



ASA

Ethernet pro oblasti Small-Middle-Business & Enterprises



Obsah

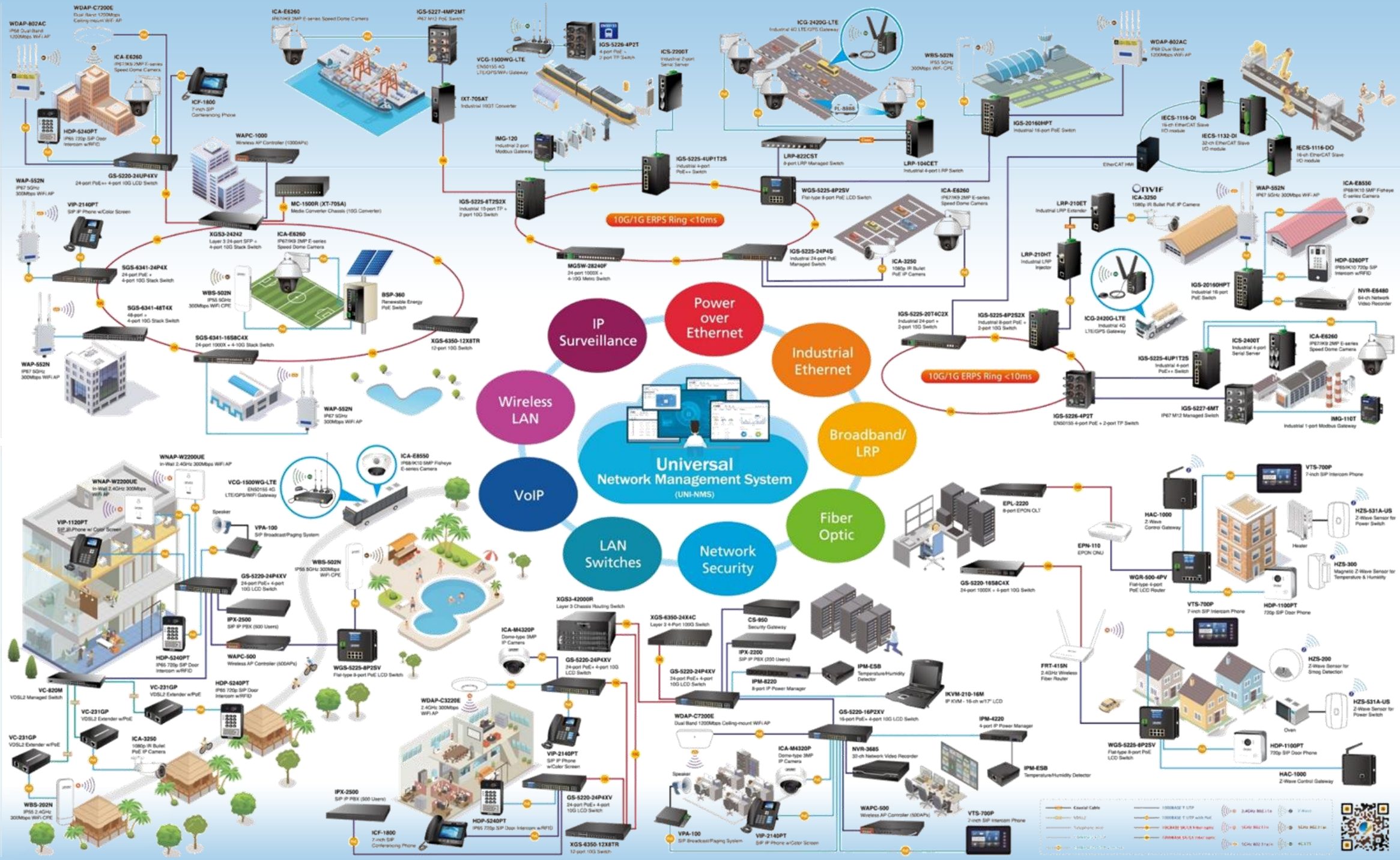
- Kdo jsme?
- Seznámení s technologií Ethernet
- Hardware pro Small-Middle-Businesses & Entreprises
- Referenční použití přepínačů v praxi
- Monitoring

- ASM tradice 30 let na trhu
- Důraz na vytváření trvalých hodnot
- Přes 20 let dodáváme a projektujeme datové sítě
- 15let jako ISP (WiFi ~ ADSL)
- 20 let průmyslové počítače a příbuzné komponenty
- 20 let kamerové systémy od CVBS po IP
- 15 let videovrátné systémy
- Zaměření na montážní firmy, systémové integrátory a ISP
- Nyní společné zázemí 100MEGA / ASM / i4wifi

Co u nás naleznete?

- Aktivní síťové prvky
- Pasivní prvky pro instalace v rámci
- Kamerové systémy
- Videovrátné systémy IP a 2-drát
- EZS zabezpečovací systémy
- Extendery, konvertory
- Optické sítě, svářečky, OTDR měřáky
- Datové a koax. kabely, racky
- Průmyslové počítače
- Speciality, které jinde snadno nepořídíte





Universal Network Management System (UNI-NMS)

10G/1G ERPS Ring <10ms

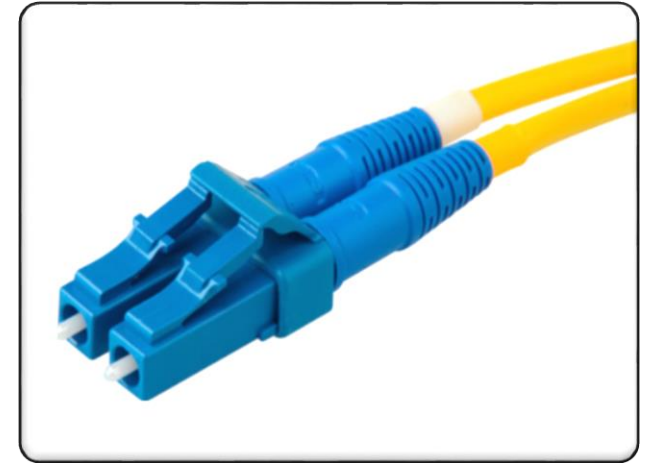
10G/1G ERPS Ring <10ms

● General Cable	● H3C/241 10/100/1000Mbps
● Coaxial Cable	● H3C/241 10/100/1000Mbps PoE
● Ethernet Cable	● H3C/241 10/100/1000Mbps PoE+
● Fiber Optic Cable	● H3C/241 10/100/1000Mbps PoE++
● Cat5e Ethernet Cable	● H3C/241 10/100/1000Mbps PoE+++
● Cat6 Ethernet Cable	● H3C/241 10/100/1000Mbps PoE++++





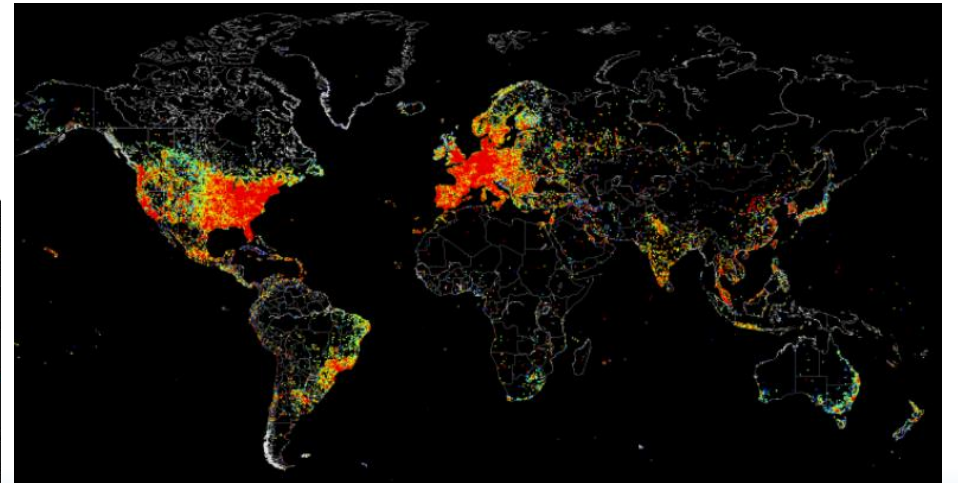
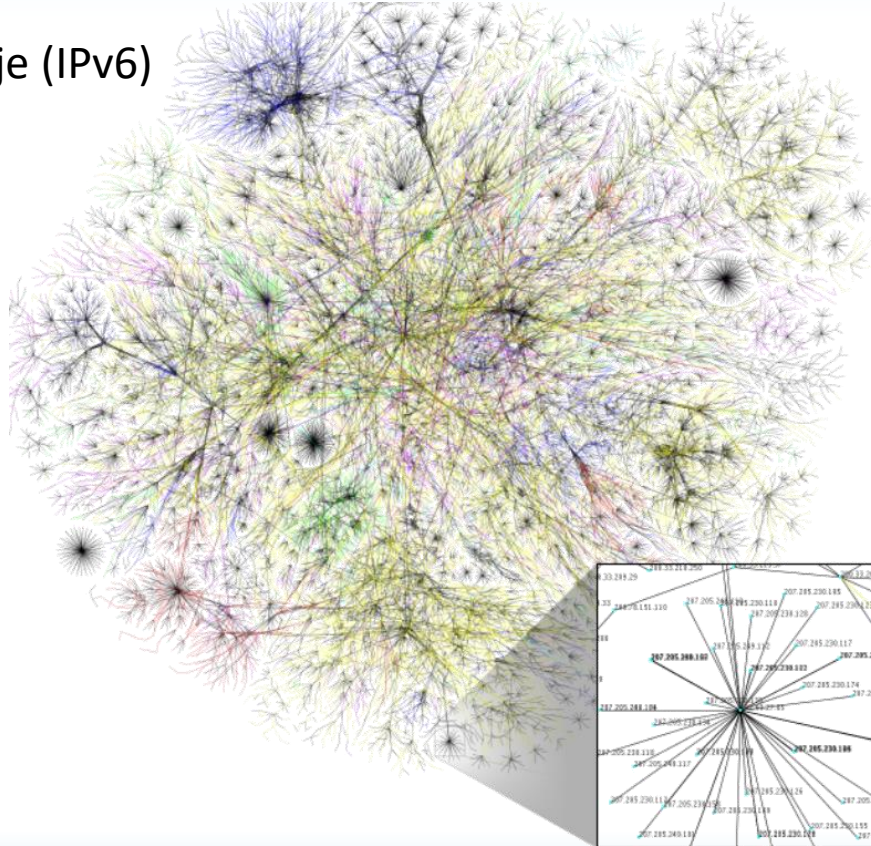
Ethernet



Internet

Ethernet není Fernet ale *může* být Internet 😊

- zatím největší infrastruktura vytvořená člověkem(!)
 - stále se rozvíjí (IoT) a inovuje (IPv6)
 - 30. výročí v ČR...
-
- standardy a normy
 - infrastruktura a topologie
 - síťový model OSI



Standardy a normy

Norma - požadavek na chování nebo vlastnosti věci, člověka, situace apod., určený buď k závaznému vyžadování nebo k posuzování jejich přijatelnosti nebo obvyklosti. V původním latinském významu slovo znamenalo „pravítko, měřítko, pravidlo“.

ISO - International Organization for Standardization, vychází však z řečtiny „isos“(Mezinárodní organizace pro normalizaci), je světovou federací národních normalizačních organizací se sídlem v Ženevě, založena 1947.

IEEE - Institute of Electrical and Electronics Engineers (Institut pro elektrotechnické a elektronické inženýrství), mezinárodní nezisková profesionální organizace usilující o vzestup technologie související s elektrotechnikou. Institut čítá nejvíce členů technické profese ve světě, přes 360 000 členů ve 175 zemích. USA, New York.

ANSI - American National Standards Institute (Americká standardizační organizace), nezisková organizace, která vytváří průmyslové standardy ve USA. Je členem organizace ISO a IEC (International Electrotechnical Commission). Založena 1918 jako American Engineering Standards Committee, reorganizována na American Standards Association v roce 1928. Roku 1966 reorganizován jako United States of America Standards Institute. Roku 1969 změněno jméno na American National Standards Institute. USA, Washington.

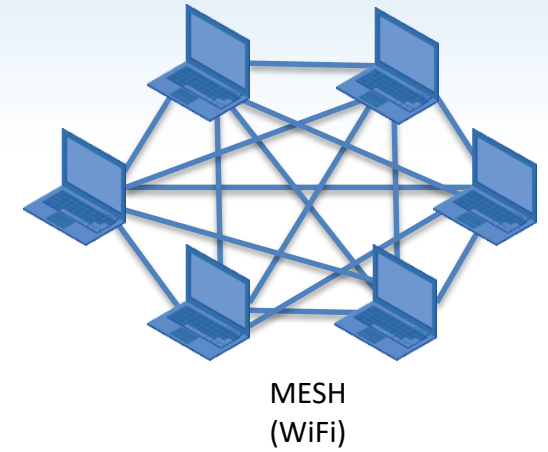
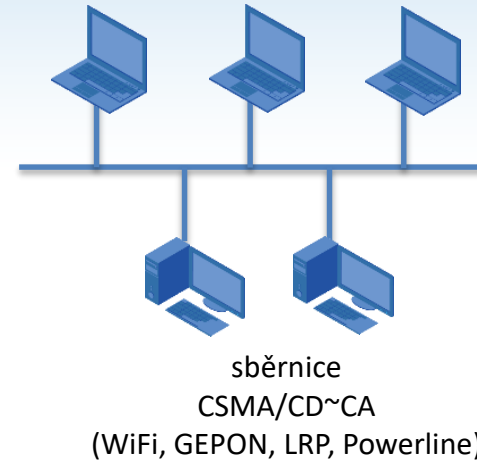
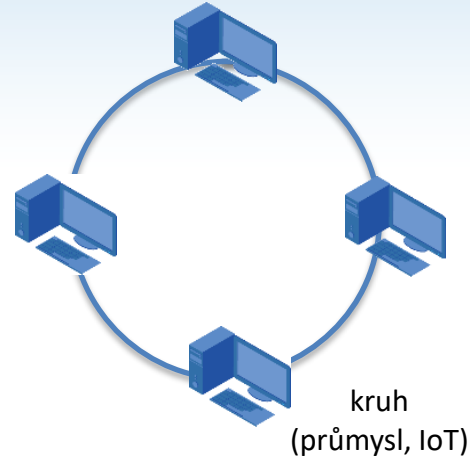
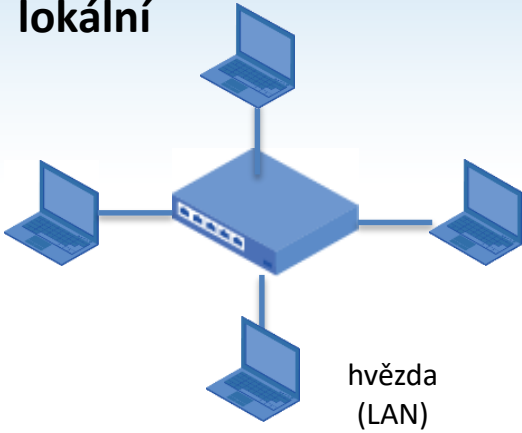
ETSI - The European Telecommunications Standards Institute, evropská obdoba ANSI, spoluvytvořila standardy pro systémy GSM, TETRA, 3GPP, telekomunikace, vysílání apod. Založena 1988 ve Francii, 740 členů v 62 státech.

Spojením ETSI (telecommunication) a CEN (other technical areas) vznikl normalizační úřad **CENELEC** - není EU institucí, je k Evropě vázána geograficky.

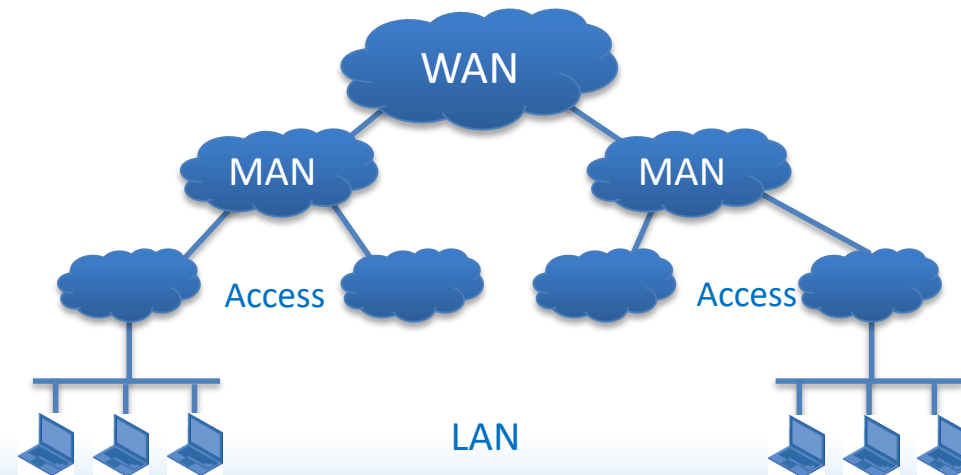
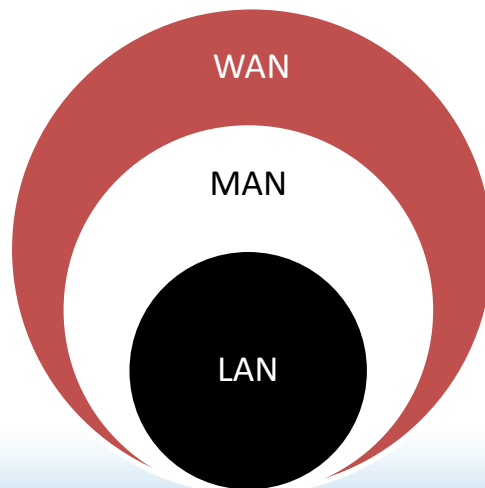
ITU - International Telecommunication Union je specializovaná agentura OSN zabývající se problematikou informačních a komunikačních technologií. Založena 1865 v Paříži při založení telegrafní konvence. Dále se rozšiřovala (CCIT, CCIR, atd), dnes Ženeva.

Topologie

➤ lokální



➤ globální

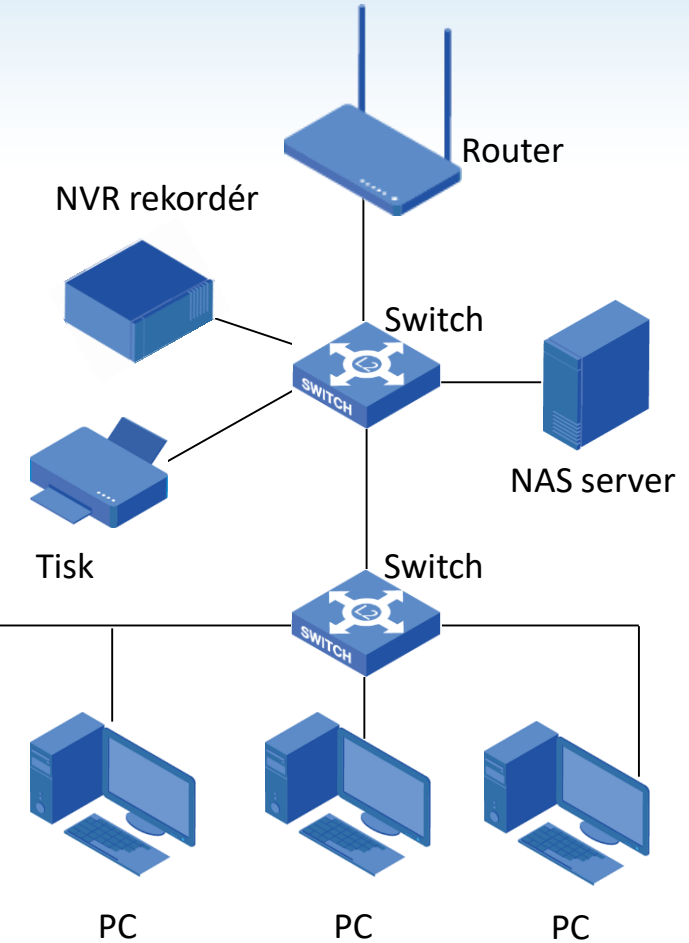


Topologie

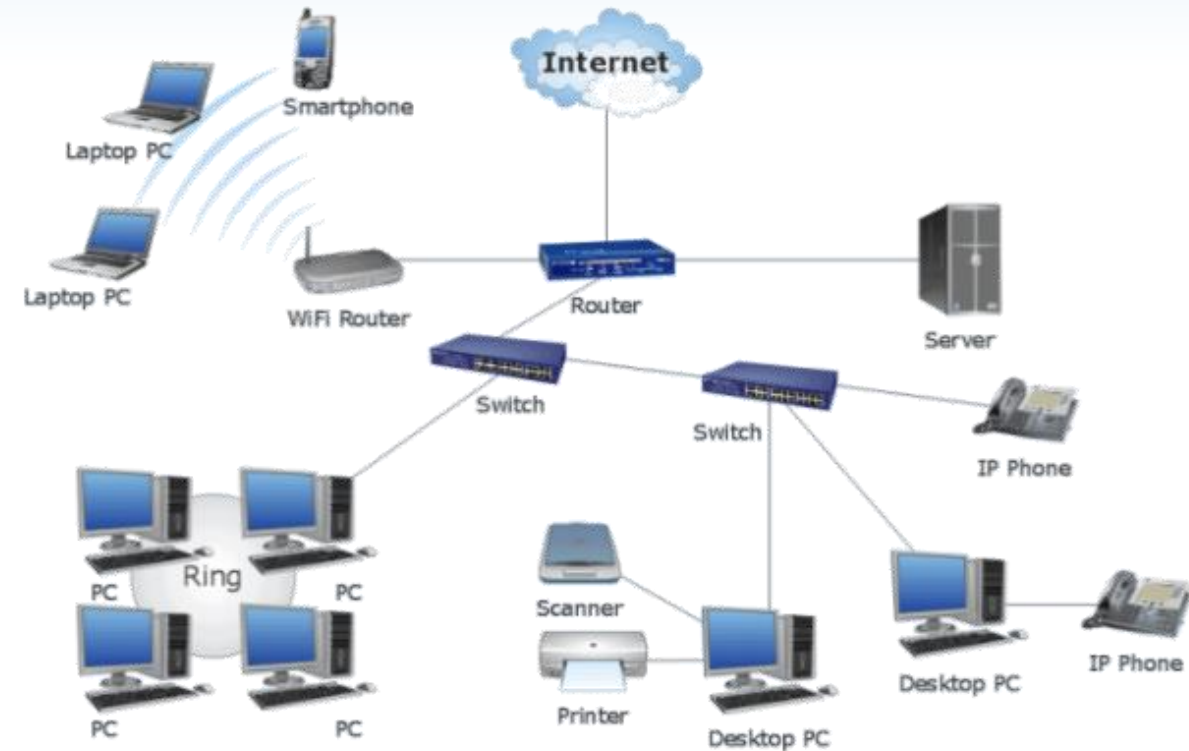
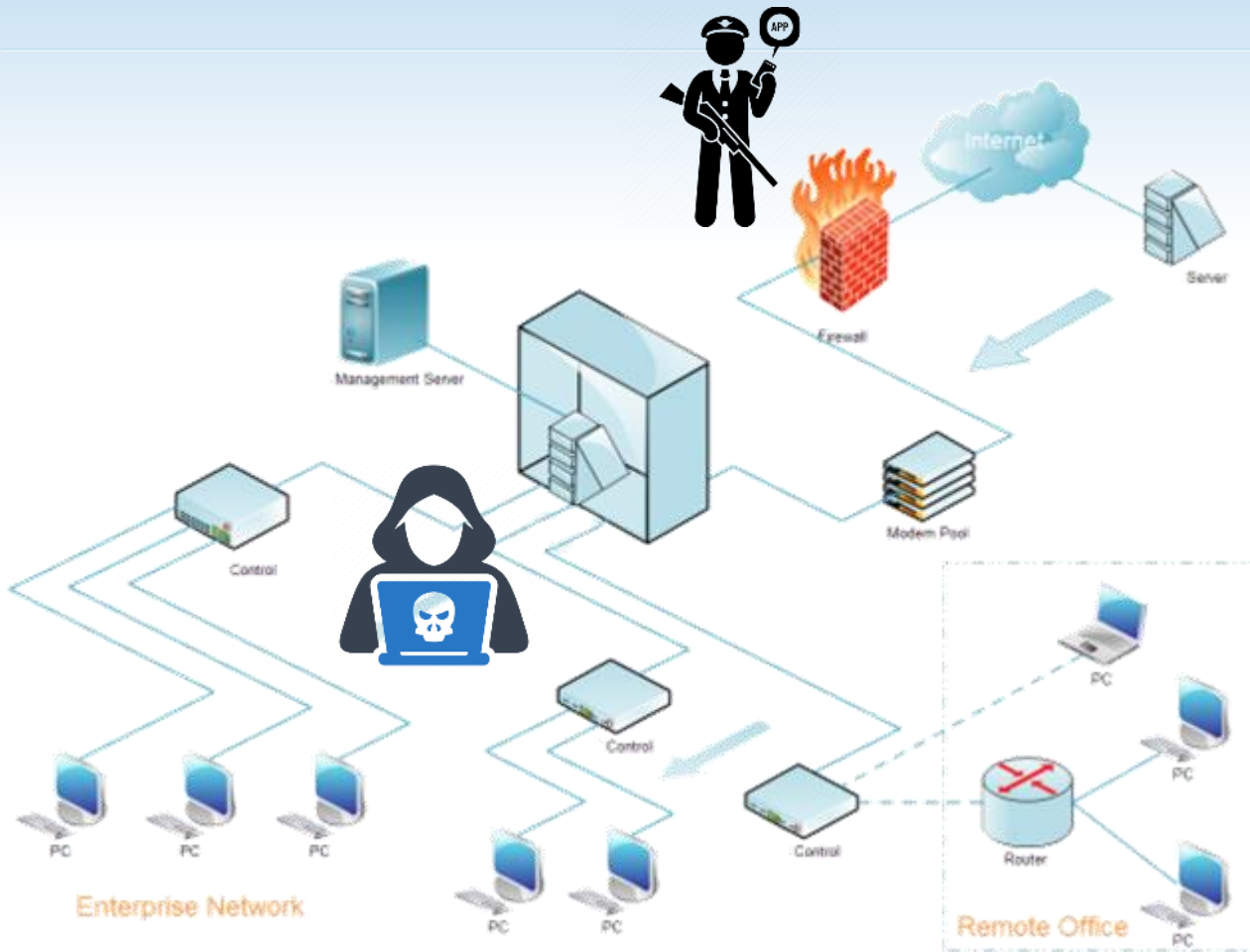
Topologie a infrastruktura SoHo síť jako základ ???

Včera / zítra:

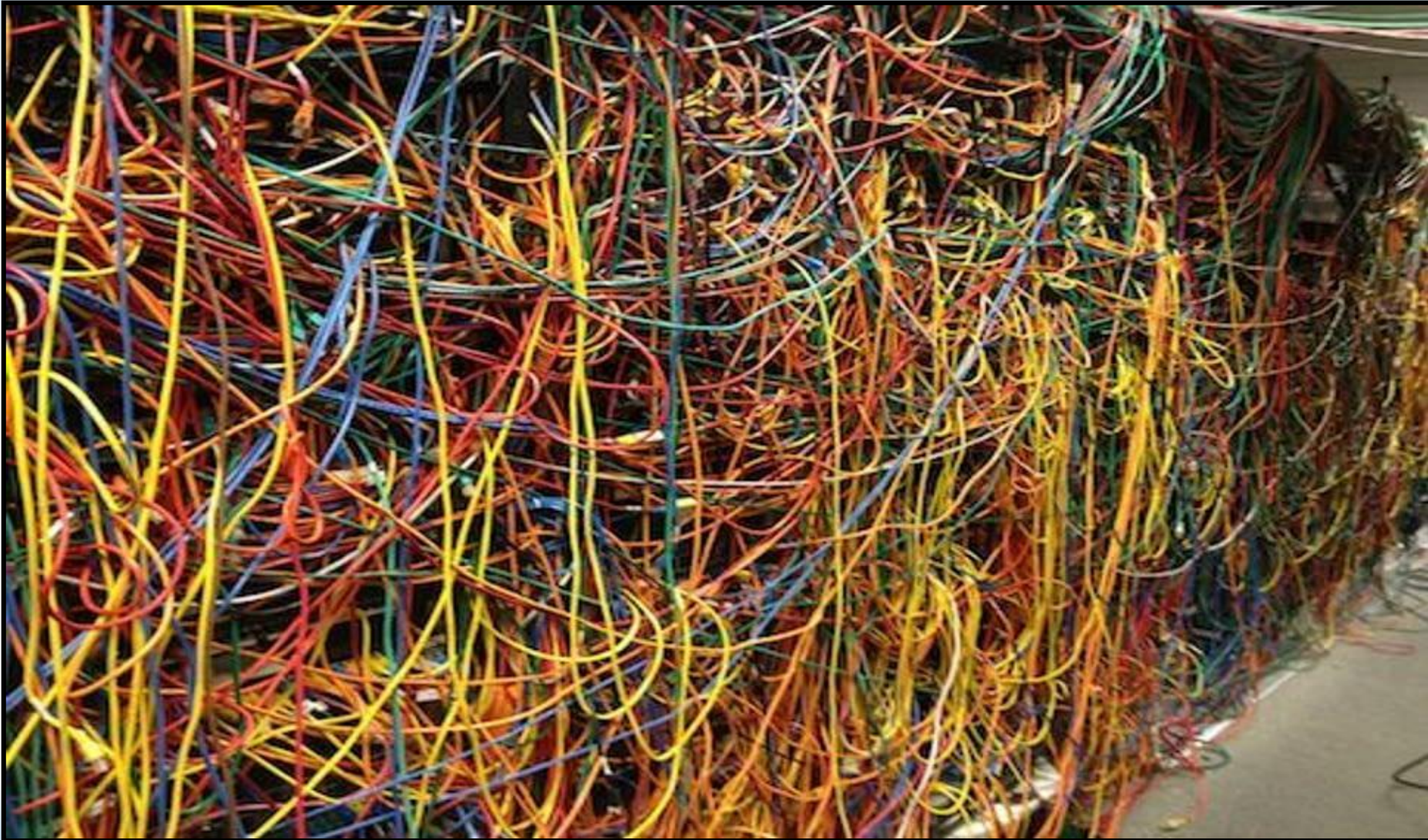
- rychlá rozhraní 2,5/10GbE
- optika WAN/LAN
- PoE pro CCTV, WiFi, VoIP
- VLAN (bezpečnost pro práci)
- multi AP (MESH)
- infrastruktura pro IoT(!)



Topologie v segmentech SMB a Ent



Špagety patří na talíř...



Ethernet

Ethernet je v informatice technologie, která se používá pro budování lokálních sítí (LAN).

V referenčním modelu ISO/OSI realizuje fyzickou a spojovou vrstvu, v modelu TCP/IP pak vrstvu síťového rozhraní. V lokálních sítích se Ethernet prosadil v 80 % všech instalací. Jeho popularita spočívá v jednoduchosti protokolu a tím i snadné implementaci i instalaci.

Původní protokol s přenosovou rychlostí 10 Mbit/s byl vyvinut firmami DEC, Intel a Xerox pro potřeby kancelářských aplikací. Později byl v poněkud pozměněné podobě normalizován institutem IEEE jako norma **IEEE 802.3**.

Tato norma byla převzata ISO jako **ISO 8802-3**. Autoři původního Ethernetu vytvořili upravenou verzi **Ethernet II** (tzv. průmyslový standard), která změnila některé časové konstanty s cílem dosáhnout vyšší kompatibility se standardem 802.3. Mezi oběma specifikacemi však zůstal rozdíl ve formátu rámce.

Ethernet - princip

Klasický Ethernet používal sběrniceovou topologii – tedy sdílené médium, kde všichni slyší všechno a v každém okamžiku může vysílat jen jeden. Jednotlivé stanice jsou na něm identifikovány svými hardwarovými adresami (MAC adresa). Když stanice obdrží paket s jinou než vlastní adresou, zahodí jej.

Karty lze ovšem přepnout do promiskuitního režimu, kdy přijímají všechny pakety, tato možnost se využívá např. při monitorování sítě.

Pro přístup ke sdílenému přenosovému médiu (sběrnici) se používá metoda CSMA/CD~CA (Carrier Sense with Multiple Access and Collision Detection~Avoidance), česky metoda mnohonásobného přístupu s nasloucháním nosné a detekcí kolizí.

- Stanice (síťová karta), která potřebuje vysílat, naslouchá co se děje na přenosovém médiu.
- Pokud je v klidu, začne stanice vysílat.
- Může se stát (v důsledku zpoždění signálu), že dvě stanice začnou vysílat přibližně ve stejný okamžik. Jejich signály se pochopitelně navzájem zkomolí. Tato situace se nazývá kolize a vysílající stanice ji poznají podle toho, že během svého vysílání zároveň zjistí příchod cizího signálu.
- Stanice, která detekuje kolizi, vyšle krátký signál (o 32 bitech).
- Poté se všechny vysílající stanice odmlčí a později se pokusí o nové vysílání.

Ethernet - princip

Mezi opakovanými pokusy o vysílání stanice počká vždy náhodnou dobu. Interval, ze kterého se čekací doba náhodně vybírá, se během prvních deseti pokusů vždy zdvojnásobuje. Stanice tak při opakovaných neúspěších „řadí“ své pokusy o vysílání a zvyšuje tak pravděpodobnost, že se o sdílené médium úspěšně podělí s ostatními. Pokud se během šestnácti pokusů nepodaří rámec odvysílat, stanice své snažení ukončí a ohlásí nadřazené vrstvě neúspěch.

Ke kolizi může dojít jen v době, která uplyne od začátku vysílání do okamžiku, kdy signál vysílaný stanicí obsadí celé médium (pak již případní další zájemci o vysílání zjistí, že médium není volné a počkají na jeho uvolnění). Tento interval se nazývá kolizní okénko a musí být kratší, než je doba vysílání nejkratšího rámce.

Tato metoda přístupu k médiu je velmi efektivní při nižším zatížení sítě (cca 30 % šířky pásma). Její efektivita klesá při větším počtu zájemců o vysílání.

Jednotlivé varianty protokolu se značí např. 10Base5, 100Base-TX a podobně. První číslice určuje maximální přenosovou rychlost v megabitech za sekundu. Následuje označení pásma (všechny verze Ethernetu pracují v základním pásmu, proto zde vždy obsahují „Base“) a určení druhu přenosového média.

OSI síťový model

Paralela mezi OSI standardem a dopisovou komunikací mezi manažery dvou firem. Každý prvek (s výjimkou fyzické vrstvy) má přímý kontakt (pomocí určitého rozhraní) pouze s prvky v sousedních vrstvách. Rozhraním se myslí např. poštovní schránka mezi 4. a 3. vrstvou nebo přihrádka mezi 3. a 2. vrstvou. Každý prvek na straně odesílatele zpracuje zprávu do takového tvaru (dle daného protokolu), aby jí rozuměl jeho ekvivalent na straně příjemce.

Protokol např. udává, jak má být správně nadepsaná adresa 5. vrstvou, nebo jak správně ve 2. vrstvě seskupit více dopisů jdoucích stejným směrem.

Vrstvový model

Každá ze sedmi vrstev vykonává skupinu jasně definovaných funkcí potřebných pro komunikaci. Pro svou činnost využívá služeb své sousední nižší vrstvy. Své služby pak poskytuje sousední vyšší vrstvě. Podle referenčního modelu není dovoleno vynechávat vrstvy, ale některá vrstva nemusí být aktivní. Takové vrstvě se říká nulová nebo transparentní.

Komunikaci mezi systémy tvoří:

- komunikace mezi vrstvami jednoho systému, řídí se pravidly, které se obvykle nazývají rozhraní (interface)
- komunikace mezi stejnými vrstvami různých systémů, řídí se protokoly

OSI síťový model

a) Na počátku vznikne požadavek některého procesu v aplikační vrstvě.

b) Příslušný podsystém požádá o vytvoření spojení prezentační vrstvou. V rámci aplikační vrstvy je komunikace s protějším systémem řízena aplikačním protokolem. Podsystémy v prezentační vrstvě se dorozumívají prezentačním protokolem.

c) Takto se postupuje stále níže až k fyzické vrstvě, kde se použije pro spojení přenosové prostředí.

