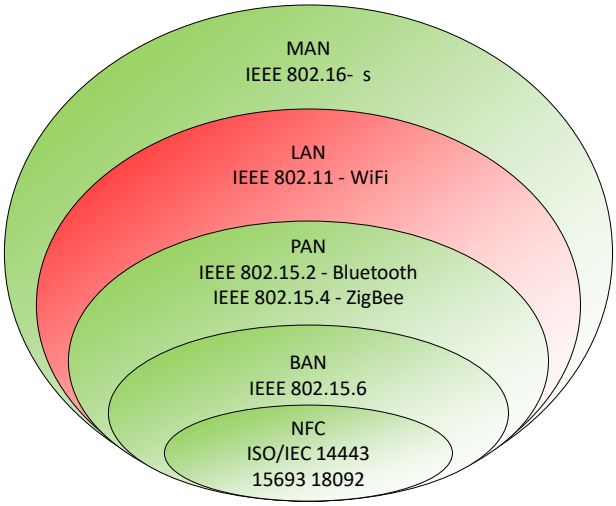
Security in 802.11 wireless networks

Wireless (data) communications: A glance



Wireless vs. cabled communications: Security issues

Broadcast communication

- Hard to enforce physical propagation boundaries
- Typical physical boundaries are useless to avoid:
  - Interference with communications
  - Eavesdropping of communications

Mitigation

- Reduce interference and eavesdropping capabilities
  - At the physical layer
  - At the data link layer

Reduce interference and eavesdropping capabilities: Physical layer

Prevent eavesdroppers from decoding the channel

- Channel coding needs to use some shared secret

Example: Bluetooth FHSS (Frequency Hoping Spread Spectrum)

- Carrier changes frequency in a pattern known to both transmitter and receiver
  - The data is divided into packets and transmitted over 79 hop frequencies in a pseudo random pattern
  - Only transmitters and receivers that are synchronized on the same hop frequency pattern will have access to the transmitted data
- FHSS appears as short-duration impulse noise to eavesdroppers
  - The transmitter switches hop frequencies 1,600 times per second to assure a high degree of data security

Reduce interference and eavesdropping capabilities: Physical layer

Present channel monopolization by transmitters

- Physical Medium access Policies

Examples

- Bluetooth FHSS
  - Unsynchronized transmitters seldom collide
- Wi-Fi
  - Each network is instantiated over a specific frequency
- GSM
  - Each terminal transmits over a specific mobile station

Interference is still possible from external sources or overlapping channels

Reduce interference and eavesdropping capabilities: data layer

Prevent attackers from identifying the participants in a communication

- Headers need to be encrypted, and temporary identifiers should be used

Prevent eavesdroppers from understanding data link payloads

- Frames need to be encrypted
- Usually, payloads only are encrypted

Prevent attackers from forging acceptable data link frames

- Frames need to be authenticated
  - Origin authentication
    - Freshness

IEEE 802.11: Architecture (in structured networks)

Station (STA)

- Device that can connect to a wireless network
- Has a (unique) identifier
  - Media Access Control (MAC) address
  - Today it is becoming popular its randomization (for anonymity sake)

Access Point (AP)

- Device that allows the interconnection between a wireless network and other network devices or networks

Wireless network

- Network formed by a set of STAs and AP that communicate using radio signals

IEEE 802.11: Structured network terminology

Basic Service Set (BSS)

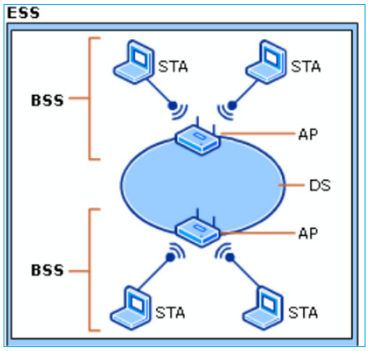
- Network formed by a set of STA associated to an AP

Extended Service Set (ESS)

