RATS (if adopted)
Internet-Draft
Intended status: Standards Track
Expires: 2 September 2026

M. Richardson
Sandelman Software Works

1 March 2026

Geographic Attestation Results
draft-richardson-rats-geographic-results-01

Abstract

Many workloads have limitations on what geography they are allowed to operate in. This is often due to a regulation that requires that the computation occur in a particular jurisdiction.

There are many mechanisms by which Evidence of location may be created and then evaluated by a Verifier. No matter which mechanism is appropriate for a given situation, the result of the Verification can be expressed in a similiarly defined EAT Attestation Result.

This document is therefore about encoding a variety of geographical conclusions in an Attestation Result. In addition, one mechanism of directly creating a geographic result in the form of an Endorsement is described in an appendix.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-richardson-rats-geographic-results/.

Discussion of this document takes place on the RATS Working Group mailing list (mailto:rats@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/rats/. Subscribe at https://www.ietf.org/mailman/listinfo/rats/.

Source for this draft and an issue tracker can be found at https://github.com/mcr/geographicresult.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 2 September 2026.

Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

Resolving the question of where certain computations are done can be critical to assessing how much trust to put into the result.

MORE USE CASES HERE.

[I-D.ietf-rats-ear] provides a framework that allows an [RFC9334] Verifier to return a conclusion as to geographic region for an Target Environment.

While [RFC9711], Section 4.2.10 provides a very good WGS84 based location claim, often very suitable as Evidence, it is not ideal for the use by Relying Parties.

There are a few reasons:

* the latitude and longitude describe a location on the Earth. The Relying Party is seldom interested in that level of detail. It needs to know if it's in the correct place.

* the geographic position leaks significant amount of private information that is not necessary for the Relying Party to know.

* for many activities, it is the Legal Jurisdiction that matters, not the actual location. Jurisdictions often do not have well defined concentric boundaries. For instance, the South Korean Consultate in Los Angelos is often for Legal purposes, in Korea. Yet, only a few meters away, possibly below the level of WGS84 accuracy, the jurisdiction would be different.

* there are many other situations involving exclaves, and even exclaves inside other exclaves where the boundaries are quite complex.

This document offers a new set of structured abstract claims that provides an evaluated view of where a Target Environment is.

The mechanism to do this appraisal may depend upon a number of factors which may be related to physical geographic position, but also include other considerations.

The most obvious way is through various Global Navitation Satellite Systems (GNSS): the United States Global Positioning System (GPS), Russia's Global Navigation Satellite System (GLONASS), China's BeiDou Navigation Satellite System (BDS) and the European Union's Galileo. These signals can be spoofed, manipulated and suppressed. There are many environments, such as inside a (Faraday) cage in a Data Center, where GNSS signals do not reach. Whether or not they are a good measure of location is not the subject of this document. Rather, if a Verifier believes that information trustworthy for the purpose intended, then it may use the format described here to document it's conclusion.

There are also other radio methods, such as time of travel calculations from a mobile (LTE) tower.

An example of mechanically determination of location without radio could be a claim that a Target Environment is less than 1ns (as light travels in a fiber optic cable) away from another Target Enviroment whose location is known. A typical fiber optic cable has a speed of 200,000 kilometers per second (slower than light in a vacuum to the index of refraction of the glass involved). So if the round trip time between environments is 1ns, then the distance between Target Environments can be appraised to be within 1m of each other. Other work contemplates claims like this one

Finally, one method to find out where a device is for a trusted human to go and look at it. Perform an audit. The result is not an Attestation Result according to [RFC9334], but instead it is an Endorsement. Appendix A describes a protocol that could be used for a human auditor to make such an evaluation.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Claim definition

This claim definition goes into the EAR submods map.

Geographic Results can contain one or more of the following claims.

1. jurisdiction-country = ISO3361 country code.

2. jurisdiction-country-exclave = booleann

3. jurisdiction-subdivision = country-specific list

4. jurisdiction-subdivision-exclave = country-specific-list

5. jurisdiction-city = subdivision-specific list

6. jurisdiction-city-exclave = subdivision-specific-list

7. enclosing-exclave-country = ISO3361 country code

8. near-to = another entity+distance

9. rack-U-number = ordinal, numbered from bottom RU as 1.

10. cabinet-number = ordinal, DC specific ordering, might ignore hallway, room and floor

11. hallway-number = ordinal

12. room-numbr = string

13. floor-number = string, usually representing an integer.

