

אפשר לסווג רשתות לפי קריטריונים שונים. נעבור על חלק מהם:

(1) מערכות ריכוזיות (Centralized Systems). זאת גישה שנחשבת היום כגישה מיושנת, אם כי ישנן עדיין רשתות שפועלות לפי השקפה זאת: מחשב מרכזי מעבד את הנתונים שמועברים אליו **ממסופים (Terminals)**. המסופ הוא התקן שתפקידו לקלוט נתונים ולשדר אותם למחשב המרכזי, ולקבל מהמחשב המרכזי נתונים ולהציג אותם. כמעט אין עיבוד נתונים במסופים, רק פעולות קלט ופלט. החסרון של השיטה הזאת: זאת רשת שקשה להרחיב אותה בעתיד (כל הרחבה דורשת שינויים בתוכנה ובחומרה במחשב המרכזי. בנוסף: כל הרחבה בעתיד מחייבת התקשרות עם אותו יצרן. כמעט בלתי אפשרית התקשרות עם יצרנים נוספים בגלל הסכנה של אי-התאמה בחומרה או בתוכנה.

(2) מערכות פתוחות (Open Systems). זאת הגישה החדשה יותר, שמטרתה לאפשר הרחבה כמעט בלתי מוגבלת בעתיד. הרחבה תתאפשר בצורה פשוטה ככל האפשר, ללא שינוי כמעט בציווד (חומרה, תוכנה) במחשבים אחרים. האינדאל הוא שכל מחשב חדש שמצטרף – אינו תלוי בכלל בחומרה או בתוכנה של האחרים, יש התאמה בין כולם למרות היצרנים השונים של התוכנות והציווד האחר ברשת. כל ציווד (חומרה או תוכנה) פועל על פי תקנים (Standards) של היצרן, לכן נדרשת כאן התאמה בין מספר עצום של תקנים שונים, עקב מספר הגדול של היצרנים.

(1) רשת מקומית (Local Area Network-LAN). בדרך כלל זו רשת קטנה יחסית (אם כי ישנן רשתות LAN ענקיות, כלל עולמיות כמו רשתות של חברות ענק כגון General Boeing וכדומה). כלומר, אי אפשר לזהות LAN רק על פי גודלו. היחוד ברשתות המקומיות הוא בכך שבכל רשת כזאת יש הנהלה שקובעת כללים לכל המשתמשים האחרים, למשל שימוש במחשבים אחידים, הקפדה רבה על תקנים אחידים בכל מרכיבי הציווד (תוכנה וחומרה). לכן רשת LAN מאופיינת בכך שיש אחידות בציווד, הקפדה על תקנים בכל פרטיהם. יצרן הציווד ברשת הוא יחיד בדרך כלל, לכן אין בעיות של התאמה בין מרכיבי הרשת. ההנהלה משקיעה כסף רב בהקמת LAN ולכן בדרך כלל רשתות LAN מאופיינת על-ידי תקשורת מאד איכותית (כבלים מעולים, קצבי תקשורת גבוהים מאד וכדומה).

(2) רשת מרחבית (Wide Area Network-WAN). בדרך כלל זו רשת גדולה, כן במספר המחשבים וכן בפריסתה הגיאוגרפית. המאפיין ברשת WAN הוא שאין הנהלה מרכזית שקובעת כללים קשוחים לכל המשתמשים. יש מגוון רב של סוגי מחשבים וציווד אחר (כגון תוכנות תקשורת, סוגי כבלים, סוגי מרכזיות). דוגמה טיפוסית של רשת WAN: רשת האינטרנט.

בדרך כלל, ברשת WAN נעשה שימוש גם ברשת הטלפוניה למטרות של תקשורת נתונים. רשת הטלפוניה: כבר קיימת ובעלת פריסה צפופה על פני כל כדור הארץ, אבל מאד לא מתאימה לתקשורת מחשבים עקב קצבי התקשורת הנמוכים שהיא מאפשרת.

לסיכום: ברשת WAN יש מגוון עצום של ציווד (חומרה, תוכנה, סוגי תווך, מרכזיות תקשורת) הפועלים על פי תקנים רבים מאד. עקב חוסר האחידות בתקנים, יש בעיות של התאמת ציווד, במידה הרבה יותר גדולה מאשר ברשת LAN.

1) רשת הפצה (Broadcast Network). זאת רשת שבה יש שיטת תקשורת שבה מחשב אחד "מדבר" (משדר מידע), וכל המחשבים האחרים יכולים לקלוט את המידע הזה (אם רצונך בכך). שיטה זאת נהוגה בדרך כלל ברשתות מסוג LAN.

2) רשת נל"ן (מנקודה לנקודה) (Point to Point Network). זאת רשת שבה יש שיטת ניתוב (Routing) של המידע מהמקור אל היעד בלבד. שיטה זאת נהוגה בדרך כלל ברשתות מסוג WAN.

1) רשת פס-בסיס (Baseband). ברשת כזאת, המידע מועבר בין המחשבים בצורה ספרתית ישירות (בצורת אות ריבועי, ללא איפנון - Modulation). העברת המידע בצורה כזאת (ללא איפנון) אפשרית רק אם מדובר בכבלים קצרים (עשרות מטרים בלבד) וגם זאת רק עם הכבלים מעולים, בעלי רוחב סרט גדול (כדי שהאותות הריבועיים יעברו ללא עיוותים גדולים). כלומר שיטת פס-בסיס אפשרית רק ברשתות LAN קטנות.

2) רשת פס-רחב (Broadband). ברשת כזאת, המידע הספרתי מאופקן (בעזרת מודם) לפני שידורו בקו התקשורת. המידע עובר בצורה מאופנת וכאשר מגיע ליעד מתבצעת פעולת גילוי (Demodulation) בעזרת המודם של מחשב היעד. שיטת פס-בסיס הכרחית עם מדובר ברשת עם כבלים ארוכים, ו/או כאשר מדובר בכבלים לא איכותיים, בעלי רוחב צר (כגון כבלים רבים ברשת הטלפוניה). כלומר שיטת פס-רחב נפוצה ברשתות WAN.

סוגי מרכזיות תקשוב.

1) לפי שיטת מיתוג מעגלים (Circuit Switching). זאת שיטה דומה לזו הנהוגה ברשתות טלפוניה: המרכזיה מנסה ליצור קשר פיזי ישיר בין שני המתקשרים. חסרונות השיטה:

- שני הצדדים צריכים להיות מוכנים לתקשורת באותו זמן.

- כאשר נוצר הקשר, התשדורת תועבר בקצב של המחשב האיטי יותר.

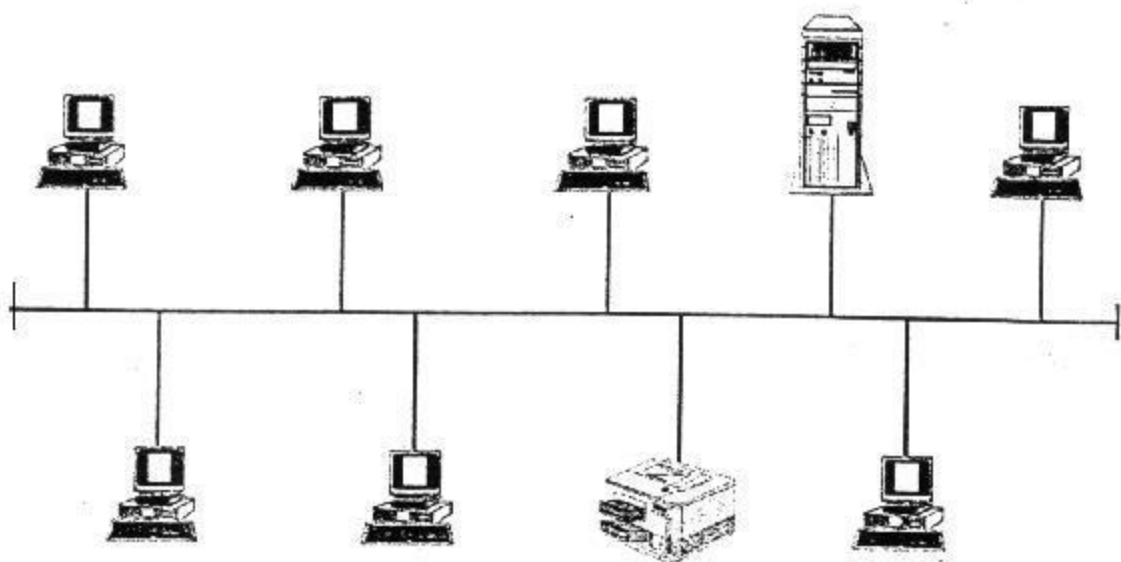
2) לפי שיטת מיתוג הודעות (Message Switching). כאן יש זכרון במרכזיה והיא מקציבה זכרון לכל מנוי שלה. כאשר מנוי מתקשר, המרכזיה קולטת את כל ההודעה והלקוח סיים את תפקידו. תפקיד המרכזיה לשדר את ההודעה אל המרכזיה של לקוח היעד. המרכזיה ביעד מאחסנת את ההודעה בתא זכרון שמיועד ללקוח היעד. לפי שיטה זאת פועל הדואר האלקטרוני (E-Mail). המגבלה: אם יש הודעות ארוכות מאד ש"מעסיקות" את המרכזיה ואת הכבלים המשותפים במשך זמן ארוך, הלקוחות "הקטנים" מקופחים בקבלת שרות.

3) לפי שיטת החלוקה למנות (Packet Switching). לפי שיטה זאת, המרכזיה הראשונה שקולטת את ההודעה-מחלקת אותה למנות (Packets). כל מנה מקבלת תוספות (קידומות וסיומות שמציינים: כתובת השולח, כתובת היעד, מיספור המנה בתוך התשדורת, תווי בקרה לצורך גילוי טעויות תקשורת וכו'). המרכזיה משדרת את המנות של משתמשים רבים לסירוגין (לא משדרת את ההודעה של לקוח יחיד ברצף). בצורה כזאת – כל משתמש מקבל שרות שוויוני יותר. זאת השיטה הנפוצה והמקובלת ביותר באינטרנט, למשל.

טופולוגיות ברשתות LAN של אתרנט.

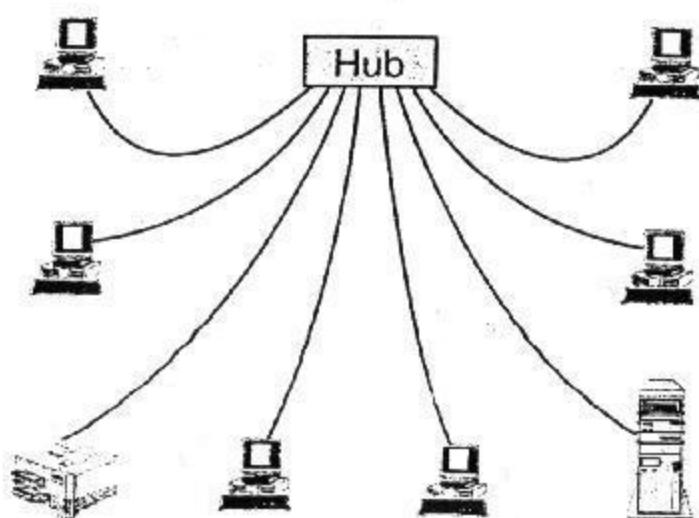
א) רשת אפיק משותף (Common Bus).

ההודעות מועברות לאורך אפיק שידרה יחיד שמקשר בין המחשבים. בכל קצה של האפיק המשותף נמצא נגד סיום (Terminator). טופולוגיה זאת מקובלת בחלק מרשתות אתרנט (Ethernet).

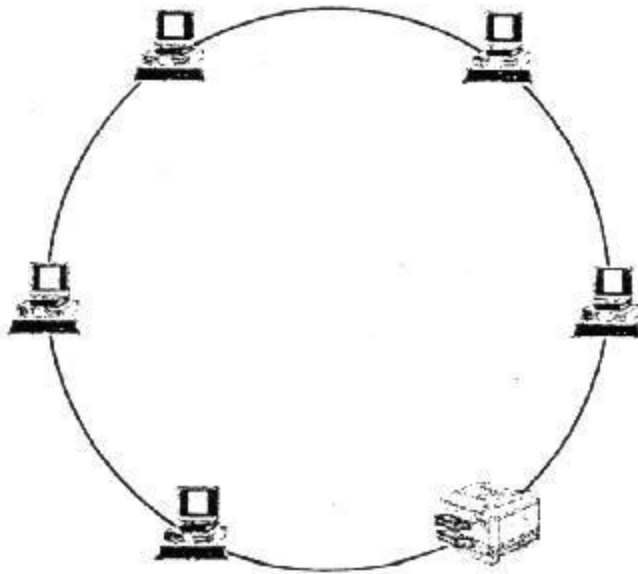


ב) רשת כוכב (Star Network).

