Dial Case Study Overview

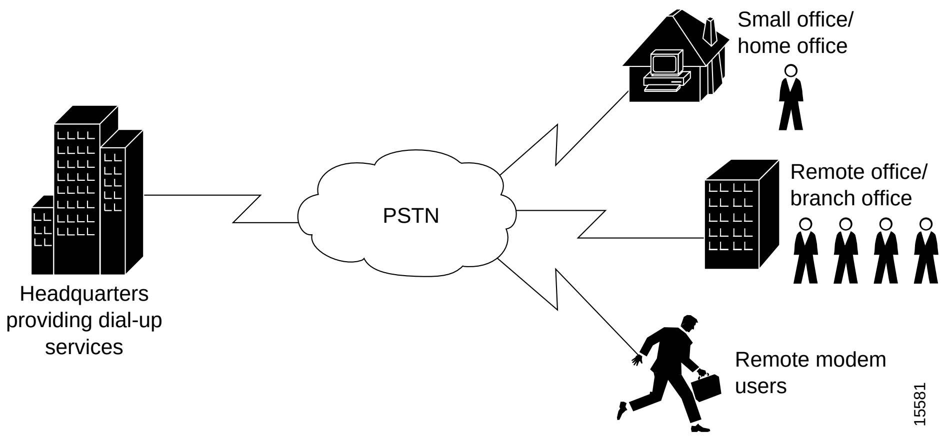
CHAPTER 1

Introduction

This document presents a case study that:

- Is a basic foundation from which you can scale to support larger dial implementations.
- Demonstrates how to configure a headquarters network that provides dial-up services to one small office/home office (SOHO), one remote office/branch office (ROBO), and remote modem users (Figure 1-1).
- Assumes that the equipment has been properly installed at each of the sites and are powered up as described in the manuals and installation guides that were included in the boxes with the equipment.

Figure 1-1 Typical Dial-Up Business Scenario



Case Study Scenario

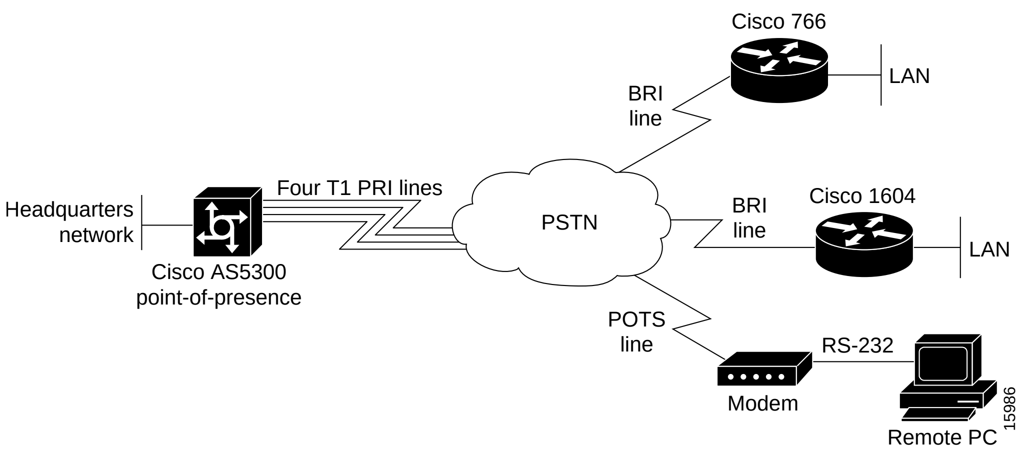
In this case study, a single Cisco AS5300 network access server (NAS) supports remote users and remote local-area networks (LANs) that are connected with modems and ISDN routers (Figure 1-2):

- The remote ISDN routers are a Cisco 1604 and Cisco 766. Only IP and basic security are used.

- The Cisco AS5300 is a network access server (NAS) that supports 96 concurrent modem and ISDN connections by using four T1 PRI lines and 96 integrated modems.
- Modem connections are established through the Cisco IOS command line interface (CLI) for lines and corresponding asynchronous interfaces.
- Digital ISDN connections are established through the Cisco IOS CLI for channelized serial interfaces.
- The public switched telephone network (PSTN) provides the core interconnecting fabric between the devices.

Figure 1-2 shows the physical elements of this case study as Layer 1 of the Open Systems Interconnection (OSI) reference model.