14. Data Center

There are some additional things which may be received as Evidence, but which is sometimes important to convert to Results, having verified some aspects. (TBD) 1. range-to-tower = designation of tower, distance-readings 2.

(NOTE: There are apparently exclaves that ar inside other countries exclaves, like Nahwa. Unclear if exclave information is even relevant, or if second order matters at all)

4. CDDL Definition

```
; # import rfc9711 as eat
; # import rfcXXXX as corim

$$ear-appraisal-extension //= (
    ear.geographic-result-label => geographic-result-claims
)

geographic-result-claims = non-empty<{
  ? grc.jurisdiction-country-label => iso-3361-alpha-2-country-code
  ? grc.jurisdiction-country-exclave-label => bool
  ? grc.jurisdiction-subdivision-label => tstr .size (2..16)
  ? grc.jurisdiction-subdivision-exclave-label => bool
  ? grc.jurisdiction-city-label => tstr .size(2..16)
  ? grc.jurisdiction-city-exclave-label => bool
  ? grc.enclosing-exclave-country-label => iso-3361-alpha-2-country-code
  ? grc.near-to-label => corim.uuid-type
  ? grc.rack-U-number-label => uint .gt 0
  ? grc.cabinet-number => uint .gt 0
  ? grc.hallway-number => uint
  ? grc.room-number => tstr .size (2..64)
  ? grc.floor-number => int
  ? grc.data-center-name => tstr .size (2..64)
}>

ear.geographic-result-label = eat.JC<"TBD02", TBD01>

grc.jurisdiction-country-label = eat.JC<"grc.jurisdiction-country", 0>
grc.jurisdiction-country-exclave-label = eat.JC<"grc.jurisdiction-country-exclave", 1>
grc.jurisdiction-subdivision-label = eat.JC<"grc.jurisdiction-subdivision", 2>
grc.jurisdiction-subdivision-exclave-label = eat.JC<"grc.jurisdiction-subdivision-exclave
", 3>
grc.jurisdiction-city-label = eat.JC<"grc.jurisdiction-city", 4>
grc.jurisdiction-city-exclave-label = eat.JC<"grc.jurisdiction-city-exclave", 5>
grc.enclosing-exclave-country-label = eat.JC<"grc.enclosing-exclave-country", 6>
grc.near-to-label  = eat.JC<"grc.near-to", 7>
grc.rack-U-number-label = eat.JC<"grc.rack-U-number", 8>
grc.cabinet-number = eat.JC<"grc.cabinet-number", 9>
grc.hallway-number = eat.JC<"grc.hallway-number", 10>
grc.room-number = eat.JC<"grc.room-number", 10>
grc.floor-number = eat.JC<"grc.floor-number", 11>
grc.data-center-name = eat.JC<"grc.data-center-name", 12>

iso-3361-alpha-2-country-code = tstr .size 2
```

   There are a number of different fields in this claim, and all of them
   are marked optional. But, at least some result MUST be provided.
   Which one will be needed is subject to the target usage and the needs
   of the Relying Party.

The explicitely geographic based jurisdiction fields are arranged in a hierarchy of values. The outer most values are REQUIRED when any inner value is also present. This includes the claims: country, subdivision, and city, or the equivalent exclave claims (country-exclave, subdivision-exclave, and city-exclave).

Note that the ISO 3166 term for a part of a country is called a "subdivision". This should be understood to mean "state" (e.g., in the USA, Australia), "province" and "territory" (e.g., Canada, France). There are no IANA maintained values for "subdivision", but the ISO 3166-2 has codes for many subdivisions, which can be seen in the ISO's Online Browsing Platform [obp].

In general, subdivision lists are maintained by countries. It is usually the case that city lists are maintained by subdivisions, and there are no lists of these in any hierarchial databases, such as the ISO might maintain for countries. It is therefore not unsual for there to be a Paris, Texas, USA, and a Paris, France, and a London, Ontario, Canada, as well as a London, England, UK. Equally, there are many cities called Springfield in different states of the USA.

Exclaves can exist at all levels: one part of a city might be within another city, but both are in the same country and subdivision.

Even when in an exclave, it is acceptable for a Verifier to only return the non-exclave version, hiding that an exclave is involved. In that case, the Relying Party will receive the country, subdivision and city of where the computation is.

In general, only one of country or country-exclave, subdivision or subdivision-exclave, and city or city-exclave will be present. When the exclave versions are present, if the Relying Party needs to indicate where the exclave is located, it may use the enclosing-exclave-country label.

