WEB ARCHITECTURE FINAL PROJECT

HOW GREEN RECYCLING BOX WORKS IN OSI MODEL

DOUBLE S-TEAM : SHICHEN ZHANG, SHUTING YU

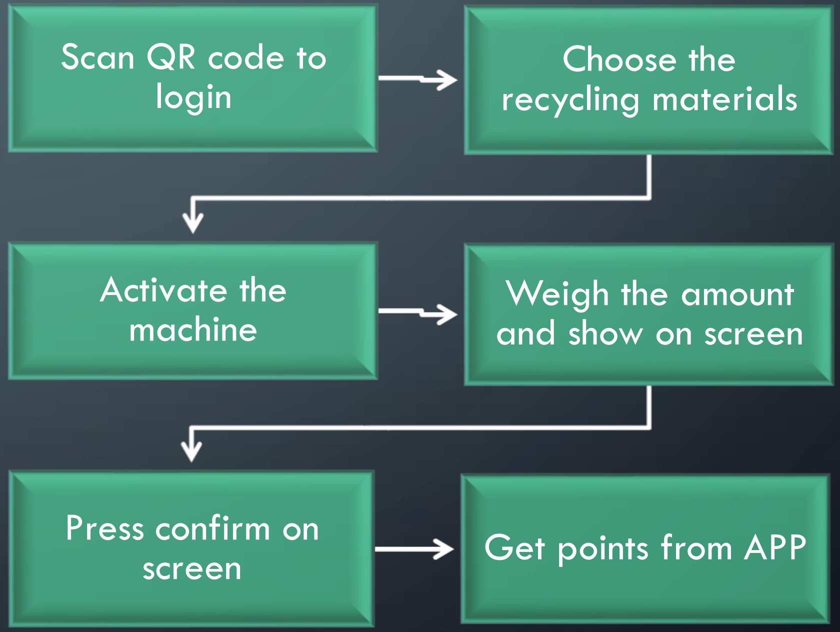
2022-02 RISDCE WINTER SEMESTER

ABOUT PROJECT-GREEN RECYCLING BOX

Green world

Purpose: Encourage people to do recycling daily

User Flow in General:



Scan QR code to login → Choose the recycling materials → Activate the machine → Weigh the amount and show on screen → Press confirm on screen → Get points from APP

