Lecture 4b
AAA protocols
(Authentication Authorization Accounting)

Network security
(*19*265400 / *20*1000086)
Lecturers:

Aiko Pras
Pieter-Tjerk de Boer
Anna Sperotto
Ramin Sadre
Georgios Karagiannis

Lecture material

- to be found via Blackboard:
  - Course Information => Course material that can be downloaded: => radius_diameter.txt

  file can also be downloaded via:

  http://wwwhome.ewi.utwente.nl/~karagian/network_security/radius_diameter.txt
  - radius_diameter.txt includes text copied from RFC2865, RFC2866, RFC3588

Outline

- Goal of this lecture
- What's AAA?
- Basic operation RADIUS

  (Remote Authentication Dial In User Service)
- Basic operation DIAMETER
- Main differences DIAMETER vs. RADIUS
- Summary & References

Goal of this lecture

- understanding what is the AAA concept and which main AAA protocols are used and how they are used

Outline

- Goal of this lecture
- What's AAA?
- Basic operation RADIUS
- Basic operation DIAMETER
- Main differences DIAMETER vs. RADIUS
- Summary & References

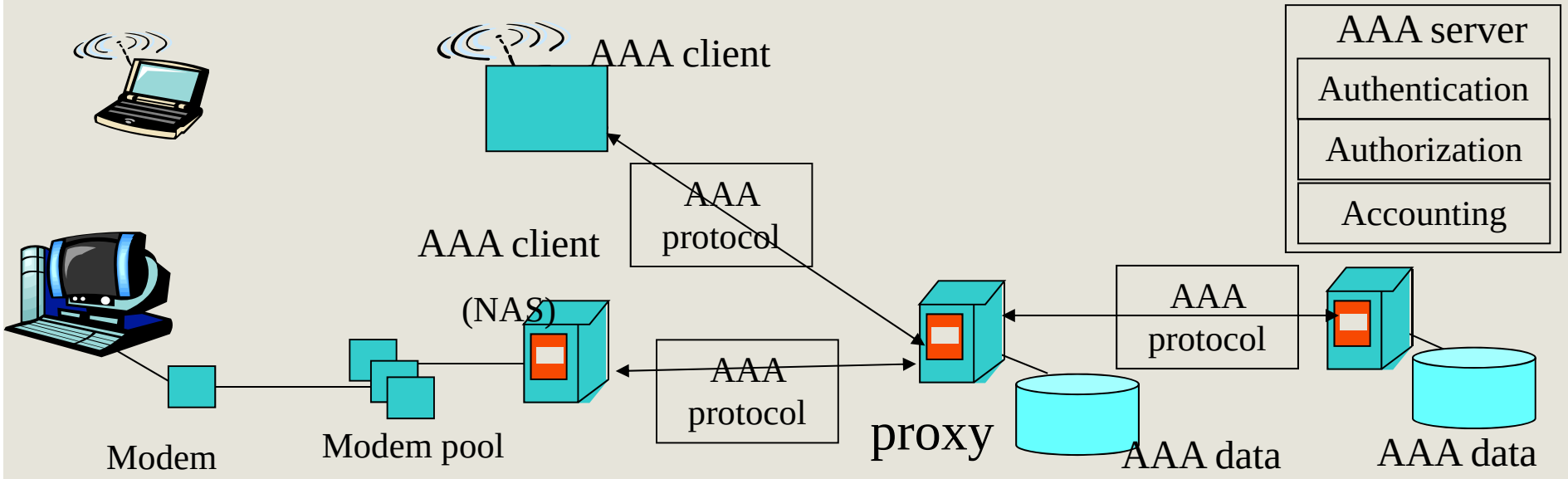
What's AAA

- Authentication, authorization and accounting processes are needed when user tries to access and use Internet
  - Authentication: act of verifying identity of entity
  - Authorization: act of determining whether requesting entity is allowed access to a resource
  - Accounting: act of collecting info on resource usage for the purpose of capacity planning, auditing, billing or cost allocation

  Concept standardized by IETF, e.g.:
    - Generic AAA architecture (RFC2903)
    - AAA Authorization Application Examples (RFC2905)
    - AAA Authorization Framework (RFC2904)

  - Example use: AAA can be used in combination with IEEE 802.1x to enhance WLAN authentication & authorization

What's AAA (example scenario)



