PANA Framework

53rd IETF - Minneapolis, MN

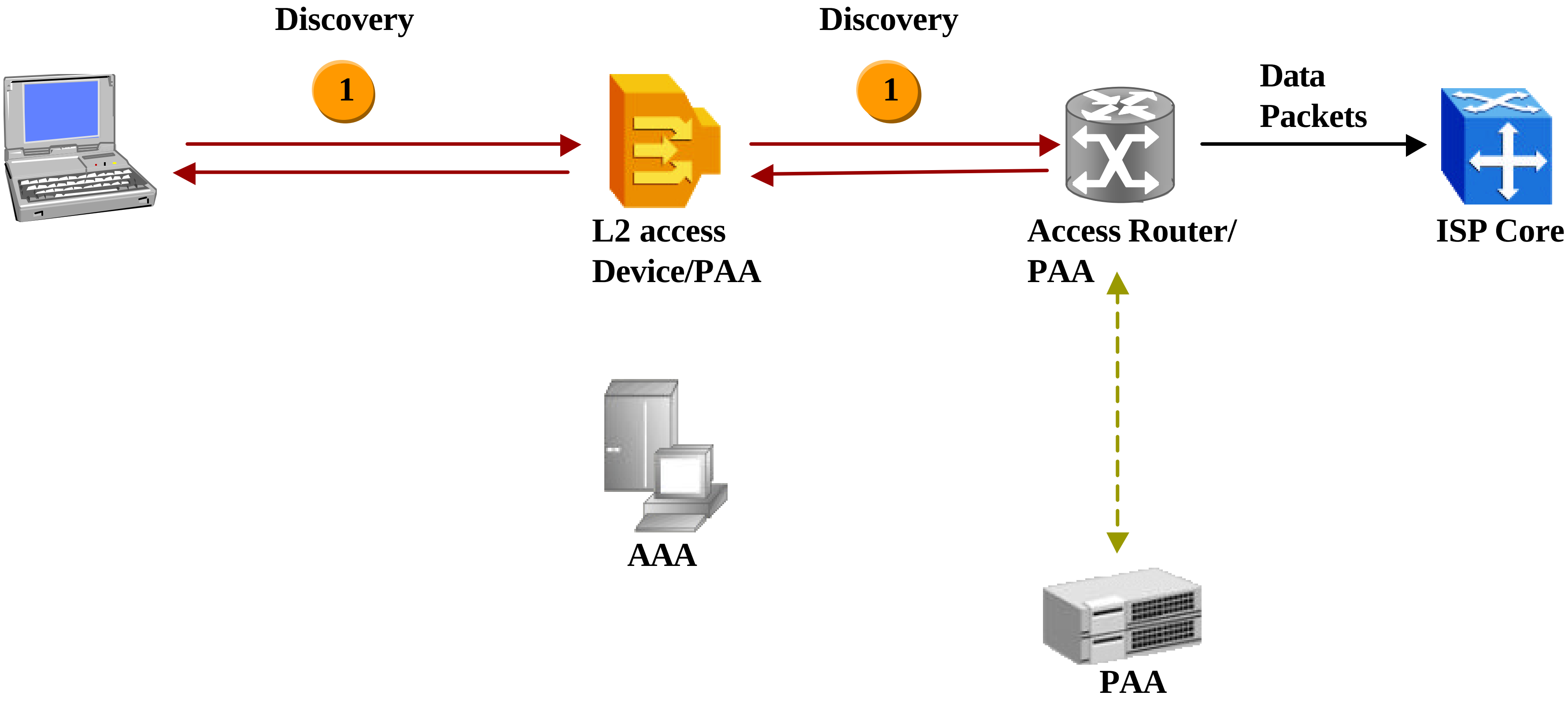
Reinaldo Penno rpenno@nortelnetworks.com

Contributions from James Carlson, Alper Yegin, Yoshihiro Ohba and Basavaraj Patil