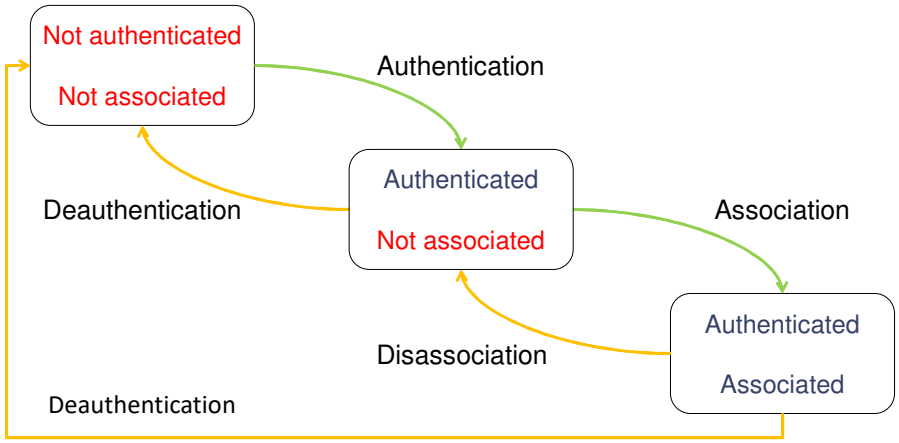
- Network formed by several BSS interconnected by a Distribution System (DS)

Service Set ID (SSID)

- Identifier of a wireless network served by a BSS or ESS
- The same infrastructure can use several SSID



IEEE 802.11:
Authentication & Association state machine



IEEE 802.11: Frame types

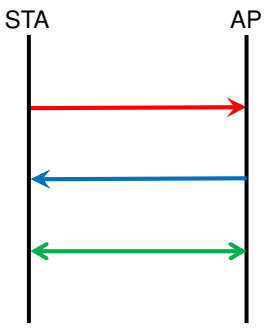
Management frames

- Beacon
- Probe Request & Response
- Authentication Request & Response
- Deauthentication
- Association Request & Response
- Reassociation Request & Response
- Disassociation

Control frames

- Request to Send (RTS)
- Clear to Send (CTS)
- Acknowledgment (ACK)

Data Frames



IEEE 802.11 data link security: Overview

Network Type / Functionality		pre-RSN	RSN (Robust Security Network)	
		WEP	WPA	802.11i (ou WPA2)
Authentication		Unilateral (STA)	Bilateral with 802.1X (STA, AP and network)	
Key Distribution			EAP ou PSK, 4-Way Handshake	
IV Management Policy			TKIP	AES-CCMP
Data Cipher		RC4		AES-CTR
Integrity Control	**Headers**		Michael	AES CBC-MAC
	Payload	CRC-32	CRC-32, Michael	

Other

- SSID hiding (on beacons)
- MAC address filtering (on associations)
- (Privacy) MAC client randomization before association

IEEE 802.11: WEP (Wired Equivalent Privacy)

Optional and unilateral Authentication

- Can support multiple types simultaneously

OSA: Open System Authentication

- No authentication, just for the state transition model

SKA: Shared Key Authentication

- Challenge/response between STA and AP
- Key (password) per person (MAC address) or network
- Unilateral STA authentication
  - No AP / network authentication

Frame payload encryption

- With RC4, using 40 or 104 bit keys

Frame payload authentication with CRC-32

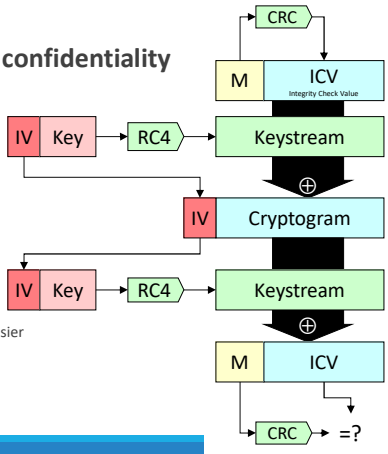
WEP: Lots of security problems …

SKA is completely insecure
- An eavesdropper gets all it needs to impersonate a victim
  - No need to discover the password
- Rogue APs cannot be detected

Same key for authentication and payload confidentiality
- No key distribution, keys overused

Weak integrity control
- CRC-32 is linear
- Frame deterministic modification is trivial

Mediocre IV management
- IV is too short (24 bits)
  - Easy to get cryptograms produced with the same IV
  - Same IV, same key ⇒ same keystream, cryptanalysis becomes easier
- IV is not managed at all
  - Reuse is not controlled / prevented



