

同维电子有限公司 测试部	拟 制 人	时 间
	朱世旺	2010/8/21

文档摘要:

用于指导新入职测试人员测试 ALG。

关键字:

ALG

缩略语:

正文:

ALG 测试指导书

1.ALG-FTP

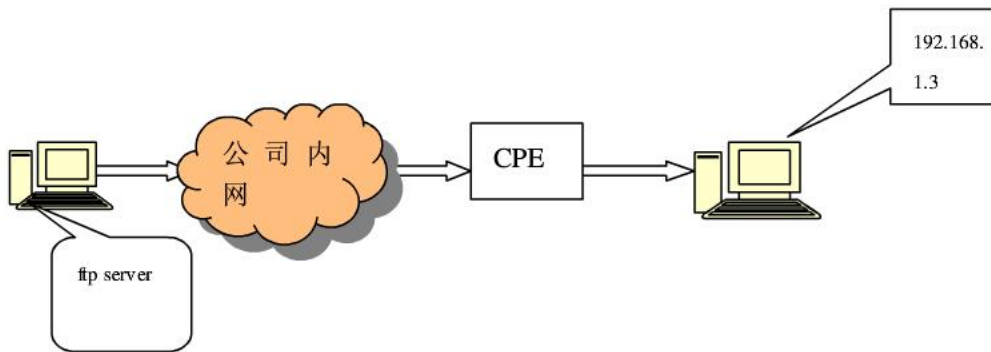
FTP 的的数据连接工作模式有主动 (PORT) 和被动 (PASV) 两种。访问 WAN 侧 FTP 服务器时, 控制主动模式下的 FTP, 访问 LAN 侧虚拟主机 (FTP 服务器) 时, 控制被动模式下的 FTP。测试步骤如后面所述。

先了解主动和被动模式的工作:

主动模式: 1) 建立控制链路: Client 端向 Server 的 FTP 端口 (默认 21) 发起连接请求, 服务器接受后建立一条控制链路。2) 当需要传输数据时, 客户端在控制链路上用 PORT 命令告诉服务器 “我打开了 xx 端口, 你来连我”, 于是服务器向客户端的 xx 端口发送连接请求, 建立一条数据链路来传送数据。

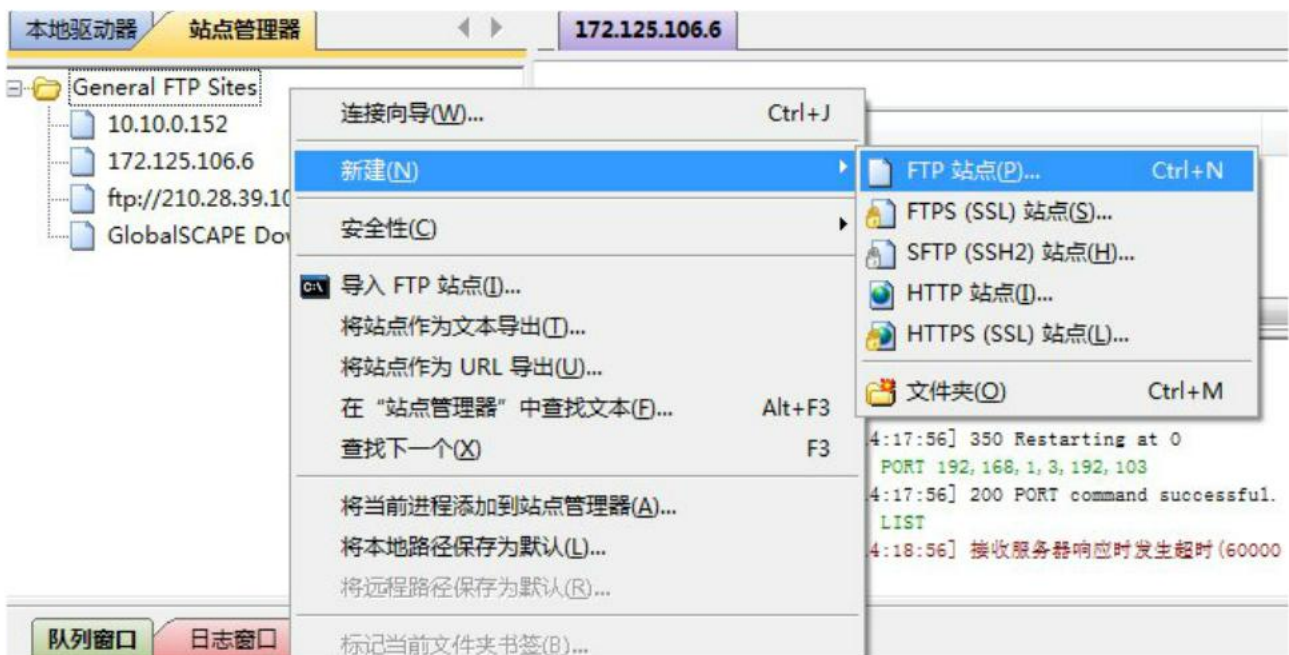
被动模式: 1) 建立控制链路: Client 端向 Server 的 FTP 端口 (默认 21) 发起连接请求, 服务器接受后建立一条控制链路。2) 当需要传输数据时, 客户端告诉服务器 “我要用 PASV 模式和你传输数据, 请打开一个端口”, 然后服务器在命令链路上用 PASV 命令回答客户端: “我已经打开了 xx 端口, 你可以过来连接我了”, 最后客户端向服务器的 xx 端口发送连接请求, 建立一条数据链路来传送数据。

