

Лекція 4.

Тема. Мережеве забезпечення глобальних систем обробки та обміну інформацією.

Розділ. Стек протоколів TCP/IP.

План лекції:

- 4.1. Місце стеку протоколів TCP/IP в моделі OSI.
- 4.2. Склад стеку протоколів TCP/IP.
- 4.3. Протоколи фізичного рівня. Протокол RS-232, 802.11 Wi-Fi, IRDA.
- 4.4. Протоколи канального рівня. Протокол Ethernet, ARP.
- 4.5. Протоколи мережевого рівня. Протокол IP.
- 4.6. Протоколи транспортного рівня. Протоколи TCP, UDP.
- 4.7. Протоколи сеансового рівня. Протокол DNS.
- 4.8. Протоколи представницького та прикладного рівня. Протоколи FTP, HTTP, IMAP4, Telnet, SMTP, POP3.

4.1. Місце стеку протоколів TCP/IP в моделі OSI.

Типи даних, які використовує модель OSI.

Модель OSI		
Тип даних	Рівень (layer)	Функції
Байти, Слова	7. Прикладний (application)	Доступ до мережевих служб
	6. Представницький (presentation)	Представлення і кодування даних
	5. Сеансовий (session)	Управління сеансом зв'язку
Сегменти	4. Транспортний (transport)	Прямий зв'язок між кінцевими пунктами і надійність
Пакети	3. Мережевий (network)	Визначення маршруту і логічна адресація
Кадри	2. Канальний (data link)	Фізична адресація
Біти	1. Фізичний (physical)	Робота з середовищем передачі, сигналами і двійковими даними

У літературі найчастіше прийнято починати опис рівнів моделі OSI з 7-го рівня, названого прикладним, на якому користувальницькі додатки звертаються до мережі. Модель OSI закінчується 1-м рівнем - фізичним, на якому визначені стандарти, пропоновані незалежними виробниками для середовища передачі даних:

- тип передавального середовища (мідний кабель, оптоволокно, радіоефір та ін),

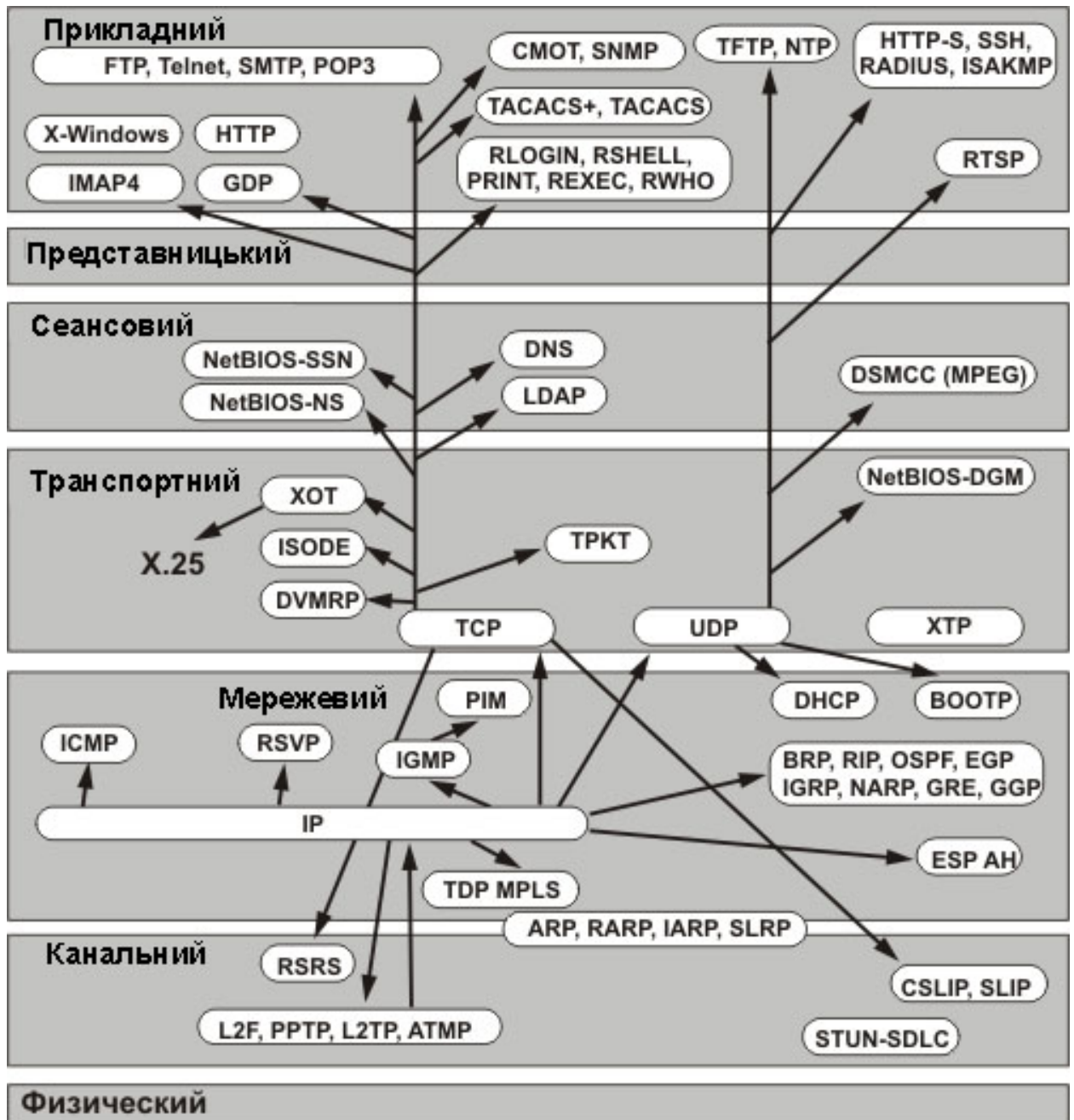
- тип модуляції сигналу,
- сигнальні рівні логічних дискретних станів (нуля і одиниці).

