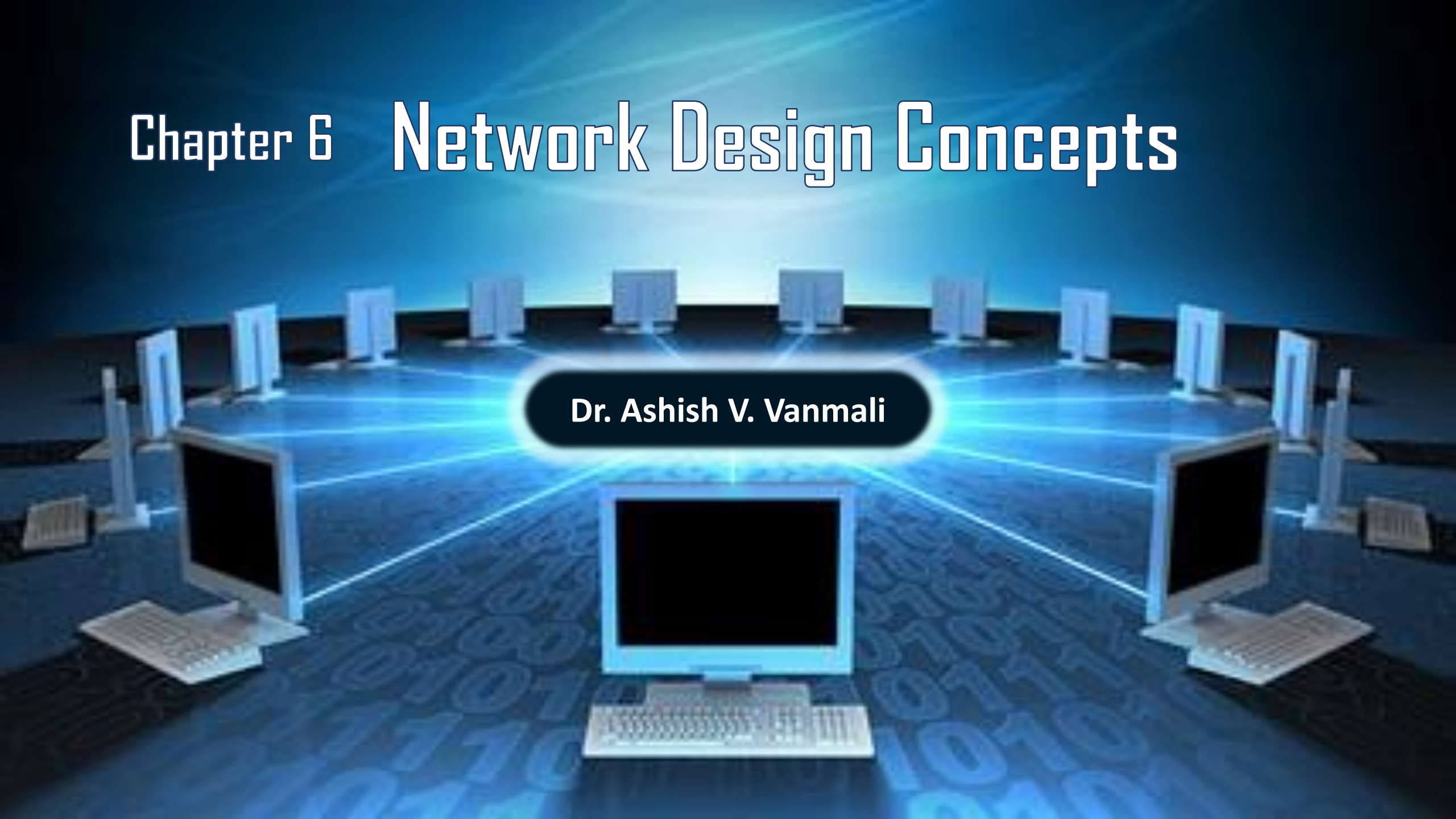
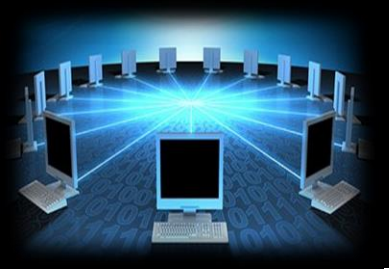
Chapter 6 Network Design Concepts