- AAA protocol: supports AAA communication between AAA client and AAA server(s):
  - TACACS (RFC1492)
  - RADIUS (RFC2865)
  - DIAMETER (RFC3588)

Outline

- Goal of this lecture
- What's AAA?
- Basic operation RADIUS
- Basic operation DIAMETER
- Main differences DIAMETER vs. RADIUS
- Summary & References

Basic operation RADIUS

RADIUS:

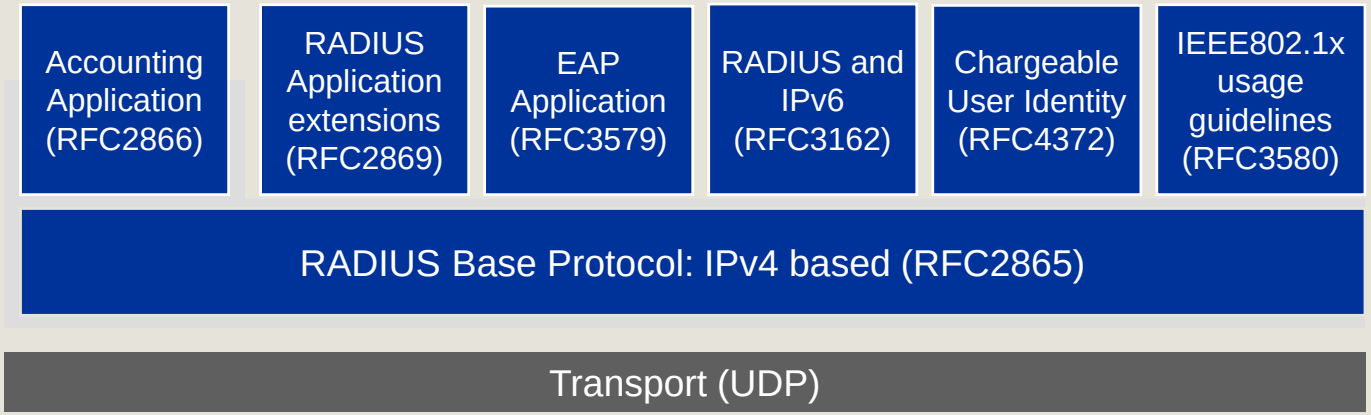
- AAA protocol used to carry AAA information between AAA client (e.g., Network Access Server) and a shared AAA server

Basic operation RADIUS (key features)

- Client/Server Model
  - Client: NAS (Network Access Server): generates AAA request
  - Server: RADIUS server handles request (operates also as proxy)
- Network Security:
  - transactions authenticated using shared secret key, **manually distributed**, between client/server
  - any user passwords, hidden using MD5 (RFC1321) + other
  - End-to-end security (for non proxy RADIUS), but cannot be guaranteed
- Flexible Authentication Mechanisms, e.g.:
  - PPP CHAP (Challenge Handshake Authentication Protocol), EAP (Extensible Authentication Protocol)
- Extensible protocol:
  - AAA attribute information carried in Attribute- Length-Value; new attribute values added without disturbing existing implementations
- Uses UDP as transport protocol

Basic operation RADIUS (document architecture)

- (IPv4) base specification defining base protocol on authentication and authorization
- Accounting application for support of accounting
- RADIUS extensions for AAA application extensions
- EAP application for support of various authentication methods
- RADIUS operation when run over IPv6
- Chargeable user identity attribute used in case of real time accounting
- RADIUS usage guidelines for IEEE 802.1x



