Certificate provisioning with DHCP

Ciprian Popoviciu, Ralph Droms,
Eric Levy-Abegnoli

IETF 71, March 09/14th 2008
Philadelphia

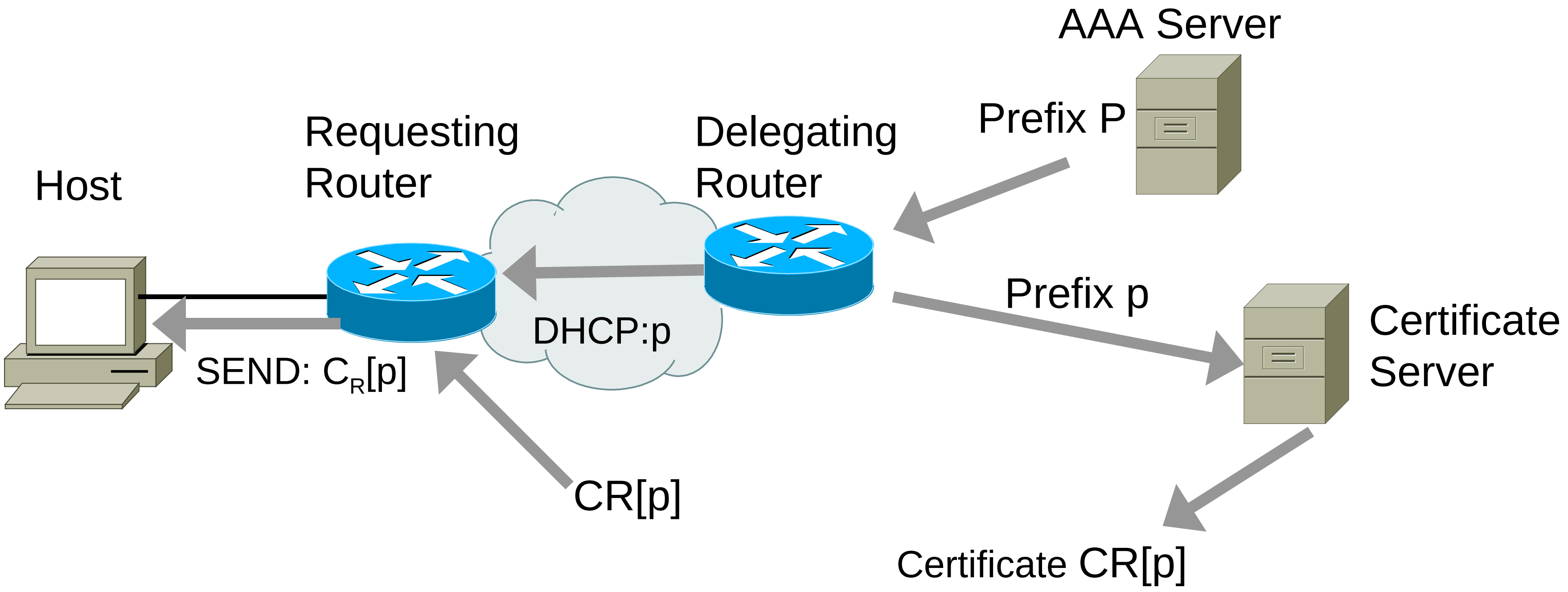
Premise

- DHCP-PD (RFC3633) provides a prefix to a CPE to use for provisioning its interfaces
- The DHCP-PD server maintains state on how long the CPE is allowed to use that prefix
- If devices behind the CPE use SEND (RFC 3971), they will require the CPE to certify it is allowed to advertise the prefix via RAs

