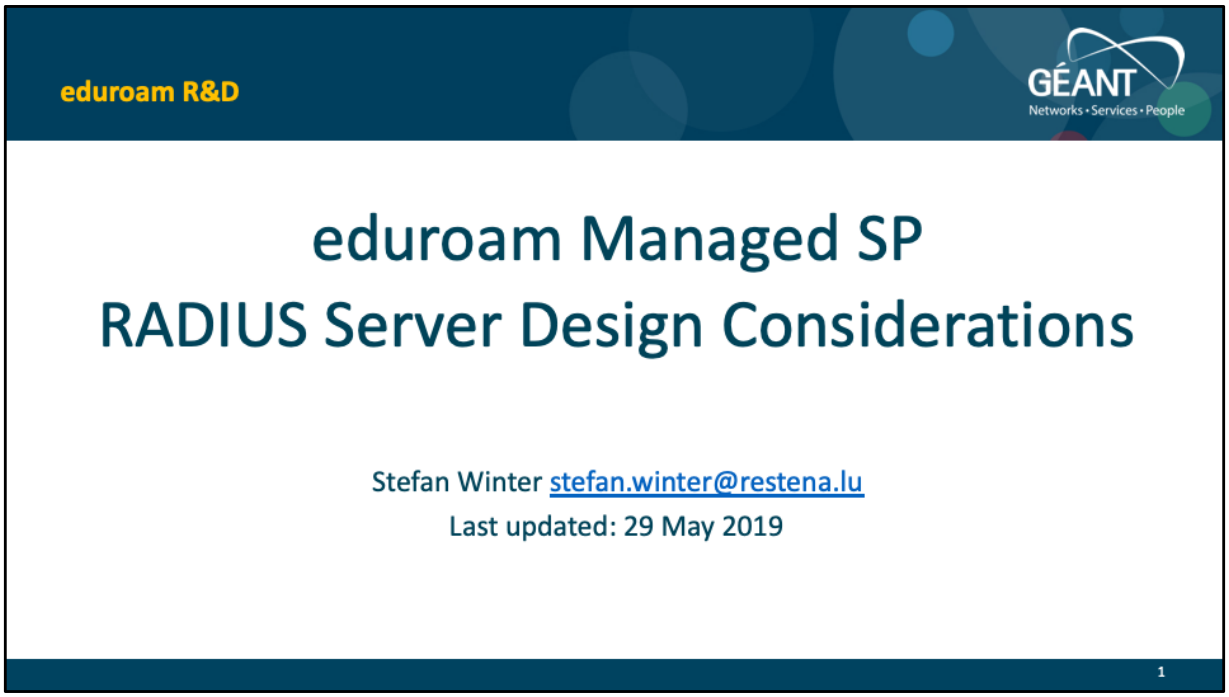
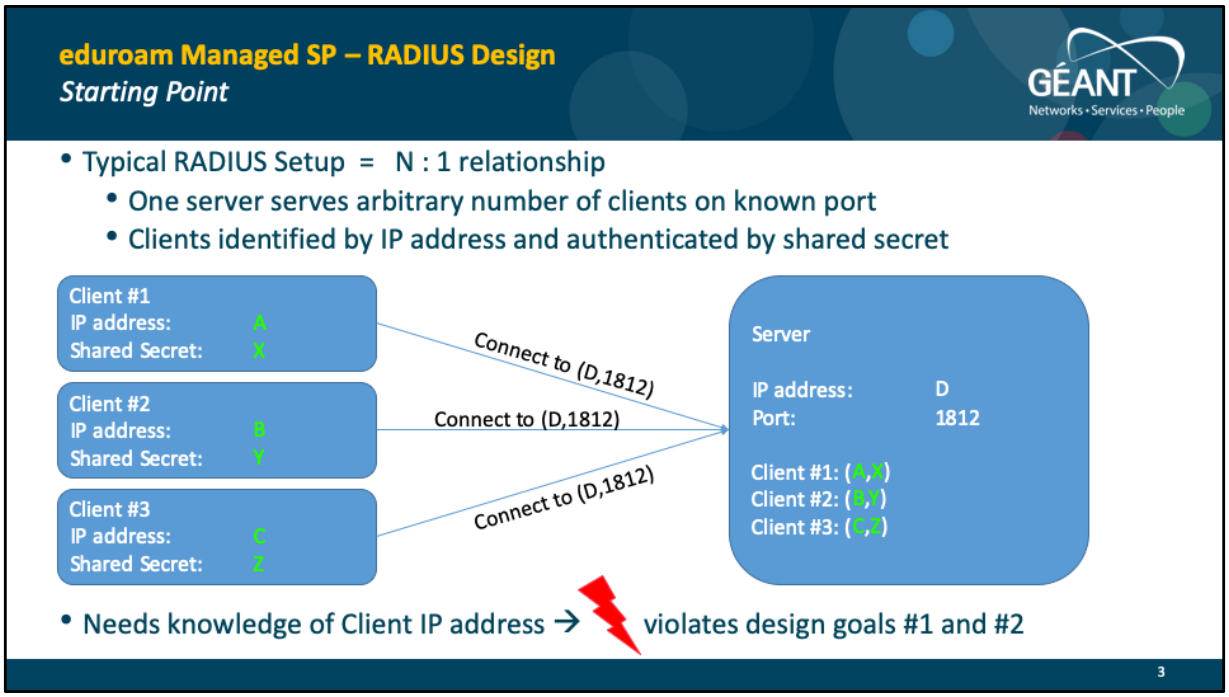


