UNIK4250 Security in Distributed Systems
University of Oslo
Spring 2012

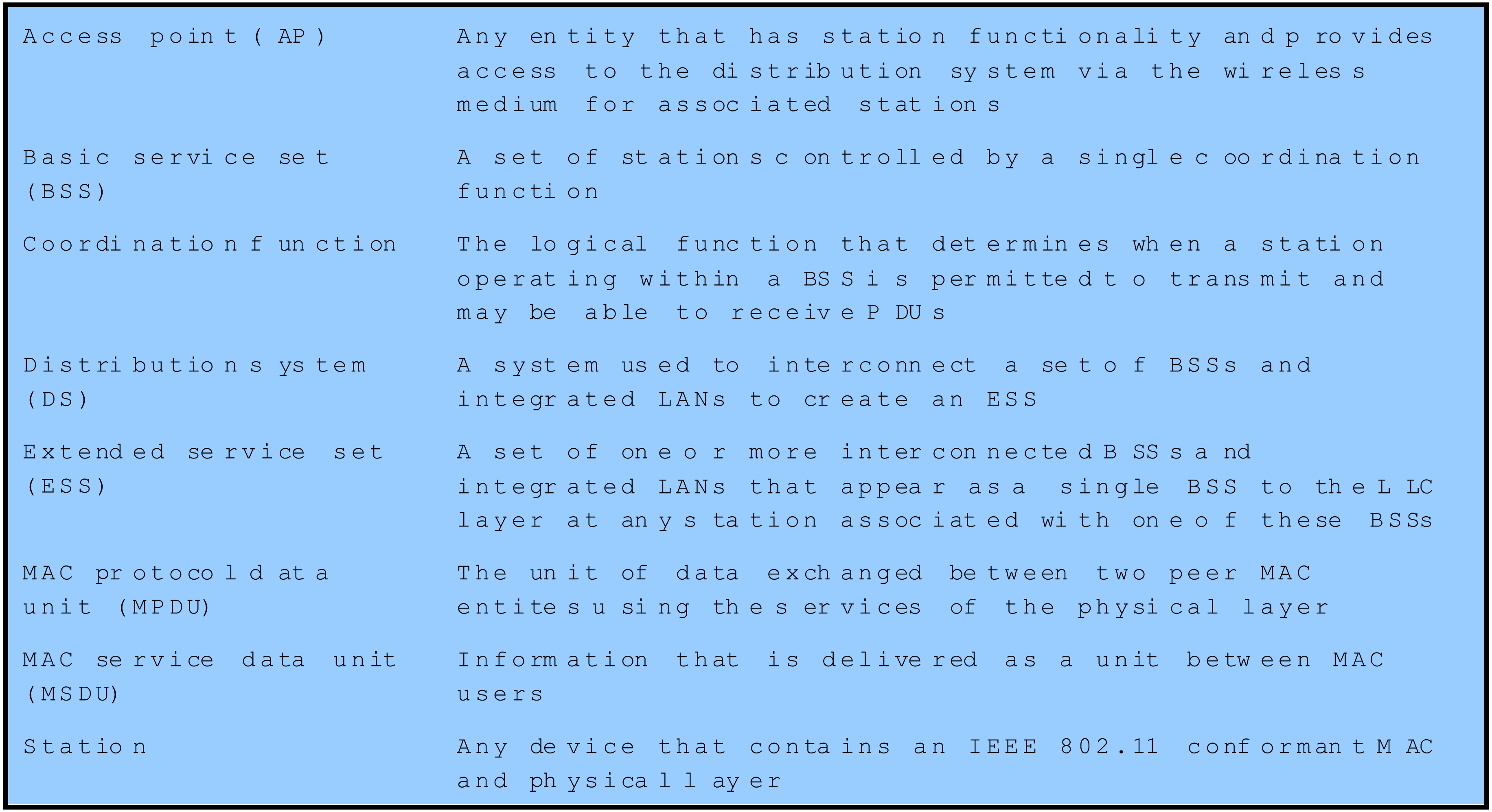
Part 7

Wireless Network Security

IEEE 802.11

- IEEE 802 committee for LAN standards
- IEEE 802.11 formed in 1990’s
  - charter to develop a protocol & transmission specifications for wireless LANs (WLANs)
- since then demand for WLANs, at different frequencies and data rates, has exploded
- hence seen ever-expanding list of standards issued