Будь-який протокол моделі OSI повинен взаємодіяти або з протоколами свого рівня, або з протоколами на одиницю вище і / або нижче свого рівня. Взаємодії з протоколами свого рівня називаються горизонтальними, а з рівнями на одиницю вище або нижче - вертикальними. Будь-який протокол моделі OSI може виконувати лише функції свого рівня і не може виконувати функцій іншого рівня, що не виконується в протоколах альтернативних моделей.

Кожному рівню з деякою часткою умовності відповідає свій операнд - логічно неподільний елемент даних, яким на окремому рівні можна оперувати в рамках моделі і використаних протоколів: на фізичному рівні найдрібніша одиниця - біт, на канальному рівні інформація об'єднана в кадри, на мережевому - в пакети (датаграми), на транспортному - в сегменти. Будь-який фрагмент даних, логічно об'єднаних для передачі - кадр, пакет, датаграма - вважається повідомленням. Саме повідомлення в загальному вигляді є операндами сеансового, представницького і прикладного рівнів.

До базових мережних технологій відносяться фізичний і канальний рівні.

4.2. Склад протоколів TCP/IP.



Розподілення протоколів по рівням моделі OSI

Розподілення протоколів по рівням моделі OSI		
7	Прикладний	напр., HTTP, SMTP, SNMP, FTP, Telnet, SSH, SCP, SMB, NFS, RTSP, BGP
6	Представницький	напр., XDR, AFP, TLS, SSL
5	Сеансовий	напр., ISO 8327 / CCITT X.225, RPC, NetBIOS, PPTP, L2TP, ASP
4	Транспортний	напр., TCP, UDP, SCTP, SPX, RTP, ATP, DCCP, GRE
3	Мережевий	напр., IP, ICMP, IGMP, CLNP, OSPF, RIP, IPX, DDP
2	Канальний	напр., Ethernet, Token ring, HDLC, PPP, X.25, Frame relay, ISDN, ATM, MPLS, ARP, RARP
1	Фізичний	напр., електричні провідники, радіозв'язок, волоконно-оптичні провідники, інфрачервоне випромінювання

Зазвичай в стеці TCP / IP верхні 3 рівня (прикладний, представницький і сеансовий) моделі OSI об'єднують в один - прикладний. Оскільки в такому стеку не передбачається уніфікований протокол передачі даних, функції з визначення типу даних передаються додаткам. Спрощену інтерпретацію стека TCP / IP можна уявити так:

Розподілення протоколів по рівням моделі TCP/IP

4	Прикладний «7 рівень»	напр., HTTP, RTP, FTP, DNS
3	Транспортний	напр., TCP, UDP, SCTP, DCCP (RIP, протоколи маршрутизації, подібні OSPF, що працюють поверх IP, є частинами мережевого рівня)
2	Мережевий	Для TCP/IP це IP (допоміжні протоколи, типу ICMP и IGMP, працюють поверх IP, але також відносяться до мережевого рівня; протокол ARP є самостійним допоміжним протоколом, працюючим поверх фізичного рівня)
1	Канальний	Ethernet, IEEE 802.11 Wireless Ethernet, SLIP, Token Ring, ATM и MPLS, фізичне середовище та принципи кодування інформації, T1, E1

Фізичний рівень

Фізичний рівень описує середовище передачі даних (будь то коаксіальний кабель, вита пара, оптичне волокно чи радіоканал), фізичні характеристики такого середовища і принцип передачі даних (поділ каналів, модуляція, амплітуда сигналів, частота сигналів, спосіб синхронізації передачі, час очікування відповіді і максимальна відстань).

Канальний рівень

Канальний рівень описує, яким чином передаються пакети даних через фізичний рівень, включаючи кодування (тобто спеціальні послідовності біт, що визначають початок і кінець пакету даних). Ethernet, наприклад, в полях заголовка пакета містить вказівку того, якій машині або машинам в мережі призначений цей пакет.

Приклади протоколів канального рівня - Ethernet, IEEE 802.11 Wireless Ethernet, SLIP, Token Ring, ATM і MPLS.

PPP не зовсім вписується в таке визначення, тому зазвичай описується у вигляді пари протоколів HDLC / SDLC.

MPLS займає проміжне положення між канальним і мережним рівнем і, строго кажучи, його не можна віднести ні до одного з них.

Канальний рівень іноді поділяють на 2 підрівня - LLC і MAC.

Мережевий рівень

Мережевий рівень спочатку розроблений для передачі даних з однієї (під) мережі в іншу. Прикладами такого протоколу є X.25 і IP в мережі ARPANET.

З розвитком концепції глобальної мережі в рівень були внесені додаткові можливості по передачі з будь-якої мережі в будь-яку мережу, незалежно від протоколів нижнього рівня, а також можливість запитувати дані від віддаленої сторони, наприклад, в протоколі ICMP (використовується для передачі діагностичної інформації IP-з'єднання) і IGMP (використовується для управління multicast-потоками).

ICMP і IGMP розташовані над IP і повинні потрапити на наступний - транспортний - рівень, але функціонально є протоколами мережевого рівня, і тому їх неможливо вписати в модель OSI.

Пакети мережевого протоколу IP можуть містити код, який вказує, який саме протокол наступного рівня потрібно використовувати, щоб витягти дані з пакета. Це число - унікальний IP-номер протоколу. ICMP і IGMP мають номери, відповідно, 1 і 2.

До цього рівня відносяться: DHCP, DVMRP, ICMP, IGMP, MARS, PIM, RIP, RIP2, RSVP

Транспортний рівень

Протоколи транспортного рівня можуть вирішувати проблему

негарантованої доставки повідомлень («чи дійшло повідомлення до адресата?»), А також гарантувати правильну послідовність приходу даних. У стеці TCP/IP транспортні протоколи визначають, для якого саме застосування призначені ці дані.

Протоколи автоматичної маршрутизації, логічно представлені на цьому рівні (оскільки працюють поверх IP), насправді є частиною протоколів мережевого рівня, наприклад, OSPF (IP ідентифікатор 89).

TCP (IP ідентифікатор 6) - «гарантований» транспортний механізм з попереднім встановленням з'єднання надає додаткам надійний потік даних, що дає впевненість у безпомилковості отриманих даних, перезапитує дані у випадку втрати та усуває дублювання даних. TCP дозволяє регулювати навантаження на мережу, а також зменшувати час очікування даних при передачі на великі відстані. Більш того, TCP гарантує, що отримані дані були відправлені точно в тій же послідовності. В цьому його головна відмінність від UDP.