The near-to-label is an arbitrary relative reference, and it refers to some other claim that the Relying Party is assumed to already know about. The definition of "near" is up to the Verifier, but in general, it is expected that it is close enough that it is in the same jurisdiction as the other entity.

The series of claims, Data-Center, Floor-Number, Room-Number, Hallway-Number, Cabinet-Number and Rack-U-Number form a partial hierarchy designed to identify where a piece of equipment is. This set of claims is more useful when a location Endorsement is created by an auditor, such as through the process described in Appendix A.

Not all data centers are numbered in the same way. For some, the Room-Number implies the Floor-Number. For others, the Hallway-Number implies both room and floor, and for still others, the Cabinet-Number is unique per building.

Rack-U numbers refer to the system within a cabinet, with the bottom most position labelled as 1. This accomodates cabinets of varying heights and capacities.

5. Security Considerations

These considerations do not cover the protocol described in Appendix A.

This document describes attributes that would go into an EAT format Attestation Result (EAR). This is an artifact that is communicated from a Verifier to a Relying Party. The threat model for this artifact is governed by a typical "CIA" list: Confidentiality, Integrity and Availability.

5.1. Confidentiality Threats

This artifact contains abtracted information about a location. The location could include where a person operating the computation is, such as if this describes the location of a person’s smartphone, in which case the location, even abstracted would be PII. It is almost always preferable for this artifact to remain private, however the integrity of the artifact is not compromised if that is not the case.

5.2. Integrity Threats

The most important threat is that claims could be corrupted or intentionally changed as they are transfered from Verifier to Relying Party. EAR are signed objects, and the signature from the Verifier maintains the integrity of that object. The claims present in this document will most often be combined with other claims in the same artifact.

When an EAT format Endorsement is created by an auditor, the auditor signs the artifact. The Endorsement may be provided to a Verifier through out of band means, or it can be stored by the Attesting Environment, and carried through another protocol from Attester to Verifier.

5.3. Availability Threats

This artifact is the result of a calculation or audit that establishes a result. Once created, it can be valid for a period of time from seconds (GNSS result on a smartphone) to months (human audit of a data center).

Distruptions to the mechanism of location calculation do not make the result of the previous calculation invalid. However, it is possible that such an attack could make subsequent calculations infeasible. For instance, the GNSS signals can easily be jammed.

6. IANA Considerations

IANA is asked to allocate TBD01 from the "CBOR Web Token Claims" registry [IANA.cwt] (from a Specification Required Integer range), and TBD02 (suggestion: "ear.geographic-result-claims") from the "JSON Web Token Claims" registry [IANA.jwt].

7. References

7.1. Normative References

[I-D.ietf-rats-ear]
Fossati, T., Voit, E., Trofimov, S., and H. Birkholz, "EAT Attestation Results", Work in Progress, Internet-Draft, draft-ietf-rats-ear-02, 27 January 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-rats-ear-02>.

[I-D.ietf-rats-endorsements]
Thaler, D., Birkholz, H., and T. Fossati, "RATS Endorsements", Work in Progress, Internet-Draft, draft-ietf-rats-endorsements-08, 25 February 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-rats-endorsements-08>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC7468] Josefsson, S. and S. Leonard, "Textual Encodings of PKIX, PKCS, and CMS Structures", RFC 7468, DOI 10.17487/RFC7468, April 2015, <https://www.rfc-editor.org/rfc/rfc7468>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC9334] Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote ATtestation procedureS (RATS) Architecture", RFC 9334, DOI 10.17487/RFC9334, January 2023, <https://www.rfc-editor.org/rfc/rfc9334>.

[RFC9711] Lundblade, L., Mandyam, G., O'Donoghue, J., and C. Wallace, "The Entity Attestation Token (EAT)", RFC 9711, DOI 10.17487/RFC9711, April 2025, <https://www.rfc-editor.org/rfc/rfc9711>.

7.2. Informative References

[IANA.cwt] IANA, "CBOR Web Token (CWT) Claims", <https://www.iana.org/assignments/cwt>.

[IANA.jwt] IANA, "JSON Web Token (JWT)", <https://www.iana.org/assignments/jwt>.

[IDevID] IEEE Standard, "IEEE 802.1AR Secure Device Identifier", 2018, <https://1.ieee802.org/security/802-1ar/l>.

[LLDP] IEEE Standard, "802.1AB-REV - Station and Media Access Control Connectivity Discovery", 19 June 2009, <https://www.ieee802.org/1/pages/802.1AB-rev.html>.

