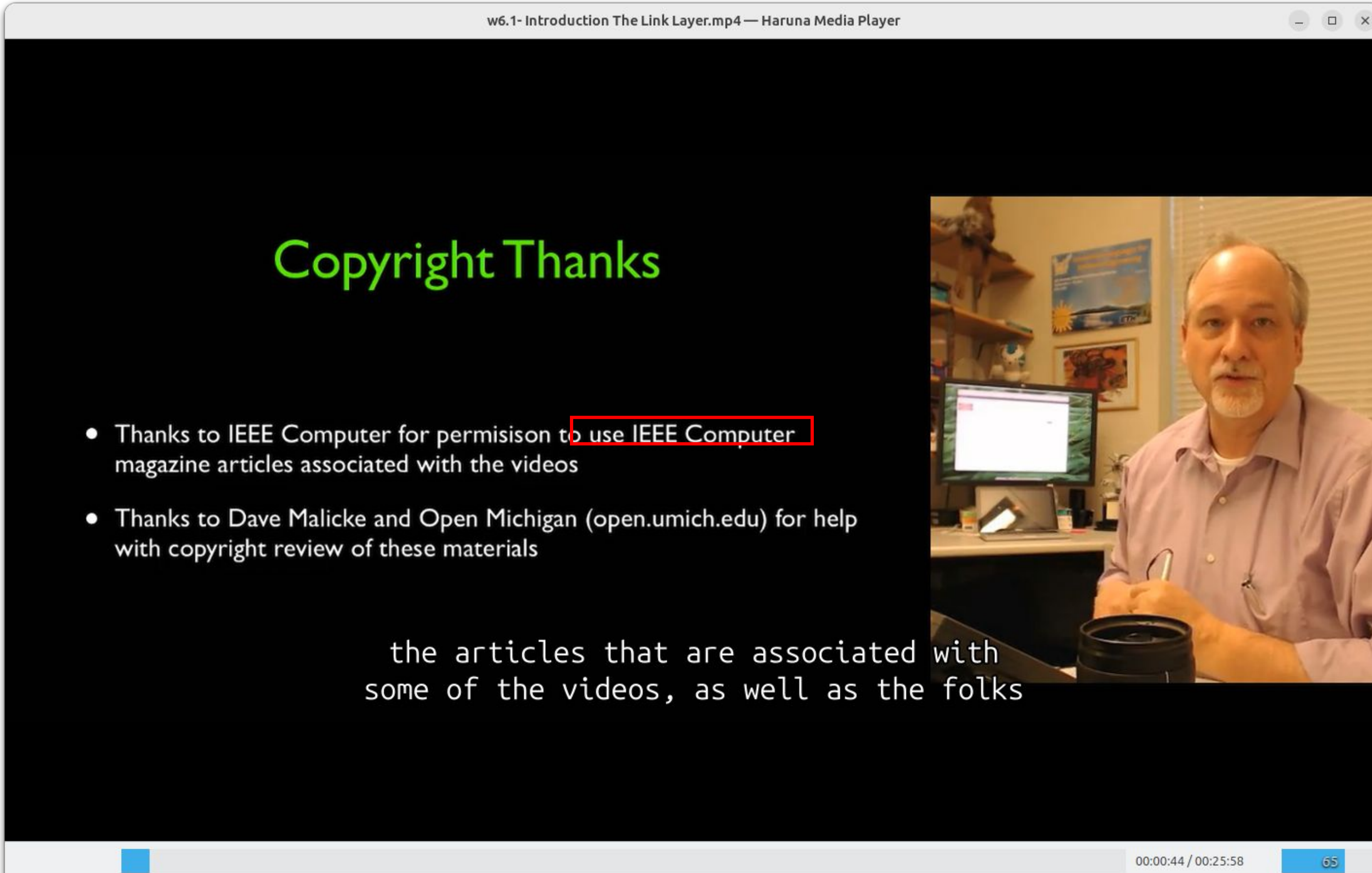
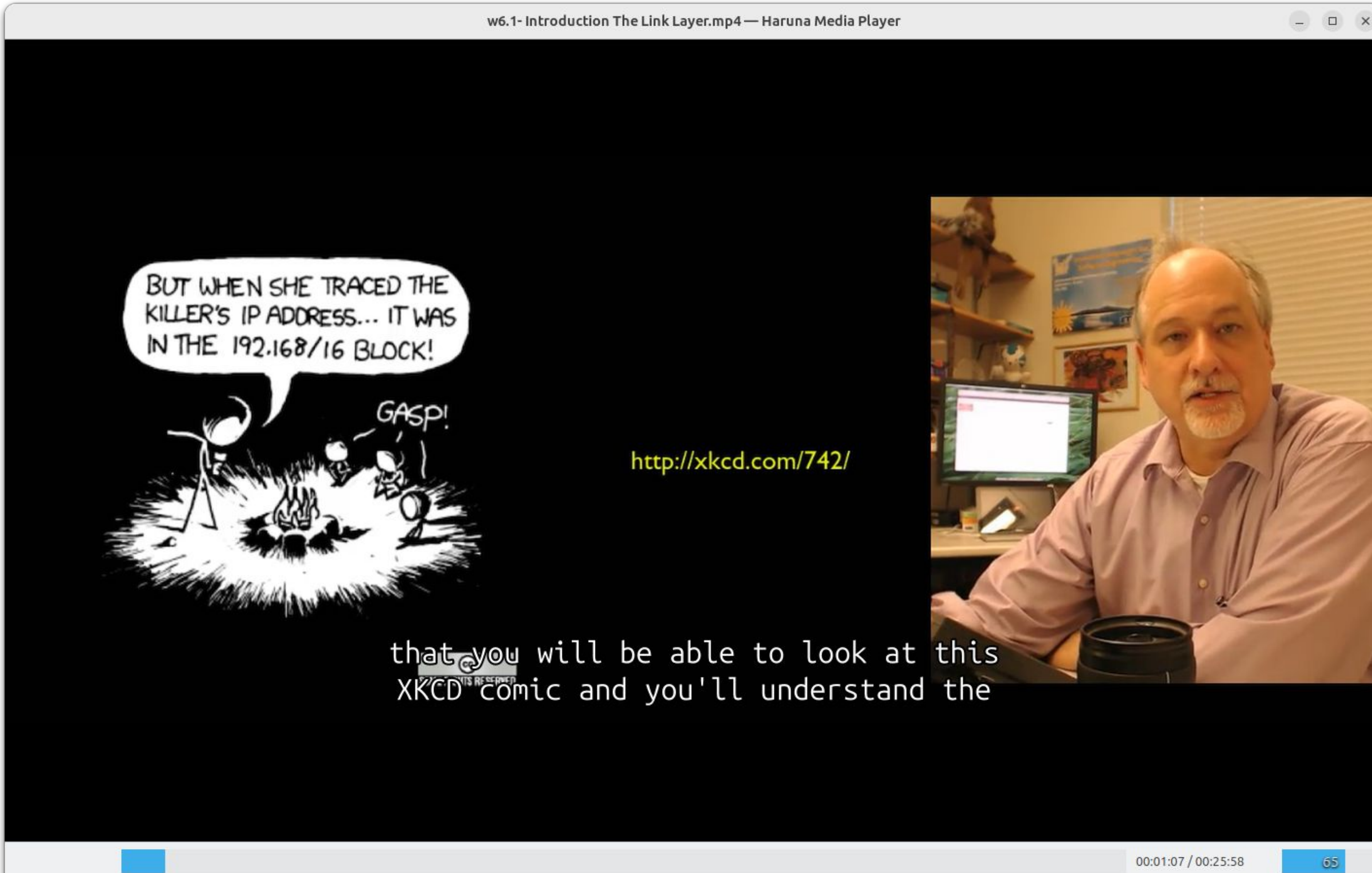
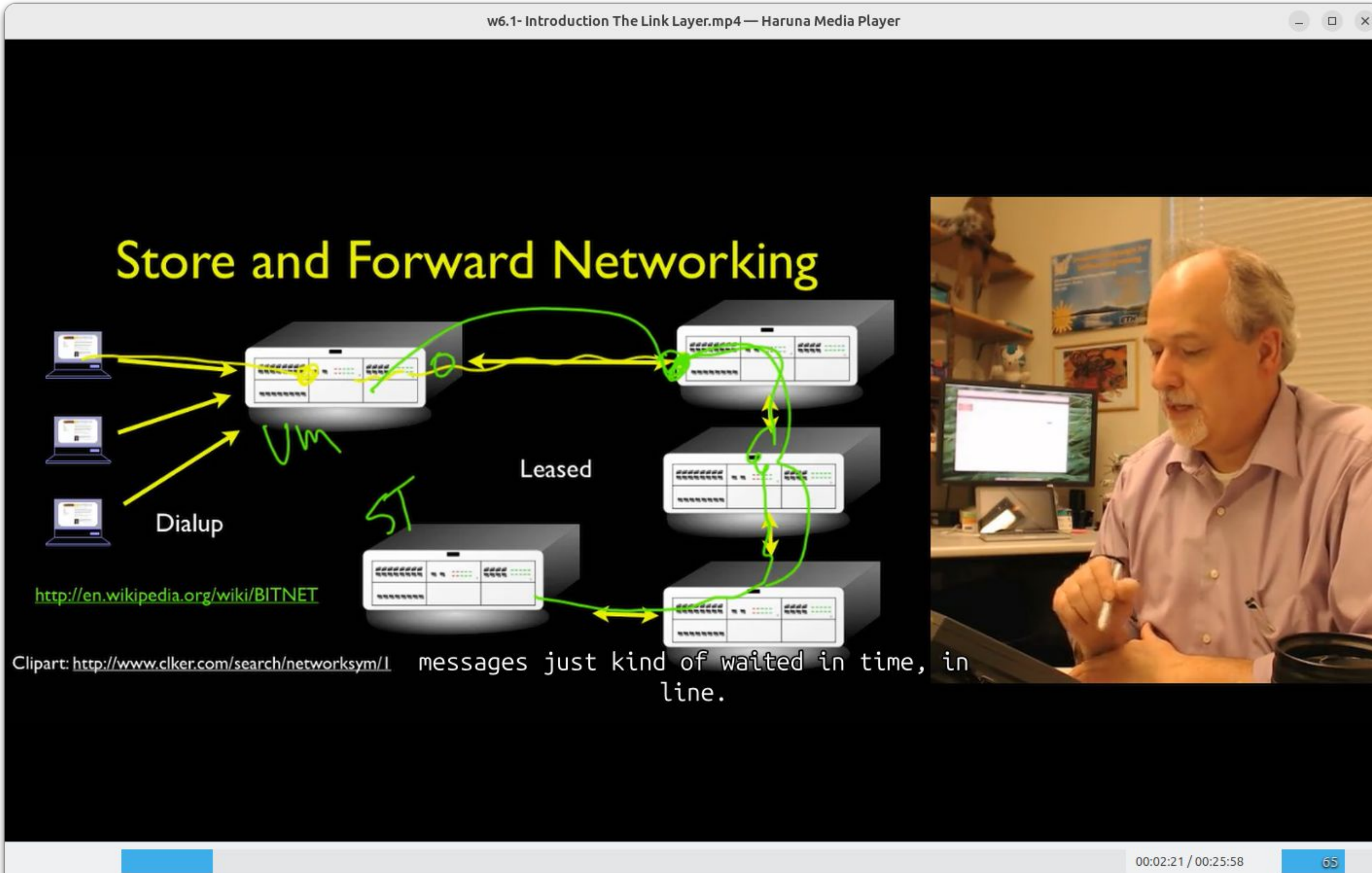
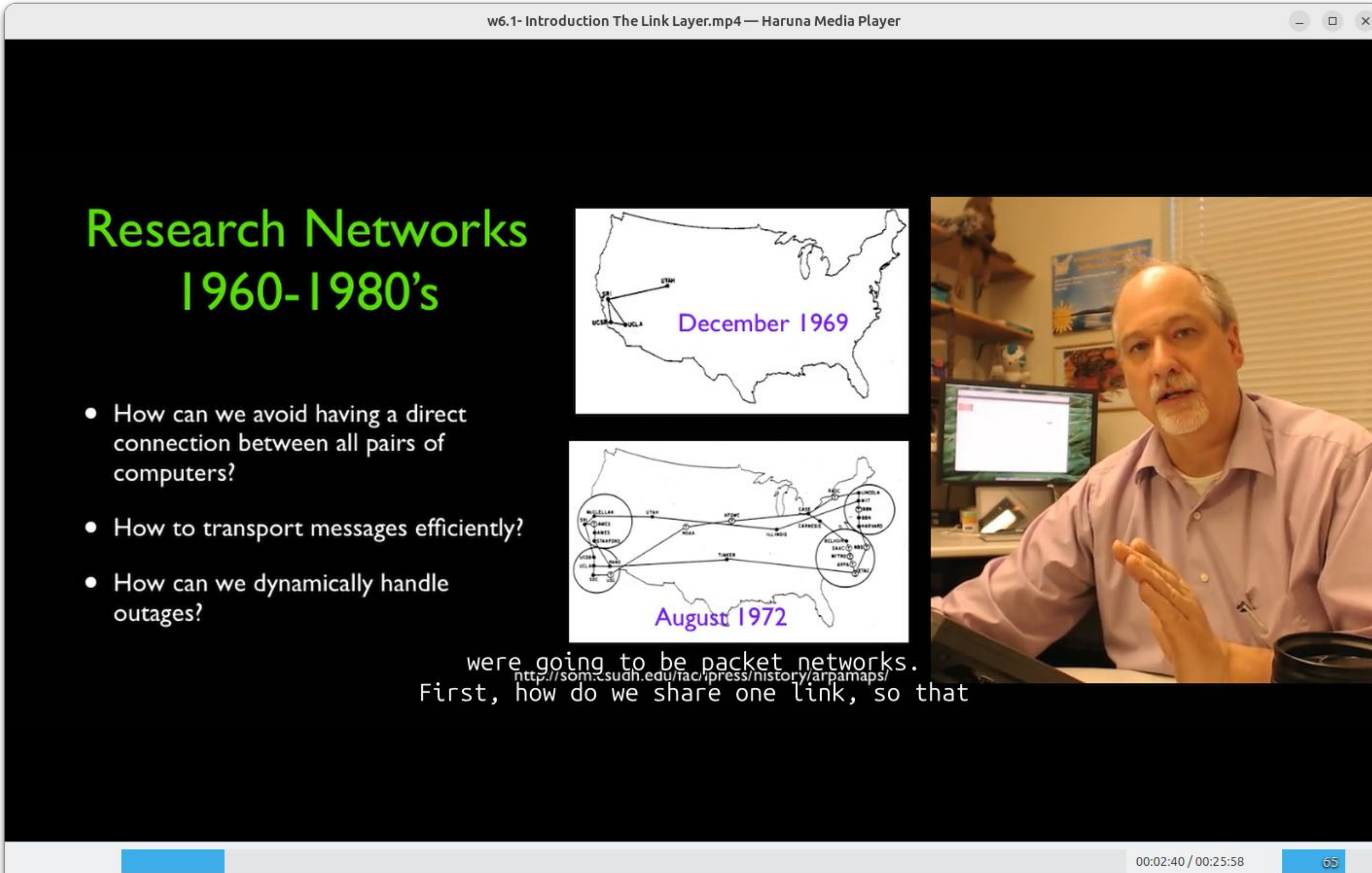
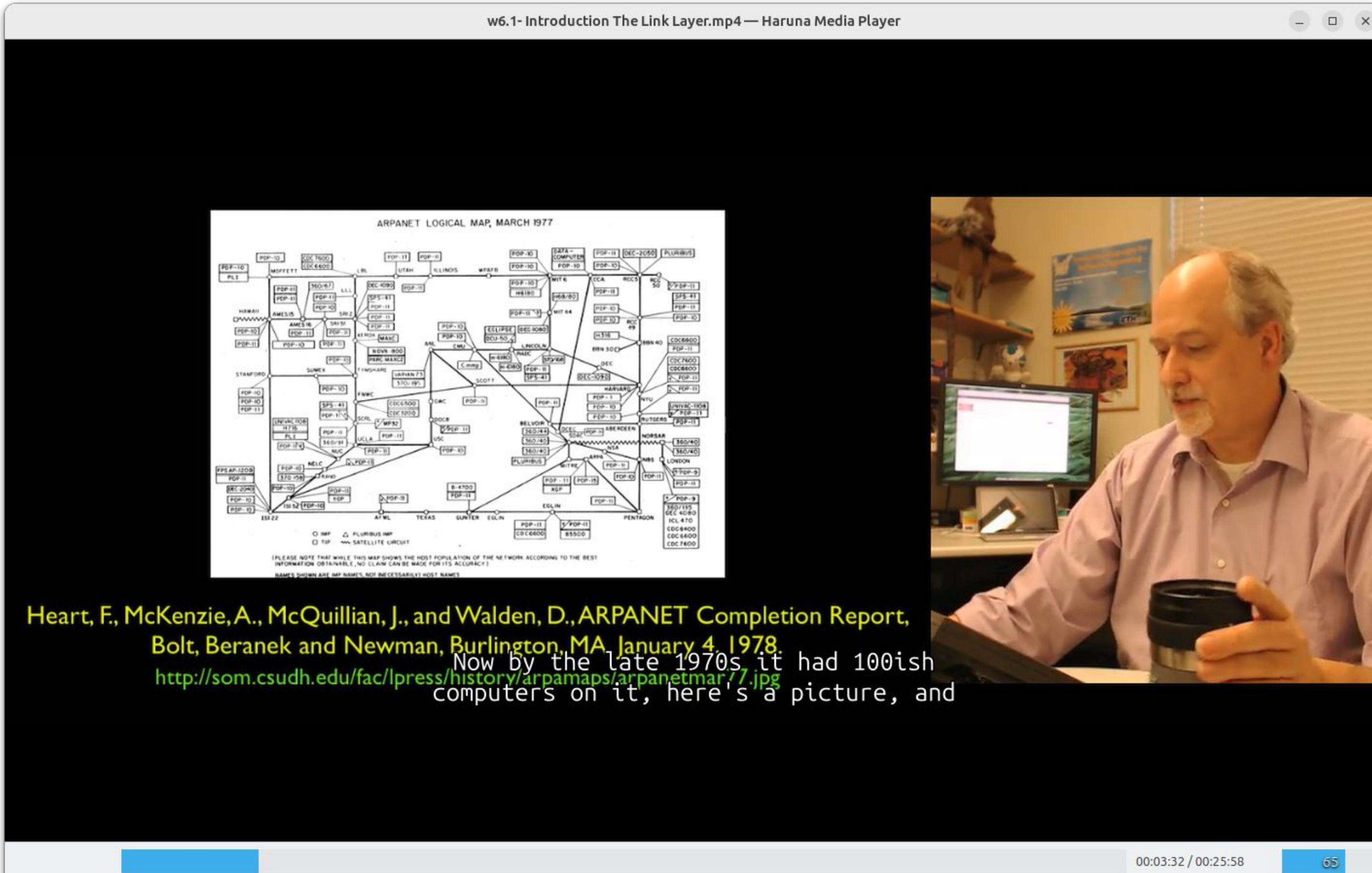
w6.1- Introduction The Link Layer

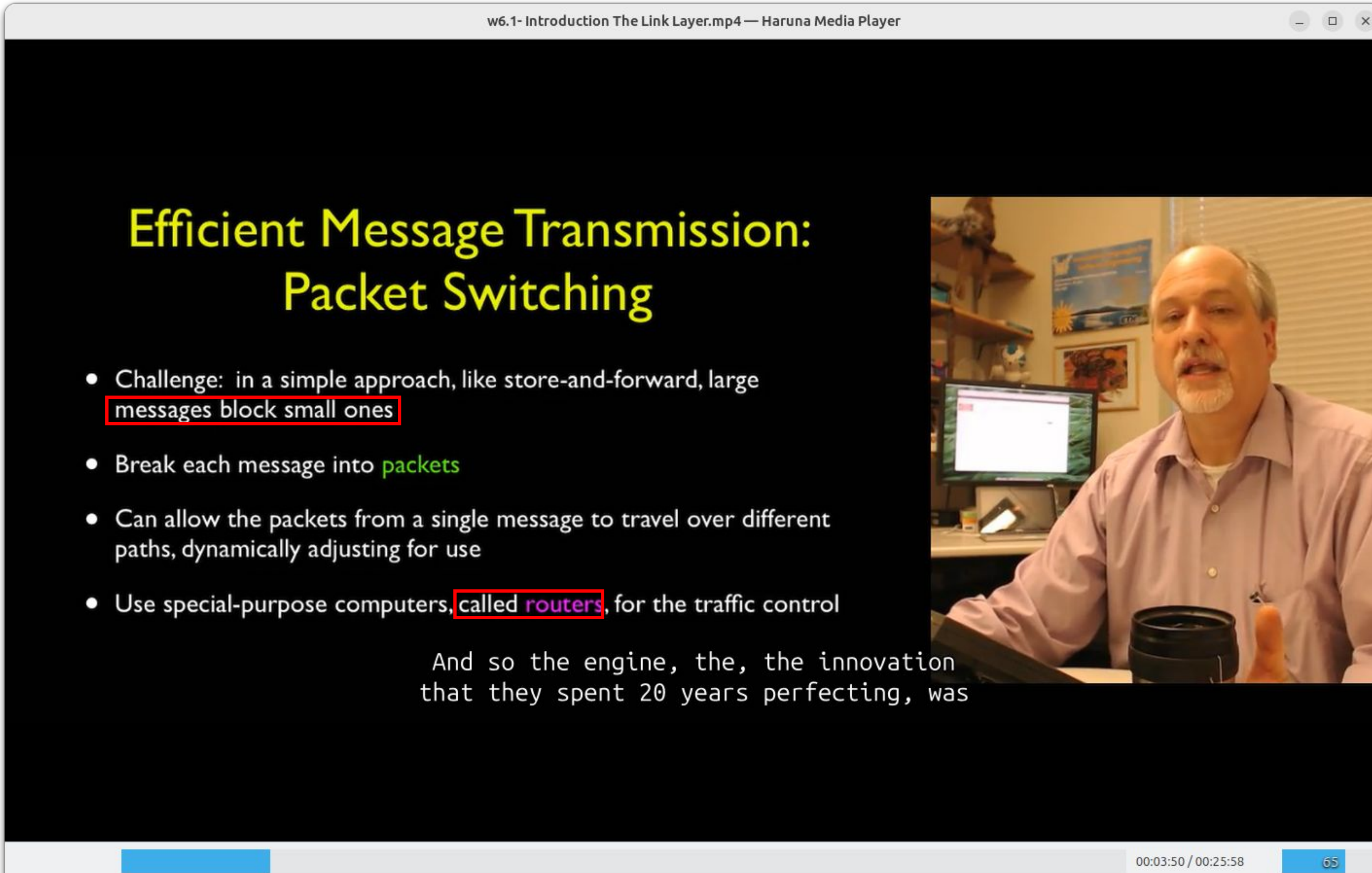

w6.1- Introduction The Link Layer.mp4 — Haruna Media Player
Copyright Thanks
• Thanks to IEEE Computer for permisison to use IEEE Computer magazine articles associated with the videos
• Thanks to Dave Malicke and Open Michigan (open.umich.edu) for help with copyright review of these materials
the articles that are associated with
some of the videos, as well as the folks
00:00:44 / 00:25:58
65