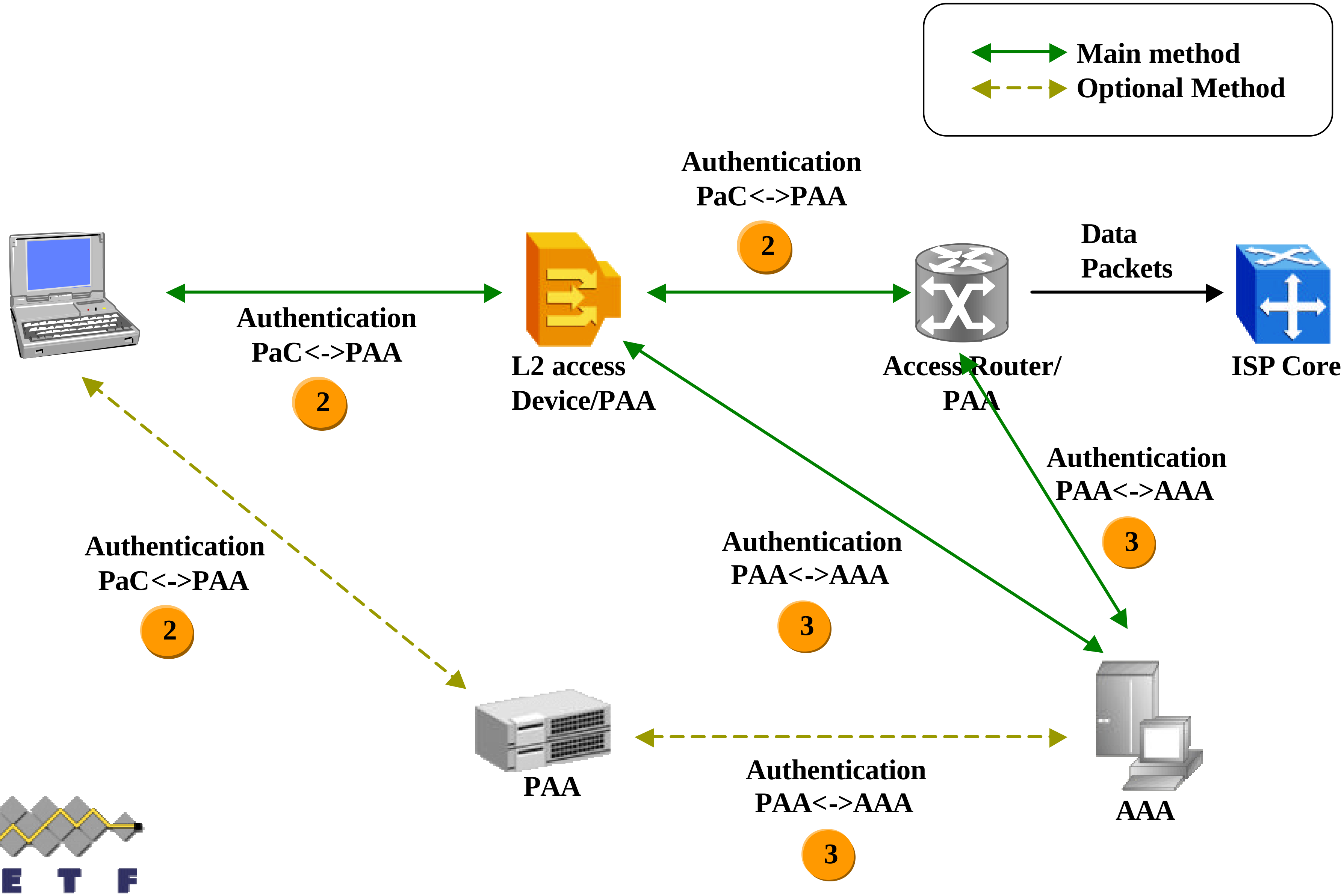
PANA Framework Issues in Charter

- The relative location of the PAA and any access control functions in the network and how their location affects the performance and scalability of the PAA solution, as well as the tradeoffs in the level of access control enforcement. (in framework draft)
- Chosen approach for handling the security issues and which existing security mechanisms that are chosen for the protocol. (in framework draft)
- What assumptions the protocol is making on the AAA infrastructure e.g. in terms of security. (in framework draft)