[obp] International Standards Organization, "ISO Online Browsing Platform", 1 March 2026, <https://www.iso.org/obp/ui/#search>.

[ptp] Wikipedia, "Precision Time Protocol", 7 October 2025, <https://en.wikipedia.org/wiki/Precision_Time_Protocol>.

[RFC9360] Schaad, J., "CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing X.509 Certificates", RFC 9360, DOI 10.17487/RFC9360, February 2023, <https://www.rfc-editor.org/rfc/rfc9360>.

[rollover] Wikipedia, "Console Rollover Cable", 26 April 2025, <https://en.wikipedia.org/wiki/Rollover_cable>.

[speed] Genuine Modules, "How fast does fiber optics travel?", 7 October 2025, <https://www.genuinemodules.com/how-fast-does-fiber-optics-travel_a6553>.

Appendix A. Proof of Presense

Some aspects of a device can not be intuited by the device itself. For instance, a router platform may have no way to know what color the case is, where in a cabinet it is located, or which electrical circuit it is connected to. This kind of information must be provided through an Endorsement: a statement from a third party.

These statements may require human audiitors to inspect the device physically. But, which device is really in front of an auditor? This document describes a mechanism by which an auditor can make physical contact with a device and collect information to identify the device in a cryptographically strong manner.

The Proof of Presence protocol is intended to provide a mechanism by which device identity can be established via non-networked, physical cabling such as a USB cable, or a serial (craft) console.

A.1. Introduction

In the RATS Architecture [RFC9334], an important input to the Verifier function is the Endorsement. Endorsements [I-D.ietf-rats-endorsements] provide information that the Attester can not inherently know. This includes a statement that a particular (Attester) keypair belongs to a device of a particular type. Some of this information might be placed into device identity certificate (such as an IDevID [IDevID]), but many other kinds of claims would not belong.

For instance, the physical location or connectivity of a device would be subject to change. In some cases a GPS coordinate might make sense, but in other cases GPS might not be trustworthy, or might be inadequate. The physical location of a router, as being in "Building 4, Aisle 37, Cabinet 9, Rack Unit 2-3" would be a level of precision that GPS would be unable to provide. Other claims might involve knowledge of the color of a device ("the red car"), or the connectivity of the device ("the device plugged into the blue cable"). A relative claim might also be relevant: The house on top of the person with Ruby Slippers.

In these cases an endorsement will need to be created, often by a human inspector/auditor that will have to physically visit the device and ascertain the state of the device. There are some challenges for such an auditor: they could be led astray by malicious intent to inspect the wrong device, or they could simply not locate the device they intended to audit. This results in an endorsement linked to the wrong device.

A.1.1. Overview of mechanism

The auditor is equiped with a portable device (e.g., a tablet computer) containing an endorsement signing key. This is the audit device. (This could be an actual key, or it could just be a secure/ tamperproof container in which endorsements will be stored until a long-term/more-secure endorsement key can be employed)

The auditor finds the device in question and then collects whatever information is relevant. For instance, the location in whatever form makes sense for the endorsement. That might include taking pictures of the device in-situ, scans of serial numbers on the outside of the case, and which cables are connected to which physical ports.

The auditor then plugs a physical cable between their audit device and the device under audit. This cable is envisioned to be either a USB console "rollover" cable [rollover]. The audit device then initiates some commands over this cable that will result in a proof of the idnetity of connected device.

A.2. Terminology

Audit Device: The device that is used to collect information that will go into endorsements.

Device Under Audit: Abbreviated to DUA. The device for which endorsements are being made.

Auditor: The human who inspects the Device Under Audit.

A.3. Presence Protocol

It is assumed that the console port has been designed for use by humans. This protocol is designed to interact as if it’s a human. Note that more sophisticated mechanisms such as SLIP or PPP would be more vulnerable to spoofing.

A.3.1. Initial Handshake

The audit device sends carriage returns (octet 13) until it sees a response with a colon (":") in it. This is usually a "login:" or "username:" prompt of some kind. The audit device then sends the word "endorsementaudit" with a carriage return. This represents a user login, and for some systems this can be set as a real login with limited permissions. It could run a special audit shell that only can perform system audits. On other systems, this might just an unpriviledged account with the normal prompts and commands.

The handshake is over when the word "endorsement" is seen.

