

Wireless Network

Esercitazioni



Alessandro Villani
avillani@science.unitn.it



Radius

AAA

- Dato un certo numero di punti di accesso dall'esterno alla rete
- Data una grande quantità di utenti
- Abbiamo la necessità di gestire in maniera centralizzata il processo di AAA (*Authentication, Authorization, Accounting*)

Protocollo Radius

- ❑ RADIUS (*Remote Authentication Dial-In Service*) è un protocollo client/server
- ❑ Definito nella RFC 2865 disponibile sul sito dell'IETF:
<http://www.ietf.org/rfc.html>
- ❑ La porta (UDP) per autenticazione è la 1812
- ❑ L'Accounting è definito nella RFC 2866
- ❑ La porta (UDP) per accounting è la 1813

Protocollo Radius

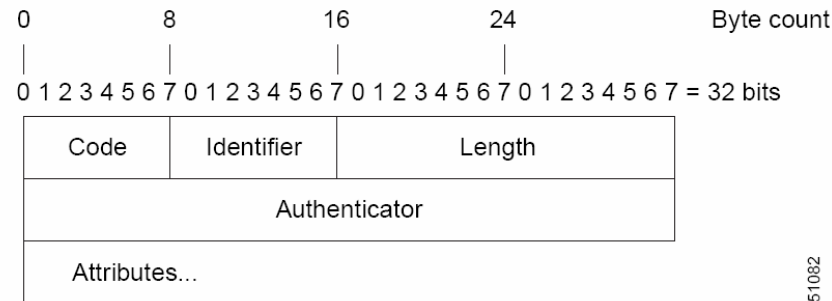
- ❑ Un NAS (*Network Access Server*) comunica con un server per autenticare un utente (login e passwd)
- ❑ Il NAS può ricevere a sua volta dal server informazioni di configurazione specifiche per l'utente
- ❑ RADIUS prevede una serie di meccanismi di ritrasmissione in caso di time-out

Protocollo Radius

- ❑ Le transizioni fra il client ed il server RADIUS sono autenticate mediante una chiave condivisa (mai inviata sulla rete)
- ❑ Questo meccanismo è scomodo da gestire: un cambio della password richiede l'aggiornamento di tutti i NAS
- ❑ Tutte le password degli utenti sono inviate in forma crittata dal client verso il server

Protocollo Radius: Pacchetti

□ Schema di un pacchetto RADIUS



□ **Code**: identifica i seguenti tipi di pacchetto:

- Access-Request (1)
- Access-Accept (2)
- Access-Reject (3)
- Accounting-Request (4)
- Accounting-Response (5)
- Access-Challenge (11)

Protocollo Radius: Pacchetti

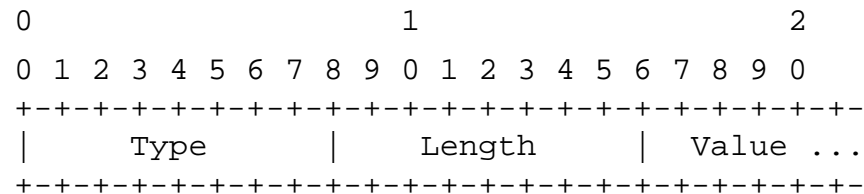
- **Identifier:** è utilizzato per associare richieste e risposte e per determinare richieste duplicate
- **Length:** la lunghezza dell'intero pacchetto
- **Authenticator:** è utilizzato per autenticare la risposta del server. Sono definiti due tipi di Authenticator:
 - Request-Authentication: utilizzato nei pacchetti *Access-Request* e *Accounting-Request*
 - Response-Authenticator: utilizzato nei pacchetti *Access-Accept*, *Access-Reject*, *Access-Challenge*, e *Accounting-Response*

