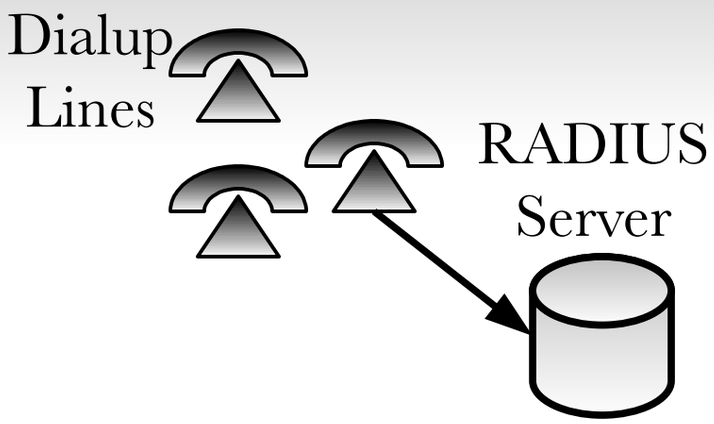
Arch·Red

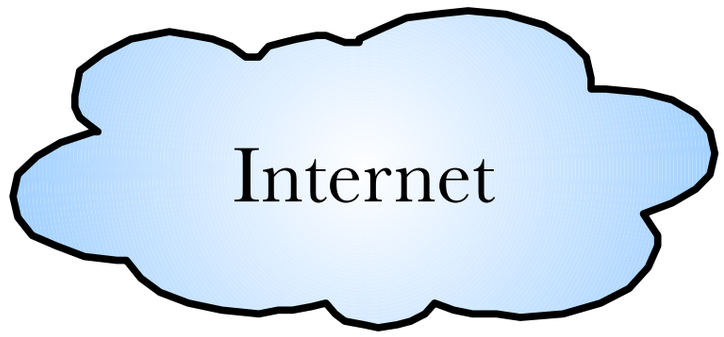
RADIUS Roaming: Issues and Solutions

Karri Huhtanen
Arch Red Oy
12th of February 2009

Arch·Red

A long time ago...

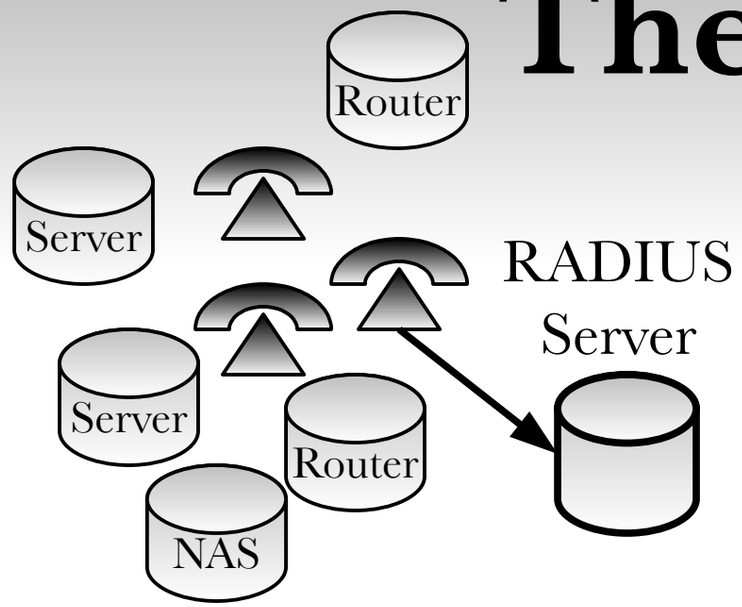


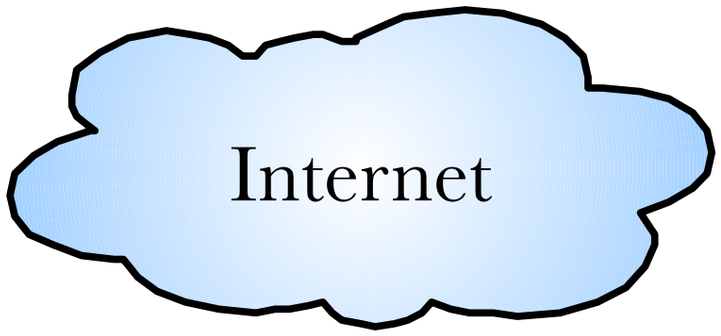


Remote Authentication Dial In User Service (RADIUS)

