SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF CSE/CST

COURSE NAME :19IT401 COMPUTER NETWORKS

II YEAR /IV SEMESTER

Unit 5- Application layer

Topic 6 : SECURE SHELL [SSH]

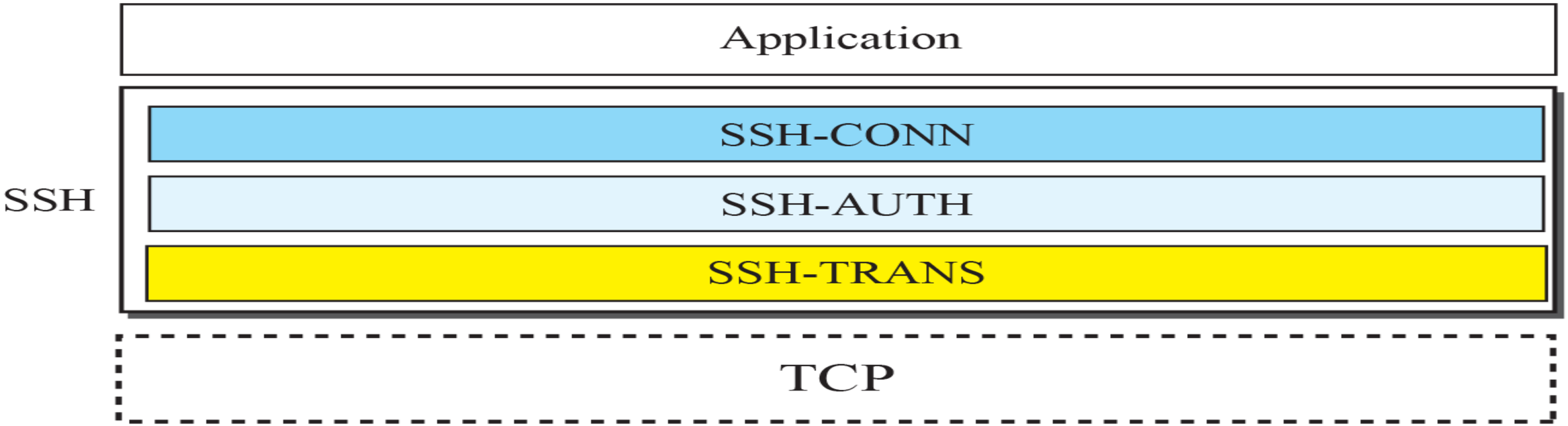
SECURE SHELL (SSH)

- ✓ SSH stands for **Secure Shell or Secure Socket Shell**. It is a cryptographic network protocol that allows two computers to communicate and share the data over an insecure network such as the internet.
- ✓ It is used to login to a remote server to execute commands and data transfer from one machine to another machine.

- ✓ Secure Shell (SSH) is a secure application program that can be used today for several purposes such as remote logging and file transfer, it was originally designed to replace TELNET.
- ✓ It provides secure access to users and automated processes.
- ✓ It is an easy and secure way to transfer files from one system to another over an insecure network.
- ✓ It also issues remote commands to the users.

Components of SSH

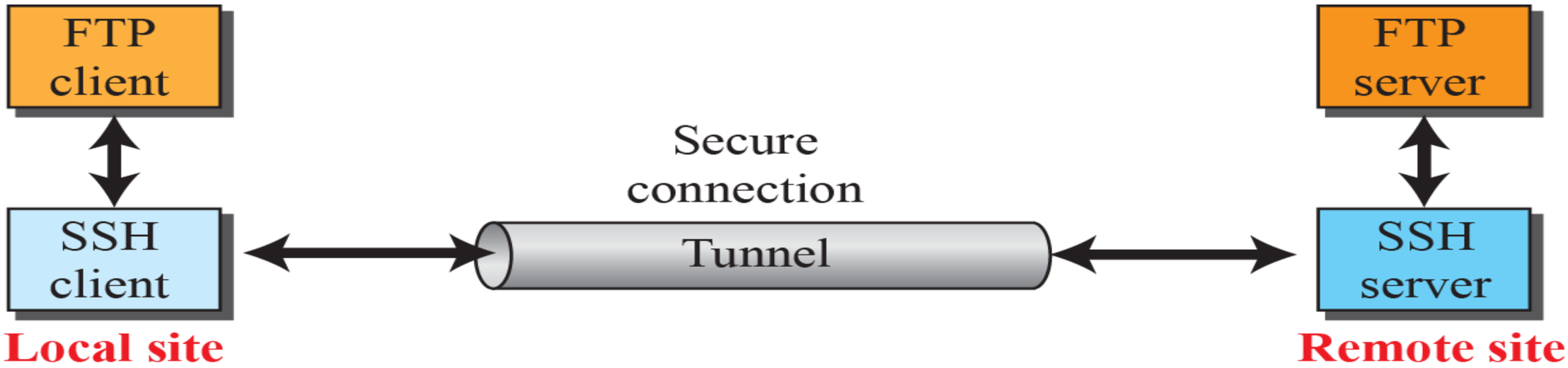
- ✓ SSH is an application-layer protocol with three components
- ✓ (SSH-CONN): SSH Connection Protocol. It allows to run multiple channels over the secure connection established.
- ✓ (SSH-AUTH): SSH Authentication Protocol. It is the component of SSH which allows to authenticate the SSH client for the server.
- ✓ (SSH-TRANS): SSH Transport-Layer Protocol. It allows to establish a secure connection between SSH client and SSH server over TCP.



Port Forwarding

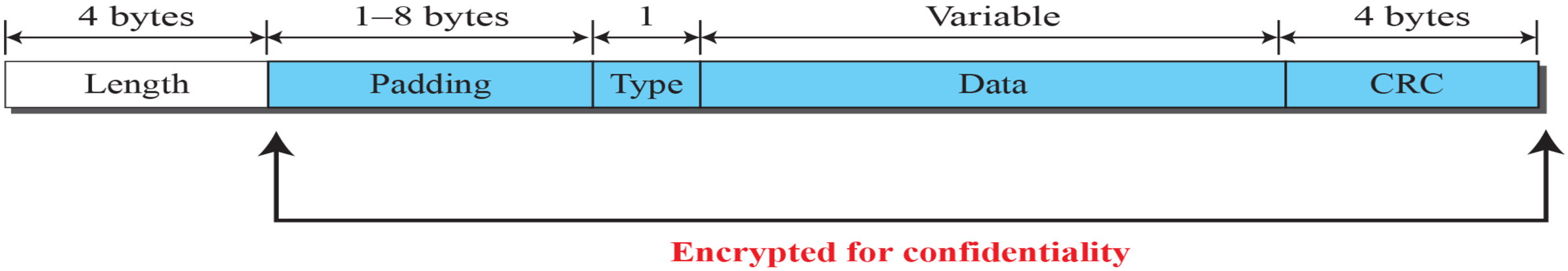
The SSH port forwarding mechanism creates a tunnel through which the messages belonging to other protocols can travel. For this reason, this mechanism is sometimes referred to as SSH tunneling.

We can use the secured channels to access an application program that does not provide security services.



SSH Packet Format

- ✓ The length field defines the length of the packet but does not include the padding.
- ✓ One to eight bytes of padding is added to the packet to make the attack on the security provision more difficult.
- ✓ The CRC field is used for error detection. The type field designates the type of the packet used in different SSH protocols.
- ✓ The data field is the data transferred by the packet in different protocols.



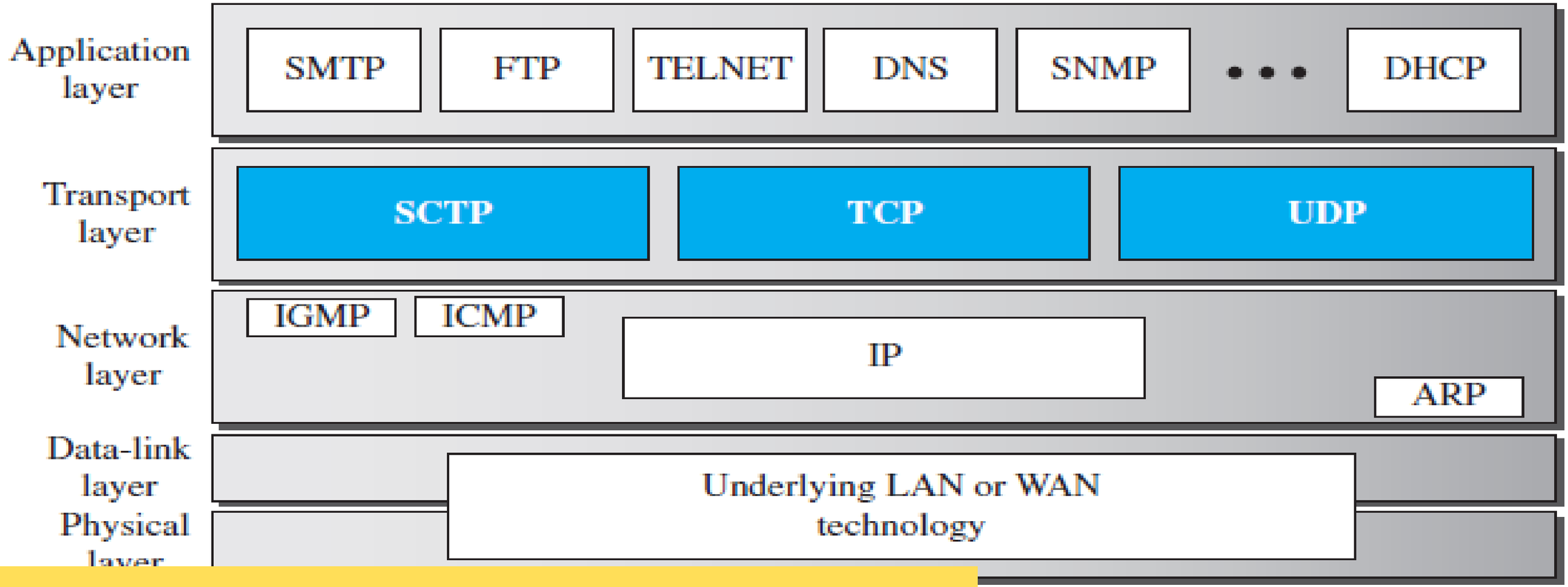
Applications:

- ✓ Once the secure connection is established between SSH client and SSH server, SSH allows different application programs to use the established secure connection.
- ✓ Remote console login, SFTP (Secure File Transfer Protocol) etc., are the examples of different applications.

Difference between SSH and Telnet

- ✓ Telnet was the first internet application protocol used to create and maintain a terminal session on a remote host.
- ✓ Both SSH and Telnet have the same functionality. Still, the main difference is that SSH protocol is secured with public-key cryptography that authenticates endpoint while setting up a terminal session.
- ✓ SSH sends the encrypted data, while Telnet sends data in plain text.
- ✓ Due to high security, SSH is the preferred protocol for public networks, while due to less security, Telnet is suitable for private networks.
- ✓ SSH runs on port no 22 by default, but it can be changed, while Telnet uses port number 23, specifically designed for the Local area network.

Figure 24.1 *Position of transport-layer protocols in the TCP/IP protocol suite*



Assessment

a) List types of SSH.
 b) What is SSH?
c) What is the application of SSH?

Reference

TEXT BOOKS

Behrouz A. Forouzan, Data Communications and Networking, Fifth Edition TMH, 2013.

REFERENCES

1. William Stallings, Data and Computer Communications, Tenth Edition, Pearson Education, 2013.
2. Andrew Tanenbaum, Computer Networks, Fifth Edition, Pearson (5th Edition) Education, 2013.
3. James F. Kurose, Keith W. Ross, Computer Networking, A Top-Down Approach Featuring the Internet, Sixth Edition, Pearson Education, 2013.
4. Larry L. Peterson, Bruce S. Davie, Computer Networks: A Systems Approach, Fifth Edition, Morgan Kaufmann Publishers Inc., 2012.