Business Data Communications & Networking:

12th Edition

Chapter 9: Wide Area Networks

Sadiq M. Sait, PhD
Professor
College of Computing Science and Mathematics
Director, Office of Planning & Quality

Fall 2023

PROLOGUE

The Wide Area Network (WAN) is a key part of the enterprise edge.

- Most organizations **do not build their own WAN** communication circuits, preferring to lease them from common carriers (STC, ITC, etc) or to use the Internet.
  - They use a dedicated-circuit network, the user leases circuits from the common carrier for his or her exclusive use 24 hours per day, 7 days per week.
  - Dedicated circuits are like having **your own private network**, **but it is managed by the common carrier**.

- This chapter focuses on the **WAN architectures and telecommunications services common carriers offer for use in enterprise WANs**, not the underlying technology that the carriers use to provide them.
- We discuss the three principal types of WAN services that are available:
  - dedicated-circuit services,
  - packet-switched services, and
  - virtual private network (VPN) services.

- Finally, again, we talk about how to improve WAN performance and how to select services to build WANs.

9.1 INTRODUCTION

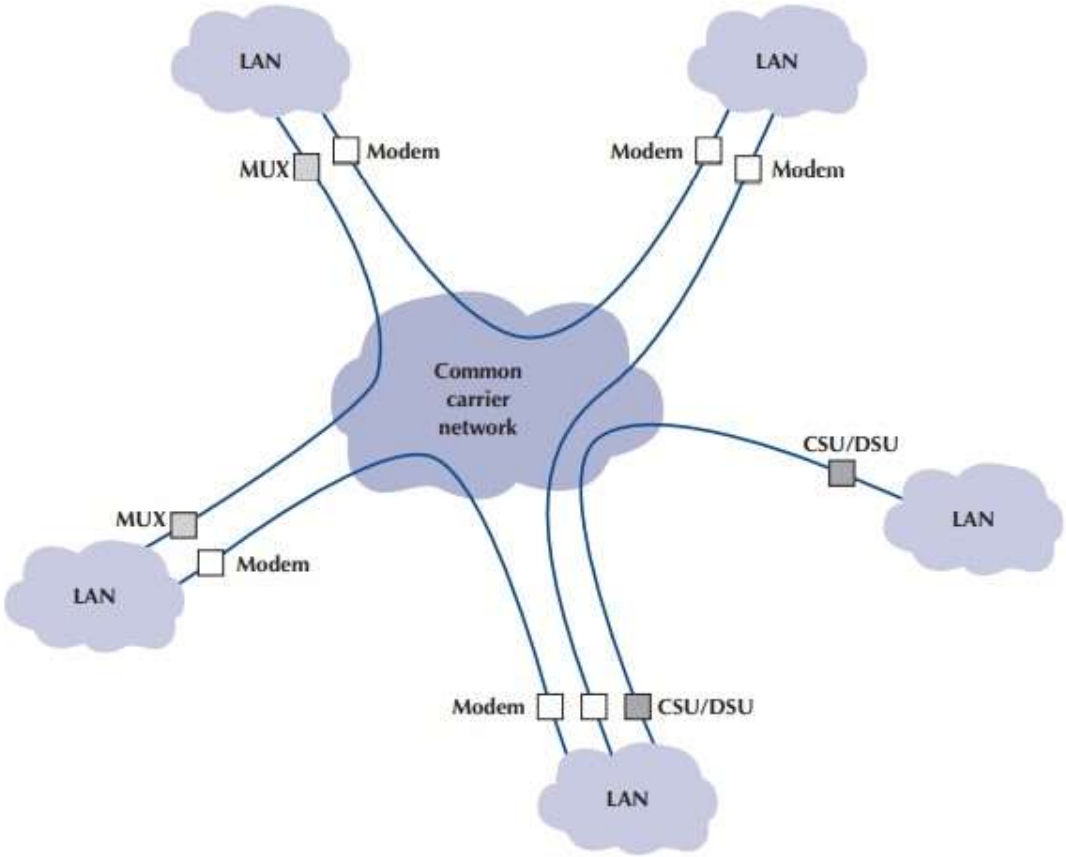
- Wide area networks (WANs) **typically run long distances**, connecting different offices in different cities or countries.
- Some WANs run much shorter distances, connecting different buildings in the same city.
- As a customer, **you do not lease physical cables per se**; **you simply lease circuits that provide certain transmission characteristics**.
- The **carrier** decides whether to use twisted-pair cable, coaxial cable, fiber optics, or other media for its circuits.
- Common carriers are profit-oriented, and their primary products are **services for voice and data transmissions**, both over traditional wired circuits as well as cellular services.
- Most countries have a federal government agency that **regulates** data and voice communications.
- We discuss two WAN services that use common carrier networks (**dedicated-circuit services and packet-switched services**) and one that uses the **public Internet (a virtual private network).**

