Lab (2)
Securing Wireless LANs

Instructor: Prof. Phone Lin (林風)
Teacher Assistants: Chia-Peng Lee(李家朋)

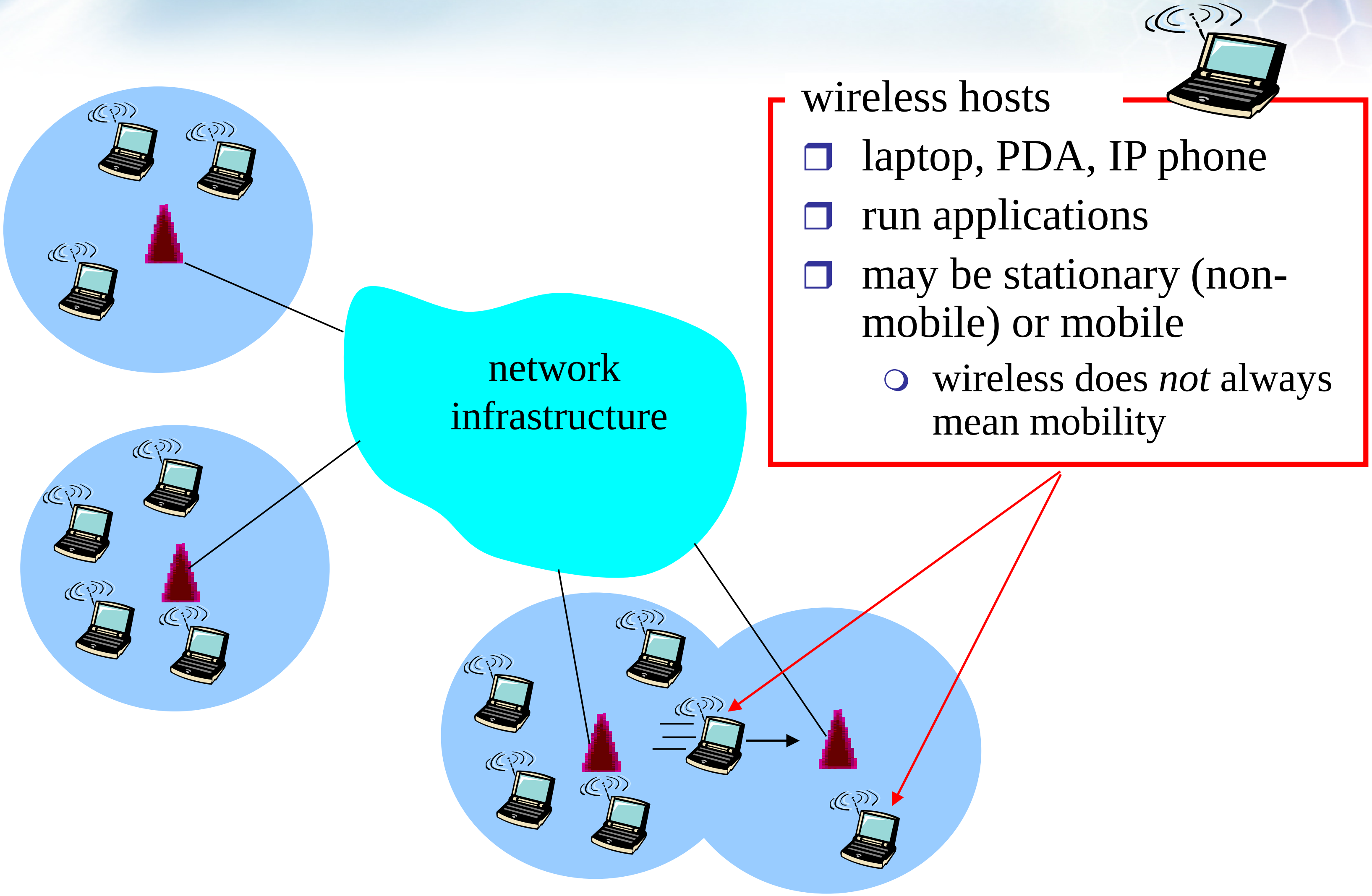
Date: 2019/3/20

Mobile Communications Networking Lab, NTU

Outline

- Introduction to Wireless Network
- Securing wireless LANs
    - Authentication, Authorization and Accounting

