

ROHC over ULE & MPEG2-TS

<http://tools.ietf.org/html/draft-wan-ipdvb-rohc-01>

Wan Tat Chee (tcwan@cs.usm.my)

Ang Way Chuang (wcang@nav6.org)

Teh Chee Hong (chteh@nav6.org)

Universiti Sains Malaysia

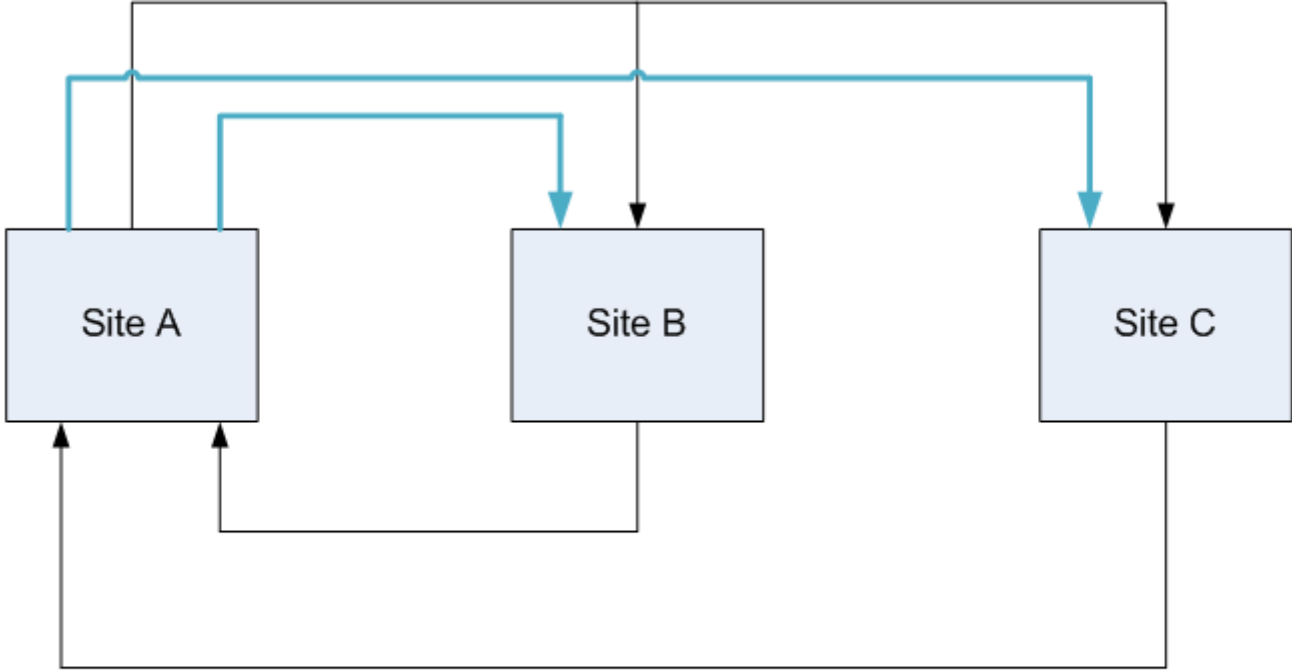
Objectives

- Provides better bandwidth utilization.
- Reduce redundancy in headers using ROHC (RFC 3095).

Channels

- Logical channel through PID of MPEG2-TS
- Two types of channels:
 - ROHC channel – dedicated to a pair of nodes. Carries compressed streams.
 - Uncompressed channel – shared by all. Carries uncompressed streams.

ROHC & uncompressed channels



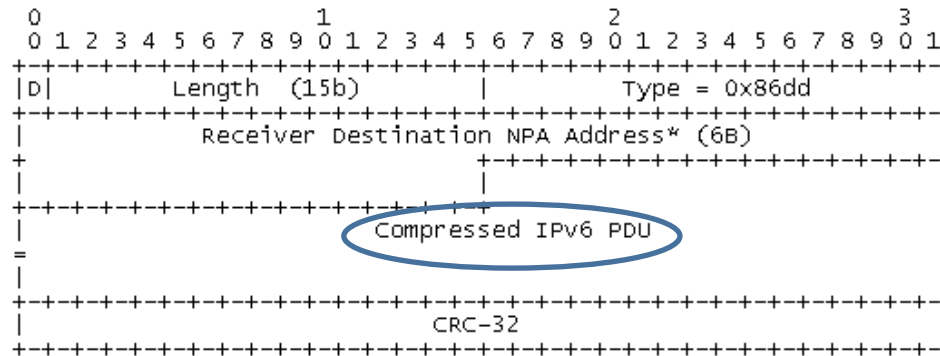
—▶ Uncompressed channel

—▶ ROHC channel

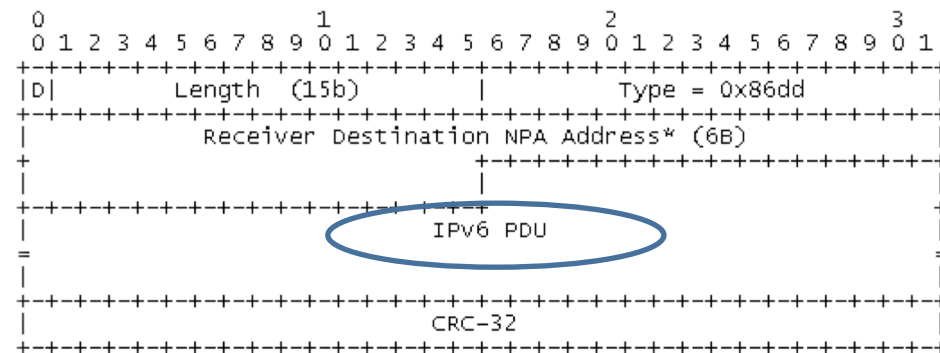
Encapsulation Format

- Structure of ROHC compressed ULE SNDU is similar with uncompressed ULE SNDU except for the ULE payload.
- ROHC feedback can be piggybacked through ROHC compressed ULE SNDU or sent independently. May be sent through uncompressed channel or ROHC channel.
- ROHC feedback requires Receiver Destination NPA address in uncompressed channel.

