

1 Internetarchitekturen

Die allgemeine Architektur des Internets ist gegeben durch die Vernetzung der Systeme auf unterschiedlichen Ebenen. Nutzer können bei Internet Exchange Points ("Internetknoten", IX or IXP, auch Network Access Point) verschiedenste Daten austauschen und generell werden diese von Providern (ISPs) zur Nutzung angeboten.

Die meisten ISPs nutzen IX als Schnittstellen zwischen Rechnernetzwerken, wobei der gesamte Verbund aller autonomen Systeme das Internet bilden. Weltweit existieren ca. 340 IXPs, wobei kleinere Knotenpunkte als Uplink zu den 'Carriern', den ISPs, dienen. Die Vorteile mehrerer IX sind primär Effizienz und Ausfallsicherheit bei Datentransfer, wobei die Kosten für den Betrieb eines IX von den dazugehörigen ISPs geteilt werden. Die Gebühren berechnen sich pro genutzten Port pro eigenen IXP. Die Kosten für den jeweiligen Port sind abhängig von dessen Transferrate - derzeit zwischen 10Mbps und 100 Gbps.

Bei den einzelnen ISPs unterscheidet man zwischen mehreren Kategorien (Tiers):

- Tier 1.: National & oftmals International, die größten Betreiber.
z.B.: Deutsche Telekom, KPN, AT&T, Verizon, NTT, Telecom Italia,...
- Tier 2.: Transit Provider. Nehmen Downstream von Tier 1 in Anspruch und bieten Upstream für Tier 3.
z.B.: Vodafone, Tele2, Comcast
- Tier 3.: Lokale Provider. Sie verkaufen Transitmöglichkeiten an Nutzer.

Es bleibt jedoch zu beachten dass die Kategorisierung regelrecht schwammig geführt wird.

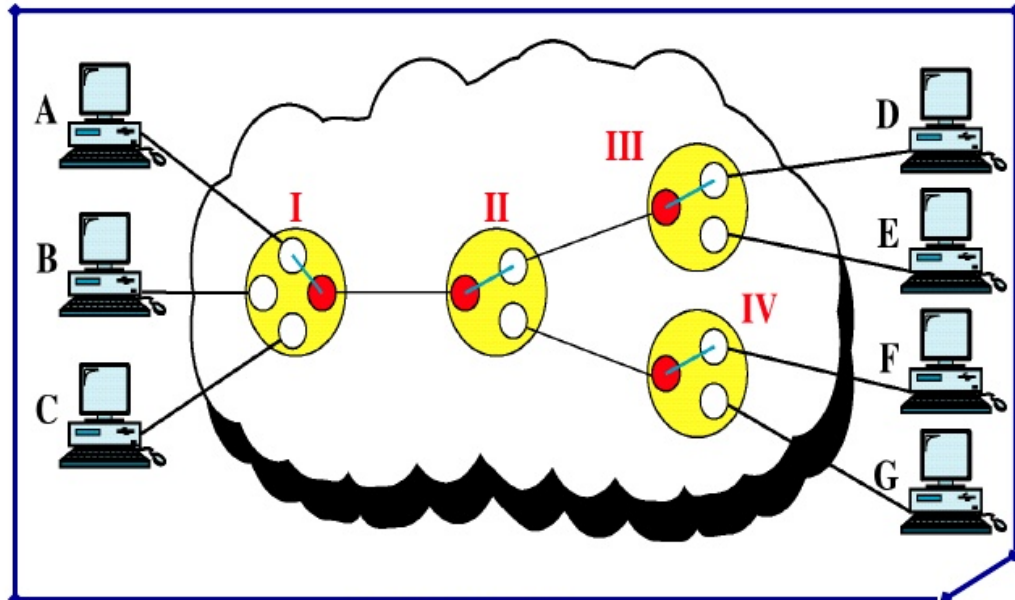
Weiters ist das Internet noch durch Protokolle unterstützt, um fehlerfreien Austausch zu garantieren, oft beschrieben mithilfe des ISO/OSI-Referenzmodells (siehe 2.3).