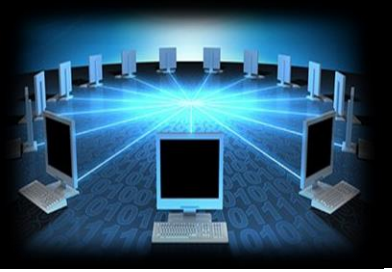


Dr. Ashish V. Vanmali



Outline of the Chapter

- Virtual LAN (VLAN)
- Virtual Private Network (VPN)



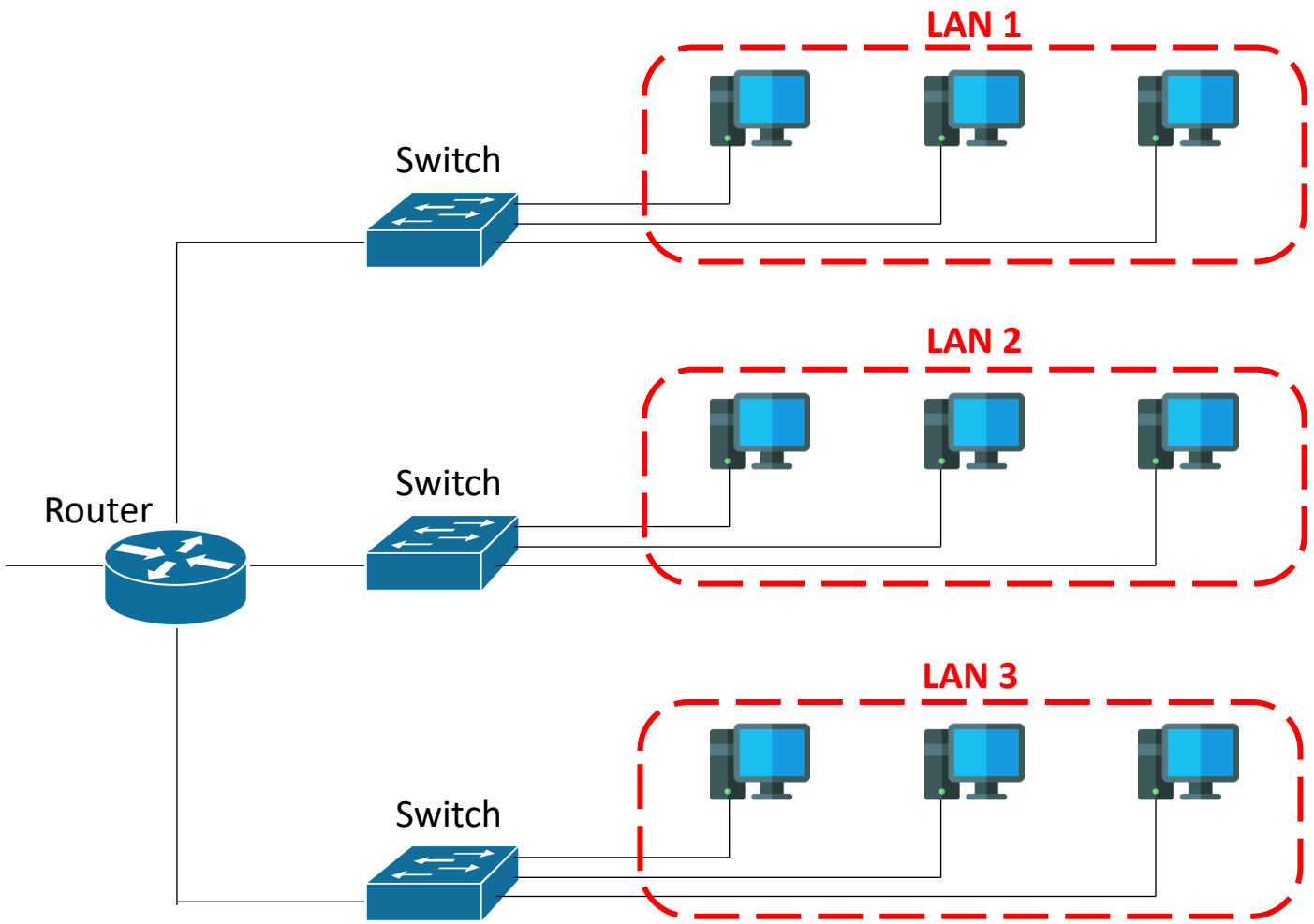
Virtual LAN (VLAN)