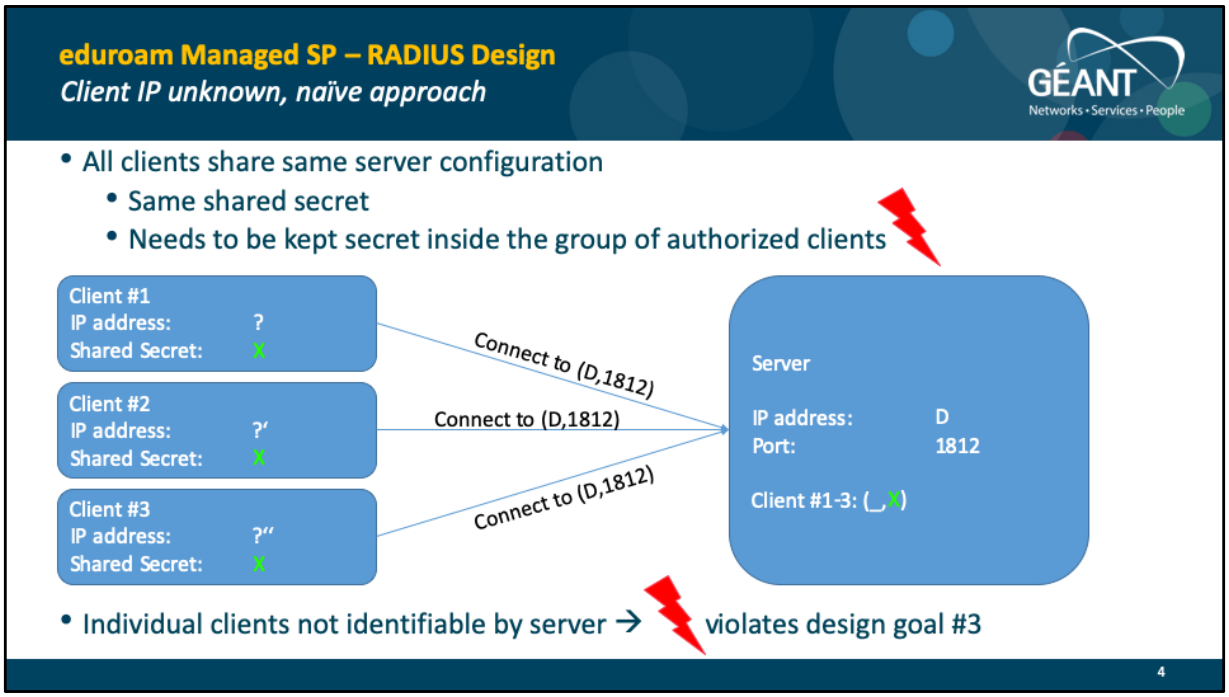

This is probably the first time ever that I make extensive use of slide annotations. Please do read them, they are essential for the understanding of the slide flow.

