Univerzita Pardubice
Fakulta elektrotechniky a informatiky

Průmyslové sítě

Studijní opora

Ing. Soňa Neradová, Ph.D.

Průmyslové sítě

Téma I: Modely síťové komunikace

Studijní cíl

Seznámit studenty s modely síťové komunikace, vysvětlit rozdělení do vrstev a popsat funkce jednotlivých vrstev.

Doba nutná k nastudování

2 hodiny

Klíčová slova

Referenční model OSI, protokol, vrstva, model TCP/IP, zapouzdření, protokolová datová jednotka

1 Referenční model ISO/OSI

Referenční síťový model byl vytvořen standardizační organizací ISO (International Organization for Standardization) jako norma OSI (Open System Interconnection, propojování otevřených systémů). Cílem referenčního modelu, je popsat všeobecné principy fungování datových sítí. Tento model se běžně označuje jako model OSI, je složen ze sedmi vrstev a funkce každé vrstvy je podrobně v tomto modelu popsána.

1.1 Vrstvy OSI modelu

V tabulce jsou vypsány jednotlivé vrstvy od nejvyšší vrstvy směrem dolů. Běžně se používá, označení L1 až L7. kde písmeno L je z anglického slova layer (vrstva).

Označení vrstvy	Model OSI
L7	Aplikační vrstva
L6	Prezentační vrstva
L5	Relační vrstva
L4	Transportní vrstva
L3	Síťová vrstva
L2	Linková vrstva
L1	Fyzická vrstva

Obr. 1 — Vrstvy OSI modelu (LAMMLE, 2015)

Aplikační vrstva (Application layer) — tato nejvyšší vrstva vytváří rozhraní mezi komunikačním softwarem hostitele a jakoukoliv potřebnou externí aplikací. Stanovují se potřebné a dostupné systémové zdroje pro komunikaci mezi dvěma zařízeními. Synchronizuje aplikace klient/server. Mezi aplikacemi poskytuje řízení chyb a integritu dat. Poskytuje hostiteli zpracování nezávislé na systému. Je to jediná vrstva, do které má uživatel přístup.

Prezentační vrstva (Presentation layer) — překládá data z nejvyšší aplikační vrstvy tak, aby byla srozumitelná všem nižším vrstvám, a naopak na straně příjemce je převádí do formátu takového, aby je cílová stanice dovedla rozpoznat a předat dané aplikaci tzn. funguje jako překladač dat. Ovládá strukturování dat a vyjednávání syntaxe transferu dat do sedmé vrstvy. Zpracování zahrnuje šifrování a dešifrování, komprimaci a dekomprimaci dat.

Relační vrstva (Session layer) — zabývá se řízením dialogu mezi zařízeními. Určuje začátek, prostředek a konec relace (session) či konverzace, která se odehrává mezi (mezilehlými) aplikacemi.,

Síťová vrstva (Network layer) — Určuje nejlepší cestu (best path) pro doručení paketu napříč sítí. Používá IP adresy, které identifikují zdroj a cíl paketu. Používá datové pakety a pakety s aktualizací tras směrovacích protokolů. Používá se na zařízench směrovač/router a L3 switch.

Linková vrstva (Data link layer) —zajišťuje přenos dat ze síťové vrstvy do fyzické vrstvy. Dohlíží na fyzickou (hardwarovou) adresaci. Zapouzdřuje pakety do rámce. Oznamuje výskyt chyb při přenosu. Používá se na rozhraních síťových zařízení a v počítači je realizována na síťové kartě.

Fyzická vrstva (Physical layer) — přenáší bity v podobě signálu mezi uzly (node). Asistuje při aktivaci, správě a deaktivaci fyzické konektivity mezi zařízeními. Používá zařízení: opakovač (repeater, kabely).

1.1.1 Horní a dolní vrstvy OSI modelu

Rozdělením celého procesu síťové komunikace na jednotlivé vrstvy umožnilo přehledněji popsat činnost a zodpovědnost každé vrstvy. Na obr. 1 jsou vyjmenovány funkce jednotlivých vrstev. Referenční model OSI neurčuje, jaké protokoly budou na této vrstvě pracovat, to je záležitostí modelu TCP/IP. Výhoda vrstevnatého přístupu je v tom, že rozdělení celého procesu komunikace na jednotlivé vrstvy usnadňuje hledání, izolování a odstraňování problémů v síťové infrastruktuře. V síťové terminologii se často odkazuje na různé funkce vyskytující se v síti podle čísla vrstvy modelu OSI, která specifikuje tuto funkcionalitu. Například proces kódování datových bitů pro přenos přes médium probíhá ve vrstvě L1, fyzické vrstvě. Formátování dat tak, aby je bylo možné interpretovat síťovým připojením v notebooku nebo telefonu, je popsáno ve vrstvě L2, vrstvě datového spojení. Jakým způsobem budeme přidělovat IP adresy, jak bude probíhat směrování dat v síti, tak to je záležitost síťové vrstvy L3. Horní vrstvy obsahují tři nejvyšší vrstvy a jejich úkolem je připravit data na další zpracování dolními vrstvami.

Skupina	Označení vrstvy	Název vrstvy	Společné síťové komponenty přidružené k dané vrstvě
Horní vrstvy	L7	Aplikační	Aplikace podporující síť E-mail Webové prohlížeče a servery Přenos souborů Překlad názvů
	L6	Prezentační	
	L5	Relační	
Dolní vrstvy	L4	Transportní	Mechanismy streamování videa a hlasu Seznamy filtrování brány firewall
	L3	Síťová	IP adresování Směrování
	L2	Linková	Karty a ovladače síťového rozhraní Přepínání sítí Připojení k síti WAN
	L1	Fyzická	Fyzické médium (měděná kroucená dvoj bezdrátové vysílače) Rozbočovače a opakovače

Obr. 2 — Horní a dolní vrstvy OSI modelu (LAMMLE, 2015)

2 Protokoly, sady protokolů

Koncová zařízení můžou komunikovat po síti, protože každé zařízení musí dodržovat stejnou sadu pravidel. Tato pravidla se nazývají protokoly a mají mnoho funkcí v síti. Síťové protokoly definují společný formát a sadu pravidel pro výměnu zpráv mezi zařízeními. Protokoly jsou implementovány koncovými zařízeními a zprostředkujícími zařízeními v softwaru, hardwaru nebo obojím. Protokol nebo sada protokolů popisuje procesy jako jsou:

- formát a struktura zprávy,
- jak síťová zařízení sdílejí informace o cestách s jinými sítěmi,
- jak a kam se posílají chybové a systémové zprávy mezi zařízeními,
- navázání a ukončení datového spojení (sezení) (session**).**

Sady protokolů o jsou protokoly, které vzájemně spolupracují. V následující tabulce jsou uvedeny různé typy protokolů, které jsou potřebné k povolení komunikace v jedné nebo více sítích

Tab. 1 – Typy protokolů a jejich popis

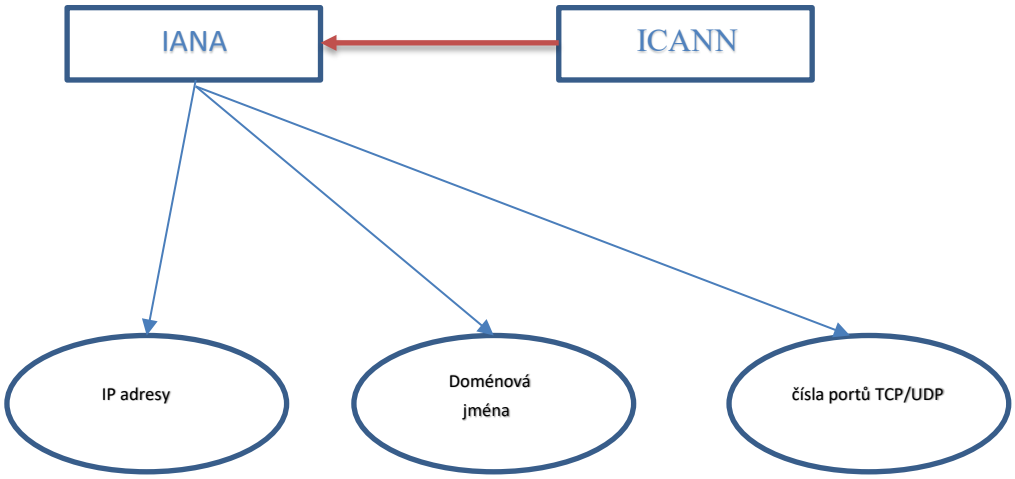
Typ protokolu	Popis protokolu
Síťové komunikační protokoly	Protokoly umožňují dvěma nebo více zařízením komunikovat v jedné nebo více sítích. Rodina technologií Ethernet zahrnuje řadu protokolů, jako je IP, protokol TCP (Transmission Control Protocol), protokol HTTP (HyperText Transfer Protocol) a mnoho dalších.
Protokoly zabezpečení sítě	Protokoly zabezpečují data a zajišťují ověřování, integritu a šifrování dat. Mezi příklady zabezpečených protokolů patří Secure Shell (SSH), SSL (Secure Sockets Layer) a TLS (Transport Layer Security).
Směrovací protokoly	Protokoly umožňují směrovačům vyměňovat si informace o trasách, porovnávat informace o cestě a poté vybrat nejlepší cestu k cílové síti. Mezi směrovací protokoly patří například protokol OSPF (Open Shortest Path First)
Protokoly zjišťování služeb	Protokoly se používají pro automatickou detekci zařízení nebo služeb. Mezi příklady protokolů zjišťování služeb patří protokol DHCP (Dynamic Host Configuration Protocol), který zjišťuje služby pro přidělení IP adresy, a služba DNS (Domain Name System), která se používá k překladu adresy.

Sady protokolů a průmyslové standardy jsou zajišťovány normalizačními organizacemi. Obvykle to jsou neziskové organizace nezávislé na dodavateli založené za účelem vývoje otevřených standardů. Otevřené standardy podporují interoperabilitu, konkurenci a inovace. Zaručují také, že produkt žádné jednotlivé společnosti nemůže monopolizovat trh nebo mít nespravedlivou výhodu nad svou konkurencí. Normalizační organizace může navrhnout soubor pravidel zcela sama, nebo v jiných případech může zvolit proprietární protokol jako základ pro standard. Pokud je použit proprietární protokol, obvykle se jedná o dodavatele, který protokol vytvořil. Standardizační organizace, které starají o vývoj a podporu TCP/IP jsou e IANA a ICANN.

- **ICANN** Internet Corporation for Assigned Names and Numbers tato organizace koordinuje přidělování IP adres, správu doménových jmen a přiřazování dalších informací používaných v protokolech TCP/IP. zastřešuje regionální organizace, které provádějí registrace na jednotlivých kontinentech, pro oblast Evropy je to RIPE NCC[1] (Réseaux IP Européens Network Coordination Centre).

[1] https://www.ripe.net/

- **IANA** Internet Assigned Numbers Authority je prováděcí úřad, který je zodpovědný za přidělování IP adres, správu doménových jmen a identifikátory protokolů TCP/IP. V současné době řídí tuto organizaci nezisková organizace ICANN.



Obr. 3 – Standardizační organizace iCANN a IANA (SOSINSKY, 2010)

3 Vrstvový model TCP/IP

Model TCP/IP dnes představuje nejpoužívanější otevřenou sadu vzájemně spolupracujících protokolů. Je to vlastně protokolová architektura, která přesně popisuje, jakým způsobem fungují jednotlivé protokoly ve vrstvách. Součinnost jednotlivých vrstev je následující postup:

a) Na začátku máme požadavek aplikace v koncovém zařízení (počítači), která potřebuje navázat spojení se serverem ležícím v jiné síti. Pro přístup ke službám sítě aplikace použije protokol na aplikační vrstvě.

b) Z aplikační vrstvy putuje požadavek na spojení do transportní vrstvy. Transportní vrstva rozdělí tok dat na menší části takzvané segmenty. Toto dělení má svůj význam. Pokud bychom přenášeli velké balíky dat najednou, tak se může stát, že data nemohou být doručena např. výpadkem sítě. Proto je lepší posílat menší části, kdy se nám lépe zajišťuje doručení dat i při výpadku nebo nestabilitě síťového spojení. Transportní vrstva má za úkol přenos dat mezi procesy pod operačním systémem v operační paměti na koncových zařízeních to znamená, že musí být rozlišeno z jaké aplikace jde požadavek. Pro rozlišení jednotlivých síťových komunikací na koncovém zařízení (email, chat, použití webového prohlížeče a atd.) používáme softwarové porty. To jsou čísla, která přidělíme jednotlivým komunikacím.

c) Přenos dat na jiné síťové zařízení zajišťuje nižší internetová (síťová) vrstva. Segmenty, které obdržela od vyšší transportní vrstvy zabalí = zapouzdří (encapsulate) do IP paketů. Použije IPv4 nebo IPv6 adresy.

d) Pro vlastní přenos signálu po přenosovém síťovém médiu je následně použita služba vrstvy síťového přístupu, která paket zapouzdří do rámce. Následně je rámec, jeho jednotlivé bity zakódovány do signálu, který je potom přenesen přes přenosové médium. Přenosové síťové médium je realizováno měděným nebo optickým kabelem, nebo bezdrátovým přenosem. Služba vrstvy síťového přístupu je realizována síťovou kartou a realizuje dvě funkce. Jednak ovladač síťové karty spolupracuje s nadřazenou vrstvou (internetovou) a jednak obsahuje fyzickou adresu – MAC adres (Media Access Control).

Vrstvy TCP/IP	**Popis**	**Nejpoužívanější protokoly**
Aplikační	Vstup dat koncového uživatele, plus kódování a dialogové ovládání	HTTP, DNS, DHCP
Transportní	Podpora komunikaci mezi různými zařízeními napříč různými sítěmi.	TCP, UDP
Internetová	Výběr a určení nejlepší cesty v síti	IP /IPv4, IPv6)
Vrstva síťového přístup	Řídí hardwarová zařízení a média, která tvoří síť.	Ethernet, WLAN

Obr. 4 – Vrstvy modelu TCP/IP (SOSINSKY, 2010)

3.1 Porovnání modelu OSI a modelu TCP/IP

Z níže uvedeného obrázku jsou vidět rozdíly v počtu používaných vrstev jednotlivých modelů. V modelu TCP/IP aplikační vrstva slučuje funkce tří vrstev L7, L6 a L5 OSI modelu. Transportní vrstva v TCP/IP modelu rozlišuje spolehlivou a nespolehlivou komunikaci. K tomu využívá protokoly TCP a UDP. Protokol TCP zajišťuje spolehlivé doručení a ve správném pořadí odeslaných dat. Protokol UDP tyto činnosti neprávádí a je tedy rychlejší. Internetová vrstva v TCP/IP a sí´tová v OSI plní stejné funkce tj. Doručení paketů od zdroje k cíli. Vrstva síťového přístupu v TCP/IP se zabývá předáním dat z internetové vrstvy na vybrané síťové přenosové médium.

OSI model	**TCP/IP**
L7 Aplikační	Aplikační
L6 Prezentační	
L5 Relační	
L4 Transportní	Transportní
L3 Síťová	Internetová
L2 Linková	Vrstva síťového přístupu
L1 Fyzická	

Obr. 5 – Porovnání vrstev jednotlivých modelů

4 Protokolové datové jednotky

PDU je označení pro protokolové datové jednotky. Obsahují informace přenášená jako celek mezi komunikujícími entitami. PDU se skládá z:

- Záhlaví (hlavičky) s protokolovou řídicí informací (Protocol control information, PCI), která může obsahovat adresu.
- Vlastních dat (nepovinná).

Protokolové datové jednotky vyšší vrstvy jsou zapouzdřeny (enkapsulovány) do protokolových datových jednotek sousední nižší vrstvy. Vrstvy L7 až L6 pracují s daty, vrstva L4 se segmenty, vrstva L3 s pakety, vrstva L2 s rámci. Vrstva L1 nemá PDU, jedná se pouze o tok bitů.

Označení vrstvy	PDU	Vrstva OSI
L7	Data	Aplikační vrstva
L6	Data	Prezentační vrstva
L5	Data	Relační vrstva
L4	segment	Transportní vrstva
L3	paket	Síťová vrstva
L2	rámec	Linková vrstva
L1	pouze bity	Fyzická vrstva

Obr. 6 – PDU jednotlivých vrstev

4.1 Průchod dat sítí

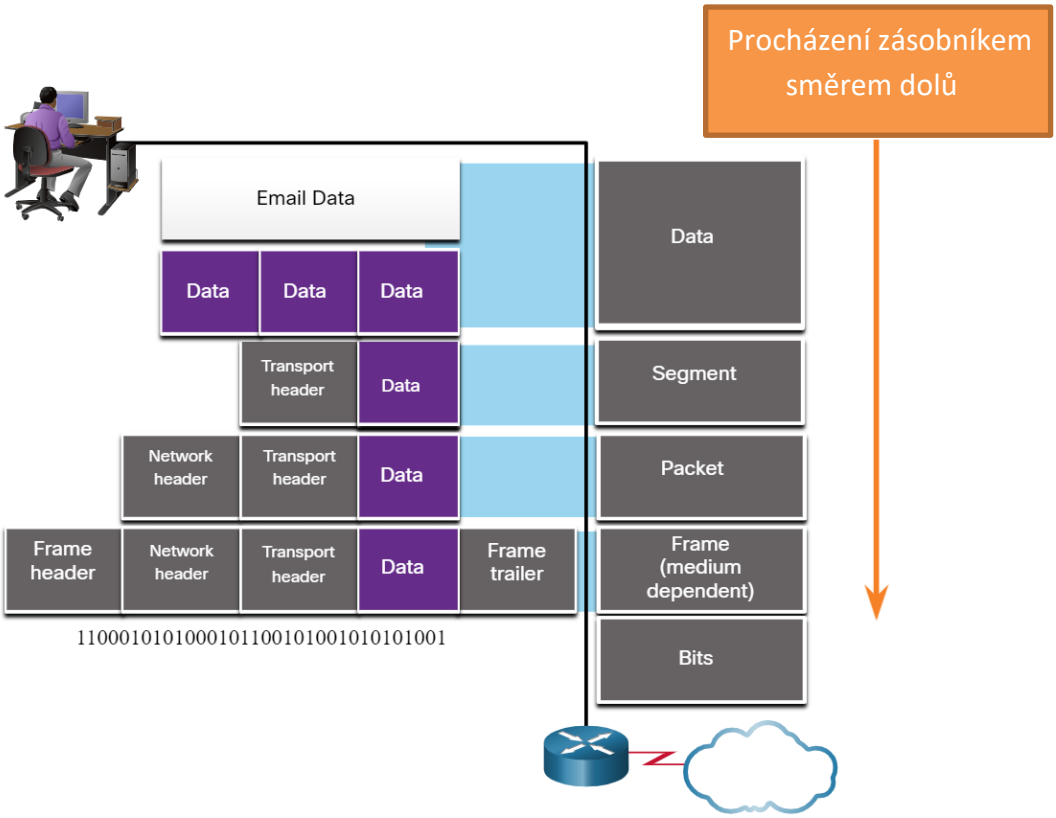
Průchod dat v síti z jednoho koncového systému (instance aplikačního programu na počítači) do druhého probíhá následovně: Aplikační data (například nepřetržitý datový tok, datastream) jsou segmentována a postupně na jednotlivých nižších vrstvách zapouzdřována (encapsulation) tzn. Na jednotlivých vrstvách jsou k datům z předchozí vyšší vrstvy přidávána záhlaví (hlavičky) jednotlivých konkrétní vrstvě příslušných PDU (Protocol Data Unit, datových jednotek protokolu).

Posloupnost datových jednotek (PDU) během síťové komunikace:

aplikační data -> segment -> paket -> rámec -> bit (bit už ale není samostatná PDU)

Data (jednotlivé bity) jsou potom přenášena v binární podobě přenosovým médiem (kanálem) a v druhém systému jsou postupně odpouzdřována (decapsulation) (tj. jsou odstraňovány hlavičky):

bit -> rámec -> paket -> segment -> data až do aplikační vrstvy.



Obr. 7 – Zapouzdřování dat (LAMMLE, 2015)

5 Kontrolní opakovací otázky a úkoly

Jaké vidíte výhody v používání vrstvových modelů?

Jaký vrstvový model je v praxi využíván?

Porovnejte vzájemně jednotlivé vrstvové modely?

Vypište si jednotlivé vrstvy OSI modelu a přiřaďte k nim správné PDU.

Popište funce jednotlivý ch vrstev.

Popište jak vypadá průchod dat v síti, kde je komunikace mezi 2 PC propojenými pouze jedním přepínačem.

Popište jak vypadá průchod dat v síti mezi 2 PC ve znázorněné topologii.

Obr. 8 – Příklad síťové topologie

6 Použitá literatura

Cisco Network Academy. *Netcad.com* [online]. Cisco, 2023 [cit. 2023-01-11]. Dostupné z: Introduction to Network.

LAMMLE, Todd. CCNA: výukový průvodce. Přeložil Jakub GONER. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.

MARSHALL, Perry a John S. RINALDI. Industrial ethernet: how to plan, install, and maintain TCP/IP ethernet networks the basic reference guide for automation and process control engineers. Third Edition. Research Triangle Park, NC: ISA, [2017]. ISBN 978-194-5541-049..

SOSINSKY, Barrie A. Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.

Seznam zkratek

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
HTTP	HyperText Transfer Protocol
ICANN	Internet Corporation for Assigned Names and Numbers
IANA	Internet Assigned Numbers Authority
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
L1	Layer 1
L2	Layer 2
L3	Layer 3
L4	Layer 4
L5	Layer 5
L6	Layer 6
L7	Layer 7
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PCI	Protocol control information

PDU Protocol Data Unit

RIPE NCC Réseaux IP Européens Network Coordination Centre

SSH Secure Shell

SSL Secure Sockets Layer

TLS Transport Layer Security

TCP Transmission control protocol

UDP User Datagram Protocol

WLAN Wireless Local Area Network

Rejstřík

Průmyslové sítě

Téma II: Kabely a propojovací prvky sítě se zaměřením na automatizaci.

Studijní cíl

Seznámit studenty s konstrukcí, složením a značením kabelů.

Doba nutná k nastudování

2 hodiny

Klíčová slova

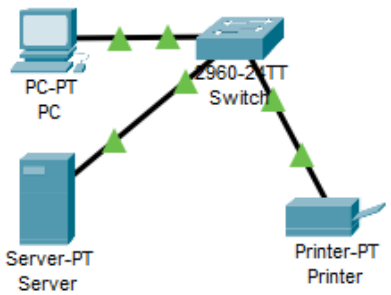
Kabely, struktura, vnější vliv, propojovací kabely, konektory

1 Propojování síťových prvků

Pro propojení jednotlivých zařízení, které se podílejí na síťové komunikaci používáme metalické nebo optické kabely, popřípadě využitím bezdrátových technologií. V této kapitole si popíšeme strukturu metalického kabelu.

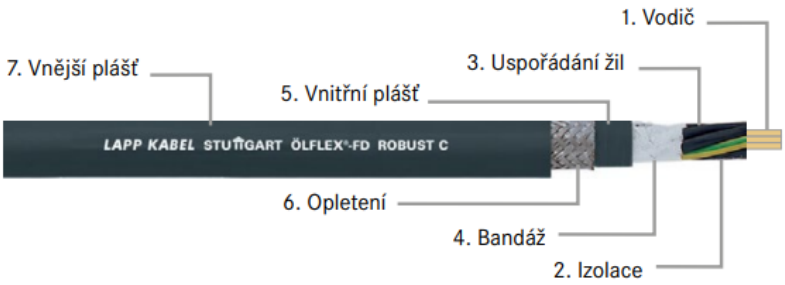
1.1 Kabely

Kabely využíváme k přenosu elektrické energie, k přenosu dat nebo signálů mezi zdrojem a spotřebičem, respektive vysílačem a přijímačem.



Obr. 1– Zapojení kabelů pro datovou komunikaci (vytvořeno v Packet Traceru)

Kabel se skládá z jednoho nebo více vodičů, které jsou obaleny vnějším a vnitřní pláštěm. Je-li jeden vodič sám o sobě tvořen několika tenkými vnitřními dráty, tak se označuje jako lankový vodič a jednotlivé dráty jsou označované jako žíly. V závislosti na požadavcích na odolnost proti elektromagnetickému záření se aplikují různé izolace. Struktura kabelu je znázorněna na níže uvedeném obrázku.



Obr. 2 – Struktura kabelu (LAPP Group, 2023)

2 Struktura kabelu

V následujících částech si podrobně popíšeme jednotlivé části metalických kabelů.

2.1 Vodič

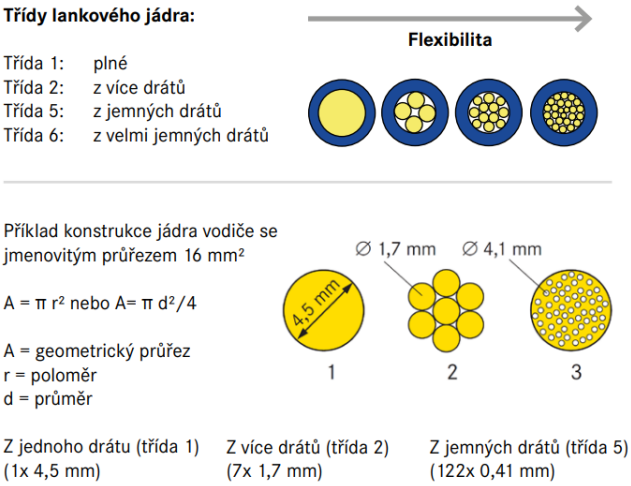
Vodič (konduktor, vodivé jádro) které slouží k přenosu elektrické energie (pro dodávku elektřiny) nebo umožňuje přenášet elektrické impulsy (pro účely datové komunikace). Vodič spolu s izolací tvoří žílu, několik žil tvoří duši kabelu. Jádra vodičů jsou obecně vyrobené z mědi nebo hliníku z důvodů jejich vlastností: vysoká úroveň elektrické vodivosti, vysoká tepelná vodivost a vysoká mechanická pevnost. Vodič mohou být holé nebo pokovené. K ochraně kovového prvku před korozí často slouží povlaky z cínu, zlata, stříbra a niklu. Mechanická flexibilita kabelu je určeno strukturou vodiče. Podle typu konstrukce rozdělujeme na:

- **pevné jádro** – z jednoho drátu (do 16 mm²) nebo z více drátů (dle ČSN EN 60228 třída 1),
- **lankové jádro** – ze 7 až několika set tenkých jednotlivých drátů (VDE 0295/IEC 602258/ČSN EN 60228 rozlišuje lankové jádro třídy 2, 5, 6).

Nejjednodušší konstrukční typ elektrického vodiče je pevný individuální vodič. Má konstantní vnější průměr a díky svému velkému průřezu má vysokou úroveň tuhosti, zatímco vícežilové verze nabízejí vyšší stupeň flexibility.

Rozhodující pro konstrukci jádra je:

- **u jádra třídy 2** minimální počet drátů v jádře a maximální odpor jádra při 20 °C,
- **u jádra třídy 5 a 6** maximální průměr drátu v jádře a maximální odpor jádra při 20 °C.