Virtual LAN (VLAN)

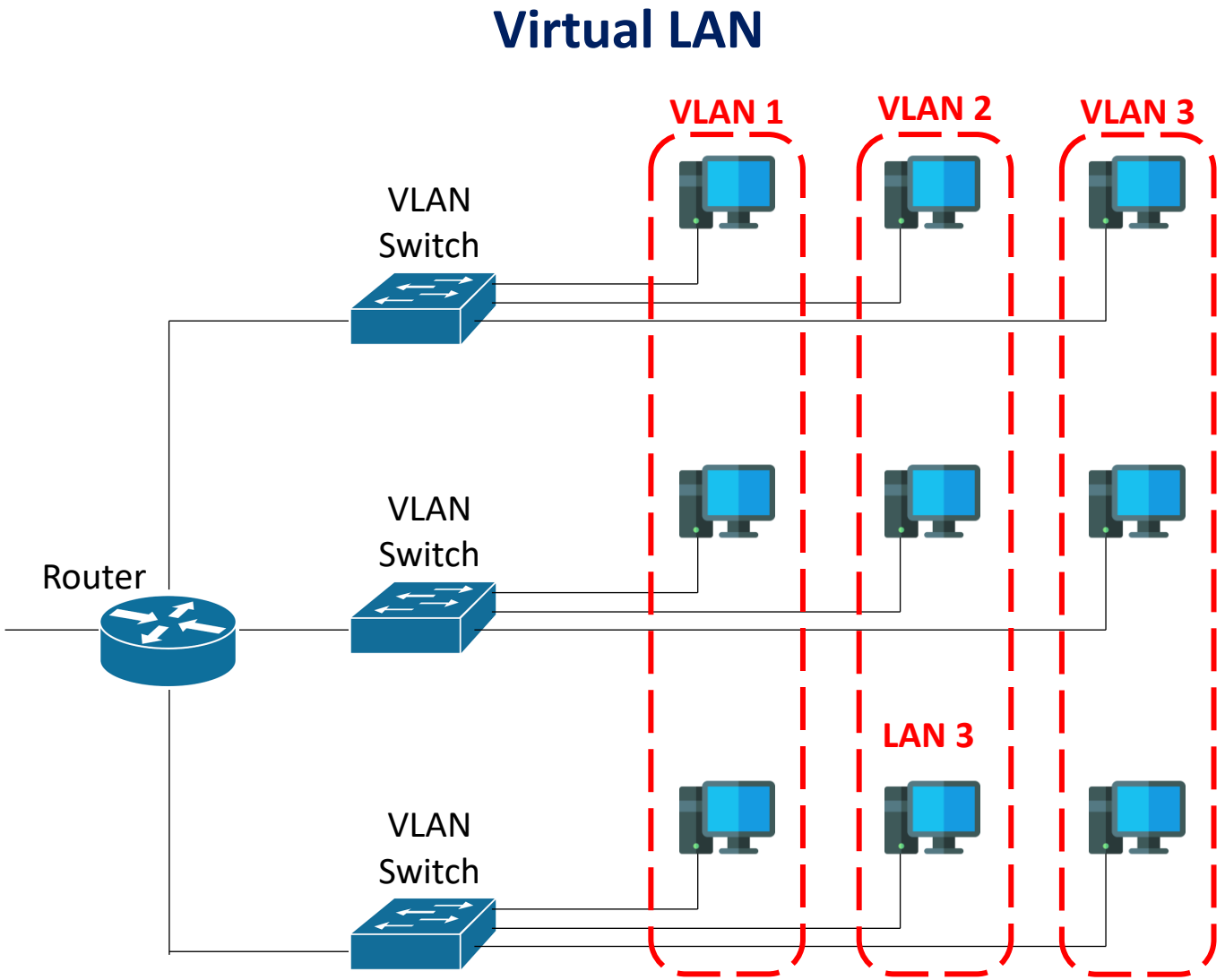
- A station is considered part of a LAN if it physically belongs to that LAN. The criterion of membership is geographic.
- In many cases we need a virtual connection between two stations belonging to two different physical LANs.
- A **Virtual Local Area Network (VLAN)** is defined as a local area network configured by software, not by physical wiring.

