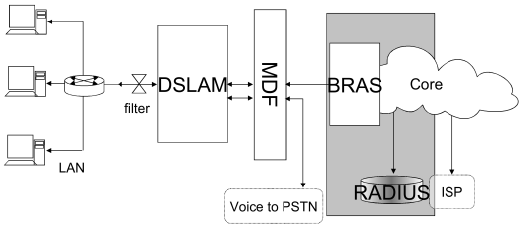
COMP312-09A
Communications and Systems Software

BRAS and Radius

Richard Nelson
richardn@cs.waikato.ac.nz

DSL connection



Evolution

- In the beginning dial up lines were connected to Remote Access Servers (RAS)
- In ADSL Networks, user connections are terminated on Broadband Remote Access Servers (BRAS)
- As more functions are added and more access methods possible the devices are being generalised to Broadband Network Gateways (BNG).

BRAS Functions

- Terminates user connections (PPPoA, PPPoE)
- Assigns addresses and other user configuration
- Aggregates user sessions, and allows the ISP to apply policy and QOS
- Interfaces with RADIUS (AAA)

A BRAS is a Router

- An edge router
  - Access control and QoS
- Many (thousands) of logical (PPP) interfaces.
- A BNG will connect multiple access technologies
- BNGs will provide triple play (voice, video, data) services using sophisticated QoS features.
- They may provide NAT if IPv4 addresses become too scarce.

Introduction to RADIUS

- Remote Authentication Dial In User Service
- Provides Authentication, Authorisation & Accounting (AAA)
- RFC2058 & RFC2059; later updated to RFC2865 & RFC2866
- UDP ports 1645 & 1646 or 1812 & 1813

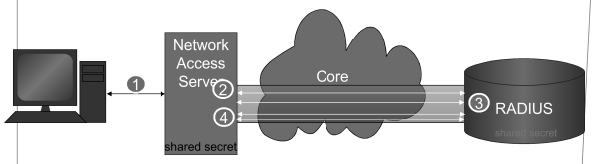
AAA

- Authentication,
  - Are they who they claim to be?
- Authorization (access control)
  - What services are they allowed to use?
- Accounting
  - How much service did they use?

AAA Protocols

- RADIUS
  - Developed for Merit 1991. Later specified in RFC 2058 (1991)
- DIAMETER
  - IETF developed to upgrade RADIUS architecture
- TACACS
  - Early Unix Terminal Access system
- TACACS+
  - Developed by Cisco and publicly specified

RADIUS Authentication



1: LLP connection established between end client and NAS

2: Access request: User authentication credentials passed to RADIUS server

3: Access reply: Accept / Deny; may include framed parameters

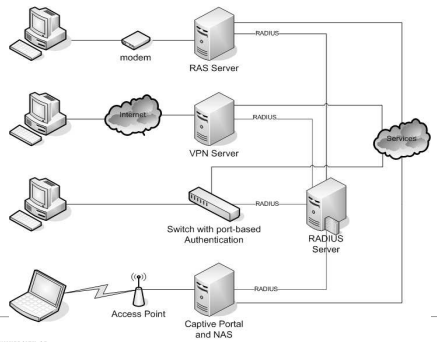
4: Service initiated. Accounting start: request and accept

Other: Accounting interim updates
Accounting stop

Authentication

- Radius specifies a protocol for carrying Authentication parameters
- Many authentication methods are supported, typically
  - PAP (Password authentication protocol)
  - CHAP (Challenge Handshake AP)
  - MS-CHAP
  - EAP (Extensible AP)
- Authentication Challenge occurs between access-request and access-accept messages

Access Modes

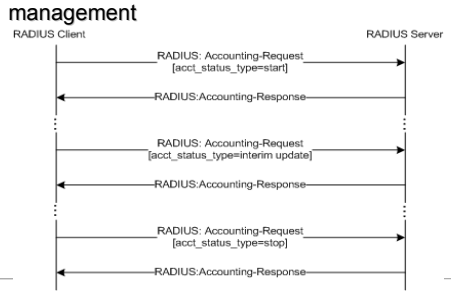


Authorisation

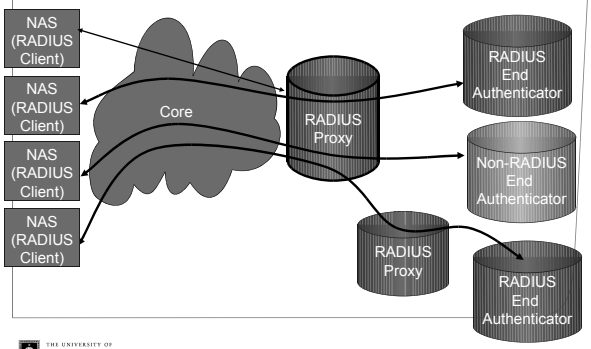
- Authorisation is combined with authentication messages
- Extra attributes are passed to the NAS specifing access control parameters, e.g.
  - IP address or range
  - Length of permitted access time
  - Access lists and priority queue assignment
  - VLAN or tunnel parameters
  - QoS profile