A.3.2. Proof of Presence

(Proof of Presence, or POP, is not a great TLA, as it often refers to proof that a private key is used. A better name is saught)

All commands are prefixed with "rfcXXXX" (with a trailing space, where XXXX is the number of this document). A second word indicates the command. The allows the device under audit to collect all operations under a single command or command sub-system.

The audit device then sends the word/command "position-proof", followed by a 33 byte nonce, base64URL encoded into a 45 byte string. (33 bytes are recommended because being divisible by three, they encode evenly in base64, leaving no trailing =)

The device under audit then responds with a CBOR format EAT object, encoded in base64URL, and wrapped in the strings "--- BEGIN COSE OBJECT ---" and "--- END COSE OBJECT ---" {XXX: or should we use CBOR Diagnostic Format?}

The EAT payload should be constructed as follows. Shown are a few attributes that would make sense to include. The above provide nonce becomes the eat_nonce.

```
{
    / eat_nonce /       10: h'948f8860d13a463e8e',
    / ueid /           256: h'0198f50a4ff6c05861c8860d13a638ea',
    / oemid /          258: h'894823', / IEEE OUI format OEM ID /
    / hwmodel /        259: h'549dcecc8b987c737b44e40f7c635ce8'
                            / Hash of chip model name /,
    / hwversion /      260: ["1.3.4", 1], / Multipartnumeric version /
    / swname /         271: "Acme OS",
    / swversion /      272: ["3.5.5", 1],
    }
```

The EAT payload is signed using the device under audit's Attestation Key. (A TPM's Endorsement Key can not sign things) The hash of the Attestation Key is provided in the unprotected headers.

```
61( 18( [
    h'A10126',                          / protected headers  /
    {
    / x5t / 34: [16, h'12344567812345678123445678123456 78'],
    },                                  / unprotected headers /
    h'A20B46024A6B0978DE0A490001020304050607 08',    / payload /
    h'9B9B2F5E470000F6A20C8A4157B5763FC45BE759
      9A5334028517768C21AFFB845A56AB557E0C8973
      A07417391243A79C478562D285612E292C622162
      AB233787'                                    / signature /
] ) )
```

x5t is from [RFC9360]. The hash algoritm SHOULD be SHA256, or newer. (Example to be updated.

A.3.3. Collection of Endorsement Claims

The audit device then validates the received EAT object from the device. The audit device locates the public part of the device's Attestation Key. This will in most cases be part of the "work order" that the auditor has been provided, but in some cases, the auditor will have to collect it from the device.

For instance, a device might have been replaced since the audit was requested, or there might be additional devices that the auditor thinks might be relevant. An example might be when a switching device has many cables connected into an adjacent optical media converter that puts multiple signals through a single multi-frequency optical cable. Such a layer of indirection might affect the audit's ability to indicate which port is physically connected to which cable.

Some key physical information that an auditor might need to collect is which fibre patches are connected to which ports of the switch. This information would be ideally collected by scanning (and checking) labels on the fibre patches.

A.3.4. Additional Commands

Some additional commands can be provided by the device under audit:

"attestation-key": This command returns the public certificate for the device's Attestation Key in [RFC7468] Certificate format.

"port-flash": This command takes an interface number/name (e.g., "GigabitEthernet 3/014"), and causes the LEDs adjacent to a particular port to flash in a distinct pattern. This is to help identity which physical port is which.

"port-down": This command takes an interface number/name (as above), and causes the switch to mark the physical port as down, but not turn off the laser. Traffic SHOULD be re-routed as if the fibre has failed. This is a disruptive test! The auditor may then physically unplug the fibre as part of an audit of the fibre paths. This command might not perform the action immediately, but could signal to the network operations center that such a test is desired, and allow them to approve it.

"port-up": Indicates the end of an path-audit started by "port-down".

"endorsements": This command is followed by a base64URL encoded CBOR Sequence of Endorsements, wrapped in the same BEGIN COSE header and footer as before. To guard against failure during, the device under audit SHOULD time out this command after 120s if no END COSE OBJECT framing is seen. This command allows the auditor to load any resulting endorsements directly into the device to be passed up along with Evidence to a Verifier.

"exit": This command indicates that the audit is over, and the device under audit can return the console interface to the normal state.

A.3.5. Generation of Endorsement

The auditor, having collected one or more proofs, then transmits them to the endorsement agency. This may be via physical transfer, secured email, or some secured online API.

The endorsement agency then needs to do the following:

1. locate the Endorsement Certificate, if it was not collected from the device.

2. validate that the provided EAT is signed by the associated Endorsement Key.

