Switching and Routing

In the previous 3 lectures, we have discussed the Physical, Data-Link and Internet layers. The focus was understanding how IP datagrams are encapsulated in a data link frame and how signals are transmitted across a cable by the physical layer. Today, we want to look at how networking devices are used to link single PCs into a single network and how single networks are interconnected to form an internet. The two most common devices are switches and routers. Switches are layer 2 devices, data link layer, which means they forward frames, not packets, using the Media Access Control (MAC) address. Routers are layer 3 devices, Internet layer, which means they forward packets, not frames, using the IP address. These two devices are used to internet local, metropolitan and wide area networks. The basic device is the switch. Routing was built on top switching so that many independent single networks can be joined into a larger network in order to share resources and exchange data. The most common networking technology today is Ethernet. The latter which started as a LAN technology is growing into MANs and WANs.

Data Link Layer

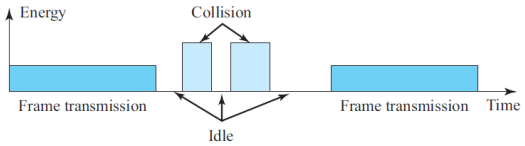
The data link layer is not a single layer, but 2 layers: Logical Link Layer and the Media Access Layer

The Logical Link Layer is only used by 802.2 Ethernet (old Ethernet) and will not be discussed). It is also used by other LAN\WAN technologies. Modern Ethernet, which is the focus of this course, is defined by the IEEE 802.3 standard and does not use the Logical Link Layer. However, all types of Ethernet have one thing in common- they all use the Media Access Layer to access the network. This layer uses a protocol called CSMA/CD to control how network PCs access the communications channel. CSMA/CD stands for Carrier Sense Multiple Access with Collision Detection. To understand Ethernet, you must first understand CSMA/CD. The term Carrier Sense means that Ethernet NICs listen to the network channel for noise level and only transmit when the noise level goes down, meaning that no other PCs are transmitting . Multiple Access means that there is nothing to prevent two Ethernet devices from transmitting at the same time. In CSMA/CD when a device wants to transmit data it must first access the transmission channel and determine whether the channel is free. If the channel is not free (noise level is high) it waits and checks again after a brief amount of time. If the channel is free, the mode transmits data. Any PC can transmit its data. However, if two nodes transmit at the same time a collision will occur which will destroy the data. This is where the third component Collision Detection comes in. If a collision occurs (a spike in the noise level), both devices stop transmitting. The NIC cards of each device will send a special 32-bit sequence that indicates to the rest of the network, that its

previous transmission was faulty and that those data frames are to be deleted. Each node then waits a random amount of time and, if the network channel is free, it automatically retransmits the data.

How collision can be detected:

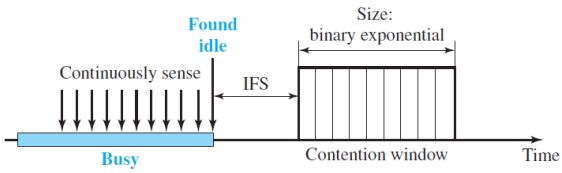
- detecting voltage level on the line
- detecting power level
- detecting simultaneous transmission & reception



CSMA/CA

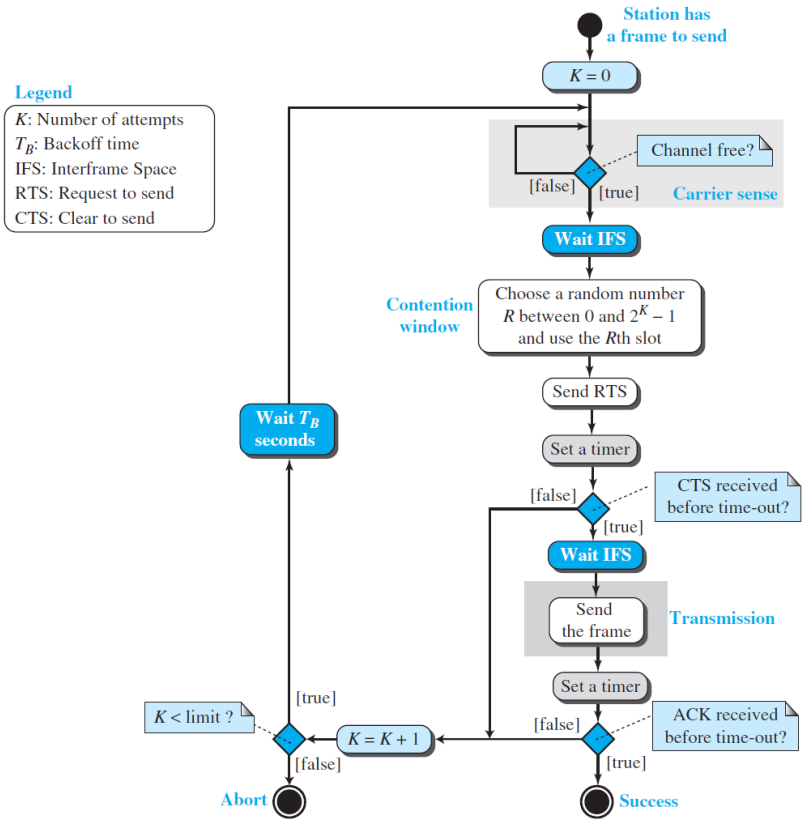
CSMA/CA uses three strategies: the **interframe space (IFS)**, **contention window**, and **acknowledgments**

IFS-First, collisions are avoided by deferring transmission even if the channel is found idle. When an idle channel is found, the station does not send immediately. It waits for a period of time called the ***interframe space*** or ***IFS*.**



Contention window- is an amount of time divided into slots.A station that is ready to send chooses a random number of slots as its wait time. The number of slots in the window changes according to the binary exponential back-off strategy. This means that it is set to one slot the first time and then doubles

***Acknowledgment*-** With all these precautions, there is still may be a collision. Data may also be corrupted during the transmission.The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.