9.2.1 DEDICATED-CIRCUITS NETWORKS: Basic Architecture

- Dedicated-circuit network: Here you lease circuits from common carriers.
- **All connections are point to point.**
- **The carrier (company) installs the circuit connections at the two end points** of the circuit and makes the connection between them.
- **The circuits run through the common carrier's cloud**, **but the network behaves as if you have your own physical circuits running point-to-point**.
- The **user installs the equipment needed** to connect computers and devices (e.g., routers or switches) to the circuit.
- This equipment may include **multiplexers or a channel service unit (CSU) and/or a data service unit (DSU); a CSU/DSU is the WAN equivalent of a NIC in a LAN.**
  - The device takes the outgoing packet (usually an Ethernet packet at the data link layer and an IP packet at the network layer) and **translates** it to use the data link layer and network protocols used in the WAN.
- **Dedicated circuits are billed at a flat monthly fee, and the user has unlimited use of the circuit.**
- Once you sign a contract, making changes can be expensive because it means rewiring the buildings and signing a new contract with the carrier.
- Therefore, **dedicated circuits require careful planning**, both in terms of locations and the amount of capacity you purchase.

9.2.1 DEDICATED-CIRCUITS NETWORKS: Basic Architecture

FIGURE 9-1
Dedicated-circuit services.
CSU = channel service unit; DSU = data service unit; and MUX = multiplexer



9.2.1 DEDICATED-CIRCUITS NETWORKS: Basic Architecture

There are three basic architectures used in dedicated-circuit networks:

- **Ring Architecture:** All computers are connected in a closed loop.
- The circuits are full-duplex or half-duplex circuits, meaning that messages flow in both directions around the ring. **Computers in the ring may send data in one direction or the other, depending on which direction is the shortest to the destination.**
- One **disadvantage** of the ring topology is that messages can take a **long time to travel** from the sender to the receiver.
- Messages usually travel through several computers and circuits before they reach their destination, so traffic delays can build up very quickly if one circuit or computer becomes overloaded.
- In general, the failure of any one circuit or computer in a ring network means that the network can continue to function. Messages are simply routed away from the failed circuit.

9.2.1 Ring Architecture

FIGURE 9-2 Ring-based design

9.2.1 DEDICATED-CIRCUITS NETWORKS: Basic Architecture (contd)

- **Star Architecture:** **All** computers are connected to **one central computer** that routes messages to the appropriate computer (Figure 9-3).
- The star topology is **easy to manage** because the **central computer receives and routes all messages** in the network.
- It **can also be faster** than the ring network because any message needs to travel through at most **two** circuits.
- However, the star topology is the **most susceptible to traffic problems** because the central computer must process all messages on the network.
- The **central computer must have sufficient capacity to handle traffic peaks**, or it may become overloaded, and network performance will suffer.
- In general, the failure of any one circuit or computer affects only the one computer on that circuit.
- However, if the central computer fails, the entire network fails because all traffic must flow through it. It is critical that the central computer be extremely reliable