IEEE 802 Terminology

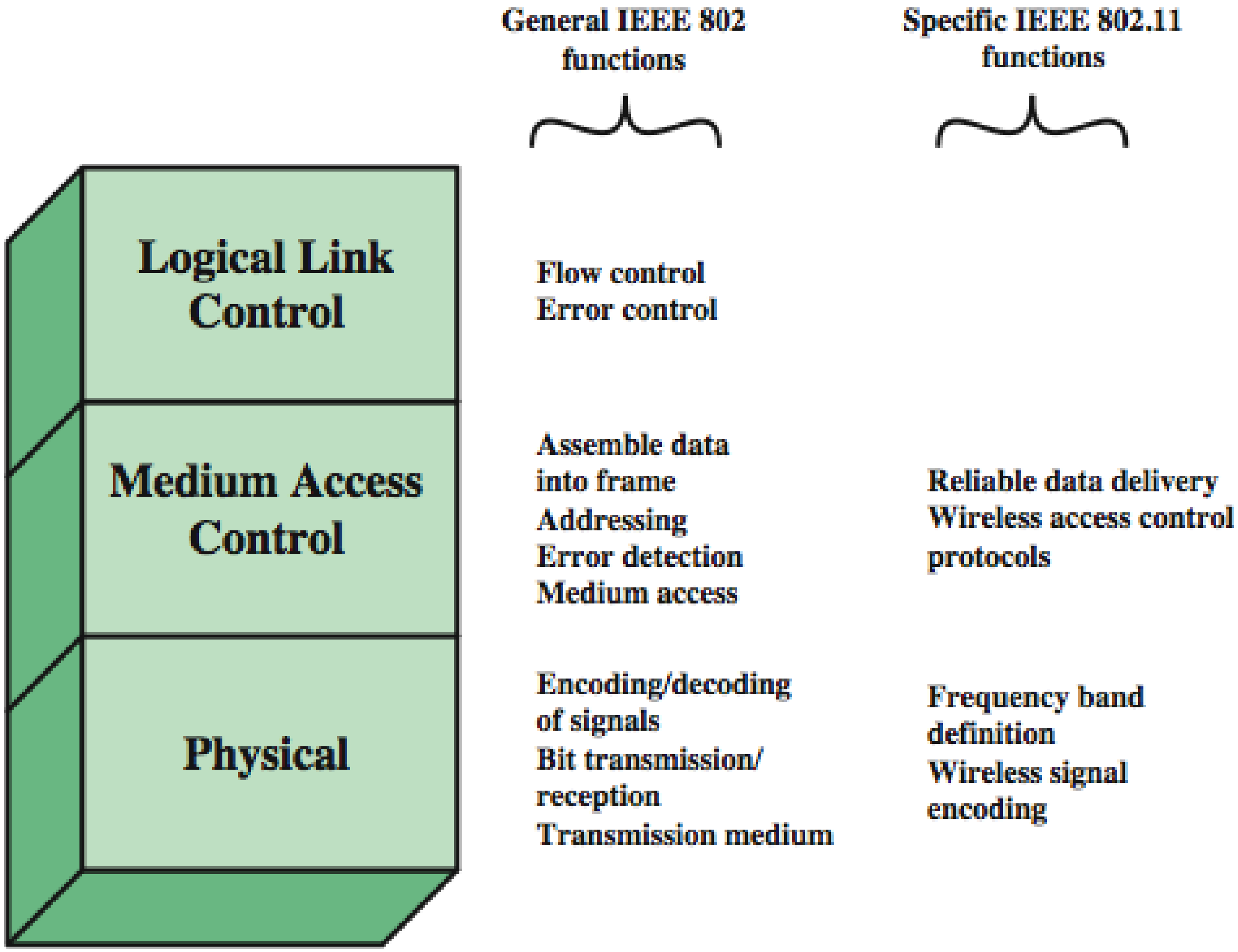


Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations
Basic service set (BSS)	A set of stations controlled by a single coordination function
Coordination function	The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs
Distribution system (DS)	A system used to interconnect a set of BSSs and integrated LANs to create an ESS
Extended service set (ESS)	A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer MAC entites using the services of the physical layer
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer

Wi-Fi Alliance

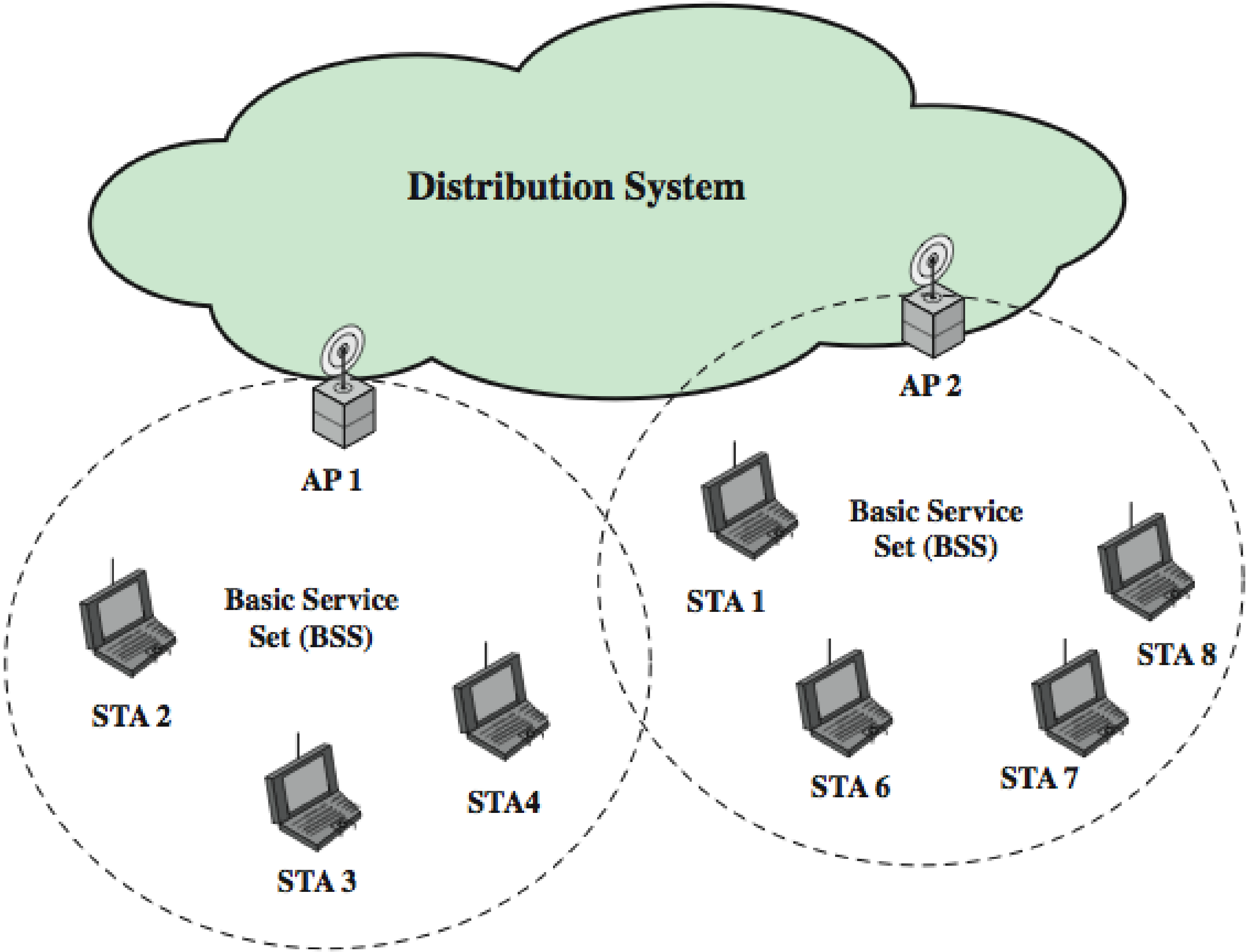
- 802.11b first broadly accepted standard
- Wireless Ethernet Compatibility Alliance (WECA) industry consortium formed 1999
  - to assist interoperability of products
  - renamed Wi-Fi (Wireless Fidelity) Alliance
  - created a test suite to certify interoperability
  - initially for 802.11b, later extended to 802.11g
  - concerned with a range of WLANs markets, including enterprise, home, and hot spots