2 Netzwerktypen

2.1 Leitungsvermittelnde Netzwerke

Leitungsvermittelnde Netzwerke, oder Circuit-Switch Networks, sind vergleichbar mit Telefonanrufen oder einem Schienennetz. Ein exklusiver logischer oder physikalischer Pfad wird zwischen Sender und Empfänger designiert, vergleichbar mit einer Kritischen Zone. Genutzte Ressourcen, benutzt oder nicht, stehen in dieser Zeit anderen Usern nicht zur Verfügung.

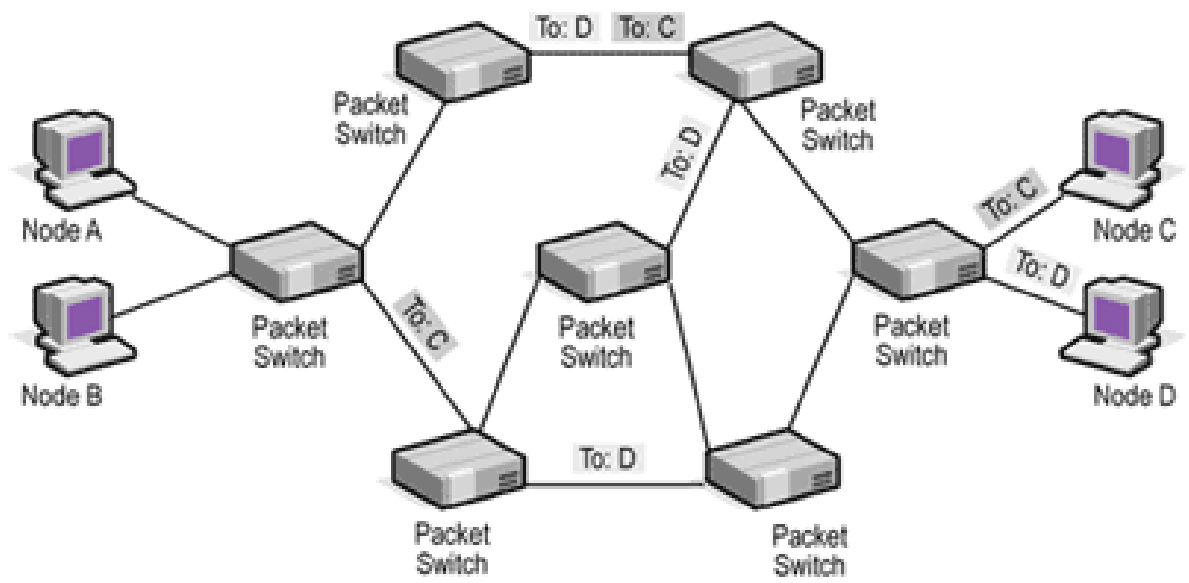
Circuit Switched Networks



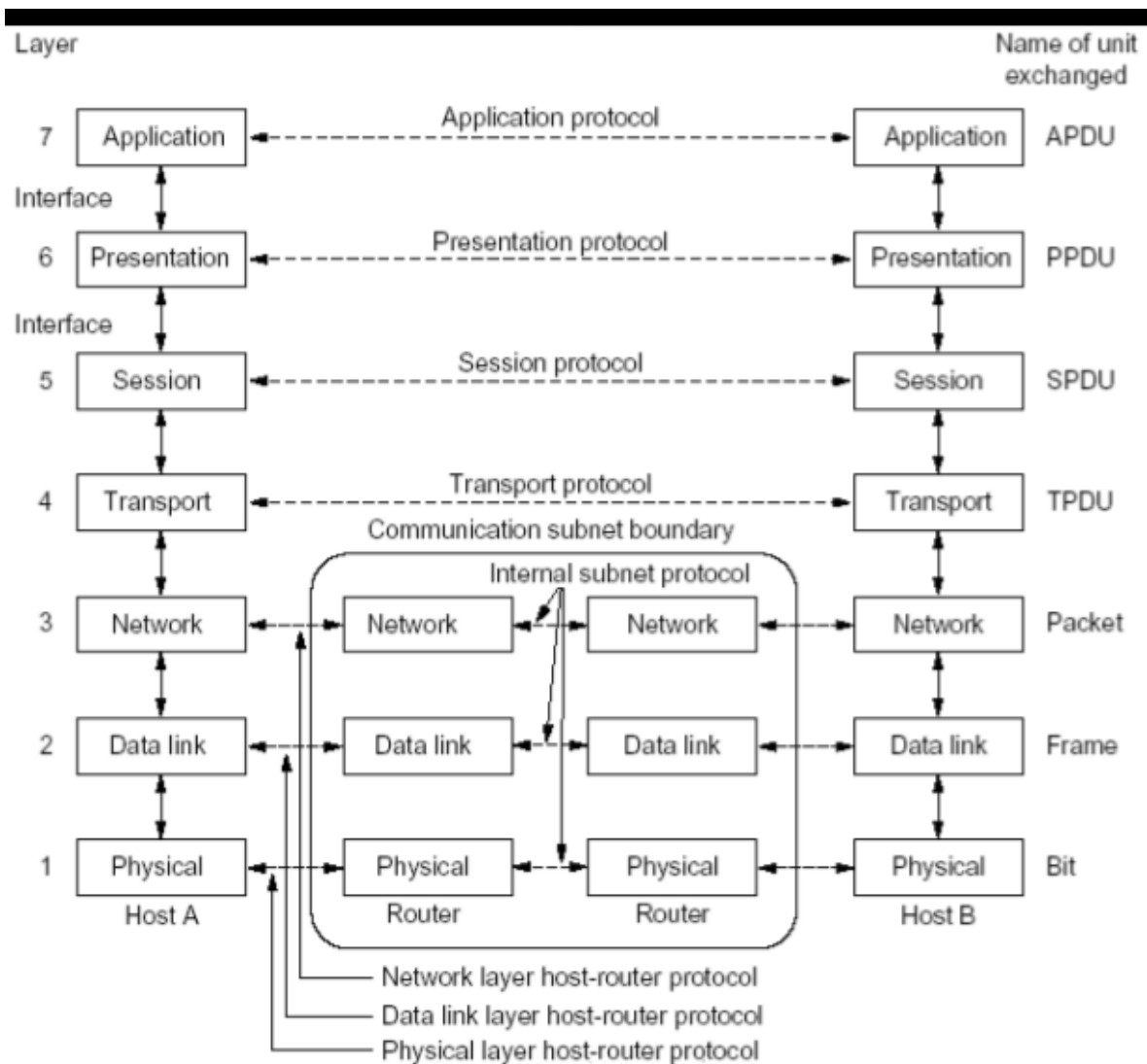
University of Education

2.2 Paketvermittelnde Netzwerke

Paketvermittelnde Netzwerke, oder Packet-Switching Networks, sind charakteristisch gesehen wie E-Mails. Daten werden Buffermäßig zu einem größeren Datensatz zusammengeschrieben, welches das Datenpaket ausmacht. Diese werden vollständig gesendet & vollständig empfangen, wobei die Pakete über dynamisch bestehende Pfade via Nodes verschickt werden. Dies ermöglicht parallelen Transfer zwischen mehreren Usern und erhöht die Ausfallsicherheit, da die Zielpfade der Pakete zur Laufzeit veränderbar sind.



3 ISO-OSI Referenzmodell



