Introduction to centralized Authentication, Authorization and Accounting (AAA) management for distributed IP networks

IETF 89 - Tutorials

London, England
March 2 - 7, 2014

Presented by: Lionel Morand

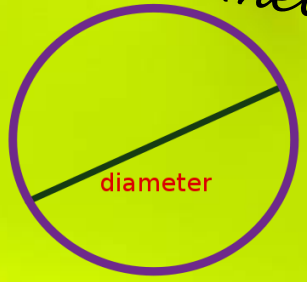
Co-authored by: Alan Dekok

x Introduction

x AAA Model

x RADIUS

x Diameter

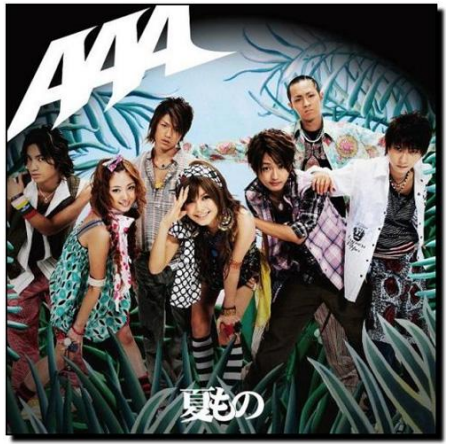


x Comparison

x Choosing a AAA Protocol

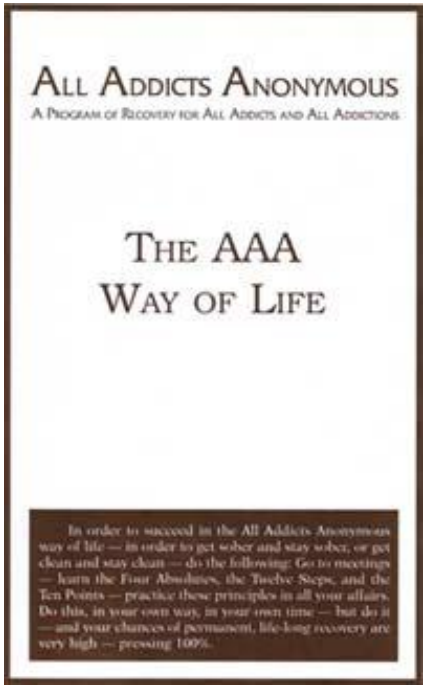

SINCE 1938
AAA
FESTIVAL
JULY 11-15, 2012
SHERATON CITY CENTER
BALTIMORE, MD
Guest Artist and Conductor of the 2012 AAA Festival Orchestra
STAS VENGLEVSKI
American Accordionists' Association
Member of the Confédération Internationale des Accordéonistes - CIA (IMC-UNESCO

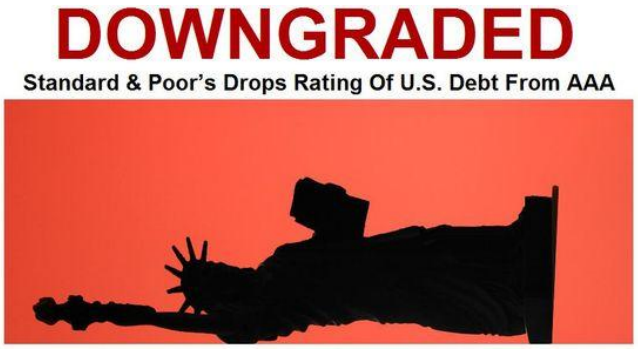

American
Accounting
Association


AAA
夏色の


Long Life
Camelion
Super Heavy Duty
1.5V AAA

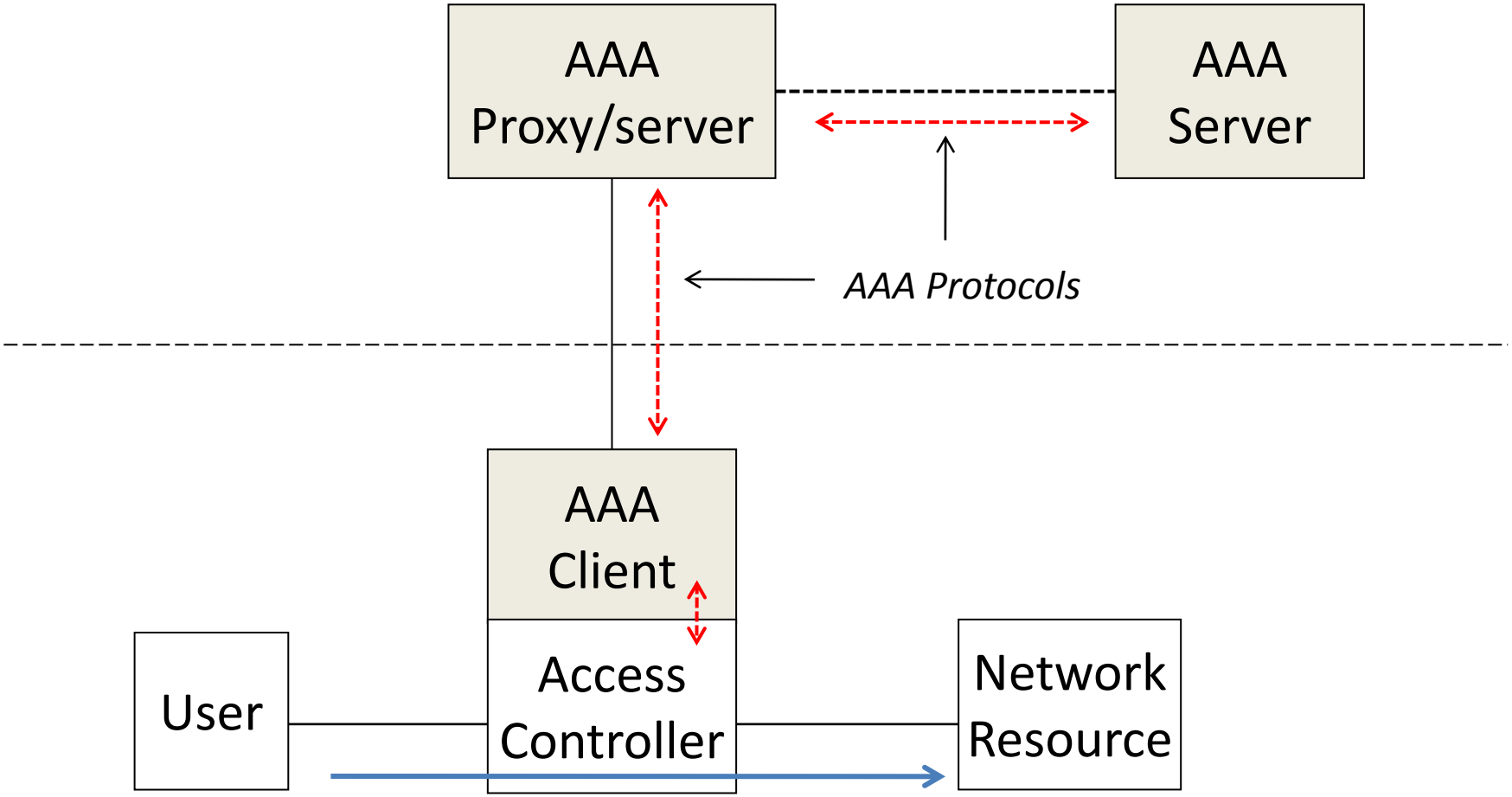

AMERICAN ARBITRATION ASSOCIATION
PANEL MEMBER 2013


ALL ADDICTS ANONYMOUS
A PROGRAM OF RECOVERY FOR ALL ADDICTS AND ALL ADDICTIONS
THE AAA
WAY OF LIFE
In order to succeed in the All Addicts Anonymous way of life — in order to get sober and stay sober, or get clean and stay clean — do the following: Go to meetings — learn the Four Absolutes, the Twelve Steps, and the Ten Points — practice these principles in all your affairs. Do this, in your own way, in your own time — but do it — and your chances of permanent, life-long recovery are very high — pressing 100%.


DOWNGRADED
Standard & Poor's Drops Rating Of U.S. Debt From AAA


BusinessDay
Moody's rea
AAA rating
December 2011

Generic 3-Tier "AAA" model



AAA… for Authentication

- Control user Identity
- Credentials provided by the user to prove his/her Id
- Examples of credentials:
  - passwords
  - one-time token
  - digital certificates,
  - or any other information related to the identity (e.g. biometric parameters.)

A**A**A… for Authorization

- Allowing access to specific types of service
- Authorization typically based on user authentication but not restricted to
- Access configuration based on user access rights and local policies.
- Examples of services:
  - IP address filtering
  - IP address assignment
  - Route assignment
  - Encryption
  - QoS/differential services
  - Bandwidth control/traffic management.

AA**A**… for Accounting

- Tracking of the consumption of network resources by users
- Typical information gathered in accounting report:
  - User Id (e.g. lionel@ietf89.com)
  - Service description
  - Data volume
  - Session duration, etc.
- Useful for management, planning, billing, etc.

AAA Protocols

- "AAA protocols" refers to IP protocols:
  - used to transport AAA related information
  - between the AAA client and the AAA server
  - in the back-end infrastructure
- "AAA protocols" does not include protocols used between the host and the AAA client (e.g. PPP)

Why use an AAA protocol?

- Why use AAA when we have Kerberos, OAUTH, etc.?
- AAA is almost entirely *pre-network access*
- Answers the questions of
  - Should this person be let on the network?
  - what should they be allowed to do?
- In many cases, a network is not available
  - No IPv4 or IPv6!
  - Just EAP, PPP, etc.

AAA is about a trust boundary

- AAA requires *trusted systems*
  - switches, access points, VPN concentrators, DSL concentrator, ASNGW, etc.
  - these systems use non-IP protocols to talk to a user.
- Other authentication protocols interact with untrusted systems, to authenticate a user
  - Some random IP is using OAUTH, that's fine. I can still authenticate the user.
  - then tie that authentication to an IP connection

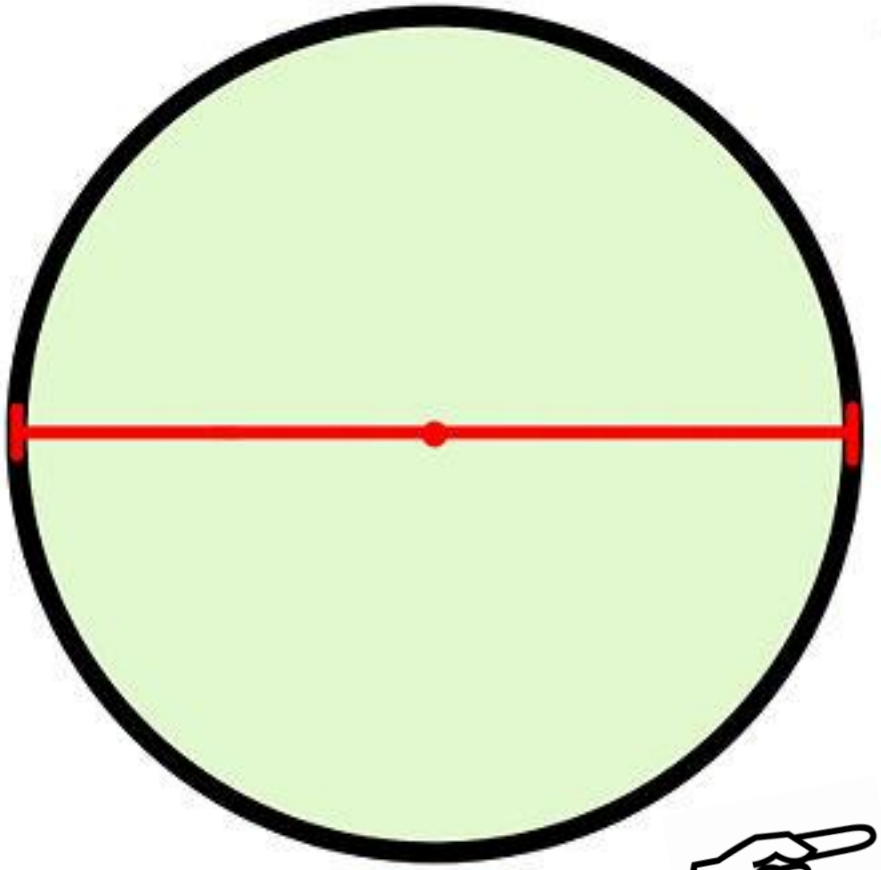
AAA is about a trust boundary (2)

- AAA - You have an "outside" and an "inside", and need to let "outside" users appear on the "inside" network
- Others - random IP addresses need access to services on a system with a public IP address
- A public system may use AAA on the back end to authenticate a user.
  - But the user is untrusted, so he/her can’t use an AAA protocol
  - The public system can be trusted by an AAA server

