
移动IP和三角路由问题

第6单元　移动IP和三角路由问题

目录

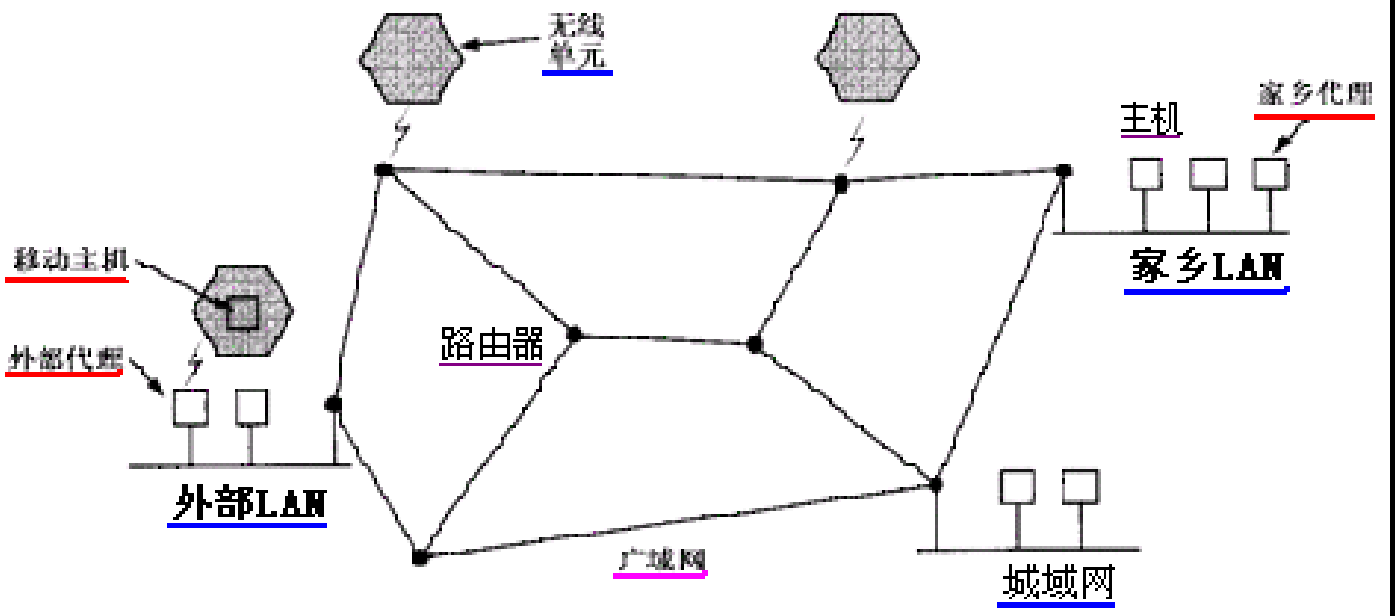
6.1 移动主机的路由选择
6.2 移动IP概要
　　6.2.1 主题
　　6.2.2 必要条件和设计目标
　　6.2.3 功能实体及其驻留位置
　　6.2.4 概要工作过程
6.3 代理发现
6.4 移动检测和移动登记
　　6.4.1 登记功能
　　6.4.2 登记协议
　　6.4.3 登记操作
6.5. 路由操作和三角路由问题

第6单元　移动IP和三角路由问题

- 今天，数以百万计的人持有可携带的计算机，他们希望在所处的任何地方都能够阅读他们的电子邮件以及访问他们通常使用的文件系统。这些移动主机引入了一种新的复杂性：为了把一个分组路由到主机，网络首先必须找到它的位置。
- 下图示出了网络设计典型使用的模型。在这个模型中，有一个由路由器和主机构成的广域网，连接到该广域网的有局域网、城域网和无线单元区。

6.1 移动主机的路由选择

在网络设计典型使用的模型中，有一个由路由器和主机构成的广域网，连接到该广域网的有局域网、城域网和无线单元区。



插图：连接局域网、城域网和无线单元区的广域网

6.1 移动主机的路由选择

- 从不移动的主机被称着是静止的。它们通过铜导线或光纤连接到网络。迁移主机基本上是静止主机，它们不时地从一个固定场点移动到另一个固定场点，但它们仅当物理地连接到网络时才会使用网络。漫游主机实际上是在运动的过程中计算，并且在移动时仍然维持网络连接和连续使用网络。人们把迁移主机和漫游主机统称为移动主机，即离开家乡仍然要连接到网络的主机。

6.1 移动主机的路由选择

- 所有的主机都被假定有一个不会改变的永久的家乡位置，主机还有一个可以用以确定它的家乡位置的永久的家乡地址。在具有移动主机的系统中，路由选择的目标是，无论它们当前是在家乡，还是在外地，都可以用它们的家乡地址给它们发送分组，而且这些分组总是能够被有效地传送给它们。
- 我们可以把上图中的模型在地理上划分出许多个小的单元，并把每个单元都称着一个区，典型地是一个局域网络或一个无线单元。每个区有一个或多个外部代理，它们是保持跟踪访问该区的所有移动主机的进程。此外，每个区有一个家乡代理，它保持跟踪其家乡在这个区但当前已外出访问另一个区的那些主机。