Protocollo Radius : Pacchetti

- ❑ Il campo Authenticator è un numero pseudo-random di 128-bit e non predicibile
- ❑ Alcune implementazioni non rispettano la non predicibilità!
- ❑ 128-bit Response Authenticator = MD5(Code + Identifier + Length + Request Authenticator + Attributes + Shared Secret)

Protocollo Radius: Pacchetti

- ❑ **Attributes**: campo di lunghezza variabile e contiene una lista di zero o più attributi
- ❑ Il formato di un Attributo è il seguente:



- ❑ Alcuni dei tipi definiti sono:
 - 1 User-Name
 - 2 User-Password
 - 4 NAS-IP-Address
 - 5 NAS-Port
 - 32 NAS-Identifier
 - 40-59 Accounting

Protocollo Radius: Pacchetti

- ❑ **Access-Request**: inviato da un client ad un server RADIUS. Conterrà le informazioni che servono al server RADIUS server per determinare se autorizzare l'accesso ad un utente di un NAS
- ❑ **Access-Accept**: Quando il server RADIUS riceve un Access-Request, invierà un Access-Accept se il valore di tutti gli attributi presenti nell'Access-Request sono accettabili. Access-Accept fornirà le informazioni di configurazione necessarie al client
- ❑ **Access-Reject**: quando il server RADIUS riceve un Access-Request, invierà un Access-Reject se qualcuno dei valore degli attributi presenti nell'Access-Request è inaccettabile

Protocollo Radius: Pacchetti

- ❑ **Access-Challenge**: quando il server RADIUS riceve un Access-Request, può inviare al client un Access-Challenge, che richiederà una risposta. Il cliente risponderà con un nuovo Access-Request
- ❑ **Accounting-Request**: inviato da un client ad un server di accounting RADIUS, fornendo informazioni di accounting. Se il server RADIUS accetta l'Accounting-Request, risponderà con un Accounting-Response
- ❑ **Accounting-Response**: inviato dal server di accounting RADIUS al client per confermare la ricezione dell'Accounting-Request

Protocollo Radius: Accounting

- Quando un client utilizza un server RADIUS per l'accounting:
 - All'inizio del servizio il client invierà un pacchetto Accounting-Start che descrive il tipo di servizio fornito e lo user
 - Il server risponderà confermando la ricezione
 - Al termine del servizio fornito, il client invierà un pacchetto di Accounting-Stop che descrive il tipo di servizio fornito e opzionalmente statistiche quali il tempo passato, gli ottetti in input e output, o i pacchetti in input e output
 - Il server risponderà confermando la ricezione
 - Il client è previsto che continui a provare ad inviare il pacchetto Accounting-Request finchè non riceve un acknowledgement

Protocollo Radius: considerazioni

- ❑ Radius può avere performance non soddisfacenti e perdita di dati quando utilizzato in grandi installazioni, visto che non include meccanismi per il controllo della congestione
- ❑ Nuovo protocollo → *DIAMETER*
- ❑ Diameter utilizza TCP



Ethereal

Ethereal

- Ethereal è un packet sniffer completamente open source
- Disponibile al sito:
<http://www.ethereal.com/>
- Dispone di decoder per moltissimi protocolli, tra cui:
 - IEEE 802.11 wireless LAN
 - Radius
 - 802.1x Authentication

Ethereal: Filtri durante la cattura

- Un “capture filter” ha la forma di una serie di espressioni primitive collegate da congiunzioni (**and/or**) ed eventualmente preceduta da **not**:

[not] **primitive** [and|or [not]
primitive ...]