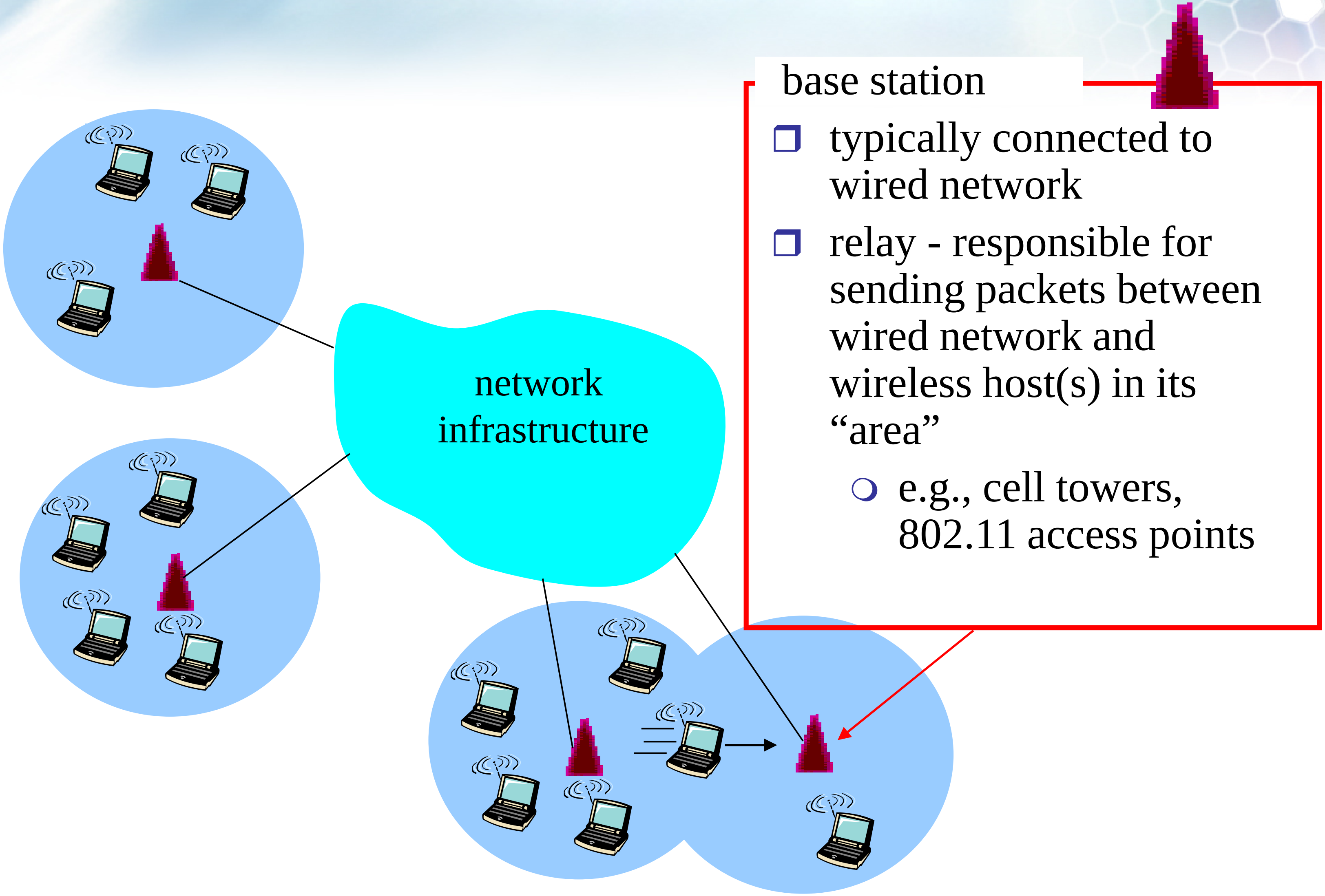
Elements of a wireless network



wireless hosts

- ❒ laptop, PDA, IP phone
- ❒ run applications
- ❒ may be stationary (non-mobile) or mobile
  - ○ wireless does *not* always mean mobility

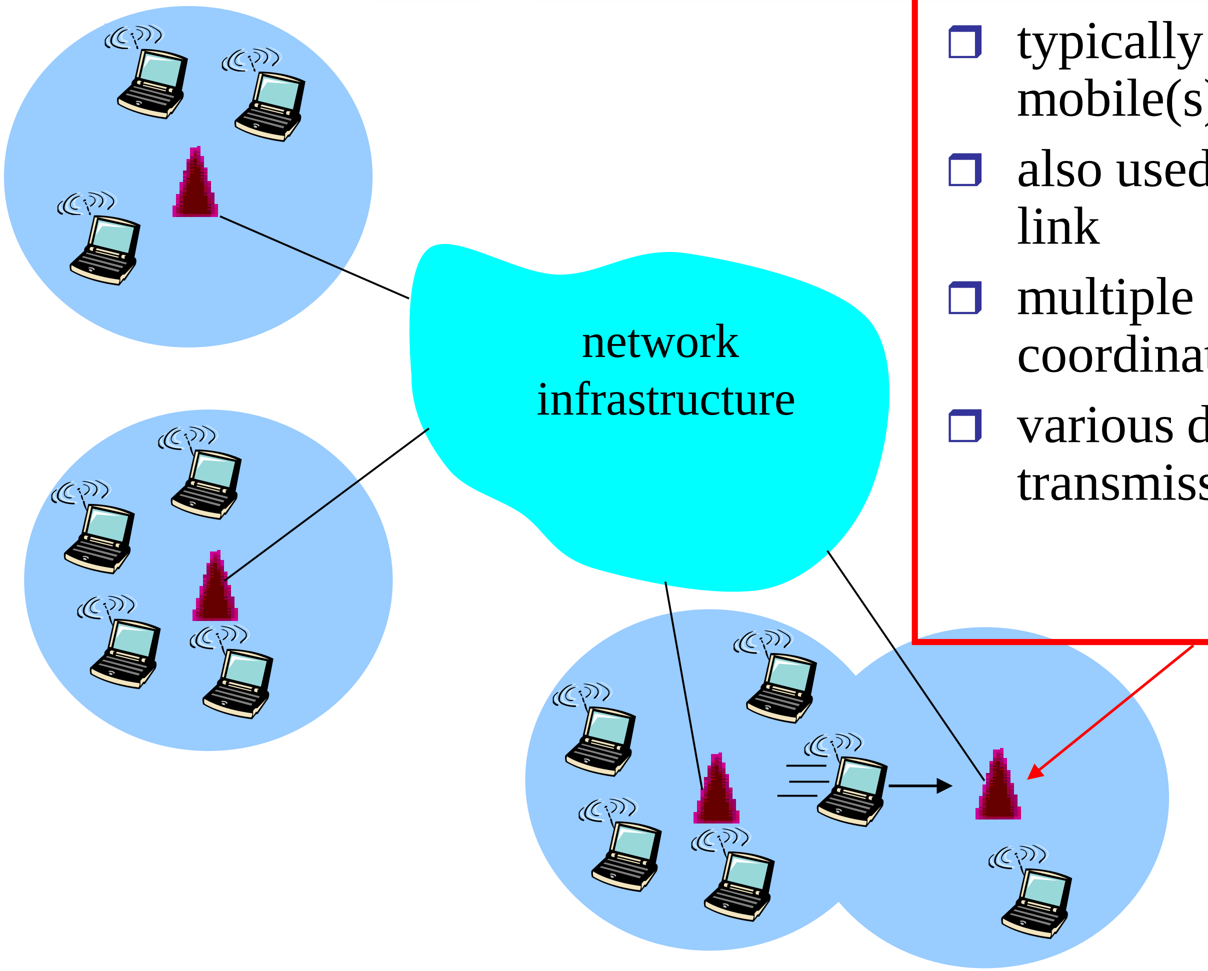
Elements of a wireless network



base station

- typically connected to wired network
- relay - responsible for sending packets between wired network and wireless host(s) in its "area"
  - e.g., cell towers, 802.11 access points

