ZigBee™ Alliance

Wireless Control That Simply Works

ZigBee Security Specification Overview

Agenda

- ZigBee Security Overview
- Residential Applications
  - Guidelines
  - Typical configurations
- Commercial Applications
  - Guidelines
  - Typical configurations

ZigBee™ Alliance

Describes Key setup and maintenance
(Commercial, Residential)

Defines Key Types
(Master, Link, Network)

CCM*
(Unified/Simpler mode of operation)

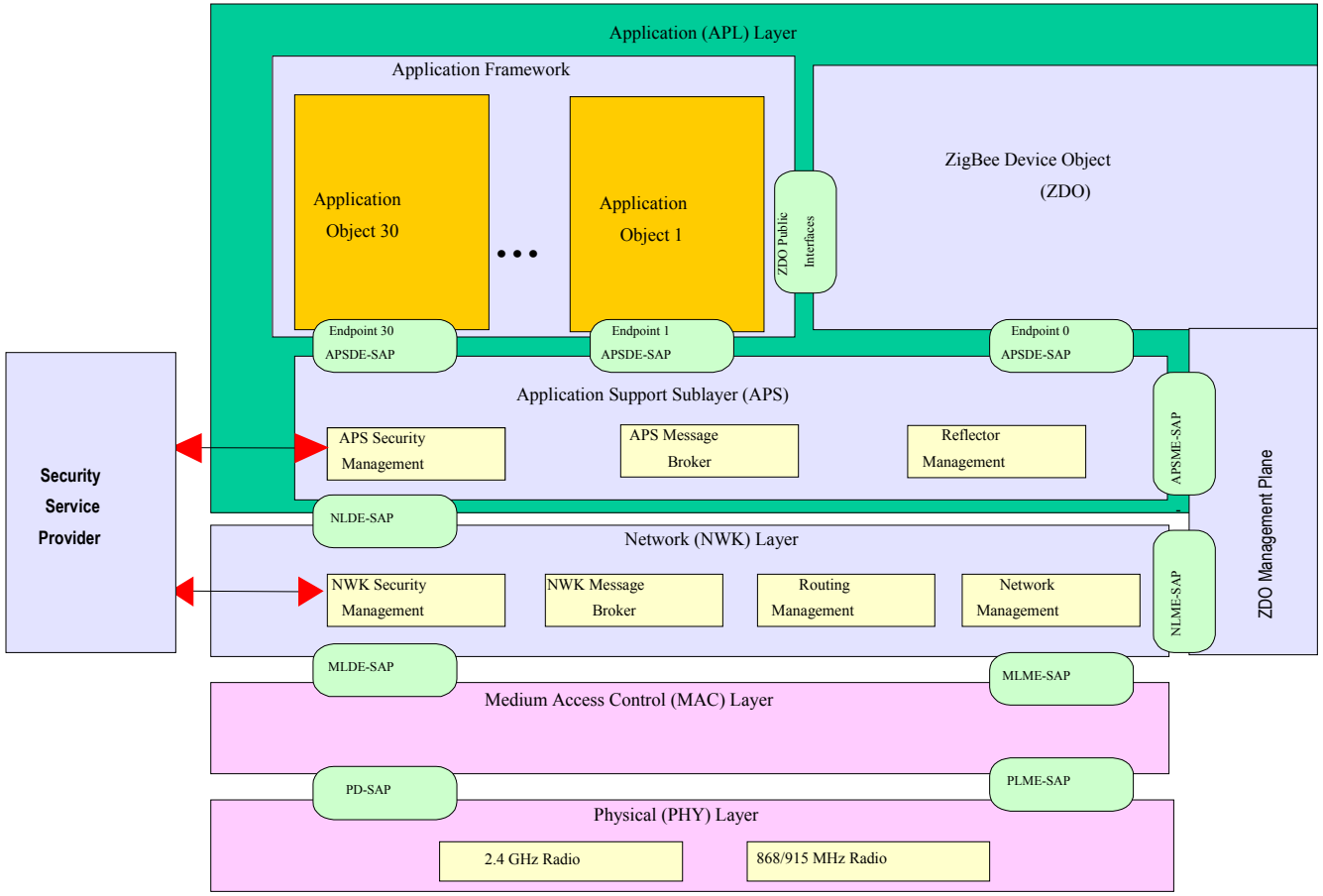
ZigBee Security

Uses 128-bit AES algorithm
Strong, NIST approved security

802.15.4 Security
AES encryption
CCM security modes

ZigBee uses the basic security elements in 802.15.4

ZigBee Security Architecture



Defines security for the MAC, NWK, and APS layers

ZigBee Provides Freshness

- Freshness check prevents replay attacks (an attacker from replaying messages)
- ZigBee devices maintain incoming and outgoing freshness counters
  - Counter is reset when a new key is created
  - Devices that communicate once per second will not overflow their freshness counters for 136 years

ZigBee Provides Message Integrity

- Prevents an attacker from modifying the message in transit
- Option of 0, 32, 64, or 128 bit integrity
  - Default is 64
- Integrity options allow tradeoff between message protection and message overhead

ZigBee™ Alliance

ZigBee provides Authentication

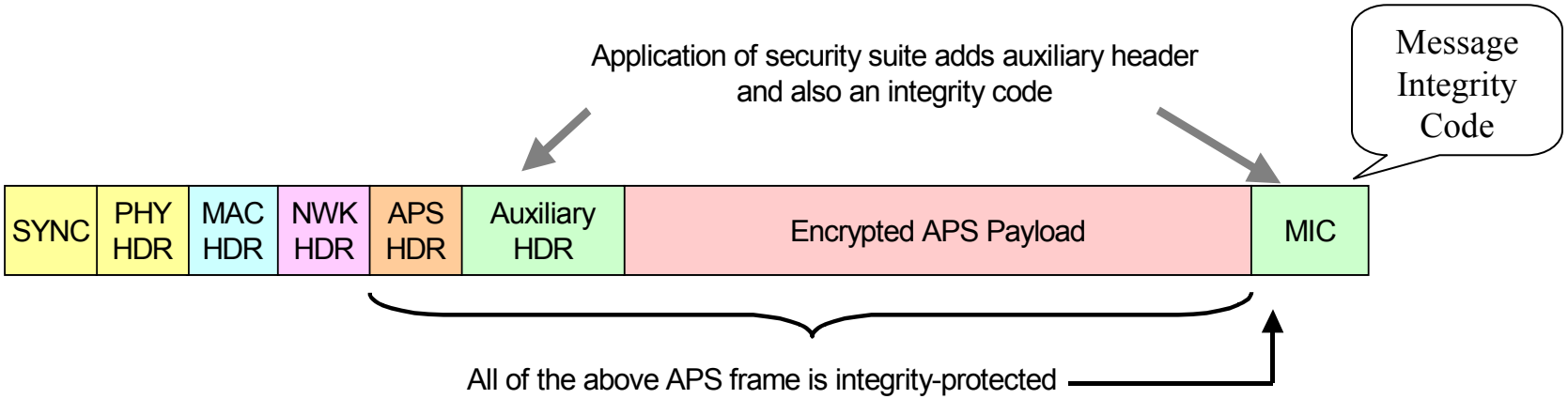
- Authentication provides assurance about the originator of the message
  - Prevents an attacker from modifying a hacked device to impersonate another device
- Authentication is possible at network level or device level
  - Network level authentication is achieved by using a common network key
    - This prevents outsider attacks while adding very little in memory cost
  - Device level authentication is achieved by using unique link keys between pairs of devices
    - This prevents insider and outsider attacks but has higher memory cost