6.1 移动主机的路由选择

- 当一台新的主机进入一个区（例如通过连接到一个LAN插座，或者是漫游进入一个无线单元）时，该计算机必须将自己向那里的外部代理登记。登记过程典型地是按下列方式进行：

（1）每个外部代理周期性地广播一个分组，宣告它的存在和它的地址。一个新到达的移动主机可以等待一个这样的报文。但如果在稍等片刻之后发现无报文到达，移动主机可以广播一个分组，说"这里有移动代理吗？"

（2）移动主机跟外部代理登记，给出它的家乡地址、当前的数据链路层地址和某些安全性信息。

（3）外部代理联系移动主机的家乡代理，说"你的一个主机在我这里。"这个从外部代理发往家乡代理的报文含有外部代理的网络地址。它也包含一些安全性信息，让家乡代理相信该移动主机确实在那里。

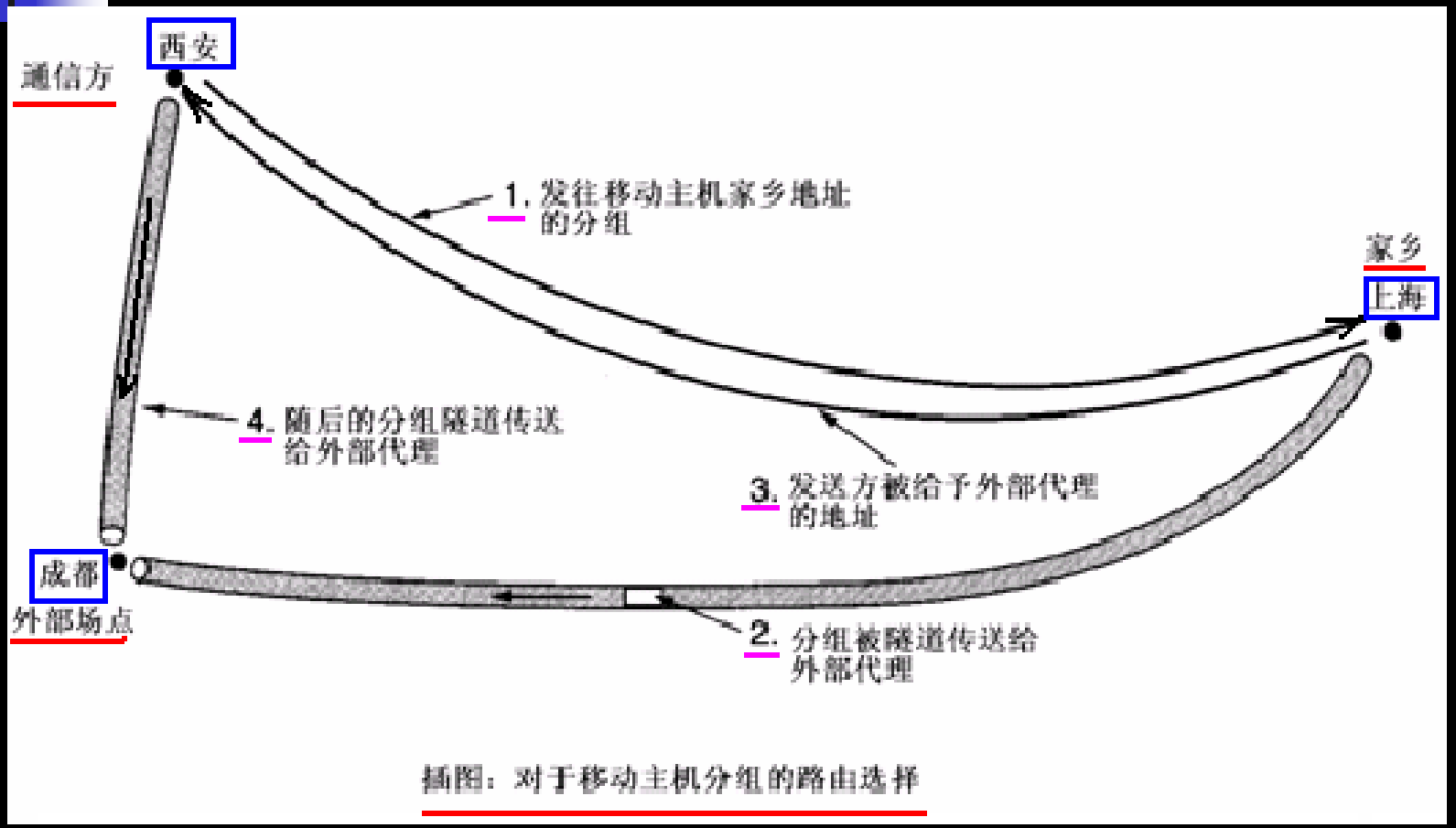
（4）家乡代理检查带有时间印记的安全性信息，证明这是在刚过去的几秒钟内产生的。如果通过了检查，它就告诉外部代理继续进行。