3. validate that the claims in the EAT are consistent with that which is expected from the device.

4. validate the format of the additional information collected by the auditor. Location, type and number of connections, (colour of device even).

From this, one or more Endorsements are then created and signed by the endorsing agency.

In some cases the auditor might be entirely self-contained, producing the endorsements directly on their audit device. In that case, they would use the "endorsements" to load the resulting Endorsements directly into the device.

A.4. Alternatives to USB/serial cables

There are a number of cases where a USB or serial console cable might be unavailable, or it's might be undesireable. Many smaller IoT devices, home routers and consumer items do not have any kind of console available. The console access might require removal of the case, which might be impossible to do while the device is operational, or while the device is physically installed. Console access might provide access to a priviledged prompt; that access might either be unsafe to give to the auditor, or might require a password to access that should not be shared.

One alternative is to use Ethernet. Most routing platforms have many ethernet ports, and usually have at least one empty ethernet port. It is also common for there to be a dedicated copper ethernet port for management even on routing platforms that otherwise only have fiber-optic ports running at multiple hundred gigabits. The use of ethernet has problems because ethernet can easily be switched; transmitting the signal to another device elsewhere. This is often the whole point of the routing platform: to switch traffic elsewhere. This would result in a false audit if the auditor is diverted.

The LLDP protocol [LLDP] is a one-hop protocol which is usually not forwarded. It can do things like tell a connected device which port of client device is connected to. While trustworthy devices will not forward LLDP frames, an untrustworthy device that has been programmed to participate in a subterfuge might well forward frames. It might be possible to construct a challenge/response system that has the auditor plug cables in some non-deterministic order in order to defeat the subterfuge.

This process would probably need to augmented with some other forms of feedback; perhaps flashing of status LEDs on the device in a pattern.

Note: the console/USB cable could also be redirected to another host!

A.5. Privacy Considerations

The ability to walk up to a device and interogate it as to it's identity is potentially privacy violating if the device is associated with a person. This would include all kinds of small devices: phones, laptops, electric bicycles, automobiles,

One countermeasure is that the device needs to be put into an audit mode before it can be interrogated. This is reasonable for some devices and some audit processes, but for other processees, the need to do random audits may countermand this need. For devices such as large routing platforms, they are often located in data centers with multiple layers of physical access control: locked buildings, locked machine rooms, and locked cabinets. For such devices, there are perhaps few privacy concerns, and the auditor needs credentials in order to access the device at all.

A.6. Security Considerations

There are three concerns with this protocol.

The first is the potential for unauthorized people to collect information about devices to which they have no authority to interogate. In industrial settings, this is mitigated by physical access controls. In those settings the ability to identify devices which may be physically misbehaving or are damaged and connect them to their digital identity significantly outweighs any concerns about device identity.

In consumer and retail settings, the device SHOULD not respond to this protocol unless an operator/owner has put the device into device identication mode.

The second concern with this protocol is that it might be spoofed or confuzzled. The auditor could be mislead as whether the device in front of them is really the device that is responding to their queries. The auditor SHOULD have the device identity with them already as part of the work order. They should therefore not be mislead as to which device they intend to audit, the issue is that it might not be the device that is physically in front of them. The device might be a mock-up designed to look right, but really it is wired secretly to the real device which is elsewhere, and is differently configured. This attack is called the "Sock-Puppet" attack.

Such attacks require physical examination to detect. Some attacks may be mitigated through careful use of the "port-flash" commands to cause signals visible to the auditor that would ideally be difficult to fake. Efforts this way are the subject of further work.

The third concern with this protocol is that it might open up the device to attacks via this console port. The Initial Handshake Appendix A.3.1 mechanism is designed so that it can be easily implemented by typical router and operating system login mechanisms. A very limited account would be created, or even a mode within the

login mechanism itself, and so no additional inquiries would be possible. Some operators prefer to never have a login process on the console/craft ports of their devices. This is usually done so that maintenance people do not need to have passwords that can then be re-used over a network, weaking the security of the device. They depend upon physical security for the console ports to provide security. Such operators might wish to rethink this policy for devices which will be subject to audit.

A.7. IANA Considerations

IANA is asked to allocate a CBOR Tag for this object. Details TBD.

Appendix B. Acknowledgements

Your name here.

Appendix C. Changelog

Acknowledgments

TODO acknowledge.

Author’s Address

Michael Richardson
Sandelman Software Works
Email: mcr+ietf@sandelman.ca