Accounting

- Used for billing and network monitoring and management



RADIUS Proxy



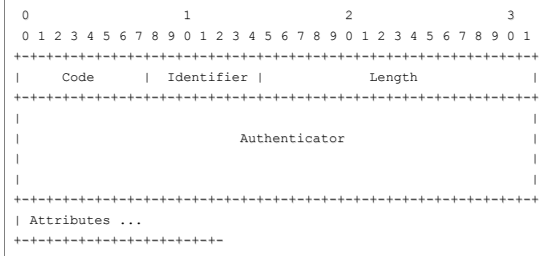
Radius Proxy

- Radius proxys can be used to allow roaming between service providers or customers of multiple service providers to use a common access infrastructure
- Usernames are appended with a *realm*.
  - e.g. **user@somedomain.com**
  - Do not have to use real domain names or the @ character.
- Proxys need to be configured with realm names

Radius Packets

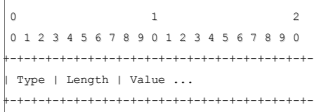
- Radius is an unreliable stateless protocol so it uses UDP
  - Applications are responsible retransmission to alternate servers.
- Traditional use ports 1645 (accounting) and 1646 (authentication)
- IANA assigned ports 1812 (authentication) 1813 (authorisation)

RADIUS Packet



RADIUS Attributes

Attribute format

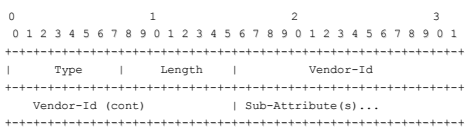


Sample Attribute Types

1 User-Name
2 User-Password
4 NAS-IP-Address
5 NAS-Port
6 Service-Type
7 Framed-Protocol
8 Framed-IP-Address
9 Framed-IP-Netmask
26 Vendor-Specific
30 Called-Station-Id
31 Calling-Station-Id
32 NAS-Identifier
64 Tunnel-Type
87 NAS-Port-Id
88 Framed-Pool

Attribute 26: VSAs

Vendor-Specific Attributes



- RADIUS Dictionaries

Dictionary Example

```
# Cisco 6510 SSG v1.1 RADIUS dictionary
#
# This dictionary is designed for and only intended to be
# used with the Cisco 6510 Service Selection Gateway
# Version 1.0.  It contains a minimal set of RADIUS
# Attribute Value Pair definitions which is not sufficient
# for use with a typical Network Access Server.
#
# This file can be used as a dictionary file replacement for
# a shareware/freeware RADIUS AAA Server when the RADIUS
# client is the Cisco 6510 Service Selection Gateway version 1.0.
#
# It is important to note that if you decide to use a Freeware
# RADIUS Server with the 6510 Service Selection Gateway, it must
# support Vendor Specific Attributes in both Access-Requests and
# Accounting-Requests.
#
ATTRIBUTE     User-Name               1     string
ATTRIBUTE     User-Password           2     string
ATTRIBUTE     NAS-IP-Address          4     ipaddr
ATTRIBUTE     Service-Type            6     integer
ATTRIBUTE     Framed-IP-Address       8     ipaddr
ATTRIBUTE     Reply-Message          18     string
ATTRIBUTE     Class                  25     string
ATTRIBUTE     Vendor-Specific        26     string
ATTRIBUTE     Session-Timeout        27     integer
ATTRIBUTE     Idle-Timeout           28     integer
ATTRIBUTE     Proxy-State            33     string
ATTRIBUTE     Acct-Status-Type       40     integer
ATTRIBUTE     Acct-Input-Octets      42     integer
ATTRIBUTE     Acct-Output-Octets     43     integer
```


RADIUS Issues

- IESG Note: This protocol is widely implemented and used. Experience has shown that it can suffer degraded performance and lost data when used in large scale systems, in part because it does not include provisions for congestion control.

Source: RFC2865: http://www.ietf.org/rfc/rfc2865.txt

QOS recap

- Quality of Service
  - Prioritisation of network traffic to ensure important or sensitive traffic traverses the network rapidly

Dynamic Profile Assignment

- Profiles are configured at (in) the BRAS (NAS)
- RADIUS accept includes profile names
- BRAS applies profiles as per RADIUS
- Profile types may include
  - Rate-limit profiles
  - QoS profiles
  - Filters