AAA Protocols in IETF

- 2 IETF standard protocols
  - RADIUS (RFC 2865) – The first one…
  - Diameter (RFC 6733) – the successor… or so…

- *NOTE: other solutions proposed as AAA protocol but not standardized by IETF.*
  - *TACACS (Terminal Access Controller Access Control System)*
  - *TACACS+: enhanced TACAS version developed by Cisco*
    - *Still used in Unix environment for remote user authentication and router configuration*



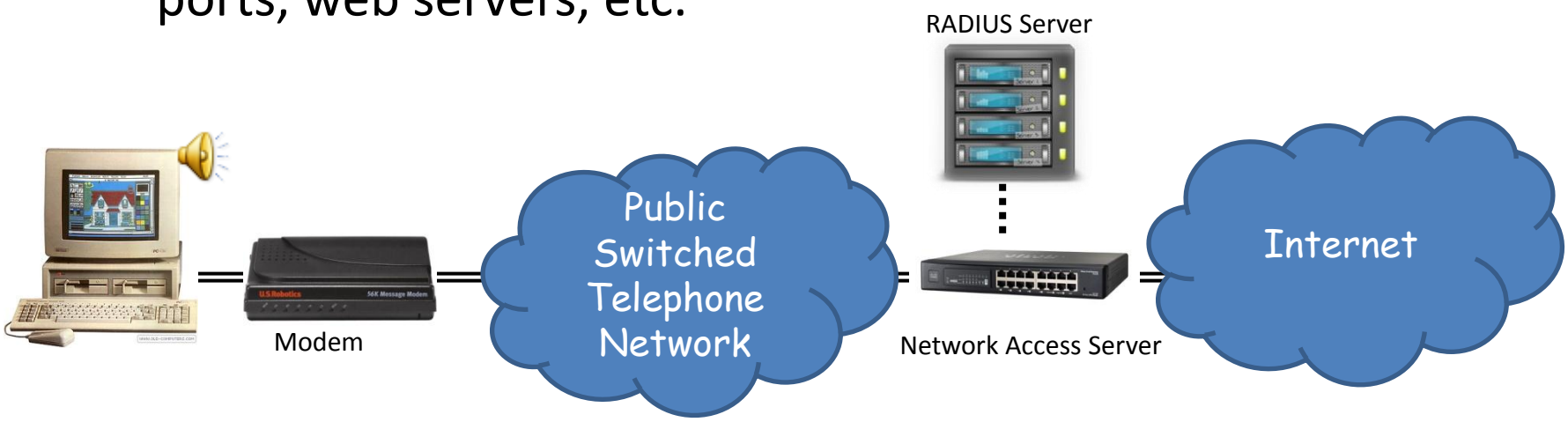
diameter

$$r = \frac{d}{2}$$

radius

RADIUS

- Remote Authentication Dial In User Service (RADIUS)
  - developed in 1991 but first RFCized in 1997
- Widely deployed by ISP and enterprises to control access to Internet or internal networks/services
  - including modems, DSL, Wi-Fi access points, VPNs, network ports, web servers, etc.



RADIUS and PPP

- RADIUS is initially designed to interoperate with the Point-to-Point Protocol (PPP – RFC 1661) used to encapsulate IP packets over a phone line.
  - **PPP** enables data link set-up between two endpoints (modem) and provides mechanisms for authentication, data encryption and compression.
  - **RADIUS** is used to transport user credentials received over PPP to an authoritative server that will grant access to the user based on successful authentication.

Authentication Protocols

- Authentication mechanisms defined for PPP are reused over RADIUS
  - **PAP** (Password Authentication Protocol),
    - User's username/password provided in clear text to the NAS.
  - **CHAP** (Challenge-handshake Authentication Protocol),
    - A challenge/response mechanism based on MD5 algorithm
    - The user must provide a response calculated based on the password and a random value received from the network
  - **EAP** (Extensible Authentication Protocol)
    - An authentication framework, not a specific authentication mechanism
    - It provides some common functions and negotiation of authentication methods called EAP methods.

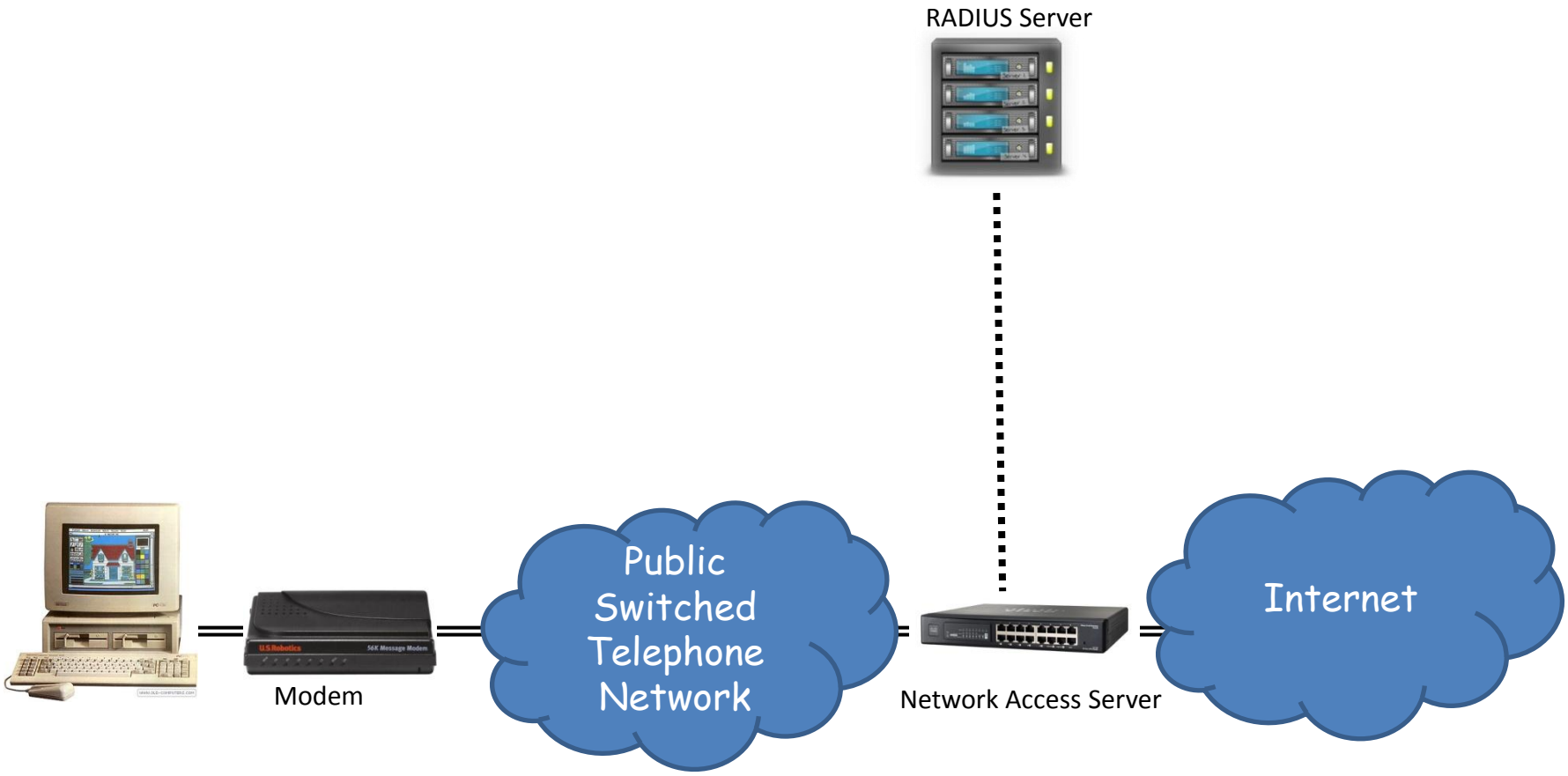
RADIUS as per RFC2865/2866

- Simple and efficient solution for AAA
  - Client/server model
  - UDP transport
  - Authentication and Authorization combined in a single transaction (RFC 2865)
  - Accounting report sent at the beginning and the end of the access session (RFC 2866)
  - Information data carried in Attributes in the TLV format (|Type|Length|Value…|)
  - Simple routing based on pre-configured IP address

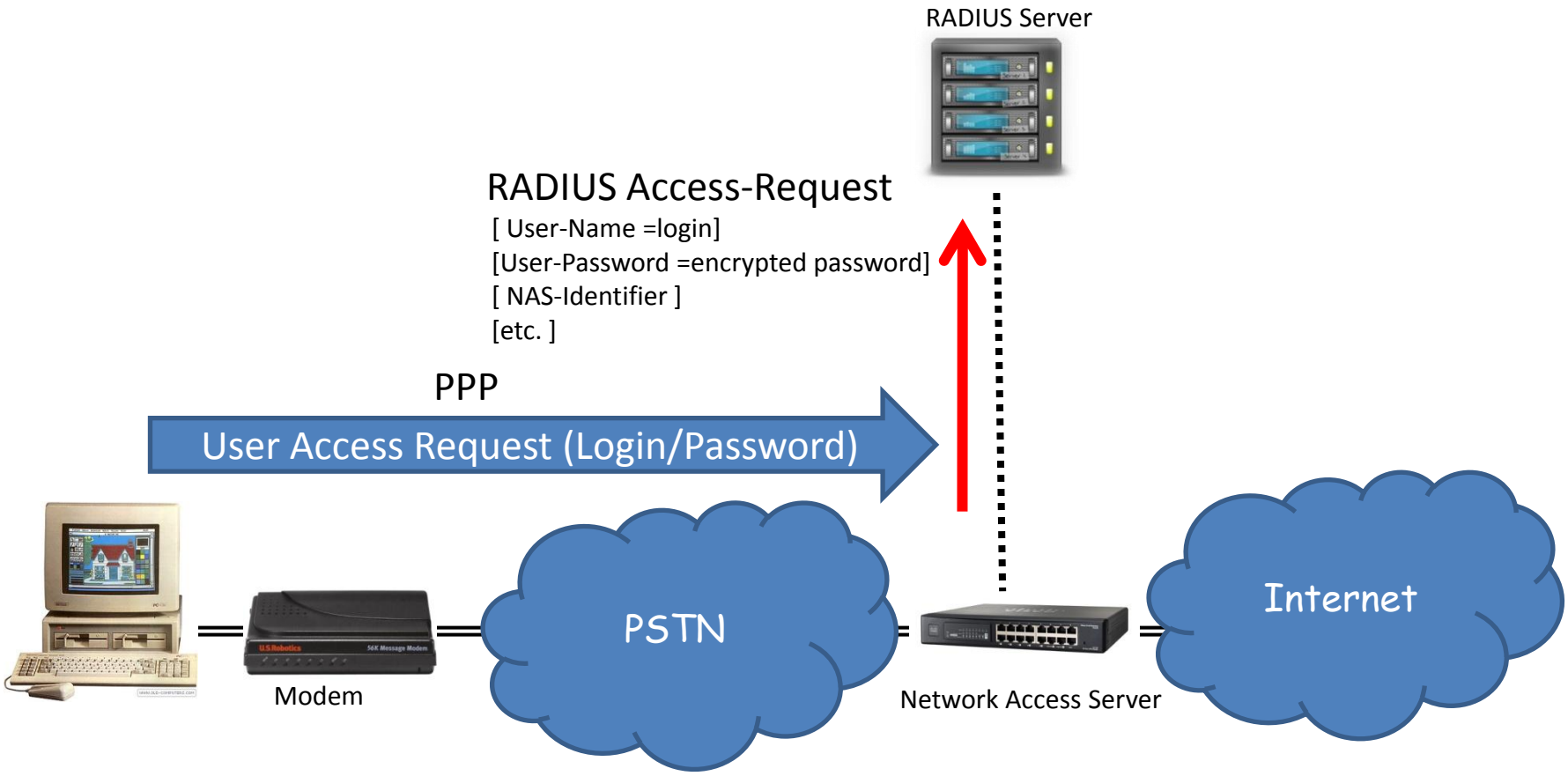
RADIUS Security

- A secret is shared between client and server
- Used to generate cryptographic hash values (using MD5) to authenticate RADIUS messages
- Used also to encrypt the user password between the client and the RADIUS server
  - The user's password is never sent in clear-text in the network.

