T-401-ICYB
Introduction to Computer Networks

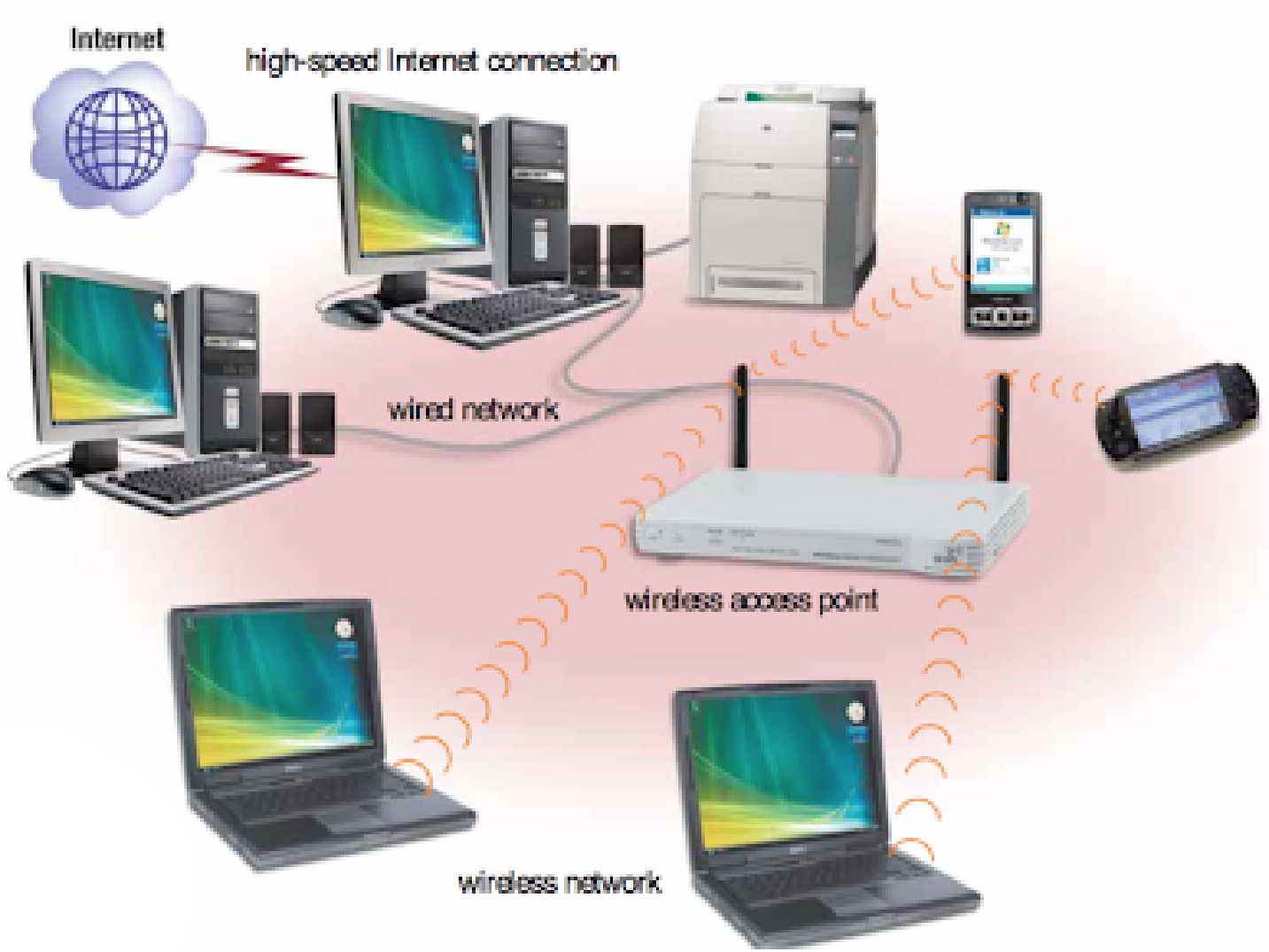
Stephan Schiffel
stephans@ru.is
Reykjavik University, Iceland

