What’s new – Volume 1 Release 1.8

Overview

Specification update overview

- Volume 1, Release 1.8, published July 31, 2024
- The specification defines InfiniBand and RoCE
- Available to IBTA Members

- 2111 pages
- 50 comments submitted and included
- New features added by both the LWG and the MgtWG

What’s new - Volume 1 Release 1.8

IBTA - Management Working Group

Next Generation Speed

- Spec 1.8 supports XDR speed ~200Gb/s per lane.
  - QSFP ➔ 800 Gb/s
  - QSFP-DD and OSFP ➔ 1600 Gb/s

Number of lanes per port	Port Speed Gb/s
1x	200
2x	400
4x	800
8x	1600

XDR Speeds

- New in 1.8 version
  - Add support for XDR FEC
- Miscellaneous
  - Solved issues found in previous release

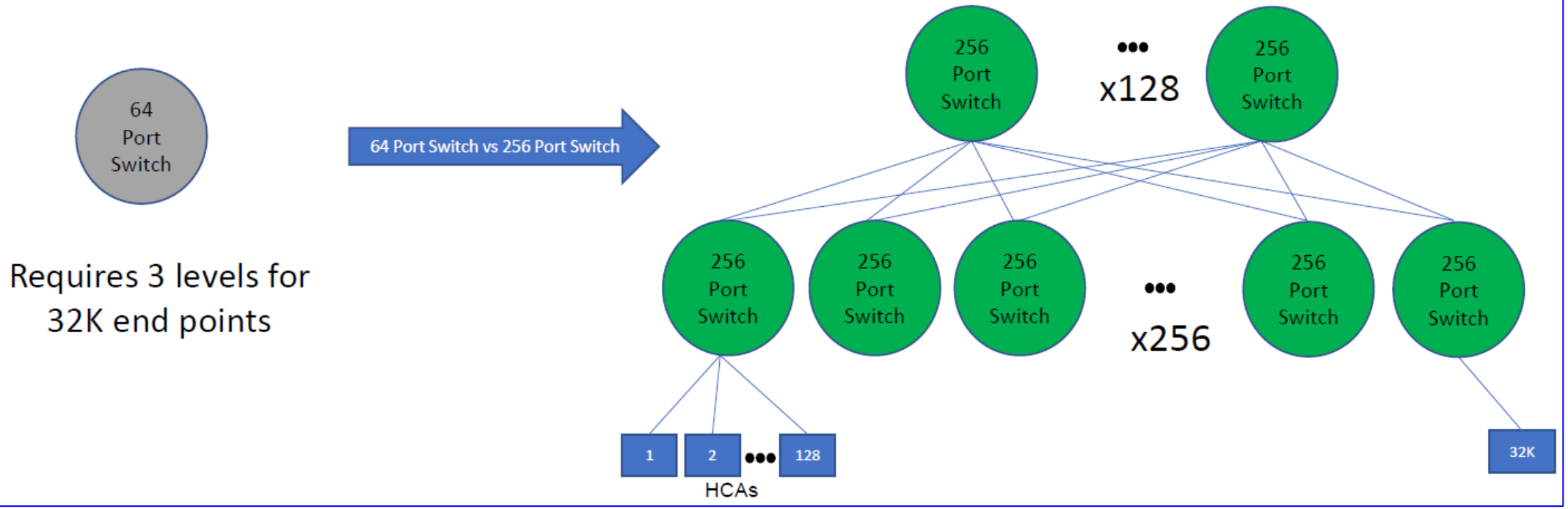
Support For Large Radix Switches

- Added multiple new class version 2 MADs in Subnet Management chapter to support large radix switches (switches with ports up to 64K).

Large Radix Switch - Example

	64 Port Switch	256 Port Switch
Largest scale non blocking 2 level FT	2K HCAs	32K HCA

32K HCAs non blocking topology



Requires 3 levels for 32K end points

What’s new – Volume 1 Release 1.8

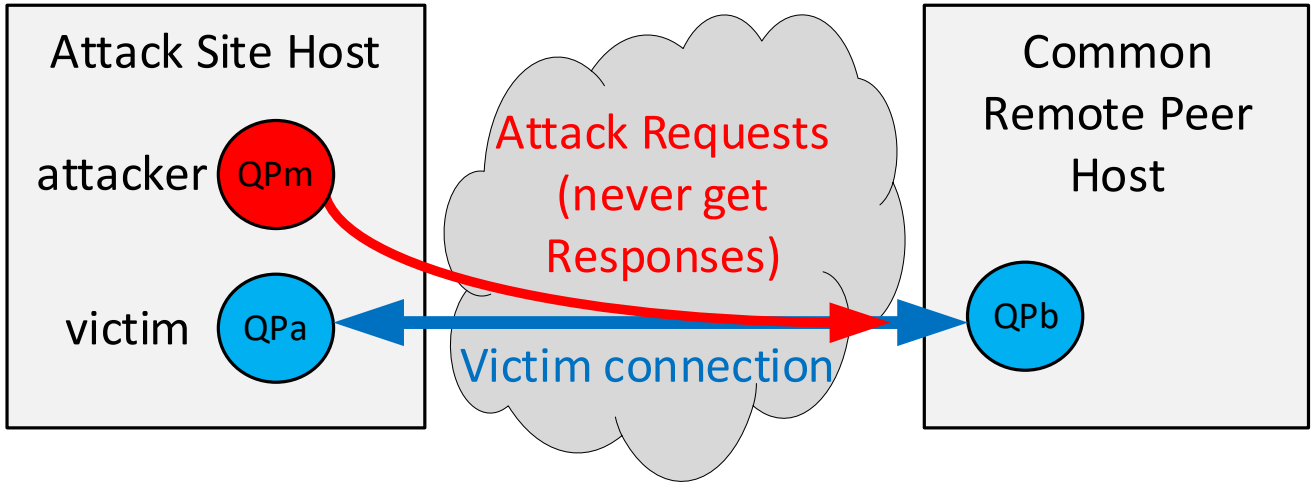
IBTA - Link Working Group

Network Probe Updates

- Network Probes are a generalized mechanism for probing the state of the network for both InfiniBand and RoCE.
- Congestion Control
  - The prime use case is to create an infrastructure to monitor the network and provide accurate congestion control schemes for high performance networking.
- Extended Telemetry
  - Enabling Congestion Control network probes to gather real time telemetry in order to converge the congestion control algorithm.
  - Telemetry format is extendable and can be driven by the network (switch) and the end points (RNIC or HCA).
  - See section A20.2.3.6 RTTPROBE32EXTENDABLE
  - See section A20.2.3.7 RTTPROBE64EXTENDABLE
- Created security architecture for Network Probing
  - Specifying Key Management Scheme for Network Probing
  - See A20.2.1.1 NP_KEY

Modify QP Security Improvements for Connection-Based Transports

- Exposed by paper: "**NeVerMore: Exploiting RDMA Mistakes in NVMe-oF Storage Applications**", by Taranov, Rothenberger, De Sansi, Perrig and Hoefler, 2022 ACM SIGSAC
- **Threat Model**
  - User-Mode attack application, running alongside victim connection-based application(s) on same (virtual) machine can cause damage to an existing victim connection



- **Solution**: Enhance Modify QP API
  - Modify QP Verb to check application has provided a valid DestQP and DLID/DGID combination
  - See change bars in Chapter 11

For more information

https://www.infinibandta.org/ibta-specification/