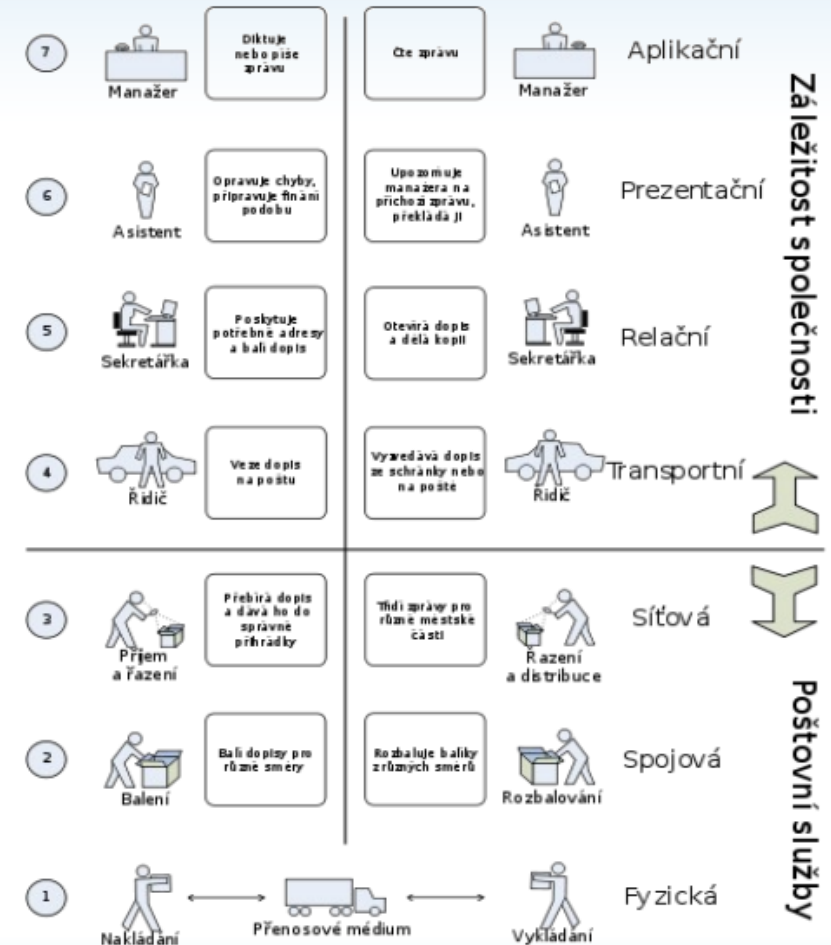
d) Současně se při přechodu z vyšší vrstvy k nižší přidávají k uživatelským (aplikačním) datům záhlaví jednotlivých vrstev.

Tak dochází k postupnému zapouzdřování původní informace. U příjemce se postupně zpracovávají řídicí informace jednotlivých vrstev a vykonávají jejich funkce.

Mnemotechnická pomůcka pro zapamatování:

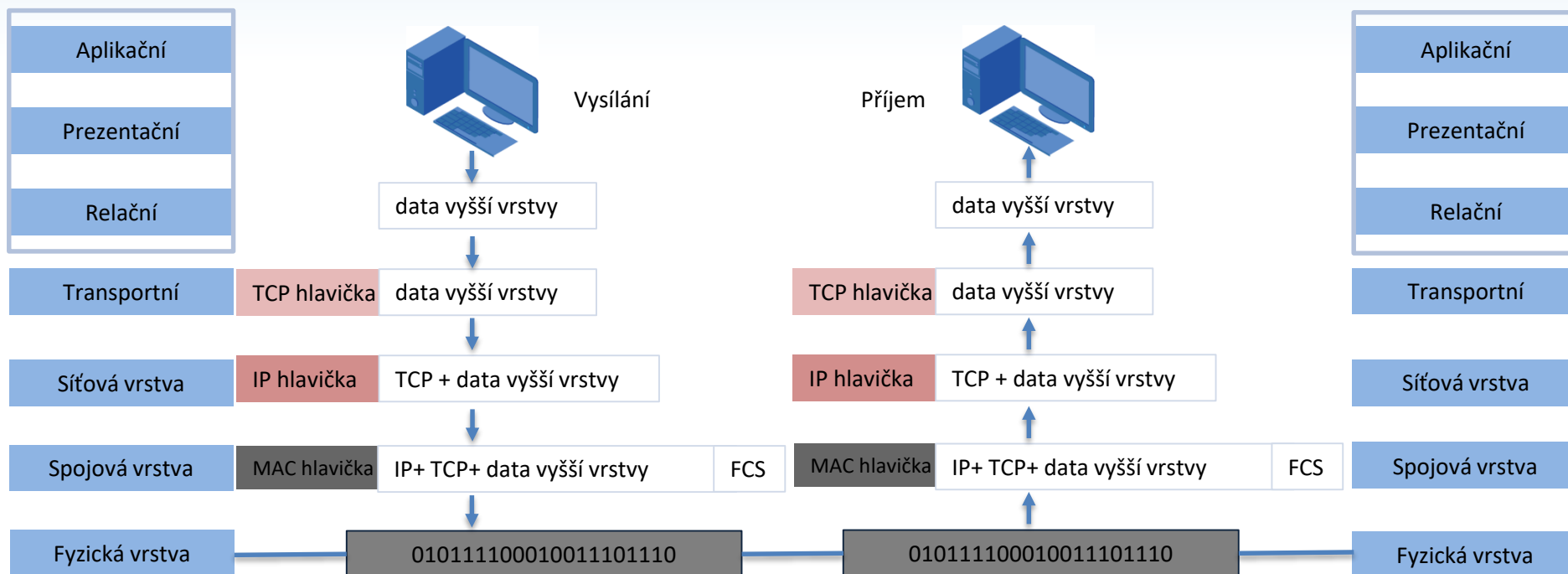
Aplikace potkala prezentaci, zrealizovaly transport sítí, spojily se fyzicky.

OSI / ISO síťový model



Paralela mezi RM - OSI a dopisy

OSI/ISO model



OSI síťový model

Layer	Type	Data unit	Layer Name	Function	Misc. examples	TCP/IP suite	SS7	OSI suite	IPX suite
7	Host layers		Application	Network process to application	NNTP, HL7, Modbus, SIP, SSI	DHCP, FTP, Gopher, HTTP, NFS, NTP, RTP, SMPP, SMTP, SNMP, Telnet	ISUP, INAP, MAP, TUP, TCAP	FTAM, X.400, X.500, DAP	
6		Data	Presentation	Data representation and encryption	TDI, ASCII, EBCDIC, MIDI, MPEG	MIME, XDR, SSL, TLS (Not a separate layer)		ISO 8823, X.226	
5			Session	Interhost communication	Named Pipes, NetBIOS, SAP, SDP	Sockets. Session establishment in TCP. SIP. (Not a separate layer with standardized API.), DNS		ISO 8327, X.225	NWLink
4	Media layers	Segments	Transport	End-to-end connections and reliability (TCP)	NBF, nanoTCP, nanoUDPTCP, UDP, SCTP		SCCP	TP0, TP1, TP2, TP3, TP4	SPX
3		Packets	Network	Path determination and logical addressing (IP)	NBF, Q.931	IP, ICMP, IPsec, ARP, RIP, OSPF	MTP-3	X.25 (PLP), CLNP	IPX
2		Frames	Data Link	Physical addressing (MAC & LLC)	802.3 (Ethernet), 802.11a/b/g/n MAC/LLC, 802.1Q (VLAN), ATM, CDP, HDP, FDDI, Fibre Channel, Frame Relay, HDLC, ISL, PPP, Q.921, Token ring	PPP, SLIP, PPTP, L2TP	MTP-2	X.25 (LAPB), Token Bus	IEEE 802.3 framing, Ethernet II framing
1		Bits	Physical	Media, signal and binary transmission	RS-232, V.35, V.34, I.430, I.431, T1, E1, 10BASE-T, 100BASE-TX, POTS, SONET, DSL, 802.11a/b/g/n PHY		MTP-1	X.25 (X.21bis, EIA/TIA-232, EIA/TIA-449, EIA-530, G.703)	

Fyzická vrstva – L1

Vrstva č. 1, anglicky physical layer. Specifikuje fyzickou komunikaci.

Aktivuje, udržuje a deaktivuje fyzické spoje (např. komutovaný spoj) mezi koncovými systémy. Fyzické spojení může být dvoubodové (sériová linka) nebo mnohobodové (Ethernet).

Fyzická vrstva definuje všechny elektrické a fyzikální vlastnosti zařízení. Obsahuje rozložení pinů, napěťové úrovně a specifikuje vlastnosti kabelů; stanovuje způsob přenosu "jedniček a nul". Huby, opakovače, síťové adaptéry a hostitelské adaptéry (Host Bus Adapters používané v síťových úložištích SAN) jsou právě zařízení pracující na této vrstvě.

Hlavní funkce poskytované fyzickou vrstvou jsou:

- Navazování a ukončování spojení s komunikačním médiem.
- Spolupráce na efektivním rozložení všech zdrojů mezi všechny uživatele.
- Modulace neboli konverze digitálních dat na signály používané přenosovým médiem (a zpět) (A/D, D/A převodníky).

Přenosová média – L1

Koaxiální kabel

Původní Ethernet byl propojován tzv. tlustým koaxiálním kabelem a označoval se jako 10Base5. Jeden segment mohl být dlouhý až 500 metrů. Na kabel byly napichovány transceivery, které se připojovaly na AUI port síťové karty.

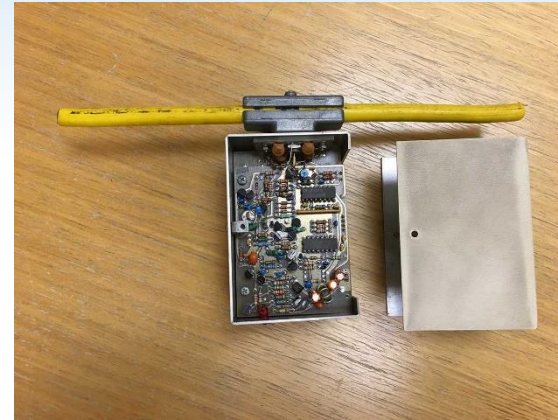
K masovému používání Ethernetu došlo se zavedením tzv. tenkého koaxiálního kabelu. Tato varianta se označuje jako 10Base2. Propojovací kabely se zakončují BNC konektory, mezi ně se vkládají odbočky ke stanicím BNC-T konektory. Ty se připojují přímo na síťovou kartu, nebo adaptérem na AUI port. Délka segmentu je maximálně 185 metrů, ve speciálních případech až 300 - 400 metrů.

Kroucený pár

Kroucený pár je dnes zdaleka nejrozšířenější druh Ethernetové kabeláže. Její použití pro Ethernet pod označení 10BaseT definuje specifikace IEEE 802.3i. Topologie sítě se změnila ze sběrnice na hvězdicovou, v jejímž středu je rozbočovač (hub) a na koncích jednotlivých spojů připojené počítače. Chování sítě napodobuje sběrnici - rozbočovač kopíruje signál přicházející z jednoho rozhraní do všech ostatních. Data vysílaná jednou stanicí jsou proto rozšířena všem ostatním, stejně jako v případě jejich přenosu po sdílené sběrnici.

Přenosová média – L1

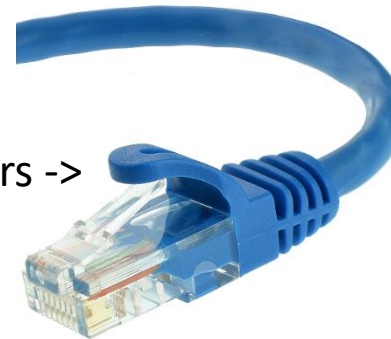
Thick ->



Thin ->



Twisted pairs ->



Přenosová média – L1

Optické vlákno

Ethernet je definován i pro optické vlákno. Používají se jednovidová i mnohovidová vlákna v závislosti na požadované rychlosti a vzdálenosti. Vybudování optické trasy je dražší, než strukturovaná kabeláž, ale umožňuje přenos na vyšší vzdálenosti. Další výhodou je, že spojení je odolné proti elektromagnetickému rušení a koncové body spoje jsou galvanicky oddělené. Je tedy vhodné pro budování LAN sítí mezi budovami a vzdálenými lokalitami. V těchto případech jsou metalické spoje nepoužitelné vzhledem k problémům se statickou elektřinou, nebo s různým nulovým potenciálem rozvaděčů budov.

Ostatní média

Ethernet lze konvertovat nebo zapouzdřit pro přenos širokou škálou fyzických prostředků. Příkladem jsou WiFi (radiokomunikace), PLC (Powerline), xDSL (telefonní dvoulinka), LTE/5G-NR (mobilní komunikace), přímé optické spojení (LiFi, laserové spoje) atd.

Každé médium je svým způsobem specifické, pro přenos se musí signály upravit = nespočet rozhraní, standardů, protokolů (bohužel ☹ i licenční politika).

Typy ethernetu – L1

- Ethernet - původní varianta s přenosovou rychlostí 10 Mbit/s. Definována pro koaxiální kabel, kroucenou dvojlinku a optické vlákno.
- Fast Ethernet - rychlejší verze s přenosovou rychlostí 100 Mbit/s definovaná standardem IEEE 802.3u. Převzala maximum prvků z původního Ethernetu (formát rámce, algoritmus CSMA/CD apod.), aby se usnadnil, urychlil a zlevnil vývoj. V současnosti ji lze považovat za základní verzi Ethernetu. Je k dispozici pro kroucenou dvojlinku a optická vlákna.
- Gigabitový Ethernet - zvýšil přenosovou rychlost na 1 Gbit/s. Opět recykloval co nejvíce prvků z původního Ethernetu, teoreticky i algoritmus CSMA/CD. V praxi je ale gigabitový Ethernet provozován pouze přepínaně s plným duplexem. Důležité je především použití stejného formátu rámce. Původně byl definován pouze pro optická vlákna (IEEE 802.3z), později byla doplněna i varianta pro kroucenou dvojlinku (IEEE 802.3ab).
- Desetigigabitový Ethernet - jeho definice byla jako IEEE 802.3ae přijata v roce 2003. Přenosová rychlost činí 10 Gbit/s, jako médium zatím slouží hlavně optická vlákna a opět používá stejný formát rámce. Algoritmus CSMA/CD byl definitivně opuštěn, tato verze pracuje vždy plně duplexně. V současnosti byla vyvinuta jeho specifikace pro kroucenou dvojlinku s označení IEEE 802.3an.

Typy ethernetu – L1

- 10Base5 - původní Ethernet na koaxiálním kabelu o rychlosti 10 Mbit/s. Koaxiální kabel o impedanci 50Ω tvoří sběrnici, ke které se připojují pomocí speciálních tranceiverů a AUI kabelů jednotlivé stanice.
- 10Base2 - Ethernet na tenkém koaxiálním kabelu o rychlosti 10 Mbit/s. Koaxiální kabel tvoří sběrnici, ke které se připojují jednotlivé stanice přímo. Kabel je impedance 50Ω (RG-58) nesmí mít žádné odbočky a je na koncích zakončen odpory 50Ω (tzv. terminátory).
- 10Base-T - jako přenosové médium používá kroucenou dvojlínku s rychlostí 10 Mbit/s. Využívá dva páry strukturované kabeláže ze čtyř. Dnes již překonaná síť, která byla ve většině případů nahrazena rychlejší 100 Mbit/s variantou.
- 10Base-F –v arianta s optickými vlákny o rychlosti 10 Mbit/s. Používá se pro spojení na větší vzdálenost, nebo spojení mezi objekty, kde nelze použít kroucenou dvojlínku. Tvořila obvykle tzv. páteřní síť, která propojuje jednotlivé menší celky sítě. Dnes je již nahrazována vyššími rychlostmi (Fast Ethernet, Gigabit Ethernet).
- 100Base-TX - varianta s přenosovou rychlostí 100 Mbit/s, které se říká Fast Ethernet, používá dva páry UTP nebo STP kabelu kategorie 5.
- 100Base-T2 - používá dva páry UTP kategorie 3, 4, 5. Vhodné pro starší strukturovanou kabeláž.
- 100Base-T4 - používá čtyři páry UTP kategorie 3, 4, 5. Vhodné pro starší strukturovanou kabeláž.
- 100Base-FX Fast Ethernet. Používající se dvě optická vlákna.

Typy ethernetu – L1

- 1000Base-T Ethernet s rychlostí 1000 Mb/s, nazývaný Gigabit Ethernet. Využívá 4 páry UTP kabeláže kategorie 5e, je definován do vzdálenosti 100 metrů.
- 1000Base-CX Gigabit Ethernet na bázi měděného vodiče pro krátké vzdálenosti.
- 1000Base-SX Gigabit Ethernet používající mnohavidové optické vlákno. Určený pro páteřní sítě do vzdáleností několik set metrů.
- 1000Base-LX Gigabit Ethernet používající jednovidové optické vlákno. Je určen pro větší vzdálenosti až několika desítek kilometrů.
- 2,5/5GBase-T rozhraní mladší jak 10Gbase-T a vyvinuté jako ekonomické řešení
- 10GBase-T - Ethernet s rychlostí 10 Gb/s, nazývaný Ten Gigabit Ethernet. Do vzdálenosti 55 metrů lze využít kabeláž kategorie 6. Pro využití plné délky 100 je nutné použít kategorii 6a (augmented Category 6 – šířka pásma 500 MHz).
- 40GBASE a 100GBASE optika s rychlostí 40 a 100 Gb/s, je možné používat optická vlákna s paralelním MPO (ekonomicky výhodné moduly).

Spojová vrstva - L2

Vrstva č. 2, anglicky data link layer. Poskytuje spojení mezi dvěma sousedními systémy.

Uspořádává data z fyzické vrstvy do logických celků známých jako **rámce (frames)**.

Seřazuje přenášené rámce, stará se o nastavení parametrů přenosu linky, oznamuje neopravitelné chyby. Formátuje fyzické rámce, opatřuje je fyzickou adresou a poskytuje synchronizaci pro fyzickou vrstvu.

Na této vrstvě pracují veškeré **přepínače**. Poskytuje propojení pouze mezi místně připojenými zařízeními a tak vytváří doménu na druhé vrstvě pro směrové a všesměrové vysílání.

Spojová vrstva - L2

Formát rámce se popisuje pomocí oktetů (osmice bitů). Důvodem je přesnost definice, protože některé počítače mohou pracovat s jinou základní délkou bajtu (např. 4 nebo 10 bitů). Níže uvedená tabulka popisuje rámec Ethernet II a 802.3, které se liší využitím jednoho pole pro typ nebo pro délku (vysvětlení je pod tabulkou).

Ethernetový rámec							
Preamble	SFD	MAC cíle	MAC zdroje	Typ/délka	Data a výplň	CRC32	Mezera mezi rámci
7× oktet 10101010	1× oktet 10101011	6 oktetů	6 oktetů	2 oktety	46-1500 oktetů	4 oktety	12 oktetů
				64-1518 oktetů			
72-1526 oktetů							

- Preamble – 7 oktetů, střídavě binární 0 a 1; slouží k synchronizaci hodin příjemce
- SFD – označení začátku rámce (Start of Frame delimiter), oktet 10101011
- MAC cíle – MAC adresa cílového síťového rozhraní o délce 48 bitů; sdresa může být individuální (unicast), skupinová (multicast) a všeobecná (broadcast)
- MAC zdroje – MAC adresa zdrojového síťového rozhraní
- Typ/délka - pro Ethernet II je to pole určující typ vyššího protokolu; pro IEEE 802.3 udává délku pole dat
- Data – pole dlouhé minimálně 46 a maximálně 1500 oktetů (46—1500 B); minimální délka je nutná pro správnou detekci kolizí v rámci segmentu
- Výplň – vyplní zbytek datové části rámce, pokud je přepravovaných dat méně než 46 B
- CRC32 – kontrolní součet (Frame Check Sequence, FCS) 32bitový kontrolní kód, který se počítá ze všech polí s výjimkou preamble a FCS; slouží ke kontrole správnosti dat – příjemce si jej vypočítá z obdrženého rámce a pokud výsledek nesouhlasí s hodnotou pole, rámec zahodí jako vadný

Přepínač pro ethernet - L2

Switch (česky **přepínač**) je aktivní síťový prvek, propojující jednotlivé segmenty sítě. Obsahuje větší či menší množství portů (až několik stovek), na něž se připojují síťová zařízení nebo části sítě. Pojem switch se používá pro různá zařízení v celé řadě síťových technologií.

Nejčastěji switch potkáte jako aktivní prvek v síti Ethernet realizované kroucenou dvojlinkou. Zde nahradil dříve používané huby (rozbočovače), které signál jednoduše kopírovaly do všech ostatních rozhraní. Pracuje zde na 2. vrstvě OSI modelu. Vedle vyššího výkonu (stanice připojené k různým rozhraním switche navzájem nesoutěží o médium) znamená přínos i pro bezpečnost sítě, protože médium již není sdíleno a data se vysílají jen do rozhraní, jímž je připojen jejich adresát.

„Kdo je kde“ se switche učí automaticky z procházejícího provozu, konkrétně z adres odesílatelů uvedených v rámcích, které do switche přicházejí. Používá se algoritmus Backward Learning Algorithm.

-----> Z těchto údajů si switch automaticky plní tabulku identifikující cílová rozhraní pro jednotlivé adresy. Pokud switch dostane k doručení rámeček směřující na jemu dosud neznámou adresu, chová se jako hub a rozešle rámeček do všech ostatních rozhraní. Lze očekávat, že oslovená stanice pravděpodobně odpoví a switch se tak vzápětí dozví, kde se nachází.

Přepínač pro ethernet - L2

Způsoby přeposílání rámců:

- **store and forward** - rámec z jednoho rozhraní přijmou, uloží si do vyrovnávací paměti, prozkoumají jeho hlavičky (zkontrolují FCS) a následně odvysílají do příslušného rozhraní.
- **cut through** - současné switche tento proces často optimalizují, takže k analýze hlaviček dochází jakmile dorazí začátek rámce. Ani s vysíláním do cílového rozhraní se nečeká, až dorazí celý rámec, ale zahajuje se co nejrychleji, aby zpoždění rámců bylo minimální.
- **fragment free** - switch začne přeposílat rámec až po přijetí 64byťů, kdy se ujistí, že na daném segmentu nevznikla kolize.

Switche dnes často nabízejí pokročilejší funkce díky pokročilému dekódování rámců!

- ✓ správa WEB/SNMP, VLAN, STP, QoS, shaper, routing L3, analýza L4....
- ✓ vazba analýzy provozu zařízení na vyšší vrstvy OSI

Vlastnosti switchů kterých lze zneužít:

- ✓ viz. seriál „Odposloucháváme data na přepínaném Ethernetu“ na Lupa.cz:
<http://www.lupa.cz/serialy/odposlouchavame-data-na-prepinanem-ethernetu/>

Přepínač pro ethernet – L2

Stack – stoh – hromada

Metody sjednocení správy přepínačů pod jedno uživatelské rozhraní a jejich redundance:

- **HW stack** – řízené čipsetem
- **IP stack** – pro účely jednotné správy
- **VSF stack** – virtuální cluster
- **Bus stack** – speciální propojení sběrnic (karta, proprietární)

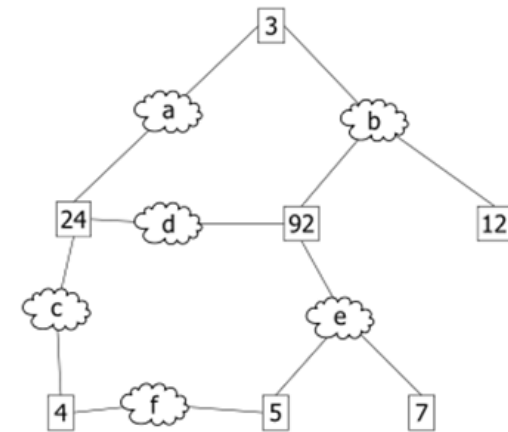
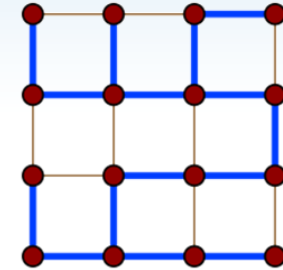
Základní parametry pro stohování:

- ID switche
- Master jednotka
- Redundance
- Nalezení nejkratší cesty



Spanning tree protocol (L2)

- IEEE 802.1D (802.1t-2001)
- převzatý matematický model pole znázorněný v bezrozměrném grafu
- protokol operující na linkové vrstvě pro účely pro účely budování zálohy spojení
- řídí provoz mezi uzly s ID- uživatelsky definováno, při rovnováze rozhoduje MAC
- „Root bridge“ je uzel s nejnižším ID
- dílčí spoje mají různou váhu-hodnotu spojení (link cost)
- zařízení díky protokolu výměnou BPDUs (bridge protocol data units) volí nejrychlejší cestu
- stavy portů: blocking, listening, learning, forwarding, disabled



RSTP / MSTP (L2)

Rapid Spanning tree protocol (RSTP)

- evoluce popsaná v IEEE 802.1w-1998, společně se STP v IEEE 802.1D-2004
- pokročilejší algoritmus logiky vycházející z definic stavů portů zaručuje zkrácení odezvy na zjištění cesty v topologii stromu z 30-50s na 6 sekund
- stavy portů: root, designated, alternate, backup, disabled

Multiple Spanning Tree Protocol (MSTP)

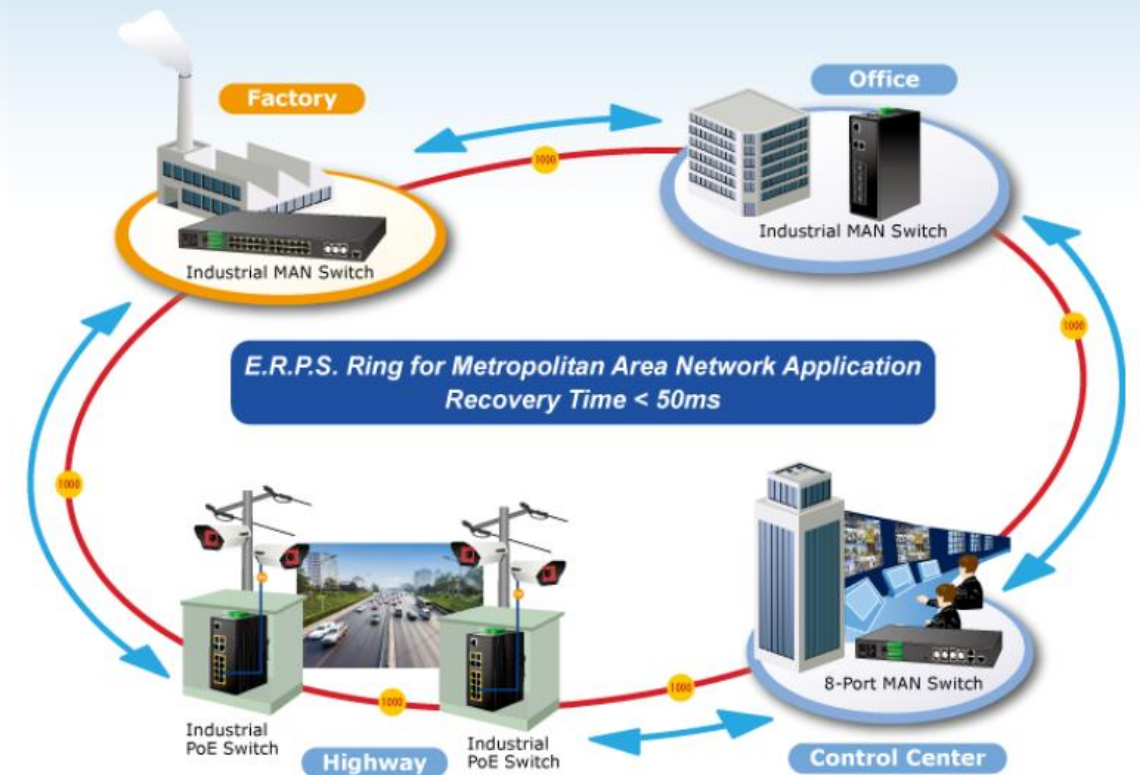
- IEEE 802.1s (IEEE 802.1Q-2003)
- obecně rozšiřuje působnost nad VLAN sítěmi
- několik implementací (Cisco: Rapid Per-VLAN Spanning Tree (R-PVST))

ERPS ring (L2)

- řešení pro rychlou redundanci a ochranu proti vzniku smyčky
- standardizováno ITU-T G.8032/Y.1344
- garance přepnutí do 50ms (řada modelů do 20ms a 10ms)
- implementace pro fyzické spoje
- především průmyslové switche

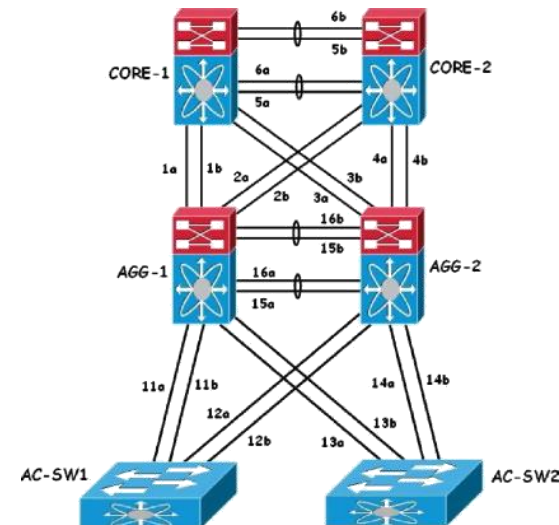
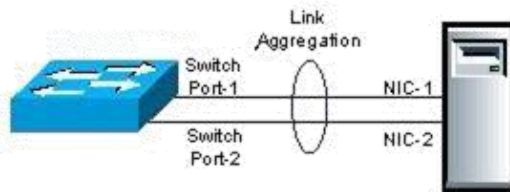
Srovnání s RSTP (Rapid Spanning Tree Protocol):

- nevýhoda je doba zotavení 2~10s
- jelikož místo rozpojení je určováno „cenou cesty“ nemusí být zřejmé kde k němu dojde (hlavně když jsou nastaveny všude stejně)



LACP – Link aggregation control protocol

- agregace linek na základě definice v IEEE 802.3ad, obecný popis v IEEE 802.1AX
- užití modulů WDM/CWDM/DWDM versus 10GBase-X ?
- v situaci agregace dvou linek není zátěž 50:50
- pro NIC není ve Windows nativně podporováno; dnes se řeší „teaming“ funkcí v rámci VM
- využití protokolu pro záložní infrastrukturu



VLAN (L2)

Virtuální LAN slouží k logickému rozdělení sítě nezávisle na fyzickém uspořádání.

Můžeme segmentovat na menší sítě uvnitř fyzické struktury původní sítě.

Dělení sítě už na úrovni 2. vrstvy ISO/OSI, v porovnání s podsítěmi na 3. vrstvě.

Výhody VLAN:

- snížení broadcastů - hlavní výhodou VLAN je vytvoření více, ale menších, broadcastových domén. Tedy zlepšení výkonu sítě snížením provozu (traffic).
- zjednodušená správa - k přesunu zařízení do jiné sítě stačí překonfigurovat zařazení do VLANy, tedy správce konfiguruje SW (zařazení do VLAN) a ne HW (fyzické přepojení)
- zvýšení zabezpečení - oddělení komunikace do speciální VLANy, kam není jiný přístup. Toho se dá samozřejmě dosáhnout použitím samostatných switchů, ale často se toto uvádí jako bonus VLAN.
- oddělení speciálního provozu - dnes se používá řada provozů, který nemusí být propojeny do celé sítě; například IP telefonie, komunikace mezi AP v centrálně řízeném prostředí, management (zabezpečení správcovského přístupu k zařízením).
- snížení HW - nesnižuje potřebný počet portů ale tím, že mohou být různé podsítě na stejném prepínači, jej můžeme lépe využít.

VLAN (L2)

- Standard IEEE 802.1Q, využívá značkování rámců, díky tomu je obsažena informace o přiřazení do VLAN v každém rámci.
- Přes jeden VLAN trunk port může díky tomu projít více VLAN.
- Vezmeme originální rámec, jeho hlavičku rozšíříme o 4B informaci, z nichž první je značka, že se jedná o protokol 802.1Q (hodnota 0x8100). Dále následuje priorita dle protokolu 802.1p, příznak, zda je MAC adresa v kanonickém tvaru a poslední je číslo VLANy.

Originální rámec

6B	6B	2B	64 až 1500B	4B
cílová adresa (DA)	zdrojová adresa (SA)	typ nebo délka	data	kontrolní součet (FCS)

Upravený rámec pomocí 802.1q

6B	6B	4B	2B	64 až 1500B	4B
cílová adresa (DA)	zdrojová adresa (SA)	802.1q tag	typ nebo délka	data	kontrolní součet (FCS)

Tvar 802.1q tagu

2B	3b	1b	12b
0x8100	priorita (802.1p)	Canonical Format Indicator (CFI)	VLAN ID
Tag Protocol ID (TPID) 2B	Tag Control Information (TCI) 2B		

Síťová vrstva – L3

Vrstva č. 3, anglicky network layer. Tato vrstva se stará o směrování v síti a síťové adresování. Poskytuje spojení mezi systémy, které spolu přímo nesousedí. Obsahuje funkce, které umožňují překlenout rozdílné vlastnosti technologií v přenosových sítích. Jednotkou informace je **paket**.

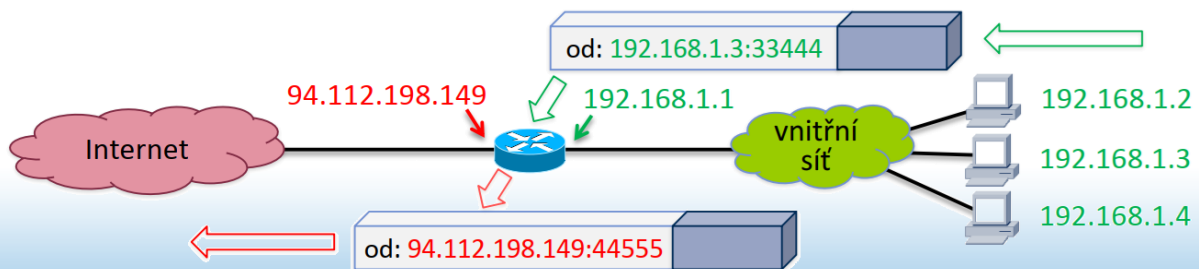
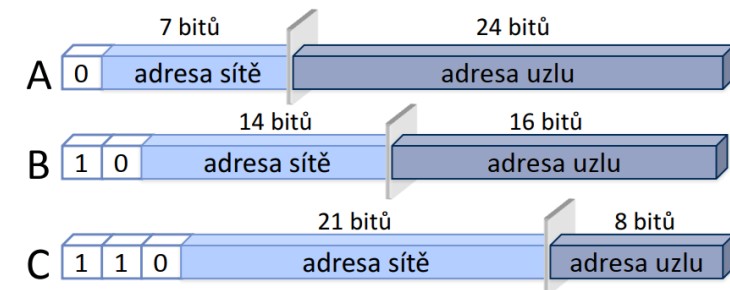
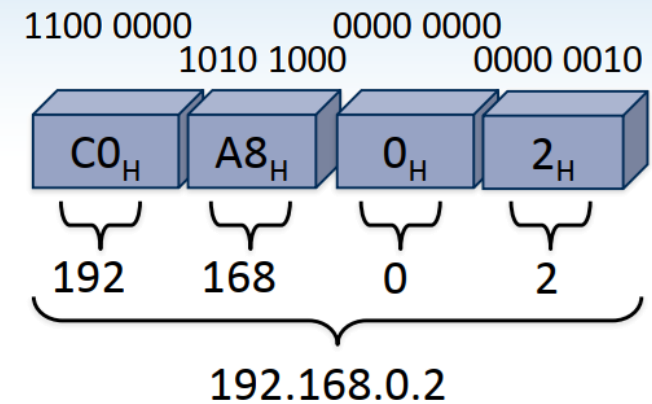
Síťová vrstva poskytuje funkce k zajištění přenosu dat různé délky od zdroje k příjemci skrze jednu případně několik vzájemně propojených sítí při zachování kvality služby, kterou požaduje přenosová vrstva.

Síťová vrstva poskytuje směrovací funkce a také reportuje o problémech při doručování dat. Veškeré směrovače pracují na této vrstvě a posílají data do jiných sítí. Zde se již pracuje s hierarchickou strukturou adres.

Nejznámější protokol pracující na 3. vrstvě je Internetový Protokol (IP), dalšími jsou ICMP a ARP...