Das ISO-OSI Referenzmodell besteht aus verschiedenen Anwendungsschichten:

1. Physical Layer

Dieser Layer beschreibt die fundamentale Netzwerkkommunikation. Datentransfer via physischem Layer sind reine Bitstreams.

Hardware:

PHY-Chip: Ein PHY implementiert die Funktionen Senden und Empfangen von Daten zwischen Geräten mithilfe des Datalink Layers (MAC, LLC). Es enkodiert und dekodiert einkommende Übertragungen und Galvanische Trennung (Blockt ungewollten Datenempfang).

Protokolle:

Integrated Services Digital Network: Internationaler Standard für Datenübertragung & Telefonie
 Universal Serial Bus: Bussystem von Verbindungen um Daten zu

bertragen Bluetooth, Ethernet, ...

Normen:

2. Data Link Layer

Der Datenlink nutzt Frames zur bertragung von Datenstzen. Frames bestehen aus einer gewissen Anzahl an Bit-Blcken und einer Prfsumme, welche die korrekte Datenflussbertragung gewhrleistet. Fehlerbehaftete Frames knnen anhand dieser Summe erkannt werden und der DLL kann das jeweilige Paket verwerfen oder sogar korrigieren. Im Falle des Verwerfens ist es allerdings nicht vorgesehen das jeweilige Frame neu anzufordern.

