虚拟专用网 VPN

虚拟专用网 VPN

由于 IP 地址的紧缺，一个机构能够申请到的IP地址数往往远小于本机构所拥有的主机数。

考虑到互联网并不很安全，一个机构内也并不需要把所有的主机接入到外部的互联网。

假定在一个机构内部的计算机通信也是采用 TCP/IP 协议，那么从原则上讲，对于这些仅在机构内部使用的计算机就可以由本机构自行分配其 IP 地址。

本地地址与全球地址

专用地址（本地地址）——仅在机构内部使用的 IP 地址，可以由本机构自行分配，而不需要向互联网的管理机构申请。

全球地址——全球唯一的 IP 地址，必须向互联网的管理机构申请。

本地地址与全球地址

问题：在内部使用的本地地址就有可能和互联网中某个 IP 地址重合，这样就会出现地址的二义性问题。

解决：RFC 1918指明了一些专用地址 (private address)。

专用地址只能用作本地地址而不能用作全球地址。

在互联网中的所有路由器，对目的地址是专用地址的数据报一律不进行转发。

RFC 1918 指明的专用 IP 地址

三个专用 IP 地址块：

(1) 10.0.0.0 到 10.255.255.255

A类，或记为10.0.0.0/8，它又称为24位块

(2) 172.16.0.0 到 172.31.255.255

B类，或记为172.16.0.0/12，它又称为20位块

(3) 192.168.0.0 到 192.168.255.255

C类，或记为192.168.0.0/16，它又称为16位块

虚拟专用网 VPN

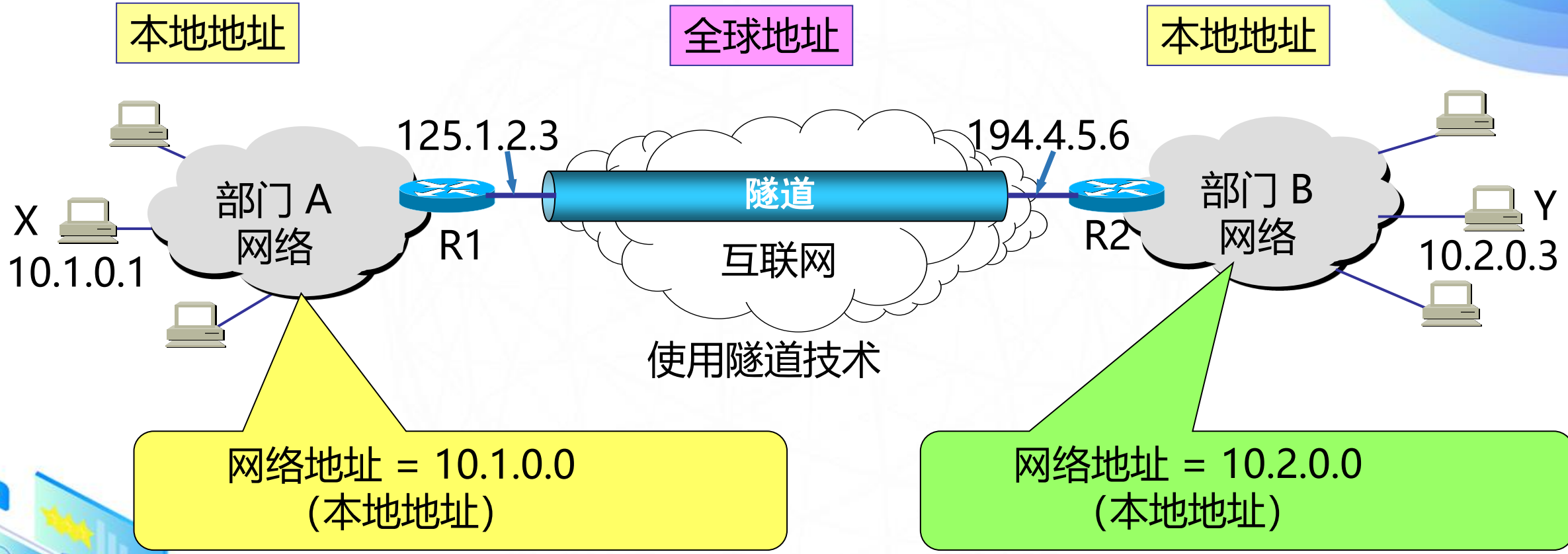
利用公用的互联网作为本机构各专用网之间的通信载体，这样的专用网又称为虚拟专用网VPN (Virtual Private Network)。