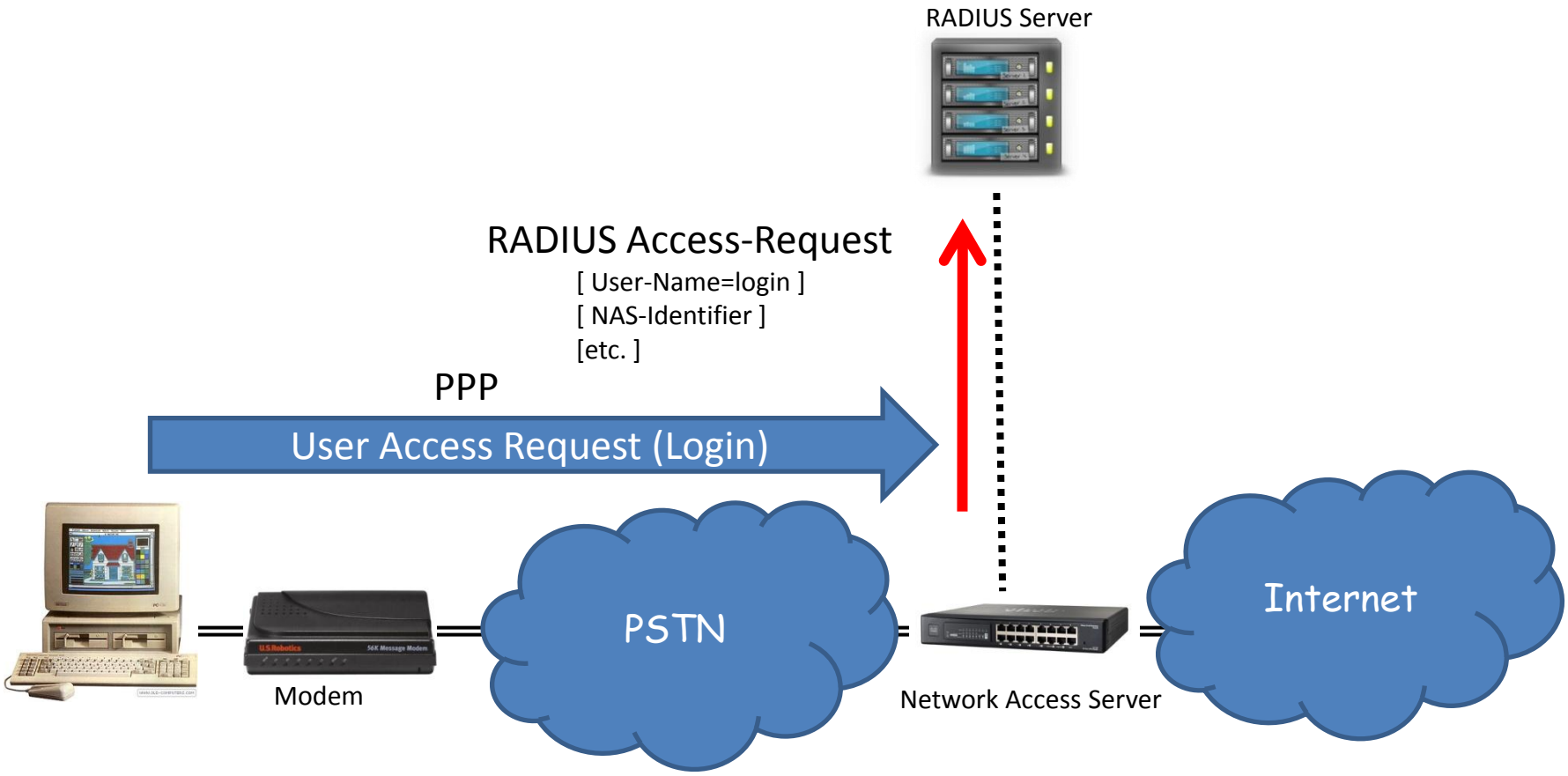
Dial-In Access Control



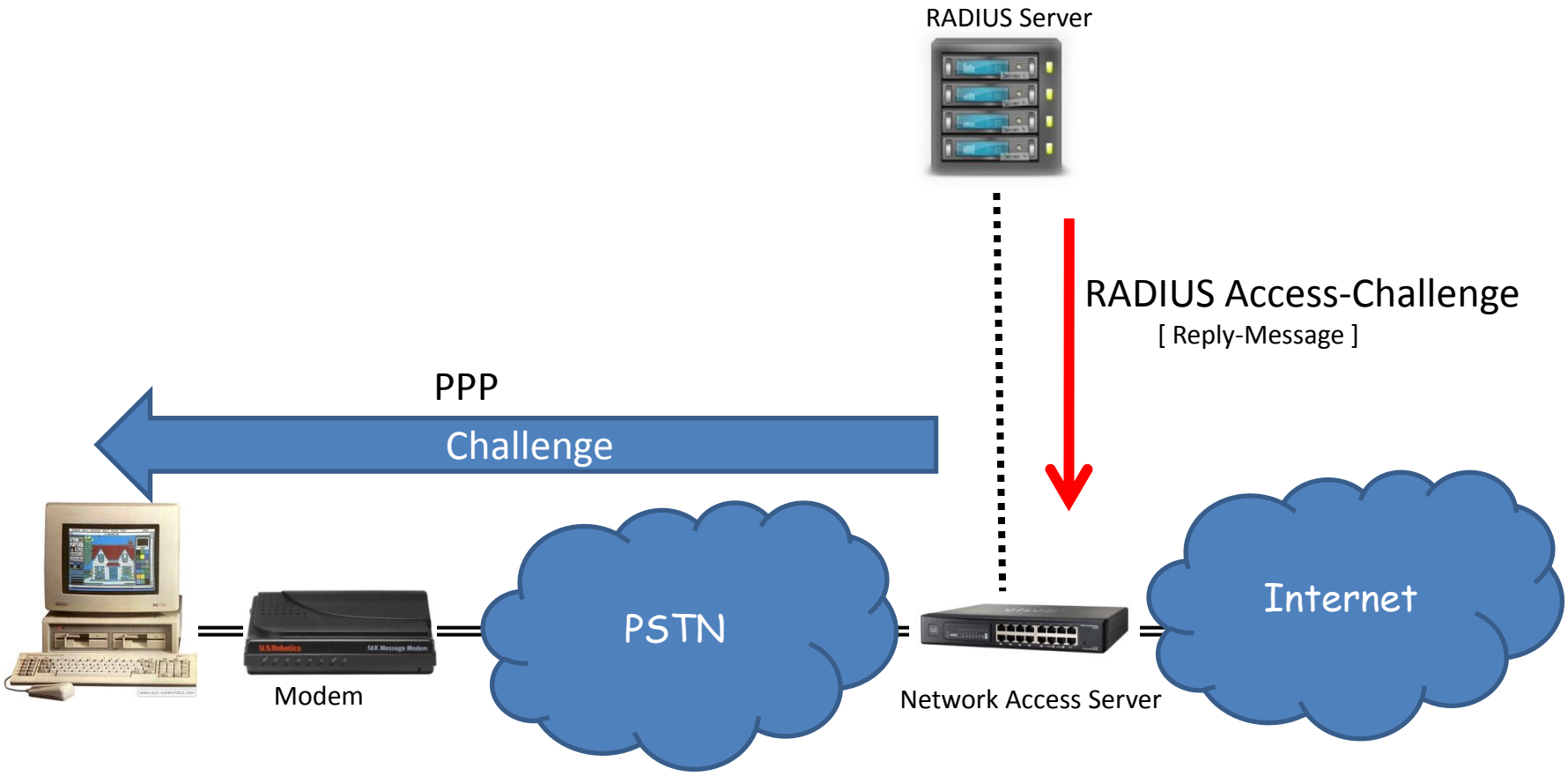
Access-Request 1/2



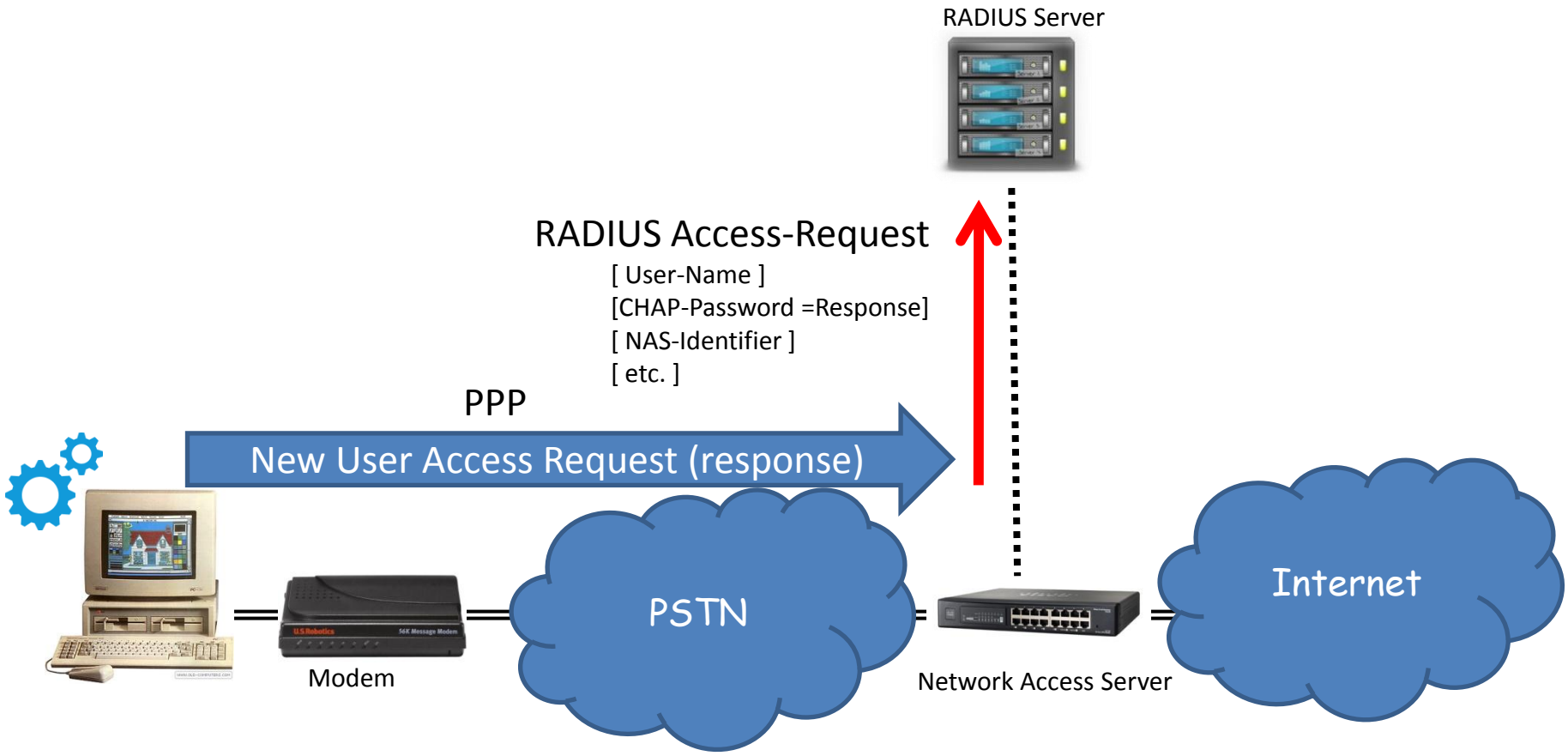
Access-Request 2/2



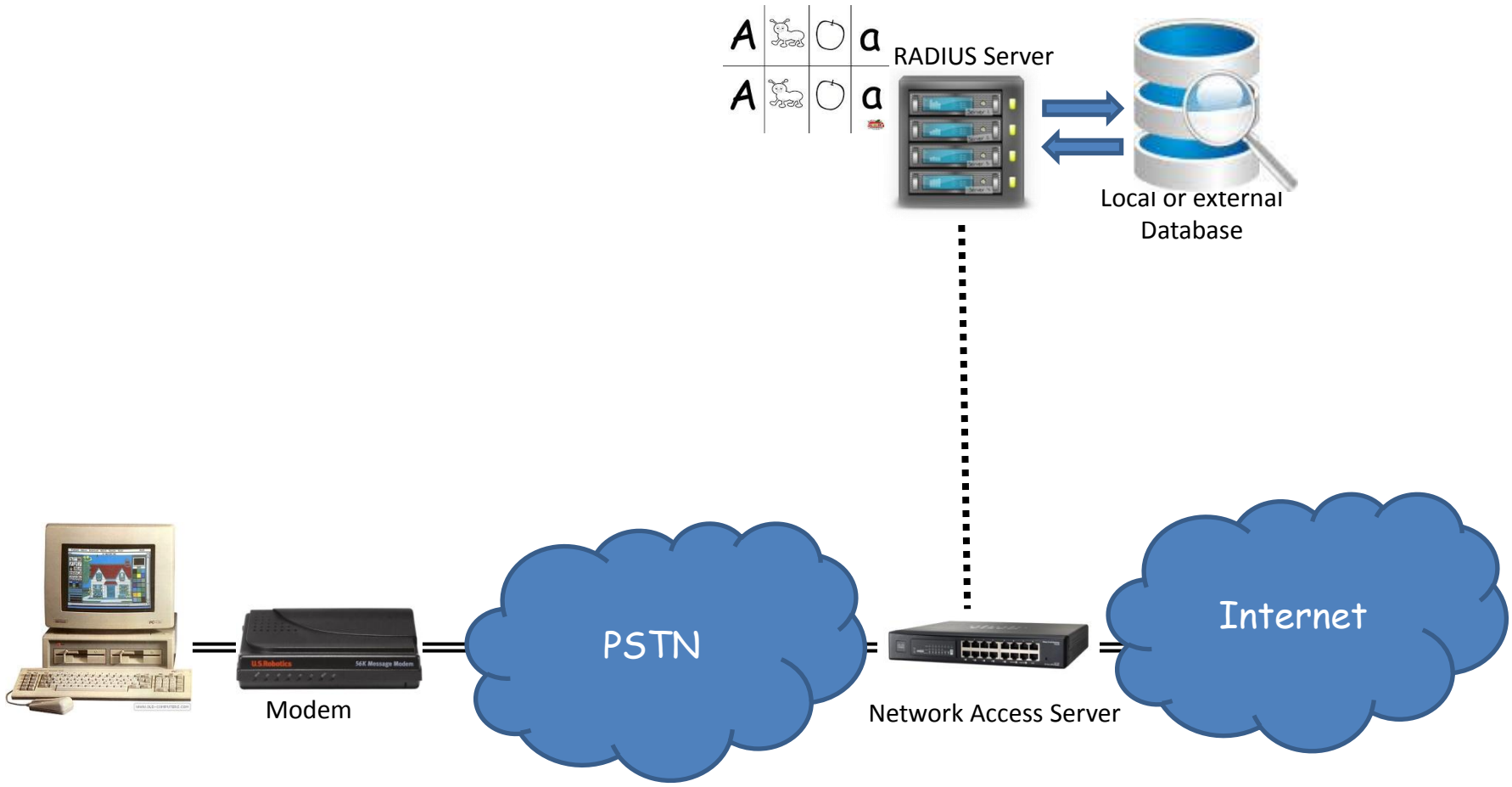