Comparison of packet format

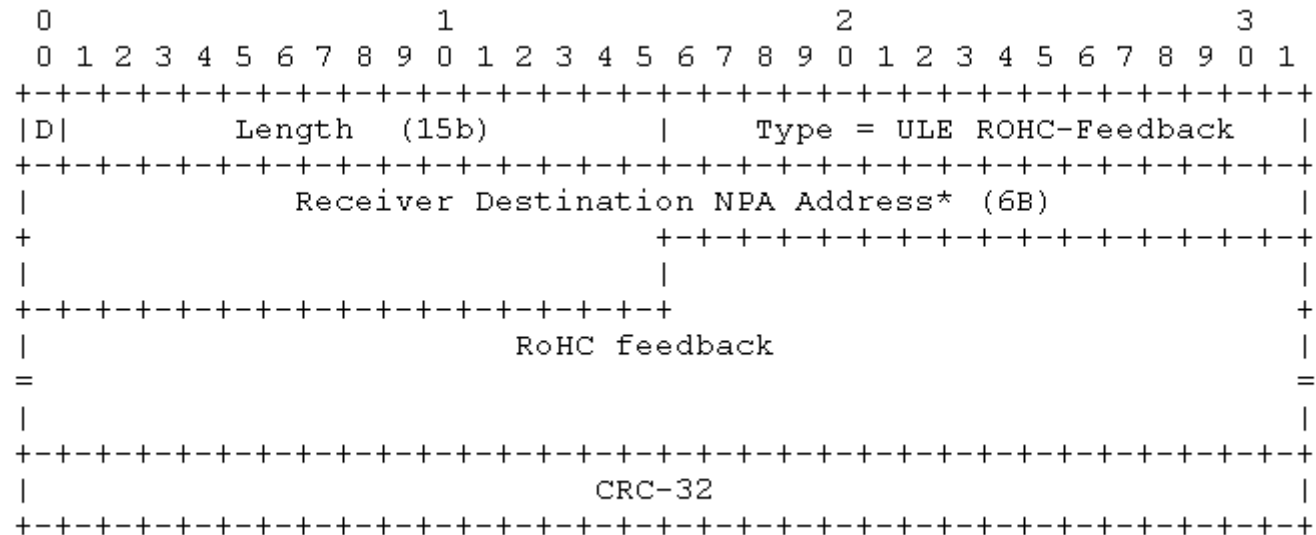


Only in ROHC
channel



Only in
uncompressed
channel

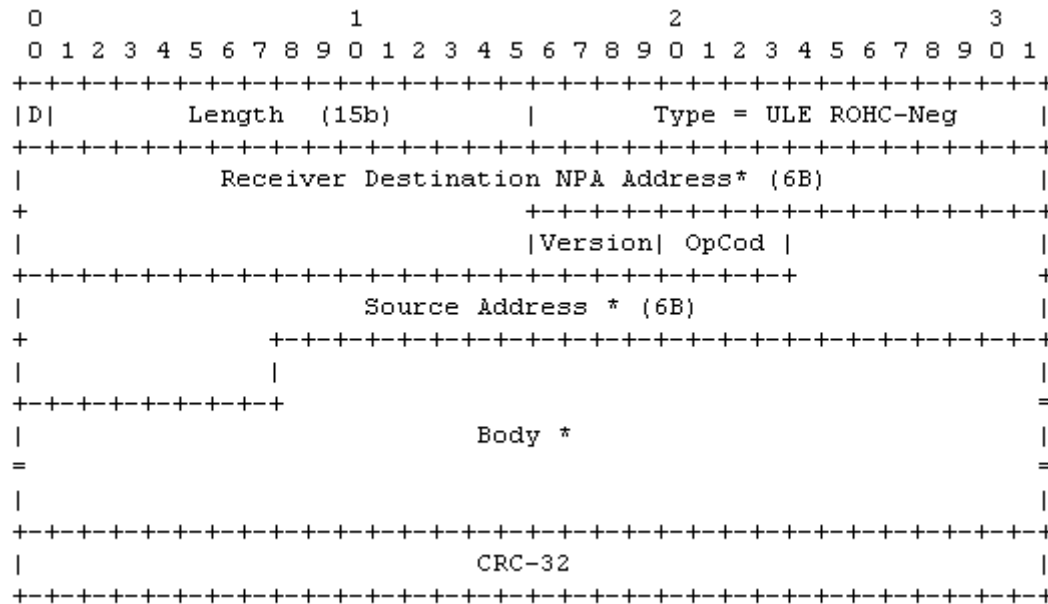
Format of ROHC Feedback



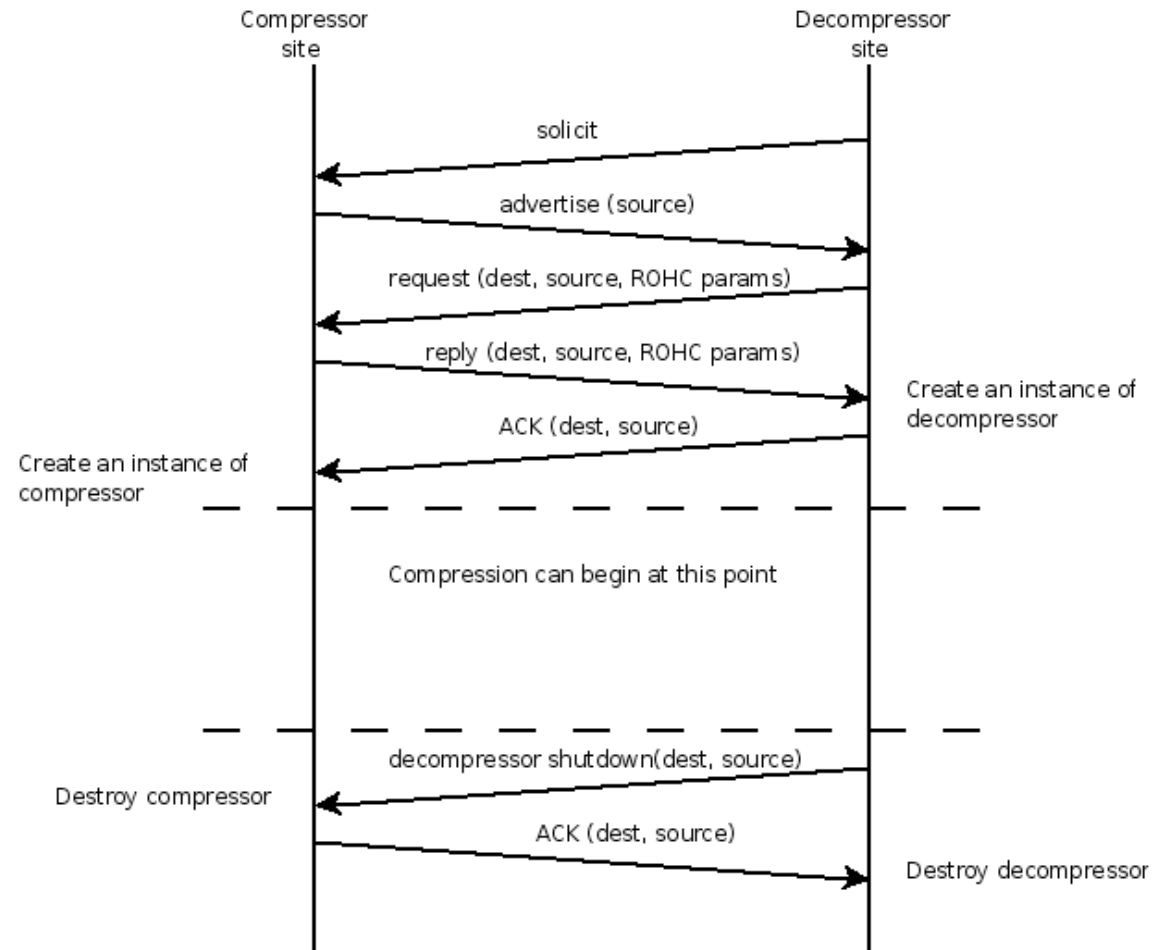
Automate the setup of ROHC channels

- Negotiate parameters of ROHC channel through uncompressed channel
- ROHC Channel Parameters Negotiation Protocol (RCPNP).
- Decompressor site solicits for compressor. Compressor advertises itself.
- Exchange of ROHC parameters then follows.

Format of RCPNP message



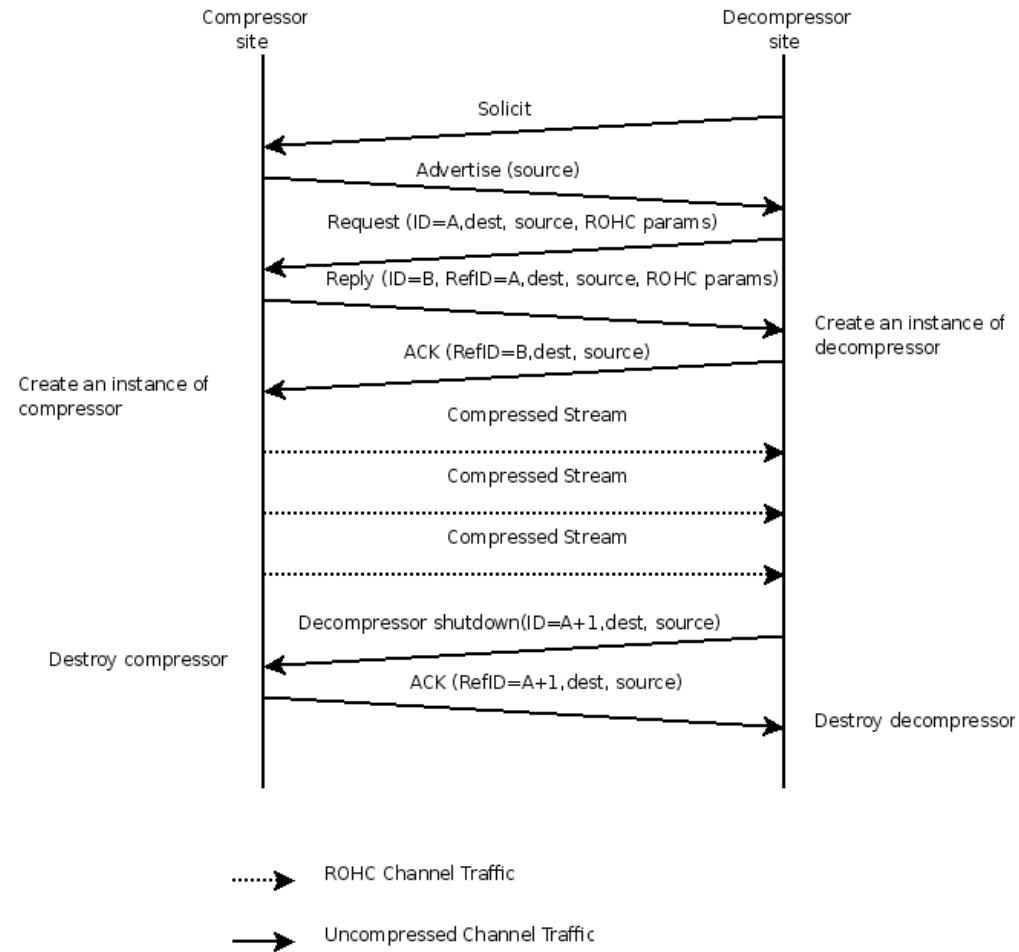
Negotiation Protocol



Negotiation Protocol

- Simple protocol.
- Decompressor site solicits for compressors.
- ROHC channel parameters negotiated through Request & Reply message.
- RCPNP has some weaknesses in current draft.
 - Ambiguity of ACK & NACK (ACK/NACK for which message).
 - Need to discover if compressor/decompressor exit abnormally

Negotiation Protocol (next draft)



Negotiation Protocol (next draft)

- Add ID to certain messages.
- NACK/ACK carries Reference ID to identify the message it's responding to.
- Add heartbeat to check for presence of counterpart if ROHC channel is idle.
- Do we need to prevent against man in the middle attack?

Topological Learning

- Compressor site needs to decide which ROHC channel to use before compression.
- Compressor site needs to listen on its receiver and maps address to a ROHC channel.
- No mapping means no compression.
- Susceptible to attack if a site injects a fake packet messing the mapping of address & ROHC channel.