（5）当外部代理从家乡代理那里得到肯定的确认应答时，它就在表中做一些登记项，并且通知移动主机已经登记好了。

6.1 移动主机的路由选择

- 在理想的情况下，当一个主机离开一个区域的时候，它也应该被宣告允许做离开登记。但是有许多用户在他们结束工作时会突然关闭他们的计算机。
- 当一个分组被发往一个移动主机时，它会被路由到该主机的家乡LAN,那是由其公布的地址决定了的。如下图所示，假定在西安的一个发送方把一个分组发送给在上海的一个主机。发送给移动主机的分组在上海的家乡LAN被那里的家乡代理截获。然后家乡代理查询该移动主机的新位置，发现为该移动主机服务的外部代理的地址是在成都。

6.1 移动主机的路由选择



插图：对于移动主机分组的路由选择

6.1 移动主机的路由选择

- 接着，家乡代理做两件事情。首先，它把收到的分组封装到一个外包装分组的载荷段，并把外包装分组发送给外部代理（参见上图中示出的步骤2）。通常人们把这一机制称作隧道。外部代理在收到外包装分组后，从载荷域中取出原先的分组，并用数据链路帧发送给移动主机。
- 家乡代理做的第二件事是告诉发送方，以后再给移动主机发送分组不用发到它的家乡地址，而代之以把它隧道封装后显式地发给它当前的外部代理。就这样，随后的分组可以通过外部代理直接前往移动主机当前所在的位置，完全旁路家乡LAN的位置。

6.2 移动IP概要

- 许多Internet用户都有可携带的计算机，并且希望在远方的Internet场点时甚至在旅途中仍然能够连接到Internet。不幸的是，IP的寻址系统使得这项工作远非像说起来那么容易。
- 真正的弊病在寻址机制本身。每个IP地址都包含网络号和主机号。例如，考虑具有IP地址160.80.40.20/16的一台机器。168.80给出了网络号，40.20是主机号。在全世界的路由器都有路由表，告诉使用哪条线路到达网络168.80。每当有一个带有168.80.xx.yy形式的目的IP地址的分组到来时，它就被转发到那条线路。

6.2 移动IP概要

- 如果具有那个地址的机器突然被携带到某个远方场点，那么发送给它的分组将继续被路由到它的家乡LAN（或路由器）。该机器的所有者将再也收不到电子邮件等信息。给该机器分配一个对应新位置的新的IP地址的做法是没有吸引力的，因为必须把这种改变通知大量的人、程序和数据库。
- 另一个方法是让路由器使用全部的IP地址做路由选择，而不仅仅是网络。然而，这一策略将需要每个路由器有数以百万计的登记项，对于Internet而言，代价太大了。

6.2 移动IP概要

- 当人们开始需要把他们的笔记本计算机无论在什么地方都可以连接到Internet的时候，IETF就成立了一个工作组来寻求解决方案。该工作组很快就制定了在任何解决方案中都需要考虑的若干个目标，它们主要包括：

（1）每个移动主机必须在任何地方都能够使用它的家乡IP地址；

（2）不允许改变固定主机的软件；

（3）不允许改变路由器软件和路由表；

（4）发给移动主机的大多数分组都不应该绕道行走；

（5）当移动主机呆在家乡时不应该有额外的开销。

6.2 移动IP概要

- 所选择的解决方案跟我们在前面叙述的移动主机的路由选择相同。当有一个分组到达该用户的家乡LAN时，它进入连接到该LAN的某个路由器。路由器用通常的方式尝试定位该主机，例如通过广播一个ARP分组询问：“160.80.40.20的以太网地址是什么？”此时，家乡代理通过给出它自己的以太网地址来应答该查询。然后，路由器就把前往160.80.40.20的分组发给家乡代理。家乡代理再把收到的IP分组隧道传送给关照地址。具体的做法是把收到的分组封装在隧道IP分组的载荷域中，并把隧道分组的目标IP地址指定成外部代理的IP地址。接下来，外部代理解封隧道IP分组，取出原先的IP分组，并把它投递给移动主机的数据链路地址。此外，家乡代理还把关照地址发给源发送方，使得后续的IP分组可以由源直接隧道传送给外部代理。显然，这一解决方案满足上述所有必须条件。

6.2 移动IP概要

- 还有一个小的细节也许值得一提。在移动主机移动的时候，也许路由器已经在它的缓存中有了该主机的以太网地址（但很快就会变得无效）。将那个以太网地址用家乡代理的以太网地址取代的工作可以通过一个称作无故ARP的小技巧来完成。移动主机可以给路由器发一个未经邀请的ARP应答报文，让它用家乡代理的以太网地址替换在缓冲区中关于即将离开的移动主机的特别登记项。但该移动主机后来返回家乡的时候可以使用同样的技巧再次更新路由器的缓冲区。
- IETF对于移动主机的解决方案还解决了若干其它的问题。例如，怎样找到代理？答案是让每个代理定期地广播其地址和它愿意提供的服务类型（家乡、外部或二者兼有的代理）。当一个移动主机到达某处时，它可以监听这些称作通告的广播。另一种做法是它自己广播一个分组，宣告自己的到来，希望本地的外部代理给以应答。