Access-Challenge



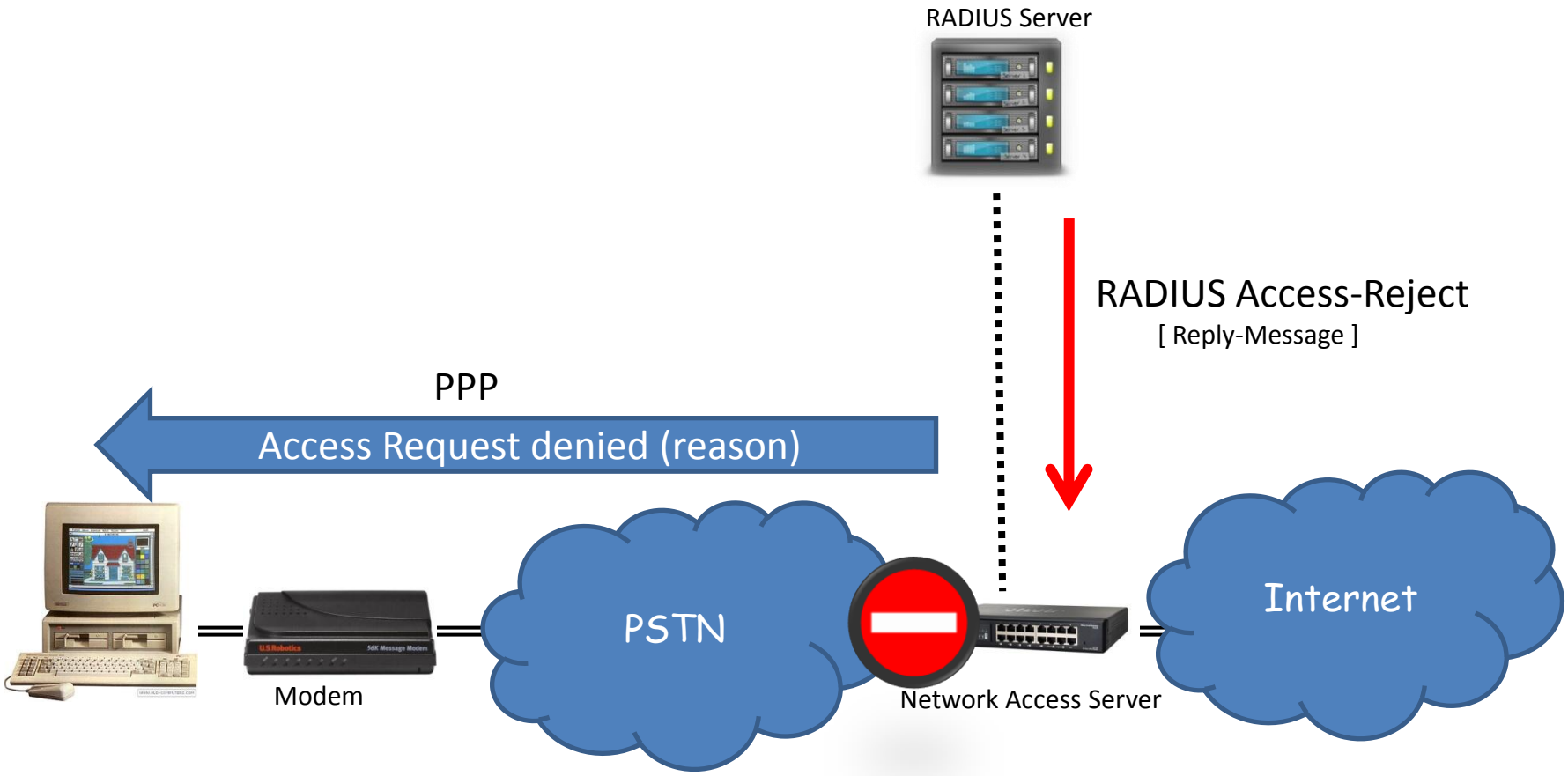
Challenge Response



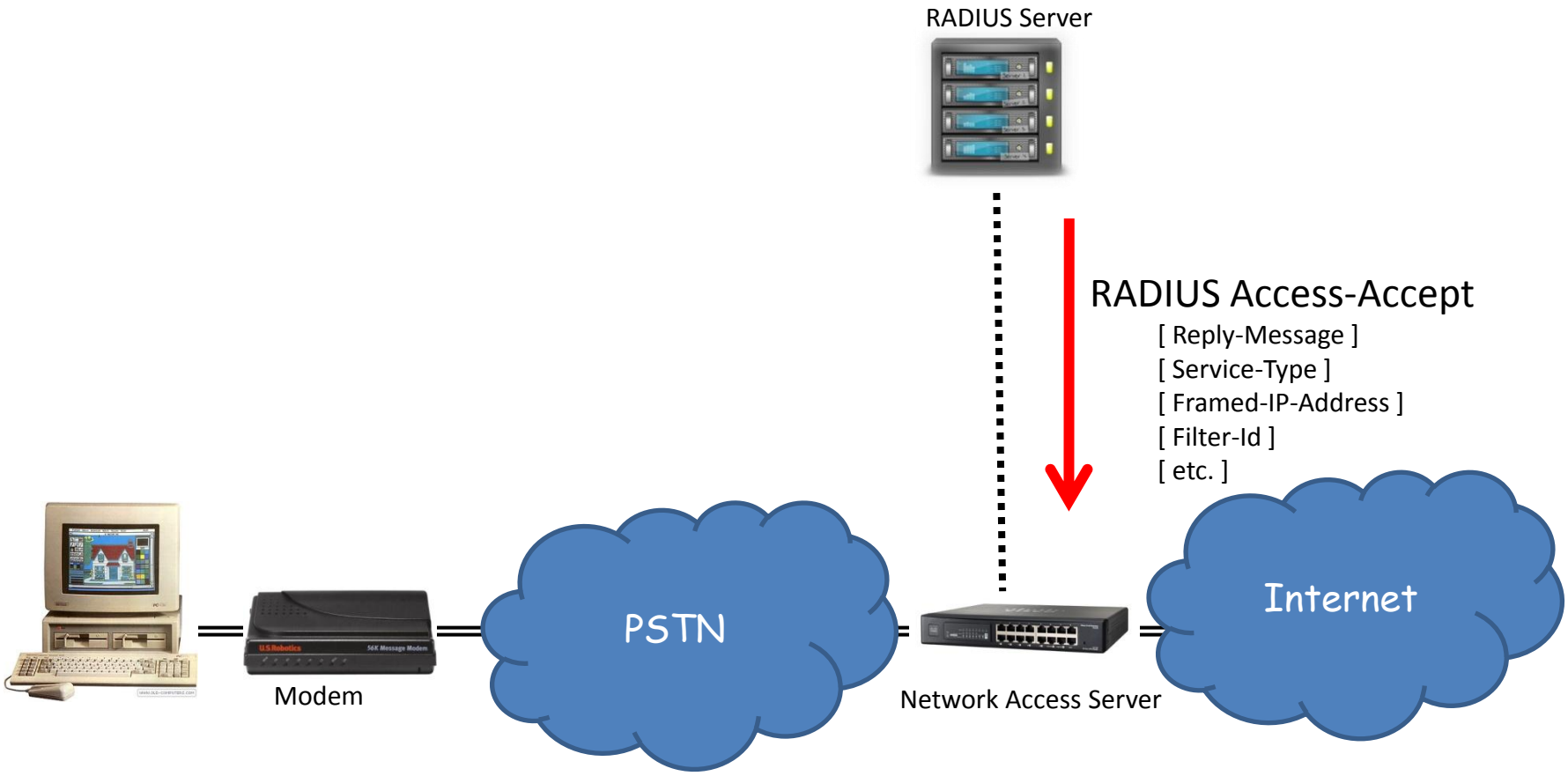
Authentication & Authorization



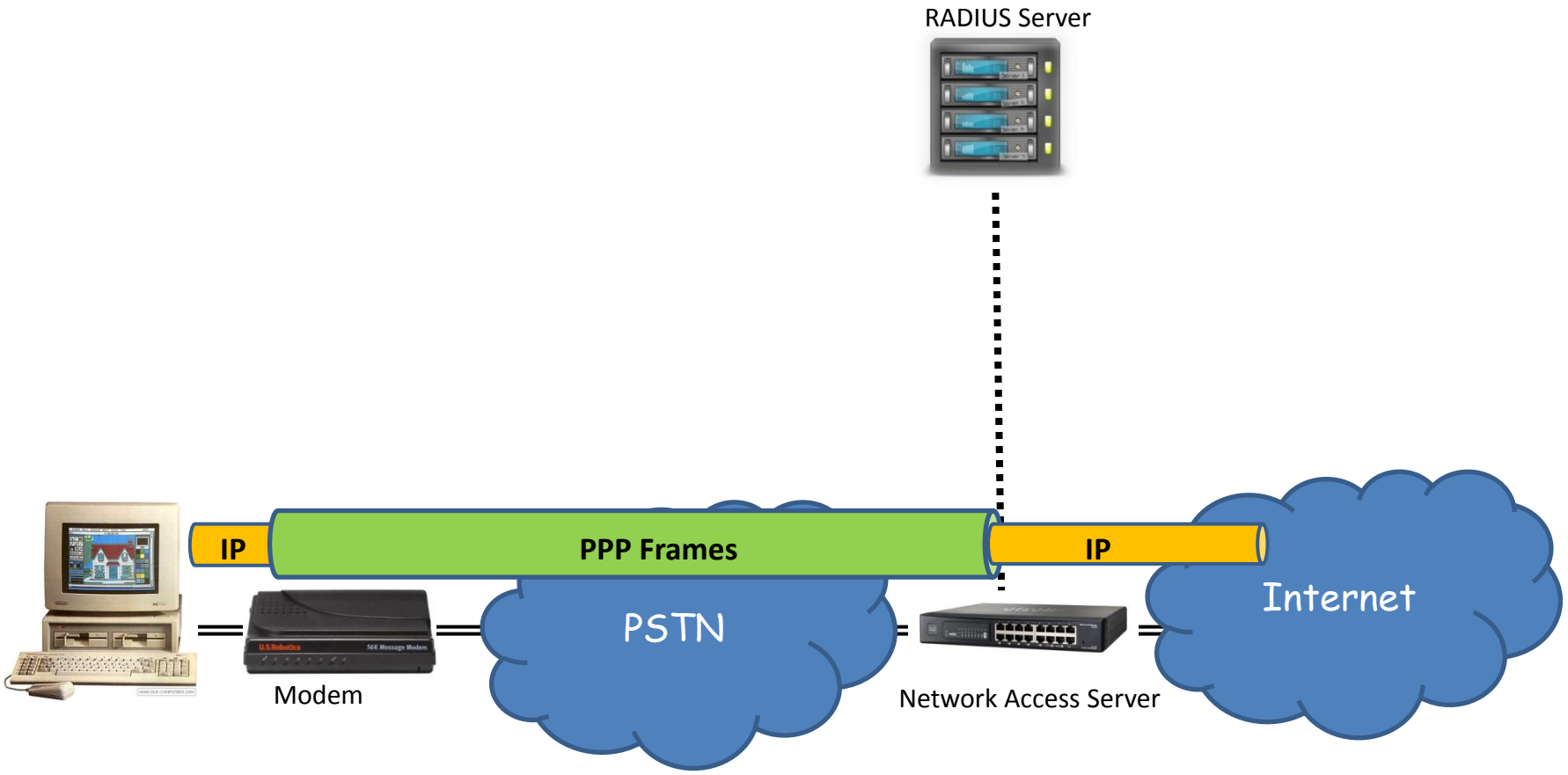