Arch·Red

Then came the NASes

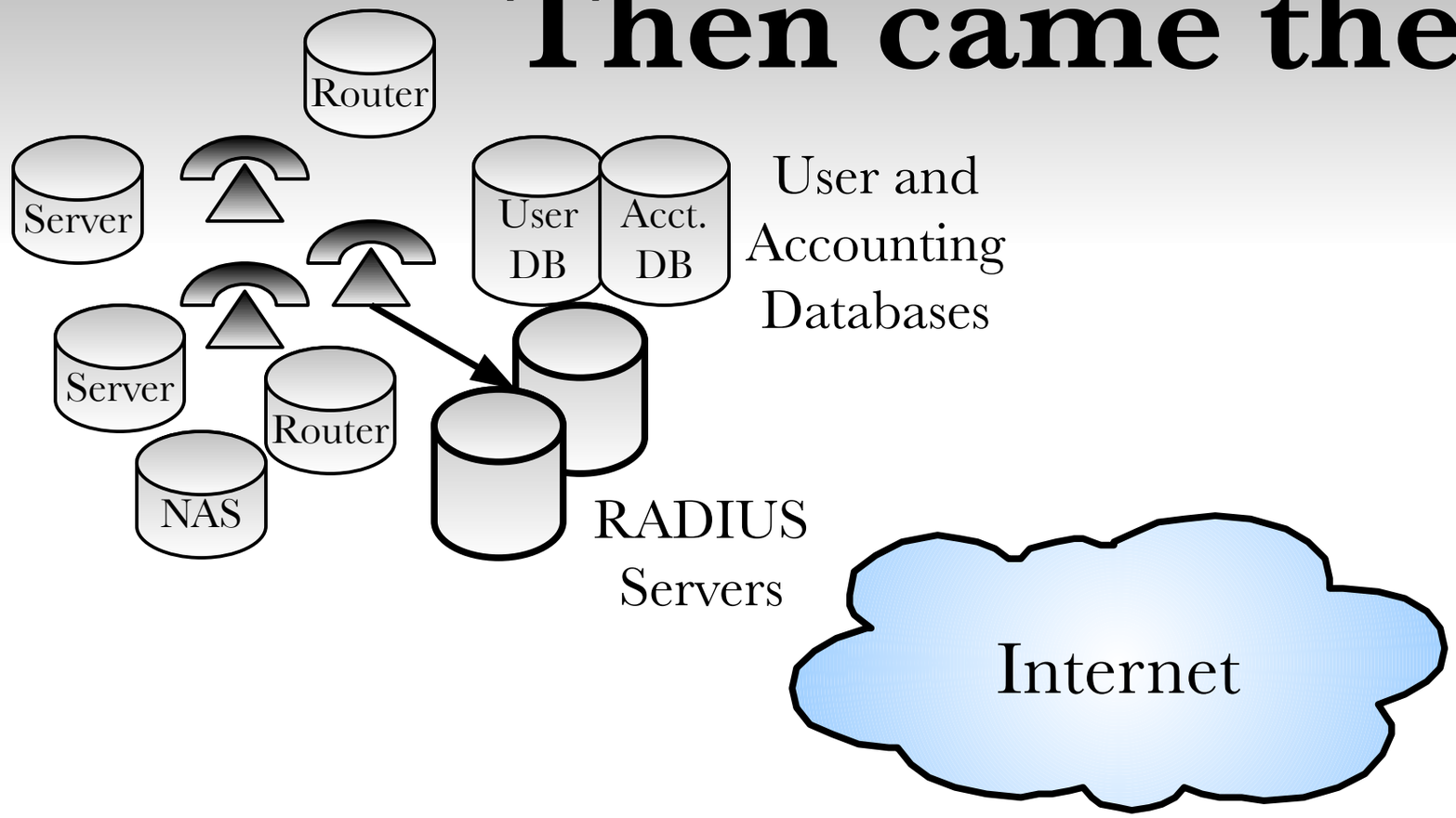




Network Access Server (NAS)

