Network transparency

Network transparency, in its most general sense, refers to the ability of a protocol to transmit data over the network in a manner which is transparent (invisible) to those using the applications that are using the protocol. In this way, users of a particular application may access remote resources in the same manner in which they would access their own local resources. An example of this is cloud storage, where remote files are presented as being locally accessible, and cloud computing where the resource in question is processing.

Contents

X Window

The term is often partially correctly applied in the context of the X Window System, which is able to transmit graphical data over the network and integrate it seamlessly with applications running and displaying locally; however, certain extensions of the X Window System are not capable of working over the network.[1]

Databases

In a centralized database system, the only available resource that needs to be shielded from the user is the data (that is, the storage system). In a distributed DBMS, a second resource needs to be managed in much the same manner: the network. Preferably, the user should be protected from the network operational details. Then there would be no difference between database applications that would run on the centralized database and those that would run on a distributed one. This kind of transparency is referred to as **network transparency** or **distribution transparency**. From a database management system (DBMS) perspective, distribution transparency requires that users do not have to specify where data is located.

Some have separated distribution transparency into location transparency and naming transparency.

Location transparency in commands used to perform a task is independent both of locations of the data, and of the system on which an operation is carried out.

Naming transparency means that a unique name is provided for each object in the database.

Firewalls

Transparency in firewall technology can be defined at the networking (IP or Internet layer) or at the application layer.

Transparency at the IP layer means the client targets the real IP address of the server. If a connection is non-transparent, then the client targets an intermediate host (address), which could be a proxy or a caching server. IP layer transparency could be also defined from the point of server's view. If the connection is transparent, the server sees the real client IP. If it is non-transparent, the server sees the IP of the intermediate host.

Transparency at the application layer means the client application uses the protocol in a different way. An example of a transparent HTTP request for a server:

```
GET / HTTP/1.1
Host: example.org
Connection: Keep-Alive
```

An example non-transparent HTTP request for a proxy (cache):

```
GET http://foo.bar/ HTTP/1.1
Proxy-Connection: Keep-Alive
```

Application layer transparency is symmetric when the same working mode is used on both the sides. The transparency is asymmetric when the firewall (usually a proxy) converts server type requests to proxy type or vice versa.

Transparency at the IP layer does not automatically mean application layer transparency.

See also

- Data independence
- Replication transparency

References

1. "The Wayland Situation: Facts About X vs. Wayland (Phoronix)" (https://lwn.net/Articles/553415/). LWN.net. 23 June 2013.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Network_transparency&oldid=1031289340"

This page was last edited on 30 June 2021, at 20:13 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.