

Dial Networking Business Applications

This chapter provides an introduction to common dial networking scenarios used by service providers and enterprises.

Providing dial access means to set up one or more access servers or routers to allow on-demand connectivity for individual remote nodes or remote offices. The dial network solutions described in this chapter are based on business case scenarios. Depending on your business application, dial access has different meanings and implementations.

This chapter provides the following sections:

- Dial Networking for Service Providers and Enterprises
- Common Business Cases Applied to Dial Scenarios
- IP Addressing Strategies to Consider

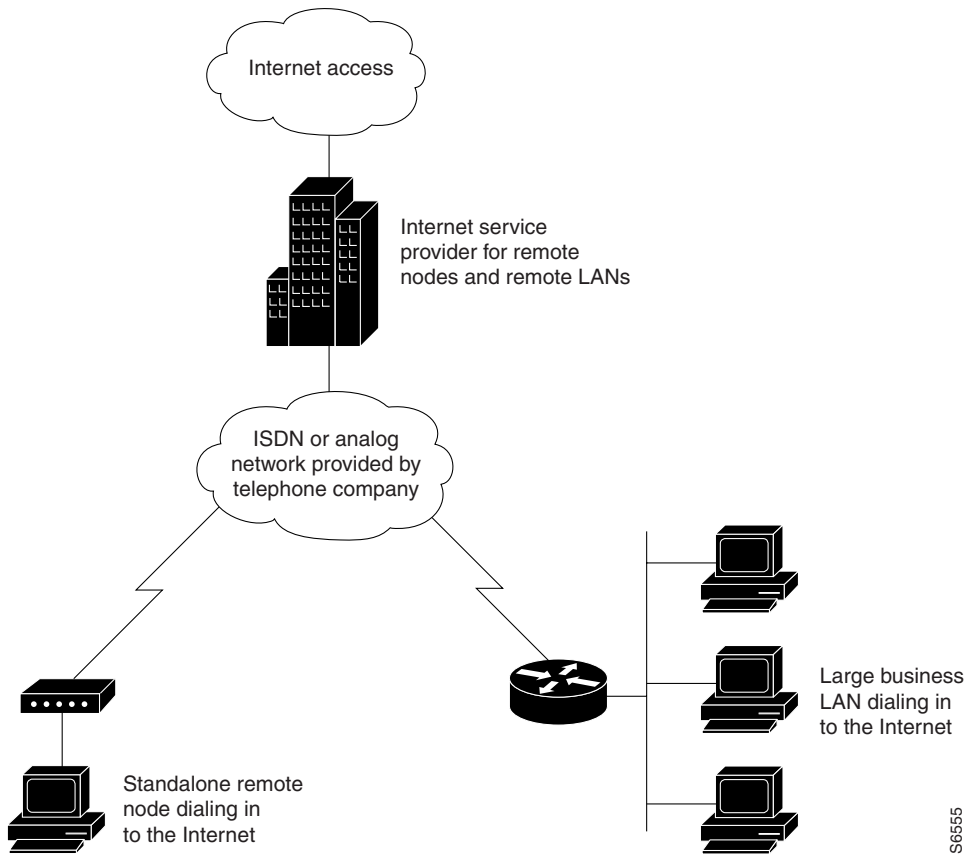
Dial Networking for Service Providers and Enterprises

Service providers tend to supply public and private dial-in services for businesses or individual home users. Enterprises tend to provide private dial-in access for employees dialing in from remote LANs (such as a remote office) or individual remote nodes (such as a telecommuter). Additionally, there are hybrid forms of dial access—virtual private dial networks (VPDNs)—that are jointly owned, operated, and set up by both service providers and enterprises.

Figure 2 displays a common dial topology used by Internet service providers (ISPs). The central dial-in site is owned and controlled by the service provider, who only accepts dial-in calls. Enterprises and individual remote clients have no administrative control over the ISP's dial-in site.