ZigBee™ Alliance

ZigBee Provides Encryption

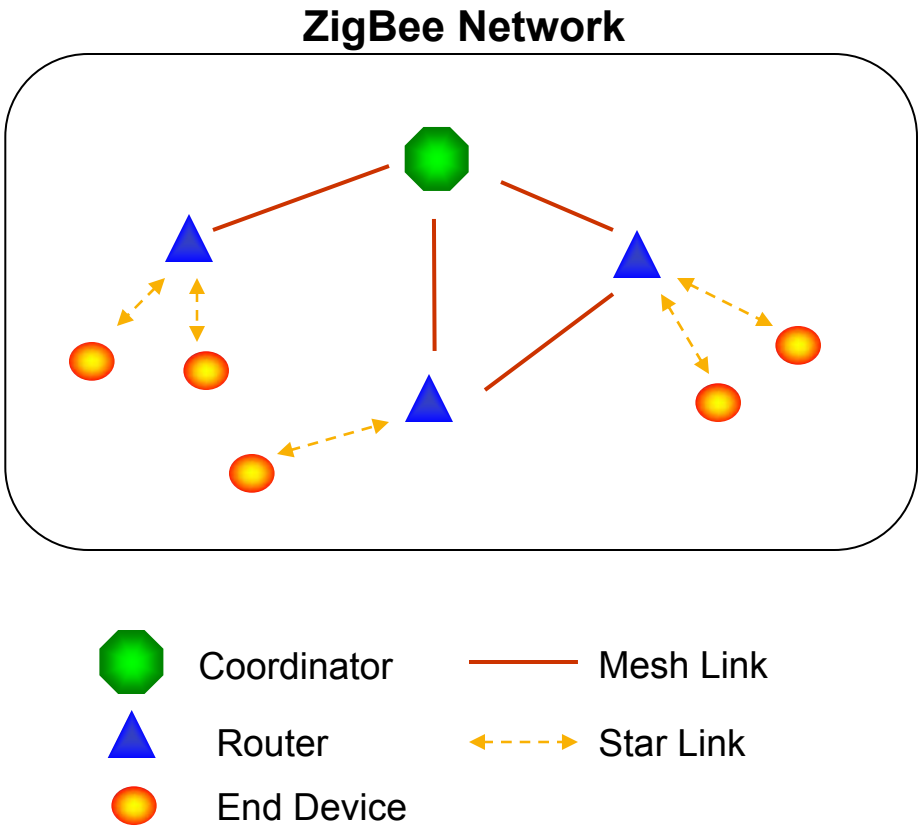
- Prevents an eavesdropper from listening to messages
  - ZigBee uses 128-bit AES encryption
- Encryption protection is possible at network level or device level
  - Network level encryption is achieved by using a common network key
    - This prevents outsider attacks while adding very little in memory cost
  - Device level encryption is achieved by using unique link keys between pairs of devices
    - This prevents insider and outsider attacks but has higher memory cost
- Encryption can be turned off without impacting freshness, integrity, or authentication
  - Some applications may not need encryption protection
  - Could help to ease export control regulation issues

ZigBee frames with Security



ZigBee Security could add headers to the data frames at the MAC, NWK, and APS layers

ZigBee introduces the concept of a Trust Center



- The trust center allows devices into the network and distributes keys
- The ZigBee coordinator is assumed to be the trust center
- It is possible for the trust center to be a dedicated device
  - e.g. a portable device

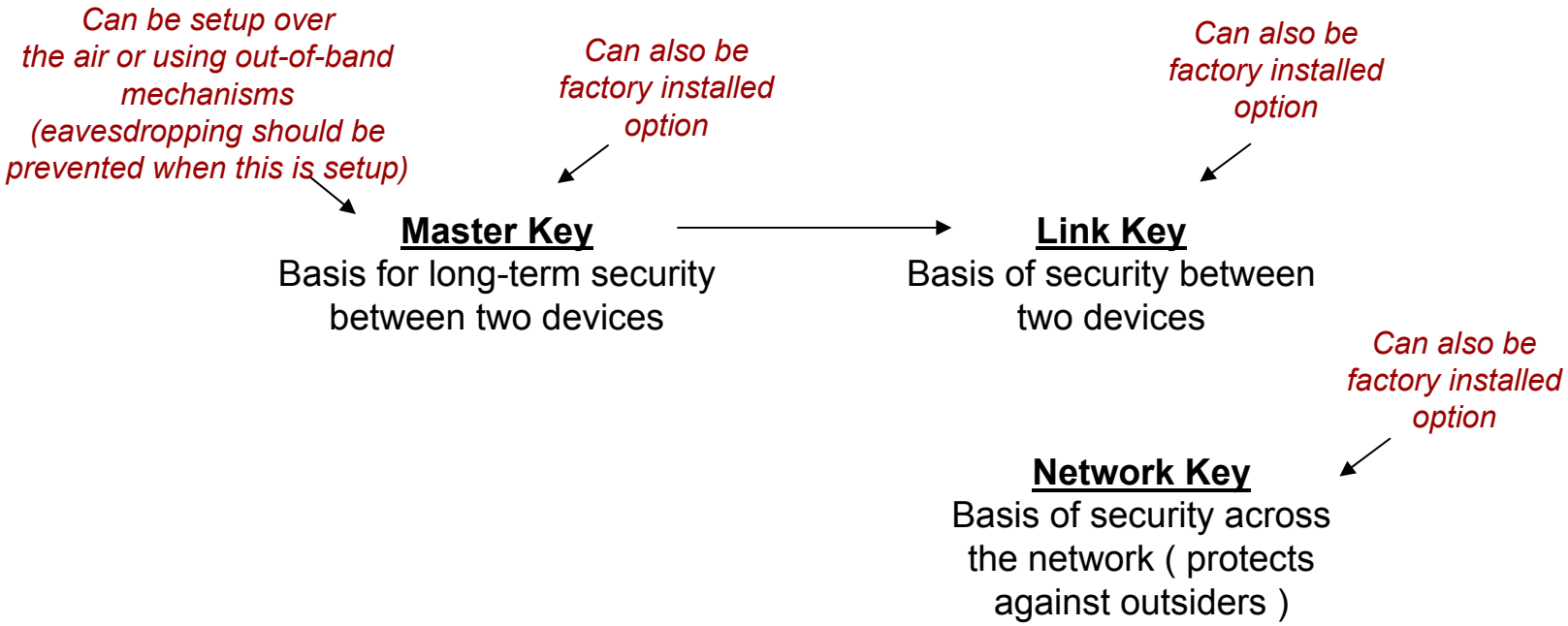
Trust Center roles

- Trust Manager
  - Authenticate device that request to join network
- Network Manager
  - Maintains and distributes network keys
- Configuration Manager
  - Enabling end-to-end security between devices