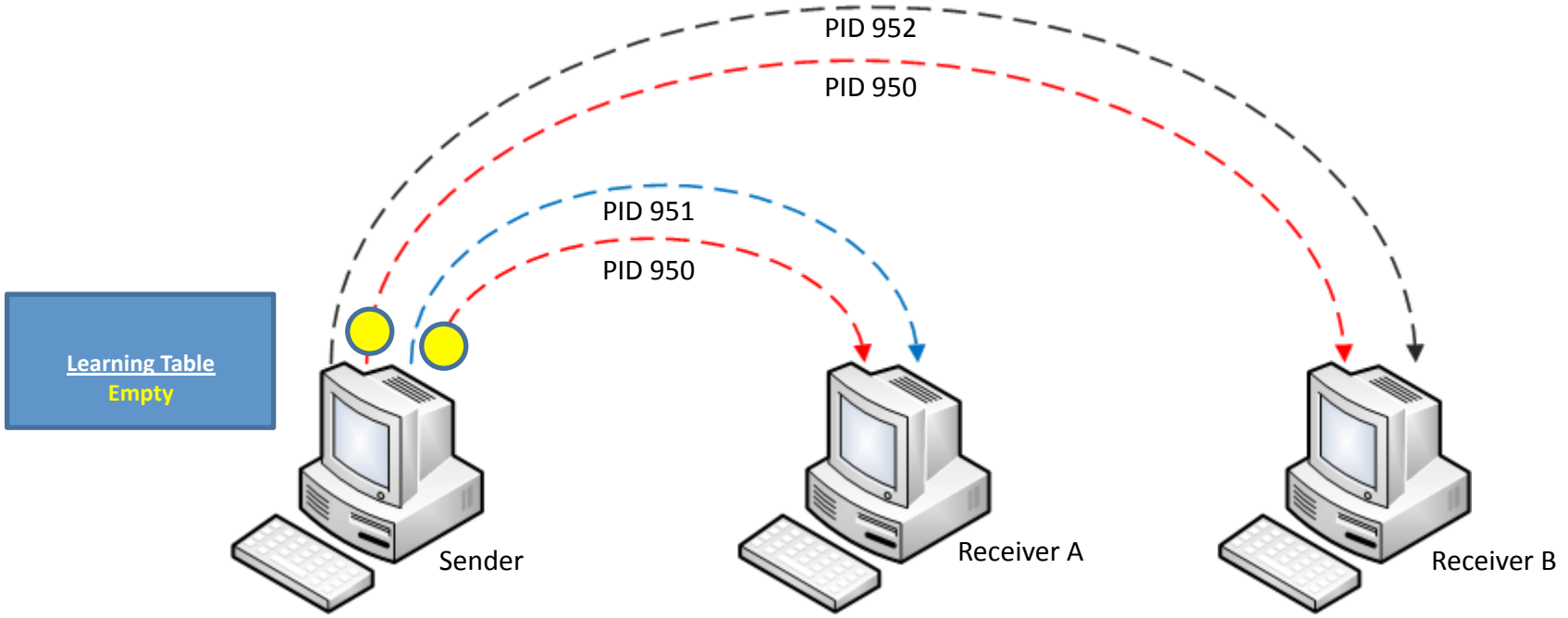
Topological Learning

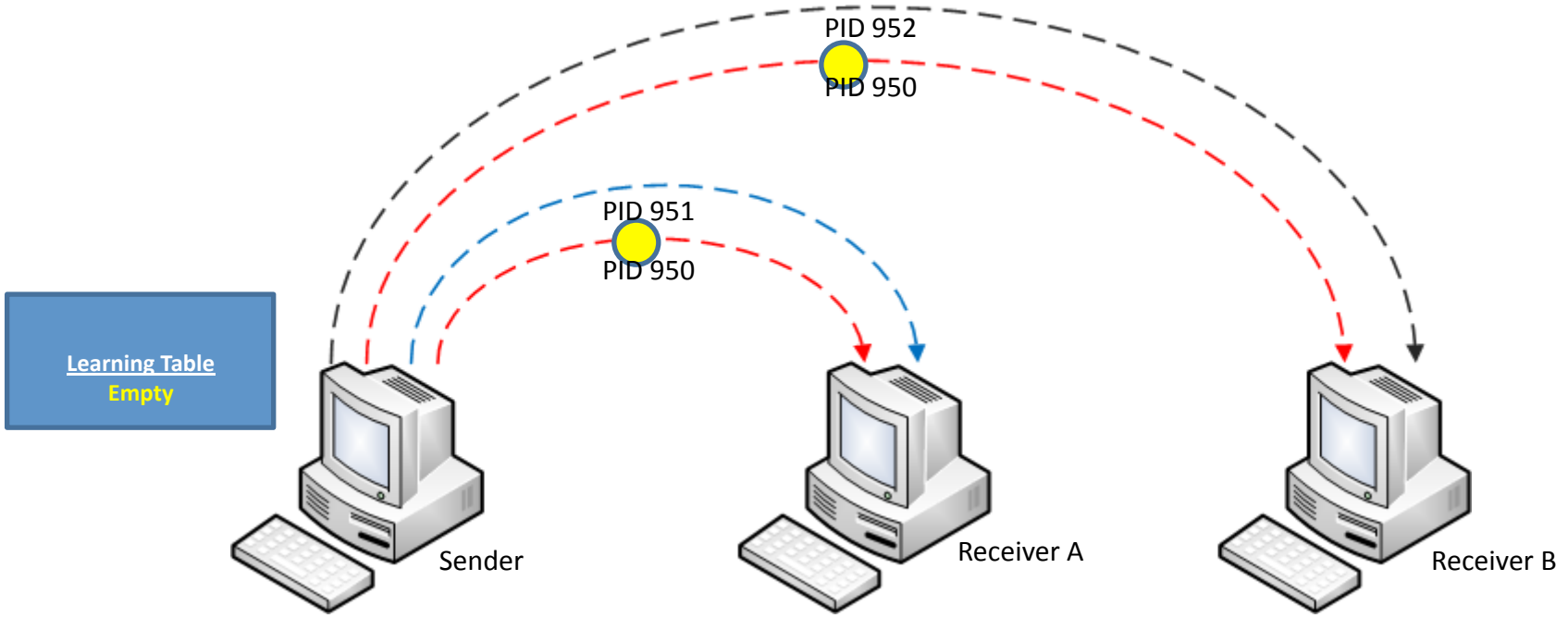
- Partial solution to this problem is to disable compression when compressor site detects conflicting mapping of address & ROHC channels.
- Only works if victim site sends a packet to sender. Otherwise, it won't receive any data from sender.
- Any idea to solve the vulnerability?