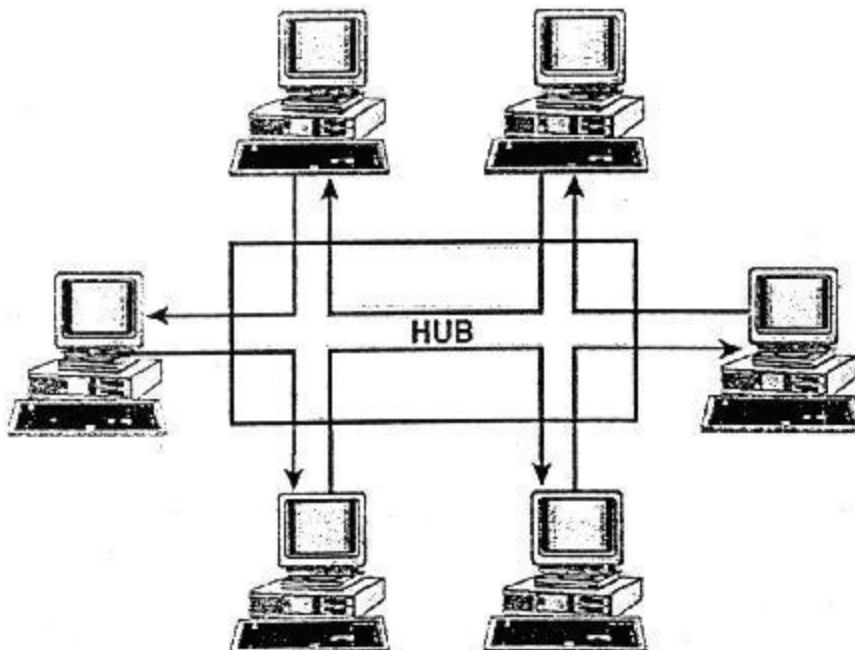
ברשת כוכב ישנה רכזת (Hub) לקישור כל המחשבים ברשת. טופולוגיה זאת מקובלת בחלק מרשתות אתרנט (Ethernet).



ג) רשתות טבעת אסימטרית של IBM (Token Ring).
המידע בין המחשבים מועבר בטבעת רציפה.



ד) רשת טבעתית עם קופסת חיבורים מרכזית (Wires Center).



שיטות קידוד (הצפנה) של מידע.

רוב הציוד (מודמים, טלפונים) מחוברים לרשת באמצעות שנאי צימוד לצורך תאומי עכבות (אם אין תאום עכבות - יהיו החזרות של מידע בצמתים הלא-מתואמים). תאום העבות הכרחי מבחינה טכנית, אבל יוצר בעיות אחרות: שנאי הצימוד אינם מעבירים מתח ישר אלא שינויי מתח בלבד. אם במידע ישנן סיביות "1" רבות רצופות, הן יוצרות מתח קבוע בקו, מתח שלא יעבור את שנאי הצימוד ללא עיוות ניכר. כדי לאפשר העברת המידע (גם אם ישנם רצפים ארוכים של סיביות "1"), נוקטים במספר שיטות:

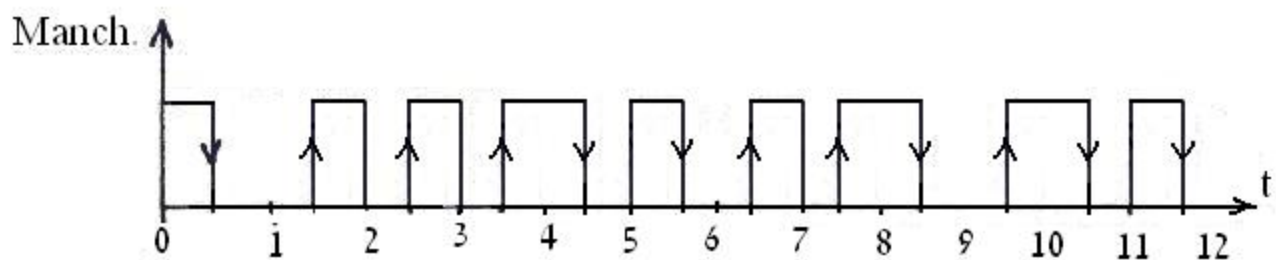
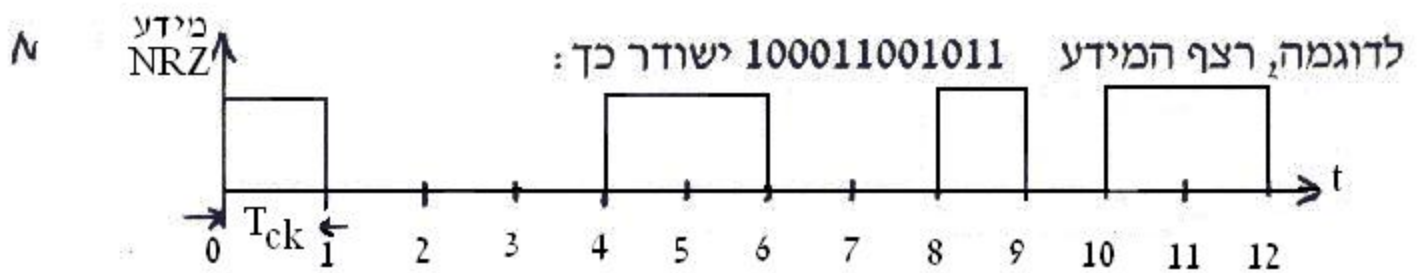
1) שיטת "השחלת האפסים" ("0" bit insertion)

תקן HDLC קובע, בין השאר, את שיטת השחלת האפסים: אחרי כל 5 סיביות "1" רצופות, "מושחלת" סיבית "0" ללא קשר למידע עצמו. הצד המשדר משחיל את סיביות ה-"0", הצד הקולט מודע לכך ומסיר אותן מהמידע שקיבל.

2) שיטות קידוד לאילוץ שינויים תכופים באות המשודר. נזכיר כאן רק שתיים משיטות הקידוד הנ"ל:

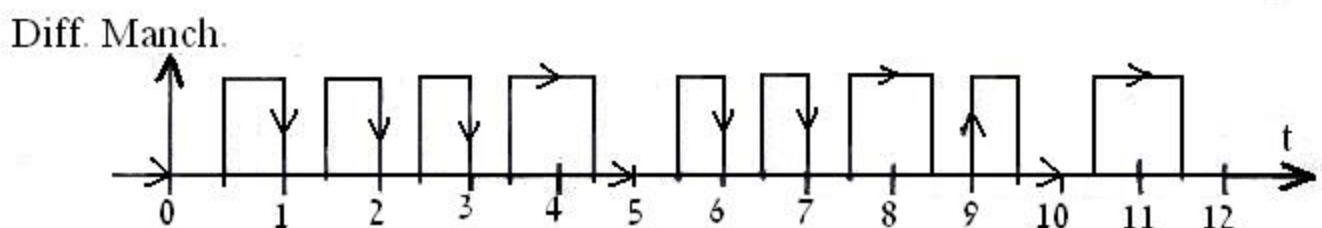
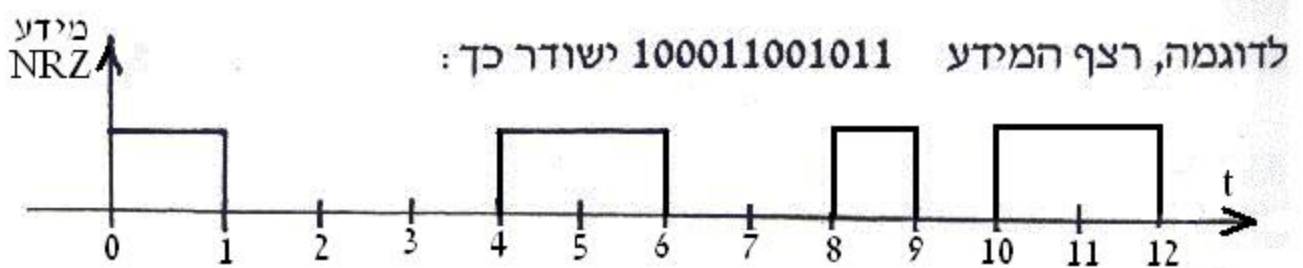
קידוד בשיטת מנצסטר (Manchester).

השיטה הזאת חשובה כי היא אומצה ברשתות אתרנט (תקן IEEE 802.3).



קידוד בשיטת מנצסטר הפרשי (Differential Manchester).

השיטה הזאת אומצה ברשתות טבעת אסימטריות (תקן IEEE 802.5).





Chapter Goals

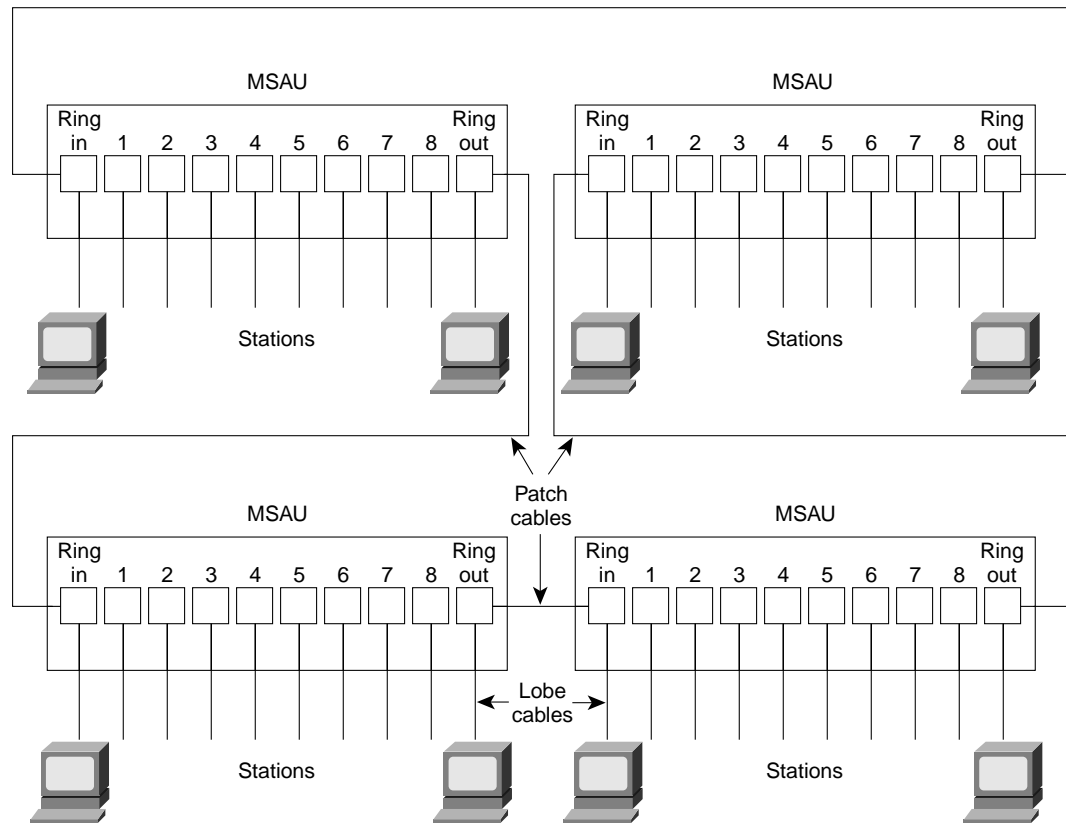
- Describe the background of Token Ring technology.
- Explain how Token Ring works.

Token Ring/IEEE 802.5

The Token Ring network was originally developed by IBM in the 1970s. It is still IBM's primary local-area network (LAN) technology. The related IEEE 802.5 specification is almost identical to and completely compatible with IBM's Token Ring network. In fact, the IEEE 802.5 specification was modeled after IBM Token Ring, and it continues to shadow IBM's Token Ring development. The term *Token Ring* generally is used to refer to both IBM's Token Ring network and IEEE 802.5 networks. This chapter addresses both Token Ring and IEEE 802.5.