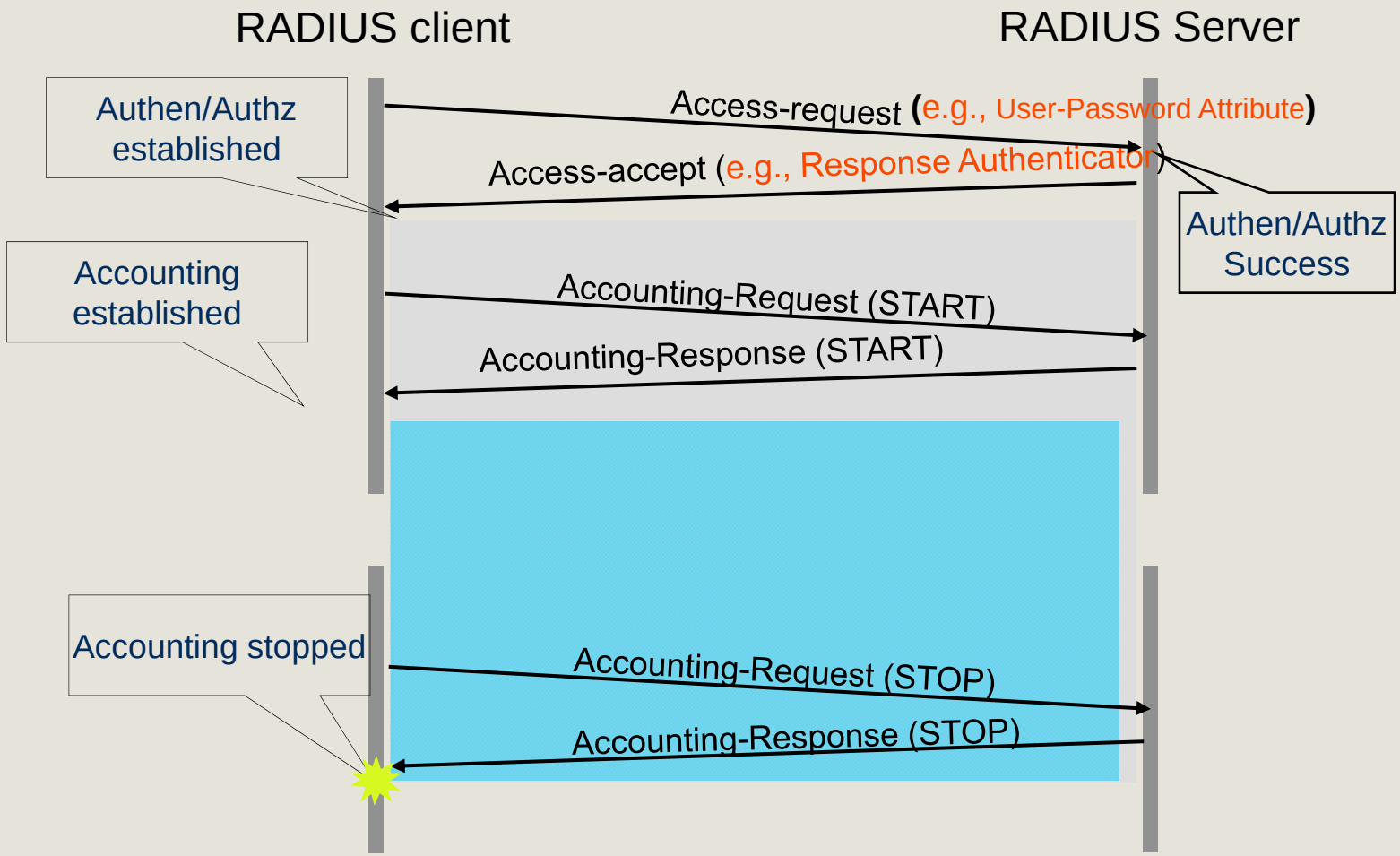
Basic operation RADIUS (message types)

Codes and message types:

- 1 Access-Request
- 2 Access-Accept
- 3 Access-Reject
- 4 Accounting-Request
- 5 Accounting-Response
- 11 Access-Challenge
- 12 Status-Server (experimental)
- 13 Status-Client (experimental)
- 255 Reserved

Basic operation RADIUS (session establishment/termination)

Same session used for authentication/authorization and accounting



Why is RADIUS using for transport UDP instead of TCP?

Advantages

- If request to primary authentication server fails, secondary server must be queried:
  - copy of request must be kept above transport layer
  - retransmission timers still required, above transport layer
- Stateless nature of RADIUS protocol within communication network simplifies use of UDP:
  - transport connection between client/server remains even if network failures are occurring

Disadvantages

- Transport is not reliable (layer above transport has to take care of packet losses)
- TCP adapt to network congestion, while UDP does not

Outline

- Goal of this lecture
- What's AAA?
- Basic operation RADIUS
- Basic operation DIAMETER
- Main differences DIAMETER vs. RADIUS
- Summary & References

Basic operation DIAMETER

DIAMETER:

- AAA protocol supports similar AAA features as RADIUS but with enhanced and additional capabilities

Basic operation DIAMETER (key features)

