IPv6自动配置和移动性

2005-2-24 16:01:06

IPv6使用两种不同机制来支持即插即用网络连接。第一种机制的示例是启动协议(BOOTP)，后来又设计了动态主机配置协议(DHCP)，允许IP节点从特殊的BOOTP服务器或DHCP服务器获取配置信息。但是这些协议支持所谓的“状态自动配置”，即服务器必须保持每个节点的状态信息，并管理这些保存的信息。不论对于为许多个人用户服务的ISP，还是雇员经常在各部门间流动的大型机构， DHCP都是IPv4网络配置的重要工具。

DHCP的问题在于，作为状态自动配置协议，它要求安装和管理DHCP服务器，并要求接受DHCP服务的每个新节点都必须在服务器上进行配置。很简单， DHCP服务器保存着它要提供配置信息的节点列表，如果节点不在列表中，该节点就无法获得IP地址。DHCP服务器还保持着使用该服务器的节点的状态，因为该服务器必须了解每个IP地址使用的时间，以及IP地址何时可以进行重新分配。状态自动配置的问题在于，用户必须保持和管理特殊的自动配置服务器以便管理所有“状态”，即所容许的连接及当前连接的相关信息。对于有足够资源来建立和保持配置服务器的机构，该系统可以接受；但是对于没有这些资源的小型机构，工作情形较差。至少对于大多数个人或小型机构，无状态自动配置是较好或较容易的解决方案。这种机制允许个人节点能够确定自己的IP配置，而不必向服务器显式请求各节点的信息。

实际上，至少在理论上且进行了某些假定的情况下，无状态自动配置规程相对容易实现。首先，如果使用IEEE EUI-64链路层地址，用户就可以确信自己的主机ID是惟一的，因此节点要完成的工作是确定自己的链路层地址并计算出EUI-64地址，然后确定自己的IPv6网络地址。向最近的路由器询问是确定网络地址的一种方法，这就是IPv6中无状态自动配置的实现方式，最后根据IPv6中的定义，状态自动配置和无状态自动配置可以共存并可一起操作。两种类型自动配置方法的合作，比单独使用其中一种更易于实现互联网络连接的即插即用。例如，使用无状态自动配置，节点可以很快确定自己的IP地址，而且一旦获得此信息，它就可以与DHCP服务器交互以获得所要求的其他网络配置值。实际上， DHCPv6很可能要依靠IPv6无状态自动配置来简化某些情况下的状态配置。如果使用无状态自动配置要简单很多，那么为什么还要使用状态自动配置呢？此问题的答案取决于构造网络的机构的要求。无状态自动配置对得到IP地址的节点提供最低程度的监视。任一节点可以连接到链路，通过路由器向能实现无状态自动配置的节点发出的通告来获知网络和子网信息，并构造有效的链路地址。但是，如果有DHCP服务器的支持，机构可以更紧密地控制网络可配置的节点。只有由网络管理员明确授权的节点才能通过DHCP服务器来配置。

RFC1971(IPv6无状态地址自动配置)中描述了IPv6的无状态自动配置。该RFC还在更新，大多数修改是对原规范的澄清或细化，例如对潜在的路由器否认服务攻击的处理方法等。无状态自动配置过程要求节点采用如下步骤：首先，进行自动配置的节点必须确定自己的链路本地地址(如IEEE EUI-64地址)；然后，必须验证该链路本地地址在链路上的惟一性；最后，节点必须确定需要配置的信息。该信息可能是节点的IP地址，或者是其他配置信息，或者两者皆有。如果需要IP地址，节点必须确定是使用无状态自动配置过程还是使用状态自动配置过程来获得。