6.2 移动IP概要

- 另一个问题是如何处置那些不礼貌的移动主机，它们不说再见就离开了。答案是让相关的登记项仅在一个固定长度的时间内有效。如果登记项没有被定期地刷新，就发生超时事件，外部代理可以清除相关的表项。
- 还有一个安全性问题。当家乡代理收到一个报文，请求它把所有发给张三的分组转发给某个 IP地址时，它最好不要急于这样做，除非能够证明张三确实是这个请求的源发方，以防止某个动机不良的人假扮张三的身份。可以将加密的身份验证协议用于这一目的。

6.2.1 主题

- 移动IP是在全球Internet上支持移动性的解决方案，希望它是可扩展的，强健的，安全的，允许节点在改变所连接的链路时仍能进行所有正在进行的通信。特别地，移动IP提供把IP分组路由到移动节点的机制，该机制允许移动节点使用它们的永久IP地址，但可以连接到任何场点的链路。
- 当一个源计算机要把一个分组发送到目的地计算机时，它不知道也不介意目的地计算机当前处在哪个位置，它只想把分组投递给正确的目标计算机。这是OSI第3层即网络层的功能。网络层负责动态地选择一条从分组的源到最终目的地的一条通路。在Internet中网络层协议是互连网协议，即IP。

6.2.1 主题

- 在一个复杂的网络中移动分组需要一个或多个路由协议。路由器使用路由协议交换关于Internet上各种各样的目的地和链路的位置信息。路由协议的例子包括OSPF(开放的最短通路优先协议)、RIP（路由信息协议）和BGP（边界网关协议）。
- 移动IP是Internet解决节点移动性的网络层方案。这就意味着移动IP需要在适当的节点建立路由表，使得在移动主机没有连接到家乡链路的情况下还能够把IP分组发送给它们。事实上，我们可以把移动IP看成是一种具有非常特别的目的的路由协议。移动IP的目的是允许把IP分组路由到有可能非常迅速地改变位置的移动节点。

6.2.1 主题

- 作为一个网络层协议，移动IP完全独立于它在其上运行的媒体。使用移动IP的一个移动节点从一种媒体移动到另一种媒体时不会丢失连接性。例如，移动IP允许一台笔记本计算机从一个有线以太网断连，然后再接到一个无线LAN。我们使用术语异构移动性表示移动节点可以在不同的媒体类型之间移动还能够继续通信的能力。
- 当然，移动IP也允许移动节点从一条网络链路移动到在不同位置的具有相同类型的媒体的另一条链路。相应地，我们把这种能力称作同构移动性。
- CDPD(蜂窝数字分组数据网，它是在北美模拟蜂窝电话系统中未被占用的无线频道上发送IP分组)和802.11仅提供同构移动性，它们都允许在各自的网络中移动，不可以在不同媒体的网络之间移动。移动IP的独特性在于不仅提供同构移动性，而且也提供异构移动性。

6.2.2 必要条件和设计目标

- 移动IP设计的必要条件如下：

（1）移动节点在改变了它对Internet的链路层连接点之后还能够跟其它节点通信。

在当前的Internet上采用的基于网络前缀的路由机制不能够把分组投递到没有连接到其家乡链路的节点。移动IP的特点就是要允许节点在可能连接到任何链路上的情况下还能够通信。

（2）移动节点必须能够仅使用它的家乡永久IP地址通信，而不管它当前对Internet的链路层连接点在哪里。

如果允许移动节点在其移动后改变IP地址，那会迫使它中止在老的链路上进行的所有通信（特别是接收发给老地址的信息），并在移动到新的链路上重新启动通信。而且，跟一个因移动而改变了地址的节点建立联系是困难的。因此，这个必要条件排除了任何需要改变移动节点的IP地址的解决方案。另外，一些网络服务在软件执照和访问权限方面是基于IP地址，这也需要移动节点不管是否移动仍保持它的IP地址不变。

6.2.2 必要条件和设计目标

- 移动IP设计的必要条件（续）：

（3）移动节点必须能够跟其它还没有实现移动IP移动性功能的计算机通信。

移动IP需要不改变现有的固定主机和路由器的协议，不能指望已经大量安装的IPv4主机和路由器可以升级支持移动性功能。因此，需要移动IP的实现限于移动主机本身以及少量代表它们提供特别路由服务功能的节点。

（4）除了那些在Internet上已经暴露的对固定节点的安全威胁之外，移动节点还应能够防止因实现移动性功能而引起的任何新的安全威胁。

移动计算意味着新的安全威胁，移动安全性必须考虑到这些威胁。特别地，移动IP的设计必须阻止拒绝服务类攻击。如果对于移动节点报告它当前的所在位置的报文没有身份验证，这类攻击是可能的。

6.2.2 必要条件和设计目标

- 笔记本计算机使得计算不局限于在桌面进行，但如果仅连接到有线网络仍然限制了可以使用网络的时间和地点。一些无线网络允许计算机在任何时间和任何地点进行通信。然而许多无线网络是昂贵的，或者是低速的。
- 路由协议需要在网络的各个节点之间传输路由更新信息。为了使得移动IP适合在广大范围的无线链路上使用，一个设计目标就是要使得这些更新的数量和频度尽可能地小。
- 另一个设计目标是使得它尽可能简单，以便易于移动节点软件的实现。这样可以增加潜在的能够使用移动IP的节点的数量。除了全功能的笔记本之外，这一目标对于像是手机、掌上电脑和其它个人随身设备这类存储器和处理能力受限的装置尤为重要。
- 最后，在Internet中，IPv4地址是短缺的，因此移动IP的另一个设计目标是节约使用地址的数量。在移动IP的解决方案中，不宜让移动节点使用多个地址，不宜为移动节点准备大的地址池，除非绝对需要。