Access-Reject



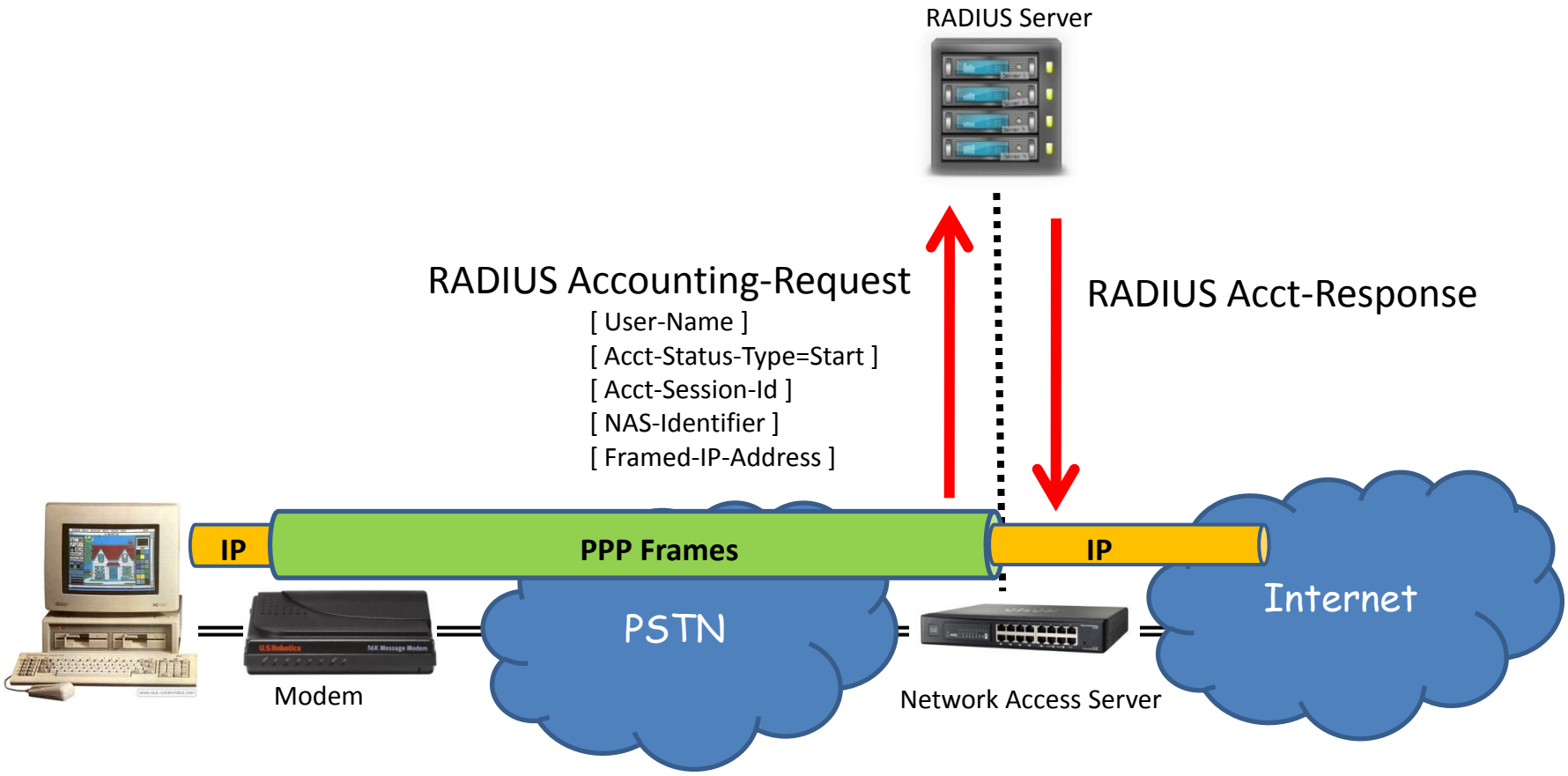
Service Configuration



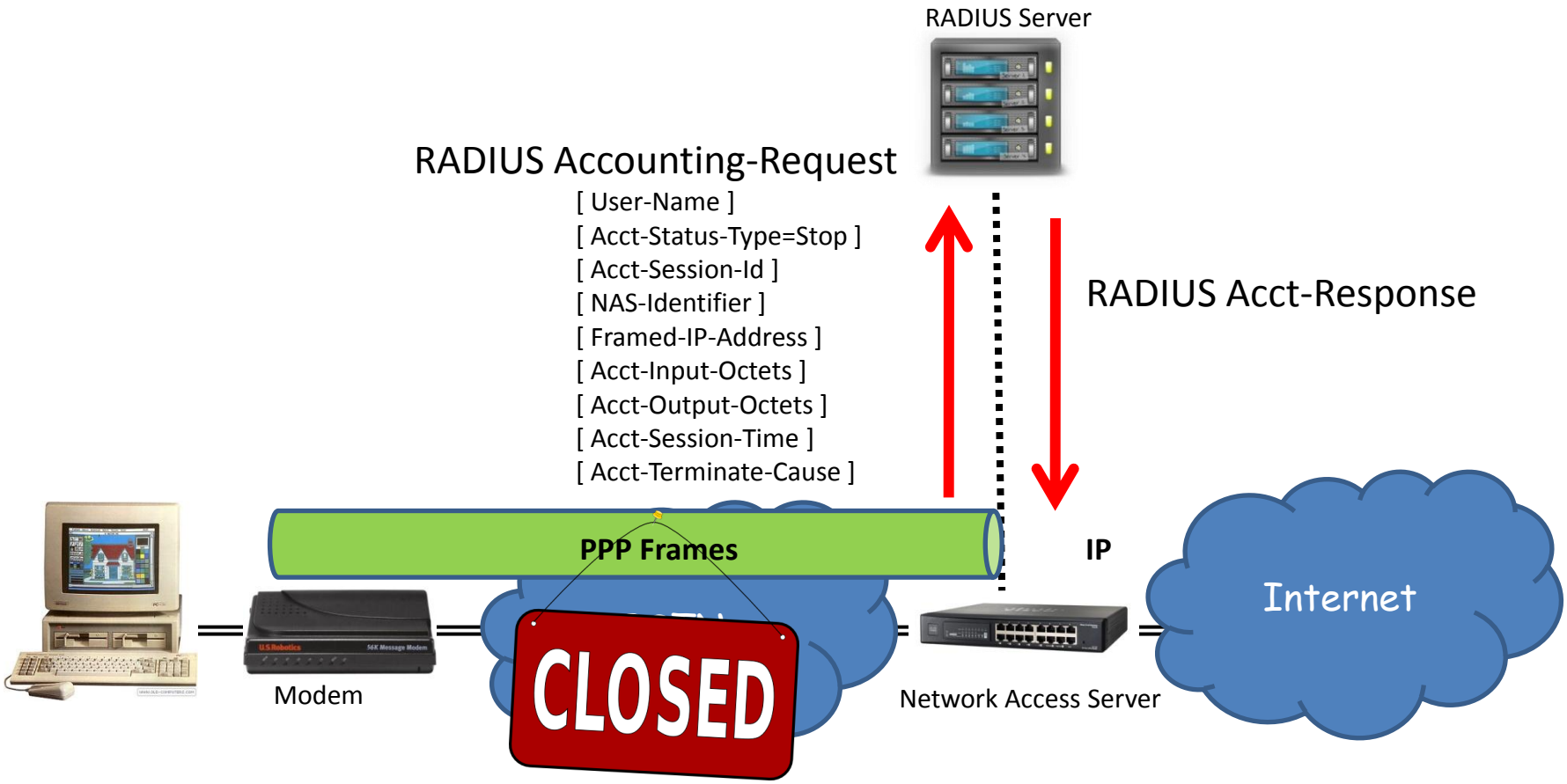
Start of service delivery



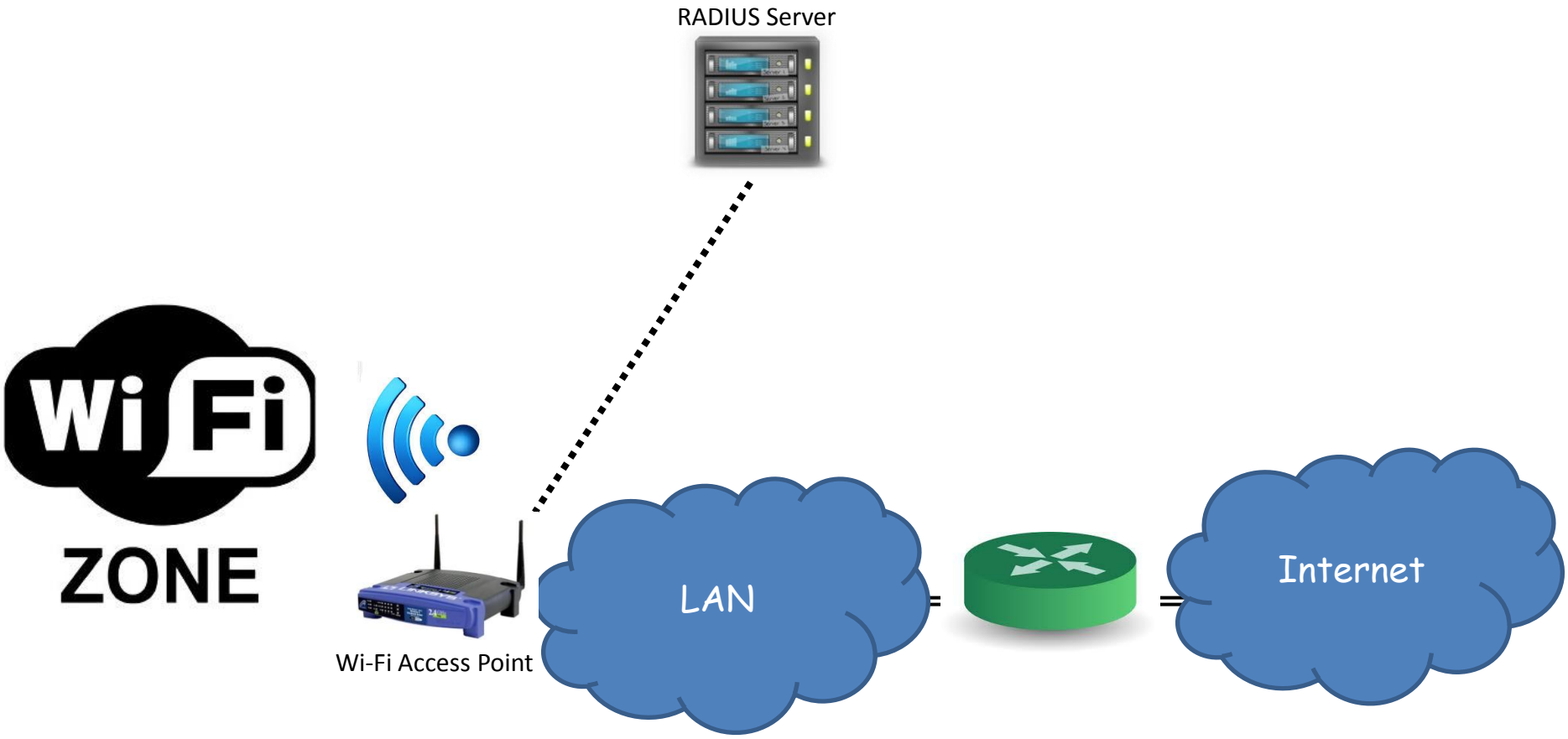
Accounting-request (START)