无状态自动配置要求本地链路支持组播，而且网络接口能够发送和接收组播。完成自动配置的

节点首先将其链路本地地址(如IEEE EUI-64地址)追加到链路本地前缀之后。这样，节点就可以开始工作：它可以使用IPv6与同一网络链路上的其他节点通信，只要同一链路没有其他节点使用与之相同的EUI-64地址，该节点的IPv6地址就是可用的。但是，在使用该地址之前，节点必须先证实起始地址在本地链路是惟一的，即节点必须确定同一链路上没有其他节点使用与之相同的EUI-64地址。大多数情况下不会出现这个问题，大多数使用网络接口卡(如以太网适配器或令牌环适配器)的节点都有惟一的48位MAC地址；而对于通过点到点链路连接的节点，链路上只有一个端节点。但是，其他网络媒体可能没有惟一的M A C地址，某些网络接口卡也可能错误地使用了它们无权使用的MAC地址。此时，节点必须向它打算使用的链路本地地址发送邻居请求报文，如果得到响应，试图自动配置的节点就得知该地址已为其他节点所使用，它必须以其他方式来配置。

如果没有路由器为网络上的节点服务，即如果本地网络孤立于其他网络，则节点必须寻找配置服务器来完成其配置，否则，节点必须侦听路由器通告报文。这些报文周期性地发往所有主机的组播地址，以指明诸如网络地址和子网地址等配置信息。节点可以等待路由器的通告，也可以通过发送组播请求给所有路由器的组播地址来请求路由器发送通告。一旦收到路由器的响应，节点就可以使用响应的信息来完成自动配置。

相对IPv4而言，移动IPv6将更易于实现和使用。首先，在IPv6中，在无状态自动配置或使用DHCPv6的状态自动配置的支持下，获得关照地址的过程更加简单。正因如此， IPv6中没有外地代理关照地址，而只有配置的关照地址。其次，应该有可能使用IPv6的各种特性来改进移动节点的操作。例如，主代理可以使用邻居发现的代理通告来截获发给移动节点的IPv6包。对于通过目的地选项来将地址更新与地址相捆绑的路由优化，节点也应该有基本的支持。移动IPv6中包含的另一个新特性是：即使在移动节点的常规主代理不可达的情况下，移动节点也有能力和驻地网络建立联系。移动节点可以向驻地网络中为主代理保留的地址发送任意点播包，结果任何可用的主代理将把自己的选项通知移动节点。

四、IPv6的身份验证和安全性

在IPv6中通过身份验证头(AH)和封装安全性净荷(ESP)头来实现身份验证和安全性，包括安全密码传输、加密和数据包的数字签名。IP层安全性用于保护IP数据报，它不一定要涉及用户或应用，这意味着用户可以愉快地使用应用程序，而无需注意所有的数据报在发送到Internet之前，需要进行加密或身份验证，当然在这种情形下所有的加密数据报都要由另一端的主机正确地解密。

这样就引入了如何实现IPsec的问题，有如下三种可能的方法：

将IPsec作为IPv4栈或IPv6栈的一部分来实现。这种方法将IP安全性支持引入IP网络栈，并且作为任何IP实现的一个必备部分。但是，这种方法也要求对整个实体栈进行更新以反映上述改变。

将IPsec作为“栈中的一块”(BITS)来实现。这种方法将特殊的IPsec代码插入到网络栈中，在现有IP网络软件之下、本地链路软件之上。换言之，这种方法通过一段软件来实现安全性，该软件截获从现有IP栈向本地链路层接口传送的数据报，对这些数据报进行必要的安全性处理，然后再交给链路层。这种方法可用于将现有系统升级为支持IPsec的系统，且不要求重写原有的IP栈软件。

将IPsec作为“线路的一块”(BITW)来实现。这种方法使用外部加密硬件来执行安全性处理功能。该硬件设备通常是作为一种路由器使用的IP设备，或者更确切一些，是安全性网关，此网关为位于它后面的所有系统发送的IP数据报服务。如果这样的设备只用于一个主机，其工作情况与BITS方法类似，但如果一个BITW设备为多个系统服务，实现相对要复杂得多。

上述各种方法的差别不在于字面上，而在于它们的适用情况不同。要求高级别安全性的应用最好使用硬件方法实现；而如果系统不具备与新的IPsec兼容的网络栈，应用最好选择BITS方法。

