



(12)发明专利

(10)授权公告号 CN 101742496 B

(45)授权公告日 2016.08.10

(21)申请号 200910221896.5

(22)申请日 2003.07.04

(30)优先权数据

60/429,714 2002.11.26 US

60/439,419 2003.01.10 US

10/417,653 2003.04.17 US

(62)分案原申请数据

03146569.2 2003.07.04

(73)专利权人 思科技术公司

地址 美国加利福尼亚州

(72)发明人 南希·卡姆·温盖特

罗伯特·C·迈耶

维克托·J·格里斯沃尔德

道格拉斯·A·史密斯

理查德·D·雷博

(74)专利代理机构 北京东方亿思知识产权代理
有限责任公司 11258

代理人 李晓冬 南霆

(51)Int.Cl.

H04W 12/04(2009.01)

H04W 12/06(2009.01)

H04W 36/00(2009.01)

审查员 李荣娟

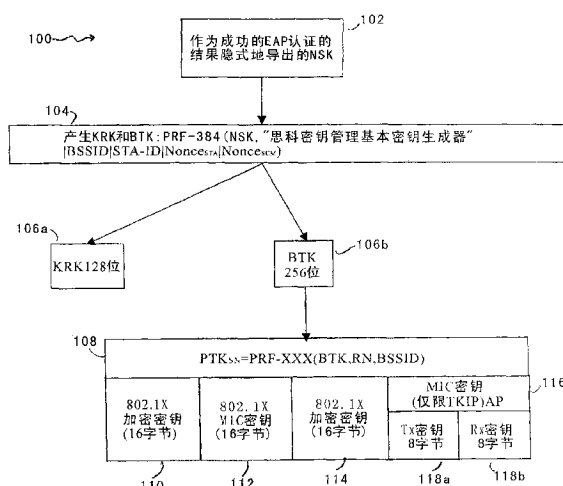
权利要求书1页 说明书113页 附图26页

(54)发明名称

在分层无线网络中提供安全无线网络通信的方法

(57)摘要

公开了在分层无线网络中提供安全无线网络通信的方法和装置。本发明公开了用于处理无线网络中漫游的移动节点的方法和系统。系统使用在移动节点被最初认证时所建立的子网上下文管理器为移动节点存储当前网络会话密钥、安全策略和会话的持续时间(例如会话超时时间)。从网络会话密钥中导出成对瞬时密钥。子网上下文管理器处理随后的重关联请求。当移动节点漫游到新的接入点时,该接入点从子网上下文管理器获取网络会话密钥,并通过从网络会话密钥中计算新的成对瞬时密钥来确认该移动节点。



1. 一种用于在分层无线网络中提供安全无线网络通信的方法,包括:
向基础结构认证者认证基础结构节点,其中所述基础结构节点具有多个后代节点;
在所述基础结构节点和所述基础结构认证者之间建立上下文传递密钥;
与处于从所述基础结构节点和所述基础结构认证者的路径上的祖先节点建立上下文传递密钥;
沿着所述路径实例为所述多个后代节点之中的解除注册的后代节点发送解除注册请求;
所述解除注册的后代节点作为响应为所述解除注册的后代节点删除所述路径实例;并且
所述多个后代节点之中在所述路径实例中处于所述基础结构节点和所述解除注册的后代节点之间的每个节点作为响应为所述解除注册的后代节点删除所述路径实例。
2. 如权利要求1所述的方法,其中,所述基础结构节点是对一响应者节点的上下文请求的发起者,该响应者节点不是所述基础结构节点的祖先节点,所述方法还包括:
确定所述发起者和所述响应者之间的共同祖先节点;
从所述共同祖先节点接收用于所述响应者的横向上下文传递密钥;
利用所述横向上下文传递密钥来产生消息完整性检验;并且
向所述响应者发送上下文请求,其中该上下文请求包括所述消息完整性检验。
3. 如权利要求2所述的方法,其中,所述上下文请求还包括所述共同祖先节点的节点标识符。
4. 如权利要求2所述的方法,还包括:
从所述共同祖先节点接收包含所述横向上下文传递密钥的票据;
其中所述上下文请求还包括所述票据。
5. 如权利要求4所述的方法,其中,所述票据被利用在所述发起者和所述共同祖先节点之间建立的上下文传递密钥来加密。
6. 如权利要求1所述的方法,其中,所述基础结构节点是对来自一发起者的上下文请求的响应者,该发起者不是该响应者的祖先节点,所述方法还包括:
接收来自发起者节点的上下文请求消息;
利用所述响应者与共同祖先节点建立的上下文传递密钥来从上下文请求消息中提取横向上下文密钥;并且
利用所述横向上下文请求密钥来认证所述消息。
7. 如权利要求6所述的方法,还包括发送对所述上下文请求消息的应答,该应答被利用所述响应者与所述共同祖先节点建立的上下文传递密钥来加以认证。

在分层无线网络中提供安全无线网络通信的方法

[0001] 本申请是2003年7月4日递交的发明名称为“利用密钥重认证漫游移动节点的方法和装置”、申请号为03146569.2的专利申请的分案申请。

技术领域

[0002] 本发明一般地涉及无线网络,特别涉及当设备在接入点之间漫游时用于认证和接通无线设备的方法和系统。

背景技术

[0003] 大多数现有的802.11网络级认证协议在无线台站从一个接入点(AP)漫游到另一个接入点后需要大量的时间重新建立该台站到网络的连接。一般地,当台站和第一接入点关联时,它必须通过中心认证服务器得到认证。当台站漫游到新接入点时,该台站失去和网络的会话并且必须再次用认证服务器认证它自身,这一般涉及一个完整的质询请求和响应。然后,建立起新的记帐会话。此方法引入了一个新的密钥层次结构,该层次结构开始初始认证并允许认证密钥在和与802.11链路相对的网络的会话期间保留。此外,这个新密钥层次结构基于计数器模式密钥产生,以允许802.11密钥的预先计算,避免了对不必要的会话拆除和重启的需要。

[0004] 在重新建立连接上的延迟大大地影响了802.11服务,达到例如IP电话(VoIP)的一些上层协议事实上失效的程度。此外,每次漫游通常要求和一个站点的认证、记帐和授权(AAA)服务器的相互作用,导致服务器负载的明显增大,达到一些服务器不能给802.11台站提供必须的认证请求速率的程度。更重要的是,在认证成功以后,802.11台站必须使用在认证时所提供的密钥来建立新生密钥,用于保护与接入点的802.11链路。

[0005] 这样,当台站从一个接入点漫游到另一个时,存在对用于认证和接通台站的快速、安全和可靠的方法的需求,该方法减少到认证服务器的业务量并优化新生的802.11密钥的产生。在设计用于在接入点之间无缝漫游台站的快速、安全和可靠的方法时,需要下列基本假设和要求:

[0006] 1)速越区切换必须将MN和AP之间的消息处理和计算减到最少

[0007] 2)快速越区切换仅在子网内的移动中受到影响,尽管建立了基础结构以顾及到将来对子网间移动的支持

[0008] 3)越区切换必须安全

[0009] 4)总体设计必须最大限度地在现有标准之间寻求平衡

[0010] 5)总体设计决不能和现有协议冲突

[0011] 6)越区切换机制基于密钥管理,因此独立于认证机制。但是注意,任何密钥管理机制必须知晓所选择的认证类型,因为它必须知道如何恰当地检索和翻译(未示出)

[0012] 7)越区切换机制依靠集中服务提供安全的密钥分配服务

[0013] 当前的认证协议,诸如PEAP或TLS需要和认证状态的相互作用。PEAP声称具有通过影响恢复操作,允许MN绕过完整的质询-响应认证交换来减少漫游时间的能力。IEEE

802.11安全任务组‘i’例如TGi已经提供了预认证的方法。这两个机制假设了在AP和MN之间的链路可以建立用于保护802.11和802.1X业务的成对瞬时密钥(PTK)之前重建网络会话密钥(NSK)的要求。但是,利用已定义的密钥层次结构,TGi还暗示了把NSK从一个AP传递到另一个的能力。此设计还使用了保留NSK的概念并只依靠密钥管理机制在漫游期间影响快速越区切换。但是,为了给每个接入点提供会话密钥的新生性和唯一性,CCKM定义一个初始的已认证密钥交换,通过此交换,MN和第一关联AP提供了用于获得用来认证密钥请求的新生密钥KRK和用来获得PTK的基本瞬时密钥BTK的材料。

[0014] 下面是在整个本说明书中所用的缩写及其相应定义列表:

[0015] AKM-已认证密钥管理(Authenticated Key Management)

[0016] AP-接入点(Access Point)

[0017] AS-认证服务器(Authentication server)

[0018] BSSID-基本服务组标识符(Basic Service Set Identifier)

[0019] BTK-基本瞬时密钥(Base Transient Key)

[0020] CCKM-中心密钥管理(Central Key Management)

[0021] CCM-校园上下文管理器(Campus Context Manager)

[0022] CCX-客户使能(Client Enablement)

[0023] CTK-上下文传递密钥(Context Transfer Key)

[0024] GTK-组瞬时密钥(Group Transient Key)

[0025] KRK-密钥请求密钥(Key Request Key)

[0026] MN-移动节点(Mobile Node)

[0027] MN-ID-移动节点标识符(Mobile Node Identifier)

[0028] NSK-网络会话密钥(network session key)

[0029] PRF-伪随机函数(PseudoRandom Function)

[0030] PMK-成对主密钥(Pairwise Master Key)

[0031] PTK-成对瞬时密钥(pairwise transient key)

[0032] RN-重定密钥请求序列号(rekey request sequence number)

[0033] SCM-子网上下文管理器(Subnet Context Manager)

[0034] SSID-服务组标识符(Service Set Identifier)

[0035] SSN-简单安全网络(Simple Security Network)

[0036] VLAN-虚拟局域网(Virtual Local Area Network)

[0037] WLCCP-本地无线上下文控制协议(Wireless Local ContextControl Protocol)

[0038] 和前述缩写一起,下面定义了在整个本申请中出现的术语的定义:

[0039] IEEE——电气电子工程师协会(Institute of Electrical and Electronics Engineers, Inc)

[0040] IEEE 802.11——802.11协议和802.11术语在1999年版的IEEE Std 802.11中定义。

[0041] IEEE 802.11 TGi——IEEE 802.11中一个当前集中于处理802.11安全性的任务组。

[0042] 802地址(address)——一个规范的IEEE 48位“以太网地址”。802.11和以太网地

址是802地址

[0043] 802.11网桥(bridge)——802.11网桥是具有以太网网桥端口和一个或多个802.11网桥端口的透明网桥。802.11双亲网桥具有连接到802.11子网桥内的802.11基本端口的802.11次级端口。

[0044] 802.11台站(station)——一个MN或AP。

[0045] 802.1X——IEEE 802.1X协议和802.1X术语在[]中定义。802.1X定义了802.1X申请者 and 802.1X认证者通过认证服务器相互认证的协议。

[0046] AAA——认证授权记帐。节点将通过提供用于提供认证、授权和会话记帐的协议和服务的认证服务器(一般如此)执行协议来请求网络接入。

[0047] AKM——已认证密钥管理。在SSN和TG1协商元件中的新选择器,在信标(beacons),探测响应和重关联(reassociation)请求/响应消息中存在。这个选择器考虑到了认证类型和密钥管理的定义。

[0048] AP——接入点。在此文档中,“AP”用作一般性术语,指任何802.11到以太网或802.11到802.11的中继设备。

[0049] 关联消息(Association Message)——802.11台站发送关联请求消息以便最初与一个双亲AP相连。双亲AP用关联响应消息应答。

[0050] AS——认证服务器。提供AAA(尤其是认证)服务的节点。

[0051] BDPU——802.1D网桥协议数据单元

[0052] BSS——802.11基本服务组。BSS是与单个802.11 AP关联的802.11台站的集合。

[0053] 基本瞬时密钥(Base Transient Key)(BTK)——在MN和SCM之间相互导出以用来产生PTK的密钥的基本瞬时密钥。

[0054] 校园网(Campus Network)——表示可能包含一个或多个802.11扩展服务组的地理位置的总的“无缝漫游域”。物理的校园网可以包含多个“校园网”。

[0055] 中心密钥管理(Central Key Management)(CCKM)——本发明的密钥管理方案,它采用中心节点,即一个AP作为使能链路(例如AP和MN)之间受保护的通信的密钥分配器。

[0056] 上下文传递密钥(Context Transfer Key)(CTK)——在两个节点之间共享以建立其数据分组的保护的密钥。如果保护机制针对每个加密和分组认证(例如MIC)需要唯一的密钥,则CTK可以由一对密钥组成。

[0057] 对端主机(Correspondent Host)(CH)——与MN进行主动通信的移动或非移动节点。

[0058] 后代(Descendant)-位于根在祖先节点的拓扑树的子树中的节点。

[0059] DRR——后代注册记录。DRR包含后代节点的状态信息。MN-DRR是移动节点的DRR, AP-DRR是AP的DRR。

[0060] DPR——后代路径记录(DPR)。PR包含后代节点的路径状态信息。

[0061] 下行链路(link)——从802.11 AP无线电设备到802.11子台站的逻辑无线电路径。

[0062] ESS——802.11扩展服务组。ESS包括一个或多个BSS并可以跨越一个或多个子网。在ESS中,MN能在AP之间漫游。SWAN校园网可以包括多个ESS。

[0063] FA——移动Ipv4外部代理

- [0064] 群瞬时密钥(Group Transient Key)(GTK)——AP所拥有和管理的密钥。它被用于保护多播和广播业务。
- [0065] HA——移动Ipv4本地代理
- [0066] 跳路由(Hopwise Routing)——当进入或离开的WLCCP消息必须被转发到在从发起者到响应者的路径上的中间AP时,使用“跳路由”
- [0067] IA——基础结构节点认证者。在独立模式中,SCM就是IA;在完整的SWAN结构中,CCM是IA。
- [0068] IGMP——互联网群管理协议。IGMP用于确定IP多播群成员资格。
- [0069] IGMP监听(Snooping)——交换机和AP“监听”在端口上接收的IGMP消息,用于确定在端口上必须传送哪些IP多播地址。
- [0070] 进入(Inbound)——在SWAN拓扑树中“进入帧”被转发到CCM。通过“基本端口”访问“进入节点”(“进入节点”不一定是“祖先节点”。)
- [0071] IN——基础结构节点。IN是AP、SCM、LCM或CCM。
- [0072] IRR——进入注册记录。
- [0073] KDC——密钥分配中心。这是由IN认证器提供的对注册的基础结构节点所要消耗的CTK进行分配的服务。
- [0074] 密钥请求密钥(Key Request Key)(KRK)——扩展的NSK用来认证密钥刷新请求/响应握手的一部分。
- [0075] 层2——数据链路层,如ISO七分层模型中定义的那样。
- [0076] L-CTK——横向上下文传递密钥。
- [0077] 链路(Link)——在SWAN拓扑树中两个紧邻的邻居之间的逻辑连接。
- [0078] 链路状态(Link State)——每个SWAN节点都负责监控通向其紧邻的邻居的链路。该链路状态可以是“连接的”或“断开的”。
- [0079] MIP——如RFC 2002中所定义的移动Ipv4。
- [0080] MN——802.11移动节点。
- [0081] MN-ID——用节点的MAC地址表示的802.11移动节点标识符。
- [0082] 网络会话密钥(Network Session Key)(NSK)——由节点和其认证者之间成功的认证所建立的密钥。CCM是所有基础结构节点的认证者,而LCM是所有MN的认证者。在SCM以独立模式活动的情况下,SCM是所有节点的认证者。
- [0083] MNR——移动节点记录。移动节点记录包含MN的状态信息。
- [0084] 移动绑定(Mobility bindings)——台站的“移动绑定”用于确定到该台站的当前路径。AP,上下文管理器和MIP代理维持802.11台站的移动绑定。
- [0085] MSC——消息序列计数器。这是有效的RC4 IV和重放保护器。
- [0086] Native VLAN ID——交换机端口和/或AP能够用“本地VLAN ID”来配置。未标记或优先标记的帧和本地VLAN ID隐式地关联。
- [0087] 网络接入标识符(Network Access Identifier)(NAI)——NAI用于标识网络域内的用户。例如,joe@cisco.com是一个典型的NAI。
- [0088] NSK——网络会话密钥。NSK是由节点和其认证者之间的成功认证所建立的密钥。(CCM是所有基础结构节点的认证者,而LCM是所有校园网的认证者。在独立子网域内,SCM是

该子网内所有节点的认证者。)

[0089] 发起者(Originator)——“发起”WLCCP“请求”消息的节点。

[0090] 离开(Outbound)——在SWAN拓扑树中,“离开帧”被从CCM转发出去。“离开节点”是SWAN拓扑树中距CCM相对更远的“后代”节点。

[0091] OMNR——离开移动节点记录。

[0092] 成对主密钥(Pairwise Master Key)(PMK)——由成功的认证所建立的密钥。这是在TGi和SSN规范草案中都使用的术语并且是用来导出PTK的密钥。

[0093] 成对瞬时密钥(Pairwise Transient Key)(PTK)——由AP和MN相互导出的密钥,并且是BTK和RN的函数。

[0094] 路径认证(Path Authentication)——路径认证是指AP或子CM相互认证和与其每个祖先建立路径CTK的过程。Path-Init和(任选地)初始注册消息被用于路径认证。

[0095] 端口(Port)——提供对SWAN拓扑树“链路”访问的逻辑实体。在单个硬件接口上可以存在多个逻辑端口。

[0096] PNR——双亲节点记录。

[0097] 基本LAN(Primary LAN)——直接连接到SCM的有线以太网LAN。每个子网具有一个基本以太网LAN。基本LAN可以包括多个以太网段和有线透明网桥/交换机。

[0098] 基本端口(Primary Port)——用于连接到SWAN拓扑树的端口。在SCM中,它是用于访问双亲LCM或CCM的端口。在AP中,它是用于向基本LAN发送帧的端口。AP基本端口可以是以太网或802.11端口。AP基本端口是用于单播泛滥目的的“缺省端口”(如果AP和SCM共存,则在AP和SCM之间存在逻辑内部链路。逻辑AP“内部基本端口”提供对SCM的访问;但是,以太网端口仍为用于帧转发目的的“基本端口”。)

[0099] PTK——成对瞬时密钥。该密钥用来保护MN和AP之间的802.1X和802.11数据分组。PTK由链路中的每一个节点根据预定义的强伪随机函数、BSSID、RN和BTK相互导出。

[0100] 重关联消息(Reassociation Message)——802.11台站发送802.11重关联请求消息以便在其漫游后与新的双亲AP关联。双亲AP用重关联响应消息应答。

[0101] 重定密钥请求号(Rekey Request Number)(RN)——用于保护PTK 密钥刷新免受重放攻击的计数器。

[0102] 转发器(Repeater)——转发器是与802.11基本端口上的双亲AP相连接的“无线AP”。

[0103] RN——请求号。用于循环移位在认证的MN和根AP之间所使用的PTK的序列值

[0104] 根AP(Root AP)——“根AP”在基本LAN的基本以太网端口上与基本LAN直接连接。

[0105] 根CM(Root CM)——在活动的SWAN拓扑树的根处的CM。在校园网中,CCM是根CM。在“独立”子网控制域中SCM是根CM。

[0106] 响应者Responder——WLCCP请求消息的目的地或发起WLCCP应答消息的节点

[0107] SARpM——SCM通告应答消息

[0108] SCM——子网上下文管理器。SCM给每一个子网提供中心控制点。SCM给每个子网建立“基本LAN”。从MN的观点,本地SCM是用于MN的本地子网的SCM,外部SCM是在任何其他“外部子网”上的SCM。

[0109] 无缝漫游(Seamless roaming)——如果MN在位于不同子网中的AP之间漫游而不

改变其“本地IP地址”，则它被说成是“无缝地”漫游。

[0110] 次级LAN(Secondary LAN)——任何通过无线链路连接到基本以太网LAN的有线以太网LAN。次级LAN可以包括多个以太网段和有线透明网桥/交换机。

[0111] 次级端口(Secondary Port)——次级端口是除了基本端口之外的任何活动的AP或CM端口。

[0112] SSID——802.11服务组标识符。认证参数为每个SSID都进行全局定义。在每个AP中,SSID可以被本地绑定到“本地子网”或VLAN。

[0113] 简单安全网络(Simple Security Network)(SSN)——有关用来提供802.11安全性框架的Microsoft规范。它要求使用802.1X EAP认证、TKIP和Microsoft用于管理单播密钥的802.1X四路握手和用于管理广播和多播密钥的802.1X双路握手。

[0114] STP——IEEE802.1D生成树协议。“STP AP”执行802.1D STP并且 802.1D STP在“STP链路”上操作。“非STP AP”不执行802.1D STP。

[0115] 子网(Subnet)——IP子网。MN在任意给定时间和单个“本地子网”关联。从MN的观点,任何其他子网是“外部子网”。

[0116] 申请者(Suppliant)——IEEE 802.1X标准定义了术语“申请者”申请者是通过认证服务器与“802.1X认证者”相互认证的节点。

[0117] SWAN——用于布网的智能无线体系结构,一种用于安全环境中无线设备、网络和移动性管理的体系结构。

[0118] SWAN拓扑树(SWAN Topology Tree)——如SWAN双亲/子关系定义的SWAN网络的逻辑结构。SWAN CCM位于拓扑树的根处。

[0119] VLAN——“虚拟LAN”,如同IEEE 802.1Q标准中所定义的那样。

[0120] TLV——类型、长度、值。“TLV’s”在WLCCP消息中包含可选参数。

[0121] 上行链路(Uplink)——从802.11子站到其双亲AP无线设备的逻辑无线路径。

[0122] URR——未绑定的注册记录。

[0123] VLAN——“虚拟LAN”,如同IEEE 802.1Q标准中所定义的那样。VLAN标记帧在VLAN主干链路上传送。

[0124] 无线台站(Wireless station)——MN、转发器、WGB或802.11子网桥。

[0125] WGB——工作组网桥是具有802.11基本端口和次级以太网端口,提供到非STP的次级以太网LAN段访问的非STP AP。

[0126] WLAN——无线LAN

[0127] WLCCP——无线LAN上下文控制协议

[0128] 除了上述缩写外,若非另外说明,来自802.11规范的缩写应该被给予其如802.11规范所定义的通常的、习惯上的含义。

发明内容

[0129] 鉴于前述需要,本发明构思了通过采用从密钥管理中去除认证会话时间的密钥层次结构,从而既减少消息也减少计算负担的方案。因为认证和密钥管理被绑定到密码套件选择,所以当前的802.11实现方式把它们紧密地捆绑在一起并实施完整的后端(重)认证。对于有线对等保密(WEP,Wired Equivalent Privacy),这可能因WEP重定密钥的要求而导

致非常频繁的(重)认证。对于漫游,当前的实现也实施完整的(重)认证。

[0130] 该密钥层次结构把建立在成功认证基础上的密钥定义为网络会话密钥(NSK),该密钥独立于802.11密码套件选择。NSK被用来产生认证密钥刷新请求的密钥刷新密钥(KRK)和用作从中导出成对瞬时密钥(PTK)的基本密钥的基本瞬时密钥(BTK)。

[0131] 只有PTK被绑定到选定的802.11密码套件,并且因此必须基于密码套件安全策略进行管理。NSK的寿命被认证服务器(AS)定义为会话超时时间,该时间现在可被定义为NSK熵随802.11协商密码套件变化的函数。人们期望积极鼓励使用可产生具有更多良好熵的动态NSK的认证类型。

[0132] 密钥由提供子网上下文管理(SCM)的中心节点管理。该SCM最好是所有MN和迫使所有MN节点隐式地注册的AP的802.1X认证者。注册过程确保注册表中的所有节点已经成功地关联、认证并使安全证书被缓存(cache)。在本申请中描述的机制被定义为中心密钥管理(CCKM),并作为如SSN/TGi草案中所定义的已认证密钥管理(AKM)信息要素中的私有值来协商。

[0133] 虽然认证机制保留不变,例如802.1X可扩展认证协议(EAP)认证,但是本设计引入了新的密钥管理方案:中心密钥管理(CCKM)。使用如这里下文所描述的SSN的IE和RSN的IE来通告和协商这种新的能力。

[0134] 本发明的一个方面是用于向网络认证移动节点的方法,步骤包括:与一个接入点关联,由该接入点使用可扩展认证协议认证所述的移动节点,并建立网络会话密钥并把该移动节点注册到网络基础结构中。网络会话密钥用于建立密钥请求密钥和基本瞬时密钥。

[0135] 在初始认证之后,网络会话密钥被发送到子网上下文管理器。本发明还构思了使用网络会话密钥来认证密钥刷新。还构思了使用网络会话密钥导出成对瞬时密钥。

[0136] 本发明的另一个方面是通过移动节点重关联的方法,步骤包括:从移动节点向一个接入点发送重关联请求,该重关联请求包括移动节点标识、重定密钥请求号和认证要素,确认该重关联请求,确认步骤包括:计算新的成对瞬时密钥,向移动节点发送响应,该响应包括认证要素,该认证要素包括:新的成对瞬时密钥和局域网上的可扩展认证协议密钥;并通过把新的成对瞬时密钥与第二计算出的成对瞬时密钥进行验证来确认响应。

[0137] 一般通过验证新的成对瞬时密钥来证实响应的有效性。该响应也可以通过验证该响应中包含的时间戳(timestamp)来验证。认证要素最好使用当前的成对瞬时密钥。确认步骤由子网上下文管理器(SCM),即一种认证服务器(AS)或接入服务器(AAA服务器)来执行。其他用于确认请求的方法包括但不限于验证重关联请求的时间戳处于可配置的值中,验证序列号大于先前值,向子网上下文管理器发送查询来证实重关联请求的有效性,其中,接入点(AP)从子网上下文管理器接收重定密钥请求号和基本瞬时密钥,并产生成对瞬时密钥(PTK)。

[0138] 本发明的另一个方面是重定密钥序列,步骤包括:计算认证要素,该认证要素包括重定密钥请求号和新的成对瞬时密钥,向响应者传送对新的成对瞬时密钥的呼叫,从响应者接收响应认证要素;并验证该响应认证要素,该响应认证要素包括新的成对瞬时密钥。重定密钥序列还可以包括发送局域网上可扩展认证协议密钥确认消息。在计算认证要素之前,重定密钥请求号增加。

[0139] 本发明的另一个方面是重定密钥序列,步骤包括:接收重定密钥请求,该请求包括

重定密钥请求号和认证要素,计算新的成对瞬时密钥;并发送一个使用新的成对瞬时密钥消息进行传送和接收的就绪信号。重定密钥请求序列还可以包括接收局域网上可扩展认证协议密钥确认消息,验证重定密钥请求号大于所缓存的重定密钥请求号,验证局域网上可扩展认证协议密钥请求的所有属性,更新所缓存的重定密钥请求号,或其组合。此外,认证要素还可以包括新的初始者成对瞬时密钥,并且该步骤还可以包括把新的成对瞬时密钥和新的初始者成对瞬时密钥进行比较。

[0140] 从下面的说明,本发明的其他目的对本领域熟练技术人员将很容易变得清晰,在下面的说明中,仅通过描述最适合实现本发明的最佳方式中的一个,示出并描述了本发明的最佳实施例。可以发现,本发明能具有其他的不同实施例并且它的一些细节能在均不偏离本发明的各种明显方面中做出修改。因此,附图和说明将在实质上被视作说明性的,而非限制性的。

附图说明

[0141] 附图被引入并构成本说明书的一部分,示出了本发明的几个方面,并和描述一起用来解释本发明的原理。附图中:

[0142] 图1是示出本发明所构思的密钥层次结构的框图;

[0143] 图2是子网上下文管理器获取网络会话密钥的表格;

[0144] 图3是示出所认证的密钥管理选择器值的表格;

[0145] 图4是示出子网上下文管理器所缓存的证书的表格;

[0146] 图5是示出由接入点缓存的证书的表格;

[0147] 图6是示出用于保护链路之间的消息的密钥的框图;

[0148] 图7A和图7B是示出AP注册到SCM的步骤的流程图;

[0149] 图8示出了成功的移动节点轻量级可扩展认证协议认证和注册的一个实例;

[0150] 图9示出了成功的移动节点非轻量级可扩展认证协议认证和注册的一个实例;

[0151] 图10A和图10B是示出在成功的认证后被触发以完成密钥建立的序列的流程图;

[0152] 图11是重定密钥序列的密钥描述符的实例;

[0153] 图12是示出重定密钥序列的框图;

[0154] 图13是包含在移动节点所发送的重关联请求中的认证要素的实例;

[0155] 图14是对接入点的重关联请求的响应的格式的实例;

[0156] 图15是示出对一个成功的移动节点重关联到新的接入点,在各种网络元件之间发生的通信的框图;

[0157] 图16是示出用于给遗留(legacy)或SSN移动节点传播密钥的方法的框图;

[0158] 图17是示出用于完整实现本发明的一个方面的拓扑树的框图;

[0159] 图18是示出WLCCP节点ID的格式的表格;

[0160] 图19是示出接入点中内部网桥结构的框图;

[0161] 图20是以太网封装的WLCCP上下文管理帧的一个实例;

[0162] 图21是WLCCP消息头的实例;

[0163] 图22是TLV格式的实例;

[0164] 图23是示出如何使用跳路由的框图;

- [0165] 图24是示出在校园拓扑上移动节点从第一接入点越区切换到第二接入点的框图；
- [0166] 图25是用于初始移动节点关联的消息序列的一个实例；
- [0167] 图26是用于移动节点从第一接入点漫游到第二接入点的消息序列的一个实例；
- [0168] 图27是示出转发器接入点从第一接入点越区切换到第二接入点的框图；
- [0169] 图28A是用于初始转发器接入点关联的消息序列的实例；
- [0170] 图28B是用于转发器接入点从第一接入点漫游到第二接入点的消息序列的一个实例；
- [0171] 图29是根接入点认证的一个实例；
- [0172] 图30是示出所定义的CTK的框图；
- [0173] 图31是AP认证并注册到基础结构的实例框图；
- [0174] 图32是用于不要求注册的路径更新的另一个序列的实例框图；
- [0175] 图33是在接入点和子网上下文管理器之间建立(刷新)CTK的实例；
- [0176] 图34是示出成功的移动节点认证和注册到完整拓扑的实例消息序列的框图；
- [0177] 图35是单个子网的WLAN生成树的框图。

具体实施例

[0178] 贯穿本说明,所示出的最佳实施例和实例应该被视作本发明的示范而非限制。

[0179] 本发明通过采用从密钥管理中去除认证会话时间的密钥层次结构从而既减少消息也减少计算负担。因为认证和密钥管理被绑定到密码套件选择,所以当前的802.11实现方式把它们紧密地捆绑在一起并实施完整的 后端(重)认证。对于WEP,这可能因WEP重定密钥的要求而导致非常频繁的(重)认证。对于漫游,当前的实现也实施完整的(重)认证。

[0180] 该密钥层次结构把建立在成功认证基础上的密钥定义为网络会话密钥(NSK),该密钥独立于802.11密码套件选择。NSK被用来产生认证密钥刷新请求的密钥刷新密钥(KRK)和用作从中导出成对瞬时密钥(PTK)的基本密钥的基本瞬时密钥(BTK)。

[0181] 只有PTK被绑定到选定的802.11密码套件,并且因此必须基于密码套件安全策略进行管理。NSK的寿命由认证服务器(AS)定义为会话超时时间,该时间现在可被定义为NSK熵随802.11协议密码套件变化的函数。目标是积极鼓励使用可产生具有更多良好熵的动态NSK的认证类型。

[0182] 新的密钥层次结构100在图1中示出。密钥(如图1中定义)由提供子网上下文管理(SCM)的中心结点管理。该SCM是所有MN和迫使所有MN节点隐式地注册的AP的802.1X认证者。注册过程确保注册表中的所有节点已经成功地关联、认证并使安全证书被缓存(cache)。在本申请中描述的机制被定义为中心密钥管理(CCKM),并作为如SSN/TGi草案中所定义的已认证密钥管理(AKM)信息要素中的私有值来协商。

[0183] 参考图1,层次结构100的顶部是NSK 102。NSK 102作为成功的EAP认证的结果被隐式地导出。从NSK 102产生如框104所示的KRK和BTK。使用以NSK、BSSID、STA-ID、Nonces_{STA}和Nonces_{SCM}作为参数的PRF产生了KRK和BTK。从NSK中导出了128位的KRK 106a和256位的BTK 106b。使用以BTK、RN和BSSID作参数的PRF,从BTK 106b产生了PTK_{SN}。从PTK导出了802.1X加密密钥110(16字节)、802.1X MIC密钥112(16字节)、802.11加密密钥114(16字节)和AP MIC密钥116(仅TKIP)。AP MIC密钥116还包括8字节的Tx密钥118a和也为8字节的Rx密钥118b。

[0184] 虽然认证机制保留不变,例如802.1X EAP认证,但是本发明引入了新的密钥管理方案:CCKM。使用如这里下文中所定义的SSN的IE或RSN的IE来通告和协商这种新的能力。

[0185] 本发明的一个实现构思确保独立自主于认证机制。像TGi和SSN一样,本发明还假定成功认证后(NSK)密钥的存在。出于安全因素,这个 密钥一般应该动态地配置和管理。本发明为短NSK而准备,并提供把它们扩展到所要求的348位长度的方法。尽管非常不鼓励,但是这个设计也能允许使用被定义为NSK的预共享密钥。

[0186] CCKM必须知晓用于翻译和检索NSK的认证类型。图2是描述SCM如何导出和检索NSK的表格200。列202描述802.1X认证类型。列204描述NSK计算。列206示出了以字节计算的NSK的长度,而列208描述SCM如何获取NSK。

[0187] 例如EAP-MD5的互不导出动态密钥的认证类型依赖拥有静态密钥,该静态密钥被类似于遗留系统如何支持预共享的密钥认证来配置。传统上,这些静态的配置在AP处管理。为了顾及后向兼容,这些配置必须持久保留。这样,CCKM将从第一个所关联的AP请求这些NSK类型作为会话NSK。

[0188] 本发明构思了快速越区切换系统和方法(此处称为CCKM),该系统和方法基于中心化的服务、子网上下文管理器(SCM)以使能把MN从一个AP转移到一个新AP所要求的无缝的、安全的上下文传递。为了保护这样的传递,SCM依靠每一个节点,既包括AP也包括MN以便和SCM相互认证。在成功的认证之后,必须建立共享机密:网络会话密钥(NSK)。

[0189] NSK的使用偏离了IEEE 802.11 TGi(还有SSN)的在认证时建立的密钥的使用。TGi/SSN把这个密钥称为PMK,PMK反过来被用作导出802.1X和802.11成对瞬时密钥(PTK)的密钥材料。尽管CCKM也从NSK导出进一步的密钥材料,但是导出的密钥被用来认证瞬时密钥请求并导出PTK。该密钥层次结构在图1中示出。

[0190] 通过定义密钥循环移位方案,CCKM允许MN在重关联前导出新的PTK。一旦MN确定了它要漫游到的新BSSID,并在重关联请求被传输之前,MN可以为新AP导出PTK。这样,在重关联请求之后,MN能准备好保护到新AP的单播通信,但是必须等待AP的重关联响应,确认双方现在都能保护单播通信。AP的重关联响应也包括使能完整的受保护通信的广播密钥(GTK)的传送。

[0191] 对于一般的PTK重定,CCKM引入与SSN/TGi中所定义的内容相类似的EAPOL密钥描述符增强来影响CCKM重定密钥。

[0192] 分别使用或者SSN或者TGi信息要素,即SSN IE和RSN IE,可以协商CCKM能力。当前,两个规范都允许对已认证密钥管理套件的协商。套件选择器既封装认证也封装密钥管理机制,图3中的表格300描述了所分配的值。列302是组织唯一标识符(OUI),列304是和列302中的OUI对应的类型,而列306是对列302中的OUI的说明。

[0193] 为了互操作性,AP和MN都必须支持CCKM。AP必须通过在如SSNv0.21和TGi草案2.3中定义的已认证密钥管理套件选择器中使用新值来通告CCKM能力。

[0194] CCKM能力必须在信标帧(beacon)中通告并在探测响应和关联请求期间协商。成功的CCKM协商使在本说明书中所定义的中心化的密钥管理成为可能。使能CCKM也暗示着激活SCM。

[0195] SCM被设计成为子网提供上下文控制并影响漫游后的客户上下文传递。SCM是可以在AP中共存,作为独立的服务器,或在AS中共存的模块。虽然SCM被设计成影响整个子网间

的移动,但是这个设计只使用了影响子网内的移动所要求的元件。这些元件包括:

[0196] -容纳认证节点的安全证书,包括节点的NSK、会话超时时间和安全策略的存储库。

[0197] -MN的安全证书包括NSK、SSID、VLAN、会话超时时间、所关联的BSSID,并可能还包括认证机制、密钥管理机制和在关联时所协商的密码套件。该证书被用于在上下文传递和PTK可以被传送之前验证会话。

[0198] -AP的安全证书包括NSK、会话超时时间和所关联的MN的列表。

[0199] -包括所有注册节点的安全证书的上下文存储库

[0200] -管理所注册的MN和AP的上下文存储库所要求的服务;

[0201] -SCM提供不需客户交互作用就自动给新AP提供MN安全证书的服务。

[0202] -产生和保护基于安全策略的PTK传送的服务

[0203] SCM维护包括MN的NSK在内的给定子网内所有注册的MN上下文的缓存(图4中所示)。AP所缓存的安全证书略有不同并在图5中描述。参考图4,列402列出MN证书的SCAM缓存,包括字段:状态408(State 408)、STA Addr 410、认证类型412(Authentication type 412)、密钥管理类型414(Key Management Type 414)、会话超时时间416(Session Timeout 416)、Krk 418、BTK 420、RN422、SSID 424、VLAN ID 426、BSSID 428、密码430(Cipher 430)、NSK密钥长度432(NSK Key length 432)、NSK 434、Tx密钥长度436(Tx Key Length436)和Tx密钥438(Tx Key 438)。以字节计算的长度和这些字段的描述分别在列404和406中提供。参考图5,AP所缓存的证书包括状态508(state 508)、节点ID 510(Node-ID 510)、NSK 512、会话超时时间514(Session Timeout 514)、CTK 516和密钥序列计数器518(keysequence counter 518),如列502所示。长度和这些字段的描述分别在列504和506中提供。

[0204] SCM建立与MN和AP共享的机密。它使用密钥请求密钥(KRK)作为和MN共享的机密来认证密钥请求。上下文传递密钥(CTK)是和AP共享的机密,用来保护SCM和AP之间的通信。图6中示出了该信赖关系。

[0205] CTK被SCM分配给AP,用于保护链路通信。注意,虽然已经建议把NSK用于保护AP到SCM的通信,但是当链路密钥需要重定时这将施加给AS更短的会话超时时间和完整的重认证。

[0206] 图6示出了用于保护所分配的链路之间通信的密钥。注意,BTK不用于直接保护消息,而是用来导出用于保护AP和MN之间的通信的PTK。如图6所示,AS 602使用NSK0 606和SCM 604通信。SCM 604使用密钥CTK1 612和CTK2 614分别与AP1 608和AP2 610通信。AP1 608使用PTK3 622和PTK4 624分别与MN3 616和MN4 618通信,而AP2 610用PTK5 628和MN5 通信。SCM 604也可以使用KRK6 630、KRK7 632和KRK8634分别与移动节点MN3 616、MN4 618和MN5 620直接通信。

[0207] 基于重定密钥序列计数器和BTK导出和刷新PTK,计数器和BTK如基于这里下文所描述的NSK而定义或刷新的一样。

[0208] 通过使用Bering的SCM能力,快速越区切换设计提供了可升级的基础结构,该基础结构在后续的公开中被要求提供子网间漫游。

[0209] SCM服务在任意AP中共存,并因此可以定义选举机制以允许选择AP 作为SCM提供者。

[0210] 虽然将不会有对SCM到SCM(例如横向的)通信的初始的支持以使能热重启,但是选举机制仍旧使能冷待机。为保护和MN的通信,AP必须首先向其SCM进行认证和注册。建立NSK需要认证,而注册实现了SCM和AP之间的安全通信。AP的NSK被AP作为和SCM的成功的802.1X EAP认证的结果导出;认证服务器通过Radius MS-MPPE属性把NSK也当作成功认证的结果传送到SCM。AP通过监听SCM的通告消息来识别其SCM。

[0211] 在向SCM的成功认证后,AP必须接着将自己作为有效AP与SCM注册。在预注册后,SCM向AP传送一组用来既加密也认证SCM和AP之间的WLCCP消息的CTK。

[0212] 图7中示出了AP如何建立所需NSK和CTK的消息图解。AP也必须建立CTK以确保没有引入不受控制的AP并危害NSK或CTK。认证机制和用于网桥的类似,其中配置LEAP用户名和密码被用于向AS认证。AP执行的任务在列702中,SCM执行的任务列在列704中,而AS执行的任务在列706中。

[0213] 对于一些实施例,SCM是对所有节点的802.1X认证者。这样,在AP和SCM之间的CTK建立必须被相互导出。

[0214] 为了保护通信,MN必须首先通过802.1X EAP认证和网络进行认证。成功认证的结果建立NSK,该NSK用于建立分别用来认证密钥刷新和导出PTK的Krk和BTK。

[0215] 像SSN一样,CCKM也开始具有四路握手的会话以建立Krk和BTK,用于使能对单播业务的保护。仅在成功的认证之后需要这些握手。或者在重关联之后,或者因一般的密钥管理重定(类似密码套件对策)所致的重定密钥请求仅要求已认证的3路握手。图8示出了与SCM成功的MN LEAP认证和注册。

[0216] 需要一种从独立于CCKM模块的EAP申请者传递NSK的机制。例如,对于Windows平台上的非LEAP EAP认证,MN的NSK一般在EAP的申请者中产生并被传到EAP框架。然后EAP框架将把NSK传递到CCKM模块。由于当前的具有SSN能力的EAP框架把CCKM当作非SSN适应的,它将仅仅处理802.1X EAP认证并在EAP认证成功后下发NSK。类似地,非SSN EAP申请者将仅仅处理802.1X EAP认证并在EAP认证成功后下发NSK。

[0217] 但是,有可能直到接收到来自AP的群密钥发送EAPOL密钥消息以后才传送NSK。这样,如图8所示,对于非LEAP EAP认证,AP需要恰在向台站发送EAP成功消息之后发送额外的具有哑群密钥的802.1X EAPOL密钥消息。

[0218] 由CCKM模块中的实现负责指示AP,它需要发送额外的EAPOL密钥消息。这个信息在关联请求RSNIE期间可能被协商。另一个方案是在EAP成功消息后一直发送哑EAPOL密钥消息。如果CCKM模块已经具有NSK,则CCKM模块可以忽略哑密钥并建立四路握手后的真密钥。

[0219] 但是,对于遗留系统,关联交换将总是触发完整的认证和四路握手。CCKM重定密钥要素的接收将被忽略。

[0220] 额外的2路握手被用来重定多播/广播密钥(GTK)。用于GTK管理的重定密钥协议和在TGi和SSN中规定的相同。AP开始2路消息握手以移交GTK和加密的EAPOL密钥消息。当前的PTK用来保护这些EAPOL密钥消息。

[0221] 在具有CCKM能力的系统中,在预注册请求/应答期间,AP将总是向SCM请求安全证书。关联意味着会话开始,并因此,在关联以后,如果安全证书在SCM中有效并且CCKM被协商,则能够绕过802.1X认证。但是必须建立新生的Krk和BTK。如果不存在安全证书,则AP必须等待MN和AS之间完整的认证。

[0222] 在成功的认证之后,触发如图10中所示的序列来完成密钥建立并导致用于保护AP和MN之间分组的必要的PTK。

[0223] 由于总是给AP提供MN的会话超时时间,所以用于管理(重)认证的策略被分配给AP。和当前的实现类似,AP能在会话超时时间到期之前触发(重)认证,并且还能管理如此处定义的KRK和BTK刷新的更新。

[0224] MN或AP均能触发PTK重定。任一节点均可请求重定密钥的情况包括:TKIP故障,特别是在Michael对策中的;IV(主要针对WEP)和对策的用尽,假如节点感知PTK已经受到损害。

[0225] 重定密钥交换是3消息EAPOL密钥握手。定义新的密钥描述符以实现如图11所示的安全的重定密钥交换。字段定义如下:

[0226] 密钥信息1102(Key Information 1102):表明它是请求(0)、响应(1)或确认(3);

[0227] 状态1104(Status 1104):由响应者和确认者使用。零值表示成功;非零表示重定密钥失败并且必须调用完整的KRK、BTK或解除认证。

[0228] EAPOL重放计数器1106(EAPOL Replay Counter 1106):是EAPOL密钥消息计数器,也被用来防止消息重放;

[0229] 保留字段1108(Reserved field 1108):增加的额外字节以使要素排列的更好;

[0230] 密钥ID 1110(Key-ID 1110):存储密钥标识符的1字节字段(0、1、2或3)分配,它必须和当前所分配的密钥ID匹配;

[0231] MN-ID 1112:客户的MAC地址;

[0232] BSSID 1114:AP的MAC地址;

[0233] RN 1116:重定密钥请求号

[0234] MIC 1118:使用当前PTK的认证要素。MIC被定义为:

[0235] $MIC_{request} = HMAC-MD5(PTK,$

[0236] Key Info || EAPOL Replay Ctr || Key ID || MN-ID || BSSID || RN),

[0237] $MIC_{response} = HMAC-MD5(PTK,$

[0238] Key Info || EAPOL Replay Ctr || Key ID || MN-ID || BSSID || RN || Status),

[0239] $MIC_{confirm} = HMAC-MD5(PTK,$

[0240] Key Info || EAPOL Replay Ctr || Key ID || MN-ID || BSSID || RN || Status)

[0241] 图12中示出了重定密钥序列1200。左边的列1202示出了初始者执行的任务而右边的列1204示出了响应者执行的任务。

[0242] 在框1206,状态转移呼叫新的PTK。初始者设置 $RN = RN + 1$,新的 $PTK = PTK_{RN+1}$,并计算 $MIC_{request}$ 。向响应者的传输被停止,直到达到有效的响应或超时时间。必须允许使用 PTK_{RN} 的接收。发送在密钥ID中使用 PTK_{RN+1} 的请求。

[0243] 响应者接收请求。如果如框1208处所示, $MIC_{request}$ 新RN不大于所缓存的RN,或者EAPOL密钥请求中的任意属性无效,则响应者不重定PTK或发送具有非零状态的响应。但是,如果如在框1210处所示, $MIC_{request}$ RN和EAPOL密钥属性有效,则响应者将更新RN并计算 PTK_{RN+1} ,清除MN传输队列,安装 PTK_{RN+1} 和发出就绪响应,以使用 PTK_{RN+1} 传输和接收(一旦响应被发送,则使用 PTK_{RN} 从MN接收到的分组将不正确地解密)。

[0244] 然后初始者接收响应者的响应。如框1212中所示,如果 $MIC_{response}$ 或任意EAPOL密钥

属性无效,则放弃重定密钥并且初始者将重试。但是,如果如框1204处所示,MIC_{response}和任意EAPOL密钥属性有效,则初始者设置PTK_{RN+1}并准备用PTK_{RN+1}传输和接收。然后初始者发送EAPOL确认消息。

[0245] 然后响应者接收EAPOL确认消息。如框1216中所示,如果MIC_{confirm}或EAPOL密钥确认中的任意属性无效,则初始者或者将触发另一次重定密钥,确定它是假情报并解除关联,或者解除认证。如框1218中所示,如果EAPOL确认是有效的,则使用PTK_{RN+1}保护链路。

[0246] 在成功的重定密钥之后,AP必须为MN同步SCM的RN的值。推荐在每次重定密钥时进行同步。为更新SCM,具有WTLV_UPDATE_RN的WLCCP_CONTEXT消息被发送到SCM。

[0247] 上面的说明假设无论请求者还是响应者都不能使用多个密钥ID来缓存PTK。但是,本发明的协议允许这个功能并因此有助于在重定密钥操作期间更平稳的转移。即,申请者可以把PTK_{RN+1}安装到新的密钥中去并因此能在PTK_{RN}或PTK_{RN+1}之下接收分组。类似地,响应者能够在另外规定的密钥ID中检测密钥并且也允许在任一密钥下的传输和接收。最终的确认是停止当前(旧)PTK_{RN}下的传输和接收。

[0248] CCKM使用SSN和TGi型的重定密钥用于更新多播密钥(GTK),故在本说明书中没有定义。关于群/广播密钥更新的细节,参考最新的TGi草案。

[0249] 为了缩短重关联握手,这个设计使得在客户台站和AP之间交换的分组的数目减少到两个分组——重关联请求和重关联响应。参考图13,引入新的专有要素1300来辅助在重关联消息中的越区切换。重关联请求中的要素包括重定密钥请求号(RN)和已认证的要素。其中:

[0250] MIC_{MN} 1314=HMAC-MD5(KRK,MN-ID||BSSID||RSNIE_{MN}||Timestamp||RN),并且

[0251] 要素ID 1302是Cisco定义的要素,其值为0x9c

[0252] 长度1304应该是CCKM要素请求的长度(例如24字节)

[0253] OUI 1306应该是00:40:96

[0254] OUI 1308类型应该是0

[0255] MN-ID(未示出)是MN的MAC地址,

[0256] BSSID(未示出)是AP的MAC地址,

[0257] 时间戳1310是当前的TSF定时器值,

[0258] RN 1312是重定密钥请求号,

[0259] RSNIE_{MN}(未示出)是MN的请求安全策略(例如AKM和密码套件协商);

[0260] CCKM(未示出)必须在RSNIE_{MN}的AKM选择器中规定。

[0261] 重关联响应包括新的要素,认证1400请求,确认PTK_{RN}的使用并传送多播密钥,如图14所示。

[0262] 其中:

[0263] EGTK=RC4(RN||PTK_{RN},GTK)

[0264] MIC_{AP}1402=HMAC-MD5(PTK_{RN},MN-ID||RSNIE_{AP}||RN||Key ID_{unicast}||Key ID_{multicast}||Key length||EGTK)

[0265] 现在参考图15,示出了MN重关联到新AP的成功实例。在重关联请求/响应交换中发生了越区切换。MN 1502在RSNIE 1530中必须包括CCKM1528以使用快速越区切换。更重要的是,MN 1502在重关联时所协商的安全策略必须和在初始关联时所规定的相符。SCM 1506必

须验证,请求中的RN 1532值大于先前的一个。该请求中所提供的时间戳也必须位于AP的TSF定时器(未示出)的可配置值中;时间戳被包括在内以确保这个请求是新生的。响应之后,AP 1504也必须在CCKM响应要素中提供其定时器值 以向MN 1502保证该响应也是新生的。

[0266] 当AP 1504接收到重关联请求并且CCKM被协商,它必须查询SCM1506以确认安全证书并在它能产生PTK_{RN}前获取RN和BTK。使用WTLV_SECURE_CONTEXT请求对SCM 1506提出请求。如果SCM 1506不能验证证书,则它将不传送任何东西并提供非零状态标识来表示失败。在成功的传递后,SCM 1506将在所加密和认证的WTLV_SECURE_CONTEXT应答中传送RN和BTK。安全证书的验证防止内部人员和不同的SSID快速重关联。

[0267] 在成功的上下文传递以后,AP 1504继续产生PTK,如这里下文所描述的那样。然后它将使用该PTK加密和认证新的信息要素来确认PTK并安全地发送多播密钥GTK。

[0268] 如果CCKM被协商但是没有提供私有要素,则AP 1504仍可以请求安全证书。如果证书有效,则触发新生的KRK和BTK的完整的WTLV_INIT_SESSION建立,并在成功的4路交换之后,KRK和BTK被SCM1506和MN 1502相互导出并且RN被重置为1。如果没有安全证书或者向SCM的请求失败,则AP可以选择实施完整的(重)认证。

[0269] 通过利用PTK序列,客户台站准备好在客户开始重关联请求前解密单播分组。客户在重关联请求中通过使用递增的认证者(请求号)和对应的认证(MIC)确认其身份。AP 1504使用重关联响应确认其身份并把多播密钥信息(GTK)捎给(piggyback)客户STA。

[0270] 对每次快速重关联尝试,将使用唯一的请求号(RN)。在每次快速重关联尝试后,客户增加RN。SCM通过缓存客户最近使用的RN并拒绝任何RN小于或等于所缓存的最近的RN的请求,以防止重放快速重关联请求。

[0271] 注意,证书和密钥信息的导出包括BSSID以防止跨过不同AP的重放企图。例如,没有BSSID,黑客可能试图再次使用对一个AP的快速重关联请求来关联到第二AP。哪一个的尝试将首先到达SCM——黑客还是真正的客户——取决于通过网络的延迟。