- Capabilities negotiation
- Carry AAA information in AVPs (Attribute Value Pairs)
- Error notification
- Extensibility, through addition of new commands and AVPs
- Basic services necessary for applications,
  such as handling of user sessions or accounting and session state maintenance
- Hop-by-hop security using IPSec (mandatory) and TLS (optional)
  - authenticate each hop by shared secret key (distributed using automatic key distribution: e.g., IKE (Internet Key Exchange)
    - HMAC-MD5-96 in [RFC2403]
    - HMAC-SHA1-96 [RFC2404])
  - encrypt at each hop by shared secret (e.g., DES-CBC (Data Encryption Standard – Cipher Block Chaining))

Basic operation DIAMETER (key features)

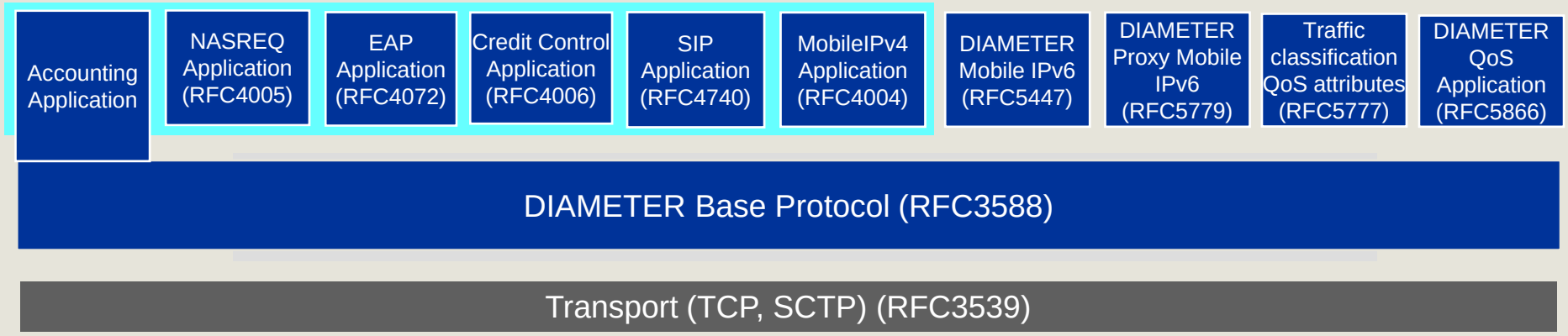
- AVPs used by base Diameter protocol to support:
  - Transporting user authentication information
  - Transporting service specific authorization information
  - Exchanging resource usage information
    - may be used for accounting purposes, capacity planning, etc.
  - Relaying and proxying of Diameter messages through server hierarchy.
- Transport:
  - Diameter clients must support TCP or SCTP
  - Diameter agents and servers must support TCP and SCTP
- Authentication/authorization session management may be independent of accounting session management:
  - accounting information can be routed to different server than server used by authentication/authorization messages:
    - Acct-Multi-Session-Id AVP in messages is used to correlate sessions

Basic operation DIAMETER (key features)

- DIAMETER base protocol provides minimum requirements needed:
  - may be used by itself for accounting purposes only
  - may be used with Diameter application, like NASREQ or MobileIPv4
  - may be extended for use in new applications with new commands or AVPs
- DIAMETER is peer-to-peer protocol
  - any node can initiate a request
- DIAMETER client:
  - node at edge of network performing access control
    - generates Diameter messages for authentication, authorization and accounting of user
- DIAMETER agent:
  - Relay, Proxy, Redirect, Translation agents
    - does not authenticate and/or authorize messages locally
- DIAMETER server:
  - node that performs authentication and/or authorization and accounting of user
- A node may act as agent for certain requests, while acting as server for others.