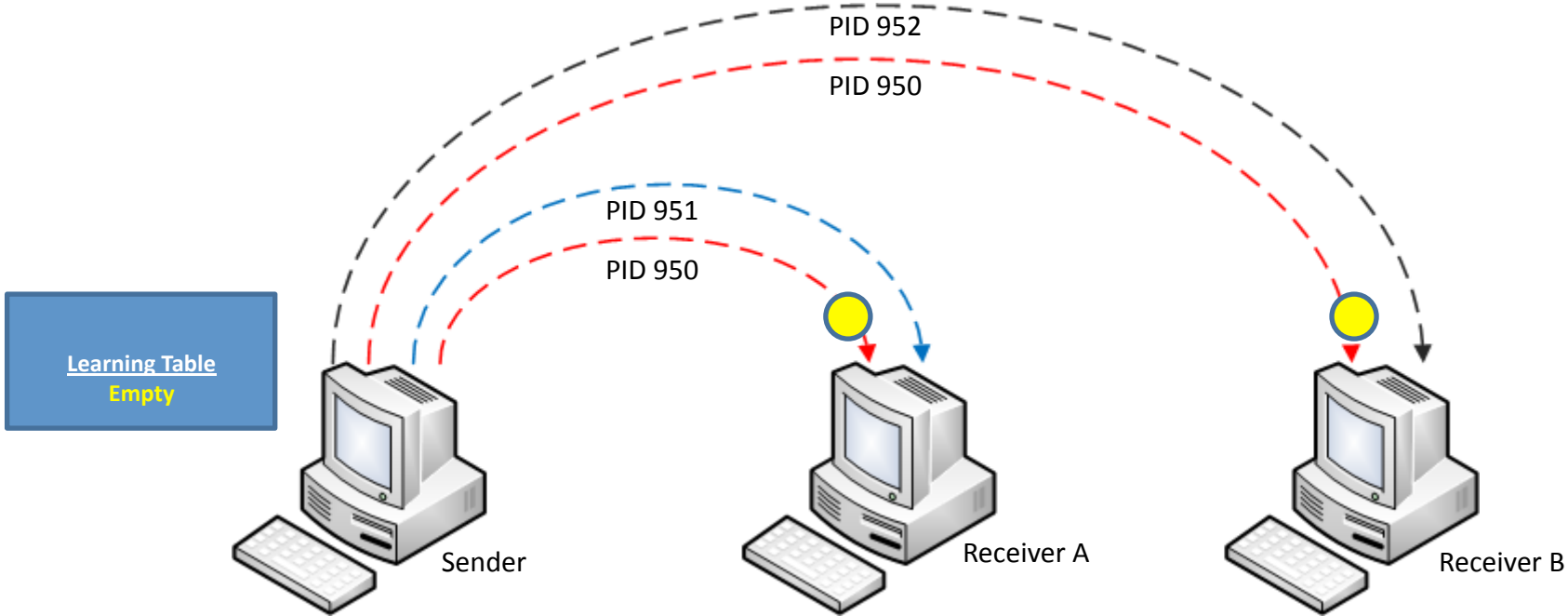
Thank you

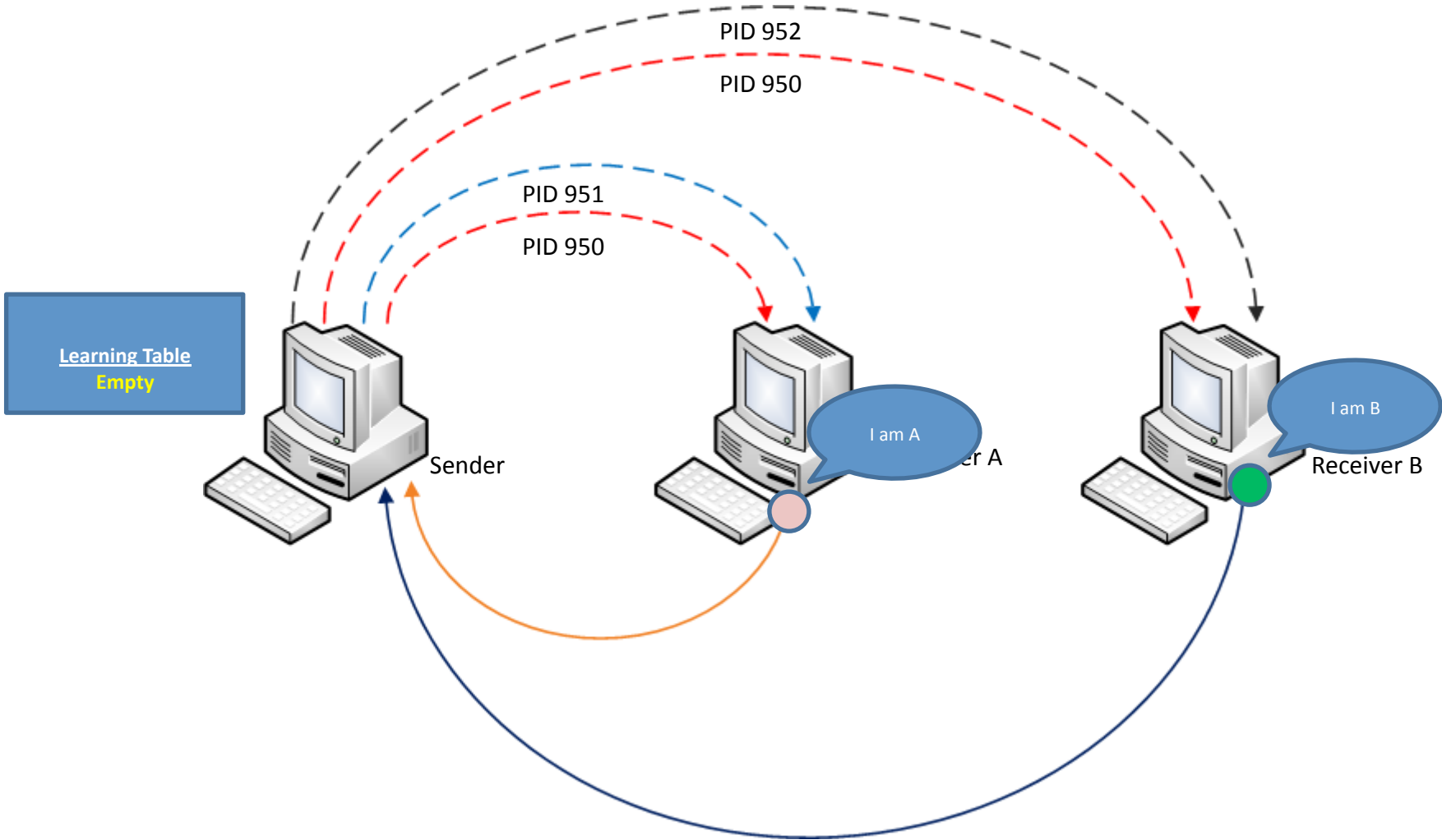
- Q & A

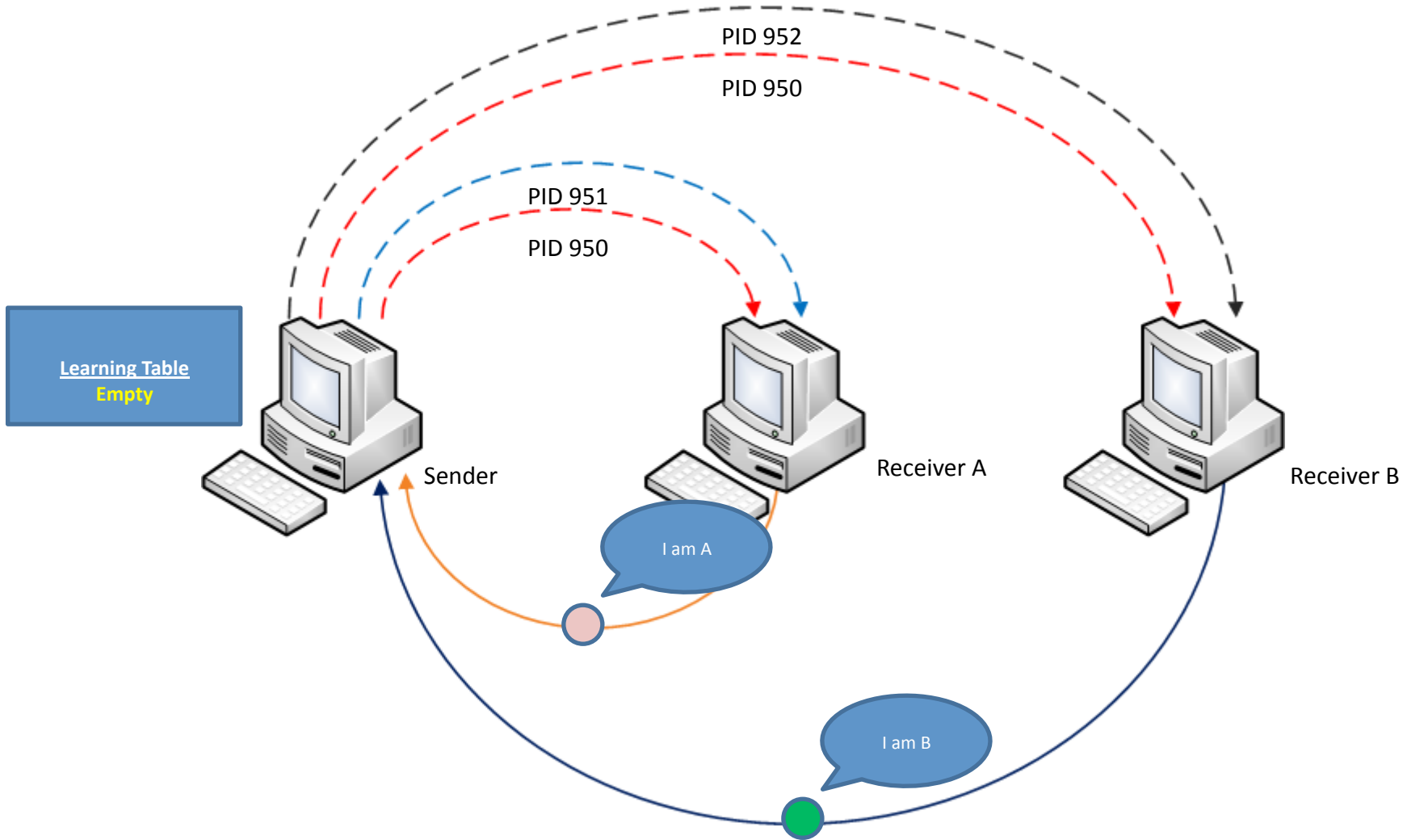
Topological Learning

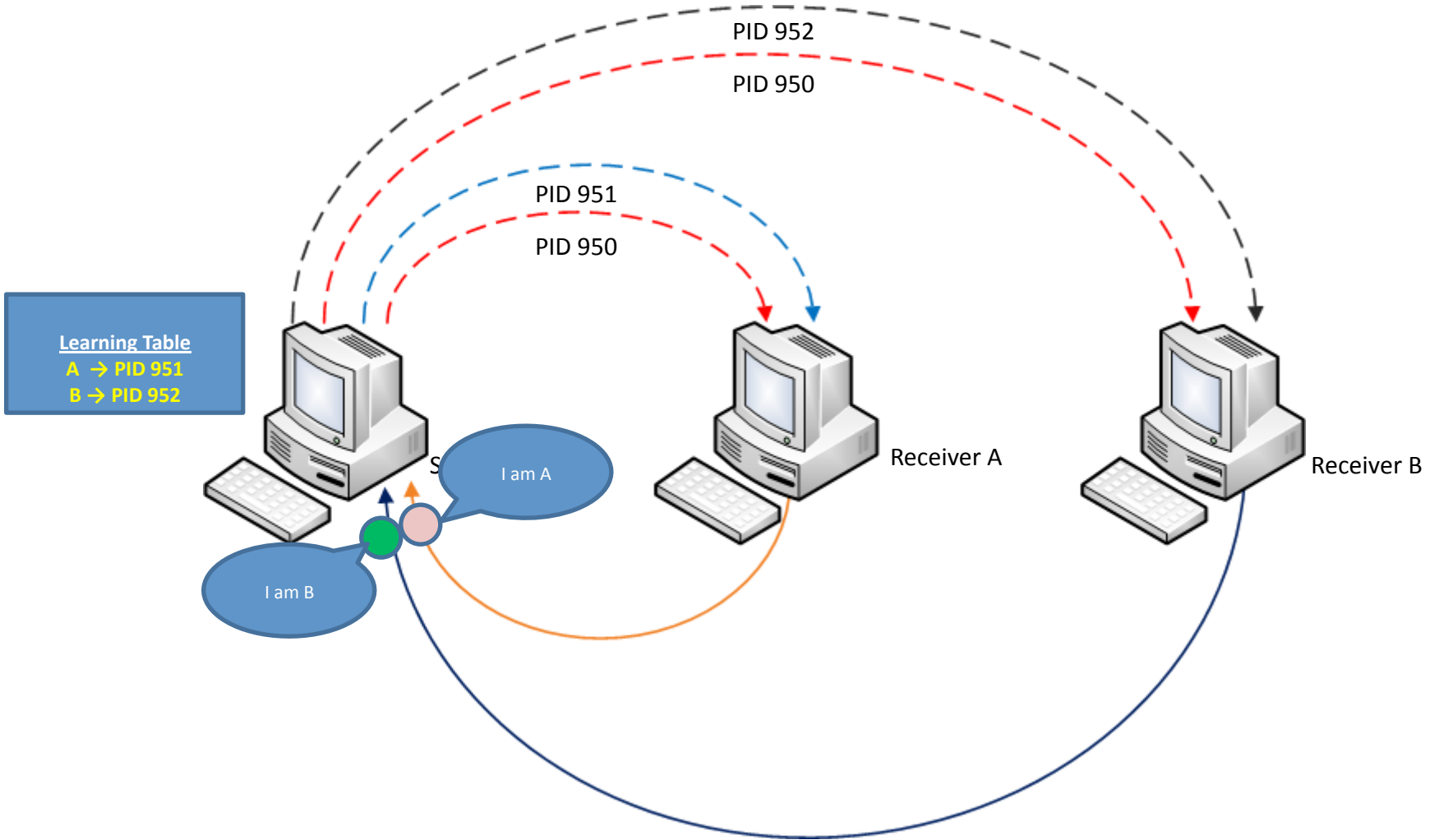




