

AAA for Fun and Profit

The logo for Suntel Communications features a stylized orange 'S' shape that is elongated and curved, resembling a double-headed arrow or a dynamic swoosh. It is positioned vertically, overlapping the text 'Suntel' and 'Communications'.

Suntel Communications

www.suntel.com.tr

Free Software/Open Source Telephony-Summit 2006

*AAA for Fun and Profit
(Why RADIUS keeps on kickin')*



Current Network Challenges

Networks are becoming geographically larger

Networks are becoming more complex

Networks are increasingly being opened to outsiders

Users are becoming increasingly mobile

User devices are becoming increasingly capable

Infected machines connecting behind firewalls



Large (and growing) number of Access Methods

- Blue Tooth
 - Calling Cards
 - Corporate PBX
 - Ethernet
 - GPRS/EDGE/UMTS
 - Instant Messenger
 - VoIP
 - VPN
 - VPDN
 - WiFi
 - WiMax
-
-

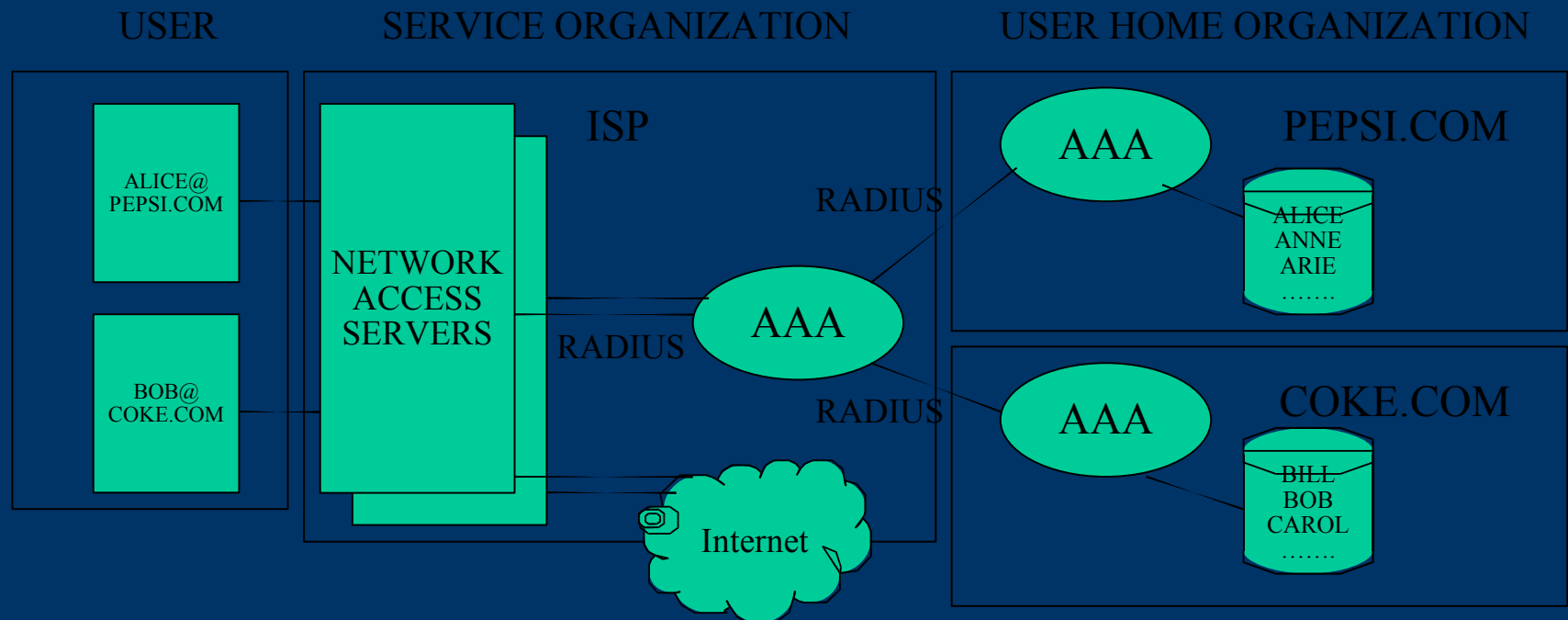
AAA to the rescue

An AAA Server is a server or servers that provide authorization, authentication and accounting services. These may be co-located with the NAS, or more typically, are located on a separate server and communicate with the NAS's User Management Interface via an AAA protocol. The three AAA functions may be located on a single server, or may be broken up among multiple servers.