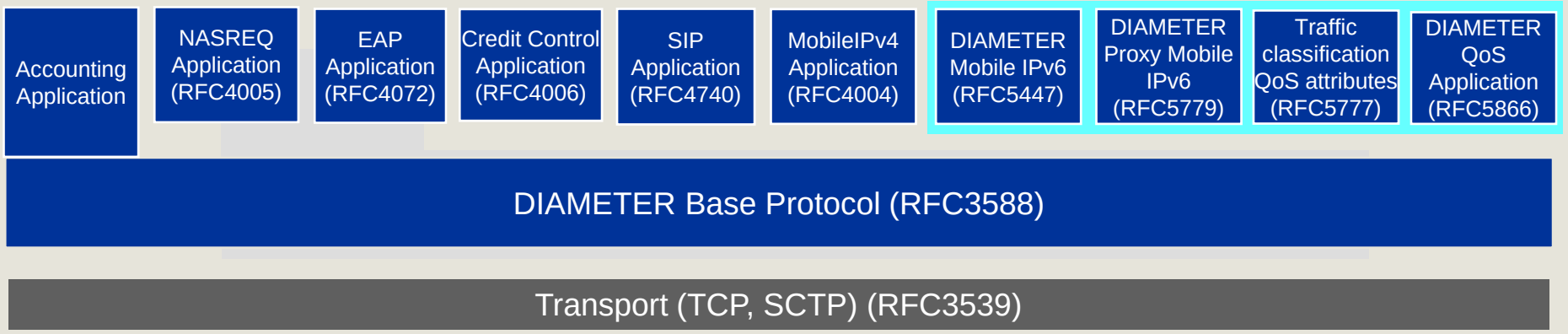
Basic operation DIAMETER (document architecture)

- base specification (IPv4 and IPv6) defining base protocol and accounting application (RFC 3588)
- Transport Profile document including failover mechanism and state machine (RFC 3539)
- NASREQ application for dial-in & terminal server applications (RFC 4005)
- EAP application for support of authentication methods (RFC4072)
- Credit Control application for real-time credit control (RFC 4006)
- SIP application provides AAA services to SIP entities (RFC 4740)
- MobileIPv4 application provides AAA support for Mobile IPv4 (RFC 4004)



Basic operation DIAMETER (document architecture)

- MIPv6 bootstrapping using Diameter Network Access Server to home AAA server interface (RFC 5447)
- AAA interactions between proxy Mobile IPv6 entities and AAA server in proxy Mobile IPv6 domain (RFC 5779)
- DIAMETER AVPs for traffic classification and QoS support (RFC 5777)
- DIAMETER QoS application (RFC 5866)

