1 Počítačové sítě, hierarchický model ISO/OSI. LAN, jejich topologie, technologie a adresování, propojování LAN do internetových struktur, adresování, směrování. IP protokoly (UDP, TCP, ICMP) a jejich aplikace v konkrétních protokolech (HTTP, SMTP, DNS). Výpočty v síťovém prostředí, klient/server, sockety. (A4B33OSS)

1.1 Histrorie internetu

- 1969 Arpanet
- 1982 TCP/IP
- 1991 WWW

1.2 Topologie sítí

- Síť, hvězda, sběrnice, kruh, strom

1.3 ISO/OSI model (International Organization for Standardization/Open Systems Interconnection model)

ISO OSI model je rozdělený na vrstvy. Teorie je taková, že v každé vrstvě se řeší něco jiného a není potřeba znát fungování jiných vrstev. Třeba emailový klient nepozná, jestli mu data přišla přes wifi nebo kabelem. Data vytvořená v aplikační vrstvě (packet) se obalí hlavičkou nižší vrstvy, postupně se uzavírá do dalších a dalších hlaviček, poslední je hlavička ethernetového rámce. Zařízení se vždy dívají jen na hlavičku z vlastní vrstvy

Vrstva	Vrstva anglicky	Protokoly	Název v TCP/IP	Zařízení	Pomůcka
Aplikační	Application	FTP, HTTP, SSH	Aplikační		All
Prezentační	Presentation	CSS, HTML, GIF	x		People
Relační	Session	SQL, SSL, PAP	x		Sleeping
Transportní	Transport	TCP, UDP	Trasportní		Through
Síťová	Network	IP	Síťová	Router	Networking
Spojová	Link	MAC	Spojová	Switch	Lectures
Fyzická	Physical	Ethernet	Spojová	Hub	Fail

Table 1.1: Vrstvy ISO/OSI modelu

- třeba router posílá packety dál podle IP adresy a je mu jedno, jestli to je TCP nebo UDP.

V praxi to ale tak vždy není. Třeba FTP posílá IP adresy uvnitř svého packetu, takže když prochází FTP packet routerem na hranici sítě (bránou), ve kterém se adresy překládají (NAT níže), je potřeba packet rozbalit a upravit IP adresy v něm.

TCP/IP je obecnější model, který má vrstvy jen čtyři.

1.4 Protokoly

1.4.1 Ethernet

- Na fyzické úrovni je nutné řešit, aby nevysílalo víc zařízení najednou, jinak se signál zaruší a nelze ho poslouchat (tomu se říká kolize)
- Kolizím lze předcházet, třeba tím, že každý připojený stroj má přidělený čas k vysílání (tak to řešil protokol token ring)
- Ethernet kolizím nepředchází, ethernet je detekuje. Každé zařízení během vysílání poslouchá, jestli nevysílá někdo jiný. Pokud ano, obě zařízení přestanou hned vysílat a budou opakovat vysílání po náhodné době.
- V ethernetu se data ověřují pomocí Cyclic Redundancy Check (CRC)

1.4.2 ARP (Address Resolution Protocol)

- Převádí IP adresu na MAC adresu
- Odesílatel pošle požadavek "Who has 192.168.37.178", aby zjistil, kdo má danou IP. Dostane odpověď a MAC adresu si uloží do tabulky pro příště.

1.4.3 IP

- Slouží k adresaci strojů v síti

- IPv4: Čtyři čísla po 8 bitech, celkem 32 bitů, má 4 miliardy adres, ale dnes už nestačí
- Adresy jsou rozděleny do menších sítí, ty se udávají maskou
- Maska v IP verzi 4 označuje, kolik bitů na začátku adresy má celá síť stejně, ostatní bity identifikují zařízení uvnitř sítě (např. 192.168.0.0/16)
- IPv6: Osm čísel po 16 bitech, celkem 128 bitů, tj 3*10^38 adres, to už by stačit mělo