Token Ring and IEEE 802.5 networks are basically compatible, although the specifications differ in minor ways. IBM's Token Ring network specifies a star, with all end stations attached to a device called a multistation access unit (MSAU). In contrast, IEEE 802.5 does not specify a topology, although virtually all IEEE 802.5 implementations are based on a star. Other differences exist, including media type (IEEE 802.5 does not specify a media type, although IBM Token Ring networks use twisted-pair wire) and routing information field size. Figure 9-1 summarizes IBM Token Ring network and IEEE 802.5 specifications.

Figure 9-2 MSAUs Can Be Wired Together to Form One Large Ring in an IBM Token Ring Network



Token Ring Operation

Token Ring and IEEE 802.5 are two principal examples of token-passing networks (FDDI is the other). *Token-passing networks* move a small frame, called a token, around the network. Possession of the token grants the right to transmit. If a node receiving the token has no information to send, it passes the token to the next end station. Each station can hold the token for a maximum period of time.

If a station possessing the token does have information to transmit, it seizes the token, alters 1 bit of the token (which turns the token into a start-of-frame sequence), appends the information that it wants to transmit, and sends this information to the next station on the ring. While the information frame is circling the ring, no token is on the network (unless the ring supports early token release), which means that other stations wanting to transmit must wait. Therefore, collisions cannot occur in Token Ring networks. If early token release is supported, a new token can be released when frame transmission is complete.

The information frame circulates the ring until it reaches the intended destination station, which copies the information for further processing. The information frame continues to circle the ring and is finally removed when it reaches the sending station. The sending station can check the returning frame to see whether the frame was seen and subsequently copied by the destination.

Unlike CSMA/CD networks (such as Ethernet), token-passing networks are *deterministic*, which means that it is possible to calculate the maximum time that will pass before any end station will be capable of transmitting. This feature and several reliability features, which are discussed in the section



Chapter Goals

- Provide background information about FDDI technology.
- Explain how FDDI works.
- Describe the differences between FDDI and Copper Distributed Data Interface (CDDI).
- Describe how CDDI works.

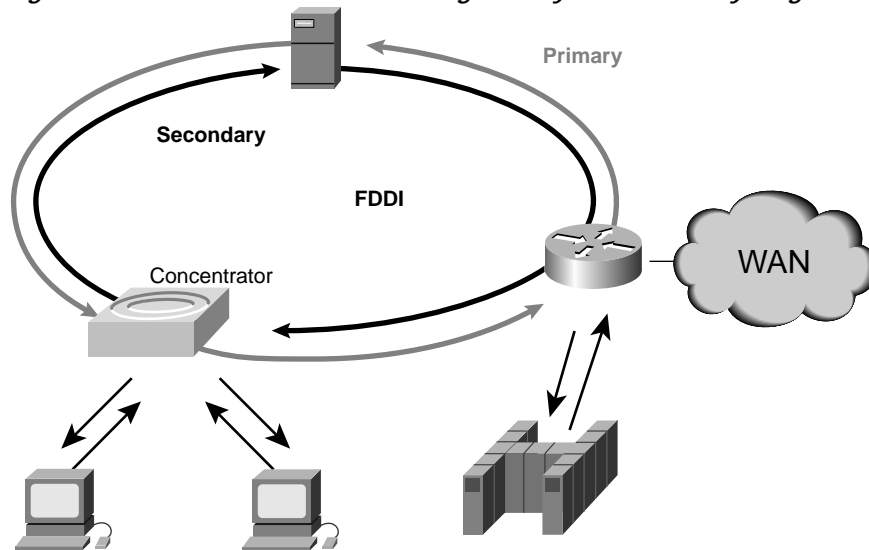
Fiber Distributed Data Interface

Introduction

The *Fiber Distributed Data Interface (FDDI)* specifies a 100-Mbps token-passing, dual-ring LAN using fiber-optic cable. FDDI is frequently used as high-speed backbone technology because of its support for high bandwidth and greater distances than copper. It should be noted that relatively recently, a related copper specification, called Copper Distributed Data Interface (CDDI), has emerged to provide 100-Mbps service over copper. CDDI is the implementation of FDDI protocols over twisted-pair copper wire. This chapter focuses mainly on FDDI specifications and operations, but it also provides a high-level overview of CDDI.

FDDI uses dual-ring architecture with traffic on each ring flowing in opposite directions (called counter-rotating). The dual rings consist of a primary and a secondary ring. During normal operation, the primary ring is used for data transmission, and the secondary ring remains idle. As will be discussed in detail later in this chapter, the primary purpose of the dual rings is to provide superior reliability and robustness. Figure 8-1 shows the counter-rotating primary and secondary FDDI rings.

Figure 8-1 FDDI Uses Counter-Rotating Primary and Secondary Rings



Standards

FDDI was developed by the American National Standards Institute (ANSI) X3T9.5 standards committee in the mid-1980s. At the time, high-speed engineering workstations were beginning to tax the bandwidth of existing local-area networks (LANs) based on Ethernet and Token Ring. A new LAN media was needed that could easily support these workstations and their new distributed applications. At the same time, network reliability had become an increasingly important issue as system managers migrated mission-critical applications from large computers to networks. FDDI was developed to fill these needs. After completing the FDDI specification, ANSI submitted FDDI to the International Organization for Standardization (ISO), which created an international version of FDDI that is completely compatible with the ANSI standard version.

FDDI Transmission Media

FDDI uses optical fiber as the primary transmission medium, but it also can run over copper cabling. As mentioned earlier, FDDI over copper is referred to as *Copper-Distributed Data Interface (CDDI)*. Optical fiber has several advantages over copper media. In particular, security, reliability, and performance all are enhanced with optical fiber media because fiber does not emit electrical signals. A physical medium that does emit electrical signals (copper) can be tapped and therefore would permit unauthorized access to the data that is transiting the medium. In addition, fiber is immune to electrical interference from radio frequency interference (RFI) and electromagnetic interference (EMI). Fiber historically has supported much higher bandwidth (throughput potential) than copper, although recent technological advances have made copper capable of transmitting at 100 Mbps. Finally, FDDI allows 2 km between stations using multimode fiber, and even longer distances using a single mode.

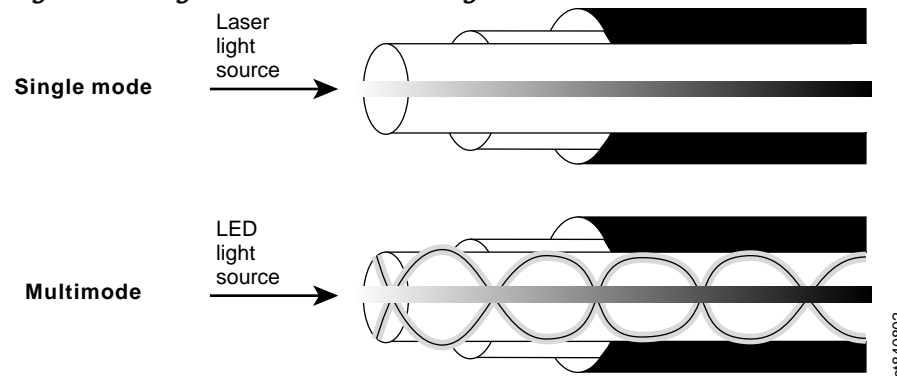
FDDI defines two types of optical fiber: single-mode and multimode. A *mode* is a ray of light that enters the fiber at a particular angle. *Multimode* fiber uses LED as the light-generating device, while *single-mode* fiber generally uses lasers.

Multimode fiber allows multiple modes of light to propagate through the fiber. Because these modes of light enter the fiber at different angles, they will arrive at the end of the fiber at different times. This characteristic is known as *modal dispersion*. Modal dispersion limits the bandwidth and distances that can be accomplished using multimode fibers. For this reason, multimode fiber is generally used for connectivity within a building or a relatively geographically contained environment.

Single-mode fiber allows only one mode of light to propagate through the fiber. Because only a single mode of light is used, modal dispersion is not present with single-mode fiber. Therefore, single-mode fiber is capable of delivering considerably higher performance connectivity over much larger distances, which is why it generally is used for connectivity between buildings and within environments that are more geographically dispersed.

Figure 8-2 depicts single-mode fiber using a laser light source and multimode fiber using a light emitting diode (LED) light source.

Figure 8-2 Light Sources Differ for Single-Mode and Multimode Fibers



FDDI Specifications

FDDI specifies the physical and media-access portions of the OSI reference model. FDDI is not actually a single specification, but it is a collection of four separate specifications, each with a specific function. Combined, these specifications have the capability to provide high-speed connectivity between upper-layer protocols such as TCP/IP and IPX, and media such as fiber-optic cabling.

FDDI's four specifications are the Media Access Control (MAC), Physical Layer Protocol (PHY), Physical-Medium Dependent (PMD), and Station Management (SMT) specifications. The *MAC* specification defines how the medium is accessed, including frame format, token handling, addressing, algorithms for calculating cyclic redundancy check (CRC) value, and error-recovery mechanisms. The *PHY* specification defines data encoding/decoding procedures, clocking requirements, and framing, among other functions. The *PMD* specification defines the characteristics of the transmission medium, including fiber-optic links, power levels, bit-error rates, optical components, and connectors. The *SMT* specification defines FDDI station configuration, ring configuration, and ring control features, including station insertion and removal, initialization, fault isolation and recovery, scheduling, and statistics collection.

FDDI is similar to IEEE 802.3 Ethernet and IEEE 802.5 Token Ring in its relationship with the OSI model. Its primary purpose is to provide connectivity between upper OSI layers of common protocols and the media used to connect network devices. Figure 8-3 illustrates the four FDDI specifications and their relationship to each other and to the IEEE-defined Logical Link Control (LLC) sublayer. The LLC sublayer is a component of Layer 2, the MAC layer, of the OSI reference model.

ארכיטקטורה של רשתות תקשורת

זהו כל המידע הדרוש למימוש הרשת (חומרה או תוכנה).

עקב המורכבות הרבה של רשתות – פיתחו מודלים של

ארכיטקטורה לפי שכבות (Layers) או רמות (Levels).

אוסף החוקים והמוסכמות שלפיהם מתנהלת שיחה בין

שתי שכבות ברמה N של שתי תחנות – נקרא בשם:

פרוטוקול של השכבה ה- N (N-layer protocol).

אוסף הפרוטוקולים (פרוטוקול אחד לכל שכבה) מכונה

בשם: מחסנית פרוטוקולים (Protocol Stack).

בין כל שתי שכבות סמוכות מצוי ממשק (Interface).

הממשק מגדיר את הפעולות הבסיסיות ואת השרותים

ששכבה אחת מציעה לשכבה השכנה במודל

מהלך OSI של ISO.

המודל של מערכת תקשורת פתוחה OSI – Open System Interconnection – פותח על-ידי ארגון התקינה הבינלאומי ISO – International Standards Org. המודל נקרא "מערכת פתוחה" כי הוא תוכנן לאפשר תקשורת בין מערכות שונות, מתוצרת יצרני חומרה ותוכנה שונים.
מודל OSI כולל שבע רמות (Levels) או שכבות (Layers).

שכבת היישום (Application Layer): בשכבה הזאת נמצאות התוכנות המופעלות ע"י המשתמש (דו-שיח בין המשתמש לבין המערכת).