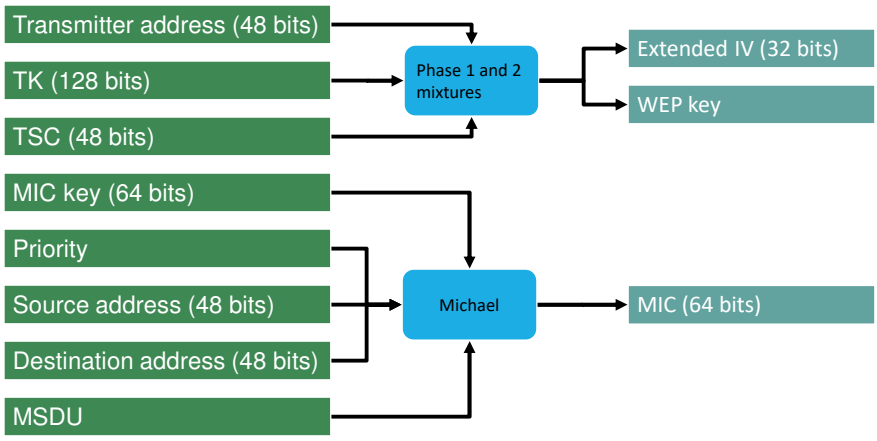
Mitigation of WEP problems: WPA (WiFi Protected Access)

WPA uses WEP in a safe way
- A different RC4 key per frame
- RC4 week keys are avoided
- Extra cryptographic integrity control with Michael
- IV strict sequencing for preventing frame reuse

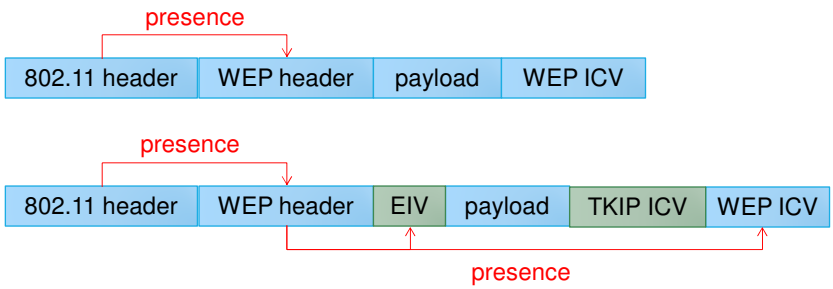
Implemented first by device drivers
- Latter on firmware

Inline with 802.11i
- The actual 802.11 security standard
- WPA can be used with 802.1X for strong, mutual authentication

WPA:
TKIP (Temporal Key Integrity Protocol)



TKIP: Frame layout



IEEE 802.1X: Port-Based Authentication

Authentication model for all IEEE 802 networks

- Layer 2 mutual authentication

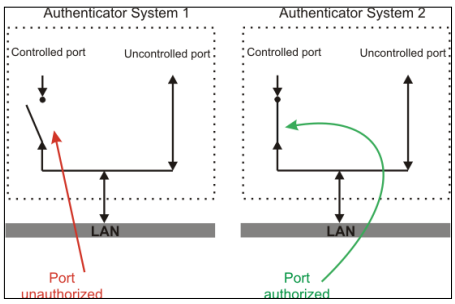
Originally conceived for large networks

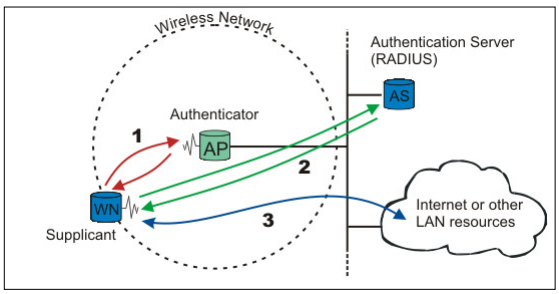
- University campus, etc.
- Model was extended for wireless networks