[0272] 在另一个实施例中,可以包括把安全证书转发到注册的AP的能力。对于AP 1504和SCM 1506之间具有较大延迟的网络,在AP 1504处也可以缓存SCM 1506的信息。在这种情况下,AP 1504可以执行一般在SCM 1506处完成的全部计算。因为用于特定BSSID的最新的RN足以防止重放,所以AP 1504无需查询SCM 1506以获得最新的RN,就能够验证客户的认证。AP 1504应该向SCM 1506发送一个更新信号以确保SCM 1506具有最新的RN信息——如果AP应该使得该信息失去时效并在以后从SCM处请求该信息,则这是特别重要的。

[0273] 重关联的过程在1510处开始,其中,MN 1502增大RN并产生新的PTK_{RN}。如1512处所示,MN 1502向AP 1512发送重关联请求,该请求包括RN 1532、带有作为协商密钥管理值的CCKM 1528的RSNIE_{MN} 1530。然后AP 1504向SCM 1506发送WLCCP(MN,Pre-Reg Req,WTLV_SECURE_CONTEXT,MN-ID,BSSID,RN,VLAN,MIC_{KRK}),如1514所示。SCM 1506用WLCCP(MN Pre-Reg Reply,WTLV_SECURE_CONTEXT,MN-ID,BSSID,RN,VLAN,BTK)响应,如1516所示。如框1518中所示,AP1504使用其AP的CTK为MN 1502认证并加密BTK,并导出PTK_{RN}。在1520处,AP 1504发送完成了PTK_{RN}的存活性和GTK传送的重关联响应(RN,RSNIE_{AP} Nonce_{GTK} E(PTK, GTK),MIC(PTK,MN-ID,BSSID,RN,RSNIE_{AP},Nonce_{GTK},E(PTK,GTK))).然后如框1522中所示,MN 1502使用PTK为该STA认证并加密GTK。一旦AP 1504已经完成建立与NM 1502的安全通信链

路,它就把MN 1502注册为可连接到AP 1504。这由步骤1524和1526完成。在步骤1524,从AP 1504向SCM 1506发送WLCCP(MN,REg Req),并且在步骤1526发送应答WLCCP(MN Reg Reply)。

[0274] 虽然本设计鼓励使用CCKM,但是也能支持其他的已认证密钥管理(AKM)类型。由于具有CCKM能力的MN是唯一的使得其证书在SCM处被缓存并因而要求注册的MN类型。但是,为了把证书正确地传播到AP,所有的MN都要求预注册。无论是支持遗留的还是具有SSN能力的客户,证书传播和预注册是相同的,如图16所示。

[0275] 定义了密钥层次结构以允许扩展密钥和导出新生密钥。这部分描述用于导出密钥的函数。然而必须进行说明以强调密钥熵的问题。

[0276] CCKM确保密钥的新生性但是依赖于供给强密钥;例如,具有好的熵。如果类似LEAP的基于密码的实现被认为具有较低的熵,则可以进一步使用加密工具来增大密钥的熵。TGi已经采用各种PKCS#5作为增大密钥熵的方法,本设计也能很容易地采用这些方法。但是注意,这要求比某些NIC所能提供的多得多的计算。

[0277] KRK和BTK推导

[0278] 为了确保新生的KRK和BTK密钥,AP和MN进行4路握手以提供用于导出KRK和BTK所需的密钥材料。每个节点必须提供一个16字节的现时标志(nonce),随后该现时标志和NSK一起使用以导出所需的密钥。该函数的定义如下:

[0279] $GK = PRF-384(NSK, "Cisco \text{ 密钥管理基本密钥} ") |$

[0280] $BSSID | STA-ID | Nonce_{STA} | Nonce_{SCM}$

[0281] $KRK = GK[0:127]$

[0282] $BTK = GK[128:383]$

[0283] PRF-384在部分0中定义。

[0284] 由于相同的PRF-XXX函数被用于产生多个密钥类型,所以字串“Cisco密钥管理基本密钥”被引入这个密钥导出函数,以确保这些密钥被唯一地构造出来,而与其他密钥类型不同。

[0285] 保护WLCCP消息

[0286] 为了保护WLCCP消息免于窃听(eavesdropping)和中间人(man-in-the-middle)攻击,大多数WLCCP消息使用RC4进行加密并使用HMAC-MD5认证。AP在预注册期间和SCM建立起CTK以便它能开始WLCCP消息的保护。

[0287] CTK是如下的用于保护WLCCP消息的256位密钥:

[0288] CTK的低128位用作RC4密钥。

[0289] CTK的高128位用作HMAC-MD5密钥。

[0290] CTK密钥推导

[0291] SCM产生并分配在AP和SCM之间使用的上下文传递密钥。链路中的每个节点必须提供一个16字节的现时标志以确保新生的密钥:

[0292] $CTK = PRF-256(NSK, "SWAN \text{ IN-IA链路上下文传递密钥推导} ") |$

[0293] $AP-ID | SCM-ID | Nonce_{AP} | Nonce_{SCM} | KSC$

[0294] CTK由SCM计算并传送到AP,用于保护后续的WLCCP消息。CTK的传送通过使用NSK加密和认证密钥来完成。

- [0295] PTK密钥推导
- [0296] PTK最大为512字节,因为它们既被用于保护802.1X也被用于保护802.11通信。它的长度取决于在关联时所建立的802.11密码套件协商。
- [0297] 使用一路哈希函数:SHA-1导出PTK,并且PTK基于BTK、RN和BSSID:
- [0298] $PTK = PRF-Len(BTK, RN || BSSID)$
- [0299] 其中,对于WRAP或CCMP, $Len = 384$,对于TKIP或CKIP 512是512。
- [0300] 尽管本发明大量使用PTK,但是所产生的PTK被分成几个用于保护下面内容的密钥(也如图1所示):
- [0301] -AP和MN之间的EAPOL密钥加密
- [0302] -AP和MN之间的EAPOL密钥认证
- [0303] -802.11加密
- [0304] -对于802.11 TKIP和CKIP:AP和MN之间的数据分组认证
- [0305] 对PTK的密钥分配如下:
- [0306] EAPOL-密钥MIC密钥 $= PTK[0:127]$
- [0307] EAPOL-密钥ENC密钥 $= PTK[128:255]$
- [0308] 802.11加密密钥 $= PTK[256:383]$
- [0309] TKIP Michael认证者Tx密钥 $= PTK[384:447]$
- [0310] TKIP Michael认证者Rx密钥 $= PTK[448:511]$
- [0311] 用于基于给定的密钥材料,产生任意长度的密钥的定义和伪代码如下(摘自TGi草案2.3):
- [0312] $H-SHA-1(K, A, B, X) = HMAC-SHA-1(K, A || Y || B || X)$ 其中,Y是包含0x00(零)的单个八位字节
- [0313] $PRF-384(K, A, B) = PRF(K, A, B, 384)$
- [0314] $PRF-512(K, A, B) = PRF(K, A, B, 512)$
- [0315] $PRF(K, A, B, Len)$
- [0316] {
- [0317] octet i;
- [0318] for($i = 0; i < (Len + 159) / 160; i++$) {
- [0319] $R = R || H-SHA-1(K, A, B, i)$
- [0320] }
- [0321] $L(R, 0, Len)$
- [0322] }
- [0323] SHA-1中使用的密钥是由SCM独立产生的并不需要任何其他方共享。
- [0324] HMAC-SHA1参考代码
- [0325] #include "stdafx.h"
- [0326] #define ULONG unsigned long
- [0327] #include <sha.h>
- [0328] void hmac_sha1(
- [0329] unsigned char *text, int text_len,

```
[0330] unsigned char *key,int key_len,
[0331] unsigned char *digest)
[0332] {
[0333] A_SHA_CTX context;
[0334] unsigned char k_ipad[65];/*inner padding-key XORd withipad*/
[0335] unsigned char k_opad[65];/*outer padding-key XORd withopad*/
[0336] int i;
[0337] /*如果key大于64字节,把它重置为密钥key=SHA1(key)*/
[0338] if(key_len>64){
[0339] A_SHA_CTX tctx;
[0340] A_SHAInit(&tctx);
[0341] A_SHAUpdate(&tctx,key,key_len);
[0342] A_SHAFinal(&tctx,key);
[0343] key_len=20;
[0344] }
[0345] /*
[0346] *HMAC_SHA1变换看起来像:
[0347] *
[0348] *SHA1(K XOR opad,SHA1(K XOR ipad,text))
[0349] *
[0350] *其中K是n字节密钥
[0351] *ipad是重复64次的字节0x36
[0352] *opad是重复64次的字节0x5c
[0353] *而text是被保护的数据
[0354] */
[0355] /*通过把密钥存储在pad中开始*/
[0356] memset(k_ipad,0,sizeof k_ipad);
[0357] memset(k_opad,0,sizeof k_opad);
[0358] memcpy(k_ipad,key,key_len);
[0359] memcpy(k_opad,key,key_len);
[0360] /*用ipad和opad的值对密钥进行XOR运算*/
[0361] for(i=0;i<64;i++){
[0362] k_ipad[i]^=0x36;
[0363] k_opad[i]^=0x5c;
[0364] }
[0365] /*执行内部SHA1*/
[0366] A_SHAInit(&context);/*用于第一次传递的初始上下文*/
[0367] A_SHAUpdate(&context,k_ipad,64);/*用内部pad开始*/
[0368] A_SHAUpdate(&context,text,text_len);/*随后是数据报文。*/
```

[illegible]

为SWAN“校园网”中的无线台站安全地管理“操作的上下文”。

[0406] WLCCP注册协议a)自动地创建和删除SWAN拓扑中的链路,b)安全地分配操作的上下文和c)(可选择地)在无线链路上可靠地建立层2的转发路径。

[0407] WLCCP SCM通告/选举协议自动地建立单个SCM,作为每个子网的中心控制点,并使AP和MN能选择提供了到骨干LAN的“最小代价路径”的双亲节点。

[0408] WLCCP“上下文”消息为上下文和管理信息提供通用的传输。WLCCP“跟踪”消息有助于网络的诊断工具。

[0409] WLCCP是面向处理的“请求/应答”协议。所有的WLCCP请求和应答消息具有固定长度的头,该消息头包含由消息类型决定的字段。接着该固定长度头的是可选的类型长度值(Type-Length-Value)对;因此WLCCP是可扩展的。

[0410] 以太网或UDP/IP封装可被用于WLCCP消息。以太网封装限于子网内(例如,AP到AP或AP到SCM)的WLCCP消息。子网间WLCCP消息必须用IP封装,并且IP封装也可以用于子网内WLCCP消息。

[0411] 本领域熟练技术人员很容易理解,具体的WLCCP实现可以不包括这里描述的所有元件。

[0412] 当MN漫游时,“分布式”上下文传递协议可被用于从“旧AP”向“新AP”直接传递上下文。例如,IEEE 802.11f草案协议定义了分布式上下文传递协议。这样的分布式方法有大量的固有的问题。最显著的问题是:1)安全的上下文传递要求AP之间的多对多信赖关系(或要求某个额外的层次结构)。2)需要一个协议使得“新AP”在MN漫游时能确定“旧AP”。(“旧AP”802.11重关联字段还不够。)台站漫游时,上下文被从AP到AP地传送;因此,关键的上下文可能丢失(例如,如果失去到旧AP的链路)。4)分布式的协议容易受内部紊乱状况的影响,在该状况下用于快速地漫游台站的“越区切换消息”可能次序混乱地到达。

[0413] 这里公开的SWAN网络被组织为分层的“拓扑树”。当台站从“旧AP”漫游到“新AP”时,上下文一般通过拓扑树中新旧AP的“最近共同祖先”传递。WLCCP注册包括必要的路由逻辑以自动地找到最近共同祖先。所缓存的配置和上下文信息存储在网络基础结构中。共同祖先在新的拓扑树的分支上为漫游的台站安全地转发所缓存的信息。因此,上下文传递被自动地“本地化”,并且假如到旧AP的链路丢失,则上下文信息不会丢失。共同祖先也把“旧AP绑定”转发到新AP。

[0414] 对于SWAN网络中的安全的上下文传递不需要802.11 AP之间的多对多安全关系。取而代之,建立起与SWAN拓扑树对应的信赖层次结构。操作上下文一般在拓扑树的分支上转发;因此,WLCCP上下文传递密钥在同一拓扑树分支上的所有节点之间预先建立。如果有必要在位于不同拓扑树分支的两个节点之间“横向地”传递上下文,则两个节点的最近共同祖先能起到所信赖的第三方的作用,以便快速地建立相互认证和瞬时上下文传递密钥。

[0415] 分层的拓扑树有助于中心管理和控制点。例如,可以在中心配置和分配网络范围内的参数。中心WLCCP控制点建立和删除拓扑链路;因此,即使用于快速漫游台站的越区切换消息抵达次序混乱,也有可能保留一致的网络拓扑。

[0416] 本地或全局所管理的48位IEEE 802地址被用作内部的WLCCP网络节点地址。不用IP地址作网络节点地址,因为:a)节点可以改变其IP地址。B)WLCCP用于管理层2的移动;它一般应该独立于任何网络层协议。

[0417] WLCCP节点地址是内部的WLCCP节点标识符并且在网络管理应用中不应该被用来给用户识别AP和CM。取而代之,网络接入标识符(NAI)或域名可用作用户的WLCCP节点标识符。

[0418] 本发明的WLCCP的设计考虑了下列基本假设和要求:

[0419] 1)目标环境是企业“校园网”。

[0420] 2)802.11是以太网接入技术,它被用于将有线以太网骨干LAN扩展到移动节点并选择“次级LAN”。

[0421] 3)802.11 AP事实上是层2的“以太网”网桥。

[0422] 4)802.11移动节点(MN)事实上是移动的“以太网”节点。

[0423] 5)WLCCP一般独立于下层的无线电技术。

[0424] 6)MN应该能在“校园网”内的单个子网内或子网之间无缝地漫游,并如同连接到以太网交换端口那样操作;因此,当MN漫游时有必要传递位置特定的操作上下文。

[0425] 7)当MN漫游时,必须可靠地重新建立MN和每个对端主机(CH)之间的路径。(简单的逆向学习不充足并容易受到“紊乱状况”影响。)

[0426] 8)如802.1D标准中所定义的那样,非WLCCP以太网网桥和交换机必须支持逆向学习。

[0427] 9)WLCCP必须为Proxy-MIP/VLAN子网间无缝移动的完整解决方案提供上下文管理服务。无缝移动解决方案必须既支持IP也支持非IP应用;它不得要求客户支持;并且它不得要求用户大量地改动他们的现有有线拓扑。

[0428] 10)WLCCP不有助于(或排除)位于不同地理位置的子网之间的无缝漫游。

[0429] 11)校园网可能包括众多数量的频繁漫游的台站;因此,用于漫游的开销必须极小。

[0430] 12)WLCCP必须支持用于Qos应用的非常快的漫游。

[0431] 13)WLCCP必须支持现有的WLAN特征,包括无线(即转发器)AP、无线网桥和移动AP和网桥。

[0432] 14)在无线链路上必须使单播和多播帧泛滥最少化。

[0433] 15)WLCCP必须支持快速安全的上下文传递但不产生对AP之间的多对多安全关系的要求。

[0434] 16)WLCCP必须独立于任何下层的生成树协议操作。

[0435] 17)WLCCP不得显著地提高用户的配置要求;因此,下层拓扑很大程度上必须自我构造的。

[0436] 18)WLCCP不得引入单个故障点。如果SWAN节点或链路发生故障,网络必须继续操作,但可能具有减少的特征。

[0437] 19)WLCCP必须最大限度地利用现有标准。

[0438] 20)WLCCP不得与现有协议冲突。特别是WLCCP不得排除标准移动IP客户。

[0439] 21)不得要求客户MN直接支持WLCCP。反之,MN能通过802.11要素间接地支持WLCCP。

[0440] 22)WLCCP必须为WLAN管理和诊断工具提供构建模块。

[0441] 23)AP在不同子网上的无线电覆盖范围可以重叠。

[0442] 24)WLCCP安全上下文传递和消息认证独立于下层的安全基础结构,例外之处是它必须能相互认证SWAN节点并建立秘密的会话密钥。

[0443] 25)WLCCP不提供MN认证;但是,它必须通过安全地传递动态的MN安全证书以有助于快速重认证。

[0444] 如这里使用的那样,SWAN网络是植根于SWAN CM处的“树状拓扑”。WLCCP用于建立和保留该拓扑树。图17示出了用于完整的WLCCP实现的示范性拓扑树。图17示出了具有两个本地控制域(LCM)1704和1706,以及三个子网控制域(SCM)1708、1710和1712的“校园拓扑”。示范性网络包括工作组网桥(WGB-1)1714及其连接的以太网节点(EN-1和EN-2,分别为1716和1718。)。在802.11链路上存在的拓扑分支如虚线1720a-f所示。可能的子网拓扑元件是该WLCCP实现所专有的。一个支持层2的路径更新和无线网桥的实现的示范性的子网拓扑将在下面说明。

[0445] 在SWAN拓扑树中,SWAN CM和AP是中间节点(IN),而MN和次级以太网节点(EN)是叶子。SWAN CCM 1702位于校园拓扑树的根处。在校园网中CCM 1702是根CM。LCM 1704和1706位于包含在本地控制域中的子树的根处。SCM 1708、1710和1712位于包含在每个网络子网中的子树的根处。“双亲AP”1722、1724、1726和1728位于包含孩子MN 1730、1732和1734以及任意孩子AP 1736和1738的子树的根处。

[0446] 图18的表格1800中示出了WLCCP节点ID的格式。64位的WLCCP节点ID标识了SWAN网络中的每个节点。节点ID是连接在一起的16位WLCCP节点类型1802和48位WLCCP节点地址1804。用于MN、EN、AP或SCM的节点地址1804是全局的48位IEEE 802地址。用于LCM或CCM的节点地址1804可以是全局的或本地管理的48位IEEE 802地址。在一个实施例中构思了CCM能够自动地为自己和其他LCM分配“本地”48位地址。“全零”的节点地址用于标识WLCCP CM或AP中的“本地WLCCP节点”。节点类型是CCM、LCM、SCM、AP、MN或EN。

[0447] 每个物理(例如以太网和802.11)通信接口由48位IEEE 802端口地址标识。SCM的LAN通信接口也由48位IEEE802端口地址标识。802端口地址可以被重新用作WLCCP节点地址。每个WLCCP CM必须具有IP通信接口,该接口由IP端口地址标识。因为CM的IP地址可能发生变化,所以不用IP端口地址作为CM节点地址。

[0448] AP通信接口一般在“混合模式”下操作;因此,AP能够在任意物理接口上接收目的地为其节点地址的WLCCP帧。在一个简单的实现中,AP节点地址可被用于标识AP中的“内部WLCCP接口”。

[0449] 图19示出了AP中的内部桥接结构。以太网802端口地址也是WLCCP节点地址。目的地为节点地址并在以太网或802.11接口上接收的帧被内部“桥接”到WLCCP协议接口;因此,节点地址也能被用作任意AP端口上的WLCCP“跳地址”。(因为WLCCP和DDP共享相同的以太网DIX类型,所以把它们一起示出。)

[0450] 应该用永久“节点名”来配置每个WLCCP AP和CM(例如,网络接入标识符(NAI)或DNS域名)。必须用节点名配置LCM以从CCM请求本地管理的节点地址。

[0451] 节点ID不是永久性的节点标识符并且也不应这么使用。NAI可以用来表示到用户的网络节点。

[0452] 实例标识符及其节点ID识别“连接的”AP或CM的每个“实例”。在WLCCP中,如下面所描述的,实例年龄用作实例标识符。

[0453] 每个WLCCP CM必须保留用于把WLCCP节点ID映射为节点名或IP地址或相反映射过程的交叉索引表。

[0454] 再次参考图17,在校园网中,每个SWAN AP 1722、1724、1726和1728,除了SWAN CCM 1702之外的CM 1704、1706、1708、1710、1712均被绑定到单个“双亲节点”和单个“双亲CM”。LCM的双亲CM是CCM。SCM的双亲CM是LCM。(注意,单个设备可以包括多个逻辑CM。包含CCM的设备总是包含逻辑LCM。)在图17中,AP 1720的双亲节点和双亲CM分别是AP 1728和SCM 1712。

[0455] 每个子网的SCM是在该SCM的子网上的所有AP以及和那些AP关联的所有MN的双亲CM。注意,即使MN通过VLAN干线(VLAN trunking)或 Proxy MIP隧道被绑定到不同的“本地子网”,但该MN仍是双亲AP的“本地”子网的SCM的孩子。例如,在图17中,SCM 1708、AP 1722和AP 1724都属于同一子网。MN 1730是AP 1722的孩子;因此,它是SCM1708的孩子。但是,如果AP-1被连接到VLAN干线链路,则MN 1730可以属于不同的子网。

[0456] LCM或SCM的“双亲节点”是双亲CM。MN的双亲节点是802.11双亲AP。“根AP”的双亲节点是SCM。非根AP的双亲节点是802.11双亲AP。节点被看作是其双亲的“孩子”。“邻居”是双亲或孩子节点。

[0457] 在节点和其每个邻居之间存在逻辑“链路”。“端口”是提供对链路访问的逻辑实体。每个CM和AP具有单个基本端口和一个或更多的次级端口。节点在其基本端口上连接到网络。在单个物理通信接口之上可以存在多个逻辑端口。例如,在图17中,AP 1728可以用同一个物理802.11接口访问到AP 1736和AP 1738的链路;但是,AP 1728针对每条链路具有独立的逻辑端口。

[0458] 拓扑树的“分支”包括一组节点和提供“祖先”节点和“后代”节点之间的最短路径的链路。进入节点是祖先,而离开节点是后代。所有的节点是根CM的后代。离开路径从祖先节点起始并终止于后代节点。进入路径从后代节点起始。

[0459] SWAN CM不在非WLCCP消息的转发路径上;因此,节点的SWAN“路径实例”和该节点的数据转发路径不同。

[0460] 在每个SWAN节点其每个邻居之间存在拓扑树“链路”。当“孩子节点”选择了“双亲节点”并通过其双亲节点向SWAN基础结构注册时,建起链路。SCM到AP链路总是以太网链路。AP到AP链路可以是以太网或802.11链路。AP到MN的链路(在当前)总是802.11链路。从概念上讲,CM到CM链路可以是任何支持IP的链路。

[0461] 节点负责为其每个邻居维护“链路状态”。活动的链路处于“连接”状态。如果失去了下层的物理通信链路或者孩子漫游到了不同的双亲节点,则链路转移到“断开”状态。节点必须能够检测在其邻居中的链路状态的变化;否则,链路可以处于“半连接”状态。(AP到AP的802.11链路状态对于WLCCP不用于层2的更新的WLCCP实现是透明的。)

[0462] CCM的IP地址或域名必须在每个LCM和每个SCM候选者中静态地配置。在一个实施例中构思了LCM或SCM通过CCM通告协议可以自动地发现CCM。

[0463] 绑定到每个LCM的子网的列表在CCM中配置。刚开始,以及任何双亲LCM丢失的时候,SCM向CCM发送请求消息以获取其双亲LCM分配。

[0464] 为每个子网自动地选举SCM。AP通过SCM通告协议自动地发现其双亲SCM。如下面所描述的,非根“孩子AP”也绑定到“双亲AP”。MN通过802.11关联协议绑定到双亲AP。

[0465] 节点或者处于“被连接”状态,或者处于“未连接”状态。最初节点处于未连接状态。CCM候选者在其变为活动的CCM时转移到连接状态。CCM在其放弃CCM角色时转移到未连接状态。非CCM节点在其最初向SWAN基础结构注册时转移到被连接状态。如果a)非CCM节点检测到其双亲节点未被连接,或b))非CCM节点不能与其双亲节点通信,则被连接的非CCM节点转移到未连接状态。

[0466] 每个CM必须保留内部实例年龄,该年龄包含以秒计算的自从节点上次转移到被连接状态的逝去的时间。实例年龄被初始化为零,并且每次当节点向新的双亲CM开始注册时被重置为零。SCM的实例寿命被复制到SCM通告应答消息中的实例寿命(Instance Age)字段,所以孩子AP能检测到其双亲SCM的新的实例。孩子AP如果接收到具有更低实例年龄的通告消息,则孩子AP变为未连接的。在一个实施例中,如果WLCCP不被用于层2的更新,则AP不需要维护实例年龄。

[0467] SWAN网络一般在具有单个CCM和相应校园控制域的“校园基础结构模式”中操作。如果LCM不能和CCM通信,则LCM和其对应的本地控制域必须在“本地独立模式”中操作。如果LCM未被分配给CCM,则它也必须独立模式中操作。同样地,如果SCM未被分配给双亲LCM,则每个SCM和对应的子网必须在“子网独立模式”中操作。

[0468] 在独立模式中,本地控制域或子网控制域的操作和SWAN校园网非常像。在本地独立模式中操作的LCM承担CCM的功能。在独立域根部的LCM或SCM起到对于基础结构节点和MN的802.1X认证者的作用。本地或子网控制域必须能够在基础结构模式和独立模式之间顺畅地转移。

[0469] LCM被用CCM的IP地址来配置,以便在基础结构模式中操作。如果因为LCM失去了到其所分配到的CCM的链路而在独立模式中操作,则它必须周期性地尝试重新建立和CCM的通信。

[0470] SCM被用CCM的IP地址或域名配置,以便在基础结构模式中操作。CCM负责把每个SCM分配给LCM,如下面名为“W2-双亲LCM分配”的部分所描述的那样。

[0471] 如果AP不能为其子网发现SCM,则AP必须在低效操作的“分布式模式”下操作。AP必须能在基础结构模式和分布式模式之间顺畅地转移。例如,在分布式模式中,AP能够使用现有的Cisco数据包传递协议(CiscoDatagram Delivery Protocol)。注意,仅通过不配置任何SCM候选者,用户就可以强迫AP在分布式模式中操作。

[0472] 总的来说,LCM或SCM可以从基础结构模式顺畅地转移到独立模式(即在到其双亲的链路丢失时)而不需要断开其子树中的节点。在“新”独立域中的节点能够继续使用先前在基础结构模式中所建立的现有注册信息和安全证书。

[0473] 当LCM或SCM从独立模式转移到基础结构模式时,必须重建那些根部在LCM或SCM处的子树。在SCM或LCM从独立模式转移到基础结构模式时,它建立新的实例ID。如果SCM的双亲LCM发生变化,则SCM也建立新的实例ID。当子树中的节点检测到新的SCM或LCM实例时,自动地删除那些根部在SCM或LCM处的子树。

[0474] 下面列出了WLCCP“上下文管理”消息类型。给每个消息类型定义了“请求”和“应答”子类型。给需要额外的握手的选择消息类型定义了可选择的“确认(confirm)”和“确认应答(ack)”子类型。

[0475] SCM-通告

[0476] CCM-通告

[0477] 注册

[0478] 预注册

[0479] 解除注册

[0480] 分离

[0481] 上下文

[0482] 路径更新

[0483] 路径检验

[0484] 跟踪

[0485] AAA

[0486] Path-Init(路径初始)

[0487] 在名为“WLCCP协议定义”的部分定义了WLCCP消息格式。

[0488] 在请求应答消息的请求消息中,“Response-Req”标志被设置为ON。总的来说,应答消息用于确认请求消息并把状态和/或上下文信息返回到发起者。请求“消息标识符”被复制到相应的应答消息以“匹配”请求/应答对。同样的消息标识符在重传输的请求消息中使用,以标识所有属于单个处理的请求/应答消息。

[0489] 可选的“确认”消息可被用于确认收到一个应答消息并把状态和/或上下文信息返回到响应者。在用来请求确认(confirm)消息的应答消息中,Response-Req标志被设置为ON。

[0490] 可选的“Ack”消息可被用于确认收到一个确认消息并把状态和/或上下文信息返回到发起者。在用来请求Ack消息的确认(Confirm)消息中,Response-Req标志被设置为ON。

[0491] WLCCP消息包含固定长度的头,后面跟着可选的、长度可变的TLV。

[0492] SCM发送周期性的SCM-通告-应答消息以在每个AP“本地”子网上通告网络参数和可用性,并有助于SCM选举协议。AP通过监视SCM通告为本地子网自动地发现活动的SCM。AP在“基本端口”上接收SCM通告并在“次级端口”上转发SCM,以把SCM和子网信息传播到SWAN拓扑中的后代节点。

[0493] 节点可以发送SCM-通告-请求消息来请求SCM-通告-应答消息(例如,为了缩短发现周期)。

[0494] CCM可以可选择地发送周期性的CCM-通告-应答消息来通告网络参数和可用性并有助于CCM选举协议。LCM和SCM通过监视CCM通告可以为本地子网自动地发现活动的CCM。CCM-通告请求和应答消息被发送到IP多播地址。

[0495] 节点能够发送CCM-通告-请求消息来请求CCM-通告-应答消息。

[0496] 注册请求消息用于为MN、AP或CM请求向SWAN基础结构的注册。SWAN节点总是向CCM以及在到该CCM路径上的每个LCM、SCM和AP注册。在SWAN拓扑中的单个分支上,注册请求总是被向内转发。有两种注册请求类型:产生“初始”注册请求来建立新的路径实例。“更新”注册请求被用来刷新路径实例并更新所缓存的动态的上下文信息。

[0497] CM返回注册应答信息确认收到注册请求,建立“路径实例”并返回包括任何“旧的移动绑定”的上下文信息。注册应答信息在无线链路上建立层2的转发路径。在相应请求的逆向路径上,注册应答总是被向外转发。

[0498] 使用预注册请求和预注册应答消息获取安全证书并在注册前为802.11MN或孩子AP建立认证状态。

[0499] 当台站漫游时,CM发送解除注册-请求消息以请求删除旧的路径实例。解除注册-请求总是由CM(SCM、LCM、或CCM)产生,并且在SWAN拓扑中的单个分支上总是向外转发。

[0500] AP或CM返回解除注册-应答信息以确认收到解除注册请求,删除相应的路径实例,并(可选择地)返回上下文和状态信息。在解除注册-应答中(可选择地)返回瞬时记帐统计和行动时间戳。

[0501] AP或CM向其双亲CM发送分离-请求消息以指示“分离的”孩子台站应该被“解除注册”。分离-请求消息被向内转发,直到它到达具有“更加新的”注册记录的CM或CCM为止。

[0502] CM可以发送分离-应答消息来确认分离请求。

[0503] 上下文请求消息用于获得或设置上下文、配置或者管理信息。上下文消息为交换信息提供通用的传送。例如,当台站从旧的LCM漫游到新的LCM时,上下文请求可以被用于开始横向越区切换。新LCM或旧LCM可以发送上下文请求。由旧LCM产生的上下文请求可以包含上下文和配置信息。上下文请求消息也能被用于有预见性地为MN把移动上下文转发给SCM或AP。(用于“获取”信息的上下文请求包含一个或更多的“请求”TLV。)

[0504] 上下文应答消息用于确认上下文请求消息。它也被用于给相应的上下文请求消息返回状态信息(例如为一个“设置”请求)或上下文、配置或管理信息(例如为一个“获取”请求)。

[0505] 路径更新请求消息用于无线台站在单个子网内从旧AP漫游到新AP时,在无线台站和每个对端主机之间重新建立逆向的学习路径。路径更新请求随着漫游的台站的源802地址被从新AP发送到旧AP。

[0506] 路径更新应答消息被可选择地用于确认收到路径更新请求消息,并被用于直接从“旧AP”向“新AP”传递瞬时上下文信息。

[0507] 路径检验消息用于实现可靠的路径更新机制(即从丢失的路径更新请求消息中恢复)。

[0508] 跟踪请求消息用于SWAN路径测试、响应时间分析和台站跟踪。

[0509] 跟踪应答用于确认收到了跟踪请求消息。

[0510] AAA消息是一般用于认证的封装的802.1X EAPOL消息。此外,AAA消息也能被归类于用于表示AAA消息交换的开始(START)或接收(SUCCESS)。最后,AAA消息也是一般被AP用于更新AS所保留的会话记帐的所封装的Cisco记帐消息。当MN使用Cisco中心密钥管理(CCKM)时,MN和MN认证者之间的初始密钥建立是通过由MN认证者向MN发送一个具有16字节的现时标志的EAPOL密钥消息,开始四路握手来触发的。为了实现此操作,使用AAA成功消息,把现时标志被从MN认证者传递到AP。在快速越区切换协议规范[8]中描述了密钥建立的细节。这是SWAM拓扑产生的唯一的EAPOL密钥消息,其他的均为802.1X EAP认证的结果。

[0511] AAA消息是802.1X EAPOL或Cisco会话记帐消息的WLCCP封装,因此不遵守请求-应答范式。但是,由于认证者能够检测到认证失败,在离开消息中提供的状态(Status)字段可以提供更多的信息以反映认证状态。

[0512] Path-Init请求、应答、确认、Ack.Path-Init消息用于IN路径认证,其中IN和其每个祖先相互认证并建立路径CTK。必要的路径认证四路握手可以包括1)Path-Init请求/应

答交换,随后是初始注册请求/应答 交换,或2)Path-Init请求/应答/确认/Ack交换。(第二个序列用于给注册的IN刷新路径CTK。)

[0513] WLCCP字段按网络字节和位顺序定义(即大端法)。每个字段中的位按从左到右编号,从‘0’开始(即高位是‘0’位)。

[0514] WLCCP消息可以被封装在以太网帧或UDP/TCP/IP包中。以太网封装能被用于处于同一子网上的两个AP或AP和SCM之间所发送的子网内消息。IP封装必须用于子网间的消息。WLCCP以太网DIX类型是0x872d。WLCCPUDP/TCP协议端口是十进制的2887。它是在互联网编号分配管理机构(Internet Assigned Number Authority)注册的“公知”的协议端口。

[0515] 单个WLCCP消息格式既用于以太网封装也用于IP封装。所有WLCCP消息共享下面定义的公共的头格式。定义头格式以使它不会与现有的以太网和IP DDP消息格式混淆。紧跟公共头的WLCCP消息体包含SAP专用的消息类型。本文档为WLCCP“上下文管理”SAP定义了消息格式,该SAP为‘0’。

[0516] 图20示出了示范性的以太网封装的WLCCP上下文管理帧2000。帧2000包括目的MAC地址2002、源MAC地址2004、DIX类型(本例为0x872D)2006,类型特定字段2012和可选的TLV 2014。

[0517] 总的来说,以太网封装可被用于限于单个子网的WLCCP消息。所有的子网间消息则需要IP封装。以太网封装用于SCM通告消息和子网内注册、解除注册、分离、路径更新和路径检验消息。UDP/IP封装用于CCM通告消息和子网间注册、解除注册、分离消息。以太网或UDP/IP封装均可用于跟踪消息。以太网、UDP/IP或TCP/IP封装可用于上下文消息。

[0518] 下面示出了以太网封装的WLCCP上下文管理帧2000的抽样的定义。

[0519] #define WLCCP_DIX_ETHER_TYPE 0x872d

[0520] #define WLCCP_DEF_UDP_PROTO_PORT 2887

[0521] #define WLCCP_IP_MCAST_ADDRESS 0xE0000128/*224.0.1.40*/

[0522] #define WLCCP_MCAST_ADDRESS_IN {0x01,0x40,0x96,0xff,0xff,0xC0}

[0523] 抽样WLCCP节点类型定义

[0524] #define WLCCP_NODE_TYPE_ANY 0

[0525] #define WLCCP_NODE_TYPE_AP 1

[0526] #define WLCCP_NODE_TYPE_SCM 2

[0527] #define WLCCP_NODE_TYPE_LCM 4

[0528] #define WLCCP_NODE_TYPE_CCM 8

[0529] #define WLCCP_NODE_TYPE_ICN 0x10/*基础结构客户节点*/

[0530] #define WLCCP_NODE_TYPE_CLIENT 0x40

[0531] #define WLCCP_NODE_TYPE_MULTI_MASK 0x8000

[0532] 抽样WLCCP端口类型的定义

[0533] #define WLCCP_PORT_TYPE_ETHER 1

[0534] #define WLCCP_PORT_TYPE_INTERNAL 2

[0535] #define WLCCP_PORT_TYPE_DOT11 0x80

[0536] #define WLCCP_PORT_TYPE_DOT11A 0x81

[0537] #define WLCCP_PORT_TYPE_DOT11B 0x82

[0538] #define WLCCP_PORT_TYPE_DOT11G 0x83

[0539] “内部端口”是共存于同一设备内的AP和SCM之间的逻辑端口。

[0540] #define WLCCP_PORT_COST_ETHER 10

[0541] #define WLCCP_PORT_COST_INTERNAL 10

[0542] #define WLCCP_PORT_COST_DOT11 50

[0543] #define WLCCP_PORT_COST_DOT11A 30

[0544] #define WLCCP_PORT_COST_DOT11B 50

[0545] #define WLCCP_PORT_COST_DOT11G 40

[0546] 1.1.1抽样混合常数

[0547] #define DEF_SCM_ADVERTISE_PERIOD FIVE_SECONDS

[0548] #define DEF_SCM_LISTEN_TIME 4*DEF_SCM_ADVERTISE_PERIOD

[0549] #define MAX_SCM_ELECT_TIME 6*DEF_SCM_ADVERTISE_PERIOD

[0550] #define MAX_SCM_AGE 8*DEF_SCM_ADVERTISE_PERIOD

[0551] 现在参考图21,有一个示出了WLCCP消息头2100字段的表格。列包含字段名2102、偏移2104、大小2106和消息头2100的每个字段的描述2108。

[0552] 固定的WLCCP头2100的长度是28字节。协议ID/Version 2110、WLCCP SAP 2112和目的节点类型2114这些字段对所有WLCCP SAP是公有的。剩余字段对所有上下文管理帧(即本文档中定义的所有的帧)是公有的。如果中继标志被设置为ON,则头后面紧跟着8字节的中继节点ID(Relay Node ID)字段。

[0553] #define WLCCP_PROTO_ID 0xC0

[0554] 定义了WLCCP协议ID(Protocol ID)2110,0xC0,以便WLCCP和DDP消息能共享同样的DIX以太网类型和UDP协议端口。附录B中定义了DDP消息头。

[0555] 目的节点类型(Destination Node Type)2114和WLCCP SAP 2112字段用于选择由以太网或IP目的地址所标识的设备内的内部目的地。发送者在发送WLCCP消息之前,必须把目的节点类型2114设置为紧邻接收者的节点类型。如果SAP唯一地标识了内部目的地,则目的节点类型2114可以是‘0’。

[0556] 跳计数(Hop Count)2116字段包含发起者和响应者之间的WLCCP跳的数量(减去一)。发起者或响应者必须把跳计数初始化为‘0’。跳计数由到发起者或响应者的路径上的每个中间节点增加。如果跳计数超过了WLCCP_MAX_HOP_COUNT,则丢弃该消息。

[0557] #define WLCCP_MAX_HOP_COUNT 25

[0558] #define WLCCP_PROTO_VERSION 1

[0559] #define WLCCP_CONTEXT_MGMT_SAP 0x00/*WLCCP(移动/上下文控制)*/

[0560] #define WLCCP_SECURITY_SAP 0x01

[0561] #define WLCCP_RRM_SAP 0x02/*无线资源管理*/

[0562] #define WLCCP_QOS_SAP 0x03

[0563] #define WLCCP_NM_SAP 0x04/*网络管理*/

[0564] #define WLCCP_MIP_SAP 0x05

[0565] WLCCP消息类型2118定义:

[0566] #define WLCCP_TYPE_SCM_ADVERTISE 1

- [0567] #define WLCCP_TYPE_CCM_ADVERTISE 2
- [0568] #define WLCCP_TYPE_REG 3
- [0569] #define WLCCP_TYPE_DEREG 4
- [0570] #define WLCCP_TYPE_DETACH 5
- [0571] #define WLCCP_TYPE_CONTEXT 6
- [0572] #define WLCCP_TYPE_PATH_UPDATE 7
- [0573] #define WLCCP_TYPE_PATH_CHECK 8
- [0574] #define WLCCP_TYPE_PREREG 9
- [0575] #define WLCCP_TYPE_TRACE 10
- [0576] #define WLCCP_TYPE_EAP_AUTHEN 11
- [0577] #define WLCCP_TYPE_PATH_AUTHEN 12
- [0578] WLCCP“应答”消息类型等于与WLCCP_TYPE_REPLY_MASK进行或运算的对应的请求类型Ored。
- [0579] #define WLCCP_TYPE_CONFIRM_MASK 0x80
- [0580] #define WLCCP_TYPE_REPLY_MASK 0x40
- [0581] 标志(Flags)字段2120如下使用：
- [0582] 在重新传输的请求或确认消息中把重试(Retry)标志设为ON。在重新传输的消息中的消息ID与在原始消息中的相同。如果重试标志在相应的请求消息中被设置为ON，则它在应答或Ack消息中被设置为ON。
- [0583] Response-Req标志在请求消息中被设置为ON以请求应答。
- [0584] TLV标志被设置为ON，表示可选的TLV跟着该固定字段。
- [0585] 进入标志(Inbound Flagand)、离开标志(Outbound Flag)和跳路由(Hopwise-Routing)标志确定WLCCP如何被转发(下面描述)。
- [0586] 如果根CM(Root CM)标志在进入消息中被设置为ON，则该消息总是被转发到位于整个拓扑树的根处的CM——“根”CM。如果根CM标志在离开消息中被设置为ON，则该消息在根CM处发出。
- [0587] 如果中继(Relay)标志被设置为ON，则WLCCP头后面紧跟着64位中继节点ID字段。(后面跟着48位节点地址的16位节点类型。)
- [0588] 在必须被认证并包含WTLV_MIC TLV的消息中，MIC标志被设置为ON。
- [0589] 响应者节点类型(Responder Node Type)位包含产生原始应答消息的WLCCP节点的节点类型。
- [0590] 发起者节点ID(Originator Node ID)2122一般标识发起请求消息的节点。响应者节点ID(Responder Node ID)2124一般标识请求消息的目标和对应的应答消息的源。在MN的WLCCP注册消息中，发起者节点ID是该MN的802地址。响应者节点ID在注册请求、通告请求或分离请求消息中可以是‘0’。响应者节点ID在任何IP封装的请求消息中可以是‘0’。响应者节点ID标识所请求的或未被请求的通告应答消息的源。
- [0591] 跳源节点ID(Hop Source Node ID)包含请求或应答消息的跳源的WLCCP节点ID。
- [0592] 在任何WLCCP消息中，可选参数可以跟在固定字段之后。可选参数在“TLV”格式中，如图22中所示。

[0593] TLV“类型”2210字段包含容器(Container)标志、加密(Encrypted)标志、请求(Request)标志、组(Group)ID和类型(Type)ID。在类型ID字段中,“请求TLV”使得请求标志被设置为ON。

[0594] #define WLCCP_TLV_CONTAINER_MASK 0x8000

[0595] #define WLCCP_TLV_ENCRYPTED_MASK 0x4000

[0596] #define WLCCP_TLV_GROUP_MASK 0x0300

[0597] #define WLCCP_TLV_REQUEST_MASK 0x0080

[0598] #define WLCCP_TLV_TYPE_MASK 0x007f

[0599] TLV组ID用于把TLV分层地分组。组ID能用于标识必须处理各个TLV类型的目标节点中的软件模块

[0600] 在WLCCP请求消息内的TLV中,请求标志被设置为ON以从目标WLCCP节点“请求”信息。“请求TLV”使得请求标志被设置为ON。

[0601] TLV容器标志可被用于把固定属性和其他可选的TLV分组为单个“容器TLV”。如果任何所需的TLV字段后面跟着其他可选的TLV,则在TLV中,容器标志应该只被设置为ON。容器TLV能够被嵌套。

[0602] TLV组ID:

[0603] #define WTLV_WLCCP_GROUP_ID 0x00

[0604] #define WTLV_SECURITY_GROUP_ID 0x01

[0605] #define WTLV_RRM_GROUP_ID 0x02/*无线资源管理*/

[0606] #define WTLV_QOS_GROUP_ID 0x03

[0607] #define WTLV_NM_GROUP_ID 0x04/*网络管理*/

[0608] #define WTLV_MIP_GROUP_ID 0x05

[0609] WLCCP TLV格式在下面的表格中定义。每个表格中的第一行包含TLV名、TLV ID和TLV描述。描述包括可以包含对应的TLV的消息类型的列表。在字段定义中不包括类型和长度字段。

[0610]

WTLV_NULL	0x0000	空TLV可被用于填充消息, 用于偶对齐。长度必须至少为 ‘4’。
-----------	--------	----------------------------------

[0611]

WTLV_CONTAINER	0x0001	通用的“容器”TLV用于把任意的TLV逻辑分组。
----------------	--------	--------------------------

[0612]

WTLV_AP_PORT_INFO		0x0002	AP 端口的类型、模式和地址。 Msgs: 包含在 AP 注册请求的 AP_PORT_LIST TLV 中。
字段名	偏移量	大小	字段描述
类型 (Type)	4	1	1 = 以太网 (Ethernet), 2 = Internal, 0x80 = 802.11, 0x81 = 802.11a, 0x82 = 802.11b, 0x83 = 802.11g
模式 (Mode)	5	1	1 = 双亲, 2 = 孩子, 3 = 双 亲/孩子 0x80 = 基本端口掩码
地 址 (Address)	6	6	802 硬件地址
NIC ID	12	2	用于在内部标识 NIC 类型的整 数。(例如 Venus 无线电)
版本字符串 TLV (可 选) (Version String TLV (optional))	14	N	

[0613]

WTLV_IPV4_SUBNET_ID		0x0003	IP 子网地址。 Msgs: 包含在 SCM 通告应答中用于通告 IP 地址和 SCM 的子网。可选择地包含在注册请求中的 PMIP_SSID_LIST TLV 中, 把 PMIP SSID 绑定到子网上。
字段名	偏移量	大小	字段描述
IPv4 地址 (IPv4 address)	4	4	IPv4 地址
前缀长度 (Prefix Length)	8	1	在子网掩码中的位的数量
标志 (Flags)	9	1	(保留—必须为 0)

[0614]

WTLV_SEC_LAN_ADDR_LIST		0x0004	次级 LAN 上的台站的以太网地址列表。Msgs: WLCCP 指定的网桥注册请求。
字段名	偏移量	大小	字段描述
计数 (count)	4	2	列表中地址的数量。
VLAN ID	6	2	次级 LAN 的 VLAN ID。‘0’ 值用于表示“本地 VLAN”。
地址列表 (Address List)	8	N X 6	以太网地址列表。

[0615]

WTLV_MCAST_ADDR_LIST		0x0005	所使能的多播以太网地址的列表。Msgs: 孩子 AP 注册请求。 (实现是可选的)
字段名	偏移量	大小	字段描述
计 数 (Count)	4	2	列表中地址的数量。
地 址 列 表 (Address) List	6	N X 6	多播以太网地址的列表。

[0616]

WTLV_IPV4_MCAST_ADDR_LIST		0x0006	被使能的多播 IPv4 地址的列表。Msgs: AP 注册请求。 (实现是可选的)
字段名	偏移量	大小	字段描述
计 数 (Count)	4	2	列表中地址的数量。
地 址 列 表 (Address) List	6	N X 4	多播 IPv4 地址的列表。

[0617]

WTLV_AP_PORT_LIST		0x0007	AP_PORT_INFO TLV 的列表(见上方)。Msgs: AP 注册请求。
字段名	偏移量	大小	字段描述
计数 (Count)	4	2	AP 端口数量。
Port List	6	N X 16	AP_PORT_INFO TLV 的列表。

[0618]

WTLV_SSID		0x0008	802.11 “请求者节点”的 SSID。如果“广播翻译”标志被设置为 ON，则台站使用广播 SSID。 Msgs: 预注册和注册请求/应答
字段名	偏移量	大小	字段描述
标志 (Flags)	4	1	第 0 位 – AAA 分配 (在应答消息中被设置为 ON 以便把 MN 分配给 SSID)。 第 1 位 – 广播解释 第 2 位 – IN WLCCP SSID 第 3-7 位 – (保留 – 必须为零)
长 度 (Length)	5	1	SSID 长度 (最大长度 = 32)
SSID	6	N	802.11 SSID

[0619]

WTLV_IPV4_ADDRESS		0x0009	“请求者节点”的 IPv4 地址 – 在请求消息中注册或在应答消息中返回。Msgs: 预注册、注册、上下文请求/应答。
字段名	偏移量	大小	字段描述
IP 地 址 (IP Address)	4	4	IPv4 地址

[0620]

WTLV_PARENT_AP_BSSID		0x000A	802.11 MN 或 AP “请求者节点” BSS 的 BSSID。Msgs: 802.11 台站的注册请求。
字段名	偏移量	大小	字段描述
BSSID	4	6	台站的当前 BSS 的 802.11 BSSID。

[0621]

WTLV_ OLD_AP_BSSID		0x000B	来自 802.11 重关联请求中的 “当前 AP”要素的 802.11 MN 或 AP “请求者节点”的先前的 BSSID。 Msgs: 对 802.11 台站的预注册 或注册请求。
字段名	偏移量	大小	字段描述
BSSID	4	6	台站的先前 BSS 的 802.11 BSSID

[0622]

WTLV_ PMIP_SSID_LIST		0x000C	容器 TLV, 它包含 SSID TLV, 并且对每个 SSID TLV, 它包含 0 或 更多的 MIPv4_AGENT TLV 或 SUBNET_ID TLV 的列表。仅在 HA 未 知而子网地址已知时包括可选的 SUBNET_ID。 Msgs: SCM 或 AP 注册请求。
字段名	偏移量	大小	字段描述
SSID TLV	4	N	包含 PMIP SSID 的 SSID TLV。 (针对每个 PMIP SSID 重复)
MIPv4_AGENT TLV	4 + N	6	绑定到 SSID 的缺省子网的 MIPv4 HA (针对子网上的每个 HA 重复)。

[0623]

WTLV_PARENT_CM (request)		0x008E	SCM 使用请求 PARENT_CM TLV 从 CCM 请求双亲 CM (LCM 或 CCM)。如果 SCM 先前被绑定到双亲 CM, 则节点 ID 字段必须包含旧双亲 CM 的节点 ID; 否则节点 ID 字段必须是 '0'。Msgs: 由 SCM 发送到 CCM 的上下文请求。
字段名	偏移量	大小	字段描述
节 点 ID (Node ID)	4	8	任何旧双亲 CM 的节点 ID 或 '0'。
IPv4 地址	12	4	任何旧双亲 CM 的 IPv4 地址或 '0'。

[0624]

WTLV_PARENT_CM		0x000E	CCM 使用 PARENT_CM TLV 把 SCM 分配给双亲 CM (LCM 或 CCM)。Msgs: 由 CCM 发送给 SCM 的上下文应答。
字段名	偏移量	大小	字段描述
节 点 ID (Node ID)	4	8	双亲 CM 的节点 ID。'0' 节点 ID 用于表示“无双亲 CM”。(即独立模式)。
IPv4 地址 (IPv4 address)	12	4	双亲 CM 的 IPv4 地址。

[0625]

WTLV_DELETED_NODE_LIST		0x000F	被删除节点的节点 ID 列表。 双亲 SCM 或 AP 使用 DELETED_NODE_LIST TLV 通知孩 子 AP，它必须重新注册。Msgs： SCM 通告应答
字段名	偏移量	大小	字段描述
计数（Count）	4	2	所删除的节点的数量。
节点实例(Node Instance)	6	12	8 字节节点 ID，后面跟着被删 除节点的 4 字节路径 ID。节点实例 字段针对每个所删除的节点重复。

[0626]

WTLV_MIPV4_AGENT		0x0010	IP 地址、子网前缀长度和 MIP HA 的能力。Msgs: 包含在 SCM 或 AP 注册请求中的 PMIP_SSID_LIST TLV 中。
字段名	偏移量	大小	字段描述
IPv4 地址 (Ipv4 address)	4	4	MIP 代理 IPv4 地址
前缀长度	8	1	代理的子网掩码中的位的数量。
标 志 (Flags)	9	1	第 0 位 – 静态配置 第 1-7 位 – (保留– 必须是零)
能 力 位 (Capability Bits)	10	2	能力位与 MIPv4 代理通告扩展中的最后 16 位相同: 第 0-8 位 – R、B、H、F、M、G、H 或 T 第 9-15 位 – (保留– 必须是零)
年 龄 (Age)	12	2	自从代理处接收到通告后以秒计算的逝去的时间。

[0627]

WTLV_OLD_AP_BINDINGS		0x0011	802.11 “请求者节点”的旧 AP 的节点 ID、IPv4 地址和 BSSID。 Msgs: 对 802.11 台站的预注册或注册应答。
字段名	偏移量	大小	字段描述
节 点 ID	4	8	旧 AP 的节点 ID。

[0628]

(Node ID)			
IP 地址 (IP address)	12	4	旧 AP 的 IPv4 地址
BSSID	16	6	旧 BSS 的 802.11 BSSID。

[0629]