שכבת התצוגה (Presentation): בשכבה הזאת מתרגמים את הנתונים לפורמט מוכר למחשב מסויים, או מצפינים ומפענחים את המידע, או דוחסים ופורסים מידע

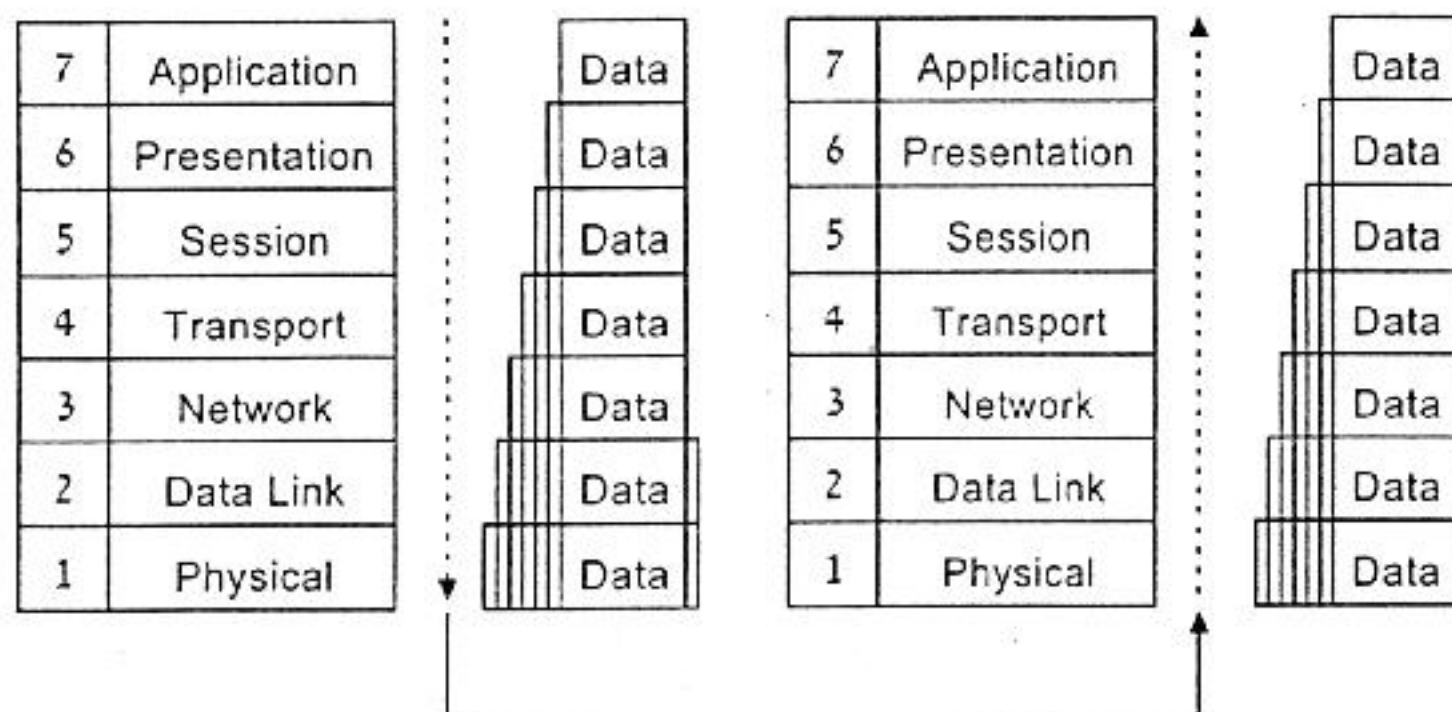
שכבת השיחה או המושב (Session): אחראית לפתיחת השיחה וסגירתה וכן להוספת נקודות בדיקה ובקורת בתוך המידע.

שכבת התעבורה (Transport): אחראית לחלוקת הנתונים למנות (Packets), מספור המנות בתשדורת, הוספת שדות כתובת השולח וכתובת היעד ועוד.

שכבת הרשת (Network): אחראית לניתוב (Routing) של המידע, מהמקור אל היעד לפי מסלול אופטימלי. כדי להשיג ניתוב אופטימלי, זקוקים להתקנים שנקראים נתבים (Routers) שפועלים בשכבת הרשת של המודל.

שכבת קישור הנתונים או שכבת הערוץ או האפיק (Data Link): בשכבה הזאת המנות נארזות למסגרות (Frames) ומבוצעים אלגוריתמים של גילוי טעויות ותיקונם. בשכבת קישור הנתונים פועלים התקנים שנקראים גשרים (Bridges).

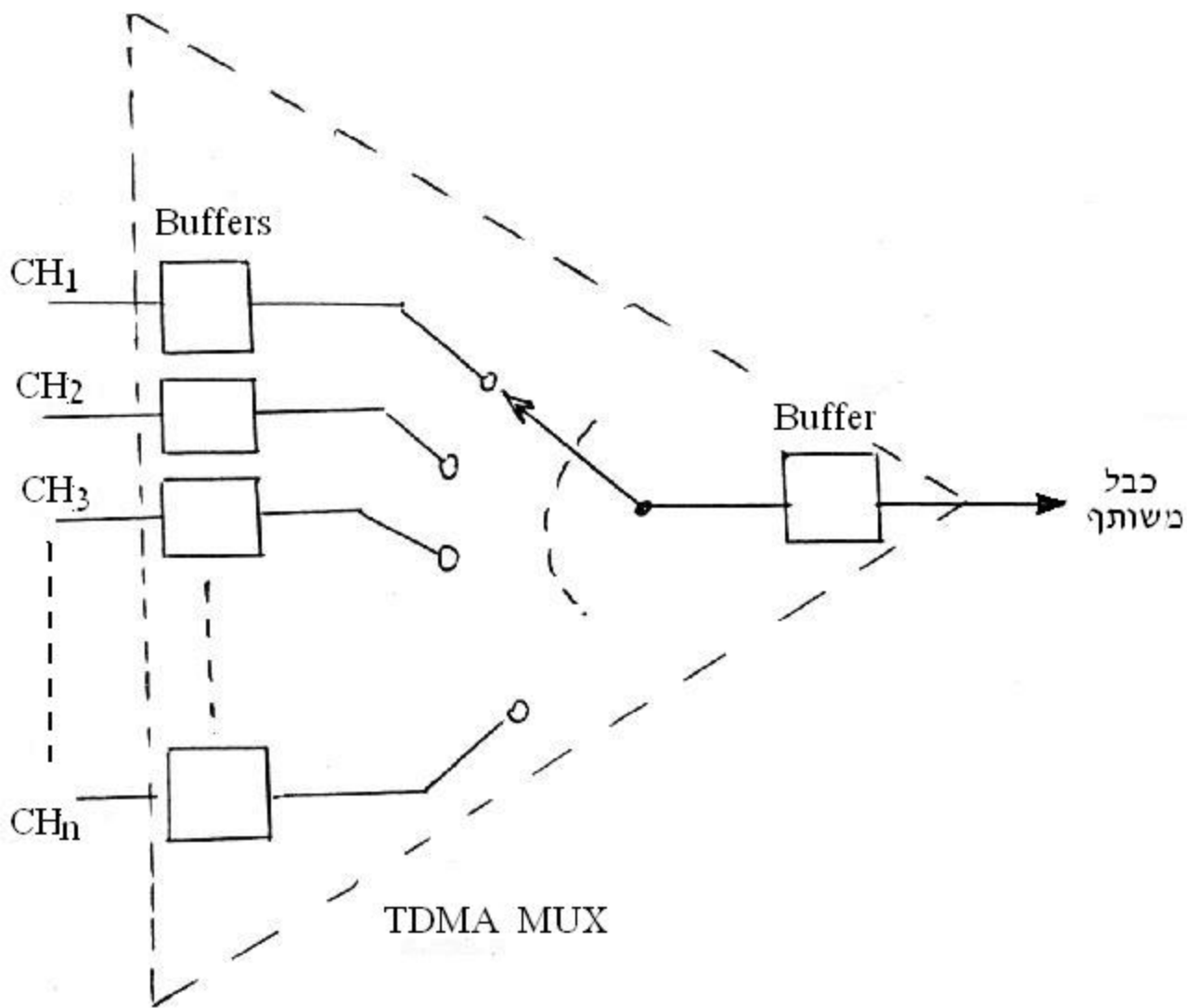
שכבה הפיזית (Physical): לשכבה זאת שייכת הטופולוגיה של הרשת, סוג התווך (Media) שדרכו מועבר המידע, הטיפול באותות החשמליים עצמם (רמות לוגיות, טיפול ברעשים חשמליים, קצב תקשורת ועוד). בשכבה הפיזית פועלים התקנים כגון: משחזרים (Repeaters), יחידות שידור וקליטה (Transceivers) ועוד.



בשיטת ריבוב TDM (ריבוב בחלוקת זמן, Time Division Multiplexing).

לכל מנוי מוקצב "חריץ זמן" (Time Slot) בתוך מסגרת TDM.

המרבב דוגם כל ערוץ במשך חריץ זמן קבוע, יוצר מסגרת TDM ומשדר אותה אל הצד השני. בצד הקולט, המסגרת מפורקת למרכיביה וכל חריץ מידע מופנה אל יעדו.



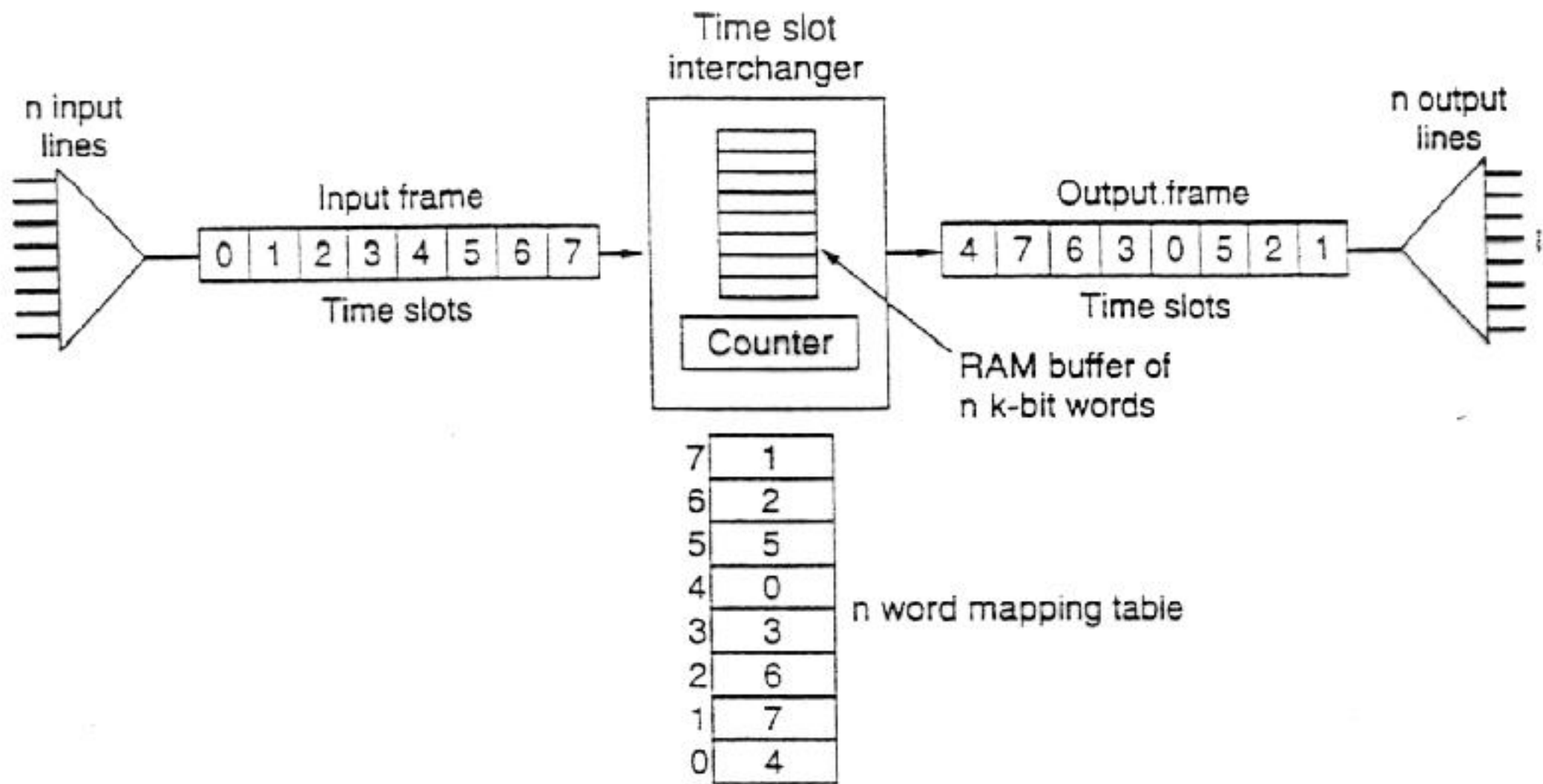


Fig. 2-40. A time division switch.

Connectivity.