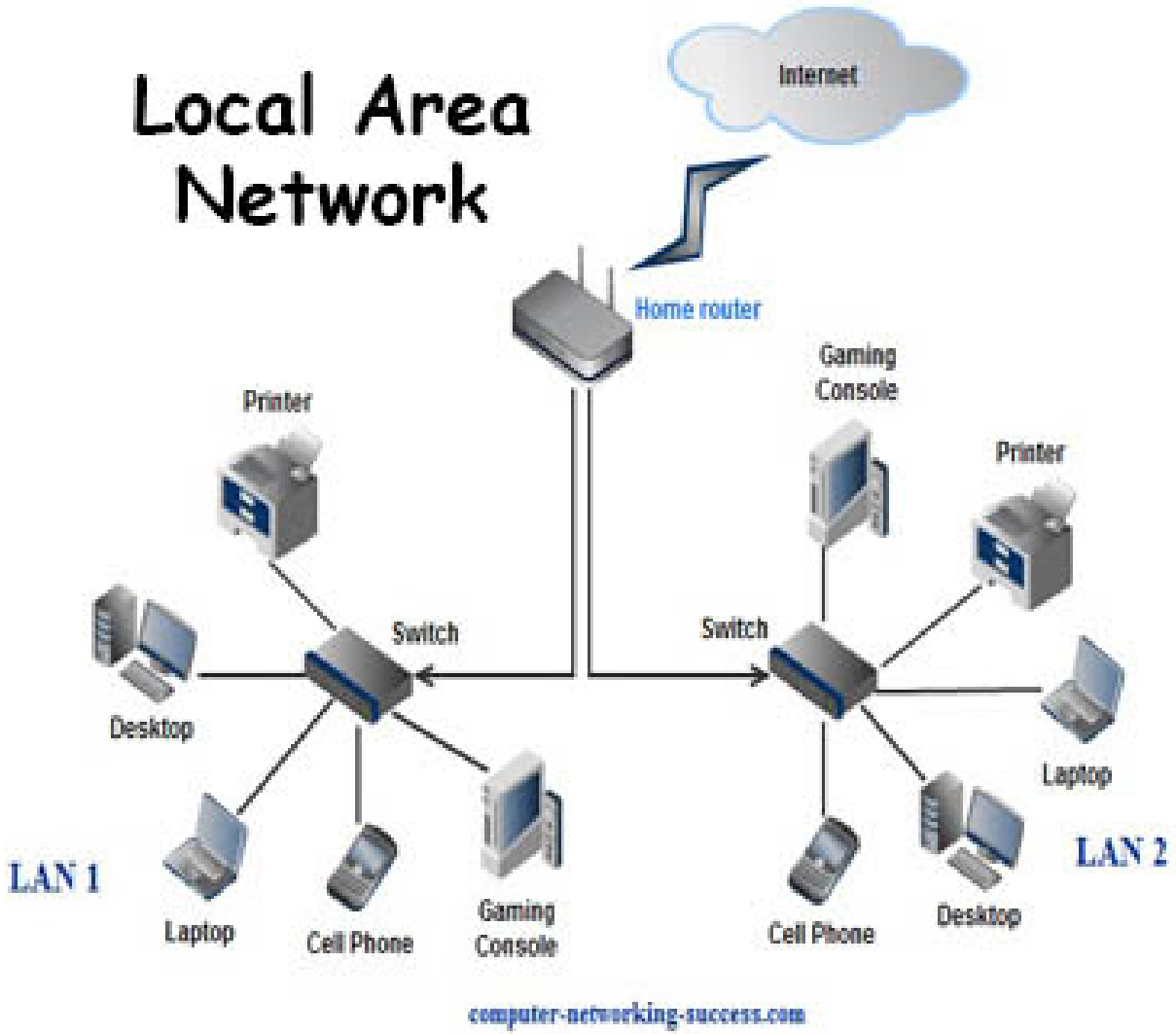
01.12.2025

Outline

Structure and Components

Local Area Network




Local Area Network
Internet
Home router
Printer
Gaming Console
Printer
Switch
Switch
Desktop
Laptop
LAN 1
Laptop
Cell Phone
Gaming Console
Cell Phone
Desktop
LAN 2
computer-networking-success.com

