IT/CYBR 4323, Chapter 5:

Other LAN's

- Mr. Donald Privitera with Gennadiy Kemelmakher
- Kennesaw State University
- Marietta Campus
- College of Computing and Software Engineering
- IT Department
- dprivit2@kennesaw.edu

Virtual Private Network (VPN)

- VPN's were originally designed to extend a private network through a public TCP/IP network.

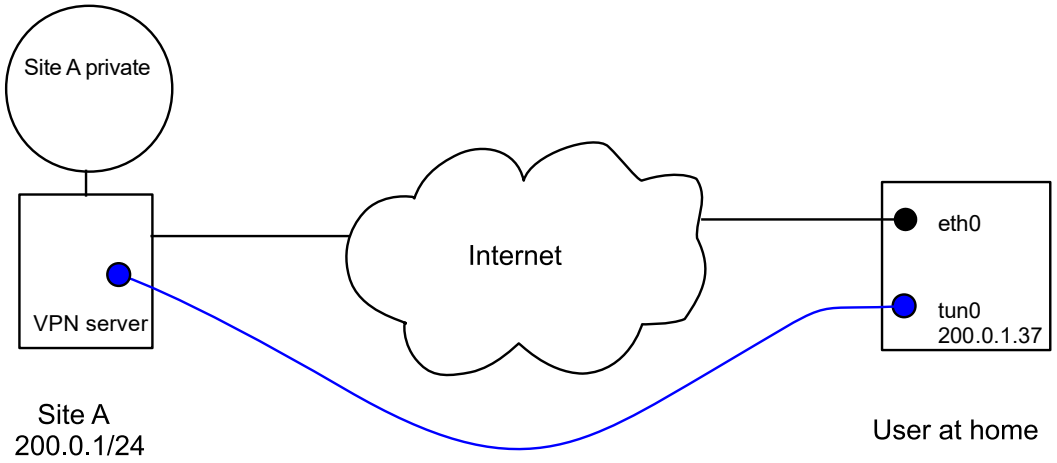
  They can do this at one of 2 layers:

  - Layer 3 most common (known as TUN mode) is a routed IP version and has less overhead but less versatility as it works on IP only.
  - Layer 2 (known as TAP mode) is a bridged/switched version and operates at a lower level creating more overhead but can transfer any network protocol.
- VPN's have been adapted for a second major purpose; to provide privacy and security because without a VPN, ISP's see and track all traffic coming and going to a customer's location; they then sell this information to data aggregators. In addition, when using a public network, a VPN adds a layer of security to prevent man-in-the-middle attacks.

Example

Each end of the connection is typically associated with a software-created virtual network interface; each of the two virtual interfaces is assigned an IP address. (Virtual interfaces are not essential; VPNs created with IPsec generally omit them.) When a packet is to be sent along the virtual link, it is actually encapsulated and sent along the original Internet connection to the VPN server, wending its way through the commodity Internet; this process is called tunneling. To all intents and purposes, the virtual link behaves like any other physical link.

After the VPN is set up, the home host's tun0 interface appears to be locally connected to Site A, and thus the home host is allowed to connect to the private area within Site A. The home host's forwarding table will be configured so that traffic to Site A's private addresses is routed via interface tun0.



VPN: blue link represents *tunnel.* Actual connection is made via eth0
The tun0 interface is a virtual network interface with a Site-A address

VPN's Explained

Peter L Dordal, An Introduction to Computer Networks

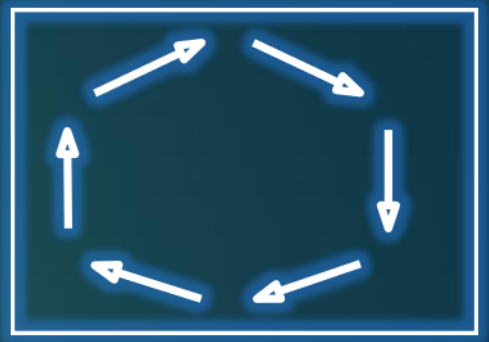
https://youtu.be/CWy3x3Wux6o

Carrier Ethernet

- Carrier Ethernet is a leased-line point-to-point link between two sites, where the subscriber interface at each end of the line looks like Ethernet.
- The physical path in between sites, however, need not have anything to do with Ethernet; it may be implemented however the carrier wishes.
- In particular, it will be (or at least appear to be) full-duplex, it will be collision-free, and its length may far exceed the maximum permitted by any IEEE Ethernet standard.
- A carrier Ethernet connection looks like a virtual VPN link, but runs on top of the provider's internal network rather than the Internet at large.
- Carrier Ethernet connections often provide the primary Internet connectivity for one endpoint, unlike Internet VPNs which assume both endpoints already have full Internet connectivity.