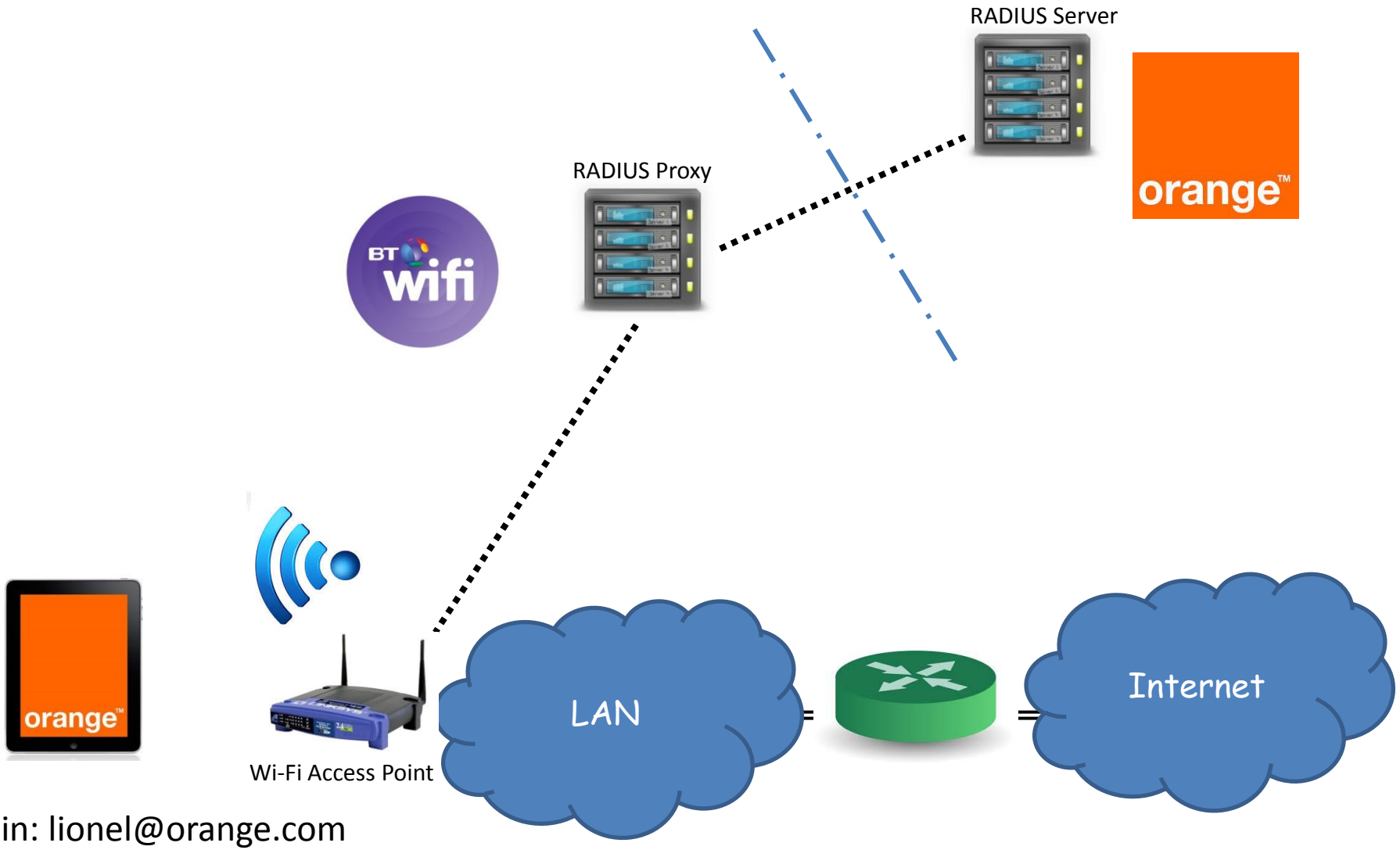
Accounting-Request (STOP)



Wi-Fi Hotspot



Roaming Agreements

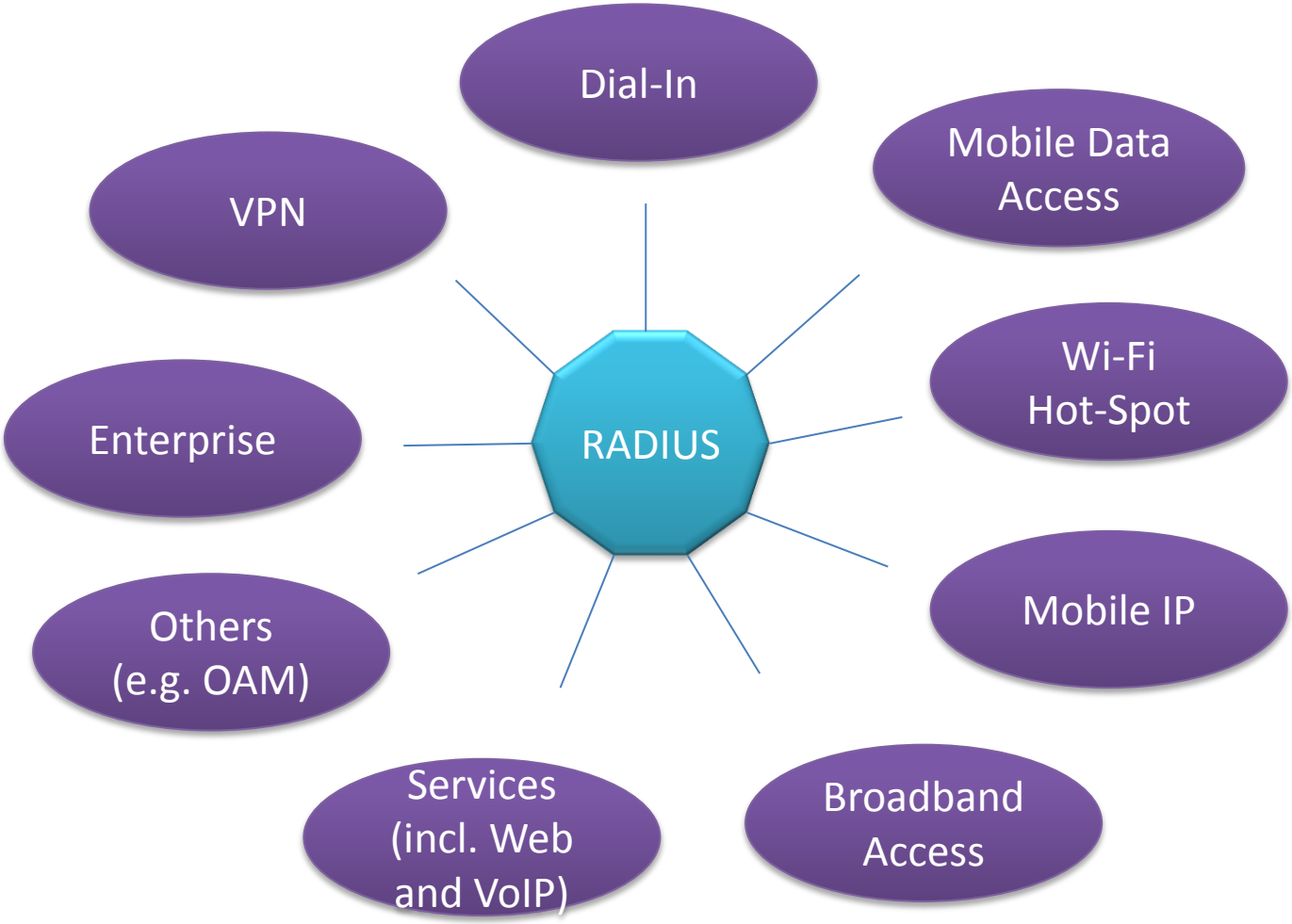


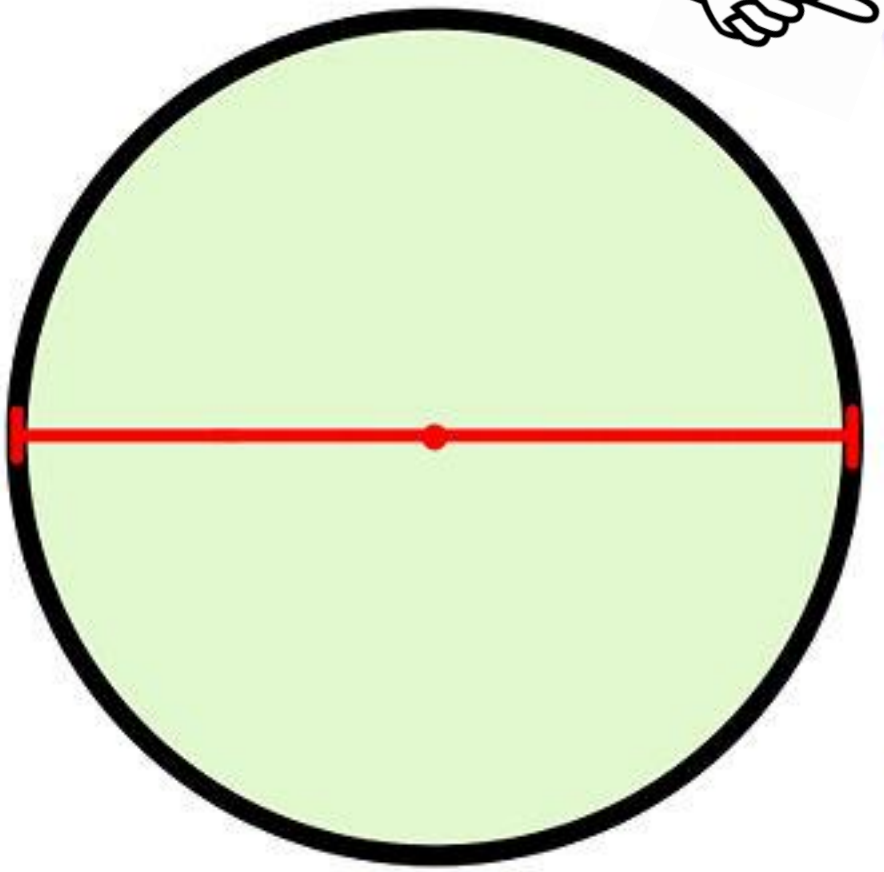
Login: lionel@orange.com

Key: RADIUS Extensibility

- New standard attributes standarized by IETF
  - but only 256 standard attributes can be defined
- RADIUS wide adoption due to the "Vendor-Specific" attribute
  - Freely used by vendors to encapsulate their own extended attributes (up to 256 per vendor)
  - unrecognized vendor-specific attributes are simply ignored by servers
- New messages need IETF Standards Action
  - but incompatible with existing RADIUS implementations

RADIUS Ubiquity





diameter

$$r = \frac{d}{2}$$

radius

Back to the Future

- RADIUS RFC 2865 published in 2000
  - Designed as simple/efficient solution for access control in size-limited networks
- but with limitations regarding new AAA service requirements:
  - IP Mobile management, Roaming operations, enhanced access control, etc.
- Need for new capabilities
  - Server-initiated messages, re-auth during session, realm-based routing, reliable and secure transport, bigger packets for more complex policies, etc.
- Need for a new protocol: Diameter

Diameter…

- Diameter was designed to be the successor of RADIUS
- Diameter = Twice the RADIUS
- So Diameter is not an acronym!!!

Diameter Objectives

- Designed as an enhanced version of RADIUS
- Designed to be a general framework for any AAA applications
- Features inherently offered by Diameter
  - Peer-to-peer protocol
  - Reliable and secure transport
  - Failover
  - Agent support
  - Server-initiated messages
  - Capabilities negotiation
  - Dynamic Peer discovery and configuration

Diameter Design

- A Reliable Transport layer
  - TCP or SCTP connection with TLS, DTLS or IPsec
- Set of common commands and Attribute-Value-Pairs (AVPs) supported by any Diameter peer, used for:
  - Dynamic peer discovery and Connectivity management
  - Dynamic routing based on Realm
  - Session management
  - accounting
  - Basic error handling
- A set of Applications used in extension of the Base protocol for specific purposes

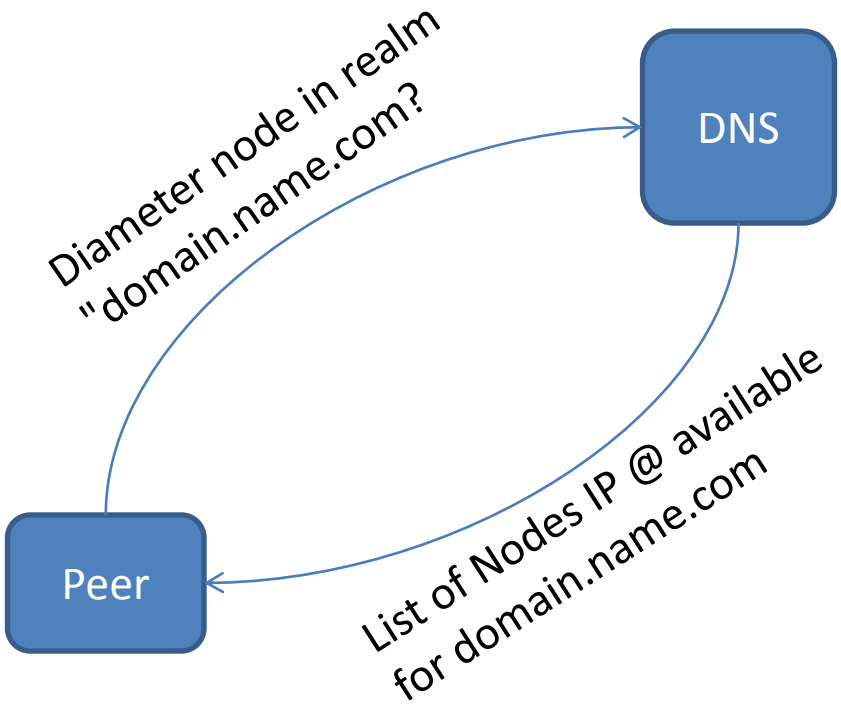
Diameter Applications

- Extension of the base protocol
  - specific commands and AVPs for specific functions
  - New specific errors
- One application uniquely identified by IANA-assigned Id
  - used to specific processing of the commands.
  - App-Id "0" assigned to the Base protocol
  - App-Id "3" for EAP or App-Id "6" for SIP
- A given Diameter peer supports only the required set of applications to serve the user

