Independent Submission
Internet-Draft
Intended status: Informational
Expires: 6 December 2026

M. K. Savich
4 June 2026

Residential Network Mapping Model
draft-savich-residential-network-map-00

Abstract

Residential networks increasingly include managed routers, switches, wireless access points, home lab systems, smart home devices, surveillance devices, guest networks, and cloud-connected equipment. These devices are often added incrementally without a durable mapping model for addressing, classification, review, or troubleshooting.

This document describes a lightweight residential network mapping model for IPv4 address planning and device classification. The model defines Network Categories, Addressing Priority, Trust Levels, Exposure Levels, device record fields, flat-network and segmented-network examples, and simple review and change-log practices.

The motivation for this document is security awareness. A residential network map can help consumers understand what kinds of devices are on their network, which devices are trusted or restricted, which devices are reachable locally or remotely, and where personal or household data may flow. The model is intended for regular users and technically capable home administrators who need a practical way to organize residential, home lab, IoT, and surveillance networks without deploying enterprise network management systems.

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 6 December 2026.

Table of Contents

1. Introduction

Residential networks are no longer limited to a router, a few laptops, and a printer. Many homes now contain managed routers or firewalls, switches, wireless access points, smart home systems, surveillance systems, guest networks, home lab equipment, cloud-connected devices, and transient client devices.

These environments often grow incrementally. A router is installed. A switch is added. A camera appears. A robotic cleaner joins the network. A guest network is enabled. A network-connected vehicle, EV charger, thermostat, streaming device, or appliance begins using an address. Over time, the administrator can lose track of which

devices exist, which addresses are assigned, which devices should receive stable addresses, which devices are trusted, and which devices are reachable locally or remotely.

This document describes a lightweight residential network mapping model that combines:

* IPv4 address planning,
* device classification,
* addressing stability guidance,
* trust posture,
* exposure posture,
* review practices, and
* lightweight change tracking.

This document does not define a new protocol. It defines an operational mapping model that can be implemented as a worksheet, spreadsheet, Markdown document, database table, configuration record, or simple network mapping tool.

2. Terminology

The following terms are used in this document.

Administrator: The person or group responsible for maintaining the residential network and its mapping records.

Address Plan: A documented allocation of IPv4 addresses or address ranges to Network Categories.

Addressing Priority: A classification field that describes how stable a device's address assignment is expected to be.

Device Record: A structured record describing a mapped network device.

Dynamic Address: An IP address assigned by DHCP without a fixed reservation.

Exposure Level: A classification field that describes how reachable a mapped device is expected to be.

Flat Network: A network where multiple device classes share a common subnet, such as 192.0.2.0/24.

Network Category: A logical network zone or administrative grouping. In segmented networks, a Network Category often maps to a VLAN, subnet, SSID, firewall zone, or equivalent control boundary. In flat networks, a Network Category can still be used as an administrative mapping label.

Residential Network Map: A structured representation of devices, addresses, categories, and classification information for a residential network.

Segmented Network: A network where devices are separated into multiple VLANs, subnets, SSIDs, firewall zones, or equivalent control boundaries.

Static Address: An IP address manually configured on a device or otherwise fixed so that the device is expected to remain reachable at that address.

DHCP Reservation: An IP address assigned by a Dynamic Host Configuration Protocol server to a specific device, typically based on a link-layer address.

Trust Level: A classification field that describes the expected access posture of a mapped device.

3. Requirements Language

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.

4. Applicability

This document applies to residential, home lab, and prosumer networks that include managed routing, switching, guest access, Internet of Things devices, and surveillance devices.

The model is intended for networks where address planning and device classification are useful, but enterprise network management systems are unnecessary or impractical.

This document is most applicable to:

* residential networks with managed routing or switching,
* home lab networks,
* smart home networks,
* residential IoT networks,
* residential surveillance networks,
* networks with guest access,
* networks maintained by technically capable homeowners,
* networks maintained by family members or informal administrators, and
* networks maintained by residential technology consultants or integrators.

The examples in this document use IPv4 documentation addresses. A real residential deployment would normally use IPv4 private address space, including the address ranges described in [RFC1918]. IPv6 mapping guidance is out of scope for this version of the document.

This document is not limited to any router, firewall, wireless, surveillance, smart home, or home lab vendor.