- Ad esempio:
 - tcp port 23 and host 193.205.194.23
 - tcp port 23 and not host 193.205.194.23

Ethereal: Filtri durante la cattura

- ❑ **Alcune primitive più utilizzate:**
- ❑ **[src|dst] host <host>**
 - Questa primitiva consente di filtrare in base all'IP dell' host o il suo nome
- ❑ **ether [src|dst] host <ehost>**
 - Questa primitiva consente di filtrare in base all'indirizzo Ethernet dell'host
- ❑ **[src|dst] net <net> [{mask <mask>}|{len <len>}]**
 - Questa primitiva consente di filtrare in base agli indirizzi delle reti
- ❑ **[tcp|udp] [src|dst] port <port>**
 - Questa primitiva consente di filtrare in base ai numeri delle porte TCP ed UDP
- ❑ **ip|ether proto <protocol>**
 - Questa primitiva consente di filtrare in base al protocollo specificato al livello Ethernet oppure al livello IP

Ethereal: Radius Accounting

- L'autenticazione attraverso RADIUS del MAC address di una scheda Wireless si traduce nel passare:
 - Come User Id il MAC address della scheda
 - Come password:
 - il secret dell'AP nel caso degli AP Avaya
 - Il MAC address della scheda wireless nel caso degli AP Cisco

Ethereal: Radius Authentication

Richiesta di accesso (Code = 1)

```
Frame 9 (107 bytes on wire, 107 bytes captured)
Ethernet II, Src: 00:00:cd:03:fe:7e, Dst: 00:80:5f:41:fb:95
Internet Protocol, Src Addr: 172.31.194.25 (172.31.194.25), Dst Addr: 192.168.194.168
(192.168.194.168)
User Datagram Protocol, Src Port: 6001 (6001), Dst Port: radius (1812)
  Source port: 6001 (6001)
  Destination port: radius (1812)
  Length: 73
  Checksum: 0xb4dd (correct)
Radius Protocol
  Code: Access Request (1)
  Packet identifier: 0xd2 (210)
  Length: 65
  Authenticator: 0x5D170000B9760000D55F00008C410000
  Attribute value pairs
    t:User Name(1) l:15, Value:"00904b-649170"
    t:User Password(2) l:18, Value:BCA8373AA383F48F1CE20A230CFE7D0D
    t:NAS IP Address(4) l:6, Value:172.31.194.25
    t:NAS Port(5) l:6, Value:0
```

Ethereal: Radius Authentication

Accesso Autorizzato (Code = 2)

```
Frame 10 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: 00:80:5f:41:fb:95, Dst: 00:00:cd:03:fe:7e
Internet Protocol, Src Addr: 192.168.194.168 (192.168.194.168), Dst Addr: 172.31.194.25
(172.31.194.25)
User Datagram Protocol, Src Port: radius (1812), Dst Port: 6001 (6001)
  Source port: radius (1812)
  Destination port: 6001 (6001)
  Length: 28
  Checksum: 0xae8b (correct)
Radius Protocol
  Code: Access Accept (2)
  Packet identifier: 0xd2 (210)
  Length: 20
  Authenticator: 0x97E2EFA2A29FDCB8F223CA43D655A499
```

Ethereal: Radius Accounting

- La procedura di accounting per gli AP Avaya prevede di registrare soltanto l'ora di inizio della sessione e la sua fine
- La procedura di accountin per gli AP Cisco registra molte più informazioni:
 - Input octects
 - Output octects
 - Input packets
 - Output packets

Ethereal: Radius Accounting

Richiesta di Accounting (Code = 4): Start

```
Frame 11 (132 bytes on wire, 132 bytes captured)
Ethernet II, Src: 00:00:cd:03:fe:7e, Dst: 00:80:5f:41:fb:95
Internet Protocol, Src Addr: 172.31.194.25 (172.31.194.25), Dst Addr: 192.168.194.168
(192.168.194.168)
User Datagram Protocol, Src Port: 6002 (6002), Dst Port: radius-acct (1813)
  Source port: 6002 (6002)
  Destination port: radius-acct (1813)
  Length: 98
  Checksum: 0x38f9 (correct)
Radius Protocol
  Code: Accounting Request (4)
  Packet identifier: 0xd3 (211)
  Length: 90
  Authenticator: 0x7726EA20EDC039C0CD37B7232FF23D0E
  Attribute value pairs
    t:User Name(1) l:15, Value:"00904b-649170"
    t:Acct Session Id(44) l:15, Value:"00904b-649170"
    t:NAS identifier(32) l:10, Value:"Avaya-15"
    t:NAS IP Address(4) l:6, Value:172.31.194.25
    t:NAS Port(5) l:6, Value:2
    t:NAS Port Type(61) l:6, Value:Wireless IEEE 802.11(19)
    t:Acct Authentic(45) l:6, Value:Radius(1)
    t:Acct Status Type(40) l:6, Value:Start(1)
```