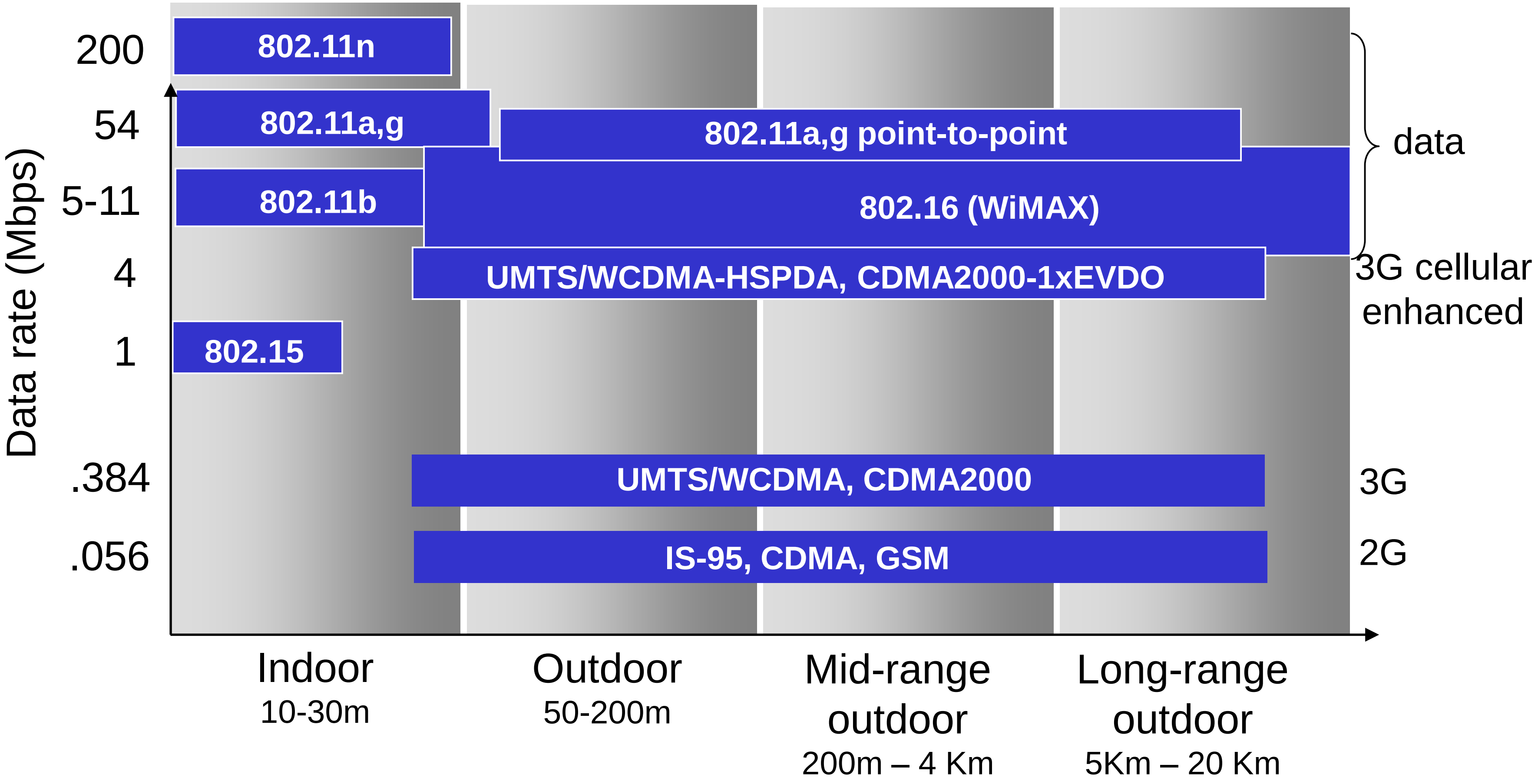
Elements of a wireless network



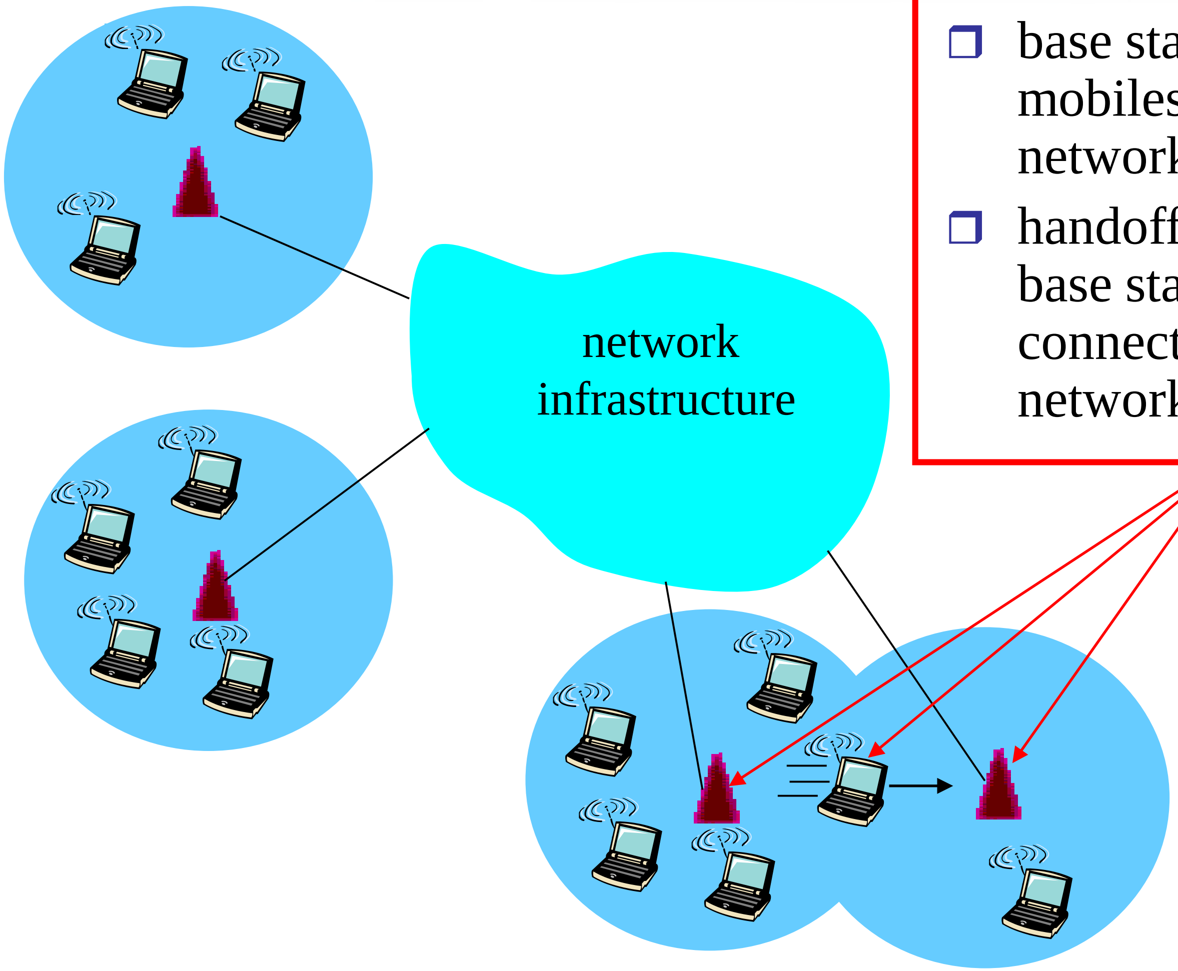
wireless link

- typically used to connect mobile(s) to base station
- also used as backbone link
- multiple access protocol coordinates link access
- various data rates, transmission distance