1.1 LAN 侧客户端主动方式



用于测试 LAN 侧 FTP 客户端和 WAN 侧 FTP 服务器之间的传输数据，在这种方式下，ALG-FTP 开关影响数据传输链接的建立。

- 1) CPE 上创建一条路由方式的 WAN 连接，LAN 侧 PC 可以 ping 通 FTP 服务器，在 CPE 页面关闭 ALG-FTP 功能；
- 2) LAN 侧 PC 用 FTP 工具连接 FTP 服务器，使用主动模式。用 CuteFTP 工具如下所示：
在【站点管理器】界面右键选择【新建】 -> 【FTP 站点】，或 Ctrl+N:



在站点属性的【常规】页面里输入 FTP 服务地址和用户名密码，在【类型】页面的[数据连接类型]里选择“使用 PORT”：

常规	类型	动作	选项
协议类型 (P): FTP (标准文件传输协议)		端口 (O): 21	
协议类型注释 这将为命令和数据处理以非安全的 (纯文本) 方式使用工业标准的 FTP 协议。			
服务器类型 (S): Auto-detect		密码保护 <input checked="" type="radio"/> 不加密 (N) <input type="radio"/> MD4 <input type="radio"/> MD5 <input type="radio"/> 自动检测 OTP (A)	
数据连接类型 (D): 使用 PASV 使用全局设置 使用 PORT 使用 PASV 使用 EPRT 使用 EPSV 无时差		<input type="checkbox"/> 自动检测 (U)	

从客户端来看，无法显示 FTP 服务器的文件，实际是不能够建立数据传输的链接，抓到的数据包如下：



Clo_FTP_POST.pc
ap

3) 开启 ALG-FTP 功能，其他所有配置都不变，LAN 侧 FTP 客户端能够与 WAN 侧 FTP 服务器创建数据连接，能够正常传输数据：

常规	类型	动作	选项
协议类型 (P): FTP (标准文件传输协议)		端口 (O): 21	
协议类型注释 这将为命令和数据处理以非安全的 (纯文本) 方式使用工业标准的 FTP 协议。			
服务器类型 (S): Auto-detect		密码保护 <input checked="" type="radio"/> 不加密 (N) <input type="radio"/> MD4 <input type="radio"/> MD5 <input type="radio"/> 自动检测 OTP (A)	
数据连接类型 (D): 使用 PASV 使用全局设置 使用 PORT 使用 PASV 使用 EPRT 使用 EPSV 无时差		<input type="checkbox"/> 自动检测 (U)	

抓包如下：

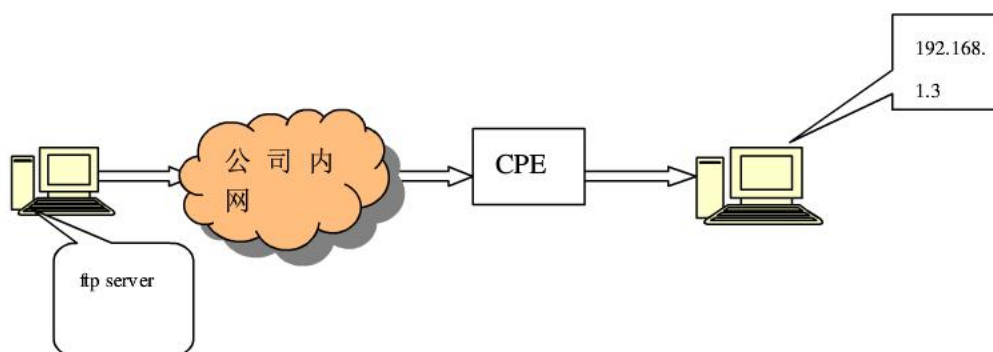
34	35.883276	192.168.1.3	172.125.106.6	21	FTP	Request: CWD /anonymous/D
35	35.950736	172.125.106.6	192.168.1.3	49893	FTP	Response: 250 CWD command successful.
36	36.001298	192.168.1.3	172.125.106.6	21	FTP	Request: PORT 192,168,1,3,194,231
37	36.075603	172.125.106.6	192.168.1.3	49893	FTP	Response: 200 PORT command successful.
38	36.113643	192.168.1.3	172.125.106.6	21	FTP	Request: LIST
39	36.201287	172.125.106.6	192.168.1.3	49895	TCP	drmsfsd > 49895 [SYN] Seq=0 win=65535 Len=
40	36.201490	192.168.1.3	172.125.106.6	4098	TCP	49895 > drmsfsd [SYN, ACK] Seq=0 Ack=1 win=
41	36.232569	172.125.106.6	192.168.1.3	49895	TCP	drmsfsd > 49895 [ACK] Seq=1 Ack=1 win=6553
42	36.261846	172.125.106.6	192.168.1.3	49893	FTP	Response: 150 opening connection for trans
43	36.288436	172.125.106.6	192.168.1.3	49895	TCP	drmsfsd > 49895 [ACK] Seq=1 Ack=1 win=6553
44	36.289361	172.125.106.6	192.168.1.3	49895	TCP	drmsfsd > 49895 [PSH, ACK] Seq=1427 Ack=1
45	36.289427	192.168.1.3	172.125.106.6	4098	TCP	49895 > drmsfsd [ACK] Seq=1 Ack=2716 win=6
46	36.289456	172.125.106.6	192.168.1.3	49895	TCP	drmsfsd > 49895 [FIN, ACK] Seq=2716 Ack=1
47	36.289485	192.168.1.3	172.125.106.6	4098	TCP	49895 > drmsfsd [ACK] Seq=1 Ack=2717 win=6
48	36.300489	192.168.1.3	172.125.106.6	4098	TCP	49895 > drmsfsd [FIN, ACK] Seq=1 Ack=2717

