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

```
+-----------------+-----------------+-------------------+
|     Type       |      Code       |         Checksum   |
+-----------------+-----------------+-------------------+
|   V | D | P |  zero  |     Length     |     Session-ID   |
+-----------------+-----------------+-------------------+
| Internet Header + leading octets of original datagram |
+-----------------+-----------------+-------------------+
| Validity (optional) |
+-----------------+-----------------+-------------------+
| Delay (optional) |
+-----------------+-----------------+-------------------+
| Policy-Class (optional) |
```

ICMP Extension Object Format

```
+---------------+---------------+---------------+
| Type          | Code          | Checksum      |
+---------------+---------------+---------------+
| unused        | Length        | Next-Hop MTU* |
+---------------+---------------+---------------+
| Internet Header + leading octets of original datagram | // |
+---------------+---------------+---------------+
| Extension (starting after Length) ... |
+---------------+---------------+---------------+
```
(continued)

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

+-----------------------------------------------+
| | Length | Class-Num | C-Type |
|-----------------|-----------------|-----------------|
| +-----------------------------------------------+

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>V</td>
<td>D</td>
<td>P</td>
<td>Reserved</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| +-----------------------------------------------+

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

+-----------------------------------------------+
<table>
<thead>
<tr>
<th></th>
<th>Session-ID</th>
</tr>
</thead>
</table>
| +-----------------------------------------------+

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

+-----------------------------------------------+
<table>
<thead>
<tr>
<th></th>
<th>Validity (optional)</th>
</tr>
</thead>
</table>
| +-----------------------------------------------+

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

+-----------------------------------------------+
<table>
<thead>
<tr>
<th></th>
<th>Delay (optional)</th>
</tr>
</thead>
</table>
| +-----------------------------------------------+

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

+-----------------------------------------------+
<table>
<thead>
<tr>
<th></th>
<th>Policy-Class (optional)</th>
</tr>
</thead>
</table>
| +-----------------------------------------------+
ICMP Extension
Object Format
(simplified)

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>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</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |      Code     |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|V|D|P| Length-A | Session-ID |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Internet Header + leading octets of original datagram |

|Version| (Reserved) | Checksum |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Length-B | Class-Num | C-Type |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Validity (optional) |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Delay (optional) |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Policy-Class (optional) |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
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?
- Network state / notifications: Using ICMP or an API?
- Discussion...
Example (overly complicated) Hotspot

Venue / Hotspot Network Owner

Venue Web Sites(s)

Hotel PMS

Hotspot

Access Point / NAS

Local Configurations:
- Walled garden settings
- Default session parameters
- One (or more) RADIUS AAA
- Local user accounts

Hotspot Service Provider

Captive Portal

RADIUS / AAA

Services
- Payment processing
- Roaming / marketing
- Vouchers, access products
- Configuration management

Roaming / Marketing Partners

Partner Website

RADIUS / AAA

RADIUS / AAA

Partner Website