供的执行资格审查的装置，该接收装置获取隔离连接的通信设备的状态信息，用于确定该状态是否满足预置的资格条件；

[0012] 在确定满足了资格条件时，将该通信设备所连接的网络连接到主网络的装置。

[0013] 根据本发明的另一个通信系统，它包括提供各种服务的多个主网络、与多个主网络独立提供的用于资格审查 / 设置的网络、接收控制部分，该接收控制部分被连接到主网络和用于资格审查 / 设置的网络，该通信系统进一步包括：

[0014] 在通信设备请求与主网络的连接时，经用于资格审查 / 设置的网络执行通信设备与接收控制部分的隔离连接的装置；

[0015] 在接收控制部分中提供的执行资格审查的装置，该接收控制部分获取隔离连接的通信设备的状态信息，用于确定该状态是否满足了预置的资格条件；

[0016] 在确定满足了资格条件时，根据资格条件选择地将通信设备所连接的网络连接到多个主网络中任何一个主网络的装置。

[0017] 根据本发明的一种用于资格审查 / 设置的网络，该网络是与提供各种服务的主网络独立地提供，并和主网络一起被连接到接收控制部分，该用于资格审查 / 设置的网络包括：

[0018] 当通信设备请求与主网络的连接时，执行通信设备与接收控制部分的隔离连接的装置；

[0019] 当确定通信设备的状态信息满足了预置的资格条件时，将与接收控制部分隔离连接的通信设备连接到主网络的设备。

[0020] 根据本发明的另一种用于资格审查 / 设置的网络，该网络与提供各种服务的多个主网络独立地提供，并和主网络一起被连接到接收控制部分，该用于资格审查 / 设置的网络包括：

[0021] 当通信设备请求与主网络的连接时，执行通信设备与接收控制部分的隔离连接的装置；

[0022] 当确定通信设备的状态信息满足了预置的资格条件时，根据资格条件，选择地将与接收控制部分隔离连接的通信设备连接到多个主网络中的一个主网络的装置。

[0023] 根据本发明的一种通信设备，该通信设备请求与通信系统中的主网络的连接，该通信系统包括提供各种服务的主网络、与主网络独立提供的用于资格审查 / 设置的网络、和接收控制部分，该接收控制部分被连接到主网络和用于资格审查 / 设置的网络，其中

[0024] 该通信设备经用于资格审查 / 设置的网络被隔离连接到接收控制部分，以便执行该设备自身是否满足预置的资格条件的资格审查，并当确定满足了资格条件时，将该设备自身所连接的网络连接到主网络。

[0025] 根据本发明的另一个通信设备，该通信设备请求与通信系统中的多个主网络的连接，该通信系统包括提供各种服务的主网络、与主网络独立提供的用于资格审查 / 设置的

网络、和接收控制部分,该接收控制部分被连接到主网络和用于资格审查 / 设置的网络,其中

[0026] 该通信设备经用于资格审查 / 设置的网络被隔离连接到接收控制部分,以便执行该设备自身是否满足预置的资格条件的资格审查,当确定满足了资格条件时,根据资格条件,将该设备自身所连接的网络选择地连接到多个主网络中的一个主网络。

[0027] 根据本发明的一种在通信系统中使用的网络连接方法,该通信系统包括提供各种服务的主网络、与主网络独立提供的用于资格审查 / 设置的网络、接收控制部分,该接收控制部分被连接到主网络和用于资格审查 / 设置的网络,该方法包括步骤:

[0028] 当通信设备请求与主网络的连接时,经用于资格审查 / 设置的网络

[0029] 执行通信设备与接收控制部分的隔离连接;

[0030] 使接收控制部分获取隔离连接的通信设备的状态信息,用于执行资格审查,以便确定该状态是否满足了预置的资格条件;

[0031] 当确定满足了资格条件时,将通信设备所连接的网络连接到主网络。

[0032] 根据本发明另一种在通信系统中使用的通信连接方法,该通信系统包括提供各种服务的多个主网络、与主网络独立提供的用于资格审查 / 设置的网络、接收控制部分,该接收控制部分被连接到主网络和用于资格审查 / 设置的网络,该方法包括步骤:

[0033] 当通信设备请求与主网络的连接时,经用于资格审查 / 设置的网络执行通信设备与接收控制部分的隔离连接;

[0034] 使接收控制部分获取隔离连接的通信设备的状态信息,用于执行资格审查,以便确定该状态是否满足了预置的资格条件;

[0035] 当确定满足了资格条件时,根据资格条件,将通信设备所连接的网络连接到一个主网络。

[0036] 换句话说,在逻辑组合通信设备的通信系统中,这些通信设备被连接到提供各种服务的网络(下文称为主网络),根据本发明的网络连接方法提供了与主网络独立提供的网络(下文称为用于资格审查 / 设置的网络),该网络验证请求连接主网络的通信设备是否满足了预置的连接条件(资格条件)。该网络连接方法使用接收控制部分来执行请求者通信设备的连接请求的验证,该接收控制部分被连接到主网络和用于资格审查 / 设置的网络,该请求者通信设备经用于资格审查 / 设置的网络通过隔离连接通信设备,来请求与主网络的连接。

[0037] 因此,根据本发明的网络连接方法,通过使接收控制部分检验请求者通信设备的连接请求,该请求者通信设备经用于资格审查 / 设置的网络进行隔离连接,即使将受病毒感染的通信设备或使用尝试未授权接入的通信设备连接到用于资格审查 / 设置的网络时,也可以采用简单的方式执行与主网络的连接,同时防止从这种设备到其它隔离设备的病毒传播,并防止在隔离期间业务量的增加。

[0038] 另外,根据本发明的网络连接方法,在将它自身的电缆连接(下文称为即插即用)到网络设备(诸如集线器),该网络设备能够实现与用于资格审查 / 设置的网络的连接,当检测到与登出(check-out)网络的连接时,通过使请求者通信设备确认连接目标,并向确认连接目标的接收控制部分发送SLP(服务位置协议)查询,就能执行服务发现(能实现所需信息的自动发现的配置),用于交换各种信息,该信息根据使用的通信环境而变化。

[0039] 在这个阶段,根据本发明的网络连接方法,当请求者通信设备满足了预置的资格条件(例如,当设备满足了资格条件,诸如应用了最新的补丁程序和防病毒测量在适当位置的状态)时,由于接收控制部分执行了请求者通信设备的名称和ID(识别信息)的自动配置,并将请求者通信设备所连接的网络连接到主网络,如果满足了资格条件,或者当执行自动配置来满足这种资格条件时,通过仅仅将电缆连接到网络设备,该请求者通信设备的用户现在将能够连接到主网络。

[0040] 更进一步,根据本发明的网络连接方法,在接收控制部分和请求者通信设备被连接到用于资格审查/设置的网络的状态中,接收控制部分作为连接主网络的每个设备的代表,会向通信设备提供密钥信息,通过使用电子签名功能来验证主网络获取的信息是否是来自正确的设备(使用KDC[密钥分配中心]模型),或者向接收控制部分提供密钥信息,通过使用电子签名功能来验证由通信设备发送到主网络的信息是否是真地来自该通信设备。当从主网络检测到这种服务时,通过使用密钥信息就能够验证服务的信息是否为正确信息,该主网络是通过即插即用方式实现连接。

[0041] 在这种情况下,当使用目录服务器(DA:目录代理)时,在目录服务器中记录了连接主网络的设备的信息,可以构造一种机制,用于验证该信息是否是来自正确的目录服务器。这个机制作为一种必要而充分的简单机制,新提供了一种获取目录服务器的公共密钥的服务。仅仅在开始时一次执行目录服务器的公共密钥的获取和验证,通过使用公共密钥就可以执行一般服务信息的获取和验证。

[0042] 而且,根据本发明的网络连接方法,当请求者通信设备的电缆从网络设备断开时,在实现与接收控制部分的隔离连接的状态下,通过接收控制部分就可以执行下一个连接该网络设备的通信设备的资格条件的验证,上述与接收控制部分的隔离连接是通过配置网络设备,使主网络的转换被返回到其初始状态(返回到与用于资格审查/设置的网络的连接)来实现的。

[0043] 根据本发明的网络连接方法,是以下面的顺序来执行使用请求者通信设备的处理。

[0044] (1) 用于使用主网络的预处理(用户协议等)

[0045] (2) 将电缆连接到网络设备(集线器等)

[0046] (3) 用于使用接收控制部分(接收盒)的登入处理

[0047] (4) 主网络的实际使用(插入到主网络)

[0048] (5) 电缆从网络设备上脱离(从主网络拔去)

[0049] (6) 脱离使用接收控制部分的检验

[0050] (7) 终止主网络的使用

[0051] 尽管上面的描述是假定安装(Bootstrap:工具安装程序)了验证软件(资格审查工具程序),以便使请求者通信设备执行(2)至(7)的处理,但是在通信设备发出新的连接请求时,还可以使请求者通信设备连接到验证软件的下载站点,以便下载和安装验证软件。

[0052] 在这种情况下,通信设备必须至少安装有Web浏览器。当通信设备的电缆连接到网络设备,Web浏览器进入任意的网站时,接收控制部分执行重新定向,用于引导进入到用于验证软件的下载站点,并安排将验证软件在从下载站点下载到通信设备上。因此,根据本发明的网络连接方法,可以以简单和强制的方式来执行配置新引入的各种工具(软件),从

而能解决前提问题,这是由于在提供服务时必须安装各种工具。

[0053] 因此,根据本发明的网络连接方法,对于与网络设备的连接监视(L2[层2]状态监视),该连接监视是一系列以L2至L3(层3)、和L3至应用的顺序的处理,由于使用L2的状态变化作为操作的触发,因此通过仅仅将电缆插入网络设备,就可以结束处理,将电缆插入网络设备是任何人都可以执行的简单操作。

[0054] 在这种情况下,通过使用验证软件,通信设备-端就可以执行VLAN(虚拟LAN(局域网))或VPN(虚拟专用网)的状态变化/切换的自动检测,另外使用相同的端口还可以检测链路的状态变化(链路良好/链路故障)。网络设备(例如,集线器)根据链路(链路良好/链路故障)的状态变化,来执行VLAN或VPN的转换。在称为SNMP(简单网络管理协议)的协议下操作的设备可以被认为是网络设备。

[0055] 根据本发明的网络连接方法,在接收控制部分执行上述的处理之后,当执行与通信设备的密钥信息的交换时,当从外部网络(异地链路)连接时,由于现在可以使用由通信设备获得的密钥信息,来建立在连接主网络的本地网关之间的VPN隧道,因此通信设备现在就可以以安全和简单的方式从外部连接到主网络。

[0056] 在通信设备-端执行下面的操作。

[0057] (1) 在插入到网络设备之后,就总是立即建立与用于资格审查/设置的网络(登入网络)的连接。在这种情况下,如果通信设备没有满足条件(例如,还没有经过隔离),就通知消息“隔离”和“登入”。如果通信设备满足了条件(例如,已经经过隔离),VLAN或VPN就被转换到主网络,以便使用主网络,并允许从主网络提供信息。

[0058] (2) 当从网络设备拔去电缆时,就通过自动检测将相关端口连接到用于资格审查/设置的网络。

[0059] (3) 当问题出现时(当发现蠕虫时),所有的端口就被连接到用于资格审查/设置的网络。

[0060] 如上所述,根据本发明的网络连接方法,通过简单地将电缆插入网络设备,现在就可以执行IPv6(网际协议6)快速服务发现的运行直到应用运行的论证等。这开启了构建通信环境的系统开发的方法,在该通信环境中能够以一种简单的操作来正确配置设备和引导操作。因此,甚至能自动地执行了设备的初始化,而不需要用户考虑该做什么操作和什么时候执行操作,获取的信息可以验证这种信息是否可靠。在执行这种操作中,现在可以以强制的方式,自动执行对受病毒感染的设备和未授权设备的隔离,而不会使这些设备进入主网络。很明显,这对于同时连接到相同网络设备的其它设备来说,防止了病毒的传播或业务量的增加。

[0061] 根据本发明的网络连接方法,可以将各种服务信息(摄像机信息、VPN[虚拟专用网]信息、网络状态信息、密钥等)确定为目标,能够经控制服务设备以简单和安全的方式来交换需要保密的密钥。另外,本发明的网络连接方法还支持各种类型(被动/主动)的IP(网际协议)设备。被动设备不允许自动的服务搜索,这些被动设备包括诸如路由器或信息应用设备等的无线LAN(局域网)AP(接入点),而主动设备允许自动的服务搜索,这些主动设备包括PC(个人计算机)和PDA(个人数字助理)。

[0062] 更进一步,根据本发明的网络连接方法能够实现混合验证,该混合验证组合自动隔离和人为验证,在自动隔离中,接收控制部分和通信设备在一对一(one on one)的基

础上通过用于资格审查 / 设置的网络进行隔离连接，人为验证能够监视可疑个体的终端使用。即使在这种情况下，当连接到网络时，用户不再需要输入密钥，并且可以以安全和简单的方式执行网络连接。

[0063] 通过按照上述的内容来配置和操作本发明，就可以获得优点，这是由于可以以简单的方式执行与主网络的连接，同时防止病毒传播到其它设备，并防止在隔离期间业务量的增加。

[0064] 附图简述

- [0065] 图 1 显示了根据本发明实施例的通信系统操作的流程图；
- [0066] 图 2 显示了根据本发明第一实例的通信系统配置的框图；
- [0067] 图 3 显示了在图 2 中显示的接收盒和通信设备的连接状态的框图；
- [0068] 图 4 显示了在图 2 中显示的接收盒的配置的框图；
- [0069] 图 5 显示了在图 2 中显示的通信设备的配置的框图；
- [0070] 图 6 显示了根据本发明第一实例的通信系统中网络连接处理的顺序图；
- [0071] 图 7 显示了根据本发明第一实例的通信系统中网络连接处理的顺序图；
- [0072] 图 8 显示了根据本发明第一实例的通信系统中隔离处理的顺序图；
- [0073] 图 9 显示了根据本发明第一实例的通信系统中隔离处理的顺序图；
- [0074] 图 10 显示了在根据本发明第一实例的通信系统中使用的登入工具处理的流程图；
- [0075] 图 11 显示了根据本发明第一实例的通信系统中确认插入目标网络的处理的流程图；
- [0076] 图 12 显示了根据本发明第一实例的通信系统中在拔去期间的操作的顺序图；
- [0077] 图 13 显示了根据本发明第二实例的通信系统配置的框图；
- [0078] 图 14 显示了根据本发明第二实例的通信系统中通信设备的操作的流程图；
- [0079] 图 15 显示了根据本发明第三实例的通信系统配置的框图；
- [0080] 图 16 显示了根据本发明第三实例的通信系统中接收盒和外围设备的连接状态的框图；
- [0081] 图 17 显示了根据本发明第三实例的通信系统中网络连接处理的顺序图；
- [0082] 图 18 显示了根据本发明第四实例的通信系统中网络连接处理的顺序图；
- [0083] 图 19 显示了根据本发明第四实例的通信系统中网络连接处理的顺序图；
- [0084] 图 20 显示了根据本发明第五实例的接收盒和通信设备的连接状态的框图。

[0085] 优选实施例详述

[0086] 现在将参照附图描述本发明的实施例。图 1 显示了根据本发明实施例的通信系统操作的流程图。现在将参照图 1 提供对根据本发明实施例的通信系统中通信设备的操作叙述。

[0087] 假定通信设备的连接请求所指向的本地链路包括主网络和登入网络，其中该主网络提供各种服务，该登入网络（用于资格审查 / 设置的网络）用于验证请求者通信设备是否满足了预置的连接条件，并且，假定用于验证是否满足这种连接条件的接收盒（接收控制部分）是通过登入网络、以一对一为基础而隔离连接到请求者通信设备的，从而确保请求者通信设备不会被连接到同一登入网络的其它设备所访问。而且，主网络和登入网络构

成 VLAN(虚拟 LAN(局域网)或 VPN(虚拟专用网))。

[0088] 请求者通信设备的用户预先执行预处理,以便提前使用主网络(用户协议等等)(图 1 中步骤 S1)。然后,当连接到主网络时,用户将通信设备的电缆插入到网络设备的端口(例如集线器)中,以连接到登入网络。