9.2.1 Star Architecture

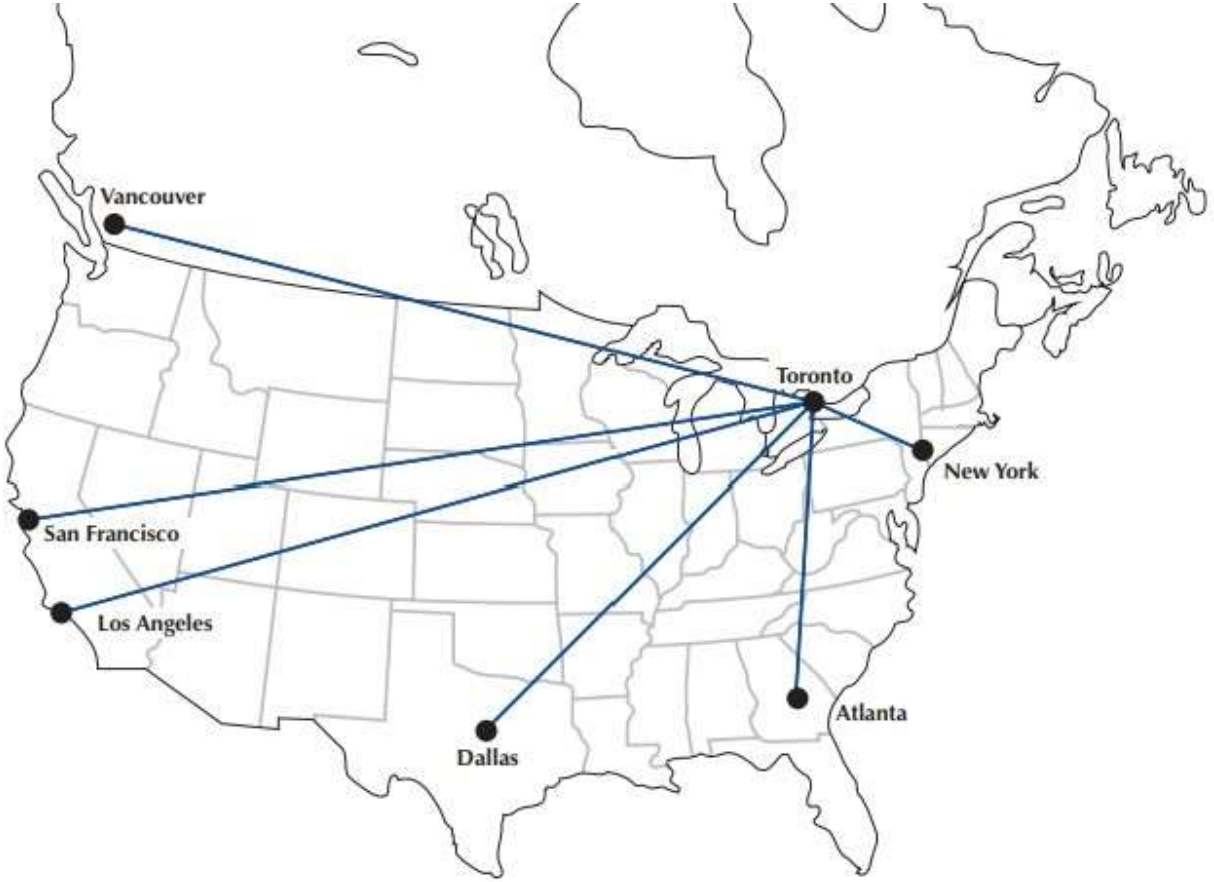
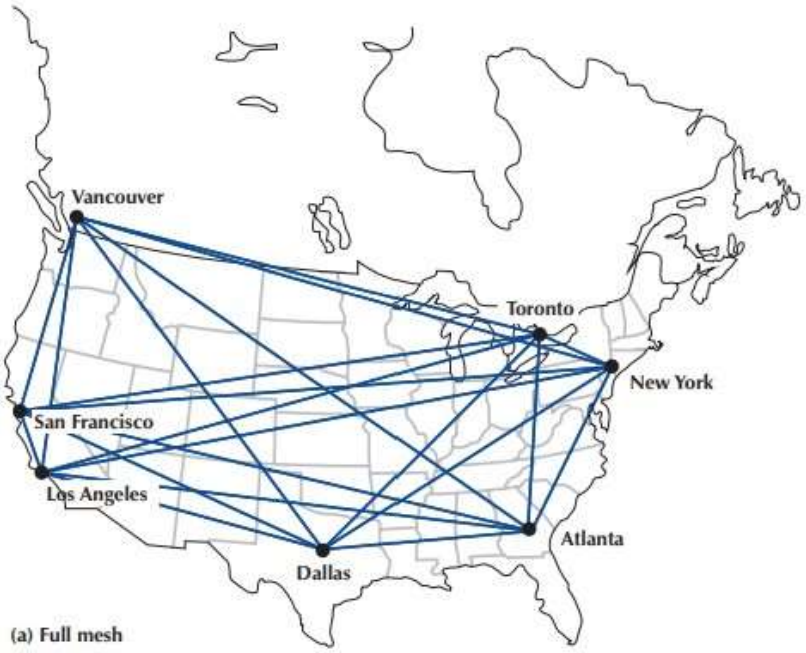