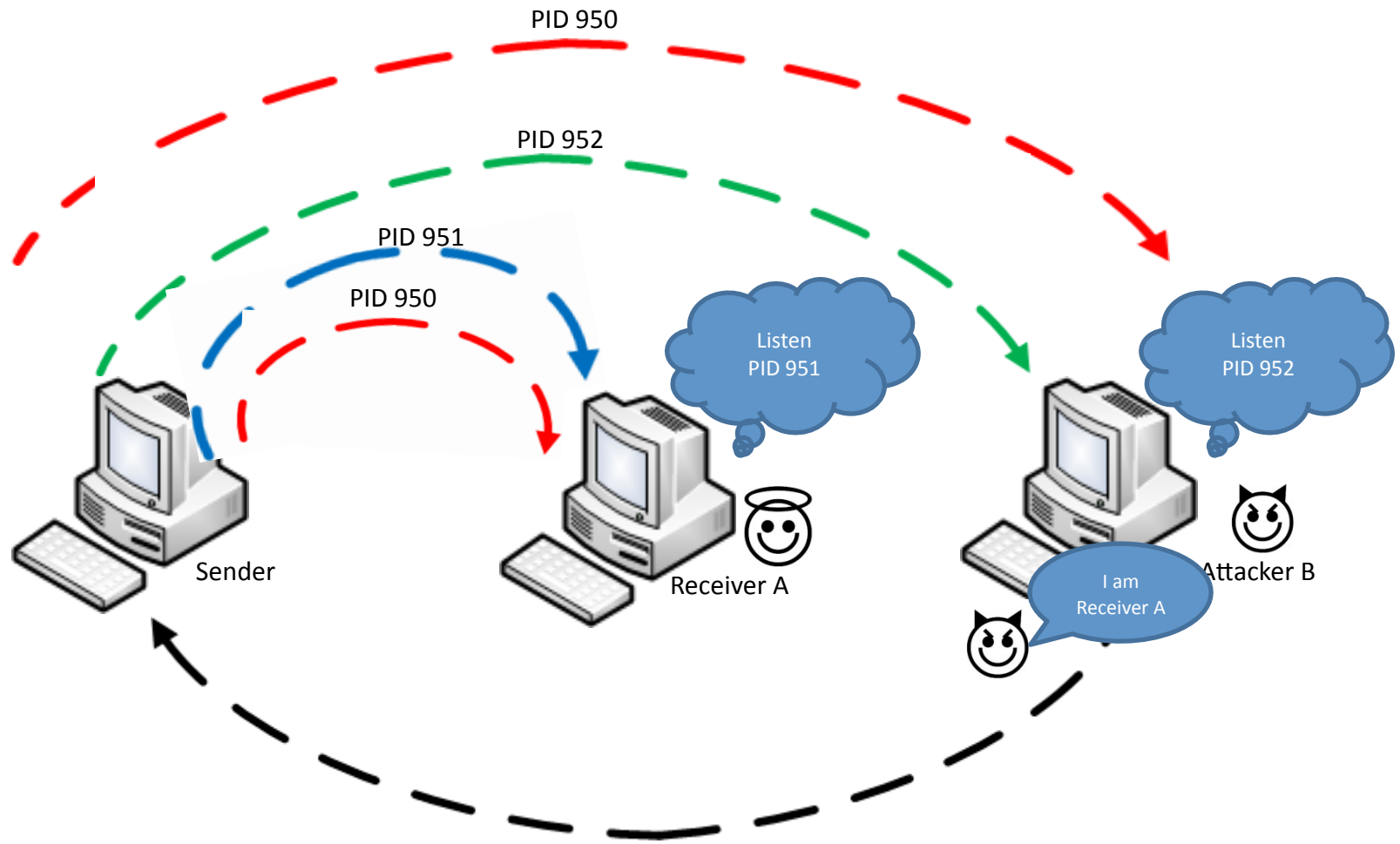


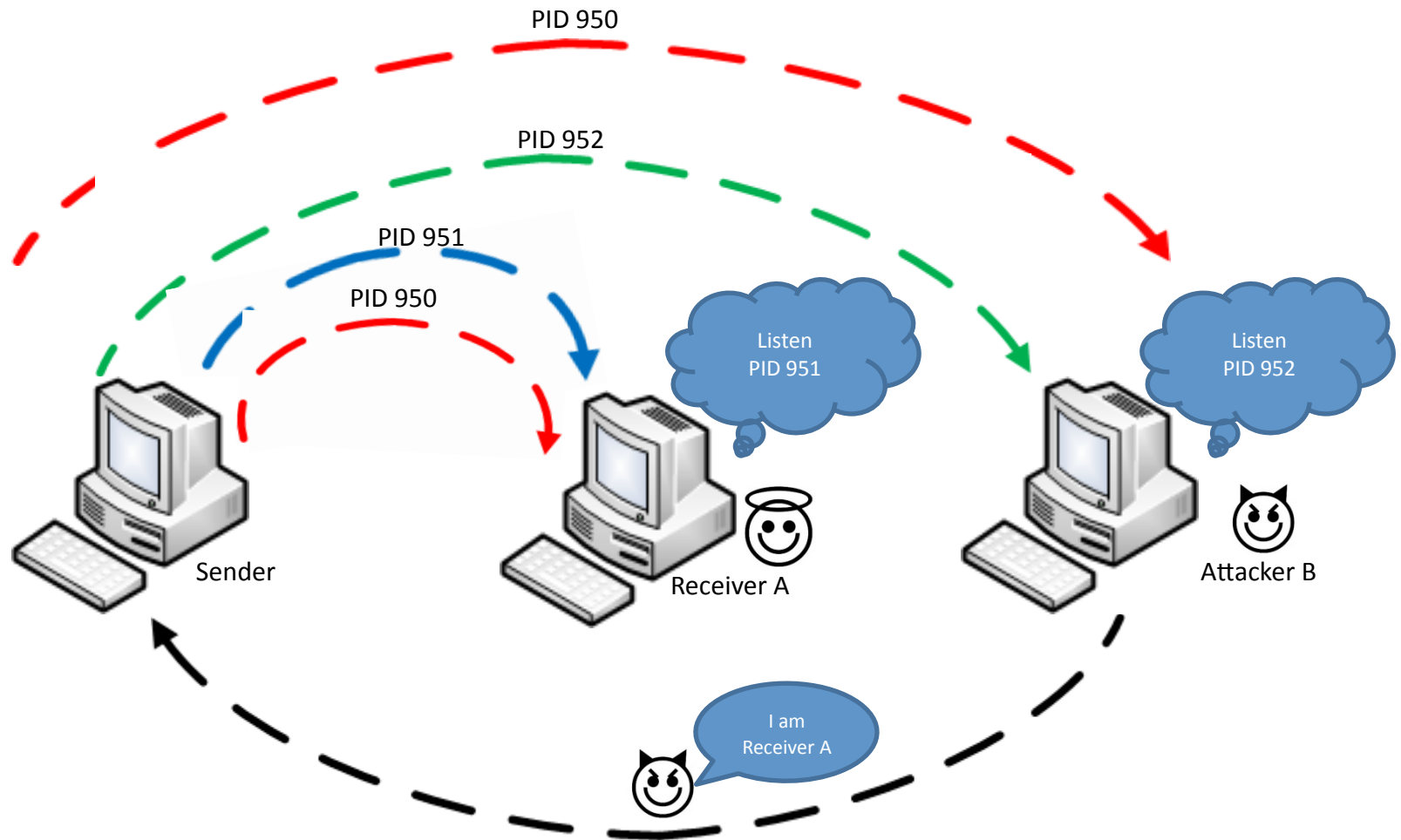


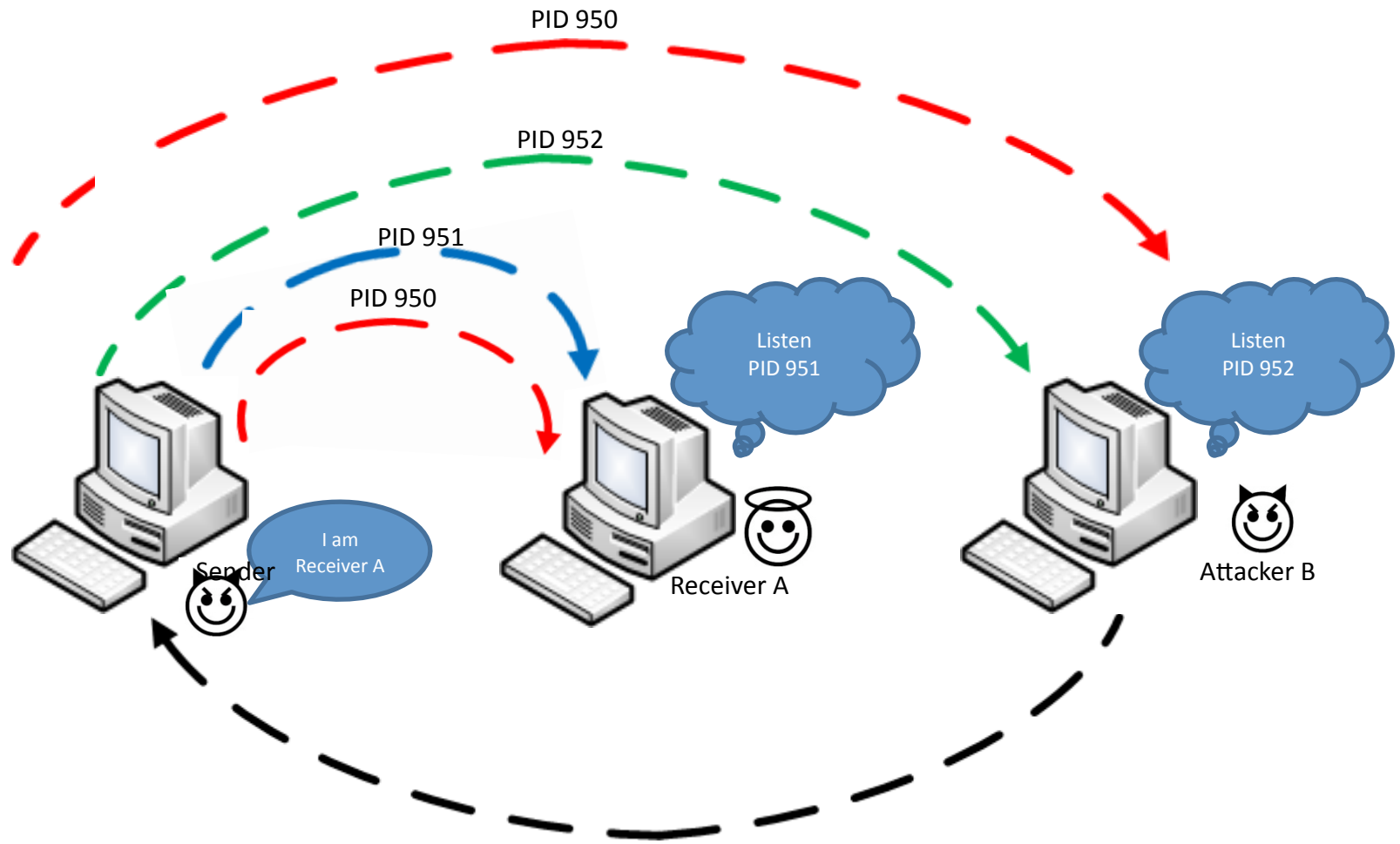


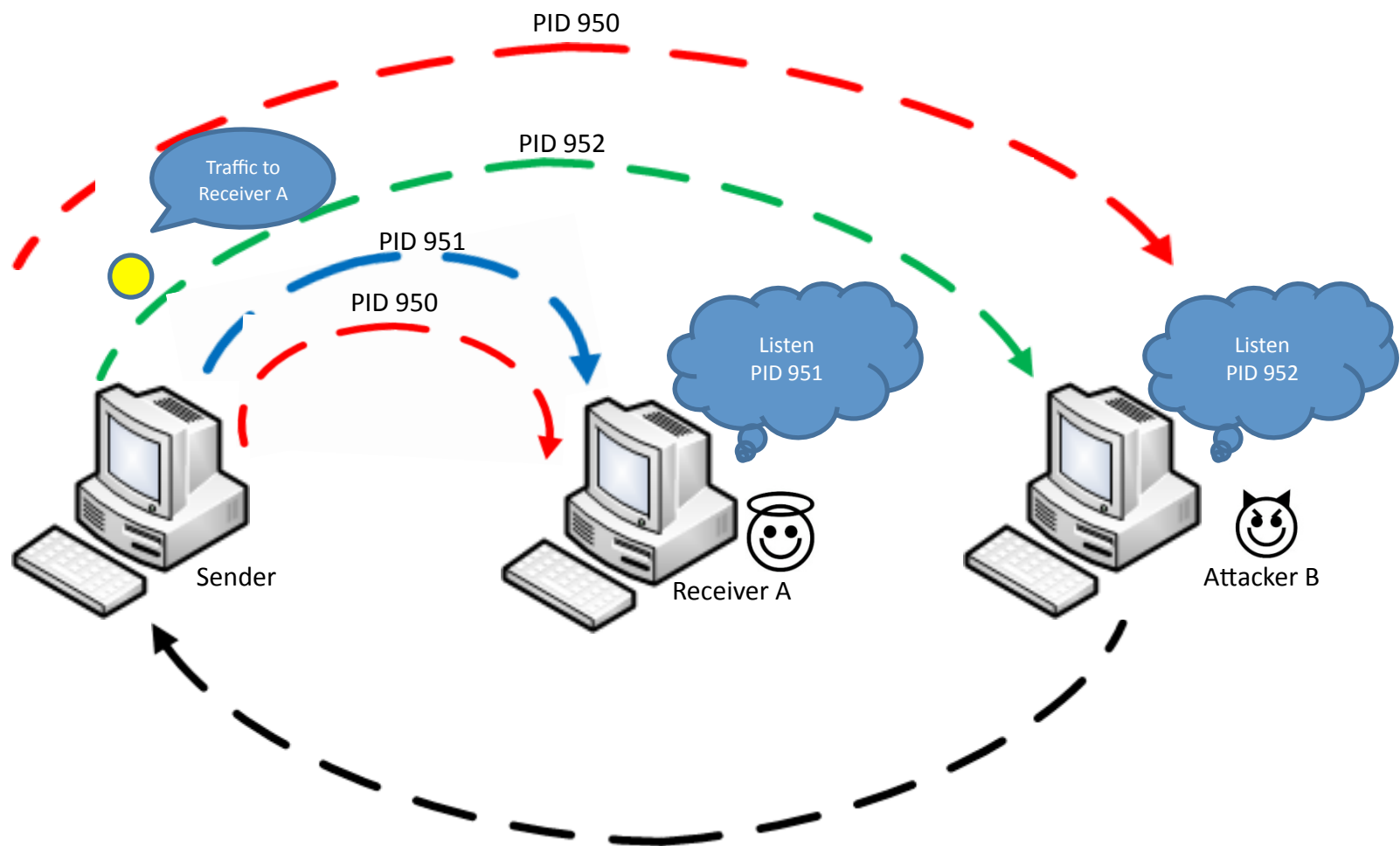


Vulnerability

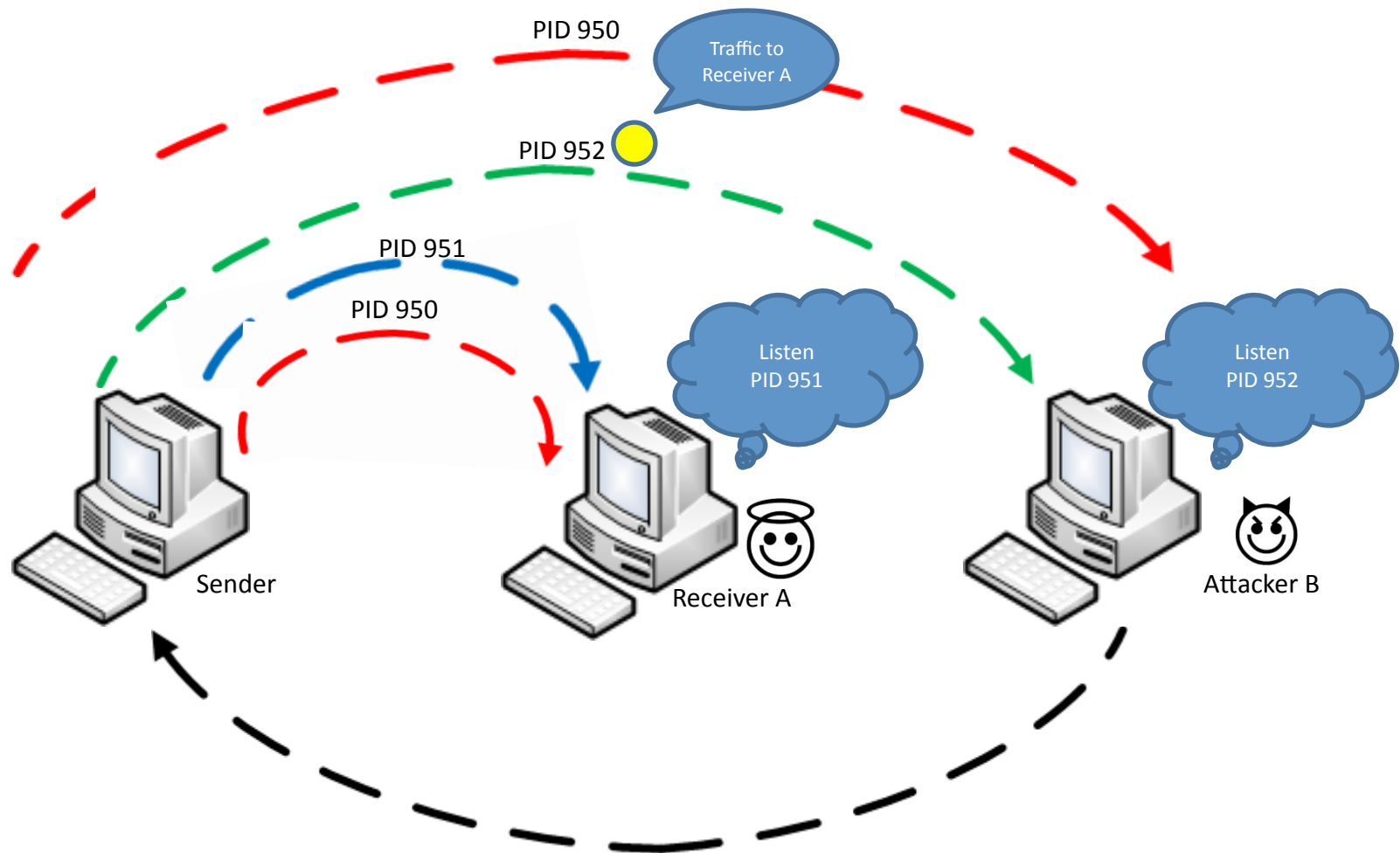


