Capport ICMP

IETF99 Capport WG

dbird@google.com

What is a NAS to do?

- Allow (forward)
  - Resources within the walled garden, DNS, the captive portal itself, etc.
- Redirect
  - HTTP (TCP port 80)
- Block
  - How?
    - Silently drop packet
    - Return existing ICMP error type (e.g. Dest-Unreach / Administratively prohibited)
    - TCP Reset
  - Current options don’t allow the NAS to accurately inform the UE of captivity

Capport ICMP Extension

- RFC 4884 - Extended ICMP to Support Multi-Part Message
  - New Capport ICMP Extension Object Class and Class Sub-types
- Provides NAS with ability to accurately inform the Capport UE of captivity state, while also providing legacy UEs *something* (e.g. Destination Unreachable), in a single packet
- Formally defines how a NAS blocks traffic in captive portal networks - for both Capport and Legacy devices

Capport ICMP Type

- Similar to Capport ICMP Extension, but specifically designed to *not* be recognized by legacy UEs
- Use-cases
  - Non-flow terminating ‘notifications’
    - Low bitrate (QoS Tier) notification. UE suggests visiting portal to upgrade session.
    - Pending policy change notification, e.g. time or data expiring soon. UE suggests visiting the captive portal to continue session.

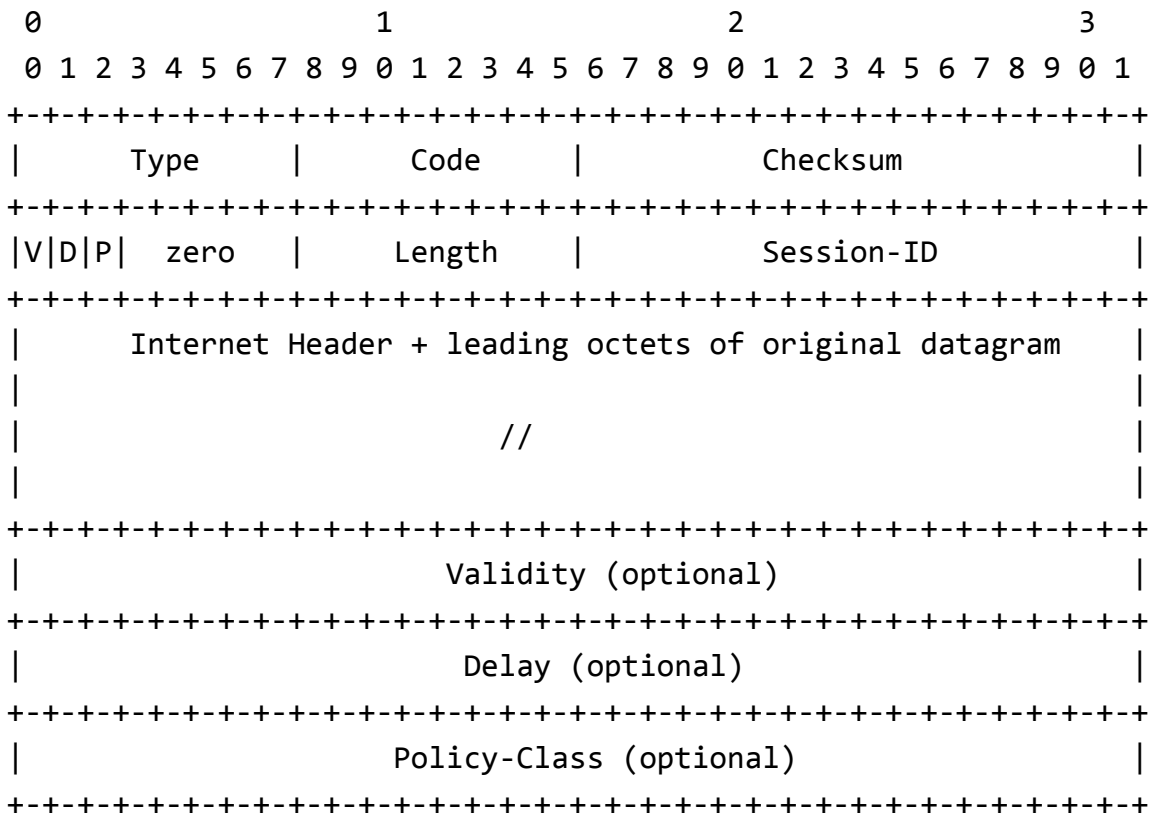
Capport ICMP Codes/C-Types

- DROP_FLOW (0) - Packet was dropped, flow terminated
  - UE: Captive portal *required* notification
- DROP_QOS_OVERFLOW (1) - Packet was dropped, flow *not* terminated
  - UE: Captive portal *suggested* notification
- WARN_FLOW (2) - Packet was *not* dropped, flow “warning”
  - UE: Captive portal *suggested* notification