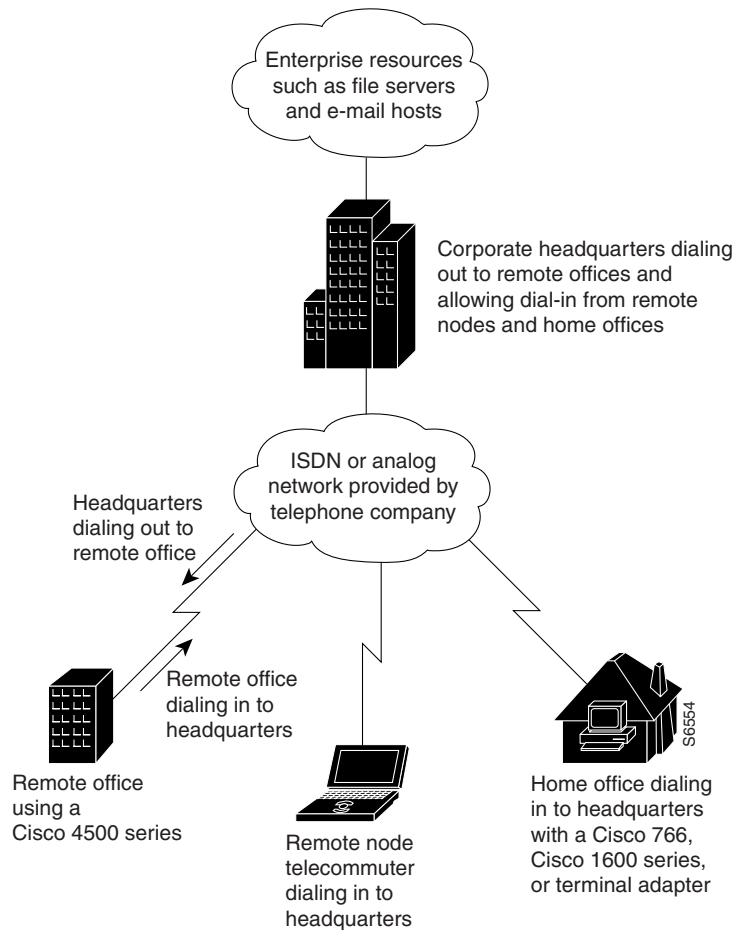
Note Many additional dial network strategies exist for different business applications. This overview is intended to provide only a sample of the most common dial business needs as experienced by Cisco Systems' dial escalation team.

Figure 2 Sample Dial Network for an Internet Service Provider



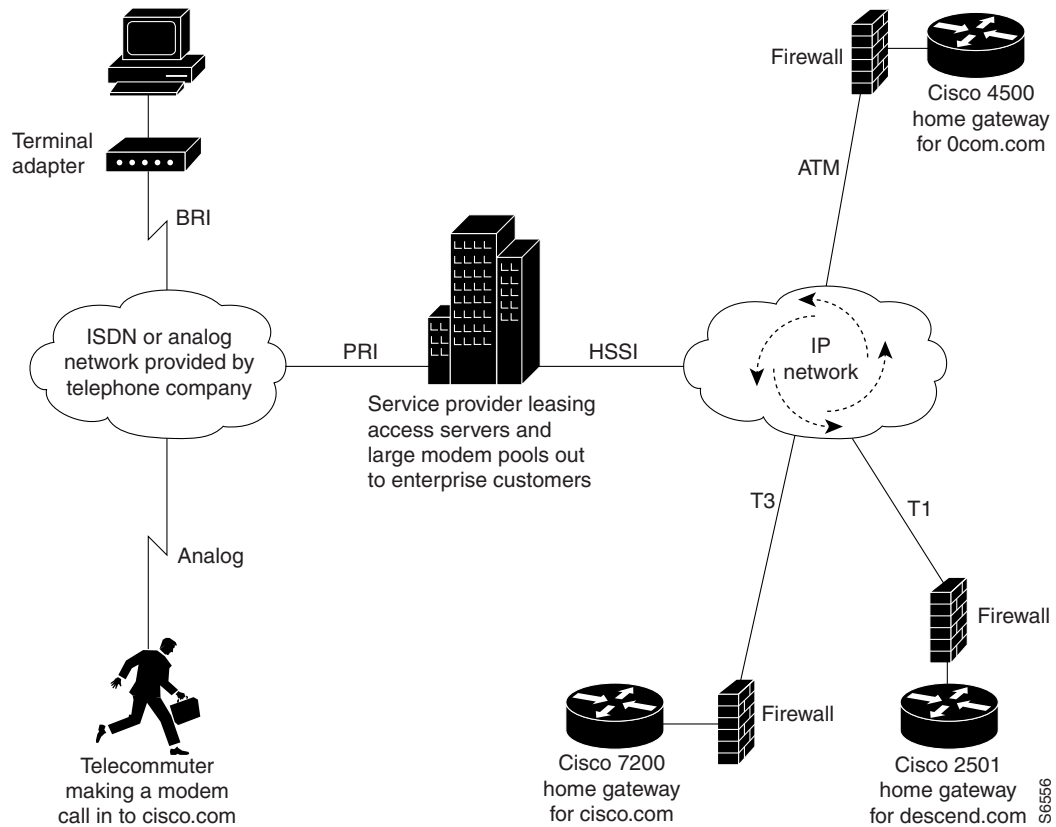
Enterprises can provide bidirectional access services with remote LANs and one-way dial-in access for standalone remote nodes. Bidirectional access means that remote LANs can dial in to the enterprise, and the enterprise can dial out to the remote LANs. A remote LAN can be a large remote office or a small home office. A standalone remote node can be an individual PC that is dynamically assigned an IP address from the enterprise's modem pool. In most cases, an enterprise has complete administrative control over its local and remote devices. (See Figure 3.)

