3.2 COMMUNICATION AND INTERNET TECHNOLOGIES

3.2.2 CIRCUIT & PACKET SWITCHING AND ROUTERS

One fundamental way of differentiating networking technologies is on the basis of the method they use to determine the path between devices over which information will flow. In simplified terms, there are 2 approaches: either a path can be setup between the devices in advance, or the data can be sent as individual data elements over a variable path.

CIRCUIT SWITCHING

In this networking method, a connection called a **circuit** is setup between two devices, which is used for the whole communication. Information about the nature of the circuit is maintained by the network. The circuit may either be a fixed one that is always present, or it may be a circuit that is created on an as-needed basis. Even if many potential paths through intermediate devices may exist between the two devices communicating, only one will be used for any given dialog. As illustrated below…

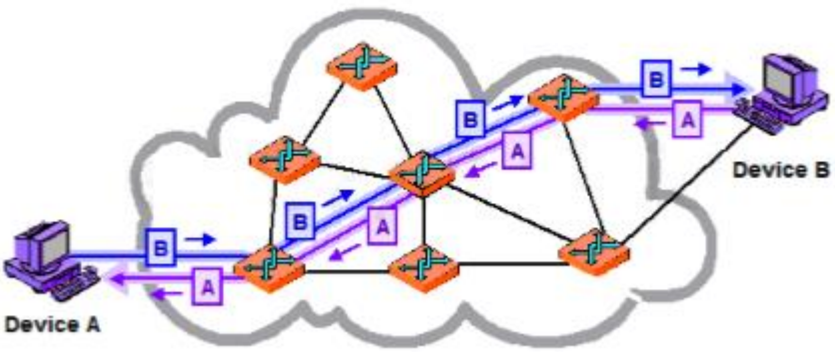


Figure 1: Circuit Switching

In a circuit-switched network, before communication can occur between two devices, a circuit is established between them. This is shown as a thick blue line for the conduit of data from **Device A** to **Device B** and a matching purple line from **Device B** to **Device A**. Once setup, all communication between these devices takes place over this circuit, even though there are other possible paths the data could be passed over the network of devices between them.

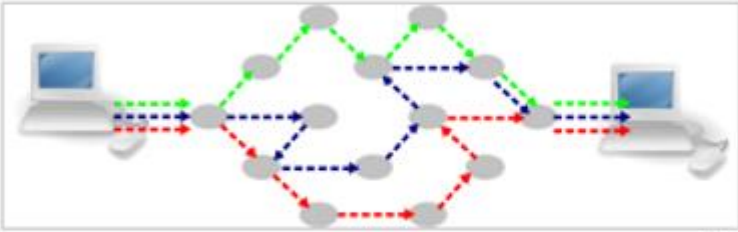
The classic example of a circuit-switched network is the telephone system. When you call someone and they answer, you establish a circuit connection and can pass data amongst each other regardless of how many intermediate devices are used to carry your voice. The circuit is used for as long as you need and is then terminated. Circuit-switching systems are ideal for communications that require data to be transmitted in real-time.

PACKET SWITCHING

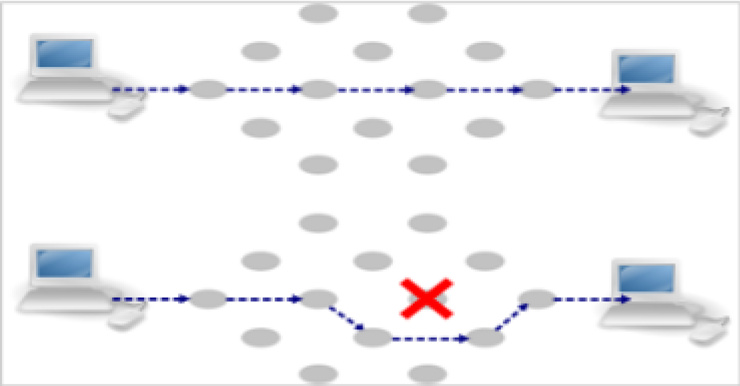
In this network type, no specific path is used for data transfer. Instead the data is chopped into small pieces called packets and is sent over the network.

Packet switching is the method by which the Internet works; it features delivery of packets of data between devices over a shared network. For example the school web server sends you a webpage over the Internet or you send an email to a friend. The packets can be routed and combined as required to get them to their eventual destination. On the receiving end the process is reversed, the data is read from the packets and then re-assembled into the form of the original data.

To get from one device to another, the data packets will have to travel through network adapters, switches, routers and other network nodes. The route taken by each packet might vary and at times there might be a lot of data travelling though these nodes meaning packets will be queued. This will result in varying times it takes to send data from one device to another depending on the traffic load in the network.



Different routes taken by three different data packets being sent to the same destination



demonstration of how the internet can re-route message if nodes fail. This makes the internet very robust

As packet switching doesn't define a set route for data to be sent by, any disruption in the network can be circumnavigated by re-routing:

PACKET SWITCHING STEPS:

1. Data is split into packets
2. Each packet has a source address, destination address and payload (data packet)
3. If data requires multiple packets, then the order of each packet is noted
4. Packets sent onto the network, moving from router to router taking different paths (set by the router). Each packet's journey time can therefore differ.
5. Once the packets arrive, they are re-ordered.
6. Message sent from recipient to sender indication that the message has been received
7. If no confirmation message received, sender transmits the data again.