Obr. 3 – Třídy lankového jádra (LAPP Group, 2022)

2.2 Izolace vodičů

Izolace vodičů slouží k ochraně elektrického vodiče, vytváří elektricky nevodivou ochrannou vrstvu kolem vodiče s cílem zabránit zkratům. Základní a zároveň nejslabší vrstva izolace může být realizována pomocí elektroizolačních laků. Základem elektroizolačních laků jsou téměř výhradně různé polymerní sloučeniny. Ten typ izolace se používá: pro některé typy vodičů (kruhového průřezu), jako impregnace vinutí elektrických strojů a přístrojů a pro látky umožňující povrchovou ochranu součástek, desek plošných spojů, senzorů apod. Další prvky, které se používá jako izolant jsou plasty a elastomery.

Plasty použité na izolaci mají zanedbatelnou elektriku vodivost, nízká schopnost absorpce vody, vysoká tepelná odolnost a vysoká odolnost proti oděru. Izolace je elektricky nevodivá ochranná vrstva kolem vodiče, která izoluje jednotlivé vodiče od sebe navzájem. Izolační materiály se nanáší na vodič vytlačováním. Nejvíce používané izolační materiály jsou sloučeniny organických prvků C, H_2, O_2, N_2, S v Tab.1 jsou uvedené izolanty.

Tab. 1– Používané izolanty zpracováno dle (LAPP Group, 20016)

termoplasty	PVC (polyvinylchlorid), PE (polyolefin),PP (polypropylén), PTFE (polytetrafluoretylen);
elastomery	CR (chloroprenový kaučuk), EPR (Etylenpropylenový kaučuk)
termoplastické elastomery	PUR (recyklovaná PUR pěna), TPE-E (kopolyesterová směs.

Poznámka: pro doplnění je rozvedena charakteristika izolantu chloroprenového kaučuku (CR): je dlouho vyráběn pro své vlastnosti jako je houževnatost a jen pozvolné stárnutí, způsobené teplotou i povětrnostními vlivy; odolává vodě, ozónu, olejům i rozpouštědlům. V ohni zabraňuje šíření plamene, ovšem vytváří dým obsahující chlorovodík a agresivní kyselinu.

2.3 Uspořádaní a identifikace žil

Izolovaný vodič se nazývá žíla. Žíly mohou být uspořádány ve svazcích, párech, vrstvách nebo rovnoběžně (u plochých kabelů). Při výrobě víceżilového kabelu se žíly většinou vzájemně stáčejí a vytvářejí lano. Díky stáčení dosáhneme menších vnějších průměrů kabelu, získá kulatý tvar a je flexibilní.

Obr. 4 – Pletený vodič (Lapp Group, 2022) **Obr. – 5 Kabel do agresivního prostředí (Lapp Group, 2022)**

Pro správné zapojení musíme žíly jednoznačně označit dle normy ČSN 33 0166 ed. 2. (účinnost od 1.5.2014). Jednožilové vodiče a žíly víceżilových vodičů a kabelů se jmenovitým napětím do 1000 V se označují:

a) barvami — všechny žíly jsou rozlišeny různou barvou izolace. Ochranný vodič je kombinací barev **zelená/žlutá;** střední vodič je používána barva **světle modrá**; krajní (fázový) vodič je používána barva **černá, hnědá, šedá**. Označení barvou se musí provádět u konců (zakončení) vodiče, přednostně však po jeho celé délce buď barvou izolace, nebo barevnými značkami (markery), kromě holých vodičů, kde barevné označení musí být u konce vodičů a u připojovacích bodů/míst.

b) písmeno-číslicovým označením — všechny žíly jsou označeny číslicemi vzestupně od 1, většinou bílými číslicemi na černém pozadí (izolace). Výjimkou je ochranný vodič, který je vždy zeleno-žlutý.

Počet žil	Se zelenožlutým vodičem	Bez zelenožlutého vodiče
2		
3		
4		
5		
6 a více	číslované žíly	číslované žíly

Obr. 6 – Označování kabelových žil (LAPP Group, 2022)

2.4 Bandáž

Pro oddělení žil od vnitřního pláště. Používá se netkaná textilie, hliníková fólie nebo slídová páska. Páska je druh izolačního materiálu z papíru s phlogopitovým slídiem nebo papíru z moscovitého slídy smíchaného se silikonovou pryskyřicí a jiným pojivem a skleněnými vlákny.

2.5 Vnitřní plášť

Úkolem vnitřního pláště je chránit žíly před vnějším měděným nebo ocelovým opletením; někdy je v provedení plastová fólie.

2.6 Opletení

Plní následující funkce: ochrana proti mechanickému poškození, ochrana proti pronikání vlhkosti ty jsou v provedení oplet z ocelových drátů chráněných a elektromagnetická ochrana (EMC) v provedení opletem z pocínovaných měděných drátů, ovinutím měděnými dráty nebo pokovenou fólií.

2.7 Vnější plášť

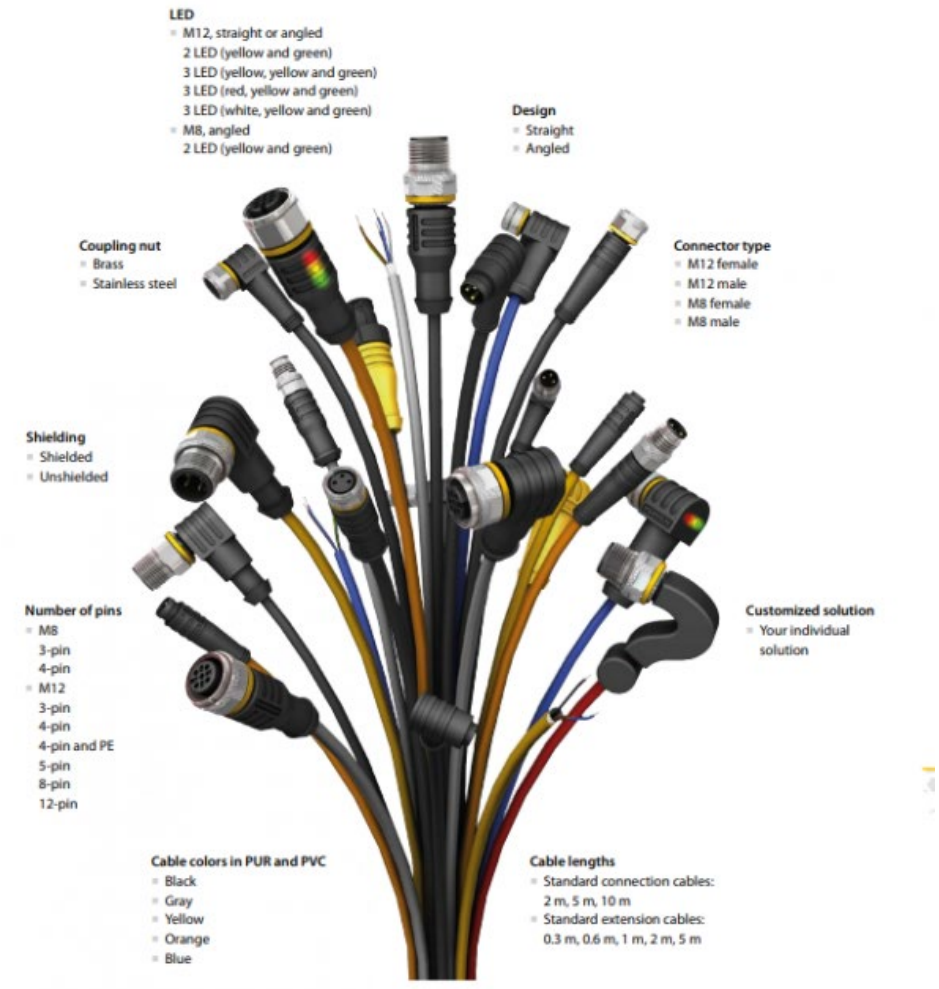
Plášť je uzavřený obal, který chrání pod ním ležící prvky proti vnějším vlivům (mechanickému, tepelnému, chemickému či fyzikálnímu poškození). Rozhodující je správná volba materiálu pláště. V tabulce jsou uvedeny jednotlivé vlivy a možnosti ochrany proti nim.

Tab. 2 – Ochrana proti vnějším vlivům zpracováno dle (LAPP Group, 20016)

Mechanické vlivy	Chemické vlivy	Tepelné vlivy	Fyzikální vlivy
oděr, náraz, ohýbání, tah, zkrut (torzní natáčení).	kyseliny, louhy, oleje, rozpouštědla, voda (od 50 °C)	zima, horko	UV záření, radioaktivní záření
opletení z ocelových drátů, nosné prvky, opěrné opletení, ochranné hadice	materiály pláště jako PTFE, ROBUST, PUR; ochranné hadice	směs na plášť s tepelnými stabilizátory, PTFE, silikon	směs na plášť s UV stabilizátory

3 Propojovací kabely a konektory

Kompletní automatizační systém je obsahuje komponenty: snímač, akční člen a řídicí počítač, které spolu komunikují pomocí průmyslové komunikační sítě. Propojení jednotlivých komponent je realizováno různými typy kabelů a konektorů. Konektor je elektromechanické zařízení, které vytváří elektrické spojení mezi dvěma elektronickými součástmi. Tím je zajištěno, že nedojde k omezení výkonu. Rozlišujeme dvě kategorie konektorů samčí a samičí. Samčí část se také nazývá kolík nebo zástrčka a je připojena k samičí části, která přenáší signál, data nebo napájení. Samičí část konektoru se nazývá spojka, pokud je koncovkou kabelu. Existuje celá řada norem pro konektory používané pro připojení elektrických a elektronických zařízení. Jednotlivé specifikace jsou rozdělené: pro pevné a volné konektory, podle používané frekvence, počtu pólů, určují mechanickou konstrukci a další. Počet typů konektorů je rozsáhlý, většina je používána napříč průmyslovými odvětvími, ale existují i orientovaná řešení například na železnici (propojení vagónů), energetice nebo medicíně. Zavádí se používání flexibilních kulatých konektorů s různým počtem připojovacích vývodů místo připojení senzorů a modulů pevnými kabely. Tento způsob umožňuje rychlejší a snazší výměnu komponent. Většina dodavatelů propojovacích kabelů, je dodává s již pevně připojenými konektory, v různých délkách a barvách. Barvené provedení zpřehledňuje kabeláž a zrychluje činnosti spojené s montáží nebo odstraňování provozních problémů.



Obr. 7 – Příklad provedení používaných průmyslových propojovacích kabelů (Turck, 2022)

4 Kontrolní opakovací otázky a úkoly

Nakreslete strukturu kabelu a popište jednotlivé části.

Jaká je úloha izolace vodičů a jaké jsou způsoby provedení?

Uveďte používané izolanty.

Jaká norma definuje označení žil?

Jakým způsobem se realizuje bandáž?

Jaký je účel vnějšího pláště?

Jaký je účel konektoru, v jakém provedení mohou být realizovány?

Co ovlivňuje výběr kabelu nebo konektoru v automatizační technice?

5 Použitá literatura

ČSN EN 60228: Jádra izolovaných kabelů. 1. Hradec Králové: TECHNOR print, 07/2005n. l.

LAPP KABEL. Hlavní katalog 2018/19 [online]. Otrokovice: t LAPP KABEL, 2018, 2018 [cit. 2023-01-10]. Dostupné z: https://lappczech.lappgroup.com/

TURCK. Kabely [online]. Hans Turck GmbH & Co., 2016 [cit. 2023-01-10]. Dostupné z: https://www.turck.cz

Seznam zkratek

C	chlór
CR	chloroprenový kaučuk
ČSN	česká soustava norem
EMC	elektromagnetická kompatibilita
EN	evropské normy
EPR	etylenpropylenový kaučuk
H2	vodík
IEC	International Electrotecnical Commission
N2	dusík
O2	kyslík
PE	polyolefin
PP	polypropylén
PTFE	polytetrafluoretylen
PUR	recyklovaná PUR pěna
PVC	polyvinylchlorid
S	síra
TPE-E	kopolyesterová směs
UV	ultrafialové záření
VDE	Verband der Elektrotechnik

Rejstřík

Průmyslové sítě

Téma III: Základní diagnostika kabeláže

Studijní cíl

Seznámit studenty s parametry kabelů a způsoby jejich ověření. Zásady při realizaci metalické kabeláže.

Doba nutná k nastudování

2 hodiny

Klíčová slova

Kabeláž, rušení, přeslechy, bezpečnost

1 Charakteristika měděné kabeláže

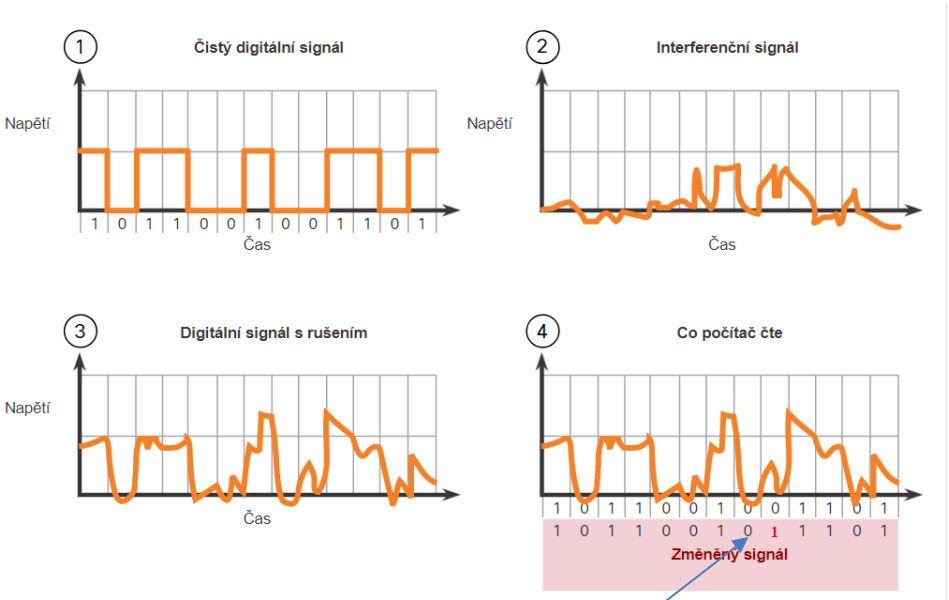
Měděná kabeláž je zatím značně využívaným typem kabeláže používaným v průmyslových sítích. Začínají se prosazovat bezdrátová připojení, zejména v oblastech, kde je obtížné vést kabely například v internetu věcí. Pro přenos velkých objemů dat na páteřních sítích se dnes používají převážně optické kabely. Instalace měděných kabelů se v sítích historicky prosadila, z důvodů v té době nižších nákladů a snadné instalace. Nicméně měděná média jsou však omezena dosahem vzdálenosti bezchybného přenosu dat a rušením signálu během přenosu.

Data jsou přenášena po měděných kabelech v podobě elektrických impulzů. Signál musí překonávát odpor vodiče a tím dochází k jeho slábnutí. Tento je se nazývá útlum (attenuation). Z tohoto důvodu musí všechna měděná média dodržovat předepsané vzdálenosti dle norem.

Zpracování signálu síťovou kartou ovlivňují dva typy rušení:

- Elektromagnetické rušení (EMI) nebo vysokofrekvenční rušení (RFI) – signály EMI a RFI mohou zkreslit a poškodit datové signály přenášené měděnými médii. Mezi potenciální zdroje EMI a RFI patří rádiové vlny a elektromagnetická zařízení, jako jsou zářivky nebo elektromotory.
- Přeslechy - přeslechy jsou rušení způsobené elektrickými nebo magnetickými poli signálu na jednom vodiči k signálu v sousedním vodiči. Situace vzniká, když elektrický proud protéká jedním vodičem, tím se vytváří kolem vodiče magnetického pole, které ovlivňuje sousední vodič.

Eliminování negativním účinkům EMI a RFI se provádí způsobem, že jsou některé typy měděných kabelů obaleny kovovým stíněním a vyžadují správné uzemnění. Zabránění negativním účinkům přeslechů se provádí tím, že mají některé typy měděných kabelů protilehlé páry vodičů zkroucené dohromady, což účinně ruší přeslechy.



Obr. 1 – Vliv rušení na přenos dat (Network Academy, 2023)

Na obrázku 1 v části jedna je zobrazen čistý přenášený signál. V části dvě je zobrazen interferenční signál. Části 3 zobrazuje jak je digitální signál ovlivněn interferenčím signálem. V části 4 je zobrazen změněný signál, který načte síťová karta počítače.

1.1 Měření parametrů kabeláže

Odhalování závad na kroucené dvoulince nebo v celém systému strukturované kabeláže vyžaduje využití měřící přístroje. Zaměříme se na profesionální měřící přístroje firmy Fluke Networks. Lze s nimi testovat kabeláž, vyhledávat vedení nebo provádět testování vyšších vrstev OSI modelu. Některé přístroje jsou dostupné v síťové laboratoři. Návody k měřícím přístrojům a popis měřených parametrů najdeme na stránkách výrobce.

1.2 Testování funkčnosti kabeláže

Nejčastějším problémem, kterým je možné otestovat je správnost zapojení a funkčnost kabeláže. Na obrázku 1 je znázorněn měřící přístroj Fluke Networks CableIQ — Tester kabelů pomocí kterého je proveden wiremap test. Tento test kontroluje správné zapojení jednotlivých párů v zásuvce nebo patch panelu. Další funkcionalitou je kontrola průchodnosti signálu po celé délce kabelu nebo-li dokáže upozornit na přerušení některého z vodičů popř. detekovat jejich zkrat. Provedení testu spočívá v připojení kabelu do přístroje a do adaptéru, otočením přepínače do polohy Autotest. Stiskneme TEST a vyčkáme dokončení testování. Po skončení testování se zobrazí seznam podporovaných standardů a pomocí navigačních kláves a funkčních kláves je možné procházet výsledky. Autostest provede otestování kabeláže a zobrazí podporované rychlosti a normy

Ethernetu, délku kabeláže a zapojení jednotlivých vodičů. Přístroj změří hodnoty přeslechu a impedance, a je tak možné odhalit další problémy, kromě špatného zapojení vodičů nebo přerušeného vedení.

Obr. 2 – Autotest kabelu s připojeným wiremap adaptérem (FlukeTestery, 2023)

1.2.1 CableIQ

Přístroj CableIQ slouží především k testování parametrů kabeláže, testuje podporované rychlosti, přeslechy, impedanční rozdíly, přerušené vedení a správné propojení jednotlivých vodičů. Také ho lze využít jako zdroj signálu pro sondu IntelliTone Probe. Přístroj podporuje ukládání výsledků a synchronizaci s počítačem. Umožňuje rychlou diagnostiku a má jednoduché, návodné ovládání.

Obr. 3 – Ovládací prvky CableIQ (FlukeTestery, 2023)

1.3 Vyhledávání kabeláže

Při řešení problému s připojením k síti je často nutné zkontrolovat zapojení kabelů. To může představovat kritický bod, protože buď chybí nebo není přesný popis kabeláže. Pomocí měřících přístrojů je možné generovat digitální nebo analogový signál, který je možné vyhledávat pomocí sondy. Sonda Fluke IntelliTone je schopna lokalizovat signál v kabelu na vzdálenost asi deseti centimetrů, pokud se nachází mezi kabelem a sondou překážka (např. zeď) vzdálenost se zkracuje.

Obr. 4 – Sonda IntelliTone (FlukeTestery, 2023)

Pomocí otočného přepínače zapneme sondu a uvedeme ji do jednoho z následujících režimů:

- digitální signál, vysoká citlivost;
- digitální signál, nízká citlivost;
- analogový signál.

Po přepnutí sondy do požadovaného režimu pohybujeme hrotem a vyhledáváme kabel, pokud sonda nalezne signál oznámí to zvukovým signálem a rozsvícením určitého počtu LED podle síly signálu.

Samotnou sondu nelze použít pro vyhledávání signálu, je nutné mít do daného kabelu zapojený další přístroj, který bude generovat signál.

2 Bezpečnost

Při realizaci a provozování měděné přenosové kabeláže je nutné dbát na bezpečnost ze strany elektrického napájení síťových prvků. Riziko elektrického napětí – průraz nebo poškození izolace silového napájecího vedení vede k poškození nízkonapěťových zařízení datových sítí nebo k úrazu personálu. Riziko vzniku ohně při elektrickém zkratu. Hořící plastová izolace produkuje jedovaté zplodiny.

Je nutné dodržovat následující zásady:

- Fyzické oddělení silového a datového kabelového rozvodu.
- Barevné značení jednotlivých druhů vedení.
- Správné připojení konektorů a jejich zapojení do zařízení.
- Pravidelné inspekce stavu a poškození kabelových rozvodů.
- Správné uzemnění jednotlivých zařízení.

3 Kontrolní opakovací otázky a úkoly

Vyjmenujte interferenční vnější signály, které ovlivňují přenos dat?

Jakým způsobem lze eliminovat tyto vlivy?

Jakým způsobem omezíme riziko průrazu nebo poškození izolace silového napájecího vedení, které by vedlo k poškození nízkonapěťových zařízení datových sítí nebo k úrazu zaměstnanců?

Jakým způsoben omezíme riziko vzniku ohně při elektrickém zkratu, které by vedlo k hoření plastové izolace a vzniku jedovatých zplodin?

4 Použitá literatura

Cisco Network Academy. Introduction to Networks [online]. Cisco, 2023 [cit. 2023-01-11]. Dostupné z: netacad.com

Fluke Networks. Test and Troubleshoot [online]. 2023 [cit. 2023-01-11]. Dostupné z: https://www.flukenetworks.com/

LAMMLE, Todd. CCNA: výukový průvodce. Přeložil Jakub GONER. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.

Seznam zkratek

EMI Electromagnetic Interference

RFI Radio Frequency Interference

Rejstřík

Průmyslové sítě

Téma IV: Sběrnice v průmyslových sítích

Studijní cíl

Seznámit studenty s používanými sériovými sběrnicemi RS 232/422/485. Představit síťové topologie, pojmy fieldbus a ethernet.

Doba nutná k nastudování

2 hodiny

Klíčová slova

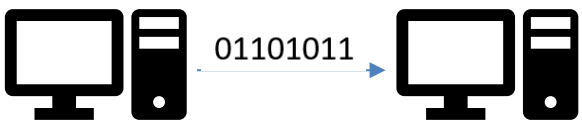
Fieldbus, Ethernet, sériové rozhraní, sběrnice, síťová topologie

1 Úvod do průmyslové komunikace

Cílem průmyslové komunikace je spolehlivý přenos dat od senzorů až po řídicí úroveň. K dosažení tohoto cíle je zapotřebí, aby byly všechny systémy a komponenty vzájemně funkčně propojeny – od snímače až po cloud. Pro propojení řídicích systémů, snímačů a akčních členů se v moderní automatizaci využívají inteligentní sběrnicová propojení. Nicméně v praxi pro přenos dat se pro přenos dat stále používají sériové sběrnice RS 232, RS 422 a RS 485.

1.1 Sériová komunikace

Sériová komunikace nebo sériový přenos je představován jako postupný tok dat komunikačním kanálem nebo po sběrnici po jednotlivých bitech (sekvenčně). Každý bit má hodinovou frekvenci. Osm bitů se přenáší současně s bitem start a stop (tzv. paritní bit), tj. 0 a 1. Sériová sběrnice může používat pro přenos dat a řízení sběrnice jeden vodič nebo více vodičů. Přenos dat se provádí změnou elektrického napětí nebo elektrického proudu, které je technicky náročnější, ale výhodou je větší odolnost proti elektromagnetickému rušení.



Obr. 1 – Sériová komunikace (DTech, 2022)

1.2 Sériové rozhraní RS 232

Standard RS-232 (Recommended Standard 232) popisuje sériové spojení mezi datovým koncovým zařízením (DTE) a zařízením pro přenos dat (DCE) s jeho elektrickými a mechanickými vlastnostmi ve dvoubodovém režimu. Rychlost přenosu záleží na vzdálenosti mezi zařízeními. Maximální délku kabelu omezuje šum dosahuje 15 metrů s běžně používanou rychlostí přenosu 9600 bit/s. Při nejkratší možné vzdálenosti pak rychlost přenosu dosahuje 115,2 kbit/s. Rozhraní RS-232 pracuje v duplexním režimu, což umožňuje současný příjem i odesílání dat, protože se pro příjem a odesílání využívají odlišné vodiče. K přenosu dat dochází v rozhraní RS-232 v digitální podobě, za použití logických hodnot 0 a 1. Rozhraní umožňuje propojení a vzájemnou sériovou komunikaci dvou zařízení, tzn., že jednotlivé bity přenášených dat jsou vysílány postupně za sebou (v sérii) po jednom páru vodičů v každém směru. Nevýhodou linky RS232 je omezená komunikační vzdálenost a nemožnost jejího větvení. Sériová linka se využívá pro prvotní konfiguraci připojeného zařízení např. PLC nebo síťového zařízení např. přepínače. Na daném zařízení se nastaví možnost vzdáleného připojení k tomuto zařízení pomocí zabezpečeného protokolu ssh.

1.3 Sběrnice RS-422

Sběrnice RS-422 používá pro sériovou datovou komunikaci dvouvodičový stíněný kabel typu kroucená dvojlinka, kde jednotlivé logické stavy jsou reprezentovány rozdílovým napětím mezi oběma vodiči. Při základním zapojení sběrnice, tj. použití dvou vodičů, po nichž se vysílají data s diferenciálním kódováním, lze přenos provádět až na vzdálenost 1200 metrů, s přenosovou rychlostí 100 kbps. V případě, že se data přenáší na kratší vzdálenost, může se přenosová rychlost ještě stokrát zvýšil. Do vzdálenosti cca 15 metrů je tak možné dosáhnout rychlosti 10 Mbit/s. Sběrnice RS-422 používá dva páry vodičů, každý pro jeden směr jednosměrný přenos dat z jednoho vysílače do několika přijímačů. Z hlediska zatížení datových linek je počet přijímačů omezen na deset. Při použití dvou RS-422 lze vytvořit náhradu RS-232 pro přenos dat na velké vzdálenosti až několika stovek metrů.

1.4 Sběrnice RS-485

Sběrnice RS-485 je ve stejném provedení jako RS-232 (kroucená dvojlinka), ale používá jeden pár vodičů pro oba směry toku dat. Přenos je poloduplexní a musí být řízení pro směr komunikace. Na rozdíl od RS 232, kde logické úrovně jsou vztaženy k referenční zemi, tak tato sběrnice používá k detekci logického stavu rozdílové napětí mezi oběma vodiči (na vodiči A napětí −2 V, na vodiči B +2 V). Pomocí této sběrnice může komunikovat maximálně 32 vysílačů a 32 přijímačů. Způsob komunikace, kdy přenášená informace se dostane do vícero přijímačů se nazývá multidrop. Přenos dat je za běžných podmínek do vzdálenosti 1200 metrů, přičemž přenosová rychlost může dosahovat hodnot až 10 Mbit/s. Podmínkou je zapojení terminátorů na konce přenosových linek s hodnotou odporu 120 Ω. Funkce terminátorů spočívá v zabránění odrazům signálu od konců vedení a zlepšuje odolnost linky proti rušivým signálům.

V praxi se lze setkat i s čtyřvodičovou verzí RS-485, která nabízí duplexní komunikaci a není zapotřebí řízení směru komunikace.