Performs key distribution

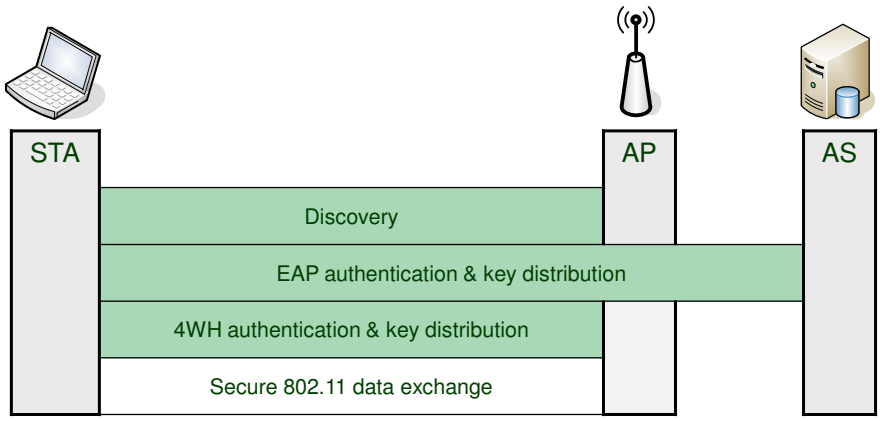
- Additional protocols focus in the remaining processes

IEEE 802.1X: Architecture

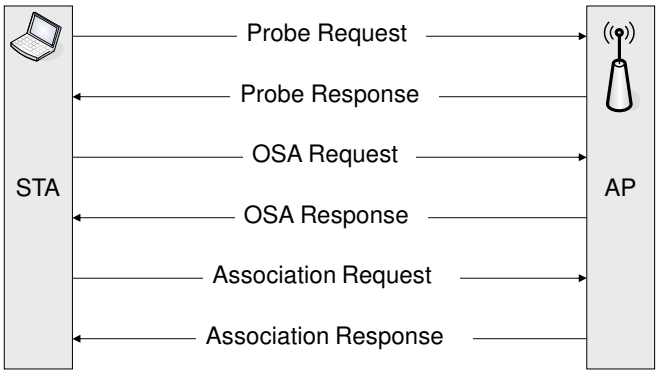




IEEE 802.1X: Operational Phases



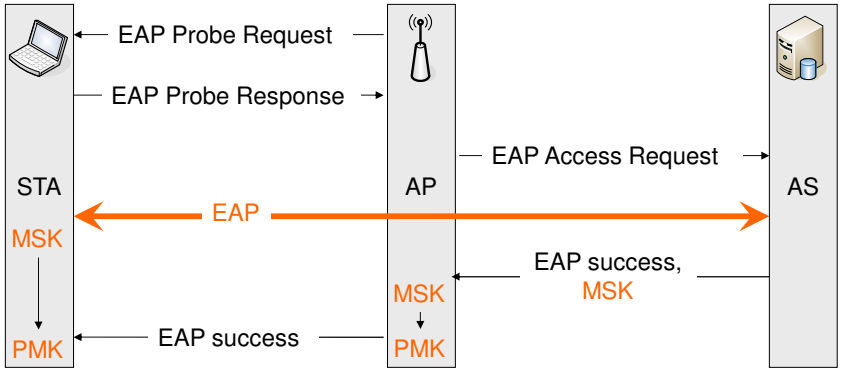
IEEE 802.1X Phase 1: Discovery (802.11 messages)



STA only got access to the AP

- 802.1X controlled port still closed

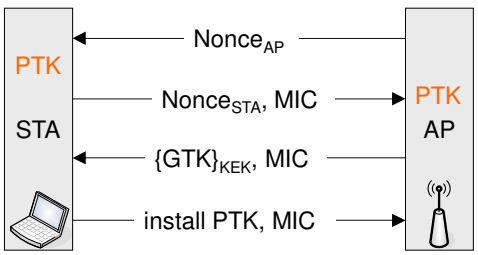
IEEE 802.1X Phase 2: Authentication (EAP Messages)

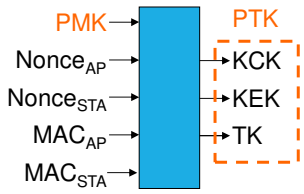


At the end of this phase AP and STA share crypto data

- PMK (Pairwise Master Key)
- But 802.1X controlled port still closed

IEEE 802.1X Phase 3: 4-Way Handshake (EAPoL Messages)