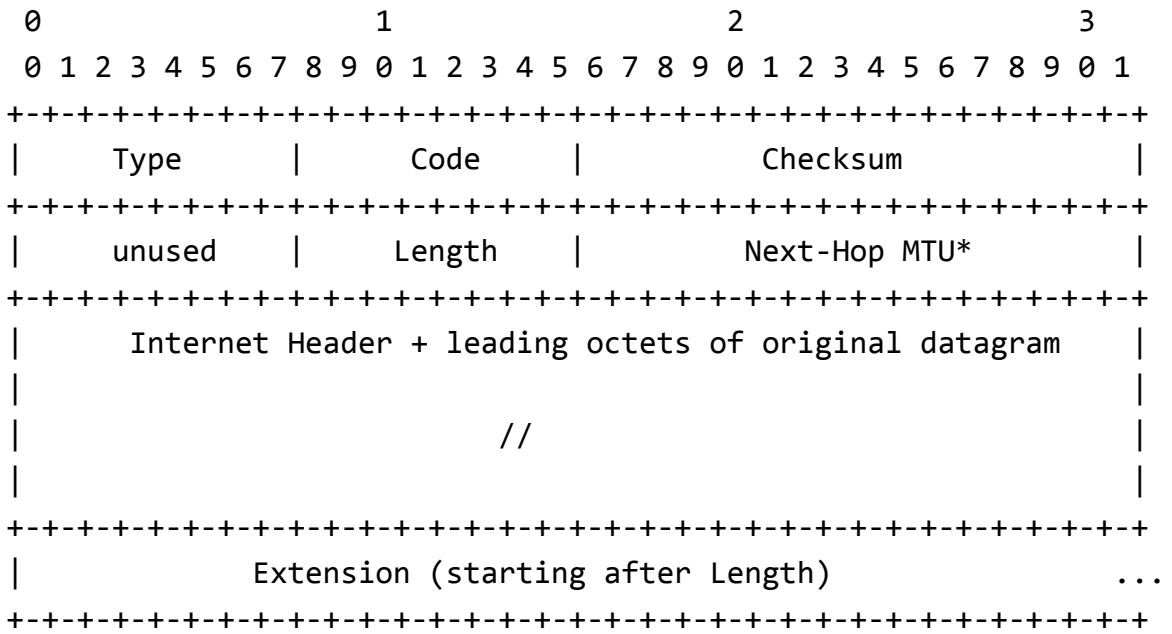
Fields, Flags, and Extensibility

- Session-ID
  - Used to group ICMP notifications into events
  - Change in Session-ID indicates a change in access policy (at the NAS)
  - Can be used to increase confidence in ICMP messages not being forged
- Flags
  - Allows for extensions to the format
  - Examples:
    - Validity time - The length of time a notification is valid. During this time the UE can expect the NAS to *silently* drop further requests for the same resource.
    - Delay time - The length of time before a notification is valid. For warning notifications like “You are about to run out of time”.
    - (Optional) Access policy - An opaque value used as a “hint” to the portal. Can be used to carry site specific “hints” to the captive portal.