IPv4 síťový protokol – L3

- spravovala organizace IANA (Internet Assigned Numbers Authority) dnes RIR (Regional Internet Registry) a 5 podorganizací, v Evropě = RIPE (Reseaux IP Europeens)
- hierarchie přidělovatelů: IANA – RIR (RIPE kontinentální) – NIR (národní) – LIR (lokální ISP)
- kombinace 4 x 8 (oktet) = 32bitů
- IP adresy jsou abstraktní, nemají přímou vazbu na HW adresy, proto jsou nutné možnosti překladu – ARP, tabulka, výpočet
- třídy A, B, C, D, E
- některé adresy mají speciální význam: broadcast, multicast, loopback, atd.
- úspora IP adres v internetu
 - subnetting: rozdělení vnitřních sítí do bloků pomocí **síťové masky** (subsítě 192.168.0.1 + 192.168.0.128 s maskami 255.255.255.128)
 - supernetting: spojení „agregace“ několika bloků do jednoho; pozor!
 - CIDR (Classless Inter-Domain Routing): spojením zmíněných v interních sítích, používá se prefix (192.168.0.1/24)
 - NAT (Network Address Translation): překlad adres sdílením společné veřejné IP, částečná „ochrana“ díky nedostupnosti(!) na síťové vrstvě přepisuje hlavičky datagramů, bohužel i těla datagramů kvůli pseudo hlavičkám UDP/TCP -> dopad na výkon
 - NAPT (Network Address and Port Translation): dynamický překlad adres i portů



IPv4 síťový protokol – L3

Subnetting

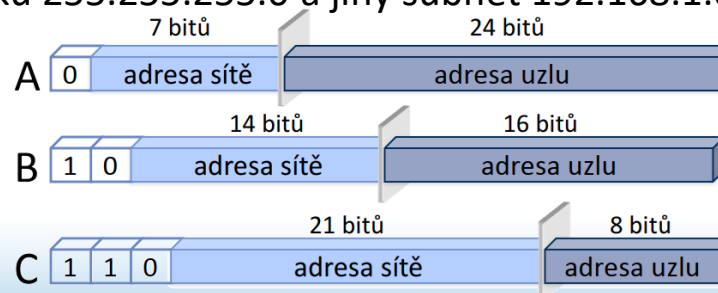
- segmentace IP sítí na menší bloky
- praktické využití v Internetu (pro WAN nezbytnost)
- v LAN to není nutné, adres je dostatek (nebo ne??)
- děje se tak na L3 aktivním prvku jako router nebo L3 switch (nejde o NAT!)
- často ve spojení s VLAN, ale pozor jestli ne! (dva IP subnety v jedné VLAN neoddělují provoz)
- ale dva IP subnety každý ve své VLAN jsou oddělené, switch vám jinou VLAN do portu nepošle
- váš router multisubnet segmentaci neumí? nahraďte ho třeba rychlým L3 switchem
- použijte IP subnet calculator (web, aplikace i mobilní, s tabulkou to zvládnete taky)

Příklad:

- ✓ jednu síť LAN 192.168.0.1/24 rozdělím na dvě 192.168.0.1/25 a 192.168.0.128/25
- ✓ nebo na čtyři: 192.168.0.1/26 + 192.168.0.64/26 + 192.168.0.128/26 + 192.168.0.192/26
- ✓ ale proč bych to dělal, když můžu použít **obvyklou** C masku 255.255.255.0 a jiný subnet 192.168.1.0

Supernetting

- agregace do větších bloků
- nevýhodné z provozních i bezpečnostních důvodů



Prefix	Maska	Počet adres
/1	128.0.0.0	2,147,483,646
/2	192.0.0.0	1,073,741,822
/3	224.0.0.0	536,870,910
/4	240.0.0.0	268,435,454
/5	248.0.0.0	134,217,726
/6	252.0.0.0	67,108,862
/7	254.0.0.0	33,554,430
Class A		
/8	255.0.0.0	16,777,214
/9	255.128.0.0	8,388,606
/10	255.192.0.0	4,194,302
/11	255.224.0.0	2,097,150
/12	255.240.0.0	1,048,574
/13	255.248.0.0	524,286
/14	255.252.0.0	262,142
/15	255.254.0.0	131,070
Class B		
/16	255.255.0.0	65,534
/17	255.255.128.0	32,766
/18	255.255.192.0	16,382
/19	255.255.224.0	8,190
/20	255.255.240.0	4,094
/21	255.255.248.0	2,046
/22	255.255.252.0	1,022
/23	255.255.254.0	510
Class C		
/24	255.255.255.0	254
/25	255.255.255.128	126
/26	255.255.255.192	62
/27	255.255.255.224	30
/28	255.255.255.240	14
/29	255.255.255.248	6
/30	255.255.255.252	2
/31	255.255.255.254	0
/32	255.255.255.255	0

IPv6 síťový protokol – L3

- Vyčerpání IPv4??? Rozšíření IoT. IPv6 = bilion adres na čtvereční centimetr Země.
- Před kompletním nahrazením IPv6 za IPv4, je zapotřebí množství tzv. mechanismů přechodu, umožňující IPv6 hostům využívat IPv4 služby a izolovaným IPv6 hostům a sítím dosáhnout IPv6 Internet přes infrastrukturu IPv4.
- IPv6 je ve velkém rozsahu konzervativním rozšířením IPv4. Většina přenosových a aplikačních vrstev protokolů vyžaduje malé nebo žádné změny pro funkčnost s IPv6. Výjimkami jsou protokoly aplikací zahrnující adresy síťové vrstvy (jako např. FTP či NTP v3). Nicméně aplikace vyžadují obvykle malé změny a novou kompilaci, aby pracovaly s IPv6.
- 128bitová délka: Hlavní změnou oproti IPv4 je délka síťové adresy. Adresy IPv6 jsou 128 bitů dlouhé (jak je určeno RFC 4291), zatímco IPv4 adresy mají 32 bitů. Zatímco IPv4 obsahuje zhruba 4 miliardy adres, IPv6 má dostatek prostoru pro 3.4×10^{38} adres.
- Adresy IPv6 se typicky skládají ze **dvou logických částí**:
64bitová (pod)síťový prefix a 64bitové části hosta, buď automaticky vytvářené na základě MAC adresy rozhraní nebo přiřazené následně.
- IPv6 adresy s obvykle zapisují jako osm skupin čtyř hexadecimálních číslic. Například **2001:0db8:85a3:08d3:1319:8a2e:0370:7334**. Pokud je jedna nebo více ze čtyřčlenných skupin **0000**, nuly mohou být vynechány a nahrazeny dvěma dvojtečkami (::). Např. **2001:0db8:0000:0000:0000:0000:1428:57ab** lze nahradit **2001:0db8::1428:57ab**.



MTU - Maximum transmission unit (L3)

(Česky maximální přenosová jednotka). V sadě protokolů internetu se jedná o označení maximální velikosti IP paketu, který je možné přenést z jednoho síťového zařízení na druhé. Obvyklá hodnota MTU v případě Ethernetu je 1500 bajtů, nicméně mezi některými místy počítačové sítě (WiFi, VDSL, PLC) může být maximální délka přeneseného paketu nižší.

Maximální možnou velikost MTU na trase lze zjistit metodou Path MTU discovery, kdy je vyslán datagram s nastaveným příznakem *Do not fragment* (nefragmentovat). Pokud některý router potřebuje provést fragmentaci (která je zakázána), je pomocí protokolu ICMP oznámena odesílateli chyba.

Fragmentace paketů

U přenosového protokolu IP je při směrování paketu do přenosového kanálu s nižším MTU než je délka paketu, provedena fragmentace paketu. V hlavičce všech fragmentů kromě posledního je nastaven příznak *More fragments*, identifikátor je zachován a příslušným způsobem je nastavena položka *Fragment offset*. Opravena je položka *Total Length*.

Fragmenty sestavuje zásadně až příjemce, protože každý fragment může využít v síti jinou cestu. Již fragmentované pakety lze dále fragmentovat. Fragmentace působí potíže zejména u vyšších protokolů, kdy je kvůli ztrátě 1 fragmentu nutné přenášet celý chybějící celek. Proto IPv6 místo fragmentace příliš dlouhé pakety zahazuje.

TTL - Time to live (L3)

TTL je v informatice číslo, které omezuje dobu platnosti dat nebo počet průchodů paketů skrz aktivní prvky počítačové sítě. TTL je v IPv4 8bitová položka v hlavičce IP datagramu, která v počítačové síti omezuje jeho maximální dobu existence a chrání ji tak před zahlcením, které by mohly způsobit datagramy zacyklené v nekonečných smyčkách (způsobených chybou nebo nesprávným nastavením směrování).

Položka TTL je nastavena na výchozí hodnotu při vytvoření datagramu (obvykle 64) a automaticky snižována alespoň o 1 při průchodu jakýmkoliv směrovačem. Po dosažení nuly je datagram zahozen a odesílatel je o tom informován ICMP zprávou *Time Exceeded* (zpráva číslo 11).

Položku TTL využívá ke své činnosti program tracert.

Přesná definice podle RFC 791:

Toto pole indikuje maximální dobu, kterou může datagram setrvat v síťovém systému. Pokud je hodnota tohoto pole nulová, pak musí být datagram zahozen. Čas je měřen v jednotkách sekund. Každý modul, který datagram zpracovává, musí snížit hodnotu TTL nejméně o jedna, a to i v případě, že ho zpracovává méně než sekundu. Cílem je zahození nedoručitelných datagramů a omezit maximální dobu existence datagramu.

Přepínače vyšších vrstev – L3/L4

Jedná se o víceméně marketingový pojem. Díky svému rozšíření v Ethernetu se pojem switch vžil pro rychlý prvek rozhodující o dopravě rámců. Když se pak objevily Ethernetové switche s rozšířenými funkcemi, které dokázaly analyzovat protokol IP a fungovat jako směrovače (router), začal se pro ně používat pojem **L3 switch**.

L3 zde označuje 3. vrstvu modelu OSI, ve které takové zařízení operuje.

Původní L3 switche byly velmi rychlé, ale jednoduché. Typicky měly jen velmi omezenou podporu směrovacích protokolů a veškerých pokročilých funkcí. Postupem času se jejich schopnosti rozšiřovaly a v současnosti se pojem **L3 switch** používá víceméně jako synonymum pro velmi rychlý směrovač s rozšířenou schopností analýzy paketů.

Analogicky se můžete setkat s pojmem **L4 switch** pro zařízení, jež umí analyzovat protokol 4. vrstvy OSI modelu a zpracovávat pakety např. podle čísel portů. Zpravidla se jedná o funkce filtrace TCP/UDP včetně provázanosti na MAC/IP autentizaci a DHCP.

Transportní vrstva – L4

Vrstva č. 4, anglicky transport layer. Tato vrstva zajišťuje přenos dat mezi koncovými uzly. Jejím účelem je poskytnout takovou kvalitu přenosu, jakou požadují vyšší vrstvy. Principiálně nabízí tato vrstva dva typy služeb orientované:

- **spojově (TCP ~ Transmission Control Protocol)**
- **nespojově (UDP ~ User Datagram Protocol)**

Hlavními protokoly této vrstvy jsou TCP a UDP:

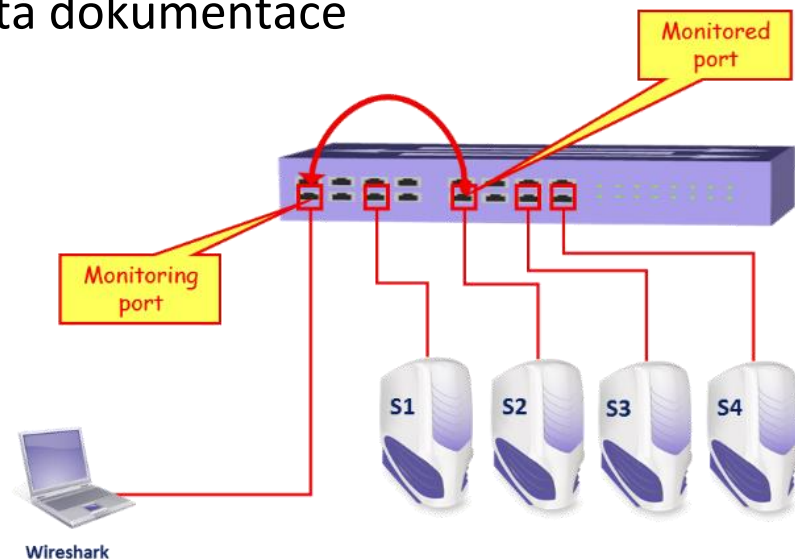
- TCP – Zajišťuje „spolehlivý“ přenos dat, který vyžadují aplikace, kde nesmí „chybět ani paket“. Jedná se o přenosy souborů, e-mailů, WWW stránek atd. Spolehlivost je zajištěna tzv. Flow control (zastavuje příjem paketů, aby bylo zabráněno přetečení zásobníku) a Windowing, kdy každý např. třetí (dle nastavení spojení) paket je uznán jako přijatý a druhý uzel žádá o přenos dalších 3 paketů. Jednotkou informace je na této vrstvě segment.
- UDP – Jedná se o „nespolehlivý“ přenos dat využívaný aplikacemi, u kterých by bylo na obtíž zdržení (delay) v síti způsobené kontrolou každého paketu. Zpožděná informace není relevantní u přenosů, jako jsou streamované video, internetová rádia, vyhledávání sdílených souborů v rámci sítě P2P, on-line hry atp.

Relační, prezentační, aplikační vrstva

- **Vrstva č. 5**, anglicky session layer. Smyslem vrstvy je organizovat a synchronizovat dialog mezi spolupracujícími relačními vrstvami obou systémů a řídit výměnu dat mezi nimi. Umožňuje vytvoření a ukončení relačního spojení, synchronizaci a obnovení spojení, oznamování výjimečných stavů. Do této vrstvy se řadí: NetBIOS, AppleTalk, RPC, SSL.
- **Vrstva č. 6**, anglicky presentation layer. Funkcí vrstvy je transformovat data do tvaru, který používají aplikace. Formát dat (datové struktury) se může lišit na obou komunikujících systémech, navíc dochází k transformaci pro účel přenosu dat nižšími vrstvami. Mezi funkce patří např. převod kódů a abeced, modifikace grafického uspořádání, přizpůsobení pořadí bajtů a pod. Vrstva se zabývá jen strukturou dat, ale ne jejich významem, který je znám jen vrstvě aplikační. Příklady protokolů: SMB (Samba).
- **Vrstva č. 7**, anglicky application layer. Účelem vrstvy je poskytnout aplikacím přístup ke komunikačnímu systému a umožnit tak jejich spolupráci. Do této vrstvy se řadí tyto služby a protokoly: FTP, DNS, DHCP, POP3, SMTP, SSH, Telnet, TFTP atd.

WIRESHARK

- Síťový software analyzátor
- Univerzální dekodér mnoha protokolů
- Multiplatformní(!)
- Offline analýza
- Velmi detailní uživatelský filtr
- Bohatá dokumentace



The screenshot shows the Wireshark interface with a capture of network traffic. The main pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 348 is highlighted, showing a DNS query for 'cdn-0.nflximg.com'. The packet details pane below shows the structure of the packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (response). The packet bytes pane at the bottom shows the raw hex and ASCII data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
343	65.142415	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
344	65.142715	192.168.0.21	174.129.249.228	HTTP	253	GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&n...
345	65.230738	174.129.249.228	192.168.0.21	TCP	66	80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
346	65.240742	174.129.249.228	192.168.0.21	HTTP	828	HTTP/1.1 302 Moved Temporarily
347	65.241592	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
348	65.242532	192.168.0.21	192.168.0.1	DNS	77	Standard query 0x2188 A cdn-0.nflximg.com
349	65.276870	192.168.0.1	192.168.0.21	DNS	489	Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge...
350	65.277992	192.168.0.21	63.80.242.48	TCP	74	37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr=...
351	65.297757	63.80.242.48	192.168.0.21	TCP	74	80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295...
352	65.298396	192.168.0.21	63.80.242.48	TCP	66	37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=329534130
353	65.298687	192.168.0.21	63.80.242.48	HTTP	153	GET /us/nrd/clients/flash/814540.bun HTTP/1.1
354	65.318730	63.80.242.48	192.168.0.21	TCP	66	80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=329534151 TSecr=491519503
355	65.321733	63.80.242.48	192.168.0.21	TCP	1514	[TCP segment of a reassembled PDU]

Ethernet dle použití nebo chuti...

- ✓ WiFi
- ✓ LRP (Long reach PoE)
- ✓ VDSL & G.Fast
- ✓ EtherCat
- ✓ Security
- ✓ VoIP
- ✓ 100GbE
- ✓ PON
- ✓ PoE





WiFi

V informatice označení pro několik standardů IEEE 802.11 popisujících bezdrátovou komunikaci v počítačových sítích (též *Wireless LAN*, *WLAN*). Samotný název WiFi vytvořilo **Wireless Ethernet Compatibility Alliance**.

Tato technologie využívá bezlicenčního frekvenčního pásma, proto je ideální pro budování levné, ale výkonné sítě bez nutnosti pokládky kabelů. Název původně neměl znamenat nic, ale časem se z něj stala slovní hříčka *wireless fidelity* (bezdrátová věrnost) analogicky k Hi-Fi (*high fidelity* – vysoká věrnost).

Wi-Fi zajišťuje komunikaci na spojové vrstvě, zbytek je záležitost vyšších protokolů. Typicky se proto přenášejí zapouzdřené ethernet rámce. Pro bezdrátovou komunikaci na sdíleném médiu (šíření elektromagnetického pole prostorem) je používán protokol CSMA/CA (ethernet používá na vodičích CSMA/CD).

WiFi - historie

V roce 1997 publikoval mezinárodní standardizační institut IEEE specifikaci standardu bezdrátové sítě pracující v pásmu ISM pod číslem **802.11**. V roce 1999 se tento standard rozšířil o 2 pokročilejší specifikace 802.11a a 802.11b. Velmi využívaná revize přišla v roce 2003 pod označením 802.11g. Rychlost byla zvýšena na 54 Mb/s v pásmu 2,4 GHz.

Novější standard 802.11n vznikl v roce 2008. Podporuje **MIMO** rozhraní (Multiple Input, Multiple Output – mnohonásobný vstup i výstup). Používá více vysílačů a přijímačů pro zlepšení přenosu signálu. Abyste měli jistotu, že své zařízení bude možno vždy propojit s ostatními, vznikla tzv. „Wifi aliance“.

Aliance testuje zařízení pracující ve standardu 802.11 a těm co vyhovují kritériím propůjčí logo, které ujišťuje kupujícího, že jeho zařízení je schopno komunikovat s ostatními wifi zařízeními s tímto logem.

Následníkem Wi-Fi měla být bezdrátová technologie WiMAX (802.16)- Worldwide Interoperability for Microwave Access, která se zaměřuje na zlepšení přenosu signálu na větší vzdálenosti. Jde o standard pro bezdrátovou distribuci dat zaměřený na venkovní sítě, tedy jako doplněk k Wi-Fi chápanému jako standard pro vnitřní sítě.

Technologie WiMAX je dnes částečně začleněna do standardů mobilních sítí 3,5G a 4G jako přenosový prostředek technologie HSPA (High-Speed Packet Access).

WiFi - standardy

Standard	Rok vydání	Pásmo	Maximální	Fyzická
		[GHz]	rychlost	vrstva
			[Mbit/s]	
IEEE 802.11	1997	2,4	2	DSSS a FHSS
IEEE 802.11a	1999	5	54	OFDM
IEEE 802.11b	1999	2,4	11	DSSS
IEEE 802.11g	2003	2,4	54	OFDM
IEEE 802.11n	2009	2,4 nebo 5	600	MIMO OFDM
IEEE 802.11y	2008	3,7	54	
IEEE 802.11ac	2013	5	1000	MU-MIMO OFDM
IEEE 802.11ad	2014	2,4; 5 a 60	7000	
IEEE 802.11ax	2021	2,4 + 5	9600	MU-MIMO OFDMA

WiFi - zabezpečení

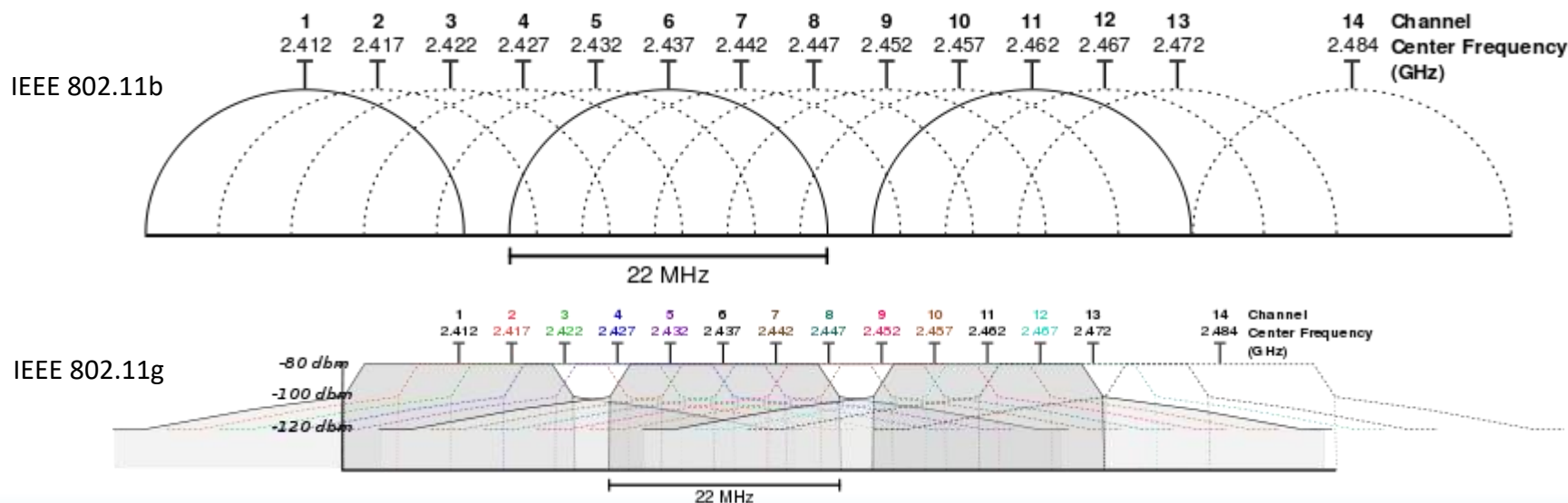
- **Zablokování vysílání SSID**
Nejjednodušší zabezpečení bezdrátové sítě pomocí jejího zdánlivého skrytí. Klienti síť nezobrazí v seznamu dostupných bezdrátových sítí, protože nepřijímají broadcasty se SSID.
- **Kontrola MAC adres**
Přípojný bod bezdrátové sítě má k dispozici seznam MAC adres klientů, kterým je dovoleno se připojit (tzv. whitelist). Zrovna tak je možné nastavit blokování určitých MAC adres (blacklist). Útočník se může vydávat za stanici, která je již do bezdrátové sítě připojena pomocí nastavení stejné MAC adresy (pokud je na AP tato funkce aktivní).
- **802.1X**
Přístupový bod vyžaduje autentizaci pomocí protokolu IEEE 802.1X. Pro ověření je používán na straně klienta program, kterému přístupový bod zprostředkuje komunikaci s třetí stranou, která ověření provede RADIUS server.
- **WEP**
Šifrování komunikace pomocí statických WEP klíčů (Wired Equivalent Privacy) symetrické šifry (RC4), které jsou ručně nastaveny na obou stranách bezdrátového spojení.
- **WPA**
Kvůli zpětné kompatibilitě využívá WPA (Wi-Fi Protected Access) WEP klíče, které jsou ale dynamicky bezpečným způsobem měněny. Autentizace přístupu do WPA sítě je prováděno pomocí PSK (Pre-Shared Key – obě strany používají stejnou dostatečně dlouhou heslovou frázi) nebo RADIUS server.
- **WPA2**
Přináší kvalitnější šifrování (šifra AES), která však vyžaduje větší výpočetní výkon.
- **WPA3**
Oprava zranitelností WPA2. Náhrada Pre-shared klíčů za metodu SAE (Simultaneous Authentication of Equals).
- **End-to-End**
S využitím SSL, SSH, PGP, VPN (IPsec, Wireguard, OpenVPN).

WiFi – přenosové médium

Standard **IEEE 802.11** zahrnuje několik druhů modulací pro přenos radiového signálu, přičemž všechny aplikují stejný **L2 protokol**. Nejpoužívanější modulace jsou definované v dodatcích k původnímu standardu s písmeny *a*, *b*, *g* ...

Např. **802.11n** přináší další techniku modulace. Původní přenosové zabezpečení bylo vylepšeno dodatkem „i“ apod; další dodatky (*c–f*, *h*, *j*) opravují nebo rozšiřují předchozí specifikaci.

Standards 802.11b a 802.11g používají 2,4 GHz pásmo; proto mohou zařízení interferovat s mikrovlnnými troubami, bezdrátovými telefony, s Bluetooth nebo s dalšími zařízeními používajícími stejné pásmo. Oproti tomu standardy 802.11a a novější používají 5 GHz.



WiFi – 802.11n

WiFi standard, který si klade za cíl upravit fyzickou vrstvu a podčást linkové vrstvy, takzvanou *Media Access Control* (MAC) podvrstvu tak, aby se docílilo reálných rychlostí přes 100 Mbit/s.

Maximální fyzická/signálová (L1-OSI) rychlost může být až 600 Mbit/s, při MAC (L2-OSI) rychlosti až 400 Mbit, v konfiguraci 4x4 MIMO. Reálná rychlost (L4-OSI) < 200 Mbit/s...

Zvýšení rychlosti se dosahuje použitím MIMO (multiple input multiple output) technologie, která využívá vícero vysílacích a přijímacích antén. Jde o abstraktní matematický model pro multi-anténní komunikační systémy. Obecně tato technologie zefektivňuje spektrální využití rádiových systémů.

Využívá vícecestného šíření k zvýšení propustnosti a dosahu nebo k snížení počtu přenosových bitových chyb, místo snahy o eliminaci efektu vícecestné propagace, o kterou se snaží tradiční *Single-Input Single-Output* (SISO).

MIMO se dnes masivně aplikuje v moderních WiFi systémech včetně mobilních LTE a 5G-NR.

WiFi – 802.11ax

Specifikace byla definována pro možný maximální provoz několika připojených stanic a klientů. Standard podporuje i vzájemnou koordinaci AP.

Reálná rychlost přenosu blíží se více teoretickému maximu je dosahována využitím:

- přenosových technik 802.11n/ac
- větší šířkou pásma až 160MHz
- až 8x8 up+down MIMO kanály a využitím MU-MIMO (multiuser)
- modulací s vysokou datovou hustotou QAM-1024
- dalšími úpravami podvrstvy MAC (L1/L2-OSI)



Teoreticky je zajištěna koexistence komunikace různých kanálových šířek (20/40/80/160MHz) a se zařízeními 802.11a/n/ac díky implementaci identifikátoru VHT(Very High Throughput) v hlavičce rámce PPDU (protocol data unit).

Standard	IEEE 802.11n	IEEE 802.11ac	IEEE 802.11ax
Radiové pásmo	2,4 + 5 GHz	5 GHz	2,4 + 5 GHz
Šířka kanálů	40 MHz	20, 40, 80, 80+80, 160 MHz	20, 40, 80, 80+80, 160 MHz
Modulace	BPSK, QPSK, 16-QAM, 64-QAM	BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM	BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM
Kódování	OFDM	OFDM	OFDMA
Podpora MIMO	(3x3) Down link	4x4 Down link + multiple user	8x8 Down+up link + multiple user
Šířka subnosné	312,5 kHz	312,5 kHz	78,125 kHz
Teoretická přenosová kapacita jednoho streamu	150 Mb/s (40 MHz, 1 SS)	433 Mb/s (80 MHz, 1 SS)	600,4 Mb/s (80 MHz, 1 SS)

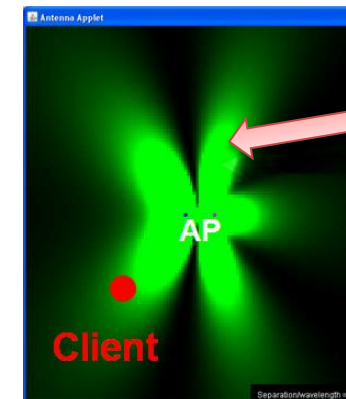
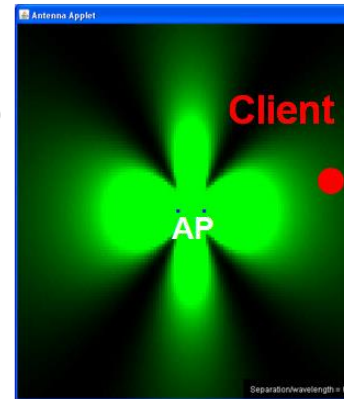
WiFi – 802.11ax

Beamforming

Ve spojení se složitou zpětnou vazbou připojených klientů je signál optimalizovaný pro šíření několika anténami směrem ke konkrétnímu klientovi.

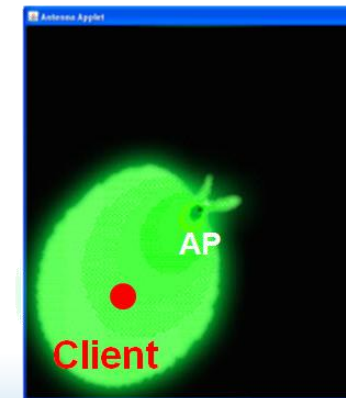
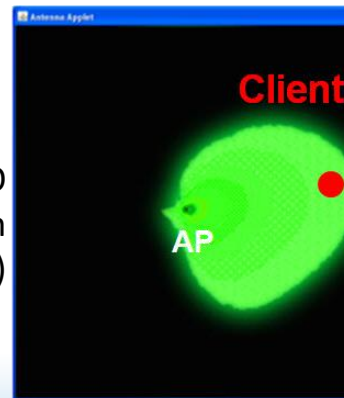
- ✓ Využívá se fyzikální a geometrická znalost parametrů použitých antén.
- ✓ 802.11ax aplikuje tento přístup v kombinaci současně ~ např. „single“ uplink nebude brzdit „multiple“ downlink.
- ✓ Veškerá WiFi zařízení **Planet MIMO** techniku 100% podporují včetně zařízení předchozí generace IEEE 802.11ac díky evolučnímu rozšíření „Wave2“.

optimalizace MIMO
řízená DSP čipem
(802.11n)



nevyužitá energie
- možné zdroje rušení

optimalizace MIMO
řízená DSP+RF čipem
(802.11ax)



WiFi – 802.11ax

OFDMA (Orthogonal Frequency Division Multiple Access)

Jde o ortogonální frekvenční modulaci (vzájemně se neovlivňující) s pokročilým kódováním, které zajistí vysílání několika spojení najednou. Technika kódování nerozlišuje pouze spojení ale především L2 (OSI) rámce různých délek, které může sdružovat do společných L1 (OSI). Procesor čipsetu rámce vyhodnocuje a řídí, do jednoho kanálu dokáže numericky vměstnat více rámců od několika uživatelů.

Díky tomu klesne doba odezvy spojení a lze obsloužit více spojení/uživatelů najednou. Rovněž snižuje energetické nároky koncových zařízení, kdy je možné přenášet malé rámce sdruženě a ne nuceně jednotlivě, statisticky klesne i režie přenosu.



WiFi – 802.11ax

OFDMA (Orthogonal Frequency Division Multiple Access)

The screenshot displays a Wireshark interface with a packet capture of a WiFi 802.11ax HE MU Trigger frame. The packet list shows a Trigger frame (No. 1) at time 0.000000, source 0.000000 9115 (6c:ab:05:9e:4b...), destination Nano_3 (50...), and type Trigger. The packet details pane shows the Radiotap Header v0, Present flags, and HE information. The HE information section highlights the HE Data 1 field, which is identified as HE_MU. A red arrow points from the 'HE_MU' entry in the packet list to the 'HE MU' field in the HE information section.

No.	Time	Time, displayed	Source	Destination	Type/Subtype	PPDU Format	Info
1	0.000000		0.000000 9115 (6c:ab:05:9e:4b...	Nano_3 (50...	Trigger	HE_MU	Trigger Basic, Flags=.....
2	0.000031		0.000031 88:42:82:00:50:e0	Nano_3	QoS Data	HE_MU	QoS Data, SN=75, FN=0, Flags=.p
3	0.000057		0.000026 WlanPi-B1	Nano_3	QoS Data	HE_MU	QoS Data, SN=77, FN=0, Flags=.p
4	0.000081		0.000024 88:42:82:00:50:e0	Nano_3	QoS Data	HE_MU	QoS Data, SN=80, FN=0, Flags=.p
5	0.000105		0.000024 88:42:82:00:50:e0	Nano_3	QoS Data	HE_MU	QoS Data, SN=83, FN=0, Flags=.p
6	0.000130		0.000025 88:42:82:00:50:e0	Nano_3	QoS Data	HE_MU	QoS Data, SN=86, FN=0, Flags=.p
7	0.000159		0.000029 88:42:82:00:50:e0	Nano_3	QoS Data	HE_MU	QoS Data, SN=88, FN=0, Flags=.p

```
> Frame 2: 2764 bytes on wire (22112 bits), 2764 bytes captured (22112 bits) on interface 0
▼ Radiotap Header v0, Length 94
  Header revision: 0
  Header pad: 0
  Header length: 94
  ▼ Present flags
    > Present flags word: 0xa9d0402a
    > Present flags word: 0xa0000820
    > Present flags word: 0xc0000820
    > Present flags word: 0x00000001
    > [Expert Info (Error/Malformed): Radiotap data goes past the end of the radiotap header]
  > Flags: 0x10
  > Channel frequency: 5580 [A 116]
  > Channel flags: 0x0140, Orthogonal Frequency-Division Multiplexing (OFDM), 5 GHz spectrum
  > Antenna signal: -57dBm
  > RX flags: 0x0000
  > A-MPDU status
  > timestamp information
  ▼ HE information
    ▼ HE Data 1: 0xc7f6, PPDU Format: HE_MU, BSS Color known, UL/DL known, data MCS known, data DCM known, Coding known, LDPC extra symbol segment kno
      .10 = PPDU Format: HE_MU (0x2)
      .1. = BSS Color known: Known
      .0. = Beam Change known: Unknown
      .1. = UL/DL known: Known
```

WiFi – 802.11ax

Roaming

Technika svým názvem známá z mobilních sítí... Z principu standardu IEEE 802.11 dojde k přepojení z jednoho AP na jiné podle zásadních parametrů a těmi jsou úroveň signálů a jejich poměry k ostatním či k rušení ~ RSRP, RSRQ, SINR, RSSI.

Děje se tak na úrovni OSI vrstvy L1 ve spojení s L2, konzistenci dat při spojení zajistí vrstvy L3 (TCP/IP protokol) a vyšší.

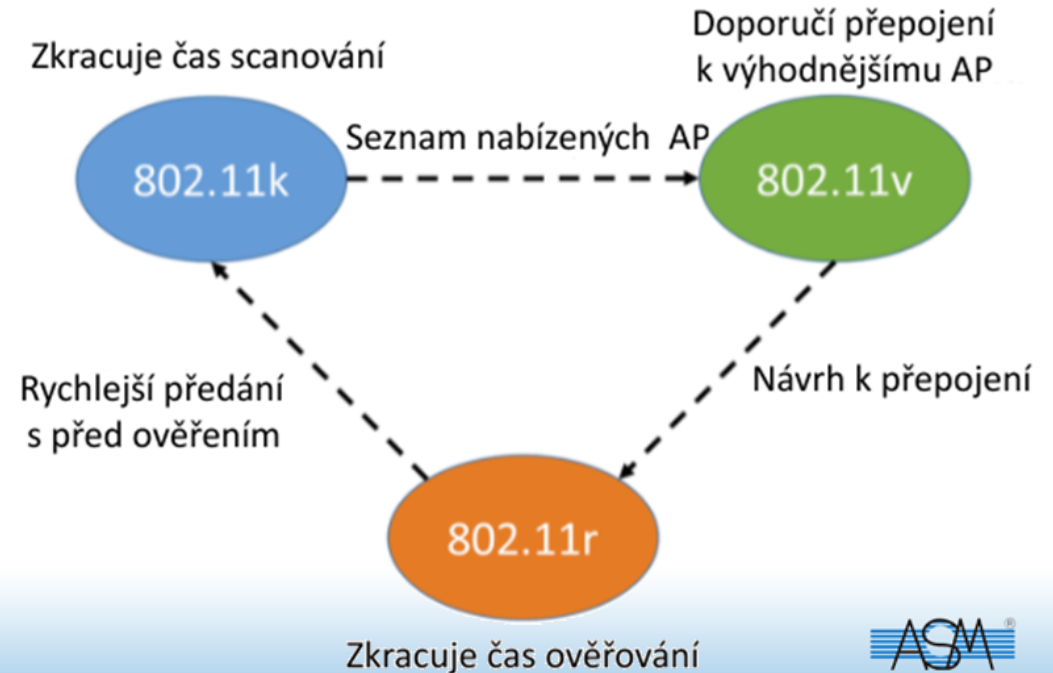
Předávání klientů zvládnou i stará AP, není třeba kontrolér ☺

RTS Threshold – parametr RSSI (Received Signal Strength Indicator) na straně AP může klienty nuceně odpojovat.

