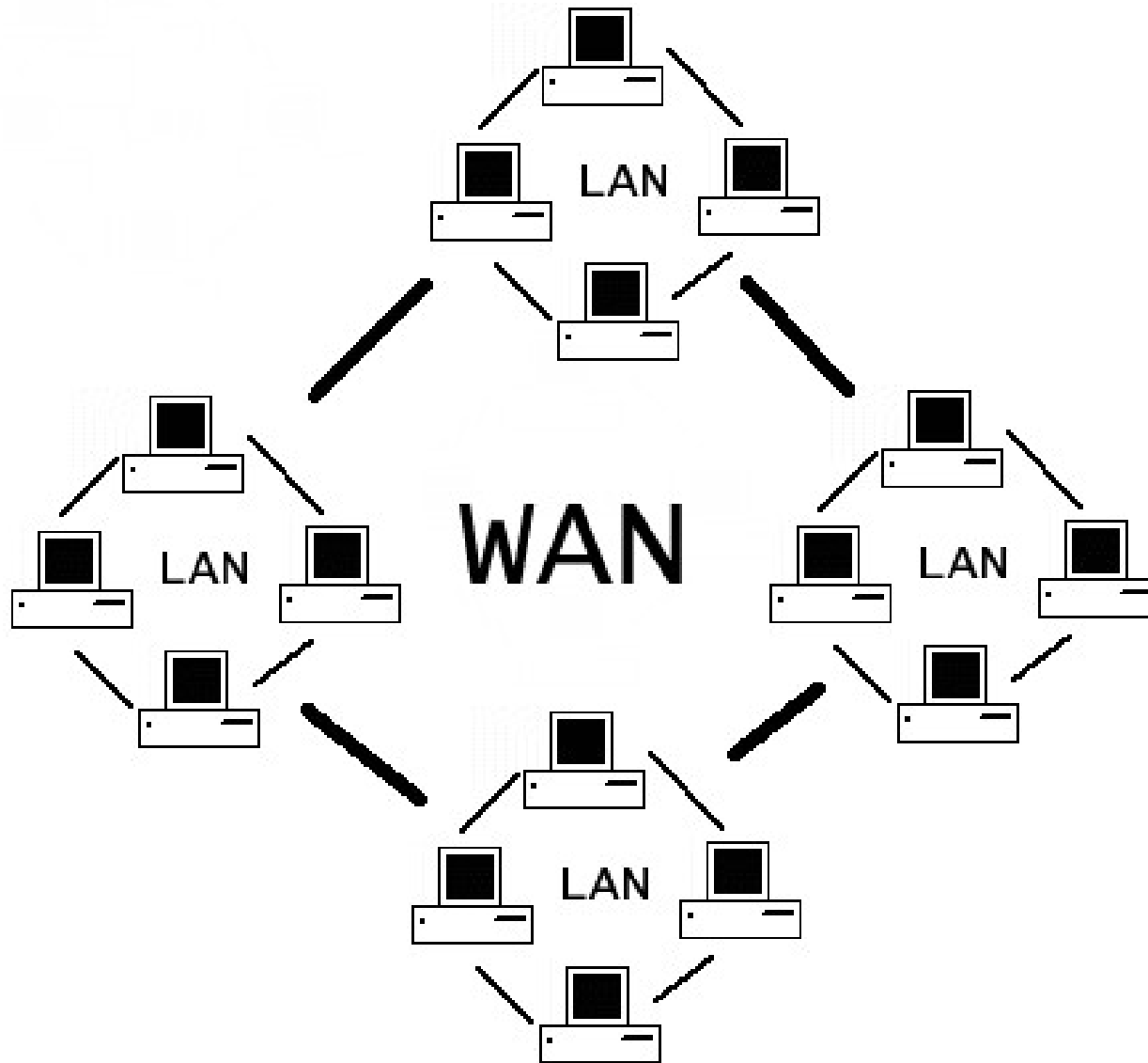




Data Communications and Networking

Lecturer: Toby Daniel

WANs, Leased Lines & VPNs



WANs

- Until fairly recently Wide Area Networks required an organisation to install their own long distance cables (expensive), or lease them from a telecommunications company.
- Leased lines, range from ISDN (integrated services digital network, 128 Kbps) to OC3 (Optical Carrier-3, 155 Mbps) fiber.
- They provide a company with a way to expand its private network beyond the LAN.