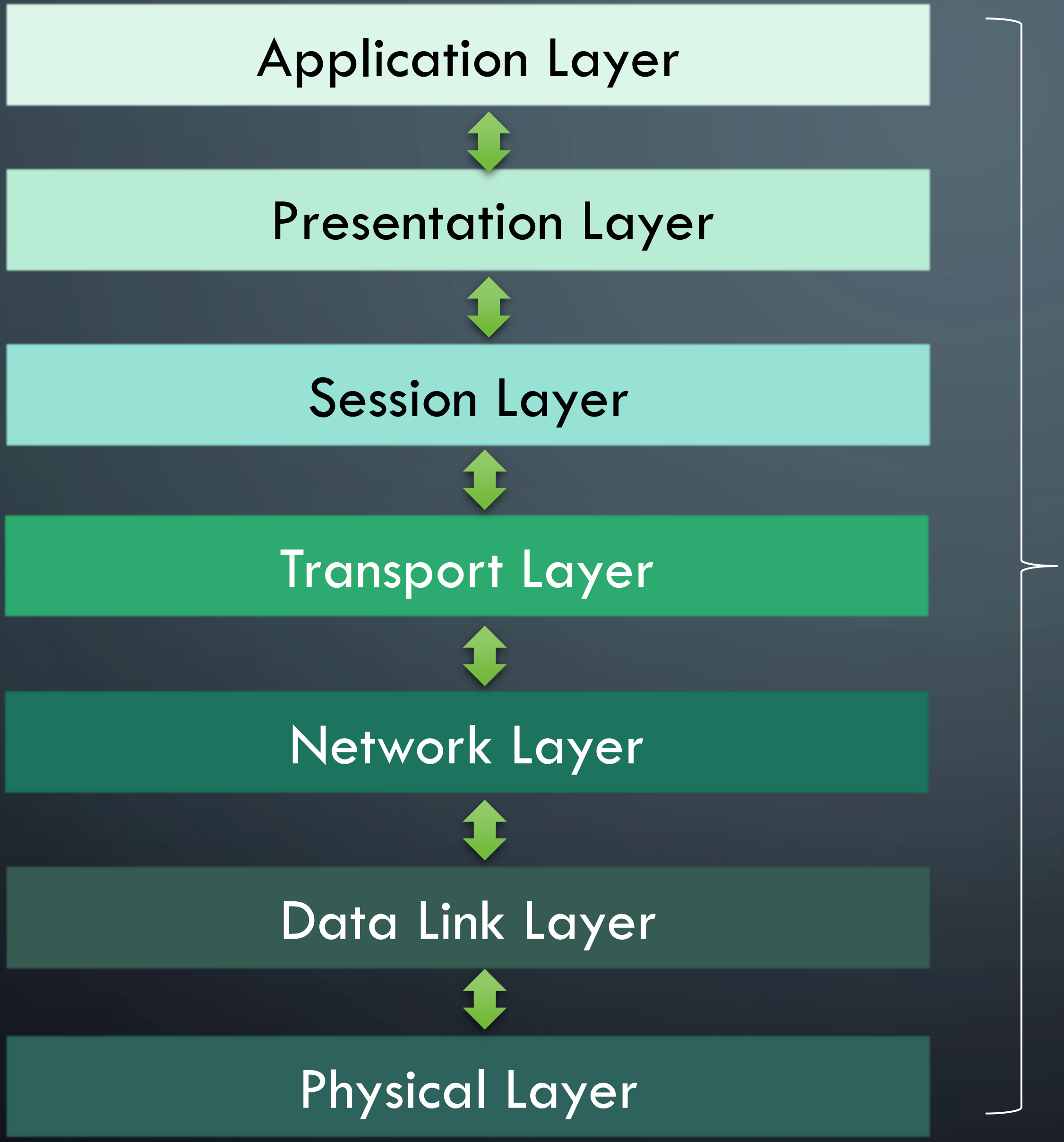
ABOUT QR CODE

QR stands for **Q**uick **R**esponse

QR codes : machine-readable barcodes representing data in a visual format of black and white squares, and capable of storing lots of data, generally for a locator, identifier, or tracker that directs to a specific webpage or application.

For more information about QR code, please check the extended reading file…

What we learnt: OSI MODEL



Application Layer

Presentation Layer

Session Layer

Transport Layer

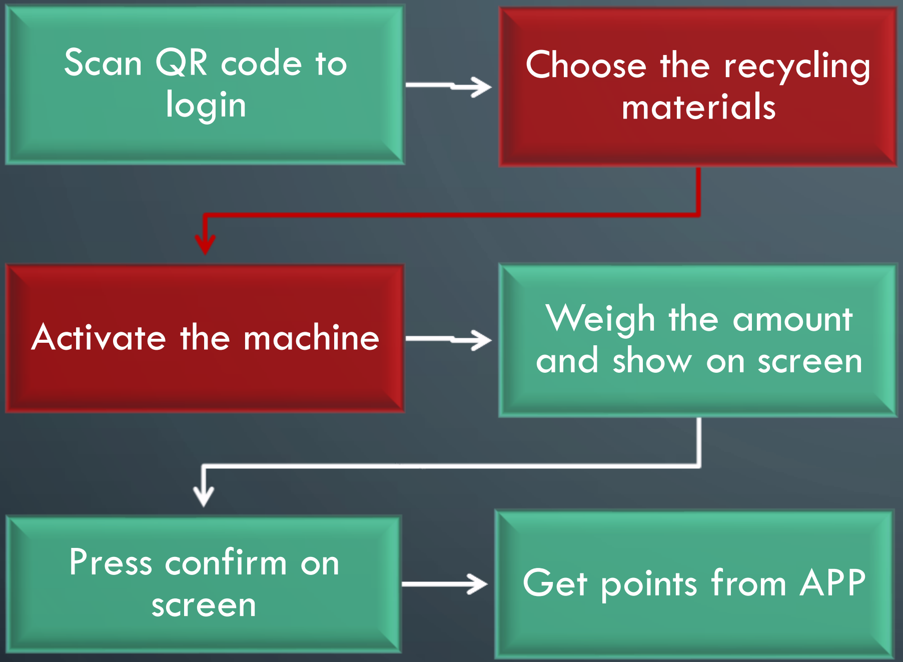
Network Layer

Data Link Layer

Physical Layer

How does my application work in OSI model??