Figure 3 Sample Dial Network for an Enterprise



Service providers and enterprises both benefit from a hybrid dial solution called VPDN. Service providers offer virtually private access to enterprises by providing the dial-in access devices for the enterprise's use (for example, access servers and modem pools). In this solution, service providers construct the networking fabric for city-to-city dial connectivity for the enterprise. Enterprises provide only a home gateway router (with no attached modems) and a WAN connection to their service provider. VPDN dial solutions enable the enterprise to continue to maintain complete administrative control over its remote locations and network resource privileges. (See Figure 4.)

Figure 4 Sample VPDN for Service Providers and Enterprises



Common Business Cases Applied to Dial Scenarios

The hardware and software configuration designs for dial networks are derived from business operations needs. This section describes several of the most common business dial scenarios that Cisco Systems is supporting for basic IP and security services.

Refer to the scenario that best describes your business or networking needs:

- The following dial scenarios are commonly used by service providers. For detailed description and configuration information, refer to the chapter “Service Provider Dial Scenarios and Configurations.”
 - Scenario 1, Remote PCs Dialing In to a Small to Medium Scale Dial-In Solution (one or two access servers at the central dial-in site)
 - Scenario 2, Remote PCs Dialing In to a Large Scale Dial-In Solution (more than two access servers at the central dial-in site, multichassis multilink PPP)
 - Scenario 3, Remote PCs Placing PPP Calls over X.25 Networks
 - Scenario 4, Remote PCs Dialing In to a Virtual Private Dial Network

- The following dial scenarios are commonly used by enterprises. For detailed description and configuration information, refer to the chapter “Enterprise Dial Scenarios and Configurations.”
 - Scenario 1, Remote Offices and Telecommuters Dialing In to a Central Site
 - Scenario 2, Bidirectional Dial Networking between a Central Site and Remote Offices or Telecommuters
 - Scenario 3, Telecommuters Dialing In to a Mixed Protocol Environment

IP Addressing Strategies to Consider

Exponential growth in the remote access router market has created new challenges for Internet service providers (ISPs) and enterprise customers in remote locations and small office/home office (SOHO) environments. Such customers seek internetworking solutions that will accomplish the following:

- Minimize Internet access costs for remote offices
- Minimize configuration requirements on remote access routers
- Enable transparent and dynamic IP address allocation for hosts in remote environments
- Improve network security capabilities at each remote SOHO site
- Conserve registered IP addresses
- Maximize IP address manageability

Remote networks have variable numbers of end systems that need access to the Internet; therefore, some ISPs are interested in allocating just one IP address to each remote LAN.

In enterprise networks where telecommuter populations are increasing in number, network administrators need solutions that ease configuration and management of remote routers and provide conservation and dynamic allocation of IP addresses within their networks. These solutions are especially important when network administrators implement large dial-up user pools where ISDN plays a major role.

Chose an Appropriate IP Addressing Scheme

You should use an IP addressing scheme that is appropriate for your business scenario as described in the following sections:

- Use a Classic Address Strategy for Remote LAN and Remote Client Dial-In
- Setup Easy IP on a Router or Access Server

Additionally, here are some addressing issues to keep in mind while you evaluate different IP address strategies:

- 1 How many IP addresses do you need?
- 2 Do you want remote clients to dial in to your network and connect to server based services, which require statically assigned IP addresses?
- 3 Is your primary goal to provide Internet services to a network (for example, surfing the web, downloading e-mail, using TCP/IP applications)?
- 4 Can you conduct business with only a few registered IP addresses?
- 5 Do you need a single contiguous address space or can you function with two non contiguous address spaces?