## eduroam Managed SP – RADIUS Design
*Design Goals*

- Design Goals
  1. SP operator does not need knowledge about outbound network connectivity
  2. System should not depend on specific nework connectivity, notably static IP address
  3. SPs are uniquely identified
  4. System does not need to ask SP operator anything; unidirectionally communicates configuration items for AP-side configuration
  5. Uplink Redundancy should be possible
  6. RADIUS server should be geographically close for shorter network roundtrips
  7. NROs should be able to attach SPs in their own vicinity/infrastructure




This is the world we live in ☺
The server identifies the client based on a two-tuple which is the (configured) shared secret and the (inherent property) client IP address.
This only works if that client IP address is unique, known, and doesn't change.

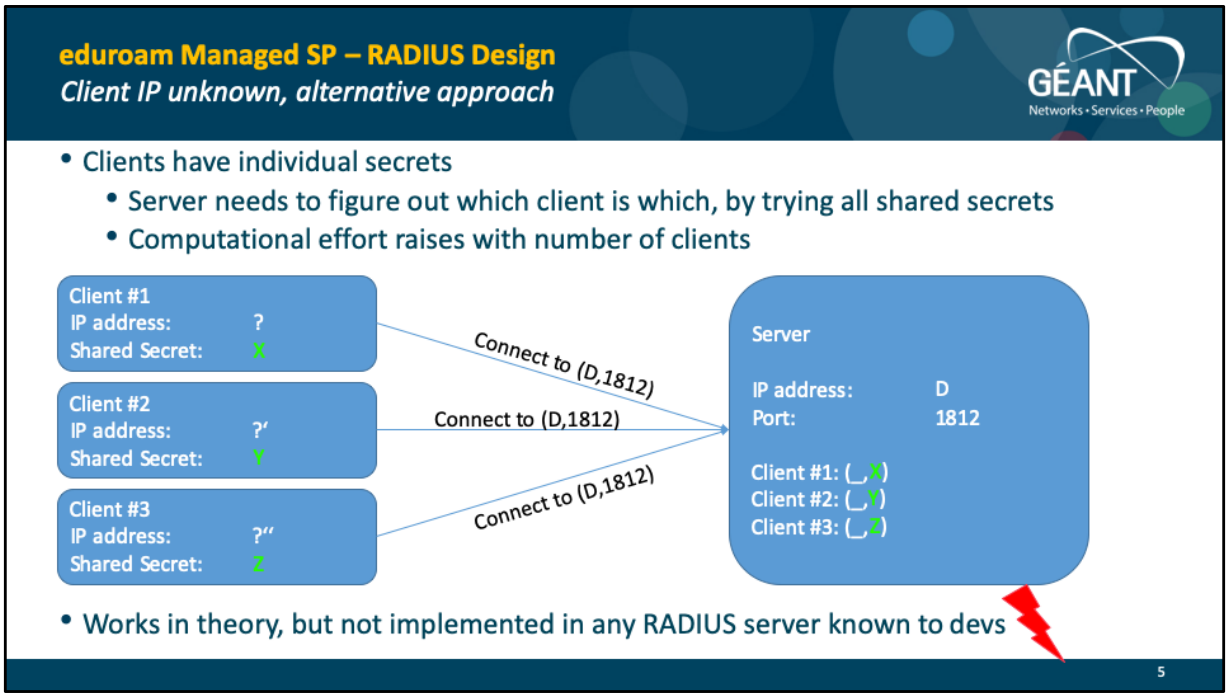



The server now does not have a two-tuple any more, but only a single value (shared secret X) which is enough to identify the group of authorised clients but not the actual individual client.

This is actually a viable approach in small-scale deployments (or so I hear) when the exact identity of the client is not important (e.g. three controllers delivering the same service at the same location; the client is then not an individual IP address but a subnet).

But this certainly does not scale to the use case we target with Managed SP where clients are independent of each other and all need their own customised treatment.

Also, distributing the same shared secret across admins in numerous administrative domains is prohibitively weak security: if one participant leaks the shared secret to unauthorised third parties *everyone* can become an SP. And changing the shared secret is impossible as it would need to be a concerted flag day action across all the authorised clients.