5. Design Goals

The mapping model described in this document has the following goals:

* provide predictable address planning,
* classify devices consistently,
* distinguish network zones from trust and exposure posture,
* identify devices that need stable addressing,
* improve consumer awareness of the types of devices on the network,
* help administrators recognize devices that may collect, transmit, or expose household data,
* encourage review of devices with remote access or unknown classifications,

* reduce address conflicts,
* support troubleshooting,
* support flat networks and segmented networks,
* remain usable by regular home-network administrators,
* avoid credential collection, and
* provide a simple path from an informal worksheet to a structured map.

6. Non-Goals

This document does not define:

* a new Internet protocol,
* a full enterprise IP address management system,
* a firewall policy model,
* a network monitoring system,
* a credential vault,
* an automated device discovery protocol,
* IPv6 address planning,
* residential audio/video system classification,
* a complete zero trust architecture,
* a vendor-specific configuration method, or
* a replacement for professional network design or security assessment.

This document does not define firewall policy between Network Categories. Administrators can use Network Categories as inputs to firewall or segmentation policy, but those policies are out of scope for this document.

7. Mapping Model Overview

A residential network map describes devices using four classification axes:

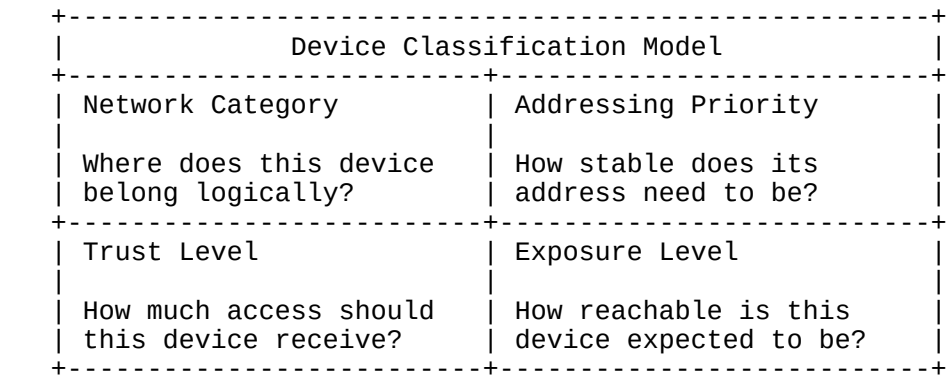
* Network Category,
* Addressing Priority,
* Trust Level, and
* Exposure Level.

These axes answer four different questions:

The four classification axes answer these questions:

* Network Category: Where does this device belong logically?
* Addressing Priority: How stable does this device's address assignment need to be?
* Trust Level: How much access should this device receive?
* Exposure Level: How reachable is this device expected to be?

The following diagram shows the four classification questions used by the residential network mapping model.



These axes are intentionally separate. For example, a device can belong to the IoT Network Category, have a Restricted Trust Level, and have a Remote Access Exposure Level. Similarly, a device can belong to the Main Network Category while still having a Restricted Trust Level if the administrator does not fully trust it.

8. Network Categories

A Network Category represents the logical network zone or administrative grouping to which a device belongs.

This document defines the following Network Categories:

* Management,
* Main,
* Guest,
* IoT,
* Surveillance, and
* Unknown.

In a segmented network, a Network Category often maps one-to-one to a VLAN, subnet, SSID, firewall zone, or equivalent control boundary. In a flat network, a Network Category can still be used as an administrative label for planning and documentation.

8.1. Management

The Management category is used for devices and interfaces involved in administering or operating the network.

Examples include:

* router or firewall management interfaces,
* switches,
* wireless access points,
* network controllers,
* local network management systems, and
* administrative appliances.

Devices in this category commonly require stable addressing.

8.2. Main

The Main category is used for trusted household or primary user devices.

Examples include:

* personal laptops,
* desktop computers,
* phones,
* tablets,
* trusted printers,
* trusted storage devices, and
* other regular household devices.

The Main category is commonly associated with the primary LAN or primary trusted Wi-Fi network.

8.3. Guest

The Guest category is used for visitor, temporary, or contractor devices.

Examples include:

* visitor phones,
* visitor laptops,
* contractor devices, and
* temporary devices that should not be treated as trusted household devices.

8.4. IoT

The IoT category is used for smart home, appliance, embedded, cloud-connected, or lower-trust connected devices.

