Microsoft® Windows®95 Dial-Up Networking 1.2 Upgrade PPTP Information

Technical Details on Use of PPTP Tunnels

1.1 Overview

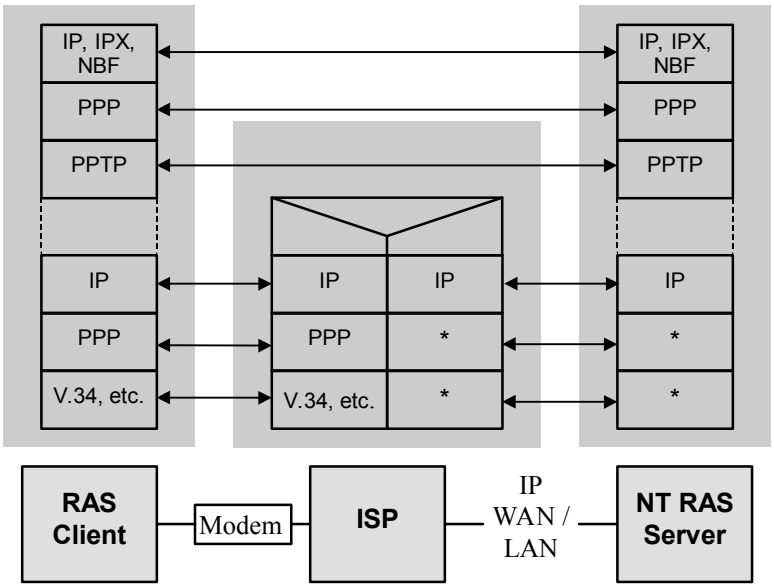
PPTP is a tunneling protocol defined by the PPTP Forum that allows PPP packets to be encapsulated within Internet Protocol (IP) packets and forwarded over any IP network, including the Internet itself. PPTP provides support for virtual LAN connection establishment/release and encapsulation of higher level protocol frames within the Generic Routing Encapsulation (GREv2) over IP. GREv2 encapsulation is connectionless, and is carried directly on top of IP. PPTP provides for congestion control using a sliding window mechanism.

1.2 Using the Internet to Access Remote Networks

Establishing a PPTP connection to a remote private network via the public Internet provides the following benefits:

- The private network's IP address space does not have to be coordinated with the Internet address space.
- All network protocols supported by RAS are supported in the PPTP connection case. Private networks that are running combinations of TCP/IP, IPX, or NBF can be accessed.
- RAS security protocols and policies are used to prevent unauthorized connections.
- All network packets being sent over the Internet can be encrypted.

Window95 PPTP Client / Internet / NT RAS Server Protocol Stack



1.3 Windows95 Support for PPTP

Windows95 supports a single instance of a PPTP connection over a LAN or WAN Internet connection. Windows95 will attempt to allow all connected networks to be visible from the client PC. As described below, this is not possible in all cases.

1.4 Network Protocol Issues

When a PPTP connection is established, the client network protocols will see an additional dial-up adapter become active. PPTP itself uses TCP/IP to tunnel network packets, so at least one adapter in the client must be bound to, and running TCP/IP. This adapter can be a NIC, in the case where the client is connecting to a PPTP server on a

LAN. The TCP/IP adapter can also be a dial-up adapter, in the case where the client is dialing into a RAS server or ISP, and then connecting to a PPTP server across a private Intranet or the public Internet.

1.4.1 NBF

It is assumed that the PPTP client is connecting to an NT RAS/PPTP server. NBF will work as expected. The PPTP client will be able to see both the original network and the new network concurrently. The client will be visible to computers on both LANs, but the networks will not be joined through the client. The client's ability to see computers on the new network is provided by the WindowsNT Server's NetBIOS gateway.

1.4.2 NWLink

Once connected via PPTP, only the target network will be visible with IPX at that time. This is unchanged from current Window95 dial-up IPX connections. Currently, when IPX is selected in a phonebook entry and IPX is active on a NIC, a dialog is presented to the user (at dial time) explaining that Netware servers on the local LAN will no longer be visible once a connection is established to the remote LAN. Users will see this same dialog when establishing a PPTP connection.