6.2.3 功能实体及其驻留位置

移动IP定义了三个必须实现移动性协议的功能实体：

（1）移动节点 该节点可以把对Internet的连接从一条链路改变到另一条链路，同时保持正在进行的任何通信，并且仅使用它的永久家乡IP地址。

（2）家乡代理 该代理是跟移动节点的家乡链路有一个接口的路由器，它当移动节点改变其连接的链路时，保持被告知移动节点的当前位置，即关照地址；

在一些情况下，还要通告对移动节点的家乡地址的网络前缀的可达性，从而引来发给移动节点家乡地址的IP分组；

截获发给移动节点的家乡地址的IP分组，并把它们隧道传送到移动节点的当前位置，即关照地址。

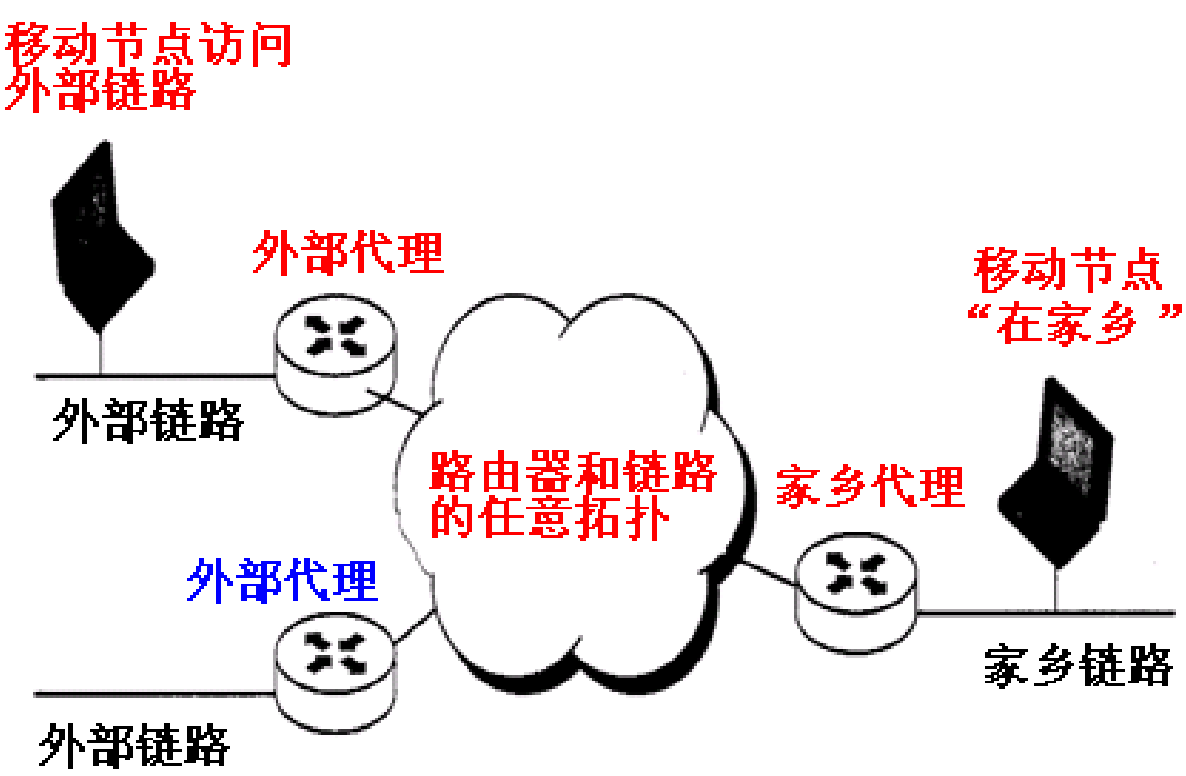
6.2.3 功能实体及其驻留位置

- 实现移动性协议的功能实体（续）：

（3）外部代理 该代理是在移动节点的外部链路上的一个路由器，它辅助移动节点通知家乡代理它当前的关照地址；提供一个关照地址，解封由家乡代理隧道传输给移动节点的分组，并递交给移动节点；为连接到这条外部链路的移动节点发送的分组担当缺省路由器的角色。