This is the CSMA protocol with collision avoidance.

Algorithm:

• The station ready to transmit, senses the line by using one of the persistent strategies.

• As soon as it find the line to be idle, the station waits for an IFS (Interframe space) amount of time.

• It then waits for some random time (contention window slot time) and sends the frame.

• After sending the frame, it sets a timer and waits for the acknowledgement from the receiver.

• If the acknowledgement is received before expiry of the timer, then the transmission is successful.

• But if the transmitting station does not receive the expected acknowledgement before the timer expiry then it increments the back off parameter, waits for the back off time and resenses the line.

Whenever the channel is found idle, the station does not transmit immediately. It waits for a period of time called interframe space (IFS).

• When channel is sensed to be idle, it may be possible that same distant station may have already started transmitting and the signal of that distant station has not yet reached other stations.

• Therefore the purpose of IFS time is to allow this transmitted signal to reach other stations.

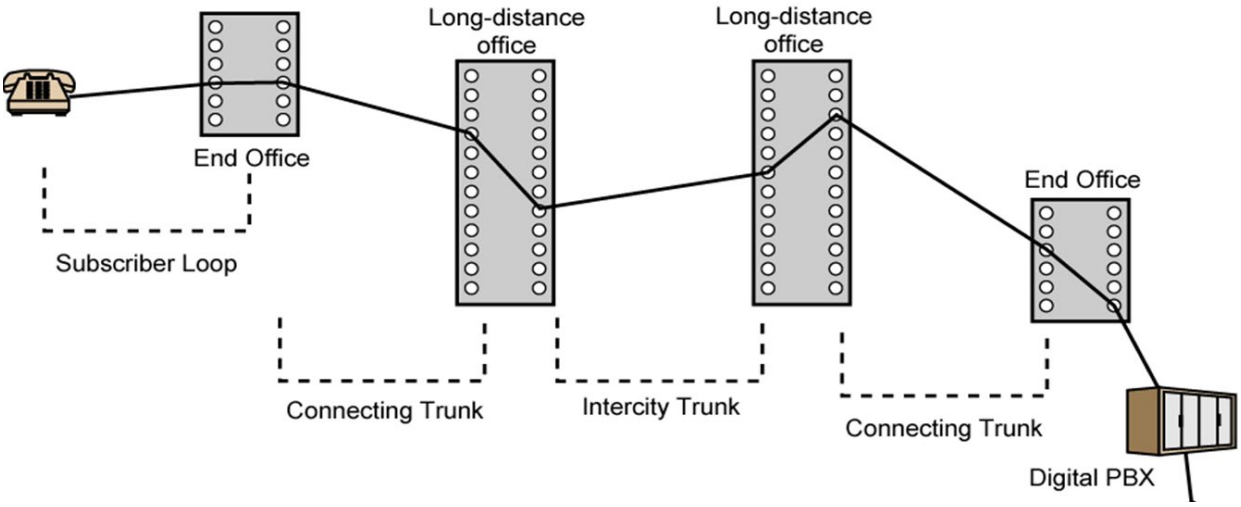
Switched Networks

A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating temporary connections between two or more devices linked to the switch. In a switched network, some of these nodes are connected to the end systems (computers or telephones, for example). Others are used only for routing

The two fundamental approaches to move any type of data through the network is circuit switching and packet switching.

Circuit Switching

Circuit switching is a physical layer technique. In circuit switching a connection is established between two network nodes before they begin transmitting data. Bandwidth is dedicated to this connection and remains available until the users terminate the communication. The Public Telephone Switched Network (PSTN) is a perfect example of a circuit switched network and for voice communication it is a good choice. For example, some network applications benefit from a "dedicated" path. Such as live audio or videoconferencing which can't tolerate the time delay if the data packets had to take different paths. Circuits can be permanent or temporary. Applications which use circuit switching may have to go through three phases: establish a circuit, transfer the data and disconnect the circuit. Another example of circuit switched networks is if you connect your home PC to an ISP's access line using DSL, previously discussed. Other examples of circuit switched networks are: ISDN (Integrated Services Digital Network), X.21, High-Speed Circuit-Switched Data (HSCSD) service in cellular systems such as GSM. It is implemented at the physical layer. Two types of switches used by circuit switched networks are: crossbar switch and multistage switch.

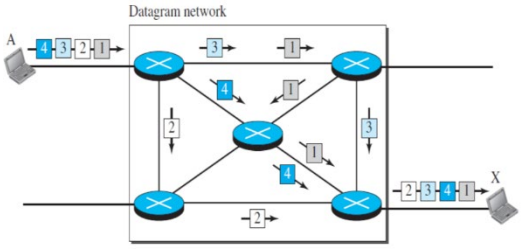


Packet Switching

A dedicated circuit is good for voice communication it is not good for transmitting digital data. The dedicated circuit is too inefficient in bandwidth when a million bits can be sent in a fraction of a second. Therefore, packet Switching is the most popular form of connection for Ethernet and the Internet.

Two types of packet switched networks

1. **Datagram switching**



Datagram switching (Network layer)

In datagram switching each packet is treated independently to all other packets. Depending on the current network situation (congestion or unavailability of the next hop) packets may take different routes/paths to the destination. Datagram switching is a connectionless approach where no connection establishment or tear down take place.

For example, suppose you and 4 of your friends had a card with the number 1 to 5 on it. And you all decided to travel independently from Seneca@York to the CN tower. One person may take a bus to the tower, another may take the subway, another a taxi and one may decide to drive his/her own car. By each travelling his/her own path, no one path will be congested. But if a traffic jam occurs and the ones driving or taking a taxi are delayed, all will eventually reach the Tower. The only problem is that some of your friends may arrive at the tower out of sequence (number 4 arrives before number 1), requiring the message to be reassembled in order.