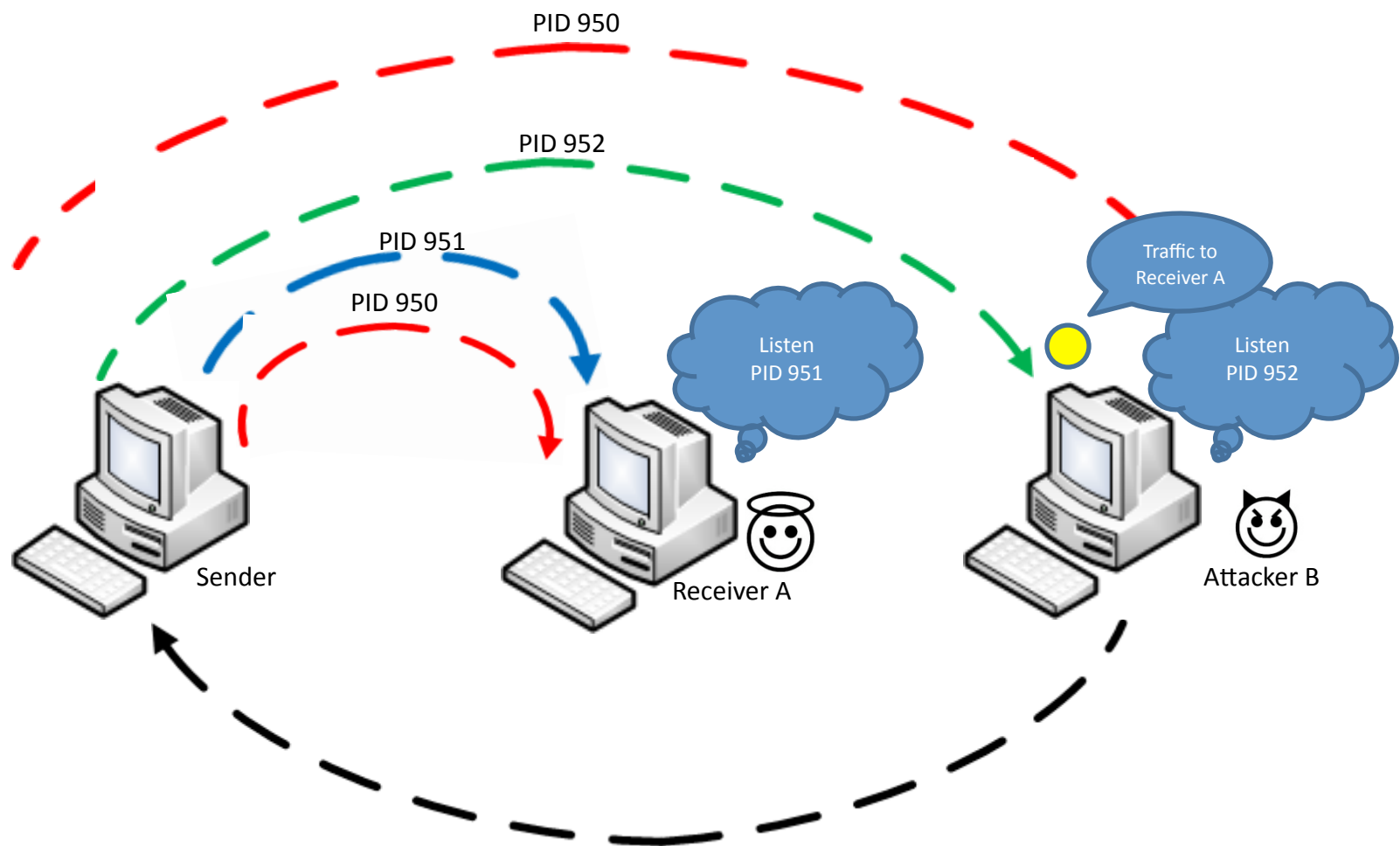






- - ➔ ROHC Channel (PID 951)

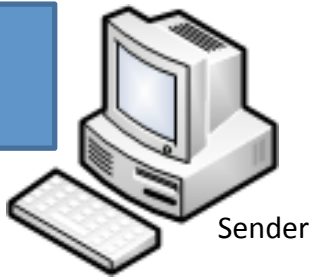




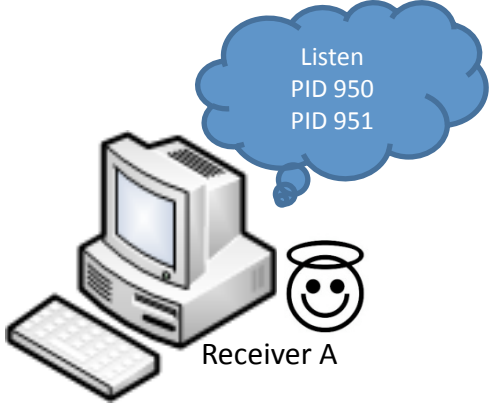
---> ROHC Channel (PID 951)