AAA History

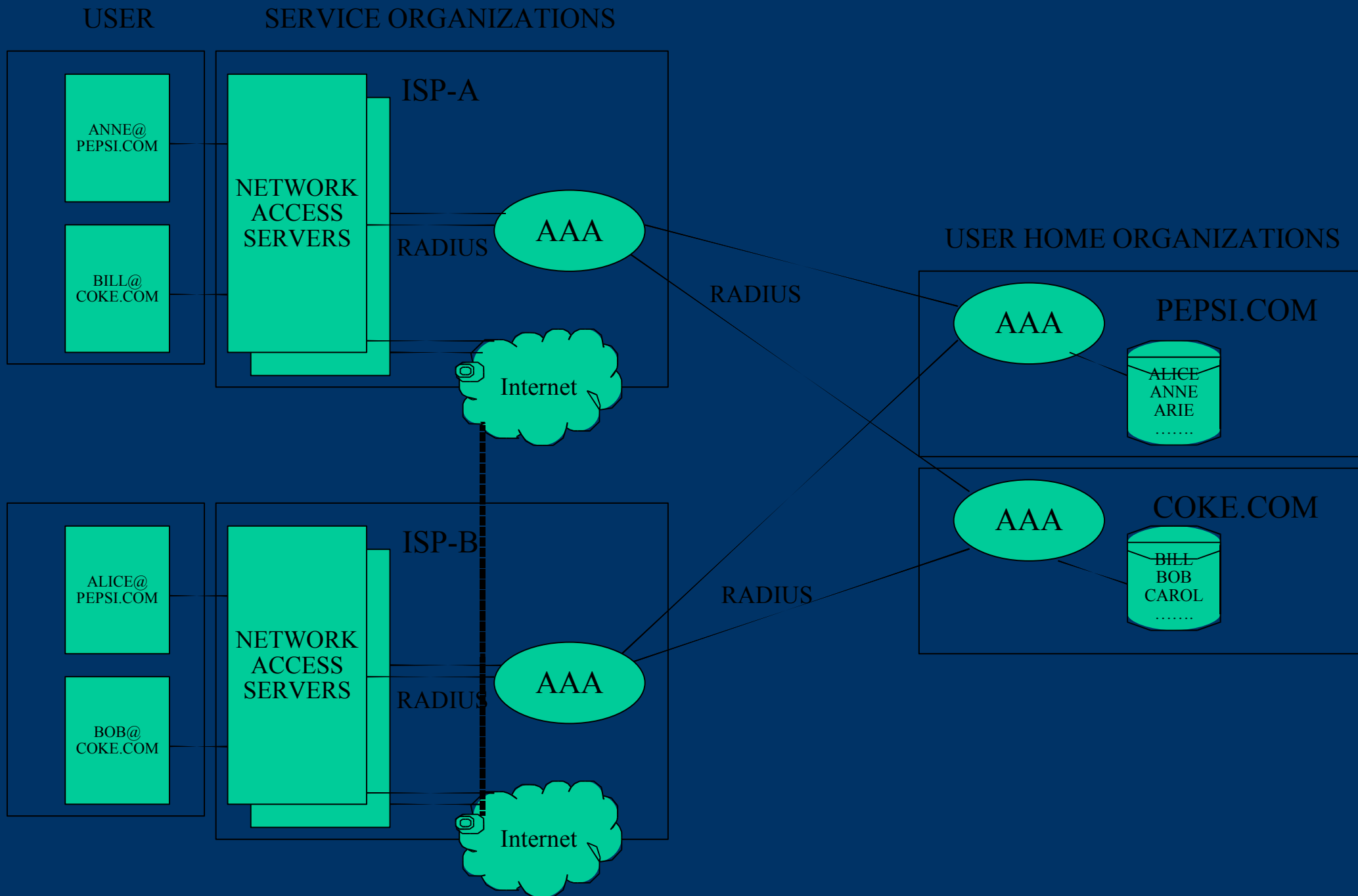
AAA roots in the “dial-in” environment where NAS use AAA servers to Authenticate & Authorize users and allow Accounting.