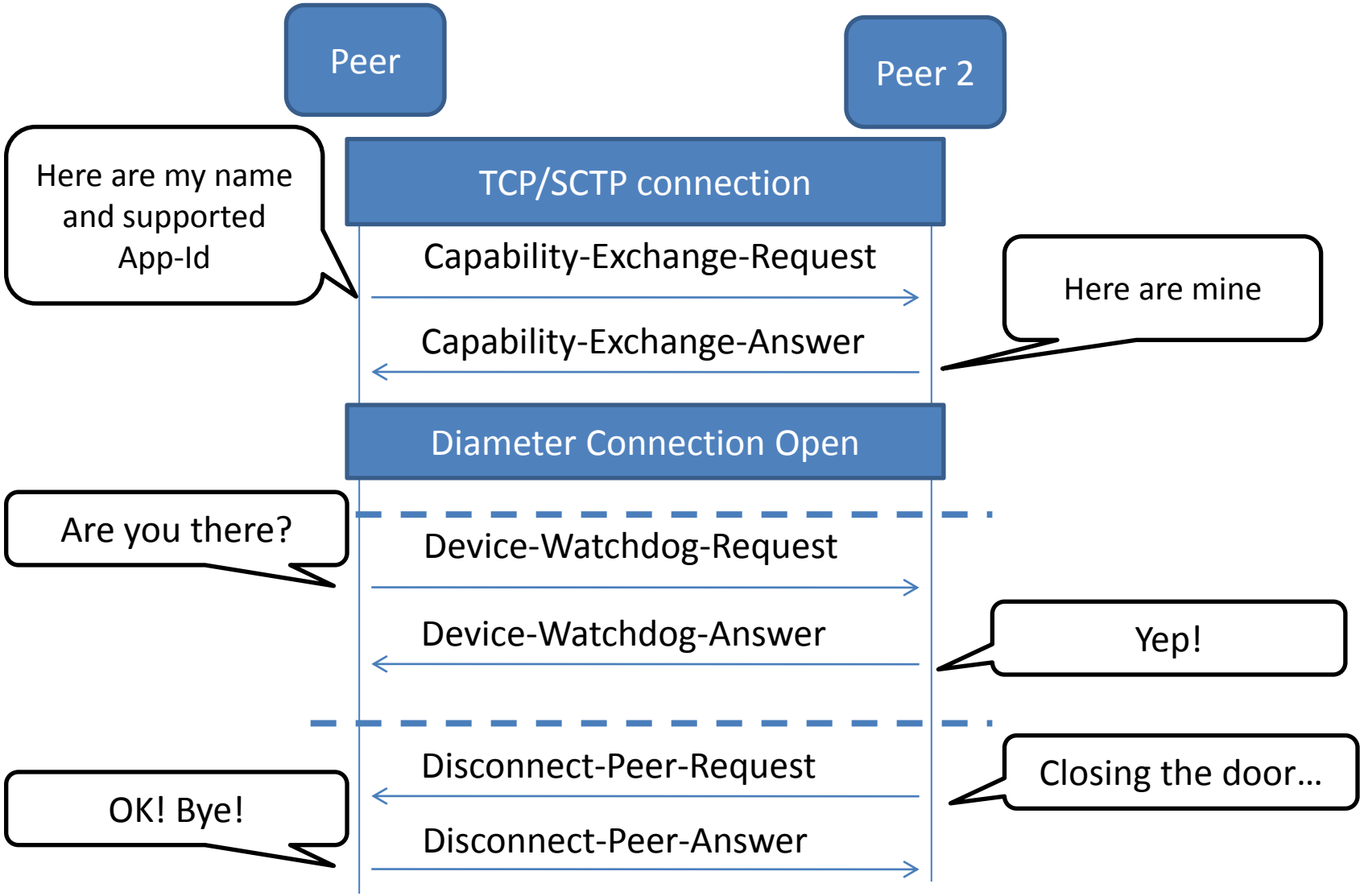
Peering

- Use DNS to discover neighbours
- Set-up transport connection
- Exchange Diameter ids and capabilities (Appl-ids)
- Update local routing tables
- Keep-alive mechanism to monitor Diameter peer connection

Peer Discovery



Diameter Peering



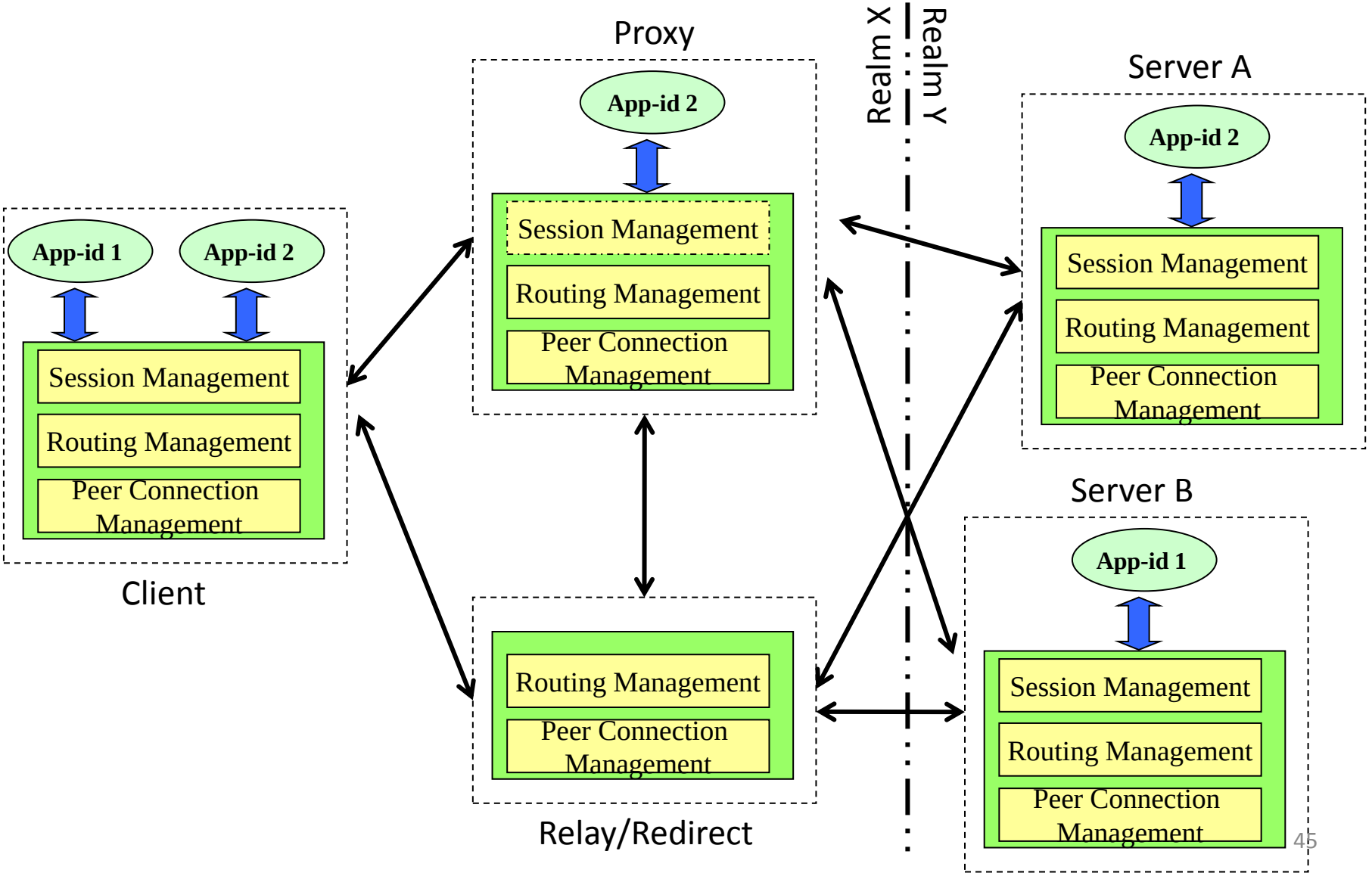
Diameter Security

- TLS, DTLS or IPsec are used to protect Diameter peer connections.
- Diameter nodes are mutually authenticated as part of TLS/TCP, DTLS/SCTP or IPsec connection establishment.
- All Diameter messages will be sent through the connection only after a successful secure connection setup.

Diameter Agents

- Besides traditional client and servers:
  - Relay Agents: forward messages to other Diameter nodes based on routing decision performed using a list of supported realms, and associated known peers.
  - Proxy Agents: Relay function + messages modification to implement policy enforcement.
  - Redirect Agents: return information necessary for Diameter agents to communicate directly with another Diameter node.
  - Translation Agents: provides translation between two protocols (e.g., RADIUS<->Diameter)

Diameter Architecture



Realm-based Routing

- As for emails or SIP
  - messages sent first to a domain
  - forward then to a host in the domain
- Hop-by-hop routing using two tables maintained by each Diameter node:
  - Routing table: peer to contact to reach a domain for given application
  - Peer table: connection to use to reach the peer

Realm-based Routing

- It is up to the Application the domain name to use in the request
  - Usually retrieved from the User id. (e.g. lionel@ietf89.com)
- If the destination node is freely selected in the Destination realm, no need of Diameter node identity in the request
- The answer always follows the path of the corresponding request

Diameter Session

- A Session identifier is used by client and servers to correlate a Diameter message with a user session.
  - Session identifier generated and inserted in the first message related to a user session
  - subsequent messages relating to the same user's session used the same session id.
- Session-Id is globally and eternally unique
  - Starting with the id of the peer initiating the session + a unique random value

Standard vs. Vendor-Specific

- Diameter extended by new application, command, AVP or error codes
- Capability exchange and pre-defined error handling ease coexistence of standard and vendor-specific extensions
  - unique values ensured by IANA assignement or namespaces defined under a vendor-id
  - Default behaviour is defined for unknown values