Examples include:

* smart thermostats,

* robotic cleaners,
* smart speakers,
* appliances,
* lighting bridges,
* smart plugs,
* EV chargers,
* connected vehicles,
* sensors, and
* vendor-managed smart devices.

8.5. Surveillance

The Surveillance category is used for physical monitoring and video security devices.

Examples include:

* IP cameras,
* network video recorders,
* video door stations,
* camera bridges,
* intercom cameras, and
* other monitoring devices.

The Surveillance category is intentionally narrower than a general "Security" category. A general Security category can become ambiguous because it could include firewalls, alarm panels, door locks, cameras, identity systems, endpoint security tools, or access control systems.

8.6. Unknown

The Unknown category is used for devices that have been discovered but not yet classified.

The Unknown category is intended as a temporary holding category by default. Devices SHOULD NOT remain in the Unknown category indefinitely without review.

If a device remains Unknown for an extended period, the Notes field SHOULD explain why the device has not been reclassified.

9. Addressing Priority

Addressing Priority describes the addressing stability expected for a mapped device.

This document defines the following Addressing Priority values:

* Static Required,
* Reservation Recommended, and
* Dynamic Acceptable.

9.1. Static Required

Static Required means the device needs predictable addressing. A static address or a functionally equivalent fixed assignment is expected.

This value is appropriate when loss of address predictability can disrupt administration, routing, switching, surveillance, automation, or core network operation.

Examples include:

* router or firewall management interfaces,
* switches,
* wireless access points,
* network controllers,
* network video recorders, and
* other devices that must remain reachable for troubleshooting.

9.2. Reservation Recommended

Reservation Recommended means the device should receive a stable DHCP reservation when practical, but the network can tolerate temporary dynamic assignment.

This value is appropriate for devices that are easier to maintain when their address is stable, but that are not core network infrastructure.

Examples include:

* cameras,
* printers,
* smart home hubs,
* robotic cleaners,
* EV chargers, and
* devices commonly accessed from applications or local dashboards.

9.3. Dynamic Acceptable

Dynamic Acceptable means the device can use ordinary DHCP without a fixed reservation.

This value is appropriate for devices that do not require a predictable address.

Examples include:

* ordinary phones,
* laptops,
* tablets,
* guest devices, and
* transient devices.

10. Trust Levels

Trust Level describes the expected access posture of a mapped device.

This document defines the following Trust Levels:

* Management,
* Trusted,
* Restricted,
* Guest, and
* Unknown.

10.1. Management

The Management Trust Level is used for devices or interfaces that administer, control, or operate network infrastructure.

Examples include router management interfaces, switch management interfaces, wireless controller interfaces, and network administration systems.

10.2. Trusted

The Trusted Trust Level is used for known household or primary user devices that are expected to have ordinary access to the Main network.

Examples include trusted laptops, phones, tablets, and workstations.

10.3. Restricted

The Restricted Trust Level is used for known devices that should receive limited access compared with Trusted devices.

Examples include IoT devices, surveillance devices, appliances, smart home devices, and devices with unclear update or security posture.

10.4. Guest

The Guest Trust Level is used for visitor or temporary devices.

10.5. Unknown

The Unknown Trust Level is used when the trust posture of a device has not yet been determined.

Devices SHOULD NOT remain Unknown indefinitely without review.

11. Exposure Levels

Exposure Level describes how reachable a mapped device is expected to be.

This document defines the following Exposure Levels:

* Internal Only,
* Local Shared,
* Remote Access,
* Internet Exposed, and
* Unknown.

11.1. Internal Only

Internal Only is used for devices that should only be reachable for device-specific operation or administration.

Examples include switches, management interfaces, and cameras that should not be accessed directly by ordinary client devices.

11.2. Local Shared

Local Shared is used for devices that provide services to other devices on the local network.

Examples include printers, storage devices, shared controllers, local media services, or devices intentionally discoverable by trusted local clients.

11.3. Remote Access

Remote Access is used for devices that are reachable from outside the local network through a controlled method, such as a vendor cloud service, VPN, managed remote access feature, or remote management application.

11.4. Internet Exposed

Internet Exposed is used for devices that are directly reachable from the public Internet or through an explicit port forwarding rule.

This document does not define port-forwarding record fields. The Internet Exposed value is intended only to help regular administrators identify that a device has public exposure.

11.5. Unknown

Unknown is used when reachability has not yet been verified.