[0089] 请求者通信设备通过在网络设备内的登入网络,在一一对的基础上被隔离连接到接收盒。在这种情况下,即使有其它设备连接到该网络设备,这些设备也将既无法识别、也无法访问与该网络设备连接的请求者通信设备。

[0090] 当请求者通信设备在一一对的基础上被隔离连接到接收盒时,就使用接收盒执行登入(图 1 中步骤 S2)。更具体来说,执行登入处理,以便检验在一一对的基础上被隔离连接到该接收盒的请求者通信设备是否是受病毒感染的通信设备或打算未授权接入的通信设备,并检验是否满足了预置的连接条件。

[0091] 在这种情况下,接收盒向请求者通信设备提供执行验证的数据,获取执行数据的结果(该设备是否受到病毒或间谍软件等的感染)和关于请求者通信设备自身的信息(关于 OS[操作系统]的信息及其应用的补丁程序、防病毒软件的版本信息、关于安装的应用软件的信息等),并根据获取的信息检验是否满足了预置的资格条件(请求者通信设备是否有资格连接到主网络的条件)。资格条件例如可以包括未感染病毒或间谍软件、至少安装了 Web 浏览器和防病毒软件、以及应用了最新的补丁程序。

[0092] 另外,通过交换密钥信息,以便使用电子签名功能来验证在经由登入网络连接该请求者通信设备的状态下(使用 KDC[密钥分配中心]模型),请求者通信设备获取的信息是否为正确信息,接收盒就能够通过使用该密钥信息,验证从通过即插即用的方式连接的主网络提供来的服务信息是否为正确信息。

[0093] 在这种情况下,根据本发明的实施例,当使用目录服务器(DA:目录代理)时,其中在该目录服务器上登记了关于与主网络连接的设备的信息,则可以构造一种机制来检验该信息是否是来自正确的目录服务器。这个机制作为一种必要而充分的简单机制,新提供了一种获取目录服务器的公共密钥的服务。仅仅在开始时执行一次目录服务器的公共密钥的获取和检验,并且通过使用公共密钥,就可以执行一般服务信息的获取和检验。

[0094] 当接收盒通过上述的登入处理,确定请求者通信设备满足了连接条件时,接收盒令网络设备将请求者通信设备所连接的网络,从登入网络转换(插入)到主网络(图 1 中步骤 S3)。随后,请求者通信设备转变到主网络的实际使用(图 1 中步骤 S4)。

[0095] 当请求者通信设备转变到主网络的实际使用时,如果按照上文描述的那样执行密钥信息的交换,则请求者通信设备将能够搜索出可从主网络获得什么样的服务,并通过使用密钥信息,借助电子签名功能来检验搜索的服务信息是否正确。当服务信息正确时,请求者通信设备将使用该服务信息进行相关的服务。

[0096] 另外,如果按照上文描述的那样执行密钥信息的交换,在主网络的使用终止、并从其它网络连接到上述主网络时,请求者通信设备将能够使用密钥信息,在其它网络与主网络之间建立 VPN(虚拟专用网)隧道。

[0097] 当主网络的实际使用终止时,请求者通信设备的用户从网络设备卸下(拔去)它的电缆,将通信设备从主网络断开(图 1 中步骤 S5)。在这种情况下,由于请求者通信设备与主网络的连接被终止,因此接收盒就执行登出,将网络设备的配置返回到它的原始设置,

或者换句话说,该原始设置是当插入电缆时经登入网络执行与接收盒的隔离连接时的设置(图1中的步骤S6)。

[0098] 换句话说,在验证处理中,当请求者通信设备的电缆从网络设备断开时,接收盒就执行处理,将网络设备恢复到当通信设备的电缆插入到网络设备的端口时的设置,电缆的通信设备所连接的网络将是登入网络。因此,接收盒将接下来连接到网络设备的通信设备安排为首先连接到登入网络。

[0099] 在执行上述的处理之后,请求者通信设备的用户终止主网络的使用(图1中步骤S7)。根据上述的处理流程,使用主网络来执行请求者通信设备的处理。因此,根据本发明的实施例,即使在受病毒感染的通信设备或者使用尝试未授权接入等的通信设备被连接到登入网络的情形下,仍可以建立防止接入其它设备的隔离状态,从而使得能够以简单的方式执行正确的通信设备与主网络的连接。同时,可以防止发生从上述受病毒感染的通信设备或使用尝试未授权接入等的通信设备、向同时连接到该网络设备的其它设备的病毒传播或业务量增加。

[0100] [第一实例]

[0101] 图2显示了根据本发明第一实例的通信系统配置的框图。如图2中所示,根据本发明第一实例的通信系统包括接收盒1、通信设备2、摄像机3、本地网关4和本地链路100。本地链路100包括主网络101和登入网络102。尽管在下文中将主网络101和登入网络102描述为VLAN,但是也可以构成VPN,网络的配置并不局限于这些实例。

[0102] 图3显示了在图2中显示的接收盒1和通信设备2的连接状态的框图。如图3中所示,集线器(启用VLAN)5具有端口“a”至“h”。接收盒1经端口“a”连接到主网络101,并经端口“b”连接到登入网络102。本实例可以应用于除集线器以外的网络设备(诸如路由器等)。另外,网络设备可以在诸如SNMP(简单网络管理协议)等的协议下操作。

[0103] 端口“c”至“h”被配置为在与主网络101的连接、和经登入网络102与端口“b”的一对连接之间切换与之连接的设备。因此,可以在连接端口“b”的接收盒1与连接端口“c”至“h”中任何一个端口的通信设备之间建立一对一的隔离连接。在这种情况下,集线器5不能将分别连接到端口“c”至“h”的通信设备相互连接起来。图3显示了一种状态,在该状态中,连接端口“d”的通信设备2在一一对的基础上被隔离连接到连接端口“b”的接收盒1。由于接收盒1已经完成了分别与端口“g”和“h”连接的摄像机3和本地网关4的连接条件检查(资格审查),因此该摄像机3和本地网关4被连接到主网络101。

[0104] 当通过在接收盒1与通信设备2之间交换信息,确定通信设备2满足了预置的资格条件时,接收盒1转换通信设备2所连接的端口“d”(VLAN切换),以便将通信设备2连接到主网络101。

[0105] 图4显示了在图2中显示的接收盒1的配置框图。如图4中所示,接收盒1包括CPU(中央处理单元)11、主存储器12、存储设备13、I/F(接口)部分14、和用于累积各种信息的数据库15,该主存储器12用于存储由CPU11执行的控制程序12a,该存储设备13在CPU11执行控制程序12a时被用作工作区域,I/F部分14经电缆被连接到集线器5。CPU11、主存储器12、存储设备13、I/F部分14和数据库15分别被连接到内部总线110。另外,数据库15可以被外部安装到接收盒1。

[0106] 在存储设备13中保持了由CPU11使用的各种信息,该存储设备13被提供有用于

执行登入处理的登入处理程序 131、用于存储被用来执行登入处理的登入工具的登入工具存储区域 132、、用于保持密钥信息的密钥信息保持部分 133、和登入信息存储区域 134。数据库 15 被提供有通信设备初始信息存储区域 151 和通信设备隔离信息存储区域 152，该通信设备初始信息存储区域 151 用于存储通信设备的初始信息，该通信设备隔离信息存储区域 152 用于存储通信设备的隔离信息。

[0107] 图 5 显示了在图 2 中显示的通信设备 2 的配置框图。如图 5 中所示，通信设备 2 包括 CPU21、主存储器 22、存储设备 23 和 I/F(接口) 部分 24，该主存储器 22 用于存储由 CPU21 执行的控制程序 22a，该存储设备 23 在 CPU21 执行控制程序 22a 时被用作工作区域，I/F(接口) 部分 24 经电缆被连接到集线器 5。CPU21、主存储器 22、存储设备 23 和 I/F 部分 24 分别被连接到内部总线 210。

[0108] 在存储设备 23 中保持了由 CPU21 使用的各种信息，该存储设备 23 被提供有 AP(应用) 软件 231、Web 浏览器 232、登入工具 233 和密钥信息保持部分 234，该 Web 浏览器 232 用于访问在因特网上的各种站点，登入工具 233 被用于上述的登入处理，该密钥信息保持部分 234 用于保持密钥信息。

[0109] 图 6 和图 7 显示了根据本发明第一实例的通信系统中网络连接处理的顺序图。图 8 和图 9 显示了根据本发明第一实例的通信系统中隔离处理的顺序图。图 10 显示了根据本发明第一实例的在通信系统中使用的登入工具处理的流程图，图 11 显示了根据本发明第一实例的由通信系统确认插入目标网络的处理的流程图。现在将参照图 1 至图 11 来描述根据本发明第一实例的通信系统的操作。在图 6 至图 9 和图 11 中，通过 CPU11 执行控制程序 12a 来实现接收盒 1 的处理，同时通过 CPU21 执行控制程序 22a 来实现通信设备 2 的处理。

[0110] 在通信设备 2，当电缆被连接（插入到登入网络）到集线器 5 的端口“f”（参考在图 6 中的参考字符“a1”），并且进行与登入网络 102 的连接时，通信设备 2 检测与登入网络 102 的链路良好（LinkUp）（参考在图 6 中的参考字符“a2”），使用登入工具 233 确认插入目标（参考在图 6 中参考字符“a3”）。在这种情况下，假定已经从登入工具的下载服务器（未显示）上预先下载了登入工具 233，并将登入工具 233 保持在存储设备 23 中。

[0111] 通信设备 2 经由广播来向登入网络 102 发送用于确认插入目标的查询请求（参考在图 6 中的参考字符“a4”）。在这种情况下，由于通信设备 2 是经由登入网络 102 在一对一的基础上被隔离连接到接收盒 1 的，因此接收盒 1 将向通信设备 2 返回回复（参考在图 6 中的参考字符“a5”）。

[0112] 在接收到回复时，通信设备 2 通过使用 SLP(服务位置协议) 查询、SLP 回复 (HTTP[超文本传输协议]URL[统一资源定位器]) 等来执行服务搜索的处理（参考在图 6 中的参考字符“a6”）。

[0113] 通信设备 2 准备全局地址（参考在图 6 中的参考字符“a7”），随后执行对接收盒 1 的 HTTP 接入（参考在图 6 中的参考字符“a8”）。接收盒 1 对来自通信设备 2 的 HTTP 接入执行连接条件检查（参考在图 6 中的参考字符“a9”）。在这种情况下，连接条件是上述与本发明的实施例相联系的资格条件类型中的一种类型。由于对连接条件执行的检查类似于本发明上述实施例所叙述的处理，因此将省略对它的描述。

[0114] 如果接收盒 1 通过连接条件检查发现这些连接条件得不到支持，接收盒 1 就向通

信设备 2 通知隔离画面（参考在图 6 中的参考字符“a10”），并安排通信设备 2 执行隔离处理（参考在图 6 中的参考字符“a11”）。一旦在通信设备 2 处执行隔离处理，并返回了处理结果（HTTP 提交）（参考在图 6 中的参考字符“a12”），则接收盒 1 执行隔离确定（参考在图 6 中的参考字符“a13”）。

[0115] 如果隔离处理结果是否定的，接收盒 1 就向通信设备 2 通知隔离指示画面（参考在图 6 中的参考字符“a14”），并安排通信设备 2 执行隔离。另外，如果隔离处理结果是肯定的，接收盒 1 就执行在通信设备 2 之间交换公共密钥的处理（参考在图 6 中的参考字符“a16”至“a18”）。接收盒 1 将公共密钥（通信设备 2）登记到存储设备 13 的密钥保持部分 133（参考在图 6 中的参考字符“a18”）。

[0116] 类似地，通信设备 2 将来自接收盒 1 的公共密钥（接收盒 1）登记到存储设备 23 的密钥信息保持部分 234。在这种情况下，对来自接收盒 1 的公共密钥（接收盒 1），由接收盒 1 代表下述每个设备，将与主网络 101 连接的每个设备（例如，摄像机 3 或本地网关 4）的公共密钥移交给通信设备 2。

[0117] 随后，接收盒 1 执行 VLAN 切换（参考在图 7 中的参考字符“a19”），并向通信设备 2 通知网络切换指示画面（参考在图 7 中的参考字符“a20”）。在接收到通知时，通信设备 2 通过使用 RS（路由请求）消息或 RA（路由广告）来执行地址设置的处理（参考在图 7 中的参考字符“a21”）。

[0118] 在通信设备 2 检测到登入网络 102 的链路故障（LinkDown）（移动检测）时（参考在图 7 中的参考字符“a22”），或者在通过连接条件检查而发现通信设备 2 支持连接条件的情况下，执行 VLAN 切换（参考在图 7 中的参考字符“a23”），而且检测到与主网络 101 的连接（插入主网络）时（参考在图 7 中的参考字符“a24”），则使用登入工具 233 来确认插入目标（参考在图 7 中的参考字符“a25”）。

[0119] 通信设备 2 通过广播向主网络 101 发送用于确认插入目标的查询请求（参考在图 7 中的参考字符“a26”）。在这种情况下，由于摄像机 3、本地网关 4 和目录服务器（DA：目录代理）（未显示）都被连接到主网络 101，因此来自这些设备的回复被返回到通信设备 2（参考在图 7 中的参考字符“a27”）。

[0120] 与连接到主网络 101 的设备有关的信息都被登记到目录服务器中。因此，通信设备 2 开始本地链路检测和本地链路处理（参考在图 7 中的参考字符“a28”）。当完成这些操作时，通过使用在密钥信息保持部分 234 中登记的公共密钥，通信设备 2 将能够检验该信息是否是来自摄像机 3、本地网关 4 和目录服务器。

[0121] 现在将参考图 8 和图 9 提供上述隔离处理的详细描述。在通信设备 2，当电缆被连接（插入）到集线器 5 的端口“d”（参考在图 8 中的参考字符“b1”）、并执行与登入网络 102 的连接时，通信设备 2 检测与登入网络 102 的链路良好（参考在图 8 中的参考字符“b2”），并使用登入工具 233 执行插入目标确认（参考在图 8 中的参考字符“b3”）。

[0122] 通信设备 2 经由广播向登入网络 102 发送用于确认插入目标的查询请求（参考在图 8 中的参考字符“b4”）。在这种情况下，由于通信设备 2 是经由登入网络 102 仅仅在一一对的基础上被隔离连接到接收盒 1 的，因此，接收盒 1 将向通信设备 2 返回回复（参考在图 8 中的参考字符“b5”）。在接收到回复时，通信设备 2 执行上述的服务搜索处理（参考在图 8 中的参考字符“b6”）。

[0123] 通信设备 2 准备全局地址（参考在图 8 中的参考字符“b7”），随后执行对接收盒 1 的 HTTP 接入（参考在图 8 中的参考字符“b8”）。接收盒 1 对来自通信设备 2 的 HTTP 接入执行连接条件检查（参考在图 8 中的参考字符“b9”）。由于对连接条件执行的检查类似于本发明上述实施例所描述的处理，因此将省略对它的描述。

[0124] 如果接收盒 1 通过连接条件检查发现这些连接条件得不到支持，接收盒 1 就向通信设备 2 通知隔离画面（参考在图 8 中的参考字符“b10”）。当点击隔离画面时，通信设备 2 就向接收盒 1 返回 HTTP 提交（参考在图 8 中的参考字符“b11”）。当从通信设备 2 返回 HTTP 提交时，接收盒 1 就开始通信设备 2 的隔离（参考在图 8 中的参考字符“b12”），并向通信设备 2 发送隔离开始脚本（参考在图 8 中参考字符“b13”）。

[0125] 通信设备 2 由此执行隔离开始脚本，并向接收盒 1 返回 HTTP 提交（参考在图 8 中的参考字符“b14”）。当从通信设备 2 返回 HTTP 提交时，接收盒 1 就安排由通信设备 2 下载辅助文件（本地网关 4 的公共密钥 [主密钥]，隔离数据，隔离脚本）（参考在图 8 中的参考字符“b15”）。