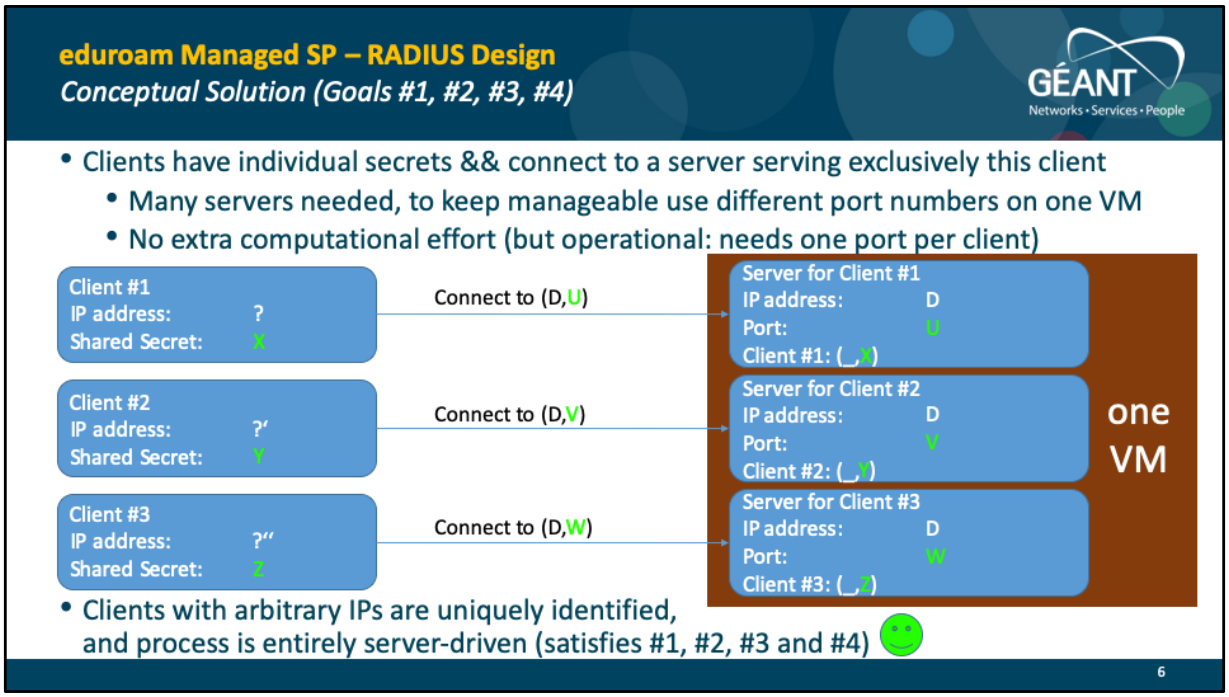



Again, there is no two-tuple for easy client identification. Identification of the exact client needs to be done with inference on which shared secret leads to a valid incoming RADIUS packet.

In fact, this is a recurring question at least on the FreeRADIUS users mailing list. It is a rather typical situation e.g. when many APs are behind a NAT gateway and come in with the same IP address but are supposed to be treated as individual clients.

Requests to implement this are routinely pushed back (and I for one understand why as this is an extremely ugly brute force attempt at client identification).

It also conceptually does not work with clients doing non-EAP and not signing their Access-Request packets with Request-Authenticator (in those cases, the shared secret is not used at all in the request so can't disambiguate clients); this is not relevant for eduroam though as we always do EAP.




We are now back in the situation that we have a two-tuple to uniquely identify the client. This time it is the shared secret && the port number which the client chose to connect to its server. I.e. the previous inherent property of the client (IP address) is replaced by a configured port number.

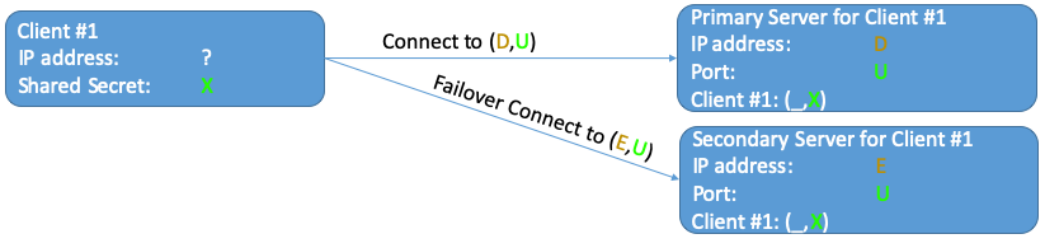
Since both parts of the tuple are configuration items that need to be synced across both parties, one party can make the first step: the Managed SP system chooses both the shared secret and a free port on a server VM, spawns up a new server exclusively for the client, and communicates the VM's address (D), the port (U/V/W/…) and the shared secret. The client only needs to put the received information into an AP config.