Devices SHOULD NOT remain Unknown indefinitely without review.

12. Classification Consistency

A mapped device can have classifications that appear unusual. For example, a device can belong to the IoT Network Category while having a Remote Access Exposure Level, or a device in the Main Network Category can have a Restricted Trust Level.

When classification fields appear to conflict, administrators SHOULD review whether the device belongs in the correct Network Category and whether the Trust Level or Exposure Level accurately reflects how the device is used.

Unusual classifications MAY be valid, but the Notes field SHOULD explain the reason.

13. Classification Examples

The following examples illustrate how the four classification axes can be applied.

* router-1
  - Network Category: Management
  - Addressing Priority: Static Required
  - Trust Level: Management
  - Exposure Level: Remote Access
  - Notes: Primary gateway with administrative access.
* switch-1
  - Network Category: Management
  - Addressing Priority: Static Required

    - Trust Level: Management
    - Exposure Level: Internal Only
    - Notes: Main switch.

* phone-1
    - Network Category: Main
    - Addressing Priority: Dynamic Acceptable
    - Trust Level: Trusted
    - Exposure Level: Local Shared
    - Notes: Trusted household device.

* camera-1
    - Network Category: Surveillance
    - Addressing Priority: Reservation Recommended
    - Trust Level: Restricted
    - Exposure Level: Internal Only
    - Notes: IP camera.

* nvr-1
    - Network Category: Surveillance
    - Addressing Priority: Static Required
    - Trust Level: Restricted
    - Exposure Level: Remote Access
    - Notes: Network video recorder.

* robotic-cleaner-1
    - Network Category: IoT
    - Addressing Priority: Dynamic Acceptable

- Trust Level: Restricted
- Exposure Level: Remote Access
- Notes: Vendor app access.

* guest-phone-1
  - Network Category: Guest
  - Addressing Priority: Dynamic Acceptable
  - Trust Level: Guest
  - Exposure Level: Local Shared
  - Notes: Visitor device.

* unknown-1
  - Network Category: Unknown
  - Addressing Priority: Dynamic Acceptable
  - Trust Level: Unknown
  - Exposure Level: Unknown
  - Notes: Needs review.

14. Device Records

A mapped device SHOULD have a device record.

A device record SHOULD contain the following fields:

The device record fields are listed below in their canonical order.

Hostname: Required. A human-readable hostname, device hostname, or administrator-assigned label.

IP Address: Required. The assigned IPv4 address.

MAC Address: Recommended. The link-layer address used for identification or DHCP reservation.

Manufacturer: Recommended. The device manufacturer or vendor.

Network Category: Required. One of Management, Main, Guest, IoT, Surveillance, or Unknown.

Addressing Priority: Required. One of Static Required, Reservation Recommended, or Dynamic Acceptable.

Trust Level: Required. One of Management, Trusted, Restricted, Guest, or Unknown.

Exposure Level: Required. One of Internal Only, Local Shared, Remote Access, Internet Exposed, or Unknown.

Notes: Optional. Location, purpose, firmware, switch port, owner, review note, or other context.

This document does not define a separate device-type taxonomy. Device type can be recorded in freeform Notes or implementation-specific metadata when useful.

This document also does not define credential fields. Administrators SHOULD NOT store credentials in the residential network map.

15. Credential Guidance

The network map defined by this document does not include credential fields.

Administrators SHOULD store credentials in a password manager or other credential management system rather than in the network map.

Administrators MUST NOT store plaintext passwords in a published or shared residential network map.

If a separate credential system is used, the network map MAY note that a credential exists elsewhere, but it SHOULD NOT include the credential itself, password hints, recovery answers, multi-factor recovery codes, or shared secrets.

16. Flat Networks and Segmented Networks

The Network Categories defined by this document can be used in both flat and segmented residential networks.

In a flat network, all devices may share a single subnet, such as 192.0.2.0/24. In this case, Network Categories are administrative labels that help the administrator plan addresses and classify devices.

In a segmented network, Network Categories can map to VLANs, subnets, SSIDs, firewall zones, or equivalent control boundaries. For example, Management, Main, Guest, IoT, Surveillance, and Unknown can each map to a separate VLAN and subnet.

This document does not require segmentation. A residential network map can begin as a flat-network planning tool and later evolve into a segmented design.