User Flow in General:

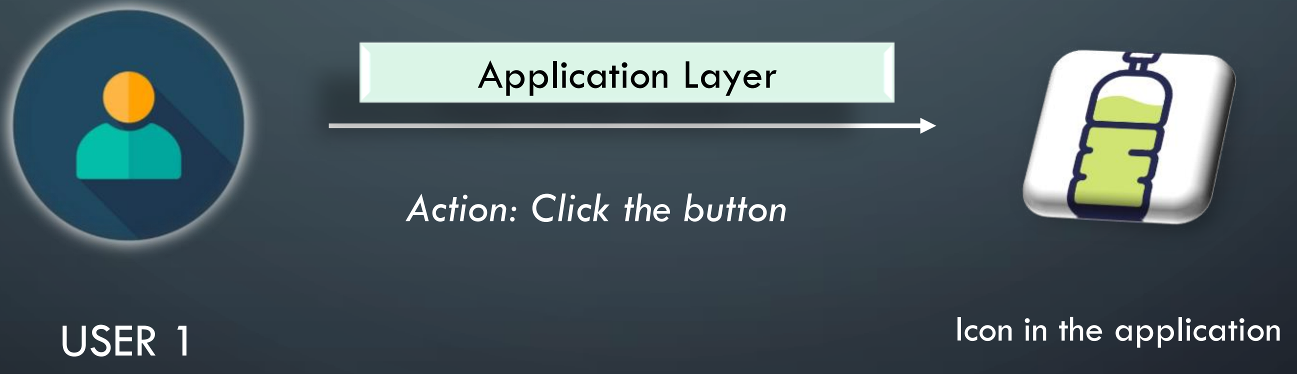


Let’s take the red box of user flow as an example…

Application Layer

ACTIONS:

- USER 1 wanted to recycle bottles to the machine this time.
- USER 1 opened our application and found the icon
- USER 1 then clicked the button to choose.



Application Layer

Action: Click the button

USER 1

Icon in the application

Application Layer

How does it work in detail

Step 1: Get URL with GUID transaction ID after scanned QR code https://recycleMe.org/transactionID/39eea9cb-0f92-449c-8b85-de02f0efd9ae

Step2: Check local hosts file

- The browser will first check the hosts file of the local hard disk to see if there are any rules corresponding to this domain name, and if so, use the IP address in the hosts file directly.

- If the corresponding IP address cannot be found in the local hosts file, the browser will send a DNS request to the local DNS server. The local DNS server is usually provided by your network access server provider. Like comcast, Verizon etc.