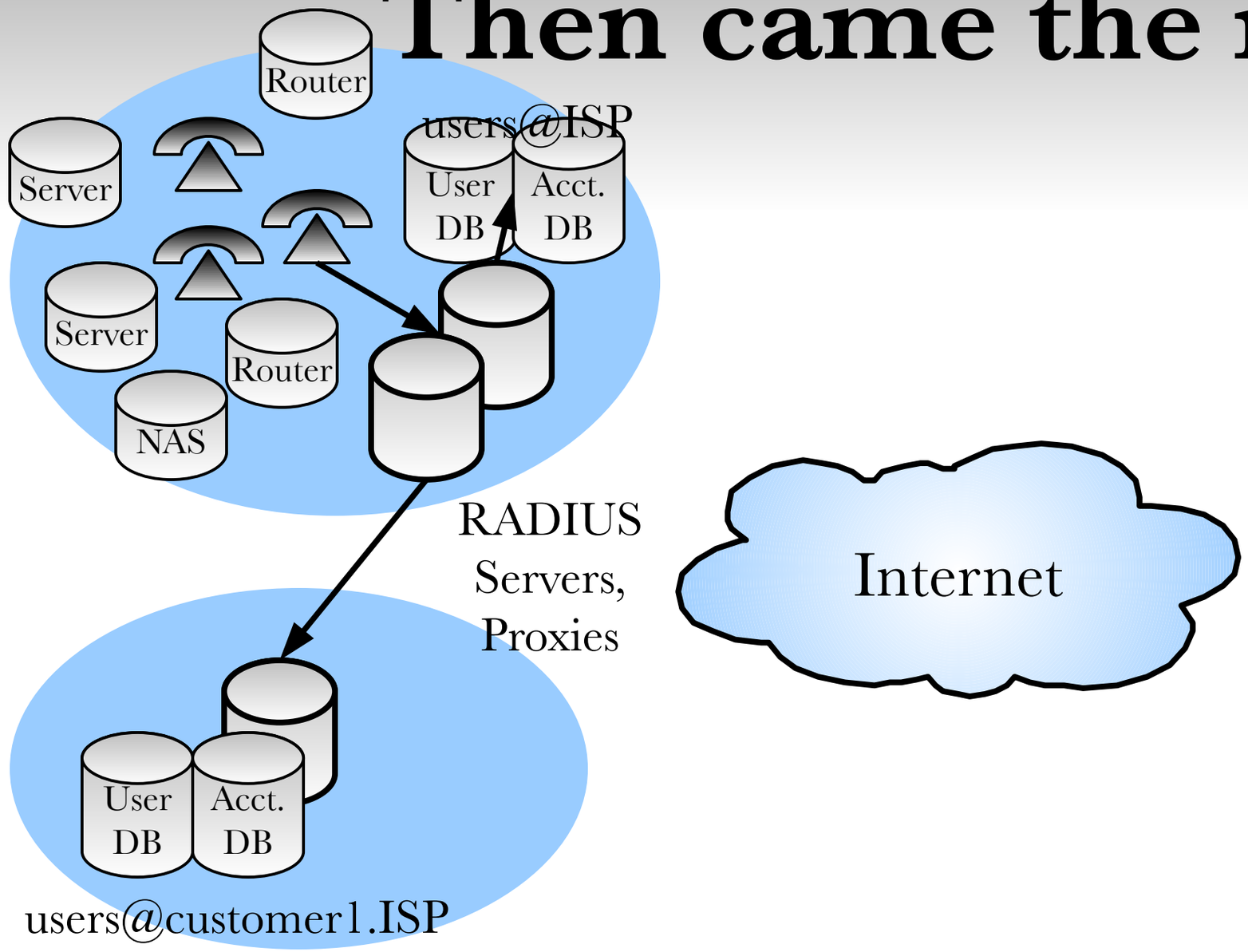
Arch·Red

Then came the SLAs



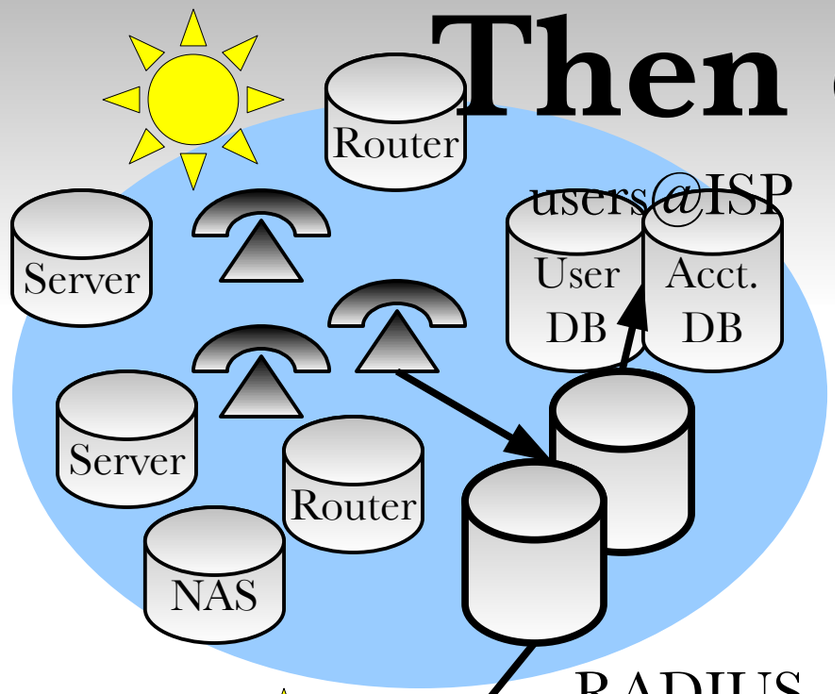
Arch·Red