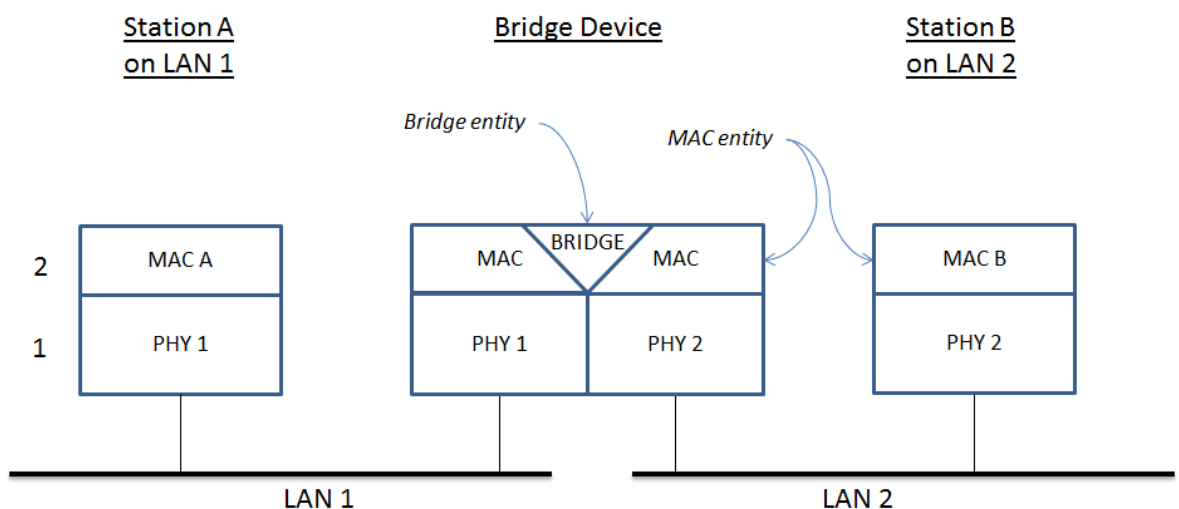
Mithilfe der 'Data Flow Control' kann man die Dynamik der Framebertragung steuern, etwa wie schnell Blcke verschickt werden.

Hardware:

Bridge & Switch: Arbeiten via Media Access Control(Mac) oder Logical Link Control(LLC).

Die MAC-Bridge schtzt gegen Kollisionen via Aufteilung des Netzes in verschiedene Kollisionsdomnen, d.H. ein Paket geht nur in das Netz, in welchem sich der tatschliche Empfänger befindet.

Die LLC-Bridge dient der Koppelung zweier Teilnetze mithilfe verschiedener Zugriffsverfahren, wie Token-Passing (Tokens werden zwischen Sendern gewechselt und dementsprechend startet Datenverkehr) oder Carrier Sense Multiple Access/Collision Detection (CSMA/CD; Typischer Router mit x-Medien).



Schemata of Bridge/Switch inside a Network¹

Protokolle:

HDLC - High-Level Data Link Control: Transmition of sync/async frames

SDLC - Synchronous Data Link Control: Bitsynchron & Serielle bertragung

¹By Crvincenzi - MS Powerpoint, CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=25610536>

DDCMP - Digital Data Communications Message Protocol: Point-to-Point Transfer (Sicherheit)

SPB - Shortest Path Bridging: Aufbau & Konfig. + Multipath Routing

Normen: IEEE, FDDI, ISO

3. Network Layer Der Network Layer behandelt Weiterleitung und Routing durch multiple Zwischenmedien innerhalb eines Netzwerkes.