WTLV_HOME_SUBNET		0x0012	代理 MIP MN 的 IP 地址、MIP HA 和子网前缀长度。 Msgs: 注册请求/应答
字段名	偏移量	大小	字段描述
IPv4 地址 (IPv4 address)	4	4	MN 的 IPv4 地址
前缀长度	8	1	MN 的本地子网掩码中的位的数量。如果该掩码未知，该字段可以为 '0'。
标志 (flag)	9	1	第 0 位 — 在本地标志 (如果 MN 在本地，设置为 0N) 第 1-7 位 — (保留— 必须是零)
HA 地址	10	4	MN 的 HA 的 IPv4 地址。在请求中它是 MN 的子网的缺省 HA。在应答中它是所分配的 HA。

[0630]

WTLV_LOST_LINK		0x0013	LOST_LINK TLV 用于报告丢失的基础结构链路。Msgs: 在注册请求中报告丢失的次级链路。丢失的 SCM 基本链路在上下文请求中被报告给 CCM。
字段名	偏移量	大小	字段描述
节点 ID (Node ID)	4	8	如果基本标志被设置为 ON, 则为双亲节点 ID, 否则为孩子节点 ID。
原因 (Reason)	12	1	原因代码。0 = 一般错误, 1 = 重试错误, 2 = 保留存活超时时间, 3 = 管理解除注册, 4 = 信标超时时间 (Beacon Timeout), 5 = 路径代价
标志 (flag)	13	1	第 0 位 – 基本 (对基本链路, 设置为 ON, 对次级链路设置为 OFF。) 第 1-7 位 – (保留– 必须为零)

[0631]

WTLV_VERSION_STRING		0x0014	AP 或 CM “请求者节点” 的硬件和软件版本。Msgs: 注册请求
字段名	偏移量	大小	字段描述
HW 版本长度 (HW Version Length)	4	1	以字节计算的 HW 版本字符串长度。该长度可以包括 “null” 填充字节。
HW 版本 (HW Version)	5	M	HW 版本字符串

[0632]

SW 版本长度 (SW Version Length)	5+M	1	以字节计算的 SW 版本字符串长度。该长度可以包括“null”填充字节。
SW 版本 (SW Version)	6+M	N	SW 版本字符串

[0633]

WTLV_NAME		0x0015	MN、AP 或 CM “请求者节点”的网络接入标识符 (NAI) 或域名。 Msgs: 注册请求
字段名	偏移量	大小	字段描述
名字类型 (Name Type)	4	1	1 = NAI, 2 = 域名
名字长度 (Name Length)	5	1	以字节计算的字符串长度
名字 (Name)	6	N	包含 NAI 或域名的字符串。

[0634]

WTLV_SYSTEM_ID		0x0016	系统 ID 值。Msgs: 注册请求
字段名	偏移量	大小	字段描述
产品 ID (Product ID)	4	2	用于在内部标识产品类型（例如 Ivory AP）的整数。
版本字符串 TLV (Version String TLV) (可选)	NA	M	可选的 VERSION_STRING TLV – 它可以包含 HW 和/或 SW 版本。

[0635]

系统名 TLV (可选)	NA	N	可选的 NAME TLV —— 它包含系统名。
-----------------	----	---	-------------------------

[0636]

WTLV_NODE_ID_LIST		0x0018	节点 ID 的列表，对到根 CM 的路径上的每个节点具有条目。Msgs: Path-Init 请求/应答
字段名	偏移量	大小	字段描述
计 数 (Count)	4	2	列表中的节点 ID 的数量。
节点 ID 列表 (Node ID List)	6	8 X N	节点 ID 的列表。

[0637]

WTLV_MIP4_REG_REQ		0x0019	SCM 发送 MIP_REG_REQ 容器 TLV 来触发双亲 AP 为请求者节点发送 MIP 注册请求。如果 MN “在本地”，则发送 MIP “解除注册请求”。 Msgs: MN 注册应答
字段名	偏移量	大小	字段描述
标志 (flag)	4	2	第 0 位 – 在本地标志(如果 MN 在本地则设置为 ON。) 第 1-15 位 – (保留– 必须是零)
本地子网 绑定 (Home subnet bindings)	6	N	HOME_SUBNET TLV (有可能只使用 HOME_SUBNET TLV 中一个标志。)

[0638]

WTLV_AUTH_METHOD		0x001A	用于“请求者节点”的认证方法。如果节点使用快速重认证，则快速重认证标志被设置为 ON。 Msgs: 预注册和注册请求
字段名	偏移量	大小	字段描述
基 类 型 (Base Type)	4	2	无 = 0, 开放 (Open) = 0x0001, 共享密钥 = 0x0002, LEAP = 0x0004, EAP = 0x0008, MAC 地址 = 0x0010, 其他 = 0x0020, 客户 = 0x0040, 未知 = 0x8000
EAP 类 型 (EAP Type)	5	1	
快速重认 证 (Fast Reauthenticat ion)	6	1	第 0 位 -快速重认证标志 第 1-7 位 -快速重认证类型。 CCKM = 1

[0639]

WTLV_IPV4_HOP_ADDRESS		0x001B	IPV4_HOP_ADDRESS TLV 用于通告 AP 的 IP 地址。 Msgs: AP 产生的 SCM 通告应答。
字段名	偏移量	大小	字段描述
IP 地 址 (IP Address)	4	4	AP IPv4 地址

[0640]

WTLV_EAP_IDENTITY		0x001C	“请求者节点”的 EAP 身份字符串。 Msgs: 预注册和注册请求
字段名	偏移量	大小	字段描述
EAP ID 长度 (EAP ID Length)	4	1	以字节计算的 EAP ID 长度。
EAP ID	5	N	包含来自节点的 EAP 身份响应消息的 EAP ID 的字符串。

[0641]

WTLV_MN_1X_AUTHEN		0x001E	802.1X MN 认证者的节点 ID 和 IPv4 地址。 Msgs: IN 注册应答和 SCM 通告应答。TLV 包含在 SCM 通告消息中以通告 MN 认证者的变化。
字段名	偏移量	大小	字段描述
节点 ID (Node ID)	4	8	802.1X MN 认证者的节点 ID。
IPv4 地址 (IPv4 Address)	12	4	802.1X MN 认证者的 IPv4 地址。

[0642]

WTLV_ROOT_CM_INFO		0x001F	WLCCP 根 CM 的节点 ID 和 IPv4 地址。 Msgs: SCM 通告应答
字段名	偏移量	大小	字段描述
节点 ID (Node ID)	4	8	根 CM 的节点 ID。
IPv4 地址 (IPv4 Address)	12	4	根 CM 的 IPv4 地址

[0643]

WTLV_REPLY_STATE		0x0020	不透明处理状态信息。请求消息中所包含的 REPLY_STATE TLV 必须按顺序被复制到应答消息。
字段名	偏移量	大小	字段描述
节 点 ID (Node ID)	4	8	进入 TLV 的节点的节点 ID。
状态	12	N	不透明处理状态信息。

[0644]

WTLV_MN_REG		0x0021	MN_REG TLV 包含注册 MN 所需的任何信息。它包含在 MN_REG_LIST TLV 中。任何未描述的字段被定义为和注册头中的相应字段相同。
字段名	偏移量	大小	字段描述
请求者节点 ID (Requestor Node ID)	4	8	MN 的 WLCCP 节点 ID。
路 径 ID (Path ID)	12	4	在应答消息中包含分配给 MN 的路径 ID。
注册标志 (Registration Flags)	16	2	
VLAN ID	18	2	
状 态 (Status)	20	1	
年龄 (Age)	21	1	自从上次 MN 处于活动以来的秒数。
可 选 的 TLV (Optional TLVs)	22	N	通过设置容器标志为 ON 可以包含可选的 TLV (例如 IPV4_ADDRESS 或 SSID)。

[0645] 任何未包含在WTLV_MN_REG TLV中的参数都取自注册消息或封装WTLV_MN_REG_LIST TLV。

[0646]

WTLV_MN_REG_LIST		0x0022	MN_REG TLV 的列表和 o。
字段名	偏移量	大小	字段描述
MN_REG TLVs 另一可选 TLV。（MN_REG TLVs an other optional TLVs.）	4	N	除了 MN_REG TLV 以外的任何 TLV，为后续 MN_REG TLV 建立缺省的参数值。

[0647] 下面的表格示出了用于SCM通告应答消息的字段。

[0648]

字段名	偏移量	大小 (字节)	字段描述
WLCCP 头 (WLCCP Header)	0	28	公共上下文管理SAP头。（Common Context Mgmt SAP Header）
跳地址 (Hop Address)	28	6	源802端口地址
SCM标志 (SCM Flags)	34	2	第15位-活动标志。在来自 活动的SCM的通告中设置为ON。 第14位-计划外标志(在计划外 通告消息中设置为ON) 第13位-未连接标志*(在来 自未连接的节点的通告中设置为 ON。) 第12位-层2的更新标志(如 果能够进行WLCCP层2的路径更

[0649]

			新,则设置为ON.缺省时设置为 OFF。) 第0-11位-(保留-必须是 零)
SCM选举 组(SCM Election Group)	36	1	(保留到将来使用-必须是零)
连接计数 (Attach Count)	37	1	跳源的连接计数
SCM优先 权(SCM Priority)	38	1	第1-7位-从0(最低)到 127(最高)的SCM优先权值。 第0位-优选标志-如果 SCM是“优选SCM”则设置为OFF。
网桥优先 权(Bridge Priority)	39	1	第1-7位-从0(最低)到127(最 高)的网桥优先权值。 第0位-网桥禁止标志.设置 为ON表示次级桥接被禁止。网桥优 先权用于在非STP次级以太网局域网 网上协商WLCCP所指定的网桥。
实例年龄 (Instance Age)	40	4	以秒计算的SCM的“实例年 龄”。
SCM节点 ID(SCM Node ID)	44	6	SCM的WLCCP节点ID
路径代价 (Path Cost)	50	2	到SCM的路径上的端口的代价 总和。

[0650]

跳计数 (Hop Count)	52	1	在到SCM的路径上的无线跳的 数量。
通告周期 (Advertiseme nt Period)	53	1	SCM通告之间的平均秒数。
(可选 TLV)	54	N	(下面定义所需的TLV)

[0651] *双亲节点发送未连接标志被设置为ON的SCM通告请求,以便迅速地通知孩子节点它已经变成“未连接的”。如果它因为活动的SCM被丢失而未连接,则它必须也把SCM节点ID设置为‘0’。

[0652] 实例年龄字段包含传输SCM通告应答消息的节点的实例的以秒计算的“年龄”。(见名为“拓扑状态信息”的部分关于“实例数量”的描述。)

[0653] SCM通告应答消息必须包括WTLV_SUBNET_ID TLV,它包含SCM的IP地址和子网掩码。

[0654] SCM通告应答消息必须包括WTLV_ROOT_CM_INFO TLV,它包含根CM的Ipv4地址(根

CM也是802.1X IN认证者)。

[0655] AP发送的SCM通告应答消息可以包括WTLV_IPV4_HOP_ADDRESS TLV,它包含AP的IP地址。

[0656] #define SCM_ADVERTISE_INTERVAL 5 /*缺省的SCM通告间隔是5秒。*/

[0657] #define SCM_INFINITE_PATH_COST 0xFFFF

[0658] #define SCM_INFINITE_HOP_COUNT 0xFF

[0659] 下面的表格示出了SCM通告请求消息的字段。

[0660]

字段名	偏移量	大小 (字节)	字段描述
WLCCP 头 (WLCCP Header)	0	28	公共上下文管理SAP头*
跳地址 (Hop Address)	28	6	源802端口地址
(可选 TLV) (optional TLVs)	34	N	

[0661] 下面的表格给出了用于注册请求/应答消息的字段。

[0662]

字段名	偏移量	大小(字节)	字段描述
WLCCP 头 (WLCCP Header)	0	28	公共上下文管理SAP头
中继节点 ID(Relay Node ID)	28	8	中继节点类型和节点地址
802跳地址(802 Hop Address)	36	6	802源端口接口地址。
请求者节点ID	42	8	“请求”网络注册的节点的 WLCCP节点ID。在“代理”请求

[0663]

(Requester Node ID)			中,它是MN的802地址。
注册子类型标志 (Registration Sub Type Flags)	50	1	第7位-初始注册标志 第6位-代理注册标志 第5位-列表注册标志 第0-5位(保留-必须是零)
桥接标志 (Bridging Flags)	51	1	第7位-次级网桥标志 第6位-单播泛滥标志 第5位-多播泛滥标志 第4位-IP多播泛滥标志 第0-3位-(保留-必须是零)
注册标志 (Registration Flags)	52	2	第15位-已认证标志 第14位-(保留-必须是零) 第13位-代理MIP标志 第12位-层2的路径更新(0= 禁止,1=使能) 第0-11位-(保留-必须是零)
延迟 (Delay)	54	2	请求消息中,自从节点上次活动以来达数百秒的时间。
路径ID (Path ID)	56	4	CM建立的路径ID。‘0’值用于表示“无路径ID”
寿命 (Lifetime)	62	1	以分钟计算的注册寿命。‘0’值 用于表示“无限”的寿命。
状态 (Status)	63	1	应答消息中的注册状态。 0-126-良好状态 127-(保留) 128-254-错误状态 255-扩展错误状态。(扩展错

[0664]

			误状态包含在TLV中。)
VLAN ID	64	2	第3位-分配的标志。如果 VLAN ID由基础结构分配,则在应答中被设置为ON。第4-15位-请求者节点的 VLAN ID。(可以是0)。
(可选 TLV) (Optional TLVs)	66	N	

[0665] #define WLCCP_DEF_AP_REG_LIFETIME 10 /*10minutes*/

[0666] #define WLCCP_DEF_CM_REG_LIFETIME 10

[0667] #define WLCCP_DEF_MN_REG_LIFETIME 0 /*infinite*/

[0668] 在应答消息中,状态字段包含注册状态。从0到126的值被用于表示“良好”状态。高位被设置为ON表示错误状态。从128到254的值被用于返回错误状态。值255用于表示扩展错误状态代码包含在WTLV_STATUSTLV之中。

[0669] 注册应答状态代码:

[0670] 0-一般良好状态

[0671] 0x80-一般错误状态

[0672] 0x81-未被认证。请求者节点没有被认证。

[0673] 0x82-路径错误。检测到路径错误。例如,如果双亲或中继节点没有注册,则将会发生错误。

[0674] 0x83-无效的更新。更新注册请求与当前路径实例不匹配或者路径实例不存在。

[0675] 0x84-顺序混乱。接收注册请求的顺序混乱。

[0676] 0x85-发生了MIC错误。

[0677] 0x86-Admin.禁止。请求者节点在管理上被禁止。

[0678] 0x87-最大节点。因为超过了注册节点的最大数量,注册被拒绝。

[0679] 0x88-存储器。注册错误因缺乏内部资源而发生。

[0680] 在对MN的请求中,已认证标志被设置为0N,表示该MN已经被双亲AP所认证。标志用于在AP从分布式转移到基础结构模式时注册已认证的MN。对于不要求认证的MN(即开放认证(open authentication)),它也被设置为0N。

[0681] 在用于代理MIP MN的注册消息中,代理MIP标志被设置为0N。

[0682] 如果使能了WLCCP层2的路径更新,则层2的路径更新标志被设置为0N。

[0683] 在对MN的初始注册请求中,VLAN ID被设置为用于MN的SSID的缺省VLAN ID。如果所分配的VLAN ID标志被设置为0N,则在对MN的初始应答消息中的VLAN ID包含所分配的VLAN ID。在对孩子AP的请求中的VLANID总是‘0’。在对孩子AP的初始应答中的VLAN ID是AP的本地VLANID。(孩子AP从其双亲AP继承它的本地VLAN ID)。在重定密钥请求或应答中的VLAN ID可以是‘0’或者是用于请求者节点的当前VLAN ID。

[0684] WTLV_IPV4_ADDRESS TLV总是包含请求者节点的IP地址。IP地址包含在将其向WLCCP基础结构注册的请求当中。IP地址包含在对MN的应答中,该MN把它传递到新的双亲AP。

[0685] 对MN的初始注册请求必须包括包含MN认证类型的WTLV_AUTH_METHODTLV。

[0686] 对802.11台站(MN或孩子AP)的初始注册请求必须包括包含来自台站的802.11(重)关联请求消息的SSID的WTLV_SSID TLV。

[0687] 对802.11台站(MN或孩子AP)的初始注册请求必须包括包含台站的双亲AP的BSSID的WTLV_PARENT_AP_BSSID TLV。

[0688] 对已经“重关联”的802.11台站的初始注册请求必须包括包含来自对应的802.11重关联请求消息中的“旧AP”字段的BSSID的WTLV_OLD_AP_BSSID TLV。

[0689] 对AP的注册请求必须包括包含一个或多个WTLV_AP_PORT_INFO TLV列表的WTLV_AP_PORT_LIST容器TLV。

[0690] 如果台站先前与“旧AP”关联,则对802.11台站的注册应答必须包括WTLV_OLD_AP_BINDINGS TLV。

[0691] 下面的表格示出了预注册请求/应答消息的格式。

[0692]

字段名	偏移量	大小 (字节)	字段描述
WLCCP 头 (WLCCP Header)	0	28	公共上下文管理SAP头
中继节点 ID(Relay Node ID)	28	8	中继节点类型和节点地址
请求者节点ID (Requester Node ID)	36	8	孩子802.11台站(MN或孩子 AP)的WLCCP节点ID。
预注册标志 (Preregistration Flags)	42	2	第0-15位-(保留-必须是零)
(保留) (reserved)	44	1	(必须是零)
状态 (Status)	45	1	应答消息中的预注册状态。 0-良好状态
VLAN ID	46	2	第0-2位-(保留-必须是零) 第3位-所分配的VLAN标志 第4-15位-请求者的节点

[0693]

			ID(可以是0)。请求消息中的缺省 VLAN ID。应答消息中的可选的、所分配的VLAN ID。
(可选TLV)	48	N	

[0694] 在对MN的预注册请求中的VLAN ID被设置为用于该MN的SSID的缺省VLAN ID。如果被分配VLAN ID标志被设置为0N,则在对MN的应答消息中的VLAN ID包含所分配的VLAN ID。在对孩子AP的请求中的VLAN ID总是‘0’。在对孩子AP的应答中的VLAN ID是该AP的本地VLAN ID。(孩子AP从其双亲AP继承它的本地VLAN ID。)

[0695] 对802.11台站(MN或孩子AP)的预注册请求必须包括包含来自台站的802.11(重)关联请求消息的SSID的WTLV_SSID TLV。

[0696] 对已“重关联”的802.11台站的预注册请求必须包括包含来自相应的802.11重关联请求消息中“旧AP”字段的BSSID的WTLV_OLD_AP_BSSID TLV。

[0697] 如果台站先前与“旧AP”关联,则对802.11台站的预注册应答必须包括WTLV_OLD_AP_BINDINGS TLV。

[0698] 参考下面的表格,示出了解除注册请求/应答消息。

[0699]

字段名	偏移量	大小 (字节)	字段描述
WLCCP头	0	28	公共上下文管理SAP头
中继节点ID	28	8	中继节点类型和节点地址
路径ID	36	4	CM所建立的路径标识符。
状态	40	1	请求中的“原因”代码;应答 中的“状态”值。在“管理”解除 注册请求中,原因代码的高位被设

[0700]

			置为0N。
解除注册 标志	41	1	第7位-层2的路径更新(0= 禁止,1=使能) 第0-6位-(保留-必须是零)
注册消息 ID	42	2	接收到的对节点的上次注册请 求的消息ID。
目标节点 ID	44	8	其路径实例必须被“删除”的 节点的WLCCP节点ID。
活动时间 戳	52	2	在应答消息中,自从目标节点 上次处于活动以来的秒数。
(可选 TLV)	54	N	

[0701] 下面示出了分离请求/应答消息的格式:

[0702]

字段名	偏移量	大小 (字节)	字段描述
WLCCP头	0	28	公共上下文管理SAP头
中继节点ID	28	8	中继节点类型和节点地址
路径ID	36	4	CM所建立的路径标识符。
状态	40	1	请求中的“原因”代码;应答 中的“状态”值。
分离标志	41	1	第7位-层2的路径更新(0= 禁止,1=使能) 第0-6位-(保留-必须是零)
请求者节点ID	42	8	其路径实例必须被“删除”的 节点的WLCCP节点ID。
(可选	5	N	

[0703]

TLV)	0		
------	---	--	--

[0704] 在下面的表格中示出了路径检验请求/应答消息:

[0705]

字段名	偏移量	大小 (字节)	字段描述
WLCCP头	0	28	公共上下文管理SAP头
中继节点ID	28	8	中继节点类型和节点地址
路径ID	36	4	CM所建立的路径标识符。
状态	40	1	请求中的“原因”代码;应答 中的“状态”值。

查询标志	41	1	(保留——必须是零)
双亲节点ID	42	8	开始“路径检验”的双亲AP的 节点ID。
(可选TLV)	50	N	

[0706] 后面定义了路径检验的用法。

[0707] 下面示出了路径更新请求/应答消息：

[0708]

字段名	偏移量	大小 (字 节)	字段描述
WLCCP头	0	28	公共上下文管理SAP头
路径ID	28	4	CM建立的路径标识符。
更新标志	32	2	(保留-必须是零))
双亲节点ID	34	8	新的双亲AP的节点ID。
(可选TLV)	42	N	

[0709] 应该注意,如果无需直接从旧AP向新AP传递上下文信息,则解除关联通知消息可以代替路径更新消息使用。

[0710] 在下面的表格中给出了上下文请求/应答消息的格式：

[0711]

字段名	偏移量	大小 (字 节)	字段描述
WLCCP头	0	2 8	公共WLCCP上下文管理SAP头
(可选TLV)	28+N	P	

[0712] WLCCP AAA用于封装EAPOL和例如Cisco的私有记帐消息,所以该消息能够被转发到/转发自在WLCCPMN或IN认证者中的WLCCP安全SAP。例如,转发器AP或MN的EAPOL消息将被其双亲AP做WLCCP封装。此外,AP可以用会话记帐报告来更新AS,因此必须发送适当的Cisco私有消息。

[0713] AAA消息无需加密,因为它们一般或者已经受到初始协议的保护(例如EAPOL或Cisco记帐),或者它们不需要认证。但是,对认证消息进行认证(MIC)是良好的安全练习。

[0714] 作为选择,仅有MN的EAPOL消息应该包括WTLV_MIC。如果包括了WTLV_MIC TLV,则所包含的MIC使用链路的CTK认证整个WLCCP消息。例如,如果AP把消息传输给SCM,则应该使用AP和SCM之间共享的CTK。如果MIC被使能,则在进入(或离开)路径中的每一跳必须认证并重新计算MIC。

[0715] 最后,AAA消息也必须表明状态机是否已进入AAA消息以及它已在何时完成。为了准备这些状态,据此,AAA消息被进一步归类。

[0716] 封装的EAPOL和例如Cisco的私有记帐消息的一般格式如下：

[0717]

字段名	偏移量	大小 (字节)	字段描述
WLCCP头	0	28	公共上下文管理SAP头
请求者节点ID	28	8	正在“请求”网络认证的节点 的WLCCP节点ID。
AAA类型	36	1	AAA协议消息类型： 0-启动 1-完成 2-EAPOL 3-Cisco记帐
认证类型	37	1	如果AAA类型=EAPOL认证, 则它可能是下列类型之一： 0-仅为EAP 1-仅为MAC 2-首先执行MAC,如果它失败 则执行EAP 3-执行MAC和EAP 4-仅为LEAP 5-首先执行MAC,如果它失败 则执行LEAP 6-执行MAC,然后执行LEAP
密钥管理类型	38	1	所协商的密钥管理类型,或没 有任何所协商的密钥管理类型。有 效值是： 0-无 1-CCKM 2-遗留的802.1X 3-SSN/TG
状态	39	1	状态字段

[0718]

消息	40	N	AAA消息
----	----	---	-------

[0719] WLCCP AAA消息起到了几个作用：

[0720] 1. 区别AAA状态的进入和退出

[0721] 2. 封装由AP发送到AS用于报告记帐信息的Cisco记帐消息。

[0722] 3. 封装EAPOL认证消息。第一个WLCCP(请求)消息必须定义密钥管理类型以便由MN认证者触发会话密钥动作。如果定义了CCKM,则MN认证者在接收到Radius访问认可后,将用被安全传送的NSK触发EAPOL密钥消息。否则,MN认证者将临时保存NSK以便转发给AP。(但是在预注册请求之后将去除MN的条目)

[0723] 4. 封装从MN认证者到MN的EAPOL密钥消息,以开始MN认证者和MN之间的CCKM的初始4消息握手以建立KRK和BTK。

[0724] 如果AAA消息是启动(start)类型,则消息格式仅是请求消息。(不期望应答)。启动消息不仅开始AAA消息交换的启动,还提供SSID信息以及随后的AAA认证或记帐消息。随后的AAA消息必须在启动请求中所定义的AAA认证和密钥管理类型上都匹配。其格式如下：

[0725]

字段名	偏移量	大小 (字节)	字段描述
WLCCP头	0	28	公共上下文管理SAP头
请求者节点ID	28	8	正在“请求”开始AAA消息交换 的节点的WLCCP节点ID。
AAA类型	36	1	0-用于启动
认证类型	37	1	如果AAA类型=EAPOL认证,则 它可以是下列类型之一: 0-仅为EAP 1-仅为MAC 2-首先执行MAC,如果它失败则

[0726]

			执行EAP 3-执行MAC和EAP 4-仅为LEAP 5-首先执行MAC,如果它失败则 执行LEAP 6-执行MAC,然后执行LEAP
密钥管理类型	38	1	协商的密钥管理类型,或没有任 何所协商的密钥管理类型,有效值是: 0-无 1-CCKM 2-遗留802.1X 3-SSN/TGi
状态	39	1	字段值被忽略
TLV	40	N	SSID TLV

[0727] 当AAA认证或记帐交换完成时,必须发布AAA完成(应答)消息以结束AAA状态。AAA完成也被用于表示AAA成功。(例如EAP或记帐成功)。如果AAA完成是成功的并且CCKM被定义为密钥管理,则完成消息也包括现时标志。AAA完成消息的格式如下：

[0728]

字段名	偏移量	大小 (字节)	描述
WLCCP头	0	28	公共上下文管理SAP头
请求者节点ID	28	8	正在“请求”开始AAA消息交换 的节点的WLCCP节点ID。
AAA类型	36	1	1-用于完成
认证类型	37	1	类型必须和在AAA启动中所定义 的匹配。

[0729]

密钥管理类型	38	1	类型必须和在AAA启动中所定义 的匹配。
状态	39	1	0-成功
现时标志长度	40	2	应当总是被设置为16字节
现时标志	42	16	16字节伪随机值

[0730] 下面的表格示出了Path-Init请求/应答/确认/ACK消息的格式：

[0731]

字段名	偏移量	大小 (字节)	描述
WLCCP头	0	28	公共上下文管理SAP头
中继节点	28	8	任何中间的中继AP的节点 ID。
请求者节点ID	36	8	要建立和IN认证者共享的CTK 的“请求”节点的WLCCP节点ID。
保留	44	1	用于字节对齐而保留
状态	45	1	状态字段
TLV(s)	46	N	包括安全上下文或建立CTK的 初始会话TLV。

[0732] 请求者节点在初始会话TLV中必须包括安全上下文TLV,以确保CTK在请求者节点和其IA之间相互导出。在安全上下文TLV中,请求者节点必须提供其现时标志和CTK序列计数器,以允许IA导出CTK,并确保请求不是应答。在初始版本中,如果检测到重放,则可以抛弃重定密钥;序列计数器应该足够大以使重定密钥可以永远不会用尽。但是,当值要绕回时,IN必须重认证。参考安全上下文TLV上的部分以得到关于建立CTK的进一步的细节。

[0733] 下面的802.11要素用于支持WLCCP的操作。

[0734] #define WLCCP_PATH_COST

[0735] #define WLCCP_HOP_COUNT

[0736] #define IPv4_SUBNET_ID

[0737] #define MULTICAST_802_ADDRESS_LIST

[0738] #define DOT1D_PATH_COST

[0739] #define DOT1D_ROOT_ID /*802.1D priority and 802 address of the root bridge*/

[0740] 在标准的802.11 SSID要素中包含WLCCP AP间的SSID。

[0741] 下面公开该体系结构一般的操作。

[0742] 请求消息总是从发起者被转发到响应者。应答消息总是从响应者转发到发起者。进入和离开标志确定怎样转发消息。如果进入和离开标志均被设置为OFF,则通过IP路由和/或透明桥接把消息转发到目标目的地。(即到达请求消息中的“响应者”)。

[0743] 在消息中进入标志或离开标志被设置为ON以表示该消息在拓扑树的分支上分别正被向内或向外转发。如果节点从非后代节点接收到“进入”消息,则它是个错误。如果节点从非祖先节点接收到“离开”消息,则它也是个错误。

[0744] 在进入或离开消息中跳路由标志被设置为ON,以迫使中间AP处理该消息,其中,“中间AP”是在拓扑树分支上,消息的发起者和响应者之间的任何AP。“跳路由的”进入消息被转发到双亲节点的跳地址;离开消息被转发到目标节点的路径上的“下一跳”。跳路由的消息由进入或离开路径上的每个节点处理。如果节点从非邻居的跳源接收到跳路由的消息,则它是个错误。

[0745] 例如,在注册消息中可以使用跳路由标志来更新到MN的路径上的每个AP中的层2的路径信息。在AP产生的代理注册消息中,响应者总是SCM。图23示出了如何使用跳路由。如果使能了层2的路径更新(如在W2实现中那样),则转发注册消息,跳路由被设置为ON。如果未使能层2的路径更新(如在W1实现中那样),则转发注册消息,跳路由被设置为OFF。

[0746] 如果在WLCCP消息中,中继标志被设置为ON,则一般的WLCCP头后面紧跟着中继节点ID字段。如果中继节点ID字段非零,则它包含“中继”相应的消息的任何中间节点的节点ID。发起者和响应者都把中继节点ID初始化为全零。如图23所示,AP 2304是从AP 2306发送到SCM 2302的跳路由的消息的中继节点;因此,AP 2304必须把中继标志设置为ON,并在向内往SCM转发该消息前在中继节点ID字段输入其节点ID。

[0747] 如果在进入请求消息中根CM标志被设置为ON,则该消息总是被向内转发到位于整个拓扑树根处的CM——根CM。例如,在校园网中,该消息被转发到CCM。例如,AP能使用根CM标志把MN的IP地址转发到CCM。AP能仅仅向其包含MN的IP地址并使得根CM标志被设置为ON的双亲SCM发送请求消息。

[0748] 在很多情况中,请求消息的初始响应者必须在到最终目的地的路径上转发该消息。例如,如果SCM不是“最近共同祖先”或者假如根CM标志被设置为ON,则该SCM必须向其双亲LCM转发进入注册请求。类似地,LCM必须向目标节点的双亲SCM转发离开的解除注册请求。初始的或中间的“中继响应者”如下转发这样的消息:a)响应者字段随着下一跳CM的节点ID来更新,b)中继响应者在中继节点ID字段输入其节点ID,c)发起者和消息ID字段不变。中继响应者在任何对应的应答消息中不更新响应者字段;因此,应答消息中的响应者字段在其被发起者接收时将包含“最终响应者”的节点ID。

[0749] 请求消息的发起者把Response-Req标志设置为ON以请求对应的应答消息。如果没有接收到期待的应答消息,则发起者总是负责错误恢复。发起者必须给每个要求应答的未解决的请求消息启动一个“重试定时器”。如果在对应的定时器到期之前没有接收到期待的应答消息,则重新传输带有设置为ON的重试标志和原始的消息ID的请求消息。在中间的“中继响应者”中不需要重试定时器,该“中继响应者”在到最终响应者的路径上转发请求消息。

[0750] 发起者或中继节点在请求消息中可以包括Reply_State TLV,以便减少必须保存在存储器中的状态信息的数量。Reply_State TLV包含处理(例如转发)应答消息所必需的信息。

[0751] AP消息转发逻辑一般独立于网络基础结构。在AP产生的消息中,双亲SCM是响应者,有一个例外。(如果使能层2的路径更新,则在非根AP产生的初始注册请求中,响应者是双亲AP)。在本地或校园基础结构中,SCM按要求把AP消息转发到根CM。类似地,SCM消息转发逻辑在独立的本地基础结构或校园基础结构中与之相同。双亲LCM在SCM产生的消息中总是响应者。在校园网中,LCM按要求把SCM消息转发到CCM。

[0752] WLCCP节点只接受在其本地VLAN上所传输的“有效”WLCCP消息。所有的其他消息被抛弃。如果消息未通过消息完整性检验或消息类型未知,则它是无效的。

[0753] SCM选举和通告协议用于给每个子网选举单个活动的SCM并通告网络可用性和网络参数。已注册的活动SCM向WLCCP“全节点”802组地址发送“SCM活动”标志被设置为ON的周期性SCM通告应答消息。无论何时只要SCM实例改变,则AP选择其“基本端口”并向活动的SCM注册。

[0754] SCM选举和通告的一般操作步骤如下:

[0755] 1)用非零SCM优先值在每个子网上配置一个或更多的“SCM候选者”。

[0756] 2)作为选择,每个SCM候选者可以与根CM认证以建立共享的WLCCP多播密钥。多播密钥用于可选择地认证多播SCM通告消息。(如果SCM通告消息没有被认证,则把认证推迟到活动的SCM被选举出来之后。)

[0757] 3)每个SCM候选者向CCM发送上下文管理请求消息。CCM把SCM候选者分配给双亲LCM,或者引导它在上下文应答消息中以独立模式操作。

[0758] 4)在校园基础结构模式中,每个SCM候选者开始与其所分配的LCM和CCM的路径认证。

[0759] 5)在每个子网中,SCM候选者参与SCM选举协议,为每个子网确定活动的SCM。

[0760] 6)在校园基础结构模式中,选择的“活动SCM”和其所分配的LCM和CCM注册。

[0761] 7)如果活动SCM变得未连接,则重复步骤3-5。

[0762] 8)在基础结构模式中,活动SCM仅在其已经成功地与根CM注册之后才开始产生“活

动”的SCM通告(即活动标志被设置为ON的通告)。

[0763] 9)根AP必须向活动的SCM注册并传播活动的SCM通告。

[0764] 10)其他AP必须向活动的SCM注册并传播活动的SCM。已注册的双亲AP在孩子AP被认证之后,必须马上向孩子AP发送计划外的单播SCM通告。

[0765] 在名为“活动的SCM选举”的部分中详细地描述了SCM选举协议。

[0766] SCM通告消息包含唯一地标识了本地子网的IPv4_SUBNET_ID TLV,并包含“路径代价”和“跳计数”字段。路径代价用于给相应的子网传达到达基本LAN的路径代价。跳计数字段用于和现有AP和无线电固件的后向兼容,并包含到达基本LAN的无线跳的次数。活动的SCM发送路径代价和跳计数字段被设置为‘0’的SCM通告应答消息。

[0767] SCM通告消息必须包含用于通告SWAN拓扑树中的根CM的IP地址的根CM IP地址TLV。如果SCM正在独立模式中操作,则该SCM是根CM。如果SCM正在基础结构模式中操作,则LCM或CCM的IP地址位于整个拓扑树的根处。根CM是基础结构节点的缺省的802.1X认证者。

[0768] SCM通告消息包含根CM字段,该字段包含根CM的节点ID。AP能够通过监视SCM通告中的根CM字段确定根CM是否发生变化。

[0769] AP或SCM候选者能够发送多播SCM通告请求来请求“计划外的”SCM通告应答消息。如果活动的SCM在其以太网端口上接收到请求,则它必须发送单播的计划外应答。如果“连接的”AP在次级端口上从孩子AP接收到请求,则它必须发送单播的计划外应答。计划外应答中的单播MAC目的地址取自对应的请求中的跳地址,并且和请求中的MAC源地址相同。

[0770] AP不得转发SCM通告请求。SCM和每个所连接的AP必须维护产生计划外的SCM通告应答所必需的状态信息(即用于产生最近的所计划的通告消息的信息)。

[0771] SCM候选者或者AP能够在SCM通告请求中把响应者节点ID设置为‘0’(即如果它不知道活动的SCM或双亲AP的节点ID)。实际的响应者(即活动的SCM或双亲AP)必须在应答消息的响应者字段中输入其节点ID。

[0772] 假如非根AP的双亲AP的节点ID已知,则它在SCM通告请求中应该把响应者节点ID设置为其双亲AP的节点ID。

[0773] “初始认证”用于在节点初次进入网络时对其进行完整地认证。MN最初向MN 802.1X认证者认证;最初基础结构节点(AP或CM)向根CM中的IN 802.1X认证者认证。初始认证消息在孩子和双亲802.11台站之间的802.11链路上的802.1X EAPOL消息中封装。在所有其他链路上,初始认证消息在WLCCP消息中封装。

[0774] AP或孩子CM使用“路径认证”消息相互认证并和其每个祖先建立CTK。AP或孩子CM在其最初认证之后以及任何其路径发生变化之时,开始路径认证。

[0775] “快速重认证”用于802.11台站(MN或孩子AP)漫游到新双亲AP时对其进行快速地“重认证”。双亲AP在802.11台站重关联时使用“预注册”消息提取用于快速重认证的必要的安全上下文。预注册消息不更新转发路径。

[0776] 在名为“WLCCP安全支持”的部分中详细地讨论了初始认证、预注册、快速重认证和路径认证。

[0777] WLCCP注册和越区切换协议用于在SWAN拓扑树中建立、维护和删除分支以及路径实例。注册(和解除注册)消息也被用于在节点漫游时传递上下文信息。SWAN网络中的每个已认证的孩子CM、AP和MN向SWAN拓扑树的根—根CM注册。总的来说,子树中的每个CM、AP和MN

向位于子树根处的CM进行可靠地注册。示例性的注册和越区切换消息序列在下面部分中示出。

[0778] 用三种消息类型——注册、解除注册和分离来实现注册和越区切换协议。

[0779] 每个MN、AP和孩子CM在其向SWAN基础结构注册之前必须成功地认证(或重认证)。

[0780] 产生进入的“初始”注册请求以便在节点已经成功地(重)认证之后将其向根CM注册。注册请求由包含匹配消息ID的注册应答确认。离开的 初始注册应答建立了路径实例,该实例由路径ID(可选择地)标识。“更新注册请求”用于刷新连接的台站的注册状态。更新注册请求也用于更新祖先节点中所缓存的上下文信息。

[0781] “代理”注册请求/应答消息用于注册对WLCCP敏感的MN。“所注册的”的双亲AP在所关联的MN成功地认证后为其产生代理“初始”注册请求。

[0782] 注册消息包含初始标志,该标志在“初始”注册消息中被设置为ON,而在“更新”注册消息中被设置为OFF。注册消息具有代理标志,在双亲AP为非WLCCP MN在“代理内”所产生的“代理”注册消息中该标志被设置为ON。例如,“初始、代理”注册消息使得初始标志和代理标志均被设置为ON。

[0783] 总的来说,对已经漫游的节点的注册请求被向内转发,直到它到达“最近共同祖先CM”。“最近共同祖先CM”是在包括CM以及新旧双亲节点的最小子树的根处的CM。例如,当MN在单个子网内漫游时,SCM是最近共同祖先。当MN在位于同一本地控制域内的子网之间漫游时,LCM是最近共同祖先。最近共同祖先CM被称为“共同CM”。

[0784] 共同CM向外返回注册应答以确认注册请求并且为“请求者节点”建立新的路径实例。当共同CM为节点建立了新路径实例时,它(可选择地)“解除注册”任何旧路径实例。

[0785] 非双亲CM或AP必须把“初始”或“代理”注册应答转发到由请求者节点ID字段所标识的请求者节点的“双亲”上去。因此,双亲节点是任何“初始”或“代理”注册请求的发起者,它为孩子请求者节点向内转发这些注册请求。

[0786] 根CM标志在注册请求中被设置为ON,以实施“完整路径更新”。如果根CM标志被设置为ON,则注册请求消息总是被转发到根CM。

[0787] “初始”注册请求中的路径ID字段总是被设置为‘0’。双亲CM通过把路径ID值输入初始注册应答的路径ID字段,为路径实例(可选择地)建立路径ID。“更新”注册请求中的路径ID字段被设置为路径实例的路径ID。

[0788] 总是把Response-Req标志设置为ON来传输注册请求以请求应答。如果没有接收到期待的匹配应答,则重新传输注册请求消息,直到超出REGISTRATION_RETRY_MAX的限制。同样的消息ID被用于初始注册请求和所有的重新传输。

[0789] 总的来说,接收到的注册请求被按到达时间排序。注册延迟字段可选择地用于对接收到的由双亲AP为孩子节点所产生的代理注册请求进行排序。延迟字段包含自相应的孩子节点上次传输上行链路帧以来逝去的达数百秒的时间。CM中的注册记录必须包含时间戳字段,该字段包含上次的注册请求的“到达时间”。通过从当前时间中减去延迟值来计算到达时间。

[0790] 双亲AP或SCM通过把注册应答发送到在原始注册请求的跳源字段中的端口MAC地址,把它转发到孩子AP。双亲CCM或LCM通过把消息发送到孩子CM的跳IP地址,把该消息转发到孩子CM。

[0791] 如果WLCCP用于建立转发路径,则“旧的”路径实例在节点漫游时必须被删除。进入解除注册应答和分离请求消息被可选择地用于删除旧路径实例。解除注册请求由“共同CM”产生,以在新路径实例建立时删除任何旧路径实例。此外,“管理”解除注册请求可以由根CM产生,以从管理上断开节点。

[0792] 双亲AP在孩子节点解除关联时产生分离请求。如果孩子节点是AP,则删除根在AP的子树。下面更详细地描述解除注册和分离逻辑。

[0793] 在子网中的每个AP以及和该AP关联的任何MN向子网的活动SCM注册。如上所述,AP通过SCM通告协议发现“活动的SCM”。即使MN属于不同的子网,每个MN仍向其双亲AP的SCM注册。

[0794] 子网内的注册逻辑是实现所特有的。在简单的W1实现中,WLCCP注册用于在SCM和孩子AP之间建立和分配上下文信息。它不用于建立层2的转发路径。在W1实现的注册消息中,层2的路径更新(L2-Path-Update)标志被设置为OFF,且跳路由(Hopwise-Routing)标志被设置为OFF。在W1实现中不使用分离和注册消息。

[0795] 如果使能层2的路径更新,则WLCCP注册在基本LAN和无线台站之间可靠地建立无线转发路径,所以从来没有必要把单播帧泛滥到多个802.11台站上去。注册、解除注册和分离消息必须用跳路由转发,以使路径实例上的每个AP能处理消息。例如,通过把注册应答发送给到目标节点的路径上的“下一跳”的MAC或IP目的地址,用跳路由向外转发注册应答。通过把解除注册应答或分离请求发送给在“双亲节点记录”中所标识的双亲节点的MAC或IP目的地址,用跳路由向内转发注册应答。

[0796] 非WLCCP网桥和交换机透明地转发注册消息。

[0797] 参考图24,示出了用于图解移动节点2412在校园网2400上从第一接入点2408漫游到第二接入点2410的方框图。网络2400包括作为802.1X认证者的CCM 2402、作为MN 802.1X认证者的LCM 2404、SCM 2406、第一接入点2408、第二接入点2410和移动节点2412。

[0798] 图25和26中示出了用于注册和解除注册移动节点2412的消息序列。图25示出了在移动节点2412第一次和接入点2408关联并认证时用于它的消息序列,而图26示出了在移动节点2412漫游到第二接入点2410时的消息序列。箭头表示消息的方向(源->目的地或双向的<->),而垂直条表示网络元件。

[0799] 首先参考图25,移动节点2412和第一接入点2408关联。步骤包括从移动节点2412向第一接入点2408发送关联请求2502,并且第一接入点2408发送关联响应2504。然后移动节点2412向LCM 2404(MN 802.1X认证者)和第一接入点2408进行认证。移动节点2412执行与第一接入点2408的初始认证2506,然后在第一接入点2408和SCM 2406之间执行EAP认证2508,并且在SCM 2406和LCM 2404之间执行AAA请求2510。

[0800] 对于CCKM移动节点,要求预注册。预注册由第一接入点2408向SCM2406发送初始代理注册请求2512开始。然后SCM 2406把初始注册请求2514转发到LCM 2404。把CCKM预注册应答2518从LCM 2404发送到SCM2406,然后如2516所示,从SCM 2406发送到第一接入点2408,并且第一接入点2408向移动节点2412发送CCKM键控2530。移动节点2412在初始认证和键控完成后能够通信。

[0801] 然后,第一接入点向SCM 2406发送初始代理注册请求2520,随后SCM 2406把初始代理注册请求2522转发到LCM 2404,LCM 2404作为响应者,然后,LCM 2404把初始注册请

求2532转发到CCM 2402,CCM作为响应者。随后,CCM 2402把初始注册应答2528转发到LCM 2404。然后如2526所示,LCM 2404把初始注册应答转发到SCM 2406。随后如2524所示,SCM 2406把初始注册应答转发到第一接入点2408。

[0802] 现在参考图26,示出了当移动节点从第一接入点2408漫游到第二接入点2410时的消息序列。移动节点2412通过向第二接入点2410发送重关联请求2552和第二接入点2410重关联。然后,第二接入点2410向SCM2406发送预注册请求2554来为移动节点2412获取动态证书。然后SCM2406向第二接入点2410发送预注册应答2558。随后第二接入点2410向移动节点2412发送重关联响应2556。然后移动节点2412使用其动态证书,利用快速重认证2560和第二接入点2410重认证。在重认证完成后,移动节点能够通信。然后第二接入点2410为移动节点2412向SCM 2406发送初始代理注册请求2562。然后SCM 2406向第一接入点2408发送解除注册请求2564。然后SCM 2406向第二接入点2410发送初始注册应答2566。然后第一接入点2408向SCM 2406发送解除注册应答2568。第二接入点2410向第一接入点2408发送路径更新请求2570。

[0803] 参考图27,示出了用于图解校园网2700上转发器接入点2712从第一接入点2708漫游到第二接入点2710的框图。网络2700包括作为IN802.1X认证者的CCM 2702、LCM 2704、SCM 2706、第一接入点2708、第二接入点2710和转发器接入点2712。

[0804] 图28A和图28B示出了用于注册和解除注册转发器接入点2712的消息序列。图28A示出了在转发器接入点2712第一次和接入点2708关联并认证时,用于转发器接入点2712的消息序列,而图28B示出了在转发器接入点2712漫游到第二接入点2710时的消息序列。箭头表示消息的方向(源->目的地),而垂直条表示网络元件。

[0805] 参考图28A,转发器AP 2712(AP 2712)和第一接入点2708(AP2708)关联。过程包括AP 2712向AP 2708发送关联请求2802,并且AP2708以关联响应2804响应。然后AP 2712通过初始认证2806和AAA2808,向作为IN 802.1X认证者的CCM 2702以及AP 2708进行认证。

[0806] 然后,AP 2712向AP 2708发送Path Init请求,AP 2708作为响应者。然后如2812所示,AP 2708向SCM 2706发送Path Init请求,SCM2706作为响应者。如2814所示,SCM 2706把Path Init请求转发到LCM2704,LCM 2704作为响应者。然后如2816所示,LCM把Path Init请求转发到CCM 2702,CCM作为响应者。如2834所示,然后CCM 2702向LCM2704发送Path Init应答,AP 2708作为发起者。如2822所示,LCM2704向SCM 2706发送Path Init应答,AP 2708作为发起者。如2820所示,SCM 2706向AP 2708发送Path Init应答。如2818所示,AP 2708向AP 2712发送Path Init应答。

[0807] 然后,AP 2712向AP 2708发送初始注册请求2826,AP 2712作为响应者。AP 2708为AP 2712向SCM 2706发送初始注册请求,SCM 2706是2828上的响应者。在2830,SCM 2706把初始注册请求转发到LCM 2704,LCM 2704作为响应者。然后在2832,LCM 2704把初始注册请求转发到CCM 2702,CCM 2702作为响应者。在2840,CCM 2702向LCM 2704发送初始注册应答。然后在2838,LCM 2704把初始注册请求应答转发到SCM2706。然后在2836,SCM 2706把初始注册请求应答转发到AP 2708,然后AP 2708在2834把初始注册请求应答转发到AP 2712。

[0808] 现在参考图28B,示出了在转发器AP(AP 2712)从第一接入点2708(AP 2708)漫游到第二接入点2710(AP 2710)时发生的消息序列。当AP 2712向AP 2710发送重关联请求并表明“快速重关联”能力时,过程在2850开始。然后在2852,AP 2710向SCM 2706发送预注册

请求以获取用于AP 2712的动态证书。然后在2856,SCM 2706向AP 2710发送预注册应答。随后在2854,AP 2710向AP 2712发送重关联响应。在2858,AP2712使用其动态证书,和AP 2710重认证。

[0809] 然后在2860,AP 2712向AP 2710发送Path Init请求,AP 2710作为响应者。在2862,AP 2710为AP 2712向SCM 2706发送Path Init请求,SCM 2706作为响应者。在2866,SCM 2706向AP 2710发送PathInit应答,AP 2710作为发起者。在2864,AP 2710向AP 2712发送PathInit应答。

[0810] 在2872,AP 2712向AP 2710发送初始注册请求,AP 2710作为响应者。在2874,AP 2710为AP 2712向SCM 2706发送初始注册请求,SCM2706作为响应者。在2876,SCM向AP 2708发送解除注册请求。在2880,SCM 2706向AP 2710发送初始注册应答。在2878,AP 2710向AP2712发送初始注册应答。在2882,AP 2708向SCM 2706发送解除注册应答。AP 2710向AP 2708发送路径更新请求。

[0811] 如下面所描述的,为每个子网选举出单个活动的SCM。缺省时,如果没有为子网配置SCM候选者,则子网上的AP在“分布式模式”下操作。

[0812] 活动的SCM或者在1)独立模式,或者在2)SWAN基础结构模式中操作。在任何SCM不能和双亲LCM通信的时候,SCM在独立模式中操作。在基础结构模式中,SCM向双亲LCM注册,并把WLCCP消息转发到其双亲CM。在基础结构模式中的SCM操作在名为“W2-SCM操作”的部分中做了规定。

[0813] 和CCM共存的LCM是所有SCM的缺省备份LCM。

[0814] 如果活动的SCM从独立模式转移到基础结构模式,则必须删除任何现存的根在SCM处的子树,以迫使子树中的所有节点重新注册。(SCM把其实例年龄重置为‘0’以删除其子树。在单独的部分中描述了子树删除。)

[0815] 当活动的SCM从基础结构模式转移到独立模式时候,不需要重建根在SCM处的子树。在独立模式中,SCM必须为其子网起到IEEE 802.1X认证者的作用。

[0816] 现在描述一般的SCM数据结构和状态变量。

[0817] SCM_Advertisement_Timer——当定时器(timer)到期后,由SCM候选者或者活动SCM产生SCM通告应答消息。定时器的周期为DEF_SCM_ADVERTISE_PERIOD秒。(例如5秒)。

[0818] SCM_Instance_Age——在SCM放弃活动SCM状态的任何时候,SCM_Instance_Age被初始化为‘0’或者重置为‘0’。每次当SCM_Advertisement_Timer到期时,活动的SCM增大SCM_Instance_Age的值。

[0819] Authenticated Node Table(已认证节点表)——如果SCM在独立模式中操作,则SCM是802.1X IN和MN认证者IN。在独立模式中,SCM必须保留一个认证的节点表,该表是已认证的节点条目的列表。每个已认证的节点条目包含根在SCM处的子树中的AP和MN的认证状态信息。节点条目处的认证状态被初始化为“未认证”。表中包含的状态信息在名为“WLCCP安全支持”的部分中定义。

[0820] 注册表——活动的SCM必须保留一个包含其子树中的每个AP和MN的状态信息的注册表。AP注册表包含其子网中的每个AP的AP注册记录,MN注册表包含和子网中的每个AP关联的MN的MN注册记录。在接收到对AP或MN的注册请求时,创建或更新注册记录。注册记录包含对已认证节点条目的交叉索引。MN注册记录包含对用于MN的双亲AP的AP注册记录的交叉

索引。如果具有注册生命期的各个节点没有接收到成功的注册请求,则注册记录老化并被丢弃。

[0821] SCM Candidate Path Authentication(SCM候选者路径认证)。校园控制域中的每个SCM候选者被CCM使用上下文请求/应答消息自动地分配给双亲LCM。在SCM候选者已经向根CM成功地认证后,它必须发送Path-Init请求给其所分配的LCM来开始路径认证。在校园基础结构模式中,LCM总是把Path-Init请求转发给CCM。CCM当作KDC使用以相互验证SCM候选者和LCM,并建立共享的CTK。(可选的)WLCCP“多播CTK”在路径认证过程中被转发到SCM。SCM候选者(可选择地)使用WLCCP多播CTK来标记SCM通告应答消息。如果SCM候选者没有被选举为活动的SCM,则不使用SCM候选者和LCM所共享的CTK。

[0822] 活动SCM的选举。

[0823] SCM选举协议用于为每个子网从一组一个或多个SCM候选者中选举出单个活动的SCM。根据定义,基本LAN是连接到SCM的有线以太网LAN;因此,SCM选举自动地为每个子网建立基本LAN。选举协议由SCM通告消息来协助。

[0824] 用从1到255的非零SCM优先权值配置每个SCM候选者。如果WLCCP节点被SCM优先权值‘0’配置,则它不是SCM候选者。SCM优先权值的高位被用作“优选SCM”标志,并且在“优选”的SCM中被设置为ON。优选SCM标志在“备份”SCM中设置为OFF。因此,从128到255的优先权值用于“优选”的SCM候选者。通常应该只有一个优选SCM候选者。从1到127的优先权值用于“备份”的SCM候选者。SCM“优先权值”和SCM节点ID连接在一起形成了SCM“优先权ID”。下面详细地讨论有效的相对的SCM优先权。

[0825] 下面的状态转移表定义了SCM选举协议的操作。

[0826]

状态	事件	操作	下一状态
Initial (初始)	SCM优先权非零	启动平均到期时间为 DEF_SCM_LISTEN_TIME 秒的SCM侦听定时器; 启动周期性的SCM通告 定时器;发送SCM通告 请求	SCM_CAND
SCM_CAND	接收较高优先权的 SCM通告	重新启动到期时间为 MAX_SCM_AGE(最大 SCM年龄)秒的SCM侦 听定时器	SCM_BACKUP
SCM_CAND	接收SCM通告请求或 较低优先权SCM通告 应答	发送活动标志被设置为 OFF的SCM通告	SCM_CAND
SCM_CAND	SCM通告定时器到期	发送活动标志被设置为 OFF的SCM通告	SCM_CAND
SCM_CAND	SCM侦听定时器到期	把SCM实例年龄重置为 0;发送活动标志设置 为ON的SCM通告;重 启动SCM通告定时器	SCM_ACTIVE
SCM_BACK	接收较高优先权SCM	重新启动到期时间为	SCM_BACKUP

[0827]

UP	通告	MAX_SCM_AGE秒的SCM 侦听定时器	
SCM_BACKUP	SCM侦听定时器到期	重新启动到期时间为 DEF_SCM_LISTEN_TIME 秒的SCM侦听定时器; 重新启动周期性的SCM通告 定时器;发送活动标志被设置为OFF的SCM 通告	SCM_CAND
SCM_ACTIVE	接收较高优先权 SCM通告。(如果a) “优先权值”较高, 或b)活动标志为ON 并且优先权ID较高, 则接收到的通告的有效的优先权是“较高”的。)	启动到期时间为 MAX_SCM_AGE秒的SCM 侦听定时器	SCM_BACKUP
SCM_ACTIVE	接收SCM通告请求或较低优先权SCM 通告应答	发送活动标志被设置 为ON的单播的计划 外SCM通告	SCM_ACTIVE
SCM_ACTIVE	SCM通告定时器到期	发送活动标志被设置 为ON的所计划的 SCM通告;重新启动SCM 通告定时器	SCM_ACTIVE

[0828] SCM选举/通告协议在SCM候选者和AP所共享的单个“本地”VLAN上操作。忽略在任何其他VLAN上所接收到的SCM通告消息。

[0829] 用非零的SCM“优先权值”配置“SCM候选者”。每个SCM候选者具有“SCM优先权ID”,该ID由连接起来的SCM优先权值和SCM节点地址构成。用于有效的相对SCM优先权的规则如下:

[0830] 1)如果用较高的优先权值配置SCM候选者或活动的SCM,则它具有相对“较高优先

权”。

[0831] 2)如果第一SCM候选者具有按字典编纂顺序较高的SCM“优先权ID”，则它具有比第二SCM候选者相对较高的优先权。

[0832] 3)如果第一活动的SCM具有按字典编纂顺序较高的SCM“优先权ID”，则它具有比第二活动的SCM相对较高的优先权。

[0833] 4)如果用较高的优先权值配置SCM候选者，则它具有比活动的SCM相对较高的优先权。如果用和活动的SCM相同或比活动的SCM低的优先权值配置SCM候选者，则它比活动的SCM具有相对较低的优先权。

[0834] 构造了有效的优先权以使具有相同优先权值的SCM候选者不会取代活动的SCM，即使该SCM候选者具有“较高”的节点ID。但是，用户可以通过配置较高的优先权值，明确地选择活动的SCM。

[0835] SCM候选者最初进入SCM_CANDIDATE状态，在其以太网端口上侦听SCM通告。SCM候选者在SCM_CANDIDATE状态中保留一个“侦听周期”，该周期超过3个SCM通告间隔，或者直到它发现较高优先权的SCM。如果SCM候选者在侦听周期内没有接收到较高优先权的SCM的通告消息，则它进入SCM_ACTIVE状态。在基础结构模式中，“所选举出的”活动的SCM必须马上向其双亲LCM和CCM注册。活动的SCM在它已经成功地注册或者进入“独立模式”后，在其SCM通告应答消息中把“SCM活动”标志设置为ON。

[0836] 如果SCM候选者或活动的SCM发现更高优先权的SCM，则它进入SCM_BACKUP状态。

[0837] AP或SCM候选者必须在端口被初次使能时，在每个端口上向WLCCP“全IN”组地址发送SCM通告消息。处于SCM_ACTIVE或SCM_CANDIDATE状态中的节点通过发送SCM通告应答作出响应。处于SCM_CANDIDATE状态的节点在应答中把“SCM活动”标志设置为OFF，并把路径代价和跳计数字段设置为“无穷大”值。

[0838] 作为一种选择，可以为单个子网选举出多个活动的SCM。为此目的，SCM通告请求消息包含SCM组选举字段。该字段包含SCM选举组的数目和 分配给各个SCM候选者（即由SCM节点ID所标识）的组ID。组ID必须少于选举组的数目。SCM候选者只考虑来自同一组中的其他候选者的SCM通告，所以为每个组选举出活动的SCM。注册在多个活动的SCM之间分配。用于为节点确定活动的SCM的算法在名为“WLCCP注册协议”的部分中描述。

[0839] 每个通告周期一次，所选举的活动SCM传输活动标志被设置为ON的SCM通告应答消息。活动的SCM发送的SCM通告应答消息中的字段如下设置：

[0840] WLCCP头字段：

[0841] Type(类型)-‘0x41’(SCM通告应答)

[0842] Originator(发起者)-‘0’.

