What is packet sniffing?

Packet sniffers intercept packets of data flowing across a computer network in order to view their contents. This act is called packet sniffing.

How it works ??

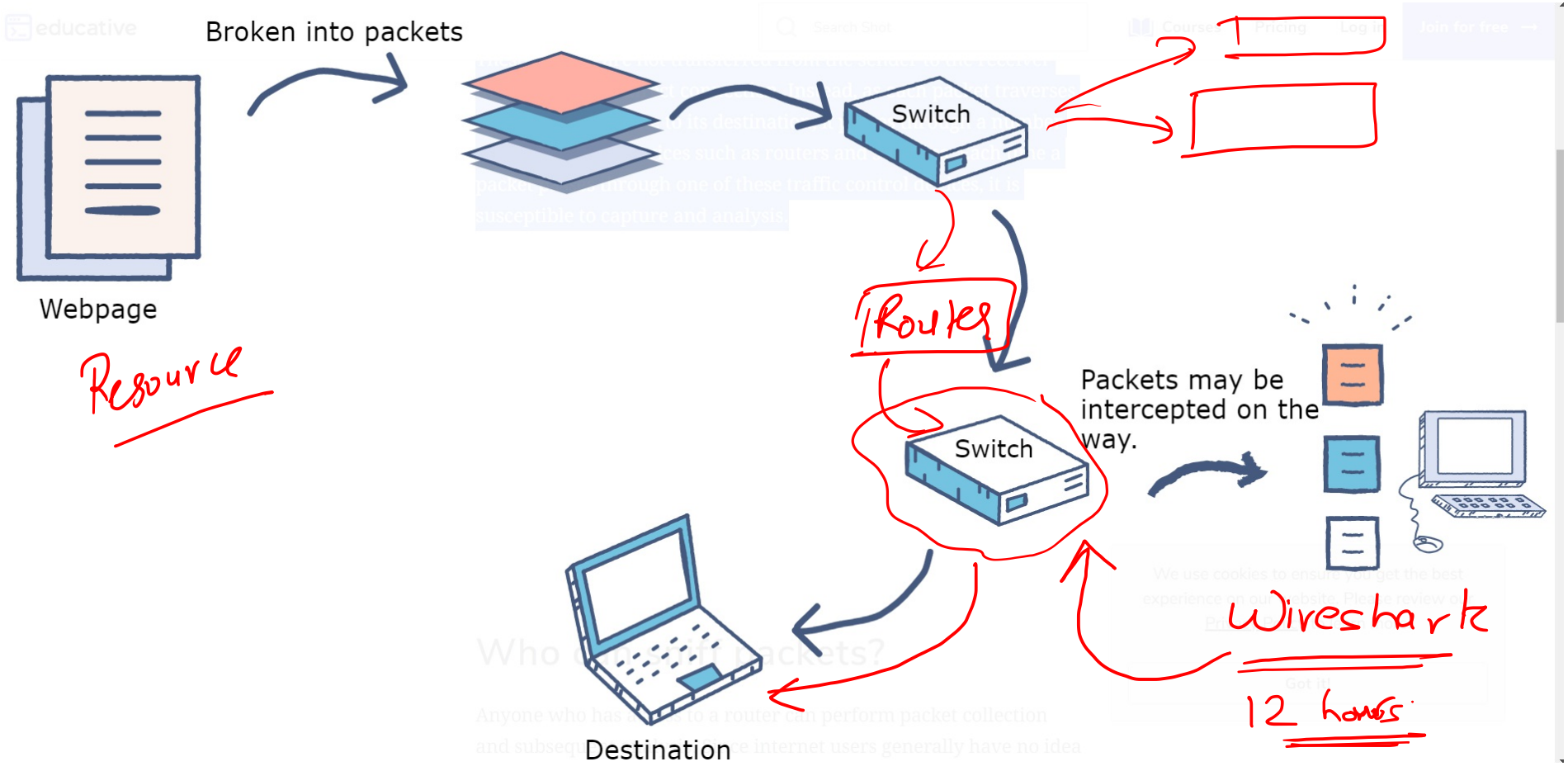
Web pages and emails are not sent through the internet as one document; rather, the sending side (your computer) breaks them down into many little data packets. These packets are then addressed to an IP address at the receiving end, which has to send back an acknowledgment of each packet it receives.

How it works ??

Web pages and emails are not sent through the internet as one document; rather, the sending side (your computer) breaks them down into many little data packets. These packets are then addressed to an IP address at the receiving end, which has to send back an acknowledgment of each packet it receives.

These packets are not transferred from the sender to the receiver through a single direct connection. Instead, as each packet traverses the internet en-route to its destination, it passes through a number of traffic control devices such as routers and switches. Each time a packet passes through one of these traffic control devices, it is susceptible to capture and analysis.

How it works ??


Broken into packets
Webpage
Resource
Switch
Router
Switch
Packets may be intercepted on the way.
Destination
Wireshark
12 hours

Who can sniff packets?

Anyone who has access to a router can perform packet collection and subsequent analysis. Since internet users generally have no idea how their traffic is being routed, it’s not really possible to know who may be observing that traffic.

ISPs use packet sniffing to track all your activities such as:

who is receiver of your email
what is content of that email
what you download
sites you visit
what you looked on that website
downloads from a site
streaming events like video, audio, etc.

Advertising agencies or internet advertising agencies are paid according to:
number of ads shown by them.
number of clicks on their ads also called PPC (pay per click).

Government agencies use packet sniffing to: ensure security of data over the network. track an organisation’s unencrypted data.

WireShark, SmartSniff are examples of packet sniffing tools.

How to prevent packet sniffing

One way to protect your network traffic from being sniffed is to encrypt it using a Secure Sockets Layer (SSL) or Transport Layer Security (TLS).

Encryption does not prevent packet sniffers from seeing source and destination information, but it does encrypt the data packet's payload so that all that the sniffer sees is encrypted content.

Any attempt to modify or inject data into the packets will likely fail since messing with encrypted data causes errors that will be evident when the encrypted information is decrypted at the other end.