[0126] 一旦下载了辅助文件，通信设备 2 就执行隔离脚本，收集信息，并创建和显示表格（参考在图 8 中的参考字符“b16”）。当在显示屏上点击给定的图标等（未显示）时，通信设备 2 就向接收盒 1 返回 HTTP 提交（通信设备的状态信息，公共密钥）（参考在图 8 中的参考字符“b17”）。接收盒 1 根据来自通信设备 2 的信息来执行隔离确定（参考在图 9 中的参考字符“b18”），如果结果是否定的，就向通信设备 2 通知修正指示画面（参考在图 9 中的参考字符“b19”）。

[0127] 当接收到修正指示画面时，通信设备 2 就根据这些指令来执行它自身状态的修正（例如，下载和应用最新的补丁程序，下载和应用防病毒软件的最新模式和补丁程序，清除感染的病毒和间谍软件等）。一旦完成了修正，通信设备 2 就向接收盒 1 发送修正结束和它自身的公共密钥（参考在图 9 中的参考字符“b20”）。通过接收盒 1 执行对通信设备 2 的上述下载，仅仅允许访问相应的专用网站。禁止从通信设备 2 到其它站点的接入。

[0128] 接收盒 1 将公共密钥保持在存储设备 13 的密钥信息保持部分 133 中（参考在图 9 中的参考字符“b21”）。一旦登记了公共密钥，或者如果满足了连接条件，接收盒 1 就向通信设备 2 通知网络切换指示画面（参考在图 9 中的参考字符“b22”）。

[0129] 接下来，将参照图 10 描述在上述处理中使用的登入工具的处理。在上述的处理中，通过将电缆插入到网络设备（集线器 5）的端口“d”在检测到与登入网络 102 的连接时，就激活登入工具 233。这里，登入工具 233 的激活使通信设备 2 执行链路状态确认（在图 10 中的步骤 S11）和网络确认（在图 10 中的步骤 S12）、以及从设备自身内部获取资格审查信息（在图 10 中的步骤 S13）。

[0130] 通信设备 2 向接收盒 1 发送获取的资格审查信息（在图 10 中的步骤 S14），当从接收盒 1 返回了资格审查的肯定结果时，就终止处理（在图 10 中步骤 S15）。另外，如果没有返回资格审查的肯定结果（在图 10 中步骤 S15），通信设备 2 就执行修正状态的确认，或者换句话说，通信设备 2 执行由接收盒 1 指示的修正，并确认它随后的修正状态（在图 10 中步骤 S16）。如果已经执行修正，通信设备 2 就返回到步骤 S13，以获取设备自身的资格审查信息。

[0131] 现在将参照图 11 来描述插入目标网络的确认的处理。当与主网络 101 链路良好

时,通信设备 2 就激活确认插入目标网络的处理(在图 11 中步骤 S21)。当激活确认处理时,通信设备 2 就经 SLP(多播)执行对主网络 101 的查询(服务类型 :x- 网络 -id, 服务 URL : 类型 +ID), 并获取网络 ID(在图 11 中步骤 S22)。

[0132] 当通信设备 2 确定该类型是登入网络 102 时(在图 11 中步骤 S23), 就通过通信设备 2 执行登入处理(隔离 + 密钥交换)(在图 11 中步骤 S24)。另外, 当通信设备 2 确定该类型是本地链路 100 时(在图 11 中步骤 S25), 通信设备 2 就执行本地链路处理(在图 11 中步骤 S26)。更进一步, 当通信设备 2 确定该类型是异地链路时(未显示)(在图 11 中步骤 S27), 通信设备 2 就执行异地链路处理(在图 11 中步骤 S28)。关于异地链路处理的叙述将在后面进行提供。

[0133] 图 12 显示了根据本发明第一实例的通信系统中在拔去 (plug-out) 期间的操作顺序图。现在将参照图 12 来描述根据本发明第一实例的通信系统中在拔去期间的操作。在图 12 中, 通过 CPU11 执行控制程序 12a 来实现接收盒 1 的处理, 同时通过 CPU21 执行控制程序 22a 来实现通信设备 2 的处理。

[0134] 在通信设备 2 的电缆从集线器 5 的端口“d”卸下, 通信设备 2 从主网络断开(拔去)的情况下(参考在图 12 中的参考字符“c1”), 就中止了摄像机 3 的状态更新(参考在图 12 中的参考字符“c2”)。这里, 由于向接收盒 1 输入了指示从集线器 5 卸下电缆的链路故障陷阱消息(linkdown trap)(参考在图 12 中的参考字符“c3”), 因此, 接收盒 1 就执行从主网络 101 到登入网络 102 的切换(VLAN 切换)(参考在图 12 中的参考字符“c4”), 并激活隔离状态清除定时器(未显示)(参考在图 12 中的参考字符“c5”)。

[0135] 由此执行从主网络 101 到登入网络 102 的切换(VLAN 切换)(参考在图 12 中的参考字符“c6”)。另外, 当隔离状态清除定时器届满时, 就清除在接收盒 1 上保持的通信设备 2 的隔离状态(参考在图 12 中的参考字符“c7”)。

[0136] 尽管本实例假定在通信设备 2 中已安装(Bootstrap: 工具安装程序)了执行上述处理的登入工具 233, 但是在通信设备 2 出现新的连接时, 通信设备 2 还可以被配置为连接到登入工具的下载站点(未显示), 用于下载和安装登入工具。

[0137] 在下载登入工具时, 通信设备 2 必须至少安装有 Web 浏览器。当通信设备 2 的电缆被连接到集线器 5, Web 浏览器进入任意的网站时, 接收盒 1 就执行重新定向, 用于引导接入到登入工具的下载站点, 并安排将登入工具从下载站点下载到通信设备 2 上。因此, 根据本实例, 可以以简单和强制的方式来执行配置新引入的各种工具(软件), 从而能够解决在提供服务时必须安装各种工具这样的前提条件。

[0138] 可以看到, 根据本实例, 对于与集线器 5 的连接监视(L2[层 2]状态监视)(该连接监视是以 L2 至 L3(层 3)、和 L3 至应用的顺序的一系列处理), 由于使用 L2 的状态改变作为操作的触发, 因此仅仅通过将通信设备 2 的电缆插入集线器 5 的端口“c”至“h”, 就可以结束处理, 这是任何人都可以执行的简单操作。

[0139] 在这种情况下, 除了检测链路的状态变化(连接 / 链路故障)以外, 通信设备 2 侧可以使用相同端口来执行 VLAN 的状态变化 / 切换的自动检测。集线器 5 根据链路的状态变化(连接 / 链路故障)来执行 VLAN 转换。

[0140] 在通信设备 2 侧, (1) 在插入后, 总是立即建立与登入网络 102 的连接。如果没有满足条件(例如, 未隔离), 就通知消息“隔离”和“登记”。如果满足了条件(例如, 已完成

隔离),就执行到主网络 101 的 VLAN 切换,以便能够使用主网络 101,获得由主网络 101 提供的信息。

[0141] 另外,在通信设备 2 侧,(2)当从集线器 5 中拔去电缆时,通过自动检测,将该相关端口连接到登入网络 102。更进一步,在通信设备 2 侧,(3)当出现问题时(例如,当发现蠕虫时),就将集线器 5 的所有端口连接到登入网络 102。

[0142] 因此,根据本实例,现在通过简单地将通信设备 2 的电缆插入到集线器 5 的端口,就可以对 IPv6(网际协议版本 6)快速服务发现的执行、直到应用程序的执行进行实证。根据本实例,这使得能够开发其中以一种简单的操作方式来正确配置设备的通信环境构造系统。因此,甚至能自动地执行设备的初始化,而不需要用户考虑该做什么操作和什么时候执行操作,并可以验证所获得的信息是否可靠。

[0143] 在完成这些操作时,根据本实例,由于受病毒感染的设备或未授权的设备经登入网络 102 保持与接收盒 101 的隔离连接,因此,现在就可以经接收盒 1,以强制的方式自动执行对这些设备的隔离,而不会使这些设备连接到主网络 101。

[0144] 在这种情况下,由于受病毒感染的设备或未授权的设备经登入网络 102 将保持与接收盒 101 的隔离连接,因此,就可以防止由这些设备引起同时连接到集线器 5 的其它设备的病毒传播或业务量增加。

[0145] [第二实例]

[0146] 图 13 显示了根据本发明第二实例的通信系统配置的框图。图 13 显示了一个实例,在该实例中,通信设备 2 进行移动(目标通信设备被视为“2a”),通过经由异地链路 200 和 IP 网络 300 建立与本地网关 4 之间的 VPN(虚拟专用网)隧道,从而连接到主网络 100。

[0147] 在这种情况下,假定在接收盒 1 执行登入处理的期间,通信设备 2a 是经由登入网络 102 在一对一的基础上被隔离连接到接收盒 1 的,并在密钥信息的交换期间,获取了本地网关 4 的公共密钥。并且,还假定本地网关 4 已经经由接收盒 1 获取了通信设备 2a 的公共密钥。使用这些公共密钥,就可以获得用于建立 VPN 隧道的密钥信息。

[0148] 图 14 显示了根据本发明第二实例的通信系统中通信设备 2a 的操作流程图。现在将参照图 13 和图 14 来描述通信设备 2a 的操作。通信设备 2a 的配置类似于在图 4 中显示的根据本发明第一实例的通信设备 2 的配置。通过通信设备 2a 的 CPU21 执行控制程序 22a,就可以实现图 14 中显示的处理。

[0149] 当通信设备 2a 确认异地链路 200 时(在图 14 中步骤 S31),如果本地链路 100 没有得到确认(在图 14 中步骤 S32),通信设备 2a 就通知不存在本地链路 100(在图 14 中步骤 S33),并终止处理。

[0150] 如果通信设备 2a 确认本地链路 100(在图 14 中步骤 S32),通信设备 2a 就查询本地链路 100 的状态(在图 14 中步骤 S34)。当没有回复时(在图 14 中步骤 S35),通信设备 2a 就通知“故障”(在图 14 中步骤 S36),并终止处理。

[0151] 如果存在回复(在图 14 中步骤 S35),通信设备 2a 就检查本地链路 100 的状态(在图 14 中步骤 S37)。如果本地链路 100 的状态为未激活,通信设备 2a 就通知“故障”(在图 14 中步骤 S38),并终止处理。

[0152] 如果本地链路 100 的状态为激活,通信设备 2a 就确定是否产生链路故障(在图 14 中步骤 S39)。如果产生链路故障,通信设备 2a 就终止处理。

[0153] 如果没有产生链路故障,通信设备 2a 就获取“所获得的组”(在图 14 中步骤 S40),执行网页的产生 / 显示(在图 14 中步骤 S41),并且仅仅对于第一次,获取异地链路 200 的日志(在图 14 中步骤 S42)。上述处理将被重复执行,直到产生链路故障(在图 14 中步骤 S39 至 S41)。

[0154] 异地链路 200 的日志是下一次及以后为了连接异地链路 200 而必需的信息(诸如 IP 地址、网络掩码、默认路由器、路由表、邻近超高速缓存表和地址解析协议表)。

[0155] 从上述内容可以看到,根据本实例,当通过上述在通信设备 2a 上的接收盒 1 执行登入处理时,由于在从外部网络(异地链路 200)进行连接时,通过使用由通信设备 2a 获取的密钥信息,就可以在与主网络 101 连接的本地网关 4 之间建立 VPN 隧道,因此通信设备 2a 将能够以安全和简单的方式从外部连接到主网络 101。

[0156] 根据本实例,可以将各种服务信息(摄像机信息、VPN[虚拟专用网]信息、网络状态信息、密钥等)确定为对象。另外,可以经由接收盒 1 以简单和安全的方式交换进行保密所必需的密钥。

[0157] [第三实例]

[0158] 图 15 显示了根据本发明第三实例的通信系统配置的框图。图 15 显示了一个实例,在该实例中,不能够实现自主服务搜索(不允许加载登入工具)的外围设备 6(例如,无线 LAN[本地网]AP[接入点]或路由器,信息设备等)被连接到主网络 101。

[0159] 图 16 显示了根据本发明第三实例的通信系统中接收盒 1 和外围设备 6 的连接状态的框图。如图 16 中所示,集线器(启用 VLAN)5 被提供有端口“a”至“h”。接收盒 1 经端口“a”被连接到主网络 101,并经端口“b”被连接到登入网络 102。本实例可以应用于除集线器以外的网络设备(诸如路由器等)。另外,网络设备可以在诸如 SNMP(简单网络管理协议)的协议下操作。

[0160] 端口“c”至“h”被配置为使与之连接的设备在与主网络 101 的连接、以及经由登入网络 102 与端口“b”的一对一连接之间切换。因此,可以在与端口“b”连接的接收盒 1、和与端口“c”至“h”中任何一个端口连接的通信设备之间,建立一对一的隔离连接。在这种情况下,集线器 5 无法将分别连接到端口“c”至“h”的通信设备彼此连接起来。

[0161] 图 16 显示了一种状态,在这种状态中,连接端口“e”的外围设备 6 是在一对一的基础上被隔离连接到连接端口“b”的接收盒 1 的。由于接收盒 1 已经完成了通信设备 2、端口摄像机 3 和本地网关 4 的连接条件检查(资格审查),因此将通信设备 2、端口摄像机 3 和本地网关 4 连接到主网络 101,该通信设备 2、端口摄像机 3 和本地网关 4 是被分别连接到端口“d”、“g”和“h”。

[0162] 当外围设备 6 通过登入网络 102 在一对一的基础上被隔离连接到接收盒 1 时,接收盒 1 根据来自外围设备 6 的信号,来确定连接设备的类型,并根据确定的结果配置外围设备 6。随后,在外围设备 6 所连接的端口“e”,接收盒 1 将外围设备 6 连接的网络连接到主网络 101。

[0163] 图 17 显示了根据本发明第三实例的通信系统中网络连接处理的顺序图。现在将参照图 15 至图 17 来描述根据本发明第三实例的通信系统的操作。在图 17 中,通过 CPU11 执行控制程序 12a 来实现接收盒 1 的处理,同时通过 CPU(未显示)执行控制程序来实现外围设备 6 的处理。

[0164] 当外围设备 6 的电缆被连接到集线器 5 的端口“e”，并建立与登入网络 102 的连接时（插入到登入网络；参考在图 17 中参考字符“d1”），集线器 5 就通知接收盒 1：外围设备 6 已经通过链路良好陷阱（linkuptrap）被连接到登入网络 102（参考在图 17 中参考字符“d2”）。

[0165] 当通知外围设备 6 已经连接到登入网络 102 时，接收盒 1 就开始连接设备的确认处理，同时参考数据库 15（参考在图 17 中参考字符“d3”），并向外围设备 6 发送与每个连接设备对应的 ping 信号（用于确认连通性的信号），直到从其中返回回复（ping 处理；参考在图 17 中参考字符“d4”）。

[0166] 当从外围设备 6 返回回复时（参考在图 17 中参考字符“d5”），接收盒 1 通过参考数据库 15 获取与回复（换句话说，对 ping 的回复）对应的制造商名称、设备类型等，并搜索数据库 15 来获取设备的 MAC（媒体接入控制）地址（参考在图 17 中参考字符“d6”）。

[0167] 接收盒 1 根据获取的 MAC 地址，向外围设备 6 发送设备信息获取请求（参考在图 17 中参考字符“d7”）。在从外围设备 6 获取设备信息之后（参考在图 17 中参考字符“d8”），接收盒 1 根据获取的设备信息来确定外围设备 6 的类型，并向外围设备 6 发送与该设备类型对应的初始化信息（参考在图 17 中参考字符“d9”），并执行外围设备 6 的初始化（参考在图 17 中参考字符“d10”）。在这种情况下，可以发送用于连接主网络 101 的设置信息，而不是发送初始化信息。

[0168] 随后，接收盒 1 执行外围设备 6 从登入网络 102 到主网络 101 的连接目标的切换（VLAN 切换）（参考在图 17 中参考字符“d11”和“d12”）。外围设备 6 通过广播向主网络 101 发送用于确认插入目标的查询请求（参考在图 17 中参考字符“d14”）。

[0169] 在这种情况下，由于摄像机 3、本地网关 4 和目录服务器（DA）（未显示）都被连接到主网络 101，因此来自这些设备的回复就被返回到外围设备 6（参考在图 17 中参考字符“d15”）。这里，由于在目录服务器中登记了关于连接主网络 101 的设备的信息，因此，外围设备 6 采用与其它设备相同的方式开始对目录服务器的登记处理（参考在图 17 中参考字符“d16”）。