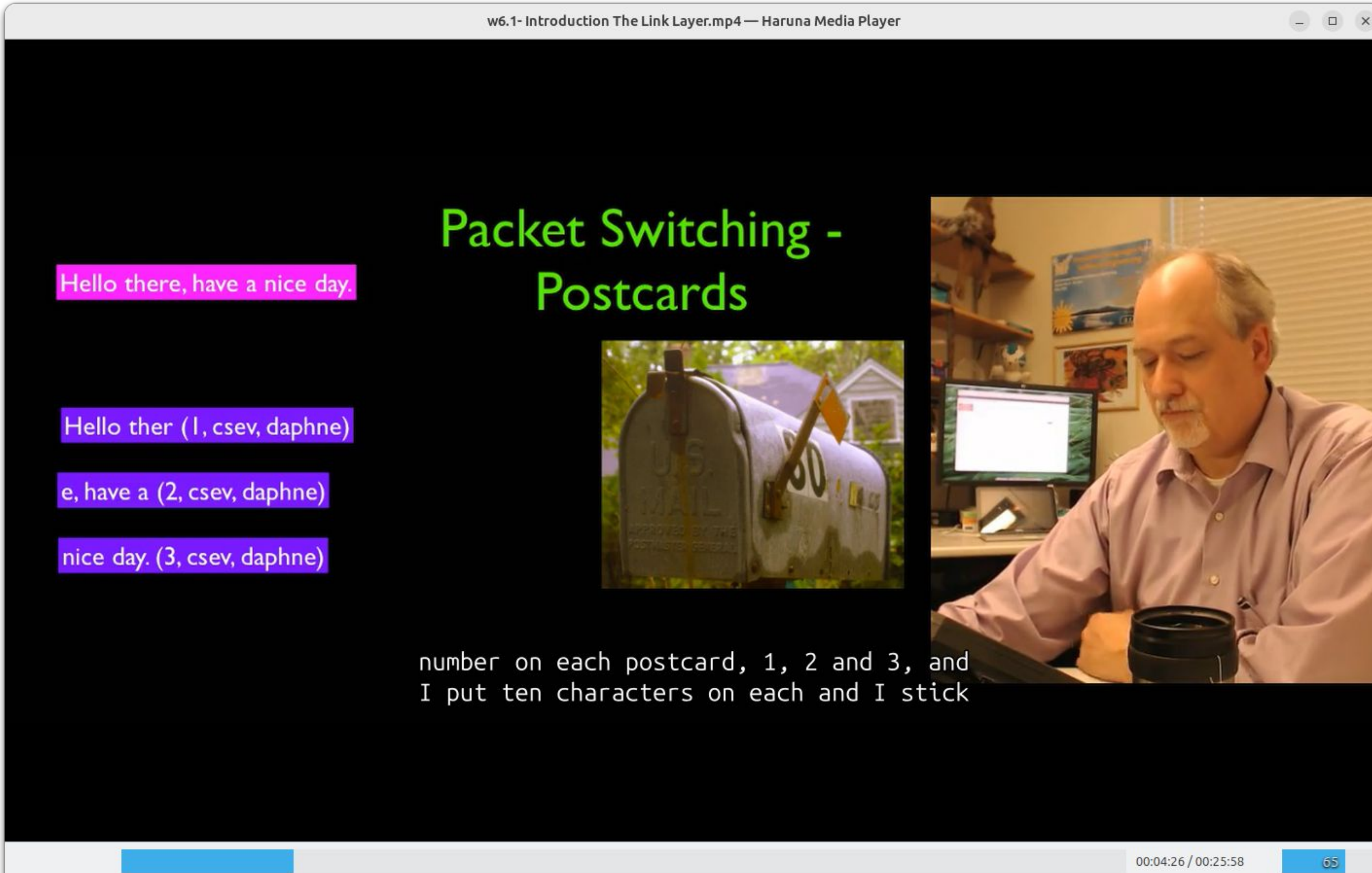

w6.1- Introduction The Link Layer.mp4 — Haruna Media Player
BUT WHEN SHE TRACED THE KILLER'S IP ADDRESS... IT WAS IN THE 192.168/16 BLOCK!
GASP!
http://xkcd.com/742/
that you will be able to look at this
XKCD comic and you'll understand the
00:01:07 / 00:25:58
65

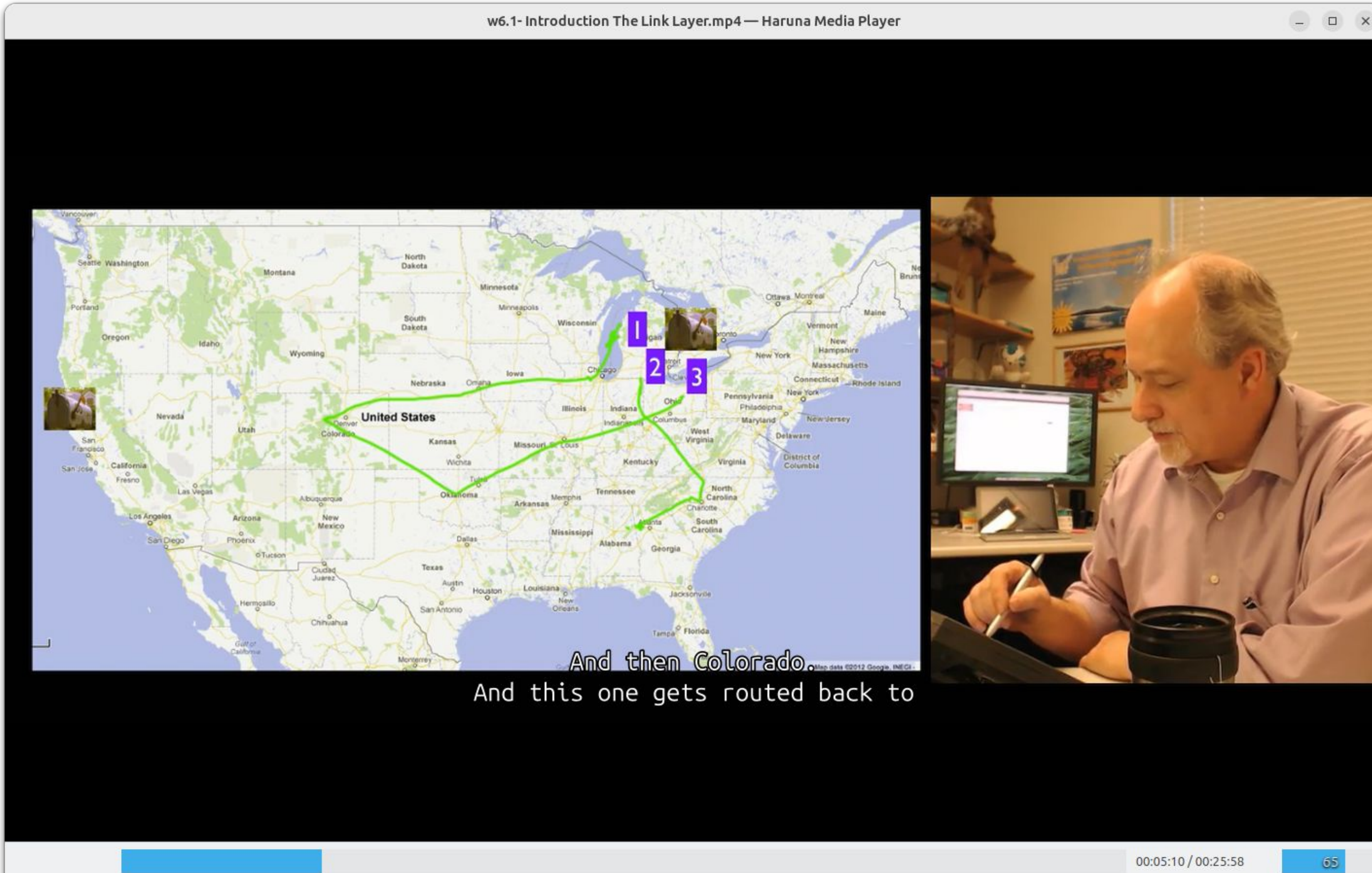

w6.1- Introduction The Link Layer.mp4 — Haruna Media Player
Store and Forward Networking
Um
Leased
ST
Dialup
http://en.wikipedia.org/wiki/BITNET
Clipart: http://www.clker.com/search/networksym/1
messages just kind of waited in time, in line.
00:02:21 / 00:25:58
65

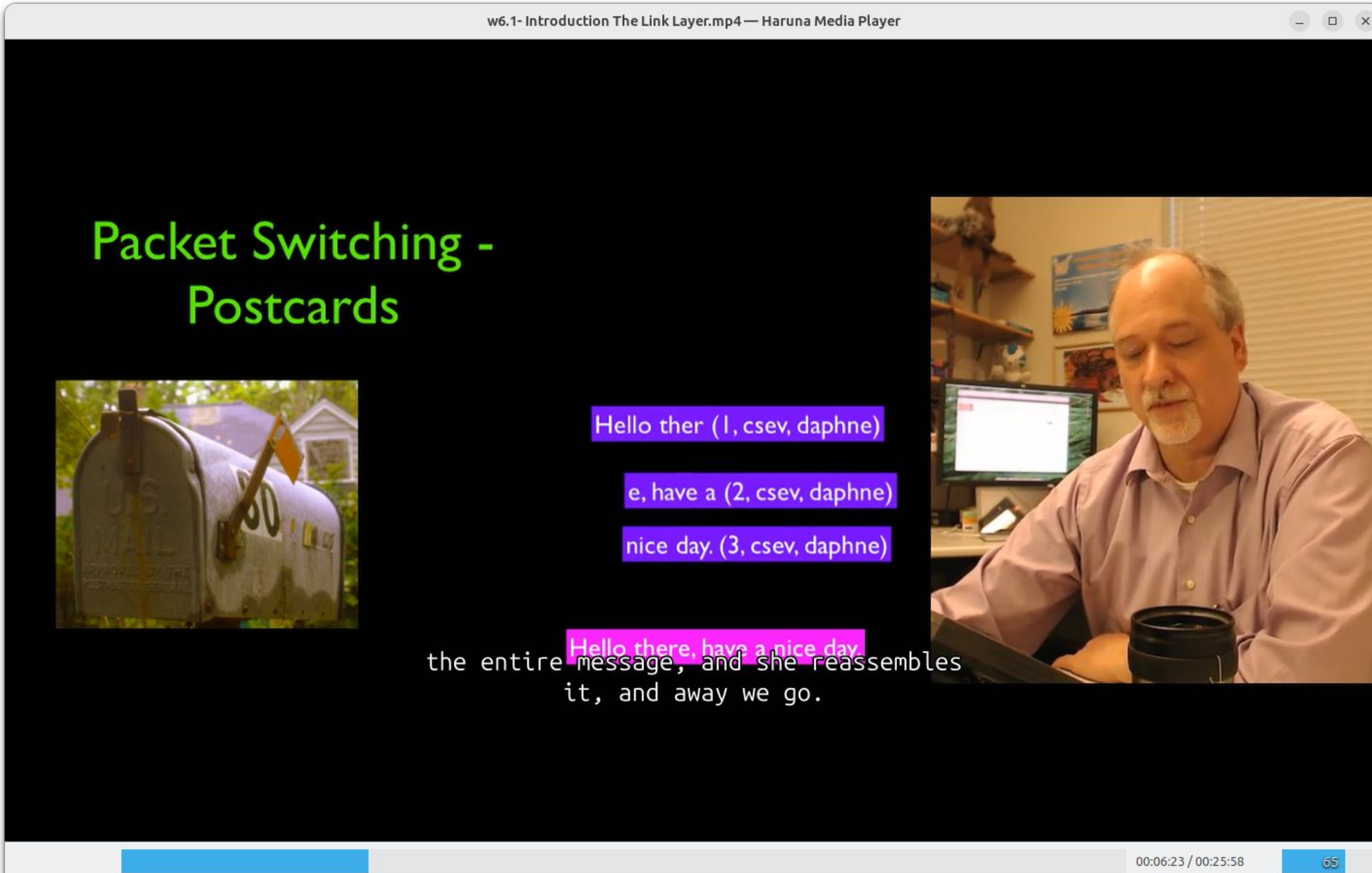

w6.1- Introduction The Link Layer.mp4 — Haruna Media Player
Research Networks
1960-1980's
• How can we avoid having a direct connection between all pairs of computers?
• How to transport messages efficiently?
• How can we dynamically handle outages?
December 1969
August 1972
http://som.csudh.edu/fac/lpress/history/arpamaps/
were going to be packet networks.
First, how do we share one link, so that
00:02:40 / 00:25:58
65

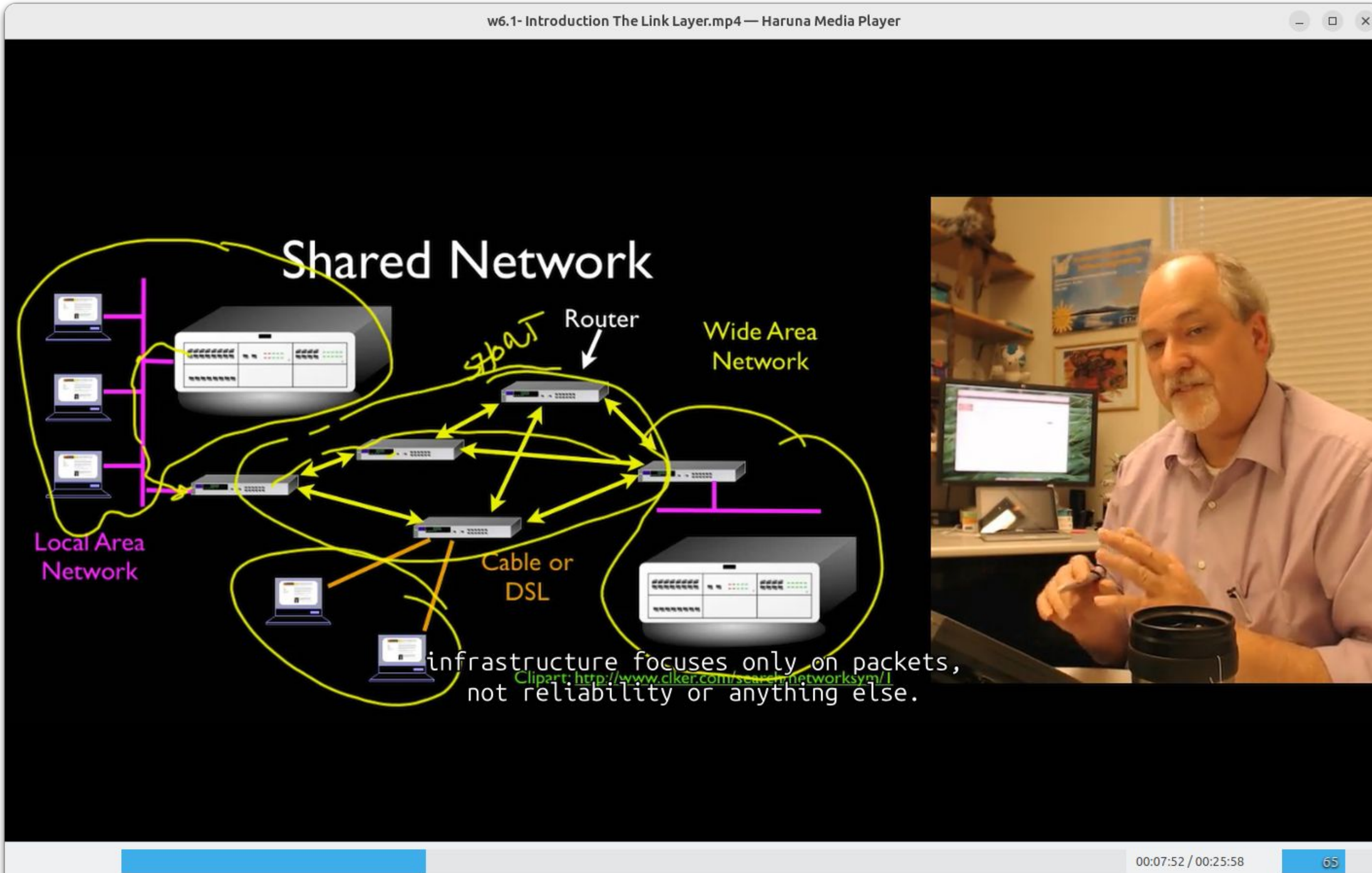

w6.1- Introduction The Link Layer.mp4 — Haruna Media Player
ARPANET LOGICAL MAP, MARCH 1977
Heart, F., McKenzie, A., McQuillian, J., and Walden, D., ARPANET Completion Report,
Bolt, Beranek and Newman, Burlington, MA, January 4, 1978.
http://som.csudh.edu/fac/lpress/history/arpamaps/arpanetmar77.jpg
Now by the late 1970s it had 100ish
computers on it, here's a picture, and
00:03:32 / 00:25:58
65

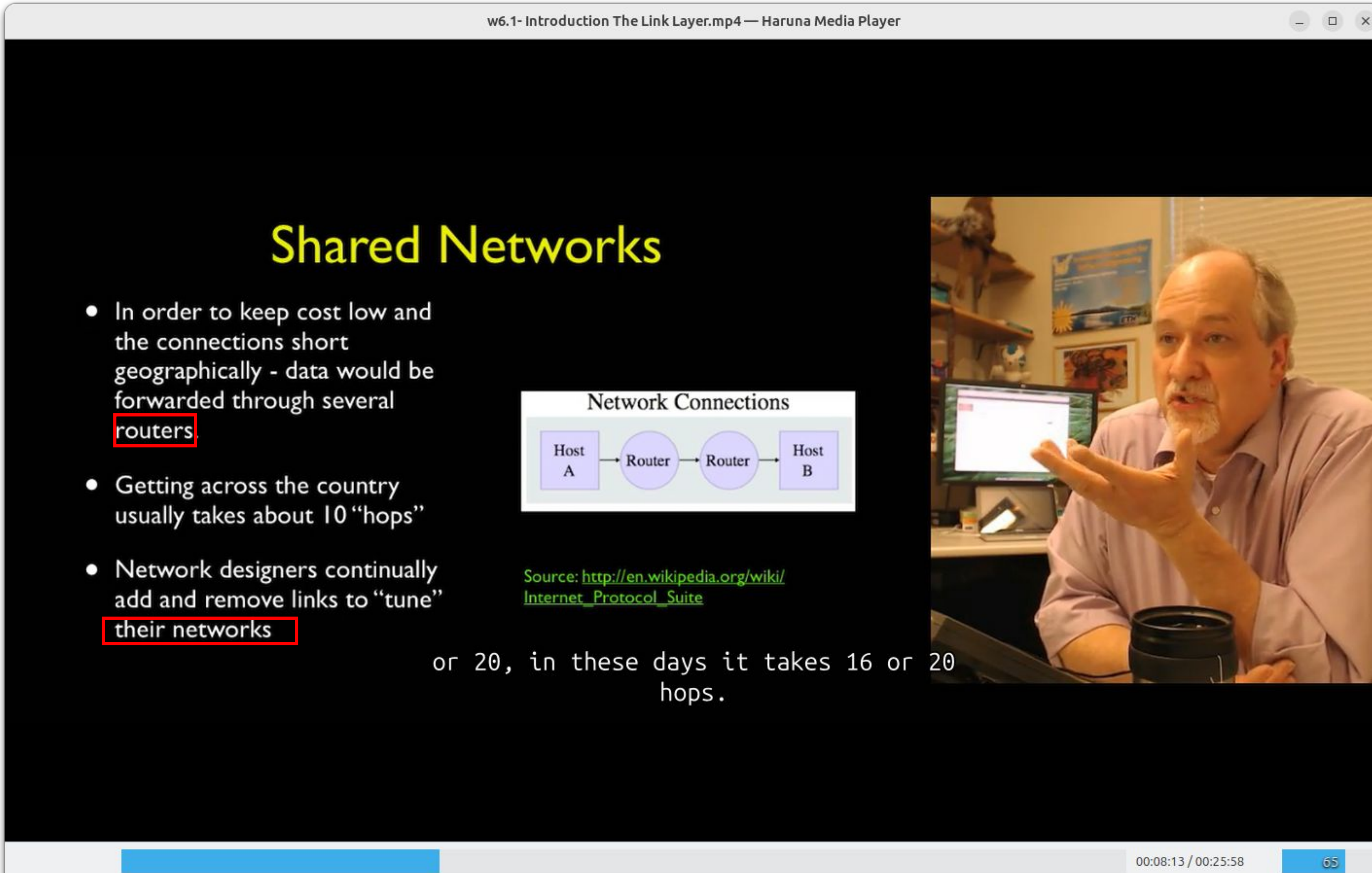

w6.1- Introduction The Link Layer.mp4 — Haruna Media Player
Efficient Message Transmission: Packet Switching
Challenge: in a simple approach, like store-and-forward, large messages block small ones
Break each message into packets
Can allow the packets from a single message to travel over different paths, dynamically adjusting for use
Use special-purpose computers, called routers, for the traffic control
And so the engine, the, the innovation
that they spent 20 years perfecting, was
00:03:50 / 00:25:58
65

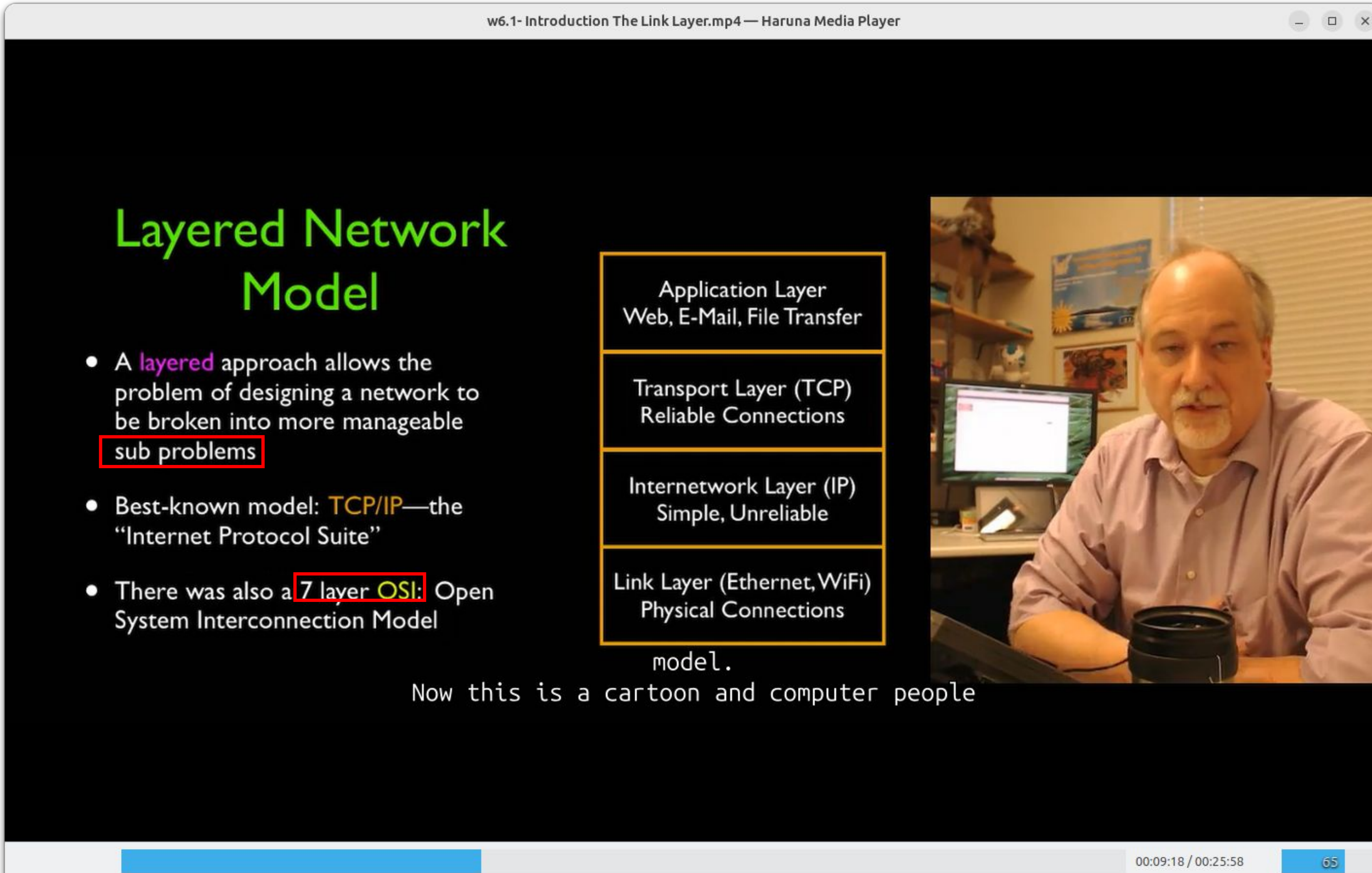

w6.1- Introduction The Link Layer.mp4 — Haruna Media Player
Packet Switching - Postcards
Hello there, have a nice day.
Hello ther (1, csev, daphne)
e, have a (2, csev, daphne)
nice day. (3, csev, daphne)
number on each postcard, 1, 2 and 3, and
I put ten characters on each and I stick
00:04:26 / 00:25:58
65