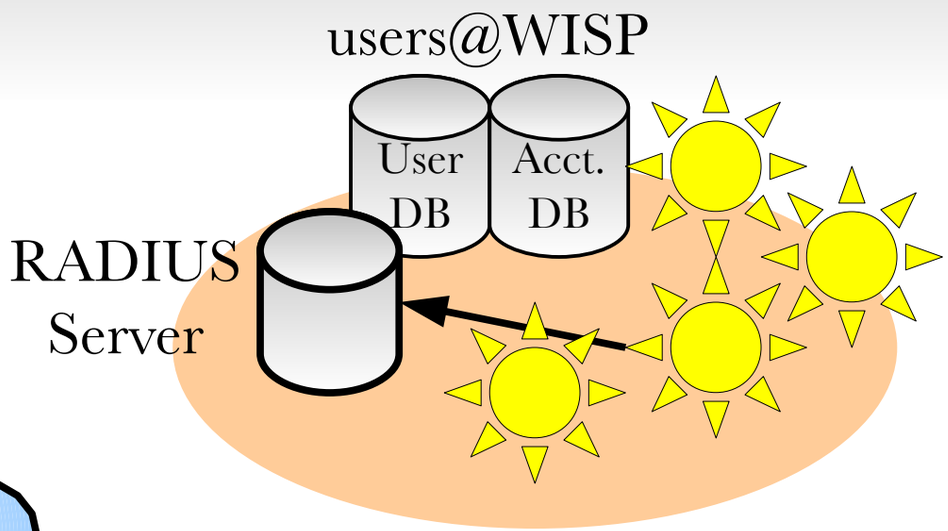
Then came the realms



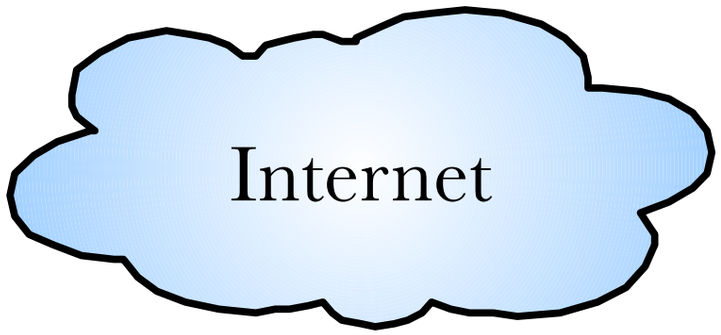
Arch·Red

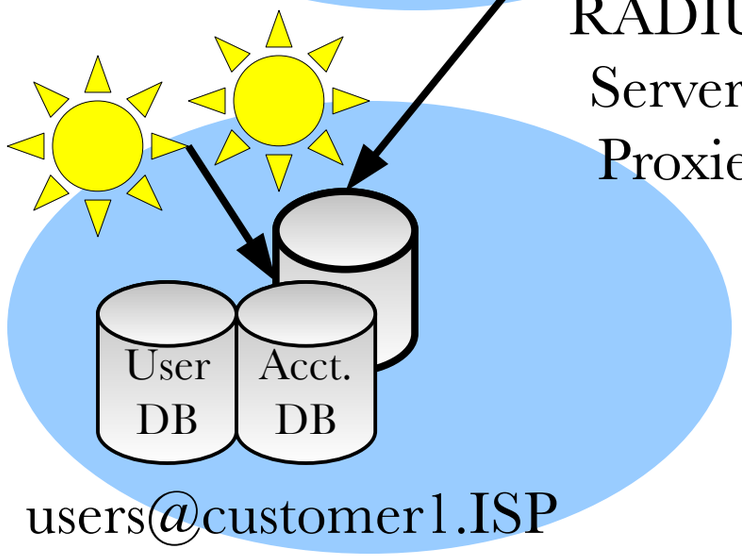