FIGURE 9-3 Star-based design

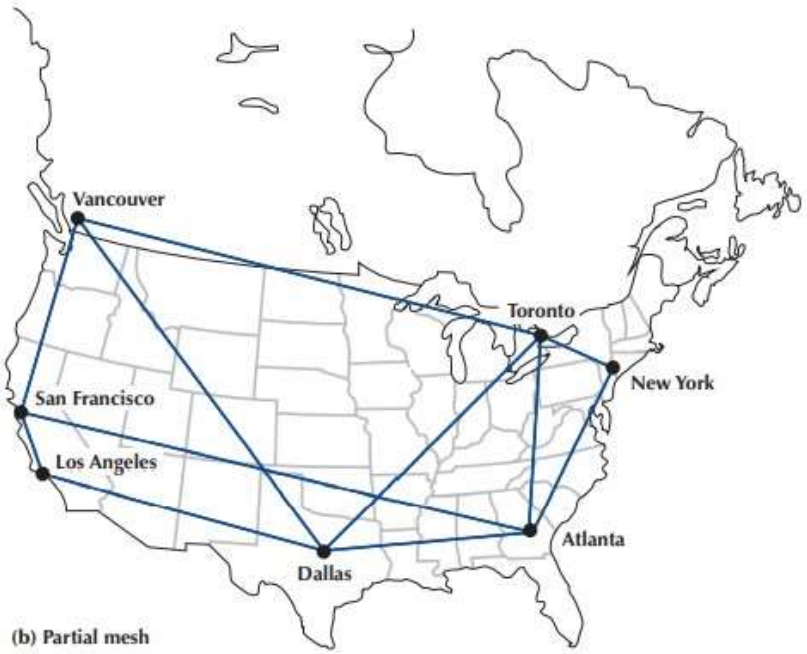
9.2.1 DEDICATED-CIRCUITS NETWORKS: Basic Architecture (contd)

- **Mesh Architecture:**
- **Full Mesh:** Every computer is connected to every other computer (cost).
- **Partial Mesh:** This is far more common. Most WANs use partial-mesh topologies.
- If there are many possible routes through the network, the loss of one or even several circuits or computers may have **few** effects beyond the specific computers involved.
- **In general, mesh networks combine the performance benefits of both ring networks and star networks.**
- Mesh networks usually provide relatively short routes through the network (compared with ring networks) and **provide many possible routes through the network.**
- The **drawback** is that mesh networks use **decentralized routing** so that each computer in the network performs its own routing.
- This **requires more processing by each computer in the network** than in star or ring networks.
  - **Also, the transmission of network status information (e.g., how busy each computer is) "wastes" network capacity.**

9.2.1 Mesh Architecture



(a) Full mesh



(b) Partial mesh

9.2.2 T CARRIER SERVICES

- There are two types of dedicated-circuit services in common use today: **T carrier services and synchronous optical network (SONET) services**.
- T carrier circuits are the most commonly used form of dedicated-circuit services
- Costs are a fixed amount per month, regardless of how much/little traffic.
- There are several types of T carrier circuits, as shown in Figure 9-5, but only **T1 and T3 are in common use today**.
- T1 circuits can be used to transmit data but often are **used to transmit both data and voice.**
  - In this case, inverse TDM provides 24 64-Kbps circuits.
  - **One Digitized voice using PCM requires a 64-Kbps circuit so a T1 circuit enables 24 simultaneous voice channels.**
  - Most common carriers make extensive **use of PCM**
  - **A T3 circuit allows transmission at a rate of 45 megabits per second. (28 T1 circuits).**
  - T3 circuits are becoming popular in MANs and WANs because of their higher data rates.
  - Fractional T1, sometimes **called FT1**, offers portions of a 1.544-Mbps T1 circuit for a fraction of its full cost.
  - The most common FT1 services provide 128 Kbps, 256 Kbps, 384 Kbps, 512 Kbps, and 768 Kbps.

9.2.2 SONET

- The **synchronous optical network (SONET)** is the American standard (ANSI) for high-speed dedicated-circuit services.
- **The ITU-T recently standardized an almost identical service that easily interconnects with SONET under the name synchronous digital hierarchy (SDH).**
- SONET transmission speeds begin at the OC-1 level (optical carrier level 1) of **51.84 Mbps**.
- Each succeeding rate in the SONET fiber hierarchy is defined as a **multiple of OC-1**, with SONET data rates defined as high as 160 Gbps.
- Figure 9-6 presents the commonly used SONET and SDH services.
- **Each level above OC-1 is created by an inverse multiplexer**.
- Notice that the slowest SONET transmission rate (OC-1) of 51.84 Mbps is slightly faster than the T3 rate of 44.376 Mbps

9.2.2 T Carrier and SONET

FIGURE 9-5
T carrier services

T Carrier Designation	DS Designation	Speed
FT1	DS0	64 Kbps
T1	DS1	1.544 Mbps
T2	DS2	6.312 Mbps
T3	DS3	44.376 Mbps
T4	DS4	274.176 Mbps