下图示出了这些实体以及它们之间的关系。

6.2.3 功能实体及其驻留位置

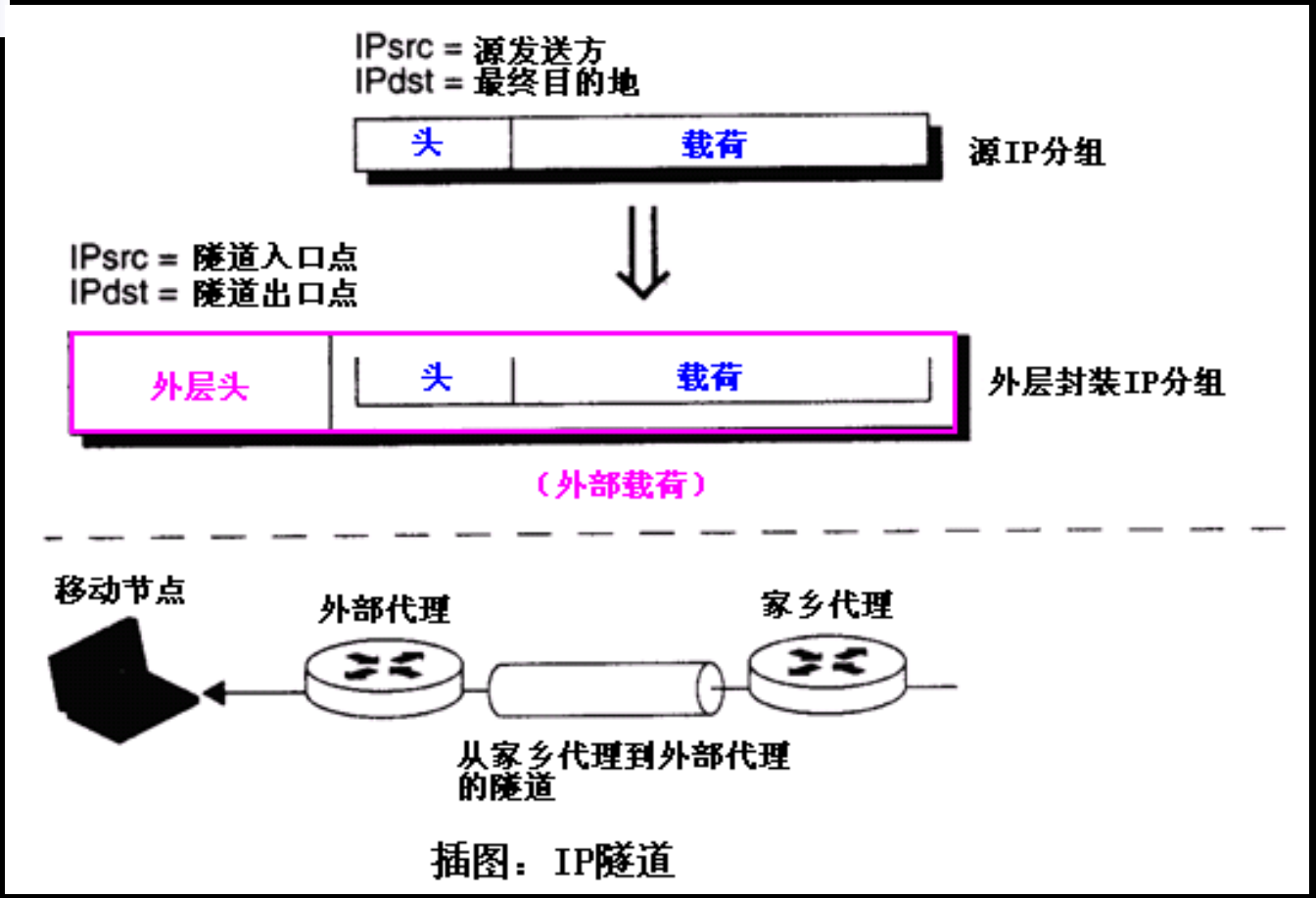


插图：移动IP实体

6.2.3 功能实体及其驻留位置

- 如下图所示，隧道是发给移动节点的IP分组行走的一段通路，此时它被分装在第二个IP分组的载荷部分。为了把一个分组投递给移动节点，家乡代理把它隧道传送到外部代理。

6.2.3 功能实体及其驻留位置



插图：IP隧道

6.2.3 功能实体及其驻留位置

- 移动节点的家乡地址跟移动节点的家乡代理紧密相关，也跟它的家乡链路紧密相关。特别地，移动节点的家乡地址的网络前缀定义了它的家乡链路。也就是说，分配给家乡链路的网络前缀和移动节点的家乡地址的网络前缀相同。移动节点的家乡代理在移动节点的家乡链路上至少有一个接口。移动节点的家乡地址是由移动节点发送的所有分组的IP源地址，也是所有发送给移动节点的分组的IP目的地址。这就需要把移动节点的家乡地址放到域名系统对应它的登记项的“IP地址”域，以便其它节点通过移动节点的主机名可以查到移动节点的家乡地址。

6.2.3 功能实体及其驻留位置

- 关照地址跟一个正在访问外部链路的移动节点相关联。关照地址具有以下属性：

（1）关照地址专用于移动节点当前正在访问的外部链路；

（2）每当刚从一条外部链路移动到另一条外部链路时，移动节点的关照地址一般都要改变；

（3）发送给关照地址的分组可以使用现有的Internet路由机制传送，也就是说，为把分组传送给关照地址，不需要移动IP特有的过程；

（4）使用关照地址作为家乡代理到移动节点方向上的隧道的出口点；

（5）在移动节点跟其它节点的会话中，关照地址几乎从不用作IP源地址或目的地址。特别地，当其它节点查询移动节点的主机名时，域名服务器永远不会返回关照地址。

6.2.4 概要工作过程

- 粗略地讲，移动IP的工作情况如下：

（1）家乡代理和外部代理在它们所连接的链路上定期地组播或广播称作代理通告的移动IP报文。

（2）移动节点倾听这些代理通告，并检查它们的内容以确定当前是连接在家乡链路还是外部链路上。当连接到家乡链路时，移动节点的操作跟固定节点相同，不使用其它移动IP的功能。下面的步骤假定移动节点发现自己是连接在外部链路上。