Trust Center modes

- Residential Mode
  - The trust center allows devices to join the network, but does not establish keys with network devices
  - The trust center cannot update keys periodically because it does not maintain keys with network devices
  - The memory cost in the trust center is minimal and does not scale with the size of the network
- Commercial Mode
  - The trust center establishes and maintains keys and freshness counters with every device in the network
  - This allows centralized control and update of keys
  - Cost memory in the trust center could scale with the size of the network

ZigBee uses three fundamental key types



Link and Network keys can be updated periodically

Setup of Link and Network keys

Master keys are installed first:

A) Installed in factory or out of band

B) Sent from Trust Center

Master Key
Basis for long-term security between two devices

→

Link Key
Basis of security between two devices

Network Key
Basis of security across the network

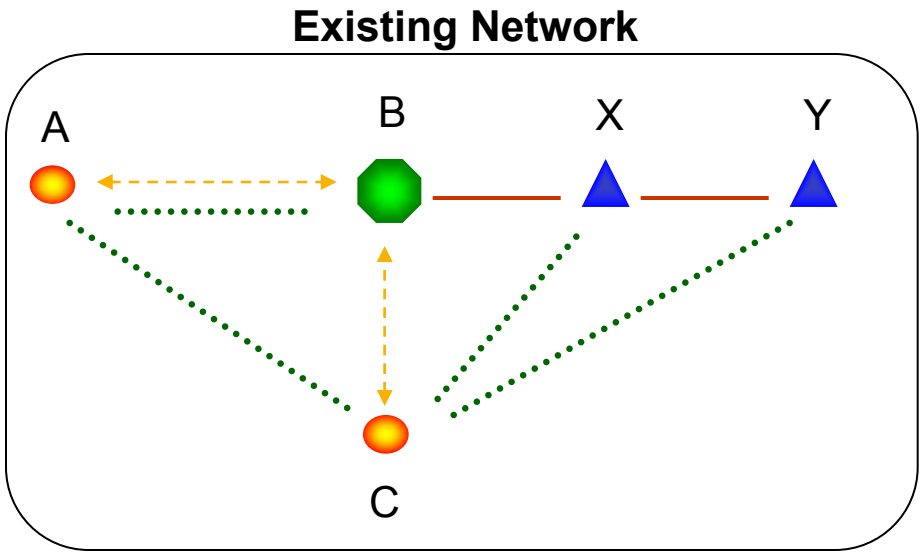
Options for installation of Link and Network Keys:

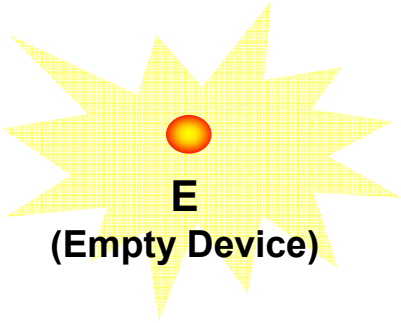
A) Installed in factory or out of band

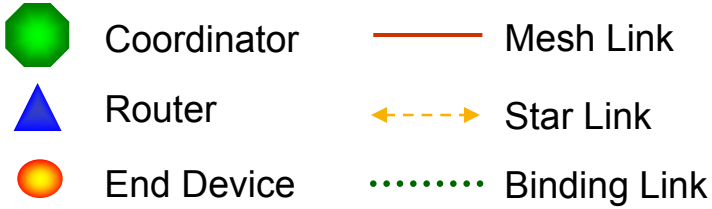
B) SKKE handshake between devices (Link keys)

C) Key transport from trust center (Link and Network keys)

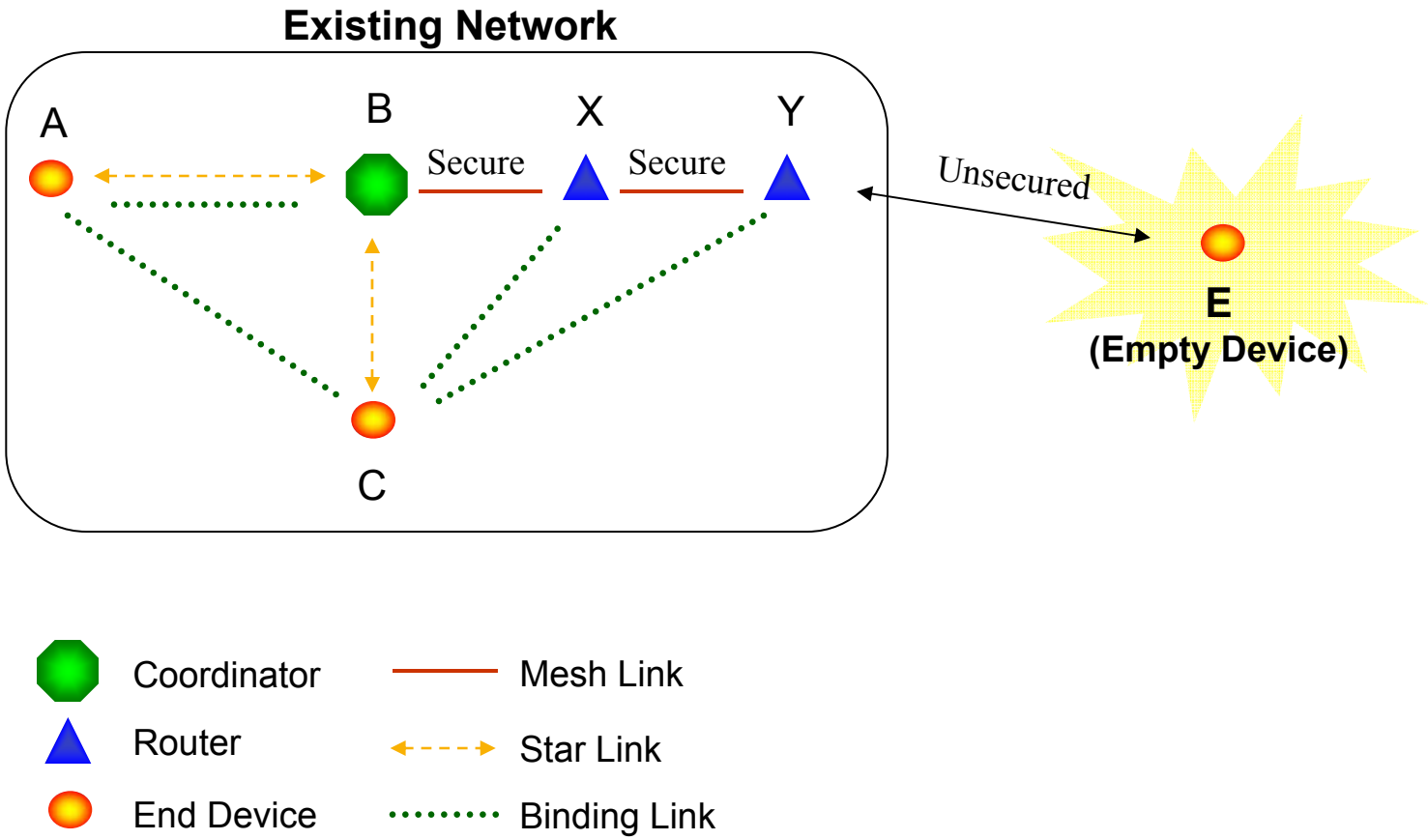
Keys need to be setup with and between new devices that join the network