Ethereal: Radius Accounting

Risposta di Accounting (Code = 5)

```
Frame 12 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: 00:80:5f:41:fb:95, Dst: 00:00:cd:03:fe:7e
Internet Protocol, Src Addr: 192.168.194.168 (192.168.194.168), Dst Addr: 172.31.194.25
(172.31.194.25)
User Datagram Protocol, Src Port: radius-acct (1813), Dst Port: 6002 (6002)
  Source port: radius-acct (1813)
  Destination port: 6002 (6002)
  Length: 28
  Checksum: 0xa6e1 (correct)
Radius Protocol
  Code: Accounting Response (5)
  Packet identifier: 0xd3 (211)
  Length: 20
  Authenticator: 0xE3ACA0C57C3FCAED9B081887B3F10FBB
```


Ethereal: Radius Accounting

Richiesta di Accounting (Code = 4): Stop

```
Frame 13 (132 bytes on wire, 132 bytes captured)
Ethernet II, Src: 00:00:cd:03:fe:7e, Dst: 00:80:5f:41:fb:95
Internet Protocol, Src Addr: 172.31.194.25 (172.31.194.25), Dst Addr: 192.168.194.168
(192.168.194.168)
User Datagram Protocol, Src Port: 6002 (6002), Dst Port: radius-acct (1813)
  Source port: 6002 (6002)
  Destination port: radius-acct (1813)
  Length: 98
  Checksum: 0x6372 (correct)
Radius Protocol
  Code: Accounting Request (4)
  Packet identifier: 0xd4 (212)
  Length: 90
  Authenticator: 0x0E739E4CD09F9C3DC8ED9CA383454D35
  Attribute value pairs
    t:User Name(1) l:15, Value:"00904b-649170"
    t:Acct Session Id(44) l:15, Value:"00904b-649170"
    t:NAS identifier(32) l:10, Value:"Avaya-15"
    t:NAS IP Address(4) l:6, Value:172.31.194.25
    t:NAS Port(5) l:6, Value:2
    t:NAS Port Type(61) l:6, Value:Wireless IEEE 802.11(19)
    t:Acct Authentic(45) l:6, Value:Radius(1)
    t:Acct Status Type(40) l:6, Value:Stop(2)
```

Ethereal: Radius Accounting

Risposta di Accounting (Code = 5)

```
Frame 14 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: 00:80:5f:41:fb:95, Dst: 00:00:cd:03:fe:7e
Internet Protocol, Src Addr: 192.168.194.168 (192.168.194.168), Dst Addr: 172.31.194.25
(172.31.194.25)
User Datagram Protocol, Src Port: radius-acct (1813), Dst Port: 6002 (6002)
  Source port: radius-acct (1813)
  Destination port: 6002 (6002)
  Length: 28
  Checksum: 0x6c6b (correct)
Radius Protocol
  Code: Accounting Response (5)
  Packet identifier: 0xd4 (212)
  Length: 20
  Authenticator: 0x7B5864A3F47B3C3C7E8ECFFA292BF4E8
```

Ethereal: Radius Authenticator

- ❑ È possibile analizzare in chiaro il contenuto dei campi crittati
- ❑ Edit→Preferences→Protocols
- ❑ Selezionando Radius si può impostare la shared secret

