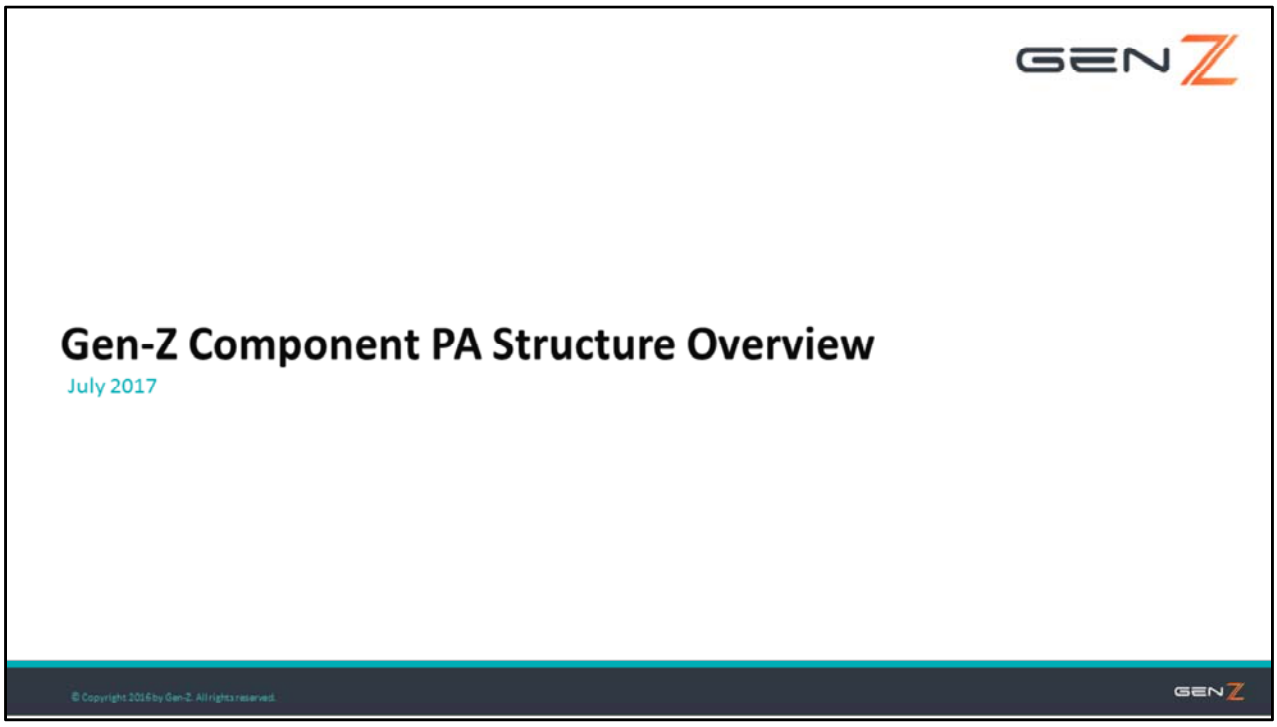


This presentation covers the Component PA (Peer Attribute) Control structure.

Disclaimer

This document is provided 'as is' with no warranties whatsoever, including any warranty of merchantability, noninfringement, fitness for any particular purpose, or any warranty otherwise arising out of any proposal, specification, or sample. Gen-Z Consortium disclaims all liability for infringement of proprietary rights, relating to use of information in this document. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Gen-Z is a trademark or registered trademark of the Gen-Z Consortium.

All other product names are trademarks, registered trademarks, or servicemarks of their respective owners.

All material is subject to change at any time at the discretion of the Gen-Z Consortium

http://genzconsortium.org/

Component PA Structure

- Primary purpose it to configure a peer component or multicast group's attributes
  - These are used to generate and validate request and response packets (unicast or multicast)
  - Only required if a component supports Access Keys, advanced protocol features, or peer component communication authentication
  - Applicable only to components when acting as a Requester or a Responder
- Structure contains a set of pointers to a set of tables
  - SSAP—Single-subnet Attribute Table
  - MSAP—Multi-subnet Attribute Table
  - MCAP—Single-subnet Multicast Attribute Table
  - MSMCAP—Multi-subnet Multicast Attribute Table
  - PA Table—Peer Attribute Table
  - SEC Table—Security Table
  - These tables may be located anywhere in Control Space
  - A component may support a subset of these tables
- Simple components may use the structure's wildcard fields instead of these tables
  - Wildcard fields provide Access Key, peer attributes, and security certificate and TIK pointers used to generate and validate all packets