IEEE 802 Protocol Architecture

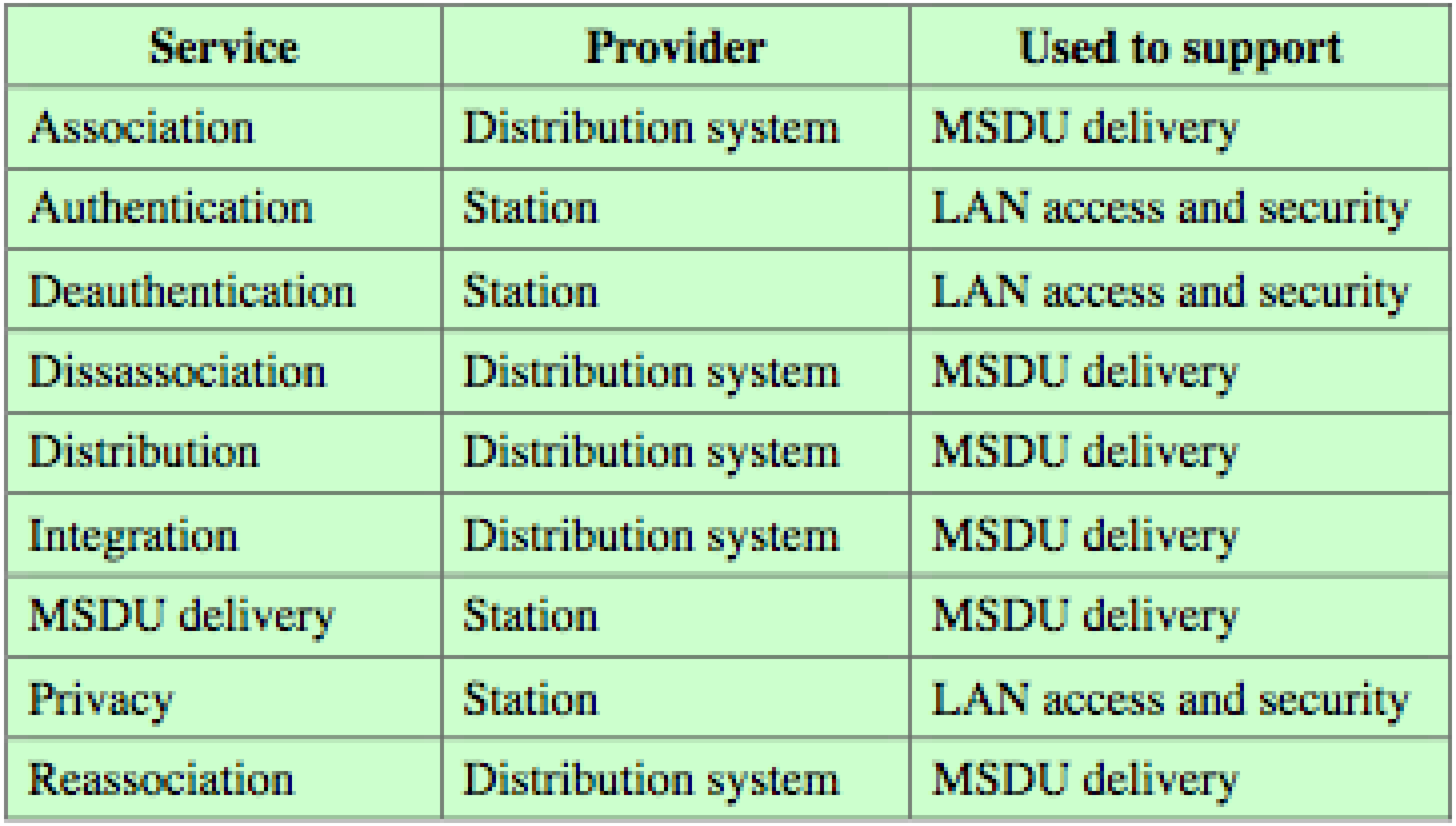


	General IEEE 802 functions	Specific IEEE 802.11 functions
Logical Link Control	Flow control Error control	
Medium Access Control	Assemble data into frame Addressing Error detection Medium access	Reliable data delivery Wireless access control protocols
Physical	Encoding/decoding of signals Bit transmission/ reception Transmission medium	Frequency band definition Wireless signal encoding

Network Components & Architecture



IEEE 802.11 Services



Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Dissassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassociation	Distribution system	MSDU delivery