Characteristics of selected wireless link standards



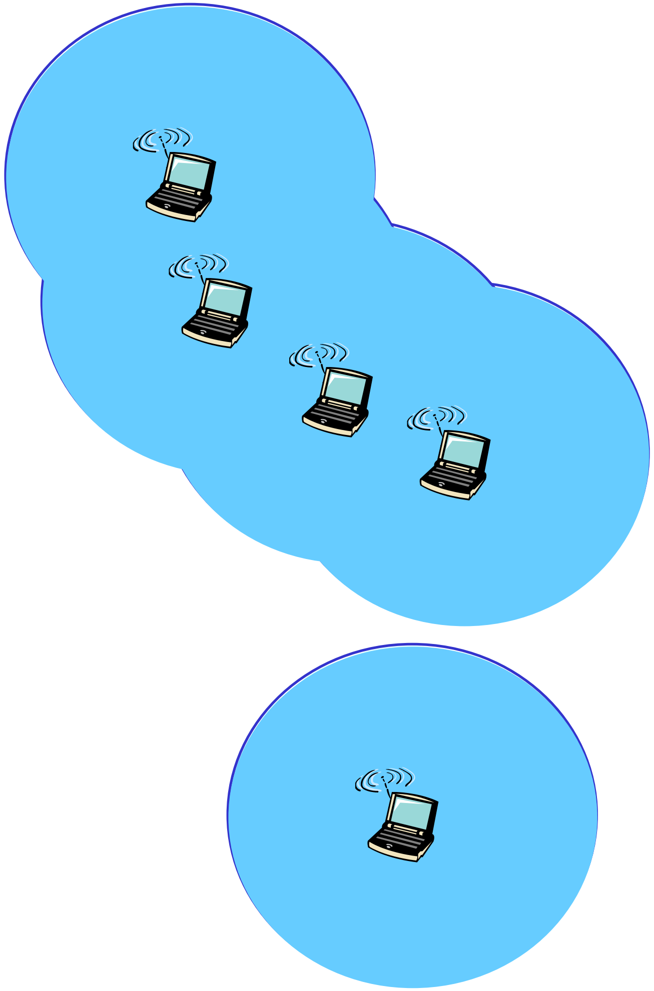
Elements of a wireless network



infrastructure mode

- base station connects mobiles into wired network
- handoff: mobile changes base station providing connection into wired network

Elements of a wireless network



ad hoc mode

- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves

Wireless network taxonomy

	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: *mesh net*
no infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET

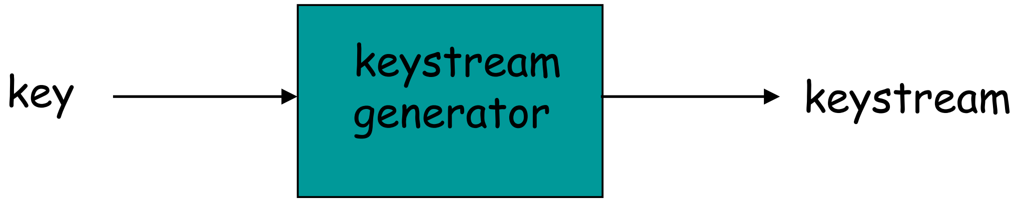
Outline

- Introduction to Wireless Network
- Securing wireless LANs
  - Authentication, Authorization and Accounting

WEP Design Goals

- **Symmetric key crypto**
  - Confidentiality
  - Station authorization
  - Data integrity
- **Self synchronizing: each packet separately encrypted**
  - Given encrypted packet and key, can decrypt; can continue to decrypt packets when preceding packet was lost
  - Unlike Cipher Block Chaining (CBC) in block ciphers
- **Efficient**
  - Can be implemented in hardware or software

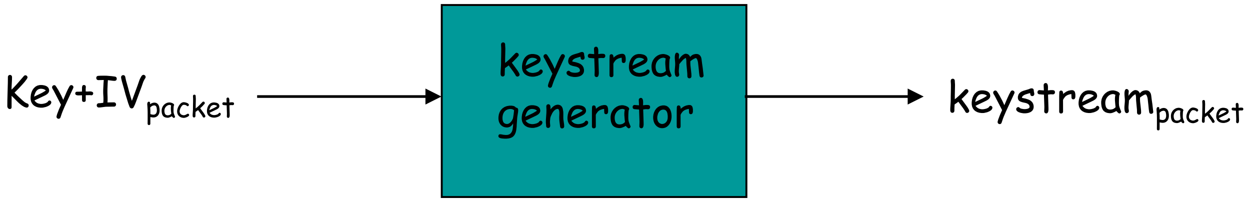
Review: Symmetric Stream Ciphers



- Combine each byte of keystream with byte of plaintext to get ciphertext
- m(i) = ith unit of message
- ks(i) = ith unit of keystream
- c(i) = ith unit of ciphertext
- c(i) = ks(i) ⊕ m(i)   (⊕ = exclusive or)
- m(i) = ks(i) ⊕ c(i)
- WEP uses RC4

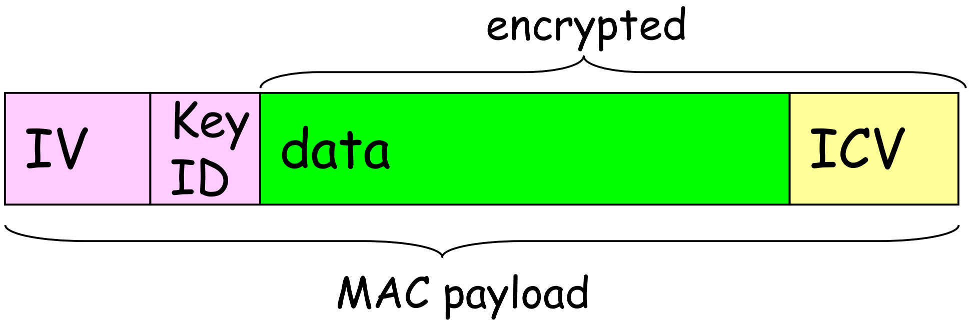
Stream cipher and packet independence

- **Recall design goal: each packet separately encrypted**
- **If for frame n+1, use keystream from where we left off for frame n, then each frame is not separately encrypted**
  - Need to know where we left off for packet n
- **WEP approach: initialize keystream with key + new IV for each packet:**