At the end AP and STA share new, fresh crypto data

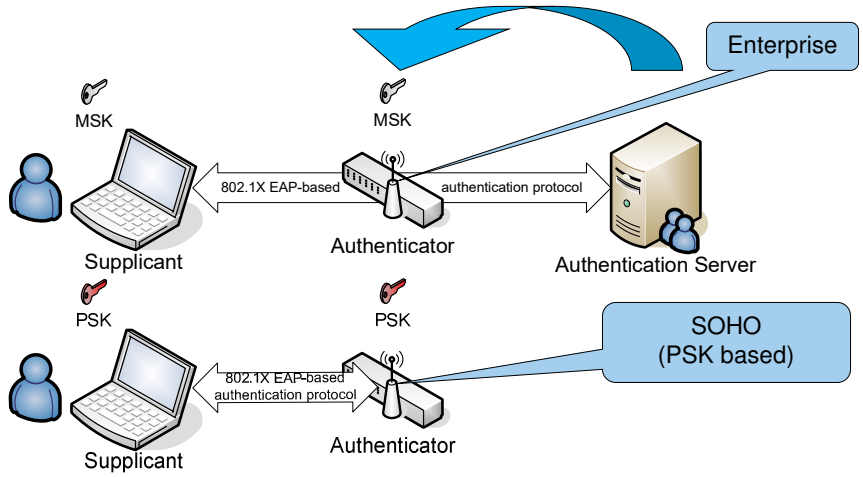
- PTK (*Pairwise Transient Key*)
- GTK (*Group Transient Key*)

Both are convinced that the peer knows PMK and PTK

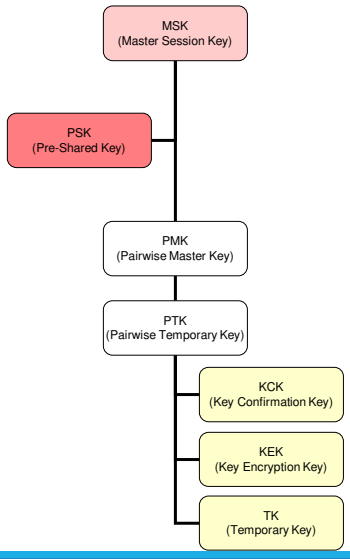
- Due to the use of MICs

802.1X controlled port is now open for unicast traffic

IEEE 802.1X: Architectural options



IEEE 802.1X: Complete key hierarchy



MSK
- Fresh outcome of an EAP protocol run
- Enterprise architecture

PSK
- Long-term AP-STA pre-shared key
- SOHO architecture

PMK
- Fresh key used for AP-STA mutual authentication and for key distribution in 4WH protocol runs

PTK
- Key used to protect AP-STA data exchanges
- KCK / KEK: 4WH protocol
- TK: 802.11 data frames

EAP (Extensible Authentication Protocol)

Initially conceived for PPP

- Adapted to 802.1X

AP not involved

- Relay EAP traffic
- Different EAP protocols do not imply changes in Aps

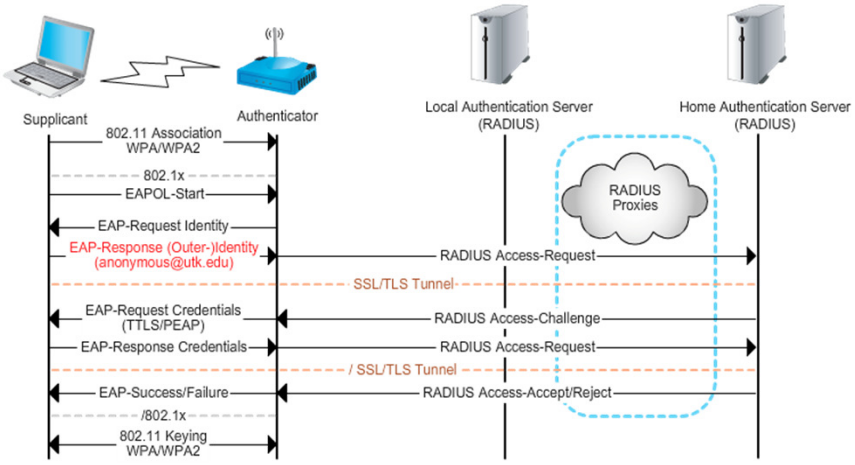
Not conceived for wireless networks

- EAP traffic not protected
- Mutual authentication not mandatory
  - An STA can be fooled by a stronger (radio level), rogue AP