Frame 36: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
 Ethernet II, Src: Dell_22:19:8e (00:1a:a0:22:19:8e), Dst: 00:74:04:05:20:35 (00:74:04:05:20:35)
 Internet Protocol, Src: 192.168.1.3 (192.168.1.3), Dst: 172.125.106.6 (172.125.106.6)
 Transmission Control Protocol, Src Port: 49893 (49893), Dst Port: ftp (21), Seq: 121, Ack: 344, Len: 26
 File Transfer Protocol (FTP)
 PORT 192,168,1,3,194,231\r\n
 Request command: PORT 模式为PORT
 Request arg: 192,168,1,3,194,231
 Active IP address: 192.168.1.3 (192.168.1.3)
 Active port: 49895 打开端口49895



op_FTP_POST.pcap
p

1.2 LAN 侧客户端被动模式



LAN 侧客户端和 WAN 侧 FTP 服务器之间传输数据时的测试，ALG 开关不能影响这种模式，所以无论 ALG-FTP 是否开关，数据传输都能够正常进行。

当客户端以被动方式连接时，步骤如下：

1) 在主动方式的基础是，修改客户端 FTP 的工作模式为被动模式，关闭 ALG-FTP，如下所示的用 CuteFTP：



2) 客户端与服务器之间能够正常传输数据，通过手抓包可以看到使用被动模式：

51	21.945779	192.168.1.3	172.125.106.6	21	FTP	Request: TYPE I
52	21.988716	172.125.106.6	192.168.1.3	52067	FTP	Response: 200 Type set to I
53	22.058868	192.168.1.3	172.125.106.6	21	FTP	Request: PASV
54	22.125074	172.125.106.6	192.168.1.3	52067	FTP	Response: 227 Entering Passive Mode (172,125,106,6,12,29)
55	22.132970	192.168.1.3	172.125.106.6	21	FTP	Request: RETR \327\242\262\341\327\245\260\374.pcap
56	22.150463	192.168.1.3	172.125.106.6	3101	TCP	52070 > hp-pxpib [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=2
57	22.190593	172.125.106.6	192.168.1.3	52070	TCP	hp-pxpib > 52070 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MS
58	22.190729	192.168.1.3	172.125.106.6	3101	TCP	52070 > hp-pxpib [ACK] Seq=1 Ack=1 win=66976 Len=0
59	22.261647	172.125.106.6	192.168.1.3	52067	FTP	Response: 150 opening connection for transfer.
60	22.261650	172.125.106.6	192.168.1.3	52070	FTP-DATA	FTP Data: 1426 bytes
61	22.261651	172.125.106.6	192.168.1.3	52070	FTP-DATA	FTP Data: 1426 bytes
62	22.261790	192.168.1.3	172.125.106.6	3101	TCP	52070 > hp-pxpib [ACK] Seq=1 Ack=2853 win=66976 Len=0
63	22.309493	172.125.106.6	192.168.1.3	52070	FTP-DATA	FTP Data: 1426 bytes
64	22.309497	172.125.106.6	192.168.1.3	52070	FTP-DATA	FTP Data: 1426 bytes
65	22.309500	172.125.106.6	192.168.1.3	52070	FTP-DATA	FTP Data: 1426 bytes
66	22.309664	192.168.1.3	172.125.106.6	3101	TCP	52070 > hp-pxpib [ACK] Seq=1 Ack=7131 win=66976 Len=0
67	22.348608	172.125.106.6	192.168.1.3	52070	FTP-DATA	FTP Data: 1062 bytes

Frame 54: 103 bytes on wire (824 bits), 103 bytes captured (824 bits)
Ethernet II, Src: 00:74:04:05:20:35 (00:74:04:05:20:35), Dst: Dell_22:19:8e (00:1a:a0:22:19:8e)
Internet Protocol, Src: 172.125.106.6 (172.125.106.6), Dst: 192.168.1.3 (192.168.1.3)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 52067 (52067), Seq: 493, Ack: 127, Len: 49
File Transfer Protocol (FTP)
227 Entering Passive Mode (172,125,106,6,12,29)\r\n
Response code: Entering Passive Mode (227)
Response arg: Entering Passive Mode (172,125,106,6,12,29)
Passive IP address: 172.125.106.6 (172.125.106.6)
Passive port: 3101

第 53 个包：客户端向服务器请求使用 PASV 模式传输数据。

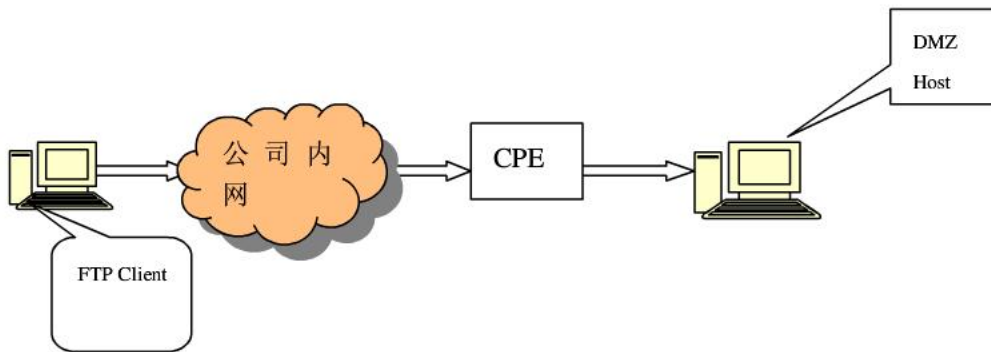
从第 54 个包可以看出，服务器打开的数据传输端口为 3101，后面传输数据时所用的服务器端口也确实是 3101。