Leased Lines

- What advantages would leased lines have compared to a public medium like the Internet?



Leased Lines

- Private lines have obvious advantages over a public network like the Internet when it comes to:
 - Reliability
 - Performance
 - Security *
- However, maintaining a leased lines can become expensive. Cost rises as the distance between the offices increases.

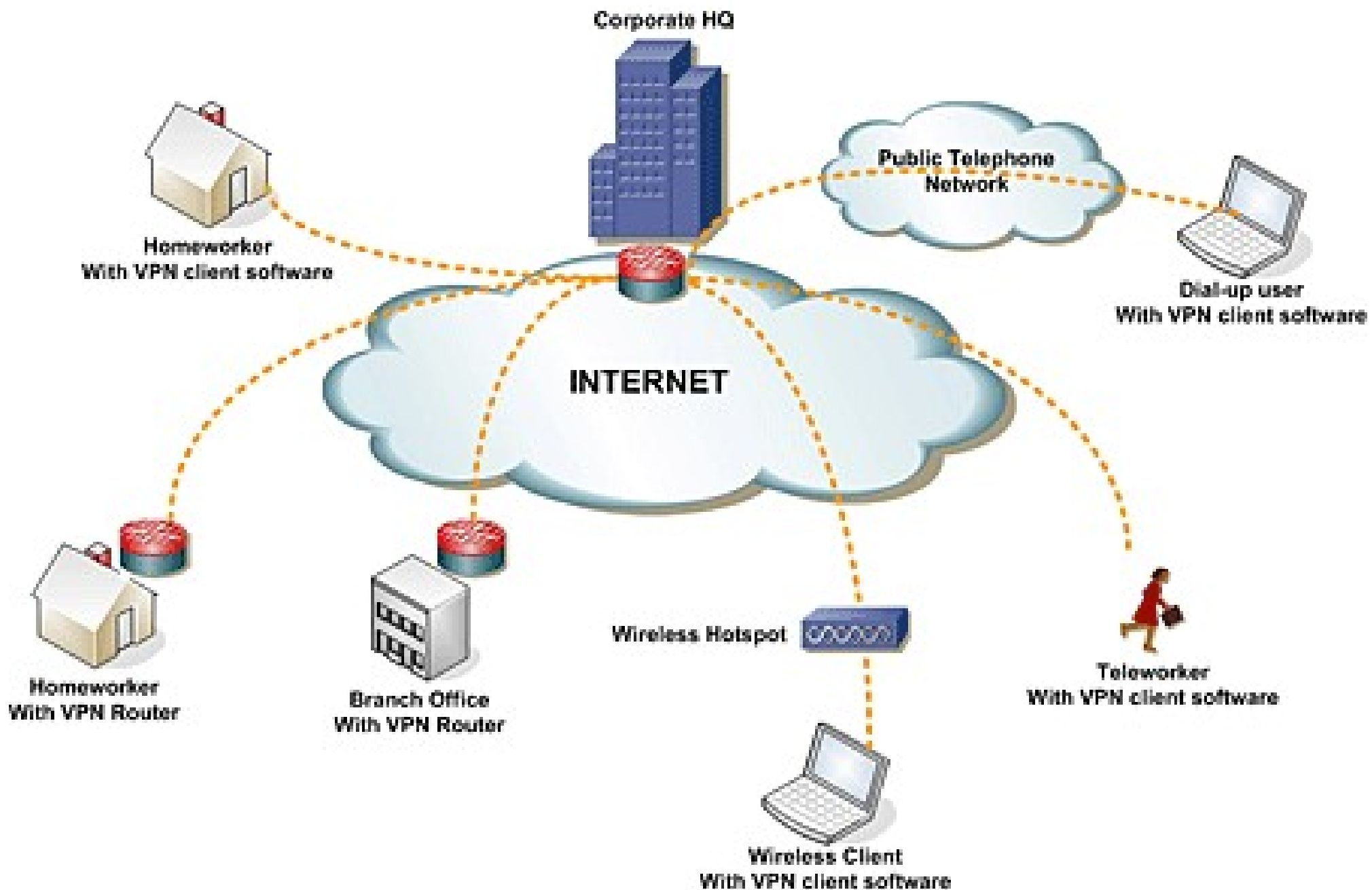
Turning to the Internet

- Over the last decade the speed and connectivity of the Internet has improved to a point where some companies have turned to the Internet as a way to connect remote offices together.
- To overcome the security problems with using a public network these WAN links use what are known as **VPNs**.

Virtual Private Networks.

VPN

- A VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together.
- Instead of using a dedicated, real-world connection such as leased line, a VPN uses **virtual connections** routed through the Internet.
- This can be used to connect the company's private network to a remote site or employee.