1.4.4 NAT

IP adresy uvnitř sítě (třeba 192.168.*.*) nejsou v celém internetu unikátní, taky se jim říká neveřejné. Routery v internetu packety z neveřejných adres mažou. Aby mohly počítače z vnitřních sítí komunikovat se serverem v internetu, musí jim být přidělena veřejná IP adresa, na kterou jim pak server pošle odpověď. Překlad neveřejných IP adres na veřejné obvykle zajišťuje hraniční router sítě (brána) protokolem Network Address Translation (NAT) s pomocí tabulky. Takový router (většinou patří poskytovateli internetu) má několik veřejných IP adres, a když přijde z vnitřní sítě požadavek něco poslat do internetu, uloží si do tabulky neveřejnou IP počítače a k tomu přidělí veřejnou IP. Jakmile přijde odpověď, podívá se do tabulky, aby zjistil, kterému počítači má packet poslat. Při pozdější komunikaci může být veřejná adresa přidělená počítači jiná. Pokud je adres málo, lze pracovat i s porty.

1.4.5 UDP

User Datagram Protocol slouží k posílání packetů přes síť. UDP neumí garantovat, že všechny packety budou doručeny, a že budou doručeny ve správném pořadí. Občas se prostě stane, že se nějaký packet úplně ztratí. UDP se používá u služeb, kde je prioritou čas, a není důležité mít kompletní informace - třeba u online streamů

1.4.6 TCP

Transmission Control Protocol také řídí posílání dat, ale garantuje, že dorazí v pořádku. Spojení je navázáno "handshakem", kdy nejprve stroj A vyšle žádost o spojení (SYN), spojení je potvrzeno strojem B (SYN ACK), a stroj A potvrdí, že bylo spojení úspěšně navázáno (ACK). Každý packet má své číslo, a přijemce musí potvrdit, že packet obdržel odesláním zprávy ACK. Pokud přijetí nepotvrdí (nebo se ACK ztratí), tak bude packet odeslán znovu. TCP se používá u služeb, kde chceme zaručeně správné a kompletní informace a nepotřebujeme je okamžitě - třeba email.

1.4.7 ICMP

Internet control message protocol je nástroj, který informuje o stavu sítě. Jeho součástí je třeba ping nebo traceroute. Zprávy "Destination unreachable" nebo "Time limit exceeded" jsou taky z ICMP - odesílá je router, když maže packet, který se pohyboval

internetem moc dlouho. Stáří IP packetu (Time To Live - TTL v jeho hlavičce) se počítá podle počtu navštívených routerů, číslo se postupně snižuje, na nule je packet smazán, protože zřejmě zabloudil.

1.4.8 HTTP

HyperText Transfer Protocol funguje na principu klient server. Klient posílá serveru požadavky, třeba GET, POST, PUT, DELETE, server je vykonává a odpovídá třímístným číselným kódem:

- 1..: Informativní
- 2..: Vše proběhlo ok (200 OK)
- 3..: Přesměrování
- 4..: Chyba na straně klienta (403 forbidden, 404 not found)
- 5..: Chyba na straně serveru (500 internal server error)

1.4.9 SMTP

Simple mail transfer protocol, stará se o emaily.
A: MAIL FROM <...@...>
B: ok
A: RCPT TO <...@...>
B: ok
A: DATA
B: ok, ukonči data pomocí \n . \n
A: ..... \n . \n
B: ok
A: QUIT
B: bye

1.4.10 DNS

Domain name system překládá doménová jména (google.com) na IP adresy. Domény mají různé řády, třeba v cyber.felk.cvut.cz je cz doména prvního řádu a cyber doména čtvrtého řádu. Domény se registrují u autoritativního serveru. Při požadavku na identifikaci domény se nejprve server podívá do své paměti, a pokud doménu nemá, ptá se dalších serverů. Autoritativní servery sdílí své domény ostatním serverům společně s jejich dobou platnosti.