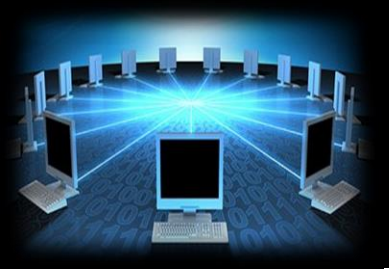
Virtual LAN (VLAN)

Traditional LAN



Virtual LAN (VLAN)

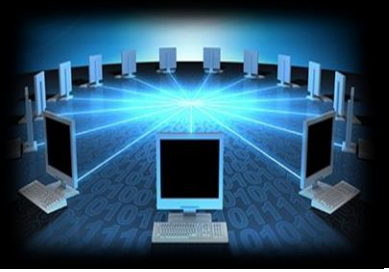




Virtual LAN (VLAN)

Features of VLANs

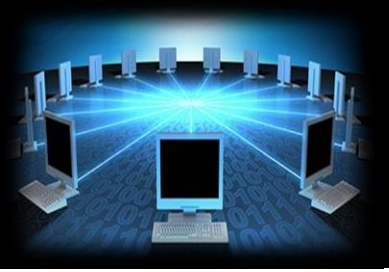
- VLANs group stations may belong to one or more physical LANs.
- VLAN creates a broadcast domain for the group stations.
- VLAN technology even allows the grouping of stations connected to different switches in the LAN.
- Since, VLANS are formed using software, rearrangement of groups is very easy compared to changing configuration of the physical network.
- VLANs provide an extra measure of security. Stations belonging to the same group can send broadcast messages with the guaranteed assurance that stations in the other group will not receive these messages.



Virtual LAN (VLAN)

VLAN Membership

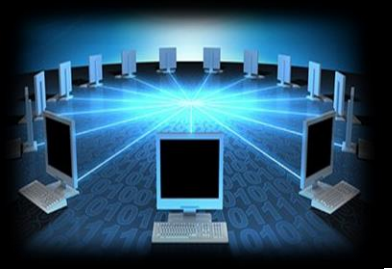
- Vendors use different characteristics such as port numbers, MAC addresses, IP addresses, IP multicast addresses, or a combination of two or more of these to define the membership of VLAN.
- Some VLAN vendors use **switch port numbers** as a membership characteristic. For example, the administrator can define that stations connecting to ports 1, 2, 3, and 7 belong to VLAN 1; stations connecting to ports 4, 10, and 12 belong to VLAN 2; and so on.
- Some VLAN vendors use the **48-bit MAC address** as a membership characteristic.
- Some VLAN vendors use the **32-bit IP address** as a membership characteristic.
- Some VLAN vendors use the **multicast IP address** as a membership characteristic.
- Recently, the software available from some vendors allows all these characteristics to be combined.



Virtual LAN (VLAN)

VLAN Configuration

- Stations are configured to VLAN in one of three ways: manual, semiautomatic, and automatic.
- In a **manual configuration**, the network administrator uses the VLAN software to manually assign the stations into different VLANs at setup. Later migration from one VLAN to another is also done manually.
- In an **automatic configuration**, the stations are automatically connected or disconnected from a VLAN using criteria defined by the administrator.
- A **semiautomatic configuration** is somewhere between a manual configuration and an automatic configuration. Usually, the initializing is done manually, with migrations done automatically.