Obr. 2 – Adaptér RS-232 na RS-485 (DTech, 2022)

2 Síťové topologie

Topologie sítě je grafická reprezentace toho, jak zařízení jsou vzájemně propojeny. V následujícím textu jsou uvedeny typy topologiích používaných v průmyslových sítích.

2.1 Spojení point-to-point

Nejjednodušším spojením je trvalé spojení mezi dvěma zařízeními (point-to-point). Může se jednat o spojení mezi PLC a PC, například. Jednou z klíčových nevýhod zde je, že pokud zařízení musí komunikovat s několika dalšími zařízeními, výhodou je zaručená komunikace mezi zařízeními.

Obr. 3 – Spojení typu point-to-point

2.2 Sběrnicová topologie

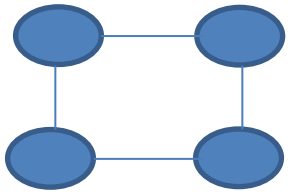
Zařízení zapojená do série za účelem vytvoření liniové topologie označovaná jako topologie sběrnice, jsou všechna zařízení připojena k jednomu přenosovému médiu. Klasické fieldbus systémy jako např. PROFIBUS má tento typ topologie.

Obr. 4 – Spojení typu sběrnice

2.3 Kruhová topologie

Propojením zařízení do kruhové topologie umožníme, že každé zařízení může v podstatě komunikovat s každým jiným zařízením přes dva kanály (ve směru hodinových ručiček, proti

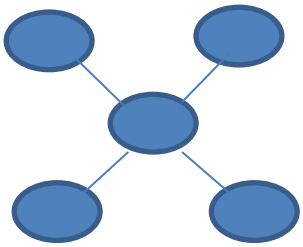
směru hodinových ručiček). A to je hlavní výhoda této struktury: komunikace mezi zařízení je stále zachováno, i když jedna část sítě je přerušeno. Tento typ redundantní kruhové struktury může realizovat například pomocí EtherCat.



Obr. 4 – Spojení typu kruh

2.4 Hvězdicová topologie

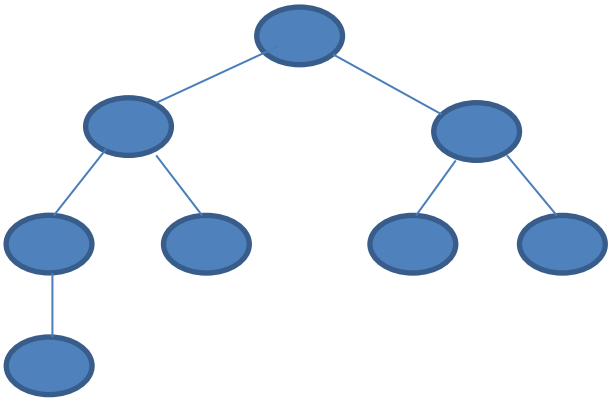
U hvězdicové topologie je vyžadována distribuční komponenta tvoří střed hvězdy. V topologii hvězdy je každý hostitel (uzel) sítě připojen k centrálnímu uzlu. Veškerý provoz, který prochází sítí, prochází centrálním uzlem, který funguje jako zesilovač nebo opakovač signálu.



Obr. 5 – Spojení typu hvězda

2.5 Topologie stromu

Topologie stromu vznikne spojením několika hvězdicových topologie přes centrální/distribuční prvky. Strom má několik centrálních prvků v závislosti na jeho velikosti. Příkladem této topologie je propojení kancelářského ethernetu pomocí přepínačů.



Obr. 6 – Spojení typu strom

Zatímco topologie sítě mohou teoreticky nabývat jakékoli podoby, každá z nich síťová technologie má specifické vlastnosti a omezení potenciálních topologií sítě, které lze použít. Tyto obecně mohou rozlišovat podle komunikačních sítí založených na fieldbus nebo Ethernet.

3 Systém fieldbus a Ethernet

3.1 Fieldbus

Fieldbus vytváří spojení mezi senzory a akčními členy a ovládat počítač. K fieldbusu lze připojit několik zařízení a posílat své zprávy přes stejnou linku. V tomto případě musí být upřesněno, kdo a kdy si může vyměňovat informace. Reálně každý výrobce PLC navrhl svou vlastní fieldbus. Pro z tohoto důvodu existuje mnoho technologií, které se liší od sebe navzájem v nejrůznějších provedení a parametrech například v maximální délce kabelu, přenosové rychlosti nebo v rozsahu funkcí. Mezi nejpoužívanější komunikační standardy typu fieldbus řadíme:

- PROFIBUS® DP – jeden z nejoblíbenějších systémů, který je spojovaný s firmou SIEMENS. Jedná se o otevřený standard. Mnoho výrobců nabízí kompatibilní zařízení a příslušenství. Dobře škálovatelný, poskytuje široký rozsah přenosových rychlostí, a tím i délku jednotlivého kabelu (až 1200 m). Je používán ve většině průmyslových odvětví. Pod názvem PROFIBUS® PA8 se také vyskytuje ve speciální verzi pro procesní automatizaci (rafinérie, chemický průmysl).
- CANopen – standard původně vyvinutý pro vozidla. Stále široce používán v automobilovém průmyslu. Právě s jeho pomocí provádějí autoservisy počítačovou diagnostiku vozidla, i když v automobilovém průmyslu má mnohem širší využití. Po rozšíření o komunikační profil se dostal do průmyslové automatizace, již jako CANopen. Používá se hlavně v Evropě, a v zámoří, díky společnosti Rockwell Automation, má podobu standardu DeviceNet.

3.2 Ethernet

Ethernet je technologie původně vyvinutá pro kancelářskou komunikaci, tj. pro výměnu dat v lokálních datových sítích na bázi PC (LAN); skládá se z řady softwarových a hardwarových komponent. Ethernet umožňuje mnohem vyšší přenosové rychlosti až 400 Gigabit/s. Řada výrobců PLC využila základní vlastnosti ethernetové technologie a upravila je tak, aby byly splněny požadavky na průmyslové aplikace daného prostředí. Základním požadavkem byla schopnost přenášet data v reálném čase, minimalizace zpoždění, zvýšení odolností vůči nepříznivým podmínkám okolního prostředí a elektromagnetického rušení. Dále jsou uvedeny nejpoužívanější ¨příklady průmyslových sběrnic vycházejících z Ethernetu:

- PROFINET® je nejvýznamnějším otevřeným standardem průmyslového Ethernetu v Evropě. Umožňuje výměnu dat v reálném čase mezi řídicími zařízeními a zařízeními pracujícími v řízené soustavě. PROFINET® je nástupcem PROFIBUSu®.

- Modbus TCP je zajímavým příkladem přizpůsobení populárního standardu FIELDBUS. Datový rámec Modbus byl „zabalen“ do Ethernetového rámce, aby se vytvořil otevřený systém, který se nyní stal jedním ze standardů v automatizaci procesů.
- EtherNET/IP je průmyslový sběrnicový systém používaný v řídicích a automatizačních systémech především v Americe. Jednou z klíčových předností tohoto otevřeného standardu je snadná integrace stávajících zařízení v řízené soustavě se sériovým rozhraním RS.
- CC-Link IE je nejvýznamnější standard založený na sítí Ethernet v Asii, nástupce systému CC-Link Fieldbus. Je určen k řízení mnohem většího (ve srovnání s jeho předchůdcem) množství dat.
- POWERLINK je otevřené a fungující v reálném čase rozšíření protokolu základní technologie Ethernet. V současnosti je nejvýznamnějším ethernetovým systémem. Pracuje v reálném čase a je používán v automatizační technice.

4 Kontrolní opakovací otázky a úkoly

Porovnejte vlastnosti a použití jednotlivých sériových sběrnic.

Nakreslete jednotlivé síťové topologie a vysvětlete jejich účel.

Co je Fieldbus a k čemu slouží?

Jaké jsou nejběžnější typy Fieldbus protokolů?

Uveďte příklady využití Fieldbusu v různých průmyslových odvětvích (např. chemický průmysl, výroba automobilů).

Jaký význam má standardizace protokolů Fieldbus pro průmyslové prostředí?

Porovnejte použití protokolů Fieldbas s protokoly na bázi ethernetu.

5 Použitá literatura

DEMBOWSKI, Klaus. Mistrovství v hardware. Brno: Computer Press, 2009. ISBN 978-80-251-2310-2.

[DTech]. In: dtechelectronics*.com* [online]. 2022 [cit. 2022-12-18]. Dostupné z: https://www.dtechelectronics.com/dtech-passive-rs232-to-rs485-standard-converter-high-quality-plug-and-play-db9-adapter_p326.html

LAPP KABEL. Hlavní katalog 2018/19 [online]. Otrokovice: t LAPP KABEL, 2018, 2018 [cit. 2023-01-10]. Dostupné z: https://lappczech.lappgroup.com/

TURCK. Kabely [online]. Hans Turck GmbH & Co., 2016 [cit. 2023-01-10]. Dostupné z: https://www.turck.cz

Seznam zkratek

PC	Personal Computer / osobní počítač
PLC	Programmable Logic controller / programovatelný logický automat
RS-232	sériový port
RS-422	standard sériové komunikace
RS-485	standard sériové komunikace pro průmyslové prostředí
SSH	Secure Shell

Rejstřík

Průmyslové sítě

Téma V: Ethernet a průmyslový Ethernet

Studijní cíl

Seznámit studenty s technologií Ethernet a základními vlastnostmi průmyslového ethernetu.

Doba nutná k nastudování

2 hodiny

Klíčová slova

Ethernet, MAC adresa, vrstvy modelu, LLC, unicast, broadcast, multicast, průmyslový Ethernet

1 Ethernet

Síť Ethernet je standard IEEE 802.3, který popisuje implementaci pro fyzickou a linkovou vrstvu. Je to v současné době nejčastěji používaná technologie v lokálních sítích, která přenos dat realizuje pomocí měděné nebo optické kabeláže.

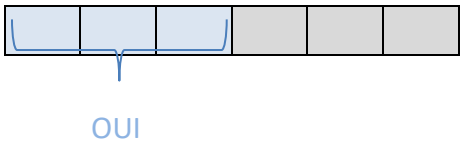
1.1 Adresa L2 vrstvy

Ethernet pracuje na linkové vrstvě s rámci, které obsahují jednoznačný identifikátor síťového zařízení – MAC[i] adresu. V operačním systému Windows ji zobrazíme v příkazovém řádku příkazem *ipconfig /all* pod názvem *Physical Address* (fyzická adresa).

```
C:\Users\user>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : D351
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : spse.cz
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : B8-88-E3-F3-8C-66
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::e691:ef1d:f718:7e6e%16(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.101.0.24(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
```

Obr. 1 – Výpis příkazu ipconfig /all

MAC adresa se skládá ze 48 bitů, standardem pro zápis adresy je šestice dvojciferných hexadecimálních čísel oddělených pomlčkami (např. CA-FE-CA-FE-CA-FE), nicméně často se k zápisu místo pomlček používají dvojtečky. Každý výrobce dostane od sdružení IEEE identifikátor OUI = Organizationally Unique Identifier. Identifikátor představuje nejvyšší 3 byty adresy (polovinu adresy), druhou polovinu si doplňuje samotný výrobce. Pro zjištění výrobce karty lze použít vyhledání pomocí nástroje Wireshark OUI, který obsahuje databázi výrobců (Wireshark · OUI Lookup Tool).



Obr. 2 – MAC adresa (LAMMLE, 2015)

Porovnání adres na L2 a L3

- L3 adresa umožňuje posílat (směrovat) paket do jeho cíle (v jiné síti) – mezi sítěmi.
- L2 adresa umožňuje, aby byl paket (zapouzdřený do rámce) přenášen na lokálním médiu přes segment (lokální) sítě.

1.2 Podvrstvy L2

Linková vrstva se dělí na dvě podvrstvy:

- LLC (Logical Link Control) – tato horní podvrstva IEEE 802.2 zprostředkovává komunikaci mezi síťovým softwarem horních vrstev a hardwarem zařízení na spodních vrstvách. Do rámce umístí informace, které identifikují, který protokol síťové vrstvy se používá. Takto umožníme protokolům vrstvy 3, jako jsou IPv4 a IPv6, používat stejné síťové rozhraní a média. Vrstva je odpovědná za:
  - připojení k vyšším vrstvám,
  - zapouzdření paketů ze síťové vrstvy do rámců,
  - identifikaci protokolu síťové vrstvy.
  - LLC je relativně nezávislá na fyzickém zařízení,
  - LLC je realizována softwarově – ovladačem síťové karty.
- MAC (Media Access Control) – tato spodní podvrstva implementuje IEEE 802.3, 802.11 nebo 802.15 do hardwaru. Je zodpovědná za zapouzdření dat a řízení přístupu k médiím. Poskytuje adresování vrstvy datového spoje a přizpůsobuje strukturu rámce různým technologiím fyzické vrstvy. Tato vrstva je zodpovědná za:
  - zapouzdření dat:
  - ohraničení rámce (synchronizace mezi vysílacím a přijímacím uzlem),
  - adresace (fyzická adresa MAC),
  - detekce chyb (CRC, FCS),
  - řízení přístupu k médiu,
  - řízení umístění a vyjmutí rámce na a z média,
  - zotavení média po chybě.

Ethernet pracuje na vrstvě L1 a L2 modelu OSI.

Poznámka:

Standardy pro L1 až L2 od IEEE, ANSI, ITU jsou zcela konkrétní. Skupina 802 v sobě zahrnuje celou řadu standardů: 802.1q, 802.2, 802.3 atd.

IEEE – Institute of Electrical and Electronics Engineers, Inc. je mezinárodní nezisková profesní organizace pro vývoj průmyslových standardů.

Vrstva modelu OSI	Standard
L2 podvrstva LLC	IEEE 802.2 pro podvrstvu LLC obecné s
L2 podvrstva MAC	IEEE 802.3 Ethernet, 802.11 Wifi
L1 fyzická vrstva	

Obr. 3 – Vrstvy modelu OSI (LAMMLE, 2015)

1.3 Formát ethernetového rámce

V současné době se používá typ rámce Ethernet II a složení je následující:

	64 — 1518 bytů				
8 bytů	6 bytů	6 bytů	2 bytů	46 — 1500 bytů	8 bytů
Preamble and SFD	Destination MAC Address	Source MAC Address	Type	Data	FCS

Obr. 4 – Struktura rámce (SOSINSKY, 2010)

Preambule (Preamble a Start Frame Delimiter) — používá se pro synchronizaci začátku rámce na síťové kartě, k rozpoznání začátku rámce na druhém konci linky.

- Preambule má délku 7 bytů
- SFD má délku 1 byt

Destination MAC Address — cílová MAC adresa je adresa cílového uzlu. Cílová adresa může být unicast, multicast nebo broadcast.

Source MAC Address — zdrojová MAC adresa je adresa vysílajícího uzlu. Zdrojová adresa cílová musí být unicast.

Type — typ nákladu tzv. EtherType, údaj o typu nákladu v těle rámce (typ protokolu vrstvy L3). Vybrané hodnoty:

- 0×0800: IPv4
- 0×0806: ARP
- 0×86DD: IPv6
- 0×8100: VLAN rámce podle 802.1Q

Data — přenášená (payload, užitečný náklad) data z vyšších vrstev.

FCS (Frame Check Sequence) — je kontrolní součet, který se vypočítává ze polí mezi SFD a FCS. Pro výpočet se používá algoritmus typu CRC (Cyclic Redundancy Check). Počítá ho jak odesílatel, tak i příjemce. Když cílové zařízení přijme rámec, vypočte si FCS přes stejná pole, stejně jako odesílatel, a pokud zjistí, že jeho vypočtená hodnota je jiná než ta od odesílatele, považuje rámec za poškozený a zahodí ho.

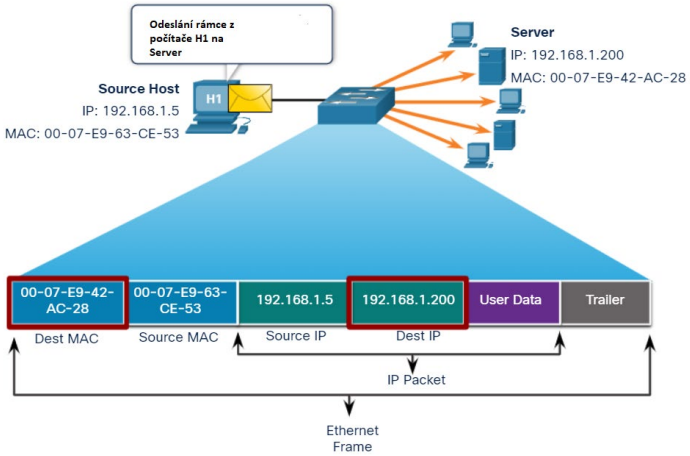
Rámce Ethernet II přenesou až 1500 bytů užitečného nákladu (TCP/IP: MTU=1500).

1.4 Unicast, broadcast a multicast v Ethernetu

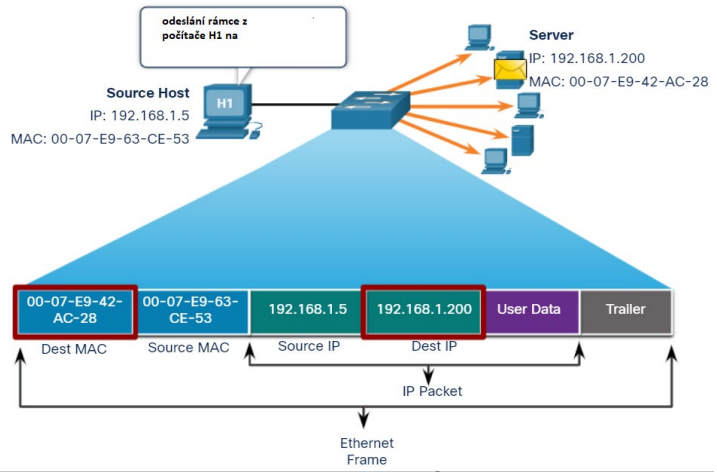
Zasílání dat v sítích probíhá několika způsoby: unicastové, multicastové nebo broadcastové vysílání. Použití konkrétního typu vysílání závisí na protokolu.

1.4.1 Unicast

Unicast je jednosměrové vysílání. IP adresa i MAC adresa reprezentují jeden cíl, jedno konkrétní zařízení, přenos k jednomu uzlu. Standardní komunikace v síti mezi dvěma uzly.



Obr. 5 – Unicastové vysílání ze zdroje (Cisco, 2023)



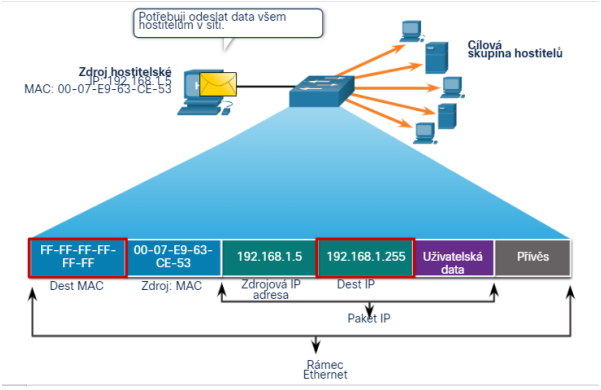
Obr. 6 – příjemce unicastového vysílání (Cisco, 2023)

V příkladu znázorněném na obrázcích požaduje hostitel s adresou IPv4 192.168.1.5 (zdroj) webovou stránku ze serveru na adrese IPv4 jednosměrového vysílání 192.168.1.200. Aby mohl

být paket jednosměrového vysílání odeslán a přijat, musí být v hlavičce paketu IP uvedena cílová adresa IP. Odpovídající cílová adresa MAC musí být také uložena v hlavičce rámce Ethernet. IP adresa a adresa MAC se kombinují a doručují data jednomu konkrétnímu cílovému hostiteli. Zdrojová adresa MAC musí být vždy jednosměrová.

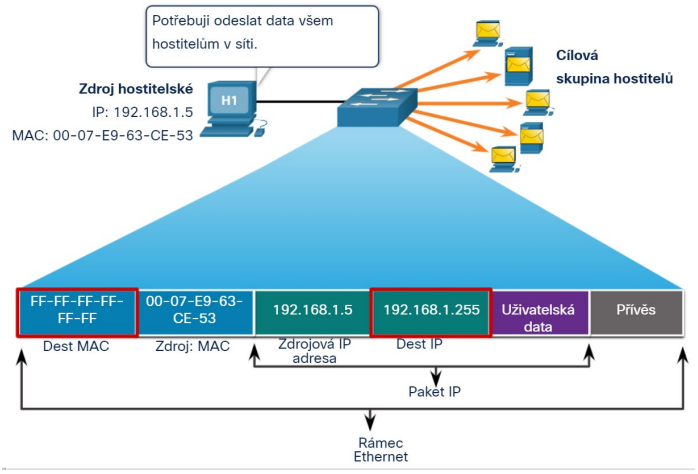
1.4.2 Broadcast

Broadcast je všesměrové vysílání, kdy se provádí přenos ke všem uzlům v rámci broadcastové domény. Broadcastová doména je logická část sítě, ve které mohou připojená zařízení přímo komunikovat tzn. ve které se nachází odesílatel. Rozlišujeme broadcast na L2 a L3 vrstvě. Přepínače propouští L2 broadcast (všesměrové vysílání) a směrovače zastavují L2 broadcast. Rámec broadcastového vysílání je přijímán a zpracováván každým zařízením v síti Ethernet LAN. Má cílovou MAC adresu FF-FF-FF-FF-FF-FF v šestnáctkové soustavě (48 jedniček v binární soustavě).



Obr. 7 – Broadcastové vysílání (Cisco, 2023)

Broadcasty využívají například služby DHCP, ARP. Tvoří velkou část provozu v LAN síti a zatěžují síťový provoz, proto je snaha o jejich minimalizaci.

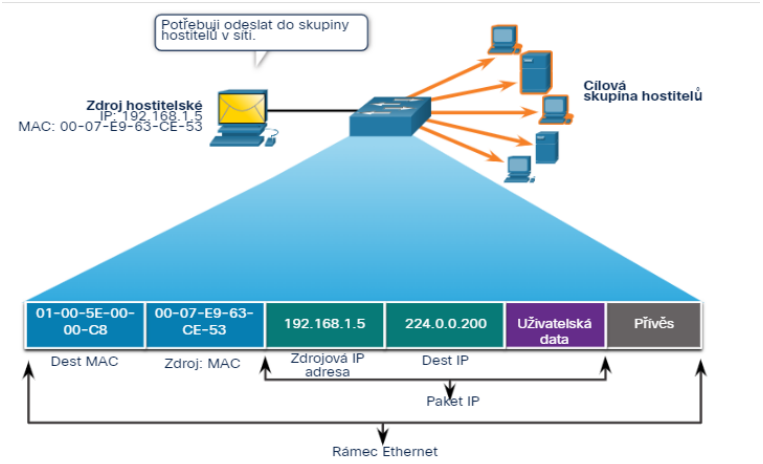


Obr. 8 – Příjemci broadcastového vysílání (Cisco, 2023)

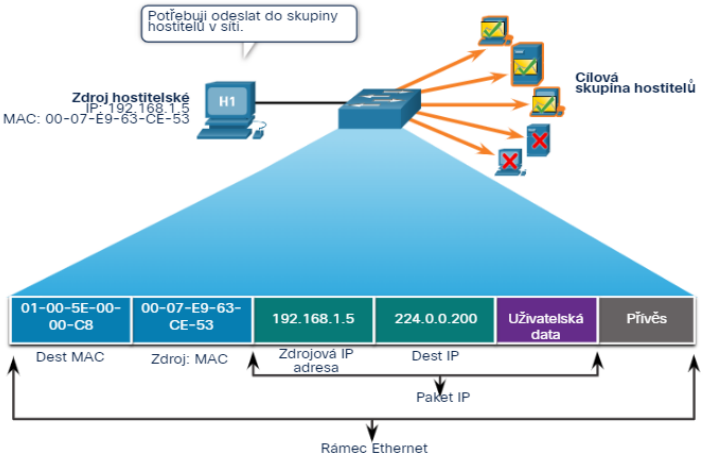
Obrázek 7 a 8 zobrazuje broadcast na L2 vrstvě. Odesílající rámec obsahuje v poli cílovou MAC adresu, kde jsou samé binární jedničky, tedy FF:FF:FF:FF:FF:FF. Rámec se vždy odesílá na všechny porty přepínače mimo příchozího portu.

1.4.3 Multicast

Skupinové (vícesměrové, multicast) je vysílání, které je určeno zařízením, která patří do stejné skupiny. Cílová MAC adresa obsahuje v prvních třech bajtech zleva hodnotu **01-00-5E** a zbytek adres je převod posledních 23 bitů IP adresy skupiny do hexadecimálního tvaru.



Obr. 9 – Multicastové vysílání (Cisco. 2023)



Obr. 10 – Příjemci multicastového vysílání (Cisco, 2023)

Použití multicastového vysílání využívají síťové protokoly pro zasílání speciálních zpráv mezi síťovými zařízeními.

2 Průmyslový Ethernet

Ethernet, který jsme si představili se označuje jako kancelářský ethernet. Rychlost sítě je v tomto případě hlavním kritériem a většinou se pohybujeme v megabitech za sekundu (Mbit/s). Hlavním požadavkem na ethernet při jeho implementaci do průmyslu byla změna jeho komunikačních parametrů s cílem odstranit stochastismus. To znamená, že v průmyslovém ethernetu odesílání a přijímání datových paketů musí proběhnout v přesně požadovaný čas. Tím se nám definovaly dvě klíčové funkcionality: systém reálného času a determinismus.

Systém reálného časuje takový systém, který je schopen správně reagovat na vstupní události do předem stanoveného pevného časového okamžiku. Dva parametry, které mají vliv na tuto skutečnost:

- včasnost (timeliness) – reakce systému (řídicího, komunikačního), kdy systém provede požadovanou operaci do určitého, předem stanoveného času (deadline),
- současnost (synchronism) – synchronizace komunikace jednotlivých zařízení s předepsanou přesností daného časového okamžiku, tj. dodržení určitého tolerančního časového pásma (jitter). Jitter je kolísání zpoždění přenosu mezi dvěma body sítě. Při měření se ignoruje chybovost či ztrátovost. Hodnota je měřena v milisekundách (ms).

Pro dosažení určitého stupně determinismu bylo nutné snížit rychlost odezvy. U kancelářského Ethernetu se jedná o milisekundy, v průmyslu potřebujeme pracovat s podstatně nižšími hodnotami. Minimalizovat časovou nejistotu a tím dosáhnout časového determinismu sítě a synchronní činnosti jejích jednotlivých účastníků lze několika způsoby:

- použití protokolu UDP místo TCP,
- prioritizace zpráv pomocí mechanismu prioritních slotů ve formátu protokolu Ethernet (podle standardu IEEE 802.1p),
- pro úlohy řízení pohybu pohonů použití prioritních zpráv s časovou značkou,
- komunikační modely publisher - subscriber a producer - consumer,
- použití tzv. vysokorychlostních variant Ethernetu,
- segmentování sítě Ethernet.

Mezi další požadavky patří odolnost proti elektromagnetickému rušení, které způsobují zařízení pro přepínání napětí. Omezení vlivu EMI na průmyslovou síť můžeme dosáhnout: oddělením obvodů, používání kroucené dvoulinky, propojením a stíněním.