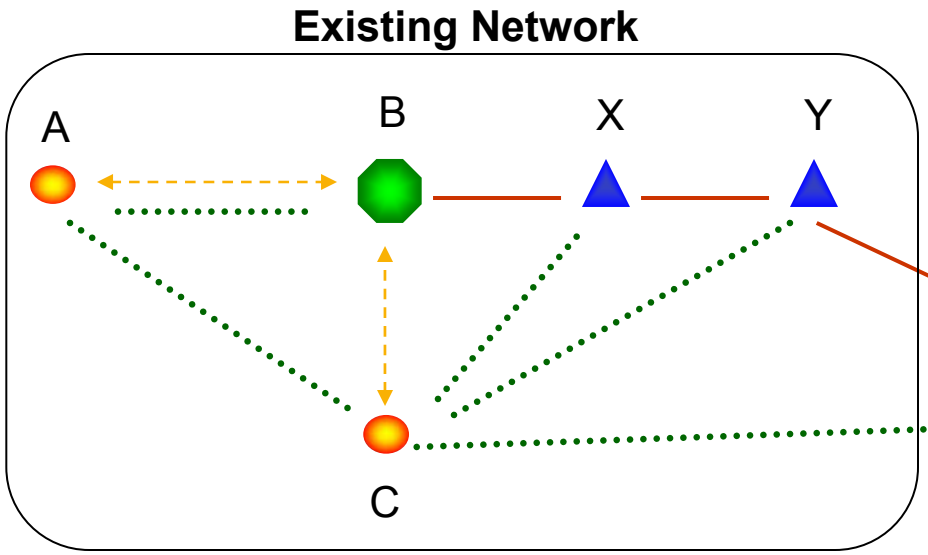


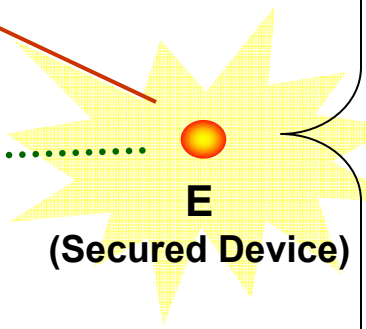


If keys are setup over-the-air only the last link is vulnerable to a one time eavesdropper attack



After a devices joins it needs to store multiple keys





Possible security material

MAC Security:
MK_{YE} = Master Key
LK_{YE} = Link Key

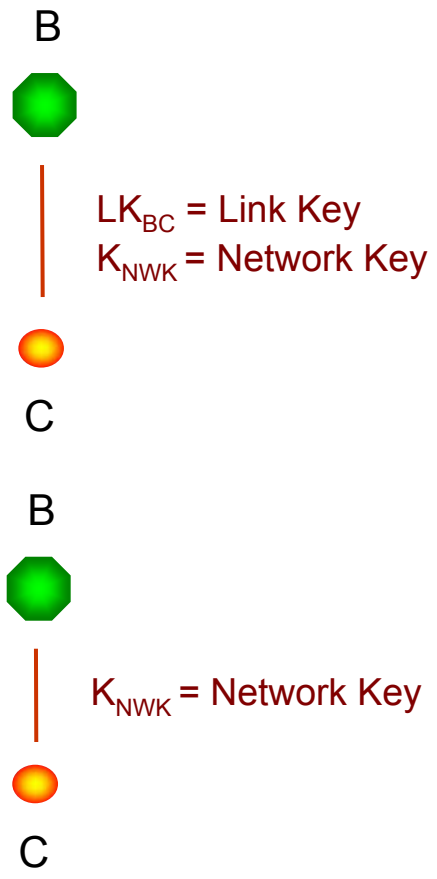
Trust Center Security:
MK_{BE} = Master Key
LK_{BE} = Link Key

Infrastructure Security:
K_{NWK} = Network Key

Application Security:
MK_{CE} = Master Key
LK_{CE} = Link Key

Coordinator — Mesh Link
Router — Star Link
End Device — Binding Link

ZigBee allows options to reduce storage cost, but the highest possible security is always used



If two devices have a link key, it is always used instead of the network key

Storage cost can be reduced by using the network key. However, this reduces security since the network key is used in many devices and cannot prevent insider attacks.

Policy decisions not defined in ZigBee Specification

- Out of band methods for key setup
- Cost/Security tradeoff for number of link keys needed
  - Choosing Commercial/Residential modes is starting point for this decision
- Handling security error conditions
- Handling loss of counter synchronization
- Handling loss of key synchronization
- Policy for expiration and update of keys
- Policy for accepting new devices