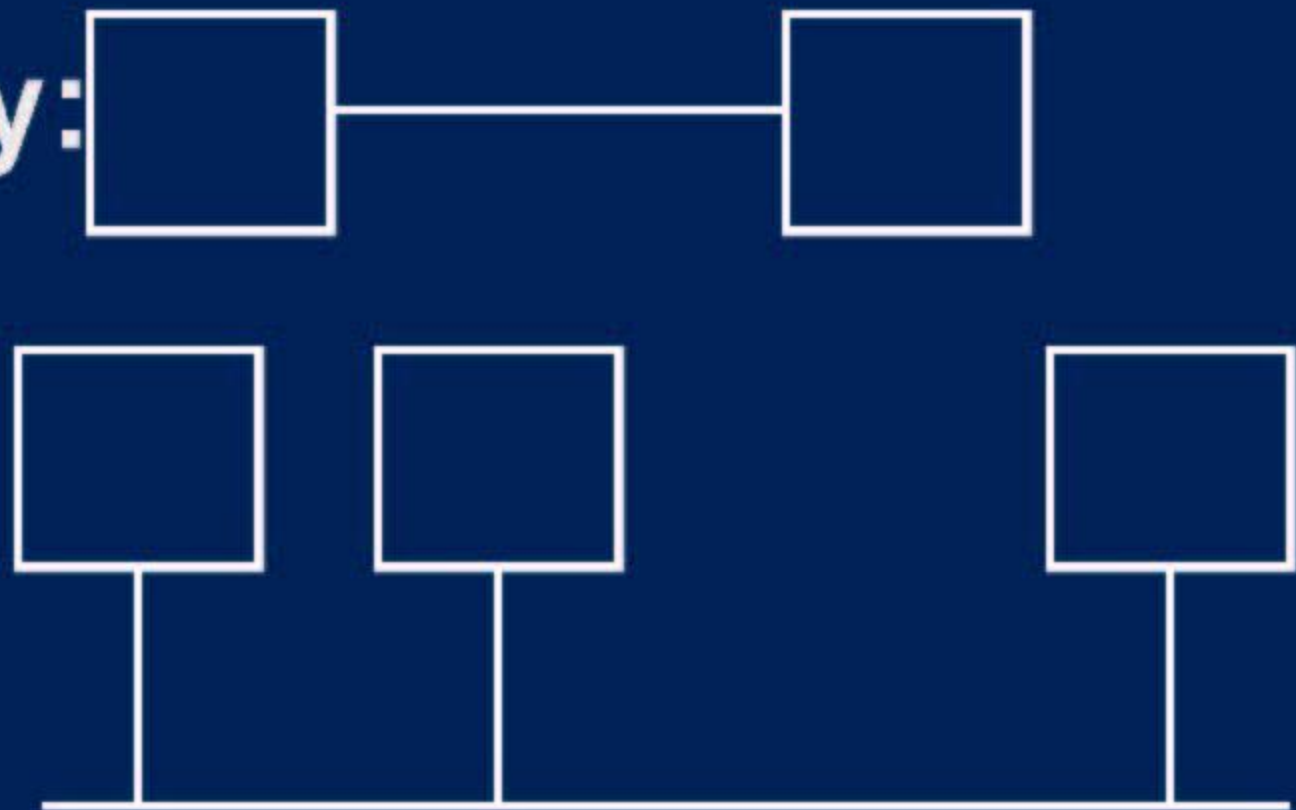
- **Building Blocks**

- links: coax cable, optical fiber...
- nodes: general-purpose workstations...

- **Direct connectivity:**

- point-to-point

- multiple access



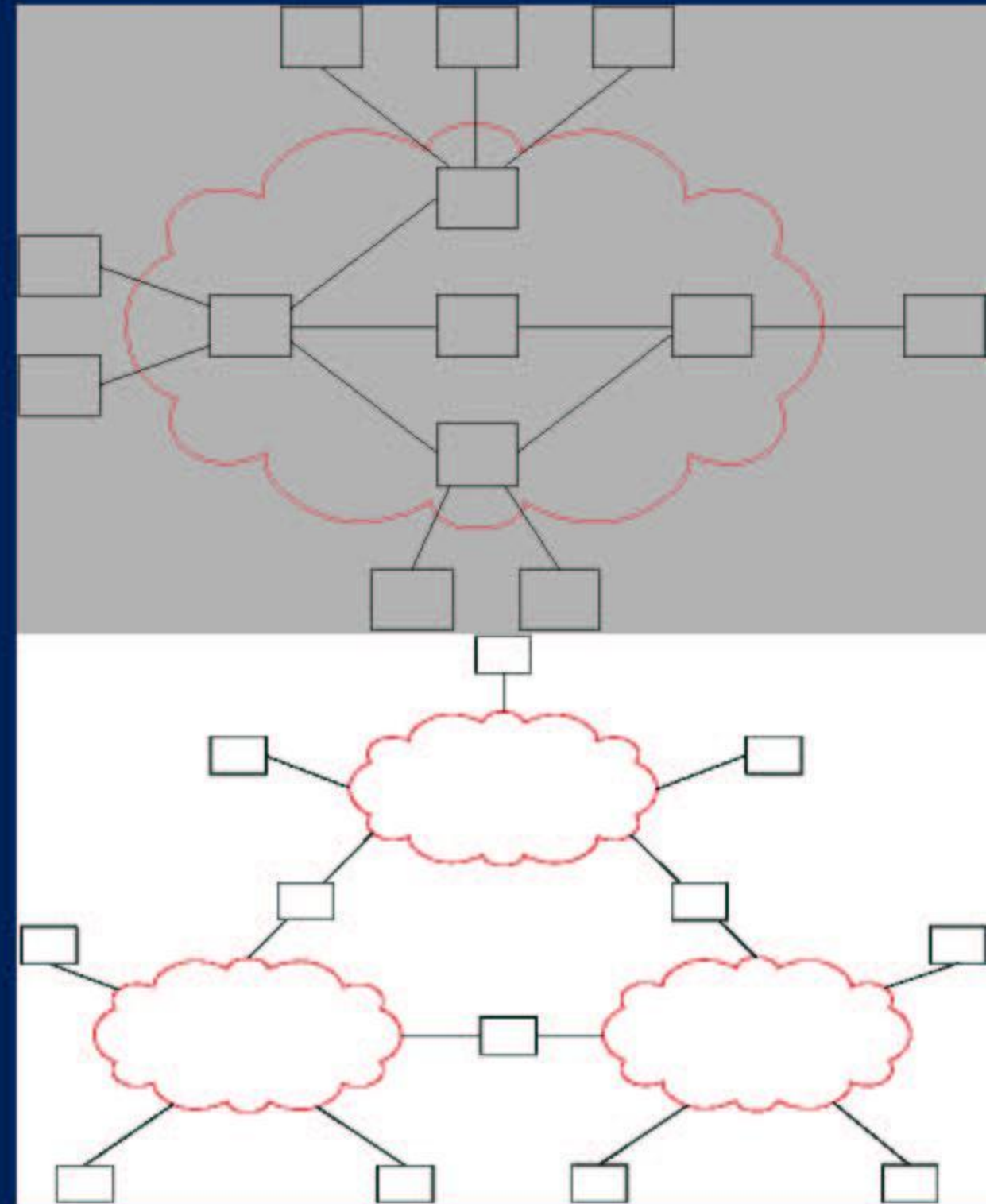
Connectivity..

- **Indirect Connectivity**
 - switched networks

=> switches

- inter-networks

=> routers



Connecting **N** users: *Directly* ...

- *Bus*: broadcast, collisions, media access control
- *Full mesh*: Cost vs simplicity



Bus



Full mesh

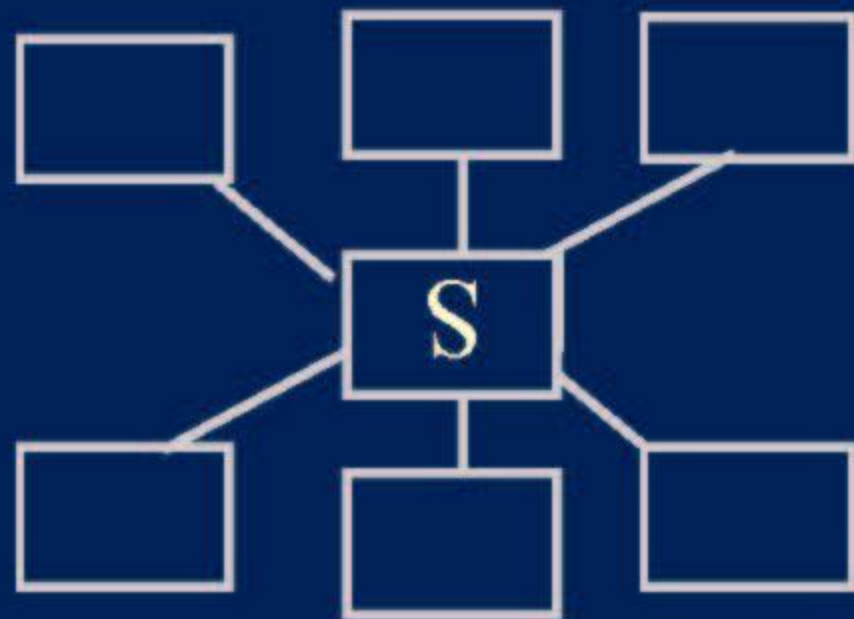
- Address concept needed if we want the receiver *alone* to consume the packet!

List of Problems

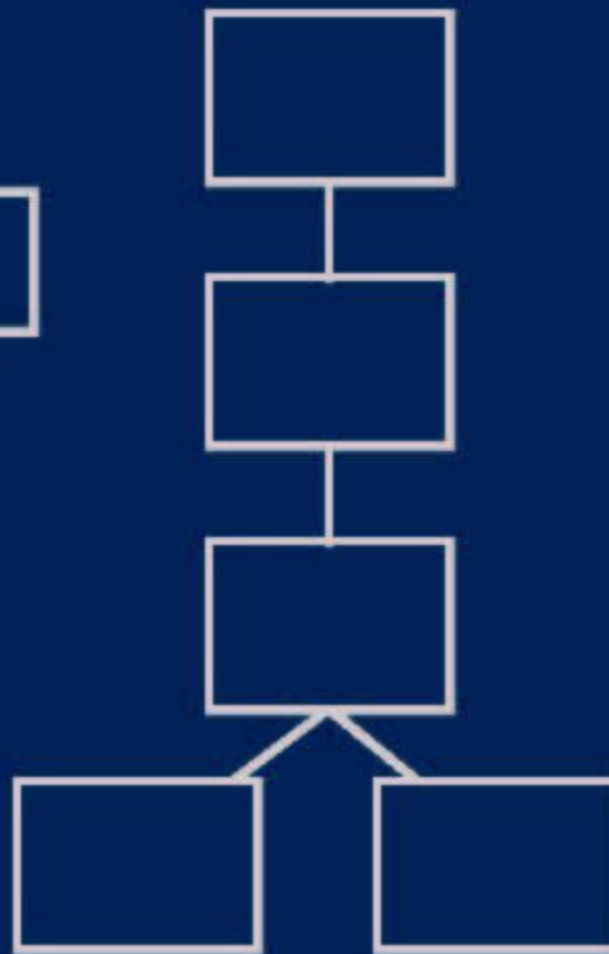
- **Topologies**
- **Framing**
- **Error control**
- **Flow control**
- **Multiple access**
 - **How to share a wire**