Then came the wireless





RADIUS Servers, Proxies

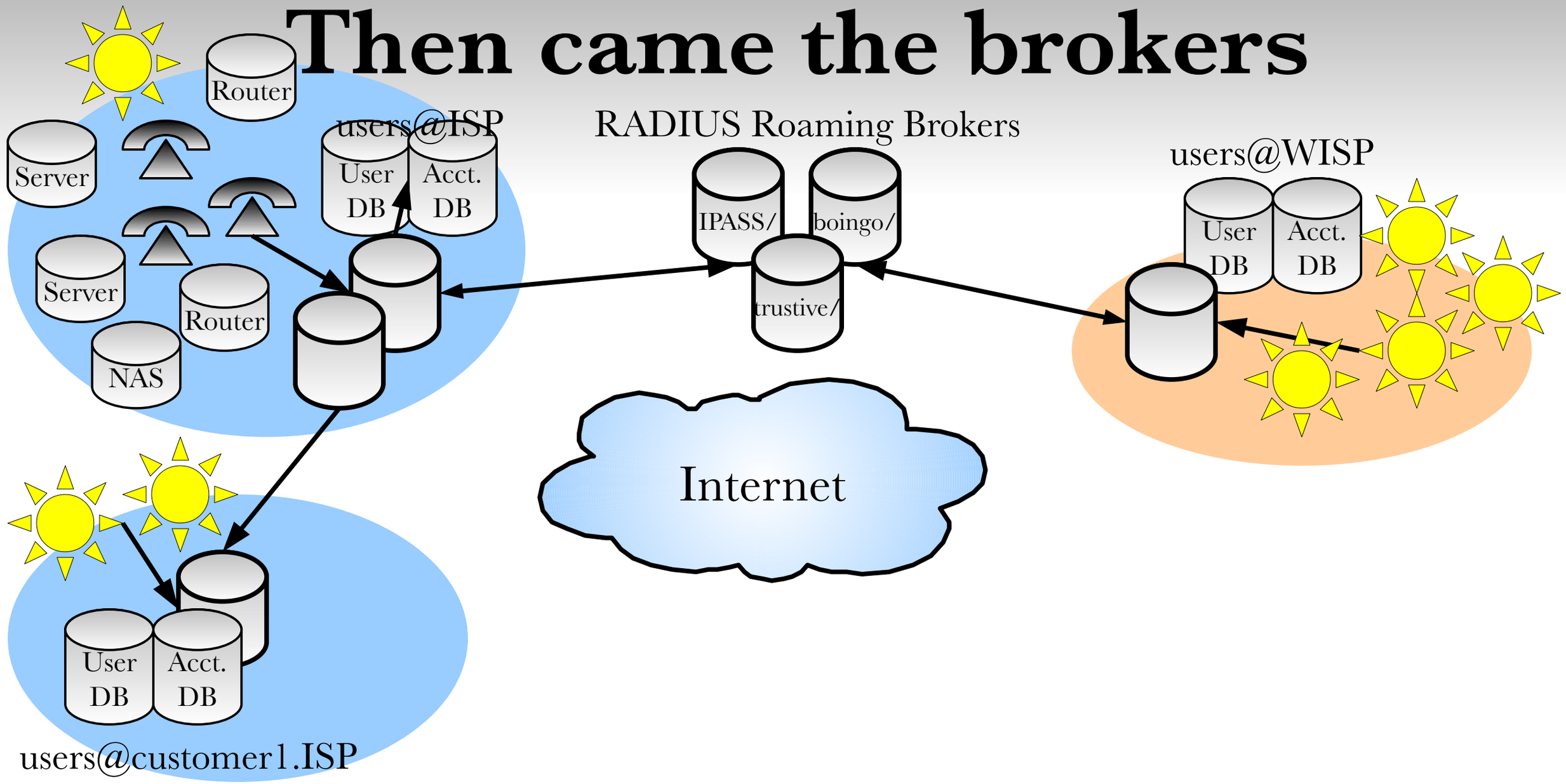




Wireless Internet Service Providers (WISPs)