Clo_FTP_PASV.pcap
ap

3) 开启 CPE 上的 ALG-FTP，其他配置不变，测试结果同关闭 ALG-FTP。

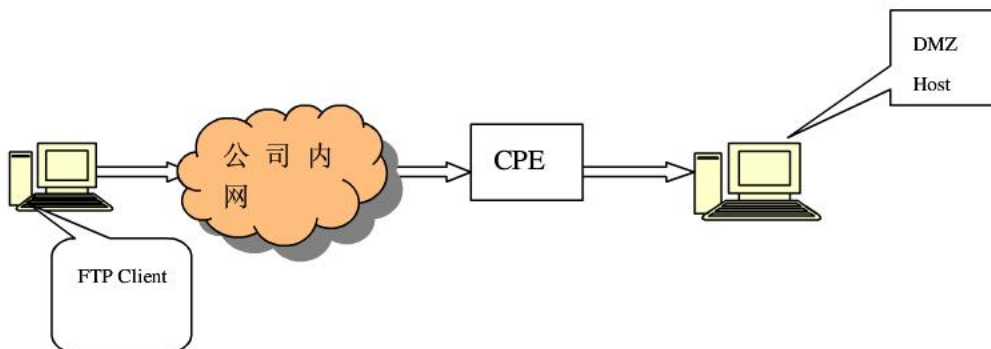
1.3 WAN 侧客户端主动方式



LAN 侧 FTP 服务器和 WAN 侧客户端之间传输数据时的测试，在这种模式下，无论 ALG-FTP 是否开关，客户端是服务器之间都可以正常传输数据。

- 1) CPE 上创建一条路由方式的 WAN 连接，开启 DMZ (DMZ 主机为 LAN 侧 PC, IP 如 192.168.1.3), DMZ 主机上搭建一 FTP 服务。
- 2) 关闭 CPE 的 ALG-FTP 功能，LAN 侧的 DMZ 主机能够 ping 通 WAN 侧的 PC2 (作为 FTP 的客户端)。
- 3) PC2 上用 FTP 工作访问 CPE 的 WAN 口 IP，工作模式为主动，同 1.1.1 中的配置。
- 4) PC2 能够访问 LAN 侧 DMZ 主机的 FTP 服务器，同 1.1.2 中的数据包。
- 5) 开启 CPE 的上 ALG-FTP，其他配置不变，结果同关闭 LG-FTP

1.4 WAN 侧客户端被动方式



LAN 侧 FTP 服务器和 WAN 侧客户端之间传输数据时的测试。

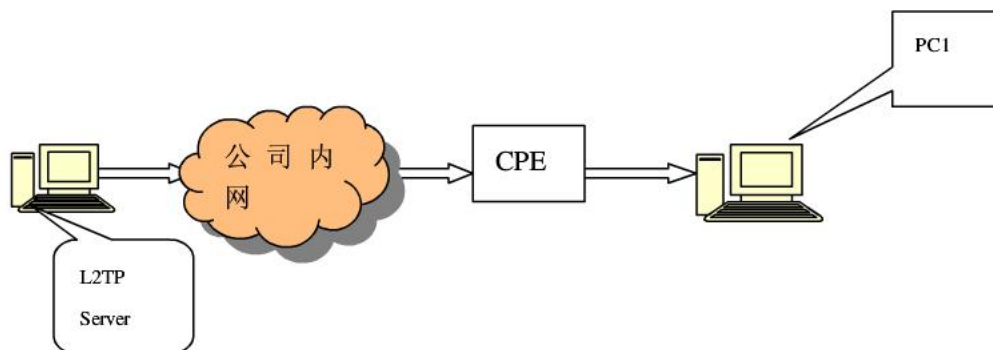
- 1) CPE 上创建一条路由方式的 WAN 连接，开启 DMZ (DMZ 主机为 LAN 侧 PC, IP 如 192.168.1.3), DMZ 主机上搭建一 FTP 服务器。
- 2) 关闭 CPE 的 ALG-FTP 功能，LAN 侧的 DMZ 主机能够 ping 通 WAN 侧的 PC2 (作为 FTP 的客户端)。
- 3) PC2 上用 FTP 客户端工具访问 CPE 的 WAN 口 IP，工作模式为被动。结果不能访问。
- 4) 开启 CPE 的 ALG-FTP，其他所有配置都不变，客户端和服务器之间可以传输数据，如下是在服务器抓到的包，与 1.2 中类似：