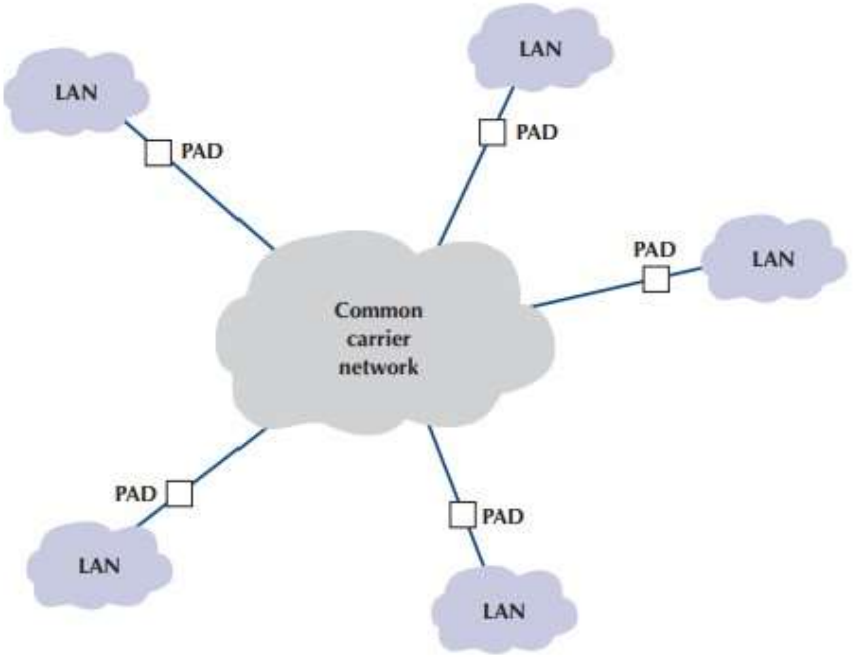
FIGURE 9-6
SONET (synchronous optical network) and SDH (synchronous digital hierarchy) services. OC = optical carrier (level)

SONET Designation	SDH Designation	Speed
OC-1		51.84 Mbps
OC-3	STM-1	155.52 Mbps
OC-12	STM-4	622.08 Mbps
OC-24	STM-8	1.244 Gbps
OC-48	STM-16	2.488 Gbps
OC-192	STM-24	9.953 Gbps
OC-768	STM-256	39.813 Gbps
OC-3072	STM-1024	159.25 Gbps

9.3 PACKET-SWITCHED NETWORKS

- Packet-switched networks operate more like Ethernet and IP networks used in the LAN and BN than like dedicated circuit networks.
- With dedicated-circuit networks, a circuit is established between the two communicating routers that provide a guaranteed data transmission capability that is available for use by only those two devices.
- In contrast, packet-switched services enable **multiple connections** to exist **simultaneously between computers over the same physical circuit, just like LANs and BNs.**

FIGURE 9-7
Packet-switched services. LAN = local area network and PAD = packet assembly/disassembly device



9.3.1 BASIC ARCHITECTURE

- With packet-switched services, the user buys a **connection** into the common carrier cloud (Figure 9-7).
- The **user pays a fixed fee for the connection into the network** (depending on the type and capacity of the service) **and is charged for the number of packets transmitted.**
- The user's connection to the network is a **packet assembly/disassembly device (PAD).**
- **The PAD converts the sender's data into the network layer and data link layer packets and sends them through the packet-switched network.**
- At the other end, another PAD reassembles the packets back into the network layer and data link layer protocols expected by the destination (usually Ethernet and IP) and delivers them to the appropriate computer router.
- One of the key **advantages** of packet-switched services is that different locations can have **different connection speeds** into the common carrier cloud.
- The PAD compensates for differences in transmission speed between sender and receiver; for example, the circuit at **the sender might be 50 Mbps**, **whereas the receiver only has a 1.5 Mbps circuit**. In contrast, a dedicated circuit must have the same speed at both the sender and receiver.

9.3.1 BASIC ARCHITECTURE (contd).

- Packet-switched networks enable packets from **separate messages** with different destinations to be **interleaved** for transmission, unlike dedicated circuits, which have one sender and one receiver.
- The connections between the different locations in the packet network are called **permanent virtual circuits** (**PVCs**), which means that they are defined for frequent and consistent use by the network.
- They do not change unless the network manager changes the network.
- **Changing PVCs is done using software**, but **common carriers** usually **charge each time a PVC is established or removed.**
- **Packet-switched services are often provided by different common carriers than the one from which organizations get their usual telephone and data services.**
- Therefore, organizations often lease a dedicated circuit (e.g., T1) from their offices to the packet-switched network **point of presence (POP).**
- The POP is the **location** at which the **packet-switched network (or any common carrier network, for that matter) connects to the local telephone exchange.**

9.3.2-5 OTHER Services

- **Frame Relay Services:** Most commonly used WANs, like wired Ethernet LANs, it is **unreliable because it does not perform error control, just discard erroneous packets, no QoS capabilities.**
- **Ethernet Services: These are somewhat popular. Provided by Ethernet Service Offering companies who have their own Gigabit Ethernet network.**
- **MPLS Services:** Multiprotocol label switching (MPLS) is another relatively new WAN technology that is designed to work with a variety of commonly used layer-2 protocols.
- **IP Services: Many experts predict that in 5 years, IP services will be the only type of packet-switched services available in the market.**
  - Most IP services use **MPLS** as the data link layer protocol.