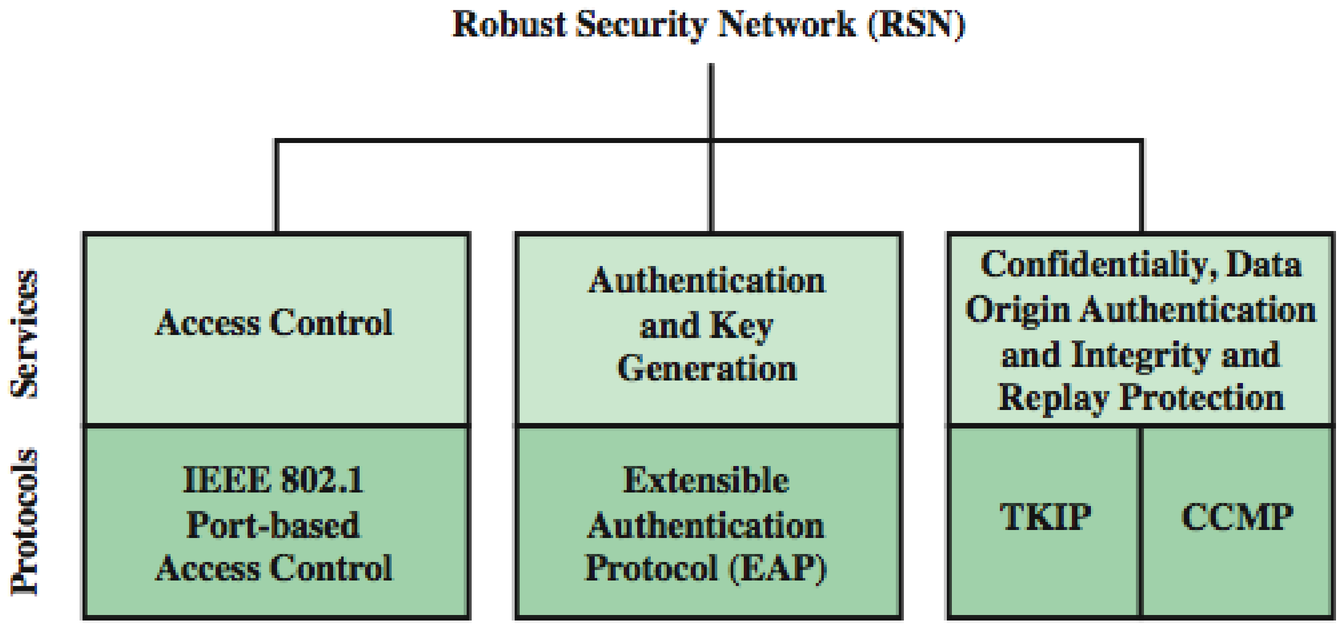
802.11 Wireless LAN Security

- wireless traffic can be monitored by any radio in range, not physically connected
- original 802.11 spec had security features
  - **Wired Equivalent Privacy (WEP)** algorithm
  - but found this contained major weaknesses
- 802.11i task group developed capabilities to address WLAN security issues
  - Wi-Fi Alliance **Wi-Fi Protected Access (WPA)**
  - final 802.11i **Robust Security Network (RSN)**
    - RSN is commonly called **WPA2**

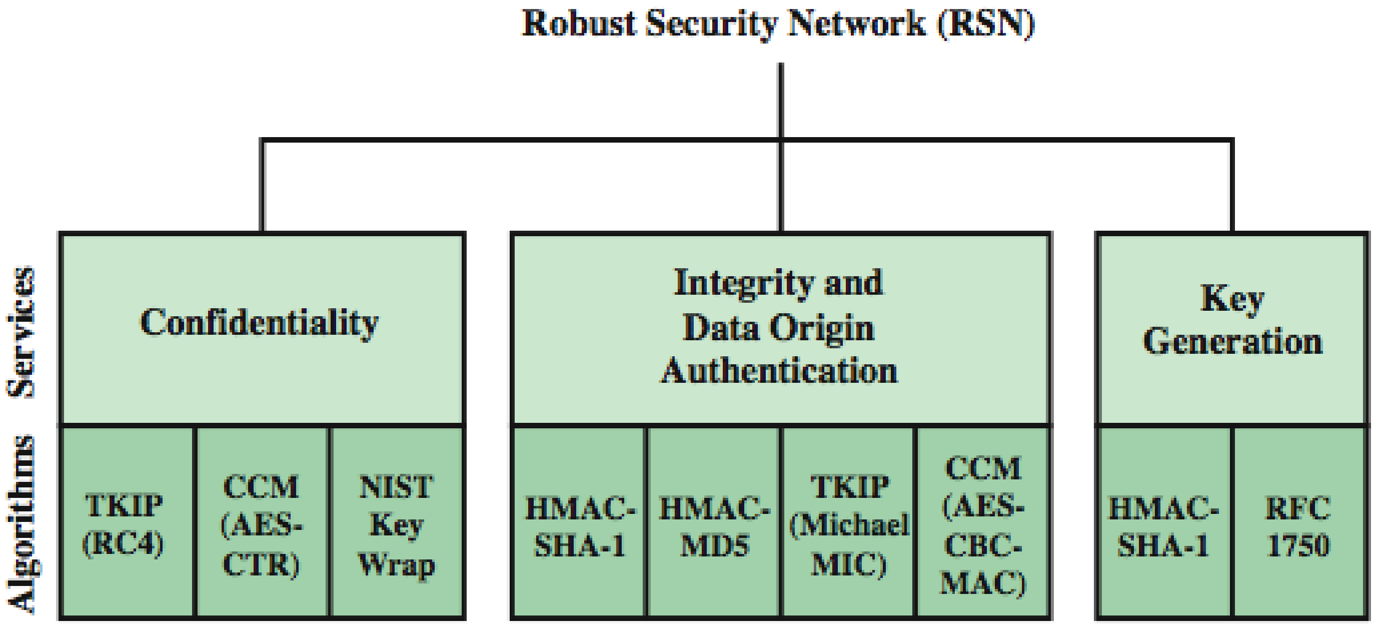
RNS Glossary

EAP:	Extensible Authentication Protocol A collection of many different alternative authentication protocols
TKIP:	Temporal Key Integrity Protocol
CCMP:	Counter Mode with CBC MAC Protocol
CBC:	Cipher Block Chaining
MAC:	Message Authentication Code
MIC:	Message Integrity Code (same as MAC)
AS:	Authentication Server
PSK:	Pre-shared key
MSK:	Master Session Key
PMK:	Pair-wise Master Key
PTK:	Pair-wise Transient Key
KCK:	Key Confirmation Key
KEK:	Key Encryption Key
TK:	Temporal Key
GMK:	Group Master Key
GTK:	Group Temporal Key

802.11i RSN Services and Protocols


Robust Security Network (RSN)
Services
Protocols
Access Control
Authentication and Key Generation
Confidentialiy, Data Origin Authentication and Integrity and Replay Protection
IEEE 802.1 Port-based Access Control
Extensible Authentication Protocol (EAP)
TKIP
CCMP

802.11i RSN Cryptographic Algorithms



Robust Security Network (RSN)

Services

Algorithms

Confidentiality

TKIP (RC4)

CCM (AES-CTR)

NIST Key Wrap

Integrity and Data Origin Authentication

HMAC-SHA-1

HMAC-MD5

TKIP (Michael MIC)