15	0.404100	172.125.106.6	192.168.1.3	21	FTP	Request: TYPE I
16	0.434022	192.168.1.3	172.125.106.6	2345	FTP	Response: 200 Type set to I
17	0.467171	172.125.106.6	192.168.1.3	21	FTP	Request: PASV
18	0.497203	192.168.1.3	172.125.106.6	2345	FTP	Response: 227 Entering Passive Mode (192,168,1,3,195,83)
19	0.532968	172.125.106.6	192.168.1.3	21	FTP	Request: LIST
20	0.533913	172.125.106.6	192.168.1.3	50003	TCP	madcap > 50003 [SYN] Seq=0 Win=65535 Len=0 MSS=1456 W5=2
21	0.534086	192.168.1.3	172.125.106.6	2535	TCP	50003 > madcap [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=
22	0.566691	172.125.106.6	192.168.1.3	50003	TCP	madcap > 50003 [ACK] Seq=1 Ack=1 win=131072 Len=0
23	0.618864	192.168.1.3	172.125.106.6	2345	FTP	Response: 150 Opening connection for transfer.
24	0.621071	192.168.1.3	172.125.106.6	2535	FTP-DATA	FTP Data: 218 bytes
25	0.621154	192.168.1.3	172.125.106.6	2535	TCP	50003 > madcap [FIN, ACK] Seq=219 Ack=1 win=66816 Len=0
26	0.663294	172.125.106.6	192.168.1.3	50003	TCP	madcap > 50003 [ACK] Seq=1 Ack=220 win=130852 Len=0
27	0.663390	172.125.106.6	192.168.1.3	50003	TCP	madcap > 50003 [FIN, ACK] Seq=1 Ack=220 win=130852 Len=0
28	0.663442	192.168.1.3	172.125.106.6	2535	TCP	50003 > madcap [ACK] Seq=220 Ack=2 win=66816 Len=0
29	0.705277	172.125.106.6	192.168.1.3	21	FTP	dbm > ftp [ACK] Seq=75 Ack=205 Win=65535 Len=0
!!!						
Frame 18: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)						
Ethernet II, Src: Dell_22:19:8e (00:1a:a0:22:19:8e), Dst: 00:74:04:05:20:35 (00:74:04:05:20:35)						
Internet Protocol, Src: 192.168.1.3 (192.168.1.3), Dst: 172.125.106.6 (172.125.106.6)						
Transmission Control Protocol, Src Port: ftp (21), Dst Port: dbm (2345), Seq: 219, Ack: 69, Len: 48						
File Transfer Protocol (FTP)						
227 Entering Passive Mode (192,168,1,3,195,83)\r\n						
Response code: Entering Passive Mode (227) 使用PASV模式						
Response arg: Entering Passive Mode (192,168,1,3,195,83)						
Passive IP address: 192.168.1.3 (192.168.1.3)						
Passive port: 50003 打开了50003端口						
之后的数据传输使用打开的端口						