Example: The ping command

To see the time it takes to send a message using packet switching you can use the `ping` command to time how long it takes to send data to another device, in this case we have used the `command prompt` to ping the www.example.com server:

```
# ping -c 5 www.example.com
PING www.example.com (192.0.43.10) 56(84) bytes of data.
64 bytes from 43-10.any.icann.org (192.0.43.10): icmp_seq=1 ttl=250 time=80.5 ms
64 bytes from 43-10.any.icann.org (192.0.43.10): icmp_seq=2 ttl=250 time=180.1 ms
64 bytes from 43-10.any.icann.org (192.0.43.10): icmp_seq=3 ttl=250 time=80.3 ms
64 bytes from 43-10.any.icann.org (192.0.43.10): icmp_seq=4 ttl=250 time=80.3 ms
64 bytes from 43-10.any.icann.org (192.0.43.10): icmp_seq=5 ttl=250 time=80.4 ms
```

As you can see the same data is being sent to the same location in all 5 attempts, but the second attempt met traffic on the way and took much longer. However, at 180.1 milliseconds you probably wouldn't notice.

Example: The trace command

The `tracert` command is used to map the route from one machine to another on the internet showing all the intermediate nodes, in this case, the message took ten steps to get there. The code above shows a trace from a home network to the www.google.com website. You can see that the 4th hop got lost and the data had to be re-routed.

```
# tracert www.google.com

Tracing route to www.l.google.com [209.85.147.99]
over a maximum of 30 hops:

  1    62 ms    99 ms    99 ms  bebox.config [192.168.1.254]
  2    53 ms    19 ms    18 ms  87-194-56-8.bethere.co.uk [87.194.56.8]
  3     *        *       83 ms  10.1.2.177
  4     *        *        *     Request timed out.
  5    20 ms    17 ms    17 ms  64.233.175.25
  6    20 ms    38 ms    19 ms  209.85.253.92
  7    26 ms    56 ms    23 ms  66.249.95.173
  8    45 ms    24 ms    24 ms  72.14.236.191
  9    33 ms    35 ms    35 ms  216.239.46.221
 10    27 ms    22 ms    22 ms  bru01m01-in-f99.1e100.net [209.85.147.99]

Trace complete.
```

HOW DOES A ROUTER WORK?

The Internet is one of the 20th century's greatest communications developments. It allows people around the world to send e-mail to one another in a matter of seconds.

We'll all used to seeing the various parts of the Internet that come into our homes and offices – the Webpages, e-mail messages and downloaded files that make the Internet a dynamic and valuable medium. But none of these parts would ever make it to your computer without a piece of the Internet that you've probably given less regard to. This technology is most responsible for allowing the Internet to exist at all: the **Router**.

When you send an e-mail to a friend on the other side of the century, how does the message know to end up on your friend's computer rather than on one of the millions of other computers in the world? Much of the work to get a message from one computer to another is done by routers, because they're the crucial devices that let messages flow **between networks**, rather than within networks.

Imagine a small company that makes animated 3D graphics for local television stations. There are 10 employees of the company, each with a computer. Four (4) of the employees are animators, while the other six (6) are in sales, accounting and management. The animators will need to send lots of large files back and forth to one another as they work on projects. To do this, they'll use a **Network**.

Each information packet sent from a computer is seen by all the other computers on the local network. Each computer then examines the packet and decides whether it was meant for its address. This keeps the basic plan of the network simple, but has performance consequences as the size of the network or level of network activity increases. To keep the animators' work from interfering with that of the folks in the front office, the company sets up two separate networks, one for the animators and one for the rest of the company. A router links the two networks and connects both networks to the Internet.

The router is the only device that sees every message sent by any computer on either of the company's networks. When the animator in our example sends a huge file to another animator, the router looks at the recipient's address and keeps the traffic on the animator's network hence only slowing down their network and not the rest of the company's. When an animator, on the other hand, want to communicate with the accounts department, then the router sees the recipient's address and forwards the message between the two networks.

One of the tools a router uses to decide where a packet should go is a **configuration table**. It is a collection of information including:

- Information on which connections lead to a particular groups of addresses
- Priorities for connections to be used
- Rules for handling both routine and special cases of traffic

A configuration table can be as simple as a half-dozen lines in the smallest routers, but can grow to massive size and complexity in the very large routers that handle the bulk of Internet messages.

In that case, the router has 2 jobs:

- To ensure that information doesn't go where it's not needed. Which is crucial for keeping large volumes of data from clogging connections of "innocent bystanders".
- To make sure that information does make it to the intended destination.

In performing these two jobs, a router is quite useful in dealing with 2 separate computer networks. It joins the two networks, passing information from one to the other and, in some cases, performing translations of various **protocols** between the 2 networks. It also protects the networks from one another, preventing the traffic on one from unnecessarily spilling over to the other. As the number of networks attached to one another grows, the configuration table for handling traffic among them grows, and the processing power of the router is increased. Regardless of how many networks are attached, though the basic operation and function of the router remains the same. Since the Internet is one huge network made up to tens of thousands of smallest networks, its use of routers is an absolute necessity.