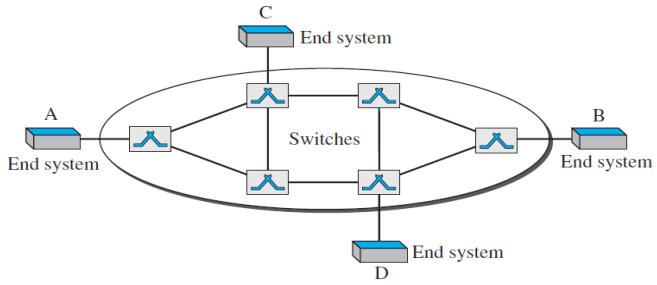
This is how packet switched networking works. Large messages are fragmented into small individual messages. Because of the time, it takes to reassemble the packets into a message, packet switching requires speedy connections, if used for live audio or video transmission. The biggest advantage of packet switching is its efficient use of bandwidth by not holding a connection open until a message reaches its destination, Packet switching also enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The Internet uses packet switching; packet switching enables the user to differentiate data streams based on priorities. Packets are stored and forwarded based on their priority to provide quality of service.

2. **Virtual Circuits**

Virtual circuit is the combination of circuit switched and packet switched techniques where data is packetized and for sending it to the destination a temporary path known as virtual circuit is established. All the packets followed the same path to the destination during the session. The header of the packet contains the address of the next switch should be and the channel on which the packet is being carried, not end-to-end address like in datagram switching where the destination address is the IP address of the destination node. There are three phases of communication:
Three phases of communication:

a. Connection establishment

b. Data transfer
c. Connection tear down



In Figure. The network has switches that allow traffic from sources to destinations. A source or destination can be a computer, packet switch, bridge, or any other device that connects other networks.

Note:

The term "Packet-Switching" is a misnomer because on single network frames are switched and on internets packets are routed. Unfortunately, data communications do not have terminology police to ensure consistent use of terms. Thus, Packet-Switching is a generic term for fragmentation of large messages into smaller ones which are independently addressed and sent across a link. The term is correctly used when referring to how the Internet routes packets, the term is never used on single networks or internets.

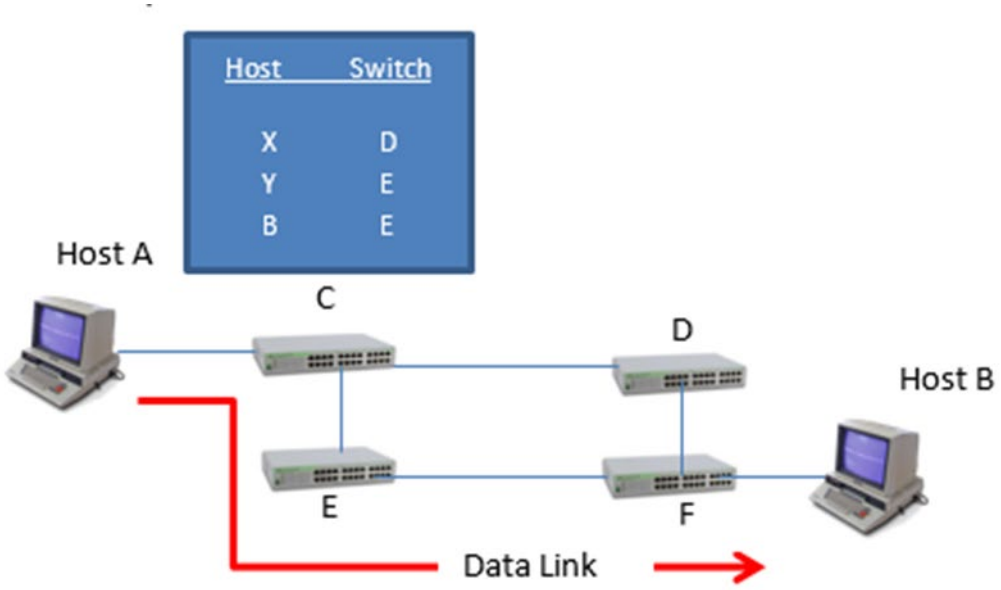
Switching and Routing

Switching

Switching is a process to forward frames coming in one port and forwarded out the destination port which copies the MAC address of the device attached to it. Switching is used because it is much faster than routing. It is used to improve performance by minimizing broadcast and collision traffic which consume bandwidth. At a broad level, switching can be divided into two major categories: circuit and packet switching

Switch Operation

Suppose Host A wishes to send information to Host B. We can see there are 2 switched paths CDF and CEF. When the frame arrives at switch C, how does switch C know to send the information to switch E, instead of switch D? The answer is switch C has a switching table with two columns: one for the destination of the frame, and the other for the switch to use to reach the destination host.