Toho se často využívá přímo v AP nebo i centralizovaně pomocí kontrolérů.

Moderní standardy:

- IEEE 802.11k (Radio Resource Measurement) – shromažďuje info o radiovém okolí a poskytuje klientům seznam blízkých AP.
- IEEE 802.11v (BSS Transition Management Frames) – řídí klienty jejich informováním k přepojení na výhodnější AP z hlediska provozních parametrů a eliminuje koncentraci klientů k jednomu AP.
- IEEE 802.11r (Fast BSS Transition) – zrychluje proces bezdrátového ověřování, snižuje latenci při přepojení.



WiFi – 802.11ax

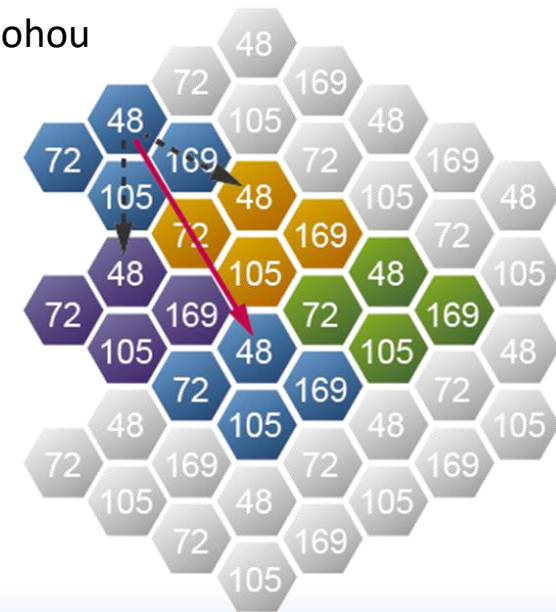
BSS (Basic Service Set) coloring

Při potřebě plošného pokrytí větších prostor s výskytem více uživatelů (nemusí jít o stadion, situaci vyhoví i škola nebo restaurace) je potřeba pokrýt signálem větší plochu větším počtem AP jednotek, ale s tím i nuceně kapacitně dimenzovat využití jednotlivých přístupových bodů. A ty jsou z hlediska počtu připojených uživatelů omezeny fyzickým výkonem a logickým řízením.

Tato technika rozlišuje AP jednotky mezi sebou „barvami“ a dovoluje AP rozpoznat, kdy může ignorovat cizí vysílání a zahájit vlastní komunikaci. V jedné fyzické síti lze vzájemně identifikovat až 63 sousedících jednotek, které mohou a často s vysíláním v rozprostřeném radiovém pásmu sdílejí vysílací frekvence společně.

BSS Coloring díky vzájemné identifikaci AP kolize eliminuje, je pak možné mnohem efektivněji využívat přístup protokolem CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), který je pro WiFi zásadní!

Ve stručnosti - AP standardu 802.11ax jednotky o sobě ví a dokáží dynamicky optimalizovat provozní vytížení stejného kmitočtu.



WiFi – 802.11ax

BSS (Basic Service Set) coloring

No.	Timestamp	Time	Source	Destination	Protocol	Length	VHT CBW	BSS Color	BSS Color Disabled	BSS Color Switch Countdown	Info
2000	2020-01-07 11:35:46,6807338...	65.036157951	Lancom_	Broadcast	802.11	469		0x2b	False		Beacon frame, SN=2175,
2002	2020-01-07 11:35:46,7831384...	65.138562577	Lancom_	Broadcast	802.11	469		0x2b	False		Beacon frame, SN=2176,
2004	2020-01-07 11:35:46,8855145...	65.240938730	Lancom_	Broadcast	802.11	469		0x2b	False		Beacon frame, SN=2177,
2006	2020-01-07 11:35:46,9879393...	65.343363469	Lancom_	Broadcast	802.11	469		0x2b	False		Beacon frame, SN=2178,
2008	2020-01-07 11:35:47,0903494...	65.445773533	Lancom_	Broadcast	802.11	474		0x2b	True	10	Beacon frame, SN=2179,
2010	2020-01-07 11:35:47,1927459...	65.548170975	Lancom_	Broadcast	802.11	474		0x2b	True	9	Beacon frame, SN=2180,
2012	2020-01-07 11:35:47,2951539...	65.650578059	Lancom_	Broadcast	802.11	474		0x2b	True	8	Beacon frame, SN=2181,
2014	2020-01-07 11:35:47,3975332...	65.752957337	Lancom_	Broadcast	802.11	474		0x2b	True	7	Beacon frame, SN=2182,
2016	2020-01-07 11:35:47,4999372...	65.855361415	Lancom_	Broadcast	802.11	474		0x2b	True	6	Beacon frame, SN=2183,
2018	2020-01-07 11:35:47,6024727...	65.957896894	Lancom_	Broadcast	802.11	474		0x2b	True	5	Beacon frame, SN=2184,
2020	2020-01-07 11:35:47,7047564...	66.060180571	Lancom_	Broadcast	802.11	474		0x2b	True	4	Beacon frame, SN=2185,
2022	2020-01-07 11:35:47,8071522...	66.162576356	Lancom_	Broadcast	802.11	474		0x2b	True	3	Beacon frame, SN=2186,
2024	2020-01-07 11:35:47,9095449...	66.264969040	Lancom_	Broadcast	802.11	474		0x2b	True	2	Beacon frame, SN=2187,
2026	2020-01-07 11:35:48,0119576...	66.367381759	Lancom_	Broadcast	802.11	474		0x2b	True	1	Beacon frame, SN=2188,
2028	2020-01-07 11:35:48,1143679...	66.469792079	Lancom_	Broadcast	802.11	474		0x1a	False	0	Beacon frame, SN=2189,
2030	2020-01-07 11:35:48,2167502...	66.572174358	Lancom_	Broadcast	802.11	469		0x1a	False		Beacon frame, SN=2190,

```

> Tag: Extended Capabilities (10 octets)
> Tag: VHT Capabilities
> Tag: VHT Operation
> Tag: VHT Tx Power Envelope
> Ext Tag: HE Capabilities (IEEE Std 802.11ax/D3.0)
> Ext Tag: HE Operation (IEEE Std 802.11ax/D3.0)
  - Tag Number: Element ID Extension (255)
  - Ext Tag length: 6
  - Ext Tag Number: HE Operation (IEEE Std 802.11ax/D3.0) (36)
  - HE Operation Parameters: 0x003ff4
  - BSS Color Information: 0xab
    - ..10 1011 = BSS Color: 0x2b
    - .0.. .... = Partial BSS Color: False
    - 1... .... = BSS Color Disabled: True
  - Basic HE-MCS and NSS Set: 0xfffc
> Ext Tag: BSS Color Change Announcement
  - Tag Number: Element ID Extension (255)
  - Ext Tag length: 2
  - Ext Tag Number: BSS Color Change Announcement (42)
  - BSS Color Switch Countdown: 10
  - New BSS Color Info: 0x1a
    - ..01 1010 = New BSS Color: 0x1a
    - 00.. .... = Reserved: 0x0
  - Ext Tag: Spatial Reuse Parameter Set
  
```

As soon as a Collision is detected, the AP disables the current BSS Color...

... and uses BSS Color Change Announcements in Beacon, Probe/(Re-)Association Responses...

... for a certain countdown interval including the new color 26 (0x1a)

WiFi Planet stále žije...

Provozní a obchodní argumenty:

- snadná instalace, není nutné se školit
- autonomní provoz AP jednotek
- výkonově na velmi dobré úrovni, bez problému do firmy/školy
- nevyžadují registraci ani kontrolér
- ale kontroléry jsou v nabídce
- průmyslové verze
- striktně dle IEEE ~ budou fungovat i proti jiným WiFi
- Mediatek nebo Qualcomm čipsety

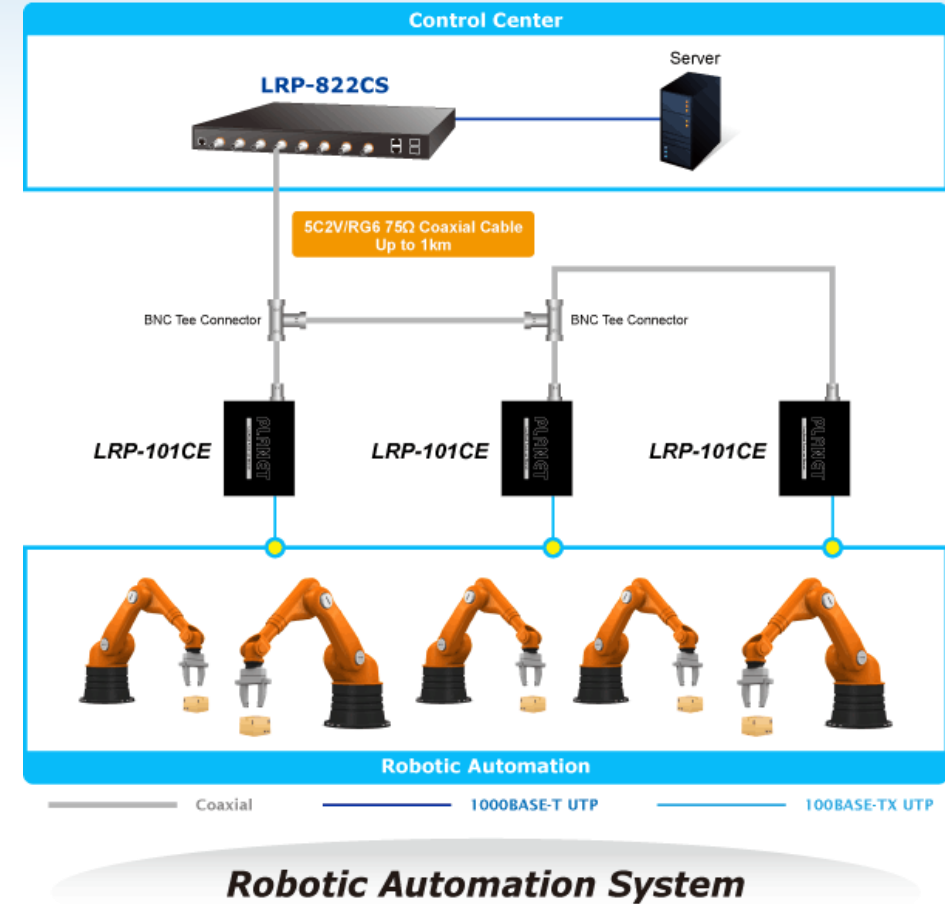


VR-300W6A
Firewall, VPN, VLAN, WiFi AP+kontrolér, Hotspot, Radius

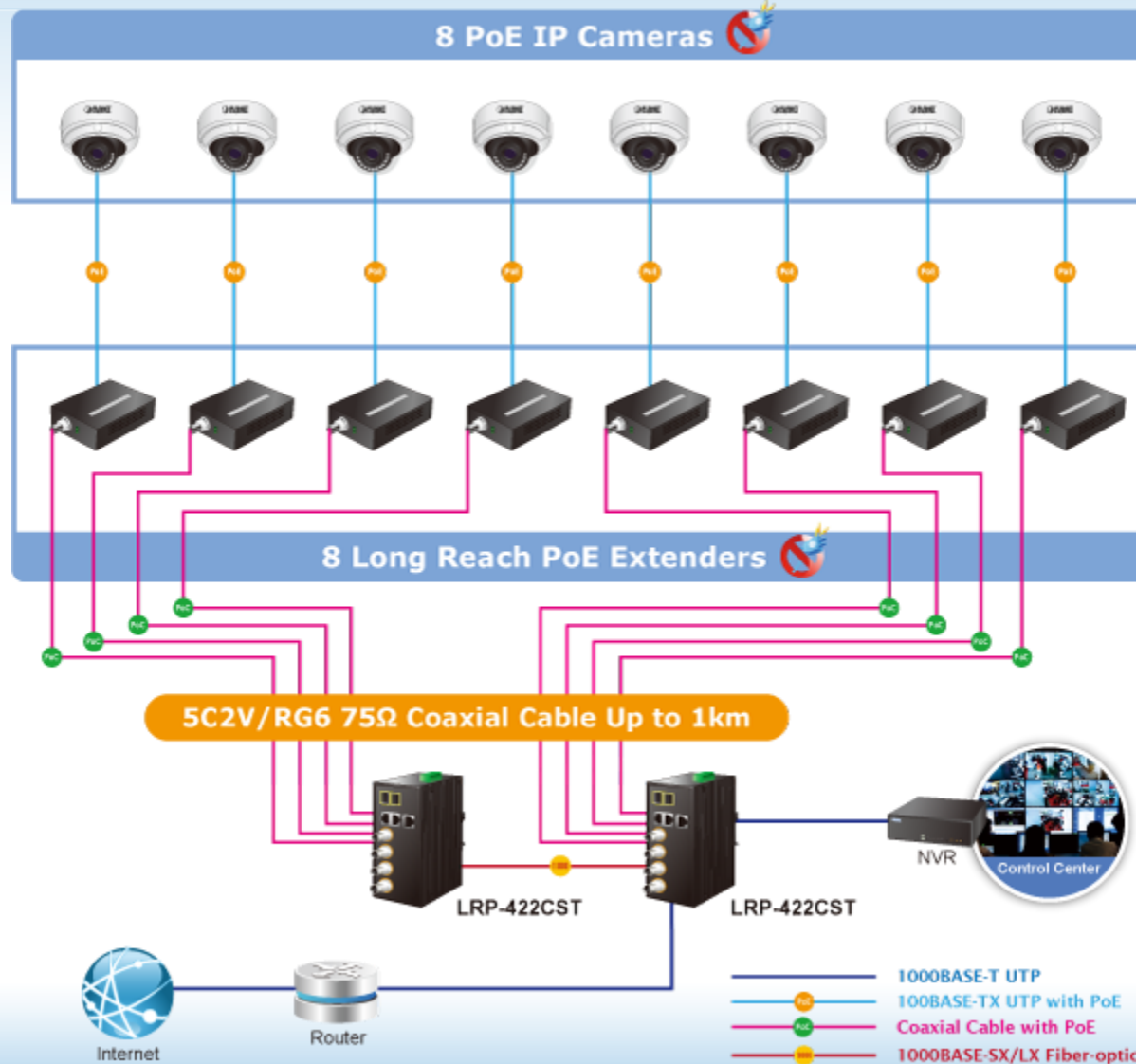


Long reach ethernet

- řešení proudloužení segmentu ethernet včetně zvětšení dosahu napájení PoE (power over ethernet) ze 100m až na 1km po koaxiálním vedení
- IEEE 1901, příbuzná technologie s HomePlug AV
- včetně zachování napájení IEEE 802.3at zařízení na konci vedení
- aplikace extenderu je ideální v místě použití IP kamer nebo bezdrátových přístupových bodů na jejich delší přípojně vzdálenosti
- technicky jde o integrované rozšíření možnosti instalovat napájená zařízení do míst vzdálenějších od centrálního switche nebo racku
- lze provozovat v CATV sítích



Long reach PoE



VDSL modemy

VC-231G

VC-232G over coax

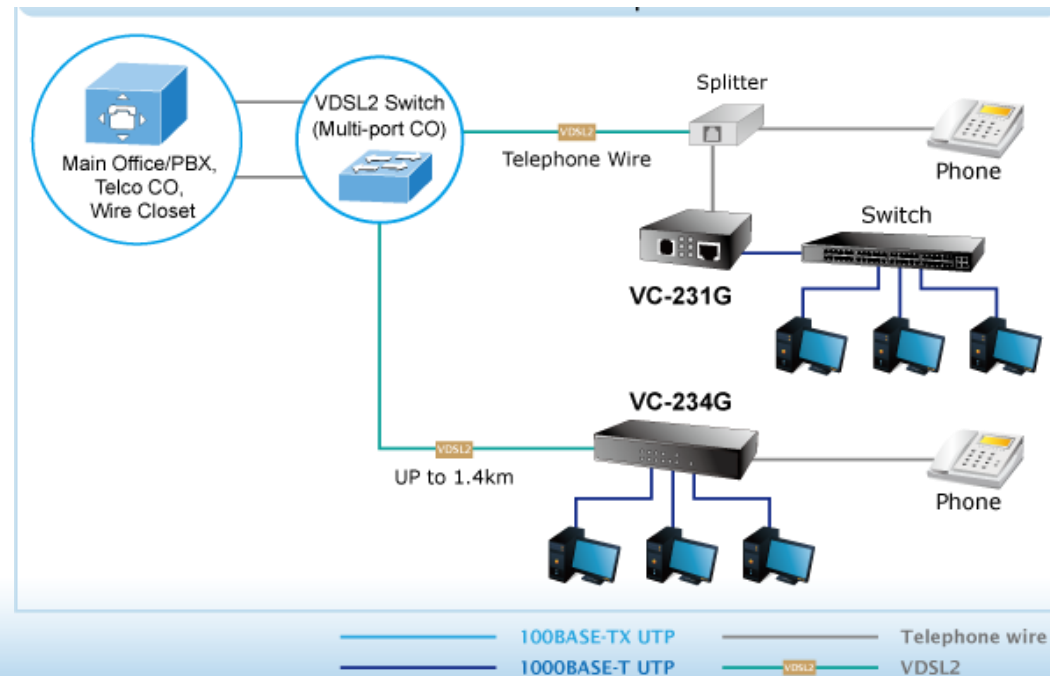
VC-234G 4x 1000Base-T

- VDSL2 modemy/bridge
- podpora G.INP
- podpora G.Vectoringu dle ITU G.993.5
- 1000Base-T rozhraní Ethernet
- kompaktní verze instalovatelné do šasi MC-700/1500
- možný provoz na VDSL CETIN lince do 100Mb/s (profil 17a)
- do 190/190Mbit 300m
- do 1,4km 20/12Mbit



VDSL aplikace v roce 2024

- SoHo segment mimo zájem... (trh s koncovými modemy přetáhli ISP)
- aplikace s výhodným využitím telefonních nebo jinak ošklivých vedení
- vhodné pro CCTV do vzdálených míst v areálech / skladech
- historické objekty / hotely
- nástupcem VDSL je G.fast

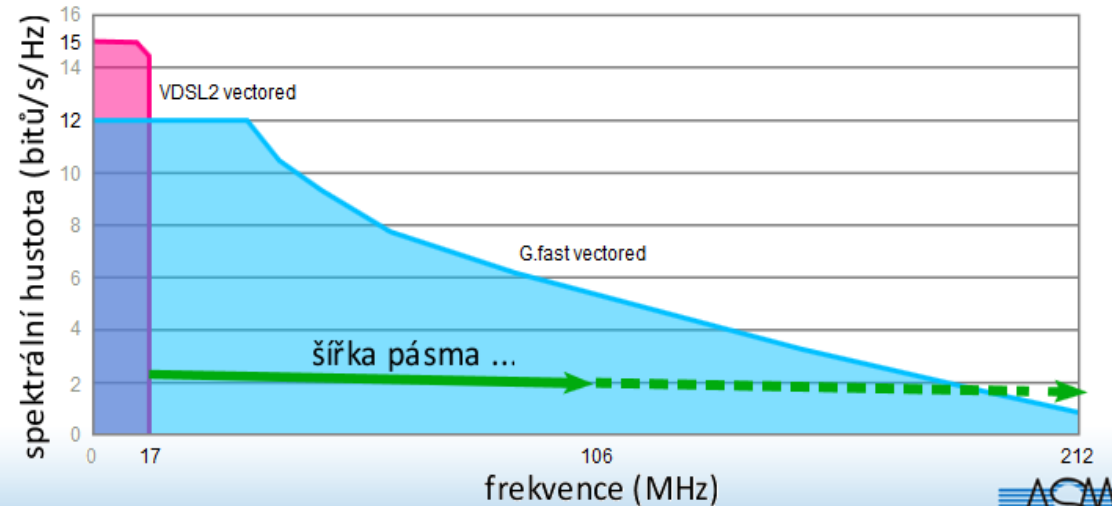
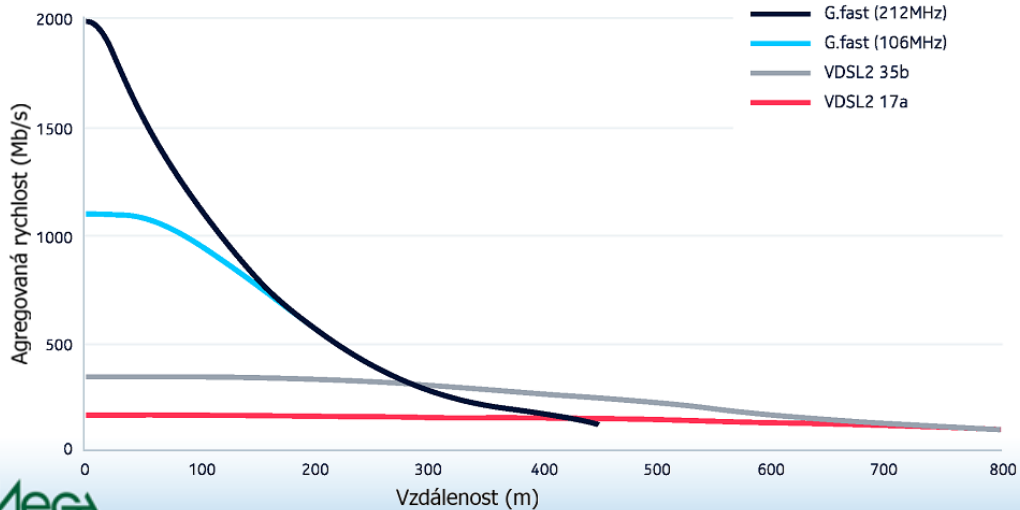
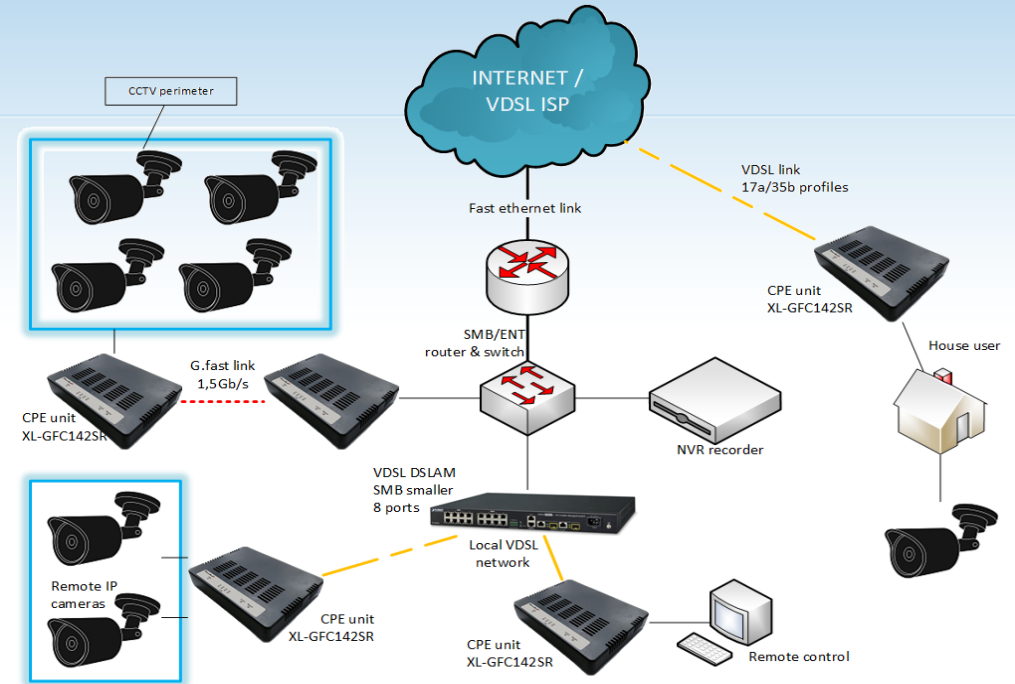


G.fast

- 4. generace xDSL
- Fast access to subscriber terminals
- ITU G.9701
- DMT modulace, TDD duplex

XL-GFC142M/SR

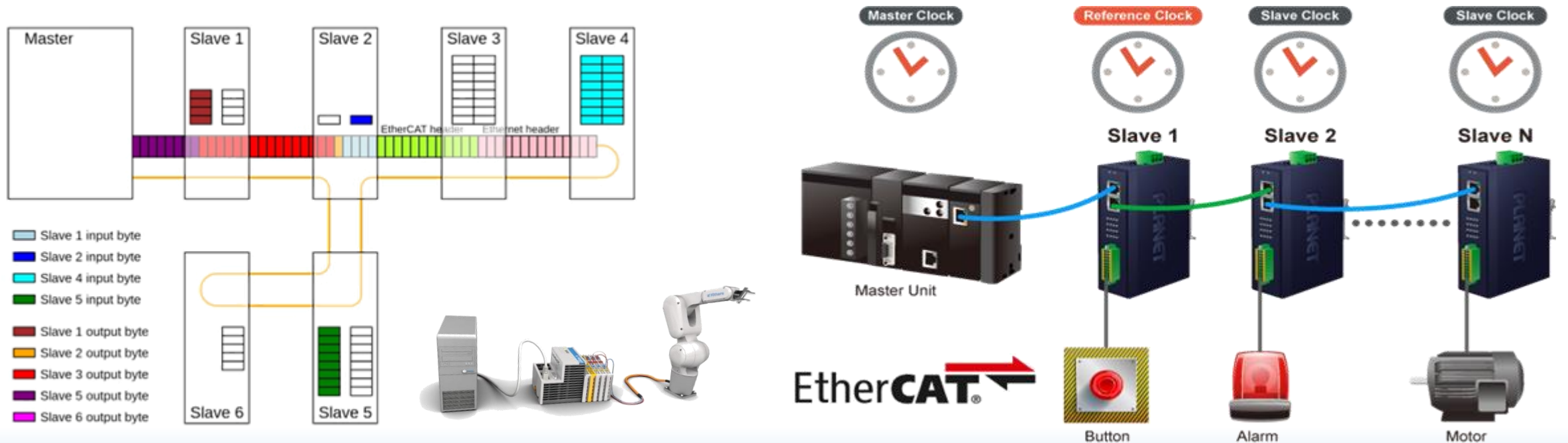
master/slave, G.fast i VDSL (35b), **Cetin kompatibilní**



EtherCAT

- Sběrníkový Ethernet (nejde o IP) pro spojování a ovládání zařízení, standardizován IEC 61158 v rámci rodiny Fieldbus
- Technologie je zaměřena na výkon a činnost v reálném čase, např. řízení servomotoru lze ovládat do $f < 30\text{kHz}$
- Délka segmentu stejná jako 100Base-TX Full duplex ethernet $< 100\text{m}$, nevylučuje se použití optiky a převodníků

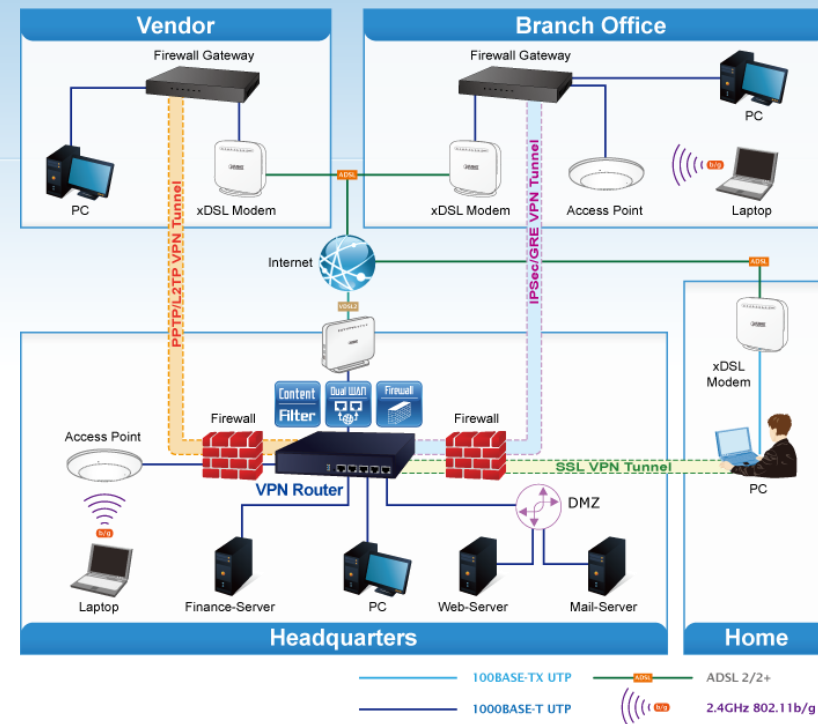
Pro představu jde o jakýsi rychlý vláček rámců...



Security a řešení Planet

Základní vlastnosti

- porty dle modelu (RJ-45, SFP, PoE, WiFi, 5G-NR, GPS)
- Multihoming - dual WAN a SD-WAN
- plnohodnotný router s podporou OSPF a IPv6
- pokročilý SPI firewall s ochranami proti DoS/DDoS
- VPN server s AES akcelerací
- QoS a Shaper
- WEB a SNMP správa, CloudViewer dohled
- podpora VLAN IEEE 802.1Q a Hotspot
- plánovaná podpora **Codefense**
- průmyslové provedení (napájení 12~56V DC, teploty -45~75°C)

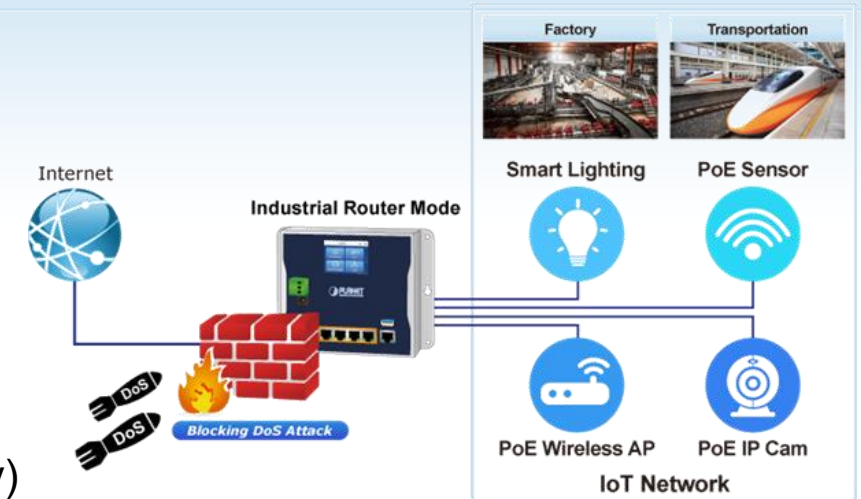


model	VR-100	VR-300	VR-300P	VR-300F	VR-300Wx	VR-300FW-NR
průmyslová verze	IVR-100	IVR-300	IVR-300P	IVR-300F	IVR-300W	-
extra			POE	SFP	WiFi	WiFi+5G(NR)
HA	-	+	+	+	+	+
AP controler	-	+	+	+	+	+

Security a řešení Planet

Přednosti VR

- řešení „vybal a jed“
- bez licencí a registrací
- dobrý výkon i pro SMB firmu
- již sestavený firewall (velmi snadná konfigurace)
- předpřipravené VPN několika typů (IPsec, IKE2, L2TP, OpenVPN)
- bude VLANovat se switchem (oddělení provozů pro hosty, uklízečky, žáky)
- bude si povídat s AP Planet (VR-300 je kontrolérem)



Security a řešení Planet

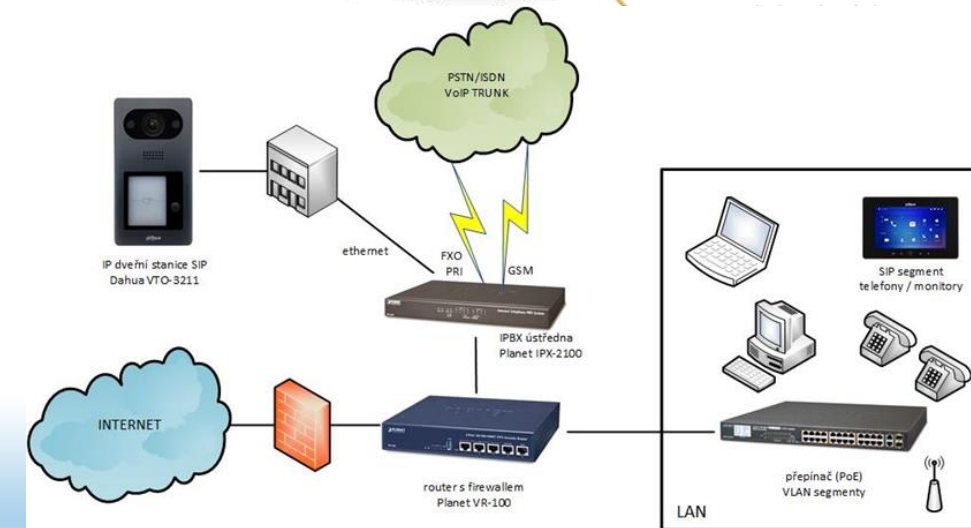
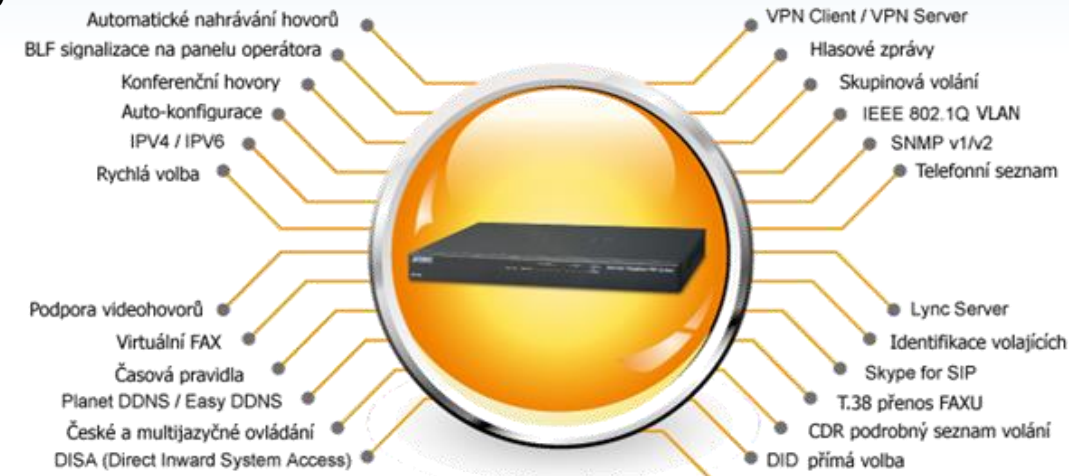
Oblasti kde to ještě/trvale není v pohodě...

- školy
- restaurace / hotely
- sklady
- autodoprava
- kanceláře
- u vás doma??



VoIP telefonní systémy

- IPBX ústředny jsou obecně ekonomicky nenákladné
- hledali jste zmínku o FAXu? IPBX ústředny jsou FAX servery, můžete s nimi komunikovat na úrovni emailu
- IPBX ústředny poskytují mnoho doplňkových služeb včetně napojení na CRM systémy
- bez přítomnosti IPBX se lze registrovat k ITSP přímo
- datový IP provoz je nenáročný na přenosovou kapacitu
- i jediným fyzickým přenosovým médiem Ethernet (UTP, optika, WiFi, 4G/5G, VDSL)
- Internet jako prostředek, díky kterému voláte po celém světě (zdarma)
- v rámci internetu se lze spojovat přímo bez závislosti na ITSP (hlasovém operátoru)
- lze integrovat analogová koncová zařízení prostřednictvím hlasových bran
- lze přenášet video(hovor)
- HD kvalita hovorů
- komunikace může být šifrovaná
- integrace dalších funkcí jako jsou videovrátné systémy apod.
- Váš mobilní telefon nebo notebook může být VoIP klientem- koncovým přístrojem
- VoIP je bez vazby na konkrétní výrobce díky standardizovaným protokolům a kodekům



Rozhraní zítřka ~ 40/100GbE

40/100GbE

100Gbitové rozhraní součástí standardu IEEE 802.3ba-2010, rozšířen v roce 2011 o 40Gb dle IEEE 802.3bg následně IEEE 802.3bj s definicí 100Gb spojení na krátké metalické propojení- typicky backplane a sběrnice a dalšími definicemi pro další typy spojení IEEE 802.3bm-2015, IEEE 802.3cd-2018.