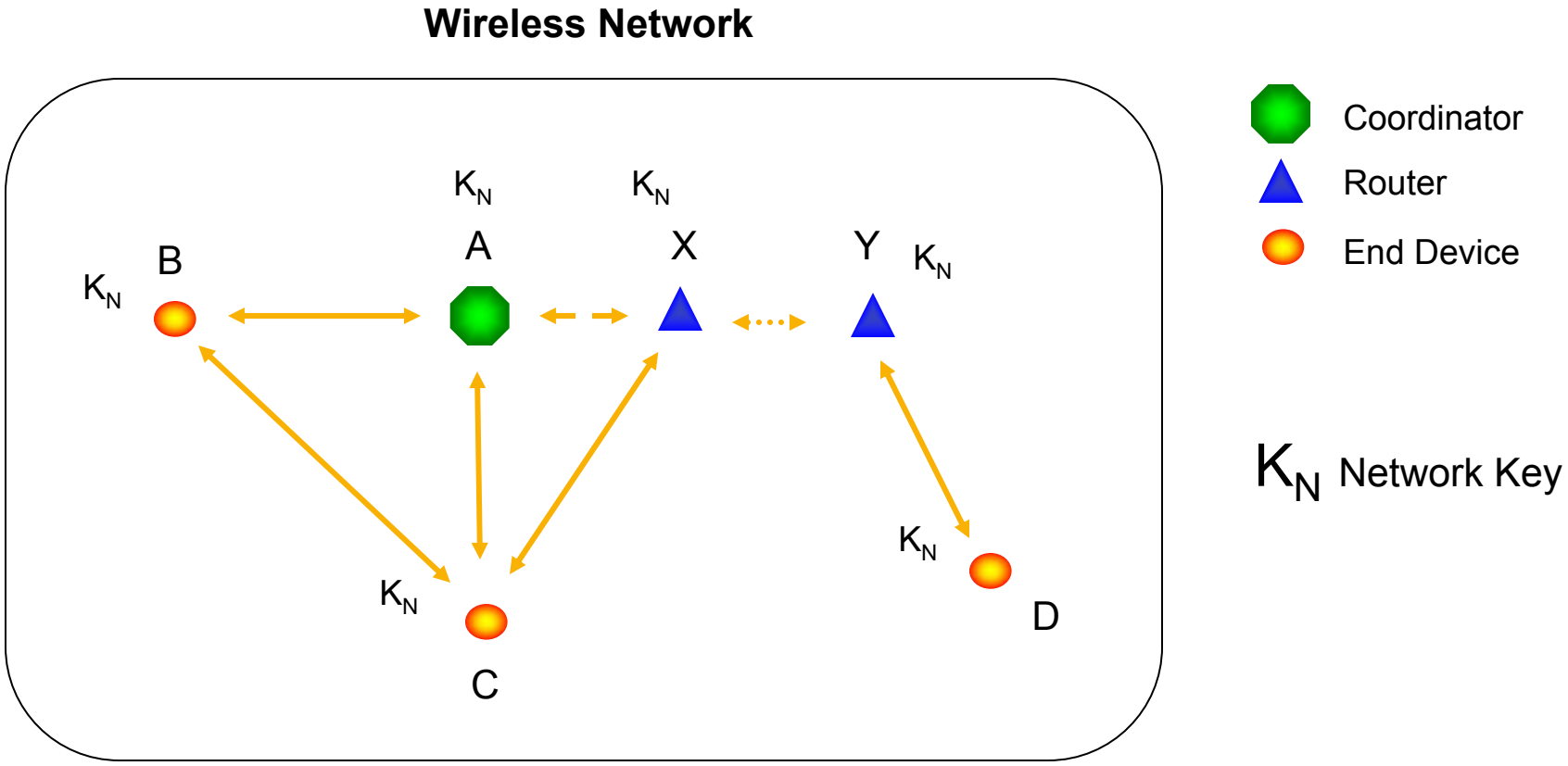
Agenda

- ZigBee Security Overview
- Residential Applications
  - Guidelines
  - Typical configurations
- Commercial Applications
  - Guidelines
  - Typical configurations

Definition of Residential Application (from a security viewpoint)

- A secure wireless network that can be installed and maintained by a homeowner with no knowledge of security
  - Security is transparent during setup
  - Must still provide best security possible
- The homeowners takes no active role in maintaining security of network
  - Homeowner may discard devices without revocation of keys

Residential Keys



A minimum number of keys/storage is used for low cost

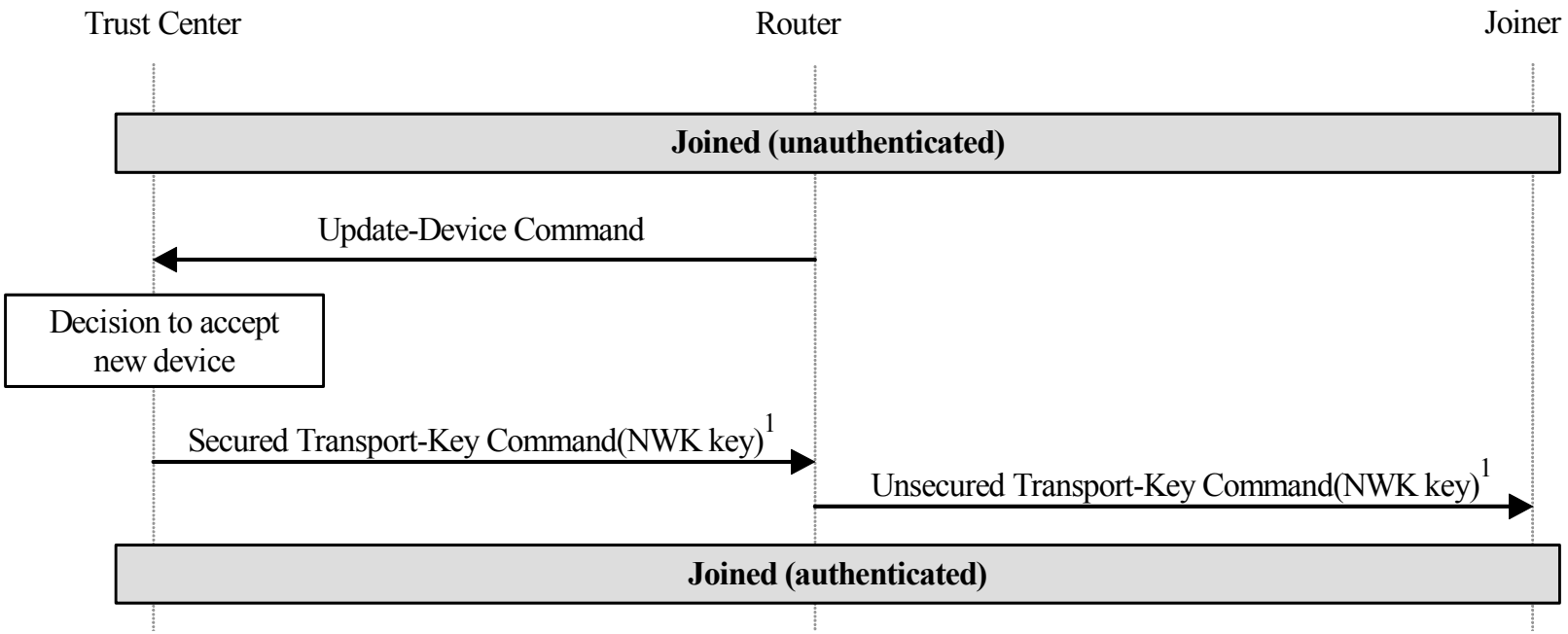
Residential Trust Center is Low Cost

- Residential Trust Center only needs to store network key
  - Minimizes storage
  - Low capability device can act as trust center
  - Trust center can be easily replaced with another device without homeowner intervention
    - When another Coordinator takes over, it becomes the trust center

Key and Frame Counter Storage Requirements for Residential Devices

- All Devices require network key and frame counters
  - One outgoing network frame counter
  - Incoming network frame counters
    - FFD: one per child
    - RFD: one for parent
- Provides only network level authentication, integrity and encryption protection
  - Vulnerable to insider attacks

Example of Residential-Mode Authentication



Note:

1. The trust center sends a dummy all-zero NWK key if the joiner securely joined using a preconfigured network key.

Agenda

- ZigBee Security Overview
- Residential Applications
  - Guidelines
  - Typical configurations
- Commercial Applications
  - Guidelines
  - Typical configurations