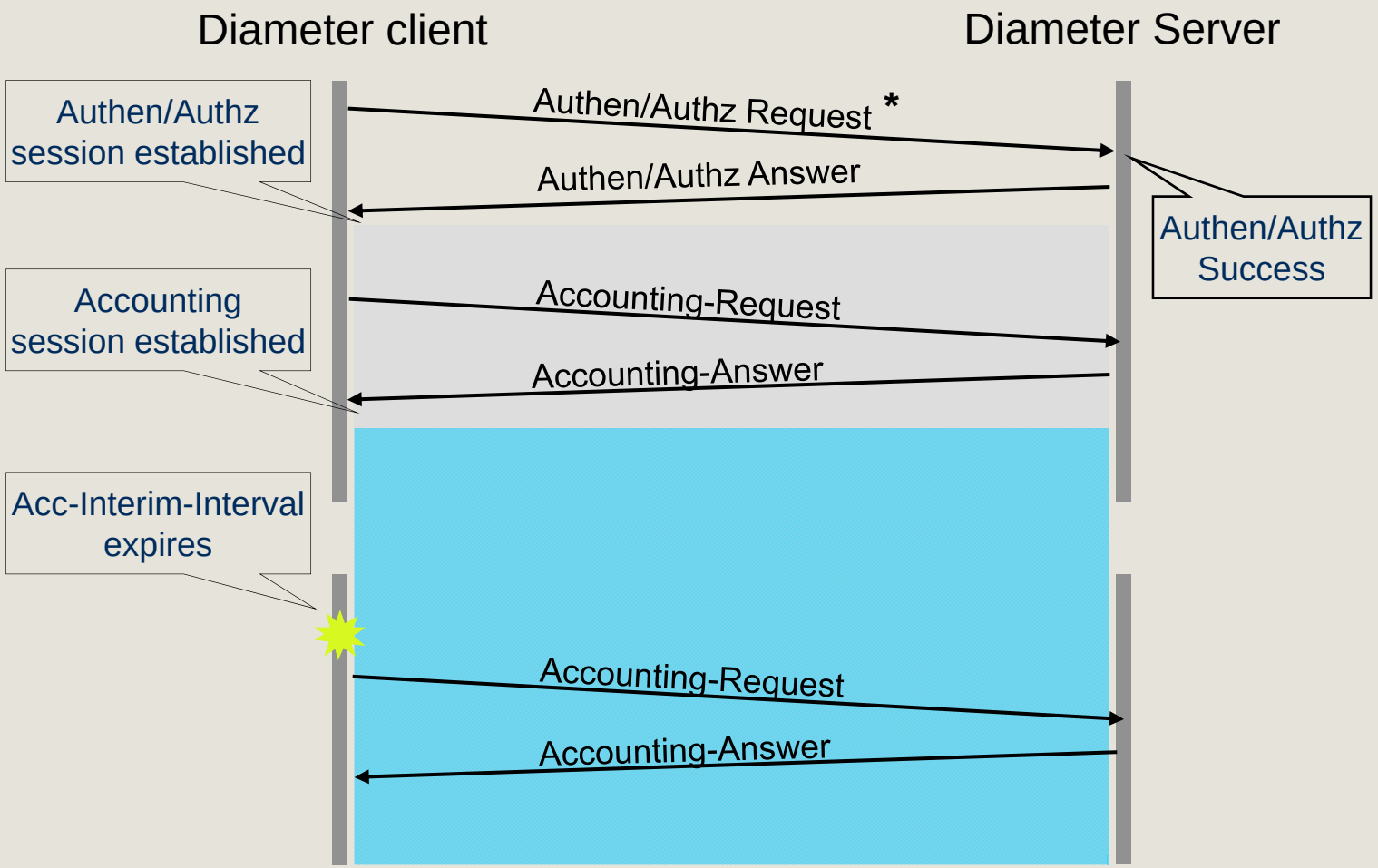


Basic operation DIAMETER (command names)

Command-Name (Authent/Authz-Request) *(Authent/Authz-Answer)*	*Abbrev.*	*Code*
Abort-Session-Request	ASR	274
Abort-Session-Answer	ASA	274
Accounting-Request	ACR	271
Accounting-Answer	ACA	271
Capabilities-Exchange- Request	CER	257
Capabilities-Exchange- Answer	CEA	257
Device-Watchdog-Request	DWR	280
Device-Watchdog-Answer	DWA	280
Disconnect-Peer-Request	DPR	282
Disconnect-Peer-Answer	DPA	282
Re-Auth-Request	RAR	258
Re-Auth-Answer	RAA	258
Session-Termination- Request	STR	275
Session-Termination-Answer	STA	275

Basic operation DIAMETER (session establishment)