9.4 VIRTUAL PRIVATE NETWORKS (9.4.1 Basic Architecture)

- A virtual private network (VPN) provides the equivalent of a private packet-switched network over the public Internet.
- It involves establishing a series of PVCs that run over the Internet so that the network acts like a set of dedicated circuits even though the data flows over the Internet.
- With a VPN, you first lease an Internet connection for each location you want to connect. (e.g.,
  - T1 circuit from a common carrier that runs from your office to your ISP, or you may use a DSL or cable modem.
  - You pay the common carrier for the circuit and the ISP for the Internet.
  - Then you connect a VPN gateway (a special router) to each Internet access circuit to provide access from your networks to the VPN.
  - The VPN gateways enable you to create PVCs through the Internet that are called tunnels (Figure 9-8).
  - The VPN gateway at the sender takes the outgoing packet and **encapsulates** it with a protocol to move it through the tunnel to the VPN gateway on the other side (to strip the VPN packet and deliver).
  - The VPN is transparent to the users; it appears as though a traditional packet-switched network PVC is in use.
  - The VPN is also transparent to the ISP and the Internet as a whole; there is simply a stream of Internet packets moving across the Internet.

9.4.2 VPN Types

- Three types of VPNs are in common use: intranet VPN, extranet VPN, and access VPN.
- An intranet VPN provides virtual circuits between organization offices over the Internet. Figure 9-8 illustrates an intranet VPN.
  - Each location has a **VPN gateway** that connects the location to another location through the Internet.
  - An extranet VPN is the same as an intranet VPN, except that the VPN connects several different organizations, often customers and suppliers, over the Internet.
  - An **access VPN** enables employees to access an organization's networks from a remote location.
    - Employees have access to the network and all the resources on it in the same way as employees physically located on the network.
    - The user uses VPN software on his or her computer to connect to the VPN device at the office.
    - The VPN gateway accepts the user's log-in, establishes the tunnel, and the software forwards packets over the Internet.
    - Compared with a typical ISP-based remote connection, the access VPN is a more secure connection than simply sending packets over the Internet. Figure 9-9 shows an access VPN.