[0170] 因此，根据本实例，通过简单地将外围设备 6 的电缆插入到集线器 5 的端口“c”至“h”中，就可以执行接收盒 1 对外围设备 6 的资格审查和连接主网络 101 的设置。因此，外围设备 6 可以采用简单而方便的方式被连接到主网络 101。

[0171] 从上述内容可以看到，本实例支持各种类型（主动 / 被动）的 IP（网际协议）设备。被动设备不允许进行自主服务搜索（不允许加载登入工具），这些被动设备包括如上所述的无线 LAN（局域网）AP（接入点），而主动设备允许进行自主服务搜索（允许加载登入工具），这些主动设备包括笔记本 PC（个人计算机）和 PDA（个人数字助理）等。

[0172] [第四实例]

[0173] 图 18 和 19 显示了根据本发明第四实例的通信系统中网络连接处理的顺序图。根据本发明第四实例的通信系统和相应设备采用与图 2 至图 5 中显示的根据本发明第三实例的通信系统和相应设备的相同方式进行配置。因此，现在将参照图 2 至图 5 以及图 18 和图 19 来描述根据本发明第四实例的通信系统的操作。假定通信设备 2 被新连接到主网络 101，还没有安装登入工具。另外，在图 18 和图 19 中，通过 CPU11 执行控制程序 12a 来实现接收盒 1 的处理，同时通过 CPU21 执行控制程序 22a 来实现通信设备 2 的处理。

[0174] 当通信设备 2 的电缆被连接到（插入到登入网络）集线器 5 的端口“f”（参考在图 18 中的参考字符“e1”），并进行与登入网络 102 的连接时，集线器 5 就通知接收盒 1：通信设备 2 已经通过链路良好陷阱消息被连接到登入网络 102（参考在图 18 中的参考字符“e2”）。

[0175] 在接收到通信设备 2 已连接到登入网络 102 的通知，并且使用 Web 浏览器访问任意的网站时（参考在图 18 中的参考字符“e3”），接收盒 1 就执行重新定向，用于引导进入到登入工具的下载站点（参考在图 18 中的参考字符“e4”），促使通信设备 2 从下载站点中下载登入工具（参考在图 18 中的参考字符“e5”和“e6”），并安排通信设备 2 安装登入工具。

[0176] 当通信设备 2 检测到与登入网络 102 的链路良好时（参考在图 18 中的参考字符“e7”），通信设备 2 就使用所安装的登入工具来确认插入目标（参考在图 18 中的参考字符“e8”）。通信设备 2 通过广播向登入网络 102 发送确认插入目标的查询请求（参考在图 18 中的参考字符“e9”）。在这种情况下，由于通信设备 2 经登入网络 102 在一对一的基础上被隔离连接到接收盒 1，接收盒 1 将向通信设备 2 返回回复（参考在图 18 中的参考字符“e10”）。

[0177] 在返回回复时，通信设备 2 通过使用 SLP 查询、SLP 回复 (HTTPURL) 等执行服务搜索处理（参考在图 18 中的参考字符“e11”）。通信设备 2 准备全局地址（参考在图 18 中的参考字符“e12”），随后执行对接收盒 1 的 HTTP 接入（参考在图 18 中的参考字符“e13”）。

[0178] 接收盒 1 执行对来自通信设备 2 的 HTTP 接入的连接条件检查（参考在图 18 中的参考字符“e14”）。在这种情况下，连接条件是上述与本发明的实施例相联系的资格条件类型中的一种类型。由于对连接条件所执行的检验类似于本发明上述实施例的处理，因此将省略对它的叙述。

[0179] 如果接收盒 1 通过连接条件检验发现这些连接条件得不到支持，接收盒 1 就向通信设备 2 通知隔离画面（参考在图 18 中的参考字符“e15”），并安排通信设备 2 执行隔离处理（参考在图 18 中的参考字符“e16”）。一旦在通信设备 2 执行隔离处理，并返回处理结果 (HTTP 提交)（参考在图 18 中的参考字符“e17”），接收盒 1 就执行隔离确定（参考在图 18 中的参考字符“e18”）。

[0180] 如果隔离处理结果是否定的，接收盒 1 就向通信设备 2 通知隔离指示画面（参考在图 18 中的参考字符“e19”），并安排通信设备 2 执行隔离。另外，如果隔离处理结果是肯定的，接收盒 1 就执行在通信设备 2 之间公共密钥的交换处理（参考在图 19 中的参考字符“e20”至“e22”）。接收盒 1 将公共密钥（通信设备 2）登记到存储设备 13 的密钥信息保持部分 133 中（参考在图 19 中的参考字符“e23”）。

[0181] 类似地，通信设备 2 将来自接收盒 1 的公共密钥（接收盒 1）登记到存储设备 23 的密钥信息保持部分 234 中。在这种情况下，对于来自接收盒 1 的公共密钥（接收盒 1），接收盒 1 代表每个设备，将与主网络 101 连接的每个设备（例如，摄像机 3 或本地网关 4）的公共密钥移交给通信设备 2。

[0182] 随后，接收盒 1 执行 VLAN 切换（参考在图 19 中的参考字符“e24”），并向通信设备 2 通知网络切换指示画面（参考在图 19 中的参考字符“e25”）。在接收到通知时，通信设备 2 使用 RS 消息或 RA 等来执行地址设置的处理（参考在图 19 中的参考字符“e26”）。

[0183] 在通信设备 2 检测到登入网络 102 的链路故障（移动检测）（参考在图 19 中的参考字符“e27”）时，或者如果通过连接条件检查发现该通信设备 2 支持连接条件而执行 VLAN 切换（参考在图 19 中的参考字符“e28”），以及在检测到与主网络 101 的连接（插入到主网络）（参考在图 19 中的参考字符“e29”）时，则使用登入工具来执行插入目标的确认（参考在图 19 中的参考字符“e30”）。

[0184] 通信设备 2 通过广播向主网络 101 发送用于确认插入目标的查询请求（参考在图 19 中的参考字符“e31”）。在这种情况下，由于摄像机 3、本地网关 4 和目录服务器（DA）（未显示）都被连接到主网络 101，来自这些设备的回复就被返回到通信设备 2（参考在图 19 中的参考字符“e32”）。这里，关于连接主网络 101 的设备的信息就被登记到目录服务器中。因此，通信设备 2 开始本地链路检测和本地链路处理（参考在图 19 中的参考字符“e33”）。

[0185] 如上所述，根据本发明，可以实现混合验证，该混合验证组合了自动隔离和人为验证，其中自动隔离是接收盒 1 和通信设备 2 在一对一的基础上通过登入网络 102 进行连接，人为验证能够监视可疑个人的终端使用。甚至在这种情况下，在连接到网络时，用户也不再需要输入密钥，并且可以以安全和简单的方式执行网络连接。尽管在本发明的每个实例中将接收盒 1 和集线器 5 描述为相互独立的设备，但是使用集成接收盒 1 和集线器 5 的设备，也可以实现上述的相同操作和优点。

[0186] [第五实例]

[0187] 图 20 显示了根据本发明第五实例的接收盒和通信设备的连接状态的框图。在图 20 中，根据本发明的第五实例，根据通信设备 2 的资格条件，该通信设备 2 被配置为可连接到三个主网络 (#1 至 #3) 201 至 203 中的任何一个主网络。

[0188] 集线器（启用 VLAN）5 提供有端口“a”至“h”。接收盒 1 经端口“a”被连接到主网络 (#1) 201，并经端口“b”被连接到登入网络。本实例可以应用于除集线器之外的网络设备（诸如路由器等）。另外，网络设备可以在诸如 SNMP（简单网络管理协议）的协议下操作。

[0189] 更进一步，端口“c”至“h”被配置为切换在与三个主网络 (#1 至 #3) 201 至 203 中任何一个主网络的连接和经登入网络 102 与端口“b”的一对一连接之间连接的设备。因此，可以在连接端口“b”的接收盒 1 与连接端口“c”至“h”的通信设备之间建立一对一的隔离连接。在这种情况下，集线器 5 不能相互连接分别被连接到端口“c”至“h”的通信设备。

[0190] 图 20 显示了一种状态，在这种状态中，连接端口“d”的通信设备 2 在一对一的基础上被隔离连接到连接端口“b”的接收盒 1，以便进行资格审查，然后根据资格条件将通信设备 2 选择地连接到主网络 (#3) 203。另外，图 20 显示了一种状态，在这种状态中，接收盒 1 已经结束了摄像机 3 和本地网关 4 的连接条件检查（资格审查），该摄像机 3 和本地网关 4 被分别连接到端口“g”和“h”，摄像机 3 和本地网关 4 被选择地连接到主网络 (#1) 201。

[0191] 可以看到，根据本实例，即使存在多个主网络（本实例能够支持四个或更多的主网络），也可以执行与上述本发明的第一至第四实例中执行的相同处理。因此，可以获得相类似的优点，可以根据预置的资格条件来选择所连接的主网络。

[0192] 尽管在上述本发明的第一至第五实例中主要描述了隔离系统，但是本发明可以替换地应用于设置和使用下列资格审查标准的系统，这些资格审查标准被使用作为连接主网络的条件。

[0193] (1) 是否已经完成了隔离对策

[0194] (2) 是否已经确认了联络事项

[0195] (3) 是否已经为每个用户通知了未处理问题

[0196] 在设置上面条件 (1) 的系统中,该系统可以考虑执行所连接通信设备的隔离(例如,设备是否受到病毒感染,最新的补丁程序是否被应用于OS等,或者是否可以使用最新的病毒定义文件等),来作为资格审查基准,并在隔离合格之后,允许与主网络的连接。在这个系统中,仅仅配置上述的登入工具便足以能够确认这些条件。该系统的配置和操作可以类似于上述本发明的第一至第五实例的配置和操作。

[0197] 在设置上面条件 (2) 的系统中,作为资格审查标准,可以考虑设置连接条件,以便连接方不会被识别,同时可以将读取由连接目标组织所共享的特殊网页安排为强制操作,以便以确保的方式来传送联络事项,或通过在读取特殊网页时所执行的操作来获得同意。

[0198] 可以考虑设置该系统,以便登入网络要求:连接通信终端的用户总是读取特殊网页,该特殊网页公布了必须由连接目标组织中的每个人读取的通知或报告;当连接到登入网络时,登入网络引导用户进入特殊的网站;在读取网页之后允许与主网络的连接。这个系统的配置和操作可以类似于上述本发明的第一至第五实例的配置和操作。

[0199] 在设置上面条件 (3) 的系统中,作为资格审查标准,该系统可以考虑包括:使用在登入处理中交换的ID信息(识别信息)来识别连接方;准备由用户分别读取的网页;引导用户进入网站,以便读取其中的内容;使用基于Web或其它浏览器的网络,允许用户参与训练或教育节目,或者提醒或强制执行未处理的事务工作,诸如调整或同意关于商业旅行等的费用开销。

[0200] 另外,在设置上述条件 (3) 的另一个系统中,作为资格审查标准,该系统可以考虑包括:使用在登入处理中交换的ID信息(识别信息)来识别连接通信设备的用户;使用ID信息来搜索在接收盒中提供的数据库,用于建立根据用户的网页,或者建立显示将由用户处理的事情的网页;并引导用户进入网页,提醒或督促用户执行显示的内容。在这种情况下,可以考虑在用户的通信设备连接到登入网络,确认执行上述处理的资料时,将允许与主网络的连接。这些系统的配置和操作可以类似于上述本发明的第一至第五实例的配置和操作。