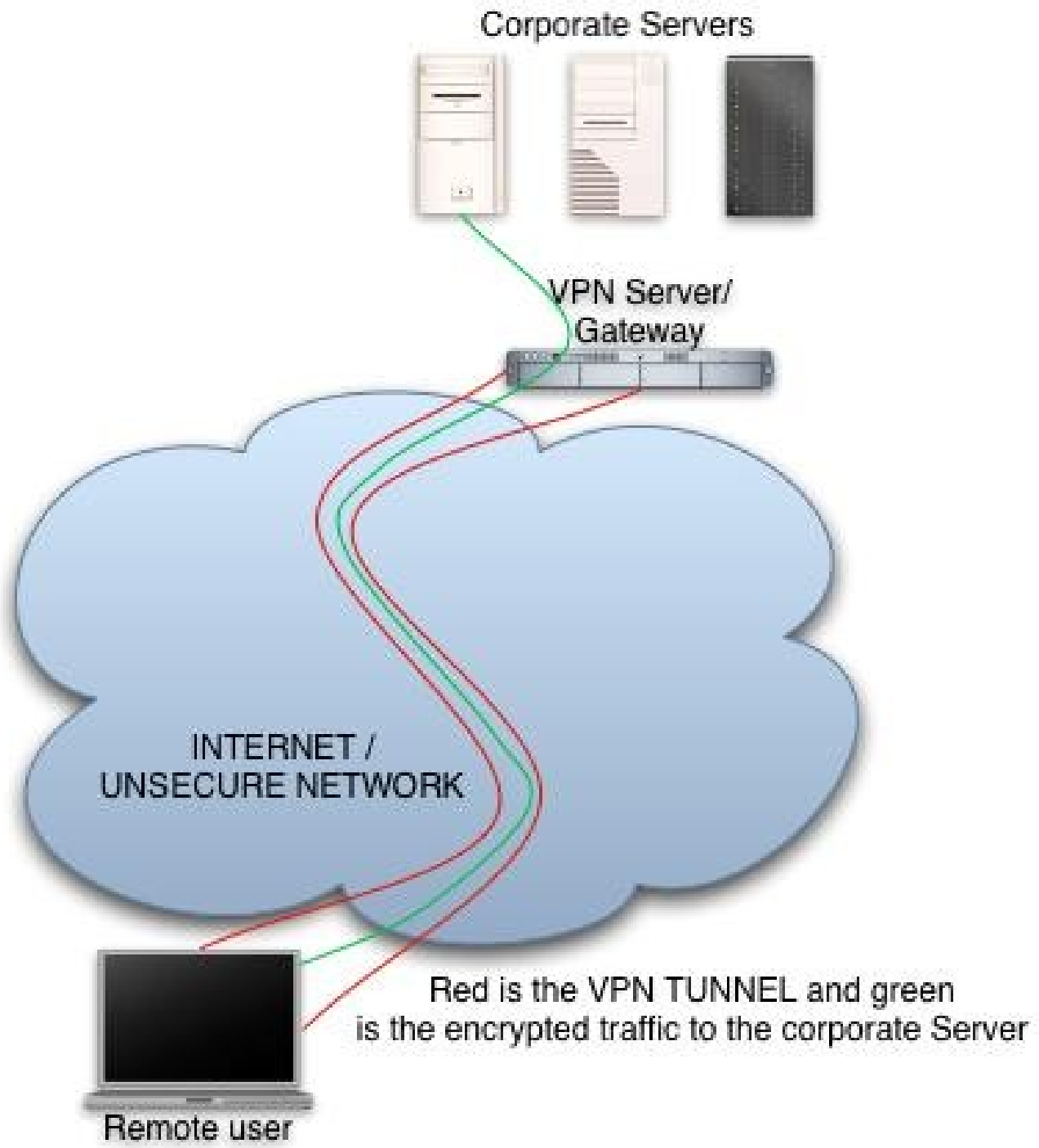
VPN types

There are two main types of VPN:

- Remote-Access VPN
- Site-to-Site VPN

Remote-access VPN

- **Remote-access**, also called a **virtual private dial-up network** (VPDN), is a user-to-LAN connection.
- It is used by a company that has employees who need to connect to the private network from various remote locations.