（3）连接到外部链路的移动节点得到一个关照地址。实际上，从外部代理的代理通告报文的某个域就可以读取外部代理关照地址。

6.2.4 概要工作过程

- 移动IP的工作情况（续）：

（4）移动节点使用移动IP定义的一个报文交换过程向家乡代理报告和登记关照地址。在这个登记过程中，移动节点需要请求外部代理提供服务。为了防止远程的拒绝服务类攻击，登记报文需要身份验证。

（5）家乡代理或者在家乡链路上的其它路由器通告移动节点的家乡地址的网络前缀的可达性，从而可以引入发给移动节点的家乡地址的那些IP分组。家乡代理采用诸如代理ARP这样的机制截获这些IP分组，然后把它们隧道传送给移动节点的关照地址。

（6）外部代理从隧道中抽出原先的IP分组，然后投递给移动节点。

（7）在相反的方向上，由移动节点发送的分组直接路由到目的地址，不需要使用隧道。外部代理为移动节点产生的所有IP分组担当路由器的角色。

6.3 代理发现

- 移动节点通过代理发现过程

*确定它当前是连接在家乡链路还是外部链路上；

*发现它已从一条外部链路移动到另一条外部链路；

*当连接到外部链路时得到关照地址。

移动节点、外部代理和家乡代理互相合作完成上述功能。

6.3 代理发现

- 代理发现包括两个简单的报文。第一个是代理通告报文，家乡代理或外部代理使用它们向移动节点宣告自己的能力。在担当家乡代理或外部代理的链路上，代理以组播或广播的形式定期发送代理通告报文。这就使得连接到链路的移动节点能够确定是否有代理存在；如果有，他们的IP地址和功能是什么。
- 第二个是代理征求报文，不想等待到下一周期才接收代理通告的移动节点就可以发送这种报文。代理征求的唯一作用就是使得在链路上的代理立即发送一个代理通告。在代理发送通告的频率太低、移动节点改变链路迅速的情况下，这类报文是有用的。
- 移动IP定义的代理征求报文格式跟ICMP路由器征求报文相同，而且必须将封装该ICMP报文的IP分组的TTL(生存时间)域置1。下图示出了代理征求报文的格式。