3 Kontrolní opakovací otázky a úkoly

Jaká je struktura ethernetového rámce?

Jaká adresa je uložena jako první v ethernetovém rámci?

Co je to zakrslý rámec a jakým způsobem se zpracovává?

Vysvětlete princip a příklad použití unicastové komunikace?

Vysvětlete princip a příklad použití broadcastové komunikace?

Kdy se používá multicastové vysílání?

Jaké jsou hlavní vlastnosti systému pracujícího s reálným časem?

4 Použitá literatura

Cisco Network Academy. *Netcad.com* [online]. Cisco, 2023 [cit. 2023-01-11]. Dostupné z: Introduction to Network.

LAMMLE, Todd. CCNA: výukový průvodce. Přeložil Jakub GONER. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.

MARSHALL, Perry a John S. RINALDI. Industrial ethernet: how to plan, install, and maintain TCP/IP ethernet networks the basic reference guide for automation and process control engineers. Third Edition. Research Triangle Park, NC: ISA, [2017]. ISBN 978-194-5541-049..

SOSINSKY, Barrie A. Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.

Seznam zkratek

ANSI	American National Standards Institute
ARP	Address Resolution Protocol
CRC	Cyclic Redundancy Check
DHCP	Dynamic Host Configuration Protocol
FCS	Frame Check Sequence
IEEE	Institute of Electrical and Electronics Engineers
EMI	Electromagnetic Interferenc
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITU	International Telecommunication Union
L1	Layer 1
L2	Layer 2
L3	Layer 3

LLC	Logical Link Control
MAC	Media Access Control
MTU	Maximum Transmission Unit
OSI	Open Systems Interconnection
OUI	Organizationally Unique Identifier
SFD	Start Frame Delimiter
TCP	Transmission Control protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
Wi-fi	Wireless Fidelity

Rejstřík

Průmyslové sítě

Téma VI: Vytváření síťové infrastruktury v simulačním prostředí

Studijní cíl

Seznámit studenty se simulačním síťovým nástrojem Packet Tracer.

Doba nutná k nastudování

2 hodiny

Klíčová slova

Packet Tracer, síťová zařízení, koncová zařízení, switch, router, topologie

1 Simulační a vizualizační nástroj Packet Tracer

Packet Tracer je vhodný softwarový nástroj, který umožňuje vytvářet různé síťové topologie, sledovat síťový provoz, zachytávat pakety a rámce. Umožňuje natrénovat problémové situace, které mohou být způsobeny chybnou konfigurací síťového prvku, Síťová zařízení obsažená v tomto nástroji se z hlediska síťových funkcionalit liší od reálných zařízení jen velmi málo.

1.1 Stažení nástroje Packet Tracer

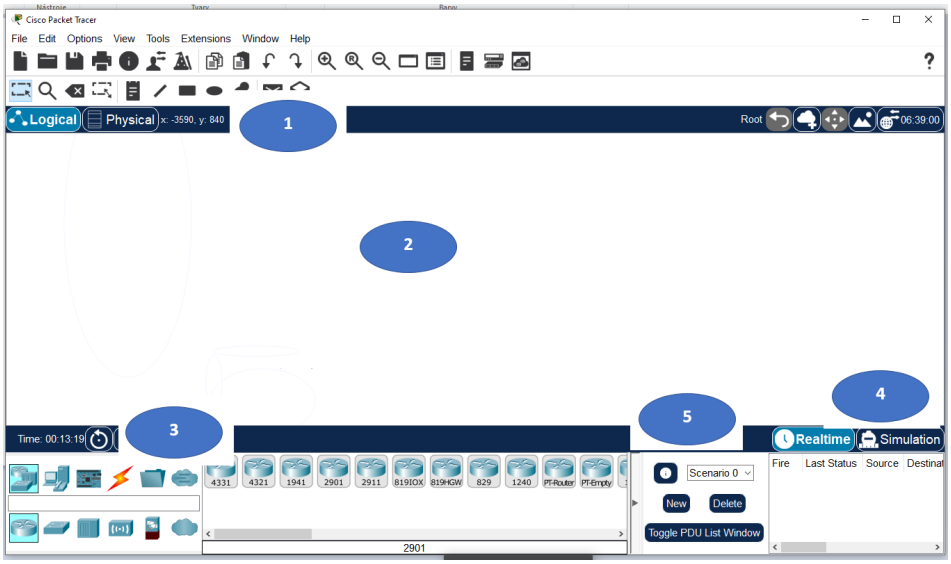
Stažení nástroj dosáhneme v následující krocích:

a) Přihlášením do síťové akademie www.netacad.com na stránku “I'm Learning”.
b) Výběr položky Resources.
c) Výběr položky Download Packet Tracer.
d) Výběr verze Packet Traceru v závislosti na používaném operačním systému.
e) Uložení do počítače.
f) Spuštění instalace programu Packet Tracer.

1.2 Popis prostředí Packet Traceru

Spuštění programu při prvním použití vyžaduje ověření pomocí vašeho e-mailu a hesla. Po spuštění aplikace se zobrazí okno, které můžeme rozdělit na tyto části:

1) Menu programu a panel rychlého spuštění.
2) Pracovní plocha aplikace, na kterou se vkládají všechny prvky a koncová zařízení.
3) Přepínač reálného a simulačního módu.
4) Výběr simulačních scénářů a jejich status.



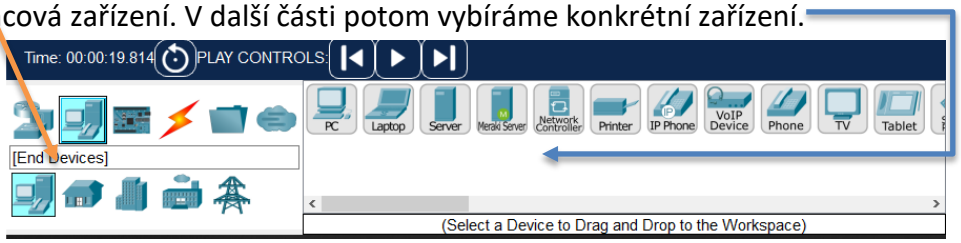
Obr. 1 – Spuštěný program Packet Tracer 8.2.0 (Cisco, 2023)

1.2.1 Vkládání jednotlivých prvků na plochu

Oblast označená číslem 3 na obrázku 1 obsahuje:

- síťová zařízení – směrovače, přepínače, huby, bezdrátové zařízení, firewaly, zařízení WAN sítí,
- koncová zařízení – počítače, stolní počítače, laptopy, servery, telefon, tablety,
- komponenty pro internet věcí – vývojové desky, akční člen, senzory,
- síťová přenosová média – měděnou kabeláž, optický kabel, koaxiální kabel, konzolový kabel a další,
- prvky umožňující propojení více uživatelů

Na obrázku 2 je zobrazena oblast, která slouží pro výběr prvku. Nyní je vybrána skupina – koncová zařízení. V další části potom vybíráme konkrétní zařízení.



Obr. 2 – Oblast sloužící pro výběr prvku (Cisco, 2023)

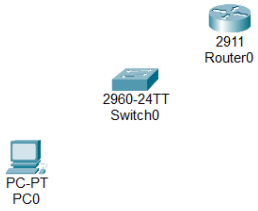
1.3 Vytvoření jednoduché topologie

V následujícím příkladu si vytvoříme jednoduchou topologii, která se bude skládat z počítače připojeného do přepínače pomocí měděného přímého kabelu. Přepínač propojíme stejným způsobem se směrovačem.

Postup:

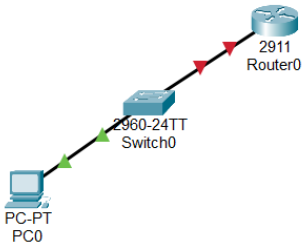
a) Vybereme dle obrázku 2 End Devices (koncová zařízení) a následně vybereme počítač PC a přetáhneme myší ikonu počítače na pracovní plochu.
b) Ve stejné části vybereme Network Devices (síťová zařízení), klikneme na ikonu Switches a vybereme přepínač s označením 2960. Ikonu přetáhneme myší na pracovní plochu.
c) Překlikneme na ikonu Routers a vybereme router s označením 2911. Ikonu přetáhneme myší na pracovní plochu.

Na pracovní ploše budeme mít tři prvky, které propojíme.



Obr. 3 – Výsledek kroků a) až c) (Cisco, 2023)

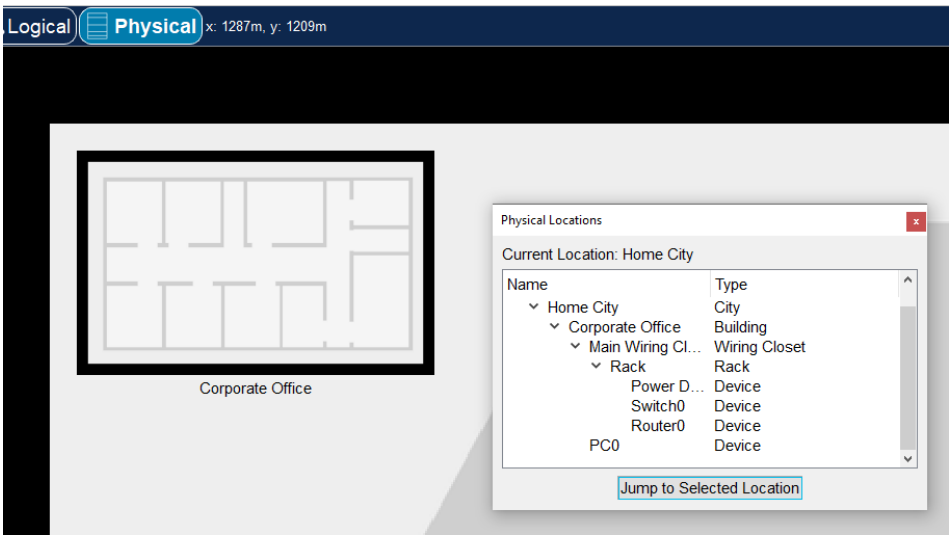
d) Klikneme na ikonu Connections a vybereme přímý kabel (Copper Straight-Through). Klikneme na počítač PC, zobrazí se nabídka připojení, kliknutím vybereme Fastethernet0. Druhý konec kabelu propojíme s přepínačem tak, že si vybereme z dostupných fastethernetových rozhraní. Na přepínači je 24 fastethernetových a 2 gigaethernetové portů.
e) Obdobným způsobem propojíme přepínač se směrovačem. Klikneme na ikonu Connections a vybereme přímý kabel (Copper Straight-Through). Klikneme na přepínač, zobrazí se nabídka připojení, kliknutím vybereme rozhraní Gigabitethernet1 a připojíme ke směrovači, kde si vybereme libovolný Gigabitový port.



Obr. 4 – Propojení vybraných síťových prvků (Cisco, 2023)

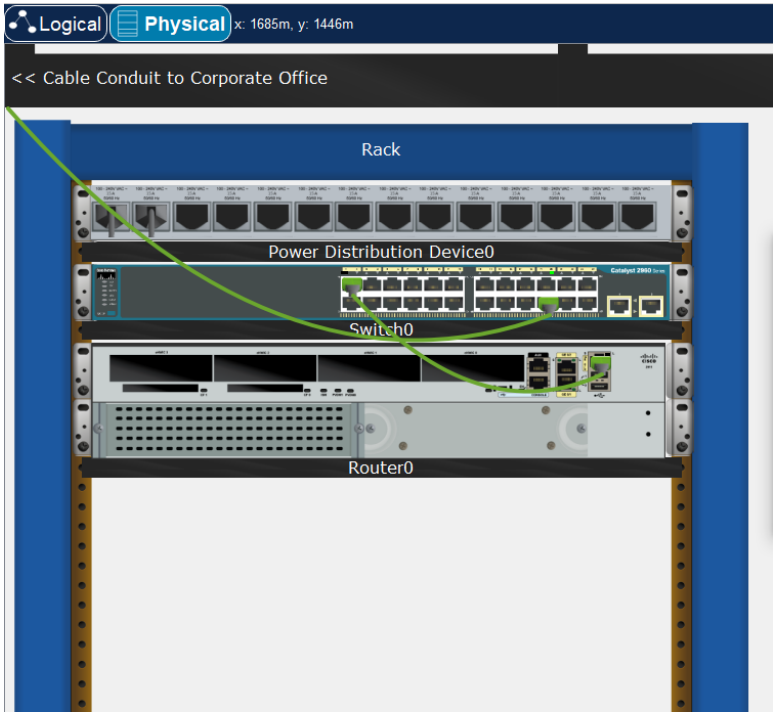
Vytvořili jsme jednoduchou logickou topologii (obr. 4). V horním rohu pracovní plochy se nachází přepínač mezi logickou a fyzickou topologií. Přepnutím na fyzickou topologii si pomocí tlačítka Home City zobrazíme okno Physical Location.

Obr. 5 – Tlačítko pro zobrazení fyzické topologie (Cisco, 2023)



Obr. 6 – Fyzická topologie v Packet Traceru (Cisco. 2023)

V tomto okně si můžeme vybrat oblast, kterou si chceme prohlédnout. Po vybrání položky Rack se zobrazí síťové prvky umístěné v racku včetně propojovacích kabelů.



Obr. 7 – Zobrazení prvků v racku v Packet Traceru (Cisco, 2023)

2 Nastavení směrovače

Nastavování směrovače vyžaduje znalost příkazů a možnosti jednotlivých režimů. Veškeré příkazy IOSu se dají zadávat zkráceně, stačí zadat první znaky, které jednoznačně určí příkaz (tedy, aby v daném kontextu neexistoval jiný příkaz, začínající těmito znaky). Klávesa tabulátor doplňuje/dokončuje příkaz. Zadáme prvních pár písmen příkazu a po stisknutí TAB se příkaz doplní, pokud je jednoznačný, nebo se doplní část, která je pro více příkazů společná. Zadáním

? (otazníku) se zobrazí seznam příkazů s krátkým popiskem, které můžeme na aktuálním místě použít. Také můžeme zadat prvních pár písmen příkazu a otazník, aby se vypsal seznam příkazů s tímto začátkem. Většina příkazů se skládá z posloupnosti klíčových slov, pokud zadáme příkaz ?, dostaneme seznam argumentů či klíčových slov, která se dají zadat na tomto místě. Některé příkazy, které najdeme na reálných síťových Cisco zařízení nejsou obsaženy v síťovém simulátoru Packet Traceru.

2.1 Režimy směrovače

Router> uživatelský režim

Router# privilegovaný režim (oprávněný, režim úrovně EXEC)

Router(config)# globální konfigurační režim

Router(config-if)# režim konfigurace rozhraní

Router(config-line)# režim konfigurace linky

Router(config-router)# režim konfigurace směrovače

Vstup do globálního konfiguračního režimu

Router> uživatelský režim poskytuje jen omezené zobrazení konfigurace. V tomto režimu nelze provádět žádné změny.

Router# privilegovaný režim umožňuje prohlížení konfigurace a provádění změn.

Router# configure terminal tento příkaz umožní přechod do globálního konfiguračního režimu

2.1.1 Konfigurace směrovače probíhá v několika krocích.

Vypsané konfigurační kroky se nemusí provádět v předepsaném pořadí, ale je to doporučný postup.

a) Nastavení názvu směrovače pomocí klíčového slova hostname na název směrovače R1

   Příkaz *Router(config)#hostname R1*

b) Nastavení zabezpečeného privilegovaného režimu EXEC.

   Příkaz *Router(config)# enable secret password*

c) Nastavení zabezpečeného uživatelského režim EXEC.
   Router(config)# line console 0
   Router(config-line)# password password
   Router(config-line)# login

d) Nastavení vzdáleného připojení pomocí protokolu Telnet nebo SSH .
   Router(config-line)# line vty 0 4
   Router(config-line)# password password
   Router(config-line)# login

Router(config-line)# transport input {ssh | telnet}

e) Nastavení šifrování na hesla v konfiguračním souboru

Router(config-line)# exit

Router(config)# service password-encryption

f) Uložení konfigurace
Router(config)# end
Router# copy running-config startup-config

2.1.2 Konfigurace rozhraní směrovače

Dalším krokem je konfigurace rozhraní směrovače. Potřebujeme to z důvodu, že směrovače nejsou dosažitelné koncovými zařízeními, dokud nejsou nakonfigurována jejich rozhraní. Na směrovačích Cisco je k dispozici mnoho různých typů rozhraní. Příkazy pro nastavení rozhraní jsou následující:

Router(config)# interface type-and-number

Router(config-if)# description description-text

Router(config-if)# ip address ipv4-address subnet-mask

Router(config-if)# ipv6 address ipv6-address/prefix-length

Router(config-if)# no shutdown

Poznámka: Je-li povoleno rozhraní směrovače, měly by se zobrazit informační zprávy potvrzující povolené propojení. Tyto zprávy generuje zařízení a mají na začátku oznámení použitý znak procento (%).

Příkaz description není nutný k nastavení rozhraní. Může být užitečný při řešení potíží v produkčních sítích poskytnutím informací o typu připojené sítě a pro dokumentaci síťové topologie. Text popisu je omezen na 240 znaků.

Použití příkazu no shutdown aktivuje rozhraní a je podobné zapnutí rozhraní. Rozhraní musí být také připojeno k jinému zařízení, jako je přepínač nebo směrovač, aby byla fyzická vrstva aktivní.

2.1.3 Konfigurace rozhraní přepínače

Přepínače Cisco IOS vrstvy 2 mají fyzické porty pro připojení zařízení. Tyto porty nepodporují adresy IP vrstvy 3. Proto mají přepínače jedno nebo více přepínačů virtuálních rozhraní (SVIs). Jedná se o virtuální rozhraní, protože v zařízení není žádný fyzický hardware, který je k němu přidružen. SVI se vytváří v softwaru. Pro vzdálený přístup k přepínači musí být v SVI (switch virtual interfaces) nakonfigurována adresa IP a maska podsítě.

Sw1# configure terminal

```
Sw1(config)# interface vlan 1
Sw1(config-if)# ip address 192.168.1.120 255.255.255.0
Sw1(config-if)# no shutdown
Sw1(config-if)# exit
```

Přepínače nakonfigurované s adresou IPv4 musí mít přiřazenou výchozí bránu, kterou je adresa rozhraní lokálního směrovače.

```
Sw1(config)# ip default-gateway 192.168.1.1
```

Po nakonfigurování těchto příkazů má přepínač všechny prvky IPv4 připravené pro komunikaci po síti.

3 Kontrolní opakovací otázky a úkoly

Zkuste si upravit velikost písma postupným výběrem záložky: Options ► Preferences ► Font a následně posuvným měřítkem v části Applications.

Vytvořte si Packet Traceru jednoduchou topologii: zapojte pomocí ethernetových kabelů počítač do přepínače, přepínač do směrovače. Nastavte na počítači IPv4 adresu, masku a bránu. Použijte pro počítač IPv4 adresu 192.168.1.20, masku 255.255.255.192 a výchozí bránu s IPv4 adresou 192.168.1.62. Na přepínači nastavte IPv4 adresu (192.168.1.50, maska 255.255.255.192) tak, aby se dalo k zařízení přistupovat vzdáleně. Nastavte na příslušném rozhraní směrovače IPv4 adresu (192.168.1.62, maska 255.255.255.192).

Procvičte si konfiguraci IP adresy na směrovači. Pomocí příkazu Router#show ip interface brief ověřte správnost nastavení.

Jaké je využití SVI u přepínače?

4 Použitá literatura

Cisco Network Academy. *Netcad.com* [online]. Cisco, 2023 [cit. 2023-01-11]. Dostupné z: Introduction to Network.

LAMMLE, Todd. CCNA: výukový průvodce. Přeložil Jakub GONER. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.

SOSINSKY, Barrie A. Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.

Seznam zkratek

IPv4 Internet Protocol version 4

IOS Internetwork Operating System

PC Personal Computer

SVI Switch Virtual Interfaces

WAN Wide Area Network

Rejstřík

Průmyslové sítě

Téma VII: Protokol ARP

Studijní cíl

Seznámit studenty se činností protokolu ARP s cílem v lokální a vzdálené síti. Popsat strukturu ARP zprávy.

Doba nutná k nastudování

2 hodiny

Klíčová slova

Fyzická a logická adresa, síťová karta, komunikace, protokol ARP

1 Použití fyzické a logické adresy

Síťová komunikace uživatele se realizuje pomocí síťové karty, na které je uložená fyzická adresa. Tato adresa se označuje také jako MAC adresa a je používána protokolovou datovou jednotkou druhé vrstvy k doručení rámce do jiné síťové karty ve stejné síti.

	64 — 1518 bytů				
8 bytů	6 bytů	6 bytů	2 bytů	46 — 1500 bytů	8 bytů
Preamble and SFD	Destination MAC Address	Source MAC Address	Type	Data	FCS

Obr. 1 – Struktura ethernetového rámce (LAMMLE, 2015)

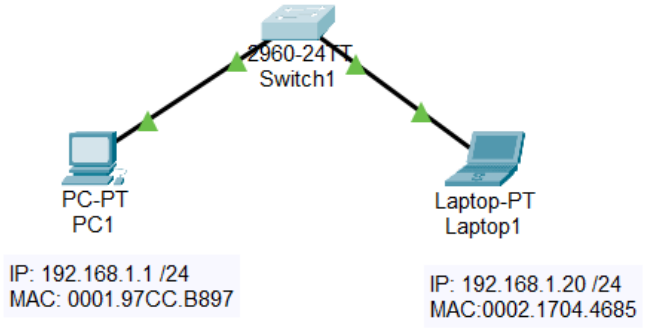
Type — typ nákladu tzv. EtherType, údaj o typu nákladu v těle rámce (typ protokolu vrstvy L3). Vybrané hodnoty:

- 0×0800: IPv4
- 0×0806: ARP

Koncová zařízení jsou propojena v síti pomocí přepínače, který přenáší rámce obsahující cílovou a zdrojovou MAC adresu. Na obrázku 3 je zobrazeno připojení dvou počítačů k přepínači. K přepínači jsou připojena dvě koncová zařízení počítač PC1 a laptop Laptop1. Dále jsou uvedeny jejich fyzické a logické adresy. Logická adresa (IP adresa) – slouží k odeslání paketu ze zdrojového zařízení do cílového zařízení. Cílová adresa IP může být ve stejné síti IP (obr. 3) jako zdrojová nebo může být ve vzdálené síti (obr. 5).

Cílová MAC adresa	Zdrojová MAC adresa	Zdrojová IPv4 adresa	Cílová IPv4 adresa
0001.97CC.B897	0002.1704.4685	192.168.1.1 /24	192.168.1.20 /24

Obr. 2 – Fyzické a logické adresy PC1 a Laptop1 (LAMMLE, 2015)



Obr. 3 – Komunikace s cílem ve stejné síti (Cisco, 2023)

Pokud komunikují zařízení ve stejné síti, tak k dosažení cíle musí znát MAC adresu cíle nebo jeho IP adresu, které budou představovány jiným koncovým zařízením ve stejné síti.

Poznámka: síťové konfigurace jsou provedeny v síťovém simulátoru Packet Tracer, kde je zvolený formát zápisu MAC adresy je xxxx.xxxx.xxxx.

Postup pro výpis fyzické (MAC) adresy na počítači s operačním systémem Windows:

- WINDOWS+R→ napsat cmd a do otevřeného okna napsat ipconfig /all. Vypíší se detaily všech síťových adaptérů včetně jejich MAC adres:

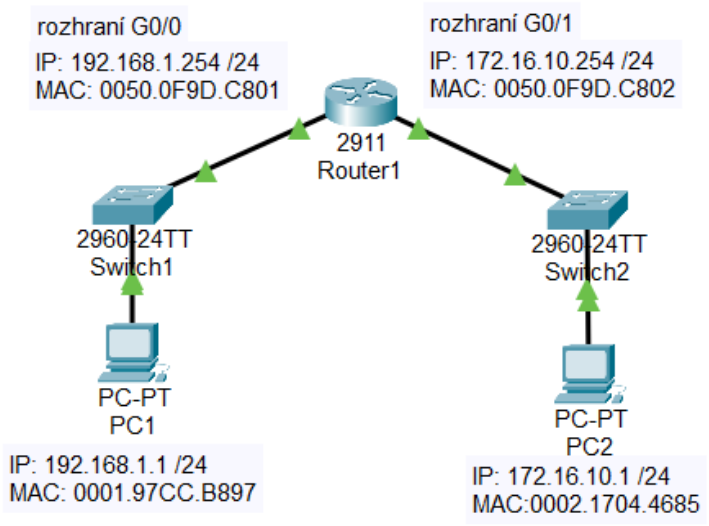
```
Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : lan
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (10) I219-LM
   Physical Address. . . . . . . . . : 74-78-27-0A-80-FB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

Obr. 4 – Zjištění fyzické adresy

Na obrázku 5 je zakreslena topologie, která obsahuje dvě různé sítě propojené směrovačem Router1. k rozhraní G0/0 je připojena síť 192.168.1.254 /24 s PC1 a k rozhraní G0/1 je připojena síť 172.16.10.0 /24 s PC2. V případě komunikace mezi PC1 a PC2 se jedná o komunikaci se vzdáleným cílem.

Cílová MAC adresa	Zdrojová MAC adresa	Zdrojová IPv4 adresa	Cílová IPv4 adresa
0050.0F9D.C801	0002.1704.4685	192.168.1.1 /24	172.16.10.254 /24

Obr. 5 – Fyzické a logické adresy PC1 a PC2 (LAMMLE, 2015)



Obr. 6 – Komunikace s cílem ve vzdálené síti (Cisco, 2023)

Linková vrstva přepravuje rámce pouze v rozsahu jednoho síťového segmentu. To znamená, že se MAC adresy na každém segmentu mění a paket je na každé lince zapouzdřen do jiného rámce. Rámec, který odchází z PC1 bude mít v poli cílová MAC adresa, MAC adresu rozhraní G0/0 tj. 0050.0F9D.C801. Ve směrovači se rámec rozbalí. Na základě cílové IP adresy a směrovací tabulky se vybere odchozí rozhraní, kterým bude paket odeslán. Před odesláním se zabalí do rámce, kde zdrojová a cílová MAC adresa, budou MAC adresy rozhraní G0/1 a PC2. Cílová a zdrojová adresa zůstanou po celou dobu přenosu stejné.

2 Protokol ARP

V předchozím textu byl popsán princip použití MAC a IP adresy. Protokol ARP (Address Resolution Protocol) používáme pro nalezení MAC adresy zařízení, když známe IP adresu zařízení, ale neznáme jeho MAC adresu. Standardizovaný protokol ARP pracuje na síťové vrstvě. Zdrojové zařízení nejprve prohledá paměť pro uchování informací o mapování fyzických a síťových adres (ARP cache), pokud se příslušná MAC adresa v paměti nenachází, tak se spouští protokol ARP. Úlohy protokolu jsou následující:

- Zjištění MAC adresy pro zadanou IPv4 adresu tj. mapovaní IP adres na MAC adresy.
- Správa vyrovnávací paměti namapovaných hodnot tj. ARP tabulky.

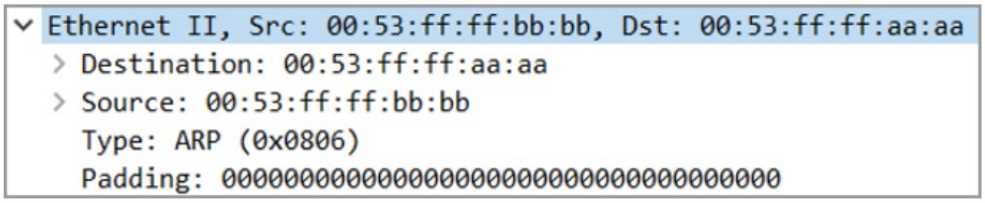
Činnost protokolu probíhá v několika krocích:

- Zdrojové zařízení sestaví rámec obsahující ARP žádost (request), Do rámce vloží svoji fyzickou a IP adresu, IP adresu cíle, se kterým chce komunikovat a rámec odešle na všesměrovou (broadcast) fyzickou adresu. Broadcastová adresa na L2 vrstvě má hodnotu FFFF-FFFF-FFFF.
- Všechna zařízení na lokálním segmentu přijmou rámec se žádostí. Rozbalí rámec, porovnají IP adresu s IP adresou zařízení. Pokud se IP adresy nerovnají, tak je rámec zahozen.

- V případě, že se IP adresy rovnají, tak bylo nalezeno cílové zařízení. Toto zařízení sestaví rámec obsahující ARP odpověď (response) a odešle jako unicastové vysílání, které obsahuje v poli zdrojová adresa svoji MAC adresu.
- Pokud se cíl komunikace nachází v jiné síti, ARP dotaz je vyslán pro zjištění fyzické adresy směrovače, který slouží jako výchozí brána pro danou síť.

2.1 Struktura ARP zprávy

Na obrázku je zachycen výpis komunikace pomocí síťového analyzátoru Wireshark. Informaci o tom, že rámec přenáší paket ARP, poznáme podle hodnoty v poli Type. Hodnota pro zprávu ARP je 0×0806.



Obr. 7 – Výpis obsahu rámce

Struktura ARP paketu je zobrazena na obrázku 8 a na obrázku 9 jsou zachycené hodnoty analyzátorem Wireshark.

Typ přenosového přenosového média/ Hardware type	Typ protokolu/ Protocol type	Délka linkové adresy/ Hardware size	Délka síťové adresy/ Protocol size	Kód zprávy/ Opcode	Zdrojová linková adresa/ Sender MAC address	Zdrojová síťová adresa/ Sender IP address	Cílová linková adresa/ Target MAC address	Cílová síťová adresa/ Target IP address

Obr. 8 – Formát zprávy ARP (LAMMLE, 2015)

Jaké hodnoty najdeme ve výpisu? Typ přenosového média – *Hardware type* je v tomto případě ethernetový kabel. Další je pole *Protocol type*, tato pole spolu označují, jaký typ adres se navzájem mapují. V tomto případě mapujeme ethernetovou adresu (MAC adresu) na adresu IPv4. Následují pole: *Hardware size* s délkou 6 bytů, což odpovídá MAC adrese (48 bitů) a *Protocol size* s délkou 4 byty, což odpovídá IP adrese (32 bitů). Hodnota pole *Opcode* nabývá 1 pro žádost (ARP request) a 2 pro odpověď (ARP Response). Pole *Sender MAC address* a *Sender IP address* jsou adresy MAC a IP iniciátora žádosti ARP. Pole *Target MAC* a *IP address* jsou cílem žádosti ARP. Je vyplněna cílová IP adresa hodnotou 10.0.0.22, cílová adresa MAC obsahuje nuly.

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 00:53:ff:ff:aa:aa
    Sender IP address: 10.0.0.11
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 10.0.0.22
```