[0201] 上述的每个系统代表了本发明的示例性应用。然而,本发明还可以被应用于需要资格审查的任何系统,并不局限于上述的实例和系统。

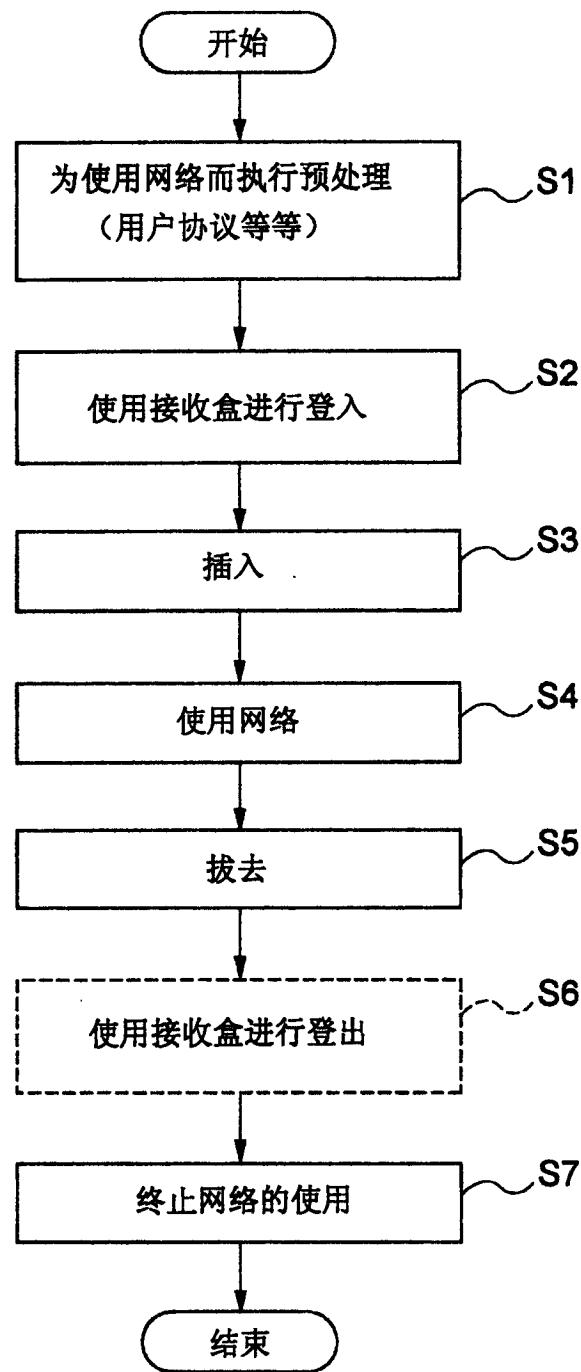


图 1

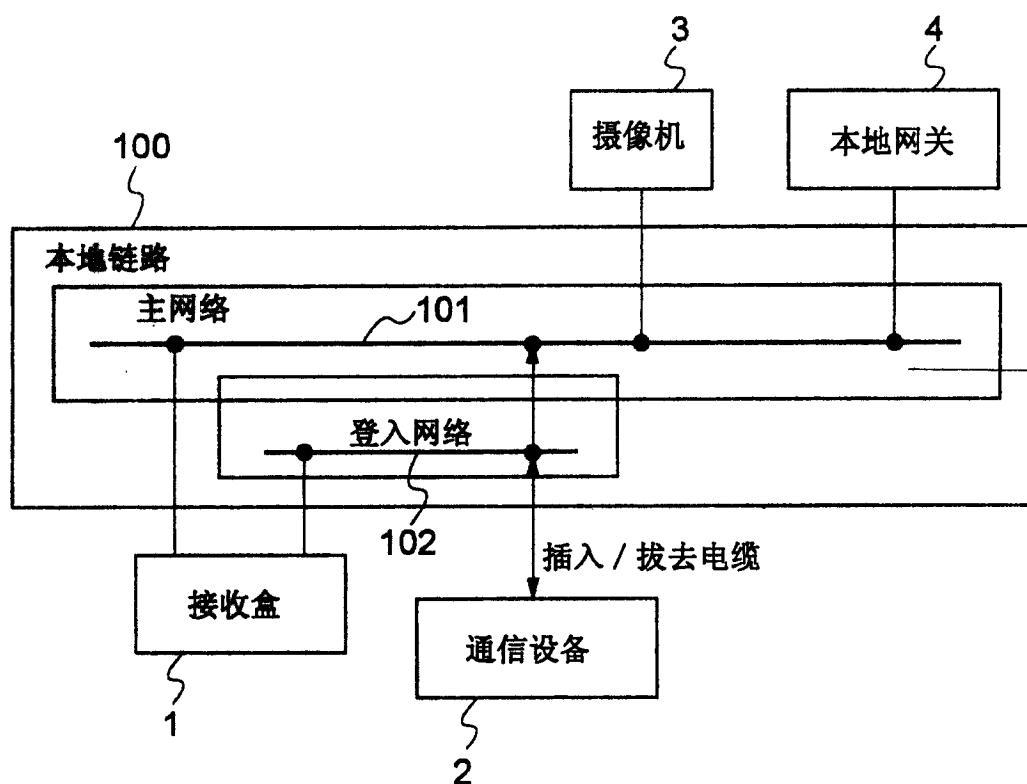
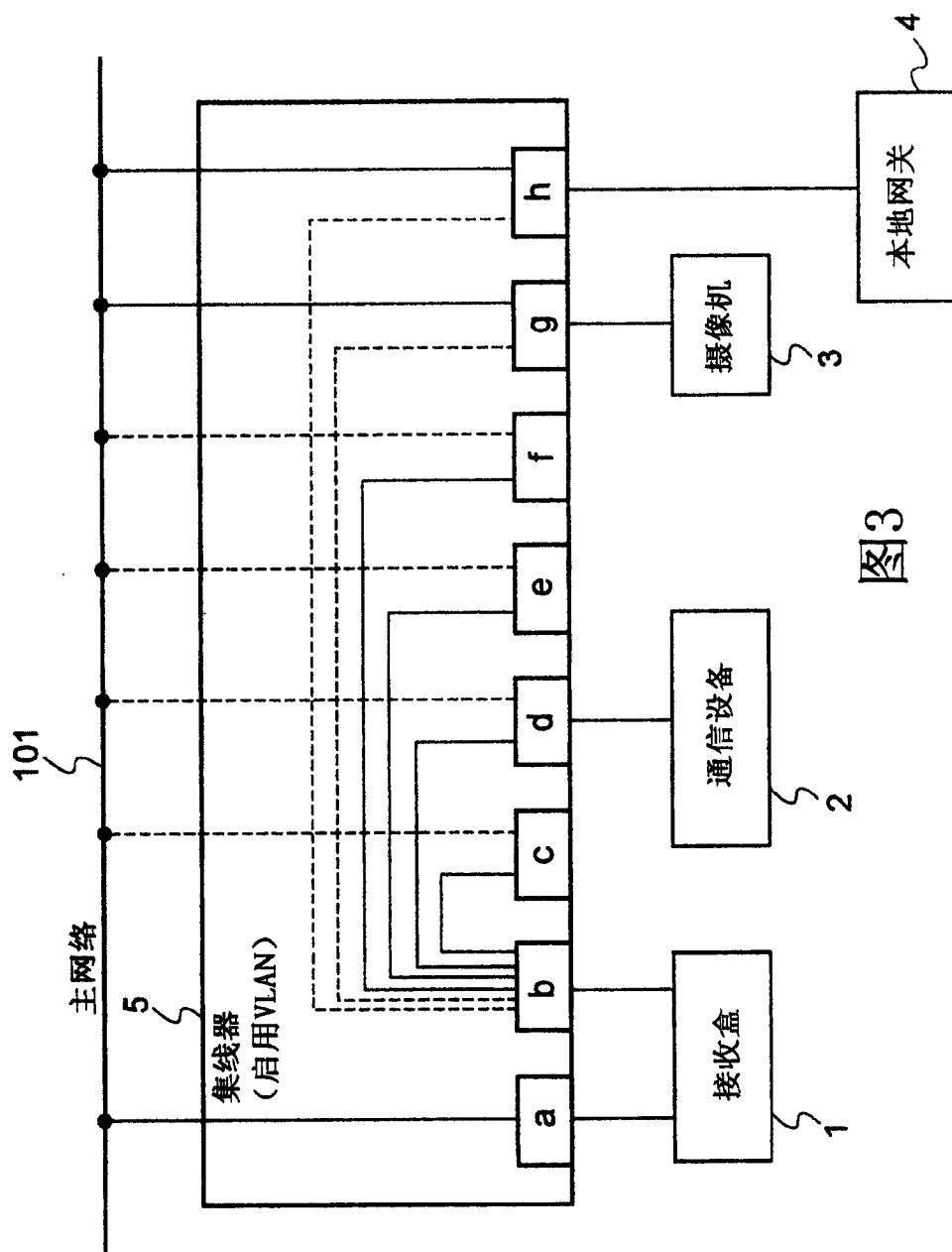