Network Hub

Netgear Hub

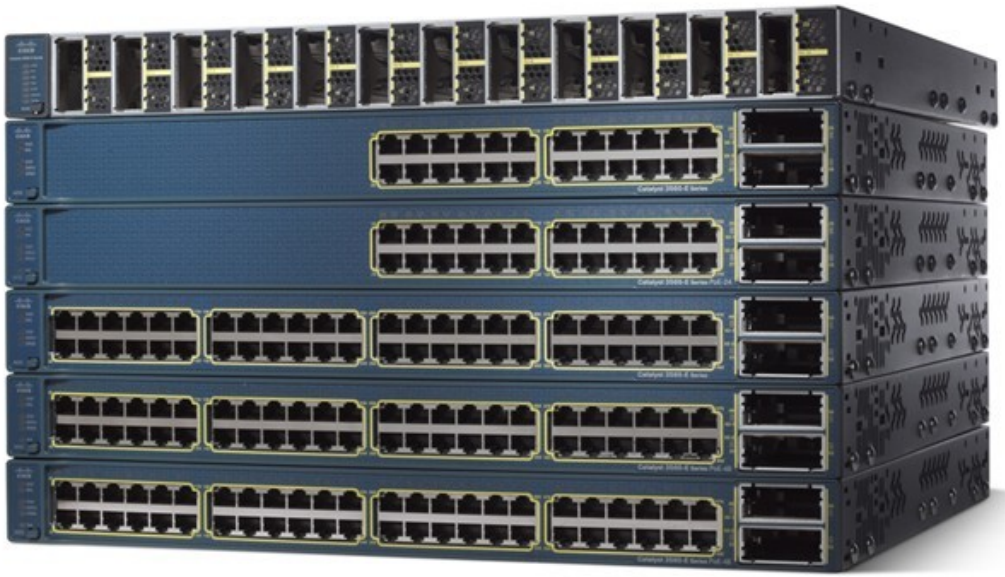
- Hubs are simple connection devices
- Connects several devices onto one link
- Broadcasts received packets to all connected devices
- Bandwidth split between all connected devices
- Today typically replaced by network switches

Network Switch

Cisco LAN Access Switch

- Network switches connect directly to computers, printers, phones, etc.
- Packets are sent only to the destination computer
- Unmanaged: works out of the box, no configuration
- Managed: can be controlled and customised
- Handles a Local Area Network (LAN)

Routers



Cisco Router

- Routers forward packets between (local) networks
- For example, the campus network to the Internet
- Or your home network to the Internet