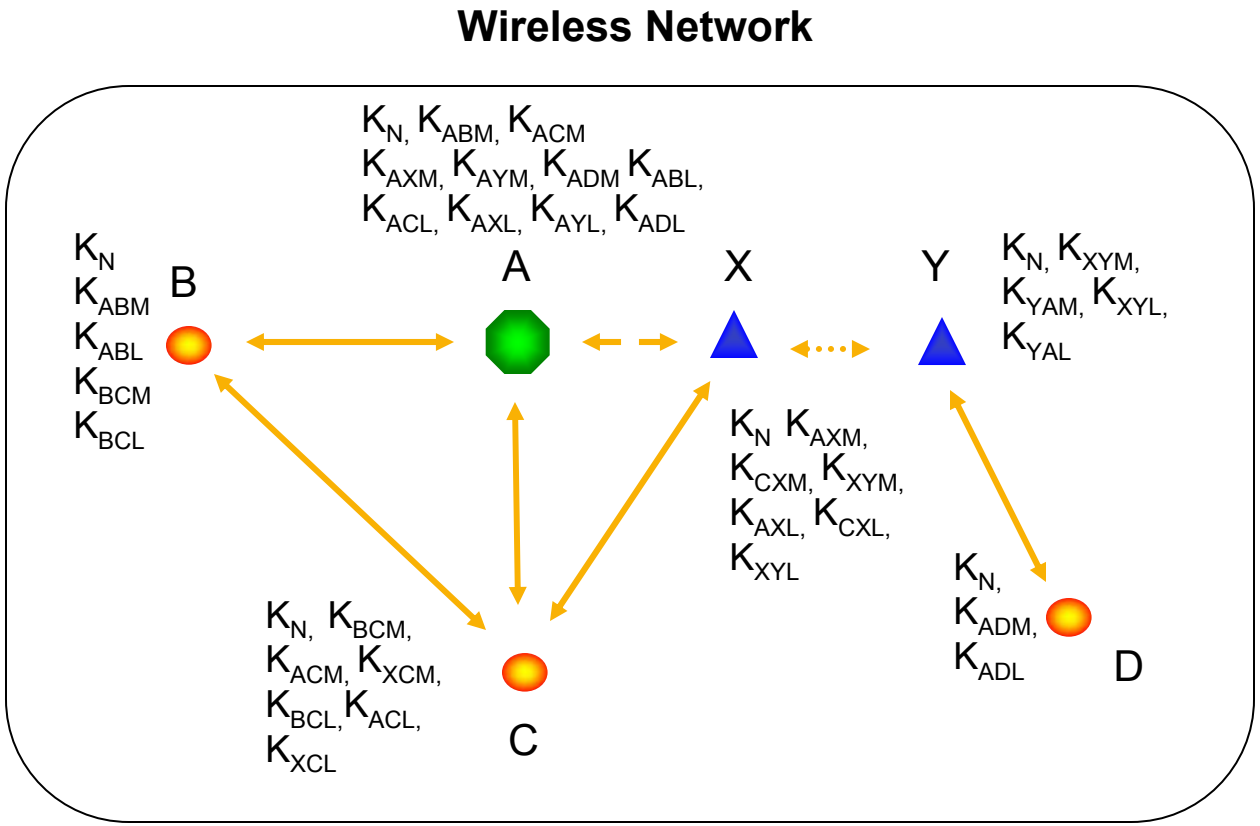
Definition of Commercial Application (from a security viewpoint)

- A wireless network which is controlling mission critical applications
  - Commercial lighting, HVAC, Alarm
  - Production monitoring and control
  - Critical residential applications might use commercial security
- A wireless network which is actively monitored and maintained
  - Scheduled key updates
  - Controlled addition of new devices
  - Revocation of discarded devices

Commercial System Guidelines

- Trust Center should only admit new devices when manually enabled
  - Prevents unauthorized devices from joining
- Trust Center should update network key for legitimate devices periodically
  - Encrypt with link key (not network key)
  - Compromised devices will not get updated key
- Network key should only be used by the network layer
  - Prevents attacker from using network key to control devices