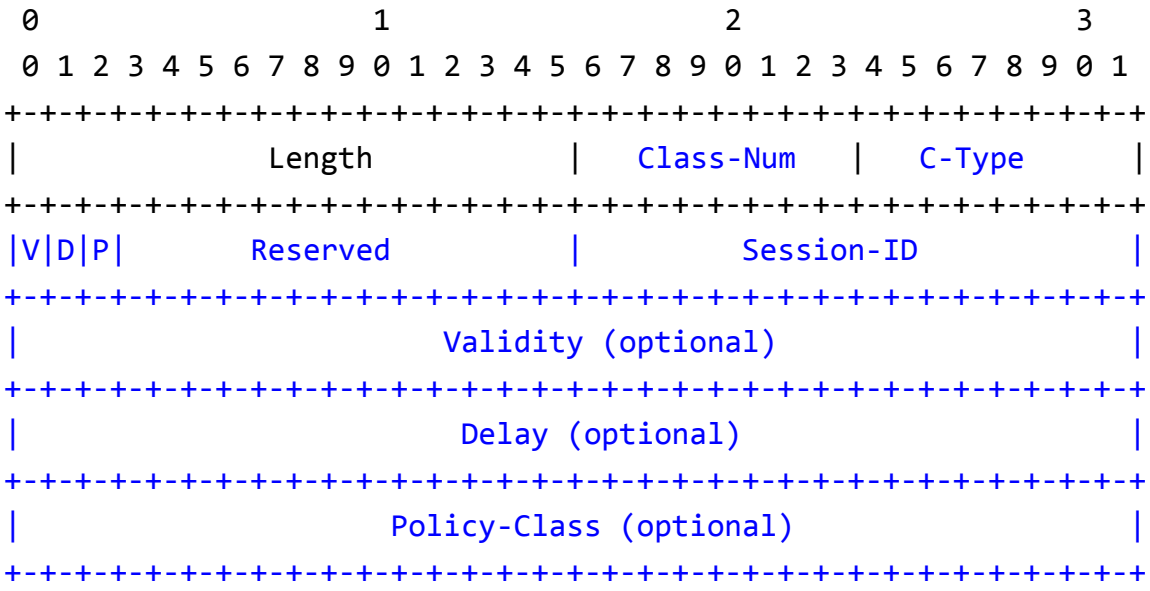
Capport ICMP Type



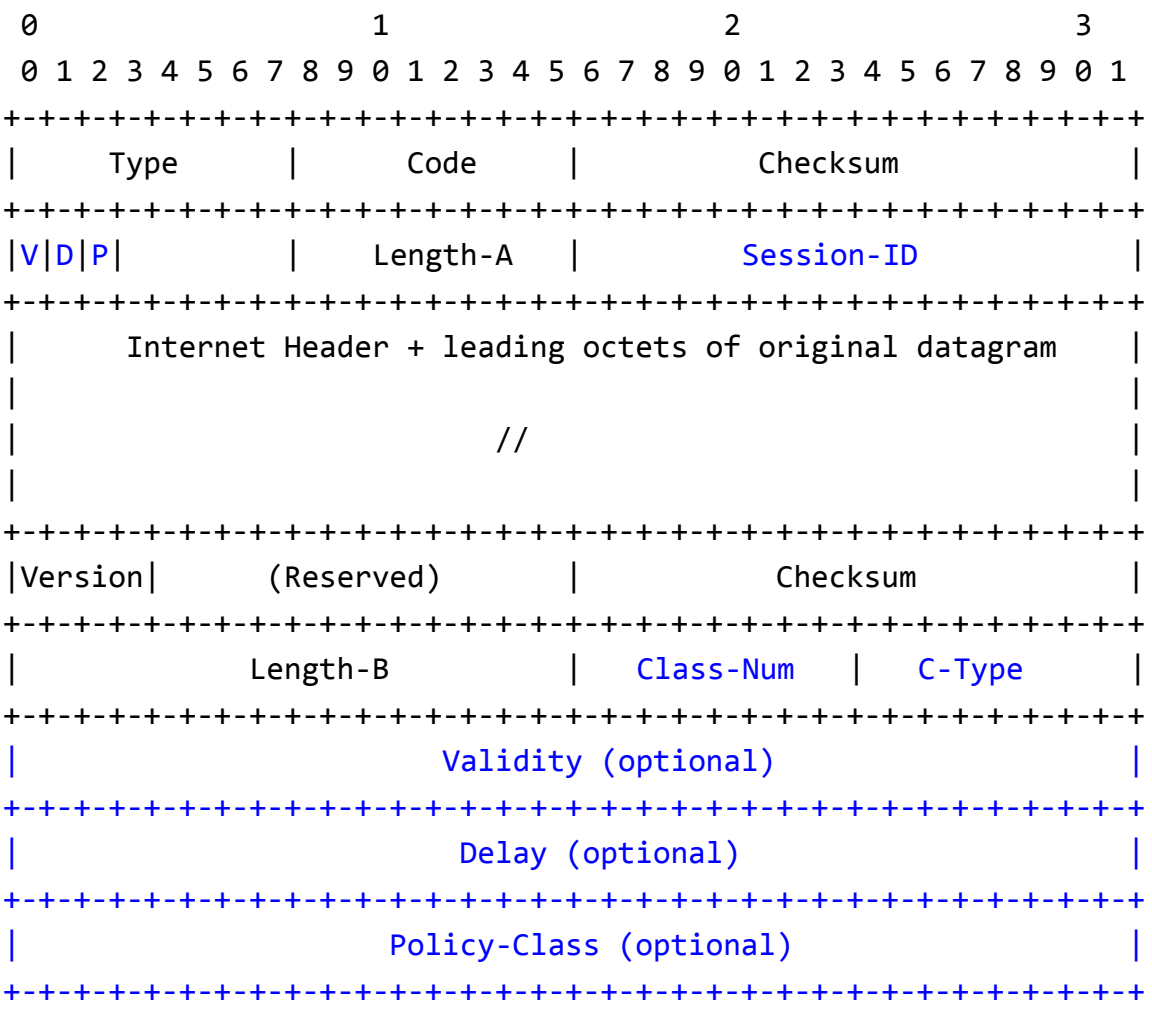
ICMP Extension Object Format



(continued)


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Length
Class-Num
C-Type
|V|D|P|
Reserved
Session-ID
Validity (optional)
Delay (optional)
Policy-Class (optional)

ICMP Extension Object Format (simplified)



Keep it simple!

- The NAS is always the Source of Truth in terms of the policies it is enforcing.
  - Access policies and session parameters, including walled garden settings, can come from *multiple* sources: Local configurations, dynamic system configurations (sometimes retrieved via RADIUS or other ways), and session specific parameters that might come from the WISP or user's "home" service provider's RADIUS server.
- Don't dump the complexity onto the network operator's infrastructure!
  - With Capport ICMP notifications coming from the NAS, the implementation is done by the NAS vendor(s). There is minimal impact on the WISP infrastructure.
- Don't assume a single vendor.
  - It is not uncommon for NAS functions to be split between systems. An example might be a time/data limiting NAS from one vendor and a rate limiter from another.

Moving forward with ICMP?

- Should we continue with the Capport ICMP draft?
- Discussion...