Home Router

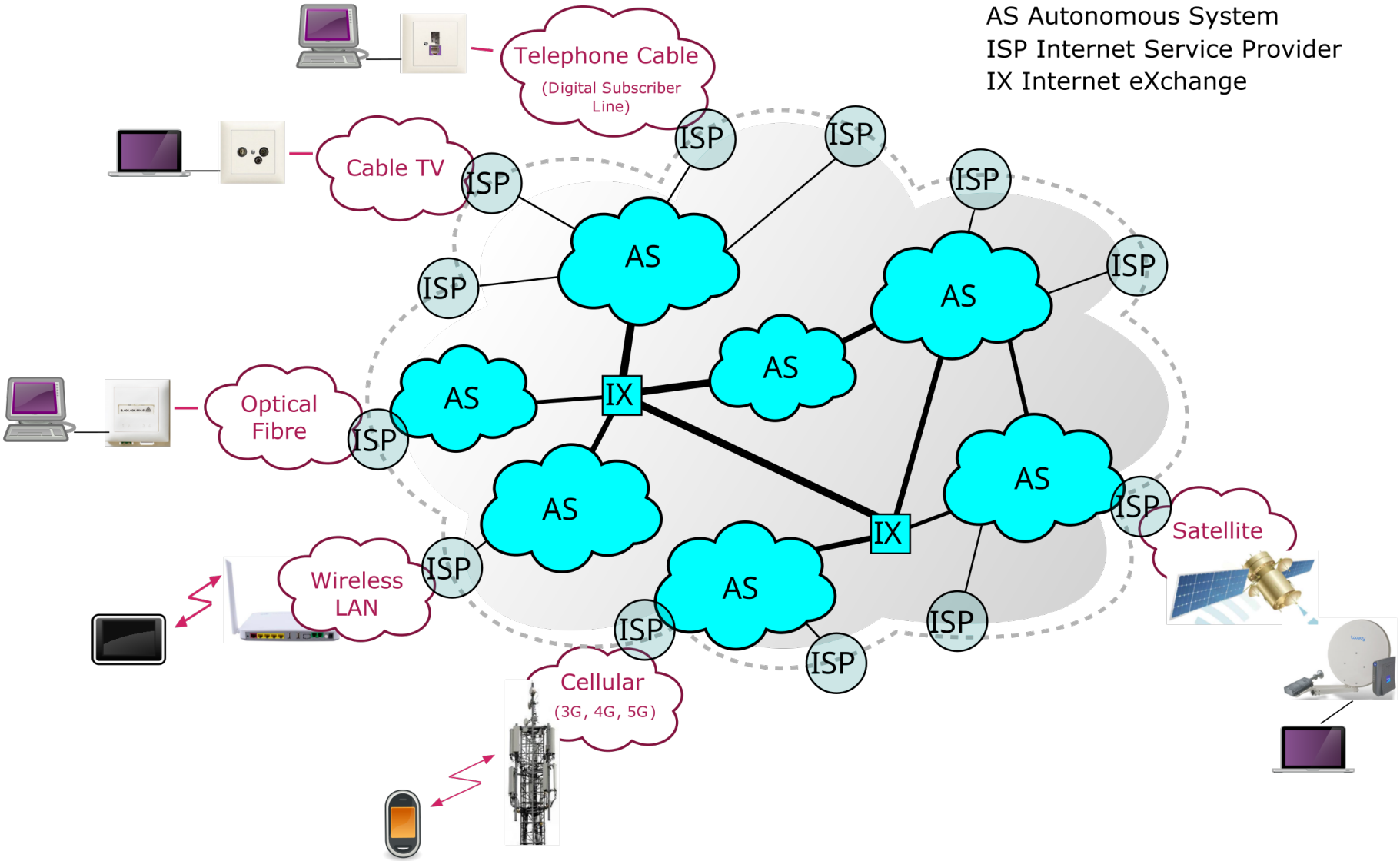
Linksys Home Router

= Switch + Wifi Access Point + Router + NAT (Network Address Translation) + Firewall