Peter L Dordal, An Introduction to Computer Networks

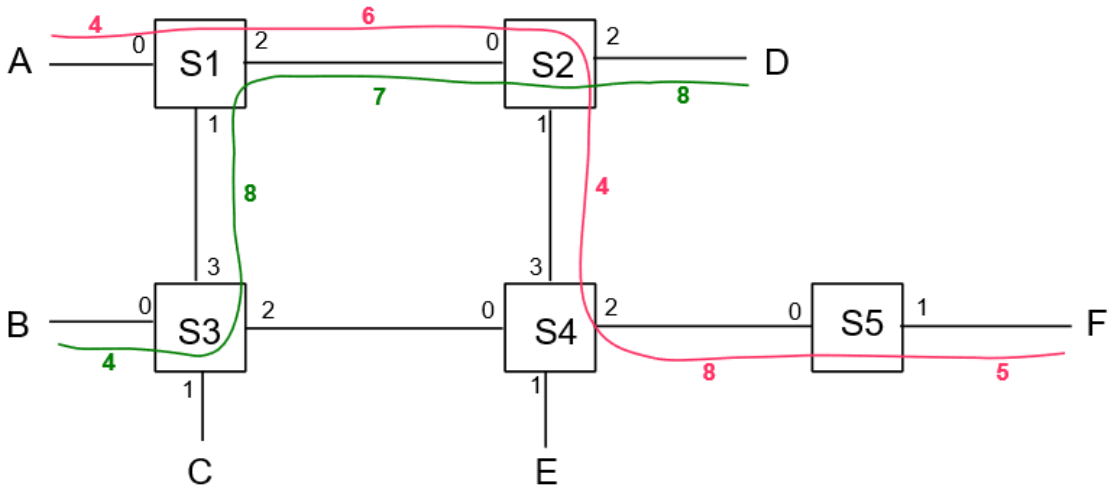
Token Ring



- Token Ring is a simple multiple-access mechanism that is not only collision-free, but which supports fairness in the sense that if N stations wish to send then each will receive 1/N of the opportunities.
- Actual implementations come in several forms, from Fiber-Distributed Data Interface (FDDI) to so-called "IBM Token Ring". The central idea is that stations are connected in a ring:
- Packets will be transmitted in one direction.
- Stations in effect forward most packets around the ring, although they can also remove a packet.

Virtual Circuits

- Virtual circuits are The Road Not Taken by IP.
- Virtual-circuit switching (or routing) is an alternative to datagram switching, which was introduced in Chapter 1. In datagram switching, routers know the next_hop to each destination, and packets are addressed by destination. In virtual-circuit switching, routers know about end-to-end connections, and packets are “addressed” by a connection ID.



Asynchronous Transfer Mode (ATM)

- ATM is a network mechanism intended to accommodate real-time traffic as well as bulk data transfer. We present ATM here as a LAN layer, for which it is still sometimes used, but it was originally proposed as a replacement for the IP layer as well, and, to an extent, the Transport layer. These broader plans were not greeted with universal enthusiasm within the IETF. When used as a LAN layer, IP packets are transmitted over ATM as in 5.5.1 ATM Segmentation and Reassembly.
- ATM also made the decision to require fixed-size cells. The penalty for one partially used cell among many is small. Having a fixed cell size simplifies hardware design, and, in theory, facilitates an easier design for parallelism.

ATM Segmentation & Reassembly

- Due to the small packet size, ATM defines its own mechanisms for segmentation and reassembly of larger packets. Thus, individual ATM links in an IP network are quite practical. These mechanisms are called ATM Adaptation Layers, and there are four of them: AALs 1, 2, 3/4 and 5 (AAL 3 and AAL 4 were once separate layers, which merged). AALs 1 and 2 are used only for voice-type traffic; we will not consider them further.
- The ATM segmentation-and-reassembly mechanism defined here is intended to apply only to large data; no cells are ever further subdivided. Furthermore, segmentation is always applied at the point where the data enters the network; reassembly is done at exit from the ATM path.
- IPv4 fragmentation, on the other hand, applies conceptually to IP packets, and may be performed by routers within the network.