Virtual LAN (VLAN)

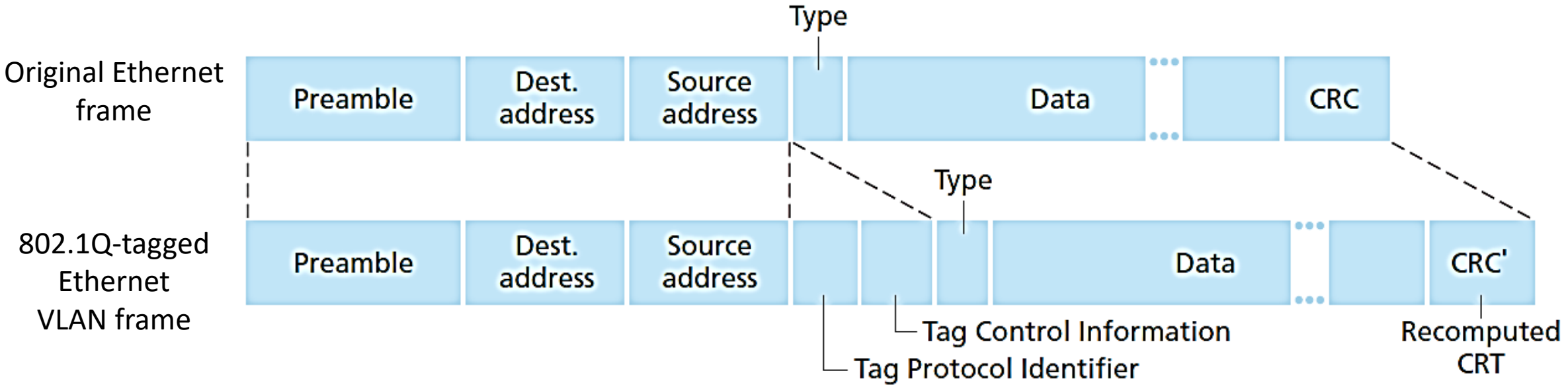
Communication Between Switches

- In a multi-switched backbone, each switch must know not only which station belongs to which VLAN, but also the membership of stations connected to other switches.
- Three methods have been devised for this purpose: table maintenance, frame tagging, and time-division multiplexing.
- In **Table Maintenance**, when a station sends a broadcast frame to its group members, the switch creates an entry in a table and records station membership. The switches send their tables to one another periodically for updating.
- In **Frame Tagging**, when a frame is traveling between switches, an extra header is added to the MAC frame to define the destination VLAN. The frame tag is used by the receiving switches to determine the VLANs to be receiving the broadcast message.
- In **Time-Division Multiplexing (TDM)**, the connection (trunk) between switches is divided into timeshared channels.

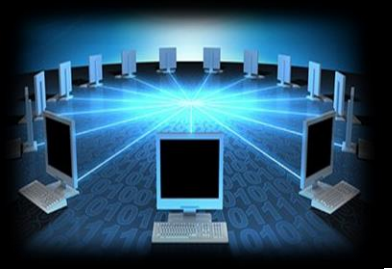
Virtual LAN (VLAN)

IEEE Standard

- In 1996, the IEEE 802.1 subcommittee passed a standard called 802.1Q that defines the format for frame tagging.
- The standard also defines the format to be used in multi-switched backbones and enables the use of multivendor equipment in VLANs.



Virtual Private Network (VPN)