● ○ ○

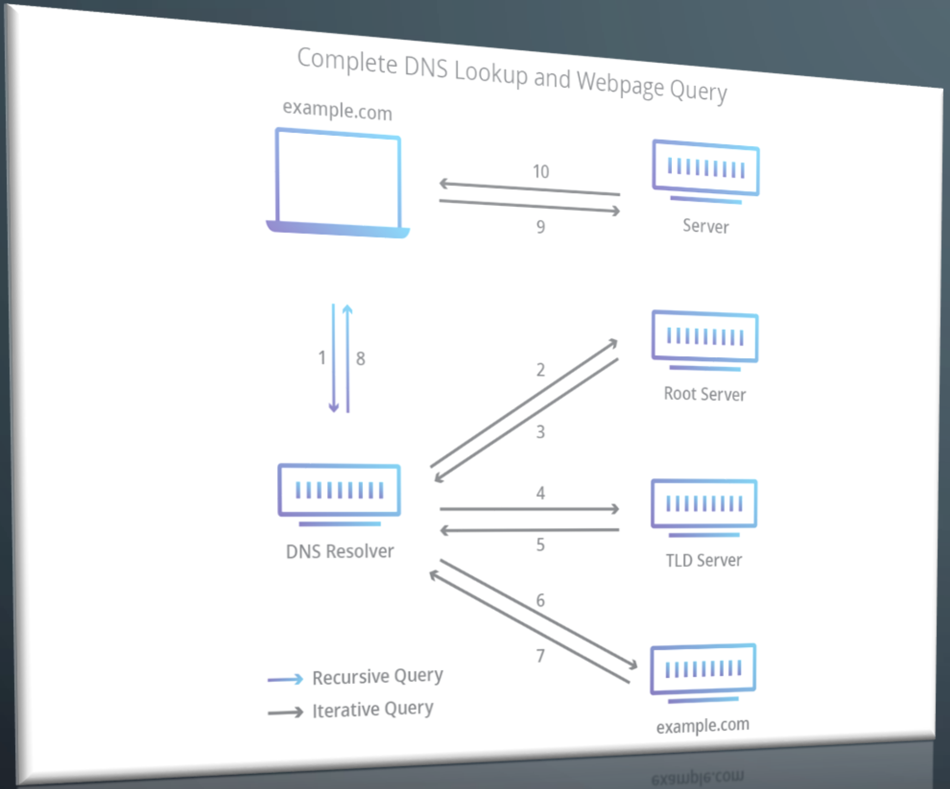
Application Layer

Step 3: DNS query

- After the DNS request for querying the URL you entered reaches the local DNS server, the local DNS server will first query its cache record. If there is such a record in the cache, the result can be returned directly. This process is a **recursive** query. If not, the local DNS server will also query the DNS root server.

- The root DNS server does not record the corresponding relationship between the specific domain name and IP address but tells the local DNS server that you can go to the domain server to continue the query and give the address of the domain server. This process is an **iterative** process.

Application Layer



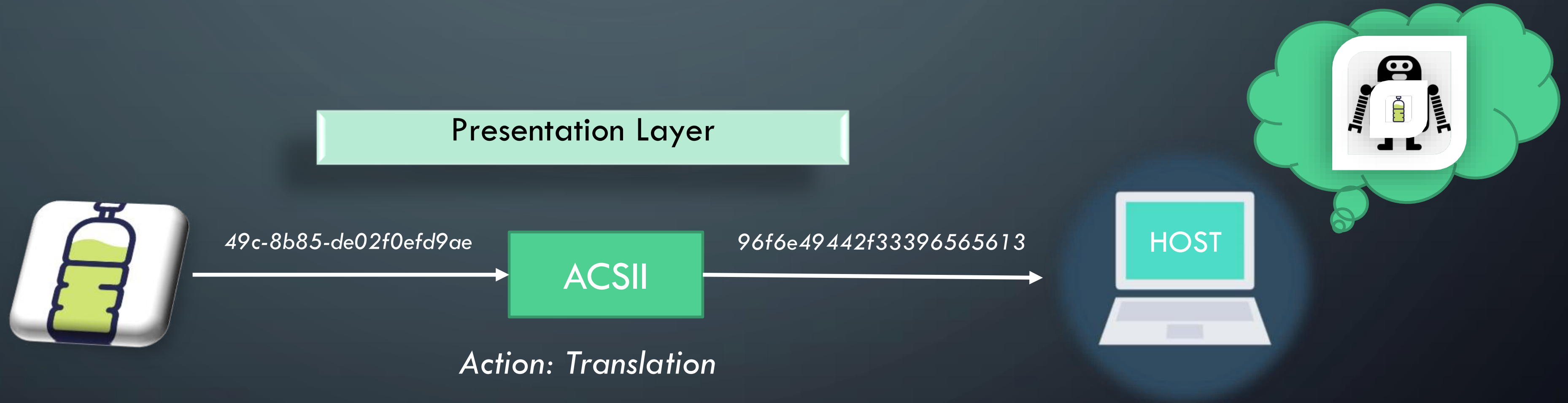
Recursively query vs Iteratively query:

Finally, the local DNS server sends a request to the resolution server of the domain name, and then a corresponding relationship between the domain name and the IP address can be received. The local DNS server not only returns the IP address to the user's computer, but also saves the corresponding relationship in the cache. , so that when another user queries next time, the result can be returned directly to speed up network access.

Presentation Layer

ACTIONS:

- Host application wanted to understand what was sent.
- Host application used ‘translator’ to understand the content.