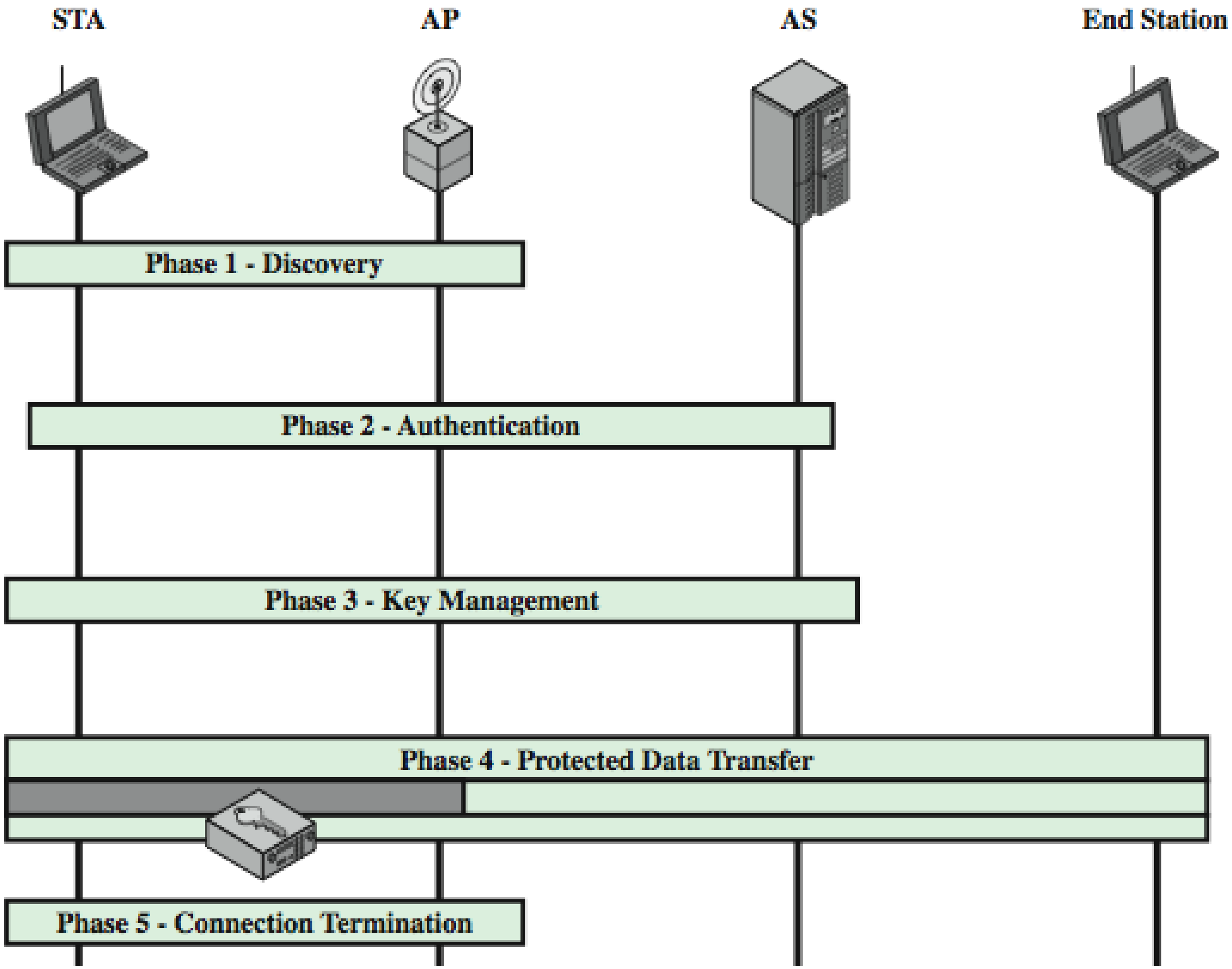
CCM (AES-CBC-MAC)