[0843] Responder(响应者)-SCM节点ID.

[0844] Outbound Flag(离开标志)-‘1’.

[0845] TLV Flag TLV标志-‘1’(请求必须包括IPV4_SUBNET TLV和ROOT_CM_INFO TLV)。

[0846] SCM通告应答字段：

[0847] Hop_Address(跳地址)-SCM以太网端口地址.

[0848] SCM标志：

[0849] Active Flag(活动标志)-‘1’

- [0850] SCM Priority(SCM优先权)-用户配置的SCM优先权。
- [0851] SCM Node ID(SCM节点ID)-SCM节点类型和以太网端口地址。
- [0852] Instance Age(实例年龄)-SCM_Instance_Age值。
- [0853] Path Cost(路径代价)-‘0’
- [0854] Hop Count(跳计数)-‘0’
- [0855] Advertisement Period(通告周期)-DEF_SCM_ADVERTISE_PERIOD秒。
- [0856] WTLV_IPV4_SUBNET_ID TLV-IPv4地址和SCM前缀长度。
- [0857] WTLV_ROOT_CM_INFO TLV-包含根CM的IPv4地址(根CM也是802.1X IN认证者)。
- [0858] SCM注册
- [0859] SCM在它被选举为其子网的“活动的SCM”后必须马上向根CM注册。(注意,它已经完成了路径认证)。所选举的活动SCM向其所分配的双亲LCM发送“初始”注册请求。在校园基础结构模式中,LCM总是把初始注册请求向内转发到CCM。CCM把初始注册应答消息返回到双亲LCM,双亲LCM把初始注册应答消息转发到SCM。应答消息在根CM TLV中包含“根CM”的IP地址和节点ID。
- [0860] SCM必须产生周期性的“更新”注册请求消息以刷新它在双亲LCM和CCM中的注册绑定。更新注册请求消息总是被转发到根CM。根CM返回更新注册应答消息来确认注册请求。双亲LCM在接收到具有“良好”状态的“匹配的”注册请求时,为SCM把DPR的年龄重置为‘0’。如果双亲LCM没有接收到用于具有注册生命期的SCM的更新注册应答消息,则它必须删除根在SCM处的子树。
- [0861] 任何时候只要SCM被分配给不同的双亲LCM实例,它就必须重复路径认证和初始注册过程。
- [0862] 现在讨论一般的AP操作。
- [0863] WLCCP AP或者在1)“分布式模式”或者在2)SWAN“基础结构模式”中操作。
- [0864] AP操作模式取决于SCM的存在和AP“操作模式”参数,该参数可以被设置为下列值之一:
- [0865] a)仅为基础结构
- [0866] b)自动低效操作(缺省)
- [0867] 如果WLCCP AP发现了SWAN SCM,则它总是在“基础结构模式”中操作。如果AP不能向活动的SWAN SCM注册,并且“操作模式”被设置为“自动低效操作”,则AP在“分布式模式”中操作。在分布式模式中,CISCO数据报传送协议(DDP)用作AP间的协议。应该注意,在分布式模式中,当台站漫游时,可以使用WLCCP上下文或路径更新消息把上下文从“旧AP”直接传递到“新AP”。(可以从802.11重关联消息中获取“旧AP”的MAC地址)。在分布式模式中,每个AP必须起到802.1X认证者的作用。如果网络包含非WLCCP AP,则AP应该在在分布式模式中操作。
- [0868] 如果“操作模式”被设置为“仅为基础结构”,则AP不能在“在分布式模式”中操作。
- [0869] 基础结构模式中的AP操作在独立子网基础结构、独立本地基础结构或校园基础结构中一般都是相同的。
- [0870] 在基础结构模式中操作的AP如果向活动的SCM注册,则它被视作“连接”的;否则,它被视作“未连接”的。在“分布式”模式中操作的AP如果具有在双亲或双亲/孩子模式中所

配置(见下文)的良好的以太网链路,或者它和双亲AP关联,则它被视作“连接的”;否则,它被视作“未连接的”。未连接的AP必须禁止802.11台站关联,以防止台站和不能提供到基本LAN的访问的AP进行关联。在其他台站被禁止时,管理台站能够使用特殊的“管理SSID”和未连接的AP关联。

[0871] 孩子802.11网桥或者转发器AP不能在基础结构模式中操作,除非它和在基础结构模式中操作的双亲AP关联。(在基础结构模式中操作的双亲AP向孩子AP和网桥传输周期性的SCM通告应答消息。)

[0872] 下面是一般的AP状态变量的列表。

[0873] Infrastructure_Mode(基础结构模式)——如果存在活动的SCM则为TRUE,否则为FALSE。

[0874] AP_Top_Level_State(AP顶层状态)——包含当前的顶层AP状态。在名为“AP操作模式”的部分描述了顶层AP的状态和顶层状态转移。

[0875] Parent_SCM_Record(双亲SCM记录)——包含下列关于活动的双亲SCM的信息:

[0876] SCM_Node_ID(SCM节点ID)——从SARpM复制的活动SCM的节点ID。

[0877] SCM_Age(SCM年龄)——每个SCM通告周期增大一次。当接收到“活动的”SARpM时重置为‘0’。当SCM_Age(SCM年龄)等于MAX_SCM_AGE(最大SCM年龄)时,Infrastructure_Mode(基础结构模式)重置为False。

[0878] SCM_Instance_Age(SCM实例年龄)——从SARpM复制的SCM的实例年龄。

[0879] SCM_Subnet_Address——从SARpM中的WTLV_IPV4_SUBNET_ID TLV复制来的SCM的(可选)子网掩码和Ipv4地址。

[0880] SCM_Priority(SCM优先权)——从SARpM中的SCM优先权字段复制来的活动SCM的优先权。

[0881] SCM_Advertisement_Period(SCM通告周期)-从SARpM中的通告周期字段复制来的、在所计划的SCM通告之间的秒数。

[0882] SCM_Path_Cost(SCM路径代价)-来自SARpM的路径代价值,加上分配给AP基本端口的代价。

[0883] SCM_Hop_Count(SCM跳计数)-来自SARpM的跳计数值,对于基本端口加‘1’。

[0884] SCM_Advertisement_Timer(SCM通告定时器)(可选)-当WLCCP被使能时,每“SCM通告周期”到期一次的定时器。定时器的持续时间是SCM_Advertisement_Period秒。(见上文)。

[0885] IN_1X_Authenticator(IN_1X认证者)-WLCCP基础结构802.1X认证者的Ipv4地址和节点ID,该认证者在简单WLCCP实现中总是SCM。

[0886] AP必须监视本地VLAN上的它的基本端口上所接收到的SCM通告应答消息,以确定是否存在本地VLAN的活动SCM。如果存在AP的本地VLAN的活动SCM,则AP在基础结构模式中操作并执行WLCCP协议。

[0887] 每次AP接收到SCM通告应答消息,它必须更新其“双亲SCM记录”。当AP第一次接收到“Active_Flag(活动标志)”设置为ON的SCM通告时,使能基础结构模式。使用下列方法之一,AP必须在其每个次级端口上产生SCM通告应答消息1)AP能够当它在其基本端口上接收到SCM通告后,仅在其每个次级端口上产生SCM通告,或者2)AP能够在每次定时器到期时启

动周期性的SCM_Advertisement_Timer(SCM通告定时器),并且在其次级端口上产生SCM通告应答消息。定时器的周期是在基本端口上所接收到的通告中的非零的通告周期值。如果在基本端口上所接收到的通告中的通告周期值为零,则必须使用第一种方法。

[0888] 转发器AP在它第一次和双亲AP关联时,必须在其基本端口上发送多播SCM通告请求,以请求单播的、计划外的SCM通告应答消息。

[0889] 下面的AP顶层状态转移表规定了SCM通告应答消息(SARpM)处理逻辑。“活动的”SARpM使得“活动标志”设置为ON。

[0890] IN 802.1X认证者在AP处于I,R状态时位于根CM中;否则IN802.1X认证者在AP中。MN的预注册和注册只有在I,R状态中才被使能。

[0891] 下面描述AP顶层状态:

[0892] D,*-分布式模式中的任何状态。因为AP尚未发现任何活动SCM,“Infrastructure_Mode(基础结构模式)”为False。

[0893] D,L-AP处于上电的SCM发现周期。

[0894] D,A-AP在分布式模式中活跃地操作,并且正在接受台站的关联。

[0895] D,SC-AP在上电的SCM发现周期期间发现了SCM候选者。

[0896] I,U-Infrastructure_Mode(基础结构模式)为True并且AP还没有向根CM认证。

[0897] I,A-Infrastructure_Mode(基础结构模式)为True并且AP已经向根CM成功地认证。

[0898] I,P-AP已经成功地完成路径认证。

[0899] I,R-AP已经向根CM成功地注册;使能了MN(预)注册。

[0900] I,*-Infrastructure_Mode(基础结构模式)为True的任何状态。

[0901] 顶层AP状态转移表

[0902]

状态	事件	动作	下一状态
Initial (初始)	系统重新置位;良好 的以太网链路;使能自动 低效操作	启动到期时间为10 秒的SCM侦听定时器;发 送SCM通告请求	D,L
D,*	接收活动的SARpM	把Infrastructure_Mode 设置为TRUE;更新双亲 SCM记录和	I,U

[0903]

		IN_1X_Authenticator(IN 1X认证者);开始和SCM 的认证。	
D,L	接收非活动的SARpM	重新启动到期时间为 MAX_SCM_ELECT_TIME的 SCM侦听定时器;保存 SCM候选者的优先权ID	D,SC
D,SC	接收较高优先权的非活动 SCM通告	重新启动到期时间为 MAX_SCM_ELECT_TIME的 SCM侦听定时器;保存 SCM候选者的优先权ID	D,SC
D,L	SCM侦听定时器到期	启动分布式模式中的 活动操作。	D,A
D,SC	SCM侦听定时器到期(即因 为活动的SCM选举没有完 成)	启动分布式模式中的 活动操作。	D,A
D,A	接收非活动的SARpM	(无)	D,U
I,U	与根CM的认证成功地完成。	开始路径认证。	I,A
I,A	路径认证成功地完成。	开始AP注册	P

[0904]

I,P	注册成功地完成。	使能MN预注册和注 册;注册已认证的MN;向 SCM传递MN 802.1X 认证 者函数;启动 SCM_Advertisement_Time r(SCM通告定时器)	I,R
I,*	从活动SCM实例接收 活动SARpM。	把SCM_Age(SCM年 龄)重置为0;更新 Parent_SCM_Record(双 亲SCM记录)	I,*
I,*	从活动SCM接收具有 较小实例年龄的非活动 SARpM或“活动” SARpM。	把Infrastructure_Mode 设置为False	D,U
I,*	从不同优先权SCM接 收较高优先权的活动 SARpM。	更新SCM状态信息; 开始对新活动SCM的认证	I,U
I,*	从不同SCM(候选者) 接收非活动SARpM或者较低 优先权的活 动SARpM。	(无)	I,*

I,R	SCM_Advertisement_Timer到期;SCM_Age小于 MAX_SCM_AGE。	以当前通告周期重启 定时器;增大SCM年龄;在每个次级端口上产生SARPM	I,R
I,R	SCM_Advertisement_Timer到期;SCM_Age等于 MAX_SCM_AGE	把Infrastructure_Mode 设置为False	D,U

[0905] SCM通告应答消息没有被WLCCP AP透明地转发。相反,注册的AP在其每个活动次级端口上产生“次级”SCM通告应答消息,具有和SCM相同的周期。(SCM通告应答消息中包含通告周期)。SCM通告应答消息不在AP基本端口或下层STP“阻塞”的AP端口上被传输。

[0906] 在AP次级端口上传输的SCM通告包含被更新的“路径代价”(path-cost)和“跳计数”(hop count)值。给每个AP端口分配一个用户可配置的“路径代价”。针对每个AP端口类型(例如以太网、802.11a、802.11b)都定义了强大的路径代价值。被更新的路径代价通过把分配给AP的基本端口的路径代价加上双亲AP的路径代价(即在基本端口上接收到的SCM通告中的路径代价)来计算;如果AP的基本端口是无线端口,则“跳计数”增加‘1’。子网地址和被更新的路径代价以及跳计数信息也在802.11信标和探测响应消息(802.11 Beacon and Probe Responsemessage)中通告,并在AP 802.11次级端口上发送,以使未关联的无线AP和MN能迅速地发现到基本LAN的最小代价路径(即不用向每个潜在的双亲AP反复地关联和认证)。

[0907] AP可以向被包含在同一硬件箱中的逻辑SCM注册。在那种情况下,分配给“内部基本端口”的代价应该和以太网端口代价一致(即防止台站迁徙到作为SCM共存在同一箱中的AP)。

[0908] 非SWAN AP可以透明地转发不同的SWAN节点产生的SCM通告应答消息。孩子AP必须丢弃任何不是由其双亲产生的SCM通告应答消息。孩子AP能够使用SCM通告跳源字段确定其双亲是否产生了SCM通告消息。跳源地址必须和双亲AP的跳地址相同。

[0909] 根AP总是绑定到本地VLAN上的活动SCM。根AP只在其基本端口上接收在本地VLAN上的SCM通告应答消息。非根AP必须和其双亲AP属于相同的子网;因此,非根AP总是绑定到和双亲(或祖先)根AP相同的SCM。

[0910] 用单个“WLCCP SSID”配置SWAN AP。如果校园网仅包含根AP,或者非根AP能够动态地绑定到任何子网,则校园范围的WLCCP SSID是足够的。特定于子网的WLCCP SSID可被用于把非根AP绑定到特定子网上(即具有带匹配WLCCP SSID的根AP的子网)。(孩子AP能够使用DHCP动态地绑定到子网;但是,本地VLAN与双亲或孩子AP中被使能的VLAN的组必须匹配。)

[0911] 孩子802.11端口(即转发器AP或孩子802.11网桥)使用WLCCP SSID与双亲AP关联。孩子AP发送包含WLCCP SSID的探测请求(ProbeRequest),并且潜在的双亲AP使用也包含WLCCP SSID的探测响应(Probe Reply)来应答。孩子AP只能连接到具有匹配WLCCP SSID的双亲AP。

[0912] AP或孩子CM在它已经和802.1X IN认证者成功地认证后,必须认证其到根CM的路径,以便和SWAN拓扑树上的它的分支上的每个祖先节点相互认证并建立秘密的上下文传递密钥(CTK)。只要AP检测到新SCM实例,它也必须开始路径认证。只要非根AP漫游到新双亲AP,它也必须开始路径认证。(作为一个选择,如果孩子AP支持快速重认证,则非根AP漫游时不需要完整的认证)。路径认证包括Path-Init请求/应答交换和初始注册请求/应答交换。在名为“基础结构路径认证”的部分中更详细地描述了路径认证和CTK更新。

[0913] 未连接的AP必须在其选中的基本端口上发送Path-Init请求给它的选中的双亲节

点,以开始路径认证。在Path-Init请求和对应的应答中,发起者是未连接的AP,请求者也是未连接的AP;而响应者是选中的双亲节点(即双亲AP或SCM)。

[0914] 未连接的AP发送的Path-Init请求中的非安全字段(Non-securityfield)如下所述被设置。(没有规定的字段被设置为‘0’)。跳路由标志(Hopwise-Routing Flag)被设置为‘1’,所以到SCM的路径上的每个祖先AP都处理请求和对应的应答。Path-Init消息(和初始注册消息)中包括安全TLV。

[0915] WLCCP头字段:

[0916] Type(类型)-‘12’

[0917] Originator(发起者)-未连接的AP的节点ID。

[0918] Responder(响应者)-SCM的节点ID。

[0919] Response-Req Flag(响应请求标志)-‘1’用于请求应答。

[0920] Inbound Flag(进入标志)-‘1’。

[0921] Hopwise-Routing Flag(跳路由标志)-如果使能层二路径更新则为‘1’;否则为‘0’。

[0922] Root CM Flag(根CM标志)-‘1’。

[0923] TLV Flag(TLV标志)-‘1’。(该请求必须包括EAP_IDENTITY_TLV。)

[0924] Path-Init字段:

[0925] Requester(请求者)-AP的节点ID。

[0926] Relay Node ID(中继节点ID)-‘0’。

[0927] Proxy Flag(代理标志)-‘0’。

[0928] 双亲节点必须把Path-Init请求从未连接的AP或CM向内转发,直到它到达根CM。双亲节点在向内转发请求之前,在发起者字段输入其节点ID,并且在响应者字段输入其双亲CM的节点ID。中间的LCM在它把请求向内转发到CCM之前,必须用CCM节点ID更新响应者字段。CCM向双亲节点(即发起者)返回Path-Init应答。双亲节点在把应答转发到未连接的AP或CM之前,用请求者节点ID更新响应者字段。

[0929] 在AP能够与SWAN基础结构注册之前,它必须向根CM认证。AP通过包含在SCM通告消息中的WTLV_ROOT_CM TLV发现根CM。根CM可以是本地SCM、LCM或者CCM。

[0930] 未连接的AP在其每个配置为孩子或双亲/孩子模式的端口上扫描潜在的双亲SCM或AP。(注意,连接的AP如果发现了其双亲AP或SCM的新的实例,它就变为未连接的)。未连接的AP或CM必须在其选中的基本端口上发送初始注册请求到其选中的双亲节点,以便请求连接到网络。发起者是未连接的AP;请求者也是未连接的AP;而响应者是初始注册请求和对应的应答中选中的双亲节点(即双亲AP或者SCM)。

[0931] 未连接的AP发送的初始注册请求中的字段按如下描述被设置。(未规定的字段被设置为‘0’)

[0932] WLCCP头字段:

[0933] Type(类型)-‘3’

[0934] Originator(发起者)-未连接的AP的节点ID。

[0935] Responder(响应者)-选中的双亲节点(双亲AP或双亲SCM)的节点ID。

[0936] Response-Req Flag(响应请求标志)-‘1’用于请求应答。

- [0937] Inbound Flag(进入标志)-‘1’。
- [0938] Hopwise-Routing Flag(跳路由标志)-‘1’。
- [0939] TLV Flag(TLV标志)-‘1’。(该请求必须包括每个AP端口的WTLV_AP_PORT_ADDRESS TLV)。
- [0940] 注册字段：
- [0941] Requester(请求者)-未连接的AP的节点ID。
- [0942] Hop Address(跳地址)-未连接的AP选中的基本端口的802地址。
- [0943] Relay Node ID(中继节点ID)-在发起者或响应者产生的注册消息中为‘0’。否则，是转发该消息的中间“中继”节点的节点ID。
- [0944] Initial Flag(初始标志)-‘1’。
- [0945] VLAN ID-未连接的AP和双亲节点的本地VLAN ID。VLAN ID值可以是‘0’。如果VLAN ID值与双亲节点的本地VLAN ID不同，则是错误的。
- [0946] 双亲节点必须把初始注册请求从未连接的AP向内转发，直到它到达根CM。双亲节点在向内转发请求之前，在发起者字段输入其节点ID，并且在响应者字段输入其双亲CM的节点ID。中间的LCM在它把请求向内转发到CCM之前，必须用CCM节点ID更新响应者字段。CCM向双亲节点(即发起者)返回注册应答。双亲节点在把应答转发到未连接的AP或CM之前用请求者节点ID更新响应者字段。
- [0947] AP周期性地发送“更新”注册请求消息到SCM，用于“刷新”它在到SCM的路径上的每个节点处的移动绑定。更新注册请求使得初始标志被设置为OFF，并且它包含有效的路径ID(Path ID)。连接的AP或CM能够把“更新”注册请求直接发送到其双亲CM，它自身既作为发起者节点也是请求者节点，而双亲CM作为响应者。双亲CM在向内转发请求之前，必须用其双亲CM的节点ID更新响应者字段。
- [0948] AP(重)传输注册请求，直到它接收到具有匹配消息ID的注册应答，或者直到超过了最大重试。当AP接收到具有“良好”注册状态(RegStatus)的匹配注册应答时，它被“注册”。注册应答包含SCM设置的路径ID，该ID标识了从AP到SCM的“路径实例”。
- [0949] 来自AP的注册请求必须包括WTLV_AP_PORT_LIST TLV，WTLV_AP_PORT_LIST TLV包括WTLV_AP_PORT_INFO TLV的列表。每个PORT_INFO TLV包括物理通信接口的端口类型、端口模式(双亲、孩子或双亲/孩子)以及802端口地址。
- [0950] 来自AP的注册请求必须包括一个IP地址TLV以把其IP地址绑定到其节点ID。任何时候只要AP的IP地址变化了，它必须马上产生更新注册请求。
- [0951] 来自代理MIP SSID(Proxy MIP SSID)配置的AP的注册请求，必须包括包含代理MIP SSID和MIP HA绑定列表的WTLV_PMIP_SSID_LISTTLV。
- [0952] 预注册消息用于获取注册前所要求的上下文信息。新双亲AP在它“重关联”时可选择地发送预注册请求消息给其双亲SCM，用于获取802.11台站(MN或孩子AP)的动态证书和“旧AP绑定”。(在802.11台站最初“关联”时不产生预注册请求。)当双亲AP从802.11台站接收到1)802.11重关联请求，或者2)802.11X EAP身份响应消息时，它产生预注册请求。预注册请求包含孩子台站的节点ID和其安全“标识符”。
- [0953] 预注册请求被向内转发到旧AP和新AP的最近共同祖先CM(带有一些下面指明的限制)。如果该“共同CM”具有用于孩子台站的移动绑定和安全上下文，则在预注册应答消息中

返回旧AP绑定和动态证书。否则,返回具有“未发现”状态的预注册应答,并且台站必须完整地认证。

[0954] 对MN的预注册请求从来不被转发超越最近共同LCM,因为该LCM是MN认证者。AP不能跨越子网边界漫游;因此孩子AP的最近共同祖先CM应该总是本地SCM。

[0955] 预注册应答不建立“绑定的”路径实例。当双亲AP接收到应答时,可选择地产生802.11重关联响应消息。

[0956] 如果不支持使用网络会话密钥的快速重认证,或者台站的动态证书被“预见性地”转发到新双亲AP,则新双亲AP不需要发送预注册请求来获取802.11台站的动态证书。在这种情况下,在预注册应答消息中返回台站的“旧AP绑定”。具体的预注册握手取决于802.11(重)认证方法。

[0957] 双亲AP为孩子802.11 MN产生的代理预注册请求消息(ProxyPreregistration Request message)中的字段如下设置:

[0958] WLCCP头字段:

[0959] Type(类型)-‘9’

[0960] Originator(发起者)-双亲AP的节点ID。

[0961] Responder(响应者)-SCM的节点ID。

[0962] Response-Req Flag(响应请求标志)-‘1’用于请求应答。

[0963] Inbound Flag(进入标志)-‘1’。

[0964] Root CM Flag(根CM标志)-AP为‘1’,MN为‘0’。

[0965] Hopwise-Routing Flag(跳路由标志)-‘0’。

[0966] TLV Flag(TLV标志)-‘1’。(请求必须包括EAP_IDENTITY_TLV和SSID_TLV)。

[0967] 预注册字段:

[0968] Requester(请求者)-MN的节点ID。

[0969] Relay Node ID(中继节点ID)-‘0’。

[0970] Proxy Flag(代理标志)-‘1’。

[0971] EAP_IDENTITY_TLV(EAP身份TLV)-对MN或孩子AP的预注册请求必须包含WTLV_EAP_IDENTITY_TLV,WTLV_EAP_IDENTITY_TLV包含来自可选802.11重关联要素或者来自EAP身份响应消息的节点标识符。

[0972] SSID_TLV-取自MN的(重)关联请求消息的MN的SSID。

[0973] 孩子AP在其(重)关联请求消息中能够可选择地包括Node_ID要素,以便将其WLCCP节点ID传送给其双亲AP。如果双亲AP在为孩子AP产生预注册消息时不知道孩子AP的节点ID,则它必须把请求者节点地址设置为‘0’。预注册请求应该包括包含孩子AP的MAC端口地址的WTLV_PORT_ADDRESS_TLV。

[0974] 双亲AP为关联的MN产生“代理”注册请求消息。发起者、响应者和请求者字段总是如下设置:

[0975] 发起者(Originator)-双亲AP的节点ID。

[0976] 响应者(Responder)-CM的节点ID。

[0977] 请求者(Requester)-MN的802地址。

[0978] 在双亲AP成功地认证或者重认证之后,它必须为MN产生代理注册请求(下面描

述)。

[0979] 代理MN注册逻辑特定于实现,并且在下面名为“W1代理MN注册”和“W2代理MN注册”的部分中更详细地描述。

[0980] 通过迫使SWAN基础结构节点既与根CM(CCM)也和IN节点相互认证来完成SWAN认证和保密,其中,SWAN基础结构节点将与IN节点通信。通过在IN的成功预注册之后由CCM产生并分配CTK来完成WLCCP消息的保护。

[0981] “初始认证”基于IEEE 802.1X协议。每个“安全MN”、AP和CM最初必须通过外部的认证服务器(例如RADIUS服务器)与802.1X认证者“相互”认证。基础结构节点(AP、SCM和LCM)与“IN认证者”相互认证。“安全MN”与“MN认证者”相互认证。虽然MN能够从任何支持的802.1X EAP认证类型中选择,但是对于初始的版本,IN节点应该用LEAP认证。

[0982] 在校园网中,SWAN CCM包含IN认证者,LCM包含MN认证者。在独立本地域中,IN认证者和MN认证者都被包含在LCM中。在独立子网域中,IN认证者和MN认证者都被包含在SCM中。

[0983] 所有节点在注册前都必须认证到SWAN拓扑中。节点认证者在成功地802.1X EAP认证后将缓存证书。IN认证者将缓存:

[0984]

字段	长度	描述
----	----	----

[0985]

	(字节)	
保留	1	用于字节对齐
状态(State)	1	表明该节点是否活动
Node-ID	8	WLCCP节点标识符:AP的MAC 地址(例如BSSID)
NSK	16	由成功的LEAP认证产生的密 钥
会话超时时间 (Session Timeout)	4	Radius访问认可(Radius Access Accept)所提供的会话到 期时间
CTK	32	用于保护SCM认证者和节点 ID之间的通信的当前上下文传递密 钥
密钥序列计数器	4	用于跟踪已经发生了多少次 CTK密钥刷新的序列计数器
MIC序列计数器	8	用于跟踪认证了多少消息的序 列计数器

[0986] 类似地,MN认证者将缓存:

[0987]

字段	长度 (字节)	描述
保留	1	用于字节对齐
状态(State)	1	表明该节点是否活动
STA Addr	8	WLCCP节点标识符:MN的MAC地
认证类型	1	用于认证的EAP类型
Key Management Type(密钥管理类型)	1	协商密钥管理的类型或无协商密 钥管理的类型: 0-无(不转发NSK) 1-CKM

[0988]

		2-802.1X遗留系统(执行有 效的重认证)转发NSK。 3-SSN
会话超时时间	4	Radius访问认可所提供的会话 到期时间
KRK	16	用于认证请求上下文传递的MN 请求的密钥请求密钥
BTK	32	用于导出PTK的基本瞬时密钥
RN	8	用于跟踪已经从BTK中导出多少 PTK的重定密钥号
SSID	L	MN的关联的SSID TLV
EAP-ID	P	EAP身份TLV
VLAN ID	2	MN的关联的VLAN分配
BSSID	6	定义当前关联的AP
Cipher(密码)	2	协商的密码,值为: 0x0000-无 0x0001-WEP 0x0002-TKIP 0x0003-AES-OCB 0x0004-AES-CCMP 0x0005-CKIP 0xff<值>-供应商指定
NSK Length(NSK 长度)	2	以字节计算的NSK长度
NSK	N	由成功的802.1X EAP认证产生 的密钥。这是AS发送的MS-MPPE Rx 密钥

Tx Key Length (Tx密钥长度)	2	Tx密钥长度
------------------------	---	--------

[0989]

Tx Key	M	由成功的802.1X EAP认证成功产生的密钥。这是AS发送的MS-MPPE Tx 密钥
--------	---	--

[0990] 每个注册条目中的字段或者在802.1X EAP认证成功时或者在预注册期间填充。成功的认证将导致具有已定义了适当ID、NSK和会话超时时间值的注册条目的产生。对MN，在基于EAP身份的认证时还将定义有效的BSSID、SSID和VLAN ID。

[0991] 802.1X EAP认证消息被节点的双亲进行WLCCP封装。基础结构节点在认证期间通过到IN认证者的有线链路直接通信。一旦IN双亲已接收到EAPOL认证消息，它将使用WLCCP_AAA消息对其封装。

[0992] 由于MN总是通过AP与MN认证者通信，所以AP必须对EAP消息进行WLCCP封装。由于AP已经向MN认证者认证和注册，所以可以可选择地认证WLCCP_AAA消息。如同在名为“EAP认证请求/应答消息”的部分中所描述的，WLCCP_AAA消息可以附加一个MIC_TLV。MIC适用于包括头部的整个WLCCP消息：

[0993] MIC=HMAC-MD5(CTK,WLCCP_AAA消息)

[0994] 其中，CTK=直接发送者和直接接收者之间共享的密钥

[0995] WLCCP应答或远离的消息使得有机会规定一种状态。对于错误状态，下列状态值在WLCCP_AAA期间将适用：

[0996]

状态	值	描述
NO CONTEXT(无 上下文)	1	提供了不充分的证书：在Radius访问认可消息中缺少了NSK或者会话超时时间
BAD SSID	2	规定了无效的SSID
EAP FAILURE	3	EAP认证失败

[0997]

(EAP 失败)		
----------	--	--

[0998] 每个“安全”MN必须通过外部安全服务器和MN 802.1X认证者相互认证。在基础结构模式中，MN认证者在LCM中。在SCM独立模式中，MN认证者在SCM中。

[0999] MN不需要知道AP后面的基础结构。这样，从MN的角度看，按照802.11(SSN和TGi)协议以及CCKM的使用的规定执行了MN认证。对要被SWAN拓扑适当管理的MN，它必须协商802.1X EAP认证。

[1000] MN必须使用802.1X EAP认证来得到LEAP、SSN或TGi安全优点以及SWAN可管理性的益处。在SWAN体系结构中，MN认证者从双亲AP分离。当MN进行802.1X EAP认证时，在EAP认证请求消息中，其EAPOL消息被双亲AP进行WLCCP封装，并被转发到MN认证者。

[1001] 按照协商的密钥管理，MN认证者还必须在预注册请求/应答交换中把所需密钥正确地转发给AP。下面的表格描述了MN认证者根据协商的密钥管理类型必须转发的东西：

[1002]

密钥管理类型号	描述
None	虽然Radius可以产生NSK，但MN认证者只有在 初始关联时才将转发NSK；实际上该操作是非缓存的 NSK。
Cisco-LEAP	Radius MS-MPPE密钥被转发到SCM，并且随后 到达AP，用于保护802.11分组。
SSN/TGI	Radius MS-MPPE密钥被转发到SCM，并且随后 到达AP，用于建立每个AP的PTK的802.1X 4路 握手。
CCKM	MN认证者执行4路握手以建立重定密钥认证密 钥、KRK和基本瞬时密钥BTK。只有BTK需要被转发 到AP以建立PTK。CCKM要求在初始认证之后进行预 注册请 求/应答。

[1003] 在所有密钥管理方案中，用于保护AP和MN之间的通信的成对瞬时密钥(PTK)由MN和AP产生。

[1004] AS还必须提供基于密钥管理方法的会话超时时间设置。对于LEAP，会话超时时间

仍是802.11协商密码套件的函数。但是,对SSN/TGi或CCKM,会话超时时间是每个EAP认证类型的相互导出的密钥的函数。

[1005] CCKM MN已经成功地认证后,在MN和关联的AP能够建立PTK之前,MN认证者必须触发密钥初始化来建立密钥请求密钥(KRK)和基本瞬时密钥。

[1006] 为触发KRK和BTK的导出,MN认证者必须产生16字节的现时标志。具有当前的TGi Draft[6]中所描述的格式的EAPOL密钥消息被产生,以便把该现时标志发送到MN,并且从而开始用于建立KRK和BTK的4路握手。EAPOL密钥消息被封装在WLCCP_AAA消息中,并被传送给MN。传送经AP,因此AP将解封装WLCCP消息并把EAPOL密钥消息转发给MN。接着握手如同在使用Cisco的中心密钥管理协议规范中的快速越区交换(FastHandoff)所描述的那样继续下去。

[1007] 基础结构节点必须首先使用802.1X EAP认证向IN认证者认证,以建立秘密的网络会话密钥(NSK)。对于初始版本,认证类型将是LEAP。由于已知LEAP容易受到字典攻击,同时作为良好的安全实践,CTK也必须被相互导出以保护IN和IN认证者之间交换的数据。

[1008] 认证“请求者”IN与其双亲AP或CM交换EAPOL认证消息。请求者的双亲AP或CM在请求者和根CM中的IN认证者之间中继EAPOL认证消息。EAPOL认证消息被封装在WLCCP AAA消息请求和应答消息中,但有一个例外。孩子AP必须在802.11链路上和其双亲AP交换原始EAPOL消息。

[1009] IN认证者包含RADIUS客户,该客户把EAP认证请求消息转换为RADIUS请求消息,并把RADIUS响应消息转换为AAA消息应答。IN认证者根据接收到的RADIUS消息确定认证过程是否已经失败。IN认证者通过在WLCCP_AAA应答中返回非零状态值表示认证失败。

[1010] 在初始认证期间建立秘密的“会话密钥”NSK。然后,NSK与交换的密钥材料一起被IN和IA使用以相互导出CTK。保护TLV和IN和IA之间的消息的CTK是唯一要求相互导出的CTK,所有其他链路的CTK由IA通过强伪随机函数导出并被发送到IN。

[1011] 如果用CCM的IP地址配置SCM或LCM,则SCM或LCM确定它必须和CCM中的IN认证者相互认证。

[1012] 所有的基础结构节点在成功的LEAP认证之后,也必须开始“路径认证”,以便和每个祖先相互认证并建立CTK。在下面名为“基础结构路径认证”的部分中描述了路径认证。

[1013] SCM通告应答消息包含ROOT_CM_INFO TLV,ROOT_CM_INFO TLV使得AP能够自动地发现根CM和IN认证者。最初AP必须向被包含在TLV中的IP地址标识的IN认证者认证。

[1014] 发送到AP的注册应答消息可以包括标识了当前的MN认证者的MN_1X_AUTHEN TLV。SCM能够在包含在SCM通告应答消息中的MN_1X_AUTHEN TLV中通告新的MN认证者。

[1015] IN必须周期性地重复初始认证过程以保持一个“新生”的会话密钥(例如NSK);NSK的刷新通过认证服务器(AS)定义的会话超时时间确定。

[1016] 在独立模式中时,SCM既作MN认证者,也作IN认证者。要求只具有单个安全上下文TLV的路径初始化消息,因为它只要求和IN认证者(例如SCM)的直接CTK。由于这是唯一存在的链路,所以路径初始化消息只要求3路握手:请求、应答和确认。但是,为了和完整拓扑基础结构保持一致,在SCM独立配置中,对路径初始化来说,AP应该使用请求/应答握手,并通过在注册请求/应答交换中使用认证者TLV确认密钥建立。

[1017] 但是,在完整的SWAN拓扑中,为了在请求IN和其祖先之间建立密钥传送和存活性

确认,需要完整的4消息握手。对于密钥传送需要请求/应答消息,而为了证明每个链路是存活的则需要确认/ack。图29给出了根AP认证的实例。虽然实例演示了根AP认证和CTK建立,但是对所有其他基础结构节点,例如LCM and SCM,需要相同的步骤。

[1018] 在基础结构节点已经最初认证之后,它必须和其每个祖先节点包括IA 相互认证并建立单独的秘密“上下文传递密钥”(CTK)。Path-Init消息用于在请求者IN和其祖先之间建立CTK。每个祖先节点必须提供16字节的现时标志以便实现新生CTK的分发。为此目的,IA起到被信赖的密钥分发中心KDC的作用。CTK用于产生MIC,并加密在拓扑树的分支上转发的消息中的敏感的上下文信息。CTK是256位的值,其低128位用于认证消息和TLV,而其高128位用于加密消息和TLV。

[1019] 对在IN和IA之间使用的CTK,请求者IN在Path-Init请求消息中必须提供16字节的现时标志以便IA能导出CTK。IA在Path-Init应答消息中必须提供其16字节的现时标志以便IN能导出CTK。需要最终的Path-Init确认消息以允许IN确认密钥材料的适当接收和CTK的存活性。如果通过使用WTLV_INIT_SESSION TLV请求了完整的路径认证,则需要第四个消息来建立在Path-Init请求/应答交换中分发的CTK的存活性。

[1020] 未注册的和未认证的IN“请求者”通过发送Path-Init请求消息开始路径认证并把WTLV_INIT_SESSION嵌入其选中的双亲节点。在Init会话TLV中包括安全上下文TLV,安全上下文TLV包括IN的指向IA的16字节现时标志(例如,DST-ID在安全上下文TLV中是IA)。双亲节点把Path-Init请求向内转发到包含IA的根CM。在到根CM的路径上的每个节点包括双亲节点在请求消息的Init会话TLV中插入安全上下文TLV。根CM中的IN认证者在其接收到Path-Init请求时从WTLV_IN_SECURE_CONTEXT_REQ TLV中确定请求者的祖先列表。

[1021] IA将相互导出CTK以保护请求IN和IA之间的链路。此外,IA将为请求者的每个祖先产生CTK。IA必须首先导出保护IN-IA链路的CTK,以便它能产生瞬时密钥TLV,把CTK正确地传送到请求IN。对于全部祖先,CTK被嵌入对应的(并且现在被加密的)安全上下文TLV中。对与IN-IA链路对应的安全上下文TLV,TLV包括IA产生的现时标志,并且使用新建立的CTKIN-IA计算新的MIC。安全上下文TLV中的该WTLV_MIC起到请求IN的存活性认证者的作用。

[1022] 为了更好的描述把IN认证到SWAN拓扑所需的操作,定义了简化的术语。首先,图30中明确地定义了一组CTK。

[1023] AP路径认证如下:

[1024] -在AP和CCM之间共享NSK。

[1025] -假设其祖先已经成功地注册。在图30中所示的实例中,CTK1、CTK2和CTK3是新生的并且是有效的。这是CTK用于传送和认证CTK5到LCM的传送时的要求。虽然CTK2用于把CTK6传送到SCM,但是通过LCM被发送。LCM反过来使用CTK3保护WTLV_IN_SECURE_CONTEXT_REPLY。

[1026] WTLV_TRANSIENT_KEY的使用用简写形式描述为:

[1027] $TKE1 = WTLV_TRANSIENT_KEY(CTK4, KSCAP-LCM || LCM-ID || AP-ID || CTK5 || MIC_{CTK4})$

[1028] $TKE2 = WTLV_TRANSIENT_KEY(CTK4, KSCAP-SCM || SCM-ID || AP-ID || CTK6 || MIC_{CTK4})$

[1029] 这些TKE被嵌入加密的安全上下文TLV中,其简写形式是:

[1030] $WSC0 = WTLV_IN_SECURE_CONTEXT_REQ(<no\ encryption/MIC>, IA-ID || AP-ID || Nonce_{AP})$

- [1031] WSC1=WTLV_IN_SECURE_CONTEXT_REQ(CTK2,SCM-ID|AP-ID|Nonce_{SCM}|MIC_{CTK2})
- [1032] WSC2=WTLV_IN_SECURE_CONTEXT_REQ(CTK1,LCM-ID|AP-ID|Nonce_{LCM}|MIC_{CTK1})
- [1033] WSC3=WTLV_IN_SECURE_CONTEXT_REPLY(CTK1,
- [1034] LCM-ID|AP-ID|Nonce_{LCM}|CTK5|TKE1|MIC_{CTK1})
- [1035] WSC4=WTLV_IN_SECURE_CONTEXT_REPLY(CTK2,
- [1036] SCM-ID|AP-ID|Nonce_{SCM}|CTK6|TKE2|MIC_{CTK2})
- [1037] WSC5=WTLV_IN_SECURE_CONTEXT_REPLY(<no encryption>,AP-ID|IA-ID|Nonce_{IA}|MIC_{CTK4})
- [1038] WAUTH1=WTLV_AUTHENTICATOR(CTK6,
- [1039] KSC_{AP-SCM}|SCM-ID|AP-ID|Nonce_{AP-SCM}|MIC_{CTK6})
- [1040] WAUTH2=WTLV_AUTHENTICATOR(CTK5,
- [1041] KSC_{AP-LCM}|LCM-ID|AP-ID|Nonce_{AP-LCM}|MIC_{CTK5})
- [1042] WAUTH3=WTLV_AUTHENTICATOR(CTK4,
- [1043] KSC_{AP-CCM}|CCM-ID|AP-ID|Nonce_{AP-CCM}|MIC_{CTK4})
- [1044] WAUTH4=WTLV_AUTHENTICATOR(CTK6,
- [1045] KSC_{AP-SCM}|SCM-ID|AP-ID|Nonce_{AP-SCM}+1|MIC_{CTK6})
- [1046] WAUTH5=WTLV_AUTHENTICATOR(CTK5,
- [1047] KSC_{AP-LCM}|LCM-ID|AP-ID|Nonce_{AP-LCM}+1|MIC_{CTK5})
- [1048] WAUTH6=WTLV_AUTHENTICATOR(CTK4,
- [1049] KSC_{AP-CCM}|CCM-ID|AP-ID|Nonce_{AP-CCM}+1|MIC_{CTK4})

[1050] 使用上面的术语,路径认证期间的WTLV_INIT_SESSION(WIS)TLV交换用作认证和建立请求基础结构节点和其祖先之间的路径CTK的方法。图31中示出了认证和注册到基础结构的AP实例。

[1051] 图32中示出了用于在路径需要更新但是不要求注册时的另一个序列。

[1052] 传送到请求者的每个CTK在WTLV_TRANSIENT_KEY TLV中编码。在WTLV_SECURE_CONTEXT_REPLY TLV中,CTK被直接传送到请求者的祖先。然后把TLV的列表输入到Path-Init应答消息中,该消息被发送到请求者的双亲节点。双亲节点把应答中继到请求者。在Path-Init应答的远离路径上的每个节点在它接收到它相应的WTLV_SECURE_CONTEXT_REPLY TLV时解密它与请求者共享的CTK。如图32所示,如上文所述,一旦请求者接收到Path-Init应答消息,它必须通过其双亲节点发送“初始”注册请求消息到根CM。对其每个祖先节点,请求者必须把WTLV_AUTHENTICATOR TLV输入到请求消息。每个祖先节点在它接收到其WTLV_AUTHENTICATOR TLV时“认证”请求者;因此,在产生注册应答之前,完整地认证了请求者。每个祖先节点在转发注册请求之前,必须更新和重新加密WTLV_AUTHENTICATOR TLV。请求者当其在注册应答中接收到更新的 WTLV_AUTHENTICATOR TLV的列表时,对其每个祖先节点进行相互认证。

[1053] 如图33中所示,可以类似地刷新CTK,唯一的区别是不需要注册,而且因此它把Path-Init消息扩展为使用子类型Confirm(确认)和ACK,而不是使用注册消息类型。

[1054] 必须根据用来提供保密和可认证性的密码套件所定义的熵刷新CTK。(初始版本将使用RC4和HMAC-MD5分别加密和认证所有消息或TLV。但是,将来的版本可能支持AES)。当消

息序列计数器已经耗尽或者处于不超过一天几次的频率时必须刷新CTK(6小时间隔是合理的)。但是,如果节点经历频繁的挑战和或解密失败,它应该静静地丢弃这些消息。作为选择(例如在将来的版本中),通过适当的启发,IN能够决定是否触发CTK刷新或完整的(重)认证。

[1055] 使用WTLV_INIT_SESSION,能对整个分支可选择地刷新CTK刷新,或者使用安全上下文请求/应答交换刷新单个CTK。虽然在WTLV_INIT_SESSION或WTLV_SECURE_CONTEXT_REQ和WTLV_SECURE_CONTEXT_REPLY中也建立并刷新了基础结构节点和IA之间使用的CTK,但是它的密钥不能由IA直接传送,而是交换密钥材料(如现时标志)来相互导出CTK。因此,WTLV_SECURE_CONTEXT_{REQ/REPLY}的语义根据CTK是被传送的还是被到处的而变化。

[1056] 为重定密钥或建立单个CTK,请求者IN向IA请求新生的密钥。需要2阶段的交换。在第一阶段,WTLV_SECURE_CONTEXT_TLV用于建立CTK。在第二阶段,WTLV_AUTHENTICATOR_TLV用于确认CTK的存活性。第一阶段在Path-Init请求/应答交换期间完成,而第二阶段在通过使用WTLV_AUTHENTICATOR的初始注册期间完成。需要第二阶段来确保链路节点之间的CTK存活性。

[1057] 如图33中所示,是用于保护AP和SCM之间的链路的CTK如何使用CCM用于密钥传送,从AP到SCM的直接路径认证以确认CTK的存活性的实例。

[1058] -移动节点安全上下文传递

[1059] 如上所述,在初始MN认证过程中建立了MN的动态安全证书。这些证书包括:NSK、会话超时时间、VLAN ID、SSID、Krk、BTK和RN。MN缓存的配置信息和动态证书在MN漫游时被自动地传递到新双亲AP。缓存的配置信息和动态证书也被转发到新路径上的任何新SCM,以便把将来的漫游本地化(即使得当MN在子网内漫游时不访问LCM)。在SCM注册更新期间把动态证书转发到SCM。

[1060] MN SSID认证

[1061] 必须授权MN使用其SSID。当MN认证时,802.1X认证服务器给MN返回允许的SSID的列表。SSID的列表(和任何其他静态配置信息)被缓存在到MN的路径上的每个CM中。MN的SSID被包括在MN的预注册和注册请求中。每次最近共同祖先CM接收到对MN的预注册和注册请求时,它验证MN被授权使用其SSID。

[1062] 快速漫游和重定密钥

[1063] 在重关联请求后,漫游节点影响到新AP的认证的密钥刷新请求。新AP随后通过预注册请求向MN认证者请求安全证书。MN认证者必须验证MN提供的安全证书(由新AP转发给MN认证者)。在成功的预注册应答之后,MN认证者将把安全证书转发给新AP。在失败的预注册应答之后,MN认证者将只提供表明故障点的状态码,并允许AP决定是否允许MN通过强加完整的认证来重新建立证书或者对MN完整地解除关联。

[1064] -MN安全上下文转发

[1065] 在完整拓扑中,LCM用作MN认证者。完整拓扑中MN认证者的定位可能带来更长的延迟,因此人们期望把MN的安全证书向下转发到SCM。证书的转发在注册请求/应答期间完成。这允许MN的基础结构祖先,主要是SCM,缓存MN的安全证书并辅助漫游。