Some EAP protocols for 802.1X

	LEAP	EAP-TLS	EAP-TTLS	PEAP
AS authentication	digest (challenge, password)	Public Key (certificate)		
Supplicant authentication	digest (challenge, password)	Public Key (certificate)	EAP, Public Key (certificate)	PAP, CHAP, MS-CHAP, EAP
Risks	Identity exposure Dictionary attacks Host-in-the-Middle attacks	Identity exposure		Possible identity exposure in phase 1

Eduroam: 802.1X w/ PEAP + MS-CHAPv2



Available on most University of the world

- Local Authentication Servers (using RADIUS) for roaming access

IEEE 802.11i (WPA2)

Defines Robust Security Networks (RSN)

- Those that support WPA and 802.11i

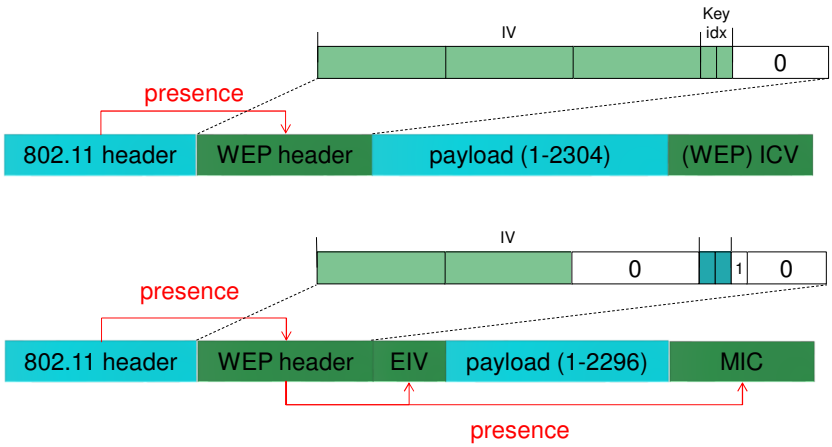
Uses advanced security mechanisms for frame protection

- Advanced Security Algorithm (AES) for payload encryption and frame integrity control

Uses 802.1X for network access authentication

- Simplified Pre-Shared Key (PSK) mode for SOHO (Small Office, Home Office) environments
- EAP-based protocol for enterprise environments

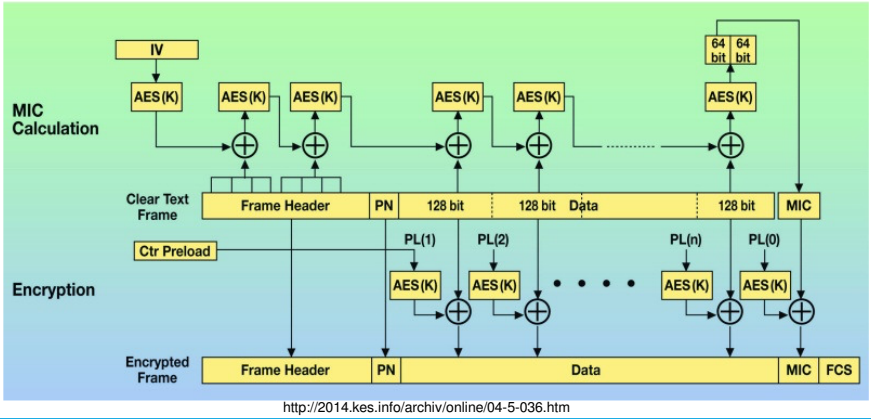
WEP vs AES-CCMP: Frame layout



WPA2 frame protection

CCMP - Counter CBC-MAC Protocol

- 128-bit keys, protection of headers, data, with cipher and authentication



http://2014.kes.info/archiv/online/04-5-036.htm

802.11w: Protected Management Frames

Management frames that can be used for DoS attacks are authenticated

- Deauthentication & Deassociation requests
- Other management frames unicasted or broadcast by an AP

BIP (Broadcast Integrity Protocol)

- IGTK (Integrity GTK)
- For protecting part of the AP broadcast traffic

Security Association Query Request / Response

- Help to deal with desynchronization issues

IEEE 802.11 security: Are all the problems solved? No!

Dictionary attacks are still possible with PSK or EAP-based authentication

- And they will continue to be as long as (weak) passwords are chosen by people

There are still some unprotected frames

Some weaknesses at the CSMA level

- Low Congestion Window (CW) values allow attackers to get all the bandwidth