Figure 1-2 Case Study Scenario OSI Layer 1 Elements



The connections going across the PSTN use the Point-to-Point Protocol (PPP), which negotiates

- The Link Control Protocol (LCP)
- Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication
- IP Control Protocol (IPCP)

to bring up IP over PPP.

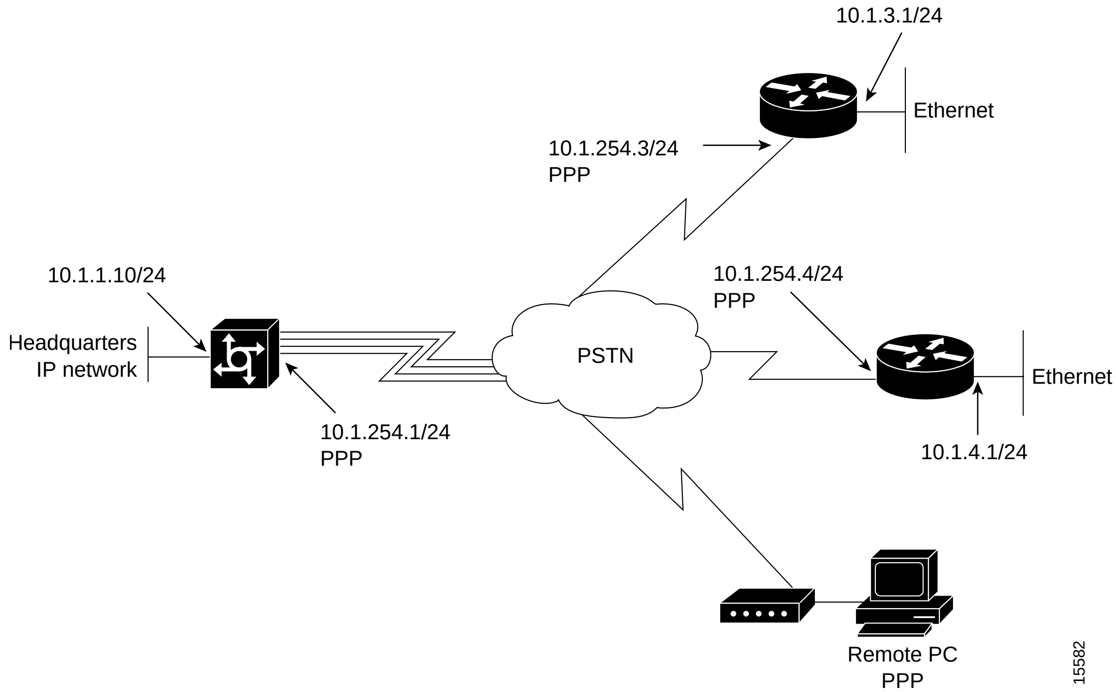
The IPCP Network Control Protocol (NCP) is the mechanism that opens the links and negotiates the IP parameters. Figure 1-3 shows these Layer 2 and Layer 3 elements as they are used in this case study.

A remote LAN is typically a router that has a next-hop address and its own IP subnet. It also requires IP routing support from the backbone, which is commonly done with a static IP route.

A remote node gets an IP address out of a central pool of IP addresses that for this case study is configured and maintained on the Cisco AS5300 in the loopback interface.

Remote LANs and remote nodes are primarily differentiated by this IP addressing scheme. Remote LANs can appear as remote nodes by using port address translation (PAT); however, for this case study, PAT is not configured.

Figure 1-3 Case Study Scenario OSI Layer 2 and Layer 3 Elements



Network Topology, Hardware, and Software Selections

Table 1-1 summarizes the types of services that can be provided by a headquarters point-of-presence (POP) to remote nodes and sites. Although port address translation (PAT) is commonly used, it is not configured in this case study. For more information, see Table 1-2.

Note Unless otherwise stated, the terms "dial-in" and "dial-out" are from the perspective of the Cisco AS5300.

Table 1-1 Device Characteristics Typically Provided by Headquarters

Scenario	Remote Hardware	Services Required	Notes
Remote node modem	Modem	Asynchronous shell (async shell) Asynchronous PPP (async PPP)	Dial-in only. Remote devices are assigned an IP address from a central pool.
Remote node ISDN	ISDN routers using port address translation (PAT), PC-based ISDN terminal adapters	Synchronous PPP (sync PPP)	Dial-in only. PAT is enabled. Connecting devices are assigned an IP address from a central pool. This option is not covered in this case study.
Remote office LAN	Cisco 1604	Synchronous PPP	Dial-in and dial-out. Distinct IP subnet. PAT is not used.
Small office LAN	Cisco 766	Synchronous PPP	Dial-in and dial-out. Distinct IP subnet. PAT is not used.