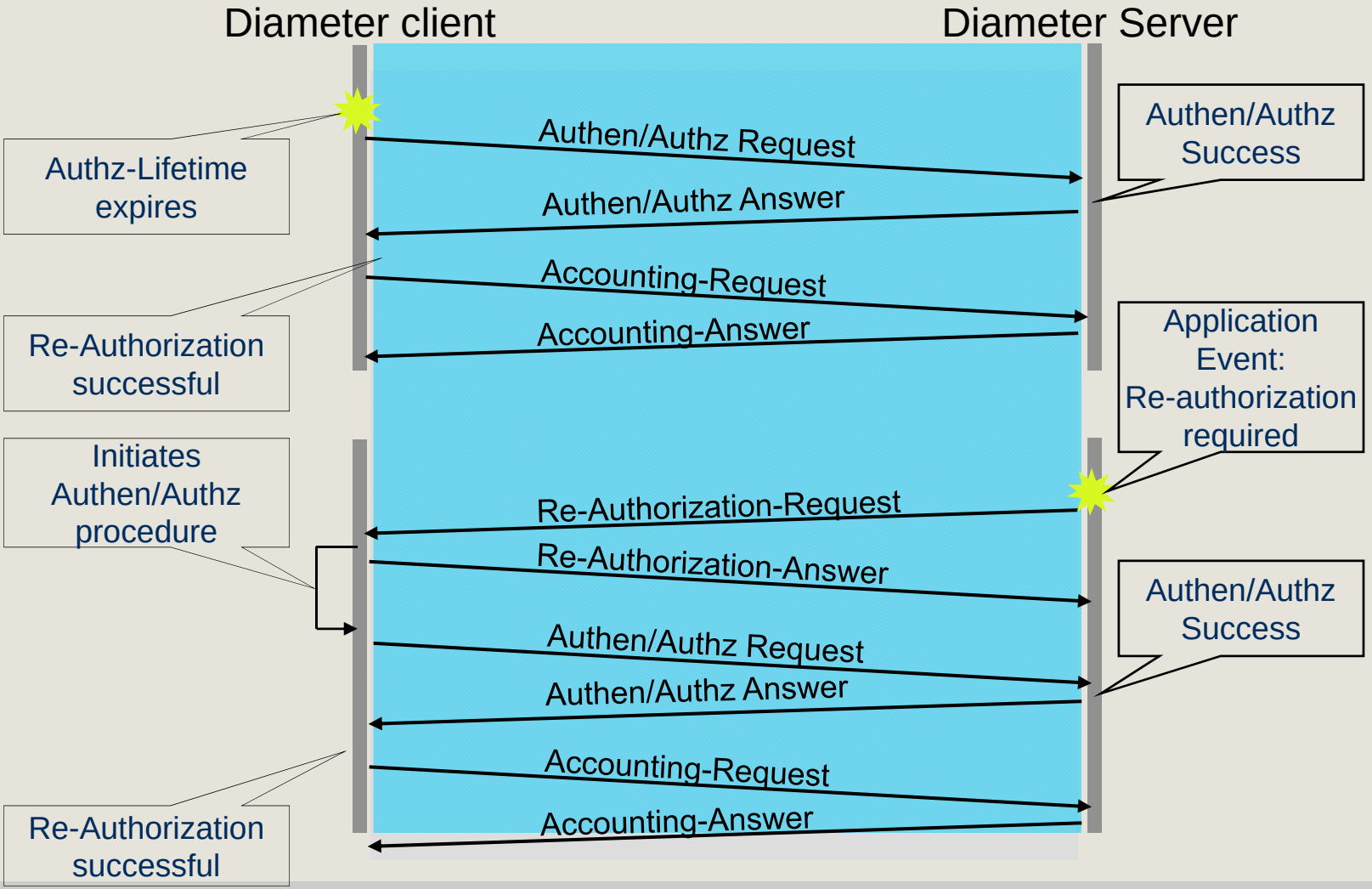
Separate Authorization and Accounting sessions maintained, but using the same DIAMETER server



*Commands and number of rounds are application specific

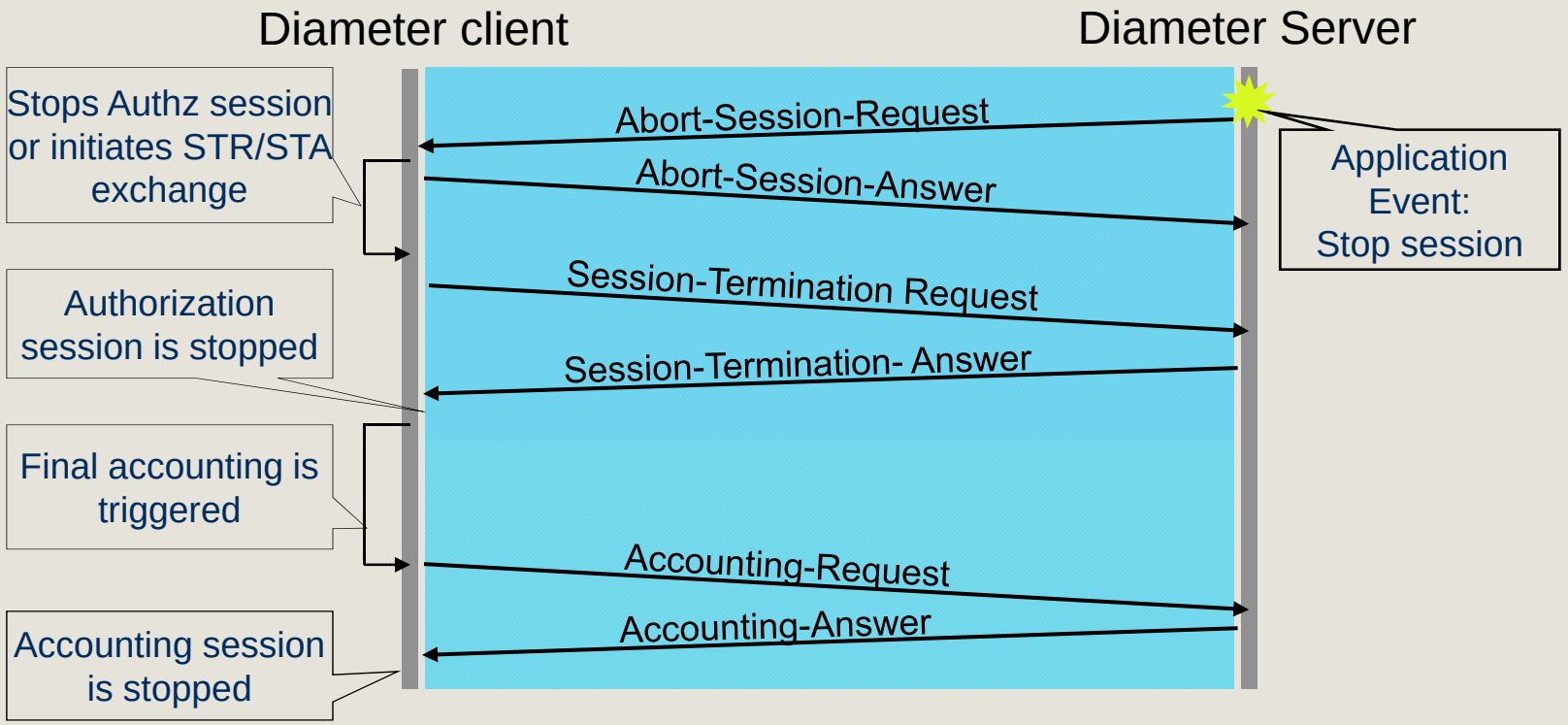
Basic operation DIAMETER (session re-Authorization)