Commercial Keys



Coordinator

Router

End Device

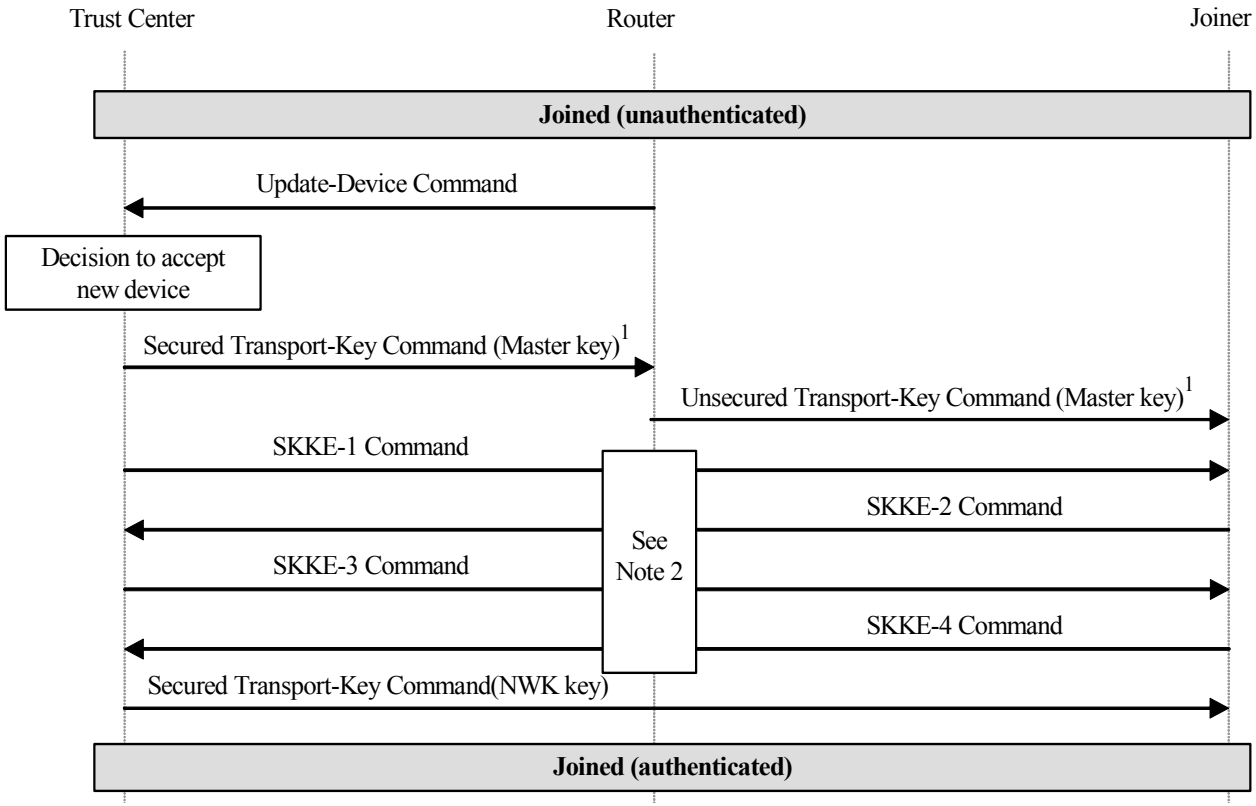
K_N Network Key

K_{ABM} Master Key

K_{ABL} Link Key

Keys with trust center allow periodic update of network keys

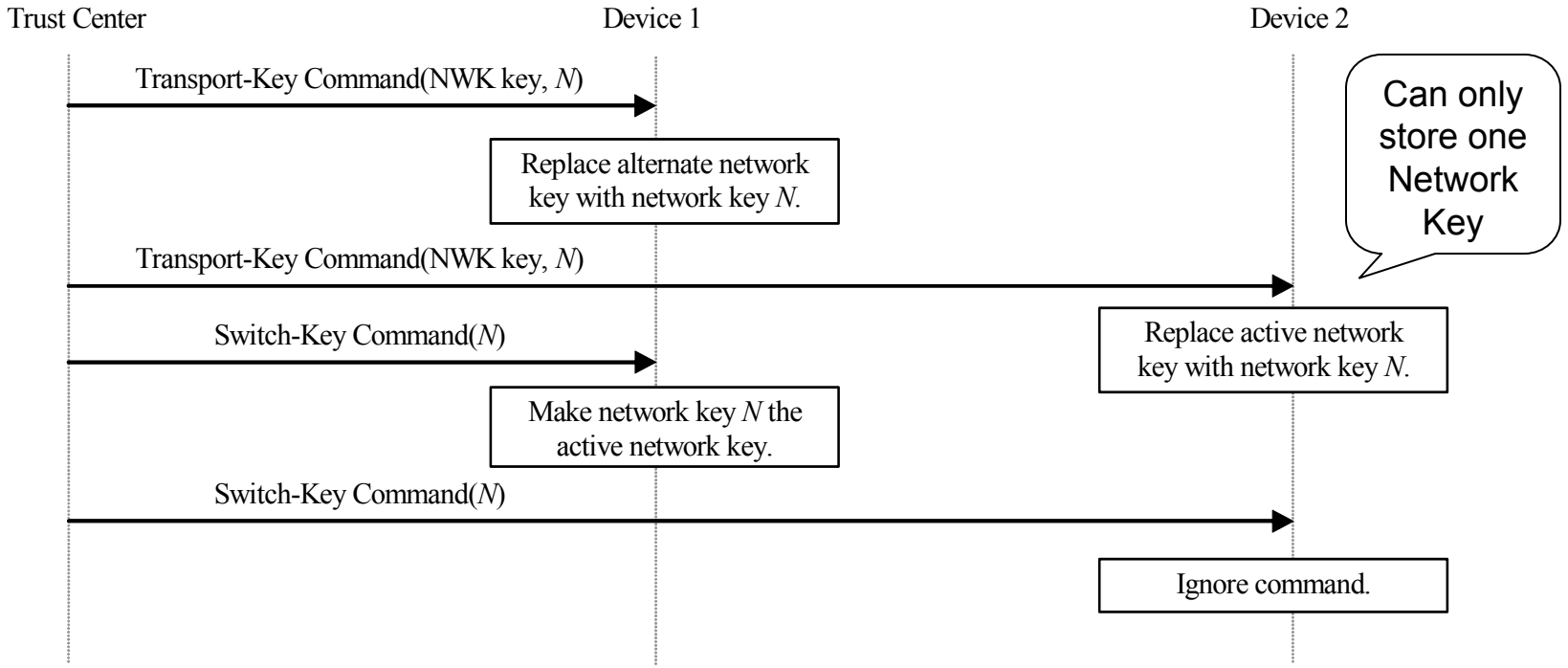
Example commercial-mode authentication procedure



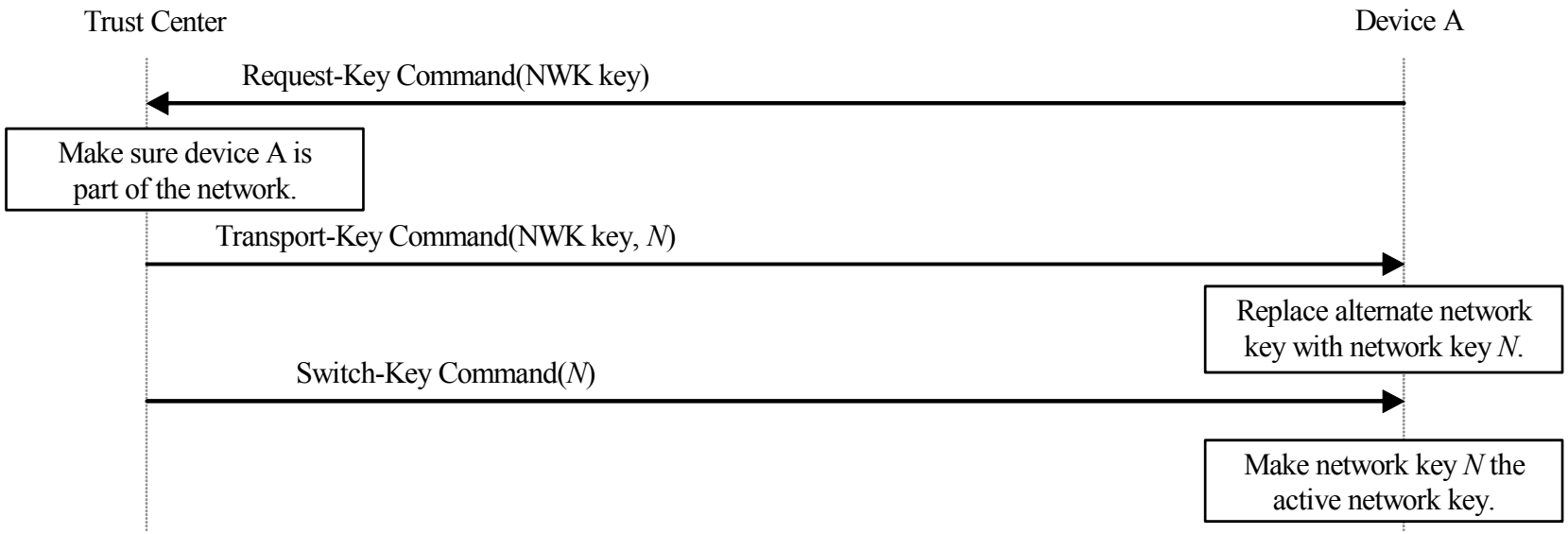
Notes:

1. The trust center does not send a master key if it already shares one with the joiner device (i.e., the pre-configured situation)
2. SKKE commands shall be sent using the router as a liaison when the *nwkSecureAllFrame* NIB attribute is TRUE (i.e., these commands will be secured between the trust center and router at the NWK layer, but not between the router and joiner).

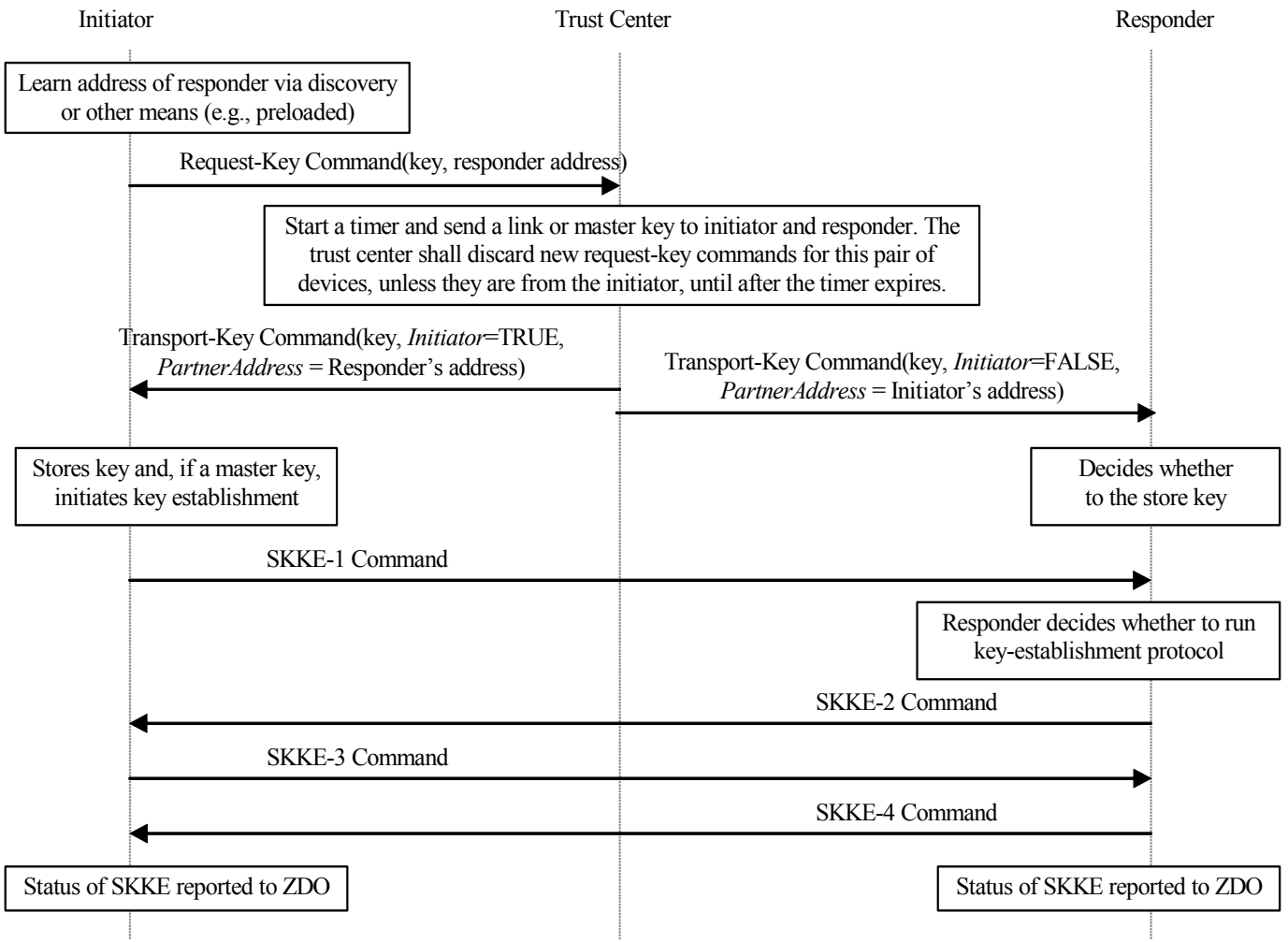
Example of Network Key-Update



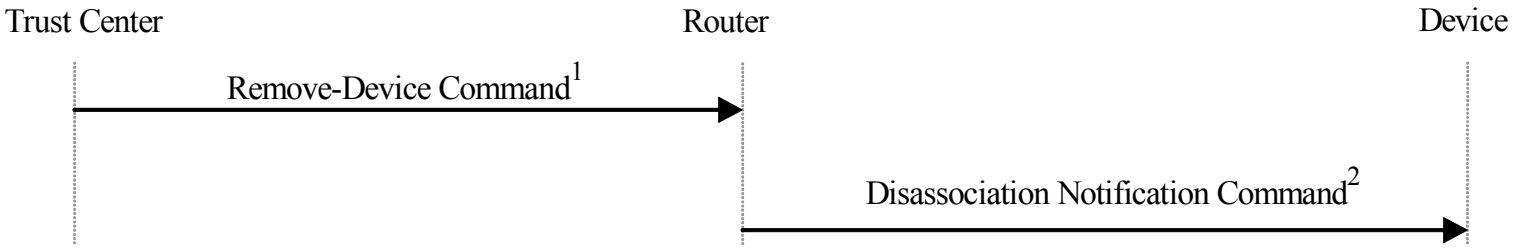
Example Network Key-Recovery



Example End-to-End Application key establishment



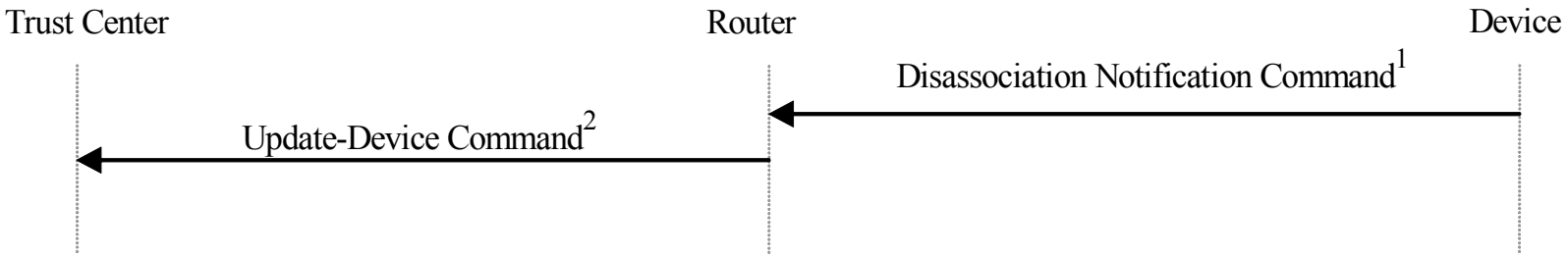
Example Remove-Device Procedure



Note:

1. If a trust center wants a device to leave and if the trust center is not the router for that device, the trust center shall send the router a remove-device command with the address of the device it wishes to leave the network.
2. A router shall send a disassociation command to cause one of its children to leave the network.

Example Device-Leave procedure



Note:

1. A device leaving the network shall send a disassociation command to its router.
2. Upon receipt of a valid disassociation command, a router shall send an update-device command to the trust center to inform it that a device has left the network.