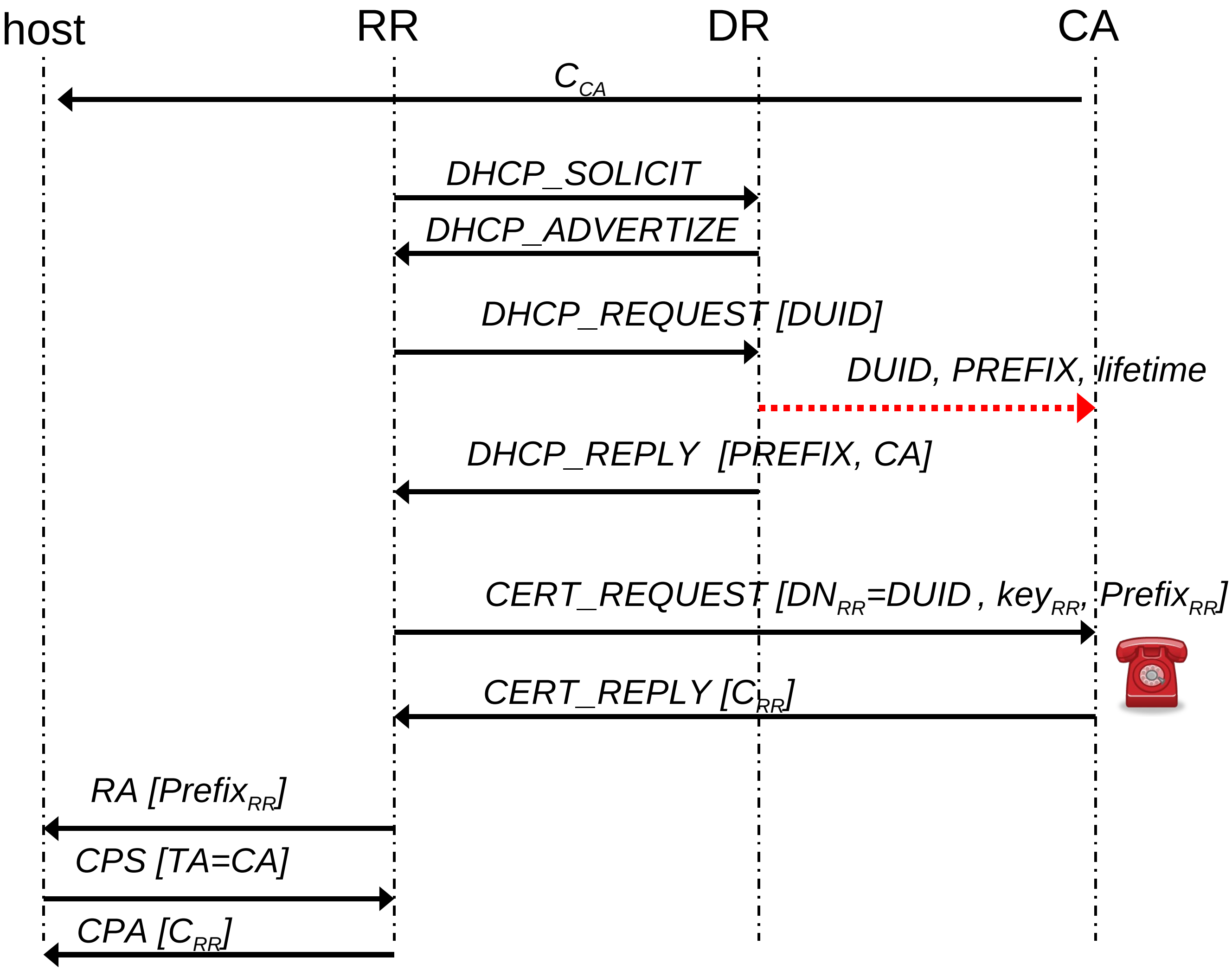
Proposal

- Extend automation of prefix delegation to environments where SEND is required
  - → Automating part or all of the certificate provisioning operation
  - → Tie up the certificate IP extensions authorizing the router for specific prefixes, and prefixes delegated to that router
- Have the DHCP-PD server do one of the following:
  - o Certify the CPE to advertise the prefix assigned to it
  - o Helper the Certification process

Terminology and deployment model



Certificate Acquisition - 1



host

RR

DR

CA

C_{CA}

DHCP_SOLICIT

DHCP_ADVERTIZE

DHCP_REQUEST [DUID]

DUID, PREFIX, lifetime

DHCP_REPLY [PREFIX, CA]

CERT_REQUEST [DN_{RR}=DUID , key_{RR}, $Prefix_{RR}$]

☎

CERT_REPLY [C_{RR}]

RA [$Prefix_{RR}$]

CPS [TA=CA]

CPA [C_{RR}]

Case 1 – Highlights

Basic Concept

A new, variable length option in the Reply message that enables the DHCP server/DR to send a pointer to the CPE/RR with the location of the Certificate server

Process

- DHCP server sends in the Reply, along with the prefix, a pointer to the location of the certificate server
- Client invokes a separate process to acquire its certificate from the certificate server using the prefix it received via DHCP-PD
- A correlation must be established between the validity of the certificate and that of the assigned prefix

Trust model

CA trust the DR but does not trust the RR. It gets the binding between the RR DUID and the delegated prefix from the DR , but must verify the binding between the certificate requester and the RR.