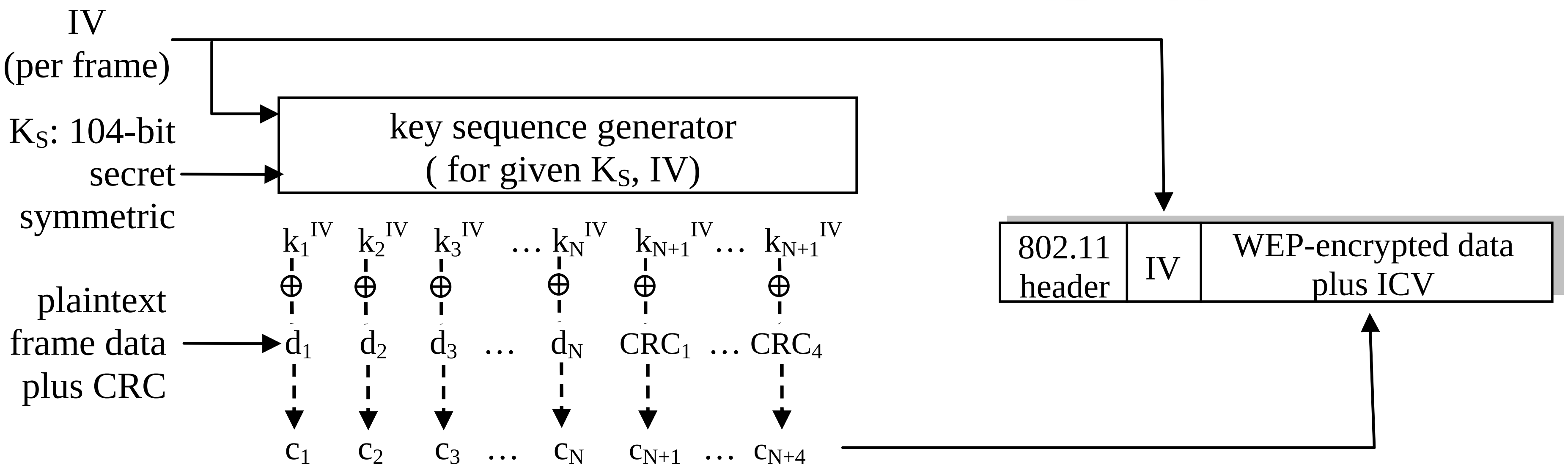

$\text{Key+IV}_{\text{packet}}$
keystream generator
$\text{keystream}_{\text{packet}}$

WEP encryption (1)

- **Sender calculates Integrity Check Value (ICV) over data**
  - four-byte hash/CRC for data integrity
- **Each side has 104-bit shared key**
- **Sender creates 24-bit initialization vector (IV), appends to key: gives 128-bit key**
- **Sender also appends keyID (in 8-bit field)**
- **128-bit key inputted into pseudo random number generator to get keystream**
- **data in frame + ICV is encrypted with RC4:**
  - Bytes of keystream are XORed with bytes of data & ICV
  - IV & keyID are appended to encrypted data to create payload
  - Payload inserted into 802.11 frame



WEP encryption (2)



IV
(per frame)

K_S: 104-bit
secret
symmetric

key sequence generator
(for given K_S, IV)

k_1^{IV} k_2^{IV} k_3^{IV} … k_N^{IV} k_{N+1}^{IV} … k_{N+1}^{IV}

⊕ ⊕ ⊕ ⊕ ⊕ ⊕

plaintext
frame data
plus CRC

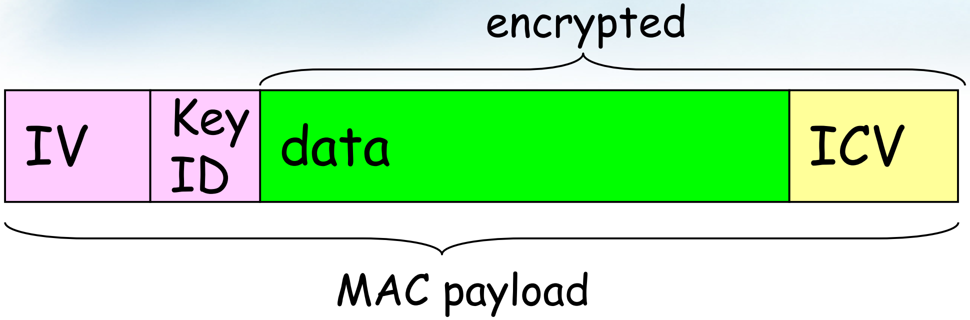
d_1 d_2 d_3 … d_N CRC_1 … CRC_4

c_1 c_2 c_3 … c_N c_{N+1} … c_{N+4}

802.11 header	IV	WEP-encrypted data plus ICV

New IV for each frame

WEP decryption overview

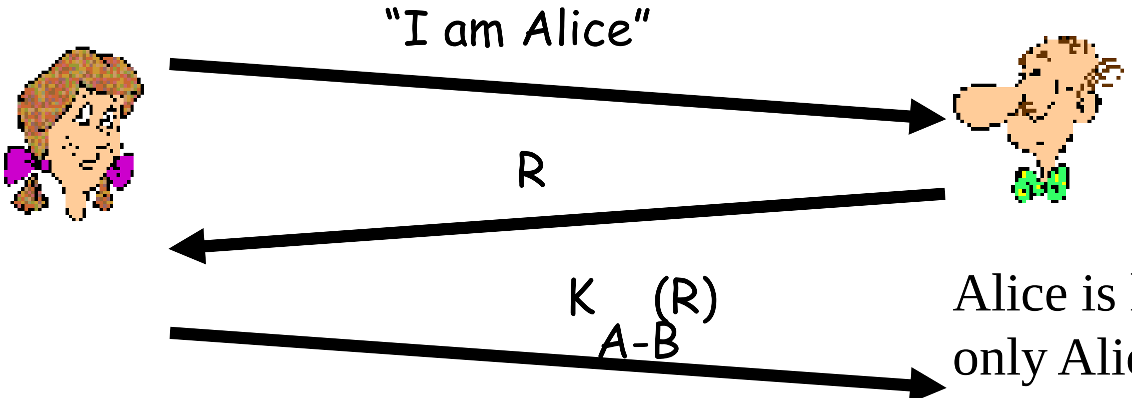


- **Receiver extracts IV**
- **Inputs IV and shared secret key into pseudo random generator, gets keystream**
- **XORs keystream with encrypted data to decrypt data + ICV**
- **Verifies integrity of data with ICV**
  - Note that message integrity approach used here is different from the MAC (message authentication code) and signatures (using PKI).

End-point authentication w/ nonce

Nonce: number (R) used only *once –in-a-lifetime*

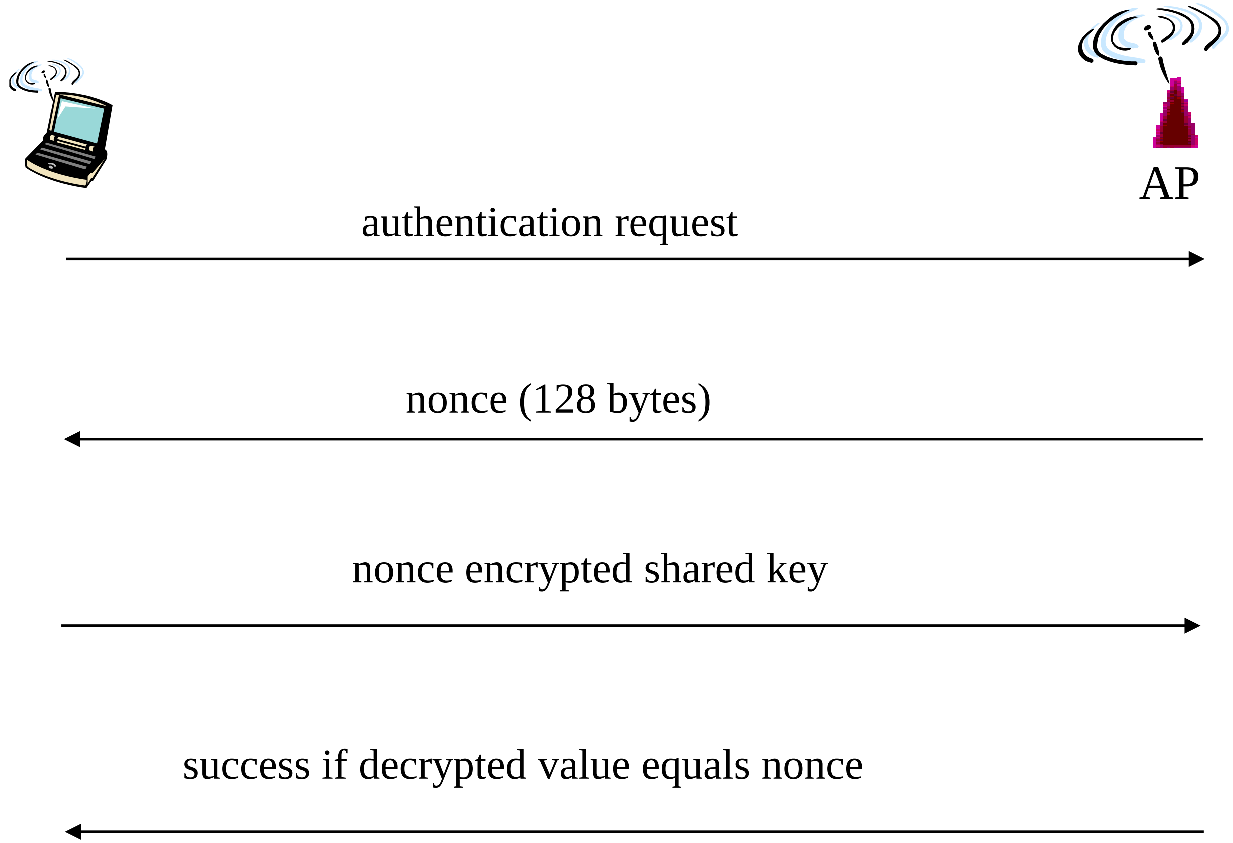
How: to prove Alice “live”, Bob sends Alice nonce, R. Alice must return R, encrypted with shared secret key



Alice is live, and only Alice knows key to encrypt nonce, so it must be Alice!

WEP Authentication

Not all APs do it, even if WEP is being used. AP indicates if authentication is necessary in beacon frame. Done before association.



AP
authentication request
nonce (128 bytes)
nonce encrypted shared key
success if decrypted value equals nonce

Breaking 802.11 WEP encryption

security hole:

- **24-bit IV, one IV per frame, -> IV's eventually reused**
- **IV transmitted in plaintext -> IV reuse detected**
- **attack:**
  - Trudy causes Alice to encrypt known plaintext d_1 d_2 d_3 d_4 …
  - Trudy sees: $c_i = d_i$ XOR k_i^{IV}
  - Trudy knows c_i d_i, so can compute k_i^{IV}
  - Trudy knows encrypting key sequence k_1^{IV} k_2^{IV} k_3^{IV} …
  - Next time IV is used, Trudy can decrypt!

What is AAA ?

- **Authentication** is essentially a login procedure involving a username and password: the process by which the network validates a dial-in user's identity – distinguishing a legitimate user from a malicious or mischievous hacker.
- **Authorization** is the process of restricting and enabling what each user can do.
- **Accounting** is the process of collecting and reporting statistics.

Outline

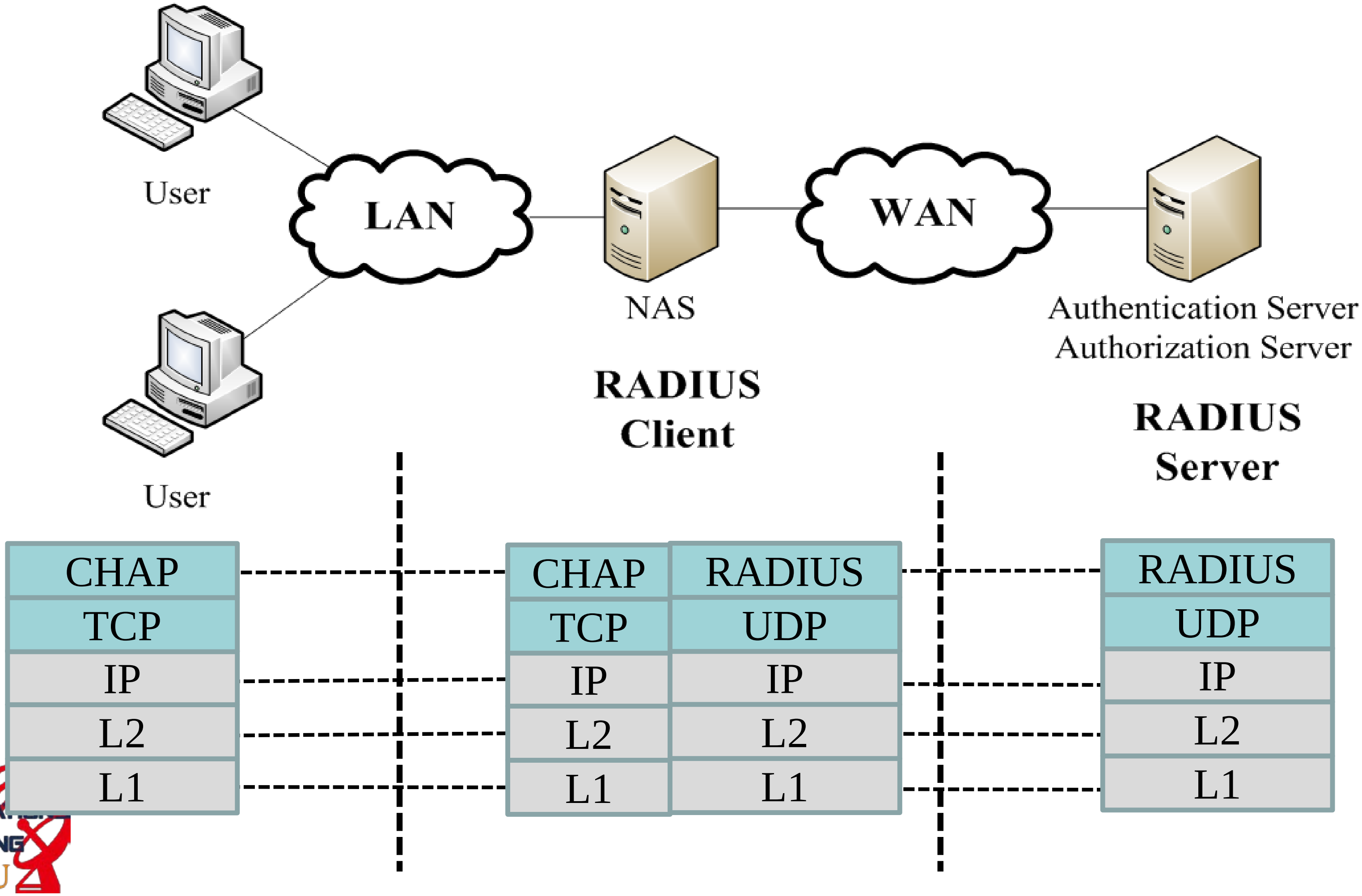
- Introduction to Wireless Network
- Securing wireless LANs
  - Authentication, Authorization and Accounting

Remote Authentication Dial-In User Service (RADIUS)

- Remote Authentication Dial-In User Service (RADIUS) is a data-communications protocol designed to provide security management and statistics collection in remote computing environments, especially for distributed networks with dial-in users.
- A central database, the RADIUS Server, maintains network security data (such as user profiles) and statistics (such as bytes transmitted and received).
- Centrally stored security data is more secure, easier to manage, and scales more smoothly than data scattered throughout the network on multiple devices.

Remote Authentication Dial-In User Service (RADIUS)

- RADIUS Client/Server Architecture



CHAP	CHAP	RADIUS	RADIUS
TCP	TCP	UDP	UDP
IP	IP	IP	IP
L2	L2	L2	L2
L1	L1	L1	L1

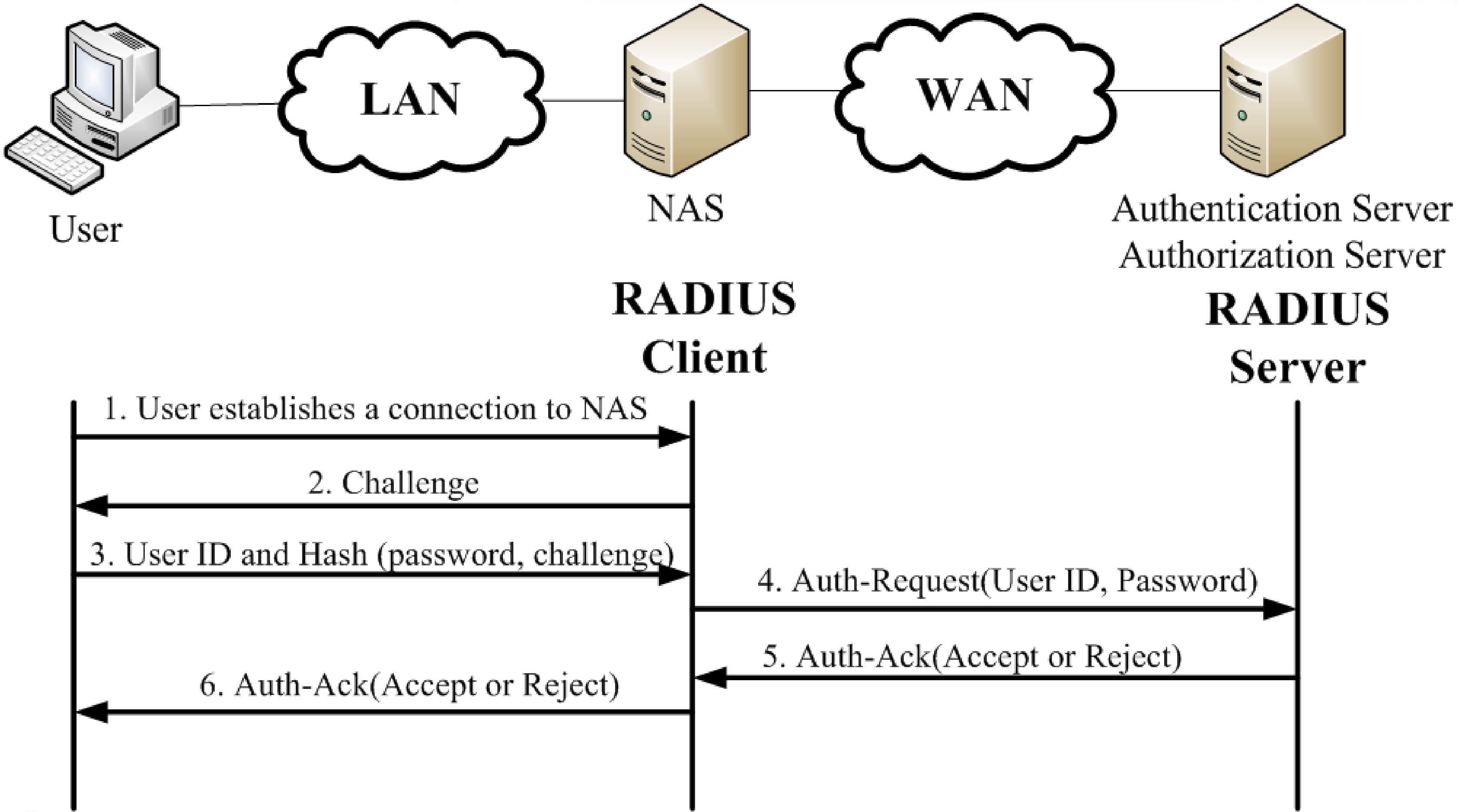
Remote Authentication Dial-In User Service (RADIUS)

- RADIUS operates on the client/server model. A RADIUS Authentication Server provides security services and stores security data.
- A RADIUS Accounting Server collects and stores statistical data.
- Most often a single machine provides both functions, however the two RADIUS servers may reside on separate machines. Network managers may configure a RADIUS Client to use RADIUS security services, RADIUS accounting services, or both.

Remote Authentication Dial-In User Service (RADIUS)

- A RADIUS client consists of a Network Access Server (NAS) which provides one or more remote users with access to network resources.
- A single RADIUS Server can serve hundreds of RADIUS clients and up to tens of thousand of end users.
- Fault tolerance and redundancy concerns can be addressed by configuring a RADIUS client to use one or more alternate RADIUS servers.
- A NAS can access a local RADIUS Server on the connected LAN, or a remote RADIUS Server via WAN connections.

RADIUS Authentication Procedure


LAN
WAN
User
NAS
Authentication Server
Authorization Server
RADIUS Client
RADIUS Server
1. User establishes a connection to NAS
2. Challenge
3. User ID and Hash (password, challenge)
4. Auth-Request(User ID, Password)
5. Auth-Ack(Accept or Reject)
6. Auth-Ack(Accept or Reject)

RADIUS Authentication Procedure

1. User dials into the NAS and establishes a connection.
2. The NAS prompts for user ID, password and challenge (CHAP).
3. User responds with user ID, password and challenge response (CHAP).
4. NAS forwards an Authentication Request Packet to the RADIUS Server, containing user identification, encrypted password, and NAS identification.

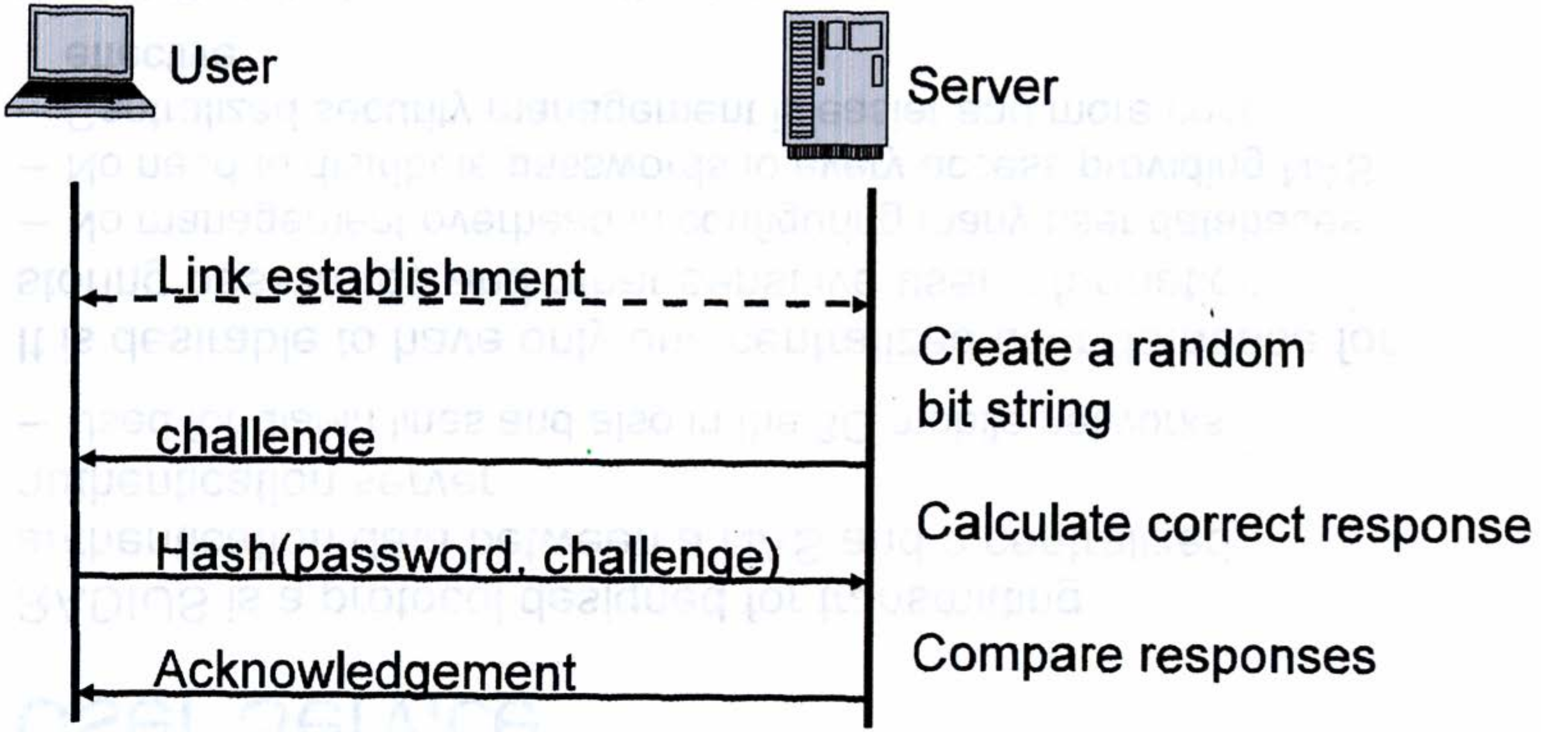
RADIUS Authentication Procedure

5. RADIUS Server validates the user and sends the NAS an Authentication Acknowledgement packet containing user configuration and either
   a) Specifying what network services and privileges the NAS should provide to the user (Access-accept), or
   b) Denying the Authentication Request (Access-reject).
6. NAS forwards the Authentication Acknowledgement packet to user.

Challenge-Handshake Authentication Protocol (CHAP)

- Used for authenticating dial-in users over a PPP(Point-to-Point Protocol) link.
- Based on the use of shared secrets
- Avoids sending passwords over a network
- The knowledge of the password is proved indirectly, using a one-way hash function
- RFC 1994 defines the packet format for CHAP message sent encapsulated in PPP frames

The CHAP 3-way handshake



User

Server

Link establishment

Create a random bit string

challenge

Calculate correct response

Hash(password, challenge)

Compare responses

Acknowledgement

CHAP Security

- The 128-bit MD5 algorithm is the default hash function used CHAP.
  - Without knowing the shared secret, it its practically impossible to create a valid response to given challenge.
  - Password guessing is still possible.
- The use of a random challenge eliminates the possibility for a replay attack.
  - The CHAP handshake procedure may be periodically repeated to limit the time of exposure to any single attack.