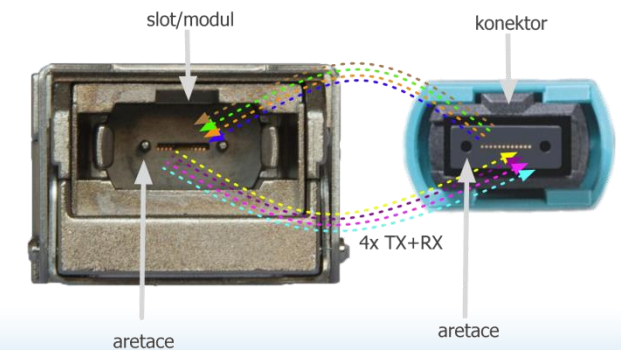
Fyzická vrstva	40 Gigabit Ethernet	100 Gigabit Ethernet
Backplane	40GBASE-KR4	100GBASE-KP4
7 m twinaxial - metalicky	40GBASE-CR4	100GBASE-CR10
		100GBASE-CR4
30m s použitím "Cat8"	40GBASE-T	
100m OM3 multimode	40GBASE-SR4	100GBASE-SR10
125m OM4 multimode		100GBASE-SR4
2km singlemode, CWDM	40GBASE-FR	100GBASE-CWDM4
10km singlemode QSFP	40GBASE-LR4	100GBASE-LR4
40km singlemode QSFP	40GBASE-ER4	100GBASE-ER4

QSFP

V rámci **Multi source agreement** společnosti (Google, Brocade Communications, JDSU, Santur, později další) definovali fyzické rozhraní a podobu modulů.

Jedním z nich je **QSFP** (Quad Small Form-factor Pluggable):

- datová propustnost **4x 10Gb/s** nebo až **4x 28Gb/s**
- implementuje Ethernet, FibreChannel, Infiniband, SONET/SDH
- Rozšířená varianta QSFP+ implementuje SAS/SCSI, 40Gb ethernet
- 3~4x větší datová propustnost kanálu proti SFP+
- MPO(Multiple-Fiber Push-On/Pull-off) konektor
- hotplug



MPO = Multi-fiber Push On

- standardizováno (IEC 61754-7, EIA/TIA-604-5)
- MPO == MTP, technicky stejná věc. MTP® je obchodní značka US Conec
- má možnost mnoha konfigurací, samo označení „MPO“ neříká ani kolik „pinů/vláken“ má v konektoru !
Jen díky nejčastější aplikaci ve spojitosti s QSFP 28 moduly půjde nejčastěji o 12 vláken! (využito 8)
- jiné konfigurace pro formáty jiné než ty používané v modulech QSFP28 nebo za účelem distribuce mnoha vláken v co nejmenším prostoru, typicky „trunk“, „fan-out“ pro 24,48,72,96 vláken v jednom MPO konektoru

Pro QSFP28 100GBASE zajímavé pouze tyto konfigurace:

- 12 vláken, MM OM3, UPC broušení, barva **modrá** „aqua“ - pro 100GBASE-SR4 do 70m
- 12 vláken, MM OM4, UPC broušení, barva **fialová** „violet“ (často violet+aqua) – pro 100GBASE-SR4 do 100m
- 12 vláken, SM (G.652), APC broušení, barva kabelu žlutá + konektoru **zelená** - pro 100GBASE-PM4 do 2km

Pohlaví – řídí se vodícími piny. SR4 modul je „male“, tj. má vodící piny. Propojovací kabel je „female“ a má dírky.

Polarita – tj. jak jsou přehozena pořadí pinů v kabelu na patch kabelu, orientace konektoru určena **tvarovým klíčem**

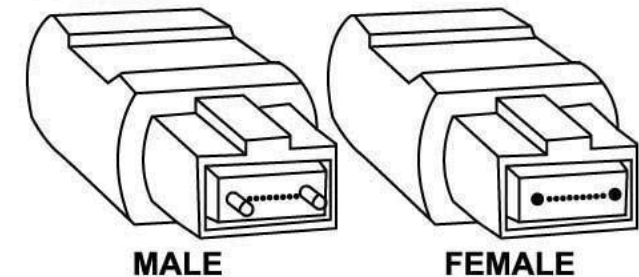
Pro přímé propojení QSFP modulů: polarita B – propojení pinů je 1-12, 2-11, 3-10 ...

➤ Jiné polarity:

- polarita A – propojení pinů je 1-1, 2-2, 3-3 ...
- polarita C - propojení pinů je 1-2, 2-1, 3-4, 4-3 ...
- ! spojením 2 kabelů polarity B dostanu polaritu A.
- ! spojením 3 kabelů polarity B dostanu polaritu B.

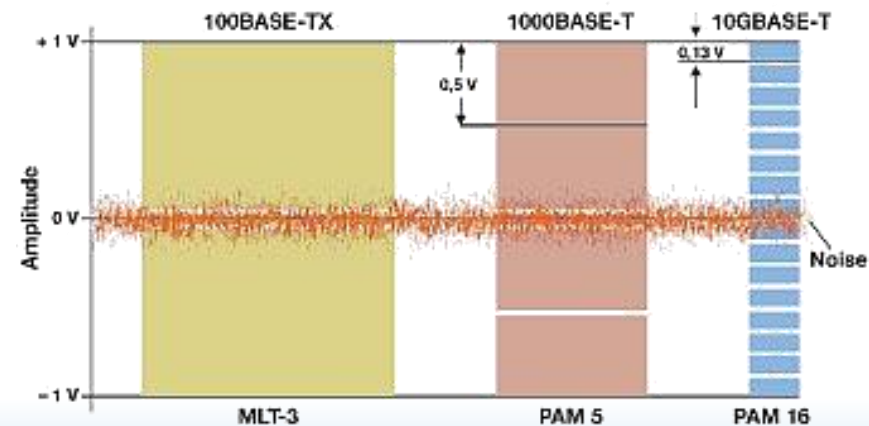
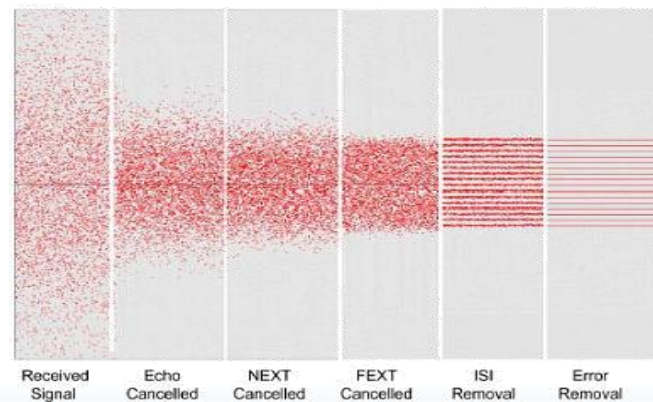


MPO 12 Female
MM OM3 /UPC



SFP+ versus 10GBase-T (RJ-45)

	SFP+	10GBase-T
příkon/port	~ 0,5W	podle spojení 5-10W
dosah	podle modulu	do 100m
kabel	MM/SM	Cat6/6a
konektory	LC	RJ-45 (terminace!!)
zpoždění	< 0,3us	~ 2,5us ($\frac{3}{4}$ RX, $\frac{1}{4}$ TX)
citlivost na přeslechy	žádná	vysoká



100GbE a RDMA

RDMA = Remote Direct Memory Access

přes Ethernetovou síť, vynechává z přenosu CPU, síťový adaptér musí poskytovat HW podporu pro RDMA

Analogie s DMA (Direct Memory Access), jenže po síti!

• Termíny:

NVMe RDMA – znáte NVMe pro SSD...tohle je analogie pro přístup do paměti vzdáleného počítače

iWARP (Internet Wide-area RDMA Protocol) - RDMA nad protokolem TCP/IP

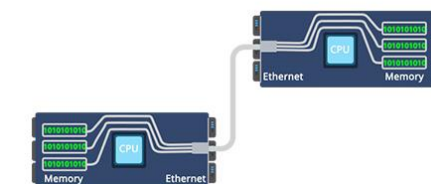
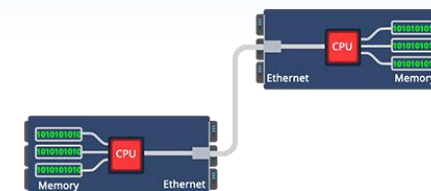
RoCE v1 - RDMA over Converged Ethernet (RoCE), také jako InfiniBand over Ethernet (IBoE). Ethernet, Layer 2.

RoCE v2 - RDMA nad UDP/IP, aktuálně nejvíce používané

- iWARP i RoCE v1,v2 byli standardizovány (IETF)
- hlavní spotřebitelé optických modulů s výkony 100Gbit/s ~ 800Gbit/s
- k čemu clustery? AI !! nové oblasti podnikání v IT....

RDMA dovoluje použít Ethernet (!!) jako základní technologii pro budování výpočetních clusterů

*bez užití RDMA
CPU 100%*



RDMA, CPU 0%

100GbE a RDMA

PCI-E

XL-ENW-9920

1 portová, PCI-E v4.0, x16

XL-ENW-9921

2 portová, PCI-E v4.0, x16

OCP 3.0

XL-ENW-OCP-9016M

2 portová, OCP 3.0 SFF

- QSFP28
- Čipset Intel E810
- Hardwarové akcelerace pro zpracování datových paketů
- iWARP a RoCE v2 Remote Direct Memory Access (RDMA)
- Intel Ethernet Adaptive Virtual Function (Intel Ethernet AVF)
- Rozšířená serverová virtualizace (256 VFs, 768 VSIs)
- IEEE 1588 Precision Time Protocol (v1 a v2) s časovým značením na paketu
- Podpora iSCSI, Jumbo Frames, síťová virtualizace (SR-IOV, VxLAN, GENEVE, GRE)



Kde najít správné kabely a moduly?

ASM
Kabely - propojovací (patch) | ASX +
https://www.asm.cz/cs/kategorie/146220-kabely-propojovaci-patch?filter=on&priceTo=9690&priceFrom=368&priceTo=9690&page=1:8

Zavřít - Filtr parametrů

Značka: Fyzické vlastnosti

Broušení: APC/APC, APC/UPC, UPC/UPC

Délka kabelu (m): 0-40

Konektory: LC/LC, E2000/E2000, E2000/FC, E2000/LC, E2000/SC, FC/FC, FC/SC, LC/LC, LC/LC, LC/SC, LC/ST, MPO/LC, MPO/MPO, MT-RJ/LC, MT-RJ/MT-RJ, SC/SC, ST/ST

Armovaný kabel: ano, ne

Provedení: duplex, simplex, 12 vláken

Specifikace vlákna: OM3 50/125um, OM1 62,5/125um, OM2 50/125um, OM3 50/125um, OM4 50/125um, 9/125um, 9/125um G652, 9/125um G657A1

Typ vlákna: multimode, singlemode

ASM
Optické moduly SFP, SFP+, XFP | ASX +
https://www.asm.cz/cs/kategorie/146246-opticke-moduly-sfp-sfp-xfp

Zavřít - Filtr parametrů

Optické moduly SFP, SFP+, XFP

Značka: Technické detaily, Sítové rozhraní, Fyzické vlastnosti

Diagnostika DDM: ano, ne

Dosah: 2 km, 3 km, 10 km, 20 km, 30 m, 40 km, 60 km, 70 km, 80 km, 80 m, 100 km, 100 m, 120 km, 300 m, 550 m

Rychlost SFP modulu: 1 Gbps, 10 Gbps, 40 Gbps, 100 Gbps

Typ modulu: QSFP+, QSFP28, SFP, SFP+, X2, XFP

Typ optického konektoru: LC, MPO/MTP, SC, SFP

Propojovací optické kabely s MPO konektorem ...

Kde hledat 40G a 100G optické moduly
Hledej QSFP+ a QSFP28...

PON

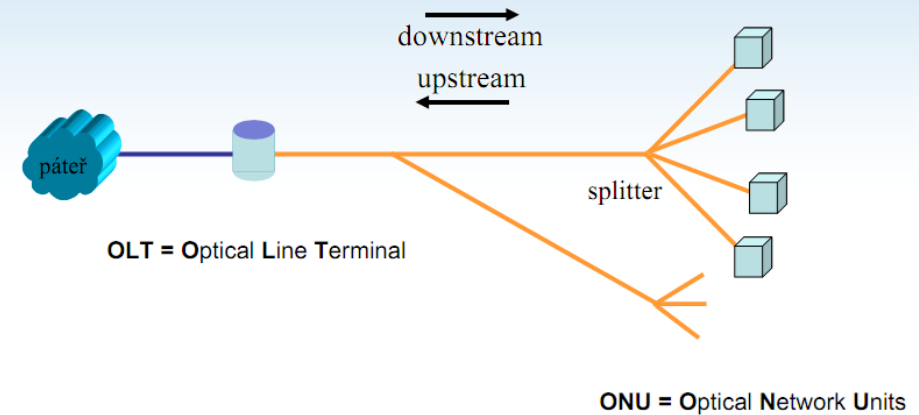
(pasívní optické sítě)

PON

- síť která se obejde bez aktivních prvků na přenosové trase
- aktivní pouze prvky na výchozích a koncových bodech
- Point-to-Multipoint

Terminologie:

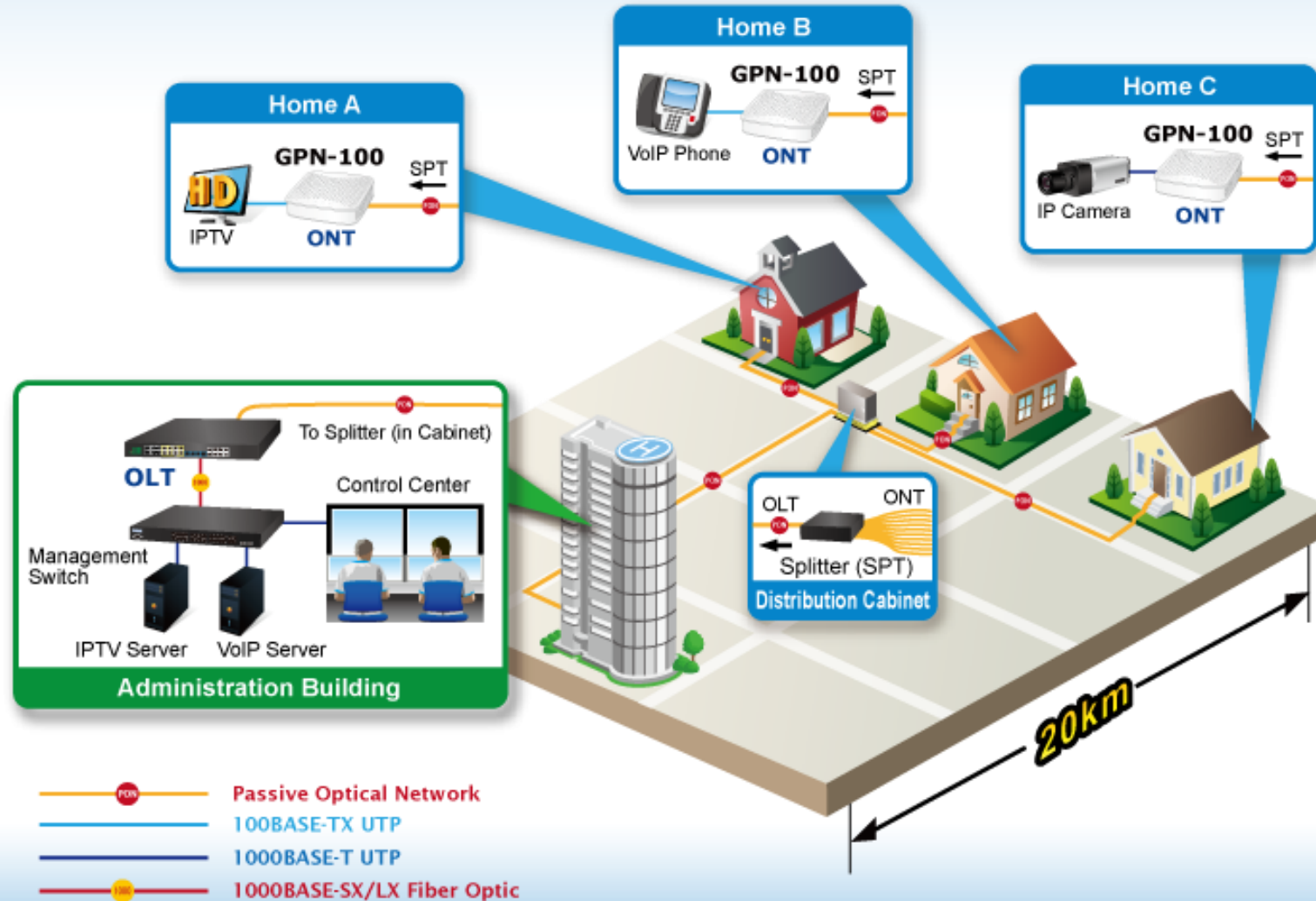
- OLT = centrální jednotka (CO, Master)
- ONU = koncové jednotky (CPE, Slave)
- **GPON** -> **ATM** vychází z APON, BPON (ITU-T G.984)
- **GEPON** -> **ethernet EPON** (IEEE 802.3ah)
- **XG(S)-PON** -> 10Gb PON (ITU-T G.987), S - symetrický



GPON Planet ONU lze provozovat i v sítích GEPON

PON

Fiber To The Home (FTTH) Application

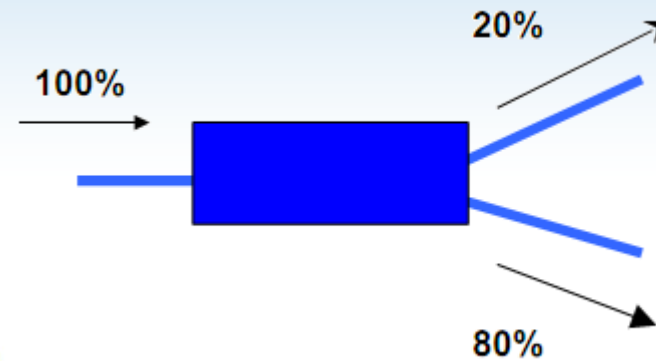


PON

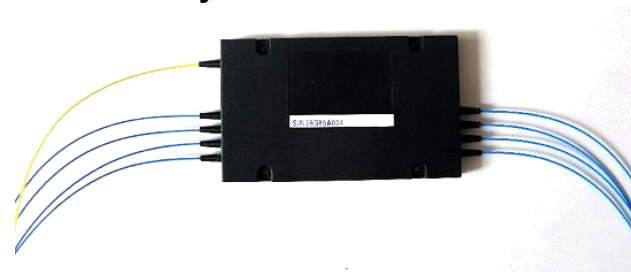
Rozbočovač 1:2 FOS-102 v různých úrovních dělení

Vyčíslení útlumu každého směru (reálně):

- 50:50 3,6 : 3,6 dB
- 30:70 6,0 : 1,9 dB
- 20:80 7,8 : 1,2 dB
- 10:90 11,3 : 0,6 dB
- 5:95 15,2 : 0,4 dB
- 1:99 23,5 : 0,3 dB



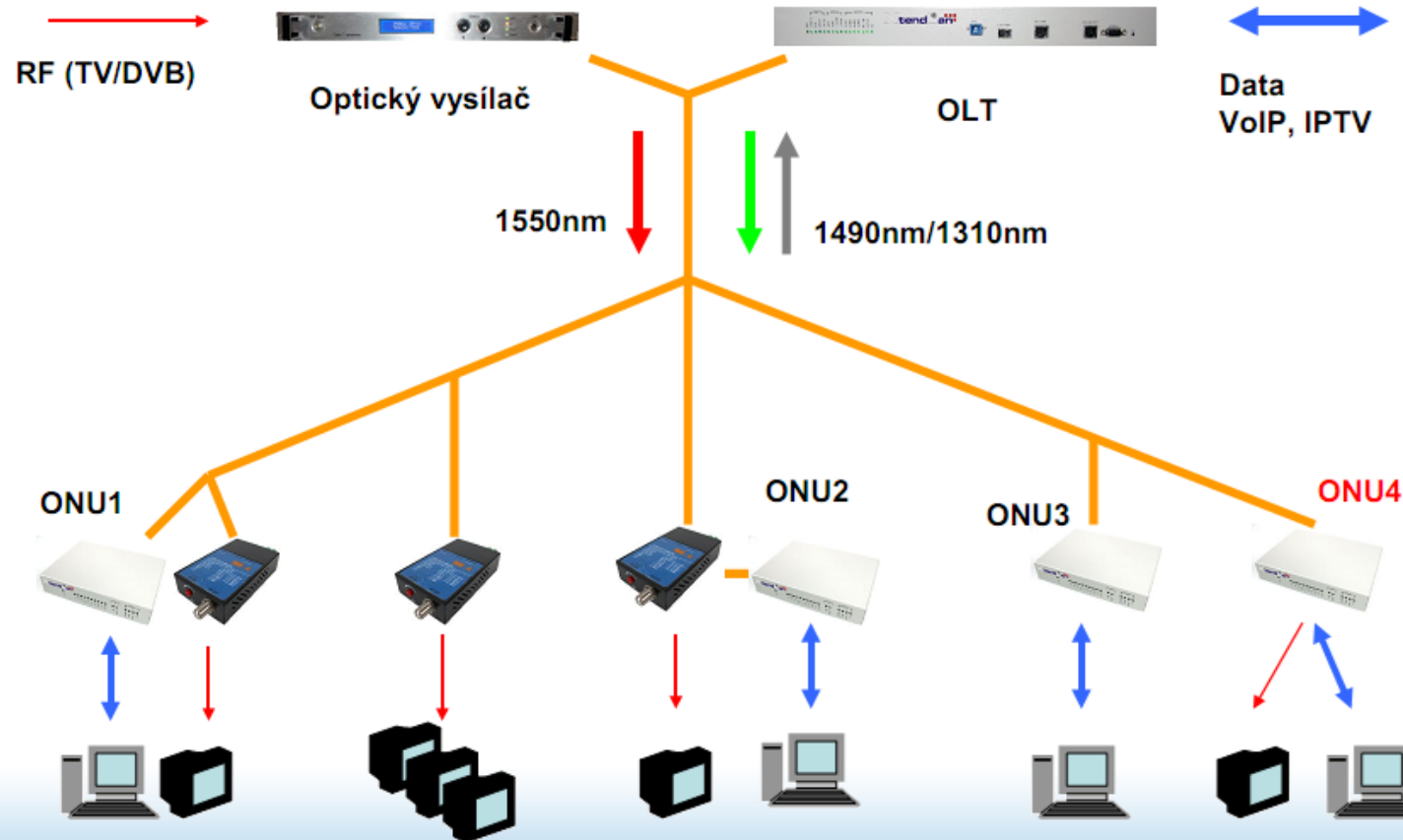
Reciprocita – každý rozbočovač je i slučovačem!



PON + HFC

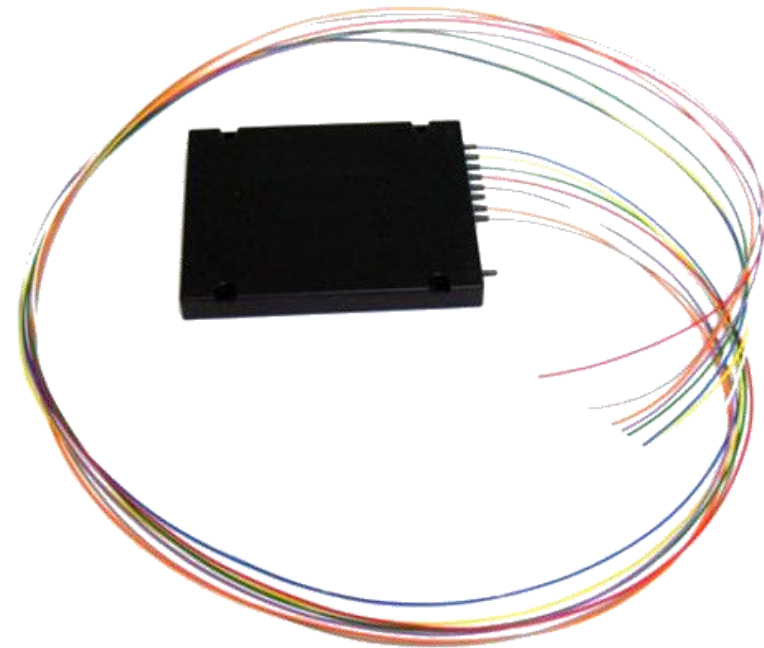
Syntéza sítí - HFC a GEAPON koexistuje v jediné PON síti

- ✓ GEAPON 1490nm a 1310nm
- ✓ HFC 1550nm



PON + HFC + data jedním vláknem

Realizace GEAPON/HFC sítě neomezuje její další využití pro vlnový multiplex CWDM = rozbarvovače.

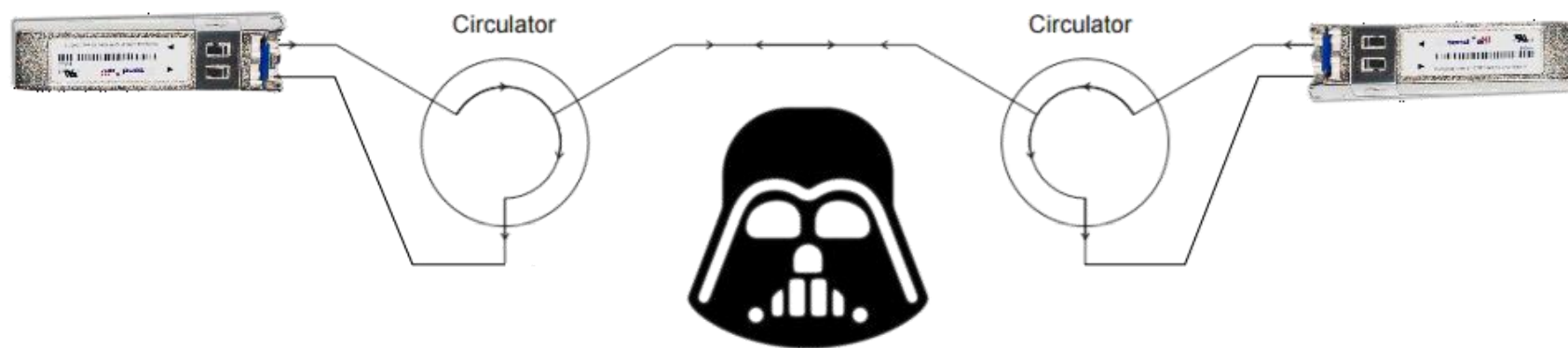


PON od ASM ??

- ✓ ano, umíme obě technologie GPON i GEPON
- ✓ kompatibilní s ISP v ČR (ONU router Planet poběží proti OLT Huawei)
- ✓ umíme HFC TV
- ✓ máme skladem nebo rychle dovezeme (včetně pasivity)
- ✓ umíme svařit



Více na školení ASM ;-)



Dark fiber spojení v MAN prostředí

Výkonové napájení PoE

PoE dle výkonu a jeho výhody

Způsob napájení koncových a síťových zařízení UTP/FTP kabelem.... **dle norem:**

- IEEE 802.3af < 15W
- IEEE 802.3at < 30W (nazýváno PoE+)
- Ultra PoE = IEEE 802.3at ale s vyšším dovoleným výkonem < 60W
- Ultra PoE někdy nazýváno 802.3at+ (neplést s PoE+ tj. 802.3at)
- **Standard IEEE 802.3bt** pro napájení až 100W; zpětně kompatibilní s „af/at“

Bezpečnost dle
EN 62368-1:2014

Důvody zavádění PoE

- 1) efektivnější instalace
- 2) možné zálohované napájení centrálního zdroje
- 3) možný dálkový restart a ovládání napájení správcem
- 4) úspora materiálu a celkové spotřeby
- 5) bezpečné napětí (max. 57V)
- 6) aplikovatelné i nad 1000Base-T
- 7) vysoká spolehlivost



Parametry

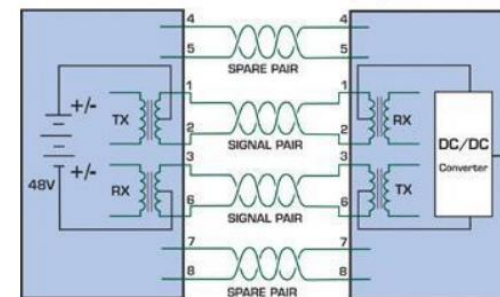
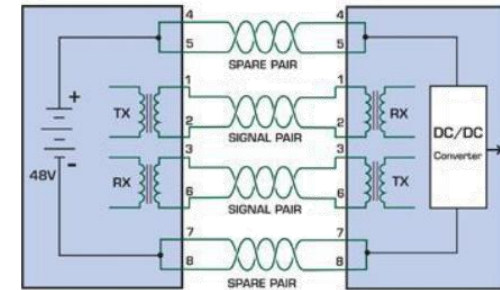
	802.3af Typ 1	802.3at Typ 2	802.3bt Typ 3	802.3bt Typ 4
Max. výkon PSE	15W	30W	60W	100W
Rozsah napětí PSE	44-57V	50-57V	50-57V	52-57V
Max. proud	350mA	600mA	600mA na pár	960mA na pár
Snížení max. provozní teploty kabelu	0°C	5°C	10°C	10°C
Správa napájení	3 úrovně	4 úrovně nebo stupně po 0,1W LLDP	6 úrovní nebo stupně po 0,1W LLDP	8 úrovní nebo stupně po 0,1W LLDP

Základní módy zapojení

Popis zapojení

- ✓ 2 módy napájení!!!
- ✓ podpora MDI, MDI-X a Auto-MDIX

Vodič	10/100Base-TX midspan (mód B)	10/100Base-TX endspan (mód A)	1000Base-T (mód B)	1000Base-T (mód A)
Pin 1	Rx +	Rx + DC +	TxRx A +	TxRx A + DC +
Pin 2	Rx -	Rx - DC +	TxRx A -	TxRx A - DC +
Pin 3	Tx +	Tx + DC -	TxRx B +	TxRx B + DC -
Pin 4	DC +	nepoužito	TxRx C + DC +	TxRx C +
Pin 5	DC +	nepoužito	TxRx C - DC +	TxRx C -
Pin 6	Tx -	Tx - DC -	TxRx B -	TxRx B - DC -
Pin 7	DC -	nepoužito	TxRx D + DC -	TxRx D +
Pin 8	DC -	nepoužito	TxRx D - DC -	TxRx D -



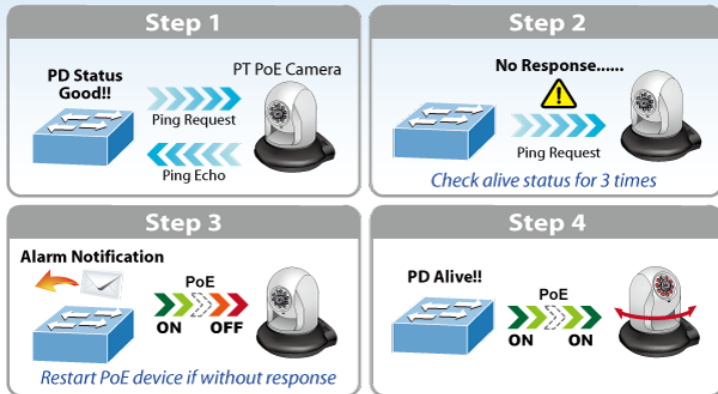
Co se děje po zapnutí

Aktivace napájení (IEEE 802.3at)

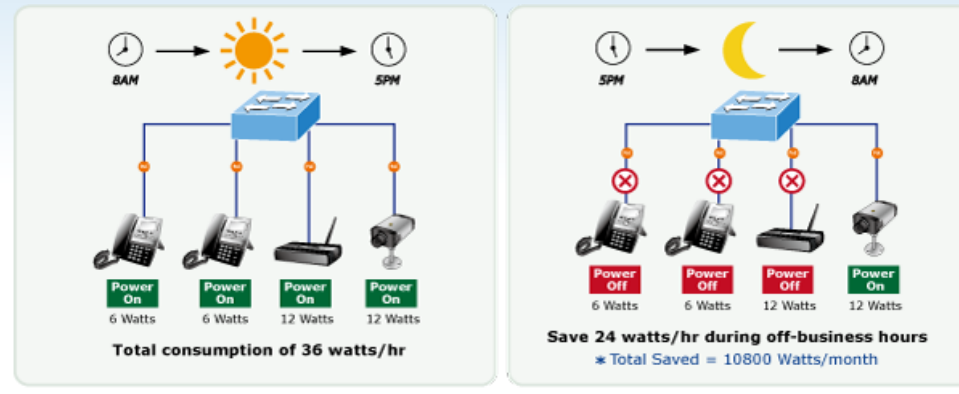
Stav	Děj	Napětí (V)	
		802.3af	802.3at
Detekce	Zdroj detekuje zda spotřebič disponuje korektní rezistancí 19 ~ 26,5kΩ	2,7 ~ 10	
Klasifikace 1	Zdroj detekuje terminaci na vzdáleném konci	14,5 ~ 20,5	
Detekce 1	Detekce zda spotřebič je 802.3at, spotřebič odpoví příkonem 0,25-4mA	—	7 ~ 10
Klasifikace 2	Zdroj opakuje detekci 802.3at	—	14,5 ~ 20,5
Detekce 2	Detekce zda spotřebič je 802.3at, spotřebič odpoví příkonem 0,25-4mA	—	7 ~ 10
Zapnutí napájení	Základní napětí zdroje	> 42	> 42
Operační režim	Plné napětí zdroje	37 ~ 57	42,5–57

- ✓ Podpora LLDP (Link Layer Discovery Protocol)

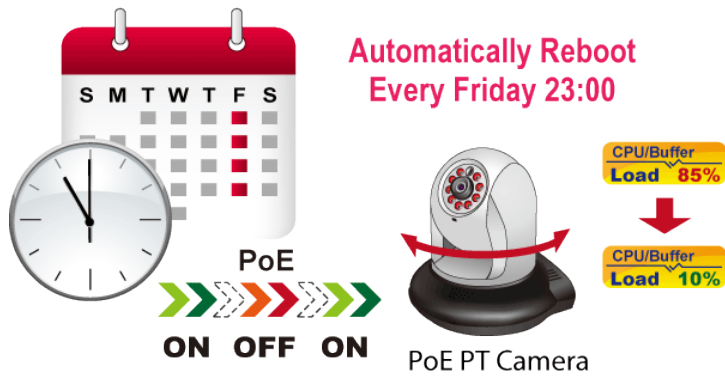
Pokročilé funkce PoE



PING alive check – ICMP detekce



Scheduler - plánovač



Auto reboot



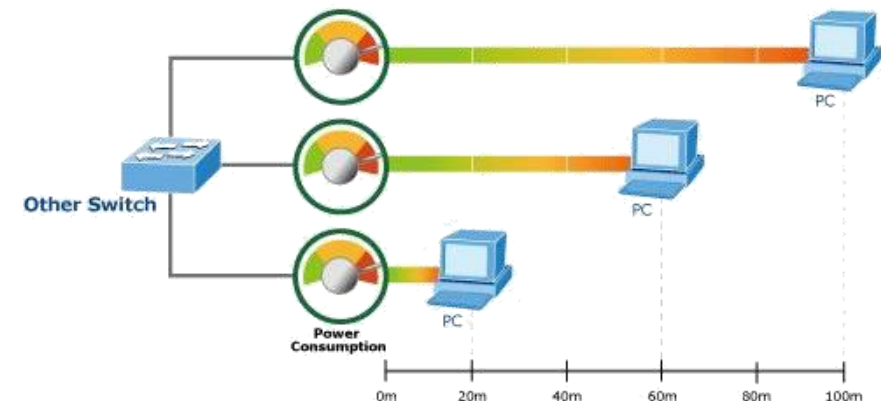
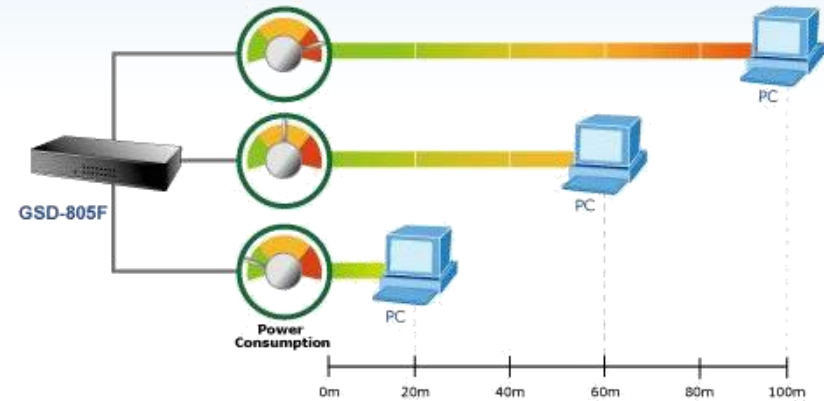
LCD ovládání

Zelený ethernet

- Energy-using Products (EuP) nařízení EU (2006) pro elektrická a energetická zařízení
 - Energy related Products (ERPs) pro pasívní prvky úspory energie
 - cílem je snížit spotřebu EuP o 25% do roku 2025
 - další info EU: http://ec.europa.eu/enterprise/index_cs.htm
- Power Green ethernet
 - Green ethernet
 - Energy Efficient Ethernet (EEE)
 - IEEE 802.3az (od roku 2010)

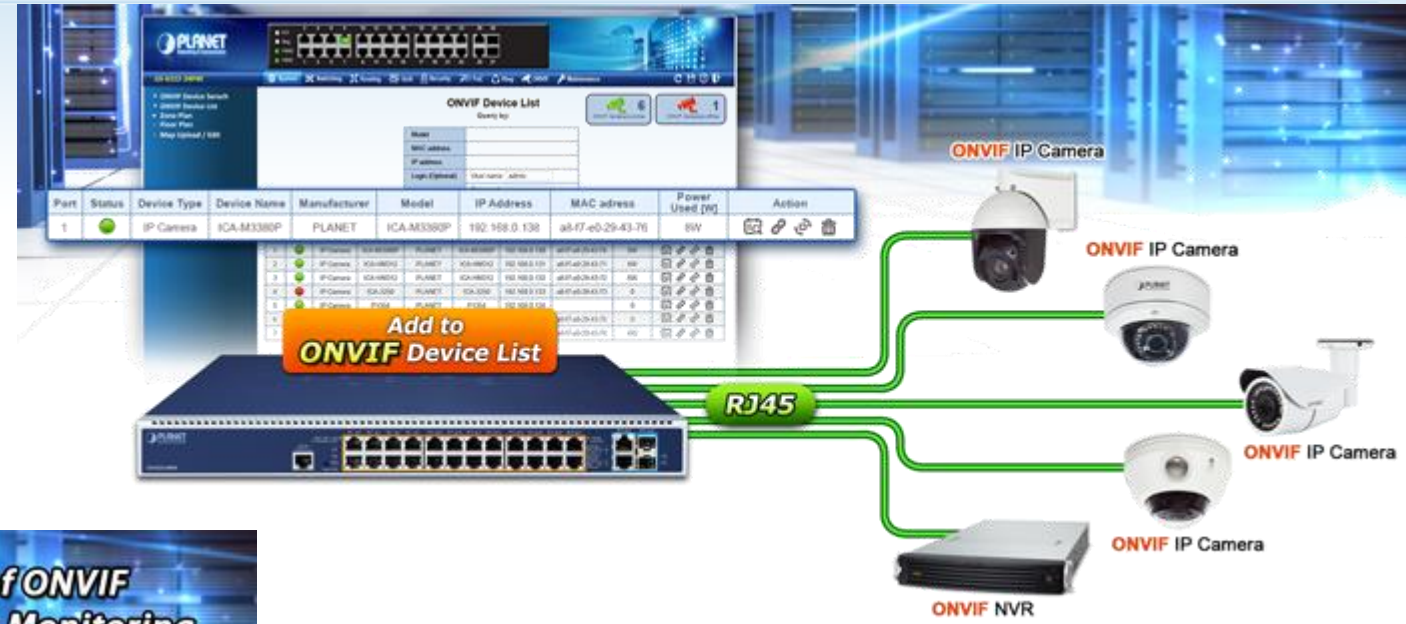
Metody:

- + aktivní detekce koncových prvků
- + měření délky UTP kabelů (TDR)
- + scheduler PoE napájení



Pokročilé funkce PoE

ONVIF modul pro detekci a monitoring...