[1066] 通过请求来转发证书。即,在MN注册请求期间,每个祖先(AP除外)可插入请求转发MN证书的WTLV_SECURE_CONTEXT_REQ,在安全上下文TLV中必须包括MIC,并由MN认证者验

证。在成功的请求之后，MN认证者随后将嵌入包括所有在TLV中加密的缓存的证书的WTLV_MN_SEC_CONTEXT_REPLY TLV。像请求一样，在应答之后，也必须对安全上下文TLV进行MIC处理。图34中示出了SWAN拓扑中MN认证和注册的完整描述。

[1067] WLCCP_AAA是为节点认证定义的唯一显式消息类型。通过WLCCP消息封装中的MIC的方法，把EAPOL消息路由到节点到认证者时，保护它们免于中间人攻击。

[1068] 通过使用一种修正型RC4算法提供保密和HMAC-MD5以提供消息认证，可以保护TLV。为了保密，使用标准RC4算法加密TLV，但是丢弃RC4流的最初256字节以阻止FMS攻击。为了可认证性，在WLCCP中包括MICTLV。因此CTK是由两个密钥构成的256位的值，高128位用作HMAC-MD5密钥，而低128位用作RC4密钥。

[1069] 使用消息完整性检验(Message Integrity Check)(MIC)TLV认证WLCCP消息。源节点能够可选择地把MIC标志设置为0N，并在WLCCP消息中输入WTLV_MIC TLV来“认证”到目的地的消息。TLV包含用由源和目的地共享的上下文传递密钥(CTK)的高128位计算的MIC。如果请求消息被认证，则对应的应答消息也必须被认证。每一个源和目的地节点都保持一个消息序列计数器MSC，该计数器在初始化或刷新CTK时被初始化为0。MSC起到重放计数器以及RC4初始化向量的作用。如果当前的MSC小于或者等于先前的MSC的值，则消息是重复的而必须被丢弃。MSC的值与CTK的低128位连接起来产生RC4密钥。按小端顺序：

[1070] $RC4\text{-key} = MSC || CTK[0:127]$ 其中 $||$ 是连接函数。

[1071] 为了避免MSC冲突和定向的CTK的定义，MSC值在进入路径上应该是偶数而在远离路径上为奇数。每次加密或认证TLV或消息时应该增大MSC值。

[1072] 使用在预注册/注册过程期间建立的CTK来认证在SWAN拓扑树的分支上转发的消息。使用动态建立的横向CTK认证被“横向”转发的消息。在下面的部分中讨论横向消息认证。

[1073] 如果在消息中，中继标志被设置为OFF，则使用由发起者和响应者共享的CTK计算MIC。中间AP可以“中继”用“跳路由”(HopwiseRouting)转发的消息。如果在消息中中继标志被设置为0N，则使用直接发送者和接收者共享的CTK计算MIC。用于为被跳路由的消息确定共享CTK的规则如下：

[1074] 进入消息的直接发送者AP使用它与双亲节点共享的CTK。

[1075] 远离消息的直接发送者(AP或SCM)使用它和下一跳孩子节点共享的CTK。

[1076] 直接接收者使用它和直接发送者共享的CTK。如果中继标志被设置为OFF，则直接发送者在请求消息中是发起者，而在应答消息中是响应者。如果中继标志被设置为0N，则直接发送者是由所需的中继节点ID字段标识的“中继节点”。

[1077] CTK也被用于加密任何包含敏感数据(例如后代节点的会话密钥)的TLV。确定用于加密敏感TLV的CTK的规则与确定用于消息认证的消息的CTK的规则相同。注意，每个中继AP必须解密并重新加密被用跳路由转发的消息中的TLV。

[1078] 定义TLV以便允许节点认证、上下文管理以及CTK和PTK管理(即路径认证和预注册)。

[1079] 建立、缓存和管理安全证书有5个基本操作；在下面的表格中这些被定义为TLV组ID(TLV Group ID)：

[1080]

TLV类型ID	值	描述
WTLV_INIT_SESSION	0x0101	IN节点必须向SWAN基础结构 初始化其CTK。MN节点必须向 SWAN基础结构初始化其BTK。
WTLV_IN_SECURE_CONTEXT_REQ	0x0102	IN节点CTK刷新
WTLV_UPDATE_RN	0x0103	MN PTK排序的更新
WTLV_TRANSIENT_KEY	0x0104	传送CTK
WTLV_AUTHENTICATOR	0x0106	注册后必须完成链路认证。
WTLV_NSK	0x0107	因为密钥被静态配置,所以MN 认证者必须从关联的AP获取 NSK。
WTLV_MIC	0x0108	可以被嵌入消息或TLV中的通

[1081]

		用MIC
WTLV_MN_SEC_CONTEXT	0x0109	用于转发所需MN安全证书的 TLV
WTLV_IN_SECURE_CONTEXT_REPLY	0x010a	用于传送IN CTK的TLV
WTLV_MN_SECURE_CONTEXT_REQ	0x010b	IN对MN证书的请求
WTLV_MN_SECURE_CONTEXT_REPLY	0x010c	IA对MN缓存请求的响应
WTLV_EAP_ID	0x010d	EAP身份
WTLV_CCKM_ASSOCIATE	0x010e	CCKM验证所需的802.11关联 的内容。
WTLV_CCKM_REASSOCIATE	0x010f	802.11重关联CCKM要素的内 容

[1082] 第四个类型WTLV_TRANSIENT_KEY是用于传送WTLV_INIT_SESSION或WTLV_SECURE_CONTEXT_REPLY中的链路密钥的嵌入式TLV。

[1083] MN的EAP身份请求/响应中提供的身份字串在SCM处被缓存,并在安全上下文TLV中用来使能AP处的适当记帐。因为EAP身份可以是任意长度,所以TLV如下定义:

[1084]

TLV类型ID	长度	身份(字节)长度	EAP身份
WTLV_EAP_ID	TLV长度	8字节	N字节

[1085] -WTLV_MIC

[1086] 另一个用于保护WLCCP消息或TLV的TLV是WTLV_MIC。它被如下定义:

[1087]

TLV类型ID	长度	消息序列计数器	MIC长度(按 字节)值=8	MIC
WTLV_MIC	TLV长度	8字节	2字节	8字节

[1088] 为了某些将来的使用,WTLV_MIC允许MIC的扩展。最初,MIC长度被预设置为8字节,以将MIC定义为8字节长度。消息序列计数器用于定义使用对应CTK产生的WTLV_MIC的数量。这个TLV将被附加到任何其标志 值包括MIC标志(0x0100)的WLCCP消息上。需要WTLV_MIC的消息必须定义HMAC-MD5函数所覆盖的字段。

[1089] 一些需要WTLV_MIC TLV的WLCCP消息和TLV是:

[1090] WTLV_MIC只用于为MN认证来认证WLCCP_AAA消息。

[1091] 在转发MN的密钥时,WTLV_TRANSIENT_KEY必须包括认证CTK的传送的MIC。

[1092] WTLV_MN_SECURE_CONTEXT_REQ、WTLV_IN_SECURE_CONTEXT_REQ、WTLV_IN_SECURE_CONTEXT_REPLY和WTLV_MN_SECURE_CONTEXT_REPLY在被增加和跳到跳地传播时必须被认证。

[1093] 在WTLV_INIT_SESSION被增加和从请求者节点向其认证者传播时,它必须被认证。

[1094] WTLV_AUTHENTICATOR必须包括MIC,确保请求者节点和祖先之间的会话存活性。

[1095] -WTLV_INIT_SESSION:路径认证和预注册

[1096] 建立CTK和BTK分别需要路径认证和预注册。对于IN节点,在节点和其直到根CM的祖先之间必须建立CTK。WTLV_INIT_SESSION TLV触发用于建立新生CTK的状态。在成功的

WTLV_INIT_SESSION之后,把序列计数器初始化到零,并且为请求IN节点和IN认证者之间的所有链路建立CTK。

[1097] 对MN节点,只需要PTK,供MN和其当前关联的AP来使用。MN和IA之间建立的密钥必须在PTK能够相互导出并在MN和AP之间使用之前,被转发到AP。但是,必须首先为CCKM MN建立BTK。WTLV_INIT_SESSION触发用于建立新生CTK和BTK的状态。在成功的802.1X认证之后,把序列计数器初始化到零,并且为请求IN节点和IN认证者之间的所有链路建立CTK,其中,WTLV_INIT_SESSION紧跟着802.1X认证。只有在成功的认证之后,才把密钥序列计数器设置为零,每次密钥被刷新就增加它们。

[1098] 对于CCKM MN,建立BTK和第一PTK用于保护AP和MN之间的数据分组;这当然暗示着,对SCM独立模式,AP必须已经保护其自身和SCM之间的CTK。即AP在能预注册或者注MN之前,它必须首先认证并注册到SWAN拓扑中去。

[1099] WTLV_INIT_SESSION TLV如下定义:

[1100]

字段名	长度	描述
WTLV_INIT_SESSION	2	TLV类型
TLV Length(TLV长度)	2	TLV长度
保留	1	保留,用于字节对齐
Path Length(路径长度)	1	请求者和IN认证者之间的祖先 的数量
Optional TLV(s)(可选 TLV)	N	取决于规定的状态和方向,必须 包括不同的TLV。

[1101] 由于TLV长度可变,所以每个TLV都以一个偏移量开头,表示下一个TLV长度或者到下一个TLV的偏移量。0(零)偏移量表示结尾,例如,不再有TLV。

[1102] -用于MN的WTLV_INIT_SESSION

[1103] -当MN成功地认证到网络中时,MN认证者将缓存其NSK和其他的相关安全证书。如果CCKM是协商的认证密钥管理选择器,则MN认证者必须用EAPOL密钥向MN作出响应,并触发KRK和BTK的建立。

[1104] 来自MN的响应提供了AP能够验证的Noncemn和协商的安全要素。但是,MN认证者也必须验证这些证书中的一些,以确保没有发生VLAN跳。

[1105] 对于进入的MN预注册请求,WTLV_INIT_SESSION包括安全上下文TLV,该安全上下文TLV包括作为目的地ID的AP身份以及协商的802.11安全信息要素(RSNIE)。SSID也包括在MN的安全上下文请求中,并由MN认证者检验,以确保MN没有跳过VLAN并因而危害安全性。必须由MN提供安全上下文的现时标志,因为该现时标志起到用于导出KRK和BTK的密钥材料的作用。

[1106] AP产生的(代表MN)WTLV_INIT_SESSION如下定义:

[1107]

字段名	长度	描述
-----	----	----

[1108]

WTLV_INIT_SESSION	2	TLV类型
TLV Length(TLV长 度)	2	TLV长度
保留	1	0
Path Length(路径长 度)	1	请求者和IN认证者之间的祖先的数量
SECURE_CONTEXT TLV	N	用SID=MN-ID和DID=AP-ID嵌入 MN_SECURE_CONTEXT,包括RSNIE

[1109] 如果MN已经协商CCKM,则它也必须已经提供一个被嵌入WTLV_MN_SECURE_

CONTEXT_REQ的现时标志。如果MN没有提供现时标志,则AP应该触发错误。

[1110] 如果MN已经协商SSN或者遗留系统,则AP必须只获取NSK。但是,如果MN已经协商CCKM,则MN认证者必须导出并把CTK传送到AP并缓存Krk。因此,响应之后,MN认证者必须把嵌入MN_SECURE_CONTEXT_TLV中的密钥(NSK或BTK)传送到AP。由于它是请求这样的密钥的MN,所以MN认证者将忽略一般用于传送NSK或BTK到MN的WTLV_TRANSIENT_KEY。当MN已经相互导出这个密钥,并且它不需要知道AP之后是什么时,这个步骤是多余的和不必要的。

[1111] 1.1.1.1.1.1用于IN的WTLV_INIT_SESSION

[1112] IN节点的路径认证和CTK的初始化假设IN的祖先已经成功地注册到SWAN基础结构中。使用包括如下表格的WTLV_INIT_SESSION TLV的Path-Init请求开始路径认证:

[1113]

字段名	长度	描述
WTLV_INIT_SESSION	2	TLV类型
TLV Length(TLV长度)	2	TLV长度
保留	1	0

[1114]

Path Length(路径长度)	1	0
Secure Context Request for IN-IA TLV(对IN-IA TLV的安全上下文请求)	N	WTLV_IN_SECURE_CONTEXT_REQ SID=IN,DID=IA

[1115] 当WLCCP Path-Init被转发到IA时,通过嵌入它们的WTLV_SECURE_CONTEXT_REQ,请求者的祖先反过来将请求一个密钥以保护它和请求IN之间的链路:

[1116]

字段名	长度	描述
WTLV_INIT_SESSION	2	TLV类型
TLV Length(TLV长度)	2	TLV长度
保留	1	0
Path Length(路径长度)	1	0
Secure Context Request for IN IA TLV	N	WTLV_IN_SECURE_CONTEXT_REQ SID=IN,DID=IA
Secure Context Request for Ancestor[i]TLV	M	WTLV_IN_SECURE_CONTEXT_REQ SID=IN,DID=Ancestor[i]
...安全上下文TLV的续表		

[1117] 当进入WTLV_INIT_SESSION请求增大WTLV_IN_SECURE_CONTEXT_REQ时,远离应答将使用这些TLV并以WTLV_IN_SECURE_CONTEXT_REPLY响应,并用CTK和将由请求者节点使用的WTLV_TRANSIENT_KEY更新它们。图33是节点如何初始化它自己和其直到IA的祖先路径之间的CTK的实例。

[1118] 当请求被转发到IA时,每个祖先必须使得Path Length(路径长度)字段加1。IA必须返回这个值并确认在WTLV_INIT_SESSION中有路径长度WTLV_SECURE_CONTEXT_REQ TLV。如果提供得太多或者太少,则它必须丢弃这个请求。

[1119] 每个祖先必须标识它自己并提供其相应的WTLV_SECURE_CONTEXT_REQ。IA反过来将把每个请求安全上下文TLV转换为WTLV_SECURE_CONTEXT_REPLY,以传送适当的CTK。由于密钥在WTLV_SECURE_CONTEXT_REPLY内传送,所以响应安全上下文TLV必须既被加密也被做MIC处理。

[1120] -WTLV_TRANSIENT_KEY:传送密钥

[1121] 密钥必须被安全地分发。为确保此事,使用源和预期接收者之间共享的秘密对密钥加密。TLV被如下封装:

[1122]

类型	长度	KSC	IN-ID	IN-ID	密钥	MIC TLV
WTLV_TRANSIENT_KEY	TLV 长度	密钥序 列计数 器	源IN ID	目的IN ID	E _{SUP_DST}	KEY- MIC _{SUP_DST}

[1123] TLV从整个WLCCP消息中暗示源IN标识符以避免太多的冗余。加密使用RC4,以便只加密密钥:

[1124] $E_{SUP_DST} = \text{Encrypted Key RC4}(\text{MSC} || \text{CTK}_{\text{Authenticator_IN-ID}}, \text{CTK}_{\text{IN-ID_SupplicantID}})$

[1125] 使用IN认证者和目的IN之间建立的密钥加密密钥CTK_{IN-ID_SupplicantID}。被传送的密钥CTK_{IN-ID_SupplicantID}用于保护目的IN和请求者之间的数据。对于请求者节点,由于它是还未注册的叶子节点,所以NSK用于传送其CTK。

[1126] 用于保护AP和MN之间的消息的密钥传送和上面定义的相同,区别是,BTK是和重定密钥序列号一起只给AP的被传送的密钥。:

[1127] $E_{AP} = \text{Encrypted Key RC4}(\text{MSC} || \text{CTK}_{\text{Authenticator_AP}}, \text{BTK}_{\text{MN}})$

[1128] TLV的认证包括在WTLV_TRANSIENT_KEY中被排除但在整个WLCCP消息内的字段。对IN节点响应的MIC如下计算:

[1129] $\text{KEY-MIC}_{\text{SUP_DST}} = \text{HMAC-MD5}(\text{CTK}_{\text{Authenticator_IN-ID}}, \text{KSC}, \text{SNonce}, \text{ANonce}_i,$

[1130] $\text{Supplicant-ID}, \text{Destination-IN_ID}, E_{\text{SUP_DST}})$

[1131] 对BTK的AP请求的响应MIC如下计算:

[1132] $\text{KEY-MIC}_{\text{AP}} = \text{HMAC-MD5}(\text{CTK}_{\text{Authenticator_AP}}, \text{KSC}, \text{SNonce}, \text{ANonce}_i,$

[1133] $\text{Supplicant-ID}, \text{Destination-IN_ID}, E_{\text{AP}})$

[1134] 用于所有传送到目的IN的密钥的计数器KSC必须被保留,并在目的IN和IN认证者之间使用以防止重放。类似地,如果密钥被传送到AP,用于保护AP到MN的通信,则它必须保持对其KSC中的这些密钥的计数。

[1135] -安全上下文TLV

[1136] 安全上下文TLV用于建立请求者节点和其祖先之间的链路密钥。由于请求安全上下文TLV不包括密钥,但包括运送请求的其他相关信息,所以安全上下文TLV被分割为请求和响应安全上下文TLV。此外,由于MN定义密钥管理类型,并由AP代理,所以用于请求MN安全证书的安全上下文和IN安全上下文有区别。

[1137] 请求MN安全上下文TLV如下定义:

[1138]

字段名	长度	描述
WTLV_MN_SECURE_CONTEXT_REQ	2	TLV类型
TLV Length(TLV长度)	2	TLV长度
Key Sequence Counter(KSC)(密钥序列计数器)	4	这个密钥已经被更新的次数
Destination-ID(DID)(目的ID)	8	请求和SID共享密钥的祖先
Supplicant-ID(SID)(请求者ID)	8	请求(请求者)节点
保留	1	用于对齐字节
Key Management Type(密钥管理类型)	1	0-无(不转发NSK) 1-CKKM 2-802.1X遗留系统(进行有效的重认证)转发NSK。 3-SSN (建立IN路径CTK时忽略这个字段)
Nonce(现时标志)	16	随机值
EAP ID	Q	EAP ID TLV

[1139]

SSID	L	SSID TLV
RSNIE	P	传播RSNIE _{req} TLV用于认证
Optional (CKKM)TLVs(可选 (CKKM)TLV)	N	如果CKKM是协商的密钥管理,则关联或重关联TLV必须 被提供
MIC	M	这个TLV的WTLV_MIC

[1140] 当CCKM是协商的密钥管理时,也提供可选的TLV,因此在关联或重关联CCKM要素之后,MN认证者要求进一步的工作来验证EAPOL密钥消息。

[1141] 请求IN安全上下文TLV如下定义:

[1142]

字段名	长度	描述
WTLV_IN_SECURE_CONTEXT_REQ	2	TLV类型
TLV Length(TLV长度)	2	TLV长度
Key Sequence Counter(KSC)(密钥序列计数器)	4	这个密钥已经被更新的次数
Destination-ID(DID)(目的 ID)	8	请求和SID共享密钥的祖先
Supplicant-ID(SID)(请求者 ID)	8	请求(请求者)节点
Nonce(现时标志)	16	随机值
MIC	M	这个TLV的WTLV_MIC

[1143] 响应MN安全上下文TLV如下定义:

[1144]

字段名	长度	描述
WTLV_MN_SECURE_CONTEXT_REPLY	2	TLV类型
TLV Length(TLV长度)	2	TLV长度
Key Sequence Counter(KSC)(密钥序列计数器)	4	这个密钥已经被更新的次数
Destination-ID(DID)(目的ID)	8	请求和SID共享密钥的祖先

[1145]

		先
Supplicant-ID(SID)(请求者 ID)	8	请求(请求者)节点
Nonce(现时标志)	16	随机值
Session Timeout(会话超时时间)	4	MN的剩余会话超时时间
EAP ID	Q	EAP ID TLV
Rx Key Length(Rx密钥长度)	2	Rx密钥长度
Rx Key(Rx密钥)	32	对应于CTK、BTK或NSK 之一
Optional Tx Key Length(可选Tx 密钥长度)	2	Tx密钥长度
Optional Tx Key(可选Tx密钥)	M	当AS将Tx密钥作为成功的认证的结果返回时,只在成功的认证后提供。
Optional MN Cached Credentials (可选的MN缓存证书)	P	只在MN注册期间提供,以便把缓存的证书从IA转发到 远离节点(SCM)。
MIC	Q	这个TLV的WTLV_MIC

[1146] 响应MN安全上下文TLV最终将把密钥传送到请求者节点。取决于请求者节点(SID)的类型,包括可选的字段。后面的分段进一步描述了基于请求的所需字段。

[1147] 当MN漫游时,WLCCP预注册用于请求安全证书。双亲AP向SCM发送预注册请求消息来请求安全证书。(如果安全证书未被缓存在SCM中,则可以按照要求向内转发请求。预注册请求包括WTLV_SECURE_CONTEXT_REQTLV。双亲AP必须被认证,并在其自己和SCM之间具有已建立的CTK(即通过路径认证)。

[1148] 包含在预注册应答中的WTLV_SECURE_CONTEXT_REPLY用于传送密钥,因此TLV必须被如下加密:

[1149] $RC4'(MSC || CTK_{IN-IA}, Key Management Type || Nonce || \langle TLV中包含的字段 \rangle)$

[1150] 类似地,在响应期间,TLV必须被如下认证:

[1151] $MIC = HMAC-MD5(CTK_{IN-IA}, DST-ID || SRC-ID || KSC ||$

$Nonce || \langle TLV中包含的字段 \rangle)$

[1153] 响应IN安全上下文TLV如下定义:

[1154]

字段名	长度	描述
WTLV_IN_SECURE_CONTEXT_REPLY	2	TLV类型
TLV Length(TLV长度)	2	TLV长度
Key Sequence Counter(KSC)(密钥序列计数器)	4	这个密钥已经被更新的次数
Destination-ID(DID)(目的 ID)	8	请求和SID共享密钥的祖先
Supplicant-ID(SID)(请求者 ID)	8	请求(请求者)节点
Nonce(现时标志)	16	随机值
Session Timeout(会话超时时间)	4	MN的剩余会话超时时间
CTK Key Length(CTK密钥长度)	2	Rx密钥长度
CTK Key(TK密钥)	32	对应于CTK、BTK或NSK之一
Optional Key TLV(可选的密钥 TLV)	N	把新CTK传送到SID的 WTLV_TRANSIENT_KEY。在IN之间建立CTK时必须提供这个字段。当SID IN和其IA相互导出密钥时没有这个字段。
MIC	Q	这个TLV的WTLV-MIC

[1155] -为CCKM传播MN关联信息

[1156] 当WTLV_CCKM_ASSOCIATE要素被与KRK做MIC处理时,它用于从MN向MN认证者转发第二EAPOL密钥消息,其中,只有MN认证者持有KRK。EAPOL密钥消息必须被MN认证者验证。因此TLV被如下定义,以传播EAPOL密钥消息用于MIC验证:

[1157]

字段名	长度	描述
WTLV_CCKM_ASSOCIATE	2	TLV类型
TLV Length(TLV长度)	2	TLV长度
EAPOL message length (EAPOL密钥消息长度)	4	EAPOL密钥消息的字节长度
EAPOL message(EAPOL密钥消息)	N	EAPOL密钥消息被AP接收并转发到MN认证者。
MIC-KRK	P	包含使用KRK的EAPOL MIC的MIC TLV

[1158] -传播MN的重关联CCKM要素。

[1159] WTLV_CCKM_REASSOCIATE要素用于转发重关联消息中,由MN提供的CCKM信息要素的MIC部分和时间戳。当CCKM有效时,MN在重关联消息中包括CCKM要素,消息格式为:

[1160]

要素ID	长度	OUI	OUI类	时间戳	RN	MIC _{MN}
1字节	1字节	3字节	1字节	8字节	4字节	8字节

[1161] AP将RN值设为MN安全上下文请求TLV中的KSC字段。此外,它在CCKM重关联TLV中如下传播这个要素:

[1162]

字段名	长度	描述
WTLV_CCKM_REASSOCIATE	2	TLV类型
TLV Length(TLV长度)	2	TLV长度
Element ID(要素ID)	1	必须为0x9c
Element ID Length(要素 ID长度)	1	应该为24(字节)
OUI	3	必须为00:40:96

[1163]

OUI Type(OUI类型)	1	必须为0
Timestamp(时间戳)	8	必须由AP验证的TSF定时器,转发用于认证。
RN	4	必须和KSC相同,并由MN认证者验证。
MIC	P	包含HMAC-MD5(KRK,MN-ID BSSID RSNIE _{MN} Timestamp RN)的MIC TLV

[1164] -使用WTLV_SECURE_CONTEXT的IN到IN CTK请求

[1165] IN节点可以通过WTLV_SECURE_CONTEXT请求来请求后续CTK。WTLV_SECURE_CONTEXT为请求者和IN之间指定的链路请求新的CTK。请求格式定义如下:

[1166]

字段名	长度	描述
WTLV_IN_SECURE_CONTEXT_REQ	2	TLV类型
TLV Length(TLV长度)	2	TLV长度
Key Sequence Counter(KSC) (密钥序列计数器)	4	用于保持SID和DID之间的链路的重定密钥状态的重放计数器。
Destination-ID(DID)(目的 ID)	8	IN要向之重定密钥的祖先。
Supplicant-ID(SID)(请求者 ID)	8	请求IN
保留	1	用于对齐字节
Key Management Type(密钥管理 类型)	1	对于IN,这个值总是被 设置为0。
Nonce(现时标志)	16	DID提供的随机值

[1167]

MIC	M	这个TLV的WTLV_MIC
-----	---	----------------

[1168] IN认证者将传送CTK,用于保护请求者和IN-ID之间的WLCCP消息。到请求者的传送机制是通过使用WTLV_TRANSIENT_KEY,尽管密钥能够在加密的WTLV_SECURE_CONTEXT中被直接传送到目的地(祖先或者请求者)。

[1169] WTLV_SECURE_CONTEXT响应必须加密现时标志、密钥和密钥TLV,并附上WTLV_MIC。

[1170]

字段名	长度	描述
WTLV_IN_SECURE_CONTEXT_REPLY	2	TLV类型
TLV Length(TLV长度)	2	TLV长度
Key Sequence Counter(KSC)(密 钥序列计数器)	4	这个密钥已经被更新的次 数
Destination-ID(DID)(目的 ID)	8	请求和SID共享密钥的祖 先
Supplicant-ID(SID)(请求者 ID)	8	请求IN
Nonce(现时标志)	16	DID提供的随机值
Session Timeout(会话超时时 间)	4	SID的剩余会话超时时间
CTK Length(CTK长度)	2	CTK长度应为32
CTK	32	SID和DID之间共享的CTK
Key TLV(密钥TLV)	N	把新CTK传送到SID的 WTLV_TRANSIENT_KEY。
MIC	Q	这个TLV的WTLV-MIC

[1171] -使用WTLV_SECURE_CONTEXT的IN到IA CTK请求。

[1172] IN和IA都必须相互导出它们的链路CTK,因为:

[1173] -在清洁(clear)的通道中不能很容易地传送密钥

[1174] -认证时提供的NSK可能不符合新生性要求

[1175] -保护消息和TLV的密钥长度要求可能没有被满足

[1176] 请求者IN在请求WTLV_SECURE_CONTEXT_REQ中必须包括现时标志,以使IA然后能导出CTK并使用它认证应答。应答消息将包括IA的现时标志和其WTLV_SECURE_CONTEXT_REPLY MIC,以及用作对请求者IN的认证者的额外的WTLV_MIC。这个密钥刷新的最终认证和存活性证明必须用WTLV_AUTHENTICATOR完成。

[1177] IN和IA都可以如下相互导出CTK:

[1178] $CTK_{IN-IA} = PRF-256(NSK, "SWAN IN-IA link Context TransferKey Derivation" |$

$|$

[1179] $IN-ID || IA-ID || KSC || Nonce_{AP} || Nonces_{CM}$)

[1180] 所定义的PRF-256函数是基于HMAC-SHA1,并允许NSK扩展到256,并通过让每个节点贡献新生密钥材料来确保新生性。

[1181] 计算出的为IN验证的额外MIC如下定义:

[1182] $MIC_{STATE2} = HMAC-MD5(CTK_{IN-IA}, DST-ID || SRC-ID ||$

[1183] $KSC || Nonce_{IN} || Nonce_{AP})$

[1184] 但是注意,虽然应答在清除中没有发送Nonce_{IN},但是它必须认证Nonce_{IN}的值。另外,由于密钥被相互导出,没有已传送的WTLV_TRANSIENT_KEY,所以这个TLV被如上面所定义的认证MIC所替代。

[1185] -初始关联的WTLV_SECURE_CONTEXT。

[1186] 当具有CKKM能力的MN首次关联,并且802.1X认证到网络中时,SCM开始和MN的4路握手以建立KRK和BTK。消息通过AP转发到MN,AP对WLCCP头解除封装,并把EAPOL密钥消息转发到MN。接收到从MN到SCM的第二个消息之后,AP触发预注册请求来请求转发BTK。快速越区交换规范[8]中描述了这个交换的细节。

[1187] 预注册使用嵌入安全上下文TLV的WTLV_INIT_SESSION,该安全上下文转发下面的MN信息:

[1188]

字段名	长度	描述
WTLV_MN_SECURE_CONTEXT_REQ	2	TLV类型
TLV Length(TLV长度)	2	TLV长度

[1189]

Key Sequence Counter(KSC)(密钥序列计数器)	4	应该被设置为1
Destination-ID(DID)(目的 ID)	8	AP ID
Supplicant-ID(SID)(请求者 ID)	8	MN ID
保留	1	用于对齐字节
Key Management Type(密钥管理 类型)	1	0-无(不转发NSK) 1-CKKM 2-802.1X遗留系统(进行有效的重认证)转发NSK。 3-SSN
Nonce(现时标志)	16	导出KRK和BTK所需的 Nonce _{MN}
SSID	L	SSID TLV
RSNIE	P	传播用于认证的RSNIE _{MN} TLV
Optional TLV(可选的TLV)	M	对CKKM,包括 WTLV_CCKM_ASSOCIATE
MIC	N	这个TLV的WTLV_MIC

[1190] 如果Key Management Type=1(CKKM),则预注册请求包括上面的TLV,以把MN贡献的Nonce_{MN}以及用于证明存活性的MIC TLV传播到MN已经从中正确地导出KRK的SCM。预注册以具有如下安全上下文TLV的应答结束:

[1191]

字段名	长度	描述
WTLV_MN_SECURE_CONTEXT_REPLY	2	TLV类型
TLV Length(TLV长度)	2	TLV长度
Key Sequence Counter(KSC)(密	4	应该为1(RN值)

[1192]

密钥序列计数器)		
Destination-ID(DID)(目的ID)	8	AP-ID
Supplicant-ID(SID)(请求者 ID)	8	MN-ID
Nonce(现时标志)	16	重确认(重发送)第一个消息Nonce _{SCM}
Session Timeout(会话超时时间)	4	MN的剩余会话超时时间
Optional Rx Key Length(可选的 Rx密钥长度)	2	必须=32
Optional Rx Key(可选的Rx密钥)	32	BTK
Optional Tx Key Length(可选的 Tx密钥长度)	2	应该=0
Optional Tx Key(可选的Tx密钥)	0	无Tx密钥可用
MIC	N	这个TLV的WTLV-MIC

[1193] 如果Key Management Type(密钥管理类型)=2 or 3,则MN认证者在它发送预注

册应答之后将去掉MN证书。即，MN认证者将既不缓存也不把PMK传播到除了紧邻AP以外的其他节点。预注册应答通过把PMK转发到使用下列安全上下文TLV的AP结束：

[1194]

字段名	长度	描述
WTLV_MN_SECURE_CONTEXT_REPLY	2	TLV类型
TLV Length(TLV长度)	2	TLV长度
Key Sequence Counter(KSC)(密钥序列计数器)	4	这个值忽略
Destination-ID(DID)(目的ID)	8	AP ID
Supplicant-ID(SID)(请求者 ID)	8	MN ID

[1195]

Nonce(现时标志)	16	这个值没有使用(忽略)
Session Timeout(会话超时时间)	4	MN的剩余会话超时时间
Optional Rx Key Length(可选的 Rx密钥长度)	2	反映基于802.1X认证类型的值
Optional Rx Key(可选的Rx密钥)	32	在MS-MPPE Rx密钥中发送的密钥
Optional Tx Key Length(可选的 Tx密钥长度)	2	反映基于802.1X认证类型的值
Optional Tx Key(可选的Tx密钥)	0	在MS-MPPE Tx密钥中发送的密钥
MIC	N	这个TLV的WTLV-MIC

[1196] 注意，对于在MS-MPPE Radius属性中既提供Rx密钥也提供Tx密钥的认证类型，具有另一种可选的Tx密钥长度。所有的认证类型将提供Rx密钥，Tx密钥是可选的，并且在它没有被认证服务器提供时，其长度将为零。注意，在任何协商的密钥管理类型中，VLAN作为预注册消息中的提供的VLAN字段被转发到AP。

[1197] 从WTLV_SECURE_CONTEXT Nonce字段到结尾(到达但是排除)使用AP和MN认证者之间建立的CTK的WTLV-MIC，加密WTLV_SECURE_CONTEXT应答。类似地，使用HMAC-MD5认证相同字段。

[1198] -用于MN重关联的WTLV_SECURE_CONTEXT

[1199] 在MN漫游时，新的双亲AP必须开始预注册来请求MN的WTLV_SECURE_CONTEXT。为了帮助上下文传递并使得AP和MN之间的处理最少，CCKM提供基本密钥BTK来产生链路密钥PTK。请求的格式如下定义：

[1200]

字段名	长度	描述
WTLV_MN_SECURE_CONTEXT_REQ	2	TLV类型
TLV Length(TLV长度)	2	TLV长度
Key Sequence Counter(KSC)	4	用于保持SID和DID之间

[1201]

(密钥序列计数器)		的链路的更新状态的重放计数器。
Destination-ID(DID)(目的 ID)	8	AP ID
Supplicant-ID(SID)(请求者 ID)	8	MN ID
保留	1	用于对齐字节
Key Management Type(密钥管理 类型)	1	0-无(不转发NSK) 1-CCKM 2-802.1X遗留系统(进行有效的重认证)转发NSK。 3-SSN
Nonce(现时标志)	16	DID提供的随机值
SSID	L	SSID TLV
RSNIE	P	如果State=0，则传播 用于认证的RSNIE _{MN}
Optional(CCKM)TLV(可选的 (CCKM)TLV)	M	对于CCKM，包括 WTLV_CCKM_REASSOCIATE
MIC	N	安全上下文MIC TLV

[1202] 新AP通过使用MN的MAC地址标识MN。BSSID、RN和MIC_{MN}必须由MN提供。RN被封装成KSC。MIC在整个WTLV_MN_SECURE_CONTEXT_REQ消息上是HMAC-MD5操作，以WTLV_MN_SECURE_CONTEXT_REQ类型开始，通过并包括MIC_{MN}。如果State=0，则必须提供MIC_{MN}；这表明MN具有协商的CCKM，并且它正通过特定的MIC_{MN}向MN认证者认证它自己。

[1203] 对于MN认证者,SSID起到验证MN的安全证书,并确保MN没有切换到禁止的VLAN的作用。虽然实际上MN认证者能够有效地匹配安全证书,但是由AP负责决定策略;例如,AP必须定义故障后它将转移到什么状态。MN认证者还必须通过计算和匹配所提供的MIC_{MN}来验证MN的授权。最后,它还必须确保MN的会话超时时间没有到期。在成功的响应之后,MN认证者将把BTK安全地传送到新AP,并改变从旧AP到新AP的切换。即,MN的注册条目将反映出新AP的BSSID,而RN将被加1。响应TLV如下定义:

[1204]

字段名	长度	描述
WTLV_MN_SECURE_CONTEXT_REPLY	2	TLV类型
TLV Length(TLV长度)	2	TLV长度
Key Sequence Counter(KSC)(密钥序列计数器)	4	RN值
Destination-ID(DID)(目的ID)	8	IN想向之更新的祖先
Supplicant-ID(SID)(请求者 ID)	8	请求IN
Nonce(现时标志)	16	DID提供的随机值
Session Timeout(会话超时时间)	4	MN的剩余会话超时时间
Optional Rx Key Length(可选的 Rx密钥长度)	2	传送的密钥的长度(按 字节)
Optional Rx Key(可选的Rx密 钥)	Q/32	如果Key Management type=1(Q=32),则为 BTK,否则为 NSK或MS-MPPE Rx密钥
Optional Tx Key Length(可选的 Tx密钥长度)	2	如果Key management type=1,则为0,否则为Tx 密钥长度
Optional Tx Key(可选的Tx密 钥)	Key长 度	否则为MS-MPPE Tx密钥
Optional MN Credential TLV(可 选的MN证书TLV)	P	MN的缓存的证书
MIC	N	SECURE_CONTEXT的

[1205]

	WTLV-MIC
--	----------

[1206] 使用AP和MN认证者之间建立的CTK,从WTLV_SECURE_CONTEXTNonce字段到结尾(到达但是排除)的WTLV-MIC来加密WTLV_SECURE_CONTEXT应答响应。类似地,使用HMAC-MD5认证相同字段。

[1207] 由于MN认证者给活动AP提供MN会话超时时间,所以AP负责在会话超时时间到期前执行重认证。

[1208] 如果MN认证者在安全上下文传递所需的检验中的任何一个中失败,则响应将用全零填充BTK字段,并包括下列状态值之一:

[1209]

状态	值	描述
NO CONTEXT(无 上下文)	1	MN无缓存的证书(没有注册条目)
REPLAY (重放)	2	RN次序混乱
SSID	3	无效SSID
SESSION EXPIRED(会 话到期)	5	MN的会话已经到期
BAD MIC	6	MN的MIC与认证者的计算的MIC不匹配

[1210] 在MN注册期间转发MN的证书。如果正在转发证书,则不转发可选密钥,而是把一个具有MN缓存的证书的大部分的新TLV传播到MN的祖先基础结构节点,在SCM处结束。在独立模式中,SCM不转发证书,除非在SCM或LCM被初始化时(静态地)配置了预见性的漫游。使用WTLV_MN_SEC_CONTEXT转发MN的证书。

[1211] -WTLV_MN_SEC_CONTEXT.

[1212] 这个TLV只在MN注册应答期间使用,以便把其证书从MN认证者转发到MN的祖先,排除该AP(除非已经配置了预见性的漫游)。例如,如果 LCM是MN认证者,则LCM将把MN证书转

发到SCM。

[1213] 这个TLV如下定义：

[1214]

字段	长度 (字节)	描述
WTLV_MN_SEC_CONTEXT	2	TLV类型
TLV Length(TLV长度)	2	TLV长度
State(状态)	1	表示这个节点是否活动
STA Addr	8	WLCAP节点标识符;MN的MAC地址
Authentication Type (认证类型)	1	用于认证的EAP类型
Key Management Type(密钥管理类型)	1	协商的密钥管理(或无)类型。有效值为：0-无(不转发NSK) 1-CKM 2-802.1X遗留系统 3-SSN
Session Timeout(会话超时时间)	4	Radius访问认可提供的会话到期时间
KRK	16	用于认证MN对上下文传递的请求的密钥请求密钥
BTK	32	用于导出PTK的基本瞬时密钥
RN	8	用于跟踪已经从BTK导出多少 PTK的重定密钥号
SSID	L	MN的关联SSID TLV

[1215]

VLAN ID	2	MN'的关联VLAN分配
BSSID	6	定义当前关联的AP
Cipher(密码)	2	协商的密码,值为：0x0000-无 0x0001-WEP 0x0002-TKIP 0x0003-AES-OCB 0x0004-AES-CCMP 0x0005-CKIP 0xff<值>-供应商指定
NSK Length(NSK长度)	2	按字节计算的NSK长度(例如, Rx MS-MPPE密钥)
NSK	N	成功的802.1X EAP认证产生的 Rx密钥。
Tx Key Length(Tx 密钥长度)	2	Tx密钥长度(如果是被Radius 发送)
Tx Key(Tx密钥)	P	成功的802.1X EAP认证产生的 Tx密钥。

[1216] 这个TLV携带高度敏感的信息,因此必须使用MN认证者和目的IN之间共享的CTK加密。此外,嵌入MN安全证书TLV的安全上下文TLV必须被认证,例如,TLV MIC也必须被使用。MN安全证书TLV从State字段到Cipher字段被加密。

[1217] WTLV_UPDATE_RN:为PTK更新排序

[1218] 这个TLV只在AP和MN认证者之间有效,因为它用于更新MN和AP之间的密钥排序。由于AP能影响PTK重定密钥,所以在任何密钥刷新发生时必须通知SCM。从AP发送到MN认证者的更新请求如下：

[1219]

类型	长度	8字节	6字节	6字节	4字节	8字节
WTLV_KEY_UPDATE	TLV长	MSC	BSSID	MN MAC	RN	MIC _{AP}

[1220]

	度			地址		
--	---	--	--	----	--	--

[1221] 使用AP和MN认证者之间建立的CTK加密和认证WTLV_KEY_UPDATE消息。

[1222] 为了成功的更新和响应,MN认证者必须正确地解密和认证这个请求。即,如果消息不能被解密、认证,或RN大于当前RN,则MN认证者丢弃这个消息,并且不进行更新。但是响应必须提供表明它怎样失败的状态。该响应如下定义：

[1223]

类型	长度	8字节	6字节	6字节	4字节	8字节
WTLV_KEY_UPDATE	TLV 长度	MSC	BSSID	MN MAC 地址	RN	MIC _{AP}

[1224] 如果更新请求失败,则它将还包括来自下表的状态值：

[1225]

状态	值	描述
----	---	----

BAD MIC	1	计算的MIC和TLV的MIC不匹配
REPLAY	2	提供的RN次序混乱,并视作重放
INVALID BSSID(无效 BSSID)	3	指定的MN没有关联到给定的BSSID
NO MN(无 MN)	4	指定的MN没有注册。

[1226] -WTLV_NSK

[1227] 在成功的EAP认证之后,MN认证者可能需要请求关联的AP的NSK。对于只支持静态WEP密钥和/或不提供动态密钥的802.1X认证类型(如EAP-MD5)的传统的MN节点,对于协商的SSID/VLAN,MN认证者必须使用静态配置NSK的AP。为此,定义了新WTLV,以允许MN认证者请求关联的AP的NSK。

[1228] 请求TLV定义是:

[1229]

类型	长度	8字节		MIC
WTLV_NSK	TLV长度	MN-ID		WTLV-MIC

[1230] 应答TLV定义是:

[1231]

类型	长度	8字节	NSK	MIC
WTLV_NSK	TLV长度	MN-ID	WTLV_TRANSIENT_KEY	WTLV_MIC

[1232] 仅当使用预共享密钥和如EAP-MD5认证类型,并导致使用静态配置的密钥时需要这个TLV。虽然因不安全而非常不鼓励这种用法,但是仍给出了这个特征,以更好地支持遗留系统并实现移动路径。密钥获取将通过使用MN和AP之间的WLCCP_CONTEXT请求/应答交换来实现。

[1233] -WTLV_AUTHENTICATOR

[1234] 需要WTLV_AUTHENTICATOR来确保链路间CTK的存活性。这实际上是发起IN向其祖先认证的方法。虽然任一链路终点能够在预注册请求响应中请求它,期望跟在安全上下文(或WTLV_INIT_SESSION)请求和应答之后,一般在注册期间。TLV如下定义:

[1235]

字段	长度	描述
WTLV_AUTHENTICATOR(WTLV认证者)	2	
TLV Length(TLV 长度)	2	
DST-ID	8	目的地IN-ID,它必须证明它使用 和SRC-ID相同的CTK _{src dst} 来保护 (SRC-ID,DST-ID)链路。
SRC-ID	8	请求存活性证据的发起IN-ID
KSC	4	用作重放保护器的密钥序列计数器。这个值必须和安全上下文请求/重放交换期间使用的值匹配。

[1236]

保留	1	
Status(状态)	1	请求消息后忽略,但是在应答后 可以被设置。非零值表示链路不共享 相同的CTK或者检测到重放。
Nonce(现时标志)	16	用于证明存活性的随机质询。发起者必须提供16字节的随机值。
MIC	ML	认证这个TLV的WTLV_MIC

[1237] 发起MIC如下计算:

[1238] $MIC_{request} = HMAC-MD5(CTK_{src-dst}, SRC-ID || DST-ID || KSC || Noncesrc)$

[1239] 目的地必须增加所提供的Noncesrc,并如下计算其MIC:

[1240] $Noncedst = Noncesrc + 1$

- [1241] $MIC_{reply} = HMAC-MD5(CTK_{src-dst}, SRC-ID || DST-ID || KSC || Nonce_{dst})$
- [1242] 请求和应答WTLV_AUTHENTICATOR都必须如下加密TLV:
- [1243] $RC4'(MSC || CTK_{src-dst}, Status || Nonce)$
- [1244] 用它们的加密的值替代无格式文本字段(注意,RC4随机流的开头的256字节在与无格式文本异或前必须首先被删除。)
- [1245] -WTLV_RSNIE
- [1246] 在以下时刻,由MN协商的安全策略必须被传播到SCM:
- [1247] MN成功地协商了CKM,并且当前被关联到AP。
- [1248] MN从当前AP漫游到新AP,并且建立到新AP的重关联。
- [1249] 在重关联期间,RSNIE被包括在签名要素中,该要素被包括在重关联消息中。这样,RSNIE必须被传播到SCM进行验证。因为RSNIE的长度变化,所以其TLV如下定义:

[1250]

字段名	长度	描述
-----	----	----

[1251]

WTLV_RSNIE	2	TLV类型
TLV	2	TLV长度
RSNIE Element(RSNIE 要素)	N	如MN提供的RSNIE的内容

- [1252] -横向消息认证和保密
- [1253] “横向”的上下文请求或上下文应答被独立于SWAN拓扑树转发。发起者和响应者可以不在同一拓扑树分支上;因此,发起者和响应者可以不分享秘密CTK。进入和远离标志在横向上下文消息中被设置为OFF。
- [1254] 横向上下文消息的发起者和响应者共享的“横向L-CTK”(L-CTK)用于认证消息和加密包含在消息中的任何敏感的TLV。发起者和响应者共同的祖先用作产生L-CTKL-CTK的受信赖的第三方。共同的祖先使用它和发起者共享的路径CTK和它与响应者共享的路径CTK把L-CTKL-CTK安全地传送到每个节点。
- [1255] 共同祖先产生“票据”(ticket)和L-CTK。用共同祖先和发起者之间共享的路径CTK加密L-CTK。票据也包含L-CTK,并被用共同祖先和响应者之间共享的路径CTK加密。L-CTK和票据在WTLV_CTK_TICKET TLV中被传送到上下文传递发起者。
- [1256] 在发送到响应者的横向上下文请求中的WTLV_CTK_TICKET TLV中,发起者包括共同祖先的节点ID、票据和“认证者”。发起者使用L-CTK产生用于认证上下文请求的WTLV_MIC TLV。响应者用它和共同节点共享的路径CTK解密票据,并提取L-CTK。然后响应者可使用L-CTK来认证消息并解密任何加密的TLV。响应者也使用CTK来认证应答消息并加密包含在应答中的任何敏感的TLV。
- [1257] 根CM是所有SWAN节点的共同祖先;因此,根CM能够给任何两个节点建立L-CTK。发起者节点能够在上下文请求消息中发送WTLV_TICKET_REQUEST TLV到根CM,为第二响应者节点请求L-CTK和票据。根CM在上下文应答消息中的WTLV_CTK_TICKET TLV中返回票据和L-CTK。
- [1258] 如果MN从旧AP漫游到新AP,则在上下文请求消息中,它可能必须从旧AP向新AP横向转发上下文信息。最近共同祖先CM能自动地在发送到旧AP的解除注册请求消息中,为新AP传送L-CTK和“票据”。如上所述,旧AP能使用L-CTK来产生WTLV_MIC TLV,并加密发送到

新AP的上下文请求中的任何敏感的上下文信息。

[1259] 当MN漫游到新的本地控制域时,类似的机制能被用来从“旧LCM”向“新LCM”横向传送上下文。

[1260] -简单的WLCCP实现(W1)

[1261] 这个部分描述了简单的单个子网WLCCP实现,其中,每个子网的SCM在SCM独立模式中运行,并且WLCCP没有被用于更新层二转发路径。该简单实现包括下列组件:

[1262] 在独立单个子网基础结构中,SCM是“根CM”。

[1263] AP和MN初始认证

[1264] SCM选举和通告

[1265] AP路径认证

[1266] MN的子网内安全上下文传递(即MN预注册)。

[1267] MN快速重认证

[1268] 简单AP和MN注册。(WLCCP注册不建立层二转发路径)

[1269] WLCCP消息认证和保密。

[1270] SCM是MN和AP的802.1X认证者。在WLCCP消息中,EAPOL消息被在SCM和双亲AP之间中继。

[1271] 简单实现不支持层二更新、子网间越区交换或子网间上下文传递。网络拓扑不包括CCM或LCM。现有的Cisco DDP协议被用来建立和删除层二转发路径。DDP也被用于子网内越区交换(即当台站在单个子网内漫游时)。

[1272] 简单实现使用下列WLCCP消息类型:

[1273] -SCM-Advertisement(SCM通告)

[1274] -Registration(注册)

[1275] -Preregistration(预注册)

[1276] -AAA

[1277] -Path-Init

[1278] 在单个子网中,W1网络拓扑包括SCM和AP。它还包括与那些AP关联的任意MN。不支持层二路径更新;转发器AP的快速重认证也不支持;因此,对于W1实现,多跳AP到AP链路一般来说是透明的。

[1279] 在简单WLCCP实现中,活动SCM在子网独立模式中运行。

[1280] W1实现所需的数据结构和状态变量与一般SCM数据结构和状态变量相同。SCM是IN和MN 802.1X认证者;因此,它必须保持已认证的节点表。

[1281] 如在名为“活动SCM选择”的部分中所描述的,用非零的SCM优先权值配置的每个SCM候选者必须参与SCM选举协议。

[1282] SCM通告应答消息中的字段按名为“活动SCM选择”的部分中描述的设置,具有下列限制:

[1283] WTLV_ROOT_CM_INFO TLV包含SCM的IPv4地址。

[1284] W1-IN认证。

[1285] 每个AP必须和802.1X基础结构认证者相互认证,在简单WLCCP实现中,802.1X基础结构认证者是活动SCM。在SCM通告应答消息中的ROOT_CM_INFO TLV中,SCM通告其IP地址。

WLCCP IP封装的上下文请求和应答消息用于在“请求者”AP和802.1X认证者之间传输EAPOL认证消息。AP/SCM相互认证过程建立请求者AP和SCM所共享的网络会话密钥(NSK)。在AP已经成功地认证(以及只要它漫游)时,AP必须和SCM开始路径认证。在路径认证过程(下面描述)中使用NSK来建立AP-SCM上下文传递密钥(CTK)。

[1286] W1-SCM注册处理

[1287] 活动SCM必须保持注册表,该表具有其子网内的每个AP以及和那些AP关联的每个MN的入口。注册表被初始化为“空”。只要活动SCM放弃活动SCM状态,则它重置该表以清空。在简单WLCCP实现中,注册表仅被用于管理MN上下文信息。它不包含层二转发信息和路径状态信息。

[1288] 当SCM接收到有效的注册请求时,它为AP或MN产生对应的注册应答 时,并为AP或MN创建或者更新注册记录。

[1289] W1-(预)注册消息认证

[1290] 在简单WLCCP实现中,用通过AP路径认证建立的SCM/AP CTK认证预注册和注册消息。CTK用于产生并检验包含在所有(预)注册消息中的WTLV_MIC TLV中的消息完整性检验。SCM总是使用它和发起者共享的CTK来认证(预)注册请求消息。AP总是使用它和SCM(即响应者)共享的CTK来认证(预)注册应答消息。在简单WLCCP实现中,中间AP不处理或认证非根AP产生的(预)注册消息。在名为“WLCCP消息认证”的部分中详细地讨论了一般WLCCP消息认证。

[1291] 当SCM接收到使得消息完整性认证失败的“无效”(预)注册请求时,SCM返回具有“Bad MIC”状态的应答消息,而不进一步处理该消息。

[1292] W1-接收到的AP Path-Init请求

[1293] 如下面所描述的,AP必须认证其到SCM的路径,以建立并更新与SCM共享的上下文传递密钥(CTK)。当SCM接收到Response-Req标志被设置为ON的Path-Init请求时,它产生Path-Init应答。如果对于处于‘已认证’、‘预注册’或‘已注册’状态的请求者AP,SCM具有已认证的节点条目,则它返回具有‘良好’状态的Path-Init应答;否则,SCM返回具有“未认证”状态的Path-Init应答。