- The Internet is used as a Wide Area Network link between the two locations.



Site-to-Site VPN

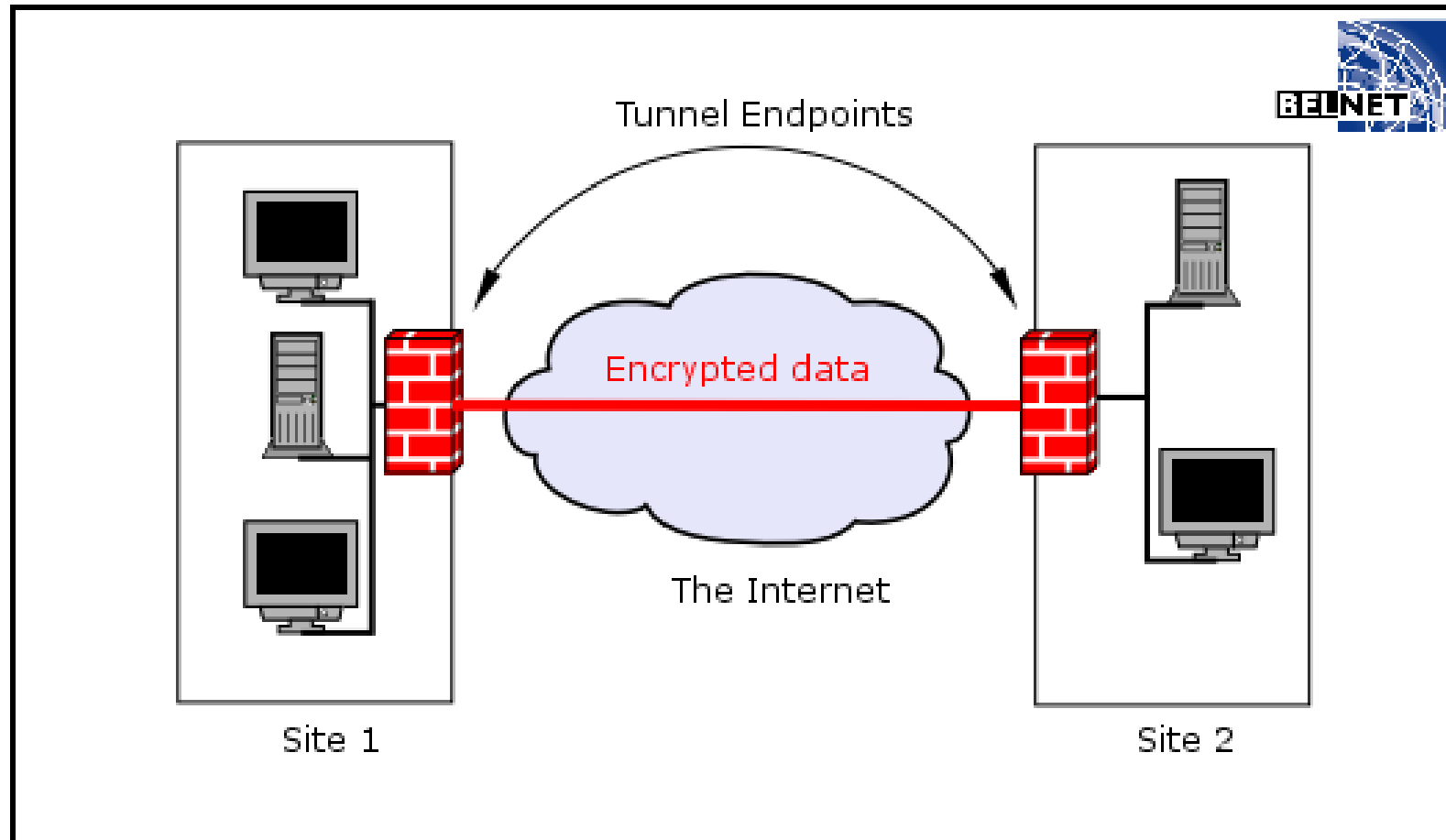
- Through the use of dedicated equipment a company can permanently connect multiple fixed sites over a public network.
- The Internet is used as a Wide Area Network link between the two locations.