Obr. 9 – Výpis obsahu žádosti ARP

2.2 ARP cache

Protokol ARP pracuje s určitými omezeními, které nedovolují koncovým zařízením zahltit síť dotazy pro každý rámec, pro který nezná cílovou IP adresu. Prvním z těchto omezení je, že si zařízení musí pamatovat, jaké dotazy již vyslalo. Pokud se již vyřizuje ARP dotaz pro chybějící MAC adresu, tak další rámce se stejným požadavkem se zařadí do fronty a počkají na odpověď na původní ARP žádost namísto generování žádosti pro každý nově vytvořený rámec. Další omezení zabraňující záplavě dotazů na fyzickou adresu je to, že zařízení může vyslat pouze jeden stejný dotaz za sekundu.

Pro větší efektivitu práce tohoto protokolu jsou získané informace dočasně uloženy do tak zvané ARP cache. Tato paměť uchovává informace o mapování fyzických a síťových adres získaných protokolem ARP, typicky po dobu 10 nebo 20 minut. Při dosažení maximální doby platnosti záznamu mapování se údaj vymaže a pro další komunikaci je nutné opět využít protokol ARP. Aktualizace této paměti probíhá nejen aktivně po přijetí odpovědi na dotaz u zdrojového zařízení, ale také pasivně díky obsažené zdrojové fyzické i síťové adrese v ARP dotazu.

3 Kontrolní opakovací otázky a úkoly

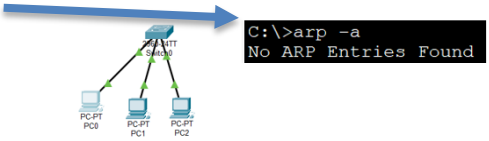
Jaká je úloha protokolu ARP?

Na jaké vrstvě pracuje protokol ARP?

Kde se používá adresa FF-FF-FF-FF-FF-FF?

Popište princip fungování protokolu ARP.

Máme zapojené 3 PC s nastavenými IP adresami. Po provedení příkazu arp -a se na každém PC zobrazí výpis viz obrázek



Následně provedeme ping z PC1 na PC2 (ping 192.168.1.3) a provedeme příkaz arp -a na PC1. Co bude ve výpisu na PC1? Dále provedeme příkaz arp -a na PC0. Co bude ve výpisu na PC0? Ověřte si své zjištění na zrealizované topologii v Packet Traceru.

4 Použitá literatura

Cisco Network Academy. *Netcad.com* [online]. Cisco, 2023 [cit. 2023-01-11]. Dostupné z: Introduction to Network.

LAMMLE, Todd. CCNA: výukový průvodce. Přeložil Jakub GONER. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.

SANDERS, Chris. Analýza sítí a řešení problémů v programu Wireshark. Brno: Computer Press, 2012. ISBN 978-80-251-3718-5.

SOSINSKY, Barrie A. Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.

Seznam zkratek

ARP	Address Resolution Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
L2	Layer 2
L3	Layer 3
MAC	Media Access Control

Rejstřík

Průmyslové sítě

Téma VIII: Objevování sousedů pomocí protokolů L2 vrstvy

Studijní cíl

Seznámit studenty s protokoly CDP a LLDP pracujících na druhé vrstvě, které umožňují zjistit přímo připojená zařízení k přepínači nebo směrovači.

Doba nutná k nastudování

2 hodiny

Klíčová slova

Protokol CDP, protokol LLDP

1 Protokol CDP

1.1 Úvod do CDP

Protokol Cisco Discovery Protocol (CDP) pracuje na 2 vrstvě, propojuje nižší vrstvy protokolu s vyššími. Používá se k získání informací o hardwaru a protokolech pro sousední zařízení typu přepínač nebo směrovač bez ohledu na konfigurovaný síťový protokol. Proprietární protokol CDP, který vyvinula firma Cisco se hodí při řešení problémů v síti nebo pro doplnění dokumentace k síťové topologii.

1.1.1 Časovače protokolu CDP

Při spuštění zařízení Cisco se ve výchozím nastavení automaticky spustí protokol CDP, každé zařízení konfigurované pro CDP vysílá periodicky zprávu, obsahující dobu platnosti. Po zadání příkazu *show cdp* (obr. 1) se zobrazí dva časovače, které lze nastavovat a jsou globální:

- Časovač CDP (CDP timer) udává, jak často se pakety CDP vysílají ze všech aktivních rozhraní.
- Doba držení CDP (CDP holdtime) je časový interval, po který se udržují pakety přijaté ze sousedních zařízení.

```
Switch#show cdp
Global CDP information:
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is enabled
```

Obr. 1 – Výstup protokolu CDP (Cisco. 2023)

Na obr.1 je uvedena informace o zasílání zpráv protokolu CDP verze v2 (*CDPv2 advertisments*). Verze CDPv1 je počáteční verze, nyní se používá verze CDPV2, která umožňuje najít příčiny problémů při duplexní komunikaci (nesprávně nastavené porty). Dále na obr. 1 jsou zobrazeny konkrétní hodnoty pro časovače. Výchozí přenosy se odesílají každých 60 sekund a pakety od sousedních zařízení se udržují po dobu 180 sekund. Konfigurace časovačů probíhá v následujících krocích: enable ► configure terminal ► cdp timer seconds ► cdp holdtime seconds ► end.

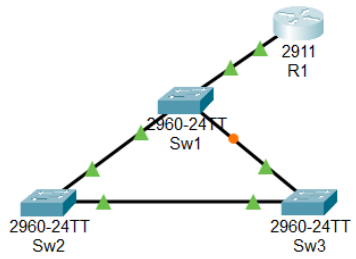
	Příkaz	Popis
Krok 1	Device> enable	Vstup do privilegovaného režimu EXEC
Krok 2	Device# configure terminal	Vstup do režimu globální konfigurace
Krok 3	Device(config)# cdp timer 30	Nastavení frekvence odesílaných paketů
Krok 4	Device(config)# cdp holdtime 90	Určuje dobu, po kterou se budou udržovat pakety CDP.
Krok 5	Device(config)# end	Návrat do privilegovaného režimu EXEC

Obr. 2 – Konfigurace časovačů (LAMMLE, 2015)

Všechna zařízení Cisco přijímají pakety CDP, zpracovávají je a ukládají do paměti cache informace v paketu. Zařízení Cisco nikdy nepředávají paket CDP. Pokud se od posledního přijatého paketu změní nějaké informace, nové informace se uloží do paměti cache a starší informace se zahodí, i když jeho časová hodnota dosud nevypršela.

1.1.2 Informace o sousedních zařízení

Pro protokol CDP platí, že funguje pouze na přímo připojených rozhraních. Zprávy jsou určeny na multicastovou adresu 01:00: 0C: CC: CC: CC. Zařízení, které přijímá zprávy CDP na rozhraní od jiných zařízení si ukládá informace do tabulky. Pomocí příkazu *show cdp neighbor* si zobrazíme uložené informace.




```
Sw1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Sw2          Fas 0/22         179           S       2960        Fas 0/24
Sw3          Fas 0/1          179           S       2960        Fas 0/20
R1           Fas 0/2          166           R       C2900       Gig 0/0
```

Obr. 3 – Výpis informací o sousedních zařízeních (Cisco, 2023)

Na obr. 3 se po zadání příkazu *show cdp neighbor* na přepínači zobrazí informace o přímo připojených zařízeních. Z výpisu je vidět že, přepínač Sw1 má jedno připojení k přepínačům Sw1 a Sw3, jedno připojení k směrovači R1. Dále vidíme, jakými porty jsou zařízení vzájemně propojená. Přepínač Sw1 je připojen portem Fas 0/2 k portu směrovače Gig 0/0. Přepínač Sw1

je připojen portem Fas 0/22 k přepínači Sw2 na jeho port Fas 0/24. Přepínač Sw1 je připojen portem Fas 0/1 k přepínači Sw3 na jeho port Fas 0/20. Z výpisu můžeme vyčíst postupně následující parametry:

- Device ID vypisuje název sousedního zařízení.
- Local interface vypisuje název rozhraní nebo číslo portu, které přijímá pakety CDP.
- Holdtime vypisuje dobu, po kterou se budou ještě udržovat pakety CDP (zbývající čas v sekundách). Po vypršení času dojde k zahození paketů, pokud se nepřijmou další pakety CDP.
- Capability obsahuje kód typu připojeného zařízení.
- Platform obsahuje produktové číslo zařízení.
- Port ID vypisuje název rozhraní nebo číslo portu sousedního zařízení, na které jsou pakety CDP odesílány multicastovým vysíláním.

Podrobnější informace o sousedních zařízeních poskytuje příkaz *show cdp neighbor detail*

```
Sw3#show cdp neighbors de
Sw3#show cdp neighbors detail

Device ID: Sw1
Entry address(es):
  IP address : 192.168.1.2
Platform: cisco 2960, Capabilities: Switch
Interface: FastEthernet0/20, Port ID (outgoing port): FastEthernet0/1
Holdtime: 156

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen

advertisement version: 2
Duplex: full
---------------------------

Device ID: Sw2
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/1, Port ID (outgoing port): GigabitEthernet0/1
Holdtime: 136


Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen

advertisement version: 2
Duplex: full
```

Obr. 4 – Detailní výpis o sousedních zařízeních protokol CDP (Cisco, 2023)

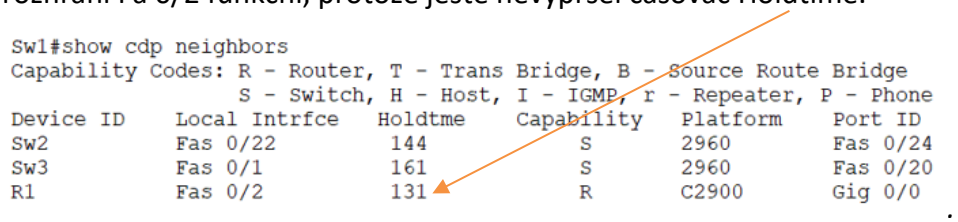
Z výpisu se dají zjistit názvy zařízení, IP adresy všech přímo připojených zařízení. Dále tento příkaz rozšiřuje proti příkazu *show cdp neighbor* informace o verzi systému IOS v sousedních zařízení. Příkaz se prováděl na přepínači Sw3, který je přímo připojen ke směrovači. Protože zařízení nepředává CDP pakety, tak ve výpisu nejsou informace o směrovači R1.

Přikazem *no cdp run* globálně vypneme protokol CDP. Popřípadě ho můžeme vypnout pro určité rozhraní, tak jak je uvedeno na obr. 5.

```
Sw1(config)#int fa0/2
Sw1(config-if)#no cdp enable
```

Obr. 5 – Vypnutí protokolu CDP na rozhraní Fa 0/2 (Cisco. 2023)

Účinnost příkazu ověříme příkazem *show cdp neighbor viz obr. 6*. Zatím protokol CDP je na rozhraní Fa 0/2 funkční, protože ještě nevypršel časovač Holdtime.



```
Sw1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Sw2              Fas 0/22          144             S       2960      Fas 0/24
Sw3              Fas 0/1           161             S       2960      Fas 0/20
R1               Fas 0/2           131             R       C2900     Gig 0/0
```

Obr. 6 – Výpis po vypnutí CDP protokolu na rozhraní Fa 0/2 před vypršením Holdtimeru (Cisco, 2023)

Na dalším obr. 7 je vidět ve výpisu, že informace o připojení ke směrovači R1 už chybí tj. protokol CDP je na tomto rozhraní vypnutý.

```
Sw1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Sw2              Fas 0/22          134             S       2960      Fas 0/24
Sw3              Fas 0/1           151             S       2960      Fas 0/20
```

Obr. 7 – Výpis po vypnutí CDP protokolu na rozhraní Fa 0/2 (Cisco, 2023)

Poznámka protokol CDP pracuje na druhé vrstvě to znamená, že pracuje s rámci. Nicméně v terminologii se používá označení paket.

1.1.3 Výhody a nevýhody protokolu CDP

Protokol CDP je užitečný nástroj pro zdokumentování síťové topologie. Po připojení ke konzolovému portu zařízení nebo přes vzdálené připojení ve součinnosti s příkazem pro výpis konfigurace (*show running-config*) máme možnost zjistit: konkrétní typy zařízení, typy rozhraní a IP adresy.

Zásadním rizikem protokolu CDP je možnost zachycení zprávy útočníkem, který ji zachytí pomocí wiresharku. Předpokladem je, že počítač útočníka je připojený na port přepínače, který používá protokol CDP. Zprávy CDP jsou v přímém textu a jejich obsah může sloužit pro realizaci dalších útoků.

Další nebezpečí může být v podobě CDP spoofing. Útočník zasílá pakety s cílovou multicastovou adresou 01:00: 0C: CC: CC: CC a falešnou zdrojovou adresou. Síťová zařízení přijmou takové rámce a přidávají je do CDP tabulky, která se začíná zvětšovat, protože útočník pošle velké množství CDP rámců na zařízení. Pokud zařízení není schopno tento útok zvládnout, tak je předpoklad, že se zařízení po nějaké době zhroutí. Z tohoto důvodu se doporučuje zakázat CDP na rozhraních, která připojují uživatelské počítače.

2 Protokol LLDP

LLDP (Link Layer Discovery protocol) je pracuje stejně jako protokol CDP na linkové vrstvě. Je využíván ke zjištění informací o sousedních zařízeních. Organizace IEEE zavedla otevřený standard s označením 802.1AB a je tedy využíván mnoha výrobci. Jedná se o jednocestný protokol s periodicky opakovaným vysíláním z každého portu. Výchozí hodnota je nastavena na 30 sekund. K šíření LLDP oznámení se využívá multicast 01-80-C2-00-00-XX (Ethernet type 0x88cc). Tuto zprávu přijímají nejbližší sousedé, informace zpracují a dále nepředávají. Pomocí LLDP je tedy možné zjistit pouze přímo připojené sousedy.

2.1.1 Časovače protokolu LLDP

Příkaz *lldp run* globálně spustí protokol LLDP. Protokol používá tři časovače:

- Doba držení LLDP (Hold time) je interval, po kterou by přijímací zařízení mělo uchovávat informace o sousedech LLDP. Pokud tento časovač vyprší a nebude přijat žádný paket LLDP, budou informace o sousedovi vymazány. Rozsah hodnot je 0 až 65535 sekund, výchozí hodnota je 120 sekund.
- Časovač LLDP (LLDP Packet frequency timer) je interval, ve kterém zařízení odesílá aktualizace LLDP sousednímu serveru. Rozsah hodnot je 5 až 65534 sekund, výchozí hodnota je 30 sekund.
- Čas opětovného spuštění (Reinit timer) je doba zpoždění v sekundách, než se LLDP inicializuje na jakémkoli rozhraní. Rozsah hodnot je 2 až 5 sekund, výchozí je 2 sekundy.

Obdobně je možné konfigurovat jednotlivá rozhraní.

Podobně jako protokol CDP, je možné protokol LLDP využít pro zjištění topologie. Protokol LLDP poskytuje informace na jakém portu bylo oznámení přijato, jaké zařízení informaci vyslalo (IP adresa a popis) a přes jaký port byla informace odeslána.

3 Kontrolní opakovací otázky a úkoly

Co je protokol CDP a jaký je jeho účel?

V jakém je výchozí nastavení protokolu CDP na zařízení?

Jaké typy zařízení podporují protokol CDP?

Jaké informace protokol CDP sdílí mezi zařízeními?

Jak lze protokol CDP využít pro správu sítě?

Jaká jsou bezpečnostní rizika protokolu CDP?

V čem se LLDP liší od protokolu CDP?

Jaké typy zařízení podporují protokol LLDP?

4 Použitá literatura

Cisco Network Academy. *Netcad.com* [online]. Cisco, 2023 [cit. 2023-01-11]. Dostupné z: Introduction to Network.

LAMMLE, Todd. CCNA: výukový průvodce. Přeložil Jakub GONER. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.

SOSINSKY, Barrie A. Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.

Seznam zkratek

CDP	Cisco Discovery Protocol
IEEE	Institute of Electrical and Electronics Engineers
LLDP	Link Layer Discovery Protocol

Rejstřík

Průmyslové sítě

Téma IX: Analýza síťového provozu

Studijní cíl

Seznámit studenty s instalací, spuštěním a ovládáním síťového analyzátoru Wireshark.

Doba nutná k nastudování

2 hodiny

Klíčová slova

Síťový analyzátor Wireshark, síťový provoz, filtr.

1 Síťový analyzátor Wireshark

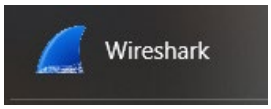
Wireshark je analyzátor síťových protokolů a používá se pro řešení problémů v síťové komunikaci, analýzu síťového toku a ve vzdělávání. Využívají ho síťový inženýři na celém světě a představuje ověřený standardní nástroj pro sledování paketů. Jedná se o otevřené zdrojový software, který je k dostupný pro různé operační systémy (Windows, Mac a Linux).

1.1 Instalace Wiresharku

Na adrese www.wireshark.org najdeme program ke stažení zdarma. Na stránkách Wireshark Foundation se zobrazí nejnovější stabilní vydání a aktuální vývojové vydání. Pro začátečníky je vhodnější stabilní verzi. Následuje výběr verze softwaru, kterou provádíme, na základě architektury vlastního počítače a operačního systému. Pro 64bitový počítač se systémem Windows, vybereme po kliknutí na Download instalaci Windows (64bitový). Po provedení výběru by mělo stahování začít. Umístění staženého souboru závisí na prohlížeči a operační systému, který je používán. Pro uživatele Windows je výchozí umístění Stažené soubory.

Obr. 1 Stažení Wiresharku (WIRESHARK, 2023)

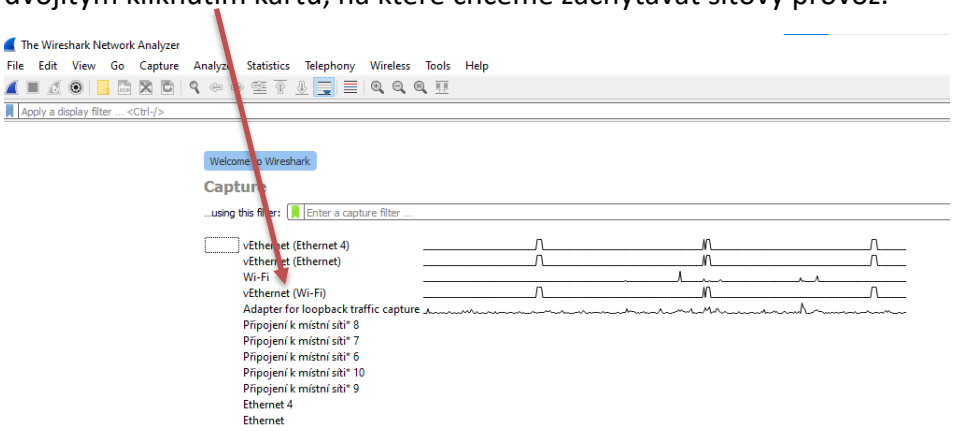
Stažený soubor se jmenuje **Wireshark-win64-x.x.x.exe**, kde x představuje číslo verze, pokud je stažena 64bit verze. Poklepáním na soubor spustíme proces instalace. Na obrazovce se mohou zobrazit bezpečnostní zprávy, na které je nutné odpovědět. Pokud už je na počítači nějaká verze Wiresharku tak, se zobrazí výzva k odinstalování staré verze před instalací nové verze. Před instalací jiné verze se doporučuje odstranit starou verzi Wireshark. Klikněte Ano, pokud chcete odinstalovat předchozí verzi Wireshark. V případě první instalace Wireshark nebo po dokončení procesu odinstalace, přejdeme do průvodce nastavením Wiresharku a vybereme tlačítko **Next.** Pokračuje se instalaci. V okně Licenční smlouva potvrdíme souhlas kliknutím na **I Agree**. V průběhu instalace se naistaluje služba Npcap, která zachycuje síťová data v reálném čase. Celý proces instalace je velmi intuitivní.



Obr. 2 Ikona Wiresharku (WIRESHARK, 2023)

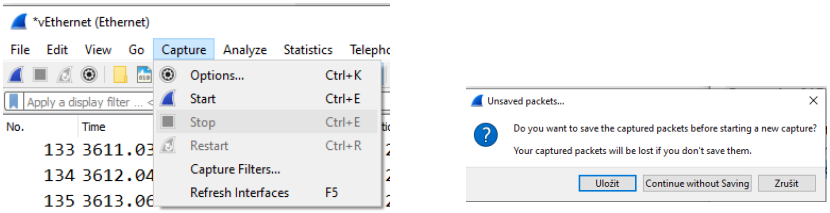
1.1.1 Používání Wiresharku

Spuštění aplikace provedeme kliknutím na ikonu Wiresharku nebo vyhledáním aplikace následným spuštěním. Wireshark nám umožňuje zachytit provoz ze síťové karty. Vybereme si dvojitým kliknutím kartu, na které chceme zachytávat síťový provoz.



Obr. 3 Úvodní okno Wiresharku (WIRESHARK, 2023)

V otevřeném okně se bude zobrazovat kompletní síťový provoz, který můžeme zachytávat a uložit do souboru. Vybereme záložku **Capture,** klikneme na **Start** a v dalším dialogovém okně si vybereme z nabídky **Uložit.**

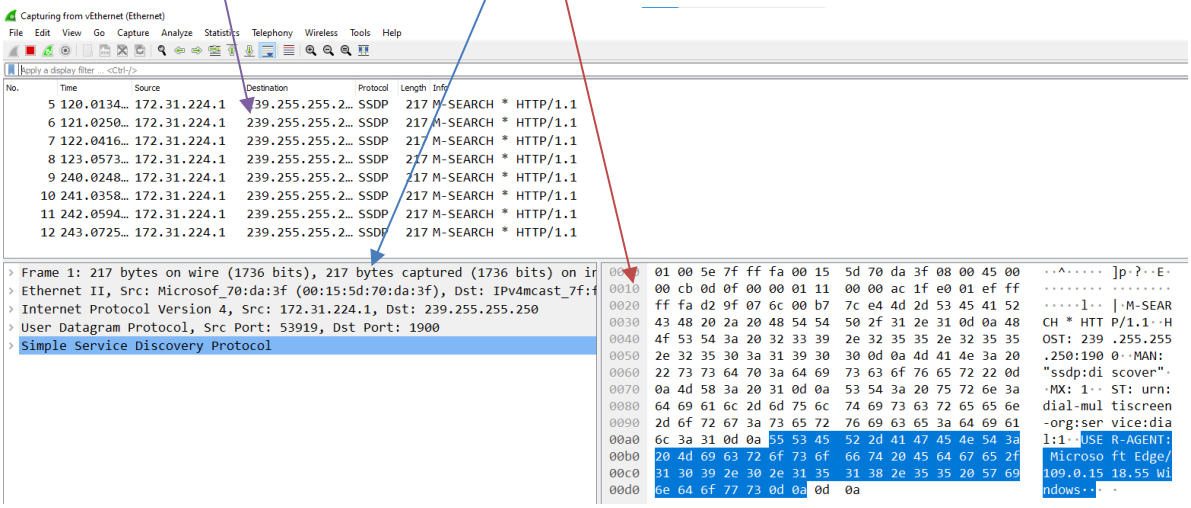


Obr. 4 Zachycení dat a uložení do souboru (WIRESHARK, 2023)

1.1.2 Analýza paketů

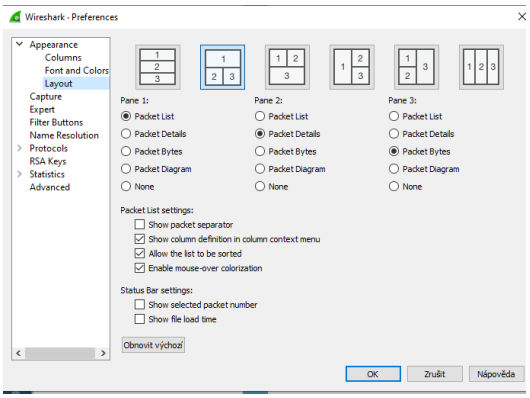
V panelu Wiresharku se průběžně zobrazuje síťový tok, který má tři sekce:

- seznam paketů zobrazuje tok paketů. Každý paket je uložen do nového řádku s přiřazeným číslem. Obsah sloupců pro jednotlivé pakety:
    - No.: číslo konverzace.
    - Time: čas, kdy byl paket zachycen.
    - Source: adresa zdroje odkud paket pochází.
    - Destination: adresa cíle kam je paket odeslán.
    - Protocol: použitý protokol.
    - Lengt: délka paketu v bajtech.
    - Info: podrobnosti o paketu.
- seznam PDU rozdělených podle vrstev,
- výpis zobrazuje nezpracovaná data každé vrstvy. Nezpracovaná data se zobrazují v šestnáctkovém i desítkovém formátu.