Funktionen:

- CL-mode: Verbindungslose Kommunikation, ber IP
- Hostadressierung, jeder Host ist einzigartig identifizierbar
- Weiterleitung: Partitionierung von Netzwerken in Subnetzwerke und Weiterleitung von Daten ber Gateways und Router

4. Transport Layer Die Transportschicht beschreibt den konkreten Datentransfer von A nach B.

Protokolle:

- Transmission Control Protocol: TCP/IP - Datentransfer wird kontrolliert weitergegeben. Wird das Paket falsch oder garnicht empfangen, so wird eine Anfrage geschickt welche das Datenpaket neu schickt. Es gibt Flow- und Congestioncontrol. Grundsätzlich genutzt bei HTTP, FTP, SMTP.
- User Datagram Protocol: UDP/IP - Datentransfer wird losgeschickt, ohne Kontrolle ob das Datenpaket tatsächlich ankommt. Es gibt also weder Flow- noch Congestioncontrol.

5. Session Layer

6. Presentation Layer

7. Application Layer

Die 5. und 6. Schicht wird meist impliziert, bzw. wird von der Praxis nicht angenommen.

4 ISO/OIS Referenzmodell vs. TCP/IP-Referenzmodell

TCP/IP Referenzmodell besteht mehr oder weniger aus den gleichen Schichten wie das ISO/OSI-Referenzmodell, jedoch besteht es lediglich aus vier Schichten, da die Schichten 5 und 6 nicht verwendet werden.

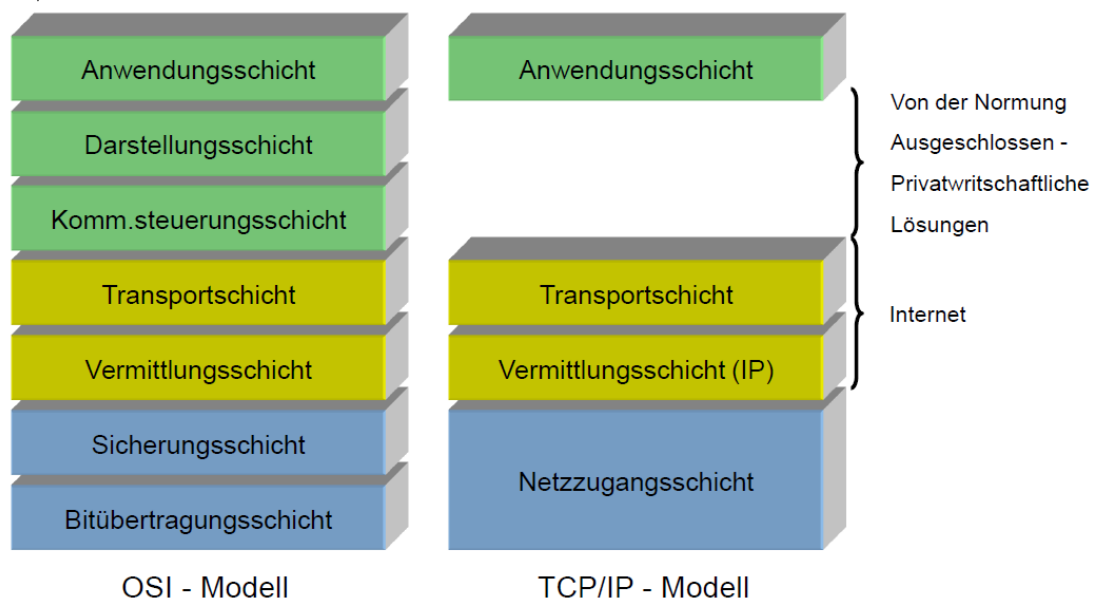
Es beruht auf den Vorschlägen, die bei der Fortentwicklung des ARPANET's gemacht wurden. Diese Art des Modells ist zeitlich vor dem OSI-Referenzmodell entstanden, weshalb auch die Erfahrungen dieses Modells in die OSI-Standardisierung miteingeflossen sind. Es bildet die Basis für sämtliche Netzwerke, sowie für das OSI-Modell, wie wir es heute kennen.

IP tut hierbei nichts anderes, als die Daten, mit bestimmten Ziel und Absender, einfach nur zu

verschicken. In Kombination mit TCP soll letztendlich gewährleistet werden, dass die Daten fehlerfrei ankommen. Als Ziele der Architektur wurden bei der Entwicklung definiert:

1. Unabhängigkeit von der verwendeten Netzwerk-Technologie
2. Unabhängigkeit von der Architektur der Hostrechner.
3. Universelle Verbindungsmöglichkeiten im gesamten Netzwerk.
4. Ende-zu-Ende-Quittungen.
5. Standardisierte Anwendungsprotokolle.