Backbone Routers

Juniper Series T Routers - up to 25.6Tbit/s

Structure of the Internet



Layered Architecture

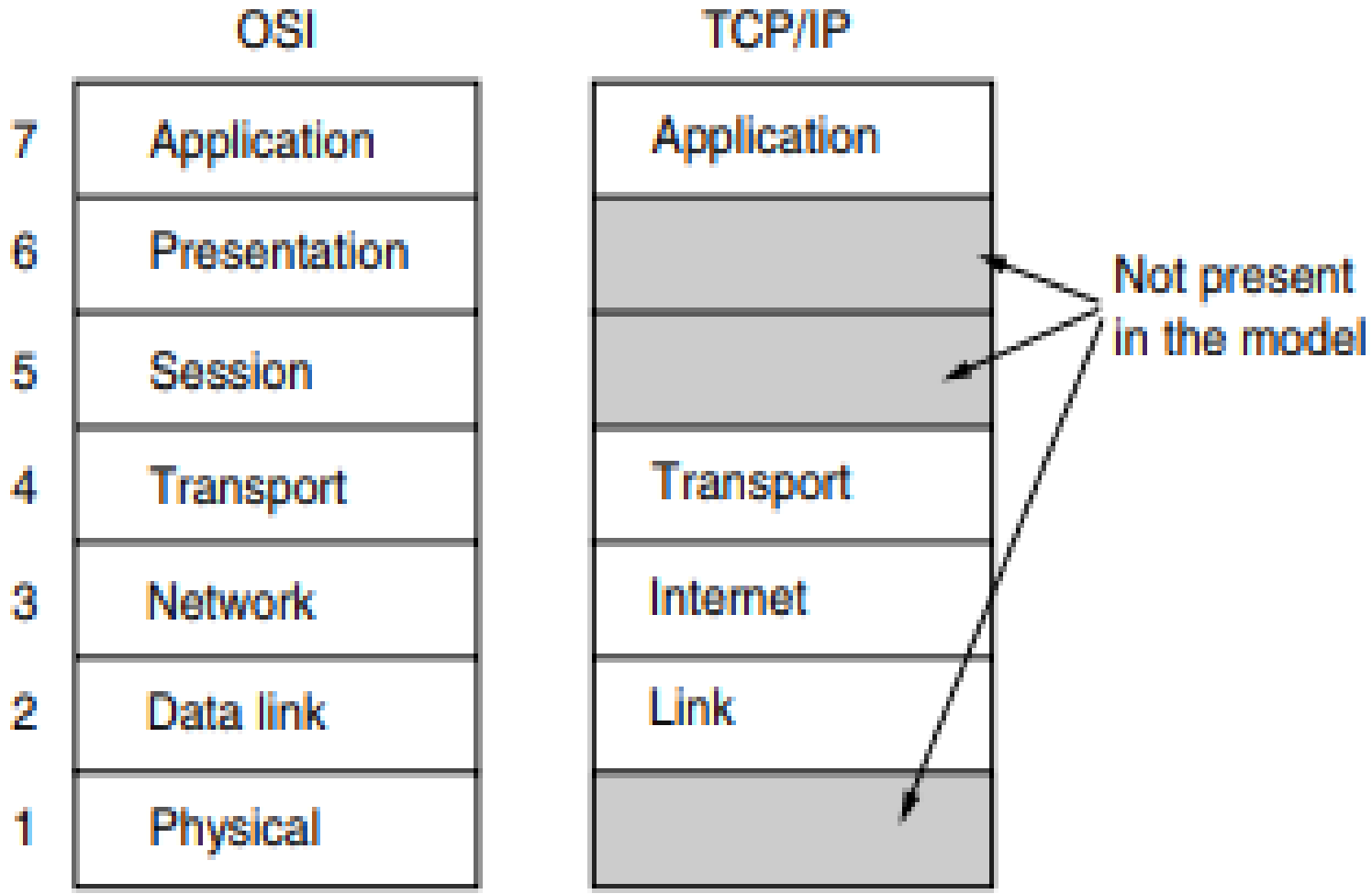
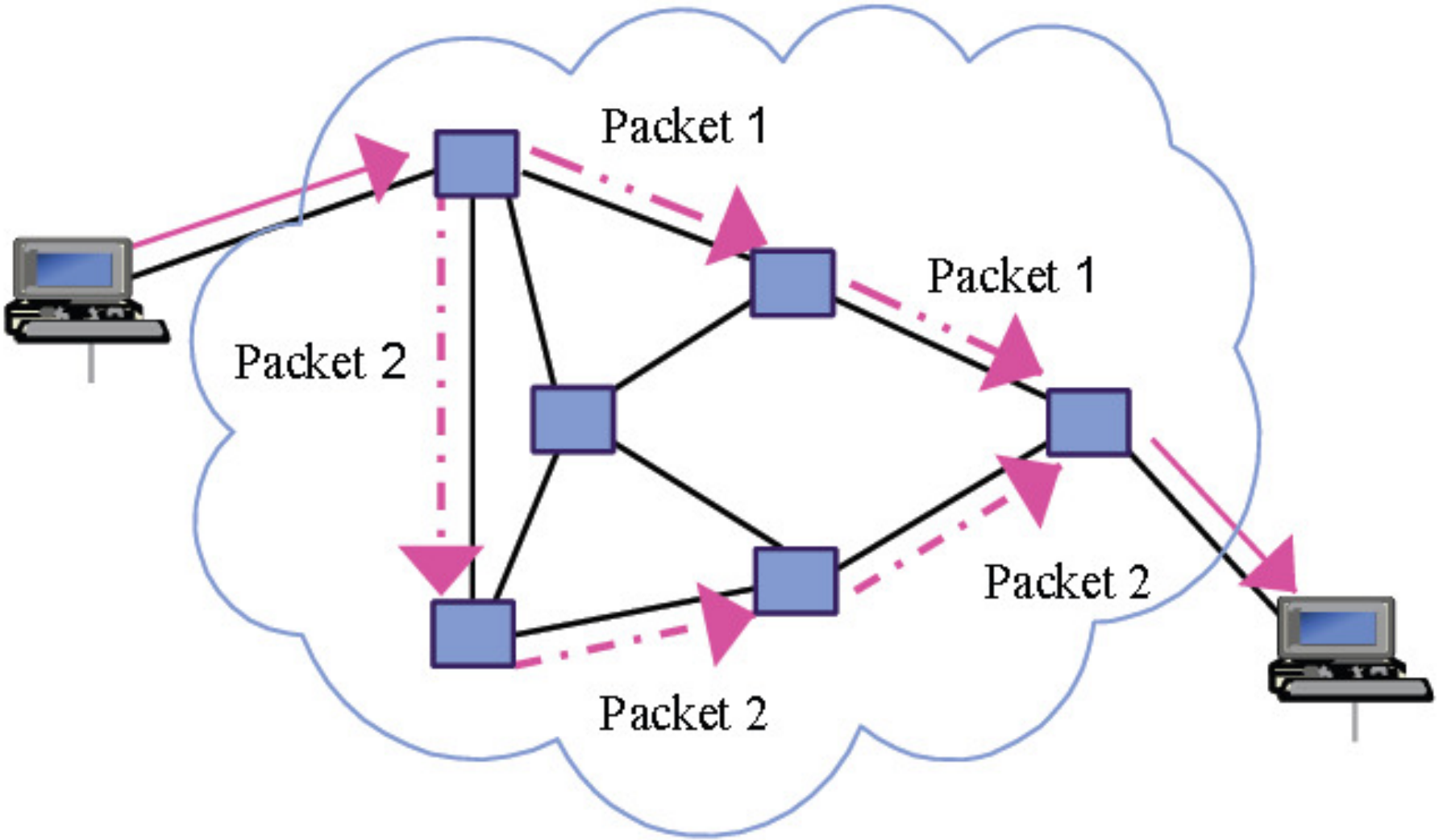