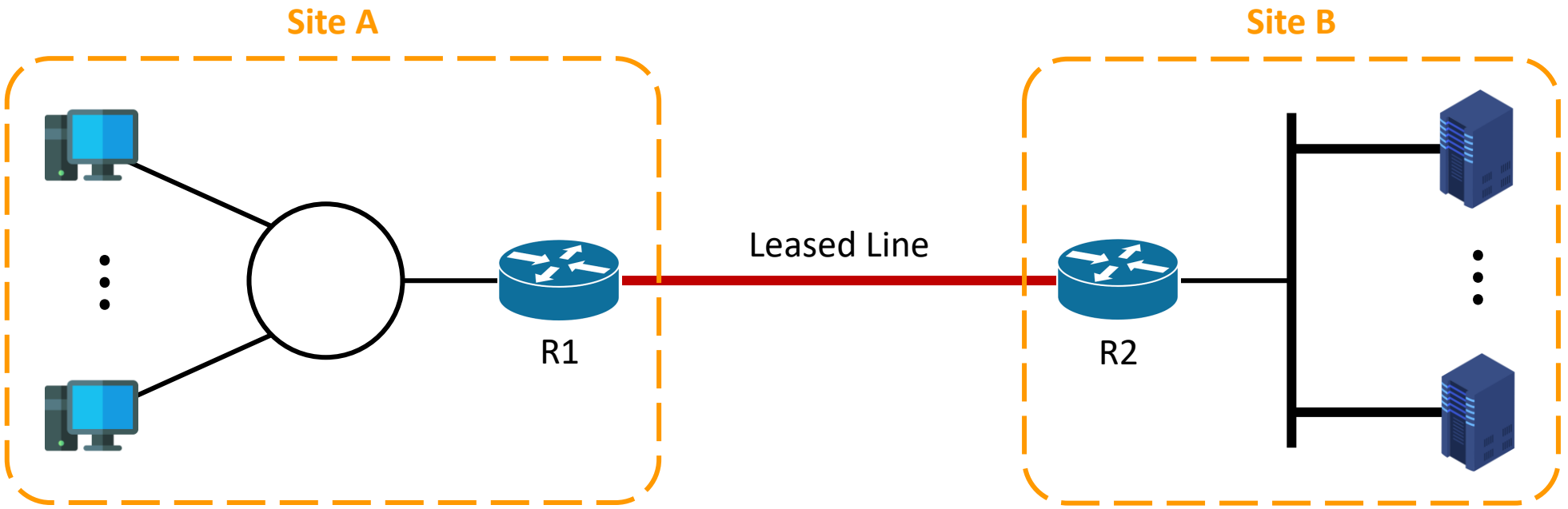
Virtual Private Network (VPN)

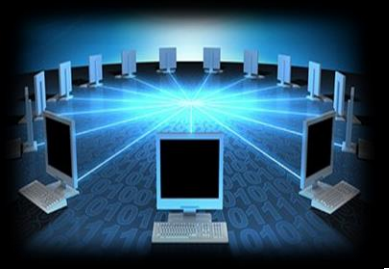
Private Network

- An institution that extends over multiple geographical regions often desires its own IP network, so that its hosts and servers can send data to each other in a secure and confidential manner.
- To achieve this goal, the institution could actually deploy a stand-alone physical network—including routers, links, and a DNS infrastructure—that is completely separate from the public Internet.
- Such a disjoint network, dedicated to a particular institution, is called a private network.
- A private network can be very costly, as the institution needs to purchase, install, and maintain its own physical network infrastructure.

Virtual Private Network (VPN)