Partial Solution

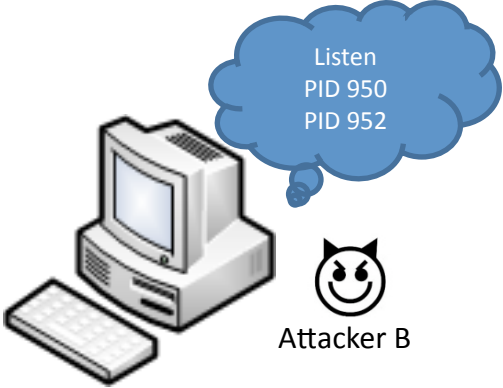
Learning Table
Empty



Sender



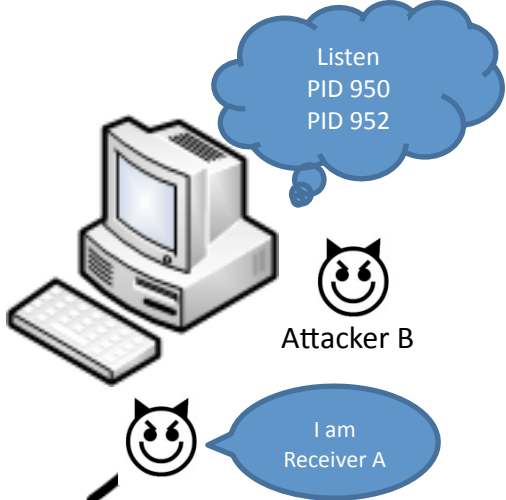
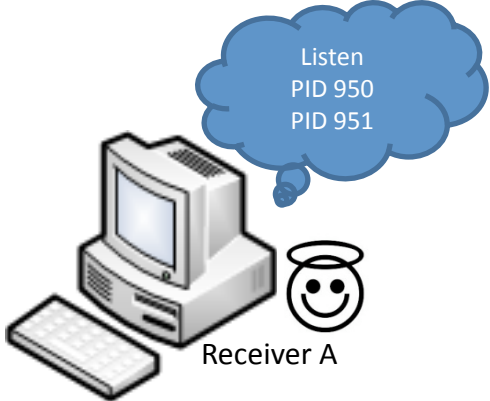
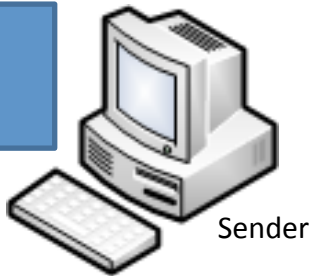
Receiver A



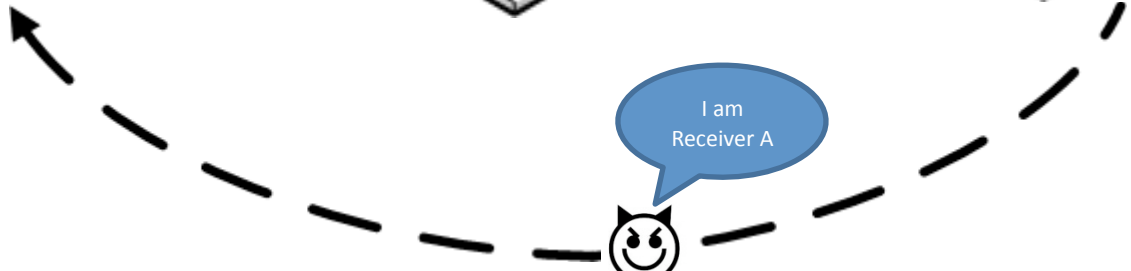
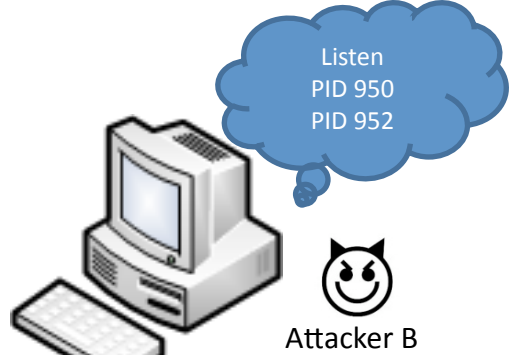
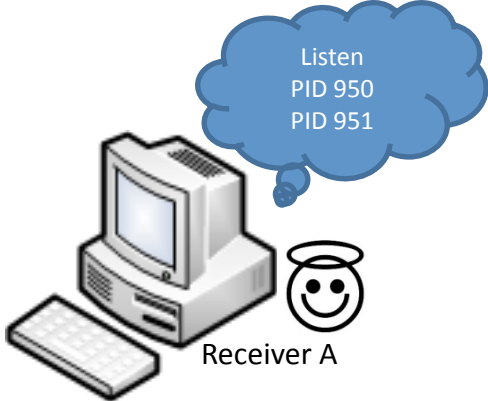
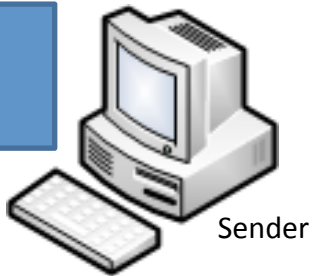
Attacker B

-- ➔ ROHC Channel (PID 951)

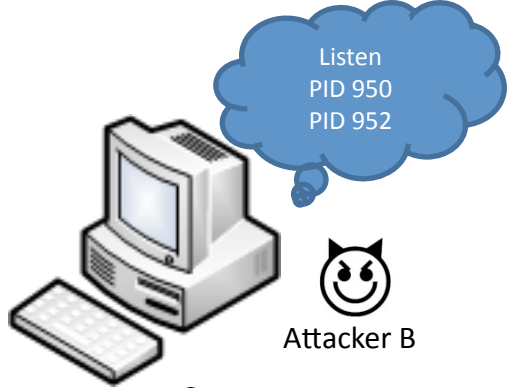
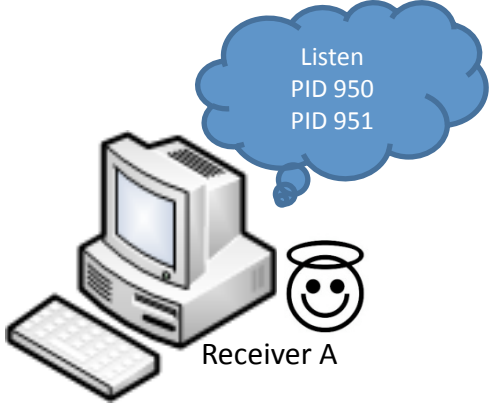
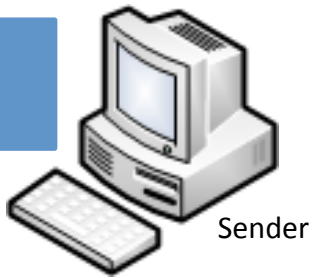
Learning Table
Empty