Figure 1-21. The TCP/IP reference model.

Great Lies in Networking

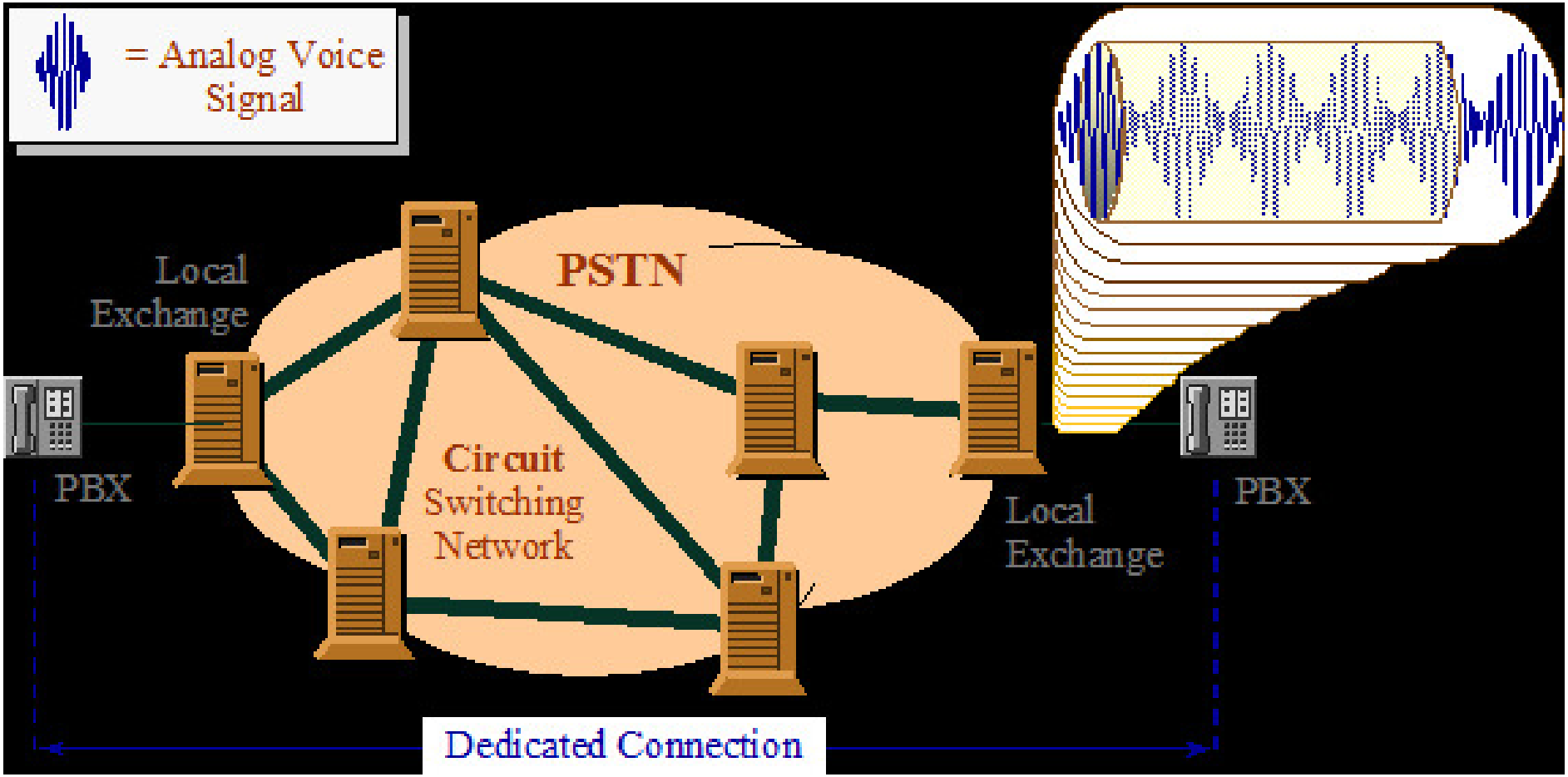
'An application, up in layer 7, does not need to know anything about the physical network.'