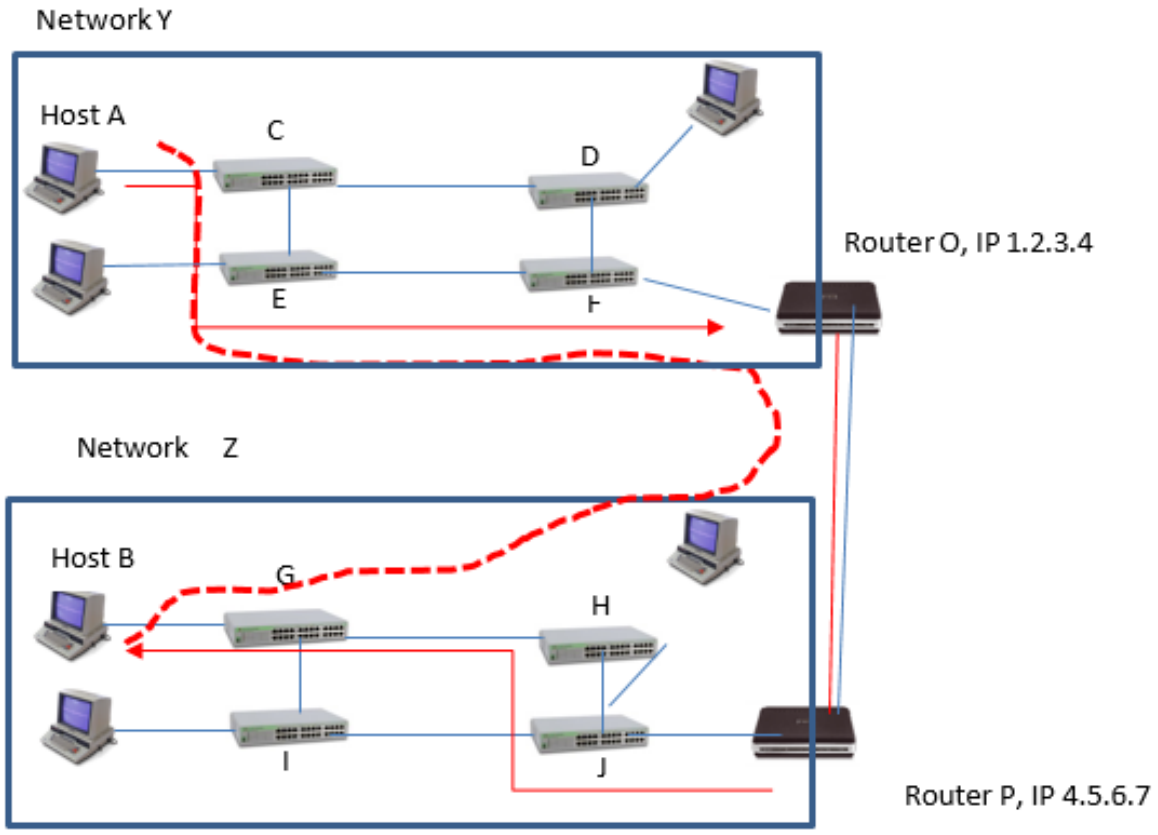


This switch-by-switch decision making continues across each physical link until the final switch forwards the frame to Host B. Switches only know their neighbor; they do not know the entire path. The path from Host A to CEF and final to Host B is called a data link. There is only 1 data link across a single network, regardless of the number of switches used.

When the Internet was being developed, ARPANET consisted of several switched networks with no communication between them. Bob Kahn and Vint Cerf devised a new device which they called a "gateway" which used a technology which linked single networks together. Today, we call this device a router (the term gateway is still used as a point of access to a network)

Routers connect different signal networks together. Single networks have no idea what a router is, they only know how to deliver frames to their neighbor. They do not open the packet and look inside to see the message in the frame. Routers work by acting as hosts on the network. Like a PC, a router has a NIC and a unique IP address. Unlike switches, routers and PCs have software that can open the frame to see the packet and view the source and destination IP addresses. Kahn and Cerf solved the problem of connecting single networks by creating a new type of message, an IP packet. Unlike frames, IP packets travel across all networks from source to destination.

Host A on Network Y, wants to send an application message to Host B on Network Z. On Network Y, the router acts as a destination host, accepting the frame across Network Y data link. Router O creates a new frame acceptable to Network Z. Looking at its routing table, Router O, knows that to reach Network Z, it needs to send the frame to interface 4.5.6.7. Router P acts like a host accepting the frame from Router O and forwards the frame to switch J. Switch J uses its switching table to forward the frame to switch H which in turn forwards it to switch G and finally to Host B.



We can see forwarding frames is done link by link. From the table below we can see that there are 9 physical links. Each single network has a single data link across it, so there are 3 data links, indicated in red in the diagram. For each data link, a frame must be created which is compatible with the next network. This is the job of the Router O. It removes the Network Y frame header, and recreates a WAN header compatible with the data link to Router P. Then it recalculates the LAN trailer and forwards the IP packet based on the destination IP address. Router P receives the packet, rips off the WAN header and recreates a LAN header compatible with Network Z. Router P also recalculates the LAN trailer and forwards the frame across the data link of Network Z to Host B. A route is a path taken by a packet from the source to the destination host across and internet. There is always only one packet created by Host A and one route from Host A to Host B as indicated by the dashed red line.

Type	Number	Description
Physical Links	9	AC,CE,EF,FO,OP,PJ,JH,HG,GB
Data Links	3	AO,OP,PB
Frames	3	AO,OP,PB
Packet	1	AB
Route	1	AB

Packets are routed across internets. Frames are switched across single networks.

Routing Operation

Routers are layer 3 devices that connects multiple IP networks together to exchange packets between them.

Unlike, switches which are organized in a hierarchical fashion and only have one path to the destination host, a router is organized in a mesh with multiple paths to the destination host. This is especially true for routers that border the Internet. Router maintains a routing table for finding the best path for the incoming data packets. The rows in the routing table are in the thousands with each row identifying a destination path. Thus, the router must make a forwarding decision as to the best route making routing much slower than switching. Routers have specific routing algorithms to help in the decision making, but all routers follow a 3-step process when a packet arrives. This is true for IPv4 and IPv6 routing:

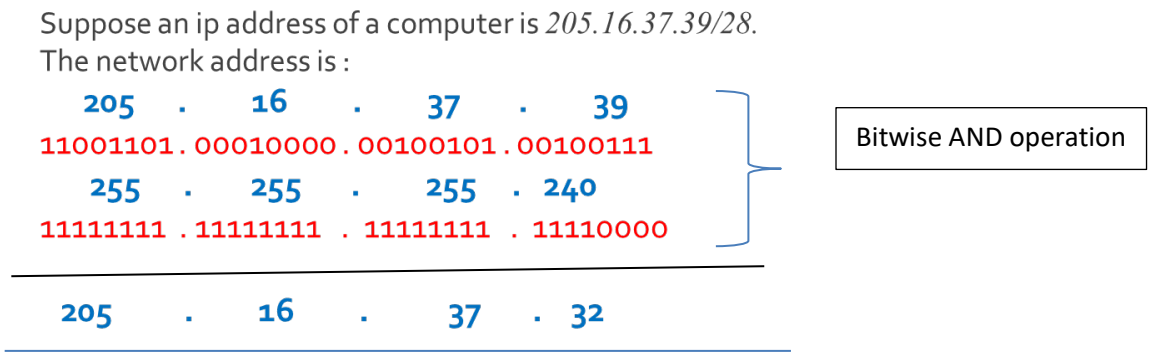
1. The router finds the destination IP address. It does this by ANDing the IP address with the network mask. For example, suppose a packet was destined to MySeneca on the Seneca College network, IPv4 142.204.250.120. The router would apply the mask of 255.255.0.0 which means that the address range is 16 bits. If we apply this mask to the network address, we get 142.204.0.0.

2. The router then compares the network address of 142.204 to every row in its routing table. Because routers are connected to meshes, the router can't stop after the first match, but must process through all rows to find all matching paths. From the list of matches, the router must decide which route is the best-match. The rule the router follows is which route is the longest match. For example, if the routing table showed 2 routes to MySeneca, 142.204.0.0/16 and 142.204.0.0/24, and the packet was destined for network 142.204.250.120; the router would choose the destination row with the 24 bit host. Why? The router's job is to get the packet as close to the destination as possible, and the longest match rule ensures the packet will get to the Seneca subnet of 250.

3. Sometimes, however, you will not only have multiple matches, but some rows may have the same longest match. In this case the router uses some metric to break the tie. The metric will depend on the routing protocol used. Usually, the tie breaker will be the shortest distance. For example, suppose two rows had identical matches, but one row had a metric of 2 and the other

of 6. The router would choose the metric of 2, or the shortest distance to the destination. Two hops is shorter than 6 hops. The metric could also be cost, which is preset by the administrator for each route and the route in this case would choose the route with the lowest cost.

Example:

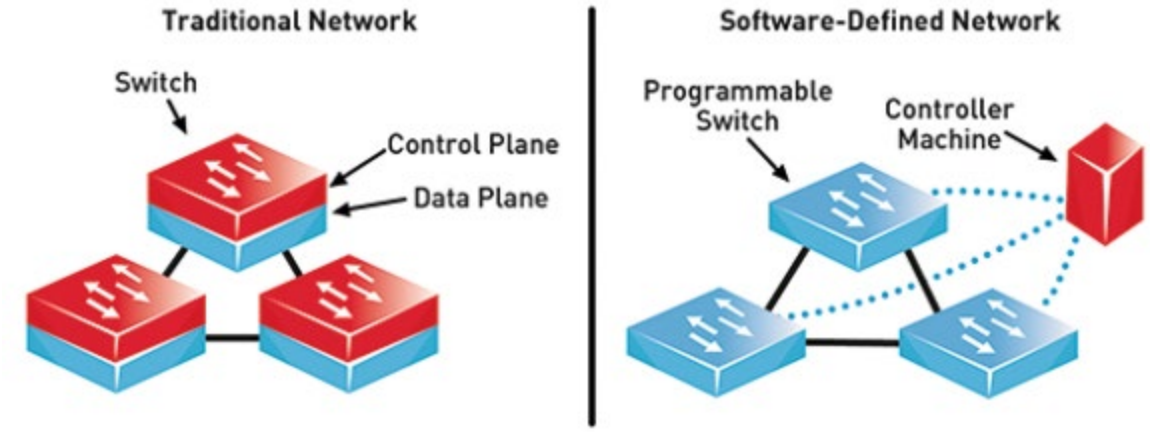


Network Virtualization

Network Virtualization (NV) is a software base that works as a traditional hardware base network device such as a switch, router, etc. by using NV, you can use one physical network device into separate, independent virtual networks. NV helps the network changes from static, inflex, and inefficient to a dynamic, responsive and enhanced. Nowadays, networks suppose to follow the demands for cloud base activities, distribute apps, and cybersecurity. With NV, you don't need to wait for a couple of days or weeks to upgrade your network system for supporting the new applications. Applications will be deployed to the system in minutes.

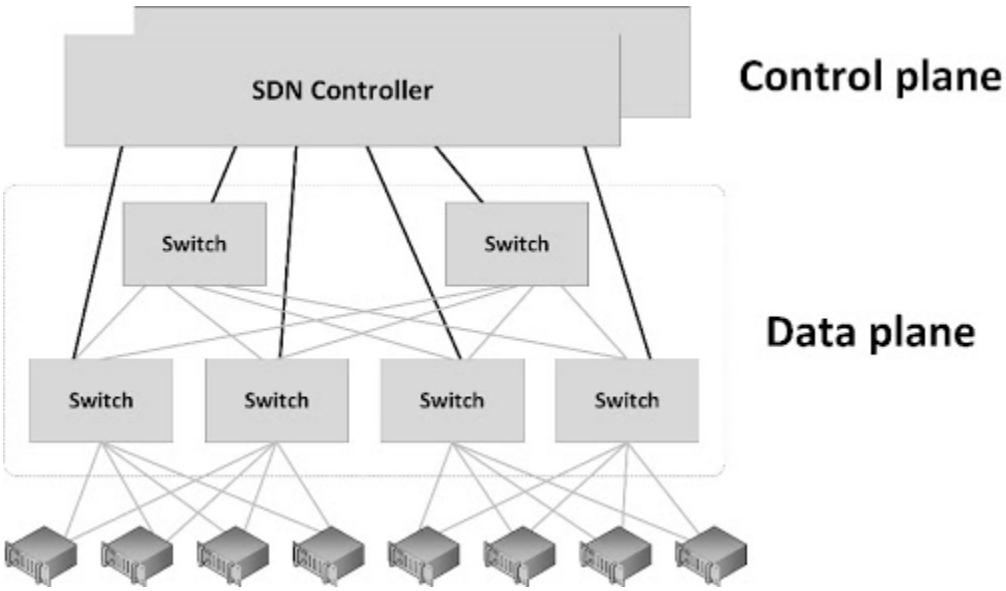
How does network virtualization work?