UDP (IP ідентифікатор 17) протокол передачі датаграм без встановлення з'єднання. Також його називають протоколом «ненадійної» передачі в сенсі неможливості упевнитися в доставці повідомлення адресату, а також можливого перемішування пакетів. У додатках, що вимагають гарантованої передачі даних, використовується протокол TCP.

UDP зазвичай використовується в таких додатках, як потокове відео і комп'ютерні ігри, де допускається втрата пакетів, а повторний запит утруднений або невиправданий, або в додатках типу запит-відповідь (наприклад, запити до DNS), де створення з'єднання займає більше ресурсів, ніж повторна відправка.

І TCP і UDP використовують для визначення протоколу верхнього рівня число, зване портом.

Прикладний рівень

На прикладному рівні працює більшість мережевих додатків.

Ці програми мають свої власні протоколи обміну інформацією, наприклад, HTTP для WWW, FTP (передача файлів), SMTP (електронна пошта), SSH (безпечне з'єднання з віддаленою машиною), DNS (перетворення символічних імен в IP-адреси) та багато інших.

У масі своїй ці протоколи працюють поверх TCP або UDP і прив'язані до певного порту, наприклад:

- HTTP на TCP-порт 80 або 8080,
- FTP на TCP-порт 20 (для передачі даних) і 21 (для керуючих команд),
- SSH на TCP-порт 22,
- запити DNS на порт UDP (рідше TCP) 53,
- оновлення маршрутів по протоколу RIP на UDP-порт 520.

Ці порти визначені Агентством по виділенню імен і унікальних параметрів протоколів (IANA).

До цього рівня відносяться: Echo, Finger, Gopher, HTTP, HTTPS, IMAP,

IMAPS, IRC, NNTP, NTP, POP3, POPS, QOTD, RTSP, SNMP, SSH, Telnet, XDMCP.

4.3. Протоколи фізичного рівня.

Фізичний рівень (англ. physical layer) - нижній рівень моделі, призначений безпосередньо для передачі потоку даних. Здійснює передачу електричних або оптичних сигналів в кабель або в радіоефір і відповідно їх прийом і перетворення в біти даних відповідно до методів кодування цифрових сигналів. Іншими словами, здійснює інтерфейс між мережевим носієм і мережевим пристроєм.

На цьому рівні також працюють концентратори, повторювачі сигналу й медіаконвертери.

Функції фізичного рівня реалізуються на всіх пристроях, підключених до мережі. З боку комп'ютера функції фізичного рівня виконуються мережевим адаптером або послідовним портом. До фізичного рівня відносяться фізичні, електричні і механічні інтерфейси між двома системами. Фізичний рівень визначає такі види середовищ передачі даних як оптоволокло, вита пара, коаксіальний кабель, супутниковий канал передачі даних і т. п. Стандартними типами мережевих інтерфейсів, що відносяться до фізичного рівня, є: V.35, RS-232, RS-485, RJ-11, RJ-45, роз'єми AUI і BNC.

Протоколи фізичного рівня: IEEE 802.15 (Bluetooth), IRDA, EIA RS-232, EIA-422, EIA-423, RS-449, RS-485, DSL, ISDN, SONET / SDH, 802.11 Wi-Fi, Etherloop, GSM Um radio interface, ITU і ITU-T, TransferJet, ARINC 818, G.hn/G.9960.

4.4. Протоколи каналного рівня.

Канальний рівень (англ. Data Link layer) - рівень мережної моделі OSI, призначений для передачі даних вузлам, що знаходяться в тому ж сегменті локальної мережі. Також може використовуватися для виявлення і, якщо можливо, виправлення помилок, що виникли на фізичному рівні.

Прикладами протоколів, що працюють на каналному рівні є Ethernet для локальних мереж (багатовузловий), Point-to-Point Protocol (PPP), HDLC і ADCCP для підключень вузол-вузол (двухвузловий).

Канальний рівень відповідає за доставку кадрів між пристроями, підключеними в одному мережевому сегменті. Кадри каналного рівня не перетинають кордонів мережевого сегменту. Міжмережева маршрутизація і глобальна адресація - це функція вищого рівня, що дозволяє протоколам каналного рівня зосередитися на локальній доставці і адресації.