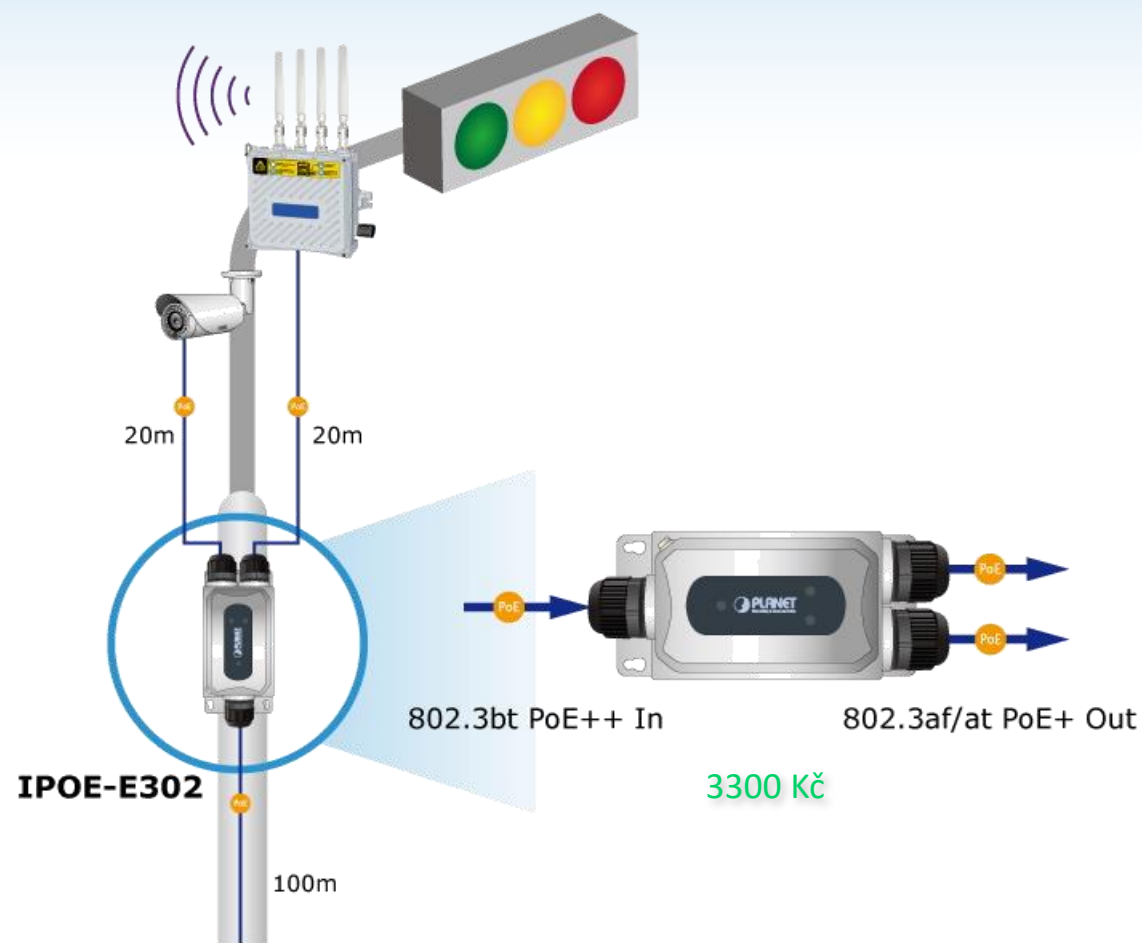
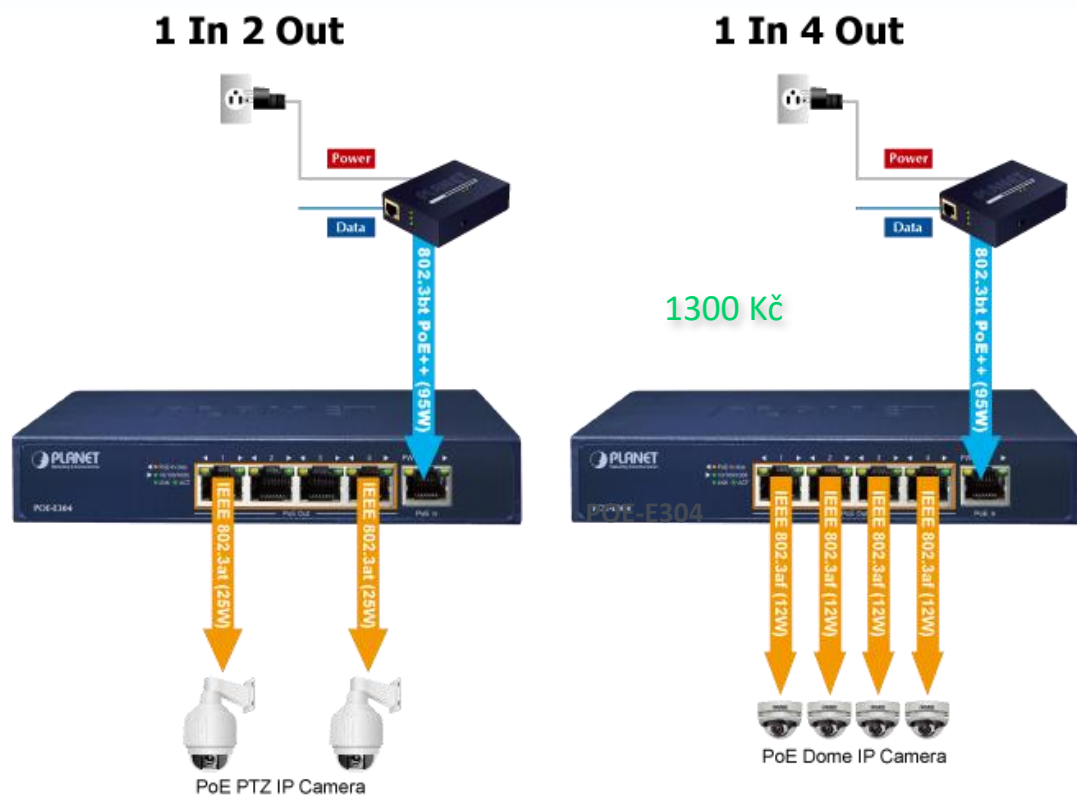
The screenshot displays the PLANET web interface for 'eMap of ONVIF IP Camera Monitoring'. It features a floor plan map with a red location pin and a hand cursor pointing to a specific area. A detailed information panel for 'Port 1' is shown, listing device details and power usage.

Port 1	
Device Name	11F Demo Room
Model	ICA-M3380P
IP address	192.168.0.20
MAC address	A8:F7:E0:11:22:33
PoE Used	12.3W
VLAN	1

Below the information panel are icons for 'Web Page', 'PoE Reboot', and 'Snapshot', along with a small video thumbnail of a conference room.

Výkonné PoE extendery

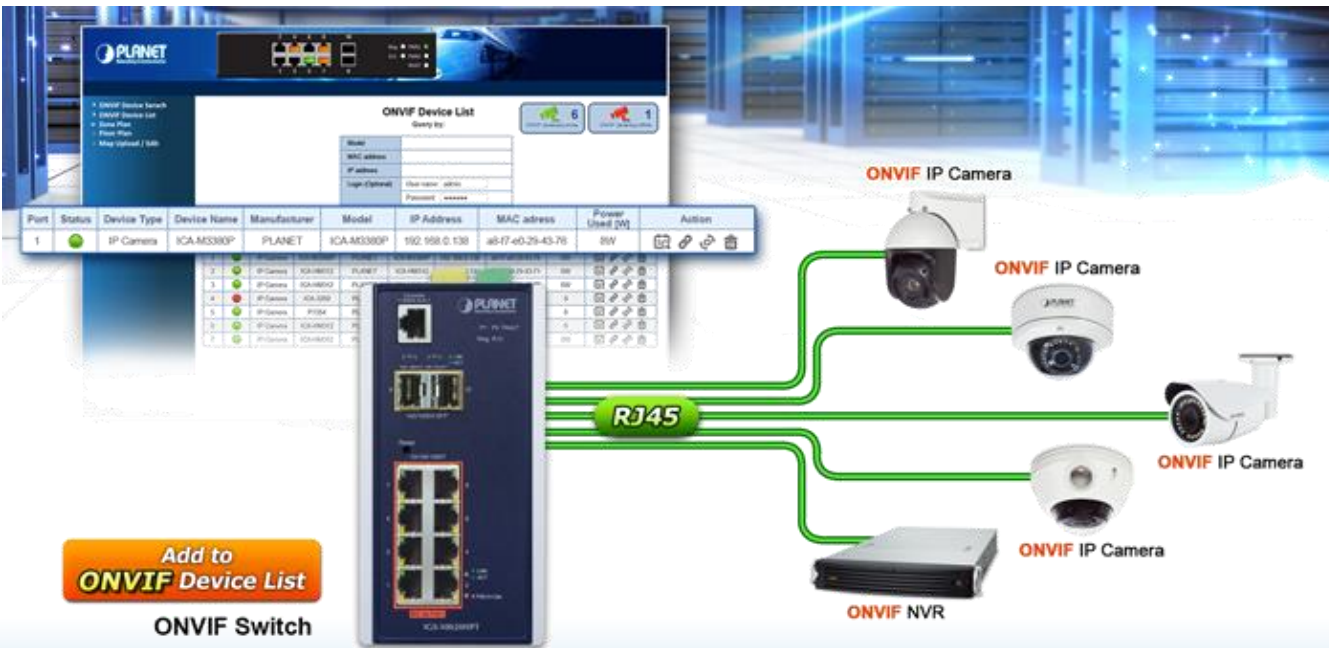
Pro vložené napájení na nepřístupných místech...



Automotive PoE přepínač

IGS-10020HPT

- **Porty:** Gigabit 8x RJ-45 + 2x SFP
- **Průmyslové provedení s homologací E24**
- běžné síťové funkce a protokoly včetně L3 statického routování
- PoE scheduler a ICMP ping detekce na portech
- ONVIF modul pro přímý monitoring IP kamer
- napájení **DC 12-48V**



— PoE — 100BASE-TX UTP with PoE
— PoE — 1000BASE-T UTP
— PoE — 1000BASE-T UTP with PoE

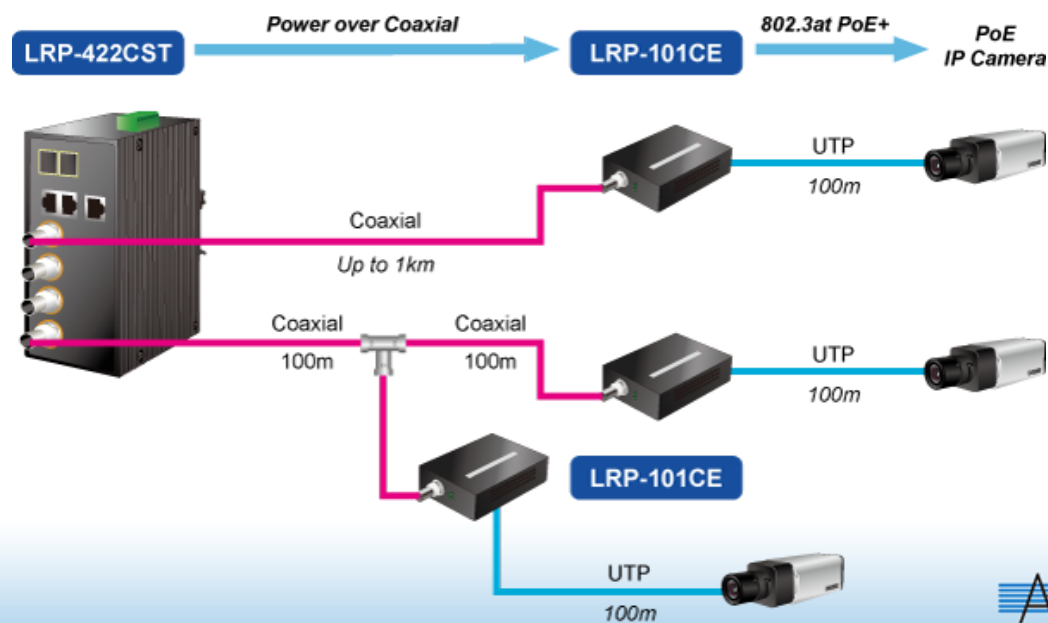
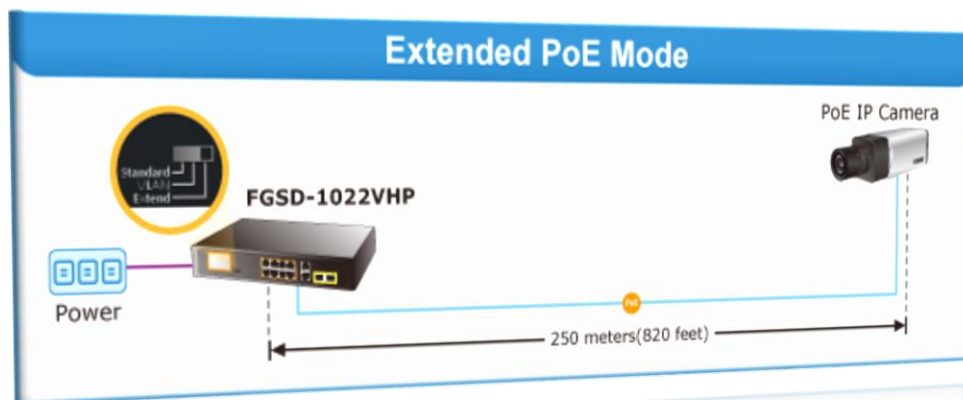
Delší segmenty s napájením PoE

a) **extendery** (násobné pospojování) x 100m

b) **přímá spojení** (10Mb spojení) 200~800m

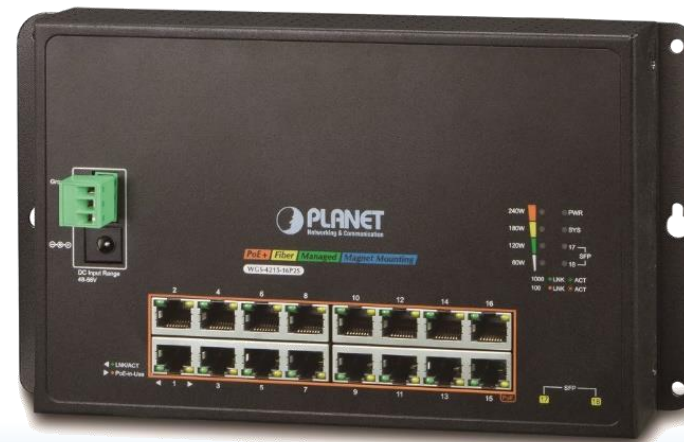
- vhodné v CCTV aplikacích zvláště ve spojení s ICMP detekcí (reakcí na PING)
- Planet (Extended PoE) dle IEEE 10Base-T, 10Mb/s < 250m
- Dahua (ePOE) vychází z BroadR-Reach, 10~100Mb/s < 800m

c) **koaxiální ethernet** (EoC, LRP) ~1km



Fanless PoE přepínače

- ✓ vždy bez ventilátorů
- ✓ podpora Extend módu pro spojení do 250m při 10Mb/s
- ✓ portové VLANy
- ✓ v nabídce přes 20 modelů



Hardware pro SMB & ENT & DCS

Planet Technology Corp.

- světově známá firma s globální distribucí
- v některých IT oblastech stále inovátorem
- referenční návrhy zařízení z kvalitních součástek (vývoj USA/EU)
- posun zaměření od SoHo směrem k SMB, ENT i ISP
- ASM fakticky jako výhradní dovozce od roku 1996
- jeden z hlavních ekonomických motorů ASM min. do rozjezdu CCTV
- osobní vazby a kontakty



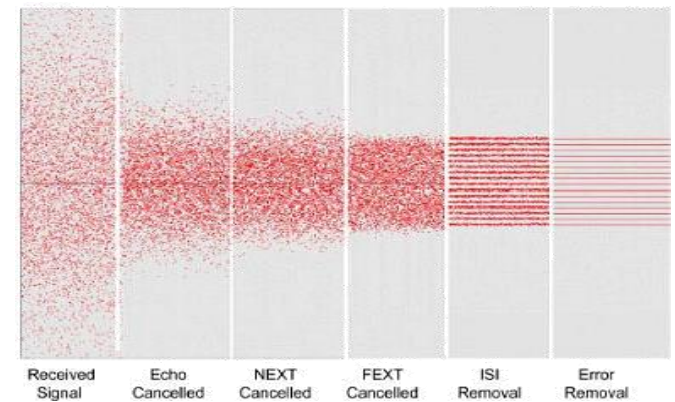
Přepínač – switch

- základní stavební prvek Ethernet sítí
- fyzicky zpracovává signály na rozhraní L1
- dekódovaná data na druhé vrstvě L2 třídí (dle MAC)
- dnešní spravovatelné modely analyzují provoz i na vyšších vrstvách (L3, L4)
- přidané funkce jako PoE, I/O, SSH přístup, LCD displej, ONVIF software



Čím se liší jednotlivé stroje??

- interně zapojením / čipovou sadou
- provedením ~ plošné spoje, použité součástky, napájení
- software / firmware
- spolehlivost kontra provozní podmínky



Přepínač – switch

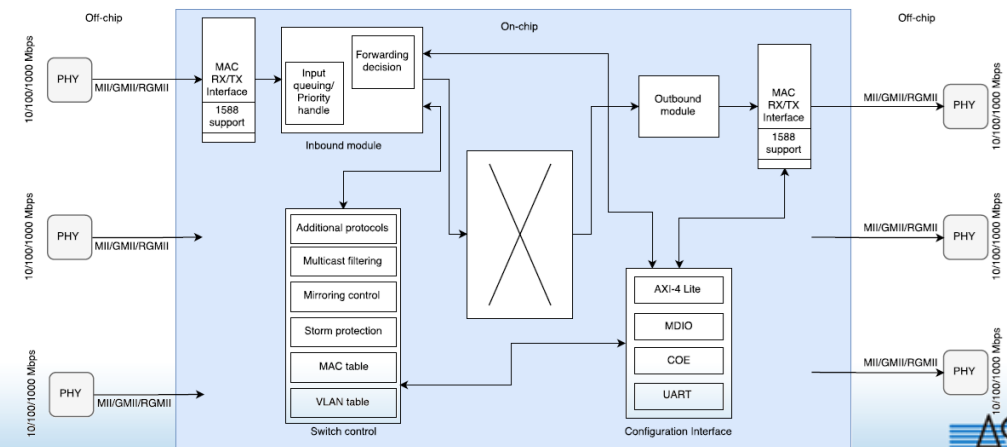
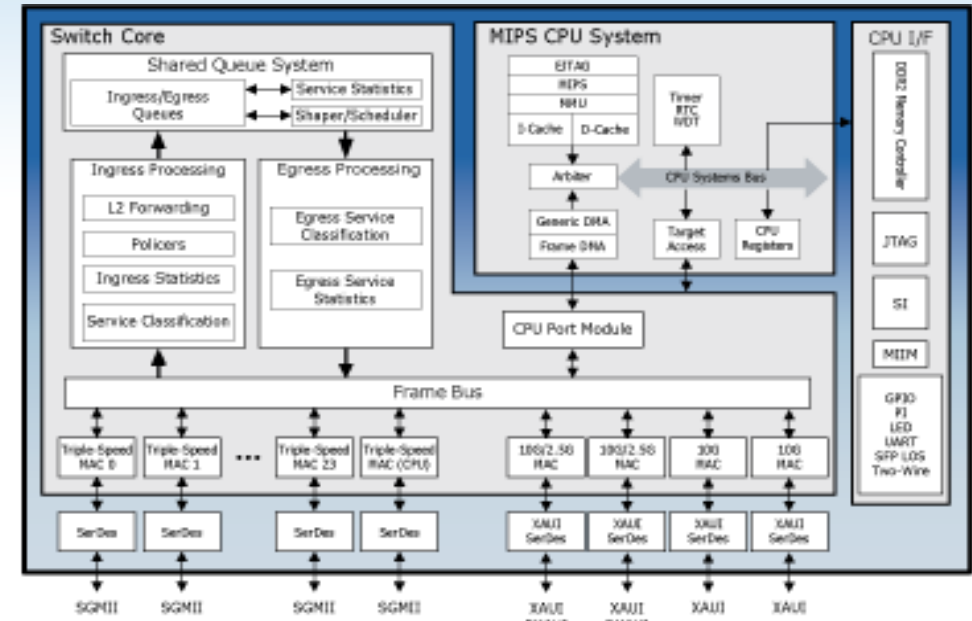
Dělení a architektura

- funkce
- rozhraní (porty)
- výkon

Planet hardware je stále vyráběný na základě návrhů skupin světových producentů čipových sad a řešení **BroadCom, Microchip (Vitesse), Realtek, Marwell.**

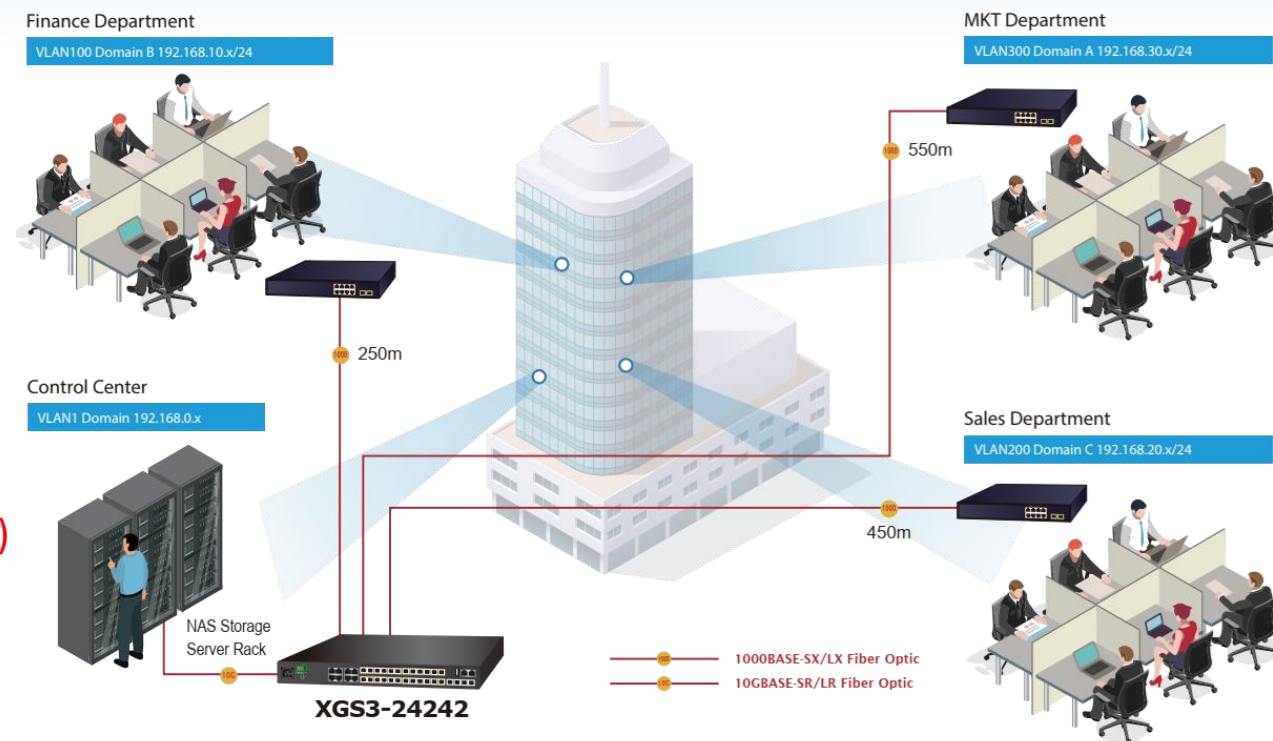
Prioritou je výkon, užitná hodnota v podobě funkcí a rozmanitost rozhraní, v neposlední řadě to je průmyslové provedení.

Velká část spravovatelných modelů implementuje hardware zpracování rámců a paketů.



Výběr pro SMB a ENT segmenty

- Dělení a výběr
 - dle rozhraní a výbavy
 - dle aplikačního segmentu SoHo, SMB, ENT, ISP
 - dle ceny
 - dle výrobce?
- Dnešní funkční výbava je absolutní
- Pro SMB a ENT segmenty extra priority výběru
 - funkce primárního využití (VLAN, filtrování, 802.1X, SNMP)
 - výkon / rozhraní
 - lifetime produkce a technická podpora
 - záruka a servis



Funkce switchů SMB / ENT segmentů

Základní / zásadní funkce pro (bezpečnější) firemní provoz

- L3 routing nad VLAN IEEE 802.1Q
- SNMP správa s šifrováním SSH/SSL
- Clustering a stohování
- Kruhové topologie Spanning tree (STP/RSTP/MTSP) a ERPS ring
- Virtualizace na vrstvách L2 a L3 modelu OSI
- QoS řízení provozu včetně shapingu
- ACL filtrace na úrovni MAC/IP/TCP/UDP
- RADIUS 802.1X a TACACS (Cisco ~ RFC 1492) autentizace připojených stanic
- IGMP multicast
- podpora IPv6 (L3 routing)
- DHCP snooping
- PoE ovládání
- měření kabeláže účastnických přípojek 😊

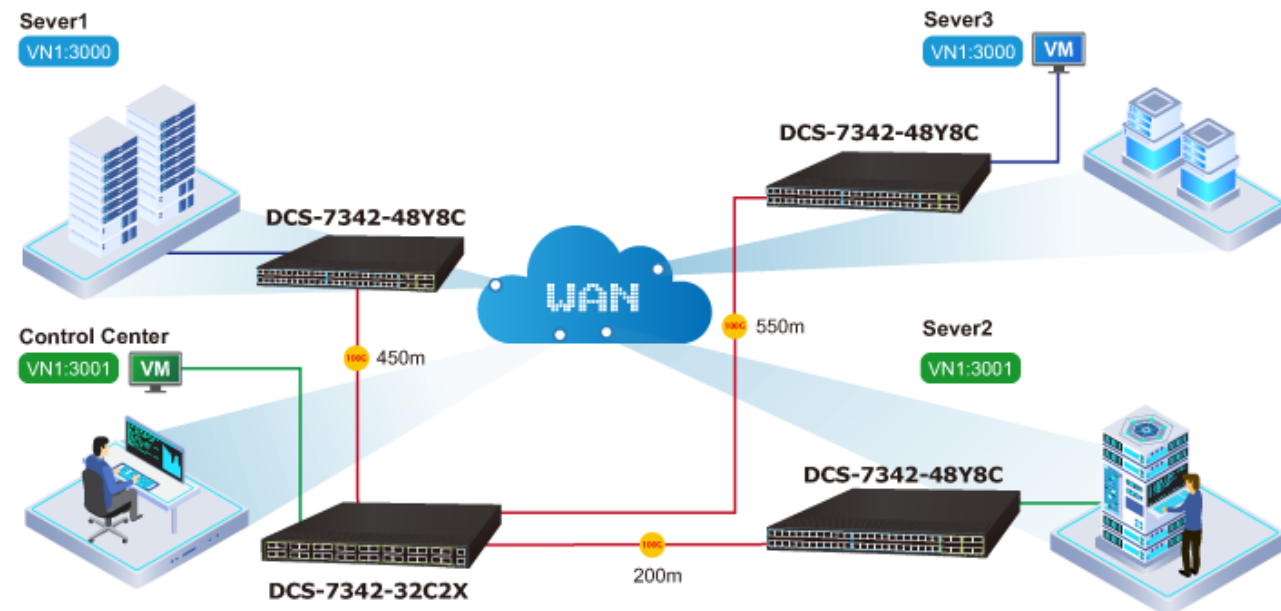
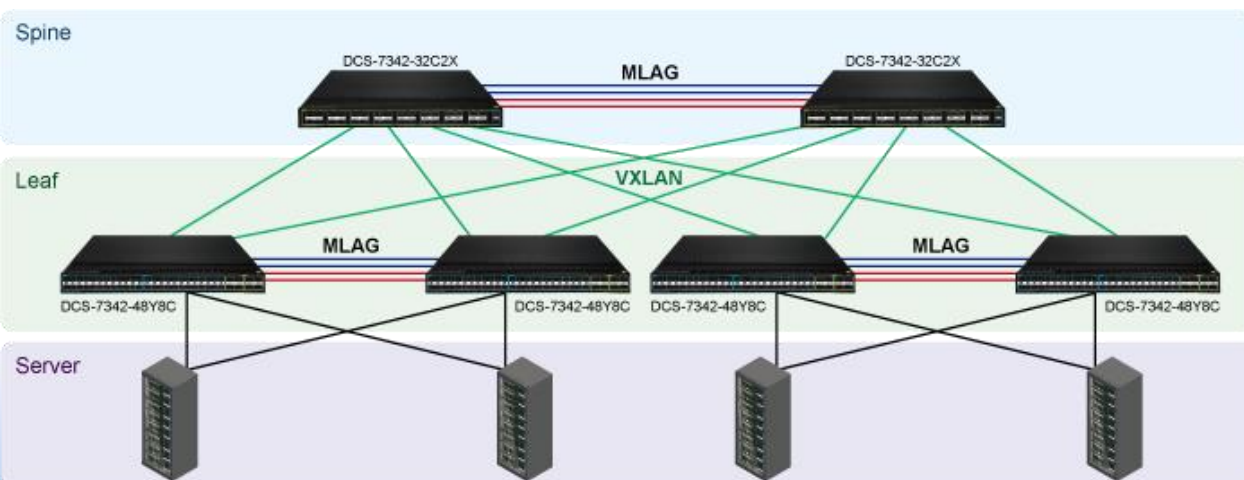
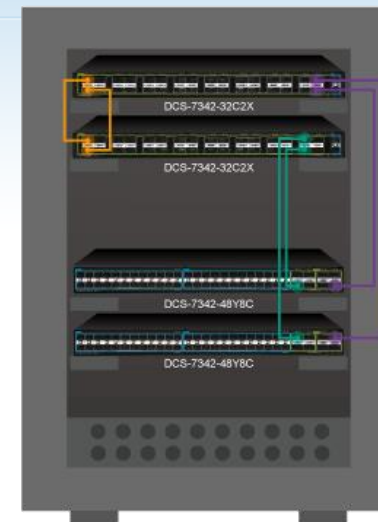
Provozní požadavky na infrastrukturu

- VLAN a L3 subsítě dle oddělení (obchod, sklad, public) a dle provozů (CCTV, VoIP, RDP, internet ano/ne)
- Vrstvy v rámci infrastruktury (core -> distribuce -> koncové připojení -> uživatelé)
- Zajištění provozu u kritických částí LAN ~ High availability (HA)
- Bezpečnost provozní (ACL) a uživatelská (RADIUS/TACACS)

Switche pro DCS segment

Provozní požadavky na switche datových center

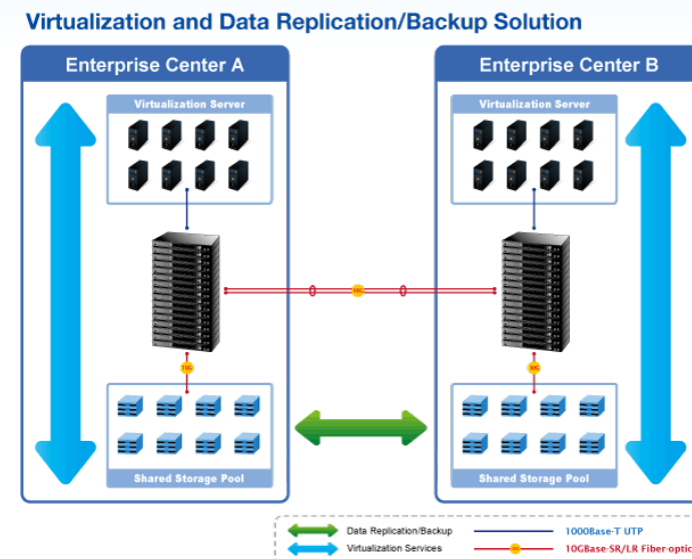
- Koncentrace rychlých (standardních) rozhraní
- Funkce pro ovládání L2, L3, L4 provozu
- L3 routing OSPF a BGP
- Propustnost a záloha prvků pomocí MLAG (Multi-chassis Link Aggregation Group)
- Podpora VXLAN (Virtual Extensible LAN dle IETF/RFC7348) pro virtuální prostředí
- Agregace správy do celků pomocí hardware stohování
- HA (high availability) na úrovni hardware včetně napájení
- Výkonné QoS a ACL (access control list) filtrace



Vlastnosti a funkce přepínačů

Význačné fyzické vlastnosti Planetů

- vývojem škála fyzických portů (10~100Gbit, (Q)SFP+, PoE)
- Stack – hw stoh nebo IP
- PoE napájení s možností 10Mb/s „extend“ módu
- centralizovaná správa UNI-NMS (Universal Network Management System)
- dotykový LCD displej
- ONVIF monitoring
- průmyslové a automotive provedení s certifikacemi (EN50155)
- fanless provedení bez ventilátorů nejen SoHo a DIN modelů
- redundantní zdvojené napájení



Novější značení přepínačů

xGS-4210-24y4z



Kategorie přepínače

- GS – Standardní
- XGS – 10G
- MGS – Metro
- IGS – Průmyslové
- SGS – Stohovatelné

Funkce

- 2 – L2 Web Smart
- 3 – L2
- 4 – L2/L4
- 5 – L2+ w/ routování

OSI vrstva

- 2 – L2
- 3 – L3

Použitý chipset

- 1 – Realtek
- 2 – Microchip (Vitesse)
- 3 – Marvell
- 4 – Broadcom
- 5 – Cavium (Marvell)

Počet hlavních portů

- 8 – 8-portů
- 24 -14-portů
- 48 – 48-portů

y: Main Port Type

- T – 10/100/1000Base-T
- P – 802.3at PoE+
- PL – 802.3at PoE+ / výkonný
- S – 100/1000Base-x SFP slot

Z: Port Type

- S – 100/1000Base-X SFP slot
- C – TP/SFP Combo interface
- X – 10G SFP+

Páteřní přepínače 10, 40 až 100GbE

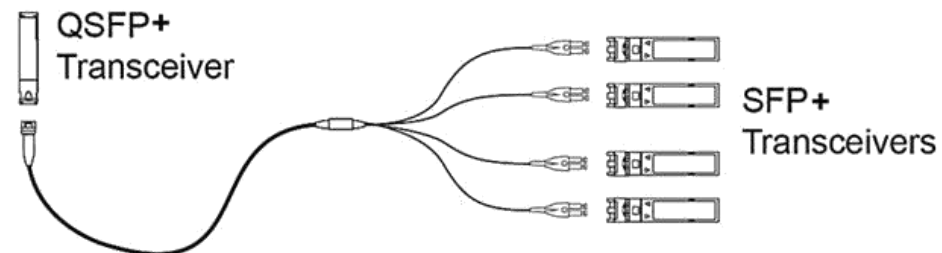
Společné vlastnosti:

- ASIC hardware switching i routing
- multiport a 40 nebo 100GbE agregační porty
- L3 dynamic routing (RIP, OSPF, BGP), veškeré funkce
- dual power-in



PLANET xtended serie

- **PLANET XGS-5240-24X2QR**, 24x 10G SFP+, 2x 40G QSFP+
- **PLANET XGS-6350-12X8TR**, 12x 10G SFP+, 8x GbE RJ-45
- **PLANET XGS-6350-24X4C**, 24x 10G SFP+, 4x 40/100G QSFP+/QSFP28
- **PLANET XGS-6350-48X2Q4C**, 48x 10G SFP+, 4x 40/100G QSFP28, 2x 40G QSFP+
- **PLANET XGS-6320-12X4TR / XGS-6320-8X8TR**
12x 10G SFP+, 4x 10G RJ-45
8x 10G SFP+, 8x 10G RJ-45



Podpora dělení QSFP+ portů na 4 linky po 10Gb

Stohovatelné přepínače 10GbE

PLANET stackable série

- **SGS-5240** (BroadCom) - L3 static routing, fanless 24-port ☺
- **SGS-6341** (Marvell) - L3 dynamic routing, VSF clustering
- **SGS-6310** (Realtek) – L3 dynamic routing, VSF clustering

Společné funkce a vlastnosti

- hardware stacking 10GbE
- vybrané řady VSF clustering
- ASIC hardware switching i routing
- nabídka rozhraní 24~48portů, včetně SFP+ 10GbE uplink
- včetně multi SFP nebo PoE
- komplexní výbava všemi síťovými funkcemi
- včetně ERPS, STP a LACP protokolů

Hardware Stacking

Up to 8 units with SGS-6310 Series



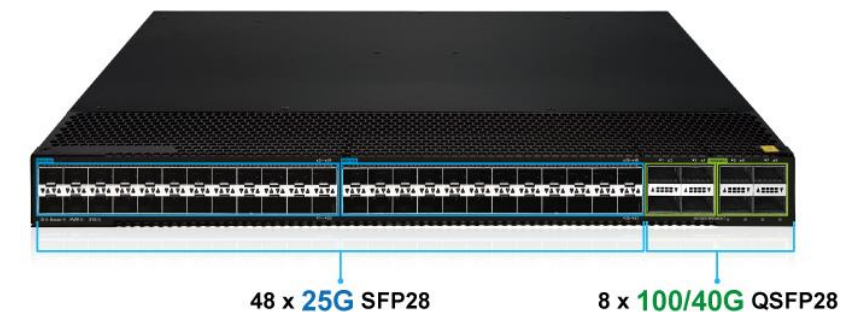
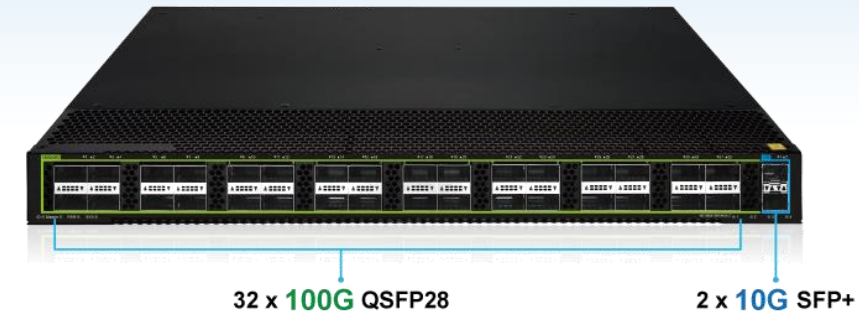
Páteř ve firmě s nimi pořešíte!