Remote-access VPN

- The company uses a **Remote Access Server** which the employees connect to over the internet.
- They then use VPN client software to access the corporate network.
- What are the security concerns with sending information over the Internet?

Encryption and Tunneling

- To protect the information VPNs use Tunneling and Encryption.



Tunneling

- Most VPNs rely on tunneling to create a private network that reaches across the Internet.
- Tunneling is the process of placing an entire packet within another packet and sending it over a network.
- The protocol of the **outer** packet is understood by the network and both end points where the packet enters and exits the network.

Tunneling

Tunneling requires three different protocols:

- **Carrier protocol** - The protocol used by the network that the information is traveling over.
- **Encapsulating protocol** - The protocol that is wrapped around the original data.
- **Passenger protocol** - The original data (IPX, NetBeui, IP) being carried.

Tunneling

- A packet that uses a protocol not supported on the Internet (such as NetBeui) can be put inside an IP packet and sent safely over the Internet.
- Or you could put a packet that uses a private (non-routable) IP address inside a packet that uses a globally unique IP address to extend a private network over the Internet.

Tunneling Protocols

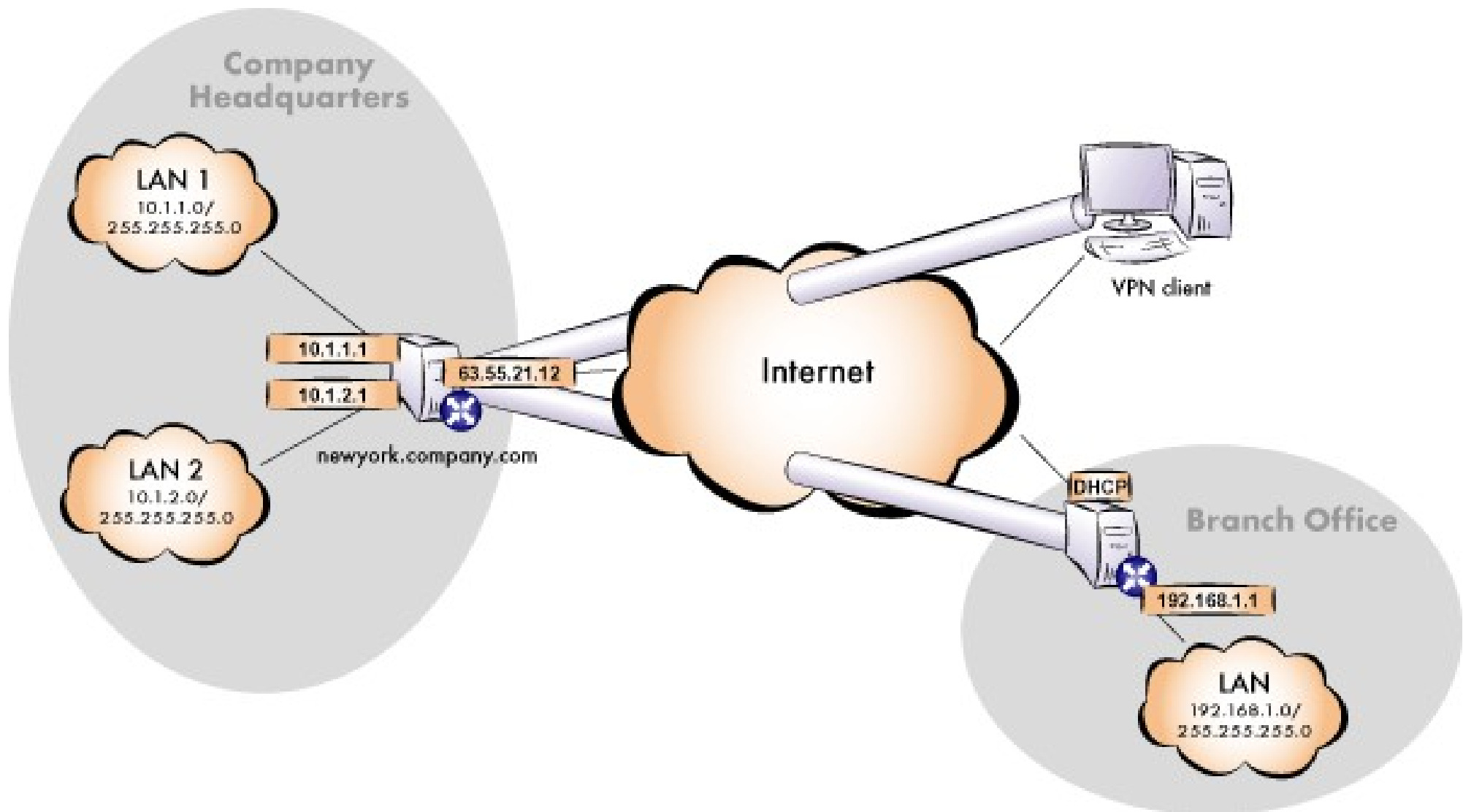
- Point-to-Point Tunneling Protocol (PPTP) is a protocol that is used to create VPN tunnels over IP networks.