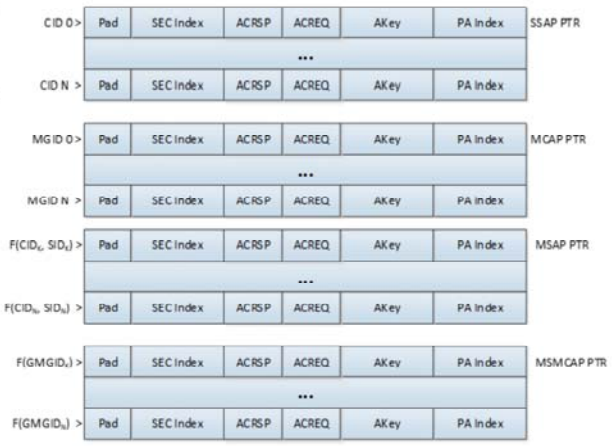
GEN Z

A solution can be composed of a variety of components with varying capabilities. To avoid being reduced to the lowest-common capabilities across all components, the Component PA structure is used to enable communications to be customized per peer component or multicast group. The Component PA structure is not used in point-to-point optimized solutions—P2P-Core, P2P-Coherency, or P2P Vendor-defined.

The structure consists of a set of tables. The SSAP, MSAP, MCAP, and MSMCAP tables contain indices into the PA Table and SEC Table (if supported). This simplifies implementations and reduces resource requirements as multiple peer components can share the same PA Table and SEC Table entries. If all peer components share the same attributes, then a component can use a set of wildcard values in place of these tables.

SSAP, MSAP, MCAP, MSMCAP Table Formats

- Each table consists of a set of indices used to access the PA and Security tables
  - If any table is not supported, then the column is not present in any of the above tables and the other columns are logically shifted to the right
- SSAP is indexed using the destination or source component's CID
- MSAP is indexed by applying a component-specific function to the destination or source component's [CID, SID]
- MCAP is indexed using the multicast group's MGID
- MSMCAP is indexed by applying a component-specific function to the multicast group's [MGID, Global Multicast Prefix]

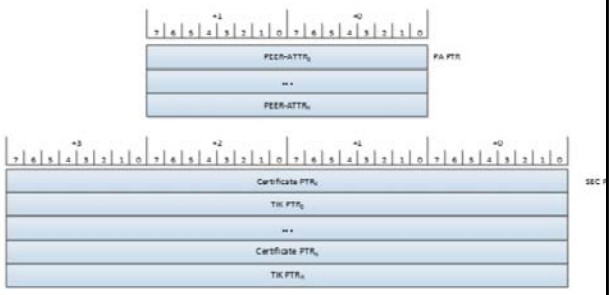


As previously discussed, each of these table contains a set of indices into PA Table and the SEC Table. Each table entry also contains an Access Key field, a Requester Access Control field, and a Responder Access Control field. All three of these fields are small, so it is simpler and more efficient to include these directly into each table entry.

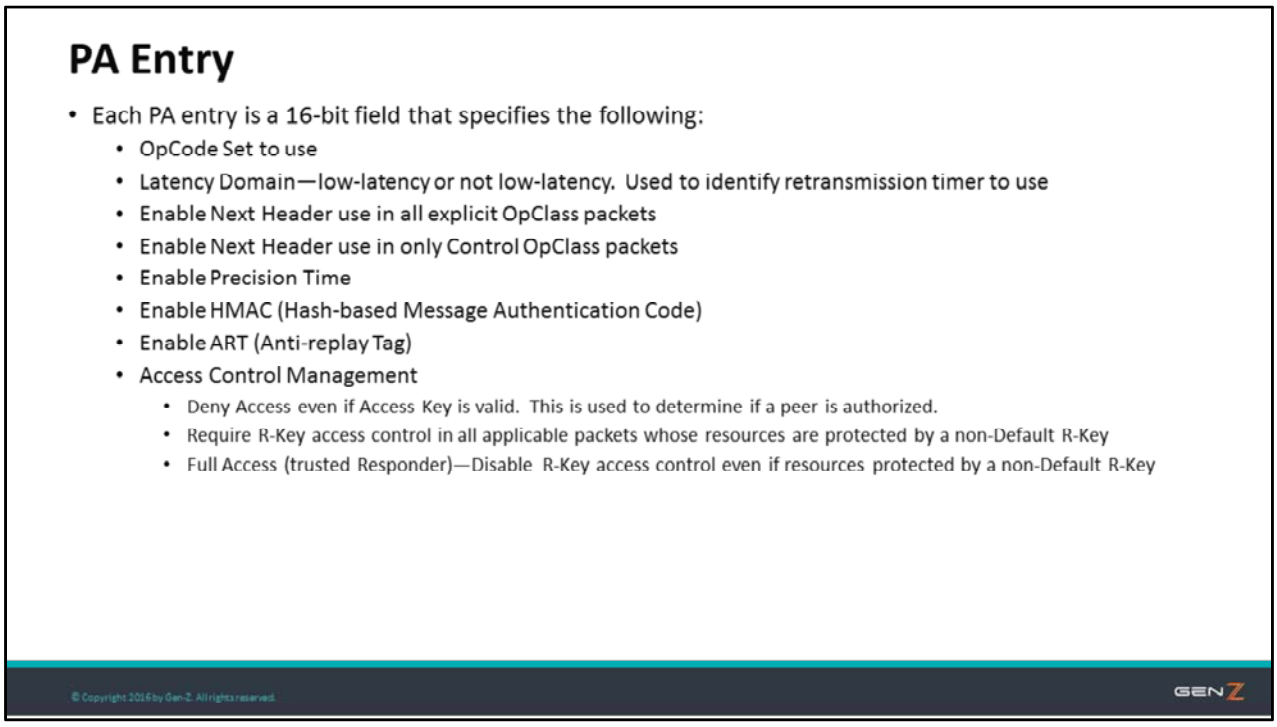
The single-subnet unicast and multicast tables are directly indexed using a CID (unicast) or a MGID (multicast). The multi-subnet unicast and multicast tables are indexed by apply a component-specific function based on the [CID, SID] or GMGID. The component-specific function is identified by a UUID; this enables software to understand how to configure the table. If the function is shared (published UUID) as a de facto method, then multiple components can be configured using the same software.