Заголовок кадру містить апаратні адреси відправника та одержувача, що дозволяє визначити, який пристрій відправив кадр і який пристрій має отримати та обробити його. На відміну від ієрархічних і маршрутизуємих

адрес, апаратні адреси однорівневі. Це означає, що жодна частина адреси не може вказувати на належність до якоїсь логічної або фізичної групи.

Коли пристрої намагаються використовувати середу одночасно, виникають колізії кадрів. Протоколи канального рівня виявляють такі випадки і забезпечують механізми для зменшення їх кількості або ж їх запобігання.

Багато протоколів канального рівня не мають підтвердження про прийом кадру, деякі протоколи навіть не мають контрольної суми для перевірки цілісності кадру. У таких випадках протоколи більш високого рівня повинні забезпечувати управління потоком даних, контроль помилок, підтвердження доставки та ретрансляції втрачених даних.

Специфікація IEEE 802 розділяє цей рівень на 2 підрівня - MAC (Media Access Control), що регулює доступ до поділеного фізичного середовища, та LLC (Logical Link Control), що забезпечує обслуговування мережевого рівня.

ФУНКЦІЇ

1. Отримання доступу до середовища передачі. Забезпечення доступу - найважливіша функція канального рівня. Вона потрібна завжди, за винятком випадків, коли реалізована повнозв'язана топологія (наприклад, два комп'ютери, з'єднаних через кросовер, або комп'ютер з комутатором в повнодуплексному режимі).

2. Виділення меж кадру. Ця задача також вирішується завжди. Серед можливих рішень цієї задачі - резервування певної послідовності, яка позначає початок або кінець кадру.

3. Апаратна адресація (або адресація канального рівня). Потрібна в тому випадку, коли кадр можуть отримати відразу декілька адресатів. У локальних мережах апаратні адреси (MAC-адреси) застосовуються завжди.

4. Забезпечення достовірності прийнятих даних. Під час передачі кадру є ймовірність, що дані спотворені. Важливо це виявити і не намагатися обробити кадр, який містить помилку. Зазвичай на канальному рівні використовуються алгоритми контрольних сум, що дають високу гарантію виявлення помилок.

5. Адресація протоколу верхнього рівня. У процесі декапсуляції вказівка формату вкладеного PDU істотно спрощує обробку інформації, тому найчастіше вказується протокол, що знаходиться в полі даних, за винятком тих випадків, коли в полі даних може знаходитися один-єдиний протокол. На цьому рівні працюють комутатори, мости.

4.5. Протоколи мережевого рівня. Протокол IP.

Протокол мережного рівня (англ. Network layer) - протокол 3-го рівня мережевої моделі OSI, призначається для визначення шляху передачі даних. Відповідає за трансляцію логічних адрес та імен у фізичні, визначення найкоротших маршрутів, комутацію і маршрутизацію, відстеження неполадок і заторів у мережі. На цьому рівні працює такий мережний

пристрій, як маршрутизатор.

У межах семантики ієрархічного представлення моделі OSI Мережевий рівень відповідає на запити обслуговування від Транспортного рівня і направляє запити обслуговування на Канальний рівень.

Класифікація

Протоколи мережного рівня маршрутизують дані від відправника до отримувача і можуть бути розділені на два класи: протоколи з встановленням з'єднання і без нього.

- Протоколи з встановленням з'єднання починають передачу даних з виклику або встановлення маршруту проходження пакетів від відправника до отримувача. Після чого починають послідовну передачу даних і потім по закінченні передачі розривають зв'язок.

- Протоколи без встановлення з'єднання посилають дані, що містять повну адресну інформацію в кожному пакеті. Кожен пакет містить адресу відправника і отримувача. Далі кожен проміжний мережевий пристрій зчитує адресну інформацію та приймає рішення про маршрутизацію даних. Повідомлення або пакет даних передається від одного проміжного пристрою до іншого до тих пір, поки не буде доставлено отримувачу. Протоколи без встановлення з'єднання не гарантують надходження інформації отримувачу в тому порядку, в якому вона була відправлена, тому різні пакети можуть пройти різними маршрутами. За відновлення порядку даних при використанні мережевих протоколів без встановлення з'єднання відповідають транспортні протоколи.

Функції Мережевого рівня:

- з'єднання: з встановленням з'єднання і без встановлення з'єднання.