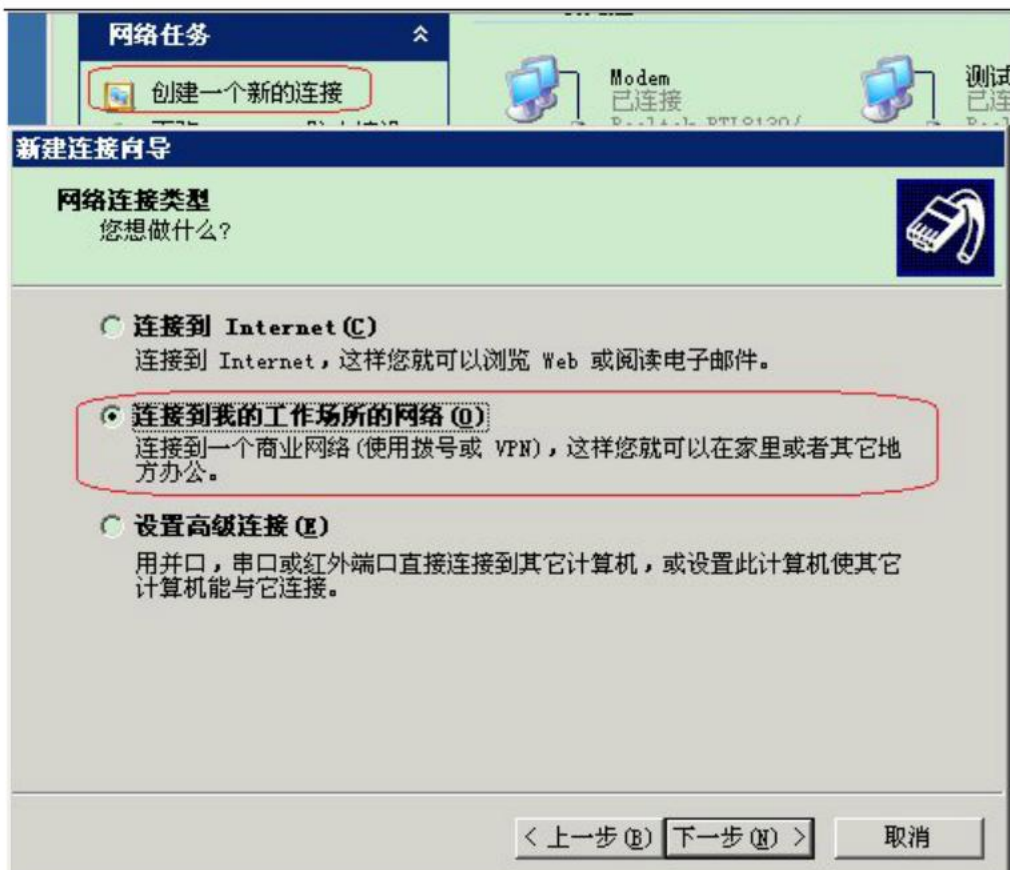


op_FTP_PASV_WA
N.pcap

2.ALG-L2TP



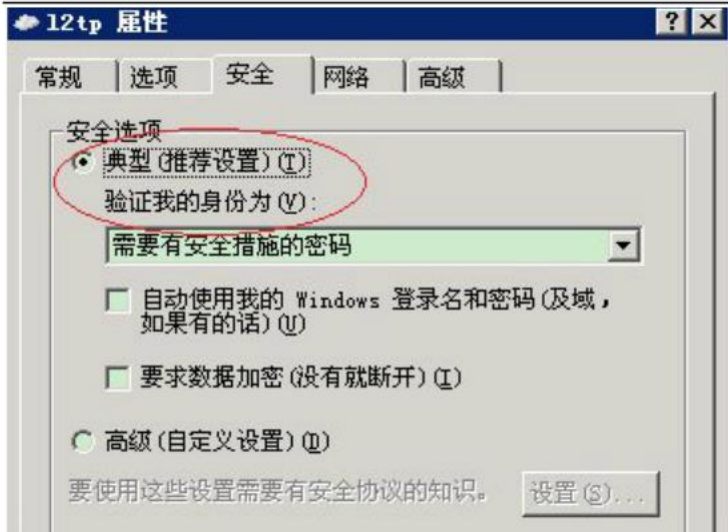
1) 配置 L2TP 拨号连接 (LAN 侧 PC: 假定 PC1), 如下步骤在 Windows 2003 中进行, 其他系统类似:
在“网路连接”里选择“新建一条新的连接”, 点击下一步后选择“连接到我的工作场所的网络”, 如下所示:



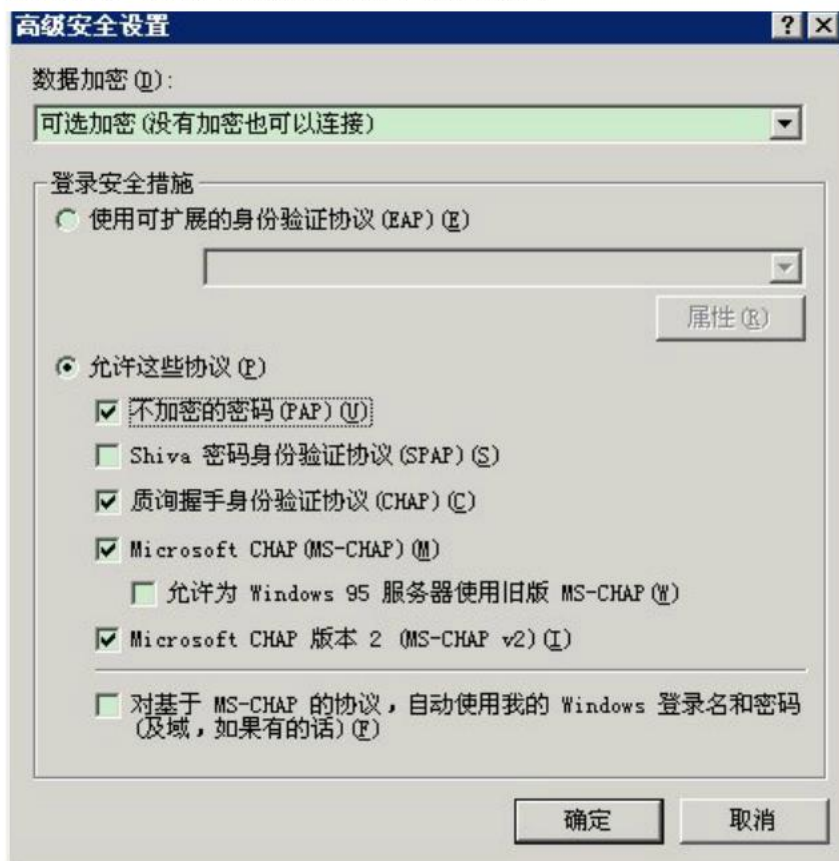
下一步选择“虚拟专用网络连接” → “连接名”任意输入 → “公用网络”页面选择“不拨初始连接” → “VPN 服务器选择”页面输入服务器地址，如 172.24.11.11。创建完成后，在虚拟专用网络下出现了刚才创建和连接，右键选择属性，在网络选项里，选择 VPN 类型为 L2TP IPSec VPN，如下所示：



在安全选项页面，选择“典型（推荐设置）”，如下配置：



如果选择“高级（自定义设置）”，配置如下：



2) 修改注册表

打开注册表（命令 regedit），找到如下路径：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters

新建一个 DWORD 的项，如下：



数值名称为 ProhibitIPSec，值为 1。

另一种方式，可以在 PC 的任意地方新建一个以.reg 为后缀的文件，然后双击运行文件即可，文件的内容如下：

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters]