The Big Picture – Message Framework



The Big Picture – Message Framework



Main method

Optional Method

Authentication
PaC<->PAA
2

L2 access
Device/PAA

Authentication
PaC<->PAA
2

Access Router/
PAA

Data
Packets

ISP Core

Authentication
PaC<->PAA
2

Authentication
PAA<->AAA
3

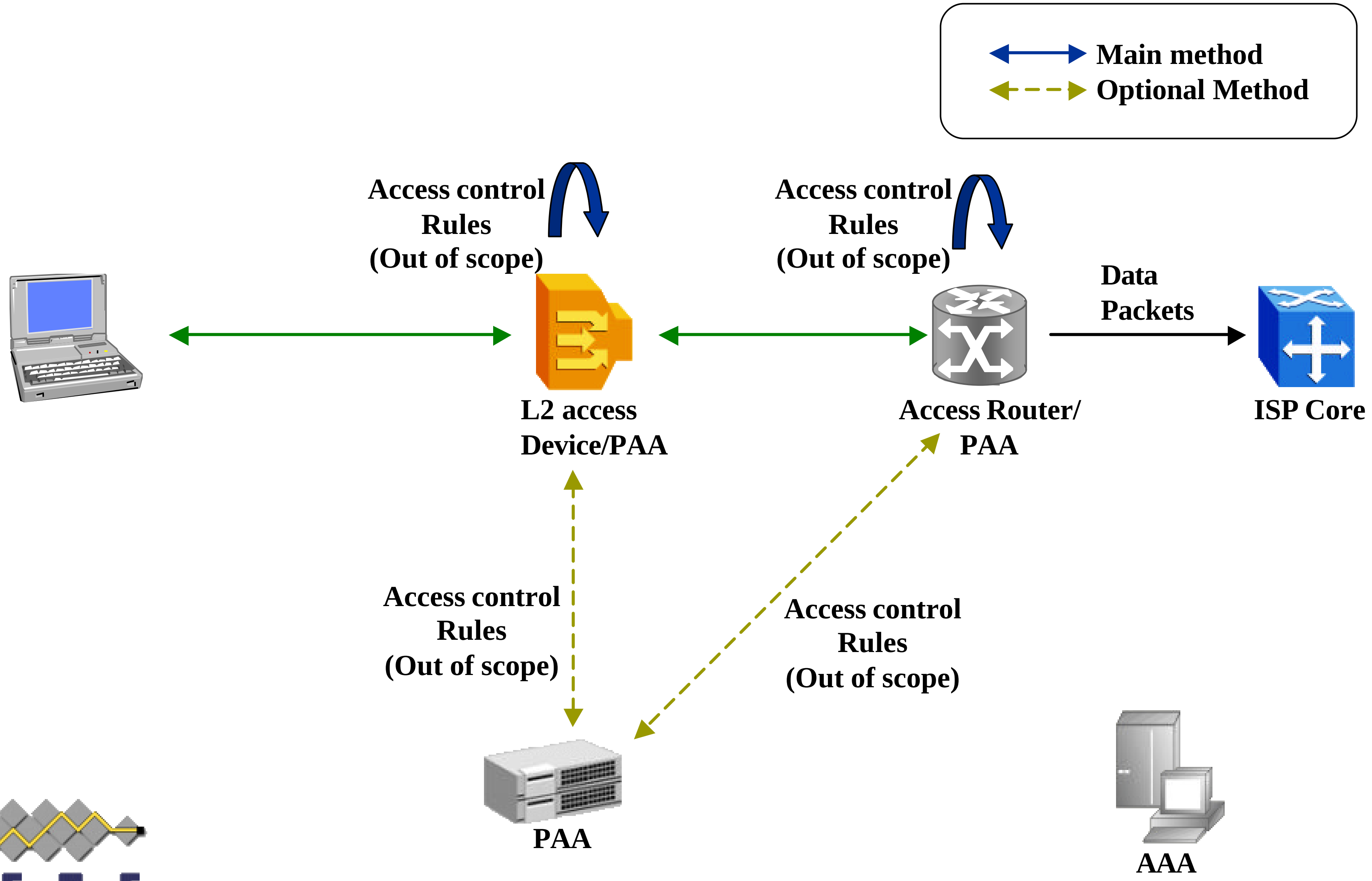
Authentication
PAA<->AAA
3

PAA

Authentication
PAA<->AAA
3

AAA

The Big Picture – Message Framework



Main method

Optional Method

Access control Rules (Out of scope)

Access control Rules (Out of scope)

Data Packets

L2 access Device/PAA

Access Router/ PAA

ISP Core

Access control Rules (Out of scope)

Access control Rules (Out of scope)

PAA

AAA

Location of PAA

- **More than one hop away from the PaC**
  - if PAA is placed somewhere behind access router on the data path, access routers and other devices on the PANA path exchange may need to keep state for access control. This will create state in more nodes.
- **Separation of PAA and Access Device**
  - A protocol between PAA and the access device is needed in order to push down authorization information from the AAA or just to remove access control restrictions
  - Should the group focus only on the case where PAA and PEP reside on the same device?

Location of PAA

- **Issues relating to address assignment.**
  - You can't really speak IP until you have at least one address, and on many networks today you can't get an address until you authenticate.
  - What address should a device use when PANA authentication occurs before obtaining a global IP address?

Security Issues

- **PANA MUST be able to create a Local Security Association (LSA) between client (e.g.,visiting user) and server (e.g., visited network).**
  - EAP-TLS, TSK, etc
- **Key derivation**
- **PANA conversation SHOULD (MUST?) be integrity protected and encrypted.**
- **EAP is one of the candidates to address security requirements**

Assumptions on the AAA Infrastructure

- AAA Infrastructure must be secure – that’s a given
- Information that needs to be carried between the PaC and PAA might also need to be carried between the AAAL and the AAAH
- If a user moves from one PAA's territory to another PAA's territory in the same AAA domain, then it MUST be possible to use the LSA obtained from the first PAA to circumvent the need to interact with the home AAA server
- AAA authorization information will be pushed down to the access device. This brings one more protocol to the table: probably MIDCOM, Diameter or something analogous.

PAA discovery

- ICMP
- DHCP
- Others?

Volunteers for the PANA doc?