图 2



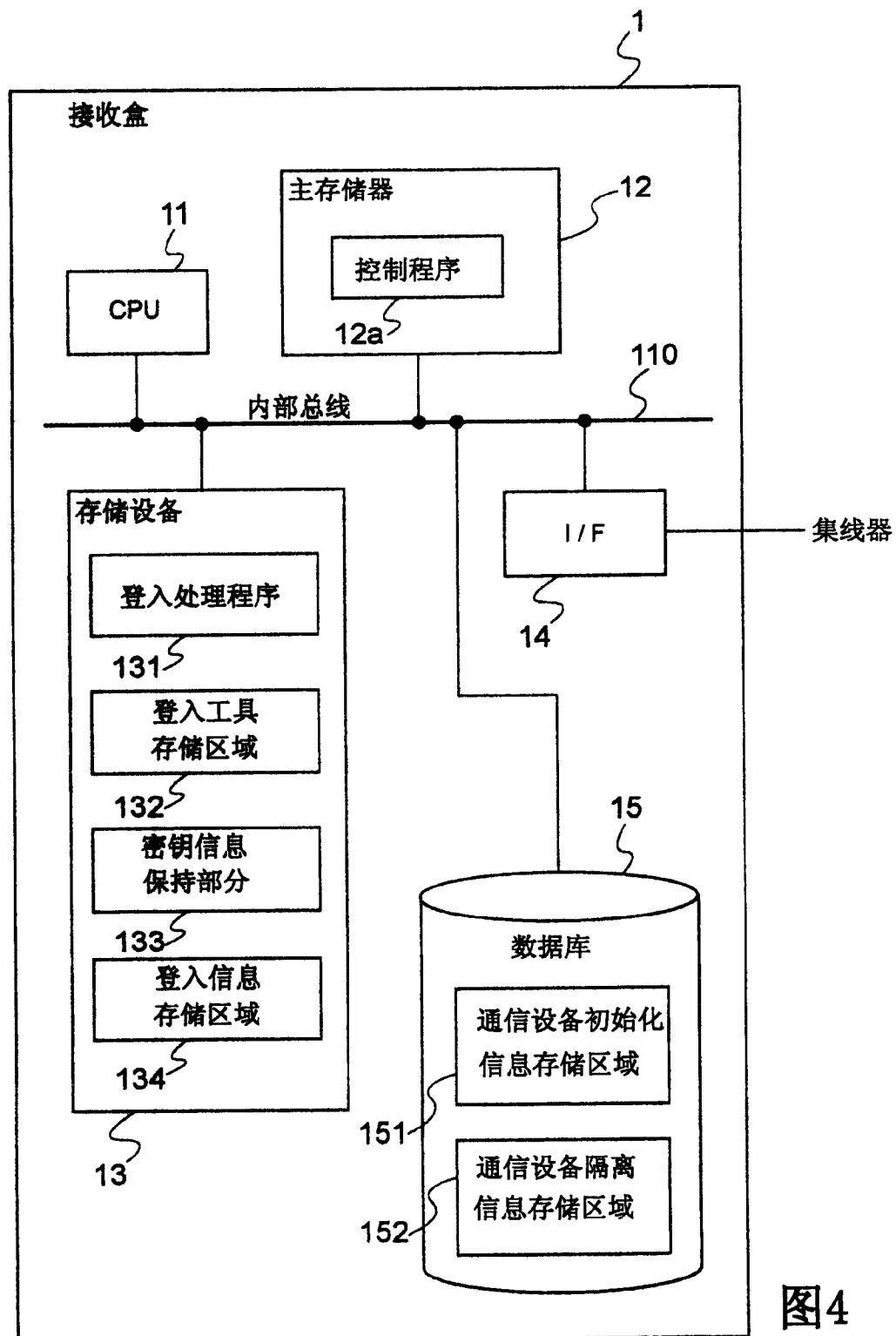


图4

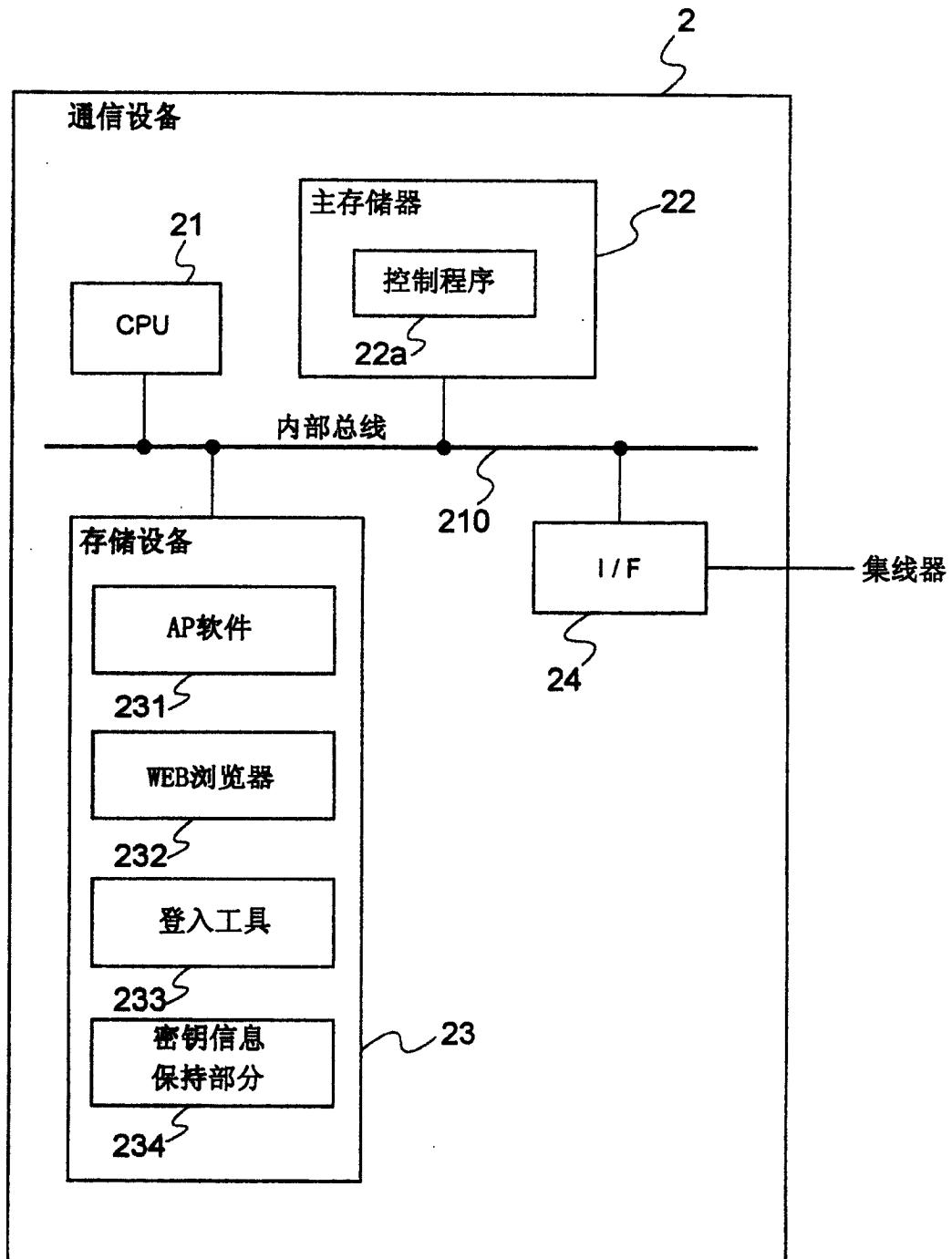


图 5

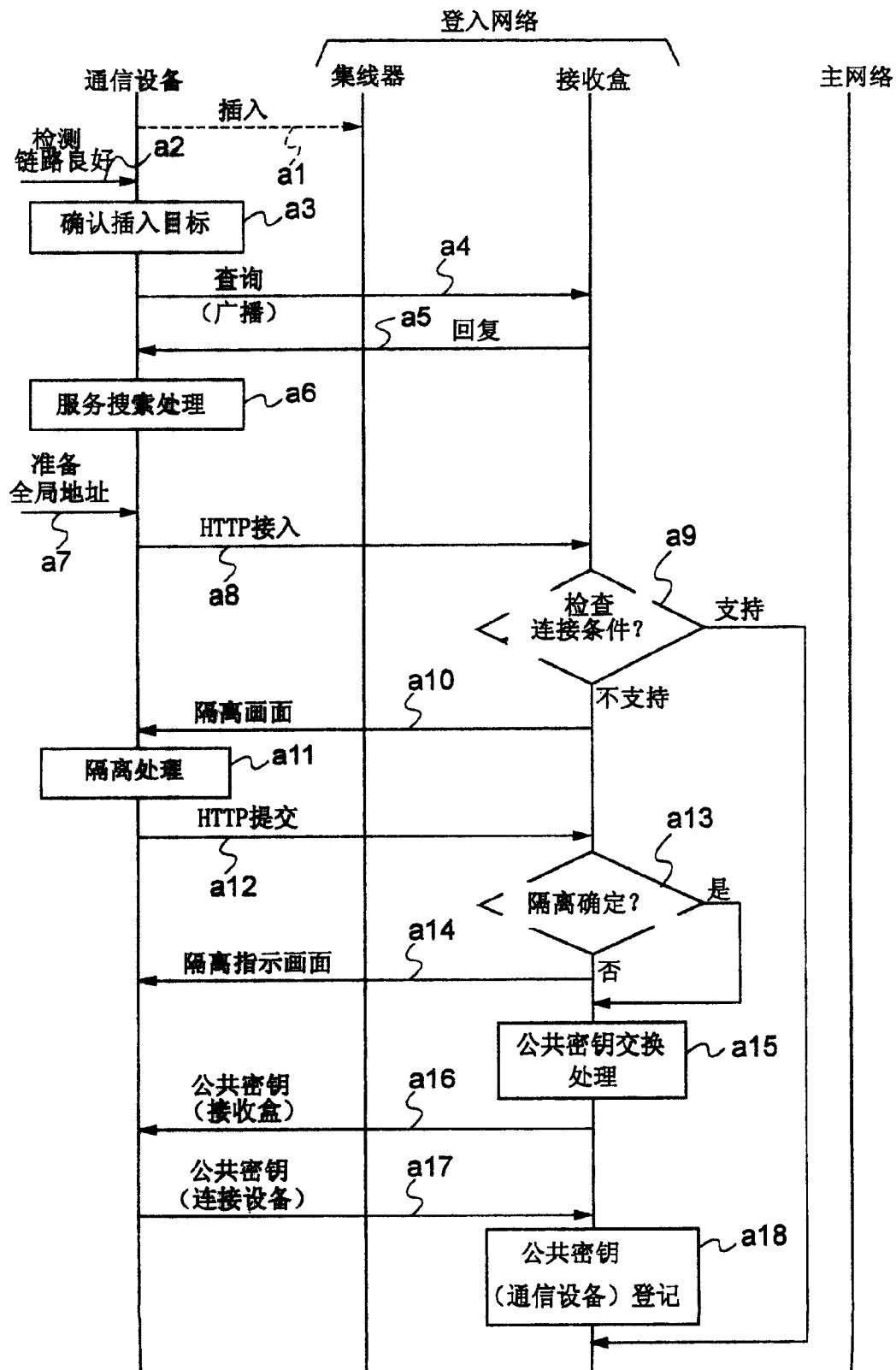


图 6

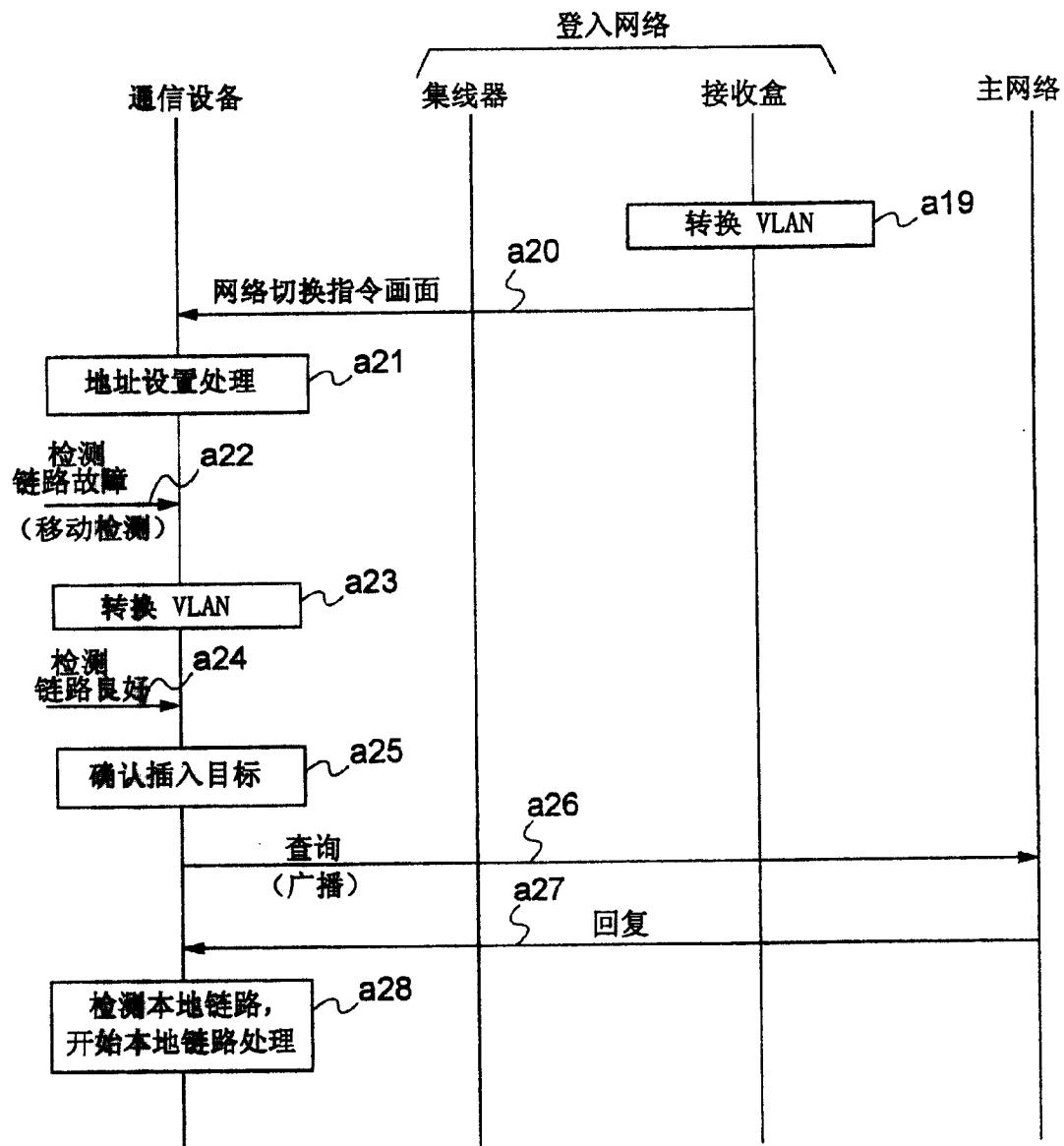


图 7

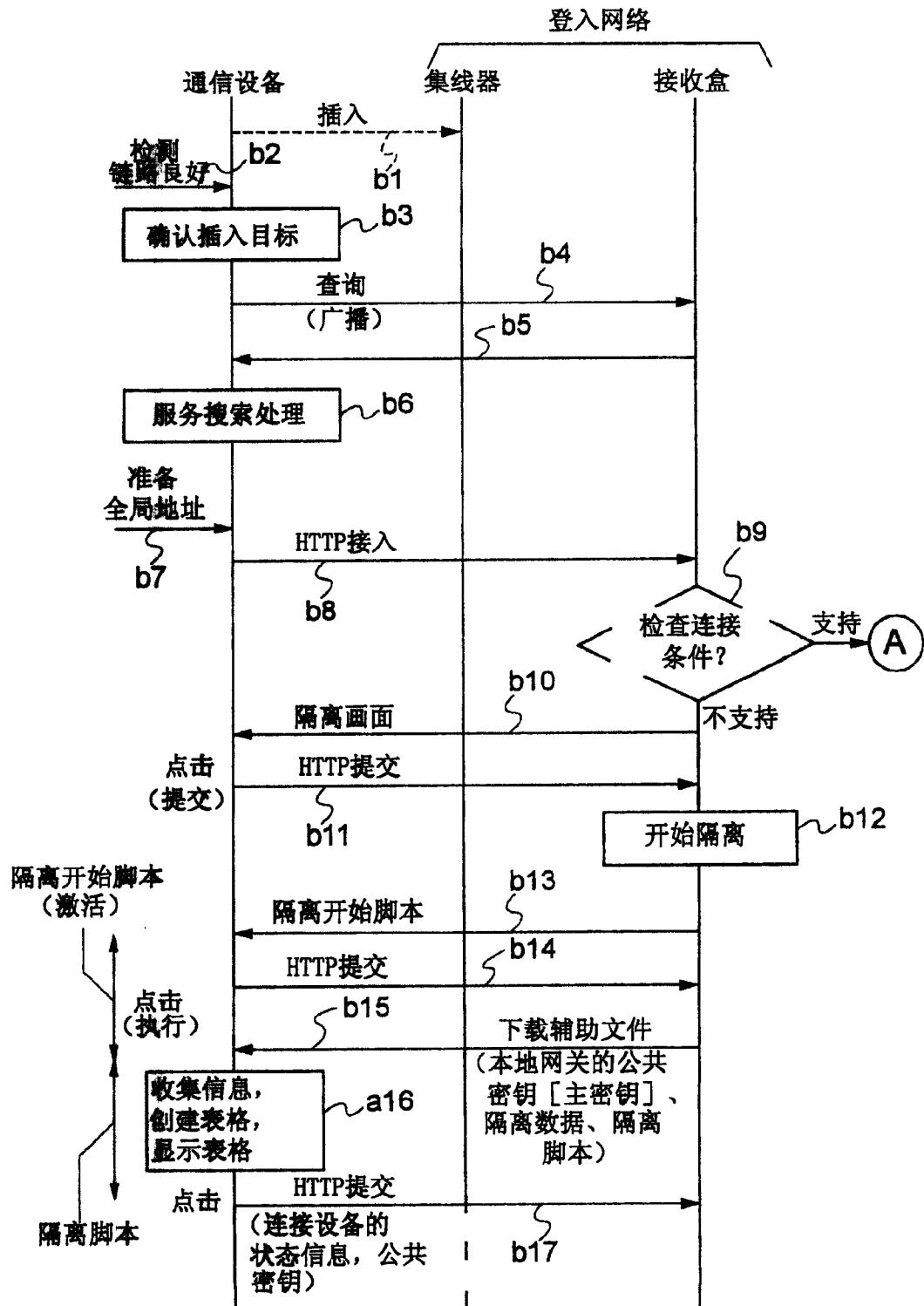