[1294] 在名为“基础结构路径认证”的部分中详细地描述了包括AP/SCM CTK产生和分配的路径认证。

[1295] W1-接收到的AP注册请求

[1296] 如下面所描述的,已经成功地完成了路径认证的AP必须向SCM注册。当SCM从Response-Req标志被设置为ON的AP接收到注册请求时,它为该AP产生注册应答。如果对于处于‘预注册’或‘已注册’状态的请求者AP,SCM具有已认证的节点条目,则它返回具有‘良好’状态的注册应答;否则,SCM返回具有“未认证”状态的注册应答。

[1297] 当SCM产生具有“良好”状态的注册应答时,它为发起者创建或更新AP注册记录。当产生了良好的应答时,注册记录的年龄被重置为‘0’。

[1298] W1-接收到的MN预注册请求。

[1299] 新双亲AP在孩子MN重关联时,向SCM发送Response-Req标志被设置为ON的预注册请求,以获取孩子MN的动态安全证书。SCM在它接收到预注册请求时为MN产生预注册应答。如果SCM对该MN具有已经认证的节点条目,则它返回具有“良好”状态的应答。在名为“MN安

全上下文传递”的部分中详细地讨论了用于传递MN的安全证书到新AP的协议。

[1300] W1-接收到的MN注册请求

[1301] SCM在它接收到来自MN的双亲AP的Response-Req标志被设置为ON的注册请求时，它为MN产生注册应答。如果SCM 1)对于请求者MN具有‘成功’状态的已认证节点条目，和2)对于发起者AP具有“绑定”的注册记录，则它返回具有‘良好’状态的注册应答。如果MN未认证，则SCM返回具有‘未认证’状态的注册应答。如果双亲AP没有绑定的注册记录，则SCM返回具有‘未注册双亲’状态的注册应答。

[1302] SCM按到达顺序接受注册请求。作为一种选择，每次为相应的MN产生‘良好’注册应答时，SCM应该为MN注册记录加时间戳。用当前时间减去对应的注册应答中的任何延迟值来计算时间戳。如果存在MN的现有的注册记录并且条目中的时间戳值大于当前时间减去注册请求中的任何延迟值，则SCM丢弃接收到的MN注册请求。

[1303] 在简单的WLCCP实现中，MN漫游到不同的双亲AP时，SCM不产生解除注册请求。

[1304] W1-AP运行。

[1305] 这部分定义了简单WLCCP实现所必需的AP状态变量、定时器和过程。AP过程一般被用AP“顶层”WLCCP状态转移的顺序来描述。在名为“AP运行模式”的部分中描述了顶层AP WLCCP状态和状态转移。

[1306] 简单AP实现要求下列AP过程：

[1307] AP必须处理SCM通告应答消息以发现活动SCM。

[1308] AP必须和802.1X认证者互相认证，并建立NSK。

[1309] 每个AP必须认证其到SCM的路径以建立CTK。

[1310] AP必须向SCM注册。

[1311] 注册的AP必须在次级端口上产生SCM通告应答消息。

[1312] 注册的AP必须预注册MN以获取MN的动态证书。

[1313] 注册的AP必须注册MN。

[1314] 跳路由标志被设置为OFF来发送预注册和注册消息；因此，中间AP不处理该消息。

[1315] W1-SCM通告消息处理

[1316] AP必须监控在本地VLAN上它的基本端口上接收到的SCM通告应答消息，以确定对于本地VLAN是否存在活动SCM。如果AP的本地VLAN存在活动SCM，则AP执行简单WLCCP协议。

[1317] 当AP向活动SCM注册时，MN 802.1X认证者在SCM中；否则，MN802.1X认证者在AP中。在W1实现中不使用路径代价和跳计数信息。SCM通告协议不用于确定AP基本端口。

[1318] W1-AP初始认证

[1319] 如在上面名为“W1-IN认证”的部分中所描述的，当AP初次发现活动SCM的新实例时，它必须和802.1X认证者相互认证。在简单WLCCP实现中，IN认证者总是活动SCM。

[1320] W1-AP路径认证

[1321] 在AP已经成功地认证之后，它必须开始向SCM的路径认证以建立由AP和SCM共享的秘密上下文传递密钥(CTK)。(AP必须通过更新注册请求/应答消息来周期性地更新其AP-SCM CTK。)

[1322] 简单W1实现中的AP路径认证如在上面名为“一般AP路径认证”的部分中所描述的，差别在于1)根CM总是SCM，和2)跳路由标志被设置为OFF。因为没有使能层二路径更新，所以

跳由标志被设置为OFF;因此,无需建立孩子AP和任何祖先AP之间共享的CTK。

[1323] W1-AP注册

[1324] 当AP最初发现SCM的新实例时,它必须和其子网的活动SCM注册,并周期性地刷新其在SCM中的注册记录。

[1325] 未连接的AP发送的初始注册请求中的字段按下面所描述的设置:(未指定字段被设置为‘0’。)

[1326] WLCCP头字段:

[1327] Type(类型)-‘3’

[1328] Originator(发起者)-未连接的AP的节点ID。

[1329] Responder(响应者)-SCM的节点ID。

[1330] Response-Peq Flag(响应请求标志)-‘1’来请求应答。

[1331] Inbound Flag(进入标志)-‘1’。

[1332] Hopwise-Routing Flag(跳路由标志)-‘0’。

[1333] 注册字段:

[1334] Requester(请求者)-未连接的AP的节点ID。

[1335] Hop Address(跳地址)-未连接的AP的选中的基本端口的802地址。

[1336] Relay Node ID(中继节点ID)-‘0’。

[1337] Initial Flag(初始标志)-‘1’。

[1338] AP(重)传输注册请求,直到AP接收到具有匹配消息ID的注册应答或者超过了最大重试。当AP接收到具有‘良好’注册状态的匹配注册应答时,AP被“注册”。

[1339] AP向SCM周期性地发送“更新”注册请求消息,以“刷新”其注册记录。更新注册记录使得Initial Flag(初始标志)被设置为OFF。

[1340] 直到AP已经与SCM成功地注册,它才能为MN产生代理预注册和注册消息。

[1341] 向活动SCM成功地注册的AP(即上面的“I,R”状态)必须在其每个次级端口上周期性地产生SCM通告应答消息。

[1342] 当AP已向活动SCM成功地认证时,最初启动SCM_Advertisement_Timer(SCM通告定时器)。每次它到期就重启动,直到AP转移到未注册状态(即当活动SCM改变或者丢失时)。SCM_Advertisement_Timer的周期总是被设置为AP的Parent_SCM_Record(双亲SCM记录)中的SCM_Advertisement_Period(SCM通告周期)值(按秒计算)。每次AP从活动SCM接收到SCM通告,就更新CM_Advertisement_Period。

[1343] 当SCM_Advertisement_Timer到期时,注册的AP进行下述操作:

[1344] 如果SCM_Age等于MAX_SCM_AGE,则禁止WLCCP。

[1345] 否则,如果SCM_Age小于增大SCM_Age,则用当前Advertisement_Period值重启动SCM_Advertisement_Timer;

[1346] 增大SCM_Age值;

[1347] 在每个次级端口上产生“活动”SCM通告应答消息。

[1348] 注册的AP产生具有下面示出的字段值的SCM通告应答消息。没有指定的字段设置为‘0’。

[1349] WLCCP头字段:

- [1350] Type(类型)-‘0x41’(SCM通告应答)
- [1351] Originator(发起者)-‘0’。
- [1352] Responder(响应者)-AP节点ID。
- [1353] Outbound Flag(远离标志)-‘1’。
- [1354] TLV Flag(TLV标志)-‘1’(请求必须包括IPV4_SUBNET TLV和IN_1X_ATHEN TLV)。
- [1355] SCM通告应答字段:
- [1356] Hop_Address(跳地址)-用于通过各个输出端口访问AP的802跳地址。(如果输出端口在混合模式中工作,则它是AP节点地址)。
- [1357] SCM标志:
- [1358] Active Flag(活动标志)-‘1’
- [1359] SCM Priority(SCM优先权)-从Parent_SCM_Record复制而来
- [1360] SCM Node ID(SCM节点ID)-从Parent_SCM_Record复制而来
- [1361] Instance Age(实例年龄)-从Parent_SCM_Record复制而来
- [1362] Path Cost(路径代价)-从Parent_SCM_Record复制而来
- [1363] Hop Count(跳计数)-从Parent_SCM_Record复制而来
- [1364] Advertisement Period(通告周期)-从Parent_SCM_Record复制而来
- [1365] WTLV_IPV4_SUBNET_ID TLV-IPv4地址和AP的前缀长度
- [1366] WTLV_ROOT_CM_INFO TLV-从IN_1X_Authenticator状态变量复制而来。
- [1367] W1-代理MN预注册。
- [1368] 在简单WLCCP实现中,MN预注册与一般代理MN预注册完全相同。
- [1369] W1-代理MN注册。
- [1370] 在AP已经成功地向活动SCM注册后(即它转移到上面的I,R状态),AP中的WLCCP MN注册被使能。在MN已经成功地认证或重认证后,双亲AP为MN产生初始代理注册请求。(注册请求可被用于完成认证握手;但是,MN在SCM产生“已认证”注册应答消息之前必须被完整地认证。)
- [1371] 在简单WLCCP实现中,WLCCP注册过程不用于建立或者删除层二转发路径;因此,L2_Path_Update标志和跳路由标志在注册消息中被设置为OFF。发起者总是双亲AP,并且响应者总是双亲SCM。对MN的注册请求必须包含MN的SSID和MN的缺省VLAN ID。
- [1372] SCM通过向发起者返回注册应答来确认注册请求。应答中的状态值表明注册请求是否被接受。
- [1373] 如果双亲AP没有接收到期望的注册应答,则它必须重传输重试(Retry)标志被设置为ON,并具有相同消息ID的注册请求,直到重试的次数等于REGISTRATION_RETRY_LIMIT。在重传输的注册请求中,延迟字段应该被设置为自MN上次传输上行链路帧之后逝去的时间。
- [1374] 注册应答寿命字段包含按分钟计算的注册寿命值。AP在注册寿命到期之前必须为MN产生更新注册请求。
- [1375] MN的初始代理注册请求中的字段如下面描述被设置。未指定的字段被设置为‘0’。
- [1376] WLCCP头字段:
- [1377] Type(类型)-‘3’

- [1378] Originator(发起者)-双亲AP的节点ID。
- [1379] Responder(响应者)-SCM的节点ID。
- [1380] Response-Req Flag(响应请求标志)-‘1’来请求应答。
- [1381] Inbound Flag(进入标志)-‘1’。
- [1382] Hopwise-Routing Flag(跳路由标志)-‘1’。
- [1383] TLV Flag(TLV标志)-‘1’(请求必须包括SSID_TLV)。
- [1384] 注册字段:
- [1385] Requester(请求者)-MN的802地址。
- [1386] Hop Address(跳地址)-双亲AP的基本端口的802地址。
- [1387] Relay Node ID(中继节点ID)-‘0’。
- [1388] Proxy Flag(代理标志)-‘1’。
- [1389] Initial Flag(初始标志)-‘1’。
- [1390] Authenticated Flag(已认证标志)-在请求中,已认证标志被设置为‘1’,以表明MN被双亲AP认证。
- [1391] Proxy MIP Flag(代理MIP标志)-如果MN使用代理MIP被使能的SSID,则被设置为‘1’。
- [1392] Delay(延迟)-自MN上次发送上行链路帧后达到数百秒的延迟。如果重试标志是‘0’,则延迟标志通常是‘0’。
- [1393] VLAN ID-分配给MN的VLAN ID。MN的VLAN ID通常是分配给MN的SSID的缺省的VLAN ID。如果MN被分配给“本地VLAN”,则分配的VLANID可以是‘0’。对MN的注册应答中的VLAN ID字段可包含不同的VLANID,以便把MN显式地分配给VLAN。
- [1394] SSID_TLV-对MN的注册请求必须包含MN的(重)关联请求中的 WTLV_SSID_TLV, WTLV_SSID_TLV包含MN的活动SSID。
- [1395] 如果MN和广播SSID关联,则广播SSID标志必须被设置为ON。对MN的注册应答可包括具有不同SSID的SSID_TLV,以便把MN显式地分配到服务组。
- [1396] AUTHENTICATION_TYPE_TLV(认证类型TLV)-包含用于认证MN的802.11认证类型(开放、共享密钥或EAP类型)。
- [1397] 为“重关联”的802.11台站产生的注册请求在WTLV_OLD_AP_BSSIDTLV中必须包含旧AP的BSSID。从台站发送的802.11重关联请求中的“旧AP”字段获取BSSID。
- [1398] 如果IP地址已知,则对MN的注册应答消息总是包含MN的IP地址。当双亲AP首次检测到MN的新的或不同的IP地址(即通过监听MN传输的IP/ARP分组),则它必须为MN产生“注册请求”。在该请求中,根CM标志被设置为ON,以产生对到根CM的完整路径的更新。
- [1399] -完整的WLCCP实现(W2)
- [1400] 这部分描述完整的WLCCP实现,它支持:
- [1401] -通过LCM和CCM的子网间上下文传递。
- [1402] -可靠的层二路径更新。
- [1403] -包括转发器AP、简单无线网桥(例如WGB)和以太网与802.11链路的任意组合的子网拓扑。
- [1404] 路径实例。

[1405] 上文指出,路径位于SWAN拓扑树的分支上。到校园网中的节点的完整路径包括该节点、CCM以及任何中间节点和链路。在一个时间点上,路径实例是完整的或部分的路径。每个CM为其域内的每个节点建立路径实例。例如,SCM为其子网域内的每个AP和MN建立“SCM路径实例”;CCM为校园网内的每个CM、AP和MN建立“CCM路径实例”。当未连接节点选择双亲节点并向SWAN基础结构注册时建立路径实例。

[1406] CM路径实例由相应的CM分配的路径ID标识。‘0’路径ID用于表示“无路径ID”。有效的路径ID从‘1’开始。当CM接收到对节点的“初始”注册请求消息时,它为该节点增大其路径ID。注册应答、“更新”注册请求、分离、解除注册、路径更新和路径检验消息总是包含有效的路径ID。

[1407] SCM路径实例在LCM路径实例的上下文内存在。LCM路径实例在CCM路径实例的上下文内存在。组合的CCM、LCM和SCM路径ID标识了校园网中的MN的完整路径实例。例如,在图1中,MN-2的完整路径实例由路径ID 15、10和6标识,它们分别由CCM、LCM和SCM建立。

[1408] 拓扑树的结构定义了“进入路径”。到节点的“远离路径”由到该节点的路径上的每个CM和AP中所保持的状态信息来定义。在本文档中,单个后代节点的路径状态信息包含在到该节点的远离路径上的每个CM和AP中的“后代路径记录”(Descendant Path Record,DPR)中。

[1409] 在拓扑树中不能存在断开的路径片断。“绑定”的路径实例由“远离”注册应答消息建立。在远离部分能够被建立之前,路径实例的进入部分必须存在。例如,在基础结构模式中,SCM不能给节点建立路径实例,除非该节点的LCM路径实例已经存在。如果MN漫游,则“旧路径”的大多数远离部分被首先删除(即通过进入注册应答或分离请求消息)。如过失失去了到孩子AP或CM的链路,则删除其根在AP或CM处的子树中的所有的路径实例。

[1410] -W2注册记录。

[1411] 每个CM或AP必须保持注册表,该表包含其子树中的每个后代节点(MN、AP或CM)的后代注册记录(DRR)。注册表可以可选择地包括不在各个AP或CM的子树中的节点的进入注册记录(Inbound Registration Records,IRR)。临时未绑定注册记录(Unbound Registration Record,URR)用于存储未注册节点的状态信息。注册记录由注册、解除注册和分离消息更新。如果注册记录在注册寿命内没有被更新,则它会老化并被丢弃。注册记录的基本密钥是各个节点的WLCCP节点ID。

[1412] 在W2实现中,AP或CM必须为每个后代WLCCP节点保持额外的转发和路径状态信息。在本文档中,“后代路径记录”包含给后代节点发送消息的任何必要信息,以及其他的路径状态信息。每个DRR指向一个DPR。“DRR/DPR”用于表示DRR和对应的DPR。

[1413] DPR可处于“绑定”或“未绑定”状态。当MN首次进入802.11“关联且认证”状态时,双亲AP为孩子802.11 MN创建未绑定DPR,并产生“初始”注册请求。初始注册请求在到CCM的路径上的每个AP和CM中也创建未绑定DPR。“未绑定”DPR包含对应的初始注册请求的消息ID。

[1414] 当接收到具有匹配消息ID和良好状态的“认证”注册应答时,DPR变成“绑定”的。“绑定”DPR包含非零的路径ID,该ID由注册应答中的双亲CM设置。SCM中的DPR包含SCM路径ID和LCM路径ID。SCM路径ID标识从SCM发起的远离路径;LCM路径ID(即LCM建立的路径ID)标识到LCM的进入路径。LCM中的DPR由于类似原因,包含LCM路径ID和CCM路径ID。

[1415] 如果路径上的每个DPR处于“绑定”状态,则路径是“绑定”的。到节点的路径可以既

是绑定的也是未绑定的。例如,如果初始注册应答消息丢失,则到MN的路径的大多数远离片断将是未绑定的(即直到恢复被开始)。未绑定DPR很快地老化并被丢弃;因此,没必要显式地删除“未绑定路径”。

[1416] 绑定DPR的最大年龄在WLCCP注册期间通过注册寿命字段建立。双亲AP和CM为孩子节点老化DPR。如果DPR在注册寿命内没有被“刷新”,则它被丢弃。孩子MN的DPR由上行链路数据或者管理帧刷新。孩子AP或CM的DPR由周期性更新注册请求刷新。如果孩子AP或CM的DPR被删除,则AP或CM被解除注册,并且整个根在孩子AP或CM的子树也被删除。

[1417] CCM对SWAN校园网内的每个活动CM、AP或MN都具有DRR/DPR。CCMDPR包含节点的双亲LCM的节点ID和IP地址。LCM对其本地控制域内(即在其被分配的子网中)的每个MN、AP和SCM都具有DRR/DPR。AP或MN的LCM DPR包含双亲SCM的节点ID和IP地址。SCM对其子网中的每个AP和MN具有DPR。如果双亲AP的节点ID存在,则SCM对它坐DPR处理,也对根AP的节点ID做DPR处理。

[1418] 在AP中,MN DPR包含指向端口记录的指针。上文指出,以太网端口、802.11 BSS和每个AP到AP链路被视作逻辑端口。在任意给定时间,每个活动逻辑AP端口或者作为“孩子”模式中的基本端口运行,或者作为“双亲”模式中的次级端口运行。端口记录包含“端口”状态和在各个逻辑端口上转发帧所必需的信息。端口记录包含802.11端口的802“跳地址”。非根AP通过在其基本端口上发送消息把该消息“向内”转发。

[1419] -W2子网拓扑

[1420] SWAN子网是以太网局域网。在本文档中,假设下层的IEEE 802.1D生成树协议(STP)或者其他STP被用于在每个AP子网中把有线以太局域网段组织成无循环生成树拓扑。WLCCP一般独立于下层STP;因此,WLCCP和其他STP兼容,如Cisco专有PVST+STP。

[1421] WLCCP SCM通告和注册协议用于在每个子网中建立可存在于任何下层(即802.1D)生成树之上的WLCCP生成树。WLCCP生成树可以用非STP链路把下层802.1D生成树扩展到非STP无线“转发器”AP或非STP 802.11网桥。AP(例如根AP、转发器AP或802.11网桥)是内部的节点,MN是WLCCP生成树中的叶子。

[1422] 在每个子网中,单个基本LAN位于WLCCP生成树的根。每个子网具有单个活动SCM。就定义来说,基本LAN是直接连接到SCM,可能是桥接的有线以太网段的集合。其他次级无线以太网LAN或者“次级LAN”通过无线802.11网桥链路连接到基本LAN。(基本或次级LAN可以包含不参与WLCCP的802.11网桥。这样的非WLCCP 802.11对于WLCCP是透明的。)

[1423] 子网控制域包括处于和相应的SCM相同的子网内的所有AP以及任何被直接或间接关联到那些AP的客户台站。例如,它包括任何与那些AP关联的MN,即使MN在网络层上通过VLAN中继或者MIP隧道被分配给不同的子网。它还包括连接到次级LAN的任何EN,次级LAN被桥接到基本LAN。

[1424] 图35中示出了用于单个子网的示范性WLAN生成树3500。802.1D STP链路和STP AP被标记为3502。用虚线示出了无线链路。

[1425] 基本和次级LAN可以包括多个以太网段和802.1D网桥和/或交换机。802.1D“根网桥”可以被包含在基本LAN或次级LAN中。对于WLCCP,基本或次级以太网LAN起到了逻辑、透明链路的作用。

[1426] WLCCP AP中的“基本端口”是用于访问基本LAN的端口。“根AP”在其以太网基本端

口上直接连接到基本LAN。“次级端口”是除了基本端口以外的任意逻辑或物理AP端口。基本或次级端口可以是以以太网或802.11端口。对于每个无线的AP到AP链路,存在逻辑802.11端口。逻辑次级BSS端口提供对本地BSS中的802.11台站的访问。AP 3508具有802.11基本端口和以太网次级端口。

[1427] 注意,在STP AP中,当且仅当802.1D根网桥被包含在基本LAN中时,802.1D根端口将和基本端口相同。

[1428] 单个“WLCCP指定AP”负责把帧桥接到次级LAN。次级以太网段的WLCCP指定AP可以与同一以太网段的802.1D指定的网桥不同。例如,在图35中,AP 3508是“次级LAN”的“WLCCP指定AP”。如果802.1D根网桥被包含在基本LAN中,则AP 3508也是次级LAN中它的以太网段的802.1D指定的网桥。WLCCP指定AP必须向SCM注册其连接的次级LAN,以在无线链路上为次级LAN建立转发和泛滥参数。

[1429] 在以太网LAN中,“逆向学习”在802.1D网桥或交换机中建立到有线台站和MN的转发路径。VLAN标签和逆向学习在以太网VLAN中建立转发路径。逆向学习是不可靠的;因此,如果目的地址的位置未知,则单播帧必须由透明网桥、交换机或AP“泛滥”。

[1430] 单播帧从不被泛滥到802.11 BSS,因为802.11台站可靠地与双亲AP关联。单播泛滥被选择性对以太网LAN使能。WLCCP“注册协议”用于可靠地建立从基本LAN到802.11台站的转发路径,并选择次级LAN。因此,从不需要把单播帧“向外”(即从基本LAN)泛滥到802.11台站和选择次级LAN。在AP基本端口上总是使能单播泛滥。缺省时,如果目的地未知,则单播帧被“向内”朝基本LAN转发。

[1431] WLCCP注册协议也被用于把多播组成员资格信息转发到基本LAN。作为一种选择,多播帧仅在用于访问由各个多播目的地址标识的成员的次级端口上被转发。(802.11台站之间的多播通信能被可选择地禁止,以进一步限制多播泛滥。)

[1432] “次级LAN”是与每个AP相关的。例如在图35中,标为“次级 LAN3510”的有线LAN从AP 3512和AP 3514的角度仅仅是个次级LAN。在单个AP中,为了帧转发的目的,“基本LAN”可被视作WLAN生成树被通过AP的基本端口访问的那部分。例如,AP 3516仅通过在其基本端口上中继一个帧来把该帧转发到基本LAN去(例如到达标为“次级LAN”的以太网LAN)。到基本LAN的无线链路对AP 3516一般是透明的。

[1433] 802.1D STP应该在用于桥接有线STP LAN的无线链路上被操作。在图35中,例如,如果次级LAN包含802.1D网桥/交换机,则802.1D STP应该在AP 3512、3514和3508之间的链路上被操作。AP 3518在非STP链路上连接到STP AP 3520。

[1434] WLAN生成树可包括到非STP无线转发器AP和“工作组网桥”(WGB)的非STP无线链路。和802.11 MN很类似,非STP转发器AP和WGB连接到WLAN生成树。

[1435] 缺省时,AP在“正常访问”基本端口上连接到网络。AP能够可选择地在VLAN主干基本端口上被连接到网络,以便单个802.11 BSS能够包括来自多个VLAN的MN。

[1436] 对于每个AP端口,用户可配置的“WLCCP端口模式”变量被设置为下列值之一:

[1437] a)孩子模式。在AP以太网端口上,孩子模式是缺省的。

[1438] b)双亲模式

[1439] c)双亲/孩子模式。双亲/孩子模式在802.11端口上是缺省的。

[1440] 被配置为“孩子模式”的AP端口只能作为WLCCP基本端口工作。配置为“双亲模式”

的AP端口只能作为WLCCP次级端口工作。802.11“双亲”端口产生信标并接受台站关联。802.11“孩子”端口和802.11“双亲”端口关联。

[1441] 被配置为“双亲/孩子模式”的802.11端口既能作为“双亲”端口也能作为“孩子”端口(即作为转发器端口)工作。被配置为“双亲/孩子模式”的以太网端口在孩子802.11网桥中能作为次级“双亲”端口工作,或在有线AP或网桥中作为基本“孩子”端口工作。双亲/孩子模式被用于辅助自配置子网拓扑。

[1442] 被配置为孩子模式或双亲/孩子模式的“未连接”AP中的一个端口(或数个端口)不断地扫描潜在的双亲AP或SCM。AP自动地选择提供到基本LAN的“最佳”(即最小代价)路径的“基本端口”和双亲节点。AP“次级端口”是基本端口以外的任意端口。

[1443] 用户能够为孩子802.11端口配置“双亲AP列表”,以限制潜在的双亲AP。注意,通过配置具有单个条目的“双亲AP列表”,用户能够显式地配置AP到AP的链路。

[1444] 连接的AP中的双亲/孩子端口如下运行:a)如果它是基本端口,则它在“孩子”模式中运行。b)如果它是次级端口,则它在“双亲”模式中运行。c)连接的转发器AP中的物理无线端口既在双亲模式也在孩子模式中运行,其中,该单个端口既提供逻辑上行链路基本端口,也提供一个或多个逻辑下行链路端口。

[1445] “根AP”总是在孩子模式中操作其基本以太网端口,在“双亲模式”中操作其次级无线端口。缺省时,不具有以太网链路的AP作为“转发器”运行,因为缺省的802.11端口模式是“双亲/孩子”。

[1446] “孩子802.11网桥”总是在“孩子”或“双亲/孩子”模式中操作其基本无线端口,在“双亲模式”中操作其次级以太网端口。注意,如果AP的以太网端口被显式地配置为“双亲”或“双亲/孩子”模式,则它只能作为孩子802.11网桥工作。

[1447] 加电后,连接的AP开始“扫描”SCM通告信息,以发现SCM并确定到基本LAN的最佳路径。然后AP选择提供最佳路径的双亲节点和基本端口,并向SCM注册。

[1448] 在配置为孩子或双亲/孩子模式的AP端口上接收到的探测响应消息和802.11信标以及SCM通告消息中包含路径代价信息。AP只接受具有“匹配”子网ID的SCM通告,并且只接受具有匹配子网ID和匹配WLCCP SSID的SCM通告。

[1449] 如果AP在其以太网端口上接收到优选SCM标志被设置为ON和零跳计数的SCM通告消息,则它马上确定它是“根AP”。根AP的双亲SWAN节点是本地SCM。根AP马上选择以太网端口作为其“基本端口”并向SCM注册。在它已经成功地注册之后,它在其每个次级端口上产生SCM通告。

[1450] 缺省时,非根AP(即没有直接连接到基本LAN的AP)选择提供到基本LAN的“最佳”路径的基本端口和双亲AP,其中,最佳路径是具有可接受信号质量的最小代价路径。非根AP通过它选择的“双亲AP”在其选择的基本端口上向SWAN基础结构注册。

[1451] 随着优选SCM标志被设置为OFF,AP可以在其以太网端口上接收SCM通告消息。在那种情况下,经过随机的间隔,AP应该在每个使能“孩子模式”的端口上扫描更高优先权的SCM。如果AP没有发现更高优先权的SCM,则它作为根AP运行。因为1)优选SCM故障,或2)有线网络拓扑被分段时,AP可以从备份的SCM接收SCM通告。对于后一种情况,为了拓扑收敛,需要扫描更高优先权的SCM。

[1452] SWAN AP能够可选择地执行802.1D生成树协议(STP)。后面讨论具有STP AP的SWAN

操作。

[1453] 孩子802.11网桥是次级以太网LAN的WLCCP指定的网桥。孩子802.11网桥负责把次级LAN和连接的次级以太网节点连接到基本LAN。在指定网桥上,到次级LAN到单播泛滥和多播泛滥被局部地使能或者禁止。单播和多播泛滥要求被向内传播到基本LAN。

[1454] 非STP孩子802.11网桥用网桥优先权配置。如下面名为“WLCCP指定网桥选择”的部分中描述那样,如果多于一个孩子网桥被连接到次级LAN,则网桥优先权用于选举WLCCP指定的网桥。

[1455] 用户配置的以太网地址列表能够在AP以太网端口上被配置。以太网地址列表包含静态802地址的列表,其中,每个地址标识一个通过以太网端口被访问的台站。(列表能够通过标准的802.1D配置选项被配置,选项支持创建“静态”数据库条目。)孩子802.11网桥把列表中的地址以及其他动态获知的地址连接到基本LAN。

[1456] 工作组网桥(WGB)是具有下列配置设置的孩子802.11网桥的特例:

[1457] 1)以太网端口被配置为“双亲”模式。

[1458] 2)802.11端口被配置为“孩子”模式。

[1459] 3)在以太网端口上禁止单播泛滥。

[1460] 4)WGB不执行STP。(WGB可以提供对作为移动网络(例如车辆中作为更大的移动网络的一部分的LAN)的一部分的次级LAN的访问。因为频繁的拓扑变化,所以不可能在移动网桥中执行标准的802.1D STP。)

[1461] WGB在其注册请求记录中必须包括WLCCP_SEC_LAN_ADDR_LIST TLV。该TLV包含802地址的列表,其中,每个地址标识一个连接到WGB的次级以太网端口的以太网LAN上的以太网台站。

[1462] WLCCP指定网桥选举协议使得两个或更多的冗余WGB能被连接到工作组次级LAN。

[1463] 注意,WGB上的以太网端口被配置为“双亲”模式;因此,即使WGB能提供更低代价的路径,它也不能在其以太网端口上连接到SWAN网络。

[1464] 如果1)节点漫游到新双亲AP或CM,2)节点被网络管理者禁止或3)节点从物理上变得和网络断开,则到该节点的“旧路径”必须被删除。对于前面两种情况,CM产生“解除注册请求”以删除旧路径。对第三种情况,双亲节点产生“分离请求”以删除旧路径。

[1465] 构造WLCCP注册/解除注册/分离协议,以防止“断开路径片段”。具有“良好”状态码的注册应答在它被从共同CM向外朝着请求者节点转发时为“请求者节点”建立路径实例。在反方向上路径实例被删除。在解除注册应答或分离请求消息被向内转发时删除路径实例。

[1466] -解除注册请求

[1467] 1)当为已经漫游的节点建立了新路径实例时,或者2)网络管理者“禁止”节点时,CM“解除注册”任何旧路径实例。随着Response-Req标志被设置为ON,CM在旧路径上向外发送解除注册请求消息来请求解除注册应答消息。解除注册应答被向内转发(如果使能层二路径更新则使用跳路由),直到它到达发起者。当接收到进入的解除注册应答时,旧路径实例在每个节点中被删除;因此,旧路径实例的最远离部分首先被删除。

[1468] 作为“最近共同祖先”的CM在节点漫游时负责可靠地解除注册节点的旧路径实例。最近共同祖先CM被称为“共同CM”。

[1469] 共同CM只为后代节点进行绑定的路径实例(即具有绑定的DPR的路径实例)解除注

册。解除注册请求和对应的应答包含旧的绑定路径实例的路径ID。共同CM在解除注册请求/应答消息中总是“发起者”。

[1470] CCM通过发送解除注册请求到“旧”LCM为节点解除注册旧路径实例,旧LCM作为“响应者”。LCM通过发送解除注册请求到旧SCM解除注册旧路径实例,SCM作为响应者。SCM通过发送解除注册请求到“旧”双亲AP解除注册到MN或孩子AP的路径,旧双亲AP作为响应者。

[1471] 共同CM重传输解除注册请求,直到它接收到具有匹配消息ID的解除注册应答。共同CM必须保持“旧”路径实例的解除注册状态信息,直到它接收到匹配应答或超过了最大解除注册重试。旧路径上的其他后代AP或CM不需要保持解除注册状态信息。

[1472] 如果可能,解除注册请求总是被转发到目标节点的直接双亲。直接双亲在它接收到解除注册请求时必须产生解除注册应答。

[1473] 如果中间CM接收到解除注册请求,则它必须首先确定它是否具有用于由目标节点ID和路径ID标识的路径实例的DPR。如果它不具有这样的DPR,则它必须返回解除注册应答。否则,它必须把请求向外朝着直接双亲转发。转发请求前,LCM必须首先把响应者改为旧SCM;SCM必须首先把响应者改为旧双亲AP。在转发解除注册请求或者应答消息到孩子或双亲CM前,中间CM必须更新路径ID字段,以标识远离或进入路径实例。

[1474] 中间AP必须把解除注册请求转发到直接双亲AP(即响应者)的远离路径上的下一跳AP,如果这样的下一跳AP存在。否则,如果这样的下一跳AP不存在,则中间AP必须产生带有错误状态的解除注册应答。注意,在MN在其子树中的孩子AP之间漫游时,AP将既在旧路径上也在新路径上。

[1475] 在旧路径实例被解除注册前,“旧双亲节点”有可能变得不连接。在这种情况下,当CM不能成功地删除旧路径实例时,旧双亲节点(AP或CM)将被解除注册,并且整个根在旧双亲节点的子树将被删除。

[1476] 如果AP或CM接收到对节点的具有匹配节点ID和匹配或“较新”路径ID的解除注册应答,则它必须为节点删除“绑定DPR”。如果AP接收到具有“较新”路径ID的注册应答,则它也必须删除节点的DPR。对应的DRR可被删除,或者作为一种选择被转换为IRR。

[1477] DPR包含上次接收到的对各个路径实例的注册请求的消息ID。如果共同CM接收到顺序混乱的初始注册请求,则它将产生包含注册消息ID的解除注册请求。如果AP或CM接收到具有匹配注册消息ID的解除注册请求,则它必须删除“未绑定”DPR。它决不能删除“绑定”DPR。

[1478] 未绑定DPR(即那些没有转移到绑定状态)被很快地老化并被丢弃;因此,无须显式地删除未绑定路径片段。

[1479] 如果MN的注册请求消息顺序混乱地到达CM,则会存在用于快速漫游的MN的不正确的瞬时路径实例。在这种情况下,CM将用解除注册请求删除到MN的正确路径。MN的双亲AP在接收到解除注册请求时必须解除关联该MN。因此,当MN重关联时,正确的路径实例将很快被建立。

[1480] 一分离请求。

[1481] 当到孩子的链路“断开”时,“双亲”节点产生分离请求以删除“孩子”的路径实例。因下列原因产生分离请求:1)当孩子802.11台站被“解除关联”时,双亲AP为该台站产生分离请求,2)如果双亲节点(AP或CM)不再能够和孩子节点通信,则它为孩子节点(MN、AP或CM)

产生分离请求,或3)如果双亲节点丢弃孩子节点的DPR(即因为在DPR被刷新前,注册寿命到期),则它为孩子节点产生分离请求。(理论上,AP或CM也能产生分离请求来把它自己从网络中断开。)

[1482] 分离请求的发起者是断开的孩子节点的双亲节点。响应者总是双亲节点的双亲CM。请求者是断开的孩子节点。

[1483] 分离请求被(重)传输,直到发起者接收到匹配的分离应答。分离请求用于在到CCM的路径上的每个AP和CM中把注册状态变为“未绑定”。分离请求包含路径实例的路径ID。如果AP或SCM接收到对MN的分离请求,且如果DPR中的路径ID不比分离请求中的路径ID“更新”,则它把DPR状态设置为“未绑定”。当台站被解除关联时,在双亲AP中DPR状态被马上设置为“未绑定”。

[1484] 当为分离请求被向内转发时,路径ID和响应者字段必须被更新,与针对进入解除注册应答的完全一样。

[1485] 子树删除

[1486] 如果“连接”的AP从SWAN拓扑树断开,则该AP和根在AP处的子树中的每个节点都必须可靠地转移到“未连接”状态。

[1487] 有两种普遍的情况:

[1488] 1)双亲AP或SCM可以“断开”孩子节点。

[1489] 2)“连接”的孩子节点可以独立地转移到“未连接”状态。

[1490] 第一种情况:如果a)孩子节点的DPR老化并被丢弃,b)双亲不再能和孩子通信,或c)接收到对孩子节点的管理性解除注册请求,则双亲AP或CM异步地断开孩子节点。如果双亲节点删除孩子AP,则孩子AP和根在AP处的整个子树必须可靠地转移到未连接状态。

[1491] 如果DPR老化并被丢弃,则保证孩子AP已经转移到未连接状态,并且不需要进一步的行动。

[1492] 仅通过改变孩子的802.11状态为解除关联,并可选择地把解除关联(或解除认证)消息传输到台站,双亲AP就能够断开其BSS中的802.11孩子。最坏情况下,孩子节点在试图发送上行链路帧时将发现它是未关联的。

[1493] 如果双亲SCM或AP断开连接到以太网次级端口的孩子AP,则它必须在以太网次级端口上传输的SCM通告应答消息中的WTLV_DELETED_NODE_LIST TLV内通告孩子AP的节点ID和路径ID。断开的AP的节点ID必须被持续通告某个阈值周期,或者直到AP重新注册。当a)孩子节点错过了在某个小阈值周期内所有来自其双亲的SCM通告消息,或b)当它在删除的节点列表中发现其节点ID时,保证孩子节点将转移到未连接状态。

[1494] 第二种情况:如果a)孩子节点失去到其双亲的链路;b)它检测到其双亲节点已变成未连接的;c)它检测到新双亲“实例”;或d)在通告消息中,其节点ID和当前的路径ID在删除的节点列表中,则“连接”的孩子节点变成“未连接”的。

[1495] 如在名为“拓扑状态信息”的部分中所描述的,每个SWAN CM必须保持一个内部“实例年龄”。实例年龄被输入通告应答消息中的实例年龄字段。节点的例年龄被初始化为‘0’,并且每次节点转移到未连接状态时,节点的实例年龄就被重置为‘0’。

[1496] AP必须保持内部的“连接计数”变量,该变量被初始化为‘0’,并且每次AP最初向SCM注册时就增大。连接计数被复制到SCM通告消息的连接计数字段,该消息在AP的次级端

口上传输。

[1497] 孩子节点必须保存其双亲CM的实例年龄。非根AP必须也保存其双亲AP的连接计数。如果连接的节点从其双亲节点接收到具有更低的实例年龄(例如,因为双亲节点已重新启动)的通告应答消息,则它转移到未连接状态。如果非根AP接收到具有不同的连接计数的通告应答,则它也转移到未连接状态。注意,通过发送具有更低的实例年龄值的SCM通告消息,SCM能直接或间接地删除其整个子树。

[1498] 孩子AP必须也保持一个包含其双亲AP的当前连接计数的变量。如果孩子AP从其双亲AP接收到具有不同连接计数(例如因为双亲AP漫游了)的通告应答,则它必须转移到未连接状态。

[1499] 当SCM转移到未连接状态时,它必须a)传输未连接标志设置为ON以及带有无限路径代价和跳计数的多播计划外SCM通告应答消息,和2)删除所有DPR。

[1500] 当连接的AP转移到未连接状态时,它必须a)在每个以太网次级端口上传输未连接标志设置为ON以及带有“无限”路径代价和跳计数的多播计划外SCM通告应答消息,和b)解除关联所有的孩子802.11台站,c)删除所有DPR,d)停止在802.11端口上发出信标,和e)开始对新双亲SCM或AP的扫描。AP通过把802.11状态改变到“未认证和未关联”来“解除关联”802.11台站;它不需要向每个孩子台站发送802.11解除关联请求。

[1501] 在AP向新双亲AP注册之前,AP必须在未连接状态停留一个控制(hold-down)周期(即5秒),以确保所有孩子802.11台站已经解除关联,并防止顺序混乱的注册请求。

[1502] W2-SCM子树删除。

[1503] 如果“连接”的SCM变得从其双亲LCM不连接,则它转移到子网独立模式。当SCM从本地基础结构模式转移到子网独立模式时,不删除根在SCM的子树;因此,SCM不能重置其实例年龄。

[1504] 当SCM转移到本地基础结构模式时,必须删除根在SCM的在独立模式中运行的子树。因此,独立SCM在最初向新双亲LCM注册后必须重置其实例年龄。

[1505] 如果“连接”的LCM变得与CCM不连接,则它转移到本地独立模式。当SCM从校园基础结构模式转移到本地独立模式时,不删除根在LCM的子树;因此,LCM不能重置其实例年龄。

[1506] 当LCM转移到校园基础结构模式时,必须删除根在LCM的在独立模式中运行的子树。因此,独立LCM在最初向CCM注册后必须重置其实例年龄。

[1507] W2-LCM路径认证。

[1508] 在校园基础结构模式中,在未连接的LCM最初认证之后,它必须向CCM发送Path-Init请求以开始路径认证。在名为“基础结构路径认证”的部分中详细地描述了路径认证。

[1509] W2-LCM注册。

[1510] 在LCM已经成功地完成了路径认证后,SCM向CCM发送“初始”注册请求。CCM返回初始注册应答消息。LCM必须产生周期性“更新”注册请求消息,以刷新它在CCM中的注册绑定。CCM返回更新注册应答消息来确认注册请求。

[1511] W2-SCM操作。

[1512] -双亲LCM分配。

[1513] 在启动时以及任何SCM到分配的LCM的链路丢失的时候,它必须向CCM发送具有“请求”WTLV_PARENT_CM TLV的上下文请求消息。当CCM接收到上下文请求时,它从注册LCM的集

合中确定SCM的双亲LCM。(用户在CCM中必须配置LCM/子网绑定。用户能为每个子网配置基本和低效运行的LCM以得到冗余度。缺省时,和CCM共存的LCM能起到故障LCM的低效备份的作用。如果SCM的子网被分配给LCM,则CCM把SCM分配给活动LCM。)CCM返回带有非空WTLV_PARENT_CM TLV的上下文应答,以把SCM显式地分配给双亲LCM。否则,CCM返回空WTLV_PARENT_CM TLV,以便指示SCM在子网独立模式中运行。非空TLV包含分配的双亲LCM的节点ID和IP地址。然后SCM必须向其分配的双亲LCM进行路径认证并注册。

[1514] 如果SCM不能和双亲LCM通信并且它不能和其分配的CCM通信,则它必须在独立模式中运行。但是,SCM必须周期性地尝试重新建立和CCM的通信。

[1515] CCM将返回空WTLV_PARENT_CM TLV(即节点ID为‘0’),以指示SCM在独立模式中运行。

[1516] 如果SCM变成未连接的,则它必须重复确定其(即新的)双亲LCM的过程。如果a)连接的SCM失去到其双亲LCM的链路,b)它不能向其双亲LCM成功地注册,c)它检测到CCM或其双亲LCM的新实例,或d)它接收到有效的管理性解除注册请求,则它变成未连接的。如果连接的SCM变得从其双亲LCM未连接,则它必须向CCM发送包含非空“请求”和WTLV_PARENT_CM TLV的上下文请求。“请求”TLV包含“旧双亲LCM”的IP地址和节点ID。如果SCM失去其到双亲LCM的链路,则它在上下文请求中也必须包括WTLV_LOST_LINK TLV。和以前一样,CCM在上下文应答中包含空的或非空WTLV_PARENT_CM TLV,以便分别指示SCM在独立模式中运行,或者把SCM分配给双亲LCM。

[1517] W2-AP操作。

[1518] W2-AP状态变量。

[1519] 在名为“一般AP状态变量”的部分中描述了用于W2实现的AP状态变量,但有一个例外。AP必须保持具有包括转发和路径状态信息的记录的注册表,如在名为“W2注册记录”的部分中描述的那样。

[1520] W2-AP路径认证。

[1521] 在AP已经成功地认证后,它必须开始路径认证,以便和其每个祖先建立秘密上下文传递密钥(CTK)。在W2实现中,AP路径认证与在上面名为“一般AP路径认证”的部分中的描述相同。

[1522] W2-AP注册。

[1523] 未连接的AP在其每个配置成孩子或双亲/孩子模式的端口上扫描潜在的双亲SCM或AP。(注意,如果连接的AP发现其双亲AP或SCM的新的实例,则它变成未连接的。)未连接的AP或CM必须在其选择的端口上向其选择的双亲节点发送初始注册请求,以请求连接到网络。在初始注册请求和相应的应答中,发起者是未连接的AP;请求者也是未连接的AP;而响应者是选择的双亲节点(即双亲AP或SCM)。

[1524] 未连接的AP发送的初始注册请求中的字段按如下描述设置:(未指定字段被设置为‘0’。)

[1525] WLCCP头字段:

[1526] Type(类型)-‘3’

[1527] Originator(发起者)-未连接AP的节点ID。

[1528] Responder(响应者)-选择的双亲节点(双亲AP或双亲SCM)的节点ID。

- [1529] Response-Req Flag(响应请求标志)-‘1’用于请求应答。
- [1530] Inbound Flag(进入标志)-‘1’。
- [1531] Hopwise-Routing Flag(跳路由标志)-‘1’。
- [1532] TLV Flag(TLV标志)-‘1’(请求必须包括WTLV_AP_PORT_LISTTLV)。
- [1533] 注册字段:
- [1534] Requester(请求者)-未连接的AP的节点ID。
- [1535] Hop Address(跳地址)-未连接的AP选中的基本端口的802地址。
- [1536] Relay Node ID(中继节点ID)-在发起者或响应者产生的注册消息中为‘0’。否则,是转发该消息的中间“中继”节点的节点ID。
- [1537] Initial Flag(初始标志)-‘1’。
- [1538] VLAN ID-未连接的AP和双亲节点本地VLAN ID。VLAN ID值可以是‘0’。如果VLAN ID值与双亲节点的本地VLAN ID不同则是错误的。
- [1539] 双亲节点必须把初始注册请求从未连接的AP向内转发,直到它到达根CM。双亲节点在向内转发请求之前,在发起者字段输入其节点ID,并且在响应者字段输入其双亲CM的节点ID。中间的LCM在它把请求向内转发到CCM之前,必须用CCM节点ID更新响应者字段。CCM向双亲节点(即发起者)返回注册应答。双亲节点在把应答转发到未连接的AP或CM之前用请求者节点ID更新响应者字段。
- [1540] 连接的AP或CM能向其双亲CM直接发送“更新”注册请求,以刷新其路径实例,它自己既做发起者节点也做请求者节点,而双亲CM作为响应者。在向内转发请求之前,双亲CM必须用其双亲CM的节点ID更新响应者字段。
- [1541] AP(重)传输注册请求,直到它接收到具有匹配消息ID的注册应答,或者直到超过了最大重试。当AP接收到具有“良好”注册状态的匹配注册应答时,它被“注册”。注册应答包含由SCM设置的路径ID,该ID标识了从AP到SCM的“路径实例”。
- [1542] AP周期性地发送“更新”注册请求消息到SCM,用于“刷新”它在到SCM的路径上的每个节点中的移动绑定。更新注册请求使得初始标志被设置为OFF并且它包含有效的路径ID。
- [1543] 来自AP的注册请求必须包括包含了AP端口描述符的列表的WTLV_AP_PORT_LIST TLV。每个端口描述符包括端口类型、端口模式(双亲、孩子或双亲/孩子)和物理通信接口的802端口地址。
- [1544] 来自AP的注册请求必须包括IP地址TLV。
- [1545] 来自用代理MIP SSID配置的AP的注册请求必须包括包含代理MIPSSID和MIP HA绑定列表的WTLV_PMIP_SSID_LIST TLV。
- [1546] W2-代理MN注册
- [1547] 这部分描述了当WLCCP注册用于建立MN和基本LAN之间的层二转发路径时的双亲AP的MN注册。
- [1548] 双亲AP中的“代理WLCCP MN”为不知道WLCCP的MN提供代理WLCCP注册服务。每个MN为其双亲AP的本地VLAN向SCM注册,即使该MN属于不同的VLAN。
- [1549] 在MN已经成功地认证或重认证后,双亲AP为MN产生“初始已认证”注册请求消息。对MN的注册请求必须包含MN的SSID和MN的缺省子网。
- [1550] 如果双亲AP没有接收到期待的注册应答,则它必须重传输注册请求,并使得延迟

字段被设置为自从MN上次传输上行链路帧以来逝去的时间。如果双亲AP在REGISTRATION_RETRY_LIMIT重传输之后没有接收到期望的注册应答,则它必须解除关联MN。

[1551] 在对MN的初始代理注册请求中的字段按如下描述设置。未指定的字段被设置为‘0’。

[1552] WLCCP头字段:

[1553] Type(类型)-‘3’

[1554] Originator(发起者)-双亲AP的节点ID。

[1555] Responder(响应者)-SCM的节点ID。

[1556] Response-Req Flag(响应请求标志)-‘1’用于请求应答。

[1557] Inbound Flag(进入标志)-‘1’。

[1558] Hopwise-Routing Flag(跳路由标志)-‘1’。

[1559] TLV Flag(TLV标志)-‘1’(请求必须包括SSID_TLV)。

[1560] 注册字段:

[1561] Requester(请求者)-MN的802地址。

[1562] Hop Address(跳地址)-双亲AP的基本端口的802地址。

[1563] Relay Node ID(中继节点ID)-在发起者或响应者产生的注册消息中为‘0’。否则,是转发该消息的中间“中继”节点的节点ID。

[1564] Proxy Flag(代理标志)-‘1’。

[1565] Initial Flag(初始标志)-‘1’。

[1566] Authenticated Flag(已认证标志)-认证标志在请求中被设置为‘1’以表示MN被双亲AP认证了。

[1567] Proxy MIP Flag(代理MIP标志)-如果MN正使用代理MIP被使能的SSID,则被设置为‘1’。

[1568] Delay(延迟)-自从MN最后发送上行链路帧后达到数百秒的延迟。如果重试标志是‘0’,则延迟标志通常是‘0’。

[1569] VLAN ID-分配给MN的VLAN ID。MN的VLAN ID通常是分配给MN的 SSID的缺省的VLAN ID。如果MN被分配给“本地VLAN”,则分配的VLANID可以是‘0’。对MN的注册应答中的VLAN ID字段可包含不同的VLANID,以便把MN显式地分配到VLAN。

[1570] SSID_TLV-对MN的注册请求必须包含包含在MN的(重)关联请求中的WTLV_SSID TLV,WTLV_SSID TLV包含MN的活动SSID。

[1571] 如果MN和广播SSID关联,则广播SSID标志必须被设置为0N。对MN的注册应答可包括具有不同SSID的SSID TLV,以便把MN显式地分配到服务组。

[1572] AUTHENTICATION_TYPE TLV-包含用于认证MN的802.11认证类型(开放、共享密钥或EAP类型)。

[1573] 为“重关联”的802.11台站产生的注册请求必须在WTLV_OLD_AP_BSSID TLV中包含旧AP的BSSID。从台站发送的802.11重关联请求中的“旧AP”字段获取BSSID。

[1574] 对MN的注册请求总是被转发到“最近共同祖先”CM。如果SCM接收到来自MN的双亲AP的注册请求,并且下列条件之一为真,则SCM必须把MN的初始注册请求转发至其双亲LCM:

[1575] SCM不具有用于MN的绑定DPR。

[1576] 接收到的注册请求中的任何BSSID不是用于该MN的SCM的DPR中的“双亲AP”上的端口的地址。

[1577] 当SCM接收到来自其双亲LCM的具有“良好”状态的匹配注册应答时,它创建或更新用于MN的“绑定”DPR。当SCM接收到来自其双亲CM的注册应答时,它产生注册应答,以便在它的子网内建立新的路径实例。

[1578] 如果LCM不具有用于MN的绑定DPR,则它必须为MN把接收到的初始注册请求向内转发到CCM。

[1579] 如果MN的IP地址已知,则MN的注册应答消息总是包含MN的IP地址。当双亲AP首次检测到MN的新的或不同的IP地址时(即通过监听MN发送的IP/ARP分组),它必须为MN产生“注册请求”。在请求中,根CM标志被设置为ON,以导致对到根CM的完整路径的更新。

[1580] 在MN已经成功地认证后,双亲AP为MN产生路径更新消息。路径更新消息总是在MN的VLAN上传输,以更新网桥和交换机中的转发表。如果“旧双亲AP”的802地址已知,并且旧双亲AP和MN在同一VLAN上,则路径更新消息被发送到该地址;否则,路径更新被发送到MN在VLAN上的802广播地址。

[1581] 如果双亲AP在一个MAX_MN_INACTIVITY周期内没有从MN接收到上行链路帧,则它必须解除关联孩子MN。当孩子台站(MN或AP)被解除关联时,双亲AP必须向SCM发送WLCCP分离请求。下面更详细地讨论分离请求逻辑。