NV divides network services from the core hardware and uses a virtual system of a whole network. In this way, NV makes it to use software to create, monitor, and manage networks. In the traditional network, devices such as switch and router have two main parts of working; Control Plane and Data Plane. The control plane gives the command to the data plane to how to deal with the coming data to the device and how to forward it.



https://netfv.wordpress.com/2018/11/02/sdn-2/

In NV, these two planes have been divided, and Control Planes set virtually on a server and they come as a central commander for Data Planes. The control plane in NV has been controlled by Software Define Networking (SDN). The SDN allows managing the physical network devices by using the software. SDN uses APIs to control, monitor and modify the network activities by sends commands to data plane devices. It provides to the network administrators to control and manage the network fast and easy. They can buy click on one button or run an API to add, modify a complex network in seconds.

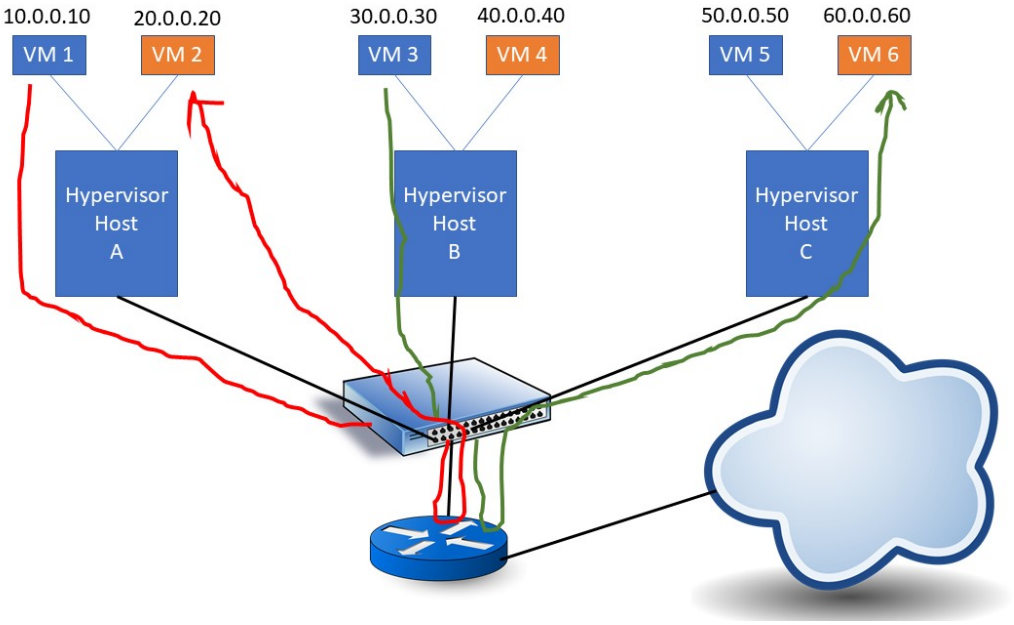


http://www.sjaaklaan.com/?e=168

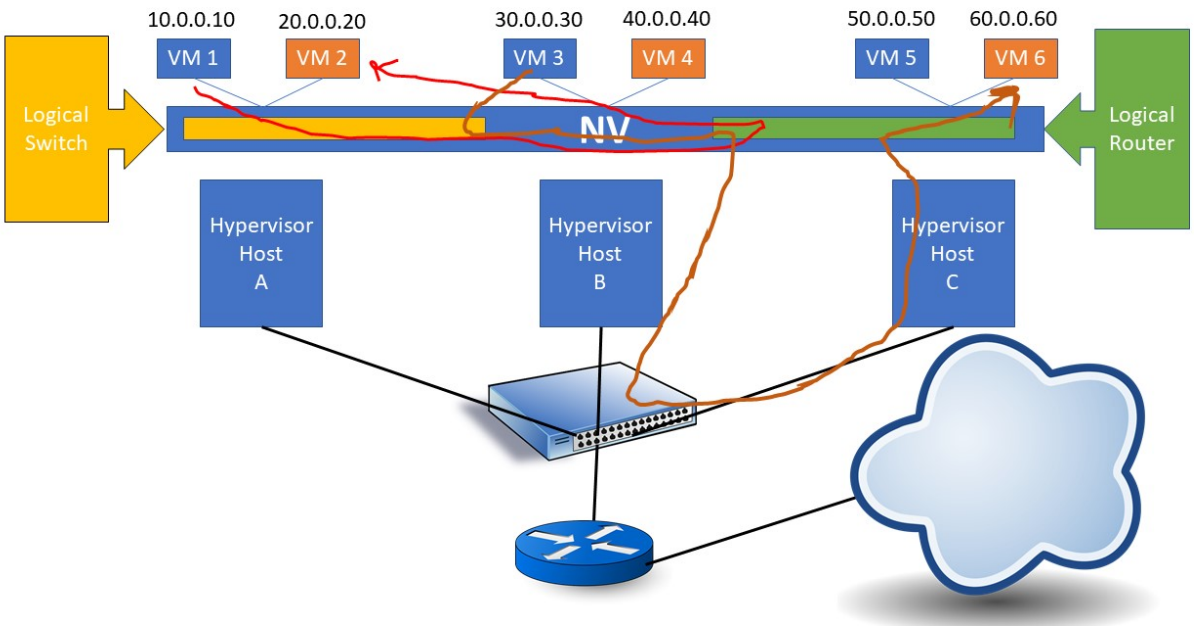
Example of Network Virtualization

In this example, there is an organization with 6 Virtual Machines (VM) such as VMWare, Hyper V. Each VM has different LAN IP addresses (they can't communicate to each other without using a router), and we have 6 LANs with 6 VMs. As you can see, the VMs need to pass the switch and router then

communicate with other VM, Especially if both VMs are in the same Host. The system works perfectly, but it has much latency between the network devices. Imagin, the organization, has 300 VMs, and it will increase the VMs to 100 more. The organization is supposed to buy more network devices, and it will increase the network latency. It will cause more expenses, more spaces, and maintenance, plus spend time researching, ordering and installing the new devices.