虚拟专用网 VPN 构建

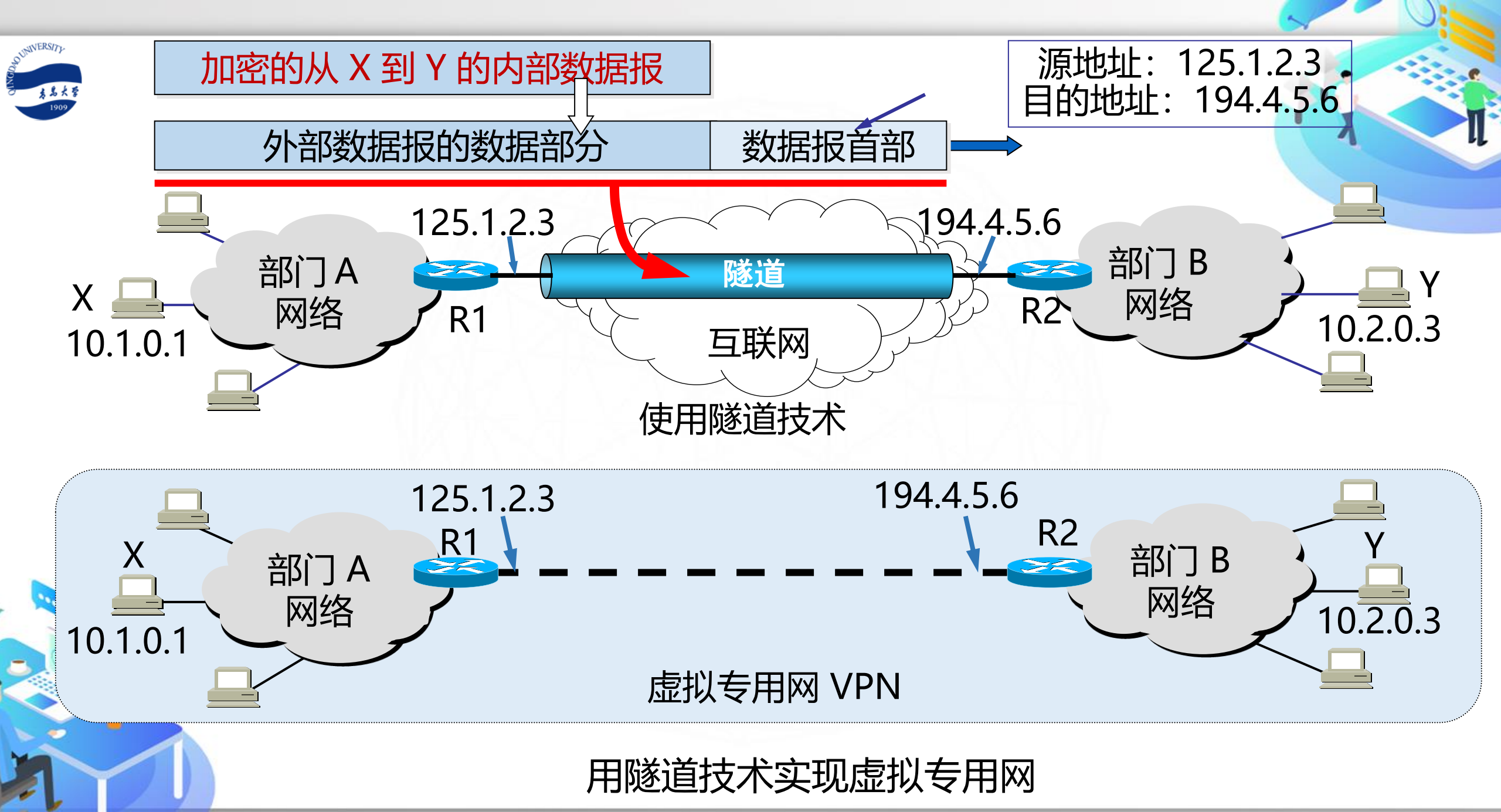
如果专用网不同网点之间的通信必须经过公用的互联网，但又有保密的要求，那么所有通过互联网传送的数据都必须加密。

一个机构要构建自己的 VPN 就必须为它的每一个场所购买专门的硬件和软件，并进行配置，使每一个场所的 VPN 系统都知道其他场所的地址。

用隧道技术实现虚拟专用网



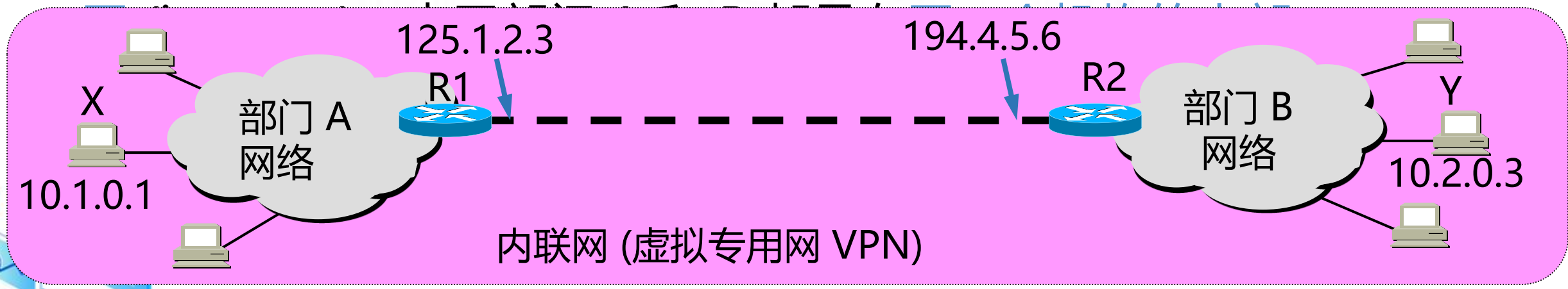
隧道技术


加密的从 X 到 Y 的内部数据报
外部数据报的数据部分
数据报首部
源地址：125.1.2.3
目的地址：194.4.5.6
125.1.2.3
194.4.5.6
部门 A
网络
部门 B
网络
隧道
互联网
R1
R2
X
10.1.0.1
Y
10.2.0.3
使用隧道技术
125.1.2.3
194.4.5.6
R1
R2
X
10.1.0.1
部门 A
网络
部门 B
网络
Y
10.2.0.3
虚拟专用网 VPN
用隧道技术实现虚拟专用网

内联网 intranet 和外联网 extranet

它们都是基于 TCP/IP 协议的。

由部门 A 和 B 的内部网络所构成的虚拟专用网 VPN 又称为内联



远程接入 VPN

远程接入 VPN (remote access VPN)可以满足外部流动员工访问公司网络的需求。

在外地工作的员工拨号接入互联网，而驻留在员工 PC 机中的 VPN 软件可在员工的 PC 机和公司的主机之间建立 VPN 隧道，因而外地员工与公司通信的内容是保密的，员工们感到好像就是使用公司内部的本地网络。