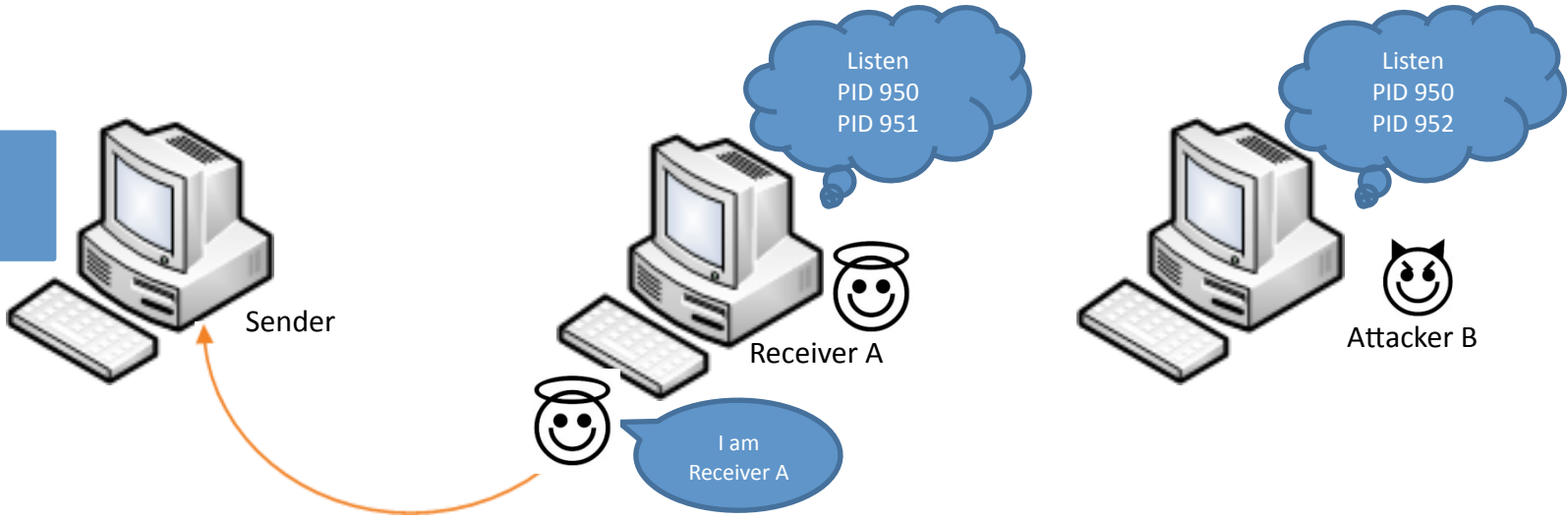
Learning Table
Empty



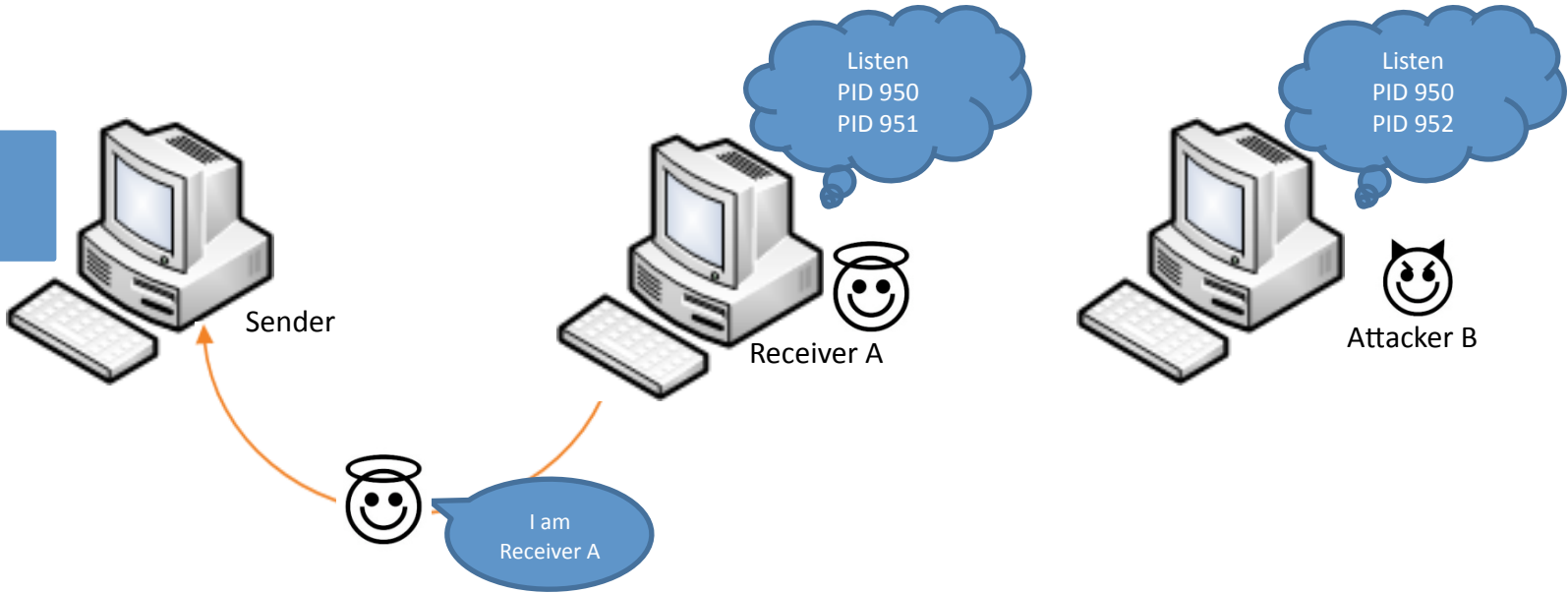
Learning Table
A → PID 952



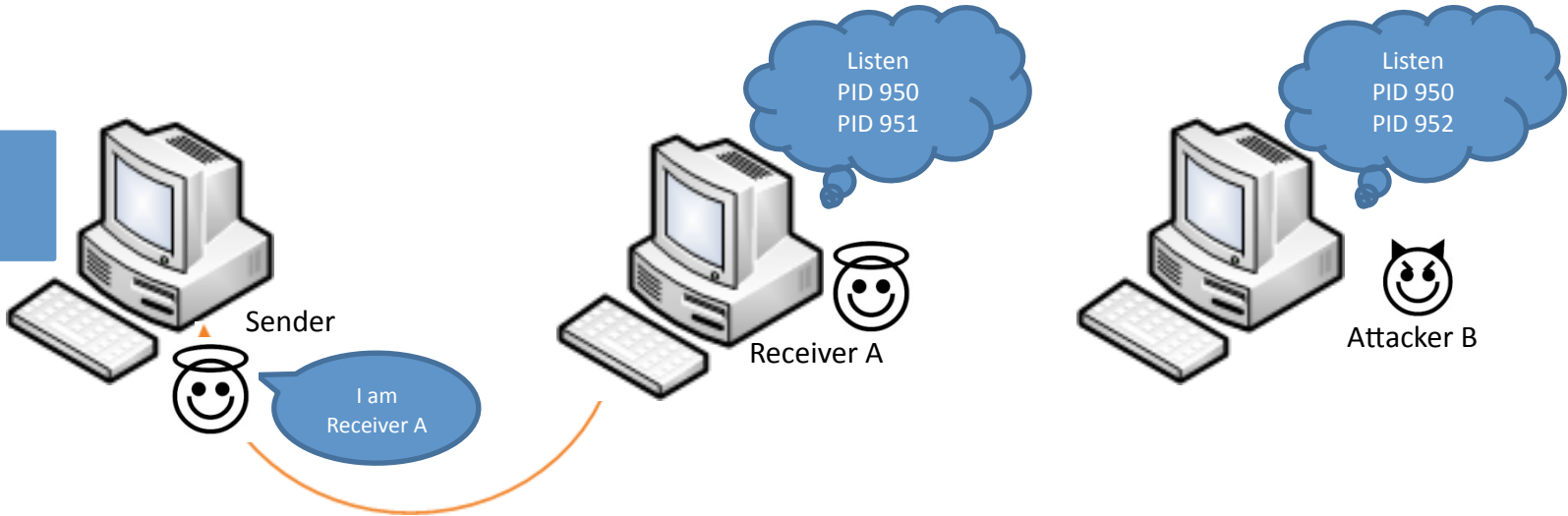
Learning Table
A → PID 952



Learning Table
A → PID 952



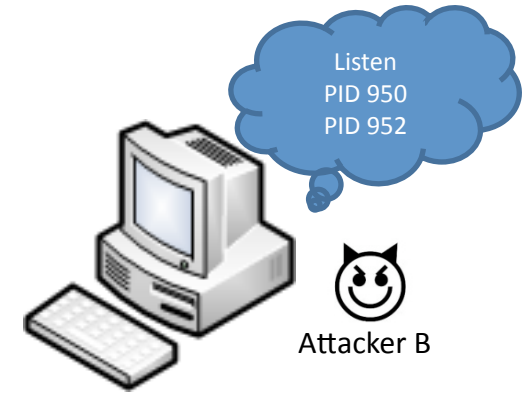
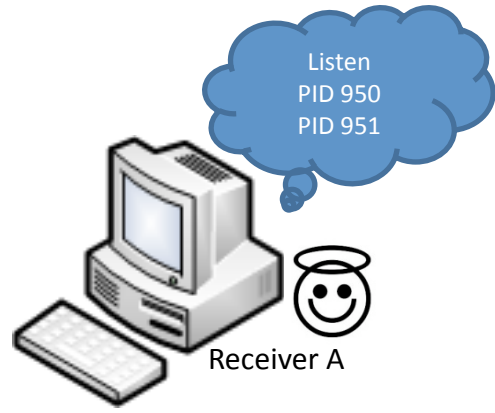
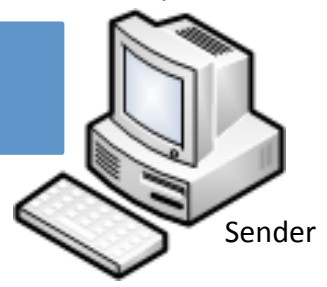
Learning Table
A → PID 952
A → PID 951



Duplicated PID
to the same
Receiver



Learning Table
A → PID 952
A → PID 951

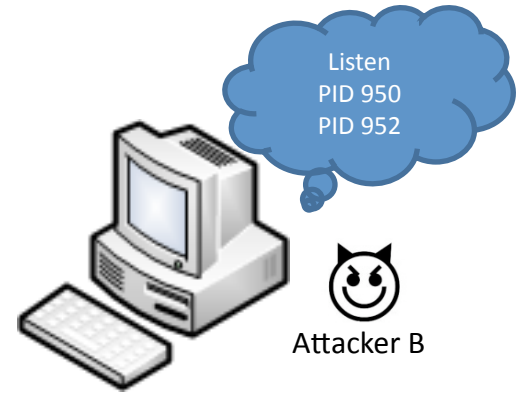
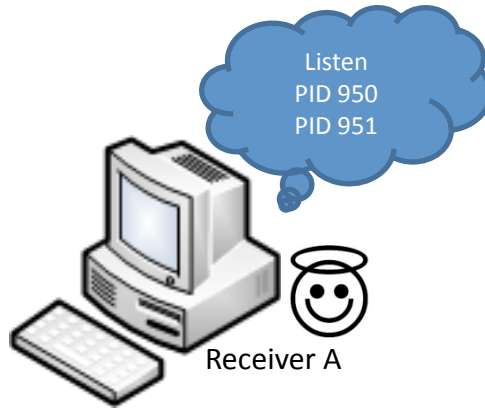
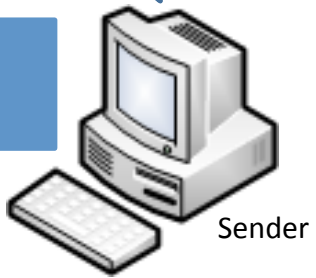


-- ➔ ROHC Channel (PID 951)

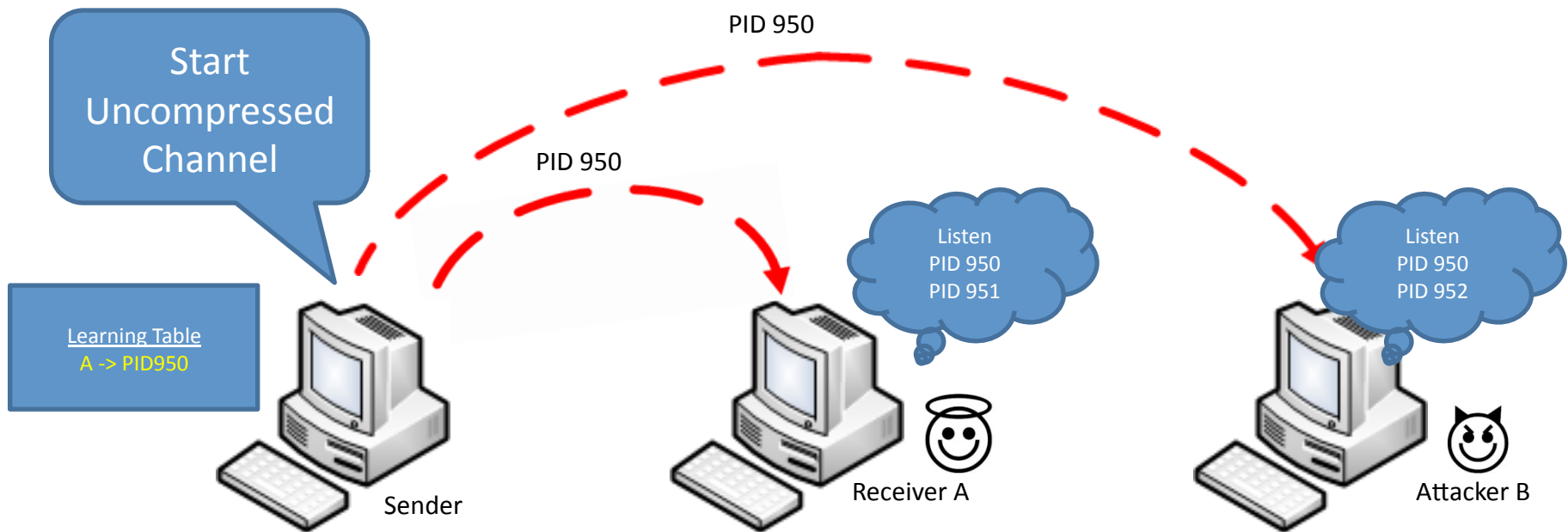
Stop sending through ROHC Channel



Learning Table
A → PID 952
A → PID 951



-- ➔ ROHC Channel (PID 951)



--> Uncompressed Channel