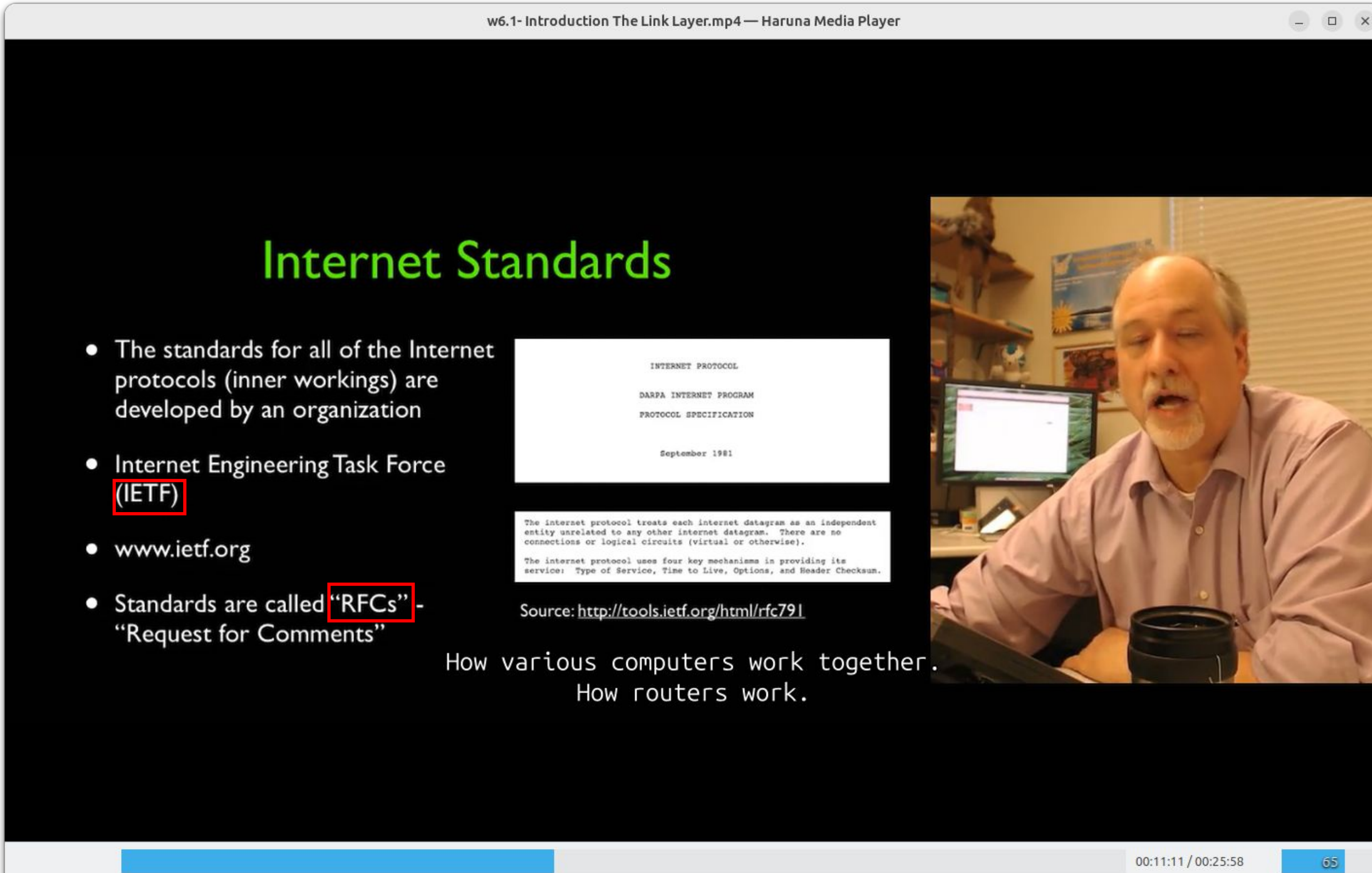

w6.1- Introduction The Link Layer.mp4 — Haruna Media Player
United States
And then Colorado.
And this one gets routed back to
00:05:10 / 00:25:58
65


w6.1- Introduction The Link Layer.mp4 — Haruna Media Player
Packet Switching - Postcards
Hello ther (1, csev, daphne)
e, have a (2, csev, daphne)
nice day. (3, csev, daphne)
Hello there, have a nice day.
the entire message, and she reassembles
it, and away we go.
00:06:23 / 00:25:58
65


w6.1- Introduction The Link Layer.mp4 — Haruna Media Player
Shared Network
Router
Wide Area
Network
Local Area
Network
Cable or
DSL
infrastructure focuses only on packets,
not reliability or anything else.
00:07:52 / 00:25:58
65


w6.1- Introduction The Link Layer.mp4 — Haruna Media Player
Shared Networks
In order to keep cost low and the connections short geographically - data would be forwarded through several routers
Getting across the country usually takes about 10 "hops"
Network designers continually add and remove links to "tune" their networks
Network Connections
Host A
Router
Router
Host B
Source: http://en.wikipedia.org/wiki/Internet_Protocol_Suite
or 20, in these days it takes 16 or 20 hops.
00:08:13 / 00:25:58
65


w6.1- Introduction The Link Layer.mp4 — Haruna Media Player
Layered Network Model
A layered approach allows the problem of designing a network to be broken into more manageable sub problems
Best-known model: TCP/IP—the "Internet Protocol Suite"
There was also a 7 layer OSI: Open System Interconnection Model
Application Layer
Web, E-Mail, File Transfer
Transport Layer (TCP)
Reliable Connections
Internetwork Layer (IP)
Simple, Unreliable
Link Layer (Ethernet, WiFi)
Physical Connections
model.
Now this is a cartoon and computer people
00:09:18 / 00:25:58
65


w6.1- Introduction The Link Layer.mp4 — Haruna Media Player
Internet Standards
The standards for all of the Internet protocols (inner workings) are developed by an organization
Internet Engineering Task Force (IETF)
www.ietf.org
Standards are called "RFCs" - "Request for Comments"
INTERNET PROTOCOL
DARPA INTERNET PROGRAM
PROTOCOL SPECIFICATION
September 1981
The internet protocol treats each internet datagram as an independent entity unrelated to any other internet datagram. There are no connections or logical circuits (virtual or otherwise).
The internet protocol uses four key mechanisms in providing its service: Type of Service, Time to Live, Options, and Header Checksum.
Source: http://tools.ietf.org/html/rfc791
How various computers work together.
How routers work.
00:11:11 / 00:25:58
65

1. IETF (Internet Engineering Task Force) = 互联网工程任务组

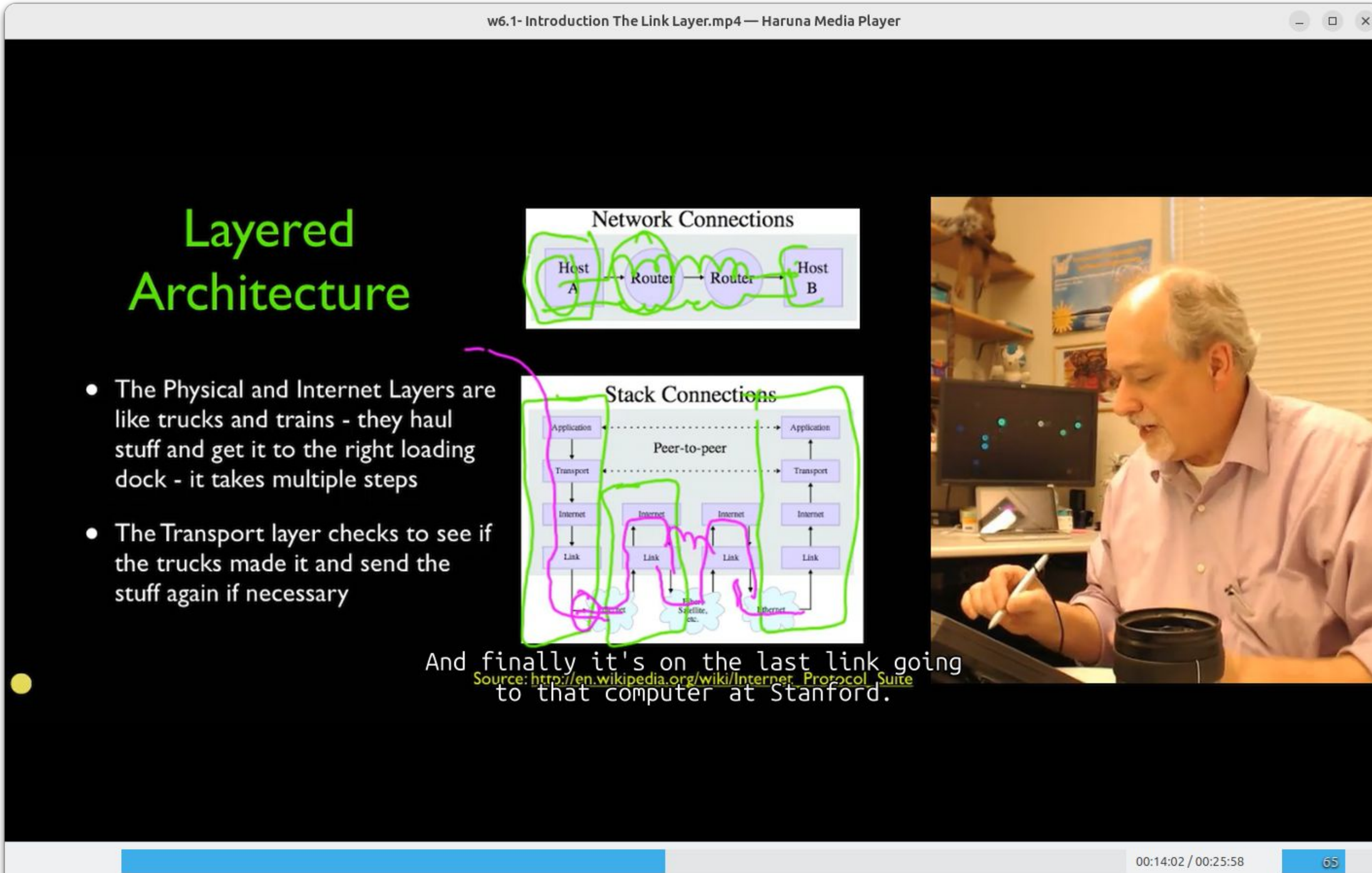
The **IETF** is the primary organization responsible for developing and promoting voluntary Internet standards. It isn't a formal government body; rather, it's a large open international community of network designers, operators, vendors, and researchers.

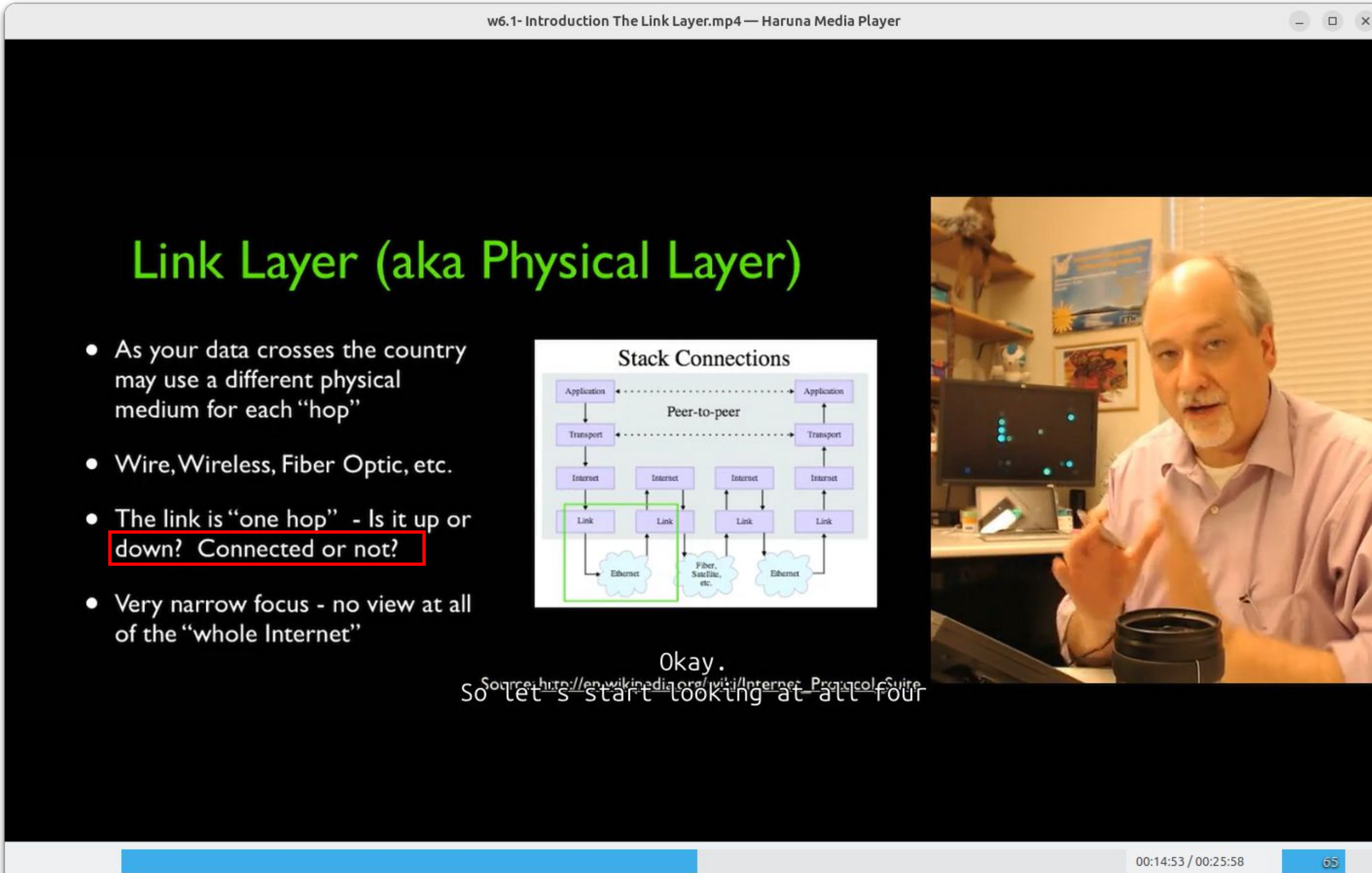
- **Their Mission:** To make the Internet work better by producing high-quality, relevant technical documents that influence the way people design, use, and manage the Internet.
- **Website:** www.ietf.org

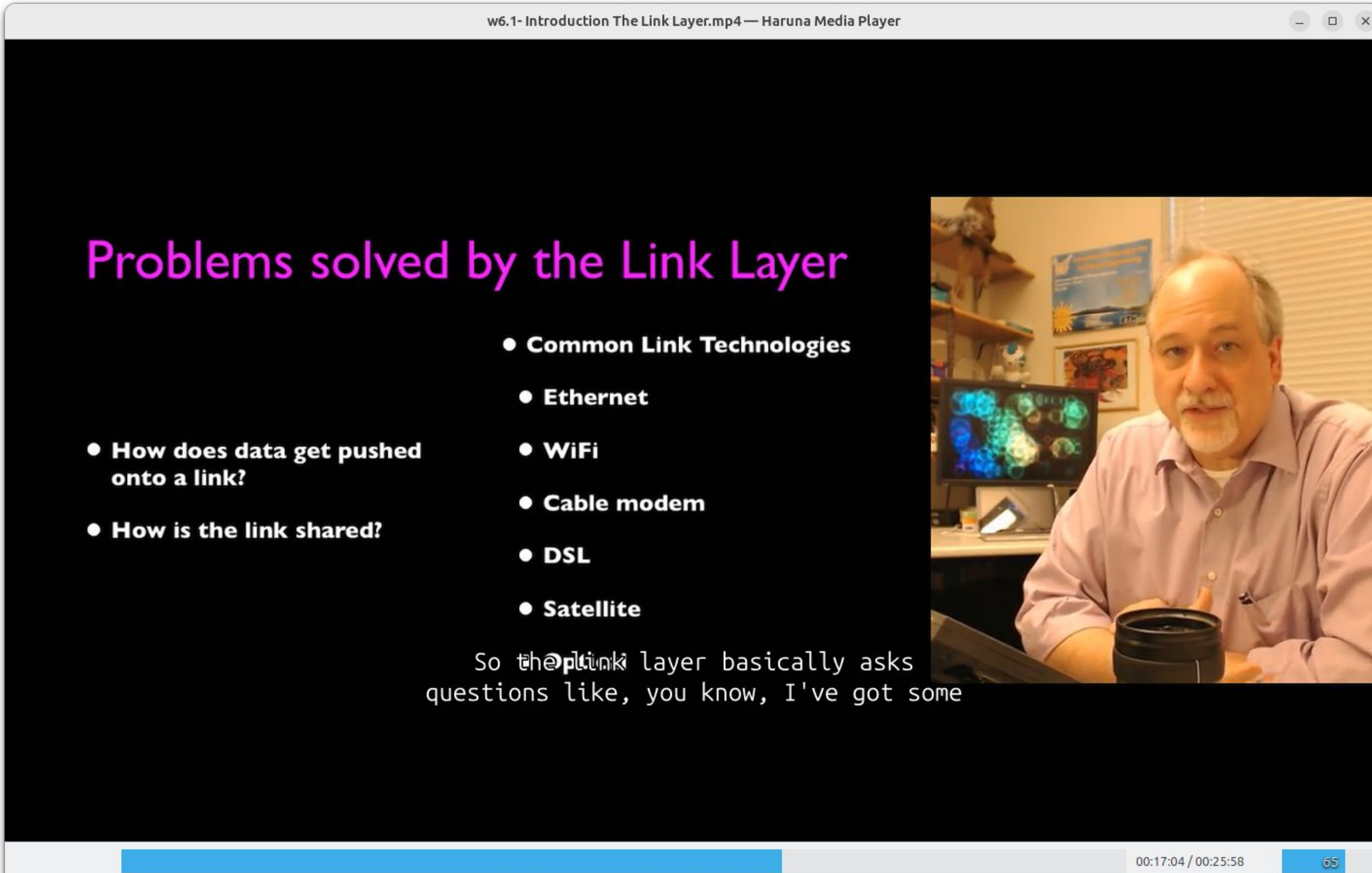
2. RFC (Request for Comments) = 请求意见稿

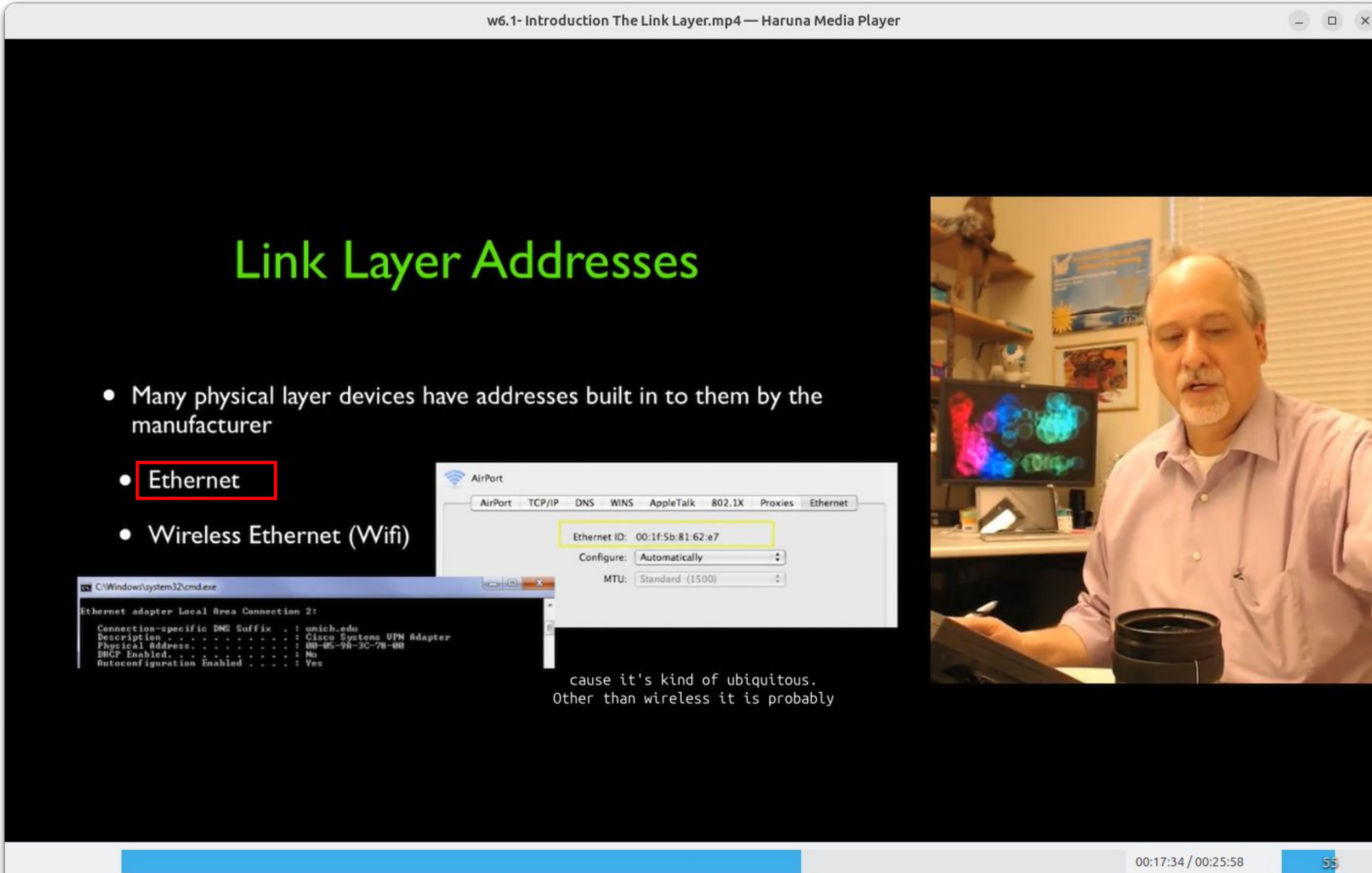
An **RFC** is a formal document drafted by the IETF. Despite the humble name "Request for Comments," these are actually the **official standards** and protocols of the Internet.