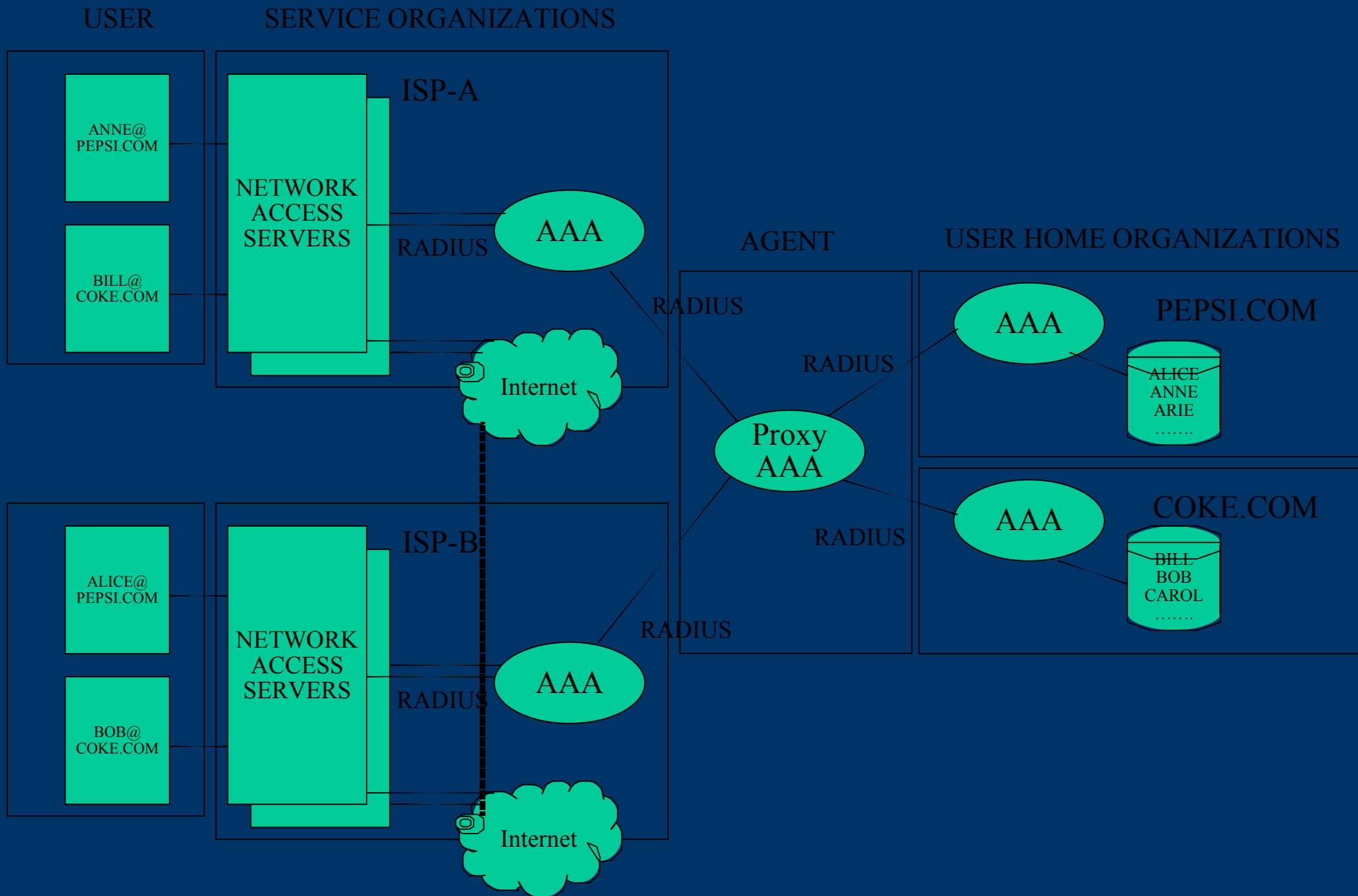
Need was generated by recognition that user-administration at or near the service equipment does not scale very well.