Design Architecture

The following sections provide the framework for this case study:

- Service Needs
- Layer 3 IP Design
- IP Subnet Rationale
- Call-Processing Components

Service Needs

In this case study, the Cisco AS5300 offers three basic services:

- Async shell
- Async PPP
- Sync PPP

These services are based on real needs as requested by the remote sites. To access these services, the remote devices connect to the Cisco AS5300 through the PSTN.

Table 1-2 Services Provided by Headquarters

Service Term	Purpose	Physical Data Path	Security Method Used
Async shell	Provides access through the Cisco IOS CLI EXEC shell to terminal services (no PPP) for the following tasks: • Change passwords • Access menus • Troubleshoot modem connections using a simple environment • Access other network resources with Telnet	Client modems, POTS, Cisco IOS integrated modems, lines, and asynchronous interfaces	Login

Service Term	Purpose	Physical Data Path	Security Method Used
Async PPP	• Provides IP (and multi-protocol) connectivity for remote node modem users • Supports any Internet application that is available by using IP, such as e-mail, web browsing, FTP, and Telnet.	Client modems, POTS, Cisco IOS integrated modems, lines, and asynchronous interfaces	PPP (CHAP, PAP, or login)
Sync PPP	• Provides IP (and multi-protocol) connectivity for BRI- or PRI-attached remote sites. • Supports any Internet application that is available by using IP, such as e-mail, web browsing, FTP, and Telnet. **Note** Terminal services through a shell are not available to synchronous link users (for example, ISDN routers and terminal adapters through a BRI channel).	End-to-end ISDN using B channels over a digital synchronous path. Calls use interface serial channels (for example, S0:1, S0:2, and so forth).	PPP (CHAP or PAP)

Layer 3 IP Design

This case study uses PPP to transport IP packets across the PSTN and into the end-user devices (remote LANs or remote nodes). IPCP is the specific service enabled over the PPP links. To deliver this service, the case study uses address space from 10.1.0.0 /16 (The "/16" means that there are 16 bits in the subnet mask. The "/24" means that there are 24 bits in the subnet mask). Figure 1-4 shows the IP subnet rationale for the case study.

Figure 1-4 Case Study Scenario IP Subnetting Diagram

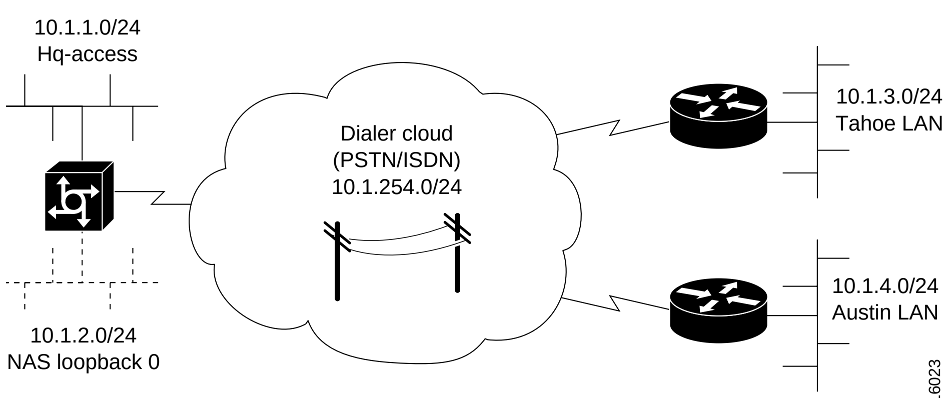


Table 1-3 IP Subnetting Table

Subnet Name	Assigned Subnet	Location
Hq-access	10.1.1.0 /24	Hq-access Ethernet
NAS loopback 0	10.1.2.0 /24	Loopback interface inside the Cisco AS5300. The loopback subnet supports the remote node devices by providing a pool of IP addresses for the remote nodes.
Dialer cloud	10.1.254.0 /24	Public switched telephone network (PSTN)
Tahoe LAN	10.1.3.0 /24	Tahoe Ethernet
Austin LAN	10.1.4.0 /24	Austin Ethernet

Using the subnetting tables and diagrams shown previously, you can create a router naming and addressing plan for the assigned host names (Table 1-4). Note that the IP addresses are derived directly from the subnet plan. You can add additional subnets and remote LANs to this solution.