- Layer 2 Tunneling Protocol (L2TP) is a newer protocol and provides additional security features.
- These Tunneling Protocols on their own do not provide strong security, encryption or authentication.

IPSec

- **Internet Protocol Security Protocol (IPSec)** provides security features such as encryption algorithms and authentication.
- IPSec is used to encrypt the data that is sent over a VPN.
- The encryption ensures that even if the information is copied, it can't be read.
- The most up-to-date protocols for VPNs are a combination of two protocols known as **L2TP/IPsec**.

IPSec Encryption

- IPSec uses **public-key encryption** technology. The sending and receiving devices share a public key with the server who has a secret private key.
- IPSec establishes a Security Association (SA) for each side of a connection between a client and server.
- The SA includes the parameters needed to communicate such as the type of encryption algorithm, a session key and an authentication algorithm.



VPNs

- What are the advantages and disadvantages of using a VPN?



Advantages of VPNs

- Encrypts all data from the client to the VPN server.
- Can compress data and speed up connections.
- Easy to use once it has been installed.
- Saves money compared to using a leased line.

Disadvantages of VPNs

- Does not encrypt anything beyond the VPN server.
- Encryption of every packet slows down the connection.
- The VPN has to be set up in advance.
- Internet link must be reliable at both ends.
- VPN link is not directly under the companies control.