An open point is whether typical APs/controllers allow to specify a non-default RADIUS port. Anecdotal evidence by the devs suggests this is typically the case (SW and TW both run this setup in their home DSL sites for many months now).

## eduroam Managed SP – RADIUS Design

*Actual Solution with redundancy (Goal #5)*

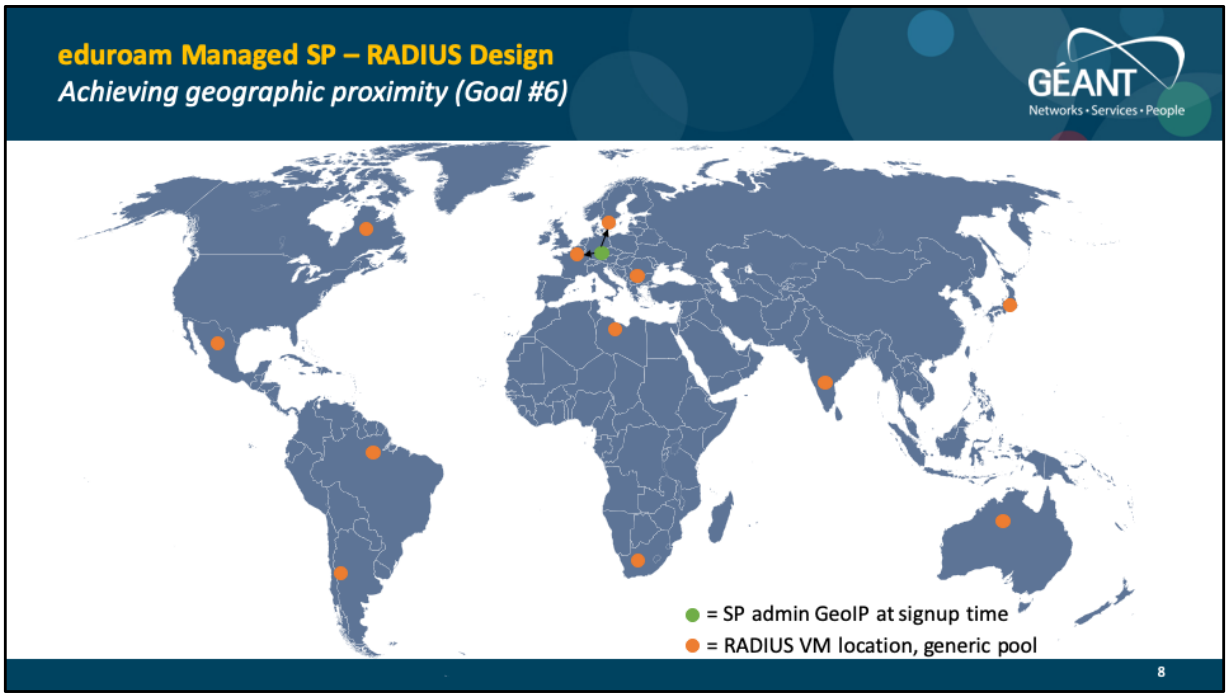
- Do it twice, exploiting APs typical capability to have a pair of RADIUS servers configured
  - Uses traditional RADIUS fail-over behavior
  - Communicate both server IP address to client




- Goal #5 achieved for clients with primary/backup RADIUS server configuration; not achieved for those without that capability
- Still under discussion: same port, or different port per server

