



CHAPTER 15

Deployment Scenarios

In the following sections, this chapter describes and shows some typical deployment scenarios for the Cisco 860 series and 880 series Integrated Services Routers (ISRs):

- [About the Deployment Scenarios, page 15-1](#)
- [Enterprise Small Branch, page 15-3](#)
- [Internet Service and IPsec VPN with 3G, page 15-4](#)
- [SMB Applications, page 15-5](#)
- [Enterprise Wireless Deployments with LWAPP, page 15-6](#)

About the Deployment Scenarios

This chapter describes typical deployment scenarios for Cisco 860 series and Cisco 880 series ISRs, and provides a high-level overview of each scenario with pointers to information about new functions.

Major features of the Cisco 860 series and Cisco 880 series ISRs include:

- 3G wireless data connectivity backup (some Cisco 880 series ISRs)
- Voice capabilities (some Cisco 880 series ISRs)
- Embedded wireless device (optional)
- Power over Ethernet (all Cisco 880 series ISRs)

3G Wireless Backup

Some Cisco 880 series ISRs have 3G wireless data backup capability. See [Chapter 4, “Configuring Backup Data Lines and Remote Management”](#) for details.

Voice

Some Cisco 880 series ISRs contain voice capabilities. Refer to the [Cisco IOS Voice Configuration Library](#) for details.

Embedded Wireless Device

- Cisco 860 series, Cisco 880 series, and Cisco 890 ISRs have an optional wireless device that runs its own version of the Cisco IOS software.
 - Cisco 890 Series ISRs with embedded access points are eligible to upgrade from autonomous software to Cisco Unified software, if the router is running the IP Base feature set and Cisco IOS 12.4(22)YB software.

- Cisco 880 Series ISRs with embedded access points are eligible to upgrade from autonomous software to Cisco Unified software, if the router is running the advipservices feature set and Cisco IOS 12.4(20)T software.
- Cisco 860 Series ISRs with embedded access points are not eligible to upgrade from autonomous software to Cisco Unified software.



Note To use the embedded access point in a Cisco Unified Architecture, the Cisco Wireless LAN Configuration (WLC) must be running version 5.1 or later.

See [Chapter 8, “Basic Wireless Device Configuration”](#) for upgrade information.

Power Over Ethernet

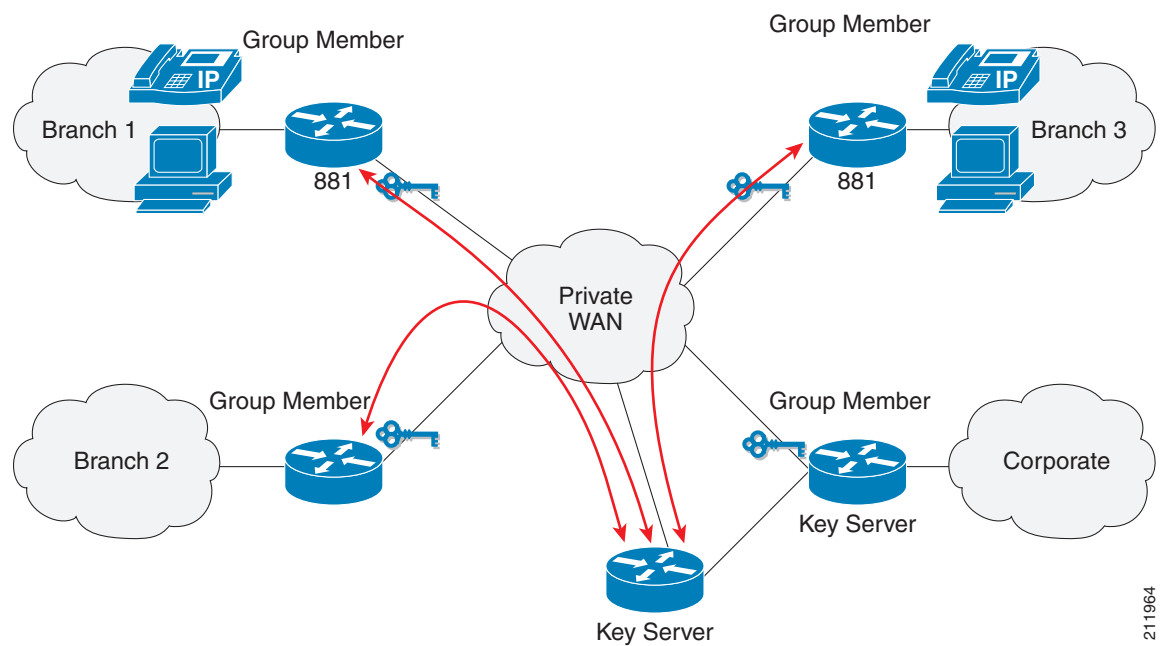
All Cisco 880 Series ISRs contain Power Over Ethernet (PoE) capabilities. See the [Cisco 860 Series, Cisco 880 Series, and Cisco 890 Series Integrated Services Routers Hardware Installation Guide](#) for details.