Presentation Layer

49c-8b85-de02f0efd9ae

ACSII

96f6e49442f33396565613

HOST

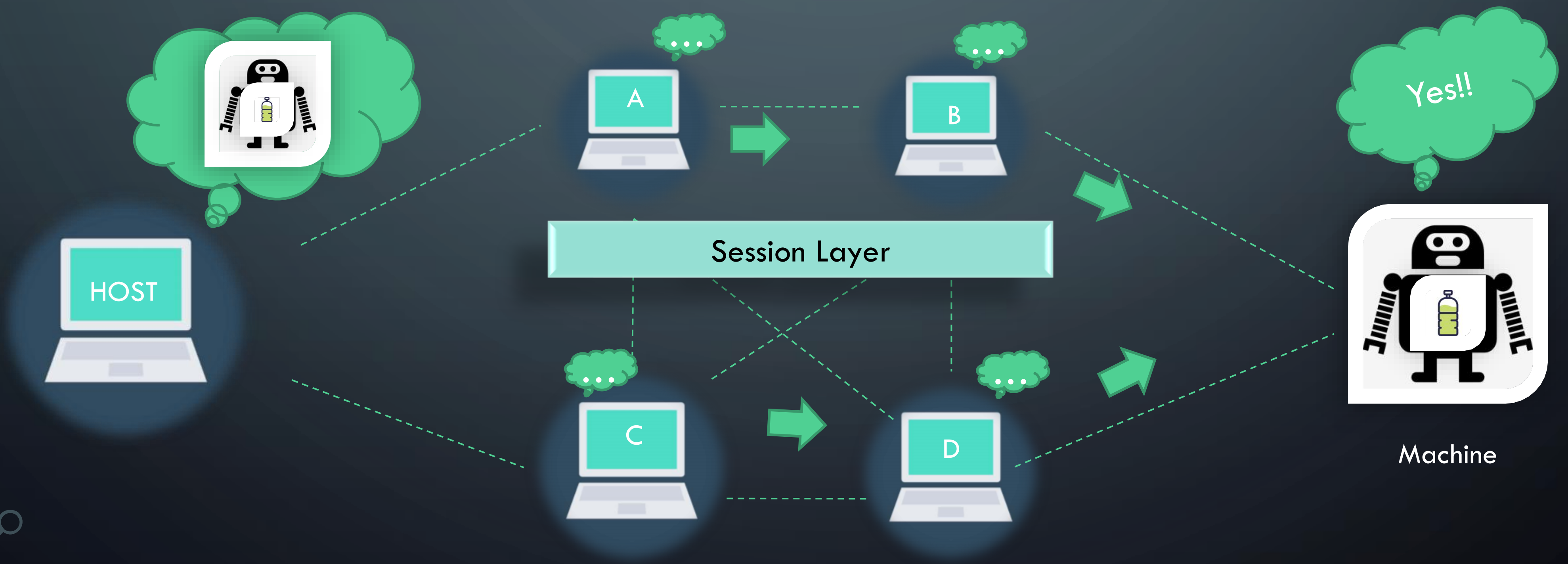
Action: Translation

Icon in the application

Session Layer

ACTIONS:

- Host application knew what was needed
- Host application tried to search through the network
- Other Host applications helped to locate the machine with bottle icon



Session Layer

How does it work in detail

After presentation layer hand over the data to session layer, we start establishing security session by SSL/TLS protocol

SSL/TLS by RSA algorithm: Handshake steps:

Stage 1: Client say 'hello' to server . This 'Hello' message includes TLS version, supported 'Cipher suite', and client random. Server reply 'Hello' to client. This 'Hello' message includes SSL certification, sever selected cipher suite and server random.

Stage 2: The client verifies the server's SSL certificate with the certificate authority that issued it. The client sends one more random string of bytes, the "premaster secret." The premaster secret is encrypted with the public key and can only be decrypted with the private key by the server.

Stage 3: The server decrypts the premaster secret.

Stage 4: Session key created. Both client and server are ready for sending message. Finally, the handshake is completed, and communication continues using the session keys.

● ○

Session Layer

SSL/TLS by Diffie-Hellman algorithm: Handshake steps:

Stage 1: Client say 'hello' to server . This 'Hello' message includes TLS version, supported 'Cipher suite', and client random. Server reply 'Hello' to client. This 'Hello' message includes SSL certification, sever selected cipher suite and server random.