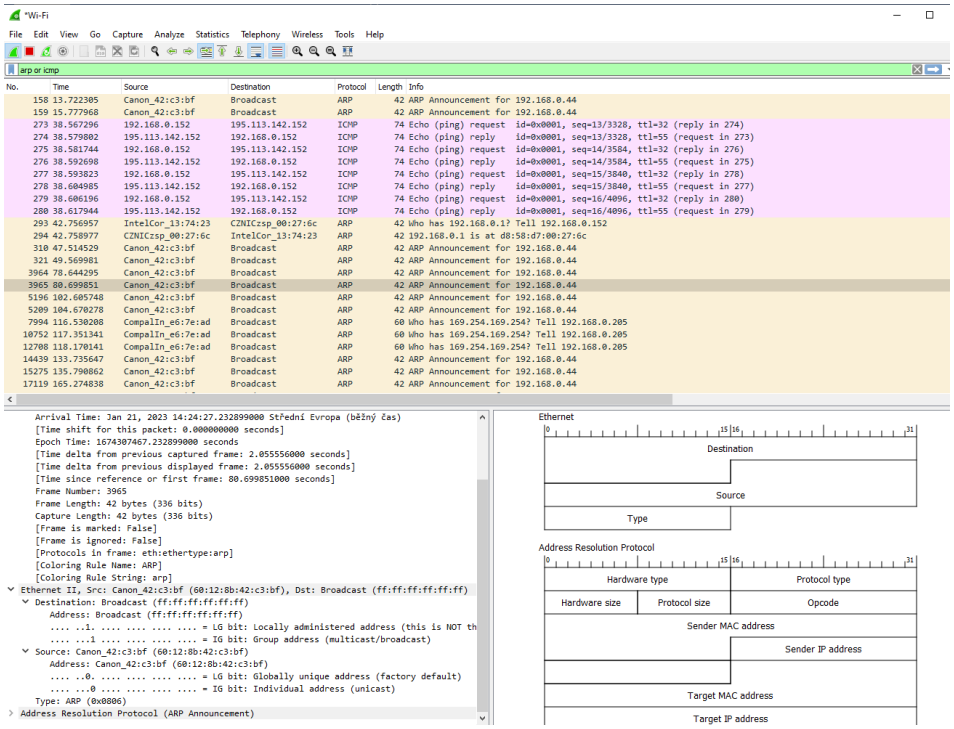
Obr. 5 Jednotlivé sekce Wiresharku (WIRESHARK, 2023)

Jednotlivé sekce lze upravit. V záložce **Edit** vybereme **Preferences** (Ctrl+shift+P). v dialogovém okně klikneme na **Appearance** a v Pane 3 změníme Packet Bytes na Packet Diagram.



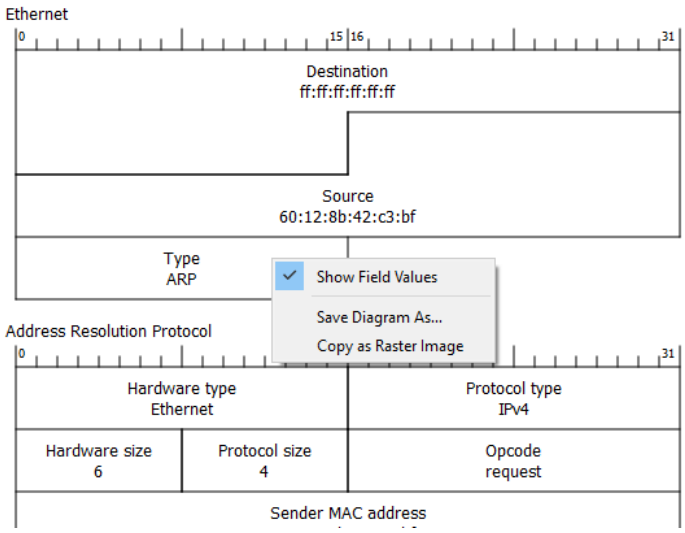
Obr. 6 Změna sekce (WIRESHARK, 2023)

Do hlavního panelu se promítne změna ve třetí sekci.



Obr. 7 Hlavní panel Wiresharku (WIRESHARK, 2023)

V této sekci vidíme vypsané hlavičky jednotlivých protokolů. Kliknutím pravé myši se otevře okno, kde zaklikneme Show Field Values a jednotlivá záhlaví se vyplní hodnotami.

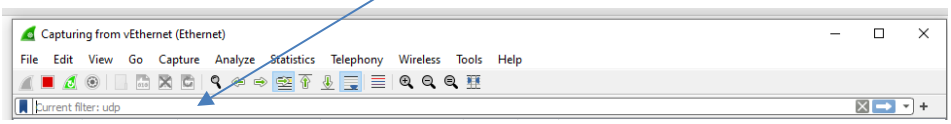


Obr. 8 Zobrazení třetí sekce (WIRESHARK, 2023)

1.1.3 Nastavení filtrů ve Wiresharku

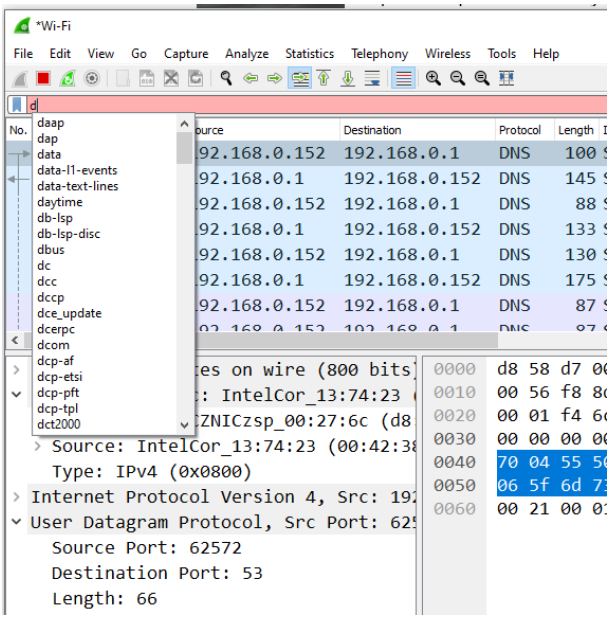
Wireshark poskytuje velké množství filtrů, jejichž výběrem se potom na výstupu zobrazí pouze určitá síťová komunikace. V současnosti Wireshark podporuje 2000 protokolů.Jednou z možností, jak použít filtr, je zadání názvu do pole filtru v horní části okna a stisknutí klávesy

Enter. Zadáme do pole například "dns" a ve seznamu paketů se budou zobrazovat pouze pakety DNS.



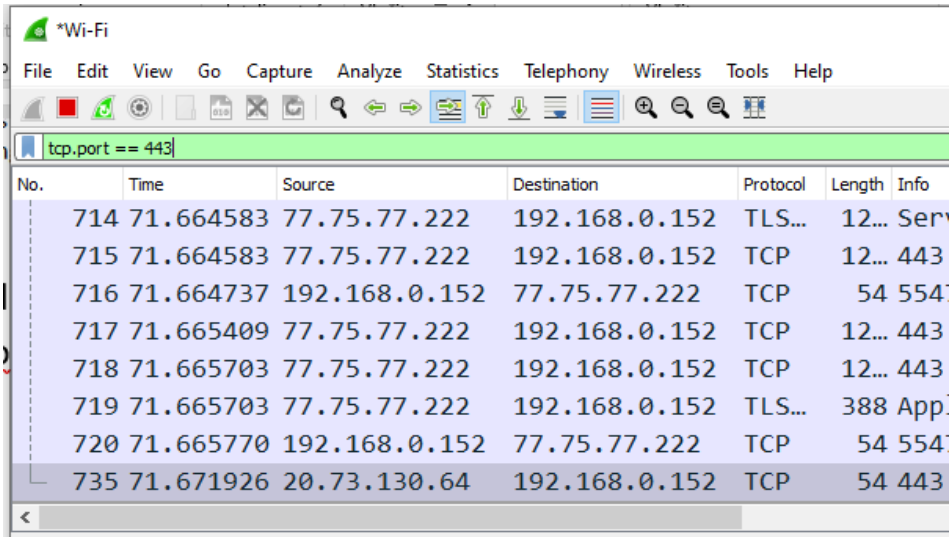
Obr. 9 Pole pro filtr (WIRESHARK, 2023)

Při vyplňování pole, aplikace Wireshark nabízí automatické doplnění filtru.



Obr. 10 Dialogové okno pro doplnění filtru (WIRESHARK, 2023)

Pokud budeme chtít vypsat komunikaci na určitém portu TCP například šifrované spojení SSL, tak zadáme tcp.port == 443.



Obr. 11 Nastavení filtru pomocí portu (WIRESHARK, 2023)

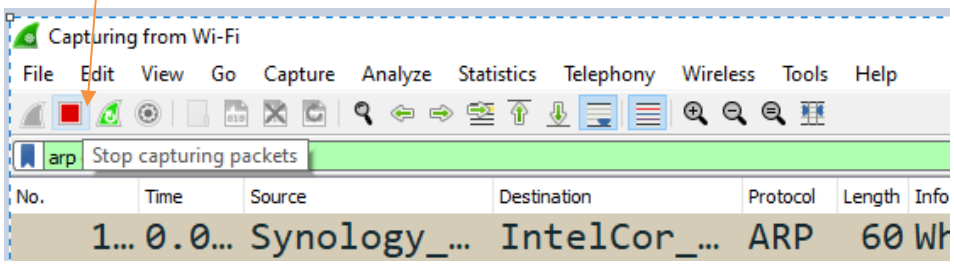
Filtry můžeme kombinovat pomocí porovnávacích a logických operátorů.

Porovnávací operátory			Logické operátory	
==	eq	Rovná se	and	Obě podmínky musí platit
!=	ne	Nerovná se	or	Jedna z podmínek musí platit
<	lt	Menší než	xor	Jen jedna z podmínek musí platit
>	gt	Větší než	not	Žádná z podmínek neplatí
<=	ge	Menší nebo rovr		
>=	le	Větší nebo rovn		

Obr. 12 Přehled porovnávacích a logických operátorů (SANDERS, 2012)

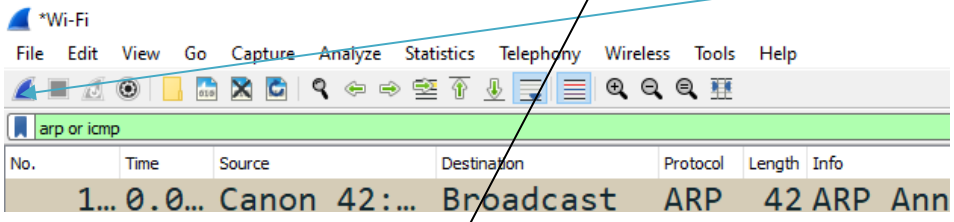
1.1.4 Zastavení zachytávání dat

Zastavení zachytávání provedeme tlačítkem Stop capturing packets (červený čtverec) nebo Ctrl+E.

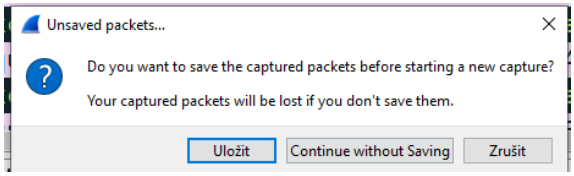


Obr. 13 Zastavení zachytávání paketů (WIRESHARK, 2023)

Na předchozím obrázku je vidět, že ikona pro opětovné spuštění je šedivá a zbarví se modře po jejím stisknutí. Otevře se dialogové okno s nabídkou.



Obr. 14 Opětovné spuštění (WIRESHARK, 2023)



Obr. 15 Dialogové okno před opětovným spuštěním (WIRESHARK, 2023)

2 Praktické použití Wiresharku

Praktické použití síťového analyzátoru provedeme na počítači s cílem zobrazit si obsah rámců protokolů ARP a ICMP.

Zopakování principu fungování protokolu ARP před analyzováním zachyceného toku. Úkolem protokolu ARP je najít MAC adresu zařízení k jeho IP adrese. Činnost protokolu probíhá v několika krocích:

- Zdrojové zařízení sestaví rámec obsahující ARP žádost (request), Do rámce vloží svoji fyzickou a IP adresu, IP adresu cíle, se kterým chce komunikovat a rámec odešle na všesměrovou (broadcast) fyzickou adresu. Broadcastová adresa na L2 vrstvě má hodnotu FFFF-FFFF-FFFF.
- Všechna zařízení na lokálním segmentu přijmou rámec se žádostí. Rozbalí rámec, porovnají IP adresu s IP adresou zařízení. Pokud se IP adresy nerovnají, tak je rámec zahozen.
- V případě, že se IP adresy rovnají, tak bylo nalezeno cílové zařízení. Toto zařízení sestaví rámec obsahující ARP odpověď (response) a odešle jako unicastové vysílání, které obsahuje v poli zdrojová adresa svoji MAC adresu.
- Pokud se cíl komunikace nachází v jiné síti, ARP dotaz je vyslán pro zjištění fyzické adresy směrovače, který slouží jako výchozí brána pro danou síť.

Protokol ICMP pracuje na síťové vrstvě a je přímo zapouzdřen v IP paketu v části přenášená data. Používá utilitu ping, kterou použijeme na zjištění dostupnosti cílového zařízení. Příkaz zapíšeme v příkazovém řádku počítače **ping adresa cíle** např. ping www.upce.cz nebo ping 192.168.1.100.

Postup pro zachycení dat:

a) Provedeme instalaci aplikace Wiresharku podle popisu uvedeném v předchozí části textu.
b) Nejprve si v příkazovém řádku zobrazíme síťové parametry počítače pomocí příkazu **ipconfig /all**. Vypíše se mimo jiné IP adresa, výchozí brána a MAC adresa počítače. Tyto hodnoty budeme sledovat ve výpisu v analyzátoru.