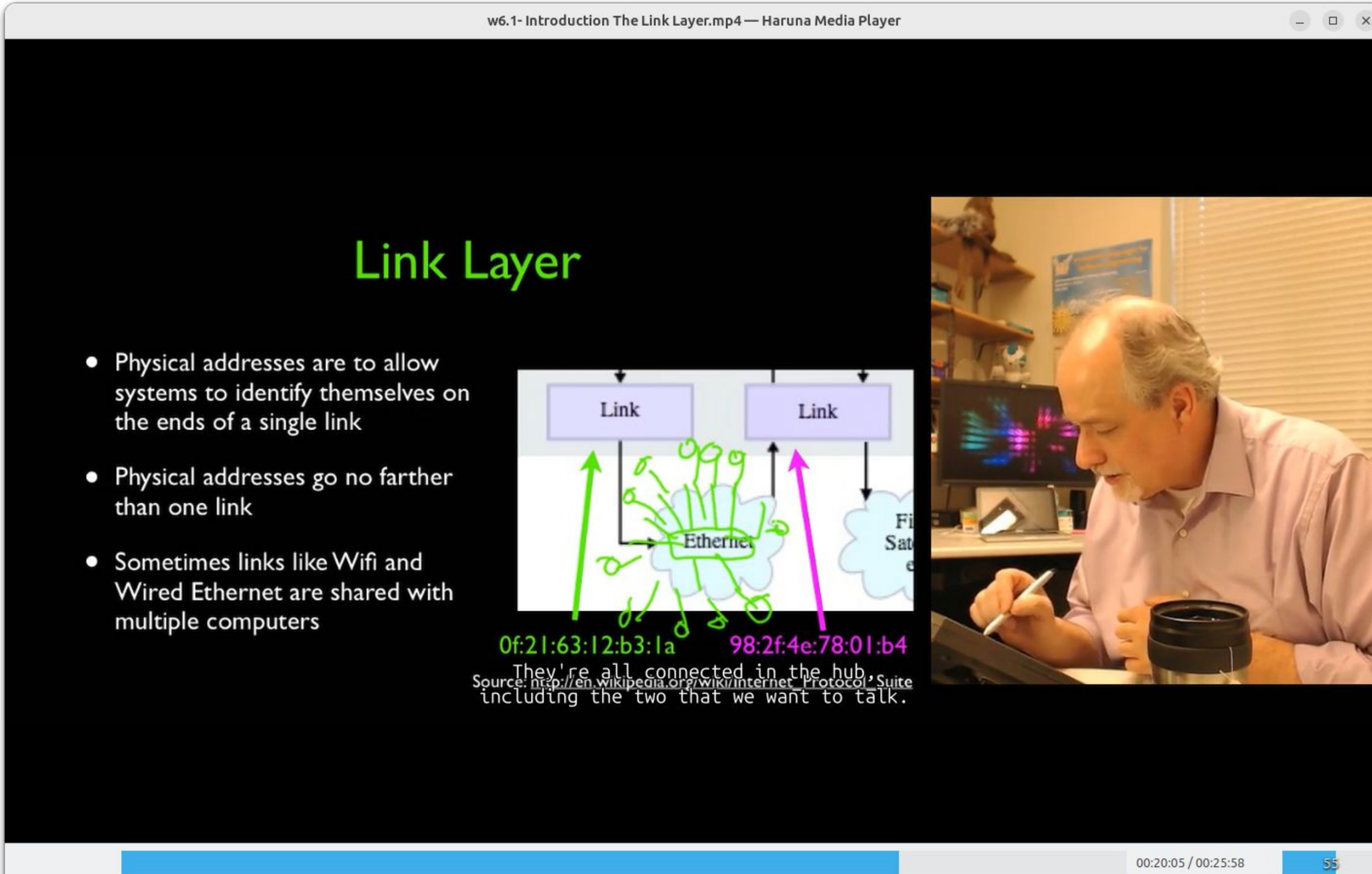
- **Evolution:** Every major technology we use—from the way email is sent (SMTP) to how websites are loaded (HTTP)—started as an RFC.
- **RFC 791:** The image specifically highlights **RFC 791**, which is the foundational specification for the **Internet Protocol (IP)** published in September 1981. This is the "DNA" of how data packets are addressed and routed across the globe.


w6.1- Introduction The Link Layer.mp4 — Haruna Media Player
Layered Architecture
• The Physical and Internet Layers are like trucks and trains - they haul stuff and get it to the right loading dock - it takes multiple steps
• The Transport layer checks to see if the trucks made it and send the stuff again if necessary
Network Connections
Host A
Router
Router
Host B
Stack Connections
Application
Application
Peer-to-peer
Transport
Transport
Internet
Internet
Internet
Internet
Link
Link
Link
Link
And finally it's on the last link going to that computer at Stanford.
Source: http://en.wikipedia.org/wiki/Internet_Protocol_Suite
00:14:02 / 00:25:58
65


w6.1- Introduction The Link Layer.mp4 — Haruna Media Player
Link Layer (aka Physical Layer)
As your data crosses the country may use a different physical medium for each "hop"
Wire, Wireless, Fiber Optic, etc.
The link is "one hop" - Is it up or down? Connected or not?
Very narrow focus - no view at all of the "whole Internet"
Stack Connections
Application
Application
Peer-to-peer
Transport
Transport
Internet
Internet
Internet
Internet
Link
Link
Link
Link
Ethernet
Fiber, Satellite, etc.
Ethernet
Okay.
So let's start looking at all four
00:14:53 / 00:25:58
65


w6.1- Introduction The Link Layer.mp4 — Haruna Media Player
Problems solved by the Link Layer
How does data get pushed onto a link?
How is the link shared?
Common Link Technologies
Ethernet
WiFi
Cable modem
DSL
Satellite
So the link layer basically asks
questions like, you know, I've got some
00:17:04 / 00:25:58
65


w6.1- Introduction The Link Layer.mp4 — Haruna Media Player
Link Layer Addresses
Many physical layer devices have addresses built in to them by the manufacturer
Ethernet
Wireless Ethernet (Wifi)
AirPort
AirPort TCP/IP DNS WINS AppleTalk 802.1X Proxies Ethernet
Ethernet ID: 00:1f:5b:81:62:e7
Configure: Automatically
MTU: Standard (1500)
C:\Windows\system32\cmd.exe
Ethernet adapter Local Area Connection 2:
Connection-specific DNS Suffix . : umich.edu
Description . . . . : Cisco Systems VPN Adapter
Physical Address. . . . . : 00-05-9A-3C-78-00
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
cause it's kind of ubiquitous.
Other than wireless it is probably
00:17:34 / 00:25:58



w6.1- Introduction The Link Layer.mp4 — Haruna Media Player
Link Layer
• Physical addresses are to allow systems to identify themselves on the ends of a single link
• Physical addresses go no farther than one link
• Sometimes links like Wifi and Wired Ethernet are shared with multiple computers
Link
Link
Ethernet
0f:21:63:12:b3:1a
98:2f:4e:78:01:b4
Source: http://en.wikipedia.org/wiki/Internet_Protocol_Suite
They're all connected in the hub,
including the two that we want to talk.
00:20:05 / 00:25:58
55

The **Link Layer** (also known as the Data Link Layer) is the lowest layer of the TCP/IP stack that your software interacts with. While the Internet Layer (IP) handles routing across the globe, the Link Layer is responsible for the actual physical delivery of data between two devices on the same local network.

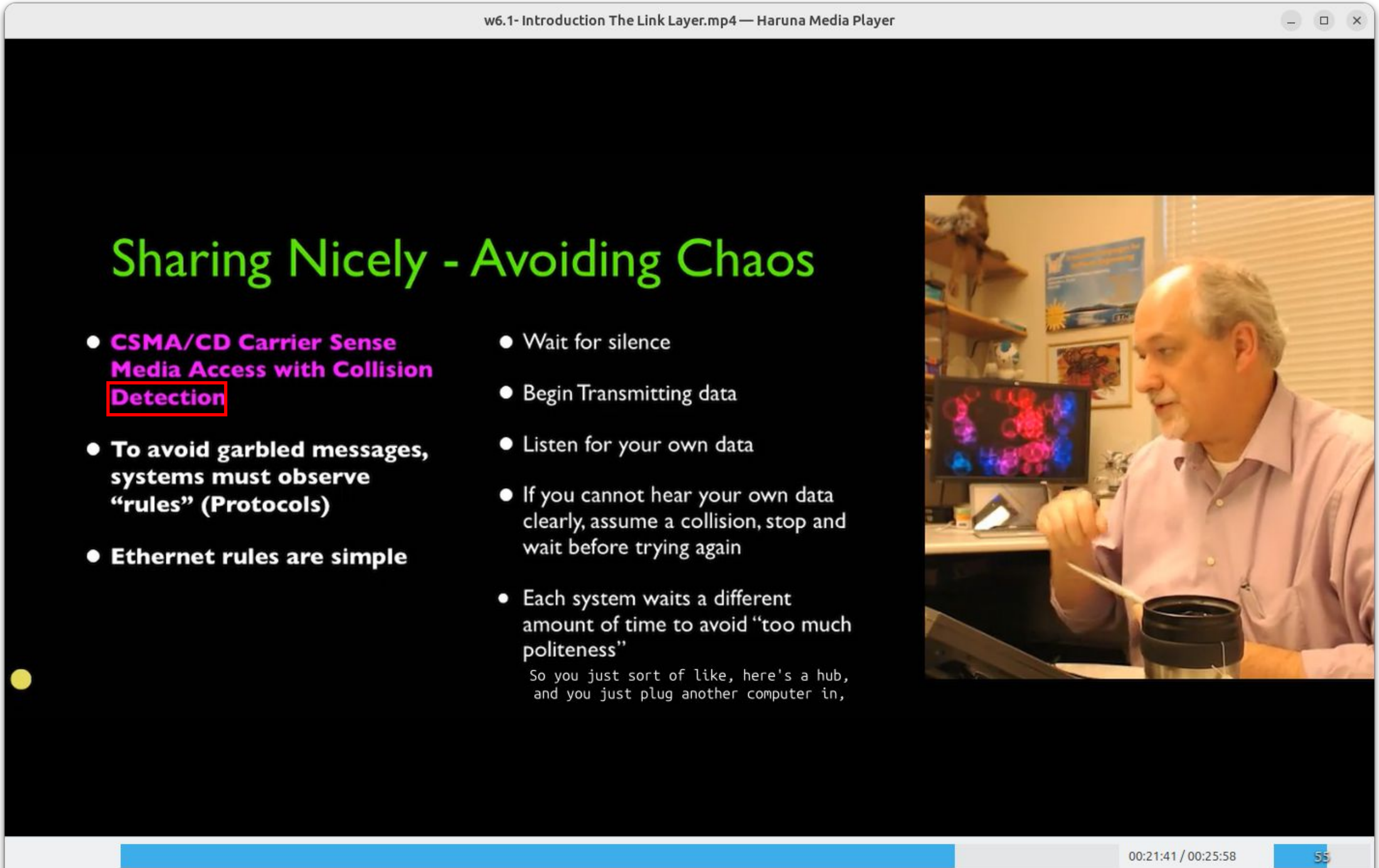
How It Works in Practice

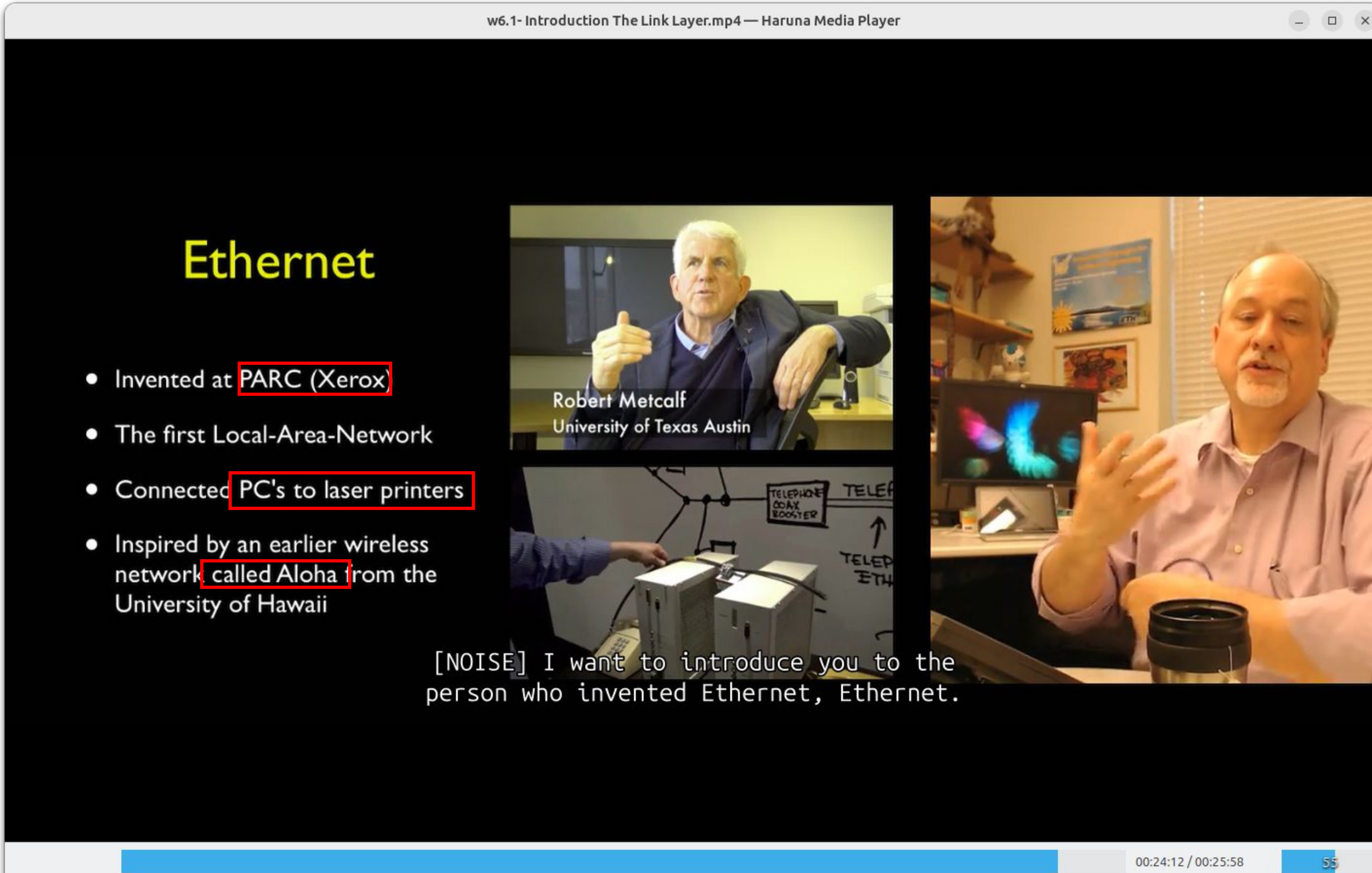
If your rover is communicating with your workstation via Wi-Fi or Ethernet, they are using Link Layer protocols:

- **Ethernet (IEEE 802.3):** The standard for wired connections. It uses cables to send electrical or optical signals.
- **Wi-Fi (IEEE 802.11):** The standard for wireless connections. It manages how data is pulsed through radio waves.
- **ARP (Address Resolution Protocol):** This is the "glue" protocol. It translates an **IP Address** (Internet Layer) into a **MAC Address** (Link Layer) so the hardware knows exactly which physical network card to send the data to.

The "Link" vs. The "Internet"

- **Internet Layer (IP):** Cares about the **Final Destination** (e.g., a server in another city).
- **Link Layer:** Cares about the **Next Hop** (e.g., the router sitting on your desk).


w6.1- Introduction The Link Layer.mp4 — Haruna Media Player
Sharing Nicely - Avoiding Chaos
CSMA/CD Carrier Sense Media Access with Collision Detection
To avoid garbled messages, systems must observe "rules" (Protocols)
Ethernet rules are simple
Wait for silence
Begin Transmitting data
Listen for your own data
If you cannot hear your own data clearly, assume a collision, stop and wait before trying again
Each system waits a different amount of time to avoid "too much politeness"
So you just sort of like, here's a hub,
and you just plug another computer in,
00:21:41 / 00:25:58
55


w6.1- Introduction The Link Layer.mp4 — Haruna Media Player
Ethernet
Invented at PARC (Xerox)
The first Local-Area-Network
Connected PC's to laser printers
Inspired by an earlier wireless network called Aloha from the University of Hawaii
Robert Metcalf
University of Texas Austin
[NOISE] I want to introduce you to the
person who invented Ethernet, Ethernet.
00:24:12 / 00:25:58

Summary

From History to Technology: The Packet Revolution

The transition from old-school "Store and Forward" networking to modern packet-switching was the "Target" of the research networks from the 60s to the 80s (ARPANET).

- **Store and Forward (The Old Way):** Messages were moved in "hops" between powerful computers with long-term storage. One message occupied a link at a time, creating massive delays (minutes to days).
- **Packet Switching (The Innovation):** Messages are broken into small **packets** (think postcards).
  - **Efficiency:** Multiple users share one link simultaneously.
  - **Dynamic Routing:** Packets can take different paths to the same destination and be reassembled using sequence numbers.
  - **Speed:** Reduces cross-country latency from days to fractions of a second.

🏗️ The Four-Layer Internet Model (TCP/IP)

To solve the "Magnitude 1,000,000" problem of global data reliability, engineers broke it into four manageable software layers. While the 7-layer OSI model exists, the **TCP/IP model** is the one that actually won the war.

1. The Link Layer (The Bottom Layer)

This is the only layer that handles the "physical" reality of moving data across a single hop (e.g., one wire or one WiFi signal).

- **Scope:** It doesn't care about the World Wide Web; its only job is to get data across one connection.
- **Hardware:** Ethernet, WiFi, Fiber, DSL.
- **Addressing:** Every piece of hardware has a unique **MAC address** (Serial Number). These are used to identify which packet belongs to which device on a shared medium.

🚦 Collision Control: CSMA/CD

Since media like WiFi (air) or Ethernet (hubs) are shared, we need "Network Courtesy" to prevent chaos. **Robert Metcalfe** (Xerox PARC) invented Ethernet based on these principles:

Carrier Sense Multiple Access with Collision Detection (CSMA/CD):

1. **Listen:** Before sending, the computer listens for silence.
2. **Transmit:** If quiet, it starts sending.
3. **Monitor:** It listens to its own transmission to ensure it isn't "crushed" by someone else.
4. **Back-off:** If a collision occurs, the computer waits for a **random** amount of time before trying again to ensure fairness.

> **Ninja Note:** This "courtesy" logic is what allows your IoT devices to talk without turning the Aachen-Sanctuary into a digital battlefield.

CSMA stands for **Carrier Sense Multiple Access** (载波侦听多路访问). It is a "traffic control" protocol used in the Link Layer to verify that a shared communication medium (like a copper wire or the airwaves) is clear before a device tries to send data.

Think of it like a polite conversation at a dinner table in your **Aachen-Sanctuary**: you listen for a gap in speech before you start talking so you don't interrupt anyone.

How It Works (The Core Logic)

1. **Carrier Sense (载波侦听):** Before sending a frame, the network interface "listens" to the line. If it detects a signal (the "carrier"), it waits.
2. **Multiple Access (多路访问):** Many devices are attached to the same physical cable or radio frequency and all have equal right to use it.

1. CSMA/CD (The Wired Approach)

In a wired Ethernet setup, devices can "listen" while they "talk." If two devices start transmitting at the exact same millisecond, they will detect a voltage spike (a collision).

- **Action:** Both stop immediately, wait a random amount of time (the *Backoff* period), and try again.

2. CSMA/CA (The Wireless Approach)

On Wi-Fi, a radio cannot usually "listen" and "talk" at the same time (the transmitter drowns out the receiver). Therefore, it cannot *detect* a collision while it is happening.

- **Action:** It tries to *avoid* the collision entirely by sending a tiny "Ready to Send" (RTS) signal. If the receiver replies with "Clear to Send" (CTS), the device transmits the full data package.

w6.4- Vint Cerf - A Brief History of Packets


w6.4- Vint Cerf - A Brief History of Packets.mp4 — Haruna Media Player
Subtitle scale: 0.3
Vint Cerf
Google Chief Internet Evangelist
specifically studied by Leon Kleinrock at
MIT, who was actually looking at message
00:00:18 / 00:15:58
95

Summary

The Genesis of Packet Switching (1961–1966)

- **Leonard Kleinrock (1961):** Developed queuing theories at MIT. While he called it "message switching," his dissertation provided the mathematical foundation for what we now know as packet switching.
- **Paul Baran (1962):** Working for RAND, he envisioned a distributed network to survive a nuclear attack. He proposed "hot potato routing" and breaking voice into 20ms message blocks. Traditional telcos (AT&T) mocked the idea as "impossible."
- **Donald Davies (1965):** At the National Physical Laboratory in the UK, he coined the actual term **"packet."** He built a single-node network that essentially functioned as the first Local Area Network (LAN).

The ARPANET Era (1966–1972)

- **The Visionaries:** J.C.R. Licklider ("Intergalactic Network" concept) and Douglas Engelbart (hyperlinking, the mouse) bonded over the idea of computers as tools for human collaboration, not just number crunching.
- **The Catalyst:** Bob Taylor at ARPA grew frustrated with having three separate terminals in his office to talk to three different machines. He secured $1M in 20 minutes to build a unified network.
- **The Implementation:** Larry Roberts was recruited to lead the project. BBN (Bolt, Beranek and Newman) was selected to build the hardware, while graduate students like Steve Crocker (RFCs) and Jon Postel (IANA) developed the protocols.
- **The Debut:** October 1972, the first public demonstration of ARPANET took place in a hotel basement in D.C.

The Birth of the "Internet" (1973–1978)

- **The Problem:** The military needed communication across mobile radios (tanks), satellites (ships), and fixed wires.
- **The Solution:** Bob Kahn and Vint Cerf realized they shouldn't build one giant network, but rather a way to **connect different networks.**
- **TCP/IP Emergence:**
  - They invented the **Gateway** (now called a **Router**).
  - They moved reliability to the "edges" (end-to-end) rather than the network itself.
  - **December 1974:** The word **"Internet"** appeared in print for the first time in their specifications.
- **The Split:** In 1978, they split TCP into **TCP** (reliable, for data) and **IP** (routing), while adding **UDP** (low-latency, for real-time voice/radar).

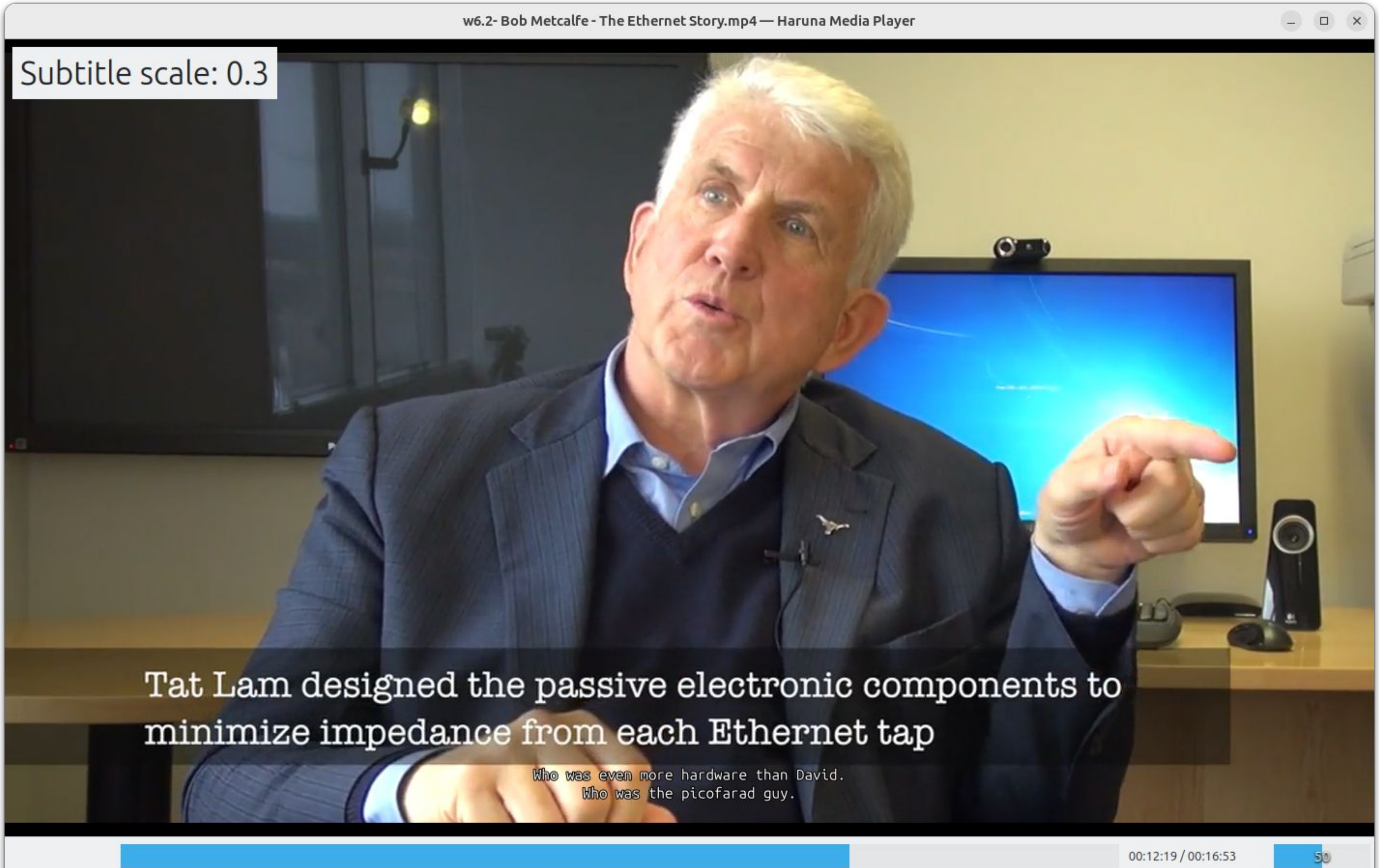
Global Scaling (1980s)

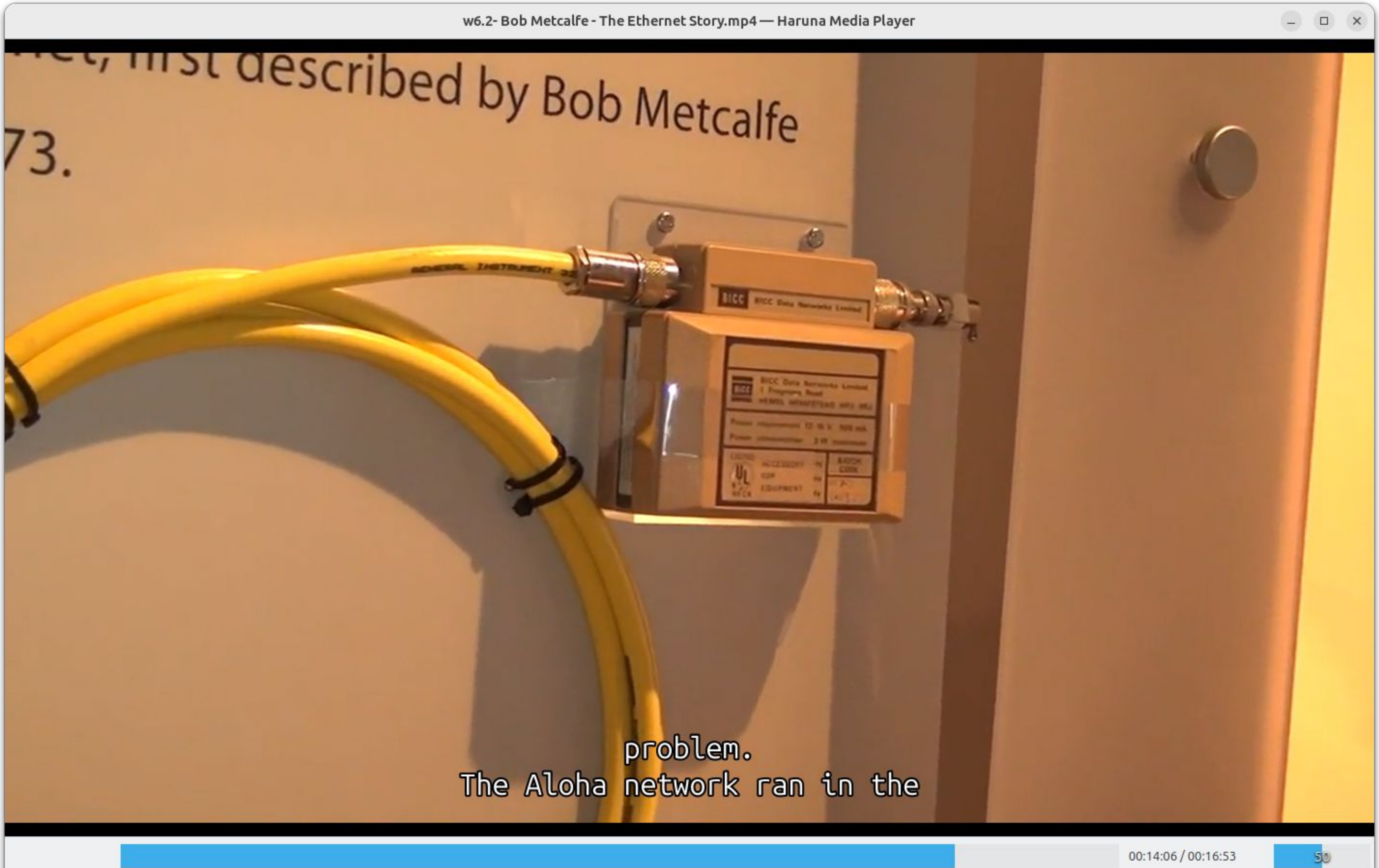
- **The "Flag Day":** The transition to TCP/IP was finalized around 1983.
- **OS Integration:** TCP/IP was baked into Unix (BSD 4.2) and adopted by Sun Microsystems. This pushed the technology into the academic and workstation market.
- **NSFNet:** As the old 50kbps ARPANET backbone became a bottleneck, the National Science Foundation stepped in to build a higher-speed backbone, paving the way for the modern web.

w6.2- Bob Metcalfe - The Ethernet Story


w6.2- Bob Metcalfe - The Ethernet Story.mp4 — Haruna Media Player
Subtitle scale: 0.3
Bob Metcalfe
University of Texas Austin
to be at the Xerox Research, Xerox Palo
Alto Research Center when a, a problem
00:00:28 / 00:16:53
60


w6.2- Bob Metcalfe - The Ethernet Story.mp4 — Haruna Media Player
CSMA/CD - Carrier Sense Multiple Access
with Collision Detection
plenty of cable to waste.
So we talk about carrier sense inclusion
00:10:23 / 00:16:53
50


w6.2- Bob Metcalfe - The Ethernet Story.mp4 — Haruna Media Player
Subtitle scale: 0.3
Tat Lam designed the passive electronic components to minimize impedance from each Ethernet tap
Who was even more hardware than David.
Who was the picofarad guy.
00:12:19 / 00:16:53
50


w6.2- Bob Metcalfe - The Ethernet Story.mp4 — Haruna Media Player
described by Bob Metcalfe
problem.
The Aloha network ran in the
00:14:06 / 00:16:53
50

Summary

🚀 The Genesis of Ethernet: Logic-Sync Summary

1. The Problem: The "Rat's Nest"

In 1973, Xerox PARC faced a Magnitude 1,000,000 challenge: a building full of PCs that needed to talk to the world's first laser printer (named **EARS**).

- **The Constraint:** Existing tech was slow (200 bps) and required "home run" wiring—a separate wire from every desk to a central point, creating a physical "rat's nest."
- **The Requirement:** The laser printer needed **20 Mbps** to stay busy.

2. The Inspiration: Aloha Net

Metcalfe pivoted from traditional designs after studying the **Aloha Net** (University of Hawaii). It solved the "distributed coordination" problem:

- **Randomized Retransmission:** If two terminals talk at once (a collision), they wait a random amount of time before trying again. This prevents them from "looping" into constant collisions.

3. The Ethernet Innovation (Hardware & Logic)

Metcalfe and David Boggs evolved the Aloha concept into what we now know as Ethernet.

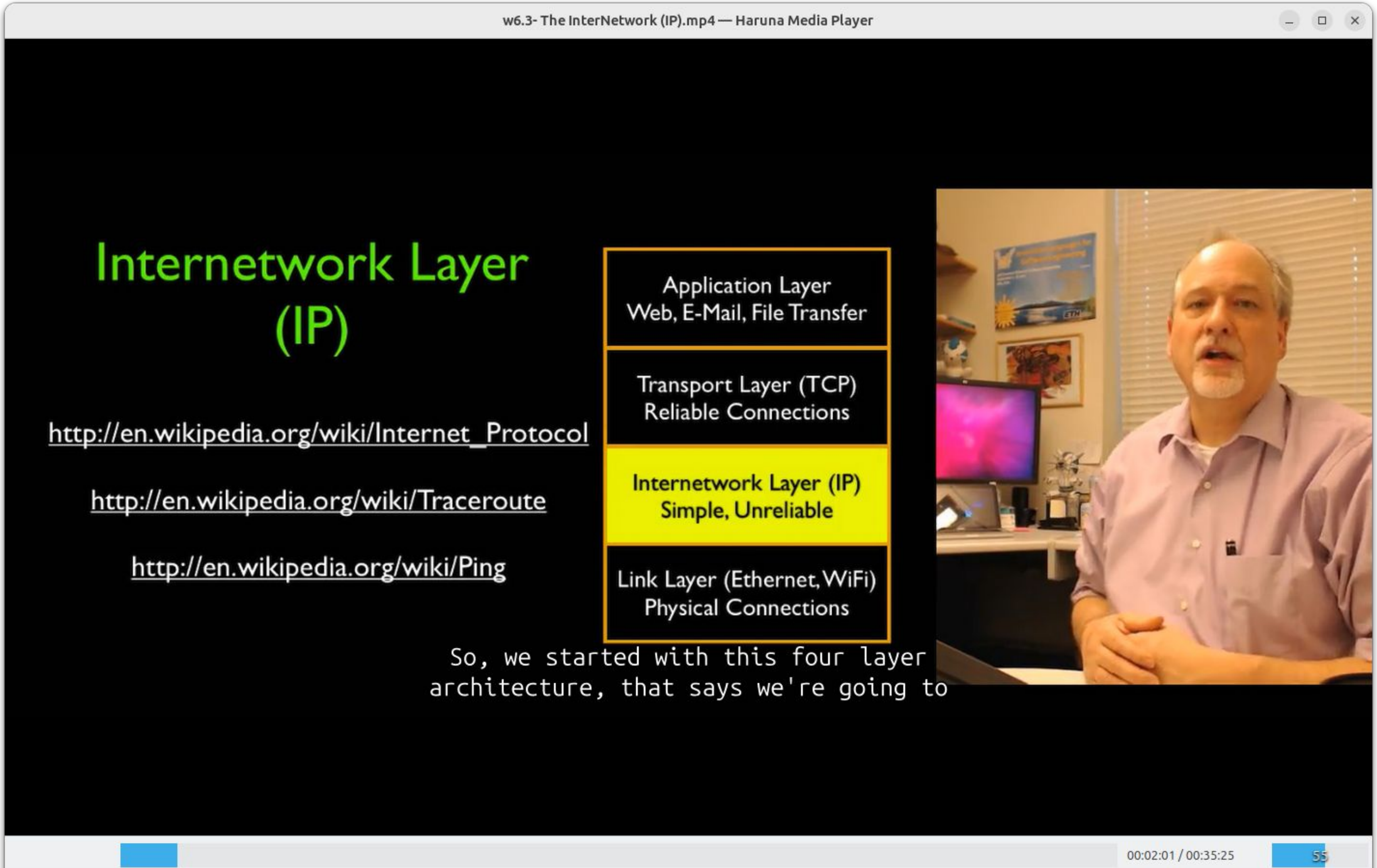
- **The Vampire Tap:** Borrowed from the cable TV industry, this allowed users to "stab" into a single coaxial cable running down a hallway without breaking the circuit or shutting down the network.
- **Manchester Encoding:** A simple digital modulation where each bit has a transition in the middle. This allowed the hardware to detect if someone else was transmitting (Carrier Sense).
- **CSMA/CD:** Carrier Sense Multiple Access with Collision Detection. Unlike Aloha Net, Ethernet could "listen" and give up immediately if a collision occurred, saving bandwidth.

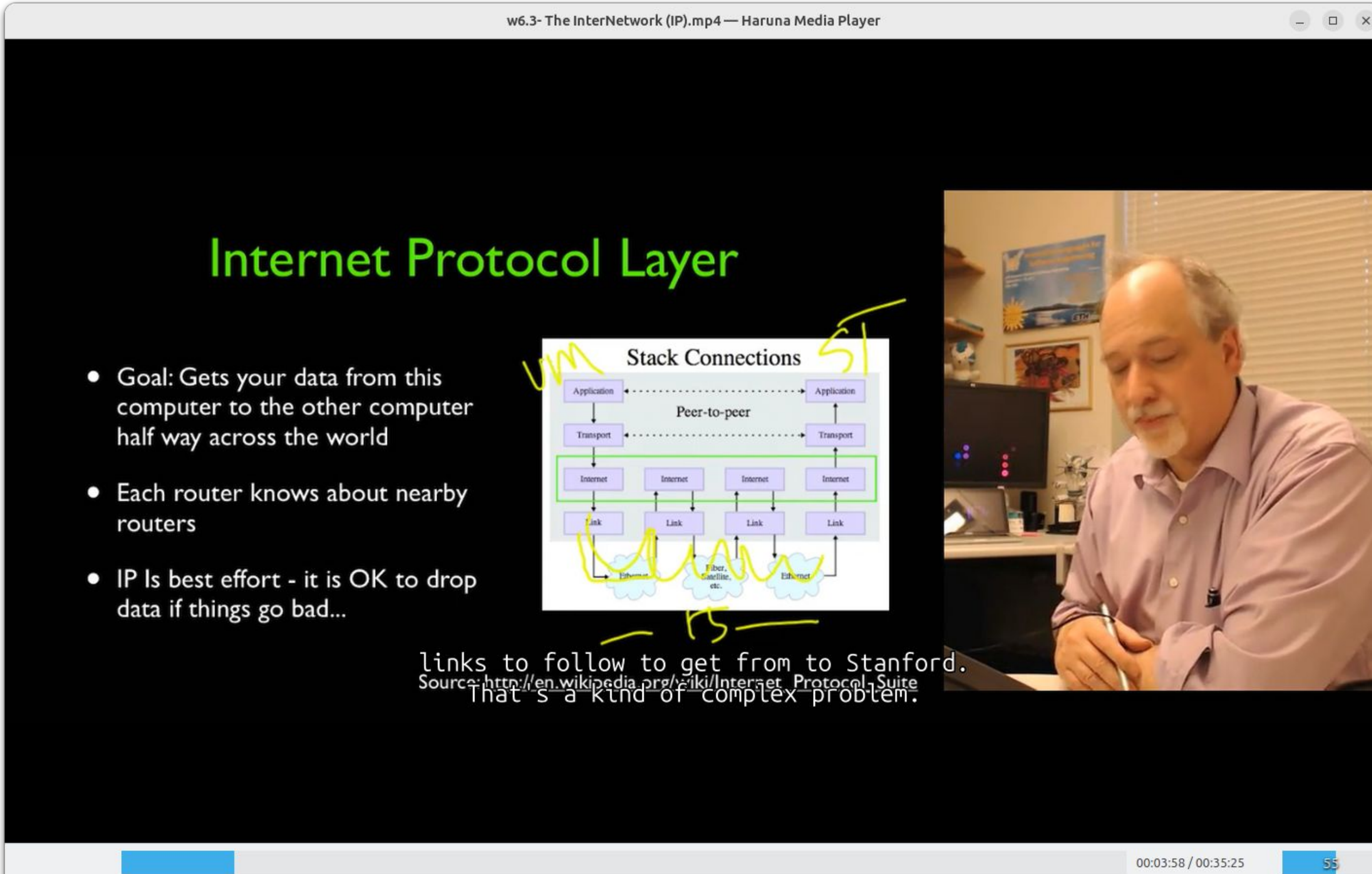
4. Evolutionary Scaling

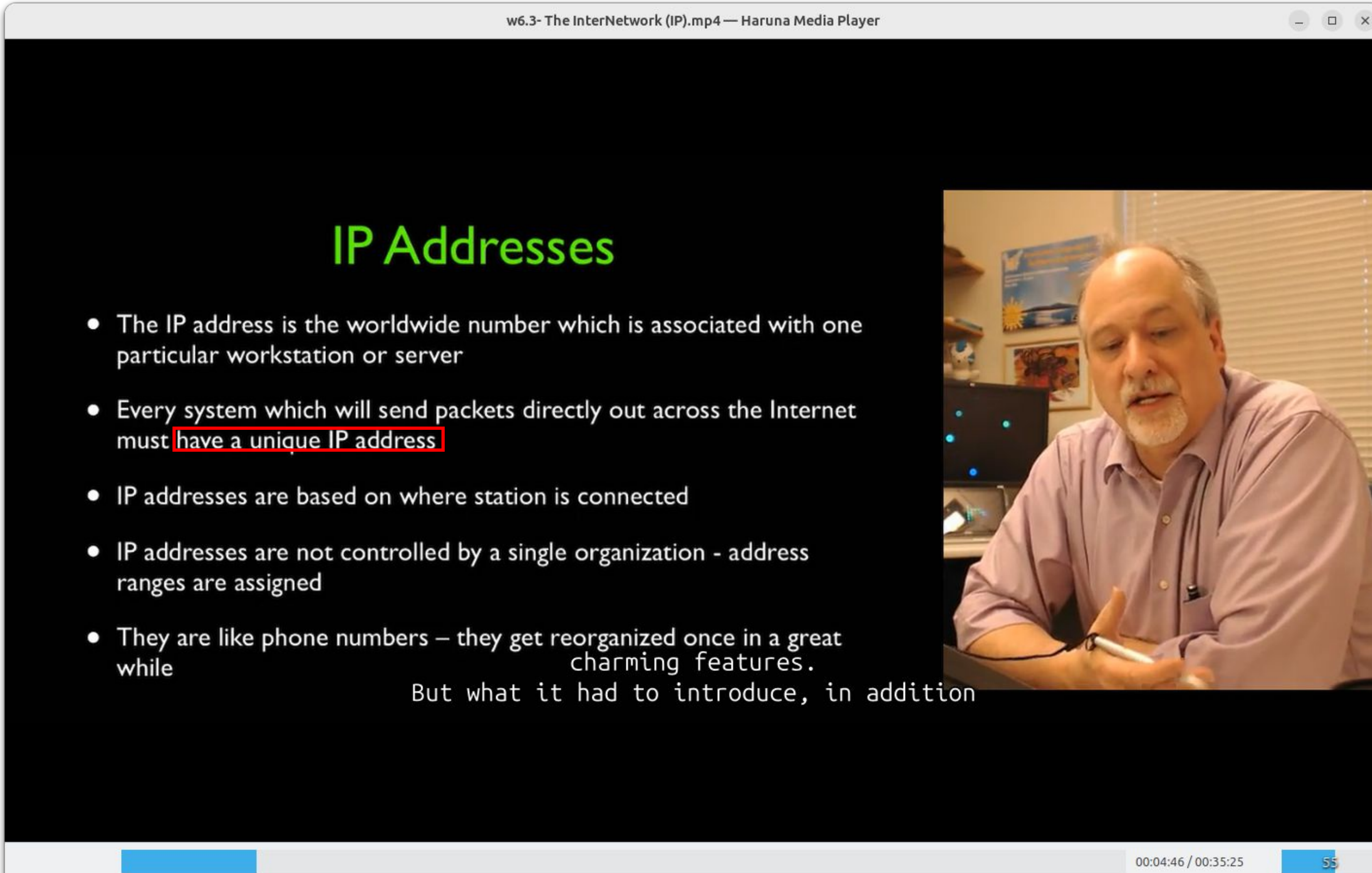
Ethernet didn't just stay at the PARC; it scaled across decades:

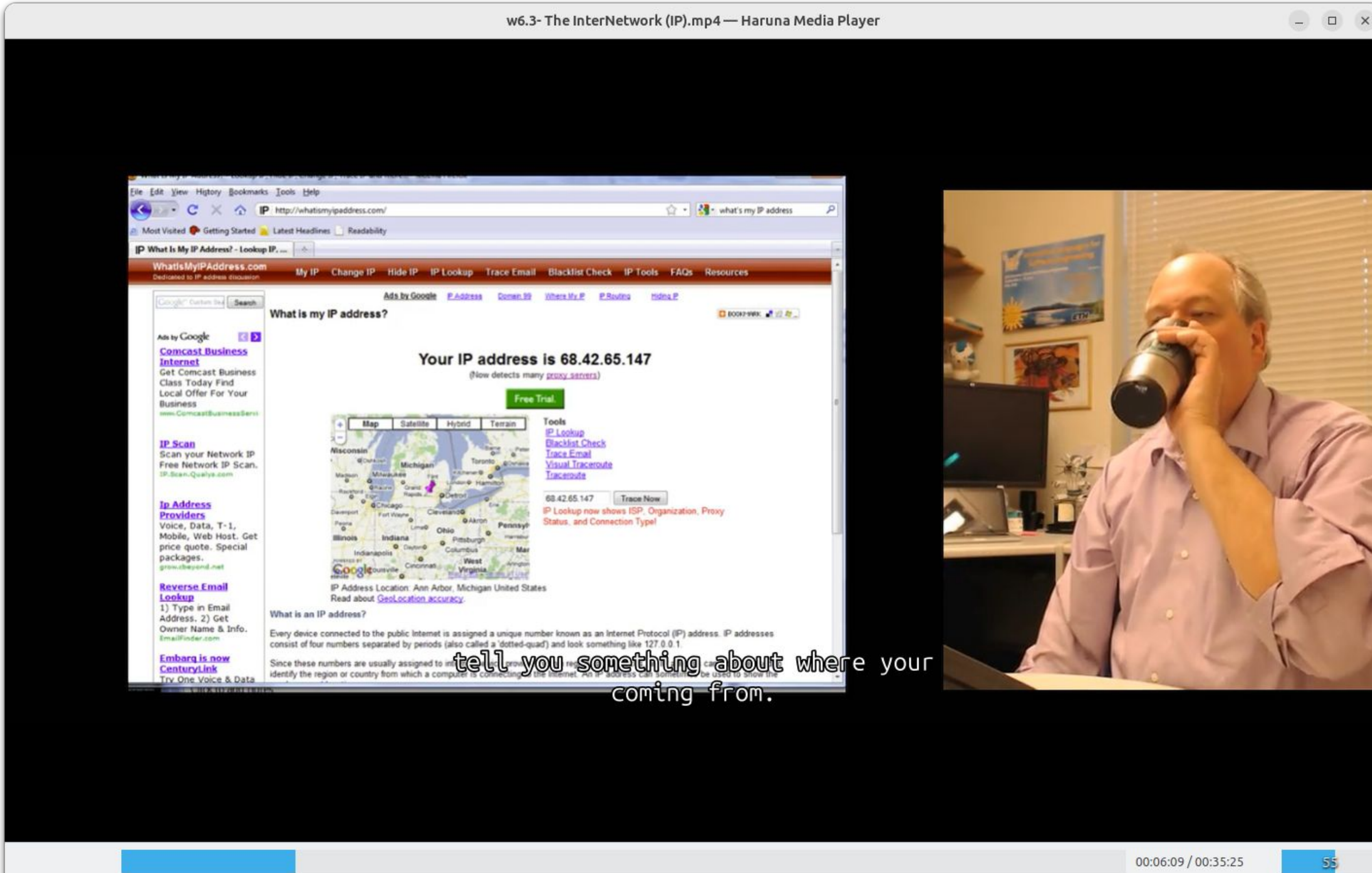
- **2.94 Mbps:** The original PARC speed.
- **10 Mbps:** The standardized speed (Logic-Sync with DEC and Intel).
- **100 Mbps (Fast Ethernet):** Metcalfe's company, Grand Junction, achieved this by shrinking the "network diameter" from 1,000 meters to 100 meters (moving toward hubs).
- **Today & Beyond:** We've moved from $\boxed{\text{10G to 100G}}$, and Metcalfe is already eyeing **Terabit Ethernet**.

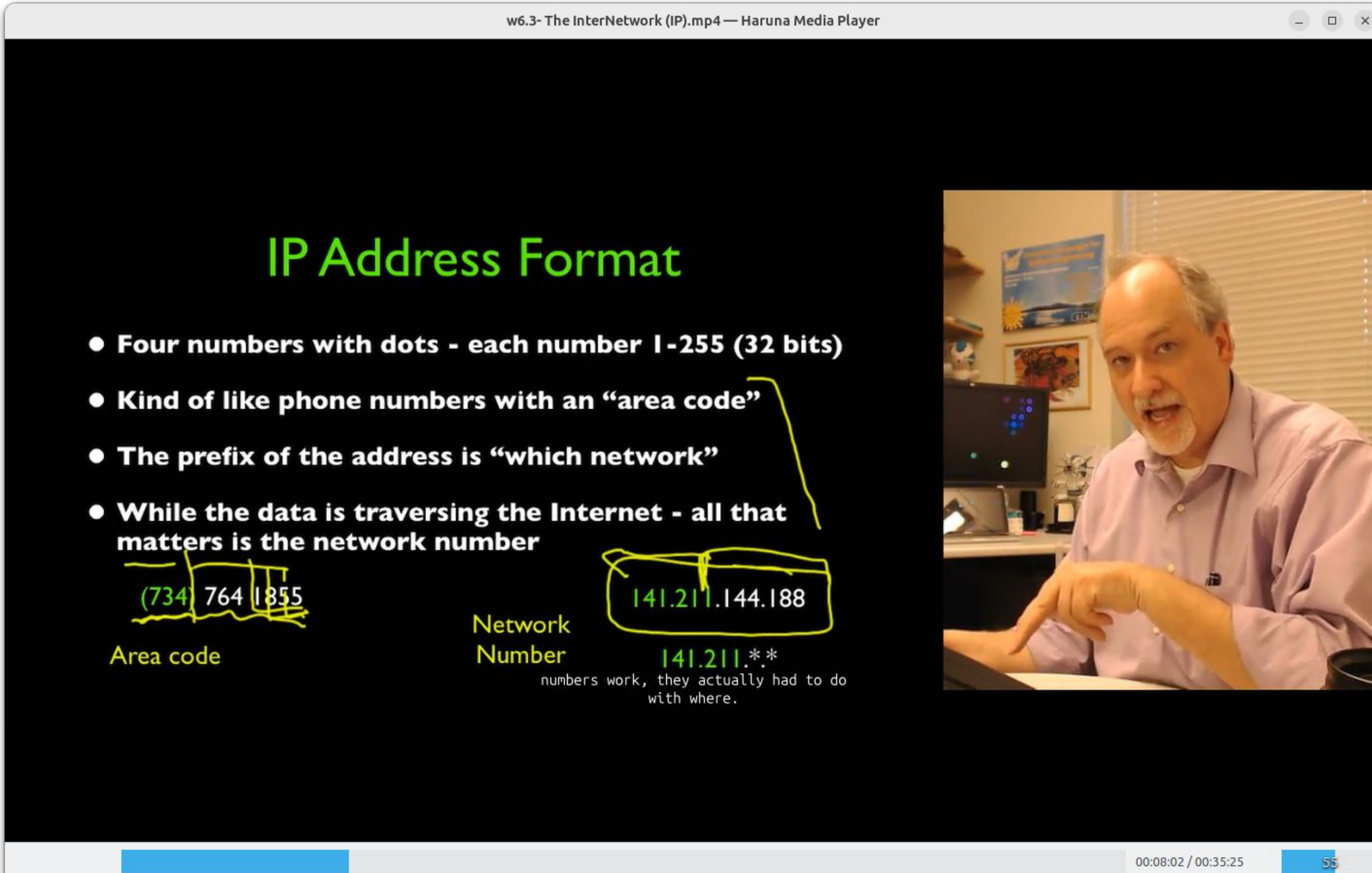
w6.3- The InterNetwork (IP)

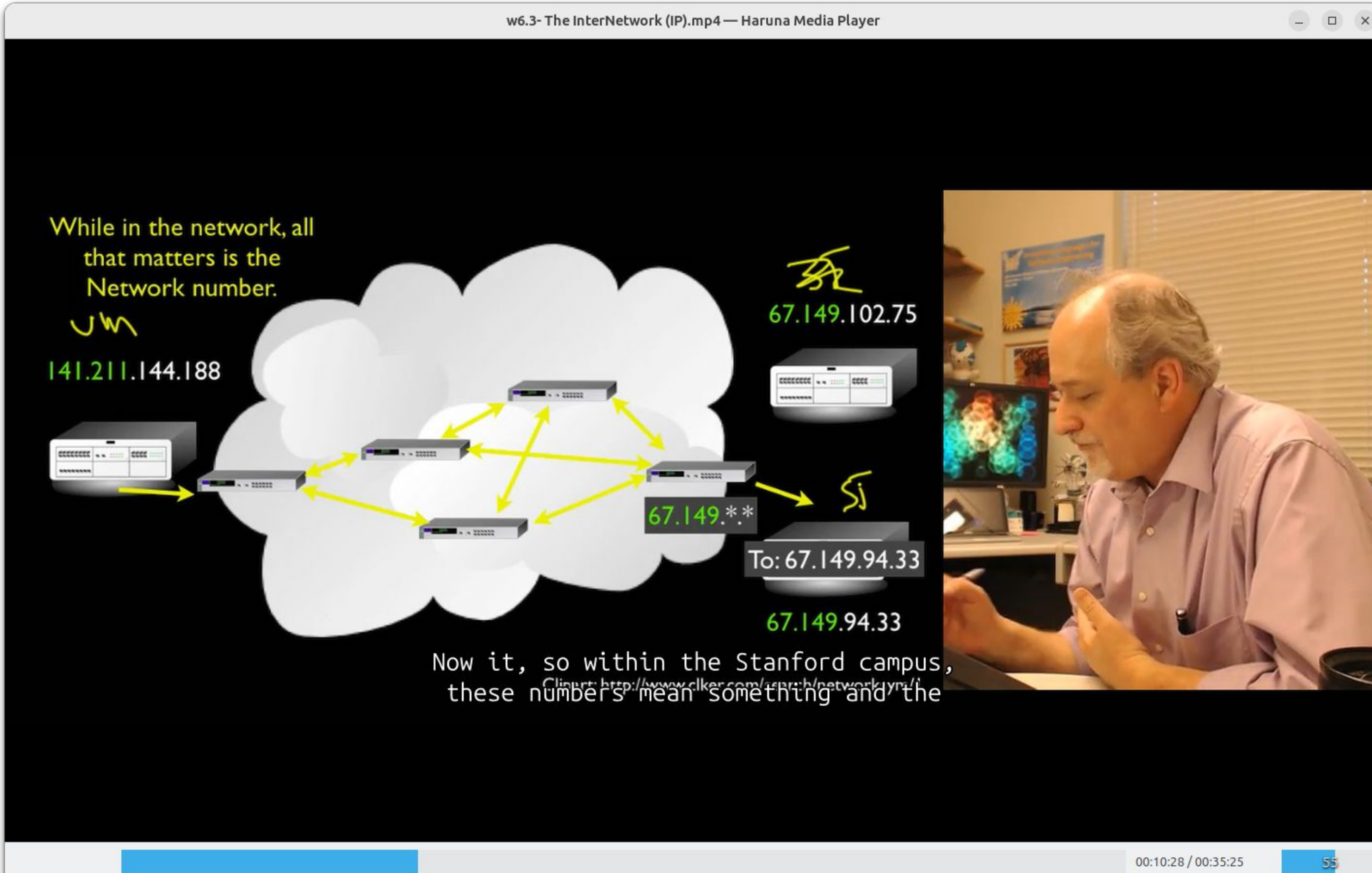

w6.3- The InterNetwork (IP).mp4 — Haruna Media Player
Internetwork Layer
(IP)
http://en.wikipedia.org/wiki/Internet_Protocol
http://en.wikipedia.org/wiki/Traceroute
http://en.wikipedia.org/wiki/Ping
Application Layer
Web, E-Mail, File Transfer
Transport Layer (TCP)
Reliable Connections
Internetwork Layer (IP)
Simple, Unreliable
Link Layer (Ethernet, WiFi)
Physical Connections
So, we started with this four layer
architecture, that says we're going to
00:02:01 / 00:35:25

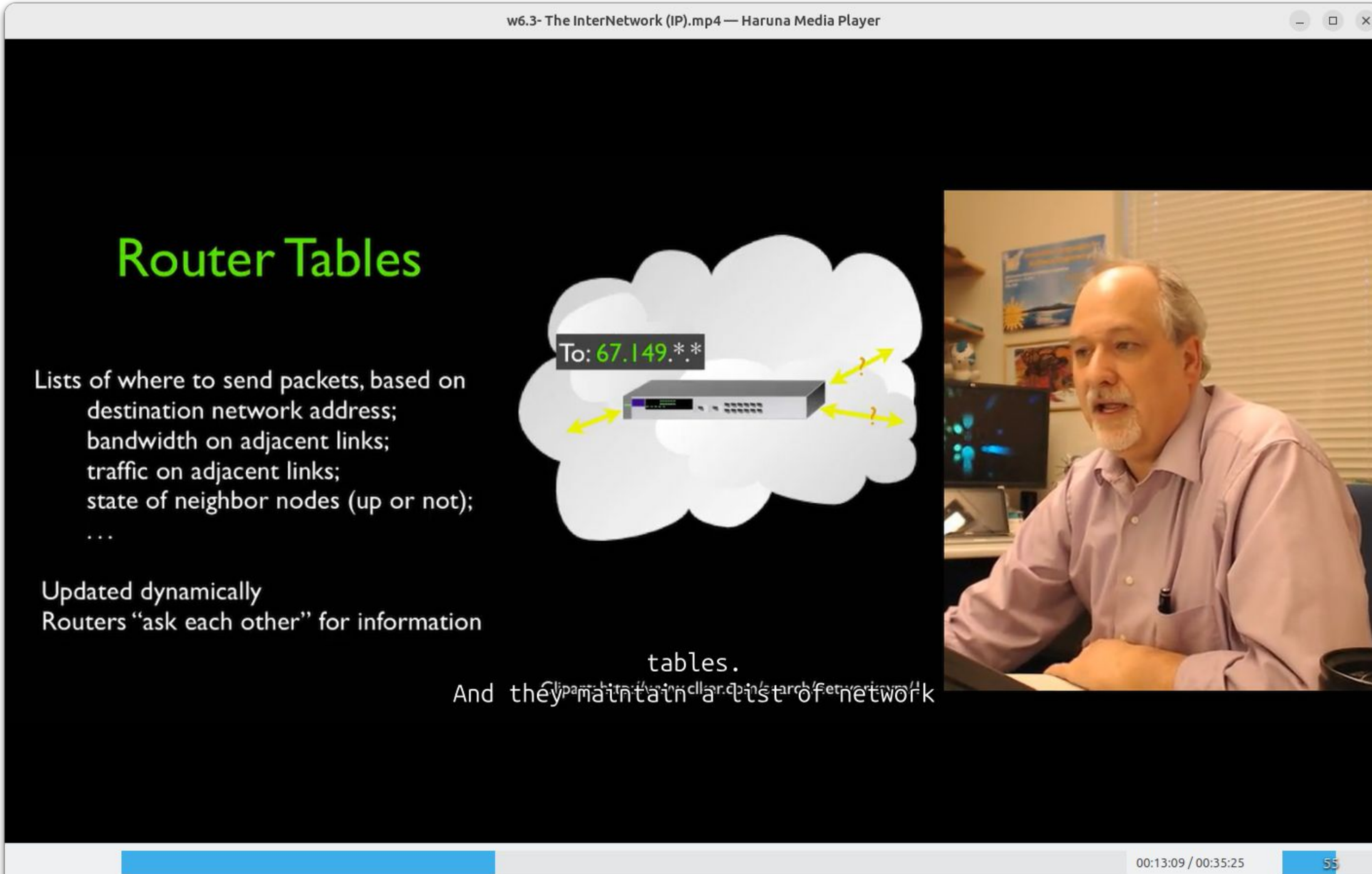

w6.3- The InterNetwork (IP).mp4 — Haruna Media Player
Internet Protocol Layer
Goal: Gets your data from this computer to the other computer half way across the world
Each router knows about nearby routers
IP Is best effort - it is OK to drop data if things go bad...
Stack Connections
Application
Application
Peer-to-peer
Transport
Transport
Internet
Internet
Internet
Internet
Link
Link
Link
Link
Ethernet
Fiber, Satellite, etc.
Ethernet
UM
ST
FS
links to follow to get from to Stanford.
Source: http://en.wikipedia.org/wiki/Internet_Protocol_Suite
That's a kind of complex problem.
00:03:58 / 00:35:25

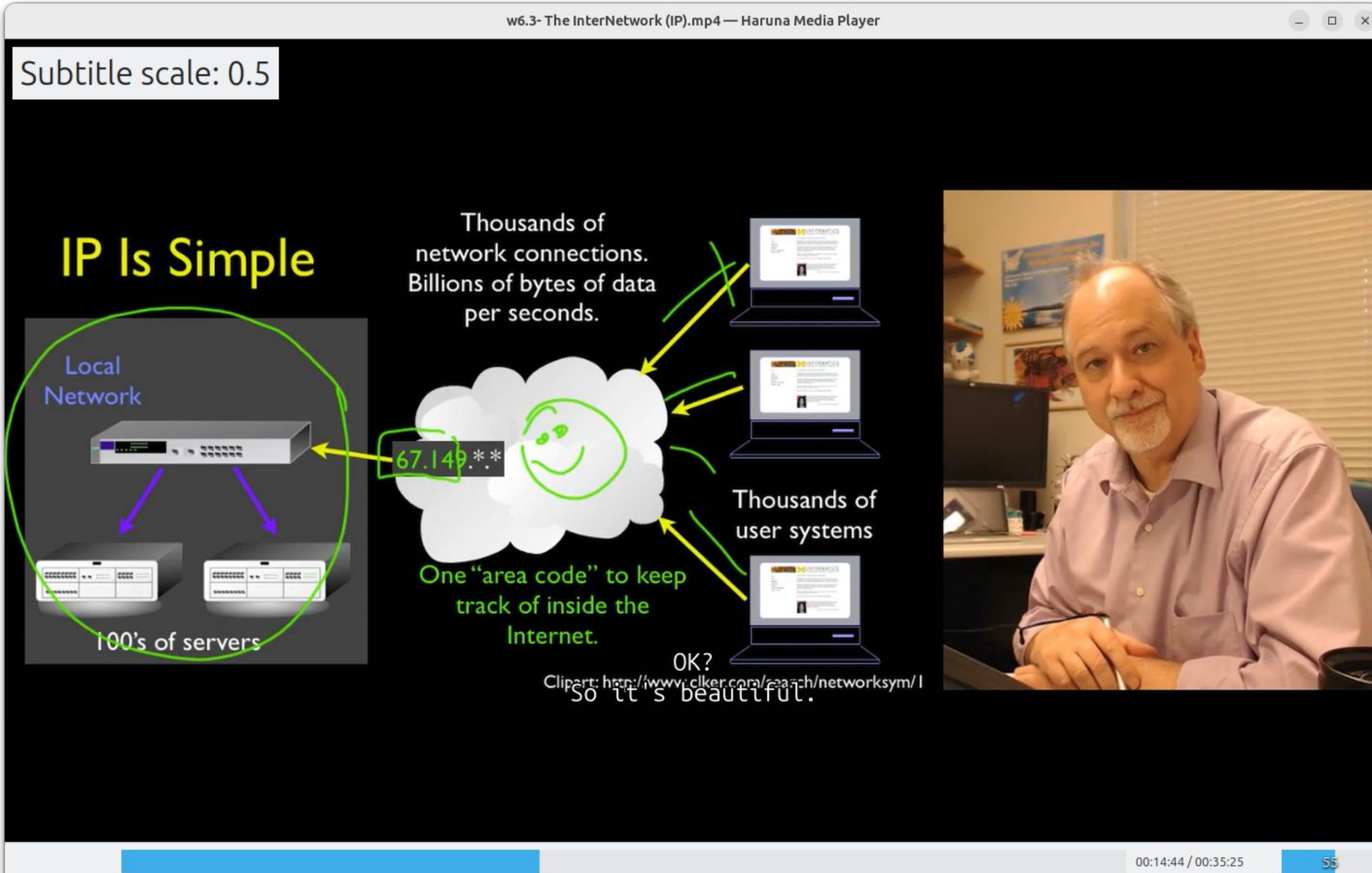

w6.3- The InterNetwork (IP).mp4 — Haruna Media Player
IP Addresses
The IP address is the worldwide number which is associated with one particular workstation or server
Every system which will send packets directly out across the Internet must have a unique IP address
IP addresses are based on where station is connected
IP addresses are not controlled by a single organization - address ranges are assigned
They are like phone numbers – they get reorganized once in a great while
charming features.
But what it had to introduce, in addition
00:04:46 / 00:35:25

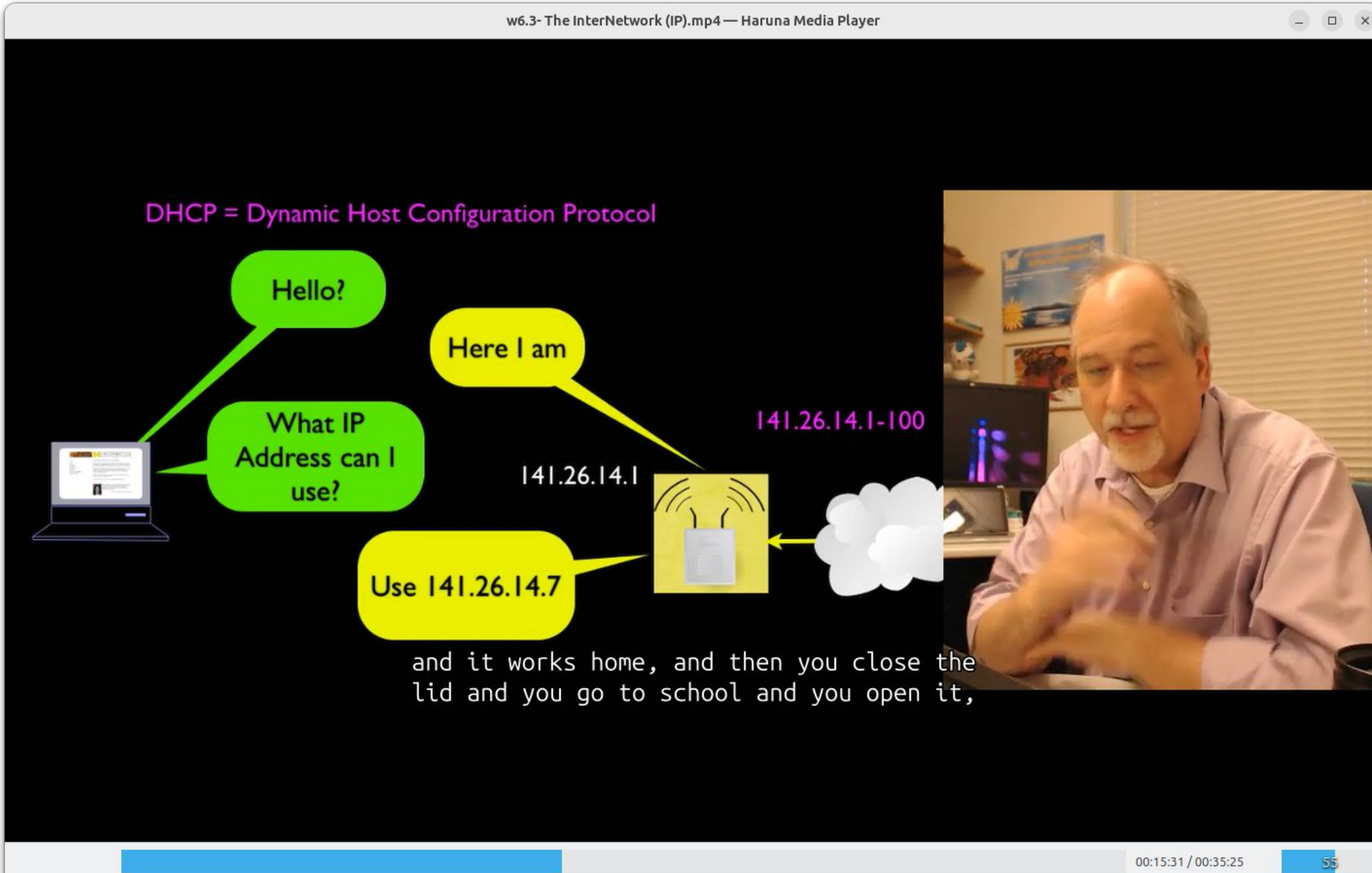

w6.3- The InterNetwork (IP).mp4 — Haruna Media Player
What is my IP address?
Your IP address is 68.42.65.147
(Now detects many proxy servers)
Free Trial
IP Address Location: Ann Arbor, Michigan United States
What is an IP address?
Every device connected to the public Internet is assigned a unique number known as an Internet Protocol (IP) address. IP addresses consist of four numbers separated by periods (also called a 'dotted-quad') and look something like 127.0.0.1.
tell you something about where your
coming from.
00:06:09 / 00:35:25

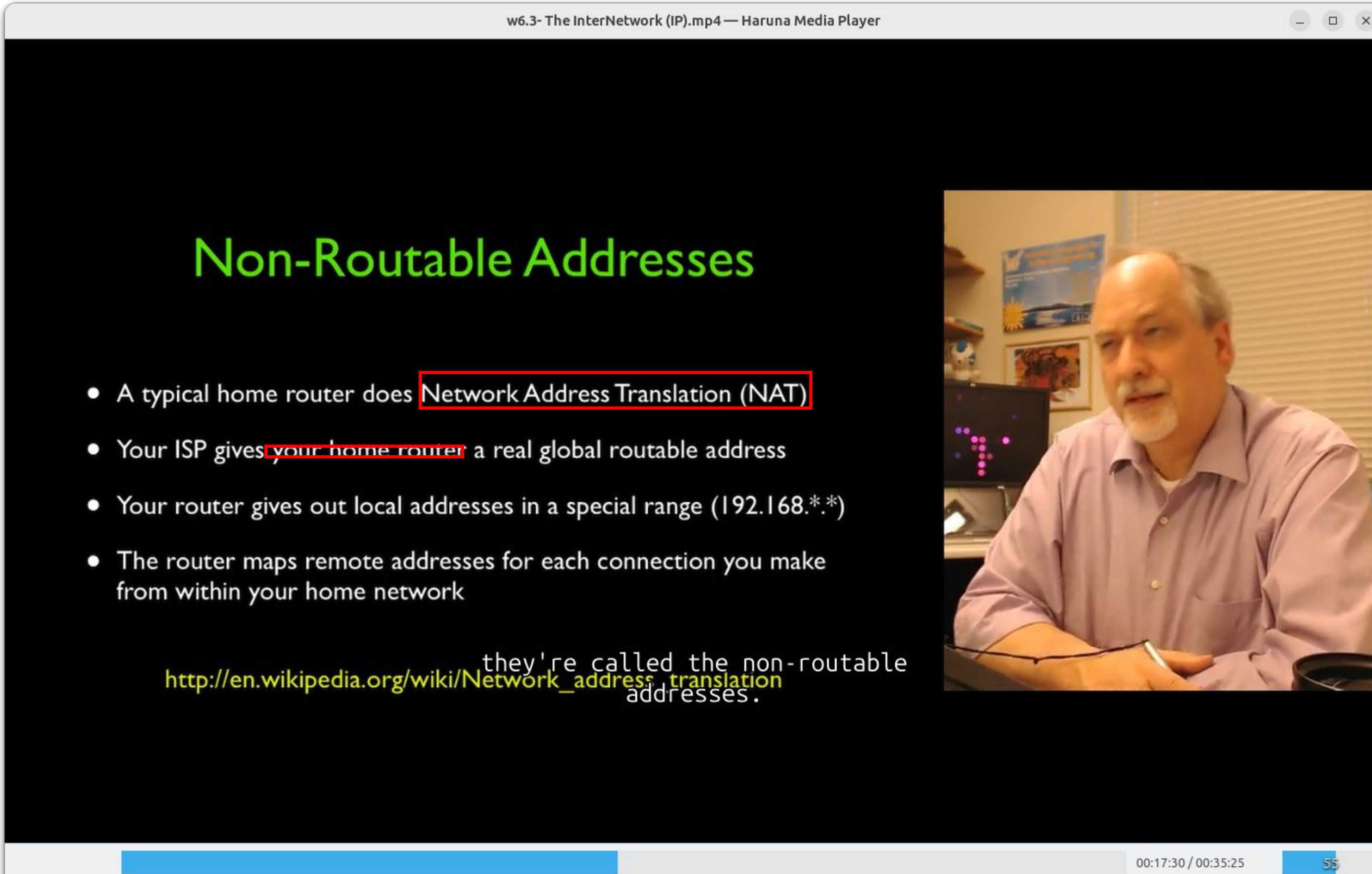

w6.3- The InterNetwork (IP).mp4 — Haruna Media Player
IP Address Format
Four numbers with dots - each number 1-255 (32 bits)
Kind of like phone numbers with an "area code"
The prefix of the address is "which network"
While the data is traversing the Internet - all that matters is the network number
(734) 764 1855
Area code
Network Number
141.211.144.188
141.211.*.*
numbers work, they actually had to do with where.
00:08:02 / 00:35:25