If the organization uses a Network Virtualization (NV) system, there is a logical switch and routers, in which all the controls are centralized, and NV can handle all data communication between all VMs. The latency will be reduced rapidly, and the VMs can communicate faster. All the communications pass through the Logical Switch and Routers. If the VMs in different Hosts, then the data passing the hardware switch to reach to the other Host. But already Control Plane has been set in Logical router. If the organization has 300 VMs, and it needs to increase to 100 more VMs, the network administrator just needs to install virtual network devices on the server and set them all. It can happen in a couple of minutes. As you can see, NV increases the speeds of data communication, maintenance, and installation of new devices, plus decrease the cost of the hardware devices and spending time.



Benefits of Network Virtualization

Network Virtualization provides speeds, more flexible, and security by automating and make more specific many activities of running data center or cloud networking. The following are some critical benefits for NV:

- Increase the time of network supplying from weeks to minutes
- By using automation in NV instead of manual processing, it achieves greater efficiency in network operation.
- Network workloads can be placed and moved separately of the physical topology
- As security in the data center or cloud networking, NV improved networking security.

Multiple Protocol Label Switching (MPLS)

Traditionally, switches are layer 2, Data link devices; however, more modern switches work at layer 3 which is the Internet layer and forward packets based on IP address. These new switches are in fact routers which work like switches.

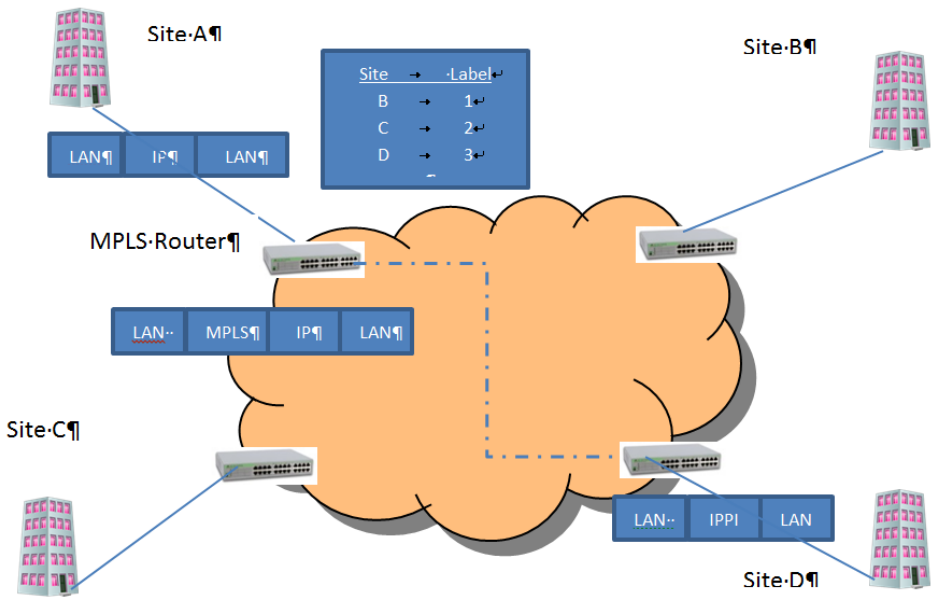
Earlier in this lecture we looked at how routers handle IP packets. They open the LAN frame to find the incoming packet's destination IP address, then they compare the address to every row in the routing table, select the best match, recalculate the FCS and send the packet out the appropriate port to reach the next link towards the destination host. The next packet arrives and the router follows the same procedure. This processing can lead to latency as each router forwards the packet. Multiprotocol Label Switching (MPLS) is a new standard which greatly simplifies routing and basically allows the router to function like a switch. This technology can be used with any LAN technology, like Ethernet, but is currently being used by third parties to provide MAN and WAN configurations. More importantly, MPLS

is done completely transparently to the sending and receiving Host. MPLS adds a new header in between the existing LAN and IP headers (note: the LAN and IP headers are not changed).

On an MPLS network, when two hosts begin to communicate, they do not immediately send packets, Instead, they determine the best path for the packets. This best path is called the "label-switched path". This dedicated path is slow to set up, but once created all subsequent packets can be forwarded very quickly. This is especially true if the MPLS network is controlled by a 3rd party MAN service provider, as in the diagram below. In this situation, each site can have a unique label number and each router only has one path to the destination host, like a switch. The router does not have to open the packet and pass the packet to the Internet layer to find the destination IP address. Also, since the packet is not opened and new MAC addresses for the next link in the route, the FCS does not have to be recalculated. These factors greatly decrease the latency of a typical router.

For example, a host at Site A wants to send a packet to a host at Site D. Host D on the MAN network is assigned a label of 3. Host A sends an ordinary LAN frame and IP packet to the Host at Site D. The first MPLS capable router places a label header in between the LAN frame header and the IP header with the label number 3. This label number identifies the label-switch path to Site D. No further routing is necessary. Since each router knows the one path to the destination network, the router is in fact functioning like a switch. The last label-switched router removes the label because the packet has reached the destination Site D.