1.4.3 TCP/IP

Several TCP/IP configurations will be examined. As a baseline, the first is the simple case of joining two routed IP networks together without PPTP.

5.4.3.1 The Baseline: Two Routed IP Networks

In this configuration, IP packets generated by *Client* that are destined for hosts on the local subnet 1.1.1 are addressed at the MAC level directly to the target host and forwarded over interface *A*.

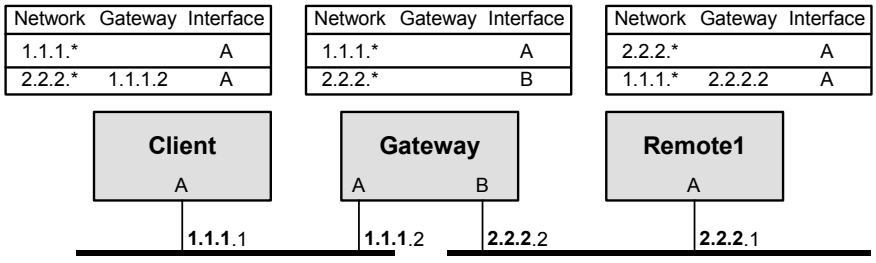
Client packets destined for *Remote1* are addressed at the IP level to *Remote1* and at the MAC level to host *Gateway*. *Gateway*, upon receiving these packets, changes the MAC address to be that of the target *Remote1* and forwards them on interface *B*.

The most common workstation configuration is a simple variation where local subnet packets are sent directly to the target host and all other packets are forwarded to a default gateway. DHCP assigns both client IP addresses and a default gateway address at boot time.

Any given host can have only a single active default gateway. This is ideal in the case of a host with a single adapter but does not work for hosts with multiple adapters. In the example below, both *Client* and *Remote1* could replace their route entry for the peer LAN with a default route, but *Gateway* requires explicit routes to each LAN in order to work properly.

PPTP effectively makes all hosts have multiple adapters and exposes the limitations of default gateway based routing schemes.

Joining two IP Networks without PPTP: The Trivial Case



5.4.3.2 Using PPTP to Securely Bridge Two Networks

In the next scenario, *Gateway* has been made a PPTP server and PPTP filtering has been enabled on interface A. PPTP filtering effectively makes *Gateway* invisible to *Client* without first establishing a PPTP connection. *Client*'s TCP/IP stack has a route to *Gateway*, and uses this to establish and maintain the PPTP connection. Since **only** PPTP packets are accepted on *Gateway*'s interface A, no applications can see *Gateway* at address 1.1.1.2.

Once the PPTP tunnel has been established, *Client* has a second active adapter, with a new IP address assigned to it by the *Gateway* PPTP server. Since the WindowsNT RAS server supports TCP/IP clients by proxy-arping for them on its local networks, *Client* is effectively bridged to the LAN side of *Gateway*.

Remote1 would send packets to *Client* by addressing them at the MAC level to *Gateway* who would forward them over the PPTP adapter to *Client*. *Remote1* is completely unaware of *Gateway*'s role in this process, since *Gateway* is pretending to be every PPTP client at the MAC level.

The issues associated with this configuration are identical to those of a conventional NT RAS server setup. This is no accident, since a PPTP server is a RAS server that uses an IP network as a media type.

On the 1.1.1 network, *Client* has an IP address of 1.1.1.1. On the 2.2.2 network, *Client*'s IP address is 2.2.2.4. Name servers on each network must be configured correctly.