"ProhibitIPSec"=dword:00000001

修改完成后，重启电脑。

3) 在 CPE 上创建一条路由连接，LAN 侧 PC（用于 L2TP 拨号的 PC）可以 ping 通 L2TP 服务器。

4) CPE 上开启 ALG-L2TP，在 PC1 上用步骤 1 中创建的 L2TP 拨号连接拨号。应该能够拨号成功，获得地址并 ping 通相应的网关。

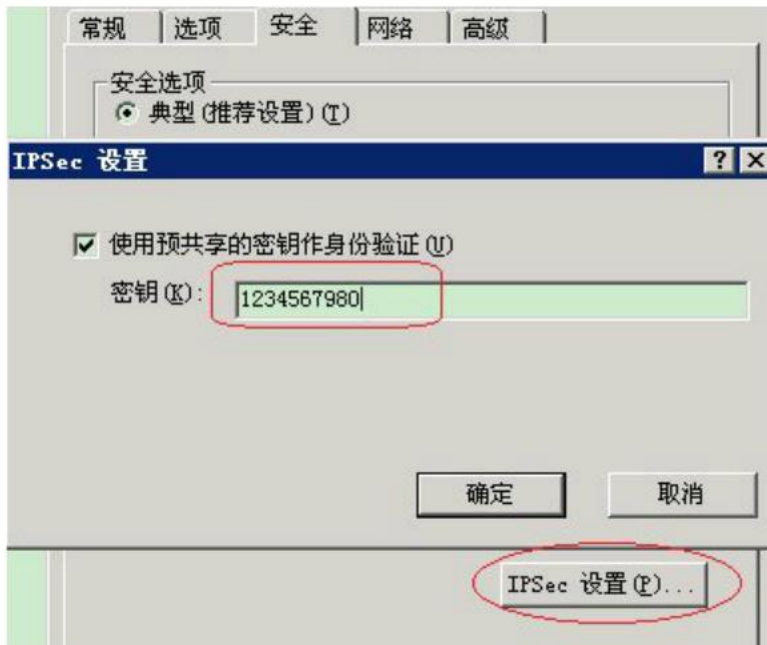
5) 关闭 CPE 上的 ALG-L2TP，PC1 用 L2TP 拨号失败。

测试 ALG-PPTP：

ALG-PPTP 的测试与 L2TP 基本相同，但不需要修改注册表，另外只需要在“属性” -> “网络”里将 VPN 类型修改为“PPTP VPN”即可。

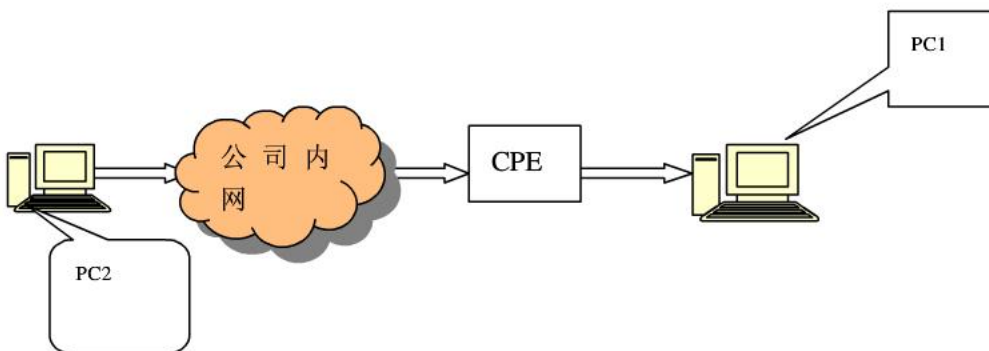
3.ALG-IPSec

1) 拨号连接配置：同 ALG-L2TP，这里不再重复。有一点需要修改，在安全选择页面，配置 IPSec 设置，如下所示：



- 2) 修改注册表：ProhibitIPSec 的值改为 0，方法同 L2TP 中所述，修改后重启电脑。
- 3) 在 CPE 上创建一条路由连接，LAN 侧 PC（用于 IPSec 拨号的 PC）可以 ping 通 IPSec 服务器。
- 4) CPE 上开启 ALG-IPsec，在 PC1 上用步骤 1 中创建的 IPSec 拨号连接拨号。应该能够拨号成功，获得地址并 ping 通相应的网关。
- 5) 关闭 CPE 上的 ALG-IPsec，PC1 用 IPSec 再次拨号，拨号失败。

4.ALG-H323

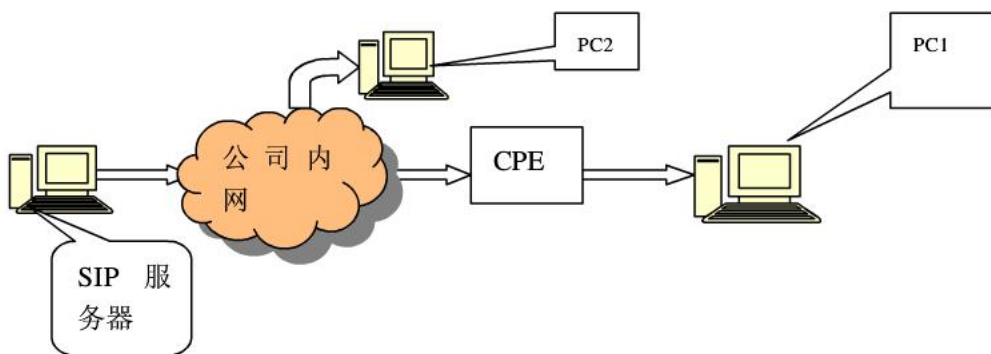


- 1) 配置 NetMeeting，如果是第一次使用，则需要通过向导配置。Netmeeting 在 C:\Program Files\NetMeeting\conf.exe，运行命令 conf 即可。Win 7 中没有 NetMeeting 插件。
LAN 侧的 PC1 和 WAN 侧的另一个 PC2 上都需要配置，配置的过程只需要按向导一步一步进行即可。
- 2) 在 CPE 上创建一条路由方式的 WAN(DHCP)连接，确定 PC1 可以 ping 通 PC2。同时开启 [ALG-H.323](#)。
- 3) 在 PC1 和 PC2 上打开 NetMeeting，PC1 上 NetMeeting 的地址栏中输入 PC2 的 IP 地址，并点击【进行拨号】按钮或回车。