How is Data Delivered? - Packet Switching



Packets may take any path through the network, reassembled by receiver

(Old) Phone Systems: Circuit Switched



Fixed circuit (path) is established before call begins

Problems and their Solutions

Identity & Addressing

Problem: How do we identify a device among billions?

- **LAN: MAC Address (Physical)** (e.g., `00:1A:2B:3C:4D:5E`)
  - Hardcoded on the Network Interface Card (NIC).
- **Internet: IP Address (Logical)** (e.g., `192.168.1.15`)
  - Routable across the global internet (unless not).
- **Application Layer: Domain Names** (e.g., `canvas.ru.is`)
  - Human readable
  - Mapped to IP addresses using **DNS** (Domain Name System)

Potential Attacks

- **Spoofing**: Faking the source address (MAC or IP address in packets)
- Attacks on the mappings between addresses: ARP Poisoning, DNS cache poisoning, ...

Finding the Path

Problem: How does a packet know which wire leads to the destination?

- **Layer 2 (LAN): MAC address table / Switching table** in a switch, **Broadcast**, **Default Gateway**
- **Layer 3 (Internet):** Routers have **Routing Tables** that contain the next hop for each possible destination. Routing protocols (e.g., BGP) are used to compute routing tables.

Potential Attacks

- Attacks on the tables or devices, e.g., overloading the switch can lead to fallback to broadcast
- Attacks on the protocols that make the table (e.g., **BGP hijacking**)

Application Multiplexing

Problem: Which application gets the data once it arrives?

- **Solution: Ports (Transport Layer)**
- **Well-Known Ports**: 0–1023 (e.g., HTTP 80, SSH 22).
- **Ephemeral Ports**: Random high numbers assigned to client apps (e.g., your browser tab).
- **Sockets**: IP Address + Port = Unique connection identifier

Security Context: Attack Surface

Every **open port** (a port connected to a process) is a potential entry point. **Port Scanning** (e.g., Nmap) is the reconnaissance phase where attackers knock on doors to see what services are listening.

Communication Language: What is a Protocol?

- **Definition**: A standard set of rules defining the format, order, and timing of messages exchanged between entities, as well as the expected behaviour of the entities.
- **Components**:
  1. **Syntax**: The format (headers, bits, structure).
  2. **Semantics**: The meaning (what the bits represent).
  3. **Timing**: Speed matching and timeouts.
  4. **Expected Behavior**: sequence of events, expected responses, etc.

Security Context: Protocol vs. Reality

Security vulnerabilities often arise when the implementation (code) assumes the other party will strictly follow the protocol.

Physical + (Data) Link Layer

Physical Layer Functions

- Transmitting and receiving bits over a physical medium
- Synchronization between sender and receiver clocks
- Encoding & Signaling: defining how bits are represented (e.g., +5V vs 0V, Light Pulses, RF Waves)

Security Context: Physical Security

- **Wiretapping**: Copper emits electromagnetic usage; it can be tapped without cutting the wire.
- **Jamming**: Denial of Service against the physical medium (common in Wireless).
- **Rogue Devices**: Plugging an attackers device directly into a wall port circumvents the Firewall.
- **Rule #1**: If an attacker can physically touch the device/network, no software protocol can save it.

Link Layer Functions

Node-to-Node delivery on the same network

- **Framing:** determing the start and end of packets (framing) in the bit stream
- **Error detection and correction**: Deal with transmission errors
- **Medium access control**: Who gets to transmit when?
  Requires multiplexing on shared media (Wifi, Bus systems, etc.)
- **Flow control**: Don't send faster than the receiver can handle
- Provide an interface to the Network Layer that is (somewhat) independent of type of physical link

Link Layer Protocols

- **Ethernet (IEEE 802.3)**:
  - The standard for wired LANs.
  - In practice often Point-to-point (switches), but technically uses a shared medium (the wire).
  - Mechanism: Random access to medium with collision detection (CSMA/CD).
- **Wi-Fi (IEEE 802.11)**:
  - Uses a shared medium. Every packet is broadcast to everyone within range.
  - Mechanism: Random access to medium with collision avoidance (CSMA/CA).
- **Bluetooth (IEEE 802.15.1)**:
  - Type: PAN (Personal Area Network).
  - Mechanism: Master/Slave topology using Frequency Hopping (FHSS) to avoid interference.
- **USB (Universal Serial Bus)**:
  - Mechanism: Host-Controlled Polling.
  - Unlike Ethernet, devices speak only when the Host asks.

Layer 2 Vulnerabilities: Wired Networks

ARP Poisoning → Man-in-the-Middle

- **Mechanism**: Attacker spams unsolicited ARP Replies: "I am the Router (192.168.1.1)" and "I am the Victim."
- **Result**: The Switch updates its table. Traffic flows through the attacker, allowing packet capture and modification.

MAC Flooding

- **Mechanism**: Attacker generates thousands of random fake MAC addresses per second.
- **Result**: The Switch's memory (CAM Table) fills up. To maintain availability, the switch **fails open**, acting like a Hub and broadcasting *all* traffic to *all* ports (including the attacker).

Layer 2 Vulnerabilities:

Bluetooth

Layer 2 Vulnerabilities: Wireless

Rogue Access Points (e.g., "Wi-Fi Pineapple")

- **Mechanism**: Listening for client Probe Requests ("Are you Starbucks-Guest?") and responding affirmatively.
- **Result**: Users connect to the attacker, allowing further attacks, e.g.:
  - **Packet Capture**: The attacker can record all unencrypted traffic.
  - **DNS Spoofing**: User types google.com, gets sent to a fake login page.
  - **Captive Portals**: Fake "Login to Free Wi-Fi" page to steal credentials.

Deauthentication / Jamming (DoS)

- **Mechanism**: Sending spoofed "Deauth" management frames to disconnect users from the legitimate router.
- **Goal**: Disruption or forcing a user to reconnect (to capture the handshake for password cracking).

Layer 2 Vulnerabilities: Physical

Physical Interface Trust (e.g., BadUSB)

- **Mechanism**: A USB flash drive masquerading as a Human Interface Device (Keyboard).
- **Result**: OS trusts keystrokes implicitly; allows instant script execution.

Up Next ..

Further Studies

- Find examples of vulnerabilities and attacks using Bluetooth and learn why Bluetooth is a terrible protocol.
- What is the best protection against Bluetooth attacks?
- How to prevent or defend against attacks that use Rogue Access Points? Distinguish between what individuals and what organizations can do.