MPLS greatly simplifies the routing process and provides faster routing. The technology is also being used on internets. For example, if a route gets too congested, the traffic can be moved between 2 routers to an alternative route. Many ISPs are using this technology to provide better load balancing on their network. Technically, there is no limit to how far MPLS networks can work. They could be used for WANs and speed up the Internet, however, this is unlikely to happen due to coordination difficulties between ISPs.



Voice Over IP (VoIP) Networks

Programmers are now designing applications which combine both data and voice. Businesses like the convergence because it means they only manage one network; this is less expensive and more efficient than managing separate networks. In addition, since calls are made using the Internet, governments have not taxed VoIP calls like land lines, thus calls are much cheaper. Employees like it too because VoIP applications increase mobility and are available from the warehouse, home or on the road. VoIP applications also increase collaboration between and improve customer relations by allowing video chat, Web conference, and instant messaging (each technology can be used individually or all of them simultaneously), through a single, easy-to-use interface. Callers are less likely to get ensnared in voicemail menus or put on hold, which can improve customer loyalty and company profits. For the above reasons, VoIP applications are growing in the business sector. We should have a basic understanding of the technology and how it works.

VoIP is a client/server architecture which uses data devices to send real time audio communication as well as data over the TCP/IP Ethernet network. The servers set up the connection, and once made, the clients then send IP packets back and forth until the call has ended and the servers take down the connection. There is an excellent 1 hour tutorial on VoIP on you tube from Eli the Computer Guy[1]

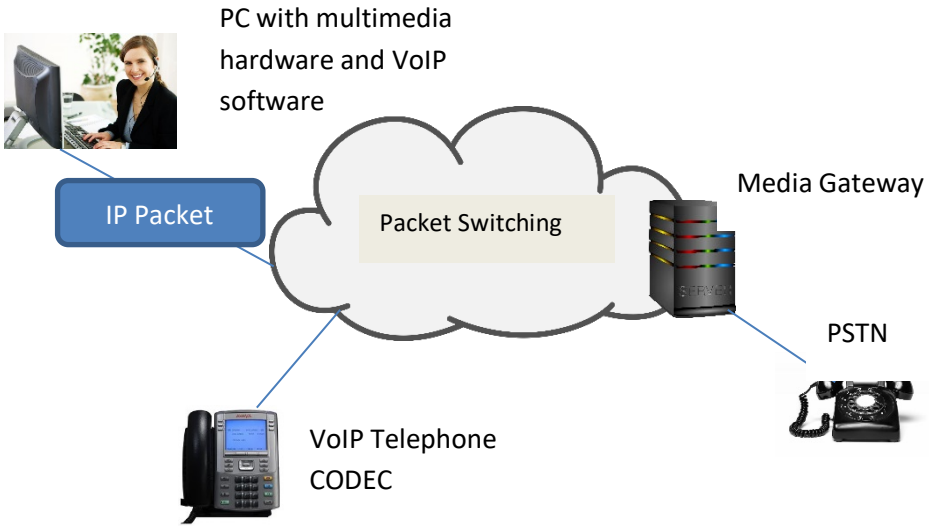
Clients

The clients can be a PC with speakers and microphone and VoIP software. A client could also be a specialized VoIP telephone, which looks like a regular land line, but instead of using a standard RJ-11 connector, it uses an RJ-45 connector. These telephones have built in codecs to convert the digital IP packet to analog voice. A traditional land line can also be a client provided the VoIP communication goes through a media gateway which does the conversion.

Servers

There are two major VoIP signaling protocols, H.323 which is an ITU-T standard or SIP (Session Initiation Protocol) created by the IETF. SIP is the newer standard and will probably replace H.323 in time. All of the major telcos and cable companies offer VoIP services. Most businesses and home users are buying the service from third party providers. But there is an open source version called OfficeSIP which works with Windows and can be downloaded onto any PC to act as a server.

[1] Eli the Computer Guy, "Introduction to VoIP" at https://www.youtube.com/watch?v=2x3Ie6VZ_sg



One would think that VoIP would be based on the TCP Transport protocol. TCP is connection-oriented which means that it sets up a pathway from source to destination before sending any packets. It also has an acknowledgement system which guarantees delivery. However, these features of TCP create latency in the communication greater than 250 milliseconds which makes verbal communication impossible. Voice needs to be transmitted in real time. To provide better voice communication, the UDP, User Datagram Protocol is used. This protocol is connectionless, does not guarantee delivery and reduces the processing load an VoIP phones. To improve UDP the Real Time Protocol (RTP) is used in conjunction. This protocol places a RTP header in between UDP header and the application message. The header adds a sequence number, so that all packets can be associated with the same conversation and reassembled in the correct order, and a time stamp. VoIP is highly sensitive to jitter, which is variable latency in packet delivery; the time stamp helps the receive to know which packets are to be played relative to the previous packet. This allows smooth playback. If packets are lost, the receiver can create fake noise for the lost codec bytes by extrapolating between the content of the proceeding and following packets.

Programming VoIP Applications

With the popularity of VoIP applications, you will no doubt be writing VoIP applications. It is important to understand some programming concepts. To get started programming VoIP applications for Windows using the .NET languages (including C#, C, C++, VB, etc.) there are several VoIP development kits. These kits allow you to build a "softphone" – a PC with telephone capabilities, a VoIP gateway sever, or a PBX system. These kits save development time because the libraries and components are prebuilt and can be integrated into your application. A common kit for Windows is Ozeki VoIP SIP SDK. A trial version can be downloaded from www.voip-sip-sdk.com. To get more information on how to use Ozeki go to http://www.voip-sip-sdk.com/p_24-ozeki-voip-sip-sdk-quick-start-guide-voip.html

A cross platform, open source SDK is Asterisk. It includes all components necessary to build softphones, PBXs, or VoIP gateways. Asterisk is open source, free to use and can be modified to fit organizational needs. It is stable, reliable and used by many of the Fortune 1000 list of companies. For more information on getting started with Asterisk go to http://www.asterisk.org/get-started