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-NB48BTC
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82577LM Gigabit Network Connection
   Physical Address. . . . . . . . . :00-26-B9-DD-00-91
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d809:d939:110f:1b7f%20(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.147(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
<output omitted>
```

Obr. 16 Výpis konfigurace počítače

c) V hlavním panelu Wireshark do části pro filtry zapíšeme **arp or icmp**. Podrobný výpis ARP replay a request najdeme v panelu seznam PDU
d) V příkazovém řádku počítače provedeme příkaz **ping** na adresu, která leží ve stejné síti.
e) Prozkoumáme zachycený síťový tok. Obsah ethernetového rámce si zobrazíme rozkliknutím Ethernet II. Případně si můžeme změnit sekci Packet Bytes na Packet Diagram, kde budou zobrazeny formáty hlaviček protokolů.
f) V příkazovém řádku počítače provedeme příkaz ping na adresu, která leží ve vzdálené síti.
g) Prozkoumáme zachycený síťový tok. Obsah ethernetového rámce si zobrazíme rozkliknutím Ethernet II.
h) Porovnejte obsahy ethernetového rámce a ARP zpráv.

Cílem úlohy bylo zachycení požadavku ICMP, který se realizuje použitím příkazu ping. Data ICMP jsou zapouzdřena uvnitř IPv4 paketu PDU (IPv4 header), který je pak zapouzdřen do ethernetového II rámce PDU (Ethernet II header) pro přenos na LAN. Realizoval se požadavek na cíl umístěný v lokální a vzdálené síti, proto se do filtru zadalo zachycení jak ICMP, tak ARP zpráv.

3 Kontrolní opakovací otázky a úkoly

Co je Wireshark a k čemu slouží?

Kde se pomocí Wiresharku zachycuje síťový provoz?

Jakým způsobem lze filtrovat zachycené pakety?

Vyzkoušejte si zachycení síťového provozu například protokolu TCP.

4 Použitá literatura

LAMMLE, Todd. CCNA: výukový průvodce. Přeložil Jakub GONER. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.

SANDERS, Chris. Analýza sítí a řešení problémů v programu Wireshark. Brno: Computer Press, 2012. ISBN 978-80-251-3718-5.

Wireshark: Packet_analyzer [online]. University of Missouri–Kansas City: Wireshark Foundation, 2023 [cit. 2023-06-06]. Dostupné z: https://www.wireshark.org/.

Seznam zkratek

ARP	Address Resolution Protocol
DNS	Domain Name System
ICMP	Internet Control Message Protocol
IPv4	Internet Protocol version 4
L2	Layer 2
MAC	Media Access Control
PDU	Protocol Data Unit
TCP	Transmission Control Protocol

Rejstřík

Průmyslové sítě

Téma X: Přiřazení IP adres koncovým zařízením

Studijní cíl

Seznámit studenty s nastavením IP adresy koncovým zařízením staticky nebo automaticky pomocí protokolu DHCP.

Doba nutná k nastudování

2 hodiny

Klíčová slova

Statická IP adresa, dynamická IP adresa, protokol DHCP

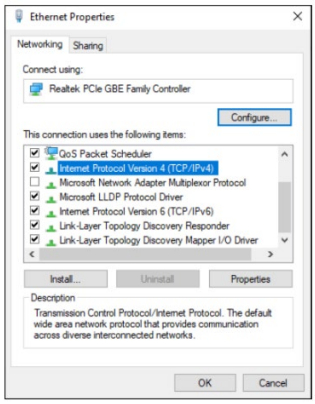
1 Nastavení IP adres koncovému zařízení

Každé zařízení, které potřebuje komunikovat s ostatními zařízeními v síti, musí mít přiřazenou IP adresu. Adresy IPv4 můžeme zadávat do koncových zařízení ručně nebo pomocí protokolu DHCP (Dynamic Host Coniguration Protocol).

1.1 Statické přiřazení IP adresy koncovému zařízení

Statické přiřazení adresy provádí ručně administrátor. Konfigurace na koncovém zařízení s operačním systémem Windows probíhá následovně:

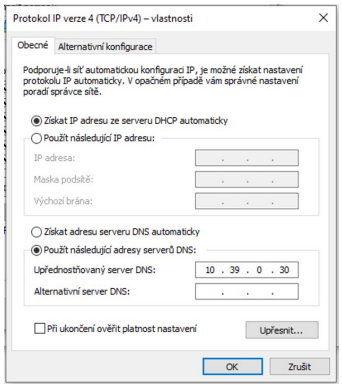
- Otevřete ovládací panel Síťová připojení takto: Otevřete menu Start.
- Vyberte položku: Nastavení.
- Dále klikněte na Síť a internet.
- Zvolte Ethernet a vyberte: Změnit možnosti adaptéru.
    - Pokud je Váš počítač vybaven bezdrátovou síťovou kartou (většina notebooků), můžete provést změny také pro tento bezdrátový adaptér.
    - Pravým tlačítkem myši klikněte na připojení, které chcete změnit, a potom klikněte na příkaz Vlastnosti.
    - Pokud vás systém vyzve k zadání nebo potvrzení hesla správce, zadejte heslo nebo proveďte potvrzení.
- Na kartě Sítě. V seznamu Toto připojení používá následující položky klikněte na položku Protokol IPv4 (TCP/IPv4 a potom klikněte na příkaz Vlastnosti.



Obr. 1 – Protokolový zásobník TCP/IP

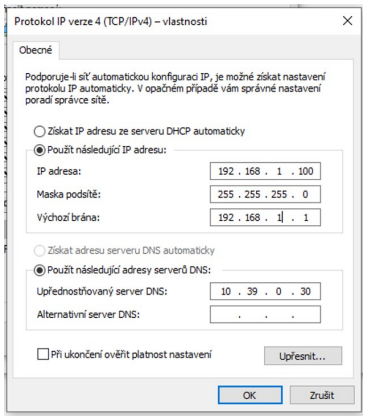
Následně se zobrazí okno, kde máme na výběr mezi možností získat IP adresu automaticky nebo nastavit si ručně jednotlivé parametry potřebné pro správnou funkci koncového zařízení.

- IP adresu
- Masku podsítě
- Výchozí bránu
- Upřednostňovaný server DNS



Obr. 2– Vlastnosti Protokolu IPv4

Na dalším obrázku je zobrazeno okno s vyplněnými údaji. Jejich hodnoty jsou dané požadavky uživatele.



Obr. 3 – Vlastnosti Protokolu IPv4 s vyplněnými hodnotami

Statické nastavení je vhodné použít pro zařízení, které musí být dostupné pro ostatní zařízení v síti a není vhodné, aby si tato zařízení měnila adresu. Jedná se o servery, síťové tiskárny, směrovače nebo L3 přepínače. Obdobným způsobem nastavíme parametry pro IPv6 adresu. Pro ověření nastavených hodnot použijeme zadáním příkazu ipconfig v příkazové řádku.

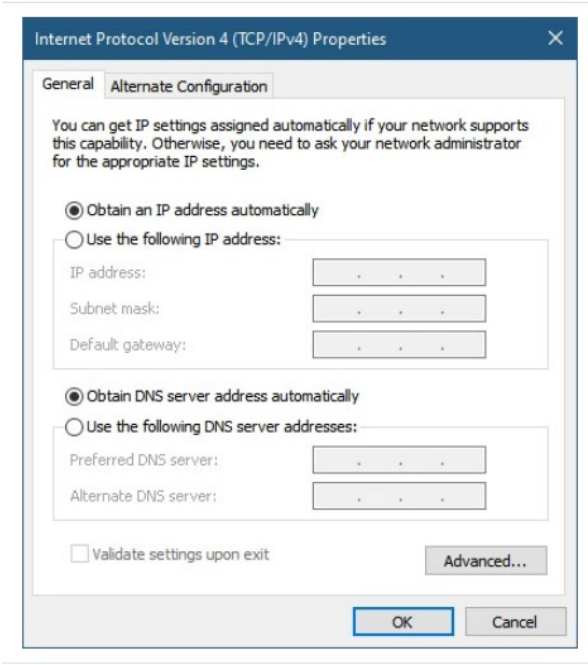
```
  IPv6 Address. . . . . . . . . . . : 2001:718:604:60:ea71:2c6a:b0c4:4b3b
  Temporary IPv6 Address. . . . . . : 2001:718:604:60:c8a7:a5d2:2abf:6ab5
  Link-local IPv6 Address . . . . . : fe80::af1c:780b:5a5e:b301%7
  IPv4 Address. . . . . . . . . . . : 192.168.60.101
  Subnet Mask . . . . . . . . . . . : 255.255.255.0
  Default Gateway . . . . . . . . . : fe80::e2d1:73ff:fef3:ee21%7
                                      192.168.60.1
```

Obr. 4 – Ověření nastavení IP adresy pomocí ipconfig

1.2 Automatická konfigurace IP adres pro koncová zařízení

Ruční nastavování adres koncovým zařízením je v reálné infrastruktuře čítající desítky nebo stovky zařízení značně nepraktické a mohlo by vést i k chybnému nastavení parametrů např. duplikace IP adres. Proto se využívá protokol DHCP pro automatickou konfiguraci adres IPv4 koncovým zařízením.

V počítači s operačním systémem Windows a službou DHCP postupujeme obdobně jako v případě statického nastavování. Po otevření okna Vlastnosti zaklikneme položku **Obtain an IP address automatically** a získat adresu serveru DNS automaticky. Následně počítač vyhledá server DHCP, který mu přiřadí IP adresu, masku, výchozí bránu, adresu DNS serveru, dobu zápůjčky. Server DHCP má nastavený fond adres (pool), z kterého zapůjčuje IP adresu každému klientovi po jeho zapnutí.



Obr. 5 – Dialogové okno DHCP

Ověření nastavení IP adresy na počítači s operačním systémem Windows provedeme příkazem ipconfig v příkazovém řádku.

2 Protokol DHCP

Protokol DHCP (Dynamic Host Control Protokol) je aplikační protokol DHCP definovaný v roce 1993. Protokol DHCP současně s IP adresou posílá server klientům další parametry: adresu nejbližšího směrovače, masku sítě, adresy DNS serverů. Přidělené údaje mají omezenou dobu platnosti a po určitém čase je třeba toto nastavení obnovit. Jedná se o tzv. zápůjčku. To znamená, že adresy a další informace přidělované službou DHCP koncovým zařízením nejsou přidělovány staticky, nastálo, ale jen na určitou stanovenou dobu. Po této době zařízení adresu vrátí, nebo obnoví. Služba DHCP přináší výhodu v efektivním nakládáním s adresním prostorem, protože uživatelé si pro připojení k síti nemusí nic nastavovat. Dále nedochází ke konfliktu adres z důvodu špatného nastavení a správci sítě usnadňuje konfiguraci sítě. Jak bylo uvedeno v předchozím textu, některá zařízení musí mít IP adresu neměnnou. Pomocí DHCP je umožněno v případě potřeby nastavit určité IP adresy staticky pomocí rezervace adresy.

2.1 Typy zpráv protokolu DHCP

DHCPDISCOVER je zpráva, která obsahuje paket, který je klientem vyslán jako první ve chvíli, kdy klient nemá přidělenou IP adresu a hledá DHCP server. Tímto paketem klient zahajuje komunikaci.

DHCPOFFER je zpráva, která obsahuje paket, který je odpovědí serveru na klientovo voláni DHCPDISCOVER. V případě, že server může klientovi přidělit IP adresu, pak posílá DHCPOFFER jako odpověď na DHCPDISCOVER a do možností vkládá konfigurační parametry. Tuto zprávu server odesílá na všesměrovou adresu i na přidělovanou IP adresu obsaženou v hlavičce.

DHCPREQUEST je zpráva, která obsahuje odpověď klienta na DHCPOFFER. Klient touto zprávou žádá o přidělení adresy a konfigurací předaných v DHCPOFFER. Paket DHCPREQUEST je odeslán na všesměrovou adresu. Pokud je klient s již přidělenou IP adresou restartován, pak použije paket DHCPREQUEST pro obnovení původní adresy bez ohledu na to, zda vypršela doba zápůjčky. DHCPREQUEST zasílá klient i v případě, že se blíží vypršení zápůjčky.

DHCPDECLINE je zpráva, kterou odesílá klient serveru v případě, že nějakým způsobem zjistí, že přidělená IP adresa koliduje s jiným zařízením. Server bz si měl tuto adresu pamatovat jako nedostupnou.

DHCPPACK je zpráva, která potvrzuje stav, pokud je klientem požadovaná IP adresa stále volná a konfigurace platná, pak server odpovídá na DHCPREQUEST paketem DHCPACK. Klient po přijetí paketu DHCPACK nakonfiguruje síťové rozhraní.

DHCPNAK je zpráva, která obsahuje se odesílá v případě, že server donutil klienta znovu požádat o obnovení IP adresy (DHCPFORCERENEW) a server požaduje, aby klient inicializoval rozhraní od začátku (DHCPDISCOVER)

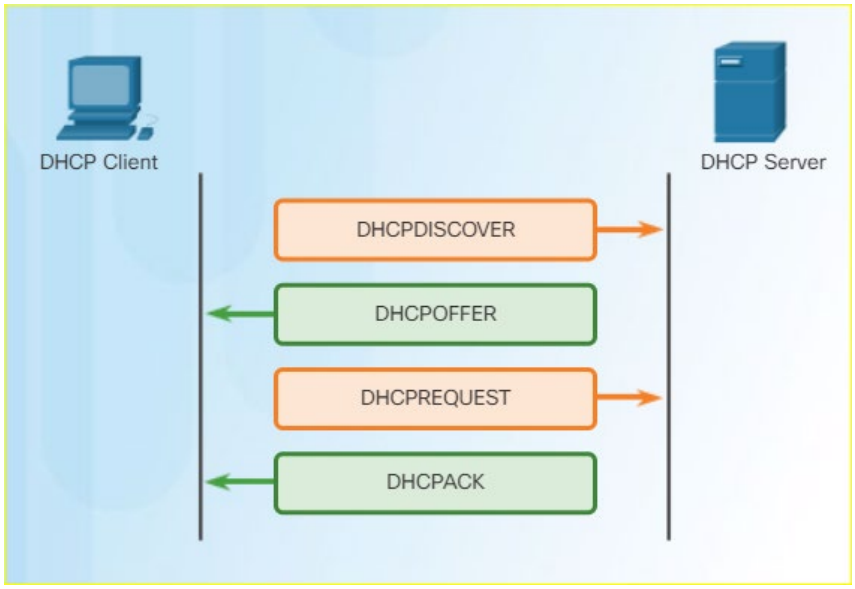
DHCPRELEASE je zpráva, která se vysílá, pokud klient chce ukončit platnost zápůjčky ještě před jejím vypršením, pak odešle serveru zprávu DHCPRELEASE.

DHCPINFORM je zpráva, která se používá v případě, že klient má IP adresu nastavenou jinak než pomocí DHCP, ale přesto některé konfigurační parametry přebírá pomocí DHCP ze serveru. DHCPINFORM je tedy požadavek klienta na zaslání ostatních konfiguračních parametrů (DNS, NTP servery, apod.). Server odpovídá opět paketem DHCPACK. V tomto případě není platná žádná doba zápůjčky a klient sám musí požádat o opětovné zaslání konfigurace. Pokud to obě strany podporují, může server donutit klienta k znovu zaslání DHCPINFORM pomocí paketu DHCPFORCERENEW.

DHCPFORCERENEW je zpráva, která se vysílá, pokud chce server donutit klienta znovu načíst konfiguraci, odešle mu paket DHCPFORCERENEW. Klient odpoví zasláním požadavku DHCPREQUEST. Pokud server pouze mění konfigurační parametry odpoví paketem DHCPACK s patřičnými parametry. Pokud vyžaduje novou konfiguraci IP, pak odešle paket DHCPNAK.

2.2 Princip a činnost DHCP

Klienti komunikují na UDP portu 68, server naslouchá na UDP portu 67. Po připojení do sítě klient vyšle broadcastovou zprávu DHCPDISCOVER. Na kterou odpoví DHCP server zprávou DHCPOFFER s nabídkou IP adresy. Klient si z nabídek vybere jednu IP adresu a o tu požádá zprávou DHCPREQUEST. Server mu zašle potvrzení v odpovědi zprávou DHCPACK. Jakmile klient obdrží zprávu DHCPACK, může už IP adresu a další nastavení používat. Klient musí před uplynutím doby zápůjčky obnovit svou IP adresu. DHCP server u každého klienta eviduje půjčenou IP adresu a čas, do kdy ji klient smí používat (doba zapůjčení / lease time). Poté co vyprší doba zápůjčky, tak se adresa vrací do fondu adres a server může adresu přidělovat jiným klientům.



Obr. 6 – Princip fungování DHCP

2.3 DHCP relay agent

Když se klient připojí do sítě, tak pomocí broadcastového vysílání DHCPDISCOVER hledá DHCP server. Broadcastové vysílání se nešíří z jedné sítě do druhé a zastavuje se na routeru, takže v situaci, kde není nakonfigurován DHCP server ve stejné podsíti jako klient, tak vysílání

neprojde a klient neobdrží IP adresu. Proto se nastavuje funkce Relay Agent, která broadcastové vysílání zkonvertuje na unicastové, které již routerem projde a umožní spojení klienta s DHCP serverem v jiné podsíti.

3 Kontrolní opakovací otázky a úkoly

Jakým způsobem může koncové zařízení získat IPv4 adresu?

Kdy není vhodné použít pro získání IP adresy protokol DHCP?

Jaké parametry přidělí koncovému zařízení protokol DHCP?

Co je protokol DHCP a jaký je jeho účel?

Jaké typy zpráv se používají v protokolu DHCP?

Jaký je proces přidělování IPv4 adresy klientovi v protokolu DHCP?

Jaký je účel funkce DHCP Relay Agent?

4 Použitá literatura

Cisco Network Academy. Netcad.com [online]. Cisco, 2023 [cit. 2023-01-11]. Dostupné z: Introduction to Network.

LAMMLE, Todd. CCNA: výukový průvodce. Přeložil Jakub GONER. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.

SANDERS, Chris. Analýza sítí a řešení problémů v programu Wireshark. Brno: Computer Press, 2012. ISBN 978-80-251-3718-5.

SOSINSKY, Barrie A. Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.

Seznam zkratek

DHCP	Dynamic Host Coniguration Protocol
DNS	Domain Name System
IP	Internet Protocol
IPv4	Internet Protocol version 4
NTP	Network Time Protocol
TCP	Transmission Control Protocol

Rejstřík

Průmyslové sítě

Téma XI: Síťová vrstva a její protokoly

Studijní cíl

Seznámit studenty s činností síťové vrstvy a nejpoužívanějšími protokoly.

Doba nutná k nastudování

2 hodiny

Klíčová slova

Síťová vrstva, adresování, zapouzdřování, směrování, odpouzdřování

1 Síťová vrstva

Síťová vrstva je třetí vrstva v OSI modelu. Síťová vrstva pracuje s protokolovou datovou jednotkou paket, který zapouzdřuje data z transportní vrstvy. Zapouzdřování (encapsulation) se provádí směrem od nejvyšší vrstvy k nejnižší.

Tab. 1– Vrstvy OSI modelu

Označení vrstvy	Vrstva OSI	PDU
L7	Aplikační vrstva	data
L6	Prezentační vrstva	data
L5	Relační vrstva	data
L4	Transportní vrstva	segment
L3	Síťová vrstva	paket
L2	Linková vrstva	rámec
L1	Fyzická vrstva	tok bitů

1.1 Základní úkoly síťové vrstvy

a) Adresování koncových zařízení. Každé síťové zařízení má přiřazenou síťovou IP adresu (logickou), která slouží k směrování paketů do cílové sítě a k cílovému zařízení. Koncové zařízení musí být nakonfigurována s jedinečnou IP adresou pro jednoznačnou identifikaci v síti.

b) Zapouzdřování segmentu transportní vrstvy do paketu znamená přidání hlavičky s IP adresou lokálního zdrojového zařízení a IP adresy cílového zařízení. Adresa cílového zařízení se pak použije pro doručení paketu do cíle. Jakmile je paket připraven, je

předán nižší vrstvě (linkové), která zajistí další úpravu dat, a následně se data vyšlou na síťové přenosové médium.

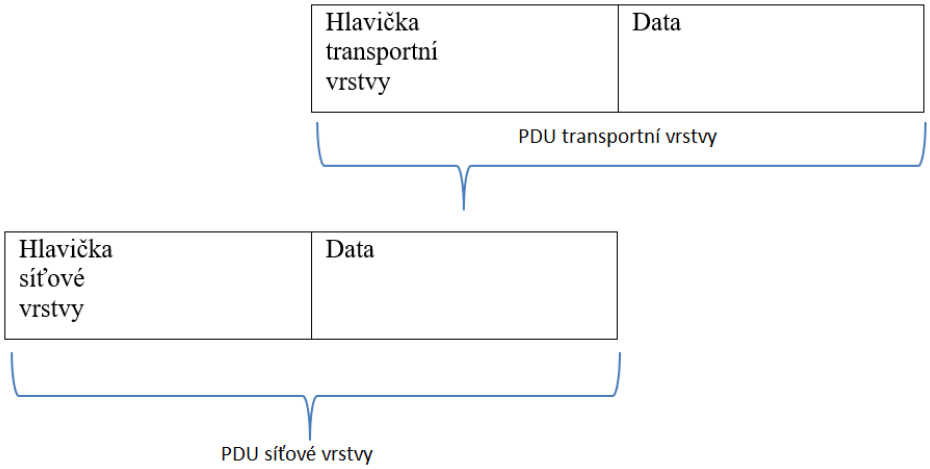
c) Směrování je vyhledání nejlepší cesty ze zdrojové sítě do cílové sítě. Rozhodnutí o výběru nejlepší cesty provádí síťová zařízení směrovače (routery) na základě obsahu svých směrovacích tabulek.

d) Odpouzdřování paketu, v kterém je zabaleno PDU transportní vrstvy nastává až ve chvíli, kdy dorazí do svého cílového zařízení. Tam je z paketu odstraněna hlavička obsahující informace o síťových IP adresách zdrojového a cílového zařízení a získaný segment je předán transportní vrstvě pro další zpracování.

1.1.1 Zapouzdření dat

Zapouzdření dat se provádí na příslušné vrstvě a pracuje se pouze se záhlavým příslušné vrstvy a nijak se nezabývá obsahem zapozdřených dat z vyšší vrstvy. V našem případě se zapouzdří data z transportní vrstvy do síťové přidáním hlavičky IP.

Obrázek znázorňuje, jak je PDU transportní vrstvy je zapouzdřena do PDU síťové vrstvy za účelem vytvoření paketu IP.

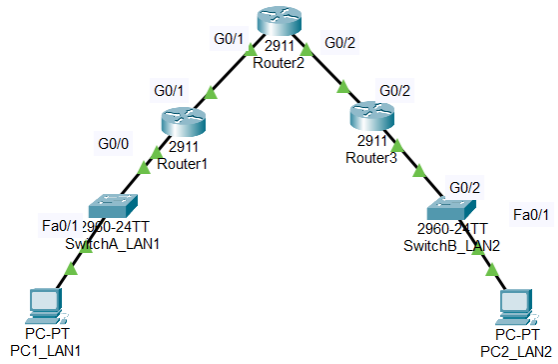


Obr. 1 – Zapouzdření PDU transportní vrstvy (LAMMLE, 2015)

Zapouzdřování dat transportní vrstvy se provádí pomocí protokolů IPv4 nebo IPv6. IP hlavička je zkoumána zařízeními třetí vrstvy 3, které mají nakonfigurované směrovací protokoly, které směrují pakety mezi sítěmi.

1.1.2 Proces zpracování dat

Proces zpracování dat na jednotlivých zařízeních si popíčeme na zobrazené síťové topologii, která je vytvořena v simulačníprogramu Packet Tracer. Nakonfigurování jednotlivých prvků bylo prováděno s cílem umožnit přenos dat od zdrojového počítače PC1_LAN1 k cílovému počítači PC2_LAN2 a opačně. Počítač PC2_LAN2 leží ve vzdálené síti. Počítače i rozhraní směrovačů mají nastavené IPv4 adresy, jejich hodnoty jsou uvedeny v tabulce.



Obr. 2 – Síťová topologie (Cisco, 2023)

Na směrovačích je nastavené dynamické směrování s nakonfigurovaným směrovacím protokolem RIP (Routing Information Protocol). Jednotlivá zařízení jsou propojena pomocí metalických kabelů.

Tab. 2 – Tabulka adres

Zařízení	Rozhraní	IP adresa	Maska
PC1_LAN1	NIC	192.168.1.1	255.255.255.0
PC2_LAN2	NIC	192.168.50.50	255.255.255.0
Router1	G0/0	192.168.1.254	255.255.255.0
Router1	G0/1	10.10.10.1	255.255.255.0;
Router2	G0/1	10.10.10.2	255.255.255.0;
Router2	G0/2	10.10.10.5	255.255.255.0;
Router3	G0/2	10.10.10.6	255.255.255.0;
Router3	G0/0	192.168.50.1	255.255.255.0;

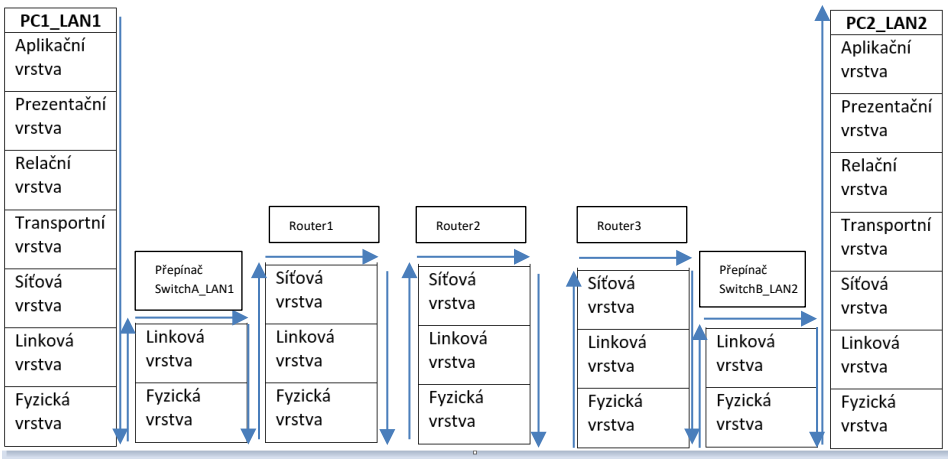
Na dalším obrázku je zobrazeno na jakých vrstvách pracují síťová zařízení. Přenos dat začíná od PC1_LAN1. Pomocí sí´tového zásobníku TCP/IP dojde k výstupu dat ze síťové karty na síťové přenosové médium. Data jsou přenesena do přepínače SwitchA_LAN1, který má připojený počítač k portu Fa0/1. Síťové rozhraní seřadí jednotlivé bity do rámce, v kterém je uložena cílová a zdrojová MAC adresa tj. MAC adresa výchozí brány a počítače. Switch přepíná rámec na základě cílové MAC adresy uložené v rámci a obsahu přepínací tabulky. Tabulka obsahuje naučené zdrojové MAC adresy z rámce spárované s číslem portu, ke kterému je připojeno koncové zařízení. Přepínač nemění obsah rámce. Předpokládejme, že v přepínací tabulce je uložena asociace mezi cílovou MAC adresou a portem. Rámec je vyslán z přepínače portu G0/0 na médium v podobě toku bitů a přijmut ve směrovači Router1 na portu G0/0.

Směrovač zpracuje bity do rámce, ze kterého se odpouzdří paket. V paketu se zmenší hodnota TTL o jedničku. Pokud je hodnota TTL rovné nule, tak se paket zahodí a do cíle je o tom odeslána zpráva ICMP. Směrovač porovná směrovací tabulku s cílovou IP adresou uloženou v paketu. Směrovač Router1 zapouzdří paket do rámce s novou cílovou a zdrojovou MAC adresou a odešle ho přes odchozí rozhraní G0/1 na další směrovač Router2.

Směrovač Router2 obdobným způsobem jako Router1 zpracuje paket. Následně odešle odchozím rozhraním G0/2 rámec s novou cílovou a zdrojovou MAC adresou na další směrovač Router3.

Směrovač Router3 obdobným způsobem jako Router1 a Router2 zpracuje paket. Následně odešle odchozím rozhraním G0/0 rámec s novou cílovou a zdrojovou MAC adresou do cílového zařízení PC2_LAN2 přes přepínač.

Obrázek ukazuje jaké vrstvy OSI modelu jsou používány na jednotlivých vrstvách. Počítače pracují ve vrstvách 1 až 7, přepínače ve vrstvách 1 až 2, směrovače ve vrstvách 1 až 3.



Obr. 3 – Průchod dat síťovými zařízeními (LAMMLE, 2015)

Směrovač označujeme jako zařízení, které pracuje na třetí vrstvě, protože je to nejvyšší vrstva ve které pracuje.

2 Vlastnosti IP protokolu

Na síťové vrstvě používáme protokoly IPv4 nebo IPv6. Protokoly jsou navrženy jako protokoly s nízkou režií. Má přiřazené pouze takové funkce, které jsou umožňují doručení paketu od zdrojového zařízení k cílovému přes síťovou infrastrukturu typu LAN nebo WAN. Protokol není navržen pro sledování a správu toku paketů Tyto funkce implementovaly jiné vrstvy.

a) Nespojovaný protokol: není vytvářeno spojení mezi koncovými body před předáním paketů.
b) Nespolehlivý protokol: neudržuje navázané spojení, takže odesílatelé nevědí, zda je cílové zařízení funkční a připraveno přijmout paket. Cílové zařízení zase neví, kdy pakety dorazí. Protokol nezaručuje, že se odeslané pakety cestou neztratí. Pokud jsou doručeny pakety mimo pořadí nebo pakety chybí, musí tyto problémy vyřešit aplikace používající data nebo služby vyšší vrstvy. To umožňuje IP fungovat velmi efektivně. V zásobníku protokolů TCP/IP je spolehlivost úlohou protokolu TCP v transportní vrstvě.
c) Nezávislý na přenosovém médiu: protokol pracuje nezávisle na médiích, která přenášejí data v nižších vrstvách zásobníku protokolu. IP pakety mohou být přenášeny jako elektronické signály přes měděný kabel, jako optické signály přes vlákno nebo

bezdrátově jako rádiové signály. Síťová vrstva sleduje maximální velikost PDU v bajtech, kterou může každé médium přenášet. Tato charakteristika se označuje jako maximální přenosová jednotka (MTU). Součástí řídící komunikace mezi linkovou vrstvou a síťovou vrstvou je stanovení maximální velikosti paketu. Linková vrstva předává hodnotu MTU až do síťové vrstvy. Síťová vrstva pak určuje, jak velké pakety mohou být. V některých případech musí zprostředkující zařízení, obvykle směrovač, rozdělit paket IPv4 při jeho předávání z jednoho média na jiné médium s menší MTU. Tento proces se nazývá fragmentace paketu nebo fragmentace. Fragmentace způsobuje latenci. Pakety IPv6 nemohou být směrovačem fragmentovány.

3 Kontrolní opakovací otázky a úkoly

Jaké jsou hlavní funkce síťové vrstvy v modelu OSI?

S jakou datovou jednotkou pracuje síťová vrstva?

Jak probíhá enkapsulace na síťové vrstvě,

Jaké jsou vlastnosti IP protokolu?

Na jakých vrstvách pracuje router?

4 Použitá literatura

Cisco Network Academy. *Netcad.com* [online]. Cisco, 2023 [cit. 2023-01-11]. Dostupné z: Introduction to Network.

LAMMLE, Todd. CCNA: výukový průvodce. Přeložil Jakub GONER. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.

SOSINSKY, Barrie A. Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.

Seznam zkratek

ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 4
LAN	Local Area Network
MAC	Media Access Control

MTU Maximum transmission unit

OSI Open Systems Interconnection

PDU Protocol Data Unit

RIP Routing Information Protocol

TTL Time To Live

WAN Wide Area Network

Rejstřík

Průmyslové sítě

Téma XII: IPv6 adresy

Studijní cíl

Seznámit studenty s IPv6 adresami.

Doba nutná k nastudování

2 hodiny

Klíčová slova

Protokol IPv6, IPv6 paket, formát IPv6 adresy

1 Vyčerpání IPv4

S masivním nárůstem uživatelů a zařízení využívajících internet došlo k vyčerpání IPv4 adres. Protokol IPv4 způsobuje problémy při využívání některých síťových technologií jako překlad adres (NAT) nebo protokoly, které zabezpečují síťovou komunikaci. Nástupcem je protokol IPv6, který má mnohem větší adresní prostor (128 bitů) a odstraňuje předešlé problémy.

1.1 Protokol IPv6

Bloky, které IPv6 přenáší se označují jako pakety. Rozdíl oproti IPv4 je: v jednodušším formátu paketu, který obsahuje jiný význam položek hlavičky než IPv4; rozšiřující hlavičky jsou úspornější a efektivnější; povinná podpora multicastového vysílání; fragmentovat může pouze odesílající koncové zařízení; má lepší podporu hierarchického směrování a zabudovanou podporu bezpečnosti.

1.1.1 IPv6 paket

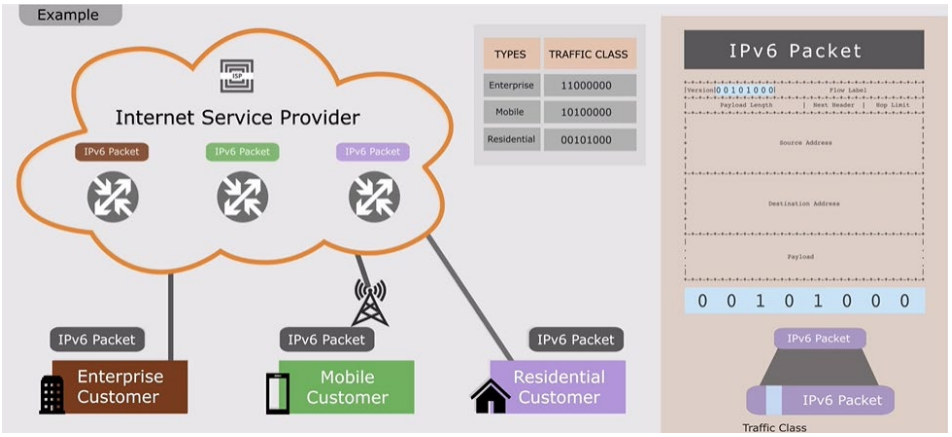
Paket IPv6 se skládá ze dvou hlavních částí: hlavičky a těla. Hlavička se nachází v prvních 40 oktetech (320 bitů) paketu a obsahuje zobrazená pole:

<table>
<tr><td>verze</td><td>třída provozu</td><td colspan="3">značka toku</td></tr>
<tr><td colspan="3">délka dat</td><td>další hlavička</td><td>max. skoků</td></tr>
<tr><td colspan="5">adresa odesílatele</td></tr>
<tr><td colspan="5">adresa cíle</td></tr>
</table>

Obr. 1 – Hlavička IPv6 paketu (SATRAPA, 2019)

Verze (Version) — identifikuje verzi protokolu. Položka Verze (Version) je obvyklým zahájením IP datagramu, které identifikuje verzi protokolu. IPv6 protokol má hodnotu 6, binárně 0110.

Třída provozu (Traffic Class)— pro služby s definovanou kvalitou. Třída provozu (Traffic class), která vyjadřuje prioritu datagramu či jeho zařazení do určité přepravní třídy. Délka pole je 8 bitů. Cílem je, aby tato položka umožnila IP poskytovat služby se zaručenou kvalitou. Používá pole diferencované služby DSCP (differentiated services code point) a pole ECN (explicit congestion notification) k nastavení priority pro datagramy pro přednostní zpracování či naopak odkládání až po ostatních.



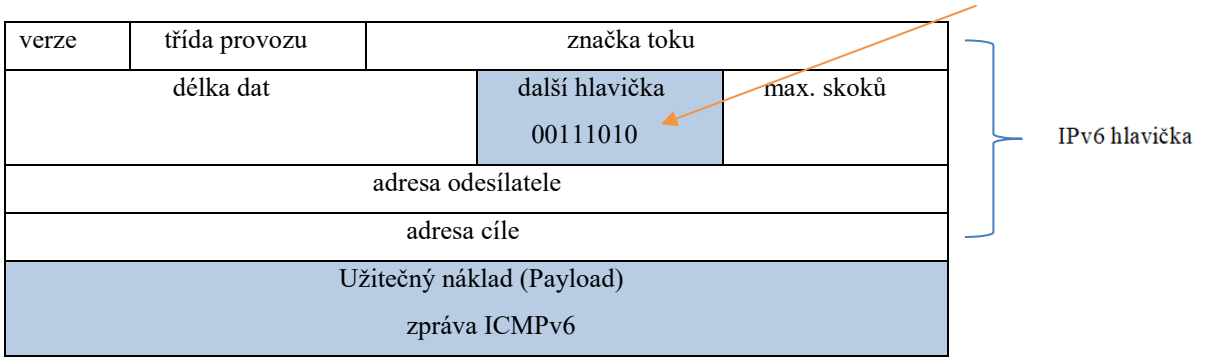
Obr. 2 – Třída provozu (RIPE, 2023)

Značka toku (Flow Label)— identifikuje tok (proud souvisejících paketů). K identifikaci toku v IPv4 musí být k dispozici následující údaje: zdrojová IP adresa, zdrojový port, cílová IP adresa, cílový port, transportní protokol. Problém je v tom, že tři z pěti údajů patří do transportní vrstvy a nemusí být snadno dostupné. K identifikaci toku v IPv6 musí být k dispozici následující údaje: zdrojová IPv6 adresa, cílová IPv6 adresa, značka toku. Všechny najdeme na třetí vrstvě.

Prostřednictvím identifikátoru (značky) a dvojice adres směrovač rychle rozpozná, že paket je součástí určitého toku, což mu usnadní rozhodování o jeho dalším osudu (bude s ním naloženo stejně, jako s předchozími členy téhož toku). Délka pole je 20 bitů. Přidělení značky toku má na starosti odesilatel datagramu. Během přepravy sítí se značka nesmí měnit a musí být příjemci doručena se stejnou hodnotou, jakou jí přidělil odesilatel. Z tohoto obecného pravidla ovšem existují dvě výjimky. První je motivována bezpečností: Pokud by některý ze směrujících strojů dospěl k závěru, že se někdo snaží zneužít značky k vytvoření tajného informačního kanálu, smí do nich zasáhnout. Druhou výjimkou je nulová značka. Jestliže se odesilatel rozhodl datagram neznačkovat, může to za něj udělat některý ze směrovačů (Typickými kandidáty pro takové chování jsou přístupový směrovač koncové sítě nebo vstupní směrovač poskytovatele Internetu). Jakmile došlo ke vložení nenulové hodnoty, musí už dále zůstat neměnná. Pokud je hodnota 0, tak tok není označen

Délka dat (Payload Length) — počet bajtů za hlavičkou. Přesně řečeno počet bajtů následujících za standardní hlavičkou. Základní hlavička se do této délky nepočítá, zatímco případné rozšiřující hlavičky ano. Pole je dvoubajtové s maximální délkou 64 kB.

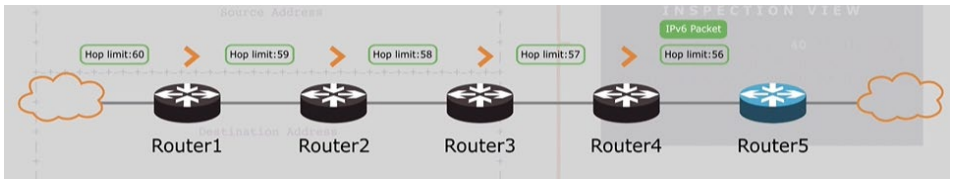
Další hlavička (Next Header)— obsahuje identifikaci, jaká hlavička či jaký druh dat následuje za standardní hlavičkou. Délka pole je 8 bitů. Rozšiřující hlavičky jsou volitelné a jsou řazeny za sebou. Položka Next Header udává typ další rozšiřující hlavičky nebo typ nákladu v těle paketu u poslední hlavičky. Identifikátory typů v rozšiřující hlavičce spravuje IANA. Hodnoty vybraných rozšiřujících hlaviček v desítkovém formátu: TCP = 6; UDP = 17; ICMPv6 = 58; Fragment Header = 44. Do pole další hlavička se zapisuje binární hodnota, takže $58_{10} = 00111010_2$.



Obr. 3 – Další hlavička (SATRAPA, 2019)

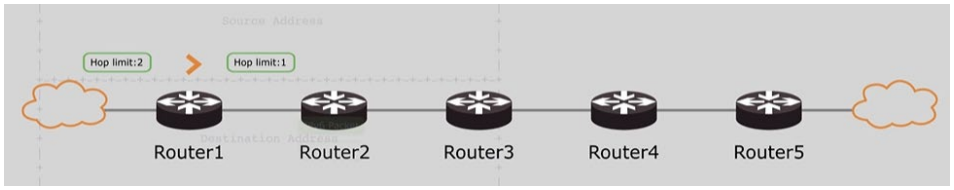
Max. skoků (Hop Limit) — obdoba TTL (životnost paketu), omezuje dosah. Nahrazuje dobu životnosti IPv4 paketu (TTL). Průchod datagramu jedním směrovačem je považován za jeden skok. Odesilatel v této položce uvede, kolik takových skoků smí datagram maximálně absolvovat. Každý směrovač po cestě pak sníží hodnotu o jedničku. Délka pole je 8 bitů. Dojde-li tím k vynulování položky, datagram bude zlikvidován a odesilateli se pošle ICMP zpráva o vypršení maximálního počtu skoků.

Příklad úspěšné doručení: Posíláme paket do Routeru 5, hodnota Hop limitu je 60. Router1 přijme paket, zpracuje, sníží hodnotu Hop limit a předá na Router2.



Obr. 4 – Úspěšné doručení na Router5 (RIPE, 2023)

Příklad neúspěšné doručení: Posíláme paket do Routeru 5, výchotí hodnota Hop limitu je 2.

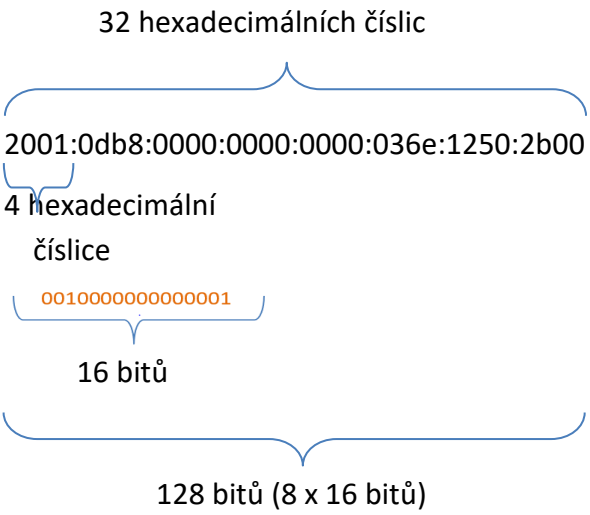


Obr. 5 – Neúspěšné doručení (RIPE, 2023)

Zdrojová a cílová adresa (Source and Destination Address)— adresa zdroje 128 bitů, adresa cíle 128 bitů.

1.2 Formát IPv6 adresy

zápis IPv6 adresy v hexadecimálním formátu, 128 bitů (16 bytů) je rozděleno po dvou bytech dvojtečkou.



Obr. 6 – Formát adresy (SATRAPA, 2019)

1.2.1 Zápis IPv6 adresy

Pro lepší zápis adresy, lze uplatnit několik pravidel:

- počáteční nuly v každé dvojici bytů lze vynechat (příklad: 2001:1488:0:3:0:0:0:2),
- sousedící nulu lze nahradit dvojitou dvojtečkou :: (příklad: 2001:1488:0:3::2).

Zkrácení zápisu dvojitou dvojtečkou lze použít pouze jednou z důvodu nejednoznačnosti interpretace výsledného zápisu adresy.

2 Typy IPv6 adres

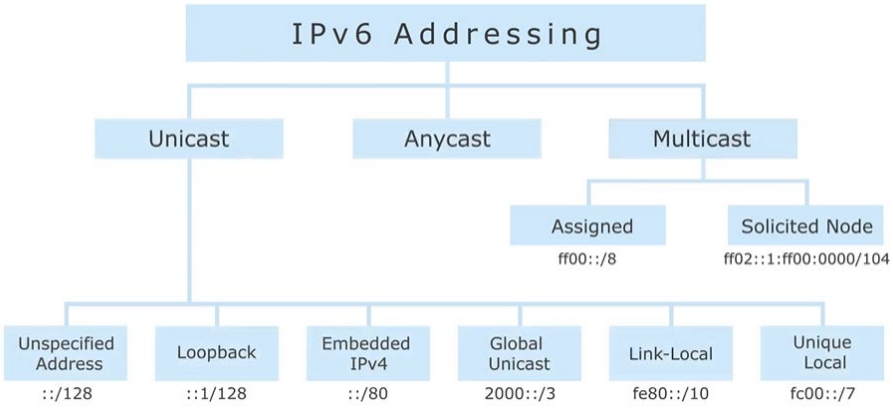
Individuální adresy (unicast) − označují jedno rozhraní připojeného počítače či zařízení.

Skupinové adresy (multicast) − představují adresu skupiny síťových rozhraní. Paket se skupinovou cílovou adresou bude dopraven všem členům skupiny. Tyto adresy se používají nejčastěji pro šíření zvukového či obrazového signálu, videokonference a podobně.

Výběrové adresy (anycast) − také označují skupinu síťových rozhraní, ale paket bude dopraven jen na jedno z nich (zpravidla to nejbližší). Výběrové adresy umožňují například realizovat některé speciální služby např. klient odešle datagram s obecnou adresou a některý z dostupných serverů se jej ujme.

V porovnání se současným IP tedy zmizely všesměrové (broadcast) adresy. Jejich roli převzaly obecnější adresy skupinové.

Pevně definované standardní skupiny (například ff02::1 pro všechny uzly připojené k dané lince) pak nahrazují původní všesměrové adresy.



Obr. 7– IPv6 adresy (SATRAPA, 2019)

2.1 Povinné adresy

IPv6 definuje určité adresy jako povinné. Každý stroj se k nim musí hlásit a pokud zařízení plní úlohu směrovače, je seznam ještě početnější.

Pro počítač (host)

- lokální linková pro každé rozhraní,
- všechny individuální a výběrové, které mu byly přiděleny,
- lokální smyčka (loopback, ::1),
- skupinové adresy pro všechny uzly (ff0x::1, kde x zastupuje odpovídající dosahy),
- skupinová adresa pro vyzývaný uzel pro všechny přidělené individuální a výběrové adresy,
- všechny skupinové adresy, jejichž je členem.

Pro směrovač (router)

- všechny adresy povinné pro počítač a navíc,
- výběrová adresa pro směrovače v podsíti pro každé rozhraní, kde funguje jako směrovač,
- skupinové adresy pro všechny směrovače (ff0x::2, kde x zastupuje odpovídající dosahy).

2.2 Objevování sousedů

Nahrazuje ARP, které v IPv4 slouží k vyhledání linkové adresy pro IP adresu sousedního počítače, a přidává k němu funkce související se směrováním či automatickou konfigurací. Seznam jeho funkcí:

- zjišťování linkových adres sousedních uzlů (ze stejné podsítě) a jejich aktualizace,
- hledání směrovačů,
- přesměrování,

- zjišťování síťových parametrů pro automatickou konfiguraci,
- ověřování dosažitelnosti sousedů,
- detekce duplicitních adres.

Používá pět zpráv, které přenáší prostřednictvím ICMPv6:

- Ohlášení směrovače (router advertisement) - v něm směrovač oznamuje síťové parametry (především prefix zdejších adres); slouží především pro automatickou konfiguraci.
- Výzva směrovači (router solicitation) - pokud nepřichází ohlášení směrovače, může o ně uzel touto zprávou požádat.
- Ohlášení souseda (neighbor advertisement) - posílá soused, aby o sobě poskytl požadované informace.
- Výzva sousedovi (neighbor solicitation) - žádá souseda o jeho ohlášení; používá se ke zjišťování linkových adres a detekci dosažitelnosti.
- Přesměrování (redirect) - doporučuje adresátovi, aby datagramy k určitému cíli posílal přes jiného souseda; umožňuje opravovat nedokonalosti ve směrovací tabulce.

2.2.1 Zjišťování linkových adres

Tato funkce objevování sousedů slouží k získání linkové (MAC) adresy sousedního počítače, kterému chce odesilatel poslat datagram. Vychází ze znalosti IPv6 adresy cíle, z níž sestaví adresu vyzývaného uzlu (solicited node address). Jedná se o skupinovou adresu s dosahem omezeným na linku, která začíná pevně daným prefixem.

2.3 Automatická konfigurace

Pro realizaci automatické konfigurace používáme dvě metody stavovou a bezstavovou automatickou konfiguraci.

2.3.1 Stavová konfigurace

Jedná se o konfiguraci prostřednictvím DHCPv6. Počítač rozešle dotaz a DHCP server mu v odpovědi sdělí vše, co by o zdejší síti měl vědět. Takhle to dnes funguje zcela běžně v řadě IPv4 sítí. V síti IPv6 však nastala zásadní změna, konfigurace klienta pomocí DHCPv6 je pouze doplňující mechanismus. Primární informace o síti se klient dozví z ohlášení směrovačů (RA). Takže v DHCPv6 nelze klientovi nakonfigurovat prefix podsítě (subnet mask), ani implicitní směrovač (default router). Přidělení IPv6 adresy protokolem DHCPv6 je volitelné, směrovač v síti určuje pomocí inzerovaných příznaků, zda má klient DHCPv6 použít pro konfiguraci adresy (příznak M=1 v RA) nebo pouze pro konfiguraci parametrů sítě (Bezstavové DHCPv6, příznak M=0 a O=1 v RA). Typické parametry, které musíme klientovi předat v DHCPv6 jsou IPv6 adresy DNS serverů (rekurzivních resolverů) a implicitní doménová přípona (domain search suffix).

2.3.2 Bezstavová konfigurace

Bezstavová konfigurace (stateless autoconfiguration) nevyžaduje žádné servery. Jejím základním pilířem je Objevování sousedů. Každý směrovač v určitých intervalech rozesílá do sítí, k nimž je připojen, tak zvané ohlášení směrovače. V něm jsou obsaženy základní informace, především prefixy adres dané sítě a zda on sám může sloužit pro předávání paketů ven (jako implicitní směrovač, default gateway).

Z ohlášení směrovačů (o které může při startu aktivně požádat pomocí výzvy směrovači) se počítač dozví, jaké adresy používá zdejší síť. K nim si doplní identifikátor rozhraní (typicky 64 bitů), který si jednoznačně vygeneruje ze své ethernetové adresy. Tak získá platné IPv6 adresy pro své rozhraní. Jejich jednoznačnost ověří pomocí detekce duplicit – pomocí výzvy sousedovi se dotáže, zda vytvořenou adresu již někdo nepoužívá. Dostane-li kladnou odpověď, nesmí adresu svému rozhraní nastavit a automatická konfigurace skončí neúspěšně.

3 Kontrolní opakovací otázky a úkoly

Jaký byl důvod pro zavedení IPv6 adres?

Jaký je formát pro zápis IPv6 adres?

Jakým způsobem lze provést zkrácení zápisu IPv6 adresy? Uveďte dvě pravidla.

Zapište IPv6 adresu ve zkrácené formátu 2001:0db8:ab00:00c3:0000:0000:0000:0002.

Kolik bitů je dlouhá IPv6 adresa a kolik to přináší možných adres?

Jaké adresy v IPv6 nejsou oproti IPv4?

Jak vypadá hlavička IPv6 adresy?

Jaká hodnota v IPv6 nahradila TTL?

Jaká je hodnota v binárním zápisu verze iPv6 v hlavičce paketu?

Jak se zjišťují v IPv6 linkové adresy?

Jakým způsobem lze získat IPv6 adresu?

Jaké jsou typy unicastových adres v IPv6?

O jaký typ adresy se jedná pokud začíná fe80::/10?

Jaké IPv6 adresy potřebuje počítač pro síťovou komunikaci?

Jaký je ekvivalent adresy 127.0.0.1 v IPv4 pro IPv6?

4 Použitá literatura

LAMMLE, Todd. CCNA: výukový průvodce. Přeložil Jakub GONER. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.

RIPE Network Coordination Centre. RIPE Network Coordination Centre [online]. RIPE NCC, 1992 [cit. 2023-06-06]. Dostupné z: https://www.ripe.net/

SATRAPA, Pavel. IPv6: internetový protokol verze 6. 4. aktualizované a rozšířené vydání. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-43-0.
https://www.ipv6.cz/cs/povinne_adresy

Seznam zkratek

ARP	Address Resolution Protocol
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DNS	Domain Name System
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Protocol version 4
MAC	Media Access Control
NAT	Network Address Translation
RA	Router Advertisement
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

Rejstřík

Průmyslové sítě

Téma XIII: Protokoly aplikační vrstvy

Studijní cíl

Seznámit studenty s nejčastěji používanými protokoly aplikační vrstvy.

Doba nutná k nastudování

2 hodiny

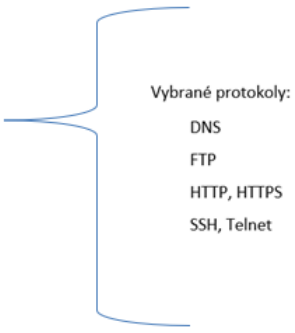
Klíčová slova

Aplikační vrstva, služby a protokoly aplikační vrstvy

1 Aplikační vrstva

V modelech OSI a TCP/IP je aplikační vrstva nejbližší vrstvou ke koncovému uživateli. Je to vrstva, která poskytuje rozhraní mezi aplikacemi používanými ke komunikaci a základní sítí, přes kterou jsou zprávy přenášeny. Protokoly aplikační vrstvy se používají k výměně dat mezi programy spuštěnými na zdrojovém a cílovém hostiteli.

<table>
<tr><th>Model OSI</th><th>Model TCP/IP</th></tr>
<tr><td>Aplikační vrstva</td><td rowspan="3">Aplikační vrstva</td></tr>
<tr><td>Prezentační vrstva</td></tr>
<tr><td>Relační vrstva</td></tr>
<tr><td>Transportní vrstva</td><td>Transportní vrstva</td></tr>
<tr><td>Síťová vrstva</td><td>Internetová vrstva</td></tr>
<tr><td>Linková vrstva</td><td rowspan="2">Vrstva síťového přístupu</td></tr>
<tr><td>Fyzická vrstva</td></tr>
</table>



Obr. 1 Protokoly aplikační vrstvy TCP/IP (SOSINSKY, 2012)

1.1 Služby z pohledu uživatele

Počítačové sítě poskytují uživatelům využívat síťové služby, které pracují v komunikačním modelu klient/server. Komunikaci vždy v tomto modelu zahajuje klient (koncové zařízení) a server čeká na požadavek klienta, kterému poskytuje data. Procesy v serveru řídí způsob doručení dat klientovi. Následující tabulka obsahuje služby, které klienti využívají.

Tab. 1 – Síťové aplikační služby (LAMMLE, 2015)

Služba	Popis
Jmenné služby	Použití DNS serveru, který překládá doménové jméno na IP adresu.
Souborové služby	Použití souborového serveru pro přístup k souborům dalším klientským počítačům
Webové služby	Použití Web serveru pro poskytnutí dat pomocí protokolů HTTP, HTTPS
Vzdálené připojení	Použití protokolu SSH. Klient se hlásí jako virtuální terminál ke vzdálenému serveru.
Elektronická pošta	Použití protokolů SMTP, POP a IMAP pro elektronickou poštu.
Tiskové služby	Použití tiskového serveru, který má připojenou tiskárnu. Obsluhuje požadavky klientů na tisk.
Dynamická klientů v lokální síti	Použití DHCP protokolu pro automatické přidělování IP adres.

2 Protokoly aplikační vrstvy

Protokoly aplikační vrstvy jsou používány zdrojovým i cílovým zařízením během komunikace. Aby byla komunikace úspěšná, musí být protokoly aplikační vrstvy, které jsou implementovány na zdrojovém a cílovém hostiteli vzájemně kompatibilní.

2.1 Protokol DNS

DNS (Domanin Name Service) je protokol pro překlad (resolve) doménových jmen na IP adresy. Klient služby DNS se označuje jako DNS resolver. Doménové jméno je jednoznačná identifikace jednoho síťového zařízení nebo jedné sítě v internetu. Domény mají hierarchickou stromovou strukturu: každý DNS server má jednoznačně definovaný nadřazený server a DNS klient má jednoznačně definovaný DNS server. DNS poskytuje následující informace:

- IP adresu hostitele,
- název domény hostitele podle jeho IP adresy,
- alias hostitele, typ jeho CPU a operačního systému,
- síťové protokoly podporované hostitelem,
- poštovní bránu,
- schránku – skupinu zpráv.

DNS servery komunikují s dalšími DNS servery a klienty (tzv. resolvery) nad protokoly TCP a UDP, v obou případech na portu 53. Při běžných dotazech se požadavek posílá jedním paketem UDP a odpověď se vrací opět v paketu UDP. Tento protokol byl zvolen pro svou jednoduchost a minimální režii, kdy se nemusí kvůli malým datům složitě navazovat spojení přes protokol TCP.

2.1.1 Princip fungování DNS

Klent si chce zobrazit ve svém prohlížeči webovou stránku www.netacad.com. Počítač tohoto klienta pošle dotaz na jméno www.netacad.com lokálnímu DNS serveru. Pokud má uloženou adresu, tak ji poskytne počítači uživatele. Ale může nastat situace, že nemá uložený záznam v paměti cache. Potom se musí lokální DNS server zeptat některého z kořenových serverů. Pokud odpověď nezná, ale jelikož zná alespoň kam je delegována doména .com, pošle seznam jmenných serverů pro doménu .com. Lokální DNS použije informaci od kořenového serveru a zeptá se jednoho z těchto serverů na jméno www.netacad.com a klient dotazuje jmenné servery dokud neobdrží potřebné informace.

2.2 Protokol FTP

FTP (File Transfer Protocol) je nešifrovaný protokol, který se používá pro přenos souborů mezi systémy. FTP vytváří dvě spojení mezi klientem a serverem. Jedno spojení je určeno pro přenos příkazů z klienta na portu 21 a druhé spojení pro přenos souborů na portu 20. Na serveru je spuštěn démon FTPd. Použití FTP závisí na nastavení práv na jednotlivých počítačích např. pro sdílení dat (např. foto, video, hudba, vlastní práce).

2.2.1 Příkazy FTP

Příkazy protokolu FTP jsou přenášeny textově. Příkaz je vždy tvořen klíčovým slovem, za kterým mohou následovat parametry oddělené mezerou.

- Příkaz **open** je pro připojení ke vzdálenému FTP serveru.
- Příkaz **dir** je pro výpis adresáře.
- Příkaz **put** je pro zaslání jednoho souboru.
- Příkaz **get** je pro přijmutí jednoho souboru.

2.3 Protokol HTTP a HTTPS

Protokol HTTP (HyperText Transfer Protocol) je jedním z nejdůležitějších protokolů, který zajišťuje přenos dat přes internet. Používá protokol transportní vrstvy TCP s portem 80. Protokol HTTP zahrnuje přenos dat v režimu požadavek-odpověď. Zároveň lze v rámci takové interakce přenášet prakticky jakýkoli typ dat – prostý text, hypertext (HTML), styly, klientské skripty, obrázky, dokumenty v různých formátech, binární informace atd.

Zpráva HTTP se skládá ze tří částí, přenášených v určeném pořadí:

- Výchozí řádek – definuje typ zprávy.
- Záhlaví – charakterizují tělo zprávy, parametry přenosu a další informace.
- Tělo zprávy – samotná data zprávy (od záhlaví musí být oddělena prázdným řádkem).

Typy zpráv http

- GET vyjadřuje žádost klienta o data ze serveru. Webový prohlížeč klienta posílá zprávu GET s žádostí o stránku na webový server.

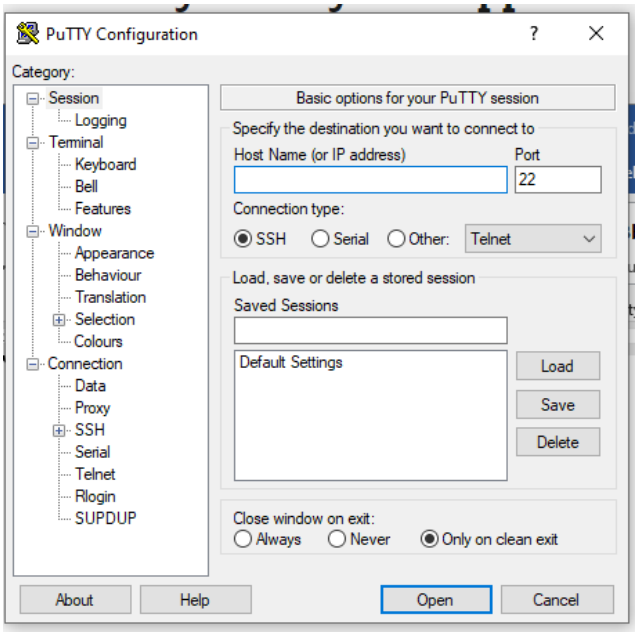
- POST a PUT zprávy jsou použity k odeslání zprávy, která umísťuje data z klienta na webový server.

Jedná se o nezabezpečený protokol, jehož zprávy POST jsou odesílány v přímém textu. Z toho důvodu je nutné používat šifrovaný protokol HTTPS, který komunikuje na portu 443.

2.4 Vzdálené přihlášení

2.4.1 Protokol Telnet

Vzdálené přihlášení pomocí protokolu Telnet (TELetype NETwork Service) je služba emulace terminálu pro vzdálený přístup k serverům a síťovým zařízením. Relace VTY (Virtual terminal) vytvoří rozhraní příkazového řádku na vzdáleném zařízení (směrovač, přepínač). Aplikace PuTTY je vhodným klientem vybavená grafickým prostředím, které umožňuje nastavení parametrů připojení.



Obr. 2 – Okno aplikace PuTTY (PuTTY, 2023)

Přístup pomocí telnetu je aktivní ve chvíli, kdy nastavíme IP adresu, ke které se budeme připojovat. Na přepínači musíme přiřadit adresu na rozhraní vlan 1. Dále musíme nastavit heslo pro telnet session. V nastavení určujeme kolik současných spojení je povoleno, maximálně 16 (záleží na modelu). Důležité je vložit příkaz login, který vyzve k zadání hesla.