图 8

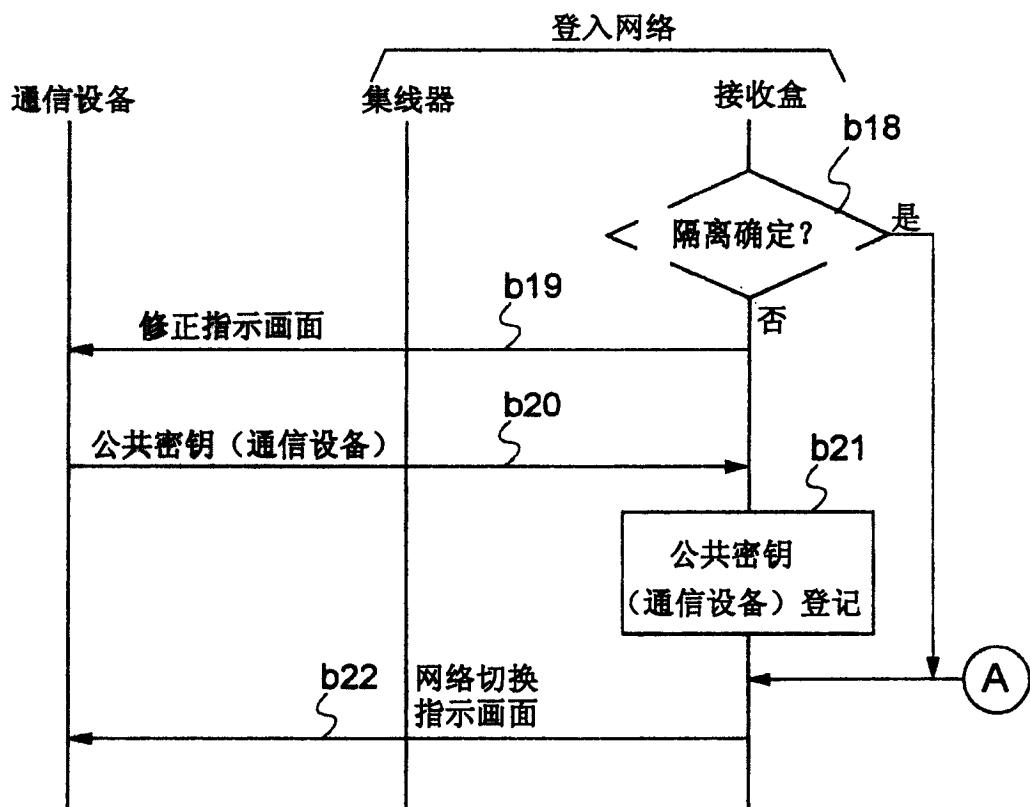


图 9

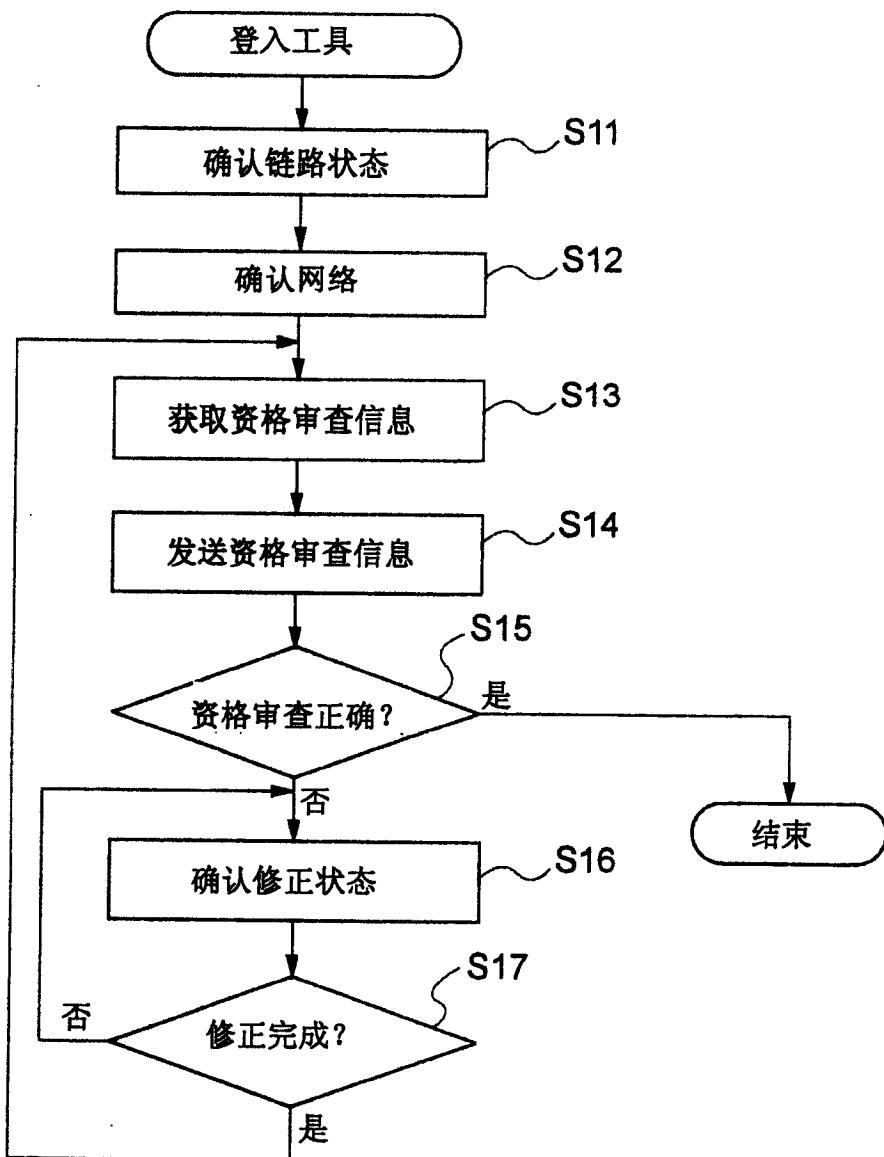


图 10

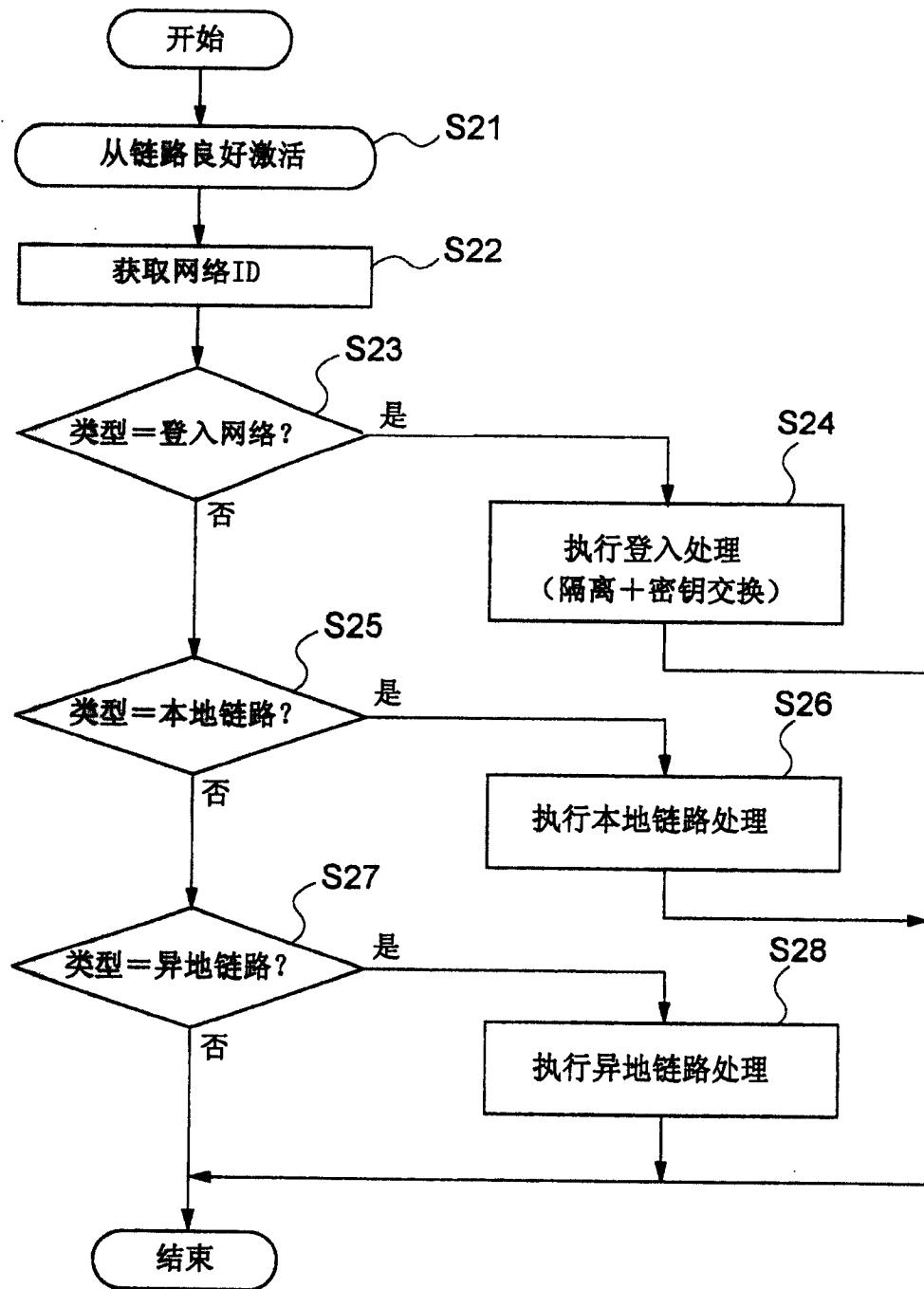


图 11

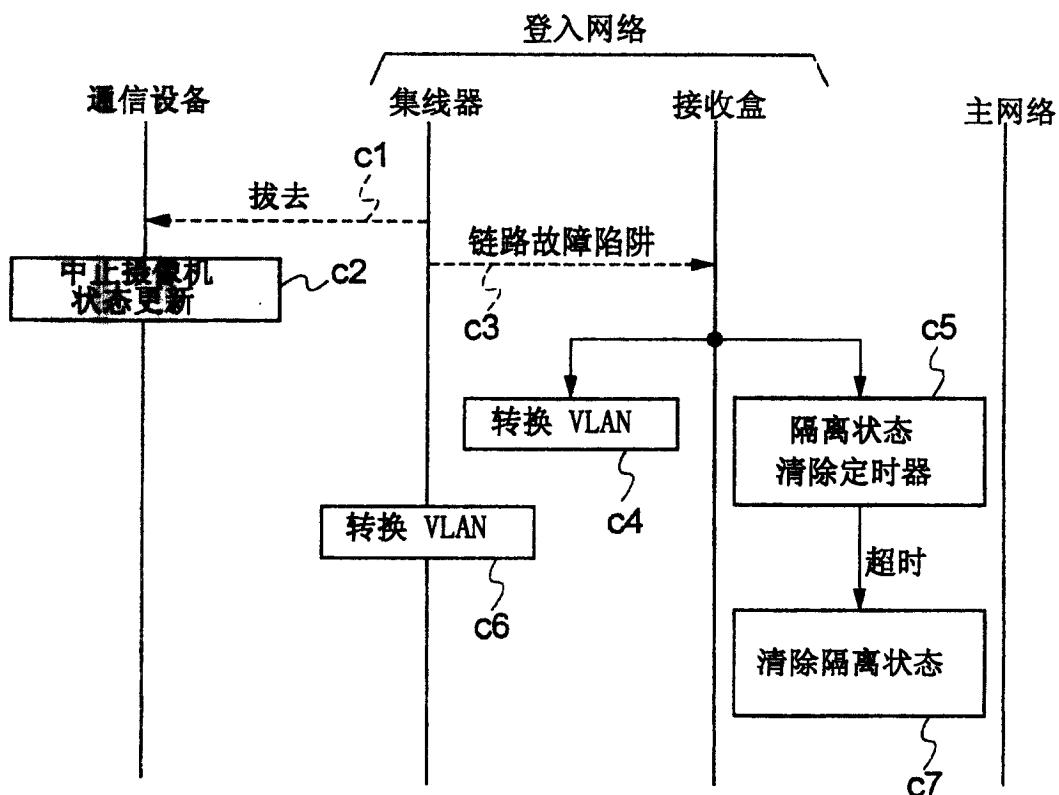
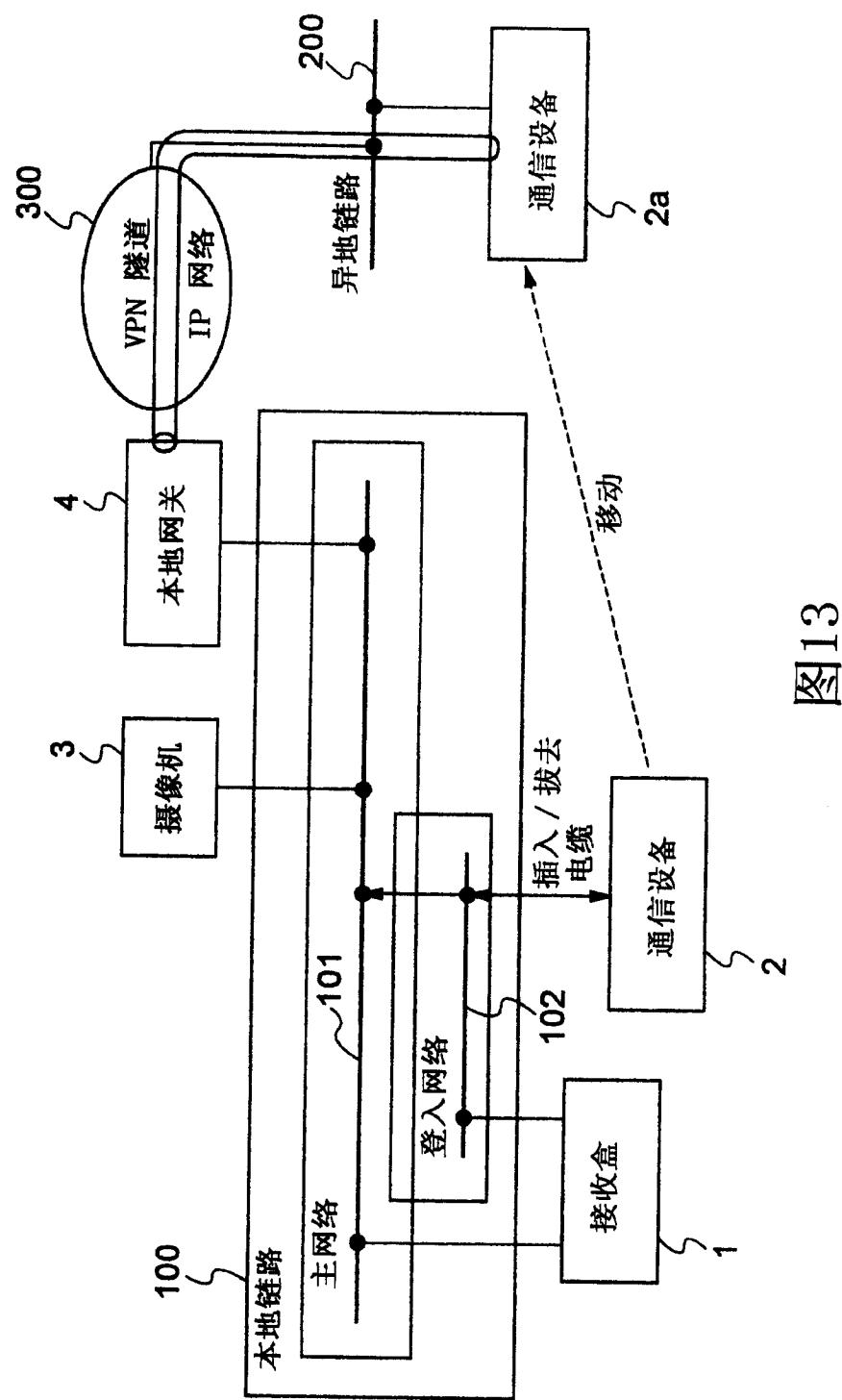