Switche pro DCS segment

DCS-7342-32C2X: 32x 100GbE QSFP28, 2x 10GbE SFP+ (sběrnice 6,4Tb/s)

DCS-7342-48Y8C: 8x 100GbE QSFP28, 48x 25GbE SFP28 (sběrnice 4Tb/s)

- hardware L2 přepínání a L3 routování (BFD, VRRP, OSPF, IS-IS, BGP, PM-DM)
- hardware stohování včetně spojení do kruhu
- Broadcom ASIC
- Podpora VXLAN včetně EVPN
- MLAG agregace portů, včetně běžných LACP, STP všech verzí
- IGMP a MLD multicast a MVR (Multicast VLAN)
- ACL filtrace na vrstvách L2, L3, L4
- Autentifikace prostřednictvím 802.1x, Radius, Tacacs+
- Pravidla ochrany proti DDoS pro každý port
- SNMP řízení přístupu



Modulární přepínač

PLANET CS-6306R

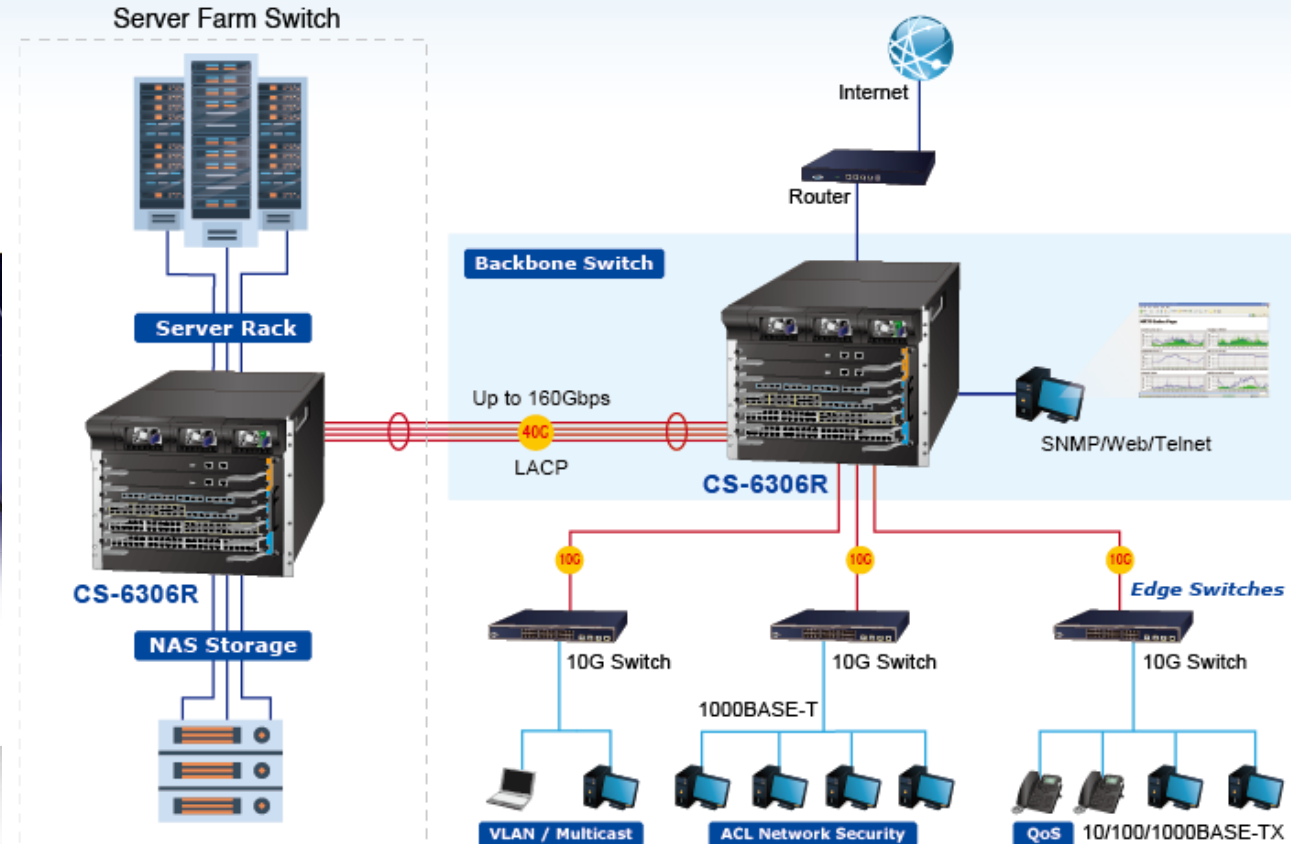
- Sběrnice 3Tb/s
- Dynamický routing včetně IPv6
- 6x šachet pro instalaci modulů

Incredibly Huge Bandwidth for Core Networking

192xTP 192xSFP 64x10G 16x40G

CS6-S24T24S 24G + 24G CS6-S16X 16x10G CS6-S24T8X 24G + 8x10G CS6-S48T 48G

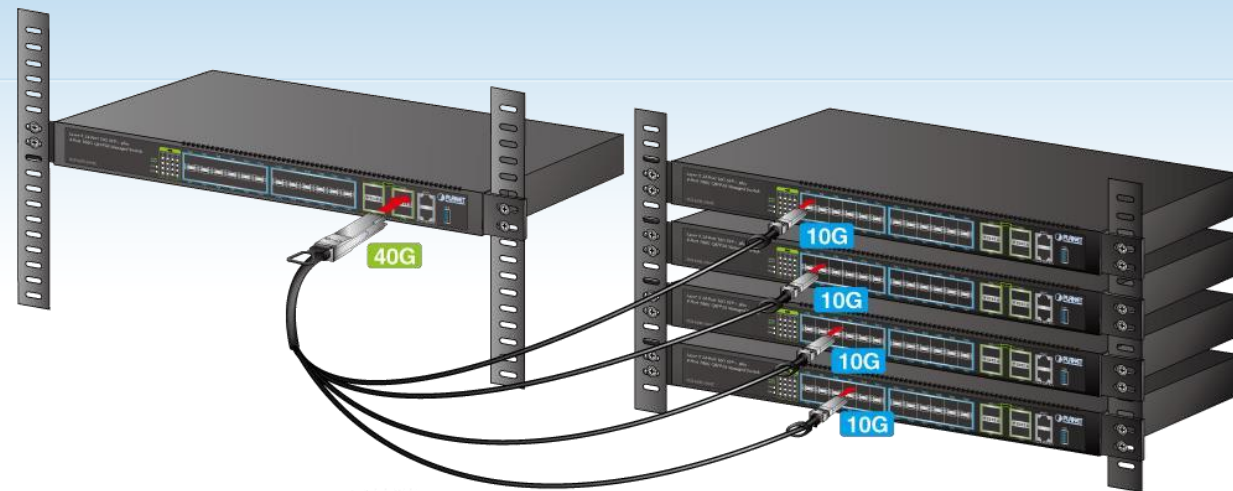
Extremely Flexible, Scalable and Resilient Chassis-based Switch
6-slot Layer 3 IPv4/IPv6 Routing Chassis Switch **CS-6306R**



Propojení 40GbE na 4x 10GbE

Standardní funkčnost QSFP+ portů:

- 40G port může být přímo rozdělen na 4x 10G
- propojení 40G do 4x 10G je standardní funkčnost napříč výrobci
- porty nemusí být jen v přepínačích, totéž platí pro síťové karty
- připojovaný switch může být jakýkoliv s 10G SFP+ portem
- propojení lze provést metalickou nebo optickou cestou



Několik možností propojení:

a) do 5m, metalický (pasivní) rozbočovací kabel (DAC) např. **Planet CB-QSFP4X10G**

b) do ~25m, optický (aktivní) rozbočovací kabel (AOC)
Má pevně připojené QSFP a SFP+ moduly. Délku musíte stanovit při objednání.
Délky jsou možné až do 100m ale obtížné na manipulaci.

c) do 150m a délku si určujete sami
XL-MQB-SR4 (MPO konektor) -- FOP-MPOMLC12PC-x-OM4 -- 4x XL-MTB-SR
Výhody: délku prodloužíte MPO-MPO kabelem nebo jednotlivé větve LC-LC kabely;
snadno opravíte/nahradíte; standardní komponenty



Průmyslové aktivní prvky

- robustní provedení se zvýšeným krytím, ocelová nebo hliníková skříň
- jsou odolné proti pádu (IEC-60068-2-32) z výšky 75cm na všechny dopadové části
- jsou odolné proti vibracím (IEC-60068-2-6) 10-500-10Hz, 4g, 0,5oct/min
- jsou odolné proti přetížení a krátkodobému zrychlení 50g, dlouhodobému 4g (IEC-60068-2-27)
- ESD ochrana proti elektrostatické elektřině do 6kV DC (EN 61000-4-2, EN 61340-3-1)
- EFT proti rychlým přechodovým jevům do 6kV DC (IEC61000-4-4)
- EMI/EMS, elektromagnetická kompatibilita a slučitelnost dle CE EN-6100-4-2,3,4,5,6
- elektrická bezpečnost dle CE EN-60950
- pracovní teplota zpravidla -10 až 60°C, rozšířená -40 až 75 °C do prostředí o vlhkosti do 95%
- instalace na DIN lištu nebo na zeď
- vždy bez ventilátorů (fanless)
- redundatní napájení (zpravidla 12 až 48V DC) s ochranou proti přepólování
- 2x delší MTBF (střední doba mezi poruchami) při rozšířených pracovních teplotách

Průmyslové aktivní prvky



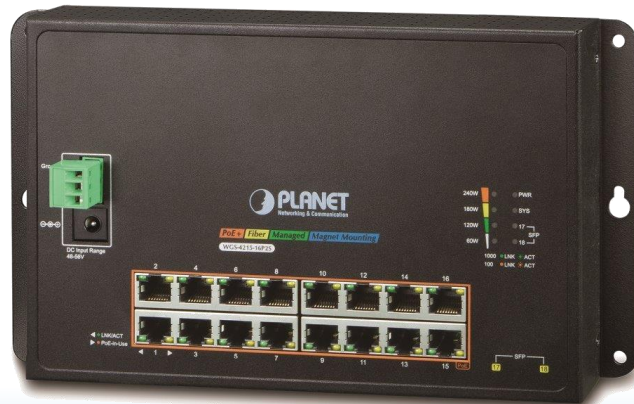
IFB-244-SLC
bypass switch



WGR-500-4PV
GW+firewall



IGS-5226-4P2T
IP67+EN50155



WGS-4215-16P2S
Flat fanless PoE



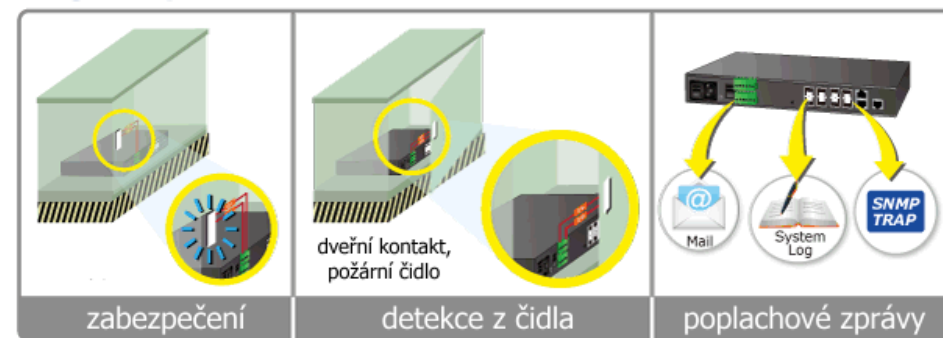
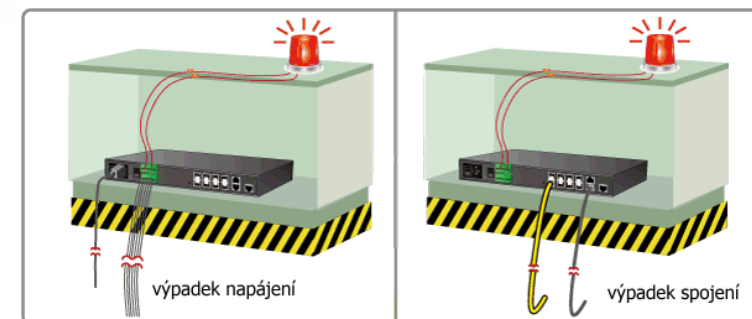
IGS-6325-8T8S4X
multiport SFP, 4x 10GbE



ICG-2515W-NR
5G router+WiFi+GPS

Metro přepínače

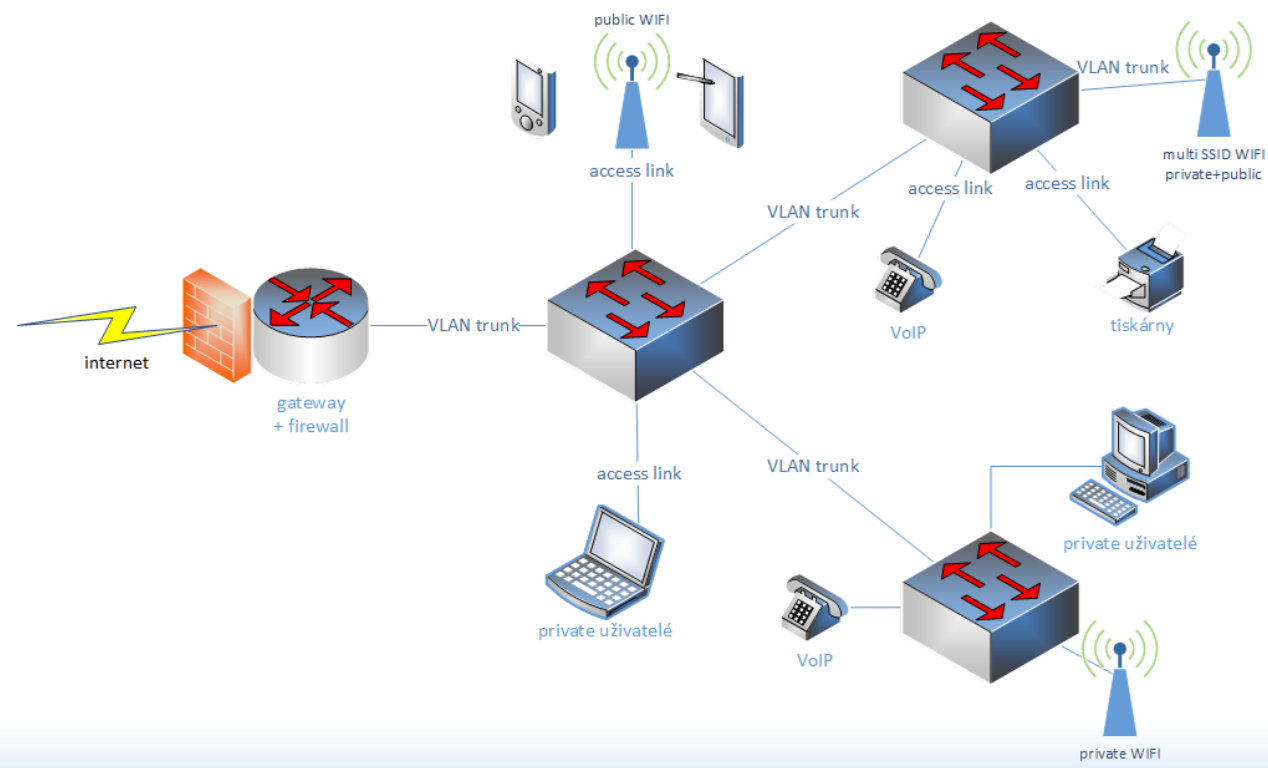
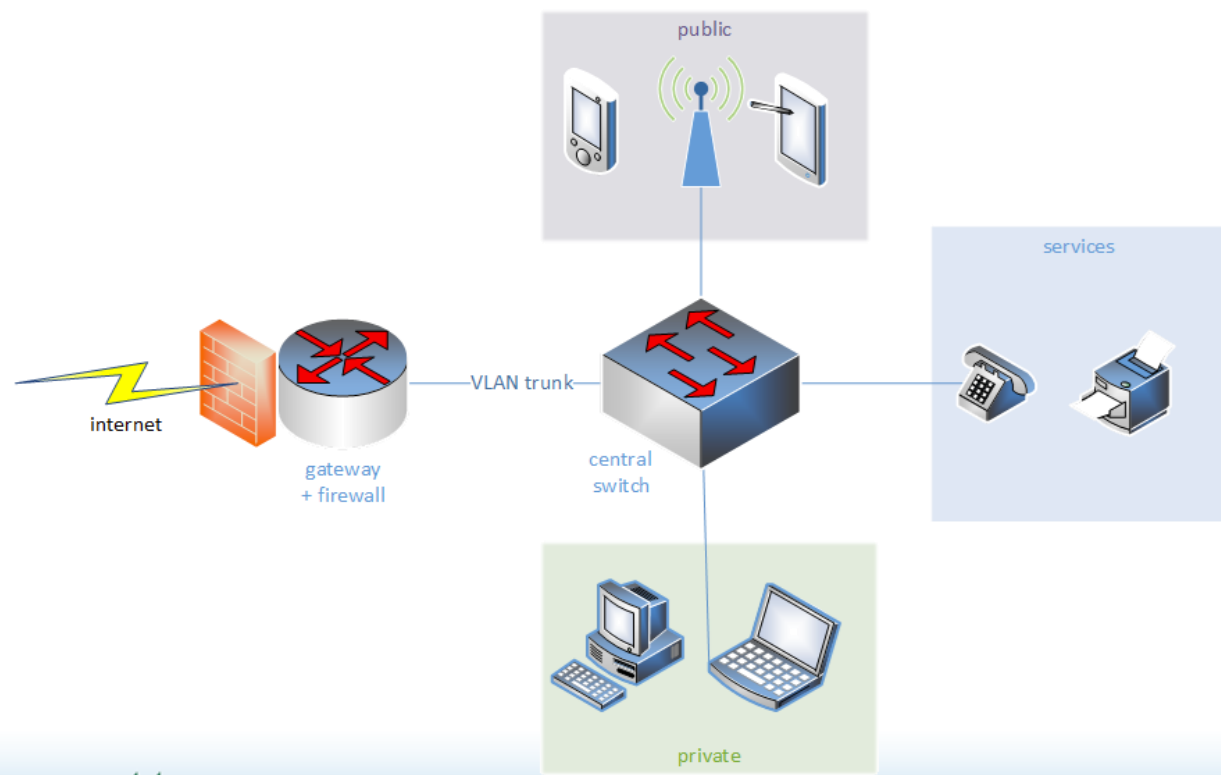
- páteřní infrastruktura pro budování „první míle“ (EFM)
- jednodušší (levnější) instalace a obsluha
- EMI/EMS elektromagnetická kompatibilita
- robustní provedení
- redundantní napájení
- I/O rozhraní
- zabezpečená správa (SSL/SSH)



Referenční použití přepínačů v praxi

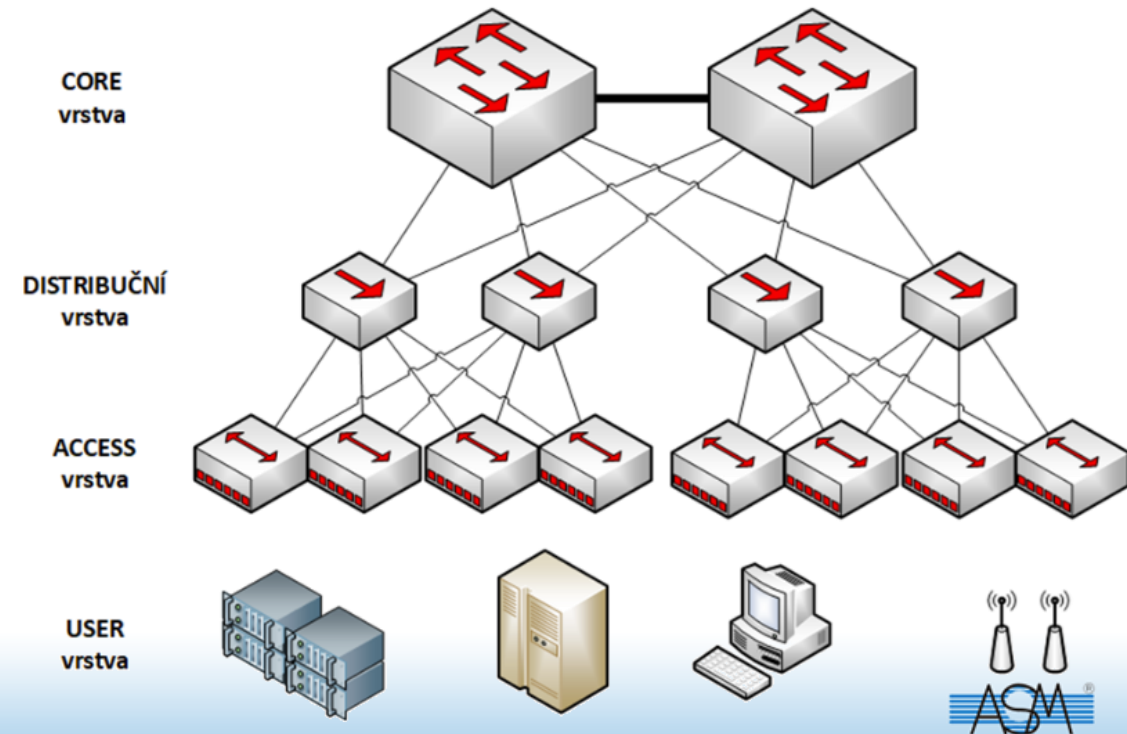
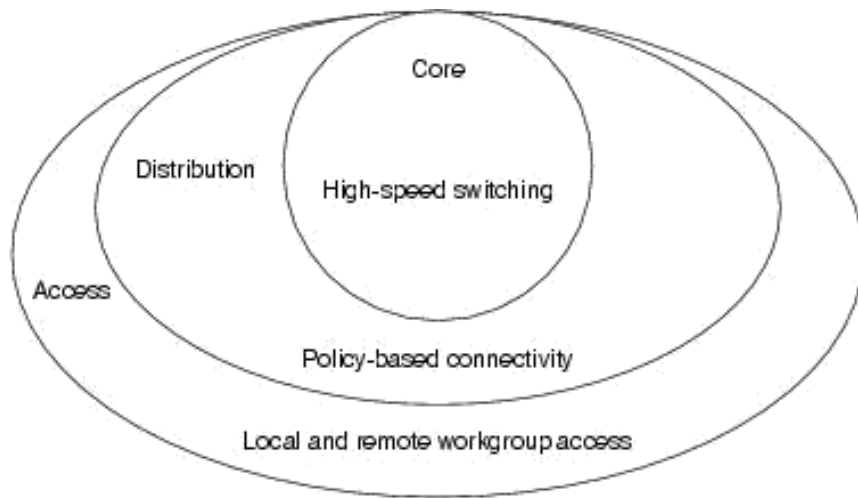
Tradiční „hvězda“ infrastruktura

- VLAN a L3 subsítě dle oddělení (obchod, sklad, public)
- a dle provozů (CCTV, VoIP, RDP, internet ano/ne)
- bezpečnost provozní (ACL) a uživatelská (RADIUS/TACACS)
- typické aplikace: restaurace, škola, SMB firma



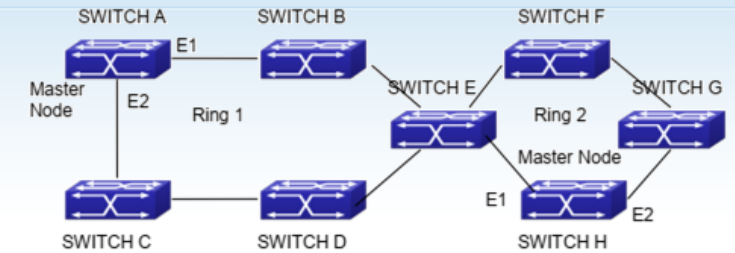
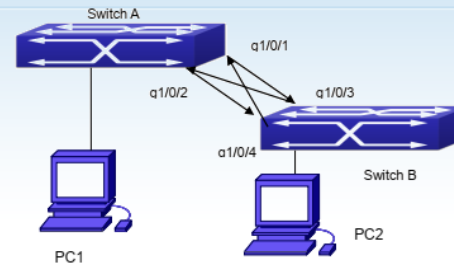
Kritická „hierarchická“ infrastruktura

- Vrstvy v rámci infrastruktury (core -> distribuce -> koncové připojení -> uživatelé)
- Zajištění provozu u kritických částí LAN ~ High availability (HA)
- Bezpečnost provozní (ACL) a uživatelská (RADIUS/TACACS)
- Není třeba zdvojení na všech vrstvách ~ dle provozních potřeb
- Typické aplikace: Ent databáze a SAN, části sítí výrobních provozů nebo obsluha online skladů
- Na straně serverů VM „teaming“ ~ OS / software

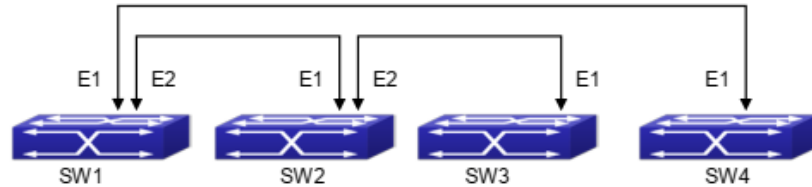


Kruhové topologie pro záložní spojení

- Protokoly STP, ERPS, LACP – zálohovaná spojení

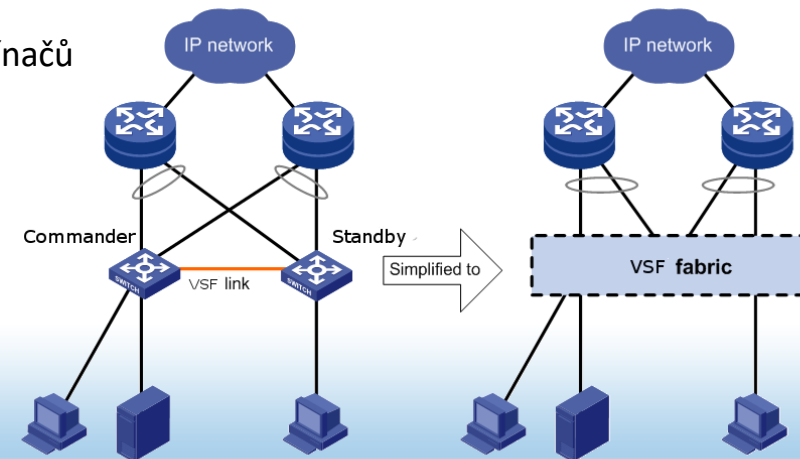


- Clustering a hardware stohování – provozní správa



- Virtualizace VSF (virtual switch framework) – komplexní spojení

- ✓ jednotná správa a řízené vícecestné spojení mezi členy VSF bez nutnosti použít protokoly detekce smyček STP apod.
- ✓ pokrytí výpadků některého z členů skupiny VSF clusteru
- ✓ rozložení zátěže, vyšší propustnost a sjednocené řízení v rámci VSF skupiny přepínačů
- ✓ funkce přibližující topologii SDN (software defined networking)

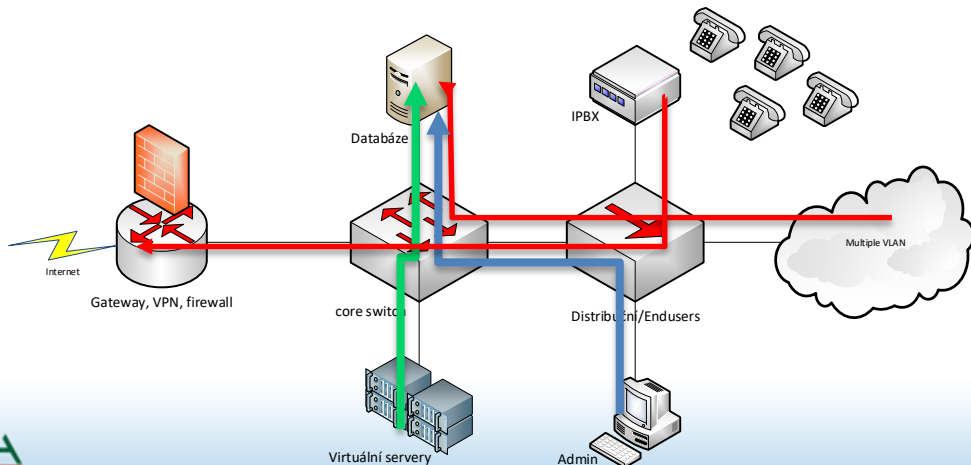


ACL filtrace

- ✓ switch jako L2 a L3 (hardware) dekodér
- ✓ filtrace na „prvním“ rozhraní (neohrozí okolí a naopak)

Příklad pustí pouze na WEB (443) z IP 192.168.1.238
+ další porty pro DHCP, DNS a PING na gateway:

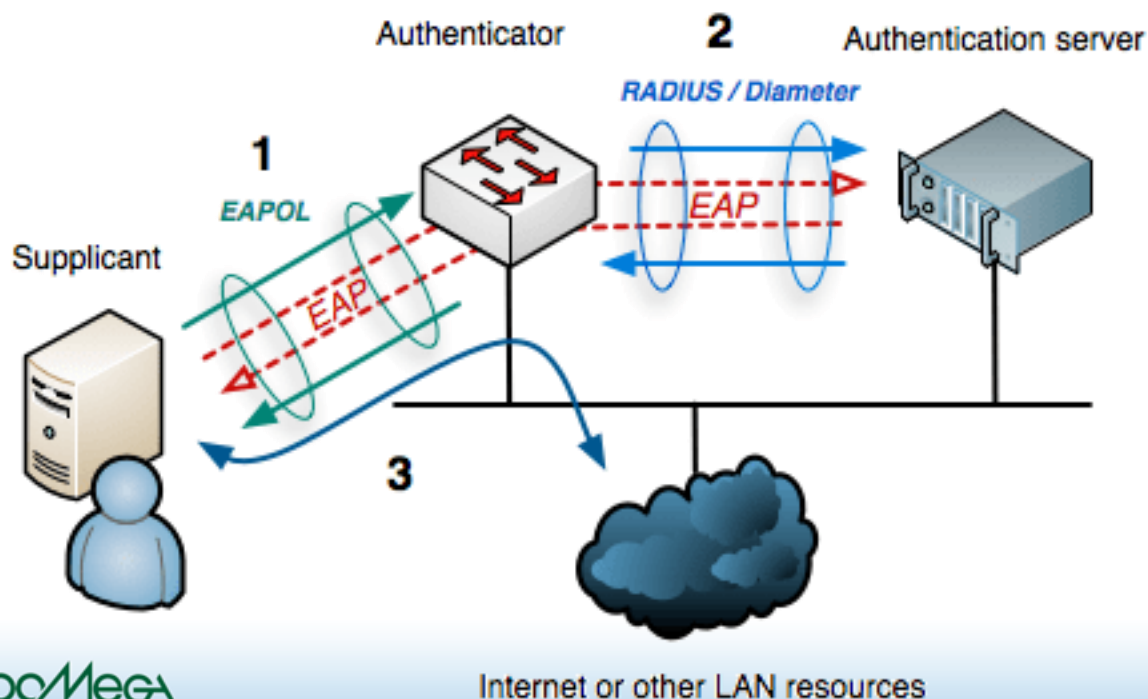
ACL Name	Sequence	Action	Protocol	Source IP Address		Destination IP Address		Source Port Range	Destination Port Range
				IP Address	Mask	IP Address	Mask		
test	2	Permit	icmp	Any	Any	192.168.1.1	255.255.255.255		
	3	Permit	tcp	Any	Any	Any	Any	Any	443
	4	Permit	udp	Any	Any	Any	Any	Any	53
	5	Permit	udp	192.168.1.238	255.255.255.255	Any	Any	67-68	67-68
	10	Deny	Any (IP)	Any	Any	Any	Any		