17. Flat-Network Address Planning

In a flat network, Network Categories can be mapped to ranges within a single subnet.

The following example uses 192.0.2.0/24, which is reserved for documentation examples.

Example flat-network ranges:

* Management: 192.0.2.1-192.0.2.19
  - Router, firewall, switches, access points, and management interfaces.
* Main: 192.0.2.20-192.0.2.99
  - Trusted household devices.
* IoT: 192.0.2.100-192.0.2.159
  - Smart home devices, hubs, sensors, appliances, and cloud-connected devices.
* Surveillance: 192.0.2.160-192.0.2.199
  - Cameras, network video recorders, and door stations.
* Guest: 192.0.2.200-192.0.2.239
  - Guest DHCP pool.
* Unknown: 192.0.2.240-192.0.2.254
  - Temporary holding range for unclassified devices.

In a /24 network, the .0 address is the network address and the .255 address is the broadcast address. These addresses MUST NOT be assigned to hosts.

The ranges in this section are examples only. Administrators can choose different ranges based on network size, router capabilities, existing address assignments, or operational preference.

18. Segmented-Network Address Planning

In a segmented network, Network Categories can map to VLANs, subnets, SSIDs, firewall zones, or equivalent control boundaries.

The following example uses one documentation subnet slice per Network Category. A real deployment would normally use private IPv4 subnets.

Example segmented-network layout:

* Management
  - VLAN: 10
  - Subnet: 192.0.2.0/28
  - Notes: Router, firewall, switches, access points, and management interfaces.
* Main
  - VLAN: 20
  - Subnet: 192.0.2.16/28
  - Notes: Trusted household devices.
* IoT
  - VLAN: 30
  - Subnet: 192.0.2.32/28
  - Notes: Smart home devices, hubs, sensors, appliances, and cloud-connected devices.
* Surveillance
  - VLAN: 40
  - Subnet: 192.0.2.48/28
  - Notes: Cameras, network video recorders, and door stations.

* Guest
  - VLAN: 50
  - Subnet: 192.0.2.64/28
  - Notes: Guest devices.
* Unknown
  - VLAN: 99
  - Subnet: 192.0.2.80/28
  - Notes: Unclassified devices pending review.

This document does not define firewall policy between these categories.

19. Review Guidance

A residential network map SHOULD be reviewed when meaningful network changes occur.

Examples of meaningful changes include:

* adding or removing a device,
* changing a device address,
* creating or removing a DHCP reservation,
* moving a device to a different Network Category,
* changing a device Trust Level,
* changing a device Exposure Level,
* adding a guest network,
* adding an IoT device,
* adding a surveillance device,
* replacing the router or firewall,
* replacing a switch, and

* replacing an access point.

Administrators SHOULD also review the map periodically to identify unknown devices, outdated records, and devices that no longer match their intended classification.

This document does not define a fixed review interval. A review interval can be selected based on the size, complexity, and risk of the network.

20. Change Log

A residential network map SHOULD include a lightweight change log.

The change log helps administrators understand when meaningful network changes occurred and why they were made.

A change log entry SHOULD include:

A change log entry SHOULD include:

* Date: The date of the change.

* Change: What changed.

* Reason: Why the change was made.

Example:

* 2026-06-04
  - Change: Added IoT Network Category.
  - Reason: Smart home devices needed separate classification.
* 2026-06-08
  - Change: Reserved address for main switch.
  - Reason: Switch should remain reachable for troubleshooting.
* 2026-06-12
  - Change: Moved unknown device to Guest.
  - Reason: Device was identified as a visitor phone.

21. Troubleshooting Uses

The mapping model is intended to support ordinary troubleshooting.

21.1. Address Conflicts

When an address conflict is suspected, an administrator can:

1. check the residential network map for the assigned device,
2. check router or firewall client lists,
3. check DHCP lease records,
4. compare the observed MAC address with the mapped MAC address,
5. identify duplicate static assignments or reservation conflicts,
6. correct the assignment, and
7. update the map.

21.2. Unknown Devices

When an unknown device is discovered, an administrator can:

1. record the IP address,
2. record the host name if available,
3. record the MAC address if available,
4. record the manufacturer if available,
5. classify the device as Unknown,
6. investigate the device,
7. reclassify the device when identified, and
8. add a note if the device remains Unknown.

21.3. Unreachable Devices

When a mapped device is unreachable, an administrator can check:

1. whether the device is powered on,

2. whether the device is connected to the expected network,

3. whether the device address changed,

4. whether the device appears in the router or firewall client list,

5. whether the mapped MAC address matches the observed MAC address,

6. whether the device moved to a different Network Category, and

7. whether recent changes explain the issue.

22. Privacy Considerations

A completed residential network map can reveal sensitive operational details.

Examples include:

* internal addressing,
* host names,
* MAC addresses,
* device manufacturers,
* network categories,
* trust posture,
* exposure posture,
* camera or surveillance device presence,
* smart home device presence,
* guest network structure,
* management infrastructure, and
* maintenance patterns.

Completed maps SHOULD be protected from unauthorized access.

Administrators SHOULD consider:

* encrypted storage,

* restricted sharing,
* secure backups,
* redaction before vendor sharing,
* removal of sensitive fields before publication, and
* avoiding publication of real host names, MAC addresses, or locations.

Public examples SHOULD use fictitious MAC addresses, fictitious host names, and non-sensitive device descriptions.

23. Security Considerations

The practices described in this document can improve residential network manageability and consumer security awareness, but they can also concentrate sensitive information into one artifact.

A residential network map can help an administrator identify devices that may affect privacy or security, including devices that collect video, audio, location, usage, occupancy, or behavioral data. It can also help identify devices that rely on remote access, vendor cloud services, or unclear connectivity patterns.

This document does not attempt to define where each device sends data or whether a device’s data handling is acceptable. Instead, it provides a simple structure that can help consumers notice which classes of devices exist on the network and which devices deserve further review.

If an attacker obtains a completed residential network map, the attacker may gain insight into device roles, management interfaces, internal addressing, device manufacturers, device trust posture, device exposure posture, and possible privacy-sensitive device categories.

Administrators MUST NOT store plaintext passwords in the map.

Administrators SHOULD restrict access to completed maps.

Administrators SHOULD avoid sharing maps that contain real MAC addresses, host names, device locations, or other sensitive operational details unless sharing is necessary and appropriately controlled.

Administrators SHOULD review Unknown devices, devices marked Internet Exposed, and devices marked Remote Access.

Administrators SHOULD pay particular attention to IoT and Surveillance devices because these devices may collect or transmit household data that users do not routinely inspect.

Administrators SHOULD update the map after meaningful network changes.

Security considerations for protocol design are discussed more generally in [RFC3552]. Although this document does not define a protocol, the same general discipline applies: operational guidance should identify risks and mitigations clearly.

24. IANA Considerations

This document has no IANA actions.

25. References

25.1. Normative References

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <https://www.rfc-editor.org/info/rfc1918>.

[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/info/rfc2119>.

[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/info/rfc8174>.

25.2. Informative References

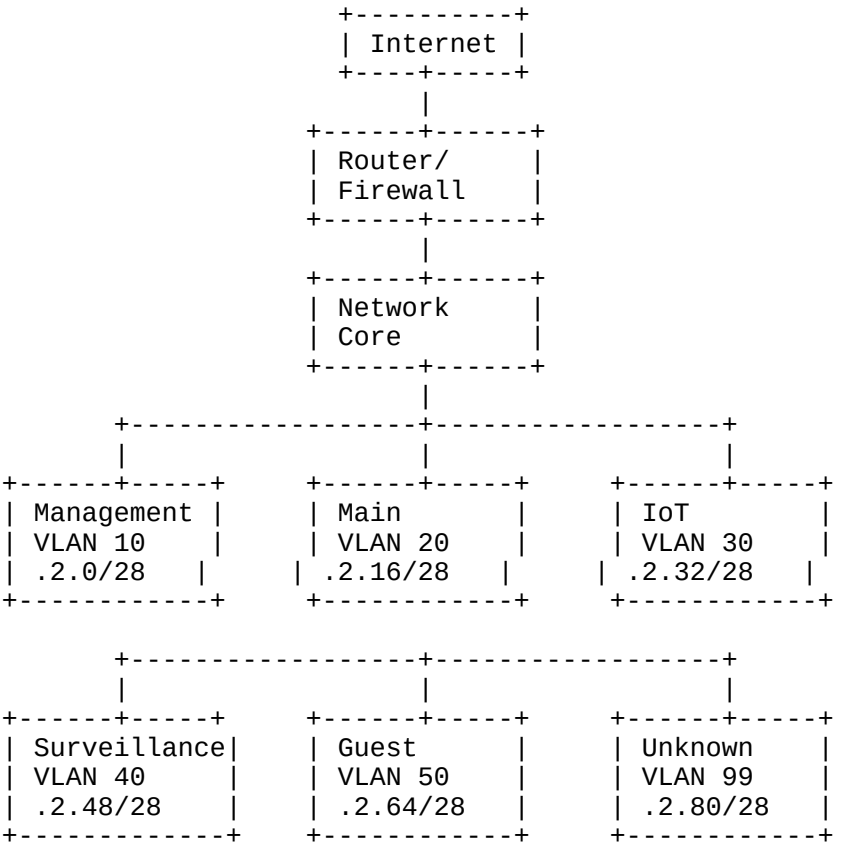
[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <https://www.rfc-editor.org/info/rfc3552>.

Appendix A. Example Network Map

The following example illustrates how the Network Categories defined in this document can be represented as a residential network map.

The diagram is illustrative only. It does not define required topology, firewall policy, routing behavior, or permitted communication between categories.

Example Residential Network Map



In a flat-network implementation, the same categories can be represented as ranges inside a single subnet instead of separate VLANs or subnets.

Appendix B. Example Device Records

The following tables provide realistic but sanitized example device records for a residential, home lab, IoT, and surveillance network. The IP addresses are documentation addresses and are not intended for deployment.

The fields are listed in the canonical order defined by this document.

B.1. Router

Field	Value
hostname	router-1
ip_address	192.0.2.1
mac_address	00:00:5E:00:53:01
manufacturer	Example Router Vendor
network_category	Management
addressing_priority	Static Required
trust_level	Management
exposure_level	Remote Access
notes	Primary gateway

Table 1

B.2. Switch

Field	Value
hostname	switch-1
ip_address	192.0.2.10
mac_address	00:00:5E:00:53:10
manufacturer	Example Switch Vendor
network_category	Management
addressing_priority	Static Required
trust_level	Management

exposure_level	Internal Only
notes	Main switch

Table 2

B.3. Wireless Access Point

Field	Value
hostname	ap-1
ip_address	192.0.2.11
mac_address	00:00:5E:00:53:11
manufacturer	Example Wireless Vendor
network_category	Management
addressing_priority	Static Required
trust_level	Management
exposure_level	Internal Only
notes	Wireless access point

Table 3

B.4. Smart Display

Field	Value
hostname	smart-tv-1
ip_address	192.0.2.50
mac_address	00:00:5E:00:53:50
manufacturer	Samsung Electronics
network_category	IoT

addressing_priority	Reservation Recommended
trust_level	Restricted
exposure_level	Local Shared
notes	Smart display or television

Table 4

B.5. Camera

Field	Value
hostname	camera-1
ip_address	192.0.2.64
mac_address	00:00:5E:00:53:64
manufacturer	Hikvision
network_category	Surveillance
addressing_priority	Reservation Recommended
trust_level	Restricted
exposure_level	Internal Only
notes	IP camera

Table 5

B.6. Robotic Cleaner

Field	Value
hostname	robotic-cleaner-1
ip_address	192.0.2.100
mac_address	00:00:5E:00:53:70

manufacturer	Espressif
network_category	IoT
addressing_priority	Dynamic Acceptable
trust_level	Restricted
exposure_level	Remote Access
notes	Robotic cleaner or embedded smart device

Table 6

B.7. Phone

Field	Value
hostname	phone-1
ip_address	192.0.2.106
mac_address	00:00:5E:00:53:71
manufacturer	Unknown
network_category	Main
addressing_priority	Dynamic Acceptable
trust_level	Trusted
exposure_level	Local Shared
notes	Trusted personal mobile device

Table 7

B.8. EV Charger

Field	Value
hostname	ev-charger-1
ip_address	192.0.2.138
mac_address	00:00:5E:00:53:72
manufacturer	Tesla
network_category	IoT
addressing_priority	Reservation Recommended
trust_level	Restricted
exposure_level	Remote Access
notes	EV charging equipment

Table 8

B.9. Connected Vehicle

Field	Value
hostname	vehicle-1
ip_address	192.0.2.143
mac_address	00:00:5E:00:53:73
manufacturer	Tesla
network_category	IoT
addressing_priority	Dynamic Acceptable
trust_level	Restricted
exposure_level	Remote Access
notes	Connected vehicle

Table 9

B.10. Streaming Device

Field	Value
hostname	streaming-device-1
ip_address	192.0.2.145
mac_address	00:00:5E:00:53:74
manufacturer	Apple
network_category	IoT
addressing_priority	Dynamic Acceptable
trust_level	Restricted
exposure_level	Local Shared
notes	Streaming device

Table 10

B.11. Robotic Vacuum

Field	Value
hostname	robotic-cleaner-2
ip_address	192.0.2.150
mac_address	00:00:5E:00:53:75
manufacturer	Roborock
network_category	IoT
addressing_priority	Dynamic Acceptable
trust_level	Restricted

exposure_level	Remote Access
notes	Robotic vacuum

Table 11

B.12. Guest Phone

Field	Value
hostname	guest-phone-1
ip_address	192.0.2.230
mac_address	00:00:5E:00:53:76
manufacturer	Unknown
network_category	Guest
addressing_priority	Dynamic Acceptable
trust_level	Guest
exposure_level	Local Shared
notes	Visitor device

Table 12

B.13. Unknown Device

Field	Value
hostname	unknown-1
ip_address	192.0.2.245
mac_address	00:00:5E:00:53:77
manufacturer	Unknown
network_category	Unknown

addressing_priority	Dynamic Acceptable
trust_level	Unknown
exposure_level	Unknown
notes	Needs review

Table 13

Appendix C. CSV Representation

A comma-separated values representation MAY use the following header. It is shown across multiple lines for readability.

```
hostname,
ip_address,
mac_address,
manufacturer,
network_category,
addressing_priority,
trust_level,
exposure_level,
notes
```

Example records are shown below with one field per line. A CSV implementation would place each record on a single row.

```
   hostname: router-1
   ip_address: 192.0.2.1
   mac_address: 00:00:5E:00:53:01
   manufacturer: Example Router Vendor
   network_category: Management
   addressing_priority: Static Required
   trust_level: Management
   exposure_level: Remote Access
   notes: Primary gateway

   hostname: camera-1
   ip_address: 192.0.2.64
   mac_address: 00:00:5E:00:53:64
   manufacturer: Hikvision
   network_category: Surveillance
   addressing_priority: Reservation Recommended
   trust_level: Restricted
   exposure_level: Internal Only
   notes: IP camera

   hostname: ev-charger-1
   ip_address: 192.0.2.138
   mac_address: 00:00:5E:00:53:72
   manufacturer: Tesla
   network_category: IoT
   addressing_priority: Reservation Recommended
   trust_level: Restricted
   exposure_level: Remote Access
   notes: EV charging equipment
```

Appendix D. JSON Representation

A JSON representation MAY use one object per mapped device.

The following field names are defined:

The following fields are defined, in canonical order.

hostname: String. Human-readable hostname, device hostname, or administrator-assigned label.

ip_address: String. Assigned IPv4 address.

mac_address: String. Link-layer address used for identification or DHCP reservation.

manufacturer: String. Device manufacturer or vendor.

network_category: String. Logical network category or zone.

addressing_priority: String. Addressing stability expectation.

trust_level: String. Expected trust posture.

exposure_level: String. Expected reachability posture.

notes: String. Freeform operational notes.

The network_category field SHOULD use one of the following values:

* Management,
* Main,
* Guest,
* IoT,
* Surveillance, or
* Unknown.

The addressing_priority field SHOULD use one of the following values:

* Static Required,
* Reservation Recommended, or
* Dynamic Acceptable.

The trust_level field SHOULD use one of the following values:

* Management,
* Trusted,
* Restricted,
* Guest, or
* Unknown.

The exposure_level field SHOULD use one of the following values:

* Internal Only,

* Local Shared,

* Remote Access,

* Internet Exposed, or

* Unknown.

Example:

```
{
  "hostname": "camera-1",
  "ip_address": "192.0.2.64",
  "mac_address": "00:00:5E:00:53:64",
  "manufacturer": "Hikvision",
  "network_category": "Surveillance",
  "addressing_priority": "Reservation Recommended",
  "trust_level": "Restricted",
  "exposure_level": "Internal Only",
  "notes": "IP camera"
}
```

Author’s Address

Melisa K. Savich
Email: hello@melisasavich.com