PA and Security Tables

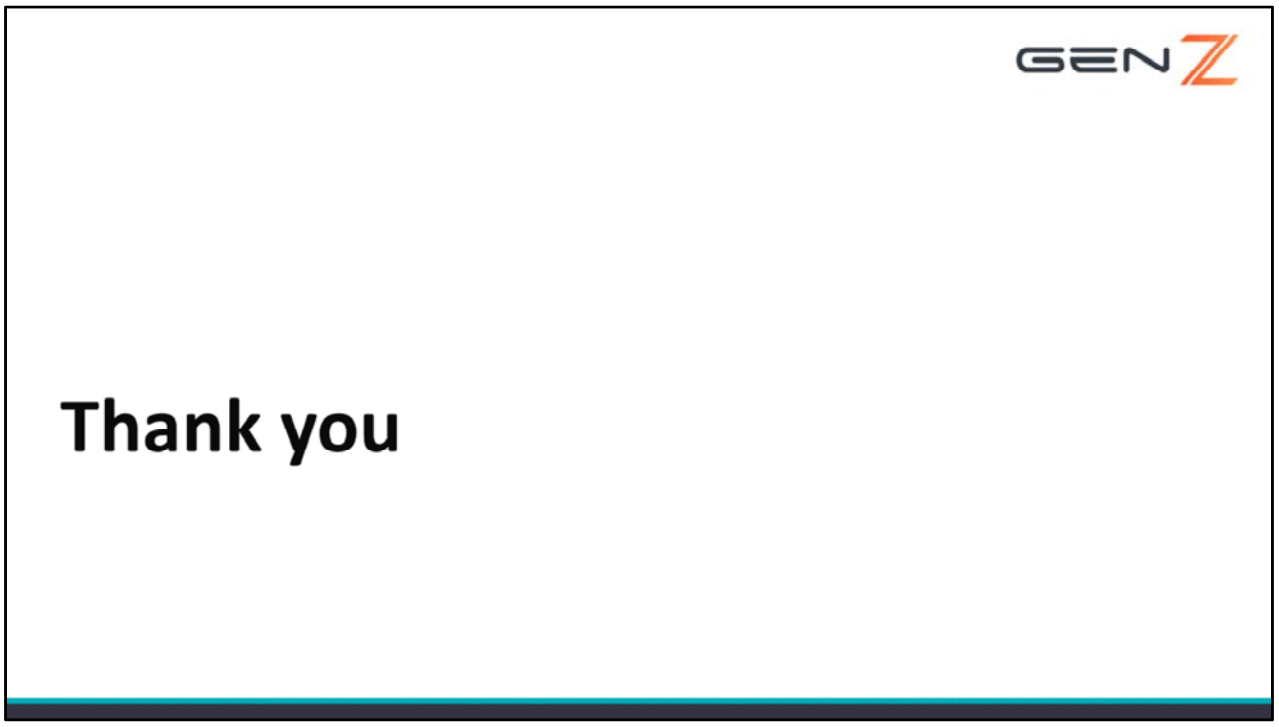
- Multiple SSAP / MSAP / MCAP / MSMCAP entries may point to the same PA or Security entries
- PA describes the peer's attributes used to generate and validate packets
- SEC Table contains pointers to the Certificate and TIK to used to generate and validate authenticated packets
  - SEC Table requires the component to support the Component Security Table



The PA Table contains a set of 16-bit fields that describe how to communicate with any peer that is associated with a given entry. Similarly, the SEC Table points to security certificates and Transaction Integrity Keys (TIK) that are configured within the Component Security Table (see Component Security structure). This table is optional and applicable to only components that support the Component Security structure.



Each PA table entry contains a set of bit fields that describe how to communicate with peer components. For example, if a component supports multiple OpCode Set structures, then the operations used to communicate with a given peer can differ from those used with a different peer. The rest of the bits are self explanatory, and are primarily associated with how specific bits set to indicate if optional fields are present in a given packet.



This concludes this presentation. Thank you.