[1582] MN一被认证,就可以把数据帧转发到MN或从MN转发。但是,直到“绑定”路径实例为目的地址存在,才在AP到AP链路上不向外转发单播数据帧。直到建立了MIP隧道,数据帧才从“本地子网”转发到“外部子网”上的代理MIP MN去。

[1583] -802.11网桥注册

[1584] “双亲802.11网桥”像任何其他AP那样注册,如同在名为“AP注册”的部分中所描述的那样。

[1585] “孩子802.11网桥”是用于次级以太网LAN的WLCCP指定网桥。指定网桥必须注册它自己,如同任何其他AP一样,并且它必须也注册其连接的次级LAN,以及次级LAN上的以太网节点。WLCCP指定的网桥在其注册请求消息中,必须把次级LAN标志设置为ON。

[1586] 在指定网桥的次级以太网端口上局部地使能或禁止到次级LAN的单播泛滥。如果单播泛滥被使能,则WLCCP指定网桥在其WLCCP注册请求消息中,必须把单播泛滥标志设置为ON,以便把单播泛滥要求传播到基本LAN。如果在端口上接收到注册请求,单播泛滥在逻辑AP次级端口上被动态使能,单播泛滥标志设为ON。总的来说,如果在AP的任何次级端口上动态或静态地使能了单播泛滥,则AP必须把其注册请求消息中的单播泛滥标志设置为ON。因此,如果根在端口的子树包含单播泛滥被使能的次级以太网LAN,则在任何AP次级端口上使能单播泛滥。如果在最大AP注册寿命期内没有接收到单播泛滥标志被设置为ON的注册请求,则在次级AP端口上被动态使能的单播泛滥被禁止。

[1587] 如果在次级LAN上单播泛滥被禁止,则WLCCP指定网桥在其注册请求记录中必须包括WTLV_SEC_LAN_ADDR_LIST TLV,以便把次级LAN上的以太网节点连接到基本LAN。该TLV包含次级LAN上的台站的VLAN-ID/802地址对的列表。地址可被静态地配置或通过逆向学习动态“获知”。

[1588] 在AP以太网端口上,可以配置用户配置的以太网地址列表。以太网地址列表包含

静态802地址的列表,其中,每个地址标识通过以太网端口被访问的台站。(列表能够通过标准的802.1D配置选项被配置,选项支持创建“静态”数据库条目。)如上面所描述的那样,孩子802.11网桥把列表中的地址以及其他动态获知的地址连接到基本LAN。

[1589] -WLCCP指定网桥选举。

[1590] 这部分描述可选的WLCCP指定网桥选举协议,该协议用于为非STP次级LAM选举WLCCP指定网桥。例如,该协议可被用于为非STP工作组网桥加强自动冗余度。

[1591] 用从0(缺省)到7的网桥优先权值来配置非STP孩子802.11网桥。网桥ID是各个孩子802.11网桥的连接起来的网桥优先权和WLCCP节点ID。如果网桥ID字典顺序较高,则它具有相对较高的网桥优先权。具有最高优先权网桥ID的孩子网桥起到其连接的次级LAN的WLCCP指定网桥的作用。

[1592] 非STP孩子网桥在其次级以太网端口上传输周期性的SCM通告消息,该消息包含其网桥ID。如果孩子802.11网桥在端口上接收到具有较高优先权网桥ID的SCM通告应答消息,则它必须阻塞其次级以太网端口。如果孩子802.11网桥在它开始传输SCM通告后的WLCCP_BRG_ELECT_HOLDDOWN秒内,在其以太网端口上没有接收到具有较高优先权网桥ID的SCM通告应答消息,则它变成其连接的次级LAN的活动WLCCP指定网桥。

[1593] -802多播地址注册。

[1594] 如果多播泛滥在AP的任何次级端口上被使能,则AP必须在其注册请求消息中把多播泛滥标志设置为ON。如果在端口上接收到多播泛滥标志被设置为ON的注册请求,则在逻辑AP次级端口上动态地使能多播泛滥。因此,如果多播泛滥在根在端口的子树中的任何其他AP或次级LAN上被使能,则它在次级端口上被使能。

[1595] AP在注册请求中必须包括可能为空的WTLV_MCAST_ADDR_LIST TLV,其中,多播泛滥标志被设置为OFF。TLV包含在AP的次级端口上被使能的802多播地址的总计列表。被使能的802多播地址的总计列表包括任何用户配置的被使能多播地址和被MN注册的多播地址的列表。

[1596] 如果多播地址被包含在注册请求中的WTLV_MCAST_ADDR_LIST TLV内或者802.11(重)关联消息或802.11动作帧中的MULTICAST_802_ADDRESS_LIST要素内,则它在AP次级端口上被动态地使能。如果动态使能的多播地址在最大AP注册寿命期后没有被注册,则它老化并被丢弃。

[1597] 缺省时,在所有AP次级端口上使能802多播泛滥。在指定网桥的次级以太网端口上局部地使能或禁止到次级LAN的802多播泛滥。

[1598] -IP多播地址注册。

[1599] “IGMP监听”通常用于自动地导出在端口上哪个IP多播地址是“活动”的。(即在端口上应该转发哪个IP多播地址)。IGMP监听可被全局使能,或者它能在每个AP(即次级)端口上被使能。如果IGMP监听被使能,则在次级端口上只转发具有“活动”多播IP地址的IP多播分组。

[1600] 如果在AP次级端口上IGMP监听被禁止,则在AP的注册请求消息中,IP多播泛滥标志必须被设置为ON,以便把所有多播IP分组泛滥到次级端口。如果在端口上接收到IP多播泛滥标志设置为ON的注册请求,则在逻辑AP次级端口上动态地使能IP多播泛滥。因此,如果IP多播泛滥在任何其他AP或根在端口的次级子树中的次级LAN上被使能,则它在次级端口

上被使能。

[1601] 缺省时,IGMP报告仅仅被向内转发到基本LAN,以便把IP多播成员资格信息传播到进入路径上的每个AP。如果要求可靠的IP多播注册,则AP可以在注册请求中包括WTLV_IP_MCAST_ADDR_LIST TLV,其中,IP多播泛滥标志被设置为OFF。TLV包含AP的次级端口上活动的IP多播地址的总计列表。

[1602] (如果IGMP报告仅仅被向内转发到基本LAN,则对于IP多播过滤不要求WLCCP支持)。

[1603] -可靠的路径更新机制。

[1604] 这部分描述可选WLCCP“可靠的路径更新”,它用于从丢失的路径更新消息中恢复。

[1605] 当MN关联时,新AP为中间网桥和交换机中的MN发送单个路径更新请求消息,以更新逆向学习的转发路径。如果失去路径更新消息,则用于MN的转发路径在中间网桥/交换机中将不被正确地更新。

[1606] 可靠的路径更新机制要求任何AP以太网基本端口必须存在于专用以太网链路上。例如,两个根AP不能被插入相同的以太网集线器。由于这个限制,“旧AP”不应该在其基本端口上为不在其子树中的MN接收帧。

[1607] 该机制如下实现:

[1608] AP必须为不在其子树中的MN保持MN-IRR。

[1609] 在孩子MN解除注册后,如果没有接收到MN的路径更新消息,则把MN-IRR放入“路径更新未决”状态某个阈值周期(例如一分钟)。如果阈值周期到期,接收到路径更新,或者路径检验应答表明MN已经离开了子网,则未决状态结束。(注意,可能在解除注册消息之前接收到路径更新消息。)

[1610] 如果a)旧双亲AP具有MN的处于路径更新未决状态的MN-IRR和b)它在其基本端口上接收到目的地为该MN的数据帧,则它为该MN产生路径检验请求消息。路径检验请求被发送到旧AP的双亲SCM。

[1611] 当双亲SCM接收到路径检验请求时,它产生路径检验应答消息。如果SCM具有较新的到MN的远离路径,则它向新双亲AP发送路径检验应答;否则,它向旧双亲AP发送路径检验应答,以表明MN不再在子网内注册。

[1612] 在新双亲AP确定MN仍旧被关联后,它向旧双亲AP发送路径更新请求消息。

[1613] -MN扩展服务组

[1614] 802.11服务组ID(SSID)标识了扩展服务组(ESS),它可被视作802.11 台站的“无线接入域”。校园网可以包含多个重叠的ESS。ESS可以生成多个子网。可以用多个SSID配置AP,以便提供对多个ESS的访问。

[1615] 为每个AP SSID配置了下列访问参数:

[1616] 认证标准(例如所需的认证算法)

[1617] 代理MIP标志(使能或禁止)。

[1618] VLAN ID(可选)。*

[1619] 如果使能代理MIP,则可以为SSID配置可选的“本地代理地址和子网掩码”。*

[1620] *为每个AP SSID至多可以配置一个VLAN ID或本地代理地址;但是,可以用同样的VLAN ID或本地代理地址配置多个AP SSID。

[1621] 用于单个ESS的VLAN和代理MIP访问参数能在每个AP中不同地配置。例如,在一个AP中,可以用VLAN ID配置SSID“F00”,而在另一个AP中可以用本地代理地址配置SSID“F00”。

[1622] 可以用“虚拟本地代理地址”配置SSID,以便代理MIP MN能被分配给MIP“虚拟本地子网”。(在简单“无缝漫游”装置中,所有代理MIPMN能够通过集中配置的代理MIP SSID被分配给单个虚拟本地子网。)

[1623] 应该在整个ESS中为SSID始终如一地配置认证参数。

[1624] 在任意给定时间,每个MN和单个ESS关联。MN的物理漫游域限于那些为MN用SSID配置的AP。“代理MIP和VLAN集成”部分包括示范ESS漫游情况。

[1625] -对VLAN中继的WLCCP支持。

[1626] 如果在AP中使能802.1Q VLAN中继,则AP必须把其子树中的每个节点分配给VLAN ID。在子网的WLCCP生成树中的所有AP和SCM位于和SCM相同的“本地”VLAN上。MN和以太网台站(即在次级LAN上)可以位于不同的VLAN上。

[1627] 子网中的所有AP属于相同的“本地VLAN”,但有一个例外。在“客户模式”中运行的WGB可以属于非本地VLAN。连接到该WGB的所有以太网台站属于和该WGB相同的VLAN。(WGB在“客户模式”中作为客户台站关联。在客户模式中,WGB在802.11 VLAN中继链路上不能连接到其双亲AP。)

[1628] 双亲AP把孩子MN分配给VLAN ID。缺省时,MN被隐式地关联到VLAN或者为MN的SSID显式地配置。双亲AP在对MN的注册请求中必须包括MN的VLAN ID。当双亲AP接收到注册应答消息时,如果注册应答消息包含不同的VLAN ID,或者注册应答消息包含WTLV_HOME_SUBNET TLV,则双亲AP可以把MN重分配到不同的VLAN ID。

[1629] 如果AAA服务器分配VLAN ID,则注册应答消息将会包含不同的VLANID。在下面的部分中描述第二种情况。

[1630] AP必须为每个被使能的VLAN“计数”在其子网内的MN的数量。如果在根在端口的子树中存在一个或更多属于该VLAN的注册台站,则VLAN在AP次级VLAN中继端口上是“活动”的。每个次级VLAN中继端口上的出口多播VLAN过滤器用于丢弃对非活动VLAN的多播传输。

[1631] 代理MIP用于给不直接支持移动IP的IP MN提供“代理”移动IP服务。

[1632] (当前,代理MIP不给非IP应用提供无缝子网间移动。通过给标准MIP增加后向兼容扩展,代理MIP能被扩展成给任何基于以太网的应用提供无缝移动性。这样的MIP扩展要求最少的WLCCP变化,并且不影响WLCCP拓扑。)

[1633] -代理MIP注册和解除注册。

[1634] 每个子网的SCM为代理MIP MN保持移动IP注册状态。“外部SCM”初次并且此后周期性地访问外部子网时候,它触发对MN的代理MIP注册请求,以为MN保持FA/HA移动绑定。(SCM不能触发MIP注册,直到为SCM中的MN建立完整的本地子网绑定(即HA地址和MN IP地址)。)当“本地SCM”从外部子网初次漫游回到其本地子网时,它触发对MN的代理MIP解除注册请求。

[1635] 必须把MIP注册请求帧和各个MN的源以太网地址一起传输到MIPFA,以便FA能发现MN的以太网地址。因此,双亲AP必须传输代理MIP 注册请求,以避免在任何中间透明网桥或交换机中的不正确的“逆向学习”。当双亲AP从SCM接收到指示时,它产生MIP注册请求。

[1636] “代理MIP MN”是要求代理MIP服务的MN。必须用代理MIP被使能的SSID配置代理MIP MN。MN的SSID包含在802.11(重)关联请求消息中;因此,MN的双亲AP能够马上确定该MN是否要求代理MIP服务。如果对于MN的SSID,代理MIP被使能,则在对MN的注册请求中,双亲AP必须把代理MIP标志设置为ON。在注册应答中,SCM包括WTLV_MIP4_REG_REQ TLV,以触发双亲AP传输MIP注册(或解除注册)请求。

[1637] SCM不在用于外部子网上的代理MIP MN的MIP转发路径上。MN的IP分组在MIP HA和FA之间的MIP隧道上,在本地子网和外部子网之间转发。FA把IP帧向外转发到MN的单播802地址。在MN的双亲AP中的代理MIP实体把IP帧从MN向内转发到FA的单播802地址(即反向隧道贯穿),或者转发到缺省路由器的单播802地址(即三角路由)。

[1638] -SSID/Home-Agent Database(SSID/本地代理数据库)。

[1639] SSID/HA数据库包含每个SSID可访问的MIP HA的列表,该SSID在SWAN网络中的AP上被配置成代理MIP被使能。SSID/HA数据库中的条目被AP自动地填充,如下面描述的那样。根据MN的源IP地址,MN不被动地绑定到本地子网,除非:1)它被授权使用其SSID(即通过RADIUS)和b)本地子网的MIP HA在MN的SSID的可访问HA的列表中。

[1640] 配置在AP上的每个SSID被隐式地或显式地绑定到缺省VLAN或MIPv4-HA/子网掩码对。如果代理MIP SSID被绑定到缺省VLAN,则AP必须通过监控在VLAN上传输的HA通告,尝试为VLAN自动发现HA。AP也必须尝试为VLAN发现子网掩码。AP能通过在VLAN上广播ICMP子网掩码请求消息或通过监控Cisco CDP消息中的子网信息,为每个VLAN发现子网掩码。

[1641] 用代理MIP SSID配置的AP必须在其注册请求消息中包括WTLV_PMIP_SSID_LIST容器TLV。该容器TLV包含WTLV_SSID TLV的列表,其中,每个SSID TLV后跟着0或者更多WTLV_MIPV4_AGENT TLV。每个MIPV4_AGENT TLV包含各个SSID可访问的HA的IP地址、子网掩码和容量。如果HA的子网掩码字段未知,则被设置为‘0’。CM合并来自其域内的所有AP的代理MIP SSID和HA的列表,并把代理MIP SSID和关联的HA的结果列表转发到CCM。CCM使用该信息自动地填充SSID/HA数据库和下面描述的“本地代理数据库”。

[1642] -本地代理数据库

[1643] CCM保持包含MIPv4-HA/子网掩码对的列表的本地代理数据库。列表中的条目被静态配置,和/或由AP自动地填充。当CCM接收到代理MIP标志设置为ON,并具有WTLV_HOME_SUBNET TLV的注册请求时,它使用该数据库为代理MIP MN确定MIP HA。HOME_SUBNET TLV包含代理MIP MN的IP地址,该MN是通过“监听”MN发送的分组中的源IP地址发现的。CCM通过把MN的子网地址和HA的子网地址进行对比,为MN确定HA。如果不知道某些子网掩码,则可以使用“最长匹配前缀”搜索算法。如前面所描述的那样,MN必须被授权访问HA的本地子网。

[1644] -代理MIP/VLAN集成

[1645] 在基本VLAN中继端口上连接到网络的AP具有到多个代理MIP“本地子网”的层二“VLAN链路”。如果双亲AP具有到代理MIP MN的本地子网的VLAN链路,则代理MIP MN被分配给对应的VLAN ID;否则,代理MIP MN被分配给本地VLAN,即使本地VLAN不是本地子网。

[1646] 每个AP必须保持具有用于在AP上使能的每个VLAN ID的条目的“VLAN表”。如果一个或更多代理MIP SSID被绑定到VLAN,则VLAN被标记为“代理MIP使能”。用于代理MIP使能VLAN的每个VLAN表入口必须包含一个或更多MIPv4 HA的子网掩码和地址。

[1647] SWAN基础结构将在对MN的注册应答消息中的WTLV_HOME_SUBNET TLV中返回代理

MIP MN的任何现有本地子网绑定。如果注册应答消息中的HA地址和VLAN表中的任何HA地址匹配。如果注册应答中的HA地址与VLAN 表中的任何HA地址匹配,则MN是“在本地的”。在这种情况下,MN被分配给包含在匹配条目中的VLAN ID。当代理MIP MN初次漫游到SCM的域中时,产生MIP“解除注册”消息,并且MN通过VLAN中继绑定到其本地子网。

[1648] -本地子网绑定

[1649] 代理MIP MN的“本地子网绑定”包括MN的MIP HA地址、子网掩码和IP地址。如上所述,MN的HA绑定可被静态配置或动态地导出。CCM为每个活动代理MIP MN保持本地子网绑定的“主拷贝”。在SCM中的代理MIP客户条目能够为MN产生MIP注册请求之前,代理MIP客户条目必须为代理MIP MN确定本地子网绑定。

[1650] 用下列(从最低到最高)区分优先次序的规则,把代理MIP MN分配给本地子网:

[1651] 1)MN被分配给为双亲AP中的它的SSID配置的缺省VLAN或本地子网地址。

[1652] 2)如果AP发现了代理MIP MN的IP地址,则把MN分配给和其IP地址对应的本地子网。

[1653] 3)MN被分配给静态配置的本地子网和MIP HA。

[1654] 具有现有MIP本地子网绑定的代理MIP MN总是被绑定到其当前的本地子网-即使MN和具有匹配SSID的AP关联,该SSID被用VLAN ID或用于不同子网的本地代理地址配置(见名为“代理MIP和VLAN集成”的部分)。如果MN连接到外部子网上的AP(即未连接到LAN链路上或VLAN中继链路上的本地子网的AP),则代理MIP用于访问本地子网。

[1655] WTLV_HOME_SUBNET TLV用于为代理MIP MN建立本地子网绑定。TLV包含下列字段:
a)MIPv4 HA,b)子网掩码,和c)MN IP地址。如果这些值未知,则子网掩码和MN IP地址地段可以是零。直到MN的IP地址被发现,MN才能绑定到本地子网。

[1656] MN本地子网分配如下进行。(注意,对MN的注册请求总是在 WTLV_SSID TLV中包含MN的SSID。)

[1657] 当代理MIP MN漫游到双亲AP时,该AP在对MN的初始注册请求消息中必须包括WTLV_HOME_SUBNET TLV。HOME_SUBNET TLV必须包含“缺省MIP HA”地址和MN的IP地址,如果此IP地址已知。缺省MIP HA是a)为代理MIP MN的SSID配置的HA,或b)绑定到为代理MIP MN的SSID配置的VLAN的HA。缺省MIP HA地址用于为不具有现有本地子网绑定的MN动态地建立本地子网。初始注册请求被转发到最近共同祖先CM——“共同CM”。

[1658] 共同CM在对应的注册应答消息中的WTLV_HOME_SUBNET TLV中,把代理MIP MN的任何现有本地子网绑定转发到MN的双亲AP。远离应答消息在到MN的路径上的每个CM和AP中建立绑定。现有绑定覆盖由双亲AP建立的绑定。注意,“现有绑定”可以已经被静态地配置或者动态地建立(即由旧双亲AP)。

[1659] 如果代理MIP MN没有本地子网绑定,则CCM是“共同CM”。在这种情况下,在代理MIP MN的注册请求中的WTLV_HOME_SUBNET TLV内的HAIP地址用于为MN确定MIP HA。在CCM产生的注册应答中的WTLV_HOME_SUBNET TLV内返回本地子网绑定。*

[1660] 双亲AP可以发现MN正在使用不属于其当前本地子网的IP地址。在这种情况下,双亲AP必须马上产生包含WTLV_HOME_SUBNET TLV内的IP地址的更新注册请求,以便把MN动态地分配给和其IP地址对应的本地子网。

[1661] CCM使用SSID/HA数据库来确认MN被允许访问和其IP地址对应的本地子网。如果本

地子网分配被授权,则本地子网绑定被包含在CCM产生的相应的注册应答中的WTLV_HOME_SUBNET TLV内。

[1662] *直到MN的IP地址和本地代理地址都是已知的时候SCM才能触发MIP注册。如果MN的IP地址未知,则当MN的双亲AP发现MN的IP地址时,它必须马上产生另一个注册请求。在已知代理MN的IP地址之前,可以把该MN分配给本地VLAN。

[1663] 注意,双亲AP始终把代理MIP MN分配给对MN的注册消息中包含的 WTLV_IPV4_HOME_SUBNET TLV中的本地子网。如果注册应答消息中的HA地址和AP的VLAN表中的HA地址匹配,则代理MIP MN“在本地”。在这种情况下,MN被分配给匹配表入口中的对应的VLAN ID。如果双亲AP接收到带有WTLV_MIP4_REG_REQ TLV的注册应答并且MN“在本地”,则它为MN产生MIP解除注册请求消息。

[1664] 如果MN变成非活动的,则MN的动态分配的本地子网绑定被老化和丢弃。因此,代理MIP MN的本地子网在某个非活动周期之后可以改变(即到达更优化的子网)。

[1665] 通过用绑定到虚拟本地子网的代理MIP SSID配置AP,可以把MN绑定到“虚拟本地子网”。

[1666] (“用于DHCP的Ipv4子网选择选项”,RFC 3011[6],被用于为外部子网上的DHCP MN保持IP地址。)

[1667] -代理MIP单播转发

[1668] 缺省时,“三角路由”用于为外部子网上的代理MIP节点转发分组。在本地子网上传输的目的地为外部子网上的MN的分组被HA封装,并被隧道贯穿到MN。被外部子网上的MN传输的分组被发送到外部子网上的IP网关的MAC地址。该网关使用普通的IP路由把分组传送到目标IP地址。

[1669] 作为一种选择,“MIP反向隧道贯穿”能被对每个MIP SSID使能。如果为代理MIP MN的SSID使能了反向隧道贯穿,则被外部子网上的MN传输的分组被封装,并被向内转发到MN的HA,如RFC 3024所规定的那样。

[1670] (由于多个原因,对于单播IP分组,需要反向隧道贯穿。用于“私有子网”的DHCP服务器可以把不可路由的“私有IP地址”分配给和该子网关联的代理MIP MH。私有子网的路由器一般包含网络地址翻译器(Network Address Translator,NAT)。通过把台站接收和发送的分组中的台站的私有地址翻译成可路由的“公共地址”,NAT用私有地址使一个台站能访问其他公共网络。端口地址翻译(Port Address Translation)(PNAT)用于把很多私有地址多路复用到单个NAT公共地址。如果具有私有本地地址的代理MIP MN漫游到外部子网,则MN传输的 分组必须在反向MIP隧道上被转发到其本地子网,以使能任何必要的NAT翻译。如果相同校园网中的多个私有子网共享相同的IP地址空间,则私有IP地址可能不是一个明确的“本地IP地址”。

[1671] 校园网可以包含被“防火墙”逻辑保护的“安全子网”。被外部子网上的MN传输的分组可能不会被允许通过在外子网和本地子网之间存在的防火墙。)

[1672] -代理MIP多播转发

[1673] 根据RFC 2002,外部子网上的标准移动IP MN必须产生IGMP成员资格报告消息,以参与IP多播组。成员资格报告既可以被中继到外部子网上,也可以被转发到MN的MIP HA。

[1674] AP使用“IGMP侦听”为MN导出IP组成员资格信息。AP关联时,它向MN发送IGMP一般

查询,来请求IGMP报告。

[1675] 双亲AP可被配置成为外部子网上的代理MIP MN以处理IGMP成员资格报告和IP多播分组,其方式为下列之一:

[1676] AP可通过本地FA把成员资格报告转发到MN的HA。MIP HA负责封装和转发在MN的本地子网上传输的多播分组到外部子网上的MN,如在RFC2002中定义的那样。如果HA把IP多播分组隧道贯穿到MN,则双亲AP中的代理MIP实体负责把“内部封装头”从多播分组中去除,该分组被HA转发到外部子网上的代理MIP MN。然后,双亲AP可把结果多播IP分组发送到MN的单播802地址。(双亲AP不能把多播IP分组发送到多播802地址,因为在不同的广播域中,它将被MN不正确地接收。)被外部子网上的代理MIP MN传输的多播分组通过MIP“反向隧道”被转发到MN的本地子网,如RFC 3024中所定义的那样。

[1677] AP能把成员资格报告中继到本地“外部”LAN上。然后,多播路由器负责把多播分组转发到MN的外部子网。AP必须(即选择性地)把多播分组转发到MN。被外部子网上的代理MIP MN传输的多播分组被中继到本地外部子网上。多播路由器负责把多播分组转发到本地子网。*

[1678] *第二种选项要求路由器支持IGMP和多播路由。因为它更有效率,所以是优选的。

[1679] -代理MIP广播域。

[1680] 当前,802.11广播域和VLAN对应。代理MIP节点应该被分隔成和本地子网对应的广播域。802.11广播域应该被一般化,以使得公共无线接口既能用于VLAN,也能用于代理MIP广播域。如果代理MIP MN不在接收广播消息,则单个代理MIP广播域可被用于对共享相同802.11广播加密套件的外部子网上的所有代理MN进行分组。按照要求,IP多播分组必须被复制,并被传输到代理MIP广播域。注意,不必把标准MIN MN分隔成这样的广播域。

[1681] -IP地址注册

[1682] 一发现每个MN、AP和CM接口的IP地址,就把它可选择地向CCM注册。在注册应答消息中,IP/802地址对被分发给到节点的路径上的每个AP和CM。IP/802地址绑定用于辅助自动ARP过滤。(见下文)。

[1683] -上下文记录。

[1684] 每个WLCCP CM为其域内的每个节点缓存上下文和配置信息。在本文档中,“上下文记录”包含当台站从旧AP漫游到新AP时所传递的上下文和配置信息。在每个AP或CM中的“上下文管理器”管理上下文记录。在WLCCP注册和上下文消息中,上下文记录被作为不透明目标传递。(当前,上下文记录只包含RADIUS配置信息。)

[1685] -横向上下文传递。

[1686] 当MN漫游时,上下文消息可被用于把MN的动态上下文从“旧”分支上的节点“横向”转发到“新”分支上的节点(例如从旧SCM到新SCM)。最近共同祖先CM通过在注册应答和解除注册请求消息中分别转发MN的旧绑定和新绑定,自动地辅助横向上下文传递。例如,在注册应答消息中,SCM能把“旧AP”的地址转发到“新AP”。如在名为“WLCCP消息 认证”的部分中所描述的那样,最近共同祖先CM起到横向消息认证的被信赖的第三方的作用。

[1687] 在上下文请求或应答消息中均可以横向传递上下文信息。例如,在请求消息中,旧AP能把上下文信息异步地转发到新AP。第二个例子是,新SCM能向旧SCM发送上下文请求来“请求”上下文信息。旧SCM在相应的上下文应答消息中返回请求上下文信息。

[1688] -动态ARP过滤

[1689] 根在“根AP”的子树中的每个节点的IP地址被向SWAN基础结构注册。每次MN漫游时,MN的IP地址被传递到新双亲AP。如果“ARP翻译”被使能,则AP必须过滤在802.11次级端口上传输的广播ARP请求。如果目标IP地址不属于其子树中的节点,则ARP请求被丢弃;否则,如果目标IP地址属于子树中的节点,则广播目的MAC地址被翻译成节点的单播MAC地址。然后结果单播帧被作为任何其他单播帧来转发。

[1690] -RADIUS记帐

[1691] LCM中的RADIUS记帐客户为每个MN保持单个RADIUS记帐会话。双亲AP在WLCCP上下文请求消息中包含的WLVTV_ACCOUNTING TLV中把记帐统计周期性地向内转发。WLCCP注册协议用于在MN漫游时传递记帐会话。当MN漫游或变得断开时,在解除注册应答和分离请求消息中,把任何“驻留”记帐统计向内转发。如果MN漫游到“新”本地控制域,则或者a)在新LCM必须启动新的记帐会话,或b)记帐会话必须通过横向上下文传递,被从旧LCM传递到新LCM。

[1692] MN对WLCCP的支持

[1693] MN不直接参与WLCCP。相反,MN可支持传输子网和路径代价信息的WLCCP 802.11要素。该要素辅助下列各项:

[1694] -MN可选择提供到MN的本地子网上的基本LAN的最小代价路径的双亲AP。

[1695] -MN能很快确定它是否已经漫游到不同的子网。

[1696] -标准移动IP MN能很快发现MIP外部代理。

[1697] -MN能可靠地注册其IP地址。

[1698] -MN能可靠地注册其被使能的多播地址。

[1699] 用于传输WLCCP信息的802.11要素在名为“WLCCP 802.11要素”的部分中定义。

[1700] 为了描述和说明的目的,已经给出了本发明的优选实施例的上述描述。不希望穷举或把本发明限制为所公开的精确形式。根据上述教导,显而易见的修正或变化是可能的。选择和描述的实施例用于提供对本发明的原理和其实际应用的最佳说明,从而使得本领域普通技术人员能够在各种实施例中使用本发明,伴有适于所构思的特定使用的各种修正。当所附权利要求被公平、合法和公正地赋予的范围来解释时,所有的这种修正和变化都在所附权利要求确定的本发明的范围之内。

[1701] 相关申请的交叉引用

[1702] 本申请要求2002年11月26日递交的No.60/429,714美国临时申请的权利。本申请要求2003年1月10日递交的No.60/439,419美国临时申请的权利。

[1703] 版权或模板作品声明

[1704] 本专利文件的公开的一部分包含受到版权保护的材料。版权的所有者不反对任何人对专利文件或专利公开如同在专利商标局的专利文件或记录中所出现的那样的复制,否则保留任何版权。

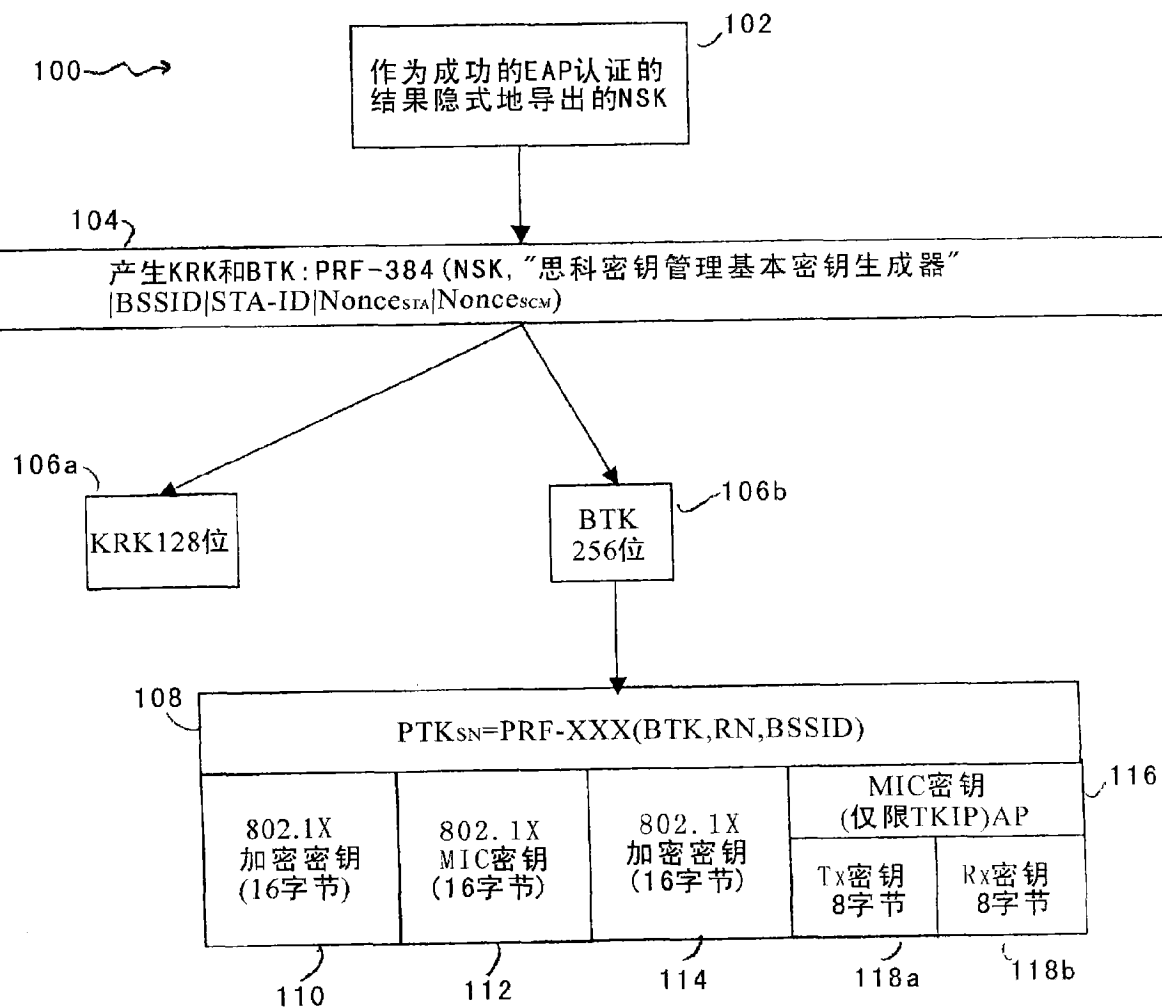


图1

202 802.1X 认证类型	204 NSK计算	206 NSK长度 (按字节)	208 SCM获取
LEAP	由MN和AS 相互导出	16	Radius属性:MS-MPPE单密钥
PEAP	由MN和AS 相互导出	32	Radius属性:MS-MPPE接收密钥 (忽略发送密钥)
EAP-TLS	由MN和AS 相互导出	32	Radius属性:MS-MPPE接收密钥 (忽略发送密钥)
EAP-MD5	无	5, 13 或 16	静态配置

200

图2

OUI	类型	含义
00:50:F2	0	无认证密钥管理
00:50:F2	1	使用802.1X上的非特定认证的认证密钥管理：缺省用于SSN
00:50:F2	2	使用802.1X上的预共享密钥的认证密钥管理
00:50:F2	3-255	保留
00:40:96	协商值	CCKM*
其他	任意	销售商指定

图3

MN证书的SCM缓存

字段	长度(字节)	描述
状态	2	标识该节点是否活动
STA Addr	8	WLCCP节点标识符：MN的MAC地址
认证类型	1	用于认证的EAP类型
密钥管理类型	1	协商的密钥管理类型，或无协商的密钥管理类型。有效的值是： 0-无 1-CCKM 2-SSN/TGi
会话超时时间	4	Radius访问接收提供的会话期满时间
KRK	16	用于认证对上下文传递的MN请求的密钥请求密钥
BTK	32	用于导出PTK的基本瞬时密钥
RN	8	用于跟踪已从BTK导出多少PTK的重定密钥号
SSID	32	MN的关联的SSID
VLAN ID	2	MN的关联的VLAN分配
BSSID	6	定义当前关联的VLAN
密码(Cipher)	2	协商的密码，值为： 0x0000 - none 0x0001 - WEP 0x0002 - TKIP 0x0003 - AES-OCB 0x0004 - AES-CCMP 0xff<值>-供应商指定
NSK密钥长度	2	MS-MPPE规定的Rx密钥长度
NSK	N	成功的802.1X EAP认证产生的Rx密钥 (MS-MPPE中的Rx密钥)
Tx密钥长度	2	MS-MPPE规定的Tx密钥长度
Tx密钥	P	成功的802.1X EAP认证导致的Tx密钥 (MS-MPPE中的Tx密钥)

图4

AP的缓存的证书

508 510	502	504	506
字段	长度(字节)	描述	
状态	1	表示该节点是否活动	
节点ID	8	WLCCP节点标识符: AP的MAC地址(例如BSSID)	
512	NSK	16	成功的LEAP认证产生的密钥
514	会话超时时间	4	Radius访问接受提供的 会话期满时间
516	CTK	32	用于保护SCM认证者和节点ID之间的 通信的当前上下文传递密钥
518	密钥序列计算器	4	用于跟踪已经发生多少次CTK密钥 刷新的序列计算器

图5

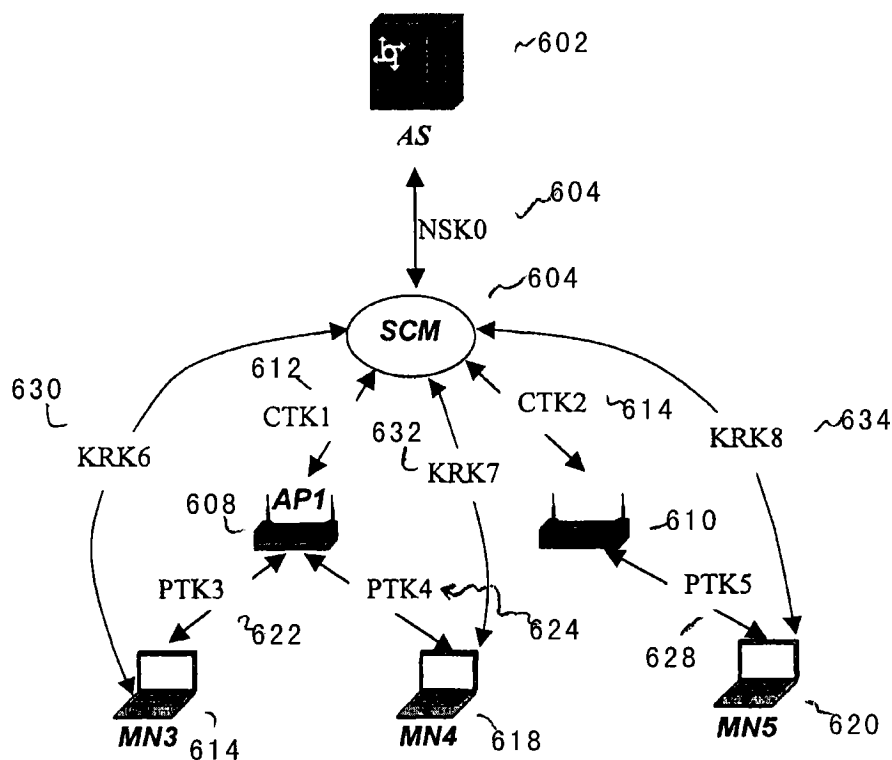


图6

AP向SCM注册

702 AP	704 SCM	706 认证服务器(AS)
	SCM丢弃所有来自未认证和未注册AP的请求	
AP接收SCM通告，AP必须首先向SCM认证	SCM在有线线路上发送通告，实现AP和MN认证。SCM是认证者	
WLCCP封装的EAP身份响应→		
	带有EAP属性的RADIUS访问请求→	
		←带有包含LEAP服务器质询的EAP属性的RADIUS质询
	←带有LEAP服务器质询的EAPOL分组	
带有LEAP质询响应的WLCCP封装的EAPOL分组→		
	带有EAP属性的RADIUS访问请求→	
		←如果无效，发送带有EAP失败属性的RADIUS拒绝
		←如果有效，发送带有EAP成功属性的RADIUS访问质询消息
	←带有EAP成功的EAPOL分组	
带有LEAP客户质询的WLCCP封装的EAPOL分组→		
	带有EAP属性的RADIUS访问请求→	
		←带有包含LEAP客户质询响应的EAP属性和包含会话以及会话超时时间的Cisco属性的RADIUS访问接受消息
	SCM缓存NSK和会话超时时间	

图7A

	←带有LEAP客户质询响应的EAPOL分组	
AP安装密钥		
WLCCP(Path Init,provide NonceAP) →		
	←如果Path Init失败,用非零状态响应	
	←如果Path Init成功,产生Nonce _{scm} 并导出CTK,设置KSC=1,发送WLCCP(Path Init Reply, Nonce _{scm} , MIC _{CTK})	
获取Nonce _{scm} 并导出CTK		
如果MIC _{CTK} 失败,用非零状态确认→		
如果MIC _{CTK} 成功,设置KSC=1,发送WLCCP(Path Init Confirm, MIC _{CTK})		
AP现在可以使用传送来的CTK保护和SCM的通信,请求MN上下文传递和注册MN		
WLCCP(注册请求) →		
	←如果注册失败,用于非零状态响应	
	←如果注册成功,发送WLCCP(Preregistration Response, status=0)	

图7B

成功的MN LEAP认证和注册

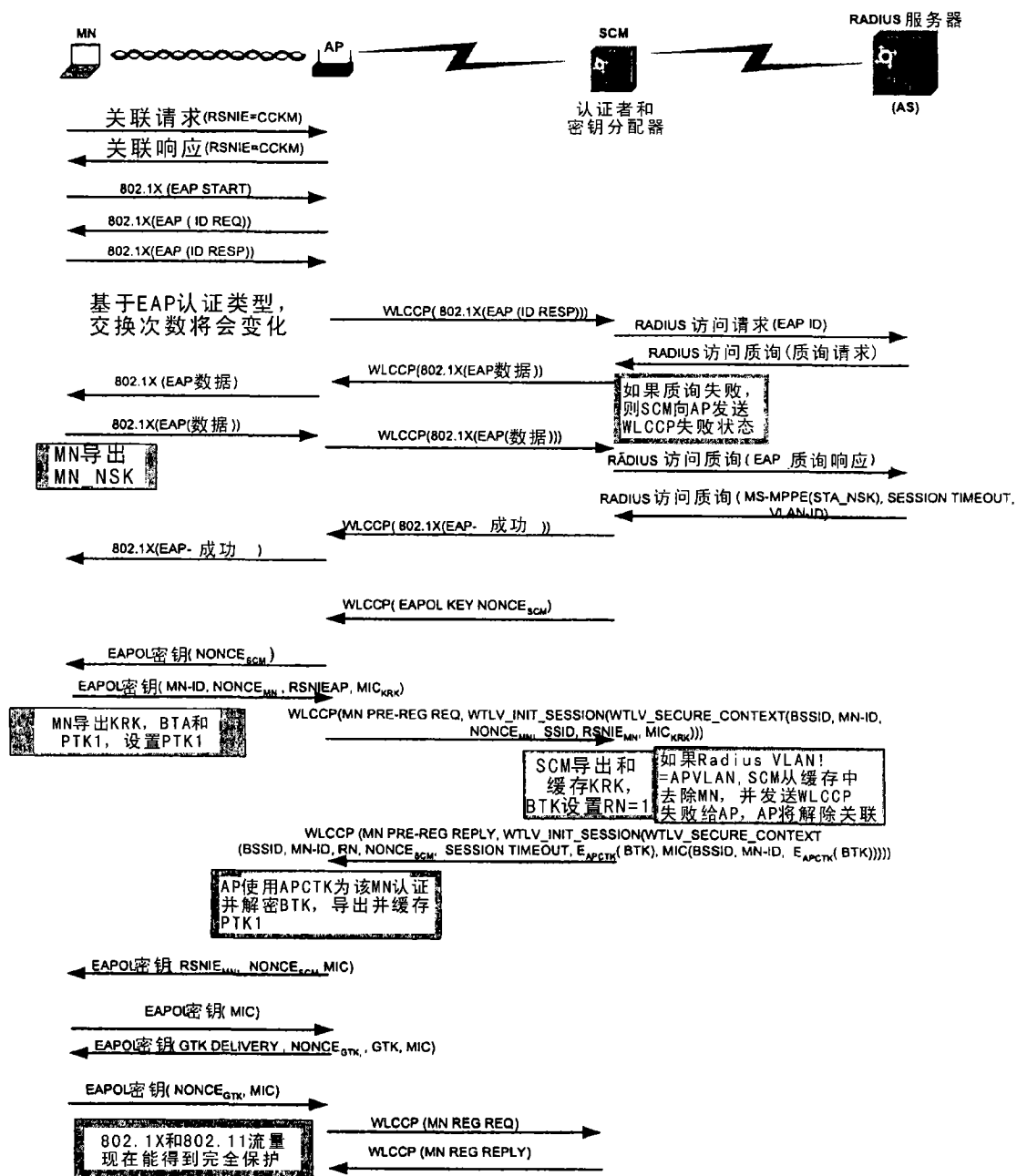


图8

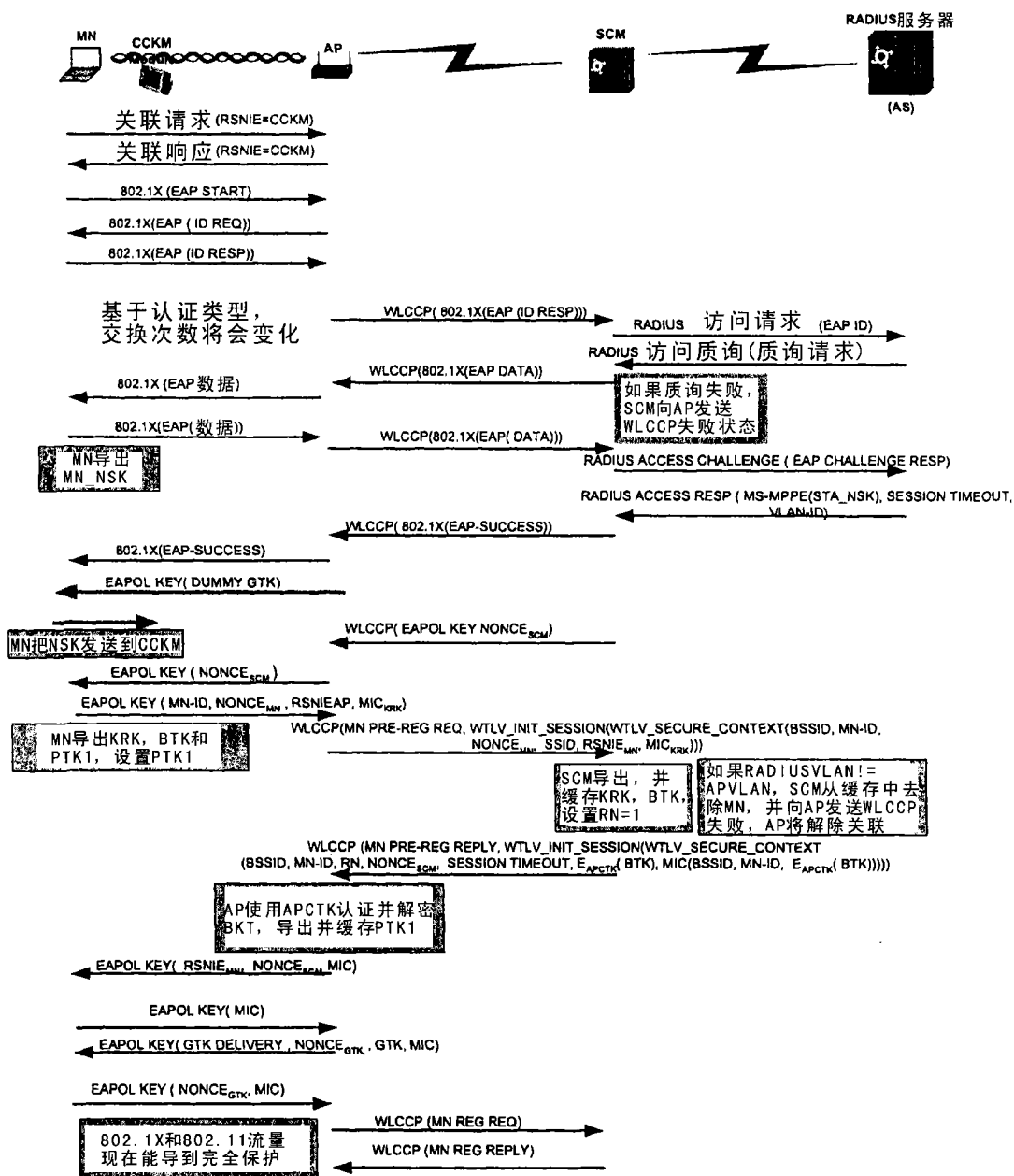


图9

MN	AP	SCM
MN成功地向SCM关联和认证. MN和SCM都有NSK.		
MN产生 $Nonce_{MN}$		MN802.1X认证完成, 生成 $Nonce_{SCM}$, 开始Krk, BTK初始化
		←具有 $Nonce_{SCM}$ 的WLCCP_AUTHENTICATE封装EAPOL分组
	←带有 $Nonce_{MN}$ 的EAPOL密钥	
从PRF($NSK, Nonce_{MN}, Nonce_{SCM}$)中计算Krk和BTK, $RN=1$, $PTK1=PRF(BTK, BSSID RN)$ 产生 $MIC_{MN}(Krk, BSSID, MN-ID, Nonce_{MN}, Nonce_{AP}, RSNIE_{AP})$		
带有 $Nonce_{MN}$ 的EAPOL密钥→ $RSNIE_{AP}$ MIC_{Krk}		
	WLCCP Pre-Reg Req packet → WTLV_SESSION_INIT request with WTLV_SECURE_CONTEXT(AP-ID, MN-ID, $Nonce_{MN}$, SSID, MIC_{Krk})	
		←如果SSID、VLAN、 MIC_{MN} 无效, 则不更新注册表, 不产生密钥。发送适当的状态值。
		←如果SSID、VLAN、 MIC_{MN} 有效, 从PRF($NSK, Nonce_{MN}, Nonce_{AP}$) $RN=1$ 发送带有 WTLV_SESSION_INIT (WTLV_SECURE_CONTEXT (WTLV_TRANSIENT_KEY(BTK, RN), session timeout))的WLCCP Pre-Reg Reply分组
	←缓存这个MN的BTK, RN和会话超时时间。组成响应EAPOL密钥 $Nonce_{MN}, RSNIE_{MN}, MIC_{AP}$	

图10A

	RSNIE _{MN} , MIC _{AP}	
MN可以接收并把受保护的802.1X和802.11单播帧传输到AP	AP可以接收并把受保护的802.1X和802.11单播帧传输到AP	
MIC _{MN} = MIC(PTK, BSSID, MN-ID, Nonce _{MN} , Nonce _{AP} , RSNIE _{AP}) EAPOL密钥MIC _{MN} →		
	← EAPOL密钥 GTK, Nonce _{GTK} , MIC _{GTK}	
EAPOL 密钥 Nonce _{GTK} , MIC →		
端口完全开放; 保护了所有分组	端口完全开放; 保护了所有分组	

图10B

	1102	1104	1106	1108	1110	1112	1114	1116	1118
描述符类型	密钥信息		EAPOL重放控制	保留	密钥-ID	MN-ID	BSSID	RN	MIC
1字节	1字节	2字节	4字节	1字节	1字节	6字节	6字节	4字节	8字节