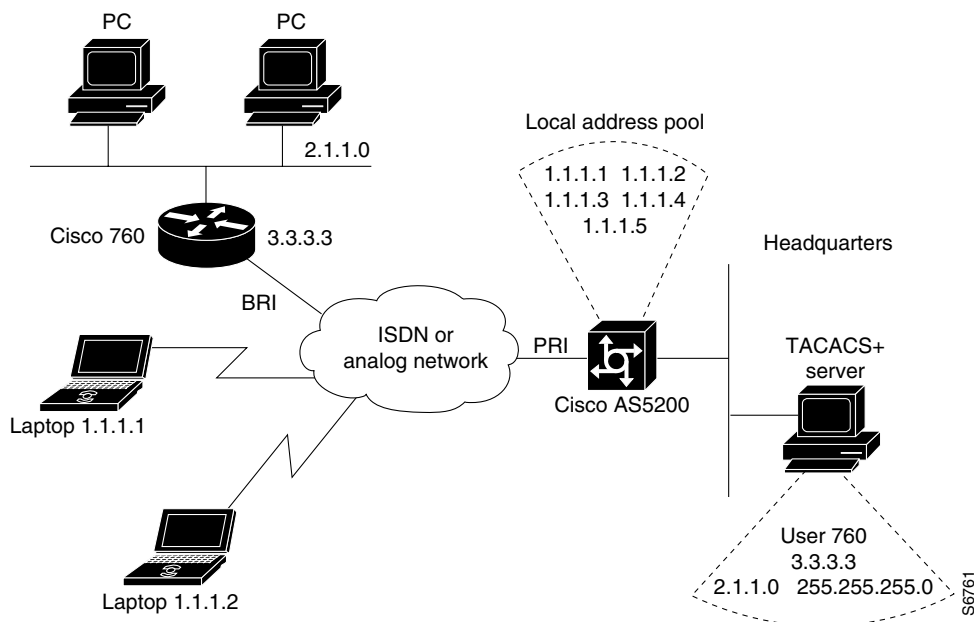
Use a Classic Address Strategy for Remote LAN and Remote Client Dial-In

This section describes two classic IP addressing strategies you can use to set up dial-in access. Classic IP addresses are statically or dynamically assigned from your network to each site router or dial-in client. The IP address strategy you use depends on if you are allowing remote LANs or individual remote clients to dial in.

A remote LAN usually consists of a single router at the gateway followed by multiple nodes such as 50 PCs. The IP address on the gateway router is fixed or statically assigned (for example, 3.3.3.3). This device always uses the address 3.3.3.3 to dial in to the enterprise or service provider network. There is also a segment or subnet associated with the gateway router (for example, 2.1.1.0/255.255.255.0), which is defined by the dial-in security server.

For individual remote clients dialing in, a specific range or pool of IP addresses is defined by the gateway access server and dynamically assigned to each node. When a remote node dials in, it receives an address from the specified address pool. This pool of addresses usually resides locally on the network access server. Whereas, the remote LANs have predefined or statically assigned addresses. The accompanying subnet is usually statically assigned too. (See Figure 5.)

Figure 5 Classic IP Address Allocation



Here are some advantages and disadvantages of manually assigning IP addresses:

- Advantages
 - Web servers or Xservers can be stationed at remote locations.
 - Since addresses are members of your network, they are perfectly transparent.
- Disadvantages
 - IP address assignments are difficult to administer or manage. You may also need to use some complicated subnetting configurations.
 - Statically assigned IP addresses use up precious address space.
 - Strong routing configuration skills are usually required.

Setup Easy IP on a Router or Access Server

Two of the key problems facing the Internet are depletion of IP address space and scaling in routing. The Easy IP (Phase 1) feature combines Network Address Translation (NAT) and PPP/Internet Protocol Control Protocol (IPCP). This feature enables a Cisco router to automatically negotiate its own registered WAN interface IP address from a central server and allows all remote hosts to access the global Internet using this single registered IP address. Because Easy IP uses existing port-level multiplexed NAT functionality within the Cisco IOS software, IP addresses on the remote LAN are invisible to the Internet.