❑ Private Network





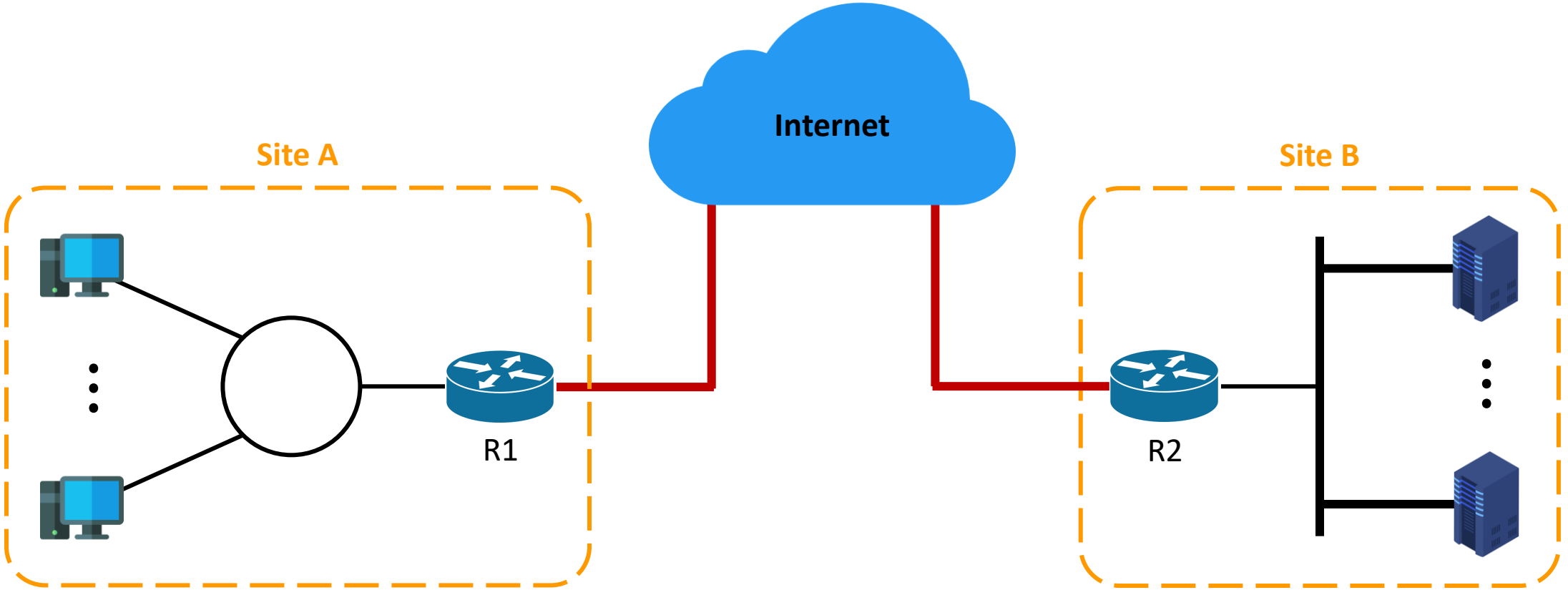
Virtual Private Network (VPN)

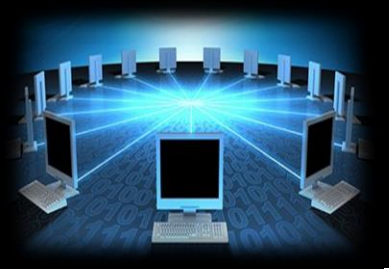
Virtual Private Network (VPN)

- Instead of deploying and maintaining a private network, many institutions today create **Virtual Private Network (VPN)** over the existing public Internet.
- With a VPN, the institution's inter-office traffic is sent over the public Internet rather than over a physically independent network.
- But to provide confidentiality, the inter-office traffic is encrypted before it enters the public Internet.

Virtual Private Network (VPN)

❑ Virtual Private Network (VPN)

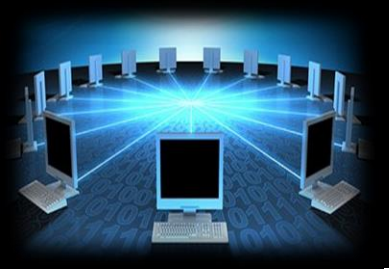




Virtual Private Network (VPN)

Features of VPN

- VPN creates a network that is private but virtual.
- It is private because it guarantees privacy inside the organization.
- It is virtual because it does not use real private WANs; the network is physically public but virtually private.



Virtual Private Network (VPN)

VPN Technology

- VPN technology uses **IPSec** in the tunnel mode to provide authentication, integrity, and privacy.
- In **tunnel mode**, each IP datagram destined for private use in the organization is encapsulated in another datagram.
- To use IPSec in tunneling, the VPNs need to use two sets of addressing.
- The public network (Internet) is responsible for carrying the packet from Rl to R2.
- Outsiders cannot decipher the contents of the packet or the source and destination addresses.
- Deciphering takes place at R2, which finds the destination address of the packet and delivers it.

Virtual Private Network (VPN)

❑ Addressing in a VPN