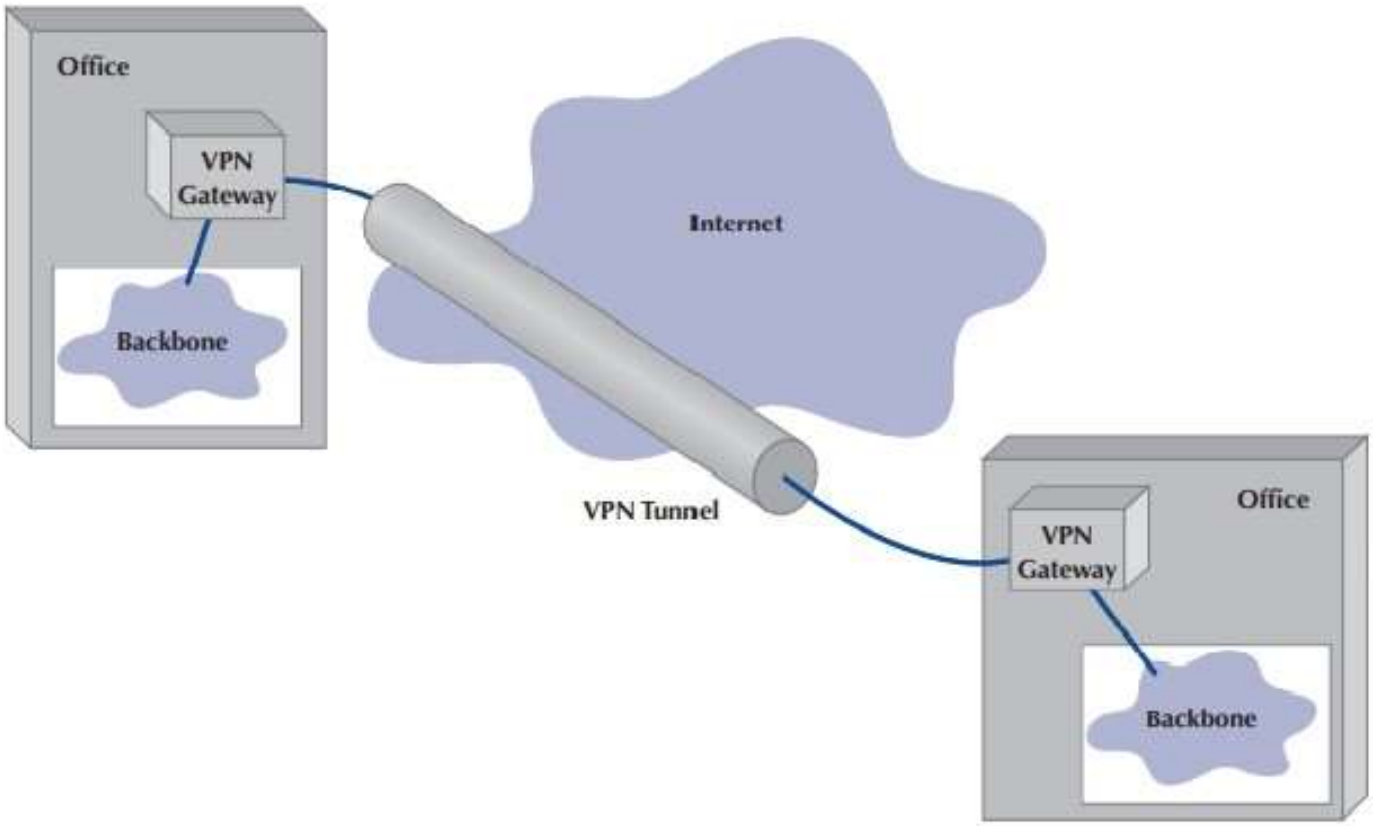


FIGURE 9-8 A virtual private network (VPN).
ISP = Internet service provider

9.4.3 How VPNs Work?

- When packets move across the Internet, they are much like postcards.
- VPNs provide security by **encapsulating** (i.e., surrounding) packets in a separate, secure packet that is **encrypted**.
- No one can read the encapsulated data without knowing the password that is used to decrypt the packet.
  - Layer-2 and layer-3 VPNs work very similarly, except that
    - layer-2 VPNs encapsulate the user's data starting with the **layer-2 packet** (**the Ethernet frame**) while
    - layer-3 VPNs encapsulate the user's data starting with the **layer-3 packet (the IP packet)**.
- Figure shows how a layer-3 access VPN using IPSec works. Suppose an employee is working at home wants to use the VPN, he or she starts the VPN software on his or her computer and uses it to log in to the VPN gateway at the office.
- The VPN software creates a new "**interface**" on the employee's computer that acts exactly like a **separate** connection into the Internet.
- Interfaces are usually hardware connections, but the **VPN is a software interface**, although the employee's computer doesn't know this—it's just another interface.
- Computers can have multiple interfaces; a laptop computer often has two interfaces, one for wire Ethernet and one for wireless Wi-Fi.

9.4.3 How VPNs Work? (contd)

- **The VPN gateway at the office is also a router and a DHCP server.**
- **The VPN gateway assigns an IP address to the VPN interface on the employee's computer that is an IP address in a subnet managed by the VPN gateway.**
  - For example, if the VPN gateway has an IP address of 156.56.198.1 and managed the 156.56.198.x subnet, it would assign an IP address in this subnet domain (e.g., 156.56.198.55).
- The employee's computer now thinks it has 2 connections to the Internet:
  - The VPN software on the employee's computer makes the VPN interface the **default** interface for all network traffic to and from the Internet, which ensures that all messages leaving the employee's computer flow through the VPN interface to the VPN gateway at the office.
  - Suppose the employee sends an HTTP request to a Web server at the office (or somewhere else on the Internet). The Web browser software will create an HTTP packet that is passed to the TCP software (which adds a TCP segment), and this, in turn, is passed to the IP software managing the VPN interface.
  - The IP software creates the IP packet using the source IP address assigned by the VPN gateway. Normally, the IP software would pass the IP packet to the Ethernet software that manages the Ethernet interface.