Key Generation

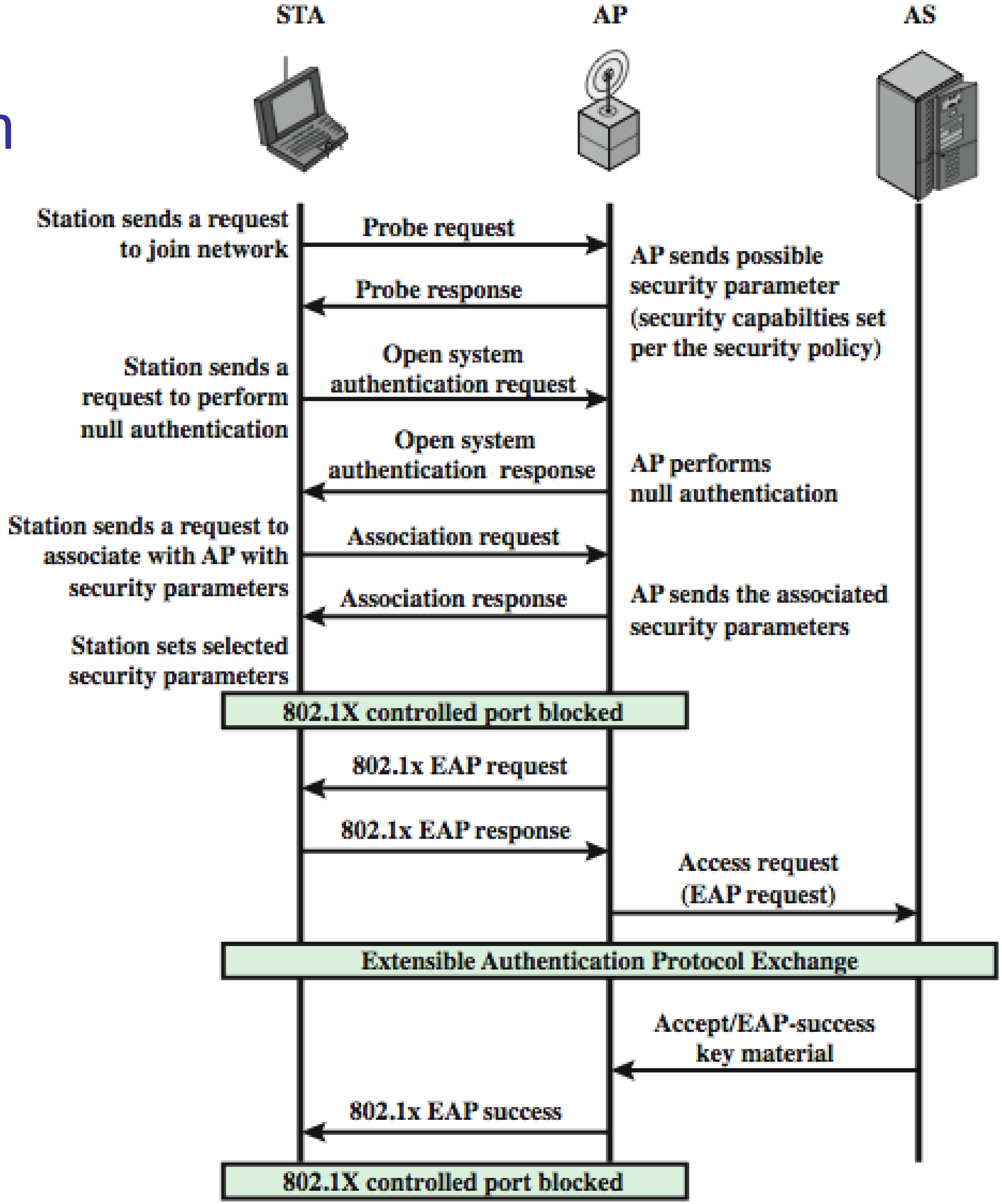
HMAC-SHA-1

RFC 1750

802.11i Phases of Operation

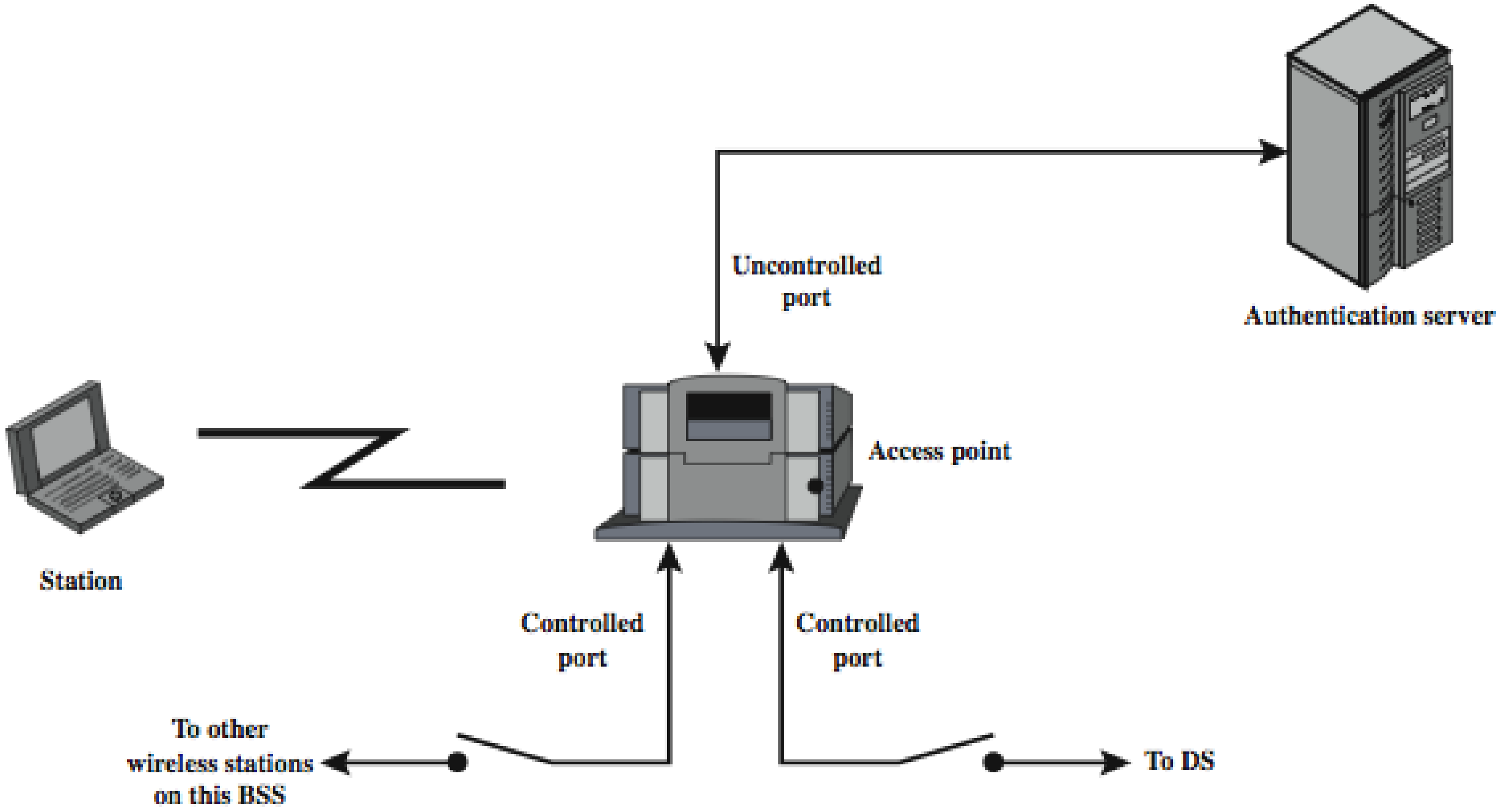


802.11i Discovery and Authentication Phases

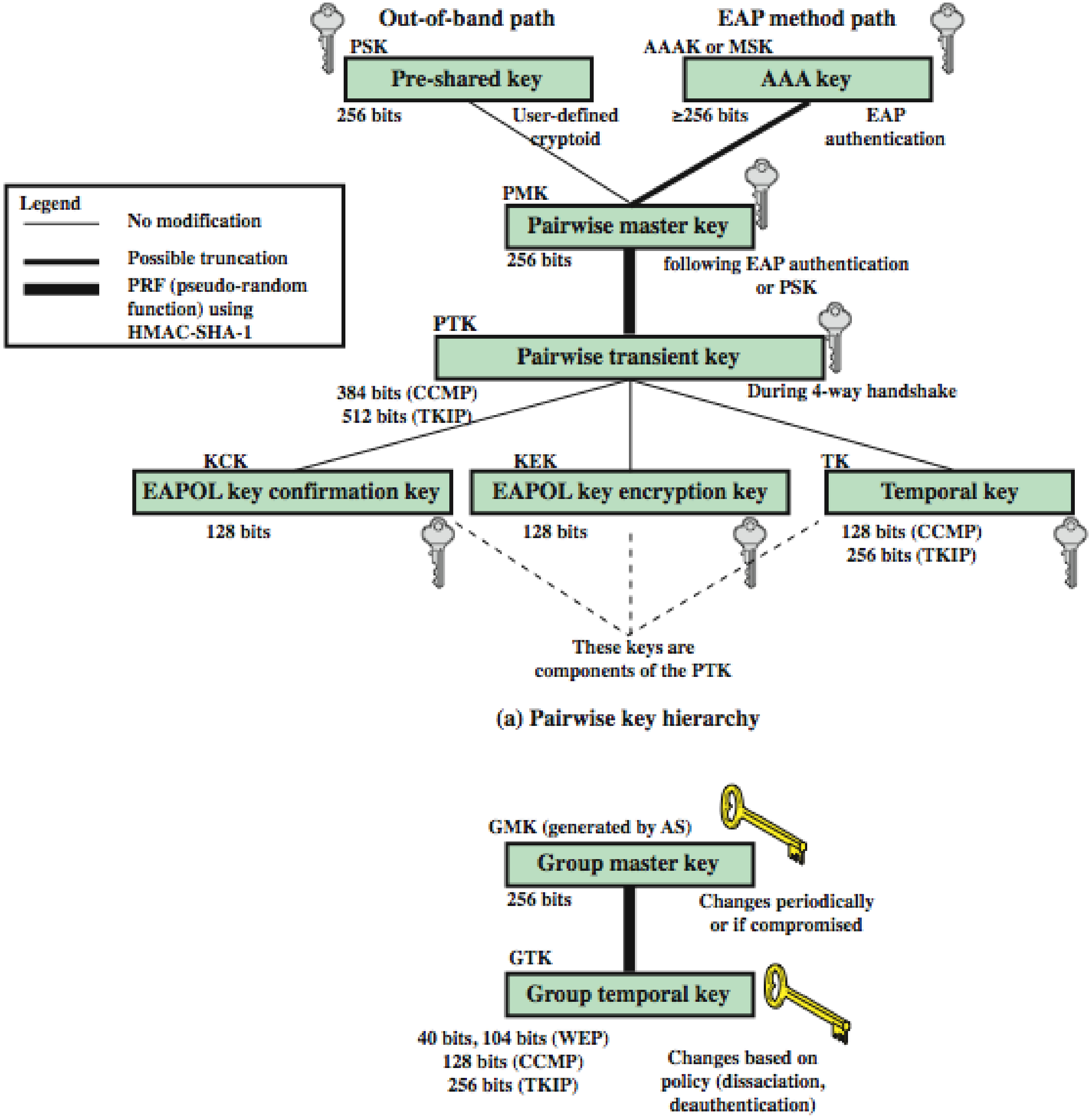


STA
AP
AS
Station sends a request to join network
Probe request
Probe response
AP sends possible security parameter (security capabilties set per the security policy)
Station sends a request to perform null authentication
Open system authentication request
Open system authentication response
AP performs null authentication
Station sends a request to associate with AP with security parameters
Association request
Association response
AP sends the associated security parameters
Station sets selected security parameters
802.1X controlled port blocked
802.1x EAP request
802.1x EAP response
Access request (EAP request)
Extensible Authentication Protocol Exchange
Accept/EAP-success key material