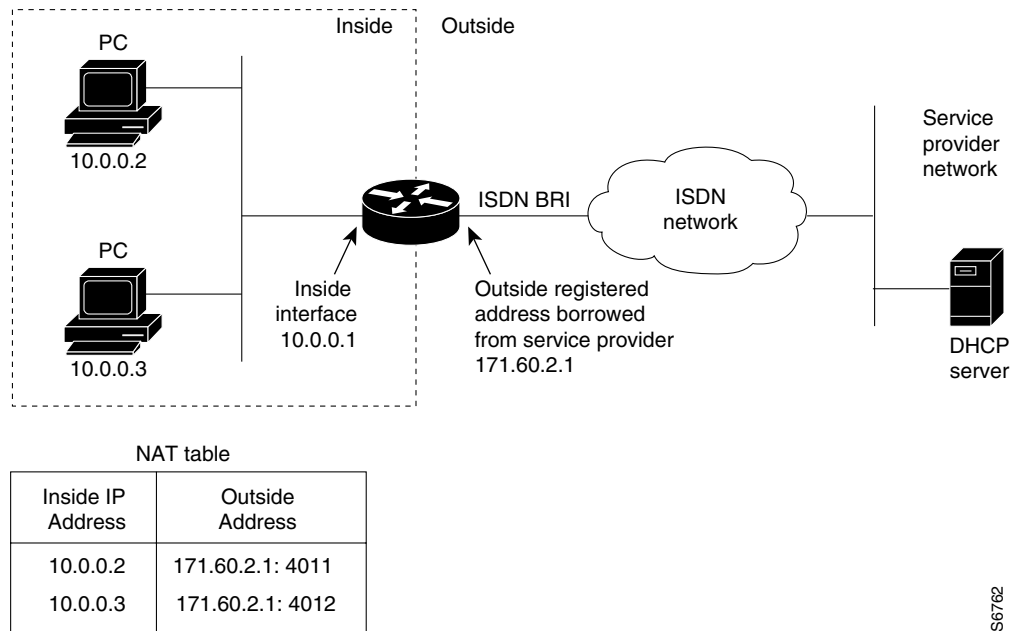
Cisco IOS Easy IP (Phase 1) Component Technologies

Cisco IOS Easy IP solution is a scalable, standards-based, “plug-and-play” solution that is comprised of a combination of the following technologies:

- NAT—Described in RFC 1631. NAT operates on a router that usually connects two or more networks together. Using Easy IP, at least one of these networks (designated as “inside” or “LAN”) is addressed with private (RFC 1918) addresses that must be converted into a registered address before packets are forwarded onto the other registered network (designated as “outside” or “WAN”). Cisco IOS software provides the ability to define one-to-one translations (NAT) as well as many-to-one translations (Port Address Translation [PAT]). Within the context of Cisco IOS Easy IP, PAT is used to translate all internal private addresses to a single outside registered IP address.
- Point-to-Point Protocol/Internet Protocol Control Protocol (PPP/IPCP)—Defined in RFC 1332. This protocol enables users to dynamically configure IP addresses over PPP. A Cisco IOS Easy IP router uses PPP/IPCP to dynamically negotiate its own WAN interface address from a central access server or DHCP server.

Figure 6 shows an example of how Easy IP works. A range of registered or unregistered IP addresses are used inside a company’s network. When a dial-up connection is initiated by an internal node, the router uses the Easy IP feature to rewrite the IP header belonging to each packet and translate the private address into the dynamically assigned and registered IP address, which could be borrowed from a service provider.

Figure 6 Translating and Borrowing IP Addresses



S6762

For a more detailed description of how Easy IP (phase 1) works, refer to the chapter “Configuring Easy IP” later in this document.

Key Benefits of Using Easy IP

The Easy IP feature provides the following benefits:

- Reduces Internet access costs by using dynamically allocated IP addresses. Using dynamic IP address negotiation (PPP/IPCPC) at each remote site substantially reduces Internet access costs. Static IP addresses cost more to *purchase* compared to dynamically allocated or *rented* IP addresses. Easy IP enables you to rent IP addresses. In addition, dynamically assigned IP addresses saves you time and money associated with subnet mask configuration tasks on hosts. It also eliminates the need to configure host IP addresses when moving from network to network.
- Simplifies IP address management. Easy IP enables ISPs to allocate a single registered IP address to each remote LAN. Because only a single registered IP address is required to provide global Internet access to all users on an entire remote LAN, customers and ISPs can use their registered IP addresses more efficiently.
- Conserves registered IP addresses. Suppose you want to connect to the Internet, but not all your hosts have globally unique IP addresses. NAT enables private IP internetworks that use nonregistered or overlapping IP addresses to connect to the Internet. NAT is configured on the router at the border of a stub domain (referred to as the *inside network*) and a public network such as the Internet (referred to as the *outside network*). The private addresses you set up on the inside of your network translate in to a *single* registered IP addresses on the outside of your network.
- Provides remote LAN IP address privacy. Because Easy IP uses existing port-level multiplexed NAT functionality within Cisco IOS software, IP addresses on the remote LAN are invisible to the Internet, making the LAN inherently more secure. As seen by the external network, the source IP address of all traffic from the remote LAN is the single registered IP address of the Easy IP router’s WAN interface.

For step-by-step configuration information on how to set up the Easy IP feature on a router or access server, refer to the chapter “Configuring Easy IP” later in this document.