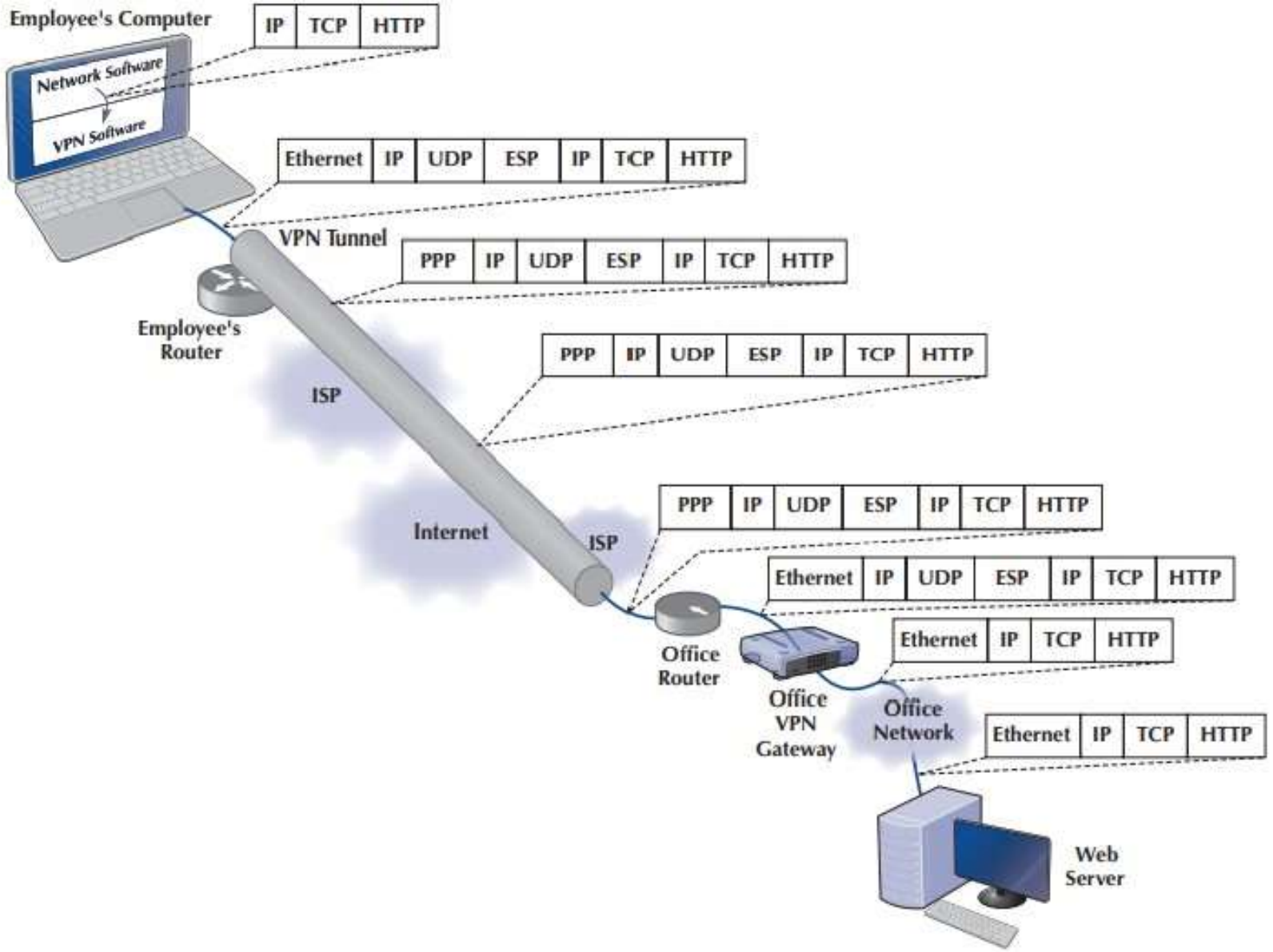


FIGURE 9-9 Using VPN software

9.4.3 How VPNs Work? (contd)

- Now **the IP packet is sent out the VPN interface, using the VPN software managing the VPN interface**.
- The VPN software receives the IP packet, encrypts it, and encapsulates it (and its contents: the TCP segment and the HTTP packet) with an **Encapsulating Security Payload (ESP) packet** using **IPSec encryption**.
- No one except the VPN gateway at the office can read and decrypt.
- **You can think of the IPSec packet as an application layer packet whose destination is the office VPN gateway.**
- How do we send an application layer packet over the Internet? Well, we pass it to the TCP software, which is exactly what the VPN software does.
- Normal Internet interface for transmission is used by the VPN software.
- UDP (instead of TCP) and PPP (since DSL uses PPP) are the protocols used.

9.5 THE BEST PRACTICE WAN DESIGN

- Developing best practice recommendations for WAN design is more difficult than for LANs and backbones because the network designer is buying services from different companies rather than buying products.
- In choice of technology, we use the same two factors as we have previously for LANs and backbones (effective **data rates** and **cost**), plus add one additional factor: **Reliability.**

9.6 IMPROVING WAN PERFORMANCE

- Improving the performance of WANs is handled in the same way as improving LAN performance. You begin by checking the devices in the network, upgrading the circuits between the locations, and changing the demand placed on the network (Figure 9-12)

FIGURE 9-12
Improving performance of metropolitan and local area networks

Performance Checklist

Increase Computer and Device Performance
- Upgrade devices
- Change to a more appropriate routing protocol (either static or dynamic)

Increase Circuit Capacity
- Analyze message traffic and upgrade to faster circuits where needed
- Check error rates

Reduce Network Demand
- Change user behavior
- Analyze network needs of all new systems
- Move data closer to users