Мережевий рівень моделі OSI може бути як з встановленням з'єднання, так і без нього. На відміну від міжмережевого рівня, стек протоколів TCP/IP підтримує тільки протокол IP, який є протоколом без встановлення з'єднання, протоколи з встановленням з'єднання знаходяться на наступних рівнях цієї моделі.

- присвоєння адреси мережевому вузлу.

Кожен хост в мережі повинен мати унікальну адресу, який визначає, де він знаходиться. Ця адреса зазвичай призначається з ієрархічної системи. В Інтернеті адреси відомі як адреси протоколу IP.

- просування даних.

Так як багато мереж розділені на підмережі і з'єднуються з іншими мережами ширококомунікаційними каналами, мережі використовують спеціальні хости, які називаються шлюзами або роутерами (маршрутизаторами) для доставки пакетів між мережами. Це також використовується в інтересах мобільних додатків, коли користувач рухається від однієї програми до іншої, в цьому випадку пакети (повідомлення) повинні слідувати за ним. У протоколі IPv4 така ідея описана, але практично не застосовується. IPv6 містить більш раціональне рішення.

Протоколи

- IPv4/IPv6, Internet Protocol

- DVMRP, Distance Vector Multicast Routing Protocol
- ARP, Address Resolution Protocol
- ICMP, Internet Control Message Protocol
- IGMP, Internet Group Multicast Protocol
- PIM-SM, Protocol Independent Multicast Sparse Mode
- PIM-DM, Protocol Independent Multicast Dense Mode
- IPsec, Internet Protocol Security
- IPX, Internetwork Packet Exchange
- RIP, Routing Information Protocol
- DDP, Datagram Delivery Protocol

4.6. Протоколи транспортного рівня. Протоколи TCP, UDP.

Транспортний рівень (англ. Transport layer) - 4-й рівень мережевої моделі OSI призначений для доставки даних без помилок, втрат і дублювання в тій послідовності, в якій вони були передані. При цьому неважливо, які дані передаються, звідки й куди, тобто він надає сам механізм передачі. Блоки даних він розділяє на фрагменти, розмір яких залежить від протоколу, короткі поєднує в один, а довгі розбиває. Протоколи цього рівня призначені для взаємодії типу вузол-вузол. Приклад: TCP, UDP, SCTP.

Існує безліч класів протоколів транспортного рівня, починаючи від протоколів, які надають тільки основні транспортні функції (наприклад, функції передачі даних без підтвердження прийому) і закінчуючи протоколами, які гарантують доставку в пункт призначення декількох пакетів даних в належній послідовності, мультиплексується кілька потоків даних, забезпечують механізм управління потоками даних і гарантують достовірність прийнятих даних.

Деякі протоколи мережевого рівня, що називаються протоколами без встановлення з'єднання, не гарантують, що дані доставляються за призначенням у тому порядку, в якому вони були послані пристроєм-відправником. Деякі транспортні рівні справляються з цим, збираючи дані в потрібній послідовності до передачі їх на сеансовий рівень. Мультиплексування (multiplexing) даних означає, що транспортний рівень здатний одночасно обробляти декілька потоків даних (потоки можуть надходити і від різних додатків) між двома системами. Механізм управління потоком даних - це механізм, що дозволяє регулювати кількість даних, переданих від однієї системи до іншої. Протоколи транспортного рівня часто мають функцію контролю доставки даних, змушуючи приймаючу систему відправляти підтвердження передавальній стороні про прийом даних.

4.7. Протоколи сеансового рівня. Протокол DNS.

Сеансовий рівень (англ. Session layer) - 5-й рівень мережної моделі OSI, відповідає за підтримання сеансу зв'язку, дозволяючи додаткам взаємодіяти між собою тривалий час. Рівень управляє створенням, завершенням сеансу,

обміном інформацією, синхронізацією завдань, визначенням права на передачу даних і підтримкою сеансу в періоди неактивності додатків. Синхронізація передачі забезпечується вміщенням у потік даних контрольних точок, починаючи з яких відновляється процес при порушенні взаємодії.

Сеанси передачі складаються із запитів і відповідей, які здійснюються між додатками. Служби сеансового рівня зазвичай використовуються в середовищах додатків, в яких необхідне використання віддаленого виклику процедур.