IPsec安全性服务完全通过AH和封装安全性净荷(ESP)头相结合的机制来提供，当然还要有正确的相关密钥管理协议。RFC1826(IP身份验证头)中对AH进行了描述，而ESP头在RFC 1827(IP封装安全性净荷)中描述。上述RFC及IP安全性体系结构RFC仅仅是解决安全性问题的第一步。IPsec工作组各成员正继续对这些扩展头的规范进行改进，这些文档的当前草案的篇幅几乎是原RFC的两倍。这些草案保留了原RFC的语言和意图，并进行了扩充，对包头及其功能的描述更加完整，综合性更强。

各安全性头可以单独使用，也可以一起使用。如果一起使用多个扩展头， AH应置于ESP头之前，这样，首先进行身份验证，然后再对ESP头净荷解密。使用IPsec隧道时，这些扩展头也可以嵌套。即，源节点对IP包进行加密和数字签名，然后发送给本地安全性网关，该网关则再次进行加密和数字签名，然后发送给另一个安全性网关。

AH和ESP头既可以用于IPv4，也可以用于IPv6，这一点很重要。AH的作用如下：

为IP数据报提供强大的完整性服务，这意味着AH可用于为IP数据报承载内容验证数据。

为IP数据报提供强大的身份验证，这意味着AH可用于将实体与数据报内容相链接。

如果在完整性服务中使用了公共密钥数字签名算法，AH可以为IP数据报提供不可抵赖服务。

通过使用顺序号字段来防止重放攻击。

AH可以在隧道模式或透明模式下使用，这意味着它既可用于为两个节点间的简单直接的数据报传送提供身份验证和保护，也可用于对发给安全性网关或由安全性网关发出的整个数据报流进行封装。

IPv6中的AH与其他扩展头一起使用时，必须置于那些将由中间路由器处理的扩展头之后，及那些只能由数据报目的地处理的扩展头之前。这意味着AH应置于逐跳扩展头、选路扩展头或分段扩展头之后。根据不同情况，AH可在目的地选项扩展头之前，也可在其后。在透明模式中，AH保护初始IP数据报的净荷，也保护在逐跳转发中不变化的部分IP头，如跳极限字段或选路扩展头。

对于目的IP地址和扩展头，仅在逐跳转发它们不发生变化的情况下，才能得到保护。当AH用于隧道模式中时，使用方法与上不同。初始的目的IP地址与整个初始IP数据报一起，封装在全新的IP数据报中，该数据报再发送到安全性网关。因此，整个初始IP数据报以及传送中不变的封装IP头部分都得以保护。AH的格式和各字段，与所有的IPv6扩展头一样，第一个字段是8位的下一个头字段，它表示后续的扩展头协议。其他字段包括：

净荷长度。此8位字段指明AH的整个长度，其值以32位字为单位，并减去2。正如初始的定义，AH包含64位，其余部分为身份验证数据。因此净荷长度字段只指出身份验证数据以32位字为单位的长度，加入序列号字段后，此值等于身份验证数据加上序列号字段的长度。

保留。净荷长度字段之后的16位为将来使用而保留。目前，此16位必须全部置为0。

安全性参数索引(SPI)。此32位字段是一个任意数。与目的IP地址和安全性协议一起使用，SPI是AH使用的SA的惟一标识。若SPI值为0，则表示只用于本地而不予传送；值1 至 255被Internet分配号码授权机构(IANA)保留作将来使用。

序列号。此32位字段是一个必备的计数器，由发送者插入IP头，但不一定由接收者使用。从0开始，每发送一个数据报，该计数器增1，这可用于预防重放攻击。若接收者使用此字段来对抗重放攻击，对于序列号与已收到的数据报相同的数据报，接收者将予以丢弃。这意味着若计数器重新开始循环，即已经接收到232个数据报，则必须协商新的SA。否则，一旦计数器重新置位，接收系统将丢弃所有的数据报。