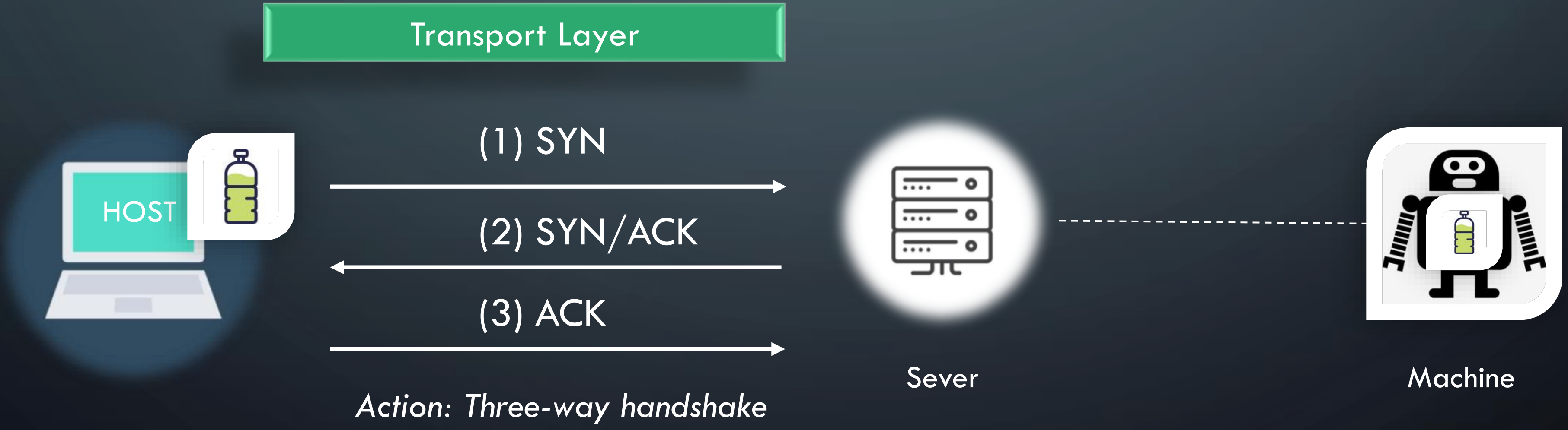
Stage 2: The server uses its private key to encrypt the client random, the server random, and its DH parameter. The client decrypts the server's digital signature with the public key, verifying that the server controls the private key and is who it says it is.

Stage 3: The client and server use the DH parameters they exchanged to calculate a matching premaster secret separately. The client and server calculate session keys from the premaster secret, client random, and server random, just like in an RSA handshake.

Stage 4: Session key created. Both client and server are ready for sending message. Finally, the handshake is completed, and communication continues using the session keys.

Transport Layer

ACTIONS:
- HTTP went by TCP protocol.
- TCP established connection by three steps.



Transport Layer

How does it work in detail

Three-way handshake:

First time 'handshake': The client sends a SYN message (SYN = 1) to the server and indicates the client's initial sequence number ISN(x), that is, seq = x. Indicates the sequence number of the first byte of the data sent in this segment . At this point the client is in the SYN_SENT state.