Enterprise Small Branch

Figure 15-1 shows an Enterprise Small Branch deployment that uses the following technologies and features:

- Group Encrypted Transport VPN (GETVPN) for highly scalable secure branch connectivity
- Cisco IOS firewall (FW) policies that secure the front line of network connectivity and provide network and application layer protection to the enterprise network
- Voice and multicast applications
- Quality of service (QoS) prioritizes critical applications and ensures timely delivery of latency-sensitive and mission-critical applications

Figure 15-1 Enterprise Small Branch

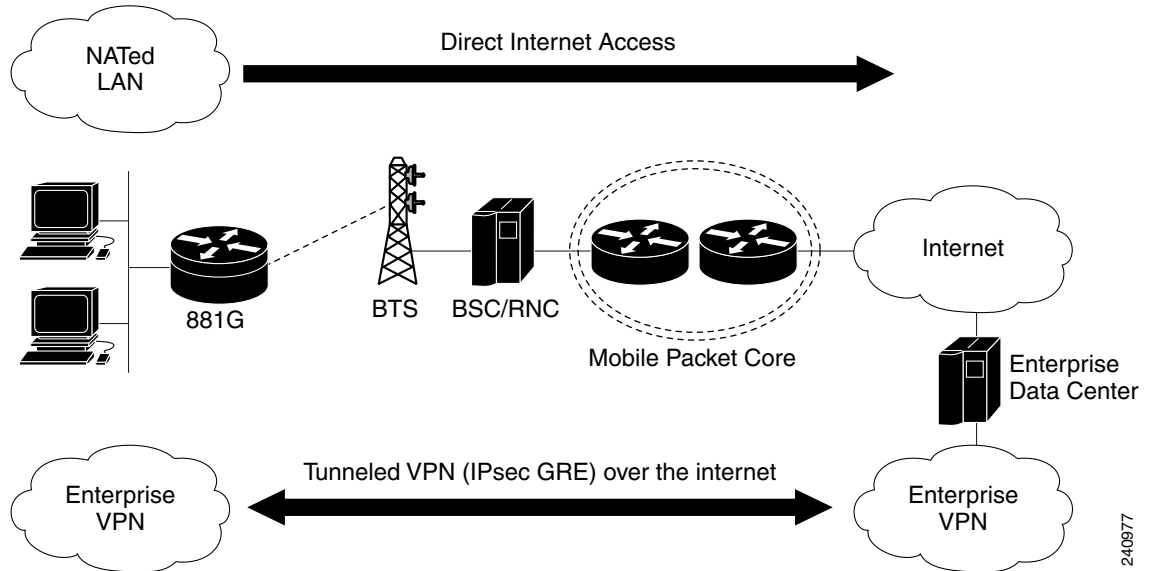


211964

Internet Service and IPSec VPN with 3G

Figure 15-2 shows a remote office deployment that uses 3G wireless technology for both backup and primary applications to communicate to their enterprise data center. Besides providing direct Internet access employing Network Address Translation (NAT), Cisco 880 series ISRs can provide tunneled Virtual Private Network (VPN) service using IP Security and Generic Routing Encapsulation (IPSec+GRE) for secure and private communication over the public Internet.