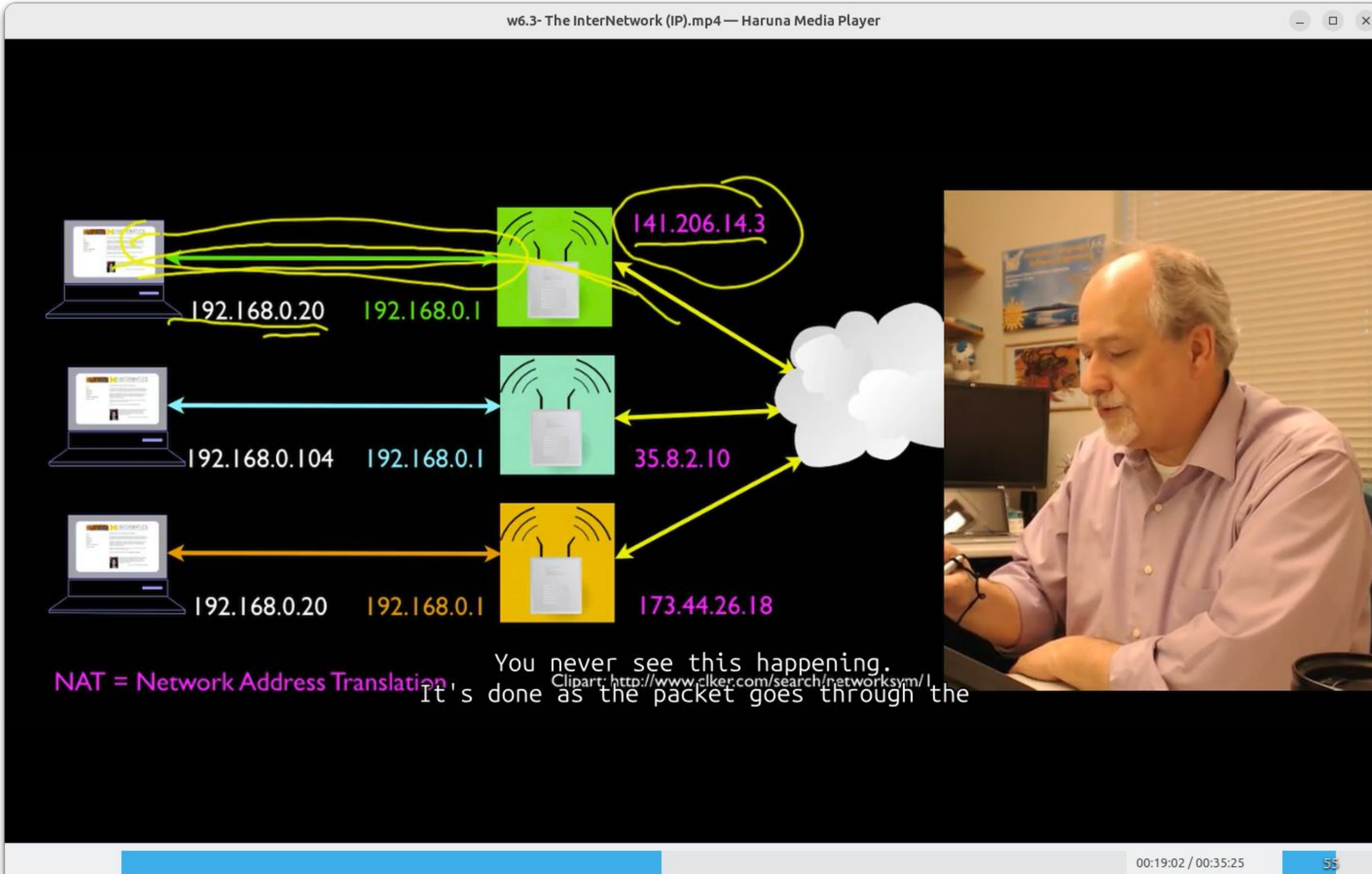

w6.3- The InterNetwork (IP).mp4 — Haruna Media Player
While in the network, all that matters is the Network number.
141.211.144.188
67.149.102.75
67.149.*.*
To: 67.149.94.33
67.149.94.33
Now it, so within the Stanford campus,
these numbers mean something and the
00:10:28 / 00:35:25


w6.3- The InterNetwork (IP).mp4 — Haruna Media Player
Router Tables
Lists of where to send packets, based on
destination network address;
bandwidth on adjacent links;
traffic on adjacent links;
state of neighbor nodes (up or not);
. . .
Updated dynamically
Routers "ask each other" for information
To: 67.149.*.*
tables.
And they maintain a list of network
00:13:09 / 00:35:25


w6.3- The InterNetwork (IP).mp4 — Haruna Media Player
Subtitle scale: 0.5
IP Is Simple
Local
Network
100's of servers
67.149.*.*
Thousands of
network connections.
Billions of bytes of data
per seconds.
Thousands of
user systems
One "area code" to keep
track of inside the
Internet.
OK?
So it's beautiful.
00:14:44 / 00:35:25
55


w6.3- The InterNetwork (IP).mp4 — Haruna Media Player
DHCP = Dynamic Host Configuration Protocol
Hello?
Here I am
What IP Address can I use?
141.26.14.1-100
141.26.14.1
Use 141.26.14.7
and it works home, and then you close the
lid and you go to school and you open it,
00:15:31 / 00:35:25


w6.3- The InterNetwork (IP).mp4 — Haruna Media Player
Non-Routable Addresses
A typical home router does Network Address Translation (NAT)
Your ISP gives ~~your home router~~ a real global routable address
Your router gives out local addresses in a special range (192.168.*.*)
The router maps remote addresses for each connection you make from within your home network
http://en.wikipedia.org/wiki/Network_address_translation
they're called the non-routable addresses.
00:17:30 / 00:35:25


w6.3- The InterNetwork (IP).mp4 — Haruna Media Player
141.206.14.3
192.168.0.20
192.168.0.1
192.168.0.104
192.168.0.1
35.8.2.10
192.168.0.20
192.168.0.1
173.44.26.18
NAT = Network Address Translation
Clipart: http://www.clker.com/search/networksym/1
You never see this happening.
It's done as the packet goes through the
00:19:02 / 00:35:25

The Three Components of NAT

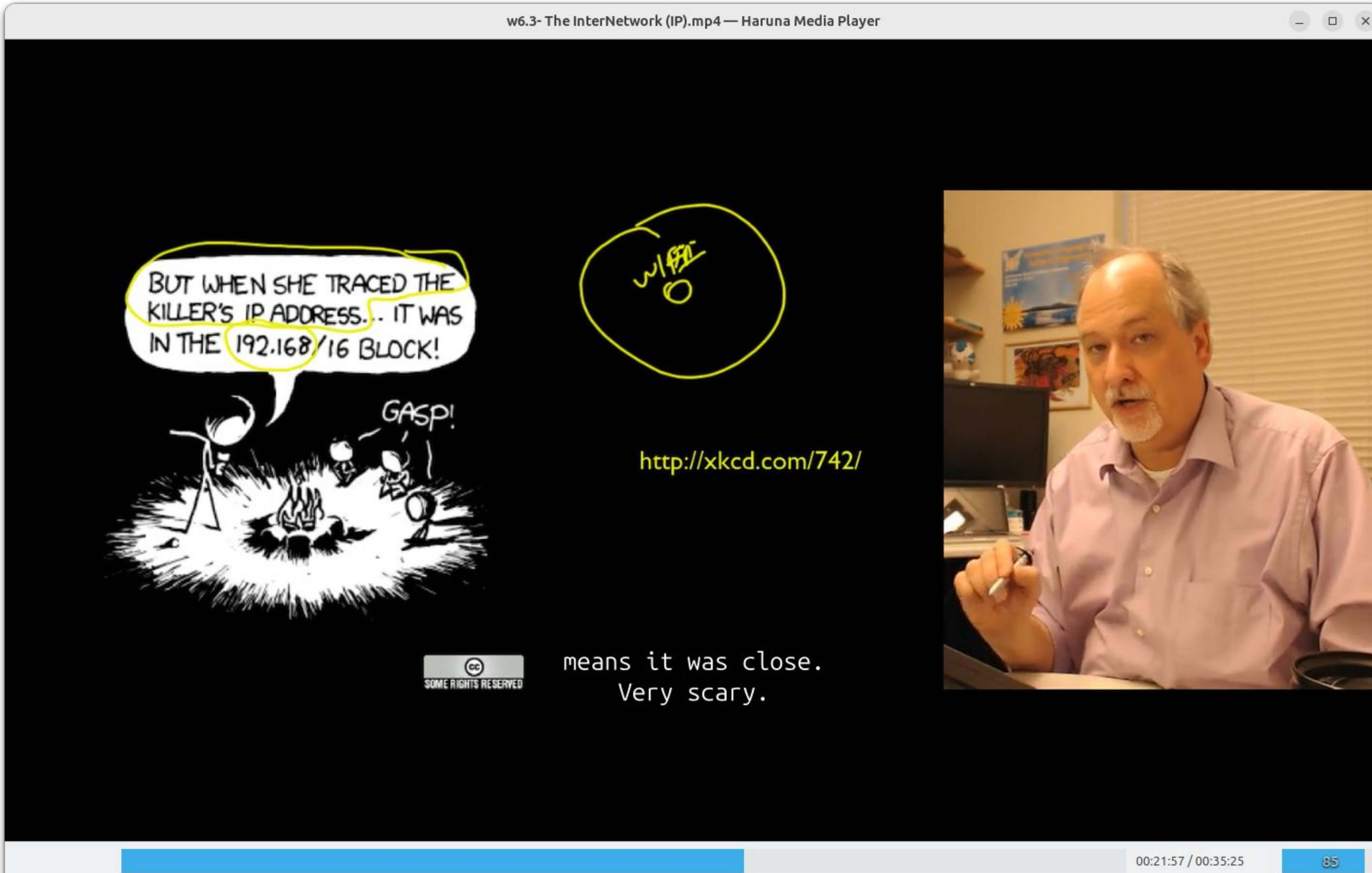
Based on the diagram, we can see how an IP address changes as it moves through a router:

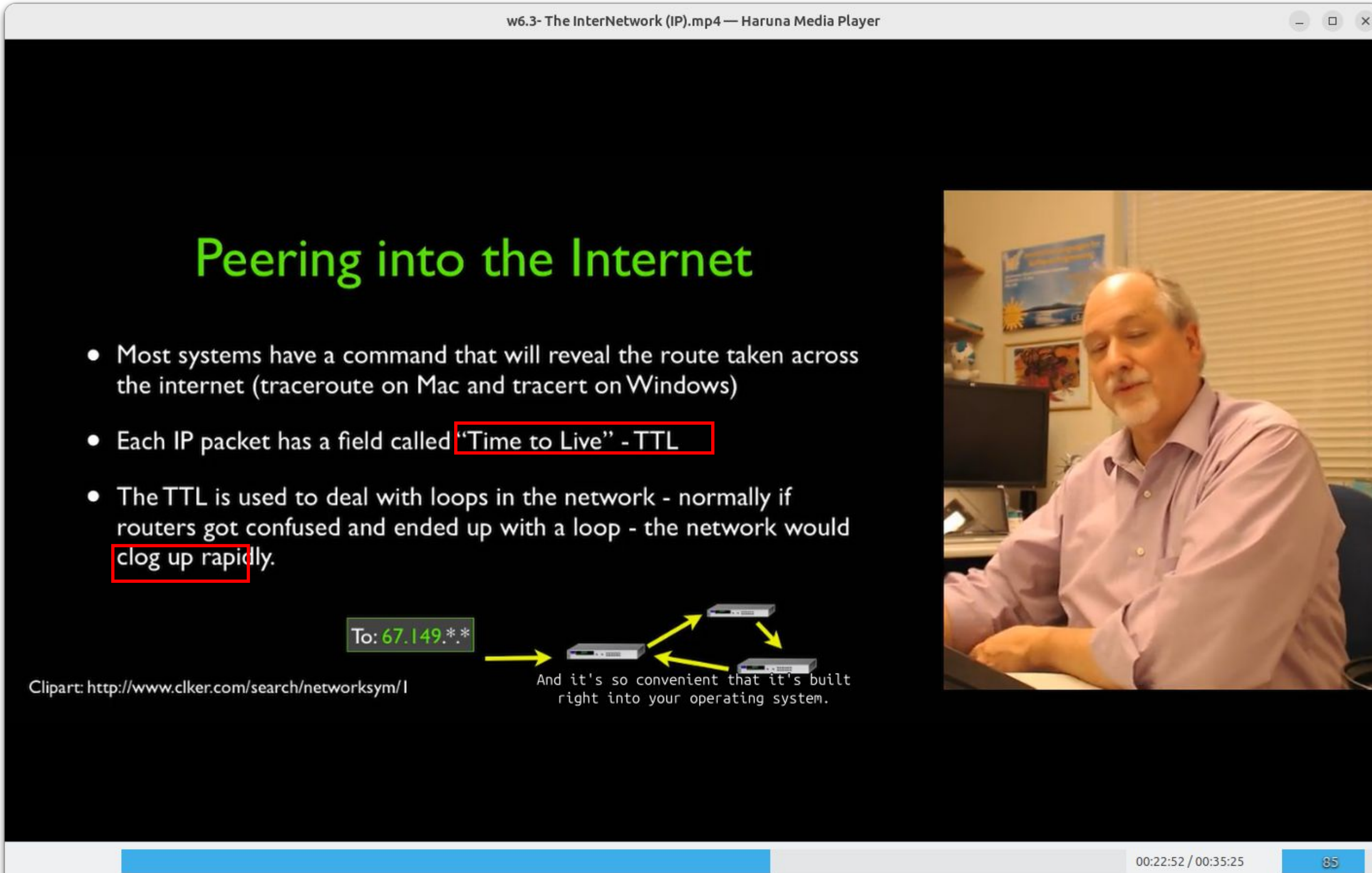
- **Private IP Address (私有 IP 地址):** The numbers on the left (e.g., `192.168.0.20`) are used inside a local network. These are "private" because millions of homes use these exact same numbers; they are not unique globally.
- **Gateway IP (网关):** The green numbers in the middle (`192.168.0.1`) represent your router's internal face. It acts as the door between your "Sanctuary" and the outside world.
- **Public IP Address (公网 IP 地址):** The pink numbers on the right (e.g., `141.206.14.3`) are your "public face." This is the unique address the rest of the world sees when you send data to the cloud.

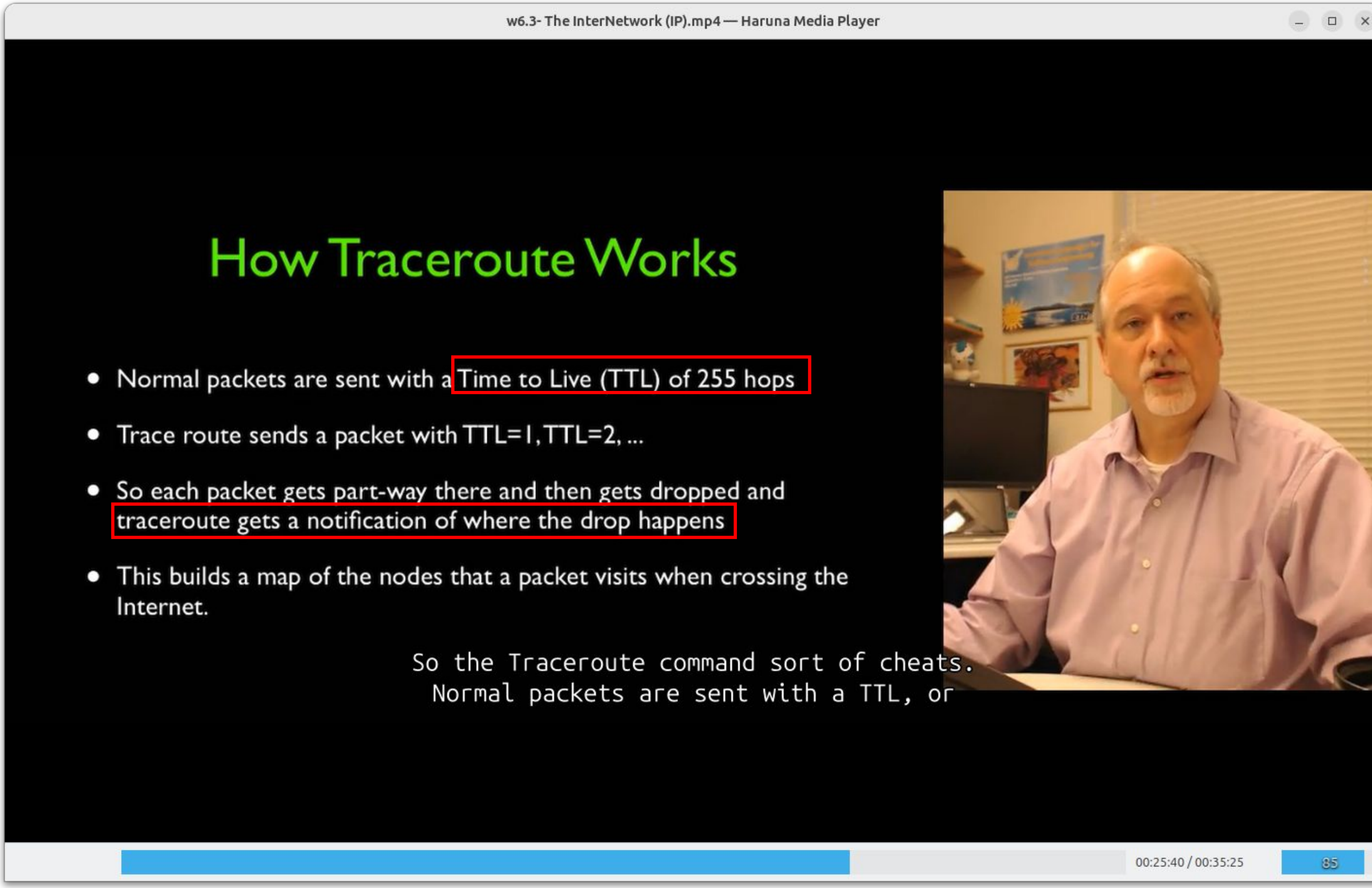
How the "Magic" Happens

The yellow circles and lines in the image show a packet's journey:

1. **Request:** Your laptop (`192.168.0.20`) sends a request to a website.
2. **The Swap:** When the packet hits the router, the router strips off your private "return address" and replaces it with its own public address (`141.206.14.3`).
3. **The Table:** The router keeps a secret "NAT Table" that remembers: *"Laptop .20 asked for this website info."*
4. **The Return:** When the website sends data back to the public IP, the router checks its table and "translates" the address back to `.20` so the right device gets the info.


w6.3- The InterNetwork (IP).mp4 — Haruna Media Player
BUT WHEN SHE TRACED THE KILLER'S IP ADDRESS... IT WAS IN THE 192.168/16 BLOCK!
GASP!
SOME RIGHTS RESERVED
http://xkcd.com/742/
means it was close.
Very scary.
00:21:57 / 00:35:25
85


w6.3- The InterNetwork (IP).mp4 — Haruna Media Player
Peering into the Internet
Most systems have a command that will reveal the route taken across the internet (traceroute on Mac and tracert on Windows)
Each IP packet has a field called "Time to Live" - TTL
The TTL is used to deal with loops in the network - normally if routers got confused and ended up with a loop - the network would clog up rapidly.
To: 67.149.*.*
Clipart: http://www.clker.com/search/networksym/1
And it's so convenient that it's built right into your operating system.
00:22:52 / 00:35:25
85


w6.3- The InterNetwork (IP).mp4 — Haruna Media Player
How Traceroute Works
Normal packets are sent with a Time to Live (TTL) of 255 hops
Trace route sends a packet with TTL=1, TTL=2, ...
So each packet gets part-way there and then gets dropped and traceroute gets a notification of where the drop happens
This builds a map of the nodes that a packet visits when crossing the Internet.
So the Traceroute command sort of cheats.
Normal packets are sent with a TTL, or
00:25:40 / 00:35:25
85

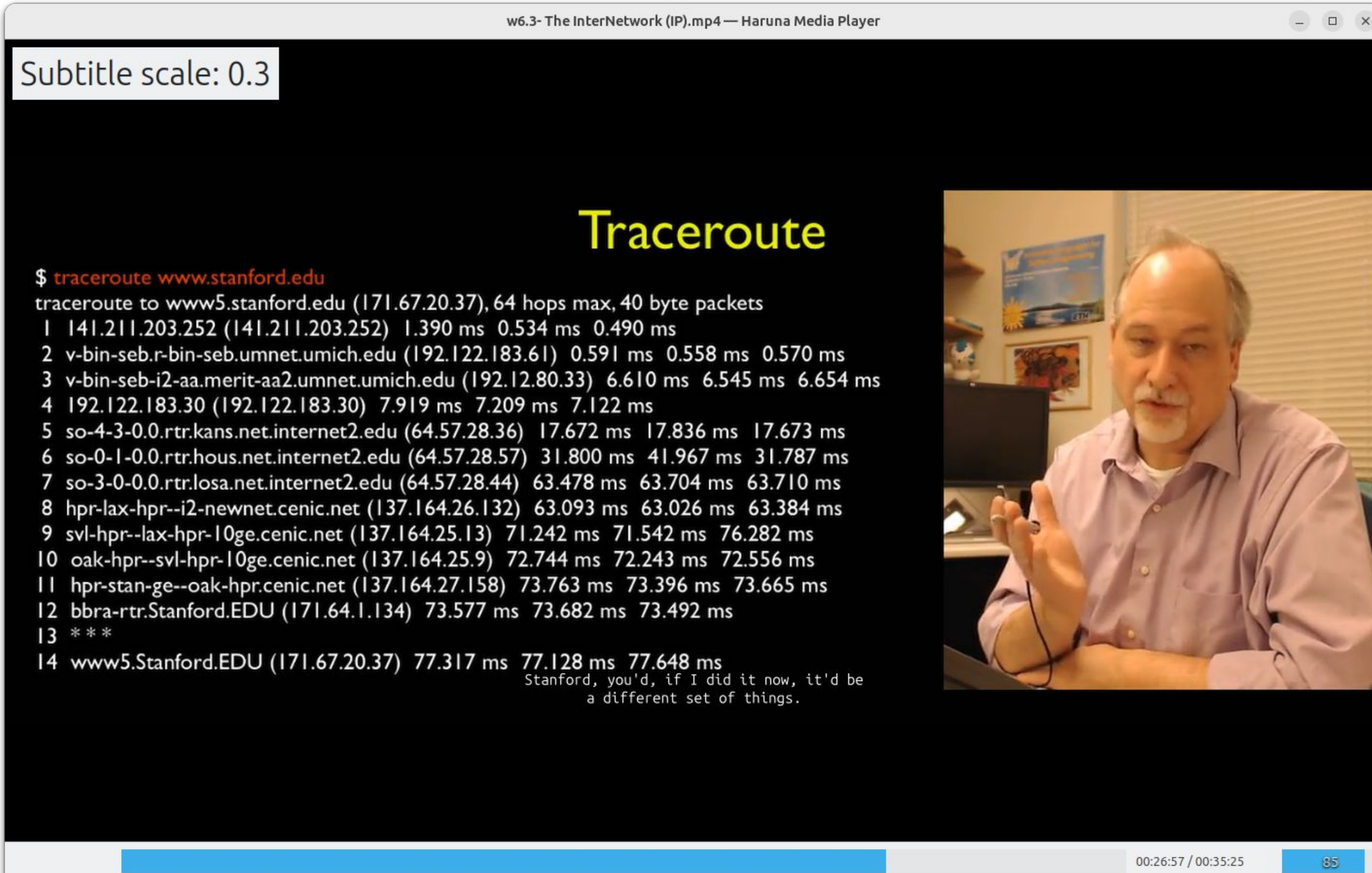
Traceroute is a diagnostic tool used to track the path a data packet takes from your computer to a destination IP address or website. It reveals every "hop" (router) the data passes through along the way.