Separate Authorization and Accounting sessions maintained, but using same DIAMETER server



Basic operation DIAMETER (session termination)

Separate Authorization and Accounting sessions maintained, but using same DIAMETER server



Outline

- Goal of this lecture
- What's AAA?
- Basic operation RADIUS
- Basic operation DIAMETER
- Main differences DIAMETER vs. RADIUS
- Summary & References

Main differences DIAMETER vs. RADIUS

- Better Transport
  - Diameter runs over reliable transport, TCP or SCTP
  - lost packets are retransmitted at each hop
  - persistent connection with application-level heartbeat message (called a Watchdog message) supports timely failover
  - TCP and SCTP adapt to network congestion
- Better Proxying
  - Hop-by-hop transport failure detection allows failover to occur at the appropriate place
    - proxies can locally failover to alternate next-hop peer
  - proxy automatically does retransmission of pending request messages following failover.

Main differences DIAMETER vs. RADIUS

- Better Session Control
  - Session management: independent of accounting
    - accounting information can be routed to different server than authentication/authorization messages
      - correlation between sessions needed => Acct-Multi-Session-Id AVP
    - session termination may be conveyed by a specific Session-Termination message rather than Accounting Stop message (when session ID authorization and session ID accounting different).
  - server may initiate message to request session termination
  - server may initiate message to request re-authentication and/or reauthorization of user
- Better Security
  - Hop-by-hop security is provided using IPsec or TLS
  - Automatic secret key exchange
  - End-to-end security is guaranteed

Outline

- Goal of this lecture
- What's AAA?
- Basic operation RADIUS
- Basic operation DIAMETER
- Main differences DIAMETER vs. RADIUS
- Summary & References

Summary, references & info homework assignments

Understand:

- AAA concept
- Main characteristics of RADIUS protocol
- Main characteristics of DIAMETER protocol
- Main differences between RADIUS and DIAMETER

References

- Many used RFCs can be located via

  http://www.ietf.org/rfc.html <then type RFC number>

  – RFC1321, RFC2903, RFC2905, RFC2904, RFC1492, RFC2865, RFC3588, RFC2866, RFC2869, RFC3579, RFC3162, RFC4372, RFC3580, RFC4740, RFC5447, RFC5624, RFC5777, RFC5778 RFC5779, RFC5866

Summary, references & info homework assignments

Homework assignments can be found via Blackboard and via: http://wwwhome.cs.utwente.nl/~pras/netsec/

- answers to homework exercises need to be sent by email to following email address before Monday 01 October, 23:55!
- Please Include "Lecture number (4B) and the number (4.B.1, 4.B.2, 4.B.3) of the exercise(s)" in the title/subject line of the email?
- Email address: network.security@ewi.utwente.nl