Das TCP/IP-Referenzmodell besteht im Gegensatz zum OSI-Modell aus nur vier Schichten.



1. Application Layer

Umfasst alle hoherschichtigen Protokolle des TCP/IP-Modells. Zu den ersten Protokollen der Verarbeitungsschicht zählen TELNET (für virtuelle Terminals), FTP (Dateitransfer) und SMTP (zur Übertragung von E-Mail). Im Laufe der Zeit kamen zu den etablierten Protokollen viele weitere Protokolle wie z.B. DNS (Domain Name Service) und HTTP (Hypertext Transfer Protocol) hinzu.

2. Transport Layer:

Ermöglicht wie im OSI-Modell die Kommunikation zwischen Quell- und Zielhost. Hierzu wurden zwei End-zu-End-Protokolle definiert:

- Transmission Control Protocol (TCP)

Ist ein zuverlässiges verbindungsorientiertes Protokoll, durch das ein Bytestrom fehlerfrei einem anderen Rechner im Internet vermittelt werden kann.

- User Datagram Protocol (UDP)

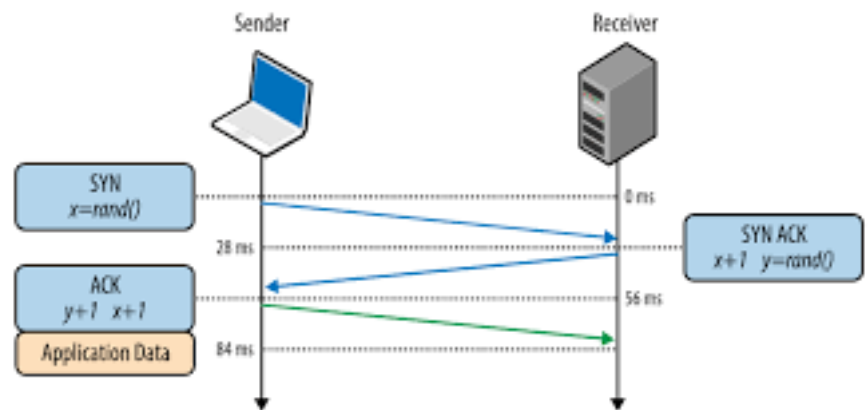
UDP ist ein unzuverlässiges Protokoll, welches vorwiegend in Client/Server-Umgebungen verwendet wird, in denen es in erster Linie nicht um eine sehr genaue, sondern schnelle Datenübertragung geht.

3. Internet Layer:

Diese Schicht definiert nur ein Protokoll namens IP (Internet Protocol), das alle am Netzwerk beteiligten Rechner verstehen kann. Sie hat die Aufgabe IP-Pakete richtig zuzustellen. Dabei spielt das Routing der Pakete eine wichtige Rolle. Das Internet Control Message Protocol (ICMP) ist fester Bestandteil jeder IP-Implementierung und dient zur Übertragung von Diagnose- und Fehlerinformationen für das Internet Protocol.

4. Network Layer:

Unterhalb der Internetschicht befindet sich im TCP/IP-Modell eine große Definitionslücke. Das Referenzmodell sagt auf dieser Ebene nicht viel aus, was hier passieren soll. Festgelegt ist lediglich, dass zur Übermittlung von IP-Paketen ein Host mit einem bestimmten Protokoll an ein Netzwerk angeschlossen werden muss. Dieses Protokoll ist im TCP/IP-Modell nicht weiter definiert und variiert von Netzwerk zu Netzwerk und Host zu Host ab. Dieses Modell macht an dieser Stelle vielmehr Gebrauch von bereits vorhandenen Protokollen, wie z.B. Ethernet (IEEE 802.3), Serial Line IP (SLIP), etc.



TCP Three-Way-Handshake:

1. Kontakt mit anderem Computer aufnehmen, indem Nachricht x gesendet wird.
2. Nun antwortet der Server mit der Sequenz, die er vom Client bekommen hatte, jedoch wurde zu dieser Sequenz plus eins dazu gerechnet.
3. Um Verbindung endgültig aufzubauen, antwortet der Client noch ein letztes mal.