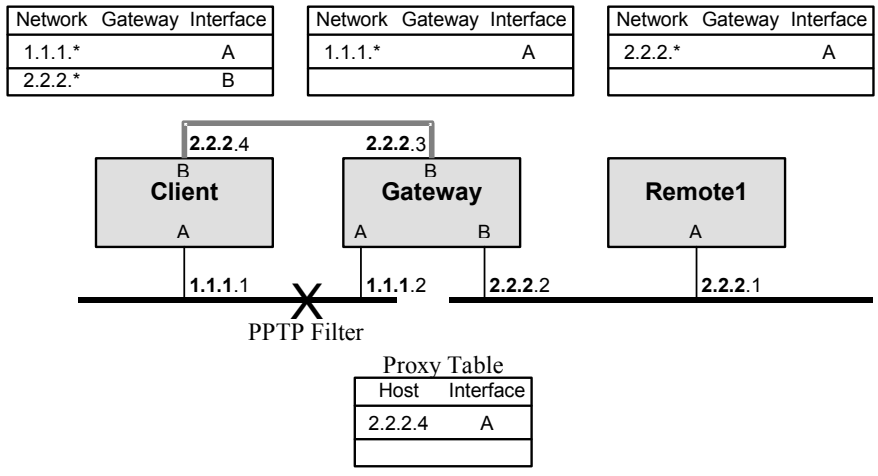
For hosts other than *Client* on the 1.1.1 network to see hosts on the 2.2.2 network, each host must be configured with a route entry that makes Client the gateway to network 2.2.2.

All hosts on the 2.2.2 network can automatically see *Client*, but not other hosts on 1.1.1. In order for this to occur, each host on the 2.2.2 network must be configured with a route entry that makes *Client* (2.2.2.4) the gateway to network 1.1.1. The packet path from a host on 2.2.2 to a host on 1.1.1 would then be:

1? Address the packet at the IP level to the target host and at the MAC level to *Client.*
2? *Gateway* steals the packet and forwards it to *Client* over the PPTP connection.
3? *Client* sees that its destination IP address is on 1.1.1 and forwards it on interface A.

Clearly configuring a network by hand is a non-trivial process. PPTP, by virtue of making clients multi-homed, further complicates this. RIP or OSPF can help automate this process.

Joining two IP Networks with PPTP



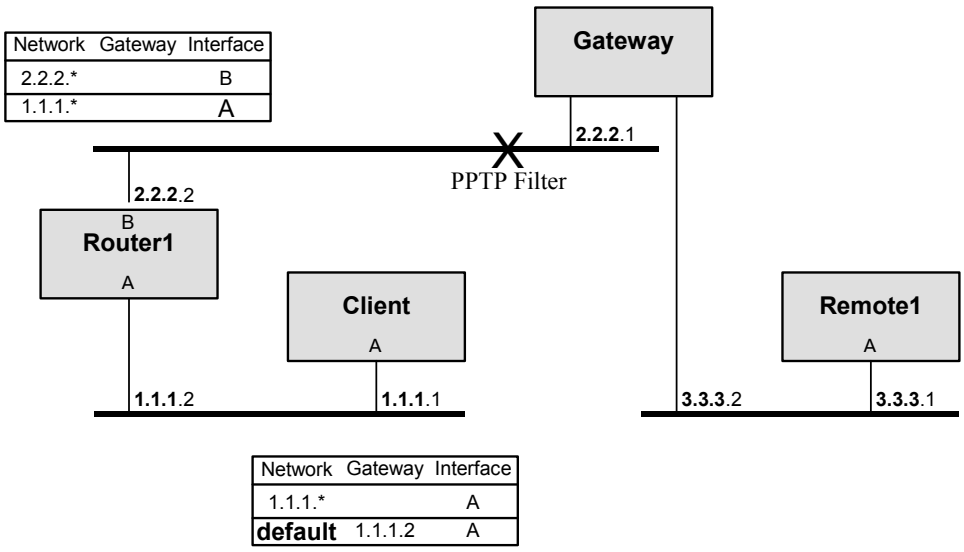
5.4.3.3 A Typical Case

The next network represents most real world networks. *Router1*, and probably *Gateway*, have been hand configured by a system administrator to have explicit routing information. Clients are relying on the routing entries created locally (and automatically) derived from each NIC's IP address and subnet mask. These entries allow the client to reach hosts on the same subnet. Additionally, a single default gateway entry forwards all other packets to a router who hides the larger and more complex routing policy.