图11

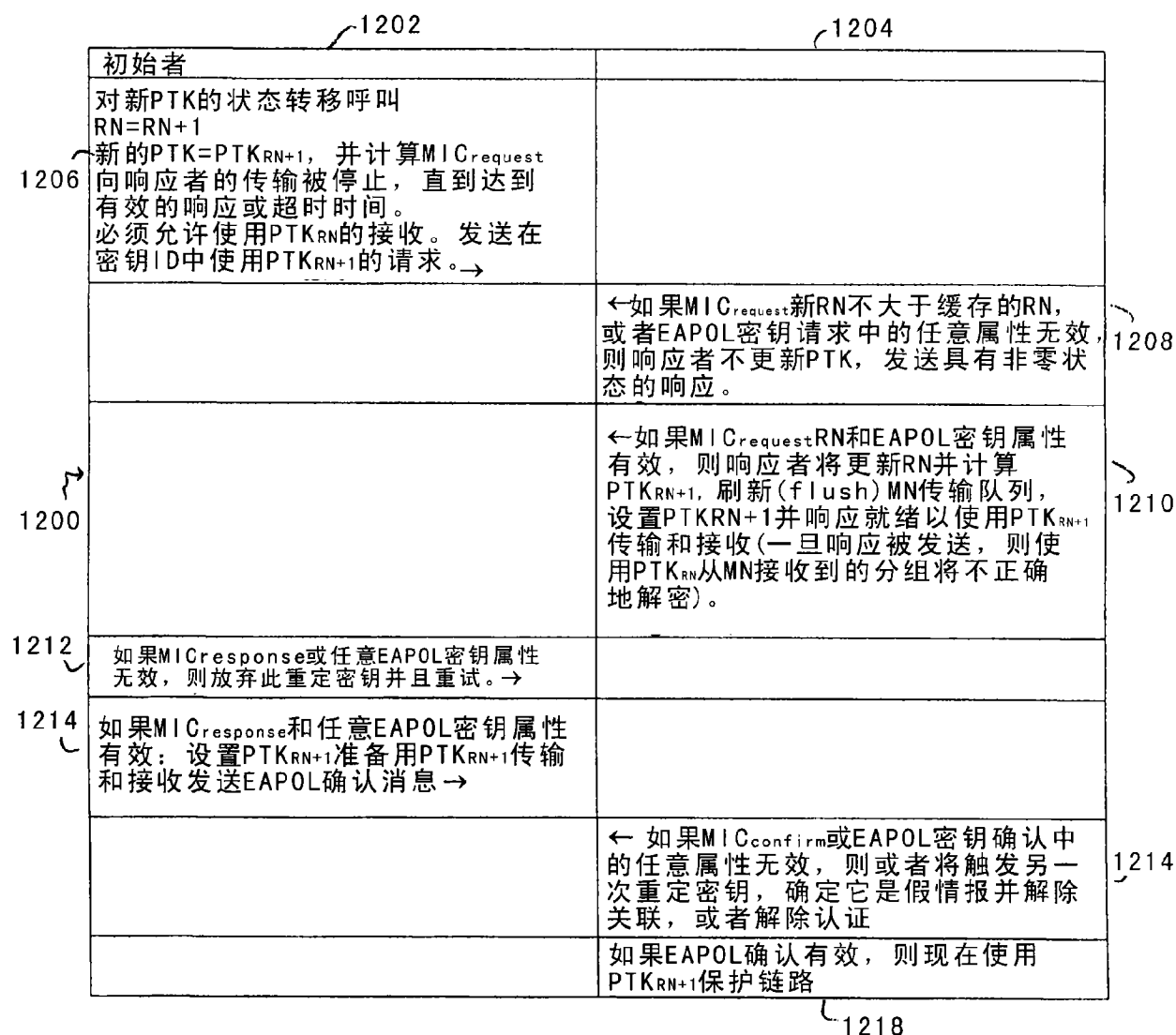


图12

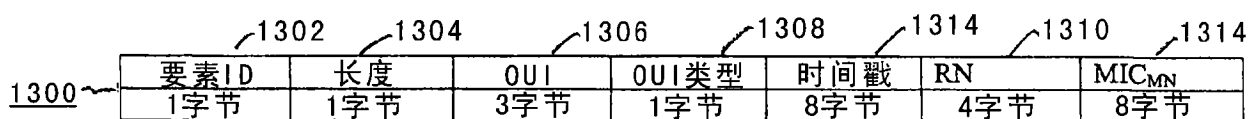


图13

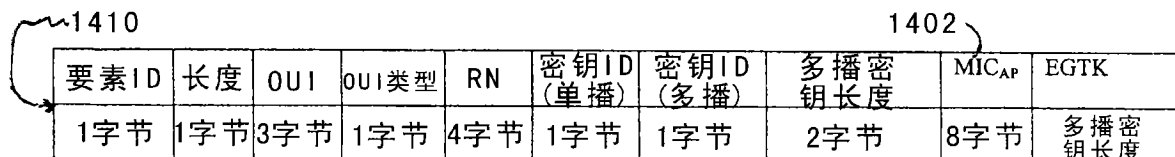


图14

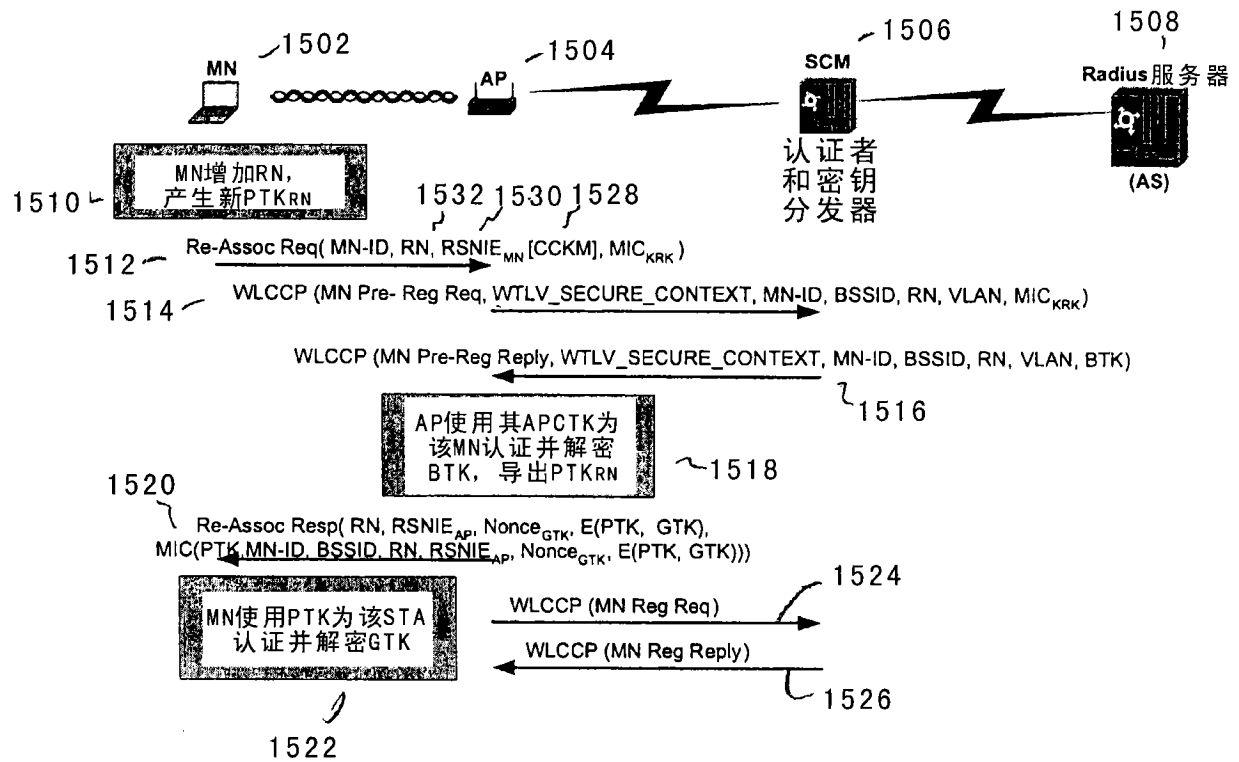


图15

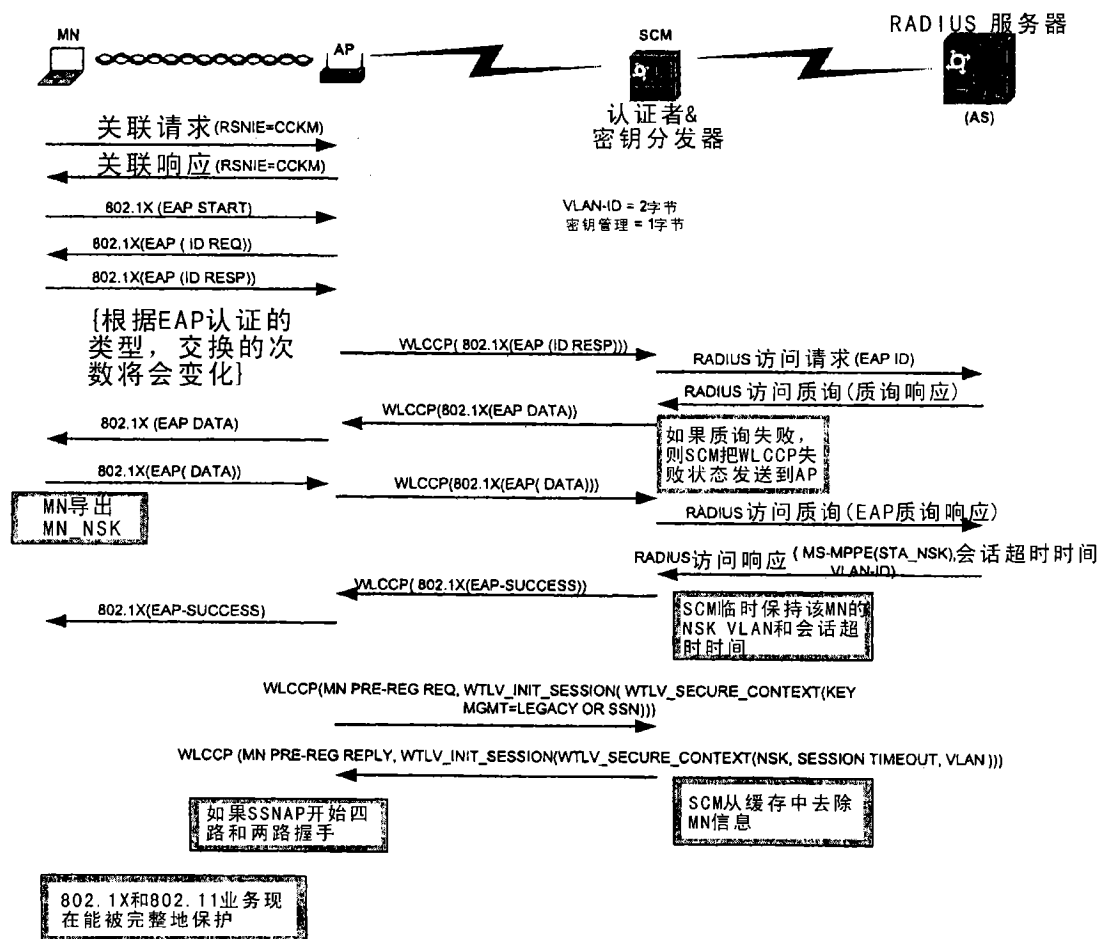


图16

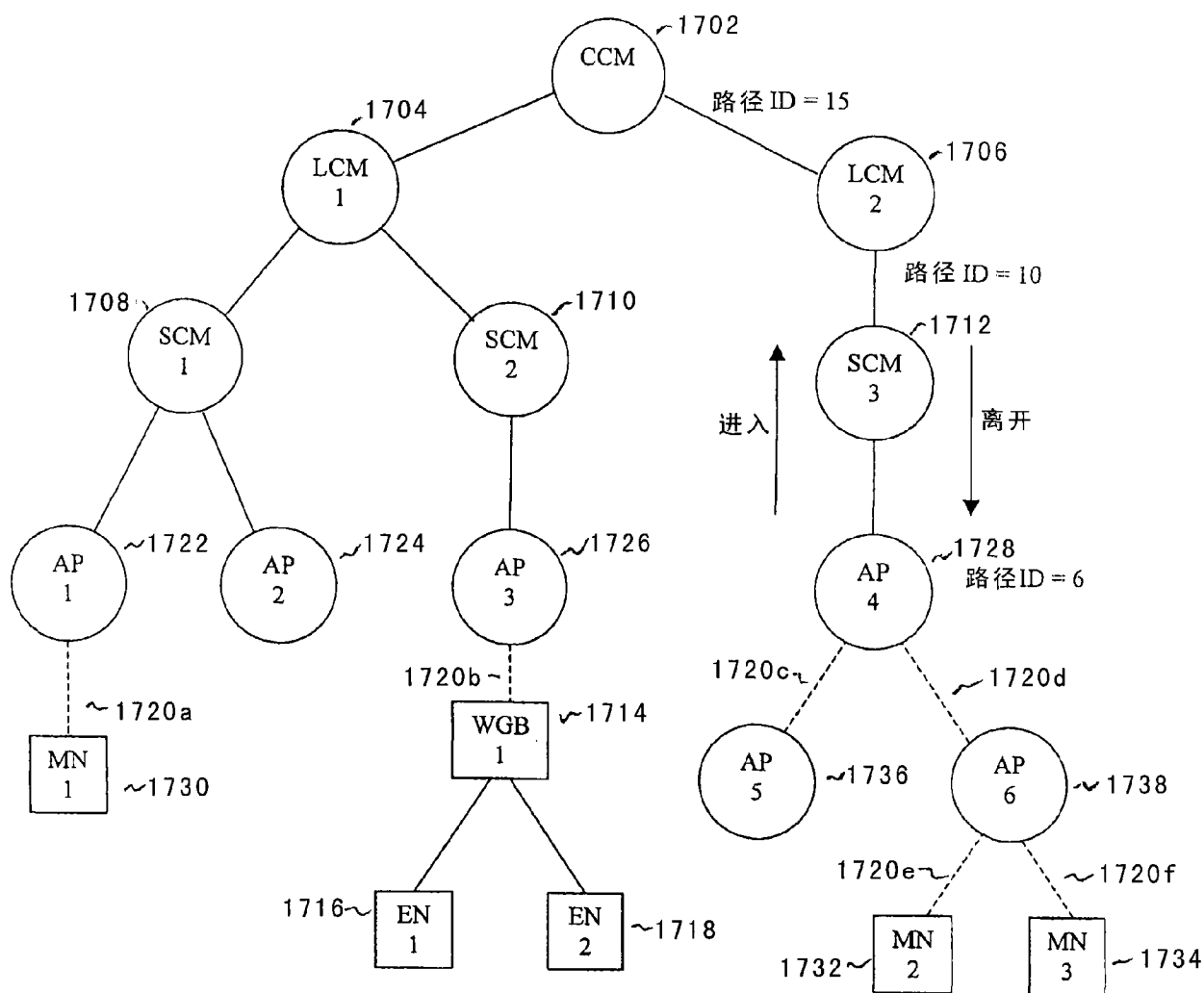


图17

字段名	偏移量	大小 (字节)	描述
节点类型 1802	0	2	(无) = 0 AP = 1 SCM = 2 LCM = 4 CCM = 8 ICN = 0x10 /* 基础结构客户 */ 客户 = 0x40 多播标志 - 0x8000
节点地址 1804	2	6	IEEE全局或局部管理的规范(即以太网)格式的48位地址

图18

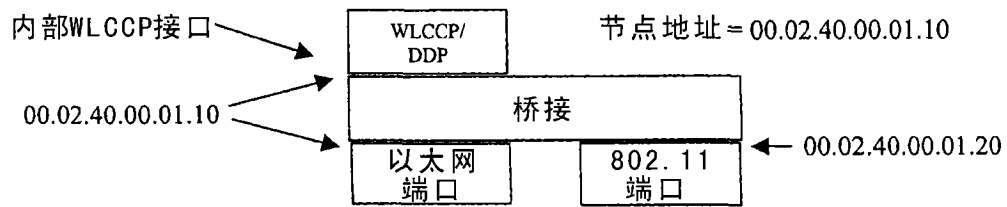


图19

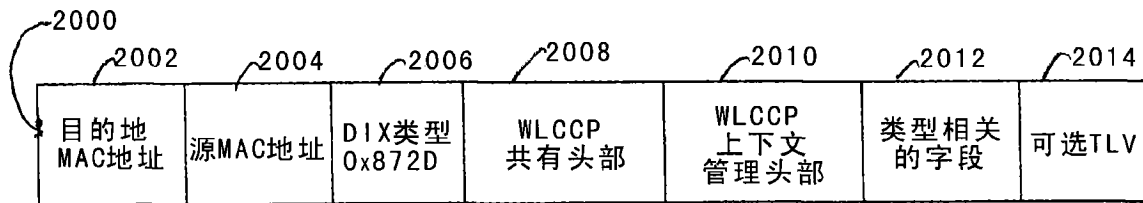


图20

	2102 字段名	2104 偏移量	2106 大小 (字节)	2108 描述
2110	协议ID/ 版本	0	1	Hex. C1-为与DDP兼容而被选择
2112	WLCCP SAP	1	1	8位协议服务接入点ID 0=WLCCP上下文管理SAP 2=无线资源管理SAP
	目的地节点类型	2	2	跳目的地的节点类型
2114	长度	4	2	消息的字节长度, 包括WLCCP头部
2118	类型	6	1	消息类型 第0-1位-子类型(0=请求, 1=应答, 2=确定, 3=Ack) 第2-7位-基本消息类型
	跳计数	7	1	WLCCP跳的数目
2116	消息ID	8	2	用于匹配请求/应答对的消息序列号
2120	标志	10	2	第0位-重试标志(在重传输中置为0N) 第1位-响应请求标志(设为0N以请求 应答) 第2位-TLV标志(设为0N以表明固定字 段后跟可选TLV) 第3位-进入标志 第4位-远离标志 第5位-跳路由标志 第6位-根CM标志 第7位-中继标志 第8位-MIC标志 第9-15位(保留-必须为0)
2122	发起者节点ID	12	8	发起者节点类型和节点地址
2124	响应者节点ID	20	8	响应者节点类型和节点地址
	数据	28	N	类型相关的字段和TLV

2100

图21

2210			
2202	2204	2206	2208
字段名	偏移量	大小 (字节)	描述
类型	0	2	TLV标识符 第0位-容器标志 第1位-被加密标志 第2-3位-(保留-必须为0) 第4-7位-组ID 第8位-请求标志 第9-15位-类型ID
长度	2	2	TLV的长度，包括类型和长度字段
值	4	N	类型相关数据，如果请求标志是OFF

图22

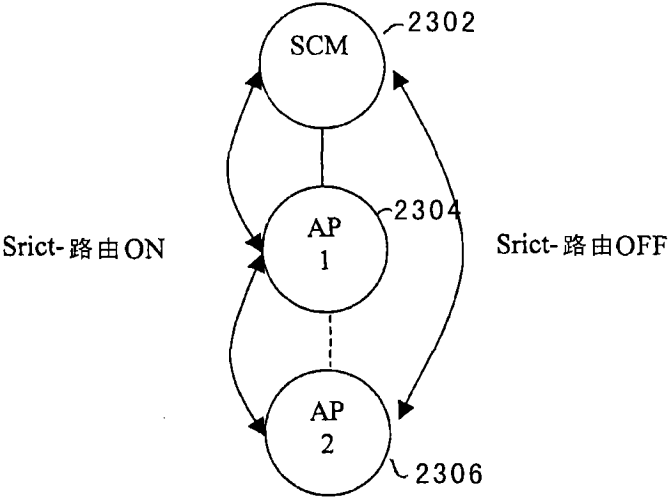


图23

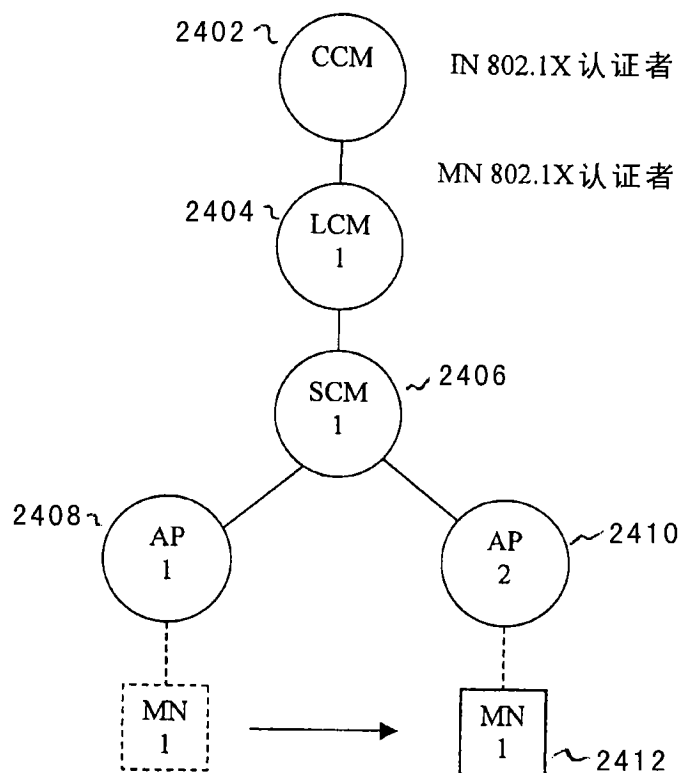


图24

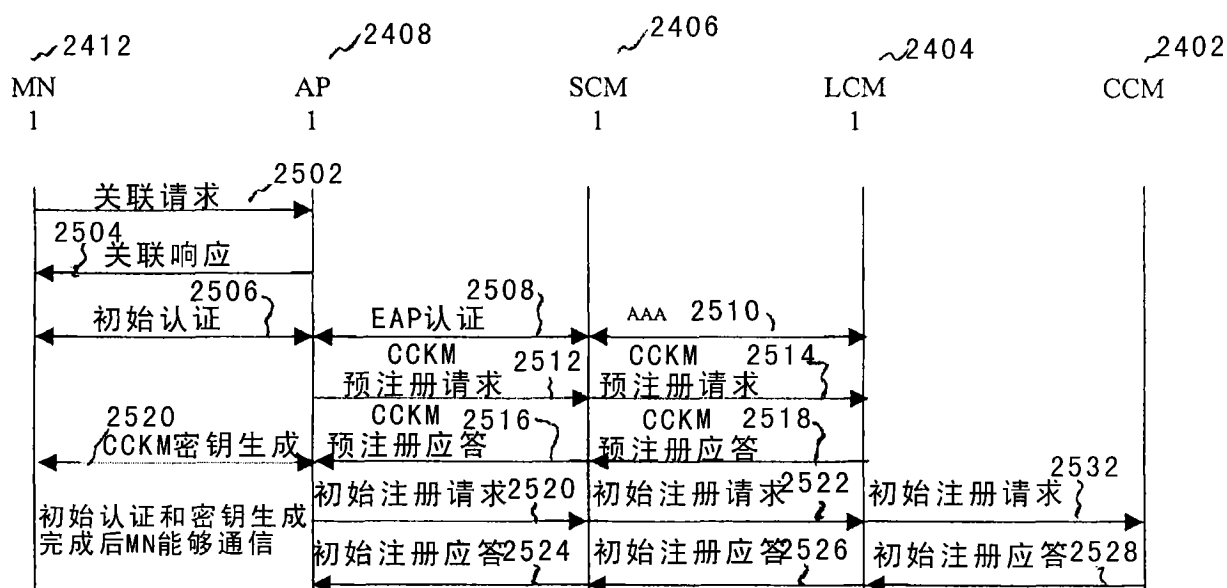


图25

MN漫游:

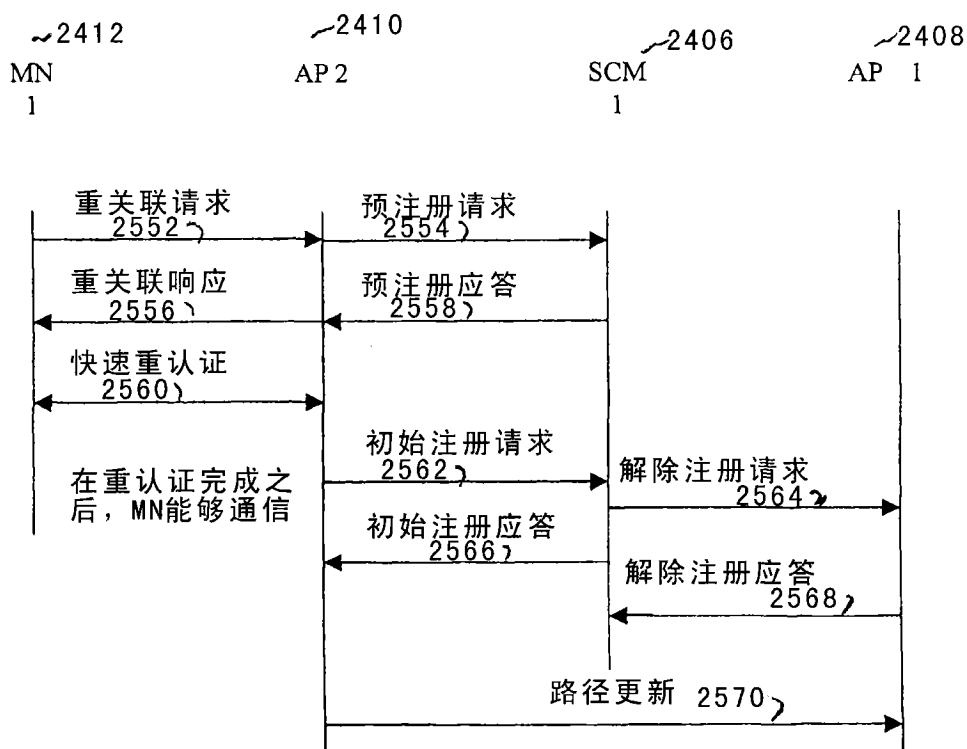


图26

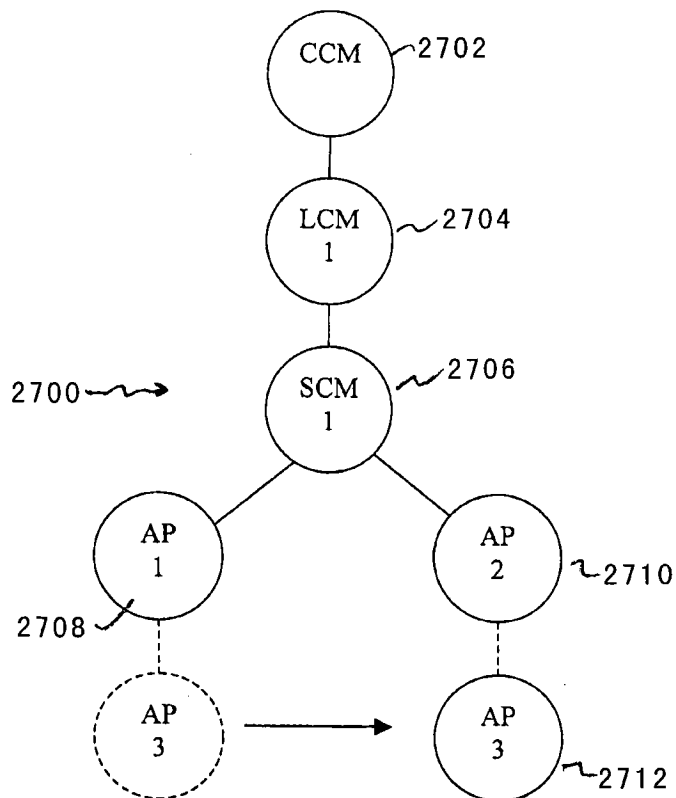


图27

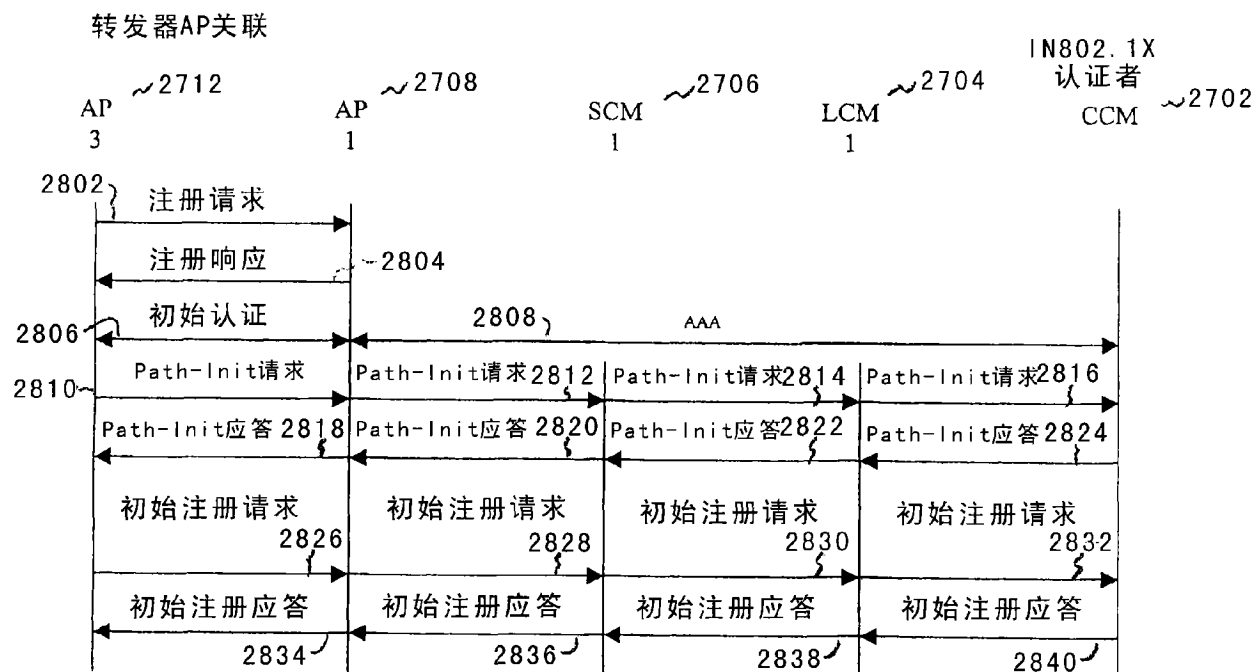


图28A

转发器AP漫游:

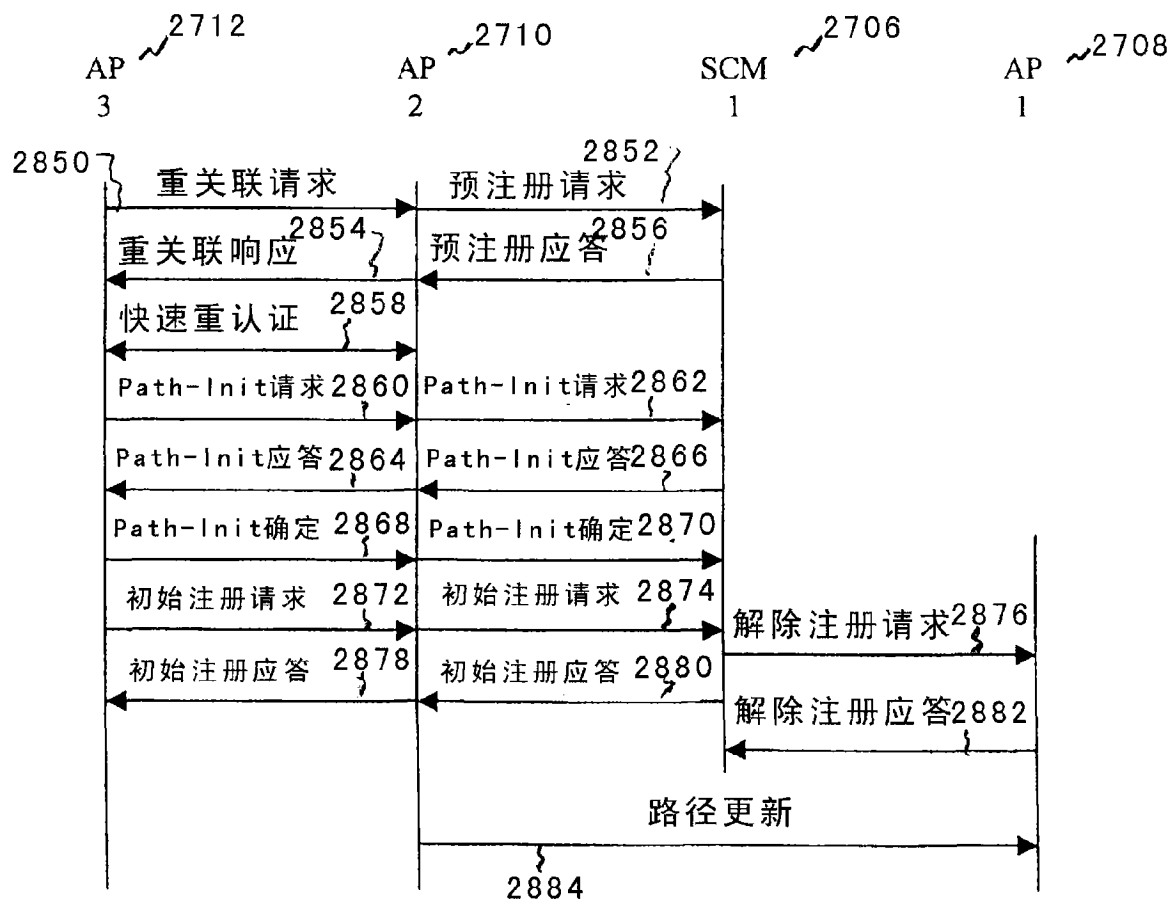


图28B

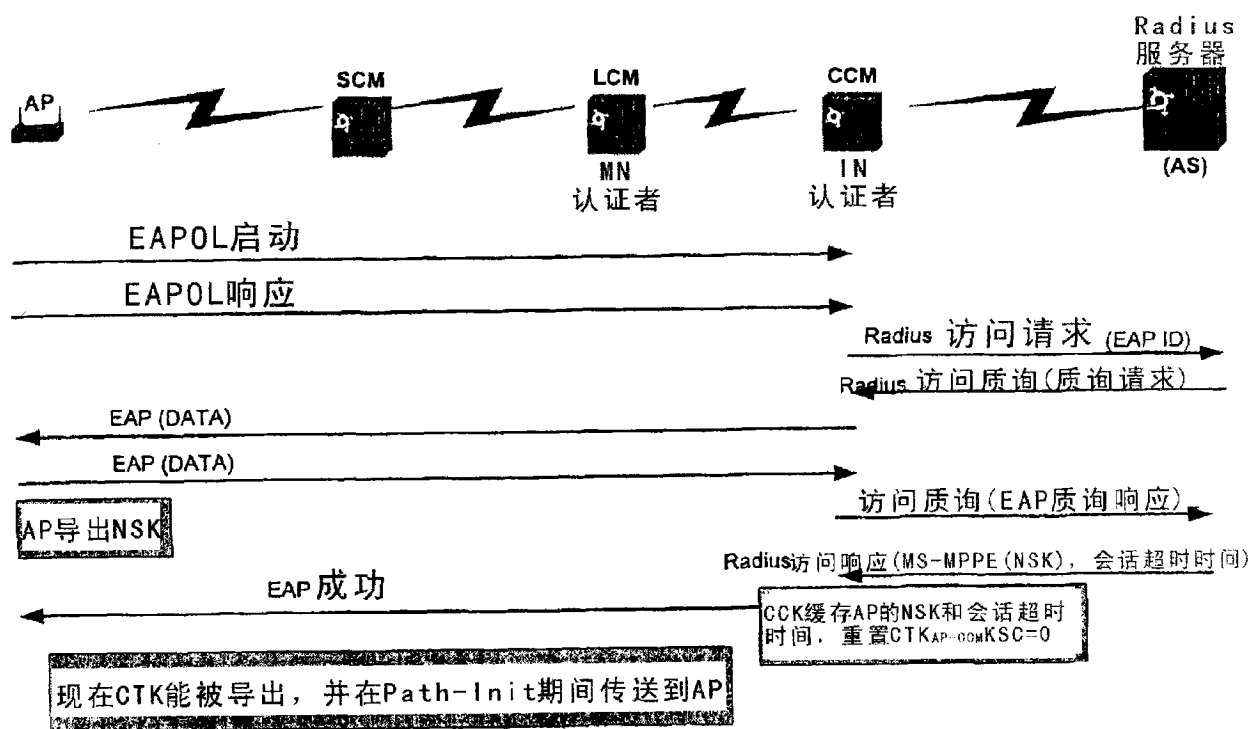


图29

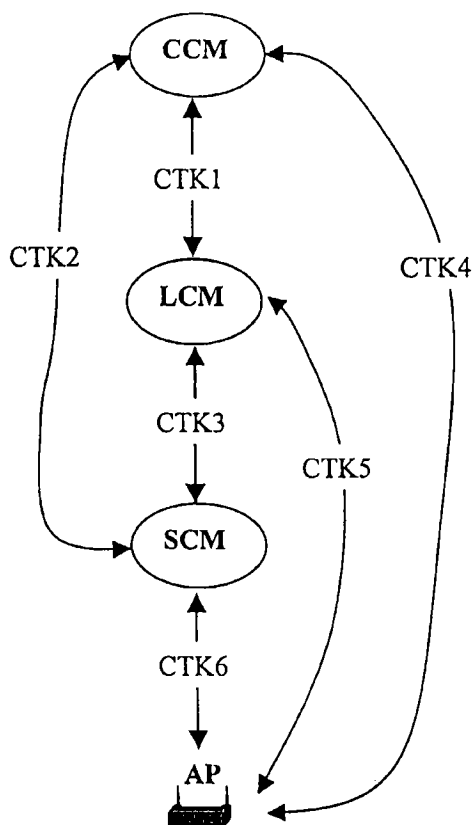


图30

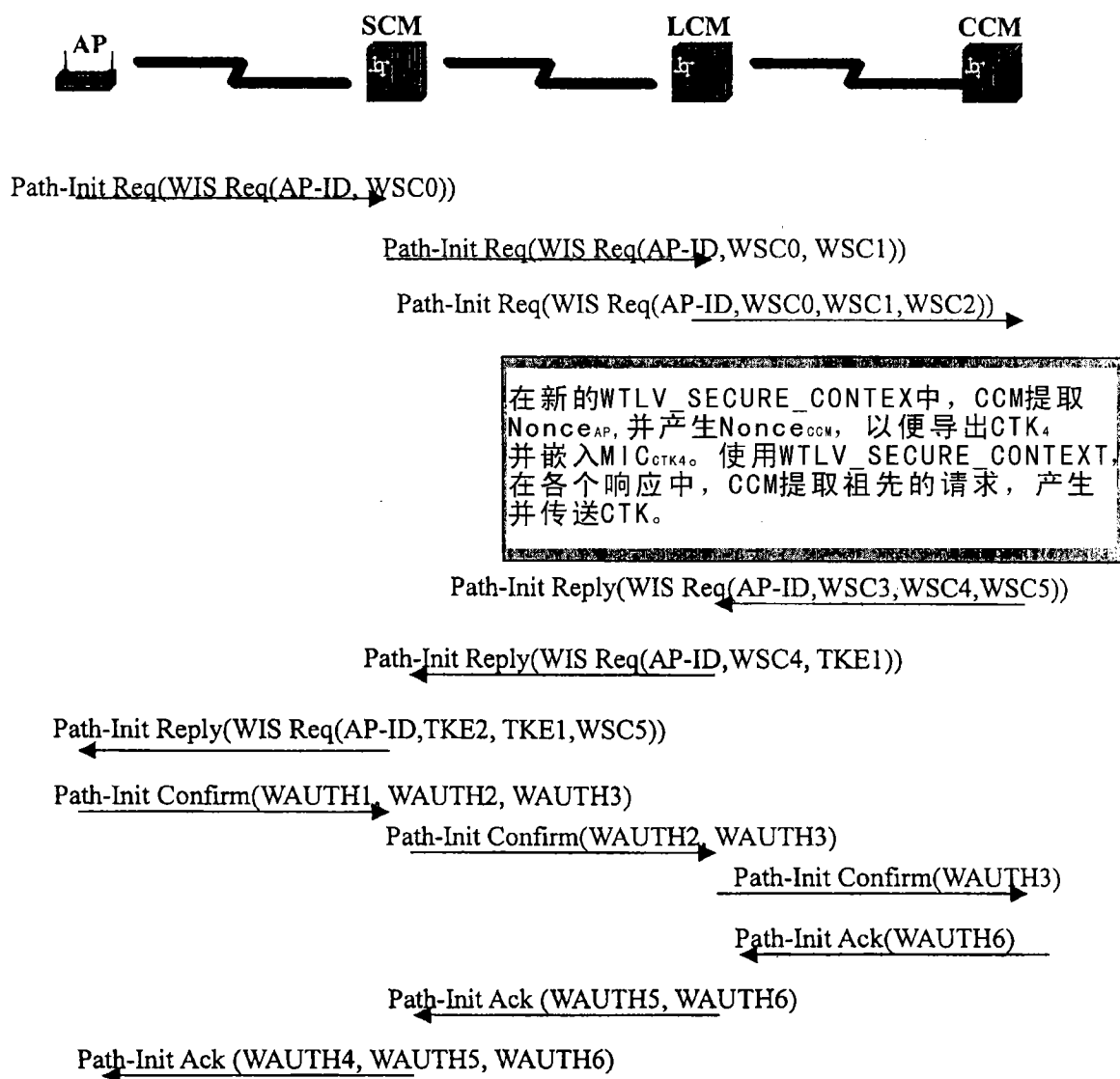


图31

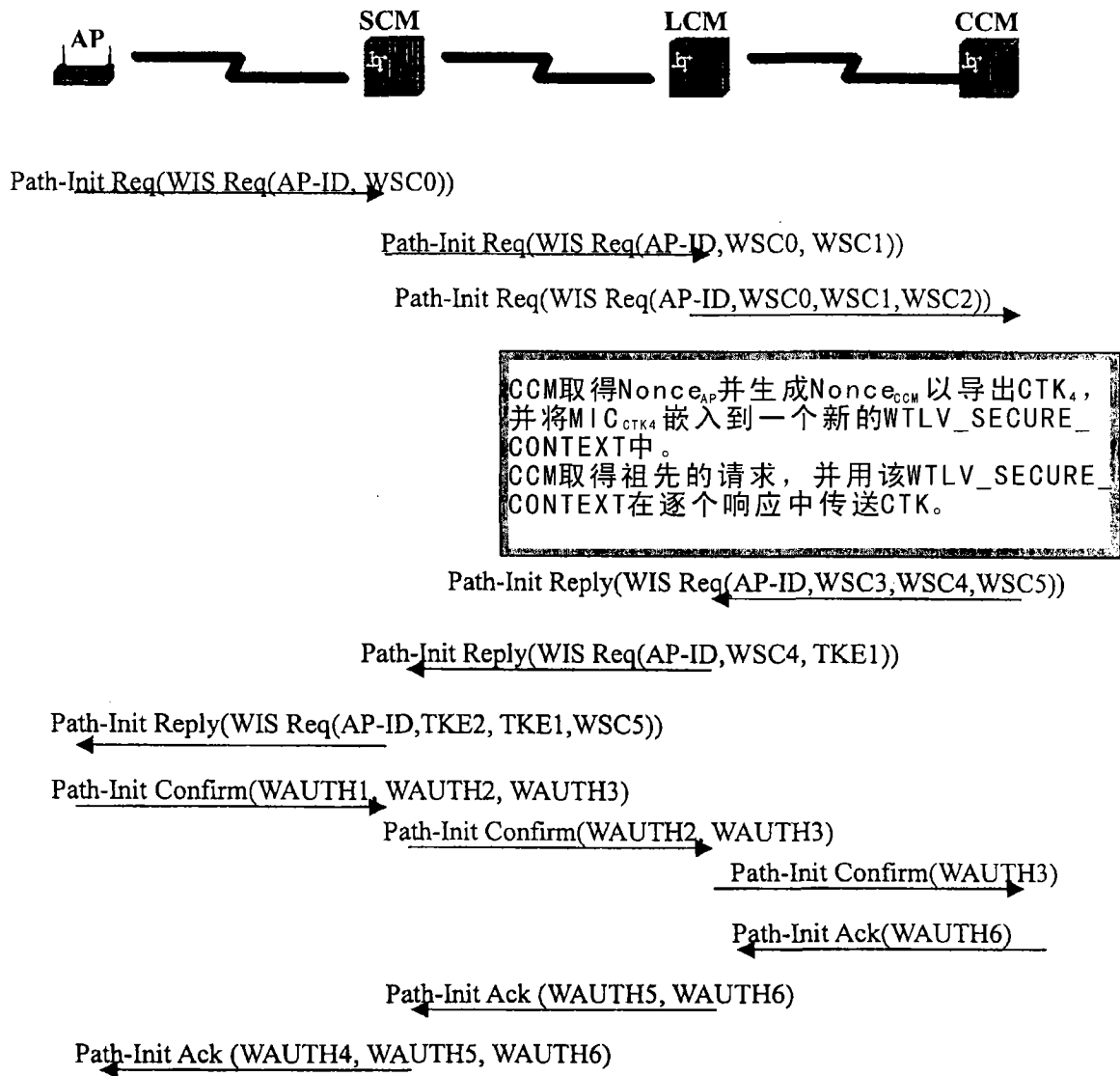


图32

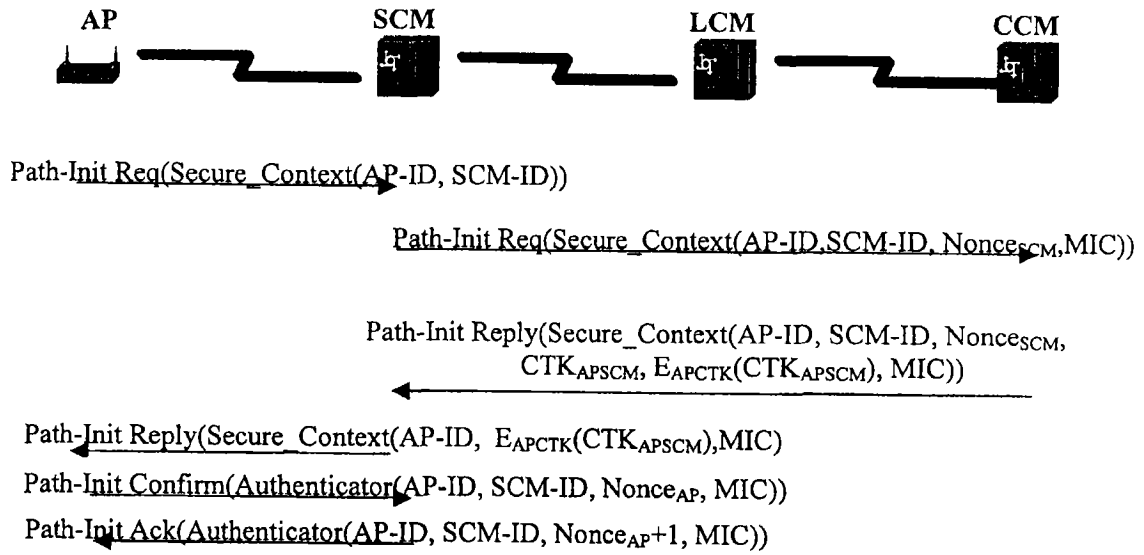


图33

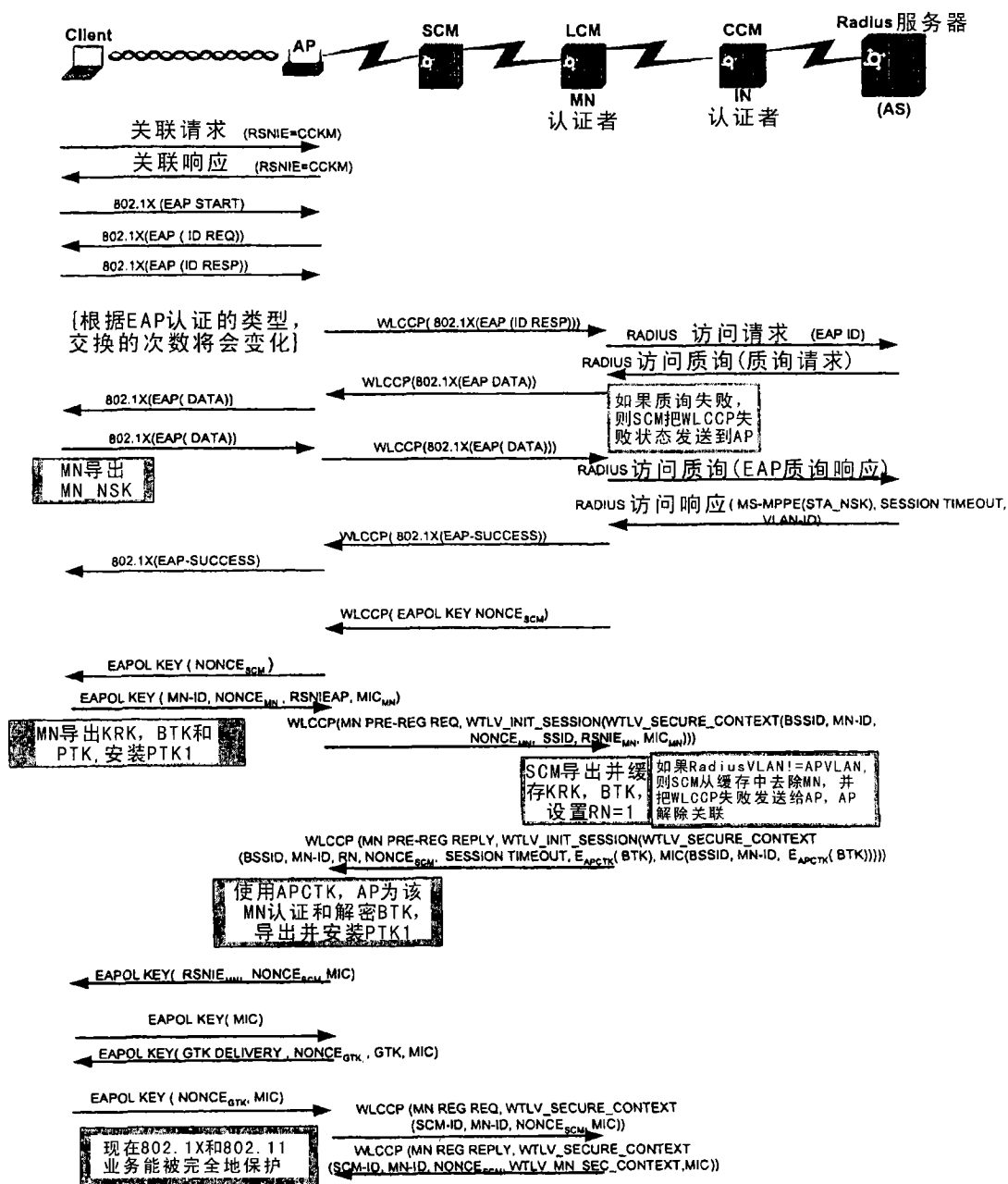


图34

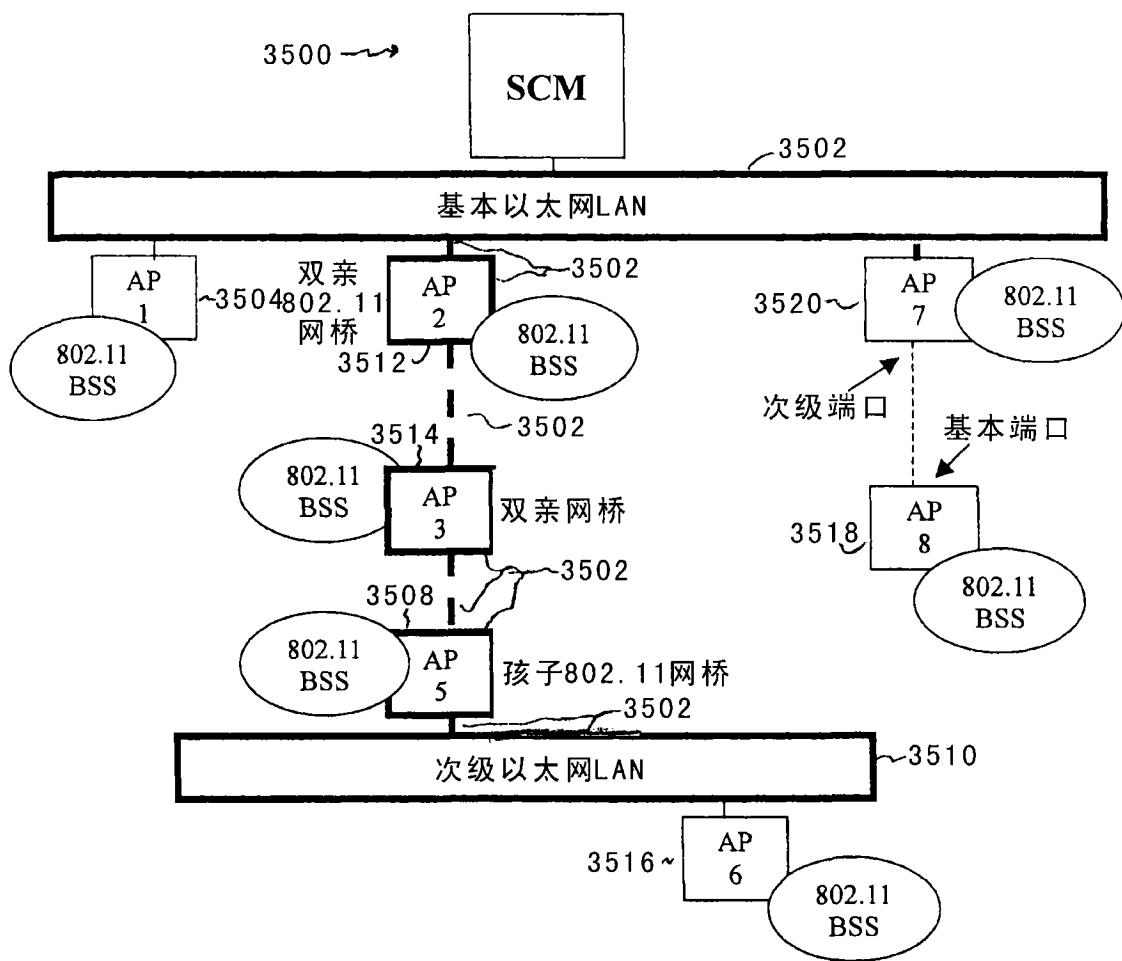


图35