Figure 15-2 Internet Service and IPSec VPN with 3G

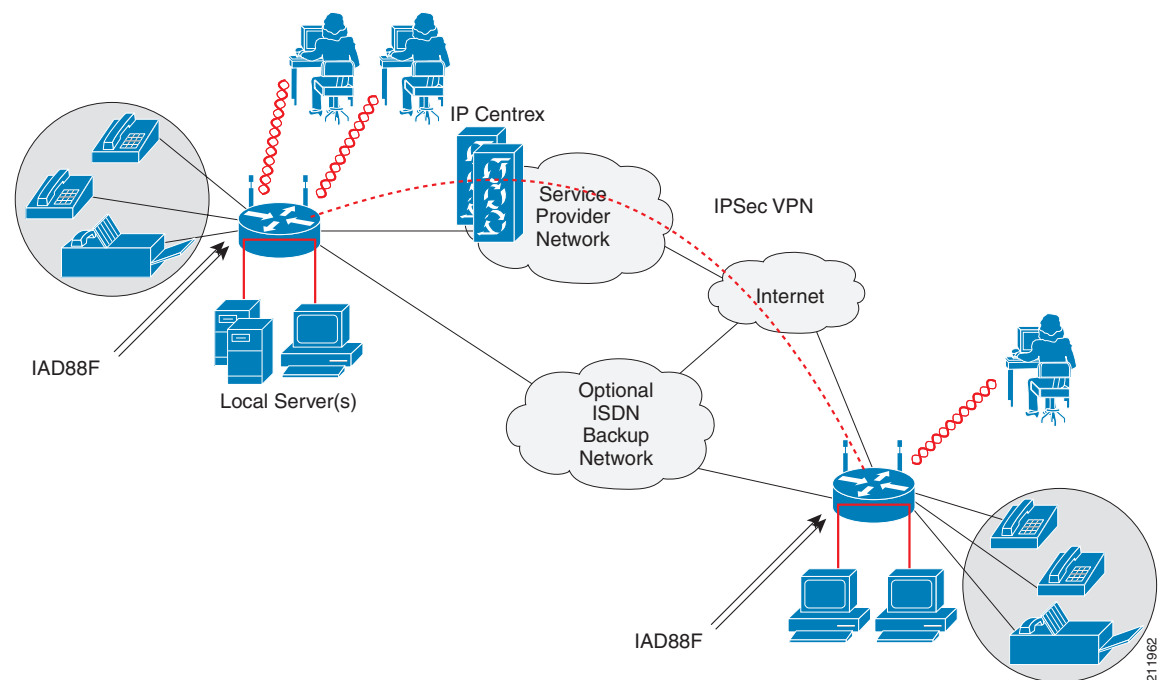


SMB Applications

Figure 15-3 shows a small-to medium-size business deployment (SMB) that uses the following technologies and features at each branch office:

- Easy VPN with Virtual Tunnel Interface (VTI) to simplify secure VPN for remote offices and teleworkers.
- Deep packet inspection firewall for security. Firewalls provide the first level of access checking. They work with other security technologies, including intrusion prevention, encryption, and endpoint security, to provide a well-rounded defense-in-depth enterprise security system.
- Inline Intrusion Prevention Systems (IPS) protection provides additional security, and is a core facet of the Cisco Self-Defending Network, Cisco IOS IPS helps enable the network to defend itself with the intelligence to accurately classify, identify, and stop or block malicious or damaging traffic in real time.
- QoS provides timely delivery of latency-sensitive and mission-critical applications.
- ISDN connectivity backup provides network redundancy in the event that the primary service provider link fails.
- Support for existing analog voice and fax capabilities.

Figure 15-3 Small-to Medium-Size Business



Enterprise Wireless Deployments with LWAPP

Figure 15-4 shows an Enterprise wireless LAN deployment using Lightweight Access Point Protocol (LWAPP) and the following technologies and features:

- Broadband Internet access and VPN connection to a central site.
- Hybrid Remote Edge Access Point (H-REAP) provides wireless LAN services to remote and branch offices without using a wireless LAN controller at each location. With HREAP, organizations can bridge traffic locally, tunnel traffic over the WAN, or tunnel traffic over LWAPP on a per Service Set Identifier (SSID).
- Dynamic RF management with Cisco Wireless Control System (WCS).
- The ability to mix and match embedded access points with external access points.

Figure 15-4 Wireless LAN with LWAPP