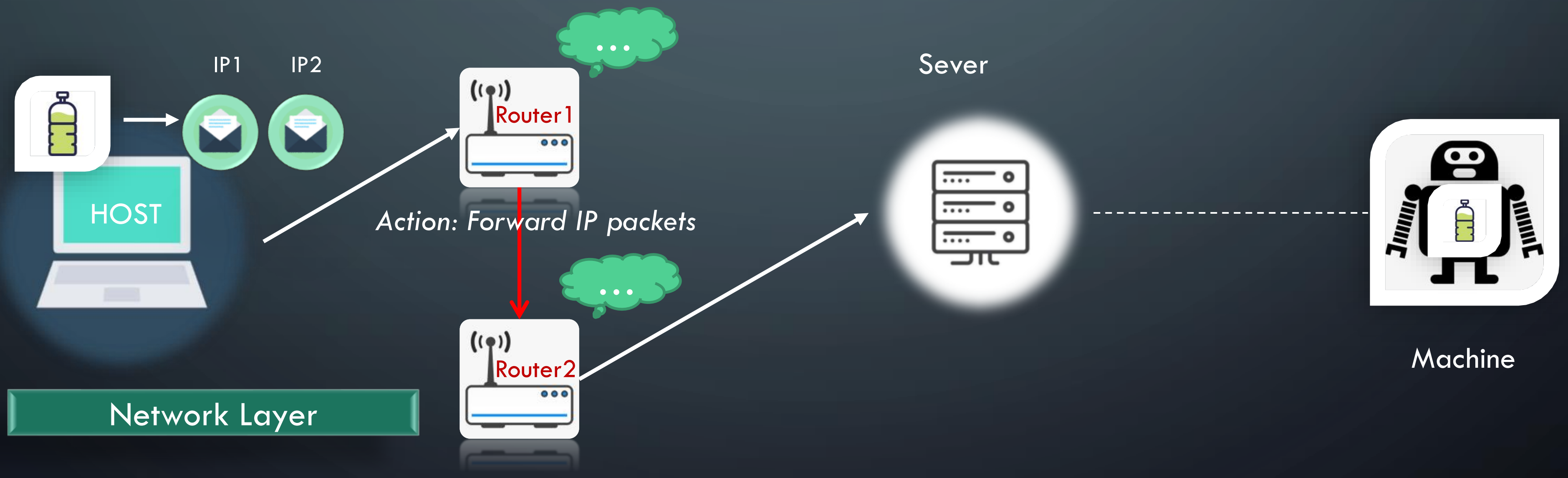
Second time 'handshake': After the server receives the SYN message from the client, it will send a SYN message as a response (SYN = 1), and specify its own initial sequence number ISN(y), that is, seq = y. At the same time, the client's ISN + 1 will be used as the value of the confirmation number ack, indicating that the SYN message sent by the client has been received, and the sequence number of the first byte of the next data expected to be received is x + 1. When the server is in SYN_REVD state.

Third time 'handshake': After the client receives the SYN message responded by the server, it will send an ACK message. It also uses the server's ISN + 1 as the value of ack, indicating that it has received the SYN message from the server and hopes to receive it. The sequence number of the first byte of the next data is y + 1 and indicates that the client's sequence number seq = x + 1 (initially seq = x, so the second segment needs +1), this When the client is in the ESTABLISHED state.

Network Layer

ACTIONS:

- Host application broke down the data into smaller pieces.
- Host application then added IP header to the data.
- The router1 transferred IP packet to next hop router2.



Network Layer

How does it work in detail

Network layer on host level:

- After established TCP connection, we start encapsulate the data.
- The encapsulation has two steps:

1. Decompose data: Break down the data into smaller pieces.
2. Reassemble data: For each small piece of data, we add the IP header to the data, which contains information about the packet itself, and the body, which is the actual data being sent. A header contains information about the content, source, and destination of each packet (somewhat like stamping an envelope with a destination and return address).

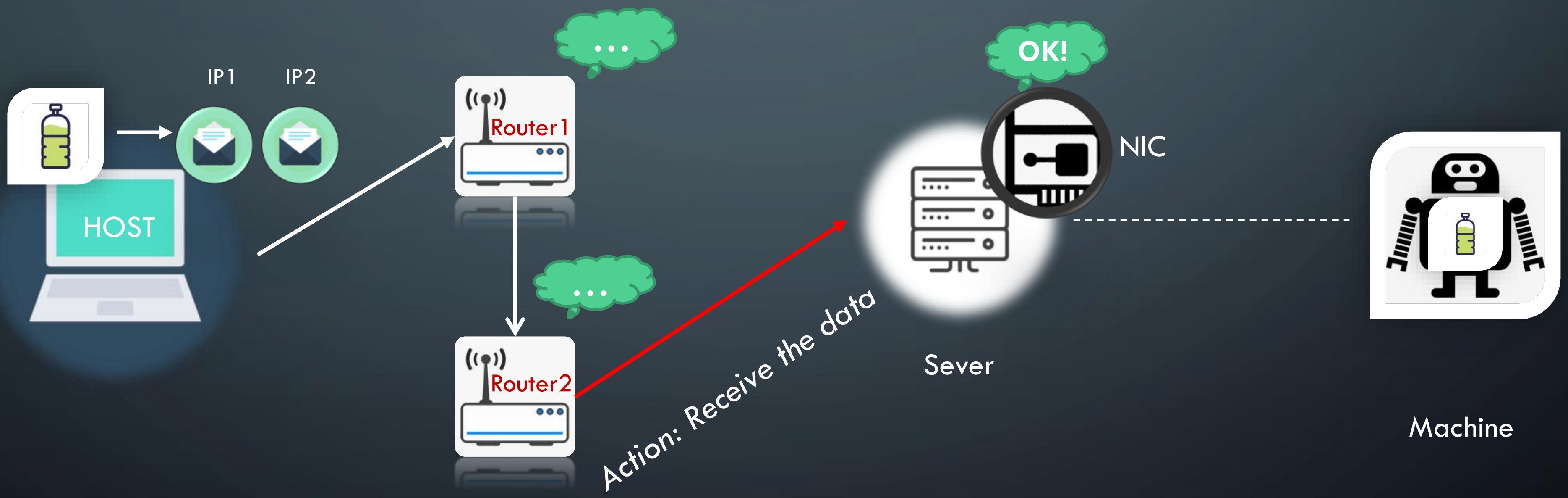
Network layer on Router level:

1. The router obtains the address that needs to be forwarded by looking at the header of the IP packet. Forward IP packets to the next hop route or host by looking at the local routing table.
2. Routers uses Link State Routing algorithm(Dijkstra algorithm) or distance vector routing algorithm(Bellman-Ford algorithm) to update its routing table and next hop router/host IP address.
3. Router chooses different routing protocols by different AS(Autonomous System). It can be RIP, OSPF, BGP etc.

Data Link Layer

When our IP packets has passed from network layer to data link layer, data link layer start breaking them into smaller pieces. We called it ‘frames’. Like the network layer, the data link layer is also responsible for flow control and error control in intra-network communication

➡ Sever got the data through NIC

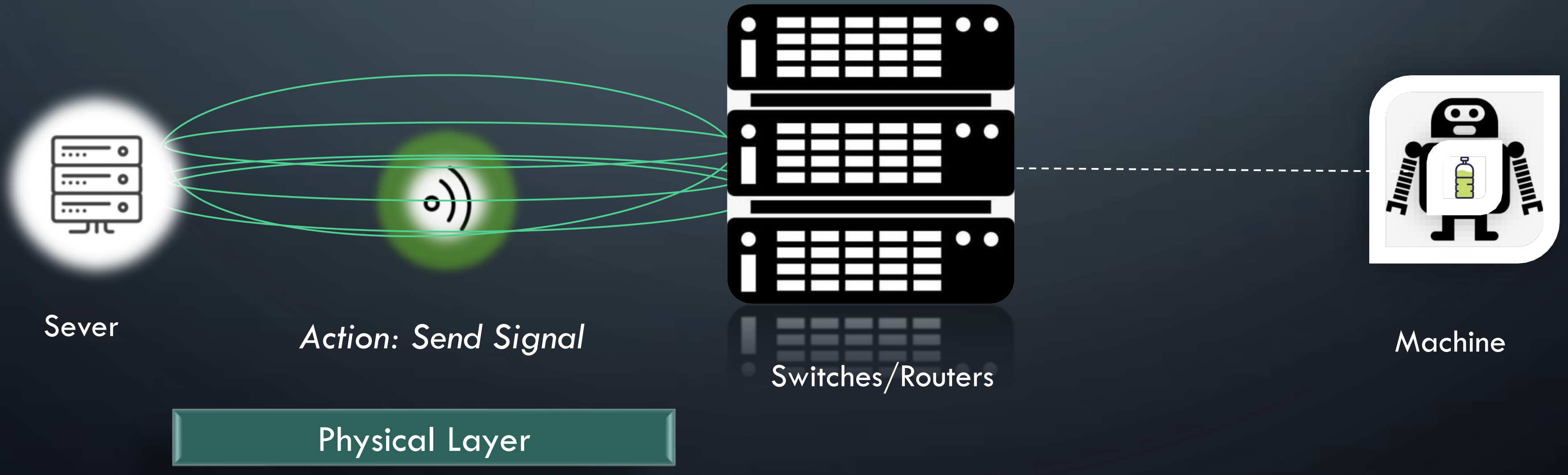


Data Link Layer

Physical Layer

Sever changed data into signal.
Signal sent to Switches/Routers.
Another 7 layers run from Physical layer to send back to Machine.

Physical layer includes the physical equipment involved in the data transfer, such as the cables and switches or routers. This is also the layer where the data gets converted into a bit stream, which is a string of 1s and 0s. The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices.



Thank you!

Should you have any question, please feel free to contact us!