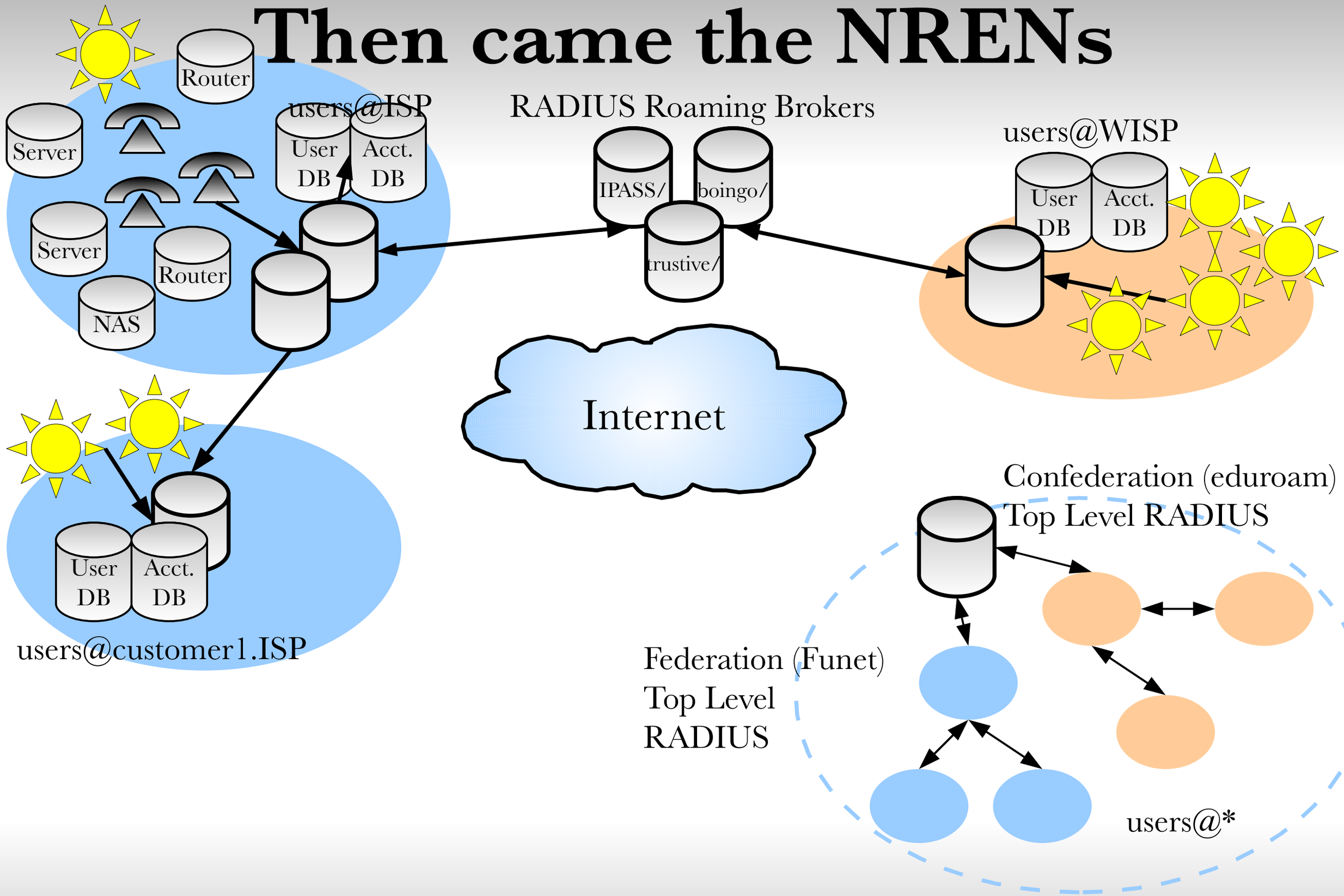
Arch·Red

Then came the brokers



Arch·Red

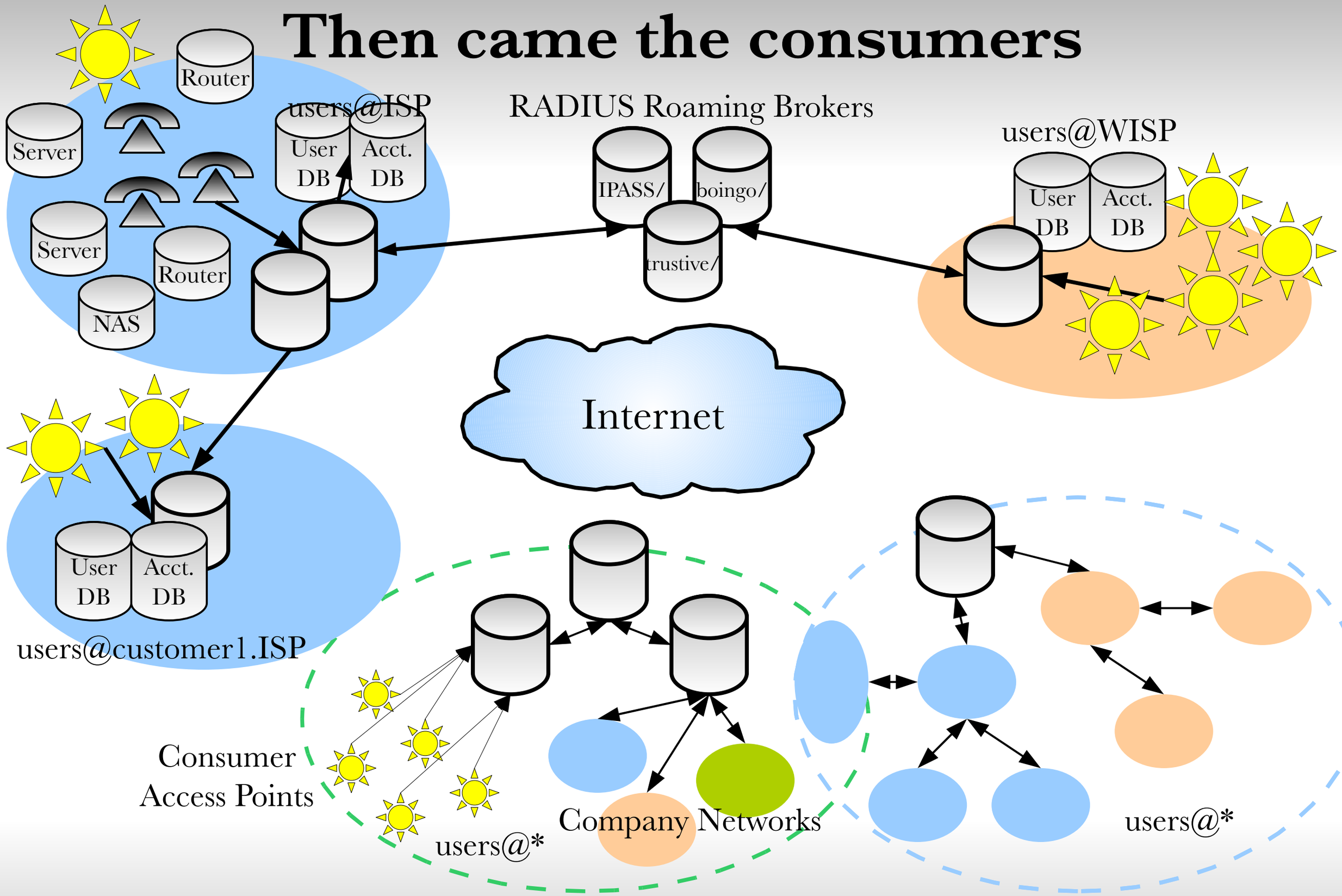
Then came the NRENs



National Research and Education Networks (NRENs)