802.1x EAP success
802.1X controlled port blocked

IEEE 802.1X Access Control Approach



802.11i
Key Hierarchy



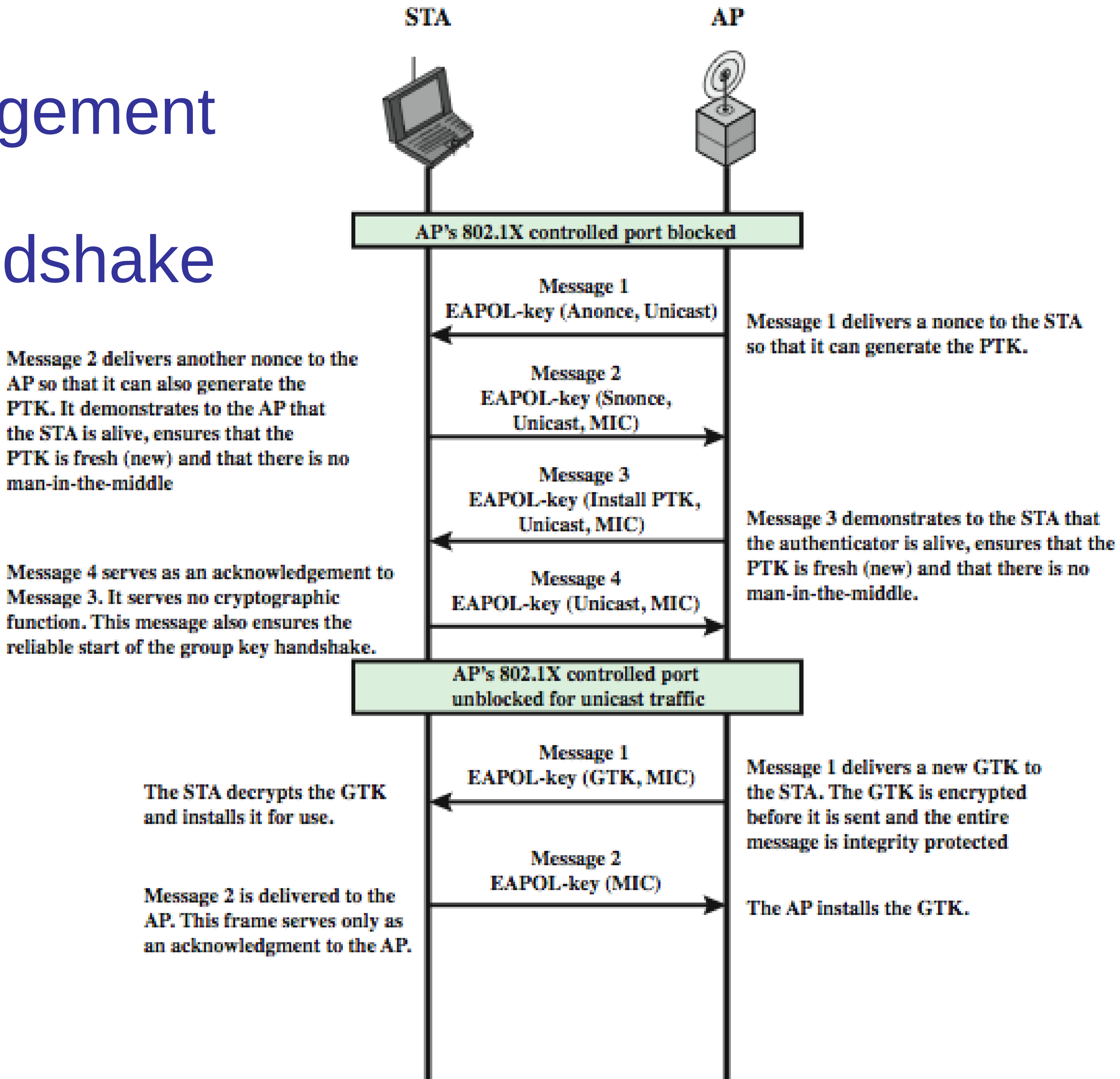
(a) Pairwise key hierarchy

(b) Group key hierarchy

Robust Security Network via 802.1X

- PTK (Pairwise Transient Key – 64 bytes)
  - 16 bytes of EAPOL-Key Confirmation Key (KCK)– Used to compute MIC on WPA EAPOL Key message
  - 16 bytes of EAPOL-Key Encryption Key (KEK) - AP uses this key to encrypt additional data sent (in the 'Key Data' field) to the client (for example, the RSN IE or the GTK)
  - 16 bytes of Temporal Key (TK) – Used to encrypt/decrypt Unicast data packets
  - 8 bytes of Michael MIC Authenticator Tx Key – Used to compute MIC on unicast data packets transmitted by the AP
  - 8 bytes of Michael MIC Authenticator Rx Key – Used to compute MIC on unicast data packets transmitted by the station
- Last two only used when TKIP is used.