Topologies: Indirect Connectivity



Star

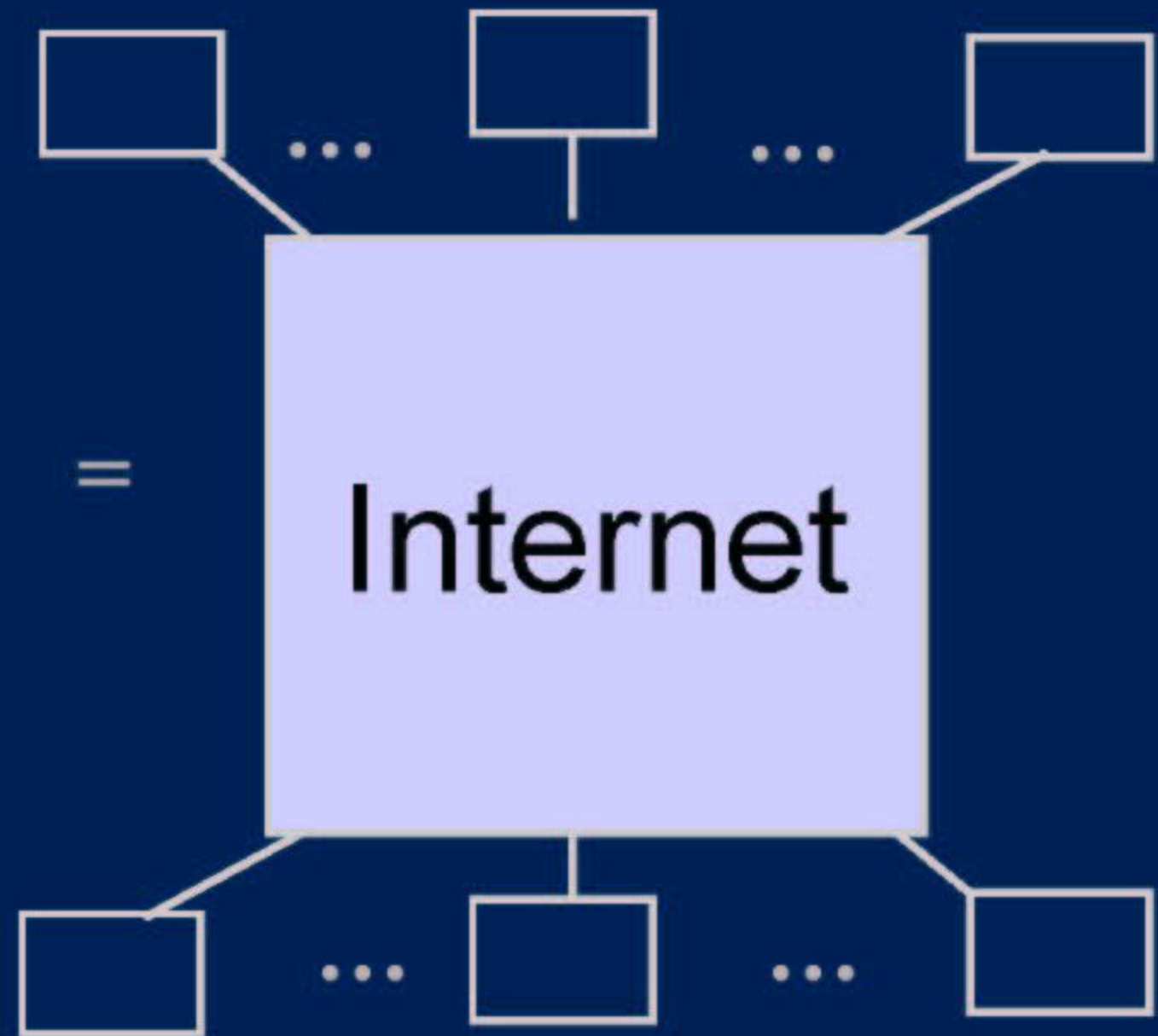
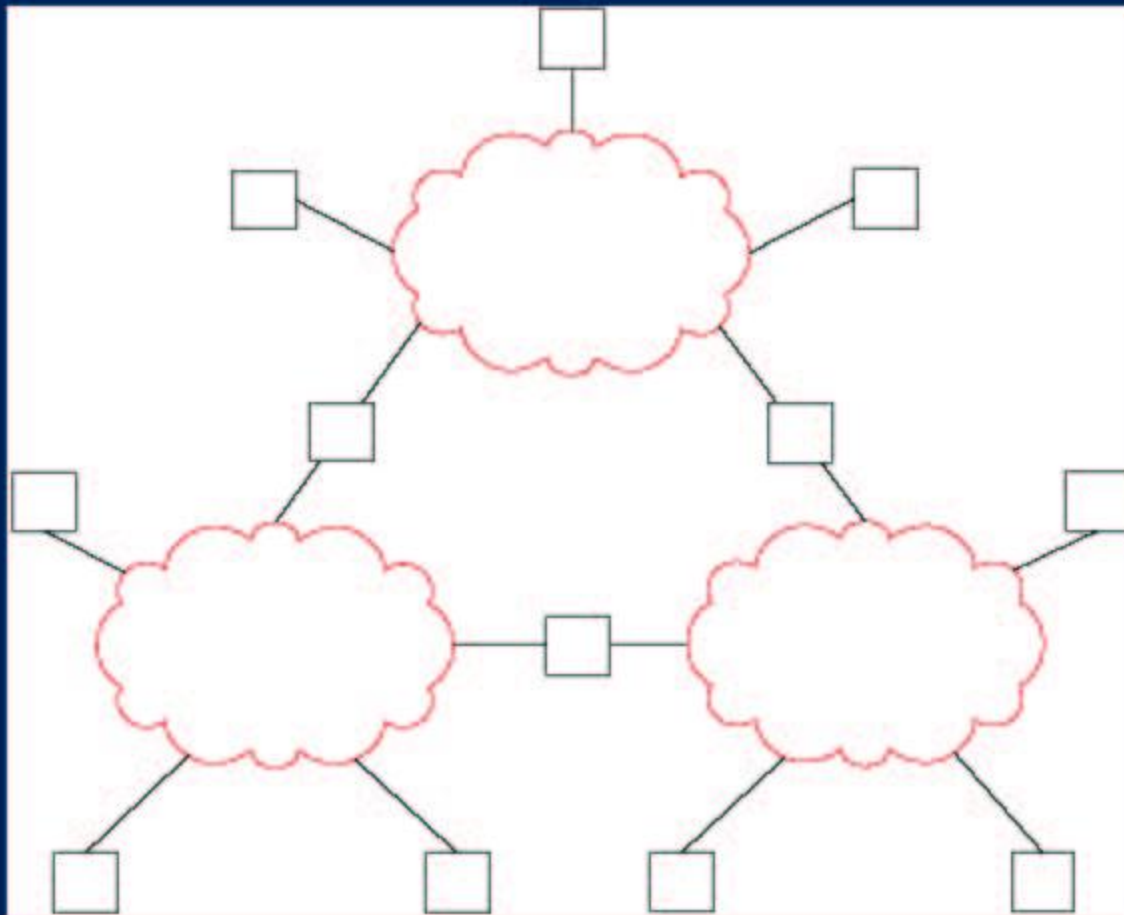


Tree



Ring

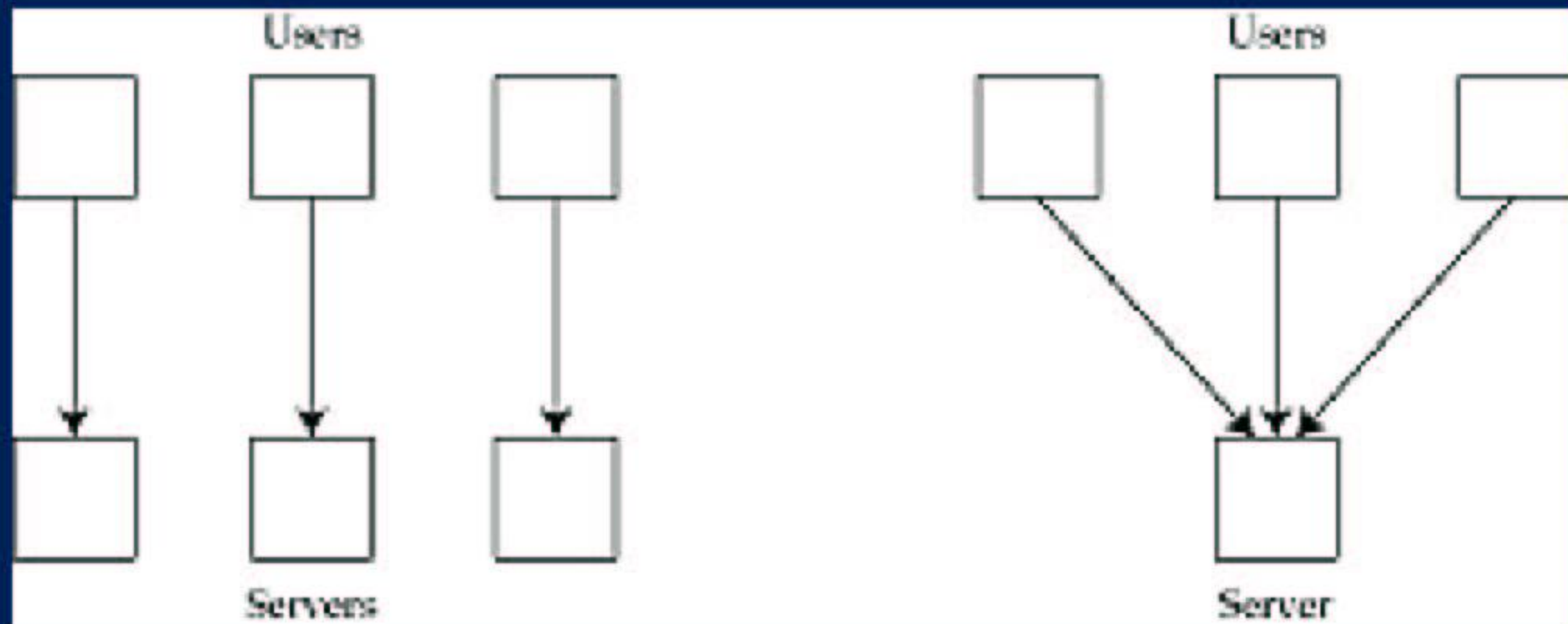
Inter-Networks: *Networks of Networks*



Building blocks: *Multiplexing*

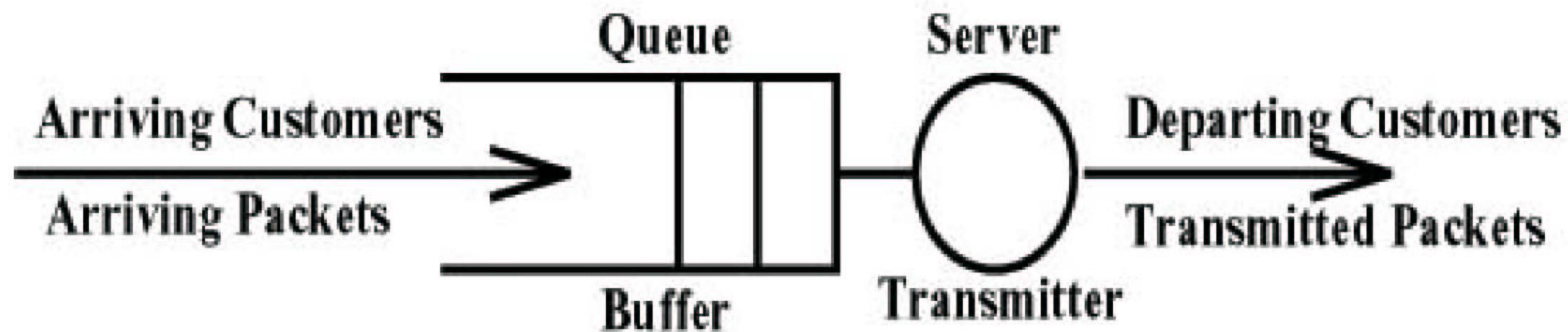
- Multiplexing

- Cost: waiting time, buffer space & packet loss
- Gain: Money => Overall system costs less