图 12



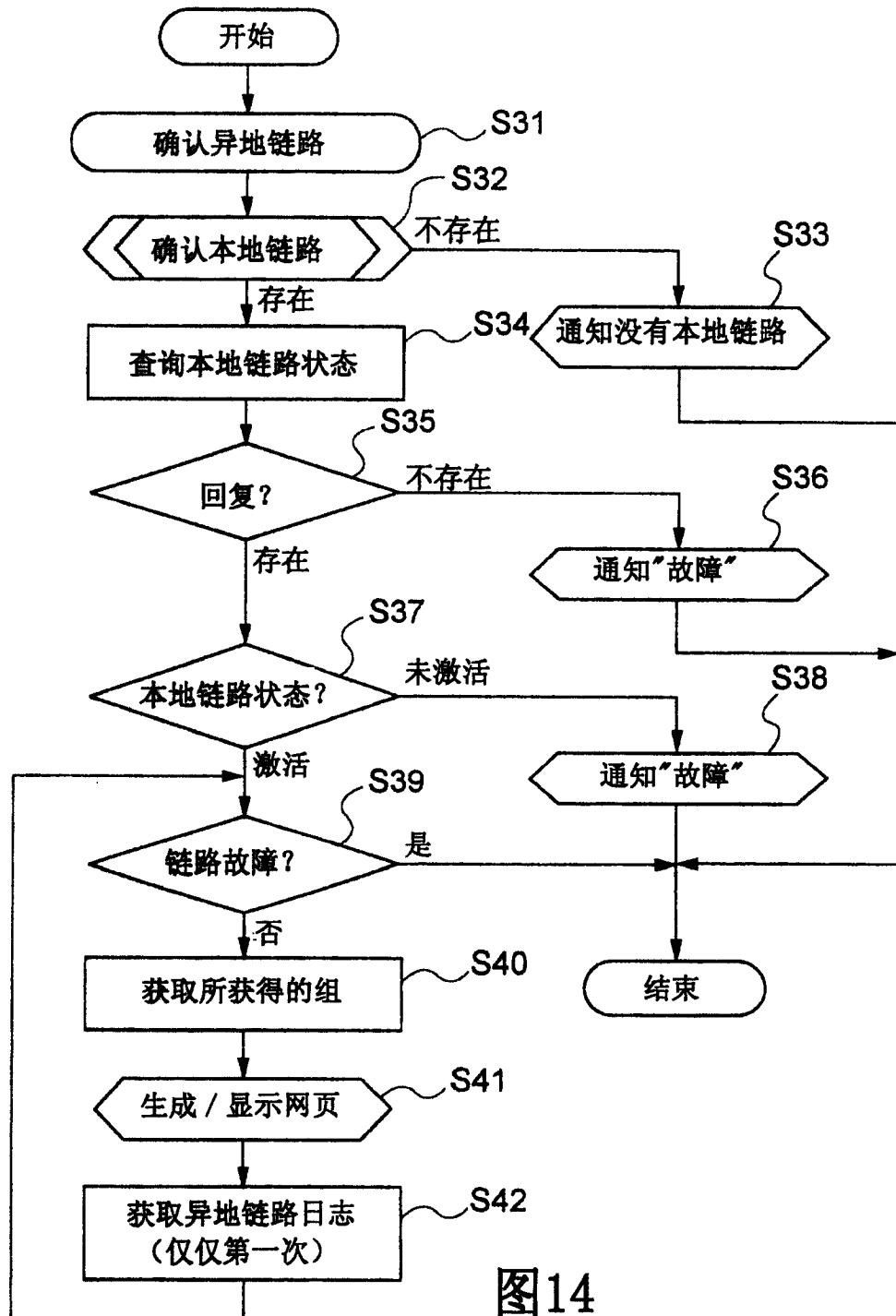


图14

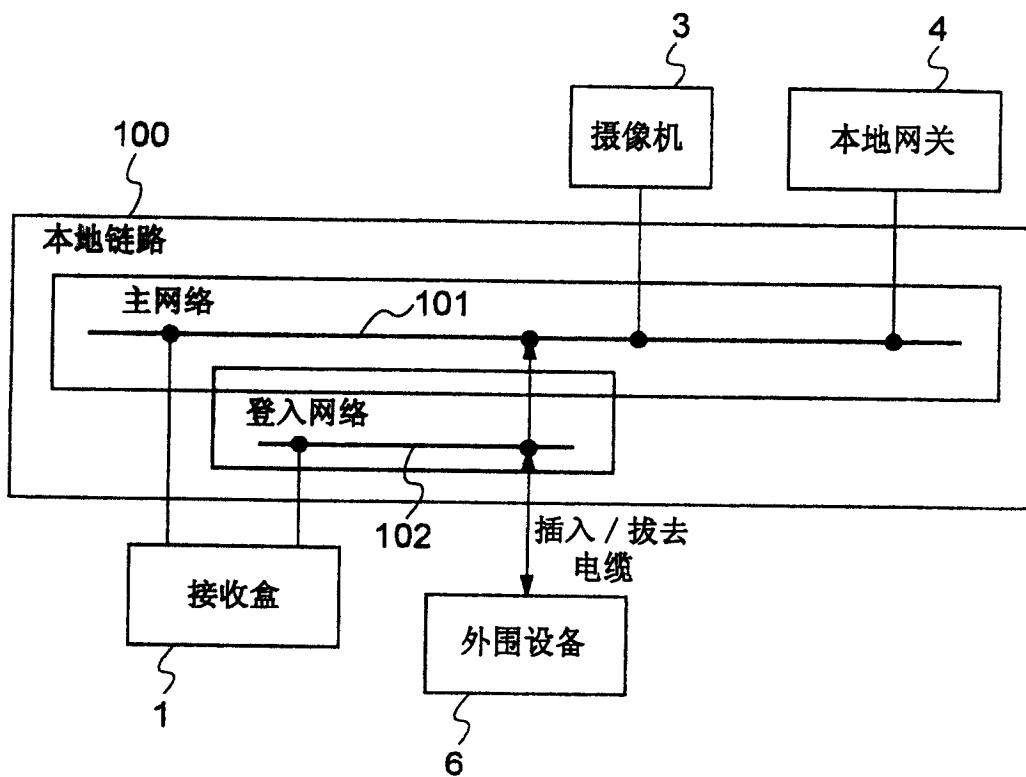


图 15

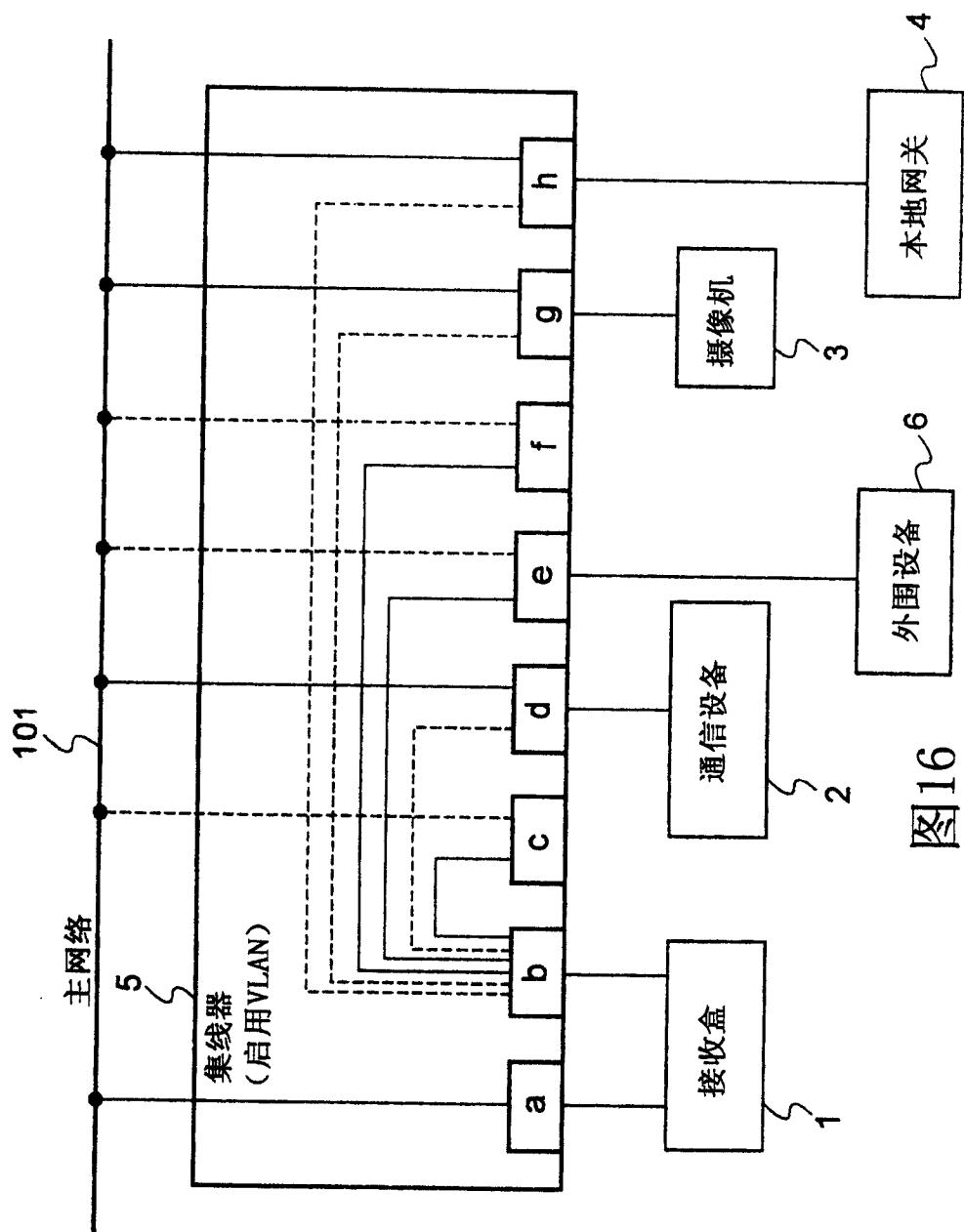


图16

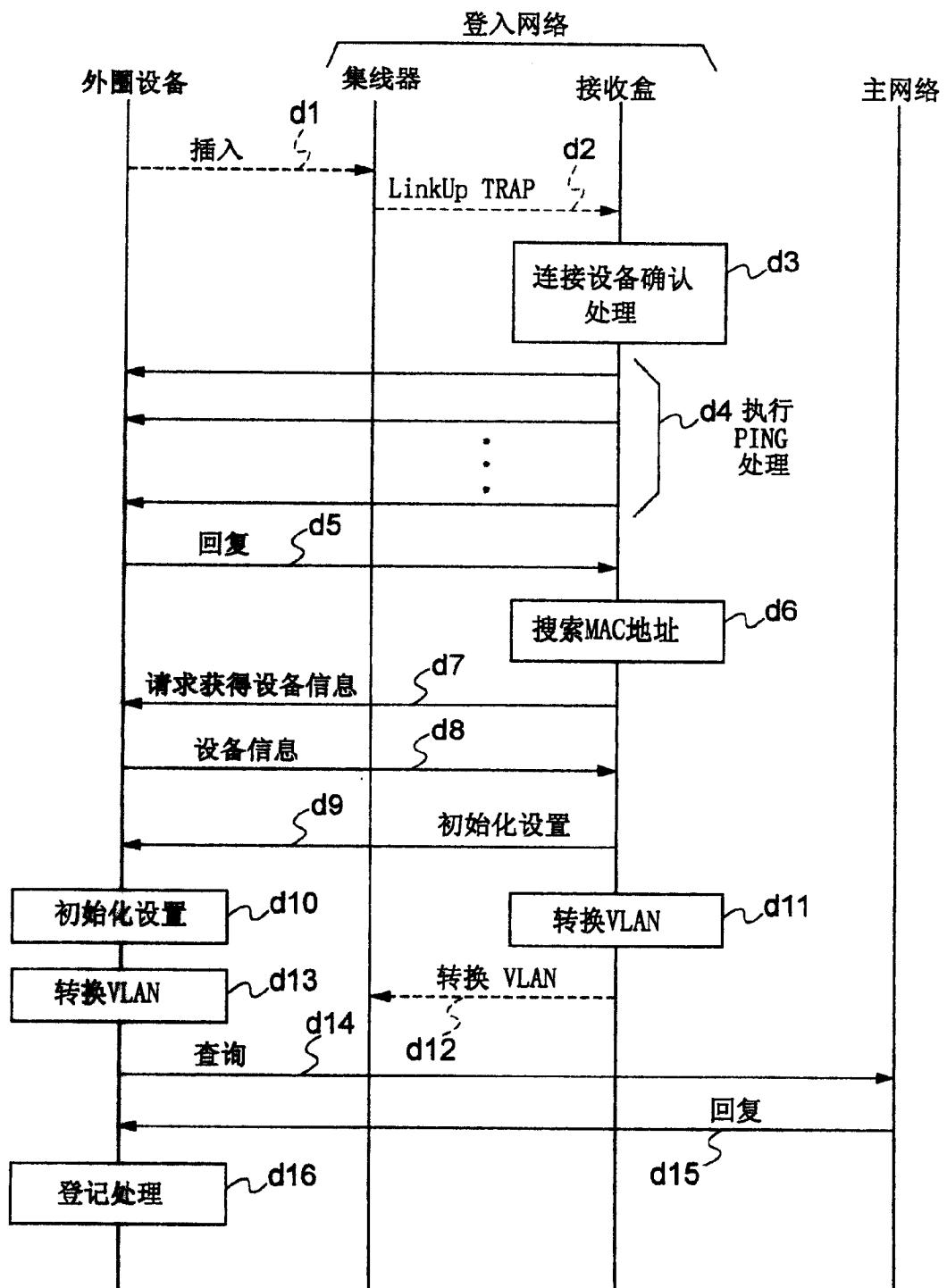


图 17

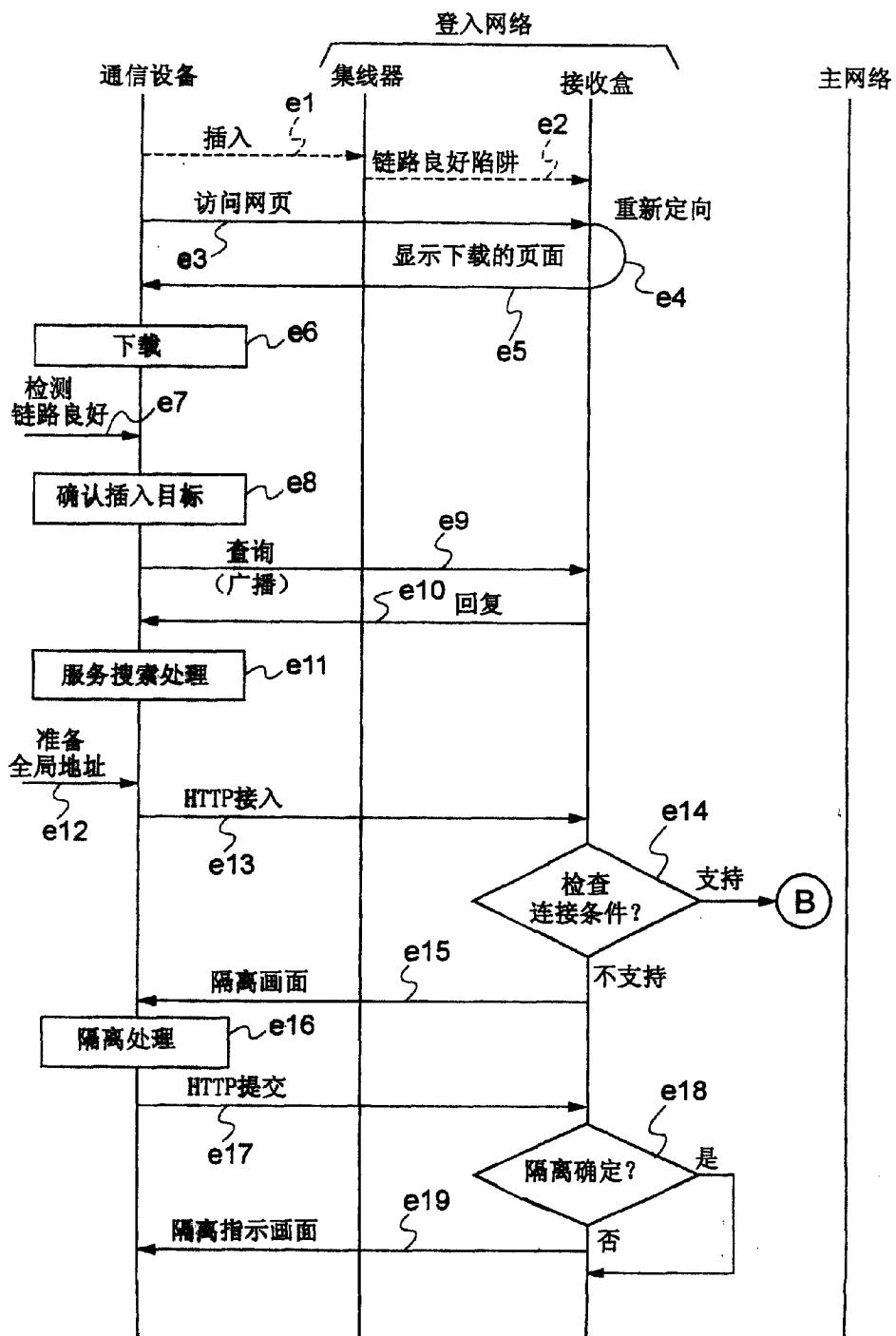


图 18

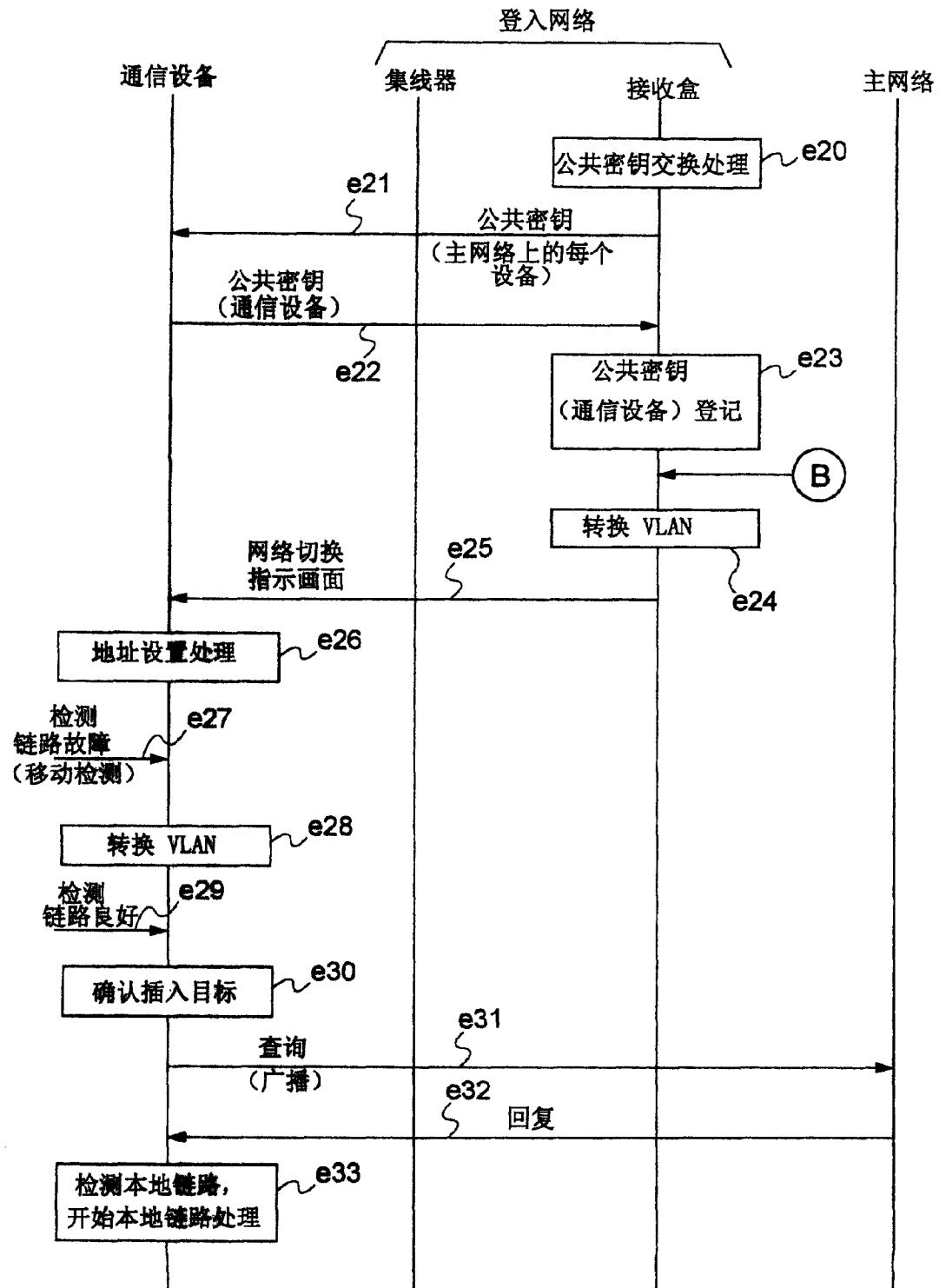


图 19

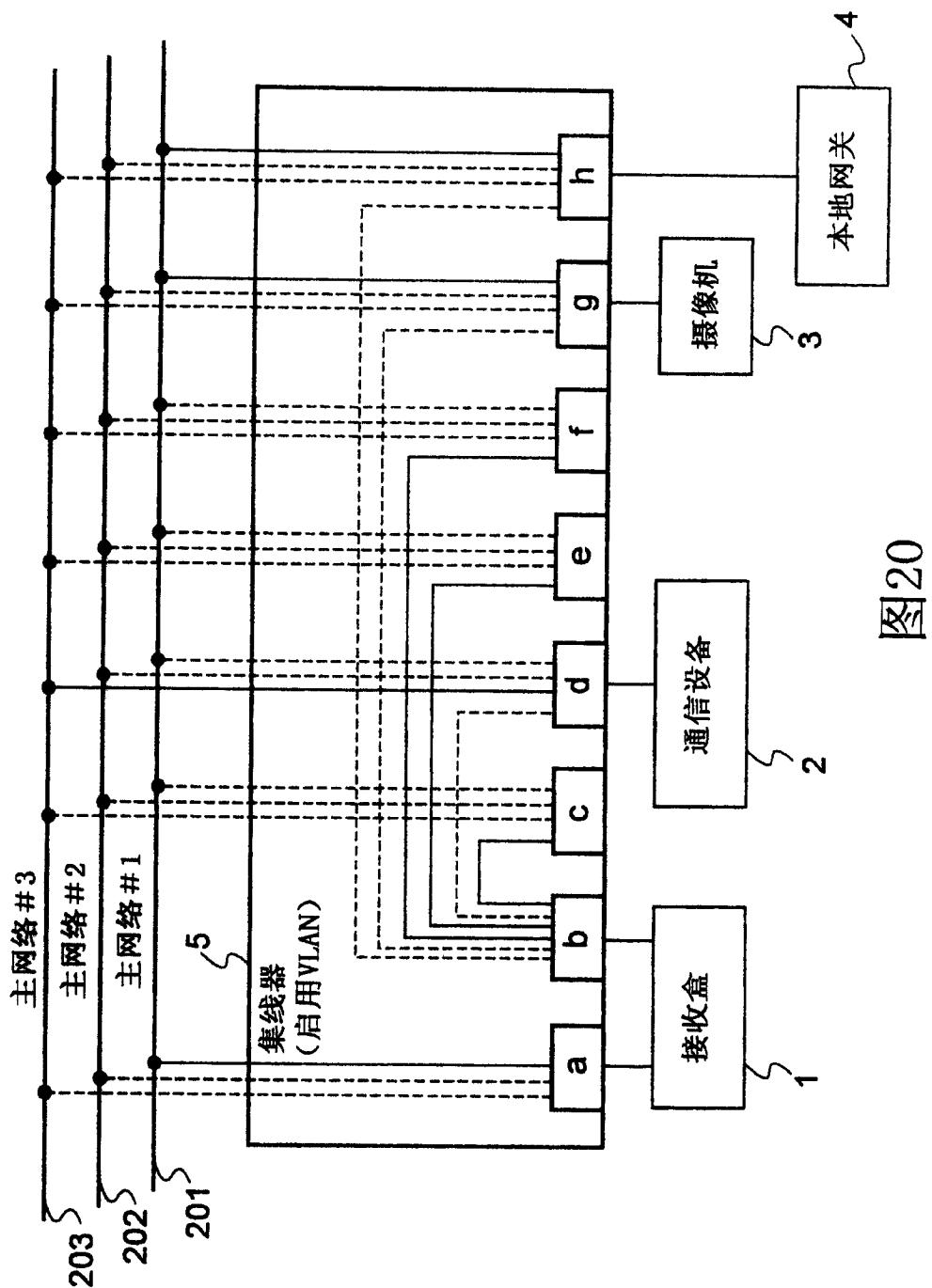


图20