7

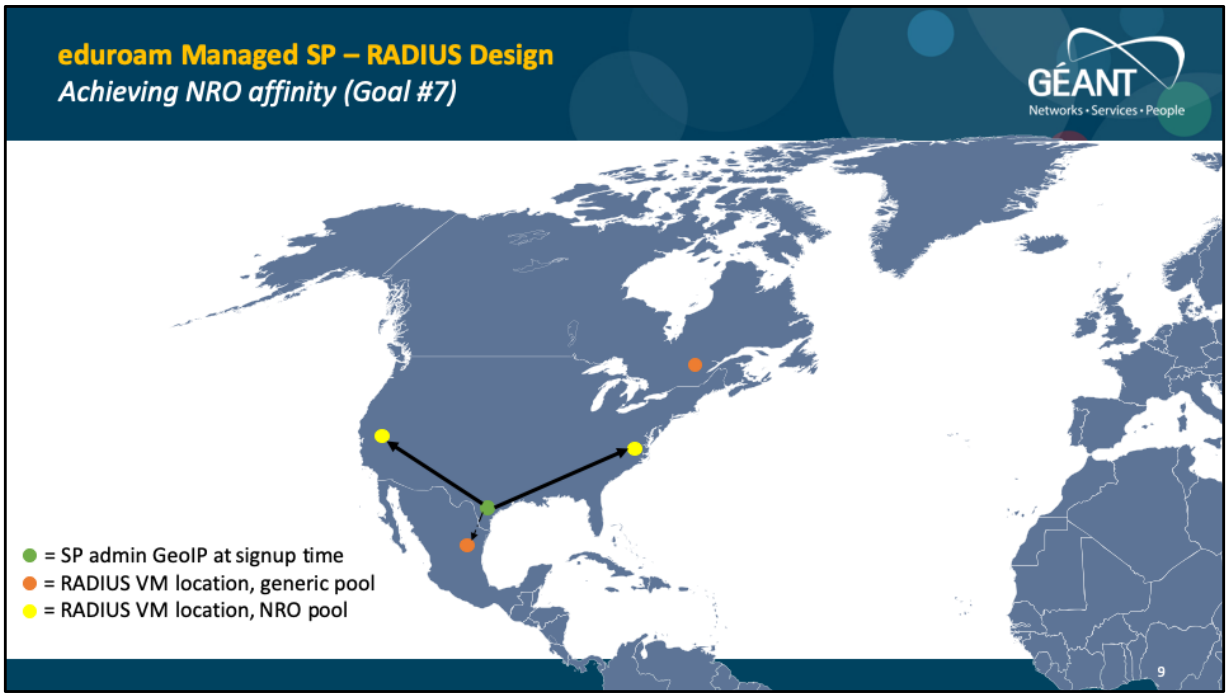
The picture uses the same port number for both primary and secondary server. For ease of use of the system, this is desirable as there is one less number to remember/typo/understand.
It makes the system-side selection process of server/port/secret pairs a bit more complex, but this is probably worth it.




eduroam Operations Team to provide multiple RADIUS VMs geographically spread across the world (typically with the help of local NROs, or possibly commercial cloud providers). Positions in this picture are entirely made up and for illustration purposes only. In particular, U.S. is left free merely to serve as example for final design goal #7 on next slide.

When registering SP, admin is geo-located by IP or HTML5, and the two nearest free servers are chosen (nearest for primary, runner-up for secondary).

(world map taken from Wikipedia, „Blank World Map with a blue slate coloring“, Author „$200inaire“, License: This file is licensed under the Creative Commons Attribution-Share Alike 3.0 Unported license.)




Actual RADIUS VM location may be in a different NRO or in cloud, which may be undesirable for an NRO. Advanced NROs who want to keep traffic local can make available VMs in their own datacenters which will be flagged as NRO-specific pools.

After geo-locating admin, NRO-specific pools (if existing) are selected with priority over the generic pool. With that, new eduroam SP deployments will be attached to RADIUS servers inside the NRO.

In the example above, even though a server from the generic pool which happens to be located in Mexico is geographically closest, the admin is part of the U.S. NRO and will be attached to the two NRO-specific RADIUS servers instead.

An open question is what to do if an NRO-specific pool is full (none of the servers have spare open port capacity) – overflow to generic pool or deny service?

(world map taken from Wikipedia, „Blank World Map with a blue slate coloring“, Author „$200inaire“, License: This file is licensed under the Creative Commons Attribution-Share Alike 3.0 Unported license.)

## eduroam Managed SP – RADIUS Design

*Resulting requirements on SPs, open design questions*

- Requirements on SPs
  - SP equipment MUST be able to allow configuration of arbitrary RADIUS server destination ports
  - SP equipment SHOULD allow configuration of a primary and secondary RADIUS server for redundancy purposes
- Open design questions
  - Take the extra effort to find common port number on both primary and secondary server?
  - For geographic proximity and NRO affinity: overflow to generic server pool or deny service?