身份验证数据。此字段包含完整性检查值(ICV)，这是AH的核心。其内容的长度必须是32位的整数倍，为满足这个条件，其中可能包含填充字段。对于如何计算ICV以及使用什么机制来计算，RFC1826的描述比较模糊。实际上，术语“完整性检查值”在该文档中并没有出现，而是出现在将要代替RFC1826的后续草案中。预期适当的身份验证算法将导致ICV的产生。建议的算法包括：

报文身份验证代码(MAC)，然后对其结果用适当的对称加密算法(如DES)进行加密。

安全散列功能，如MD5或SHA的更新版SHA-1。按照标准的约定，预计AH的任何实现将必须支持MD5和SHA-1密钥散列。

身份验证数据针对整个IP数据报净荷以及IP头的不变部分或可预测部分来计算。ESP头被用于允许IP节点发送和接收净荷经过加密的数据报。更确切一点， ESP头是为了提供几种不同的服务，其中某些服务与AH有所重叠。ESP头提供的服务包括：

通过加密提供数据报的机密性。

通过使用公共密钥加密对数据来源进行身份验证。

通过由AH提供的序列号机制提供对抗重放服务。

通过使用安全性网关来提供有限的业务流机密性。

ESP头可以和AH结合使用。实际上，如果ESP头不使用身份验证的机制，建议将AH和ESP头一起使用。

ESP头必须跟随在去往目的节点所途经的中间节点需要处理的扩展头之后， ESP头之后的数据都可能被加密。实际上，加密的净荷是作为ESP头的最后一个字段。与AH类似，ESP既可用于隧道模式，也可用于透明模式。在透明模式中，如果有AH，IP头以及逐跳扩展头、选路扩展头或分段扩展头都在AH之前，其后跟随ESP头。任何目的地选项头可以在ESP头之前，也可以在ESP头之后，或者ESP头前后都有，而ESP头之后的扩展头将被加密。

在很多方面，仅仅是常规数据报带着加密净荷从源端传送到目的端。某些情况下，适合在透明模式中使用ESP。但是，这种模式使攻击者有可能研究两个节点之间的业务流，留意正在通信的节点、节点之间交换的数据量、交换的时间等。所有这些信息都可能为攻击者提供有助于对通信双方

进行攻击的信息。

类似前面描述的AH的情形，使用安全性网关是一种替代方法。安全性网关可以直接与节点连接，也可以链接到另一个安全性网关。单个节点可以在隧道模式中使用ESP，即加密所有出境包，并封装到单独的IP数据报流中，再发送给安全性网关。然后网关解密业务流，并重新将原始IP数据报发往目的地。使用隧道模式时， ESP头对整个IP数据报进行封装，并作为IP头的扩展将数据报定向到安全性网关。ESP头与AH的结合也有几种不同方式，例如以隧道方法传送的数据报可能有透明模式的AH。

ESP头与其他扩展头不同。其一，下一个头字段的位置接近ESP头的末端。其二，ESP头之前的扩展头将其下一个头字段值置为50，以指明随后是ESP头。ESP头的其余部分将可能包括如下字段：

安全性参数索引(SPI)。与上节提到的AH中的32位SPI值相同。通信节点使用该值来指出SA，SA用于确定数据应如何加密。

序列号。32位，从0开始，每发送一个数据报，该值加1。如前所述，序列号可用于防御重放攻击，在循环用完所有232个值之前，必须建立新的SA。

净荷数据。此字段长度可变，它实际上包含数据报的加密部分以及加密算法需要的补充数据，例如初始化数据。

填充。头的加密部分(净荷)必须在正确的边界终止，因此有时需要填充。

填充长度。此字段指明净荷数据所需要填充的数据量。

下一个头：此字段像其他IPv6扩展头中的字段一样操作，但是它不位于扩展头的开始，而是靠近扩展头末端。

身份验证数据。此字段是一个ICV，它对除身份验证数据本身之外的整个ESP头进行计算。这种身份验证计算是可选的。

预计一个兼容的ESP实现至少要求支持DES加密和SHA-1身份验证。它也可以支持他算法，但支持上述两个算法是最低要求。

上一篇　下一篇