Pro-Con Analysis

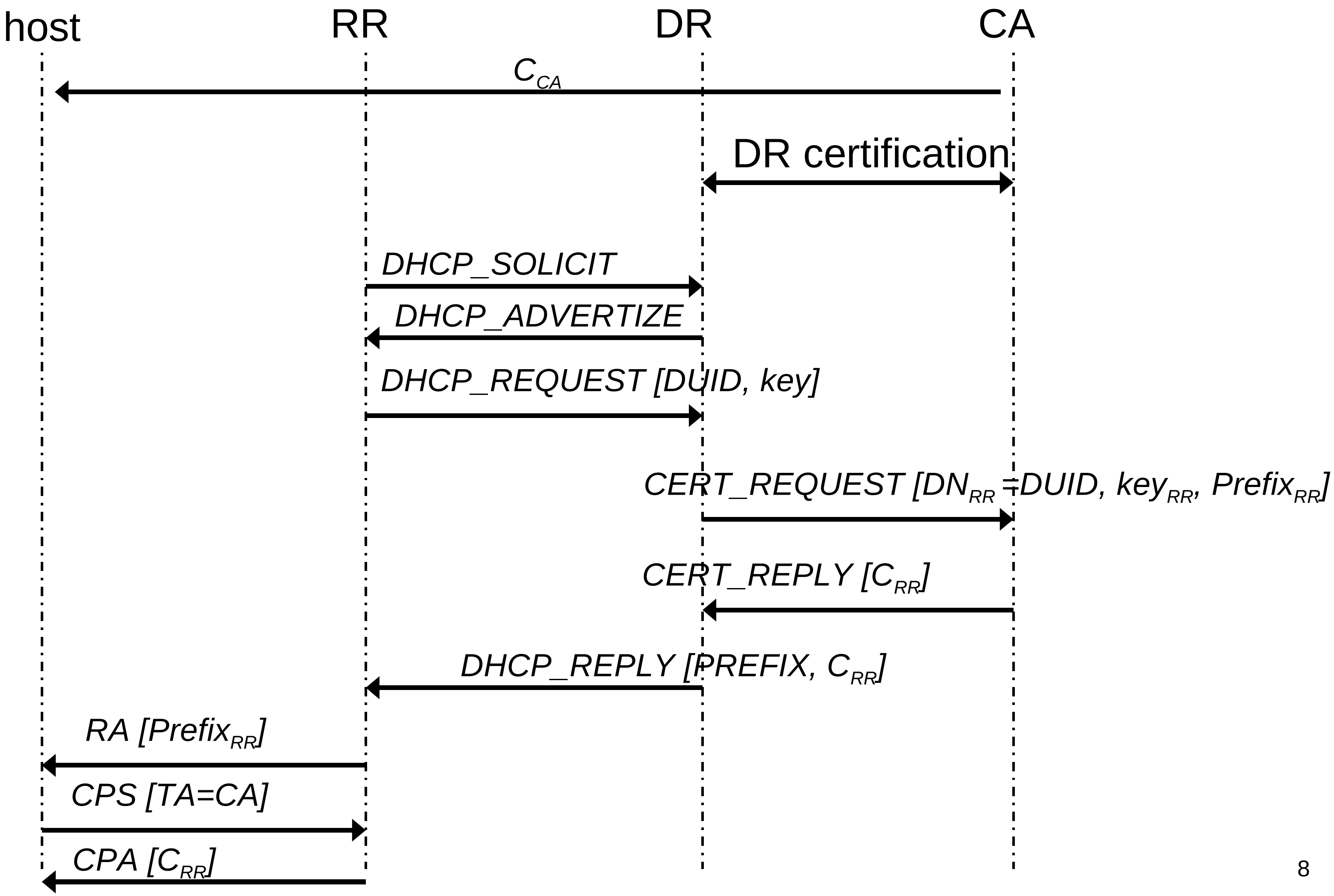
Pro

- Minimal changes to the DHCP process
- Use existing protocol

Con

- Trust model requires some manual verification
- The correlation between the lifetime of the prefix and that of the certificate will require an additional process.
- The CPE/RR might not be operational even though it has a prefix assigned because it had a problem contacting the certificate server

Certificate Acquisition - 2



host

RR

DR

CA

C_{CA}

DR certification

DHCP_SOLICIT

DHCP_ADVERTIZE

DHCP_REQUEST [DUID, key]

CERT_REQUEST [DN_{RR} =DUID, key_{RR}, $Prefix_{RR}$]

CERT_REPLY [C_{RR}]

DHCP_REPLY [PREFIX, C_{RR}]

RA [$Prefix_{RR}$]

CPS [TA=CA]

CPA [C_{RR}]

Case 2 – Highlights

Basic Concept

- A new, variable length option is introduced in the Request message through which the CPE/RR can send its Public Key
- A new, variable length option in the Reply message through which the DHCP server can send the certificate for the prefix it assigned to the CPE

Process

- RR sends Public key in the Request
- DR acts as a Registration Authority (as specified in RFC4210)
- DR builds a certificate request with RR Public Key, DN=RR DUID and Prefix delegated to RR to the certificate server
- Certificate server calculates the certificate and sends it to the DHCP server
- DHCP server sends the certificate along with the prefix in the Reply

Trust model

- CA trusts DR thru some (unspecified) DR certification process
- DR trusts RR thru some (unspecified) DHCP-PD trust model

Pro-Con Analysis

Pro

- There should be a correlation between the lifetime of the assigned prefix and the certificate. With this proposal, the DHCP server can control this easily.

Con

- New mechanism to delivering certificates
- An additional (invisible to the requestor) step in processing the Request

Conclusions

- Enabling the DHCP server to provide the certificate or help with the process makes sense because the DHCP server hands out the prefix that needs to be certified and controls, through the life of the prefix, the life of the certificate
- Can be implemented as a helper in which case, for a full system, a correlation must be established between the DHCP server and the Certificate server. The alternative is to ignore the correlation between the two lifetimes.
- Can have the DHCP server as a “relay” for the certificate process which resolves the correlation problem and simplifies the provisioning process for the Client while eliminating some corner cases.