Прикладом протоколів сеансового рівня є протокол сеансового рівня стека протоколів OSI, який відомий як X.235 або ISO 8327. У випадку втрати з'єднання цей протокол може спробувати його відновити. Якщо з'єднання не використовується тривалий час, то протокол сеансового рівня може його закрити і відкрити заново. Він дозволяє проводити передачу в дуплексному або в напівдуплексному режимах і забезпечує наявність контрольних точок в потоці обміну повідомленнями.

Іншими прикладами реалізації сеансового рівня є Zone Information Protocol (ZIP) - протокол AppleTalk, що забезпечує узгодженість процесу зв'язування по імені, а також протокол управління сеансом (англ. Session Control Protocol (SCP)) - протокол рівня сеансу IV стадії проекту розробки стека протоколів DECnet.

В рамках семантичних конструкцій сеансового рівня мережевої архітектури OSI цей рівень відповідає на запити з представницького рівня і здійснює службові запити до транспортному рівню.

Служби.

- Аутентифікація.
- Права доступу.
- Відновлення сеансу (встановлення контрольних точок та відновлення).

Сеансовий рівень моделі OSI відповідає за встановлення контрольних точок та відновлення. Він дозволяє відповідним чином поєднувати і синхронізувати інформацію декількох потоків, можливо від різних джерел.

Прикладом застосування є організація відеоконференцій в мережі, коли звуковий і відео потоки повинні бути синхронізовані для уникнення проблем із синхронізацією руху губ з промовою. Управління правами на участь у розмові гарантує, що той, хто показується на екрані, дійсно є співрозмовником, який в даний момент говорить.

Ще одним застосуванням є передачі в прямому ефірі, в яких необхідно без різких переходів накладати звуковий і відео потоки і переходити від одного потоку до іншого, для уникнення перерв в ефірі або зайвих накладень.

Протоколи

- ADSP, Протокол потоків даних AppleTalk (англ. AppleTalk Data Stream Protocol)
- ASP, Сеансовий протокол AppleTalk (англ. AppleTalk Session Protocol)
- H.245, Call Control Protocol for Multimedia Communication

- ISO-SP, OSI session-layer protocol (X.225, ISO 8327)
- iSNS, Internet Storage Name Service
- L2F, Layer 2 Forwarding Protocol
- L2TP, Layer 2 Tunneling Protocol
- NetBIOS, Network Basic Input Output System
- PAP, Password Authentication Protocol
- PPTP, Point-to-Point Tunneling Protocol
- RPC, Remote Procedure Call Protocol
- RTCP, Real-time Transport Control Protocol
- SMPP, Short Message Peer-to-Peer
- SCP, Session Control Protocol
- SOCKS, мережевий протокол SOCKS
- ZIP, Zone Information Protocol
- SDP, Sockets Direct Protocol

4.8. Протоколи представницького та прикладного рівнів. Протоколи FTP, HTTP, IMAP4, Telnet, SMTP, POP3.

Представницький рівень (Рівень представлення, (англ. Presentation layer) - шостий рівень мережевої моделі OSI.

Цей рівень відповідає за перетворення протоколів і кодування / декодування даних. Запити додатків, отримані з рівня додатків, він перетворить у формат для передачі по мережі, а отримані з мережі дані перетворить у формат, зрозумілий додаткам. На цьому рівні може здійснюватися стиснення / розпакування або кодування / декодування даних, а також перенаправлення запитів іншому мережному ресурсу, якщо вони не можуть бути оброблені локально.

На представницькому рівні інформація, що передається по мережі не змінює змісту. За допомогою засобів, реалізованих на даному рівні, протоколи прикладних програм долають синтаксичні відмінності в представлених даних або ж відмінності в кодах символів, наприклад, погоджуючи представлення даних розширеного двійкового коду обміну інформацією EBCDIC, що використовують мейнфрейми компанії IBM з одного боку і американського стандартного коду обміну інформацією ASCII з іншого.

Іншою функцією, що виконується на представницькому рівні, є кодування і декодування даних, що забезпечує таємність переданих даних відразу для всіх прикладних служб. Щоб вирішити цю задачу, процеси і коди, що знаходяться на представницькому рівні, повинні виконати перетворення даних. Прикладом протоколу, що забезпечує секретний обмін по мережі, є рівень захищених каналів (сокетів) (англ. Secure Sockets Layer - SSL).