Even if routers are dynamically exchanging RIP or OSPF routing information, in many cases the simple default gateway scheme will be used for clients. DHCP can easily assign IP addresses, subnet masks and default gateways.

In the example below, *Client* can see all hosts on his local subnet, 1.1.1 by way of the 1.1.1 route table entry. He can see all hosts on the 2.2.2 network, including *Gateway*, by using the default gateway route. Note that PPTP filtering on *Gateway's* interface A restricts traffic to *Gateway* to PPTP connections.

Joining two IP Networks with PPTP: The Problem Case (Before Tunneling)



1.4.4 The Multiple Default Gateway Problem

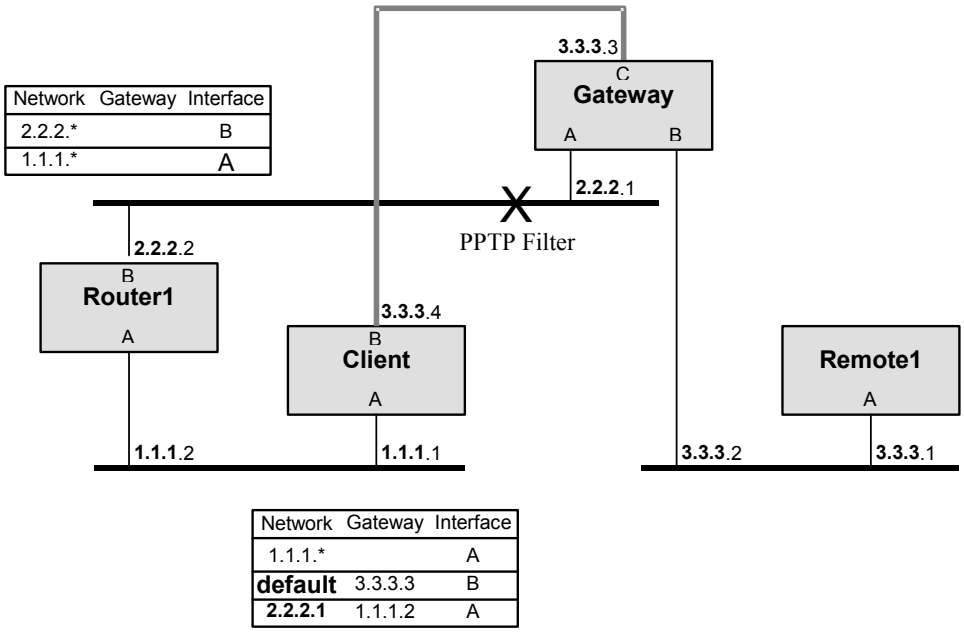
After *Client* has established a PPTP tunnel to *Gateway*, it is effectively bridged to network 3.3.3 on the new interface B. As part of establishing this connection, RAS/PPTP normally changes the default gateway of *Client* to be *Gateway*. In this example, this is not necessary to see hosts on the bridged network 3.3.3, but would be necessary if the other side of *Gateway* was attached to a more complex network.

Changing the default gateway entry has the unwanted side effect of making hosts that were visible on network 2.2.2, including *Gateway* itself, unreachable. In general, after establishing a PPTP connection from a host that was using a default gateway scheme, only hosts on local subnets (on the same LAN segment) will remain visible.

In order to prevent this problem from breaking the PPTP connection itself, Windows95 establishes a single host route entry to the PPTP gateway itself through the old default gateway, *Router1*. This solves the multiple default gateway problem for the PPTP connection itself, but leaves some hosts on the originating network invisible.

This problem occurs only when clients are using default gateways to reach some networks. Explicit host or network route table entries will continue to be valid when the a PPTP connection is established. This means that clients that are receiving local RIP or OSPF routing updates will not have any problems.

Joining two IP Networks with PPTP: The Problem Case (After Tunneling)



There is another common PPTP configuration that will be impacted by this problem. If a non-LAN attached client dials into an ISP to get on the Internet, then establishes a PPTP tunnel to their corporate network, they will loose connectivity to the rest of the Internet during the life of the PPTP connection.