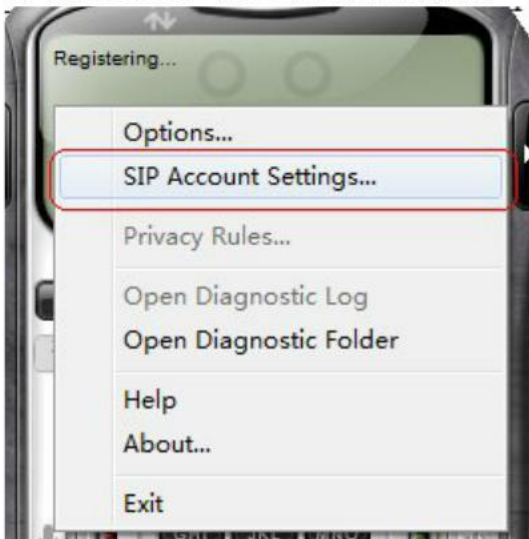


- 4) PC2 上接到呼叫后接收，即可双向通话，传输文件。
- 5) 关闭 ALG-H.323，其他配置都不变。
- 6) 重复步骤 3，发现可以建立连接，WAN 侧 PC2 上可以听到 LAN 侧 PC1 上的声音（单通），可以输入文件。

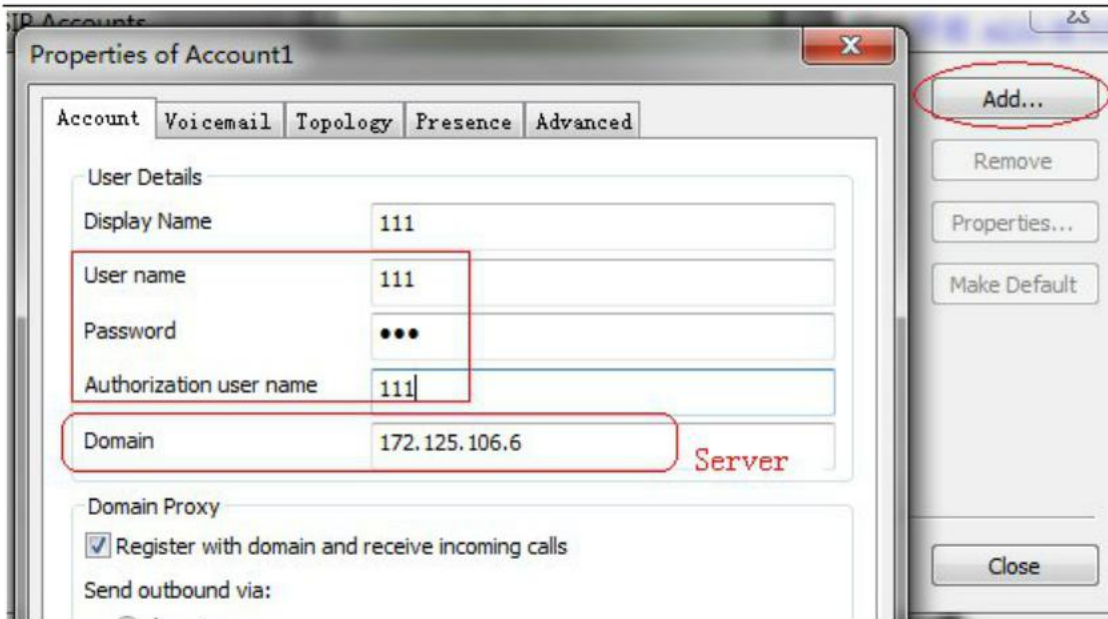
5.ALG-SIP



- 1) CPE 上创建一条路由方式的 WAN 连接，确定 LAN 侧 PC1 可以 ping 通 SIP 服务器。
- 2) 配置 X-Lite。在 X-Lite 页面右键选择“SIP Account Settings”，如下：



单击【Add】按钮，在弹出的窗口中，输入 SIP 服务器地址和账号信息，如下所示：



需要在 LAN 侧 PC1 和 WAN 侧另一个 PC2 上都需要各自配置，这里 PC1 上注册 111，PC2 上注册为 222。

3) PC1 和 PC2 上的 X-Lite 拨对方的号后可以通话，WAN 侧抓包看到 SIP 的首部已经转换为 WAN IP，如下所示：



ALG_SIP_O_wan.p
cap

4) 关闭 CPE 的 ALG-SIP，双方可以通话，但在 WAN 侧抓包后看到 SIP 首部没有转换为 WAN IP，如下所示：

```
Session Initiation Protocol
+ Request-Line: INVITE sip:222@172.125.106.6 SIP/2.0
+ Message Header
+ Via: SIP/2.0/UDP 192.168.1.3:63652;branch=z9hg4bk-d87543-2d7b5956d762977d-1--d87543-;rport
  Max-Forwards: 70
+ Contact: <sip:111@10.56.100.201:63652>
+ To: "222"<sip:222@172.125.106.6>
+ From: "111"<sip:111@172.125.106.6>;tag=8e79557d
  Call-ID: YZi5YTAXNZMZYjY1NGJlMDlmZmYxNDdmYUwM2ExNmM.
+ CSeq: 1 INVITE
  Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
  Content-Type: application/sdp
  User-Agent: X-Lite release 1006e stamp 34025
  Content-Length: 371
+ Message Body
```



ALG_SIP_C_wan.p
cap

参考文献

- 【1】：
- 【2】：
- 【3】：
- 【4】：