Stability of a Multiplexed System

**Average Input Rate > Average Output Rate
=> system is unstable!**



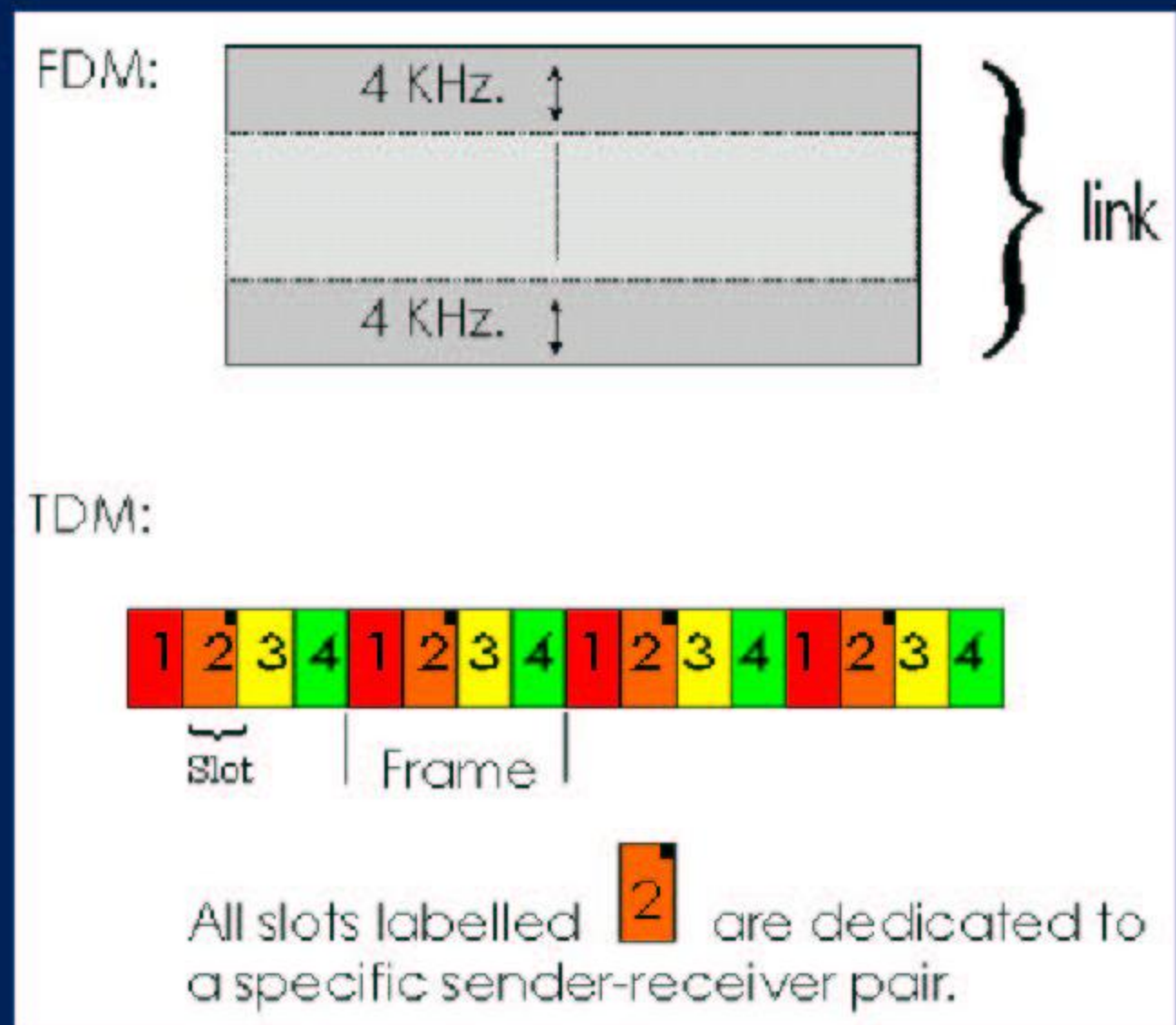
How to ensure stability ?

1. Reserve enough capacity so that demand is less than reserved capacity
2. Dynamically detect overload and adapt either the demand or capacity to resolve overload

Example Design: *Circuit-Switching*

Circuit-switching: A form of multiplexing

- Divide link bandwidth into “pieces”
- Reserve pieces on successive links and tie them together to form a “circuit”
- Map traffic into the reserved circuits
- Resources wasted if unused: *expensive*.
- Mapping can be done without “headers”.

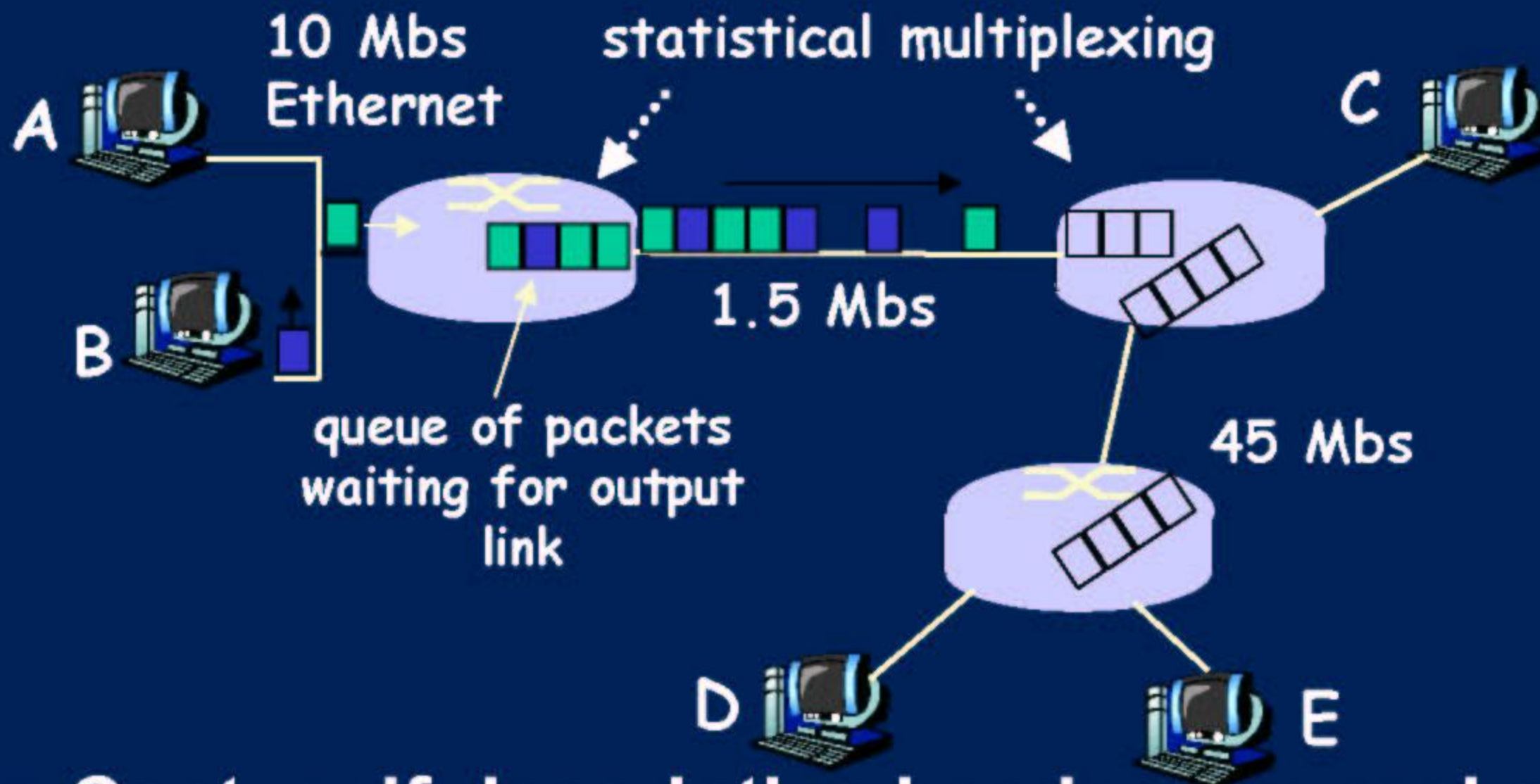


Example Design: *Packet-Switching*

Packet-switching: Another form of multiplexing:

- Chop up data into “packets”
 - Packets: data + meta-data (header)
- “Switch” packets at intermediate nodes
 - *Store-and-forward* if bandwidth is not immediately available.

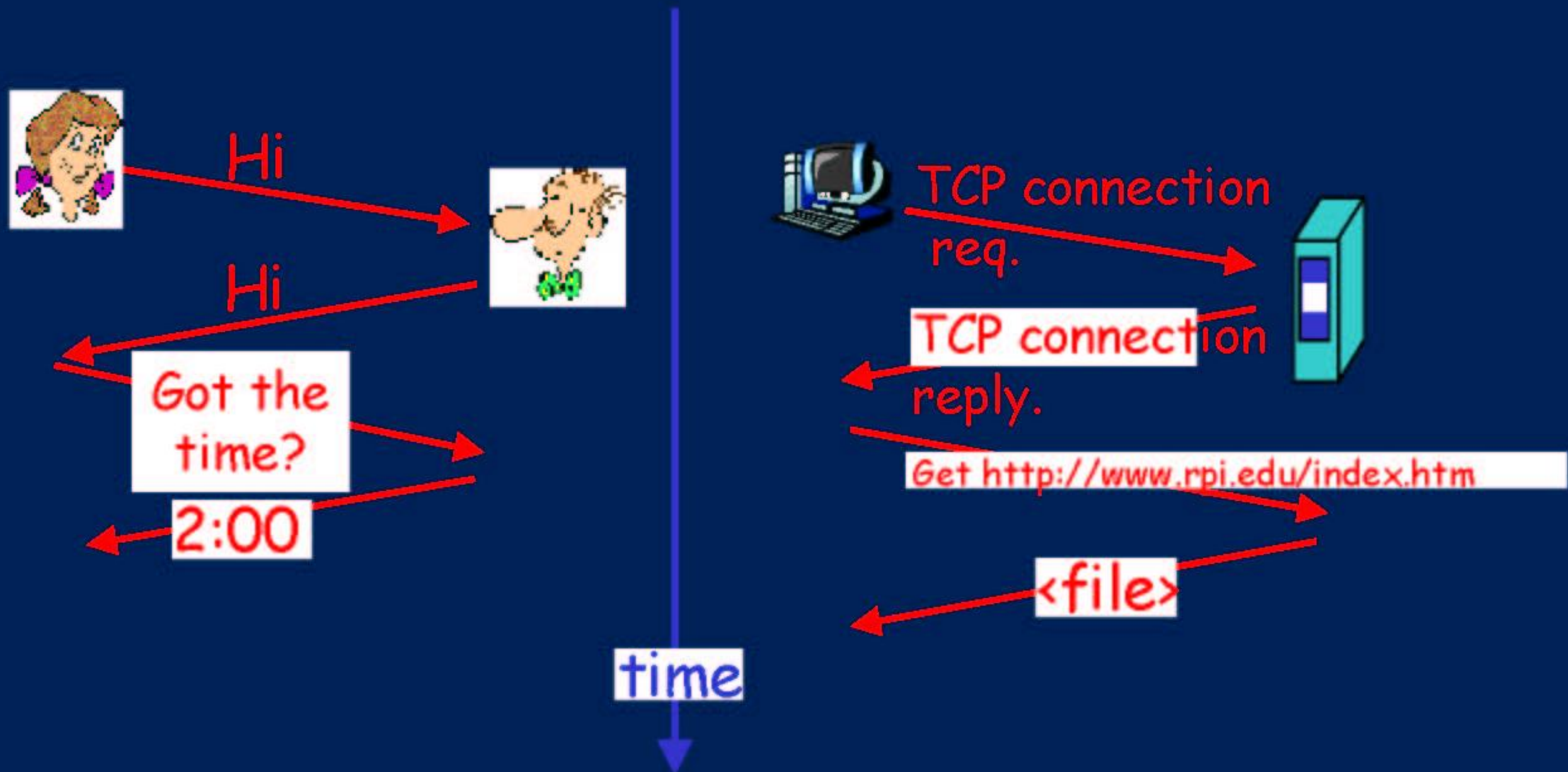
Packet Switching



- ❑ Cost: self-descriptive header per-packet, buffering and delays for applications.
- ❑ Need to either reserve resources or dynamically detect/adapt to overload for stability

What are protocols ?

- Networking software is organized as protocols
- Eg: Human protocol vs network protocol:

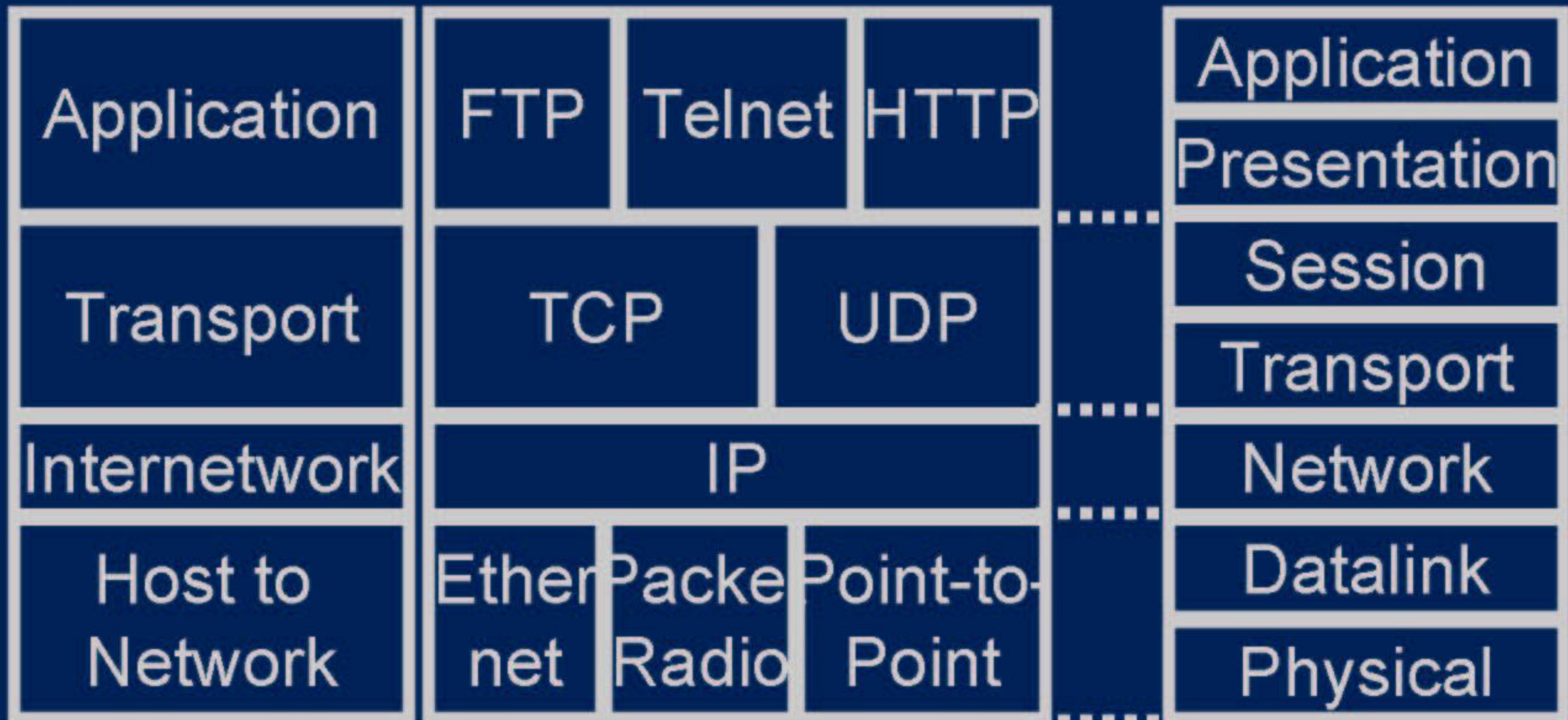


Reference Models for Layering

TCP/IP Model

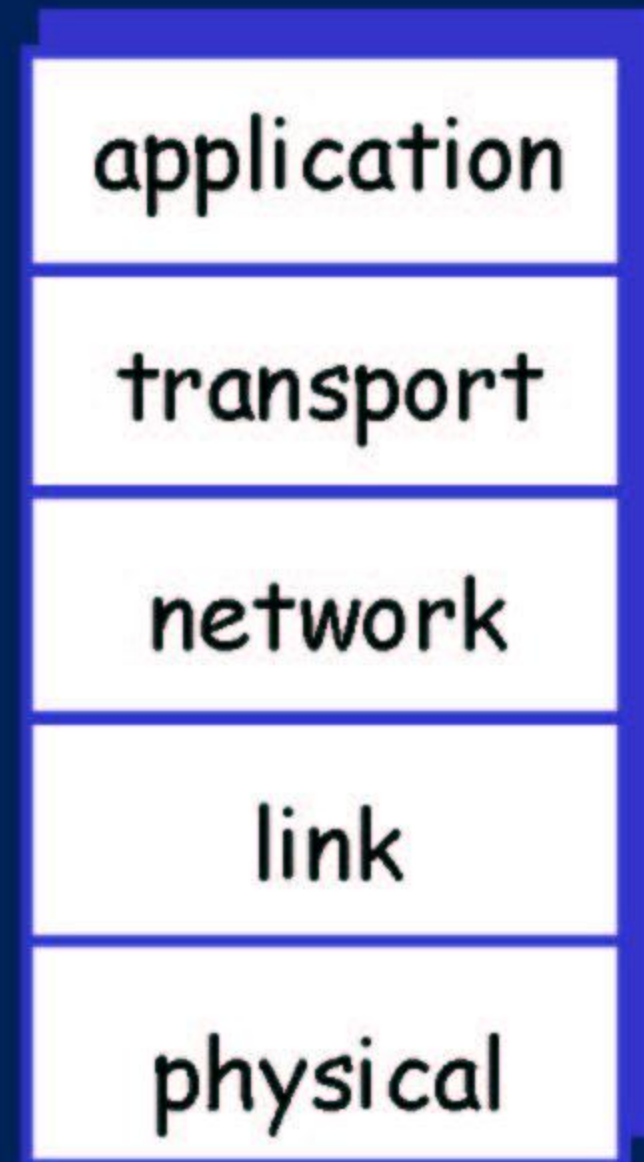
TCP/IP Protocols

OSI Ref Model



Internet protocol stack

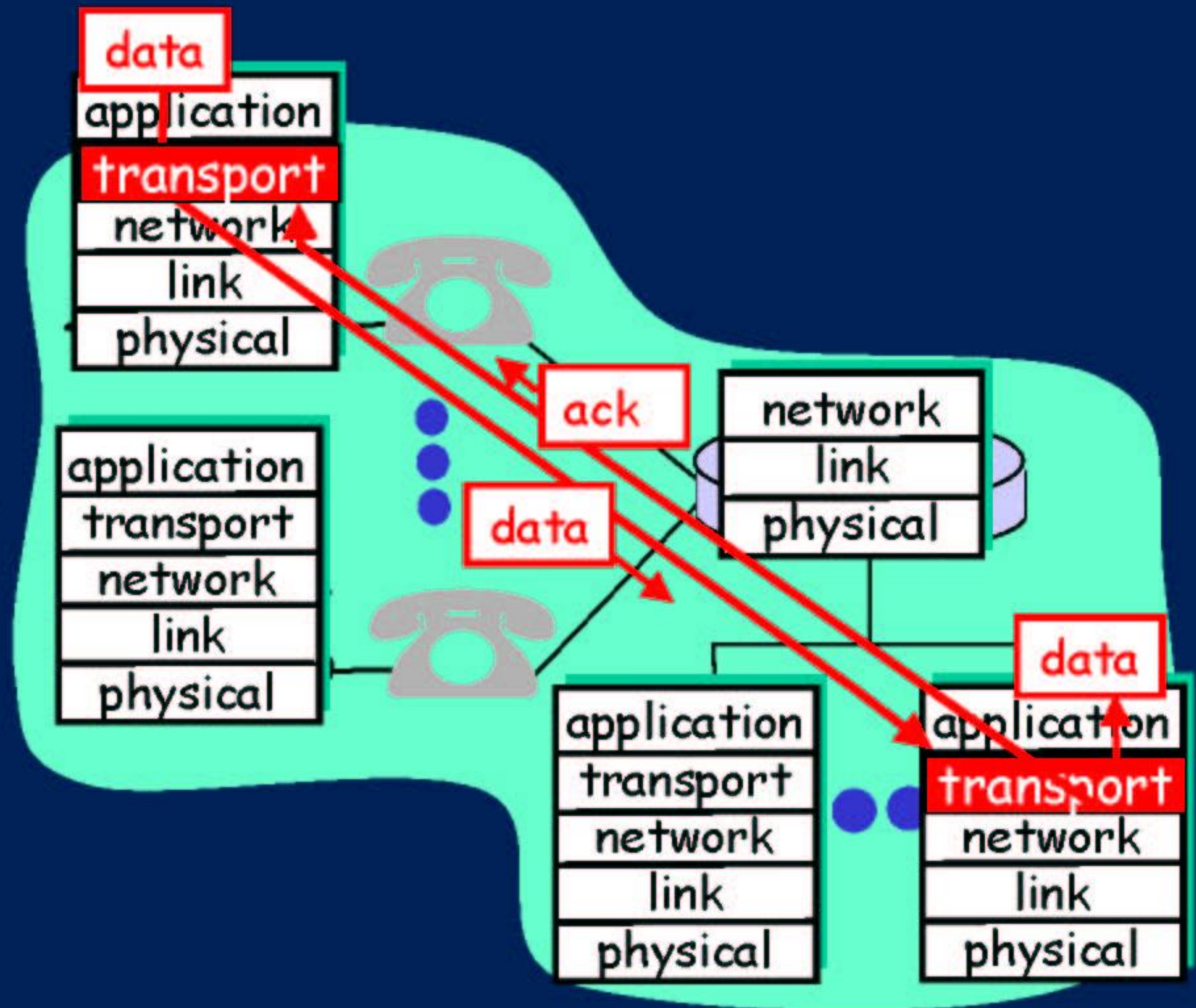
- **application:** supporting network applications
 - ftp, smtp, http
- **transport:** host-host data transfer
 - tcp, udp
- **network:** routing of datagrams from source to destination
 - ip, routing protocols
- **link:** data transfer between neighboring network elements
 - ppp, ethernet
- **physical:** bits “on the wire”



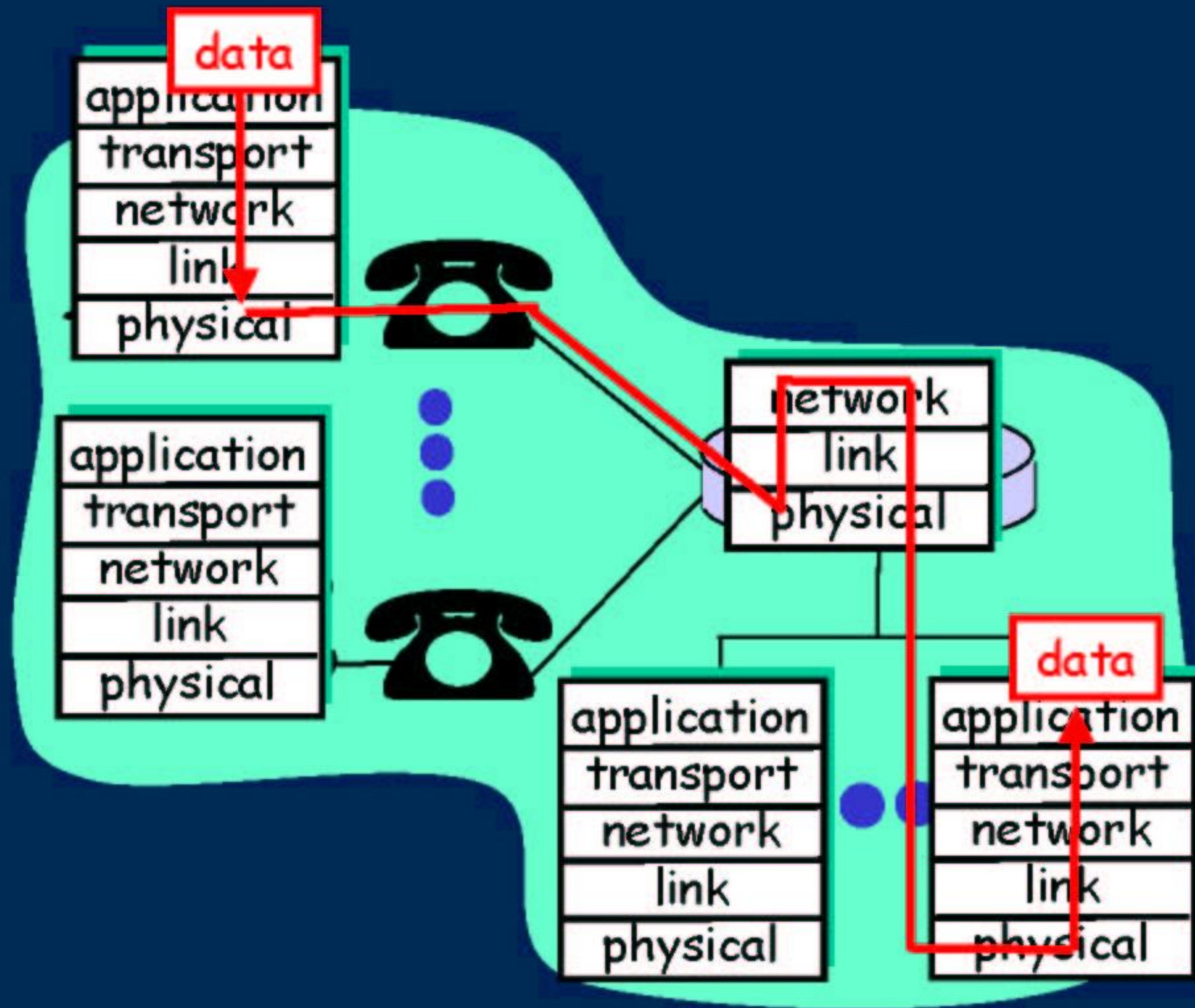
Layering: logical communication

E.g.: transport

- take data from app
- add addressing, reliability check info to form “datagram”
- send datagram to peer
- wait for peer to ack receipt



Layering: physical communication



Protocol layering and data

Each layer takes data from above

- adds header information to create new data unit (“encapsulation”)
- passes new data unit to layer below