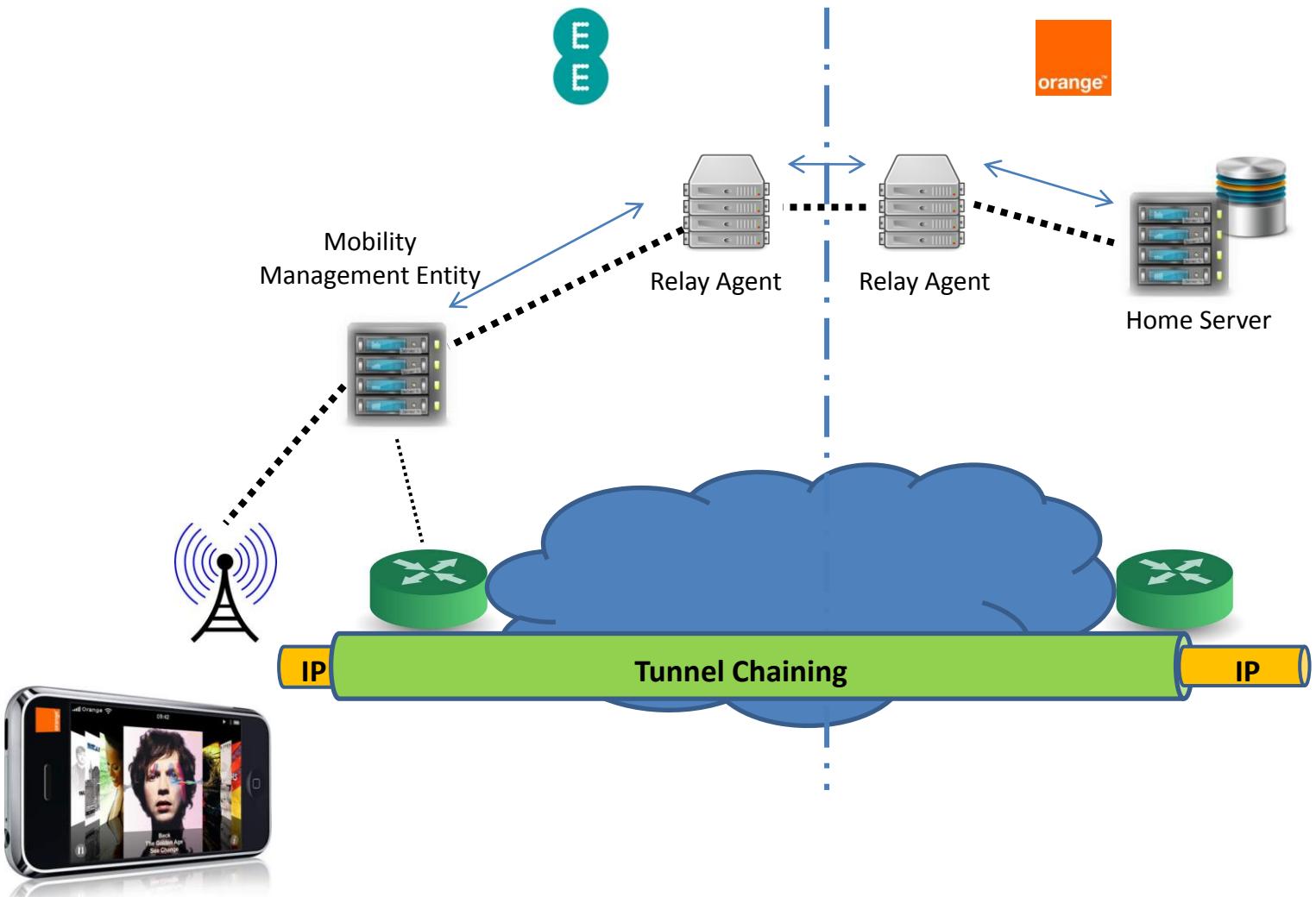
Diameter More than AAA

- Diameter extensibility allows to define any protocol above Diameter base protocol.
- Authentication, authorization and accounting may be handled separately and independently.
- Additional functionalities relying on AAA infrastructure may not even be related to AAA
  - Can be used for any procedure based on Request/answer model

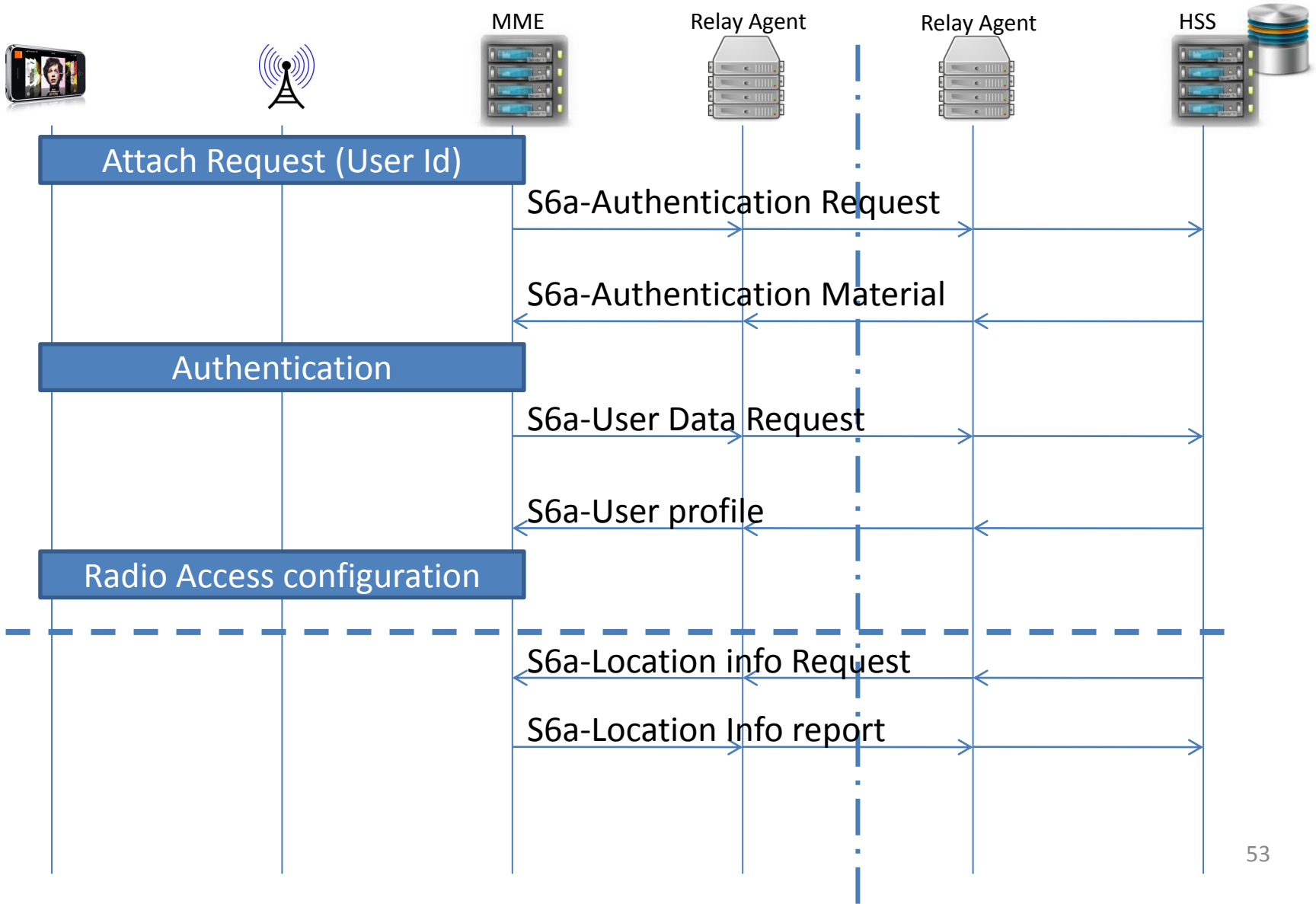
Diameter Adoption

- 14 Diameter applications defined in IETF
- About 110 vendor-specific applications
  - Most of them defined by external SDOs, identified by a specific vendor-id (e.g. 3GPP or WiMAX)
- Diameter is now the main protocol used in the control signalling plan in 4G mobile networks
  - more than 30 3GPP-defined applications used for mobility management, QoS/Charging… or even SMS transport

4G LTE (or a kind of)

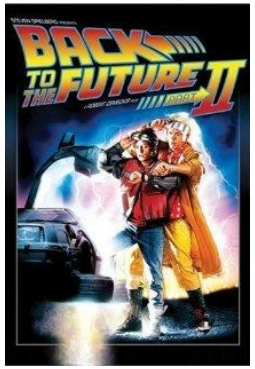


4G LTE Attachment




Today

Back to the Future (Part II)



- Diameter designed to "obsolete" RADIUS
- But RADIUS is still alive… and even stronger!
- RADIUS extensions have been defined, e.g.
  - Server-initiated messages
  - RADIUS over TCP for reliability
  - RADIUS over TLS for security
  - soon, Realm-based DNS server discovery, etc.
- Equivalent solutions for AAA today in IETF?

History

- 1997: RADIUS as RFC (RFC 2058)
  - originally developed by Livingston Enterprises for their PortMaster series of Network Access Servers
- **2000: RADIUSv2 (RFC 2865)**
  - Closed some issues of the first version widely implemented
  - **Acknowledgement of issues when used in large scale systems**
  - Dedicated IETF's AAA working group to develop a successor
- 2000: Set of new requirements for generic AAA architecture
  - Main drivers: roaming, Network access requirement enhancements, Mobile IP
- 2001 (February): first draft of the Diameter base protocol
- **2003: Diameter Base Protocol as RFC (RFC 3588)**
- 2005 -2006: Feedback from **first operational deployment** (IMS, CDMA2000, etc.)
  - and first IOT issues
- 2008: Diameter Extensibility and Diameter Routing Design teams
  - Clarification of the **rules for extensibility/routing**
- **2012: Diameter base protocol RFC-bis (RFC 6733)**
  - Not a new version of the protocol. Mainly clarifications
- **2013: RADIUS Protocol Extensions (RFC 6929)**
  - extend RADIUS with new attributes, new data types

RADIUS vs. Diameter

- Why does the IETF have two standards doing the same thing?
- Why use one protocol over another?
- What will happen in the future?

Recent RADIUS

- New RADIUS standards stopped for a while as Diameter was being developed
- RADEXT was for doing minor tweaks
- which got more major over time
- more than 256 attributes, 253 octets, etc.
- TCP, TLS, DTLS, dynamic DNS, etc.
- some standard / experimental / informational

What happened?

- Many minor tweaks to RADIUS which made it closer to Diameter
- Diameter always had better transports, which RADIUS grudgingly added 10 years later
- Diameter has the concept of "applications", which is entirely missing in RADIUS
- In many senses, Diameter is a base protocol for transporting application-specific policies

Why two standards

- DIME is standardizing applications and application-specific policy exchanges
  - Of which AAA is just one application
- RADEXT is standardizing AAA
  - and has no other applications
  - is extending AAA use-cases outside of PPP, Wi-Fi, etc. like:
    - Federated identity management (ABFAB)
    - Federated wi-Fi network access in academia (eduroam)

Feature Comparison

Features	Diameter (RFC 6733)	RADIUS (RFC 2865)	RADEXT
Transport	TCP or SCTP	UDP	*TCP (RFC 6613 - Exp)*
Security	TLS, DTLS, IPsec	IPsec	*TLS (RFC 6614 – Exp), DTLS (draft)*
Operation Model	Peer-to-Peer	Client-Server	*Server-initiated commands to modify existing sessions (RFC Info)*
intermediaries	Relay, Redirect, Proxy	Only Proxy	
Peer Discovery	Static or DNS	Static	*DNS (IETF draft)*
Routing	Realm-based + App-Id	IP routing	
Max # Application	2^32	1 (AAA)	
Capability negotiation	Yes	No	*Based on presence of attributes*

Feature Comparison (2)

Features	Diameter (RFC 6733)	RADIUS (RFC 2865)	RADEXT
Data Types	8 Basic + 7 complex	5 Basic	12 basic (RFC 6929 - Std)
Max # command	Up to 2^24	Up to 256	
Max Packet size	2^24 octets	4096 octets	*65535 (IETF Draft)*
Max # attributes	2^32 (standard)	256	About 2K (RFC 6929 - Std)
Max attribute size	2^24	253 octets	4KB by data fragmentation in consecutive attributes (RFC 6929- Stand)
Data Grouping	Generic	Tags (bad)	Sub-attributes (RFC 6929 – Std)
compatibility	Yes	No	
Failover	Yes	No	
Keep-Alive	Yes	No	

Implementations

- RADIUS
  - Commercial and open source
- Diameter
  - Commercial and open source
- Both have a wide variety of commercial offerings, with varied features, performance, etc.
- Both have really only one major Open Source implementation FreeRADIUS & freediameter


A
?
B

Choosing a protocol

- The choices are often made for you!
- 3GPP, WiMAX, etc. are almost completely Diameter.
  - Some RADIUS for interaction with legacy systems
- Access control done by Switches, routers, WiFi access points, VPNs, are entirely RADIUS.
- There is some overlap, but not a lot.

Choosing a protocol (2)

- Enterprise, University, small business wants AAA for WiFi, 802.1X, VPN, etc.
  - Probably RADIUS
- Telcos talking to other Telcos
  - Probably Diameter
- AAA only - RADIUS
- Complex authorization policies - Diameter

Check List

- Basic AAA requirement?
- Existing RADIUS infrastructure?
- Does RADIUS protocol fit?
- Do RADIUS attribute type and data types fit?
- Do RADIUS size constraints acceptable or surmountable?

One "NO" above may be a case for Diameter

Check List (2)

- When Diameter is to be used: "try to re-use as much as possible!"
  - Reuse existing Diameter application if possible
  - Extend existing Diameter application if possible
- When not possible, Create your own application
  - Using existing application as model
  - A Standard application for multi-vendor environment
  - A Vendor-specific application under the responsability of the vendor

The Future

- RADIUS and Diameter will co-exist
- Diameter will get more applications, and continue to expand out of the AAA space
- RADIUS will get more extensions, and will continue to serve new needs in the AAA space
- RADIUS will be closer to Diameter but will avoid adding the "application concept"
- Diameter will still continue doing AAA

We Can Help!

- RADEXT: RADIUS Extensions
  - http://datatracker.ietf.org/wg/radext/
  - radext@ietf.org
- DIME: Diameter Maintenance and Extensions
  - http://datatracker.ietf.org/wg/dime/
  - dime@ietf.org

Questions?