Ethereal: Sniffing sullo stesso AP

- ❑ Client A connesso wireless all'AP X
- ❑ Client B connesso wireless all'AP X
- ❑ B con ethereal
- ❑ B riesce a catturare tutto il traffico di A!

```
Unauthorized access is prohibited
```

```
-----
```

```
Attenzione: per utilizzare netscape servirsi dei sistemi linux o windows!
```

```
Digital UNIX (kirk) (ttyp5)
```

```
login: ŷŷraavviillllaanni
```

```
Password:CheNeSo
```

```
Login incorrect
```

```
login:
```

Ethereal: Sniffing sullo stesso AP

The screenshot displays the Ethereal network protocol analyzer interface. The main window shows a list of captured packets. Packet 52 is selected, and its details are shown in the lower pane. The details pane is divided into several sections: Ethernet II, Internet Protocol, and Transmission Control Protocol (TCP). The TCP section shows the source and destination ports, sequence number, and window size. The stream content pane shows the raw data of the packet, which is a Telnet login attempt. The login attempt includes the text "Unauthorized access is prohibited", "Attenzione: per utilizzare netscape servirsi dei sistemi linux o windows", "Digital UNIX (kirk) (tty5)", "login: ..aavvi1111aannii", "Password: CheNeSo", and "Login incorrect".

No.	Time	Source	Destination	Protocol	Info
52	13.598512	172.31.194.10	193.205.194.17	TCP	3018 > telnet [SYN] Seq=0 Ack=0 win=16384 Len=0 MSS=1460
53	13.599737	193.205.194.17	172.31.194.10	TCP	telnet > 3018 [SYN, ACK] Seq=0 Ack=1 win=33580 Len=0 MSS=1460
54	13.601861	172.31.194.10	193.205.194.17	TCP	3018 > telnet [ACK] Seq=1 Ack=1 win=17520 Len=0
55	13.619301	193.205.194.17	172.31.194.10	TELNET	Telnet Data ...
56	13.621075	172.31.194.10	193.205.194.17	TELNET	Telnet Data ...
57	13.622240	193.205.194.17	172.31.194.10	TELNET	Telnet Data ...
58	13.623861	172.31.194.10	193.205.194.17	TELNET	Telnet Data ...
59	13.625079	193.205.194.17	172.31.194.10	TELNET	Telnet Data ...
60	13.626862	172.31.194.10	193.205.194.17	TELNET	Telnet Data ...
61	13.758389	193.205.194.17	172.31.194.10	TCP	telnet > 3018 [ACK] Seq=31 Ack=28 win=33580 Len=0
62	13.759994	172.31.194.10	193.205.194.17	TELNET	Telnet Data ...
63	13.762088	193.205.194.17	172.31.194.10	TELNET	Telnet Data ...
64	13.763990	172.31.194.10	193.205.194.17	TELNET	Telnet Data ...
65	13.957596	193.205.194.17	172.31.194.10	TCP	telnet > 3018 [ACK] Seq=43 Ack=47 win=33580 Len=0

Frame 52 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: ...
Internet Protocol ...
Transmission Control Protocol (tcp) ...
Source port: 30
Destination port: 3018
Sequence number: 0
Header length: 20
Flags: 0x0002 (SYN)
Window size: 16384
Checksum: 0x0000
Options: (8 bytes) ...

Stream Content
.....#...'.\$.#...'.\$.P.....'.ANSI
.....!.....).
Unauthorized access is prohibited.

0.
Attenzione: per utilizzare netscape servirsi dei sistemi linux o windows
0.
0.
0.
Digital UNIX (kirk) (tty5)0.
0.
0.
0.
login: ..aavvi1111aannii
Password: CheNeSo
Login incorrect
login:

Filter: addr eq 193.205.194.17 and (tcp.port eq 3018 and tcp.port eq 23) / Add Expression... Clear Apply Transmission Control Protocol (tcp), 28 bytes P: 191 D: 62 M: 0