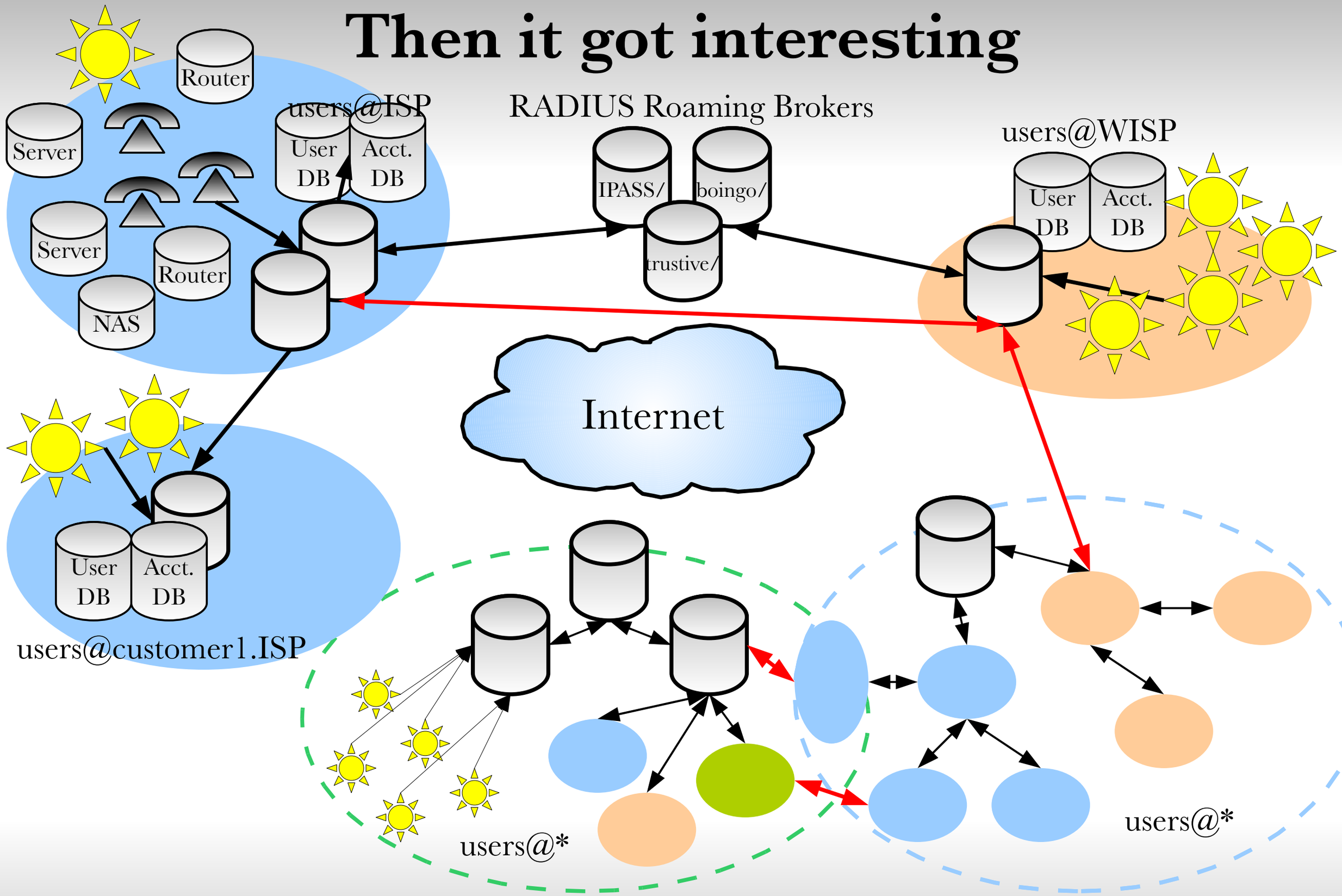
Arch·Red

Then came the consumers



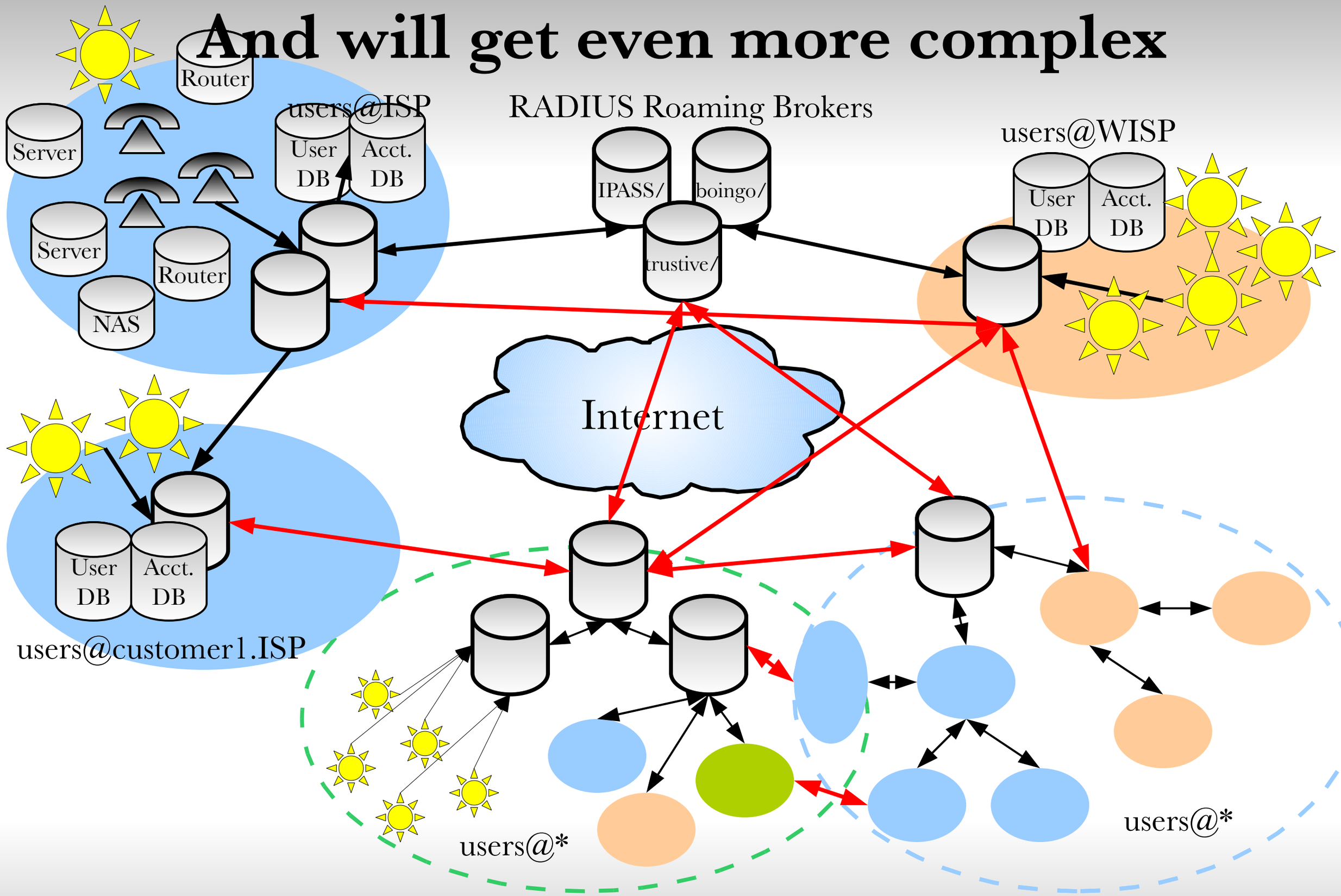
Arch·Red

Then it got interesting



Arch·Red

And will get even more complex



Arch·Red

… beginning to resemble routing

- Multiple default authentication routes
- Prefix/Realm advertisements
- Alternative authentication routes
  - With different costs and other metrics
- Preventing loops
- Securing authentication traffic and servers
- Protecting the privacy
- Sounds familiar, right?

Arch·Red

RADIUS protocol issues

- The original RADIUS has survived mainly because it has been quite easy to fix and extend with various RADIUS attributes.
- Even now when there has been a new authentication protocol called DIAMETER available, the work still continues to develop RADIUS further in RADIUS Extensions working group in IETF:
  - http://www.ietf.org/html.charters/radext-charter.html

Arch·Red

Securing authentication, protecting privacy, losing control?

- Developing EAP and EAP methods such as EAP-TLS, EAP-TTLS, PEAP made is possible to have a secured authentication tunnel from user terminal to home authentication server.
- The separate outer and inner identities such as anon@archred.com and user@archred.com made it possible to protect one's privacy, but needed something else to be developed as a unique identity.
- Chargeable User Identity was developed as a solution:
  - http://www.ietf.org/rfc/rfc4372.txt

Arch·Red

Ensuring reliable message delivery

- The current RADIUS protocol is UDP traffic => So far the tunnelling has been the only way to ensure reliable message delivery and roaming connections.

- There exists drafts to try to solve this:
  - RADIUS over TCP:
    - http://www.ietf.org/internet-drafts/draft-ietf-radext-tcp-transport-02.txt
  - TLS encryption for RADIUS over TCP (RadSec):
    - http://www.ietf.org/internet-drafts/draft-ietf-radext-radsec-03.txt

Arch·Red

From fixed RADIUS hierarchy to peer-to-peer architecture

- Solving the multiple roaming agreements and alternative route issues still needs work.
- Using DNS for discovering authentication realms is common in all proposals trying to solve the multiple roaming agreements.
- The authentication connections are done by demand dynamically from peer to peer instead of having a fixed hierarchy.
- The selection of roaming agreement and the validation of authentication servers is done with the certificates.
- The DNS discovery is actively developed within the RadSec proposal.

Arch·Red

Alternative authentication routes: costs and metrics

- Some work for specifying RADIUS attributes for these is rumored to be done, but could not get a confirmation at least from the RADIUS Extensions group?
- Work with DIAMETER/RADIUS is also done in 3GPP working groups, but their work is not covered in this presentation.
- Development of Peer-to-Peer RADIUS roaming might make these issues irrelevant?

Arch·Red

Summary

- RADIUS, just like the Internet, is not so simple anymore than it used to be.
- But just like the Internet, RADIUS still scales, evolves and new solutions and technology are build utilising it.
- New technologies like DIAMETER may gain ground, but RADIUS is likely to be around at the same time.
- Combining and (inter)connecting Internet and Telco driven authentication as well as community networks will drive the development and adoption of RADIUS and DIAMETER forward.

Arch·Red

Thank you. Any Questions?

Arch Red Oy

http://www.archred.com/

Karri Huhtanen

Firstname . Surname @ archred.com