6.3 代理发现

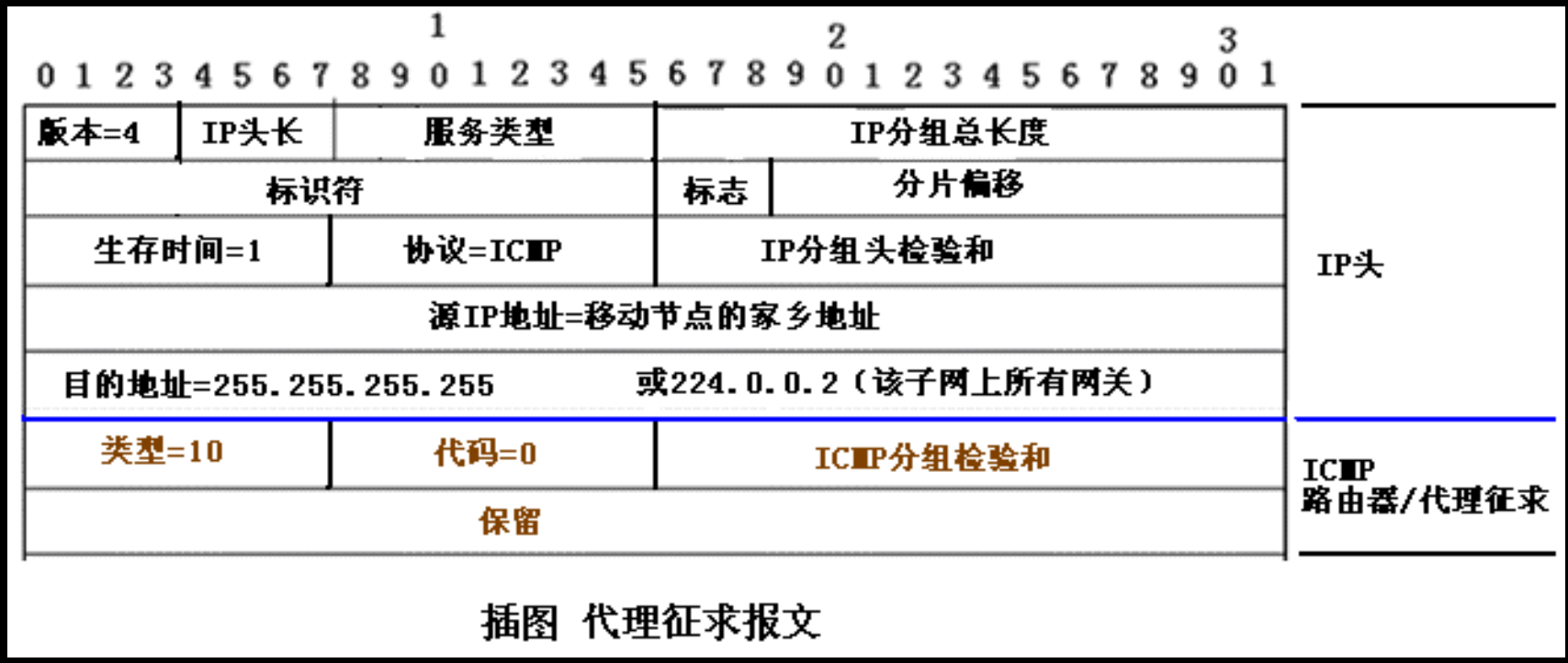


插图 代理征求报文

6.3 代理发现

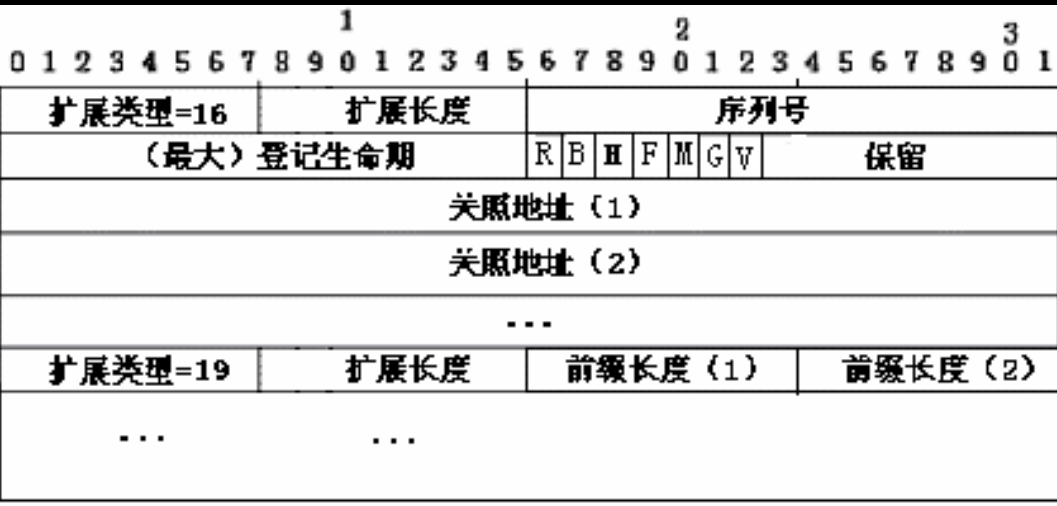
- 家乡代理或外部代理在收到一个代理征求报文后，立即发送一个代理通告报文予以响应。类型值10表示该ICMP报文是一个代理或路由器征求报文。
- 代理通告报文通过把一个或多个由移动IP定义的扩展项附加到ICMP路由器通告报文构成。如下图所示，作为代理通告，必须在报文中包括移动性代理通告扩展项。图中所示的前缀长度扩展项是可选的。

6.3 代理发现



插图　代理通告报文

6.3 代理发现



F 和 H 分别表示通告的发送方是外部代理（F）和家乡代理（H）。B 位表示外部代理太忙（B）不能接受更多的登记。R 位告诉移动节点必须通过一个外部代理做登记（R）。M 位置 1 表示家乡代理使用最小(M)头开销（简化的 IP 内外封装头）的封装，G 位置 1 表示家乡代理使用类属(G)封装（支持其它网络层协议对 IP 的封装）；它们都不采用通常的 IP 封装 IP 的封装方式。V 位置 1 表示外部代理可以支持 Van Jacobson 头压缩（发送方对 TCP 和 IP 分组头压缩，接收方解压缩，主要用于那些支持这种功能的链路，可使用低带宽链路）。

插图：代理通告报文（续）

6.3 代理发现

- 在移动IP中的扩展项都具有同样的格式，由3个域构成：

（1）类型域，区别不同种类的扩展；

（2）长度域，表示在数据域中以字节计的长度；

（3）数据域，包含从源发送到目的地的实际信息。

- 唯一的例外（特殊扩展项）是1个字节的填充扩展项，它有类型域，但没有长度和数据域，它的功能是附加到奇数长度的报文，使其变成偶数长度的报文。

6.3 代理发现

- 移动节点可以根据接收到的代理通告的IP分组头确定它是连接到家乡链路，还是连接到外部链路，这只要察看代理通告的IP分组的源地址就可以做出判断。
- 类型域的值等于9的ICMP报文是一个通告（路由器）。把代码域的值置成16可以说明这是一个移动IP代理通告，区别于一般的路由器通告。对于一般的路由器通告，此域的值是0。
- 检验和域总是用于检查收到的报文是否有错。生命期域表示代理发送通告的频度。地址数目域和地址项大小域分别说明列出了多少个路由器地址/优先级对和每对包含多少个字节。就IP地址而言，地址项大小等于8（4字节地址加上4字节优先级）。IPv6对于一个接口可以有多个地址。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/328073076010006050