802.11i
Key Management Phase
4-way handshake



STA

AP

AP's 802.1X controlled port blocked

Message 1
EAPOL-key (Anonce, Unicast)

Message 1 delivers a nonce to the STA so that it can generate the PTK.

Message 2 delivers another nonce to the AP so that it can also generate the PTK. It demonstrates to the AP that the STA is alive, ensures that the PTK is fresh (new) and that there is no man-in-the-middle

Message 2
EAPOL-key (Snonce, Unicast, MIC)

Message 3
EAPOL-key (Install PTK, Unicast, MIC)

Message 3 demonstrates to the STA that the authenticator is alive, ensures that the PTK is fresh (new) and that there is no man-in-the-middle.

Message 4 serves as an acknowledgement to Message 3. It serves no cryptographic function. This message also ensures the reliable start of the group key handshake.

Message 4
EAPOL-key (Unicast, MIC)

AP's 802.1X controlled port unblocked for unicast traffic

Message 1
EAPOL-key (GTK, MIC)

Message 1 delivers a new GTK to the STA. The GTK is encrypted before it is sent and the entire message is integrity protected

The STA decrypts the GTK and installs it for use.

Message 2
EAPOL-key (MIC)

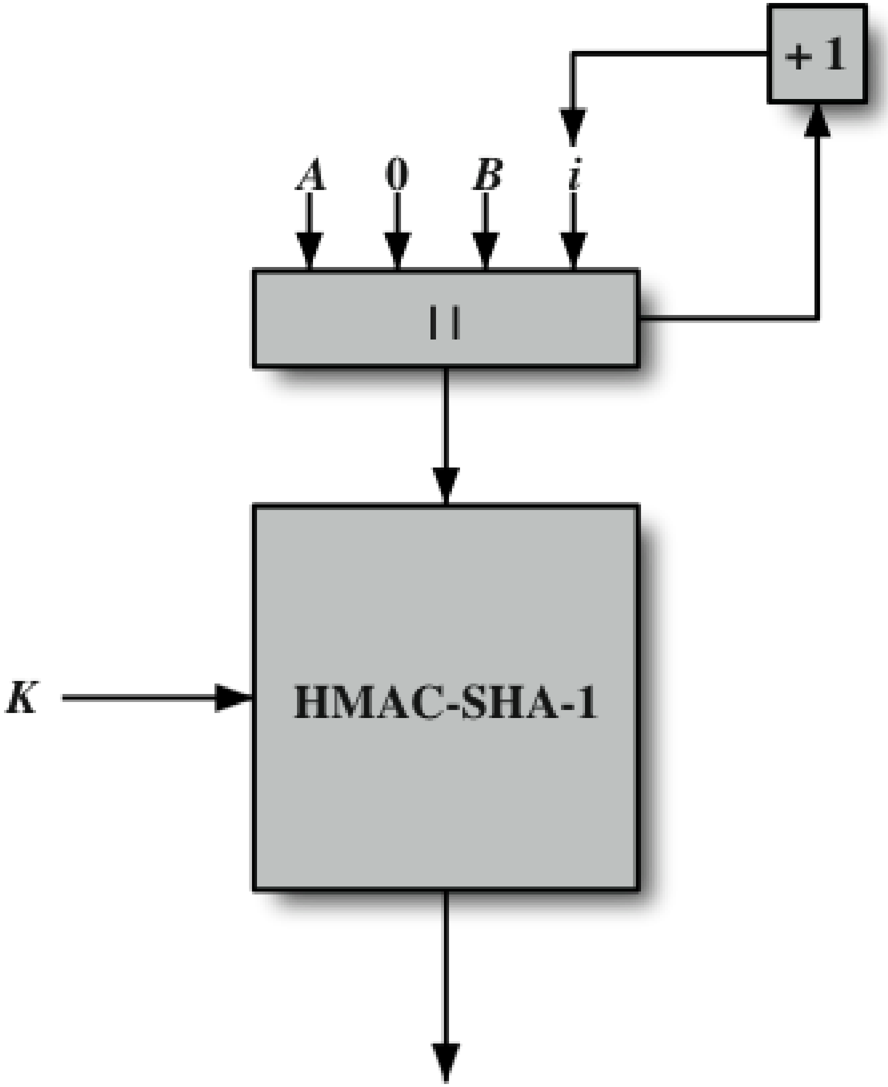
Message 2 is delivered to the AP. This frame serves only as an acknowledgment to the AP.

The AP installs the GTK.

802.11i Protected Data Transfer Phase

- have two schemes for protecting data
- Temporal Key Integrity Protocol (TKIP)
  - s/w changes only to older WEP
  - adds 64-bit Michael message integrity code (MIC)
  - encrypts MPDU plus MIC value using RC4
- Counter Mode-CBC MAC Protocol (CCMP)
  - uses the cipher block chaining message authentication code (CBC-MAC) for integrity
  - uses the CTR block cipher mode of operation

IEEE 802.11i Pseudorandom Function



$R = \text{HMAC-SHA-1}(K, A \,\|\, 0 \,\|\, B \,\|\, i)$

WPA2-PSK

- Pre-Shared Key Mode
  - Network traffic encrypted using a 256 bit PMK
  - User enters key (Pairwise Master Key)
    - 64 hex digits
    - 8-63 Printable ASCII characters
      - Takes the passphrase, salts it with SSID of AP, then runs it through 4096 iterations of HMAC-SHA-1
- Authentication, Connection, Establishment of PTK and GTK.
  - Similar process as when an AS is present except the PSK is used as the PMK.
  - Creation of PTK and GTK is the same as in Enterprise mode.

Summary

- have considered:
  - IEEE 802.11 Wireless LANs
    - protocol overview and security
  - Wireless Application Protocol (WAP)
    - protocol overview
  - Wireless Transport Layer Security (WTLS)