1.5 Sockety

Socket je způsob komunikace mezi procesy, v rámci pc i přes síť. Jeví se jako soubor a zapisuje se do něj jako do ostatních souborů v POSIX (read, write).

1.6 Bezpečnost

Bezpečnost na síti se řeší dvěma způsoby

- Symetrické klíče: Odesílatel má symetrický klíč, tímto klíčem zašifruje zprávu. Příjemce má stejný klíč a pomocí něj zprávu přečte. Je to výpočetně jednodušší než asymetrické klíče, ale je potřeba vyřešit bezpečné předání klíčů. Taky nejde vůbec poznat, kdo zprávu zašifroval. Jakmile klíč unikne, lze pomocí něj přečíst všechny zprávy.

- Asymetrické klíče: Klíč má dvě části, veřejnou a soukromou. Veřejná část je volně přístupná, a je výpočetně nemožné zjistit z ní soukromý klíč. Server, řekněme banka, má u sebe uložený svůj soukromý klíč. Ten dokáže přečíst všechny zprávy, které byly zašifrovány odpovídajícím veřejným klíčem. Veřejný klíč je registrovaný u certifikační autority danou bankou, certifikační autorita potvrzuje, že klíč opravdu patří bance. Klienti posílají svá data bance zašifrovaná pomocí veřejného klíče, a jediná banka je dokáže pomocí svého soukromého klíče číst. Je ale důležité, aby certifikační autorita (klidně i lokální databáze certifikátů) byla důvěryhodná - viz chyba Superfish u Lenova, hodně hezky to vysvětluje computerphile na youtube.

1.6.1 SSL a TLS

Transport Layer Security je novější verze SSL. Používá symetrickou kryptografii, ale k bezpečnému předání klíčů používá asymetrické klíče. TLS se používá v HTTPS (bezpečné verzi HTTP), komunikace mezi klientem (K) a serverem (S) se navazuje takto:

K: posílá úvodní packet se seznamem podporovaných šifer a verzí TLS

S: odpovídá, posílá šifru a verzi TLS, která se bude používat a svůj veřejný klíč

K: ověří veřejný klíč u sertifikační autority. Pokud je platný, tak vygeneruje symetrický klíč (ve skutečnosti vygeneruje Master secret, to je složitější), ten zašifruje pomocí veřejného klíče a pošle serveru

S: přečte zprávu pomocí svého soukromého klíče, tím získal symetrický klíč. Teď mají obě strany symetrický klíč a mohou komunikovat.

1.6.2 RSA

Asymetrická šifra, která se používá třeba u SSH. Máme náhodná hodně velká prvočísla p a q, a číslo N=p*q, které je veřejně známé. Najdeme e, které je nesoudělné s fí(N) = (p-1)(q-1). Najdeme d, aby e*d = 1 mod fí(N).

Veřejný klíč je (N, e), soukromý klíč je (N, d). Zprávu Z zašifrujeme C = Z^e mod N, a dešifrujeme Z = C^d mod N.

1.6.3 Diffie-Hellmann

Dá se použít k vytvoření symetrického klíče mezi dvěma stranami (Alicí a Bobem) bez pomoci certifikační autority. Máme veřejná čísla p, q, a tajná čísla a od Alice a b od

Boba. Alice pošle Bobovi q^a mod p, a Bob pošle Alici q^b mod p. Z toho mohou oba spočítat klíč K = g^(a*b) mod p, ale po odposlechnutí komunikace nelze kód zjistit.

1.6.4 Man in the middle

Man in the middle (MIM) je útok, během kterého útočník přeruší komunikaci mezi oběma stranami a vede ji přes sebe, u toho pak mění obsah komunikace. V příkladu Diffie-Hellmannovy výměny klíčů může MIM vygenerovat vlastní číslo x, a komunikovat s Alicí pomocí klíče g^(a*x) a s Bobem pomocí klíče g^(x*b), uprostřed zprávy rozbalí, přečte a zašifruje pomocí druhého klíče. Ani jeden z komunikujících se nemůže dozvědět, že komunikace byla narušena.