Table 1-4 Router Naming and Addressing Plan

Router Name	WAN IP Address	Ethernet IP Address
hq-sanjose	10.1.254.1 255.255.255.0	10.1.1.10 255.255.255.0
soho-tahoe	10.1.254.3 255.255.255.0	10.1.3.1 255.255.255.0
robo-austin	10.1.254.4 255.255.255.0	10.1.4.1 255.255.255.0

IP Subnet Rationale

This section describes each IP subnet and its design criteria. IP route summarization occurs at the gateway that connects the Cisco AS5300 NAS to the IP backbone. IP range 10.1.0.0/16 is propagated to the backbone.

Hq-access Subnet

IP subnet 10.1.1.0/24 is assigned to the Ethernet connected to the Cisco AS5300. If additional access servers and POP management devices are needed, they are assigned to this IP subnet. Using one subnet for the entire headquarters dial access POP simplifies network design.

NAS Loopback 0 Subnet

IP subnet 10.1.2.0/24 is assigned to the loopback interface on the Cisco AS5300. This is the subnet used to host IP addresses assigned to remote nodes. The access server has an IP pool range of 10.1.2.2 through 10.1.2.97.

Remote nodes dialing in request addresses from the Cisco AS5300’s local IP address pool. This IP pool behaves like an address server handing out IP addresses to remote nodes during IPCP negotiation (a component of PPP).

Dialer Cloud Subnet

IP subnet 10.1.254.0/24 is assigned to the public switched telephone network (PSTN). The static IP addresses are described in Table 1-4. See the column “WAN IP Address.” The PSTN becomes a “dialer cloud” from the perspective of the Cisco IOS. Dialer interfaces are used to connect to this dialer cloud. BRI and PRI interfaces are also dialer interfaces and use the same dial-on-demand routing (DDR) mechanisms to open and close circuit-switched connections.

A key design decision in this case study is to number the dialer cloud subnet. (When asynchronous routing is enabled, you can conserve network addresses by configuring the asynchronous interfaces as unnumbered. However, for this case study IP unnumbered is not used on these interfaces.) Numbering the dialer cloud ports to match the remote LAN supported by the same remote device is part of the design strategy to simplify administration. For example, remote subnet 10.1.3.0/24 is connected to the same remote site as dialer cloud node 10.1.254.3. IP node 10.1.254.4 supports IP subnet 10.1.4.0/24.

On the Cisco AS5300, all the individual serial channel interfaces are grouped under one master dialer interface. As the individual remote sites connect, their configurations must coordinate with the configuration of the master dialer interface.

Tahoe and Austin LAN Subnets

IP subnet 10.1.3.0/24 is assigned to the Ethernet connected to the Cisco 766 (soho-tahoe). IP subnet 10.1.4.0/24 is assigned to the Cisco 1604 (robo-austin) Ethernet. Each site that supports a distinct IP subnet must be assigned its own distinct IP subnet address space. Routers with LANs behind them must have their own distinct IP subnets when not using PAT.

These remote LAN routers point to the central site as the default route. The hq-sanjose NAS is configured with static routes to the remote IP subnets.

Call-Processing Components

Figure 1-5 illustrates the connectivity path as calls come into the Cisco AS5300. The contents inside the dotted square box are the internal components of the Cisco AS5300. Both analog modem and digital calls enter the Cisco AS5300 through the E1/T1 controllers. Incoming modem calls are connected with the integrated modems and routed to the asynchronous interfaces. Incoming sync PPP calls are connected to the individual interface serial channels (for example, S0:1 and S0:2).

One PPP/modem user consumes resources from one channel, one integrated modem, one line, and one asynchronous interface. An ISDN B-channel user connects directly with a channel of the T1 and a serial B channel. The group-async and dialer interfaces are used to control the interfaces’ behavior and configuration of async and serial channels.

Note The network devices in this case study are manually configured by using Cisco IOS software. The automatic Cisco IOS software setup script is not used. This setup script usually runs when no startup configuration is found in NVRAM (for example, when powering up a new router).

Figure 1-5 Call-Processing Components