Flexibility of RADIUS allows

- User organizations to outsource their access service to one or more 3rd parties
 - Service organizations to host multiple organizations requiring network access facilities
 - User organizations or Agents to migrate to other Service Providers
 - An agent, using proxy AAA to change its service without affecting the agreement with its customers
 - A service organization to have ultimate authority over its users
-
-



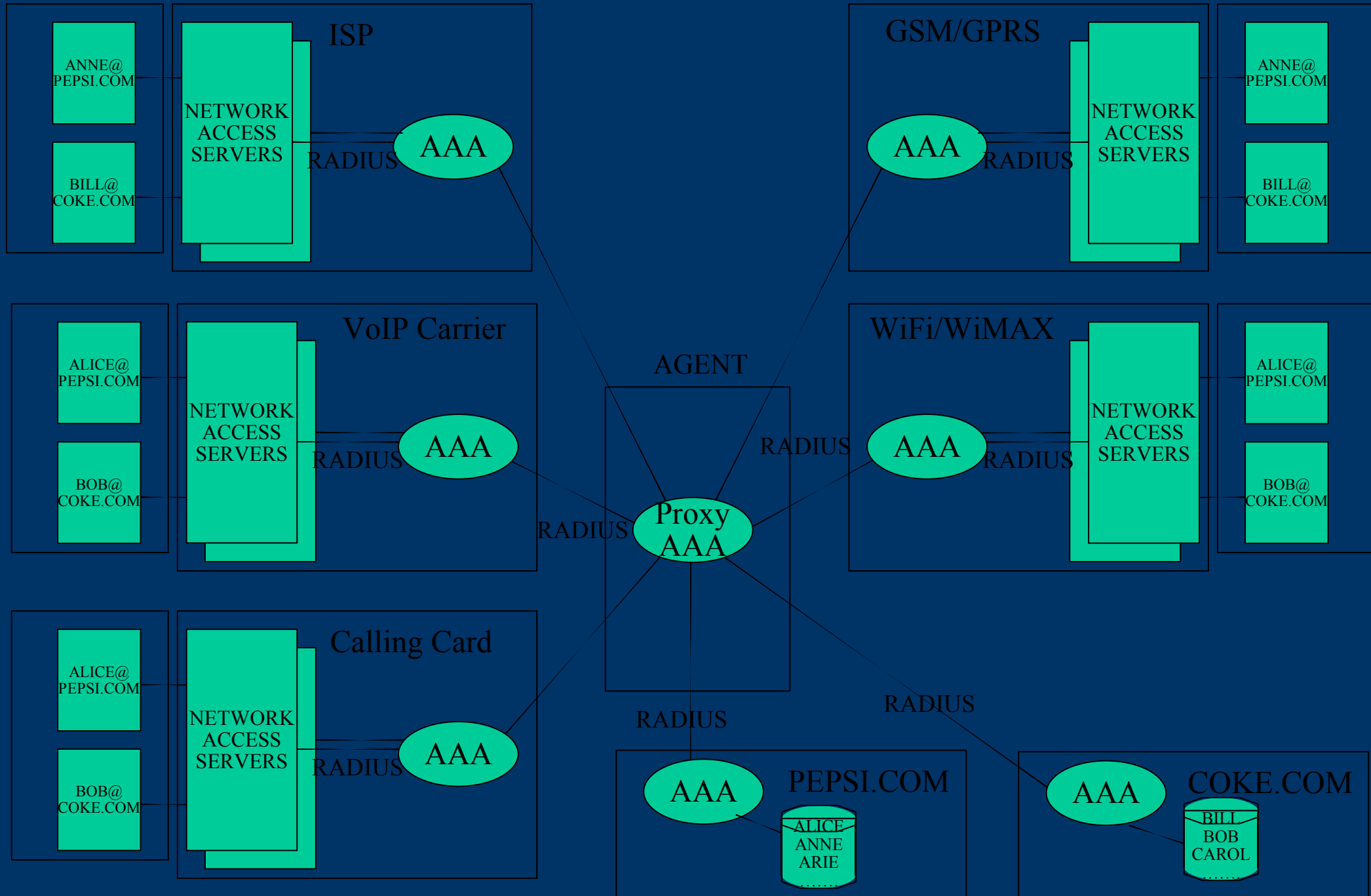


USER

SERVICE ORGANIZATIONS

SERVICE ORGANIZATIONS

USER



CDR Storage (Database of Choice)

PostgreSQL

- Rock Solid stability
- What goes in comes out again
- Excellent Date/Time handling
- Stored Procedures
- Transactions
- On-line Backups
- HA Replication



CDR Manipulation

Perl

- Extremely flexible
- Great text handling capabilities
- Easy to modify code
- We just love it ok!!!

Pg/PLSQL

- Built into Postgresql
 - Simple, easy to learn syntax
 - Fast
 - Used to abstract logic from client applications
-
-

RADIUS in Open Source Software

Apache

Asterisk

GNU Gatekeeper

Jabberd

OpenPBX.org

PAM

PPPD

PPTPD

SIP Express Router

Vovida B2BUA

Yate (Yet Another Telephony Engine)

RADIUS in Commercial products

- Check Point
 - Cisco
 - Juniper
 - Lucent
 - Microsoft
 - Newbridge
-
- Erm.. Actually, the list is too long so lets just take it as given that if a device connects to a network in some way it probably supports RADIUS...
-
-

RADIUS Authentication Request

User-Name = "peter"
User-Password = "donttellanyone"
Called-Station-Id = "suntel"
Calling-Station-Id = "902123369299"
Framed-Protocol = GPRS-PDP-Context
3GPP-IMSI = "286333340000281"
3GPP-Charging-ID = 22366668
3GPP-PDP-Type = 0
3GPP-Charging-Gateway-Address = 192.168.31.131
3GPP-GPRS-Negotiated-QoS-profile = "99-23921F9396979774F79797"
3GPP-SGSN-Address = 192.168.2.193
3GPP-GGSN-Address = 192.168.2.229
3GPP-IMSI-MCC-MNC = "28602"
3GPP-GGSN-MCC-MNC = "28602"
3GPP-NSAPI = "5"
3GPP-Selection-Mode = "0"
NAS-Port-Type = Virtual
NAS-Port = 60000
NAS-Port-Id = "GGSN"
Service-Type = Framed-User
NAS-IP-Address = 192.168.80.2
Client-IP-Address = 192.168.80.2

RADIUS Authentication Reply

Auth-Type = Accept

Framed-IP-Address = 10.11.8.10

MS-Primary-DNS-Server = 192.168.80.1

MS-Primary-NBNS-Server = 192.168.80.3

Session-Timeout = 300

OR

Auth-Type = Reject

Reply-Message = "Optional reply message"

RADIUS Accounting Start

Acct-Session-Id = "D91FE8E51545F62"
Framed-Protocol = GPRS-PDP-Context
Called-Station-Id = "suntel"
Calling-Station-Id = "902123369299"
Framed-IP-Address = 10.11.8.10
User-Name = "peter"
Acct-Authentic = RADIUS
Acct-Status-Type = Start
NAS-Port-Type = Virtual
NAS-Port = 60000
NAS-Port-Id = "GGSN"
Service-Type = Framed-User
NAS-IP-Address = 192.168.80.2
Acct-Delay-Time = 0
Client-IP-Address = 192.168.80.2
Timestamp = 1144900864



RADIUS Accounting Interim-Update

Acct-Session-Id = "D91FE8E51545F62"
Framed-Protocol = GPRS-PDP-Context
Called-Station-Id = "suntel"
Calling-Station-Id = "902123369299"
Framed-IP-Address = 10.11.8.10
User-Name = "peter"
Cisco-AVPair = "connect-progress=Call Up"
Acct-Session-Time = 288
Acct-Input-Octets = 2482
Acct-Output-Octets = 3170
Acct-Input-Packets = 36
Acct-Output-Packets = 31
Acct-Authentic = RADIUS
Acct-Status-Type = Interim-Update
NAS-Port-Type = Virtual
NAS-Port = 60000
NAS-Port-Id = "GGSN"
Service-Type = Framed-User
NAS-IP-Address = 192.168.80.2
Acct-Delay-Time = 0
Client-IP-Address = 192.168.80.2
Timestamp = 1144901152

RADIUS Accounting Stop

```
Acct-Session-Id = "D91FE8E51545F62"  
Framed-Protocol = GPRS-PDP-Context  
Called-Station-Id = "suntel"  
Calling-Station-Id = "902123369299"  
Framed-IP-Address = 10.11.8.19  
3GPP-IMSI = "286029240000290"  
3GPP-Charging-ID = 22306759  
3GPP-PDP-Type = 0  
3GPP-GGSN-Address = 217.31.232.229  
3GPP-IMSI-MCC-MNC = "28602"  
3GPP-GGSN-MCC-MNC = "28602"  
3GPP-NSAPI = "5"  
3GPP-Selection-Mode = "0"  
3GPP-Charging-Gateway-Address = 192.168.31.131  
3GPP-GPRS-Negotiated-QoS-profile = "99-23921F9396979774F79797"  
3GPP-SGSN-Address = 217.31.231.193  
3GPP-Session-Stop-Indicator = 0xff  
User-Name = "peter"  
Acct-Authentic = RADIUS  
Cisco-AVPair = "connect-progress=Call Up"
```

RADIUS Accounting Stop cont.

Acct-Session-Time = 141
Acct-Input-Octets = 1931
Acct-Output-Octets = 1718
Acct-Input-Packets = 20
Acct-Output-Packets = 7
Acct-Terminate-Cause = User-Request
Cisco-AVPair = "disc-cause-ext=No Reason"
Acct-Status-Type = Stop
NAS-Port-Type = Virtual
NAS-Port = 60000
NAS-Port-Id = "GGSN"
Service-Type = Framed-User
NAS-IP-Address = 192.168.80.2
Acct-Delay-Time = 0
Client-IP-Address = 192.168.80.2
Timestamp = 1144905076

Cool stuff to do with RADIUS

- Secure your Wireless network with WPA (Do this NOW!!)
 - Assign Wireless (and Wired) users into VLANs
 - Track user GPRS usage (Per KB pricing...)
 - Track user telephone usage (Per Min pricing)
 - Implement centralised AAA for all network equipment (No more password lists)
 - Assign DynamicDNS records to authenticated users automatically by integrating with PowerDNS (ie. “peter.softphone.suntel.com.tr”)
-
-

Thank you for flying with...

Peter Nixon

Suntel Commuincations

Web: www.suntel.com.tr

Mail: peter@suntel.com.tr

Jabber: peter@suntel.com.tr

VoIP: peter@suntel.com.tr

(Anyone notice a trend here?)

