



APPENDIX **D**

VPDN Processing

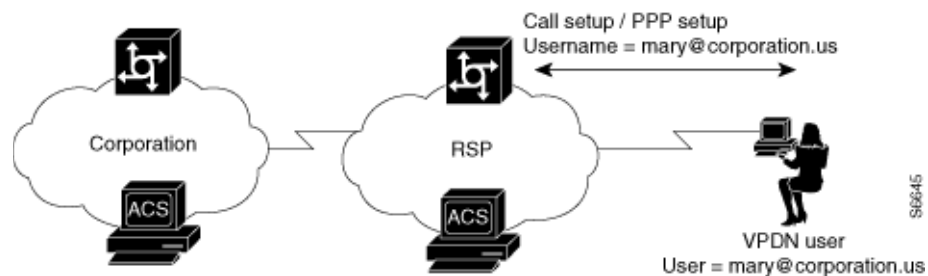
The Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS, supports authentication forwarding of virtual private dial-up network (VPDN) requests. There are two basic types of roaming users: Internet and intranet; VPDN addresses the requirements of roaming intranet users. This chapter provides information about the VPDN process and how it affects the operation of ACS.

VPDN Process

This section describes the steps for processing VPDN requests in a standard environment.

1. A VPDN user dials in to the network access server (NAS) of the regional service provider (RSP). The standard call/point-to-point protocol (PPP) setup is done. A username and password are sent to the NAS in the format *username@domain* (for example, *mary@corporation.us*). See [Figure D-1](#).

Figure D-1 VPDN User Dials In



2. If VPDN is enabled, the NAS assumes that the user is a VPDN user. The NAS strips off the *username@* (*mary@*) portion of the username and authorizes (not authenticates) the domain portion (*corporation.us*) with the ACS. See [Figure D-2](#).

Figure D-2 NAS Attempts to Authorize Domain



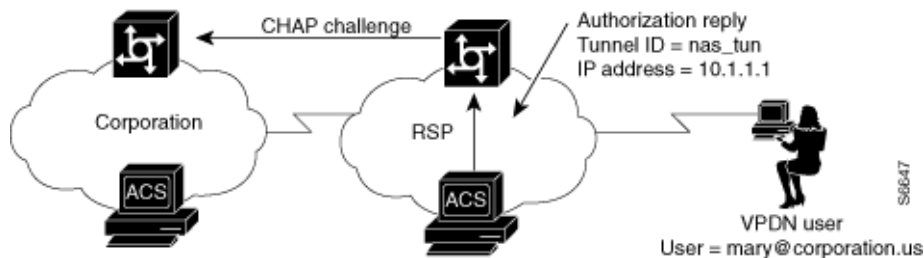
3. If the domain authorization fails, the NAS assumes that the user is not a VPDN user. The NAS then authenticates (not authorizes) the user as if the user is a standard non-VPDN dial user. See [Figure D-3](#).

Figure D-3 Authorization of Domain Fails



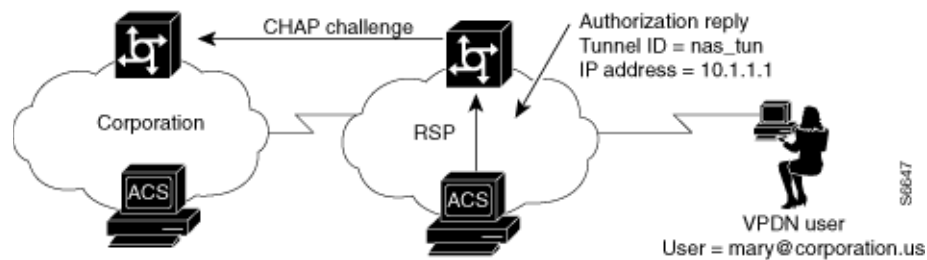
If the ACS authorizes the domain, it returns the Tunnel ID and the IP address of the home gateway (HG); these are used to create the tunnel. See [Figure D-4](#).

Figure D-4 ACS Authorizes Domain



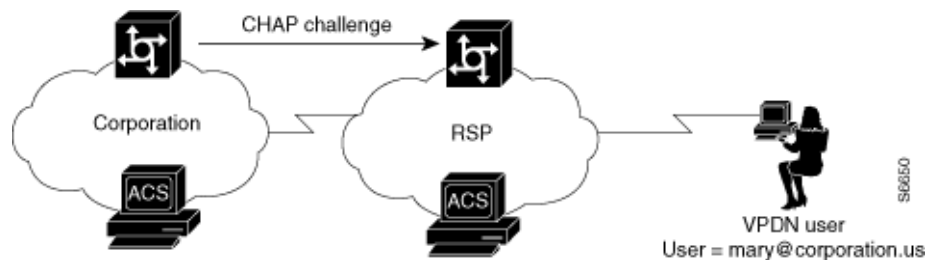
4. The HG uses its ACS to authenticate the tunnel, where the username is the name of the tunnel (`nas_tun`). See [Figure D-5](#).

Figure D-5 HG Authenticates Tunnel with ACS



- The HG now authenticates the tunnel with the NAS, where the username is the name of the HG. This name is chosen based on the name of the tunnel, so the HG might have different names depending on the tunnel being set up. See [Figure D-6](#).

Figure D-6 HG Authenticates Tunnel with the NAS

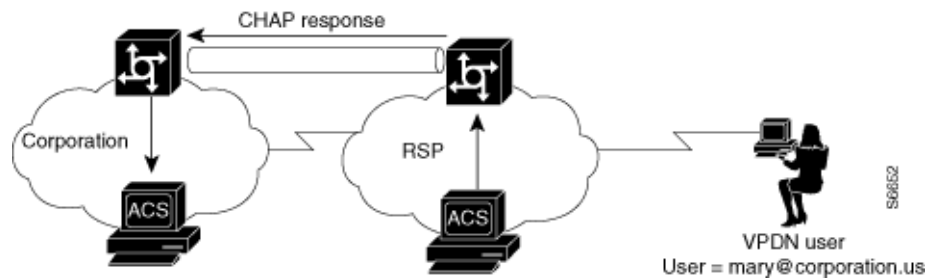


- The NAS now uses its ACS to authenticate the tunnel from the HG. See [Figure D-7](#).

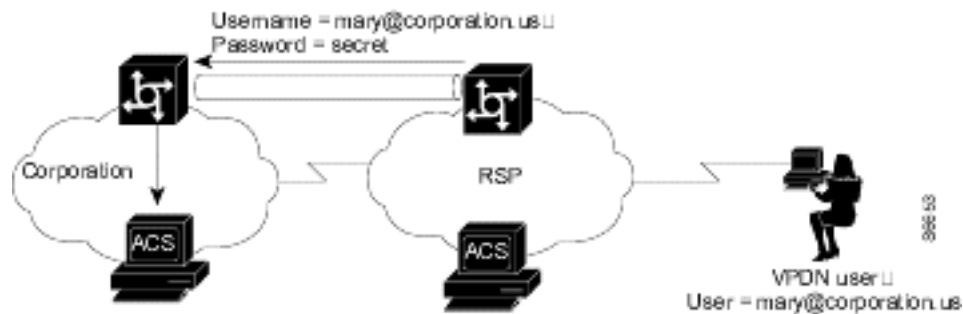
Figure D-7 NAS Authenticates Tunnel with ACS



- After authenticating, the tunnel is established. Now the actual user (*mary@corporation.us*) must be authenticated. See [Figure D-8](#).

Figure D-8 VPDN Tunnel is Established

- The HG now authenticates the user as if the user dialed directly in to the HG. The HG might now challenge the user for a password. The ACS at RSP can be configured to strip off the at symbol (@) and domain before it passes the authentication to the HG. (The user is passed as *mary@corporation.us*.) The HG uses its ACS to authenticate the user. See [Figure D-9](#).

Figure D-9 HG Uses ACS to Authenticate User

- If another user (*sue@corporation.us*) dials in to the NAS while the tunnel is up, the NAS does not repeat the entire authorization and authentication process. Instead, it passes the user through the existing tunnel to the HG. See [Figure D-10](#).

Figure D-10 Another User Dials In While Tunnel is Up