```
Sw1>enable
Sw1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1(config)#line vty 0 15
Sw1(config-line)#password HESLO
Sw1(config-line)#login
```

Obr. 3 – Nastavení Telnetu na přepínači Sw1

Na dalším obrázku je připojení klienta k přepínači Sw1 v síťovém simulátoru Packet Tracer. Klient otevře příkazový řádek a zadá příkaz telnet a cílovou adresu. V tomto případě

192.168.1.2 (adresa vlan 1 na Sw1). Pokud je povolen na přepínači protokol Telnet, tak se otevře spojení. Klient je vyzván k zadání hesla. Po úspěšném zadání je připojen k zařízení a může provádět změny.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.1.2
Trying 192.168.1.2 ...Open


User Access Verification

Password:
Sw1>
```

Obr. 4 – Připojení klienta pomocí Telnetu

Telnet má nevýhodu, že se veškerá data (včetně hesel) zasílají v přímém textu, nešifrovaná, takže je možno je odposlechnout. Vhodnější je použít protokol SSH, který je šifrovaný.

2.4.2 Protokol SSH

Protokol SSH ((Secure SHell – zabezpečený shell) poskytuje bezpečné ověřování, připojení a bezpečný přenos dat mezi síťovými zařízeními šifrováním provozu. Existují dvě verze protokolu SSH, které nejsou vzájemně kompatibilní.V současnosti se používá verze 2. Protokol SSH-2 pro svoji činnost používá tři protokoly: protokol připojení, ověřovací protokol a protokol transportní vrstvy.

Konfigurace protokolu SSH probíhá obdobně jako pro telnet. Jednotlivé kroky jsou:

- Ve výpisu je nejprve nastaveno jméno směrovači na R1.
- Následně je vytvořeno jméno domény pro certifikát (vytvořený v dalším kroku).
- Zapnutí serveru SSH na směrovači pro lokální a vzdálenou autentizaci a vygenerování klíče 0 velikosti 1024. Po potvrzení se spustí proces generování.
- Vytvoření uživatele a nastavení hesla.
- Nastavení nastavení přístupových linek pro protokol SSH.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1

R1(config)#ip domain name upce.cz
R1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.upce.cz

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 12:52:13.37: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#username Jmeno secret heslo
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#
```

Příkazy pro připojení klienta k síťovému zařízení. V příkazovém řádku **username** odpovídá hodnota zadaná na síťovém zařízení tj. Jmeno a **target** je adresa směrovače.

```
C:\> ssh /?
Packet Tracer PC SSH
Usage: SSH -l username target
C:\>
```

3 Kontrolní opakovací otázky a úkoly

Popište funkce aplikační vrstvy v síťovém modelu OSI a uveďte příklady protokolů používaných na této vrstvě.

Jaká je úloha protokolu SSH?

Porovnejte protokol Telnet a SSH?

Pokud se po zadání nějaké URL v prohlížeči objeví chybová hláška. O jaký se může jednat problém za předpokladu, že mám funkční internetové připojení?

Vytvořte si v Packet Traceru síťovou topologii a nakonfigurujte si vzdálený přístup pro přepínač.

4 Použitá literatura

Cisco Network Academy. *Netcad.com* [online]. Cisco, 2023 [cit. 2023-01-11]. Dostupné z: Introduction to Network.

Download PuTTY [online]. 1998 [cit. 2023-06-06]. Dostupné z: https://www.chiark.greenend.org.uk/~sgtatham/putty/

LAMMLE, Todd. CCNA: výukový průvodce. Přeložil Jakub GONER. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.

SOSINSKY, Barrie A. Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.

Seznam zkratek

DNS	Domain Name System
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPs	Hypertext Transfer Protocol Secure
OSI	Open Systems Interconnection
SSH	Secure Shell
TCP	Transmission Control Protocol

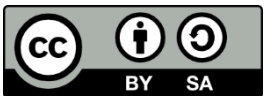
UDP User Datagram Protocol

Rejstřík

UNIVERZITA PARDUBICE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Vytvořeno v rámci projektu **Studijní program Automatizace (SPAUT) na Univerzitě Pardubice**, reg. č. NPO_UPCE_MSMT-16591/2022.

Toto dílo podléhá licenci Creative Commons BY 4.0. Pro zobrazení licenčních podmínek navštivte https://creativecommons.org/licenses/by-sa/4.0/.



Financováno Evropskou unií
NextGenerationEU

Národní plán obnovy

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY