# TRILL over IP

## draft-mrw-trill-over-ip-00.txt

Margaret Wasserman <mrw@painless-security.com>
Donald Eastlake <d3e3e3@gmail.com>
Dacheng Zhang <zhangdacheng@huawei.com>

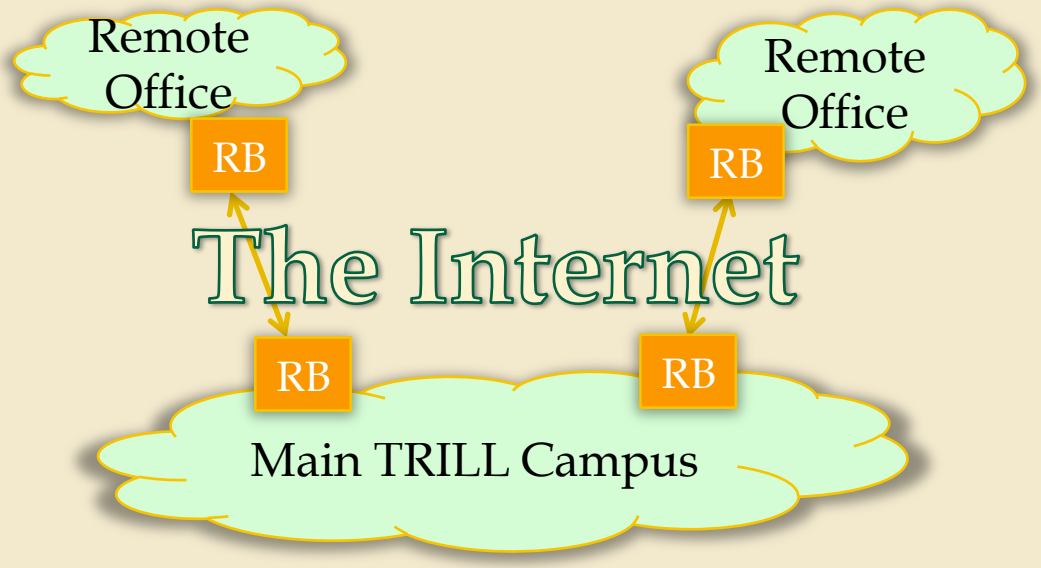
# TRILL over IP Basics

- TRILL Protocol defined in RFCs 6325, 6326 & 6327
- TRILL is already defined to work over different link layer types, both multicast and point-to-point
  - Ethernet (RFC 6325) & PPP (RFC 6361)
- TRILL over IP defines how TRILL can be run over UDP/IP
  - TRILL packets are encapsulated in UDP/IP(v4 or v6), and sent over any IP network
- Very simple encapsulation, does not modify TRILL

# TRILL over IP Scenarios

- Remote Office Scenario
  - Nodes in a remote office are connected to a central TRILL campus over a multi-hop network, possibly the public Internet
- IP Backbone Scenario
  - TRILL links within an enterprise network are connected, as a single TRILL campus, over an IP backbone

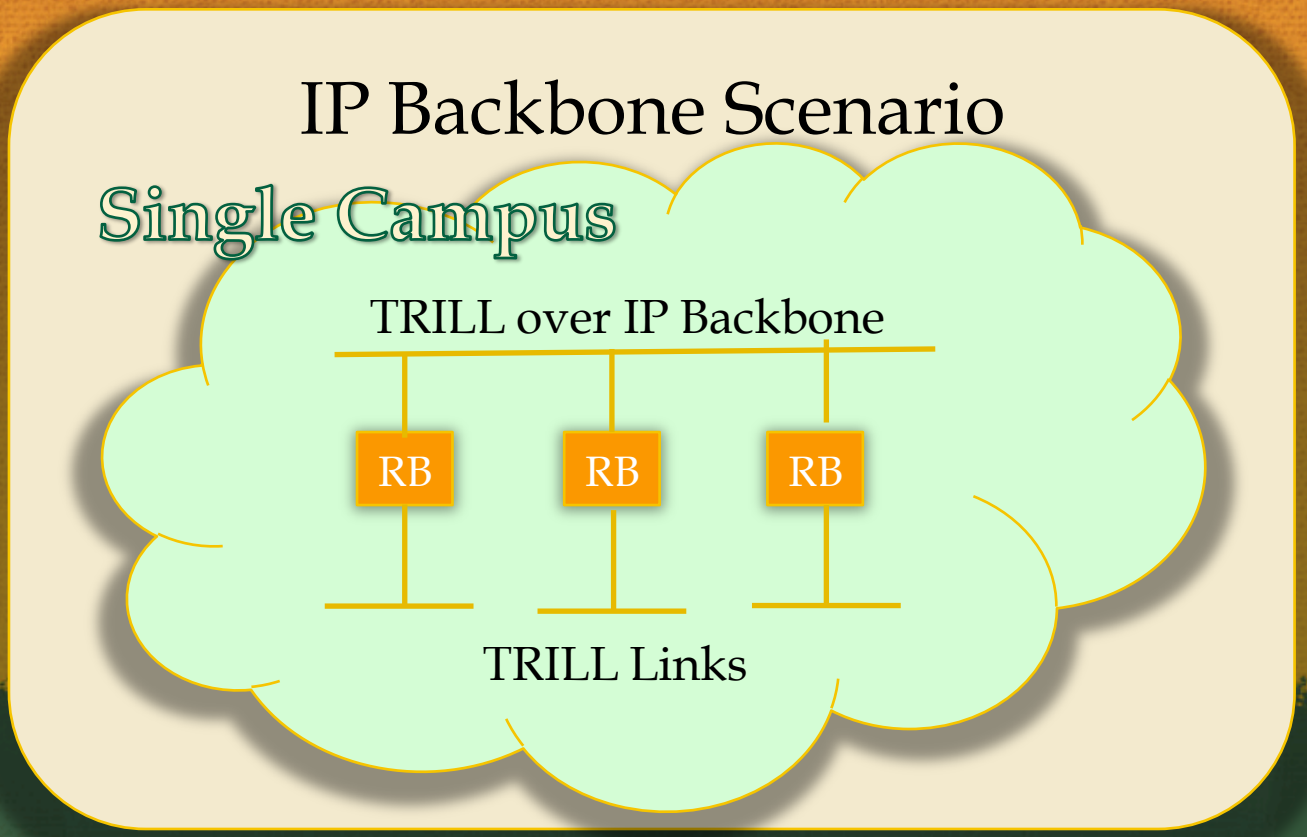
# Remote Office Scenario




Pairs (or small sets?) of RBridges used to connect remote offices to a central TRILL Campus

TRILL over IP links run across multi-hop networks (such as the public Internet). May not be under the same administrative control as the TRILL campus, may not support multicast.

# IP Backbone Scenario




Multiple TRILL links within a single campus, connected using a TRILL over IP backbone

The TRILL over IP link is part of the TRILL campus. Multiple (even many?) RBridges may be on a single TRILL over IP link, and the link will typically support multicast

# Key Differences: Security

- In Remote Office Scenario, TRILL over IP traffic will be tunneled over links that may not be in the same administrative control as the TRILL campus. Authentication and authorization of remote Rbridges, and data privacy are major concerns.
- In IP Backbone Scenario, the IP link runs over links with the same security properties as the TRILL links, so no additional security is needed for parity with L2 switching solutions (TRILL or others)

# Key Differences: Multicast

- In the IP Backbone scenario, the TRILL over IP backbone link will typically support multicast, and multicast support is highly desirable to allow Rbridges to discover adjacencies.
- In Remote Office Scenario, multicast is probably not supported across the TRILL over IP link, and automatic discovery of adjacencies is not desirable (due to security concerns).

# TRILL Frame Formats

- TRILL Data Frame (Generic Format):

| Data Link Header | TRILL Header | Encapsulated Native Frame | Link Trailer |
|---|---|---|---|

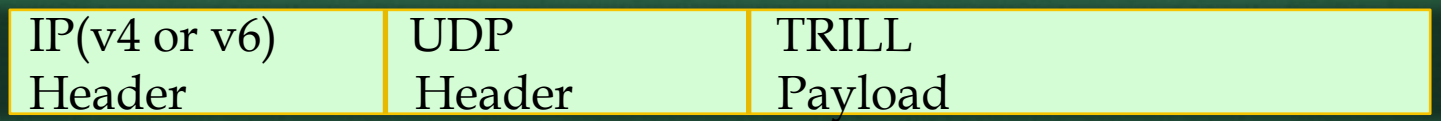
- TRILL IS-IS Frame (Generic Format):

| TRILL IS-IS Link Header | TRILL IS-IS Payload | Link Trailer |
|---|---|---|

- UDP port numbers are allocated for each of the above frame types.
- In TRILL over IP, the link header is UDP/IP and there is no Link Trailer

# TRILL over UDP/IP

- TRILL is encapsulated in UDP/IP (IPv4 or IPv6)
  - IP provides addressing, ability to route packets across a multi-hop IP network
  - UDP provides checksum (when needed) and ports to disambiguate TRILL



# Security

- In cases where authentication, authorization and data privace are required (like the Remote Office Scenario), this is accomplished using DTLS.
- DTLS does not support multicast, so in the secure case, all traffic between TRILL over IP Rbridges is unicast (multicast is serialized, when necessary).
- Note:  Use of DTLS security is not mutually exclusive with the use of IS-IS security.

# Multicast

- There are cases where data privacy is not needed on the TRILL over IP link, and multicast is highly desirable for efficiency (such as the IP Backbone Scenario).
- In this cases, multicast is supported, and IPv4 and IPv6 "All-Rbridges" multicast addresses are allocated.
  - IPv4: 233.252.14.0
  - IPv6: FF0X:0:0:0:0:0:0:205

# Next Steps

- Comments or questions?
- Is the WG interested in adopting this work as a WG work item?
- Document will be updated to address the feedback we've received, so far.  Thank you!