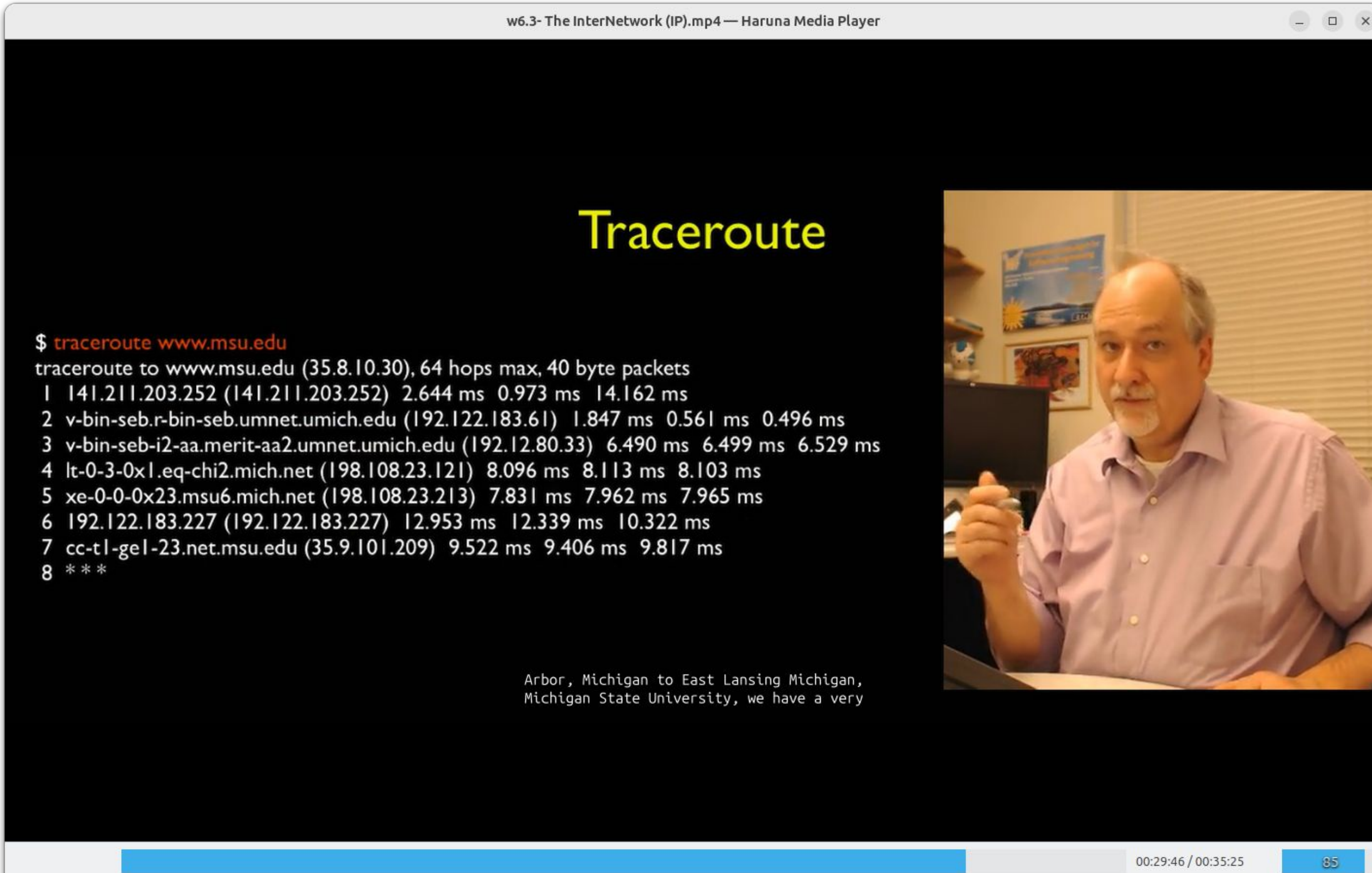
Think of it as a GPS log for your internet traffic as it leaves your **Aachen-Sanctuary**.

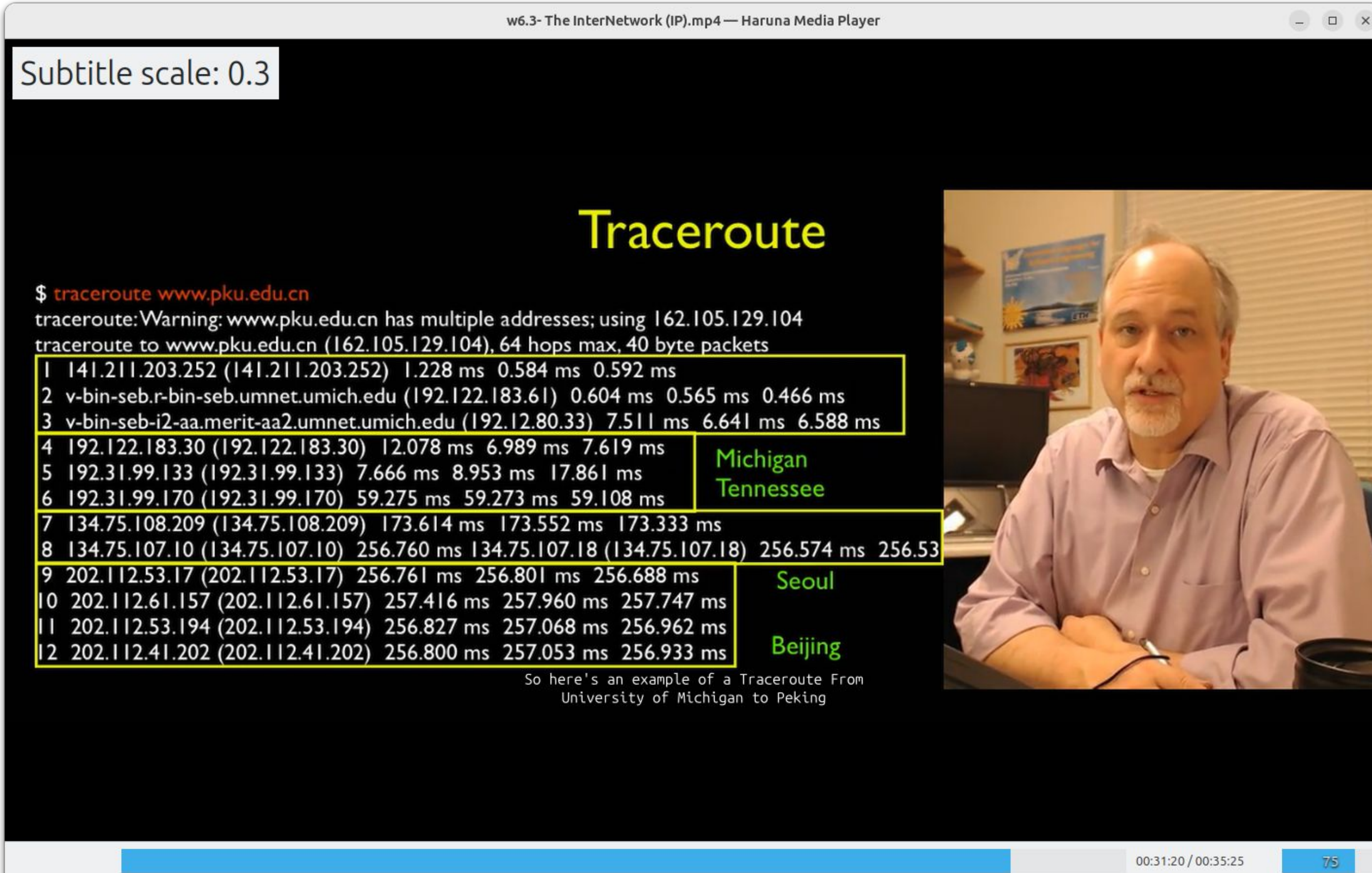
How it Works: The "TTL" Trick

Traceroute works by manipulating a field in the IP header called **Time To Live (TTL)** = **生存时间**.

1. **Hop 1:** Your computer sends a packet with **TTL = 1**. The first router it hits (your home router) drops the TTL to 0, discards the packet, and sends back an error message ("Time Exceeded"). Now you know the identity of the first router.
2. **Hop 2:** Your computer sends a packet with **TTL = 2**. It passes the first router, but the second router drops it to 0 and sends back an error. Now you have the second identity.
3. **Repeat:** This continues (TTL = 3, 4, 5...) until the packet finally reaches the destination.


w6.3- The InterNetwork (IP).mp4 — Haruna Media Player
Subtitle scale: 0.3
Traceroute
$ traceroute www.stanford.edu
traceroute to www5.stanford.edu (171.67.20.37), 64 hops max, 40 byte packets
1 141.211.203.252 (141.211.203.252) 1.390 ms 0.534 ms 0.490 ms
2 v-bin-seb.r-bin-seb.umnet.umich.edu (192.122.183.61) 0.591 ms 0.558 ms 0.570 ms
3 v-bin-seb-i2-aa.merit-aa2.umnet.umich.edu (192.12.80.33) 6.610 ms 6.545 ms 6.654 ms
4 192.122.183.30 (192.122.183.30) 7.919 ms 7.209 ms 7.122 ms
5 so-4-3-0.0.rtr.kans.net.internet2.edu (64.57.28.36) 17.672 ms 17.836 ms 17.673 ms
6 so-0-1-0.0.rtr.hous.net.internet2.edu (64.57.28.57) 31.800 ms 41.967 ms 31.787 ms
7 so-3-0-0.0.rtr.losa.net.internet2.edu (64.57.28.44) 63.478 ms 63.704 ms 63.710 ms
8 hpr-lax-hpr--i2-newnet.cenic.net (137.164.26.132) 63.093 ms 63.026 ms 63.384 ms
9 svl-hpr--lax-hpr-10ge.cenic.net (137.164.25.13) 71.242 ms 71.542 ms 76.282 ms
10 oak-hpr--svl-hpr-10ge.cenic.net (137.164.25.9) 72.744 ms 72.243 ms 72.556 ms
11 hpr-stan-ge--oak-hpr.cenic.net (137.164.27.158) 73.763 ms 73.396 ms 73.665 ms
12 bbra-rtr.Stanford.EDU (171.64.1.134) 73.577 ms 73.682 ms 73.492 ms
13 * * *
14 www5.Stanford.EDU (171.67.20.37) 77.317 ms 77.128 ms 77.648 ms
Stanford, you'd, if I did it now, it'd be
a different set of things.
00:26:57 / 00:35:25
85


w6.3- The InterNetwork (IP).mp4 — Haruna Media Player
Traceroute
$ traceroute www.msu.edu
traceroute to www.msu.edu (35.8.10.30), 64 hops max, 40 byte packets
1 141.211.203.252 (141.211.203.252) 2.644 ms 0.973 ms 14.162 ms
2 v-bin-seb.r-bin-seb.umnet.umich.edu (192.122.183.61) 1.847 ms 0.561 ms 0.496 ms
3 v-bin-seb-i2-aa.merit-aa2.umnet.umich.edu (192.12.80.33) 6.490 ms 6.499 ms 6.529 ms
4 lt-0-3-0x1.eq-chi2.mich.net (198.108.23.121) 8.096 ms 8.113 ms 8.103 ms
5 xe-0-0-0x23.msu6.mich.net (198.108.23.213) 7.831 ms 7.962 ms 7.965 ms
6 192.122.183.227 (192.122.183.227) 12.953 ms 12.339 ms 10.322 ms
7 cc-t1-ge1-23.net.msu.edu (35.9.101.209) 9.522 ms 9.406 ms 9.817 ms
8 * * *
Arbor, Michigan to East Lansing Michigan,
Michigan State University, we have a very
00:29:46 / 00:35:25
85


w6.3- The InterNetwork (IP).mp4 — Haruna Media Player
Subtitle scale: 0.3
Traceroute
$ traceroute www.pku.edu.cn
traceroute: Warning: www.pku.edu.cn has multiple addresses; using 162.105.129.104
traceroute to www.pku.edu.cn (162.105.129.104), 64 hops max, 40 byte packets
1 141.211.203.252 (141.211.203.252) 1.228 ms 0.584 ms 0.592 ms
2 v-bin-seb.r-bin-seb.umnet.umich.edu (192.122.183.61) 0.604 ms 0.565 ms 0.466 ms
3 v-bin-seb-i2-aa.merit-aa2.umnet.umich.edu (192.12.80.33) 7.511 ms 6.641 ms 6.588 ms
4 192.122.183.30 (192.122.183.30) 12.078 ms 6.989 ms 7.619 ms
5 192.31.99.133 (192.31.99.133) 7.666 ms 8.953 ms 17.861 ms
6 192.31.99.170 (192.31.99.170) 59.275 ms 59.273 ms 59.108 ms
Michigan
Tennessee
7 134.75.108.209 (134.75.108.209) 173.614 ms 173.552 ms 173.333 ms
8 134.75.107.10 (134.75.107.10) 256.760 ms 134.75.107.18 (134.75.107.18) 256.574 ms 256.53
9 202.112.53.17 (202.112.53.17) 256.761 ms 256.801 ms 256.688 ms
10 202.112.61.157 (202.112.61.157) 257.416 ms 257.960 ms 257.747 ms
11 202.112.53.194 (202.112.53.194) 256.827 ms 257.068 ms 256.962 ms
12 202.112.41.202 (202.112.41.202) 256.800 ms 257.053 ms 256.933 ms
Seoul
Beijing
So here's an example of a Traceroute From
University of Michigan to Peking
00:31:20 / 00:35:25
75

In the context of the network diagnostic tool **Traceroute** (路由追踪) shown in your image, there are two critical ways "time" is referenced:

1. RTT (Round Trip Time) = 往返时间

In the yellow-boxed data on the slide, you see three time values (in milliseconds, **ms**) for every hop. For example, in Hop 1, the times are **1.228 ms**, **0.584 ms**, and **0.592 ms**.

- **What it measures:** This is the time it takes for a "probe" packet to go from the source to that specific router and back again.
- **Why three times?** Traceroute typically sends three separate packets to each hop to ensure accuracy and to show if the connection speed is consistent or "jittery".
- **Analysis:** As your data moves further away—from Michigan to Seoul and finally Beijing—these numbers increase significantly, jumping from roughly **12 ms** in the US to over **256 ms** once it reaches Asia.

2. TTL (Time to Live) = 生存时间

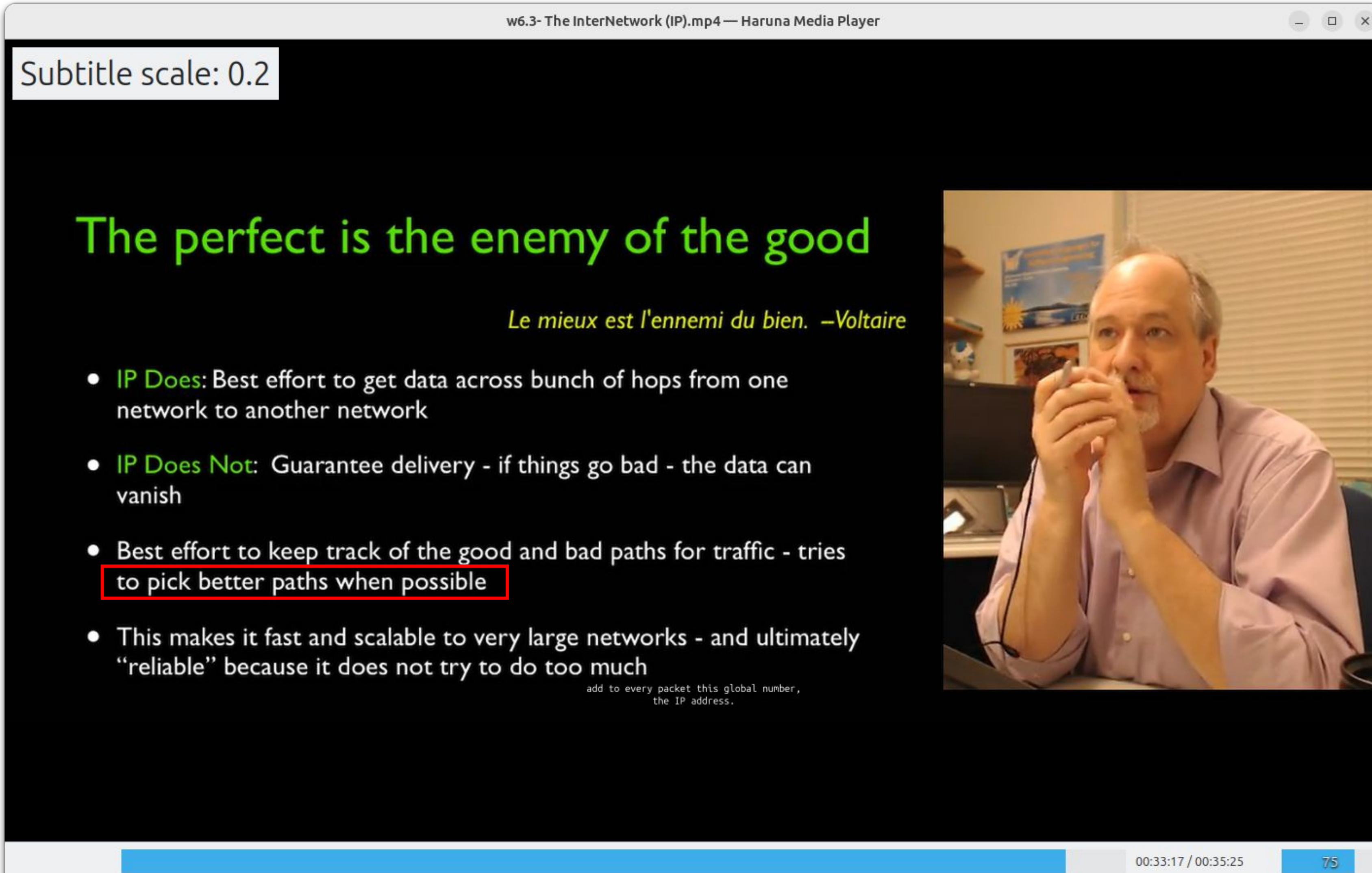
While not explicitly printed in the output table, **TTL** is the hidden mechanism that makes Traceroute work.

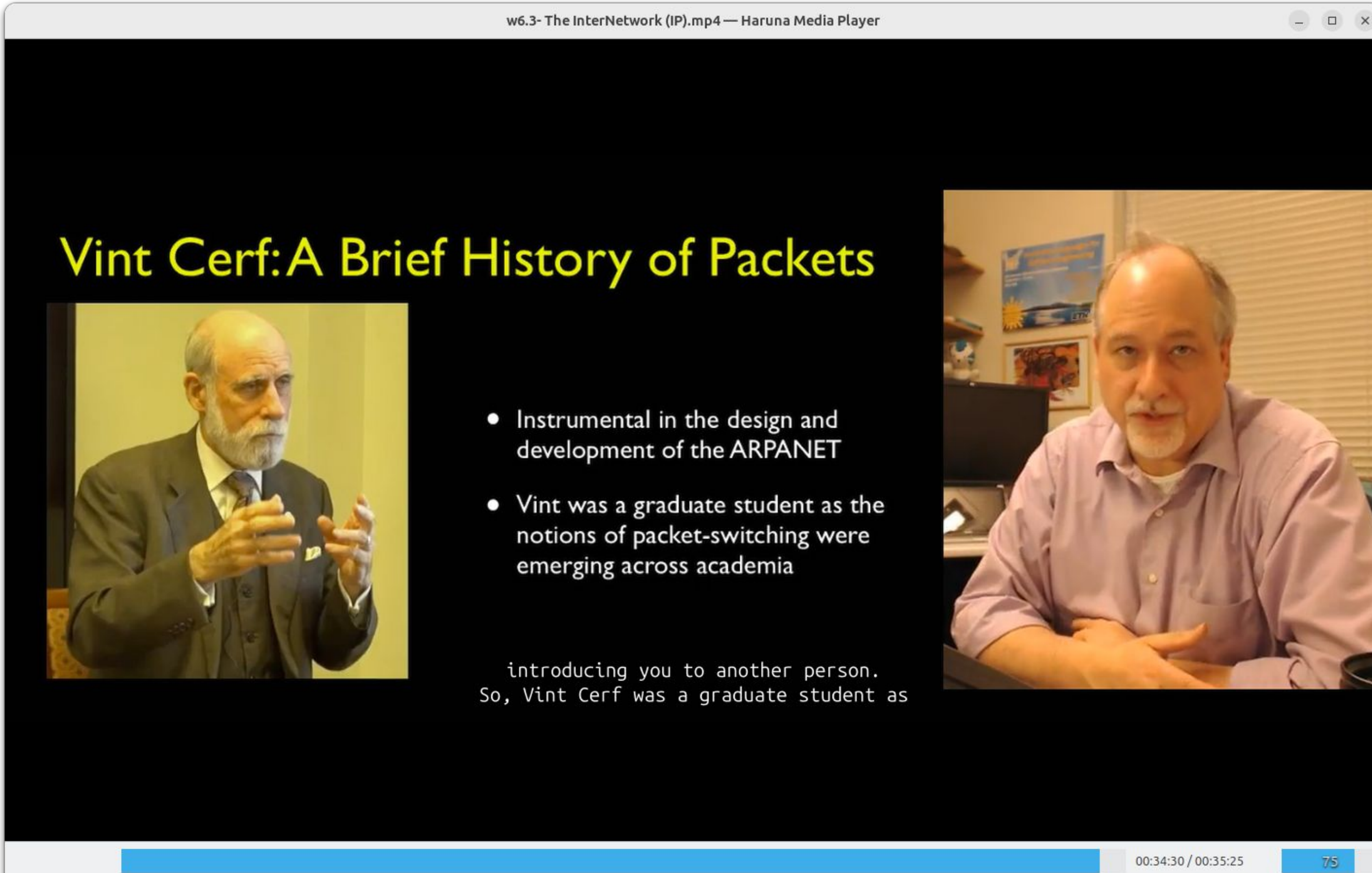
- **The Countdown:** Every IP packet has a TTL value (usually starting at 64 or 128). Each time the packet hits a router, the router subtracts 1 from this number.
- **The "Time Exceeded" Trigger:** When the TTL hits **0**, the router discards the packet and sends a message back to you. Traceroute purposely starts with a TTL of 1 to identify the first router, then TTL of 2 for the second, and so on.

3. NAT Timing (Network Address Translation)

In your other image regarding **NAT** (网络地址转换), the slide mentions that "You never see this happening" because it is done "as the packet goes through the router".

- **Real-time Translation:** This happens in microseconds. The router must instantly swap the **Private IP** (e.g., `192.168.0.20`) with the **Public IP** (e.g., `141.206.14.3`) to keep your rover or laptop connected to the web without delay.


w6.3- The InterNetwork (IP).mp4 — Haruna Media Player
Subtitle scale: 0.2
The perfect is the enemy of the good
Le mieux est l'ennemi du bien. --Voltaire
IP Does: Best effort to get data across bunch of hops from one network to another network
IP Does Not: Guarantee delivery - if things go bad - the data can vanish
Best effort to keep track of the good and bad paths for traffic - tries to pick better paths when possible
This makes it fast and scalable to very large networks - and ultimately "reliable" because it does not try to do too much
add to every packet this global number, the IP address.
00:33:17 / 00:35:25
75


w6.3- The InterNetwork (IP).mp4 — Haruna Media Player
Vint Cerf: A Brief History of Packets
Instrumental in the design and development of the ARPANET
Vint was a graduate student as the notions of packet-switching were emerging across academia
introducing you to another person.
So, Vint Cerf was a graduate student as
00:34:30 / 00:35:25
75

Summary

The IP Layer: "Postcards and Prefixes"

The Internet Protocol (IP) is the "Global Delivery Service." It doesn't care about the wires (Link Layer) or if the data actually arrives (Transport Layer). Its only job is to move a packet from one network to another.

- **The IP Address:** A 32-bit number (rendered as four numbers, 0-255, like `141.211.144.188`).
- **The Prefix (Network Number):** Routers only look at the first part of the address to decide which direction to throw the packet. It's like an area code for a phone.
- **Best Effort:** IP is "charming" because it's okay with dropping data. This simplicity is why it's so fast—it doesn't waste time double-checking.

Moving Targets: DHCP & NAT

Since you're an IoT expert in the making, these two are your bread and butter:

1. **DHCP (Dynamic Host Configuration Protocol):** When your rover wakes up in a new spot, it shouts, "I'm new! Give me an address!" DHCP is the service that hands it a temporary IP.
2. **NAT (Network Address Translation):** This is the "Aachen-Sanctuary" special. Your home router has one real IP, but it gives all your gadgets "fake" (non-routable) addresses like `192.168.x.x`.
   - **The Joke Explained:** In that XKCD comic, the "killer" has a `192.168.x.x` address—meaning he's literally inside the same house/network. *Logic-Sync: Spooky.*

The Diagnostic Ninja: Traceroute

When the network gets "whirlpooled" (packets going in circles), we use **TTL (Time to Live)**.

- Every router the packet hits subtracts **1** from the TTL.
- When TTL hits **0**, the router kills the packet and sends a "rejection note" back.
- **Traceroute** intentionally sends packets with TTL 1, then 2, then 3, to map out every single "hop" between you and the destination.