IPv4-Based ACE	
ACL Name	test
Sequence	(Range: 1 - 2147483647, 1 is first processed)
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny <input type="radio"/> Shutdown
Protocol	<input checked="" type="radio"/> Any(IP) <input type="radio"/> Select from list: icmp
Source IP Address	<input checked="" type="radio"/> Any <input type="radio"/> User Defined
Source IP Address Value	
Source IP Mask	(1s for matching, 0s for no matching)
Destination IP Address	<input checked="" type="radio"/> Any <input type="radio"/> User Defined
Destination IP Address Value	
Destination IP Mask	(1s for matching, 0s for no matching)
Source Port	<input checked="" type="radio"/> Any <input type="radio"/> Single 0 (Range: 0 - 65535) <input type="radio"/> Range 0 - 65535 (Range: 0 - 65535)
Destination Port	<input checked="" type="radio"/> Any <input type="radio"/> Single(Range: 0 - 65535) 0 (Range: 0 - 65535) <input type="radio"/> Range(Range: 0 - 65535) 0 - 65535 (Range: 0 - 65535)
TCP Flags	Urg <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Ack <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Psh <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Rst <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Syn <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Fin <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care
Type of Service	<input checked="" type="radio"/> Any <input type="radio"/> DSCP to match 0 (Range: 0 - 63) <input type="radio"/> IP Precedence to match 0 (Range: 0 - 7)
ICMP	<input checked="" type="radio"/> Any <input type="radio"/> Select from list: Echo Req <input type="radio"/> Protocol ID to match 0 (Range: 0 - 255)
ICMP Code	<input checked="" type="radio"/> Any <input type="radio"/> User Defined 0 (Range: 0 - 255)

Autentizace zařízení RADIUS 802.1X

- Řízení fyzického přístupu do sítí LAN na jednotlivých portech switchů
- Zabraňuje neautorizovaným osobám v přístupu k LAN
- Aplikuje se i nad WiFi klienty
- Lze kombinovat s ID kartami nebo certifikáty

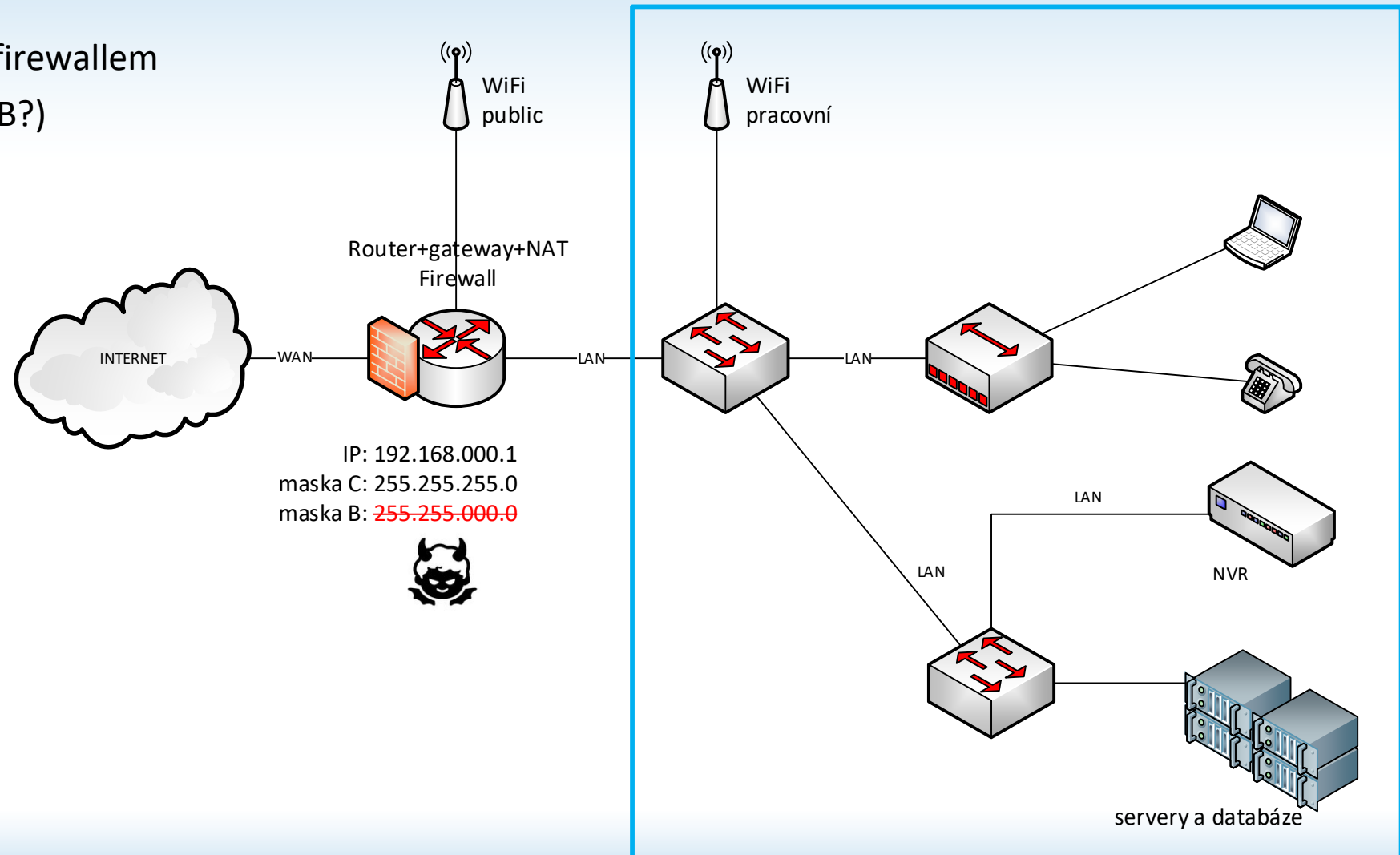


Server IP	192.168.1.200
Auth Port	1812 (0 - 65535)
Acct Port	1813 (0 - 65535)
Key String	<input type="checkbox"/> Use Default
Server Timeout	<input type="checkbox"/> Use Default 10 (1-30) secs
Server Retransmit	10 (1-30) secs
Server Priority	1 (0 - 65535)
Usage Type	<input type="radio"/> Login <input checked="" type="radio"/> 802.1X <input type="radio"/> All

GS-4210-24PL4C				System	Switching	QoS	Security	PoE	Maintenance
GE7	802.1X Disabled	-	Enable				3600	60	30
GE8	802.1X Disabled	-	Enable				3600	60	30
GE9	802.1X Disabled	-	Enable				3600	60	30
GE10	Authentication	Initialize	Disable				3600	60	30
GE11	Authentication	Initialize	Disable				3600	60	30
GE12	Authentication	Initialize	Disable				3600	60	30
GE13	Authentication	Initialize	Disable				3600	60	30
GE14	Authentication	Initialize	Disable				3600	60	30
GE15	Authentication	Authorized	Disable				3600	60	30
GE16	Authentication	Initialize	Disable				3600	60	30
GE17	802.1X Disabled	-	Enable				3600	60	30

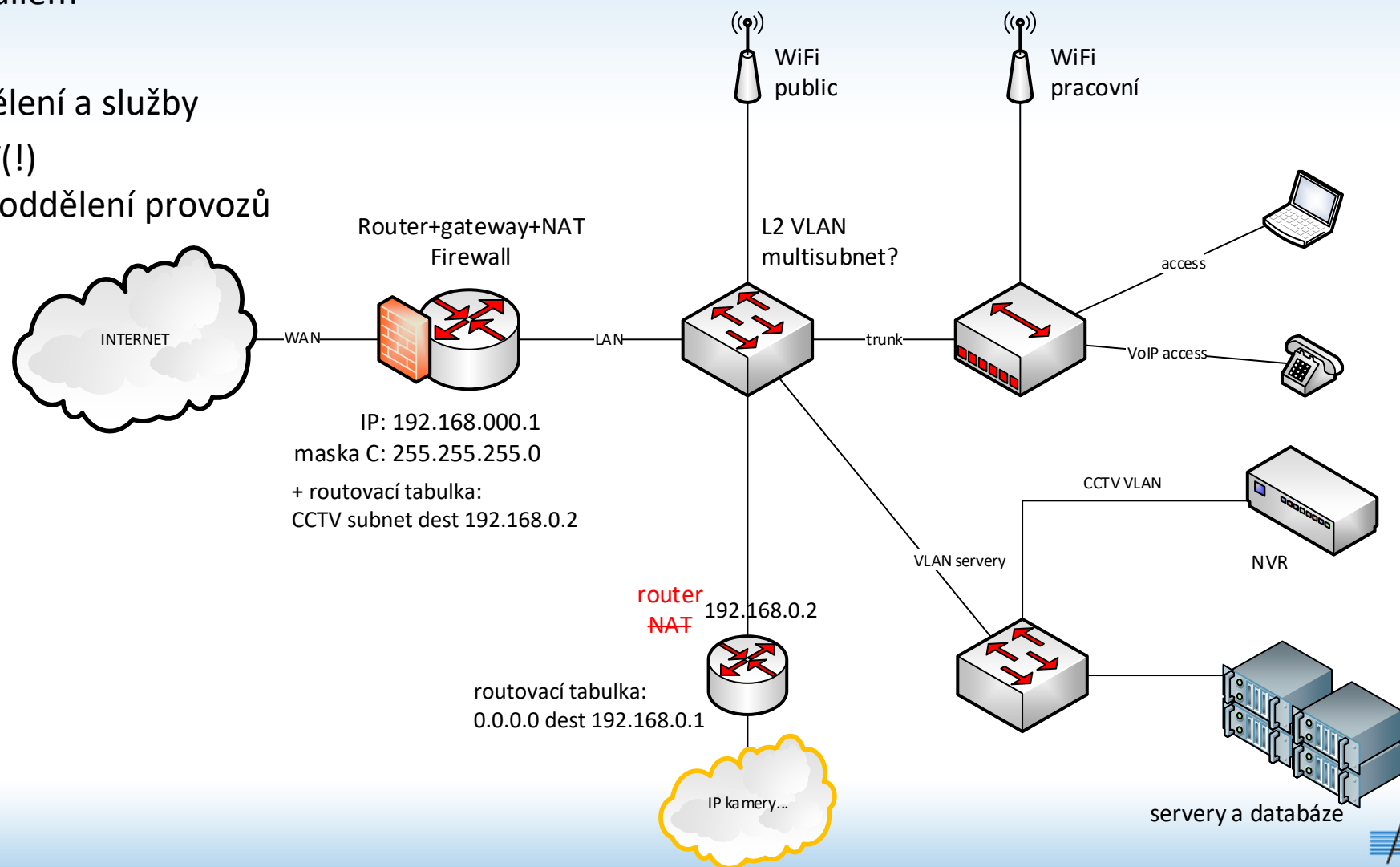
Firma včera

- ✓ GW router s NAT a firewallem
- ✓ jeden(?) IP subnet (B?)
- ✓ vše v jednom pytli



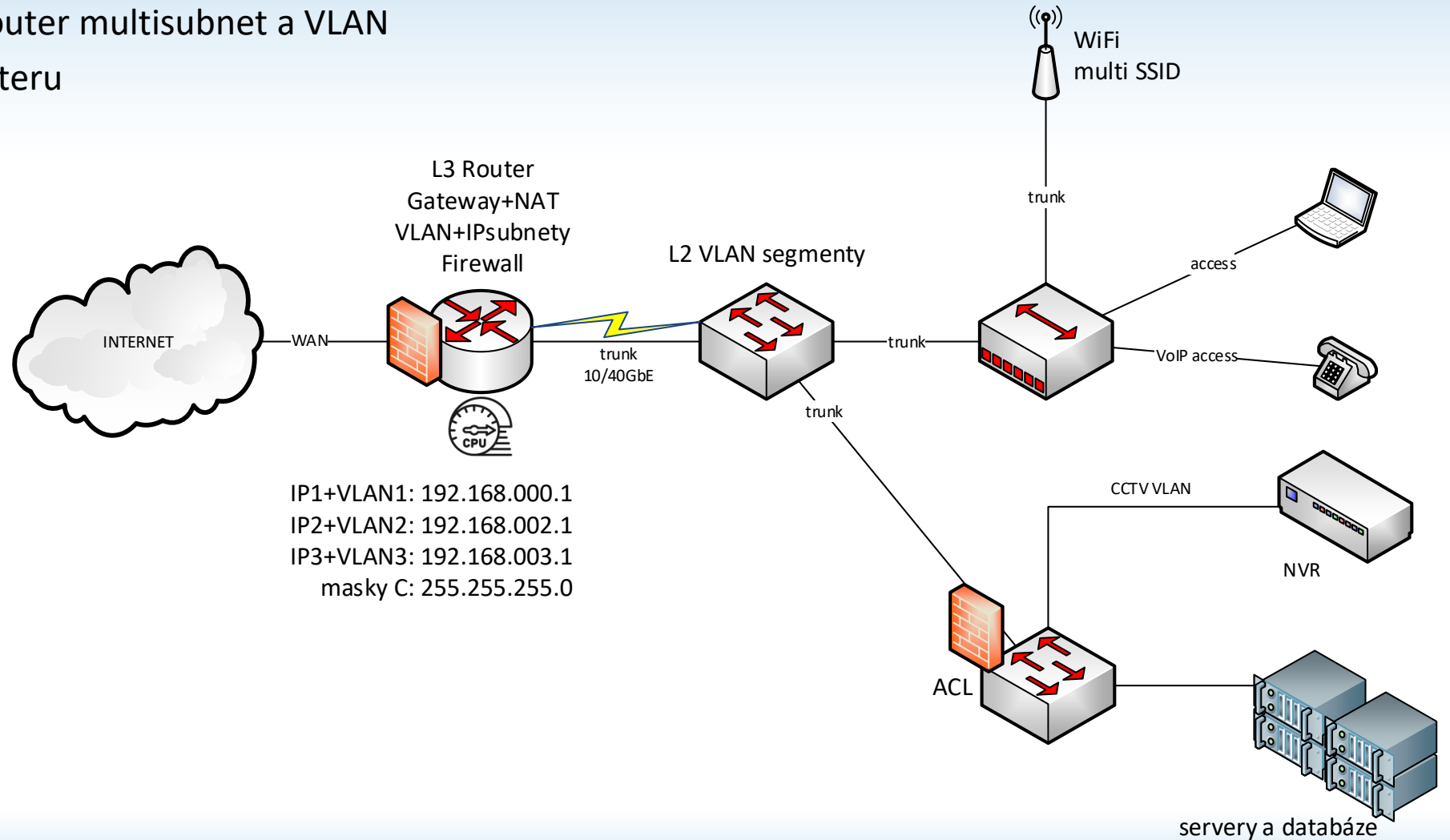
Firma dnes

- ✓ GW router s NAT a firewallem
- ✓ jeden(?) IP subnet
- ✓ VLAN segmenty pro oddělení a služby
- ✓ router pro CCTV bez NAT(!)
pomoc pro IP rozšíření a oddělení provozů



Firma zítřa

- ✓ GW s NAT a firewallem + router multisubnet a VLAN
- ✓ **centralizovaný** traffic v routeru
- ✓ náročné na výkon CPU
- ✓ rychlé trunk spoje
- ✓ ACL pro kritické segmenty
- ✓ WiFi multiSSID



IP subnet v routeru, VLAN síť

GW+router+definice VLAN

Multi-Subnet Configuration

Name	Network	DHCP Server
LAN Subnet 1	IP Address: 192.168.1.1 Netmask: 255.255.255.0	V
LAN Subnet 2	IP Address: 192.168.3.1 Netmask: 255.255.255.0	<input checked="" type="checkbox"/>
LAN Subnet 3	IP Address: 192.168.5.1 Netmask: 255.255.255.0	<input checked="" type="checkbox"/>
LAN Subnet 4	IP Address: 192.168.7.1 Netmask: 255.255.255.0	<input checked="" type="checkbox"/>

VLAN Configuration

VLAN: Enable Disable
 WAN Port: UNTAG
 WAN VLAN ID: 2

VLAN Table

Name	Subnet	VLAN ID	LAN Port 1	LAN Port 2	LAN Port 3	LAN Port 4	Action
Management Group	LAN Subnet 1 (192.168.1.1)		UNTAG	UNTAG	OFF	OFF	
VLAN3	LAN Subnet 2 (192.168.3.1)	3	OFF	TAG	OFF	OFF	
VLAN5	LAN Subnet 3 (192.168.5.1)	5	OFF	TAG	UNTAG	OFF	

Interface List

Interface	Type	Actual MTU	L2 MTU	Tx
R 1WLAN	Ethernet	1500	1596	
R 2LAN	Ethernet	1500	1596	
R vlan10	VLAN	1500	1592	
R vlan20	VLAN	1500	1592	

Address List

Address	Network	Interface
192.168.17.99/24	192.168.17.0	1WLAN
192.168.10.1/24	192.168.10.0	vlan10
192.168.20.1/24	192.168.20.0	vlan20



VLAN L2 switch

Edit Interface Setting

Port Select	Interface VLAN Mode	PVID	Accepted Type	Ingress Filtering	Uplink	TPID
Select Ports	<input checked="" type="radio"/> Hybrid <input type="radio"/> Access <input type="radio"/> Trunk <input type="radio"/> Tunnel	1 (1 - 4094)	<input checked="" type="radio"/> All <input type="radio"/> Tag Only <input type="radio"/> Untag Only	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	0x8100

Apply

Port VLAN Status

Port	Interface VLAN Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
GE1	Access	3	Untag Only	Enabled	Disabled	0x8100
GE2	Access	3	Untag Only	Enabled	Disabled	0x8100
GE3	Access	5	Untag Only	Enabled	Disabled	0x8100
GE4	Access	5	Untag Only	Enabled	Disabled	0x8100
GE5	Access	1	Untag Only	Enabled	Disabled	0x8100
GE6	Hybrid	1	ALL	Enabled	Disabled	0x8100
GE7	Hybrid	1	ALL	Enabled	Disabled	0x8100
GE8	Hybrid	1	ALL	Enabled	Disabled	0x8100
GE9	Hybrid	1	ALL	Enabled	Disabled	0x8100

Port VLAN Membership Table

Port	Mode	Administrative VLANs	Operational VLANs
GE1	Access	1F, 3UP	3UP
GE2	Access	1F, 3UP	3UP
GE3	Access	1F, 5UP	5UP
GE4	Access	1F, 5UP	5UP
GE5	Access	1UP	1UP
GE6	Hybrid	1UP, 3T, 5T	1UP, 3T, 5T
GE7	Hybrid	1UP, 3T, 5T	1UP, 3T, 5T

Multi SSID WIFI ve spojení s VLAN

Basic	Virtual AP1	Virtual AP2	Virtual AP3
Wireless Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Wireless Name (SSID)	WiFi1		
Hide SSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Wireless Mode	11 AX 20MHz		
Channel	6		
Encryption	WPA2 Personal (AES)		
Passphrase	Sifra123456789		
WiFi Multimedia	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
VLAN ID	1		

Basic	Virtual AP1	Virtual AP2	Virtual AP3
Wireless Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Wireless Name (SSID)	WiFi3		
Hide SSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Encryption	WPA2/WPA3 Personal		
Passphrase	Sifra123456789		
WiFi Multimedia	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
VLAN ID	3		

Basic	Virtual AP1	Virtual AP2	Virtual AP3
Wireless Status		<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Wireless Name (SSID)		WiFi5	
Hide SSID		<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Encryption		WPA2/WPA3 Personal	
Passphrase		Sifra123456789	
WiFi Multimedia		<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
VLAN ID		5	

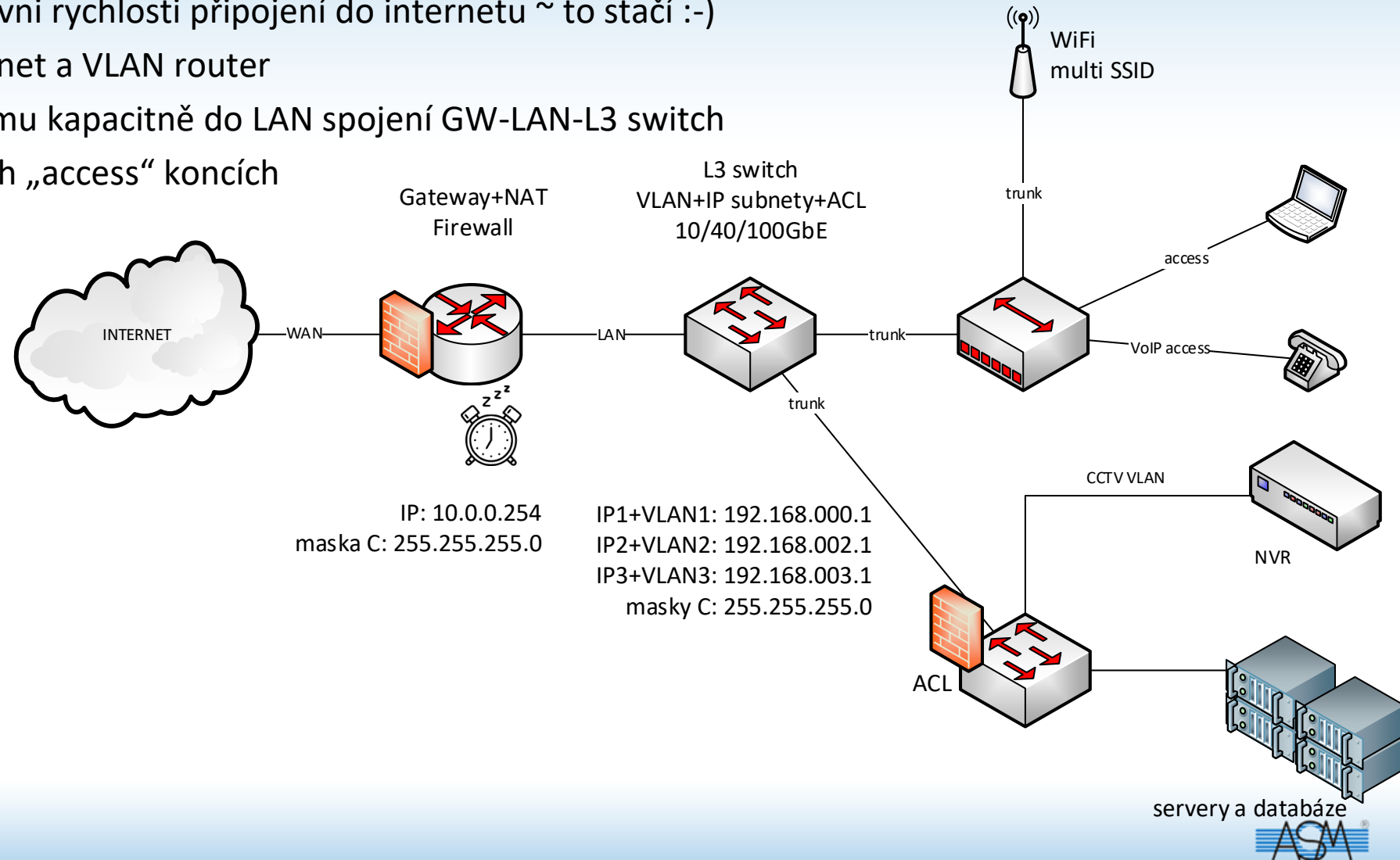
WiFi Advanced

2.4GHz Maximum Associated Clients	75	(Range 1~75)
5GHz Maximum Associated Clients	75	(Range 1~75)
2.4GHz Coverage Threshold	-95	(-95dBm ~ -60dBm)
5GHz Coverage Threshold	-95	(-95dBm ~ -60dBm)
2.4GHz TX Power	Max(100%)	
5GHz TX Power	Max(100%)	
2.4GHz WLAN Partition	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
5GHz WLAN Partition	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
RTS Threshold	2347	(0-2347)



Firma pozítří

- ✓ GW s NAT a firewallem na úrovni rychlosti připojení do internetu ~ to stačí :-)
- ✓ L3 switch jako hlavní multisubnet a VLAN router
- ✓ VPN apod. spojení bez problému kapacitně do LAN spojení GW-LAN-L3 switch
- ✓ Radius ověření na přístupových „access“ koncích
- ✓ včetně ACL
- ✓ WiFi multiSSID



L3 switch jako centrální prvek

1) definice VLAN rozhraní >>>

Global VLAN Configuration

Allowed Access VLANs	1-5
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<All>	1	<All>	<input type="checkbox"/>	<All>	<All>	1-10	
1	Trunk	1	C-Port	<input checked="" type="checkbox"/>	Tagged Only	Tag All	1-10	
2	Access	3	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	3	
3	Access	5	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	5	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag All	1	

DHCP Server Mode Configuration

Global Mode

Mode Enabled

VLAN Mode

VLAN	Enabled
1	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>

4) DHCP server >>>

DHCP Server Pool Configuration

Pool Setting

Delete	Name	Type	IP	Subnet Mask	Lease Time
<input type="checkbox"/>	VLAN3	Network	192.168.3.100	255.255.255.0	1 days 0 hours 0 minutes
<input type="checkbox"/>	VLAN5	Network	192.168.5.100	255.255.255.0	1 days 0 hours 0 minutes

2) IP subnety nad VLAN >>>

IP Configuration

Domain Name	No Domain Name
Mode	Router
DNS Server	Configured IPv4 or IPv6 192.168.1.1
DNS Proxy	<input checked="" type="checkbox"/>

IP Interfaces

Delete	VLAN	Enable	DHCPv4				Hostname	Fallback	Current Lease	IPv4	
			Type	IfMac	ASCII	HEX				Address	Mask Length
<input type="checkbox"/>	1	<input type="checkbox"/>	Auto	Port 1				60	192.168.1.2	24	
<input type="checkbox"/>	3	<input type="checkbox"/>	Auto	Port 1				60	192.168.3.1	24	
<input type="checkbox"/>	5	<input type="checkbox"/>	Auto	Port 1				60	192.168.5.1	24	

3) Routovací tabulka L3 >>>

Add Interface

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
<input type="checkbox"/>	0.0.0.0	0	192.168.1.1	1

Add Route

5) Gateway routovací tabulka >>>

(WRT-416, lze využít i RIP protokol)



WRT-416		Routing					
Status		Routing Table Management					
WAN Setup		Type	Target	Mask	Gateway		
LAN Setup		NET					
Wireless		Add					
Routing		ID	Type	Target	Mask	Gateway	Delete
NAT		1	NET	192.168.3.0	255.255.255.0	192.168.1.2	Delete
Firewall		2	NET	192.168.5.0	255.255.255.0	192.168.1.2	Delete
DDNS							
MISC							

Téma pro segmentaci a zabezpečení

- nároky na připojení do internetu a gateway (ne vždy využijete 1Gb/s)
- nároky na vnitřní spojení (databáze, SAN ~ požadavky se zvyšují)
- uzavřený firewall versus online ochrana (ekonomický pohled na řešení versus pohodlí)
- počet segmentů (VLAN) a subnetů IP
- co nekoupíte v routeru nechte odpracovat výkonější L3 switch
- záložní ~ kruhové spoje, nejen pro výrobu, co CCTV, EZS, EPS?
- CCTV ano, nenáročné, ale nutné provozně oddělit (NIS2?)
- VoIP ano, ale doporučené priorizovat (odděleně)
- WiFi ano, ale komu (autentizace) a kam (jen do internetu?)
- IoT a připojení do cloudu, bezpečné? (NIS2)
- monitoring klíčových uzlů (někdy stačí jeden hlavní)

Monitoring

Správa zařízení

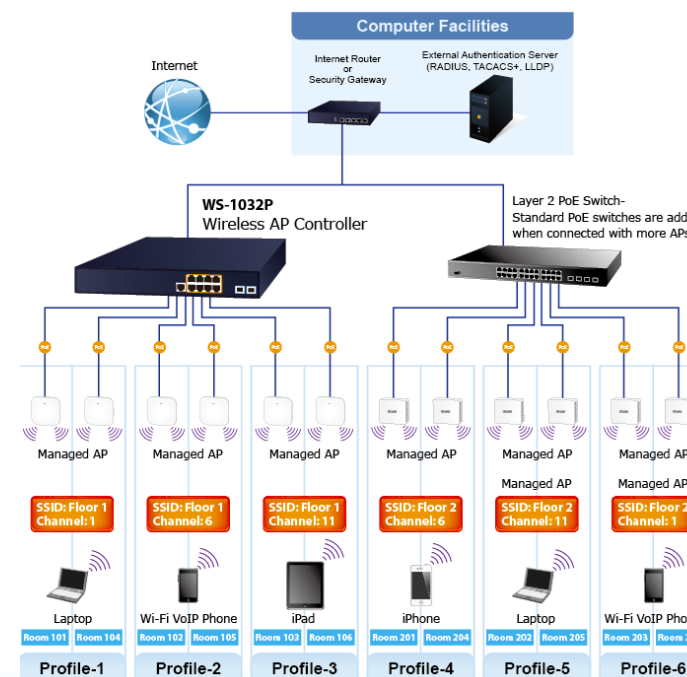
- Lokální (LCD displej)
- Sériová konzole COM
- Telnet
- HTML / Web
- **Aplikační (SNMP)**
- **Centralizovaná NMS (SNMP, MQTT)**
- Decentralizovaná (cloud)

Správa každý den ke kávě?
Paranoidní přístup...



Planet NMS kontroléry

- WiFi pro správu mnoha AP (WS přepínače, VR brány)
- Univerzální NMS-500
- Specilizované NMS-360 (solární, LoRa)
- S displejem NMS-1000V



Kontroléry Planet

Společné vlastnosti:

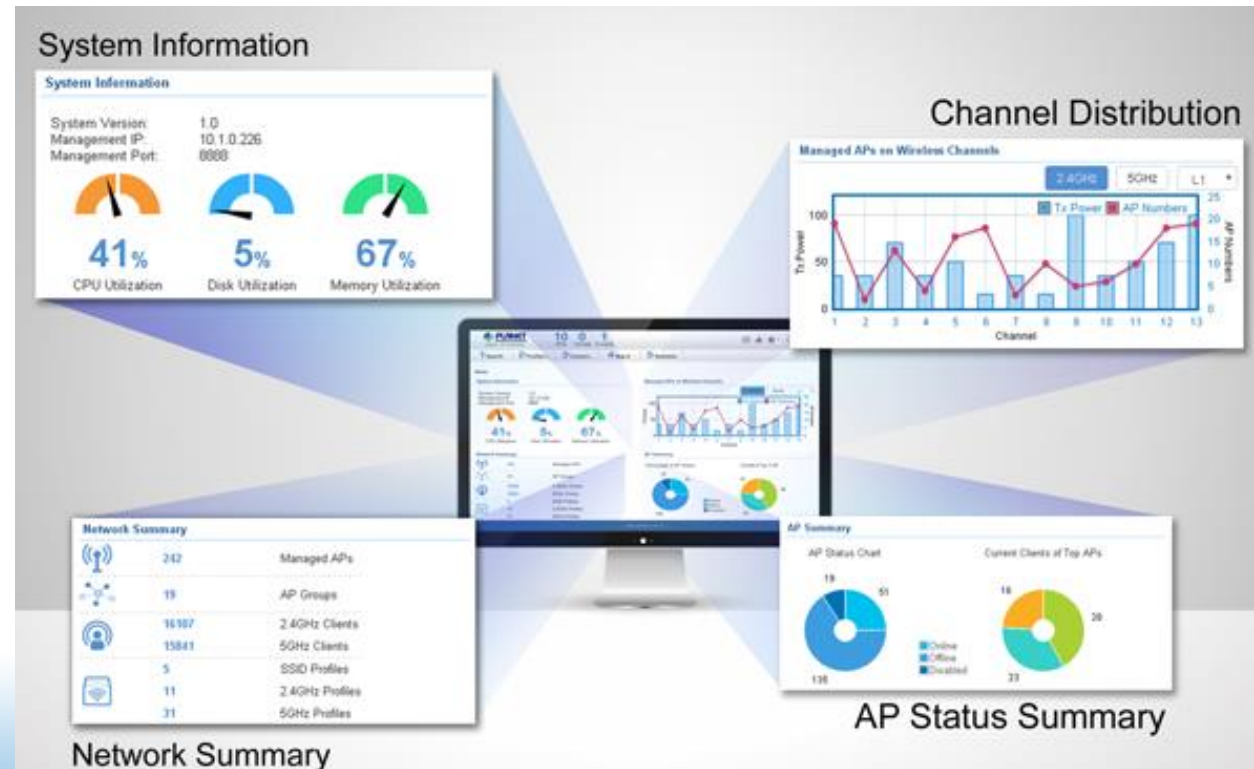
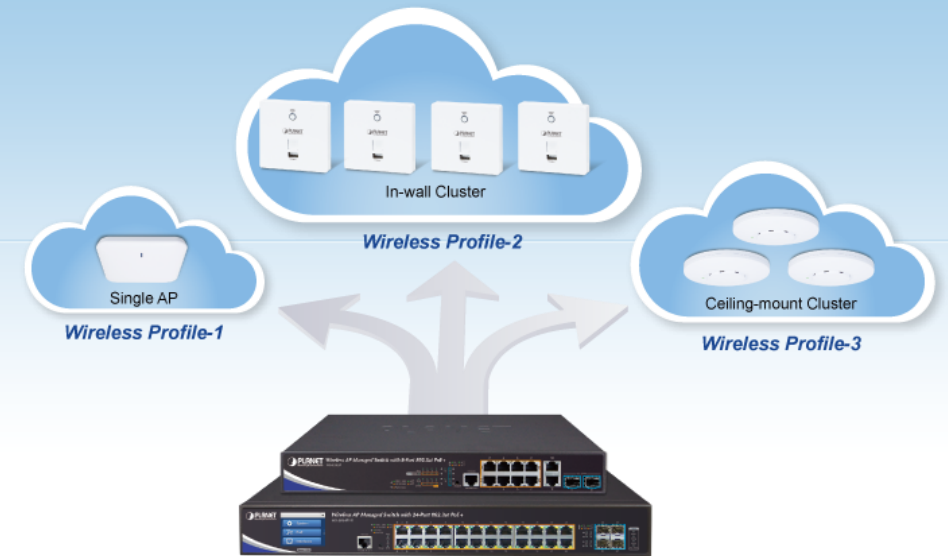
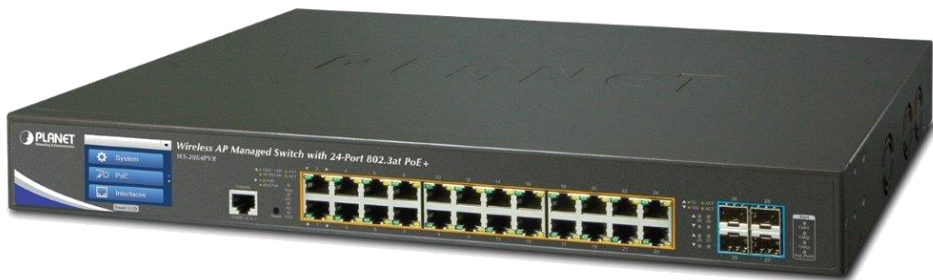
- dashboard
- autodiscovery
- přehled topologie
- status monitoring
- alarmy včetně SNMP
- podpora ověřování RADIUS
- WiFi mapa pokrytí (Heatmap)
- WiFi hromadný update profilů
- WiFi mapování SSID na VLAN
- ✓ bezlicenční politika
- ✓ bez vazby na internet/Cloud
- ✓ s využitím standardních protokolů



WiFi kontroléry

Pro centralizovanou správu AP jednotek:

- **VR-300** VPN firewall a brána <64 AP
- **WS-1232P** <32 AP, L3 switch s PoE a 10Gb SFP+
- **WS-2864PVR** <64 AP, L3 switch s PoE a 10Gb SFP+ a LCD
- **WAPC-500** <512 AP, podpora více modelů AP
- **WAPC-1000** <1024 AP, podpora více modelů AP
- software **Smart AP control**



NMS kontroléry

Pro centralizovanou správu síťových zařízení:

- **NMS-500** kontrolér pro až 512 zařízení
- **NMS-1000** kontroléry pro 1024 zařízení s **LCD**
- software **UNI-NMS**



100% **RELIABLE**

- Interactive Dashboard
- 4-step Wizard
- TFT Touch Panel
- Popup Alert Message
- Topology View
- Event Report

NMS-1000V-10

NMS-1000V-12

Extra computer not required



PLANET NETWORK PRODUCT FAMILY



Wireless (AP)



Industrial Switch



Router



Media Converter



Network Management



IP Power Management



IP Camera



Switch



VoIP

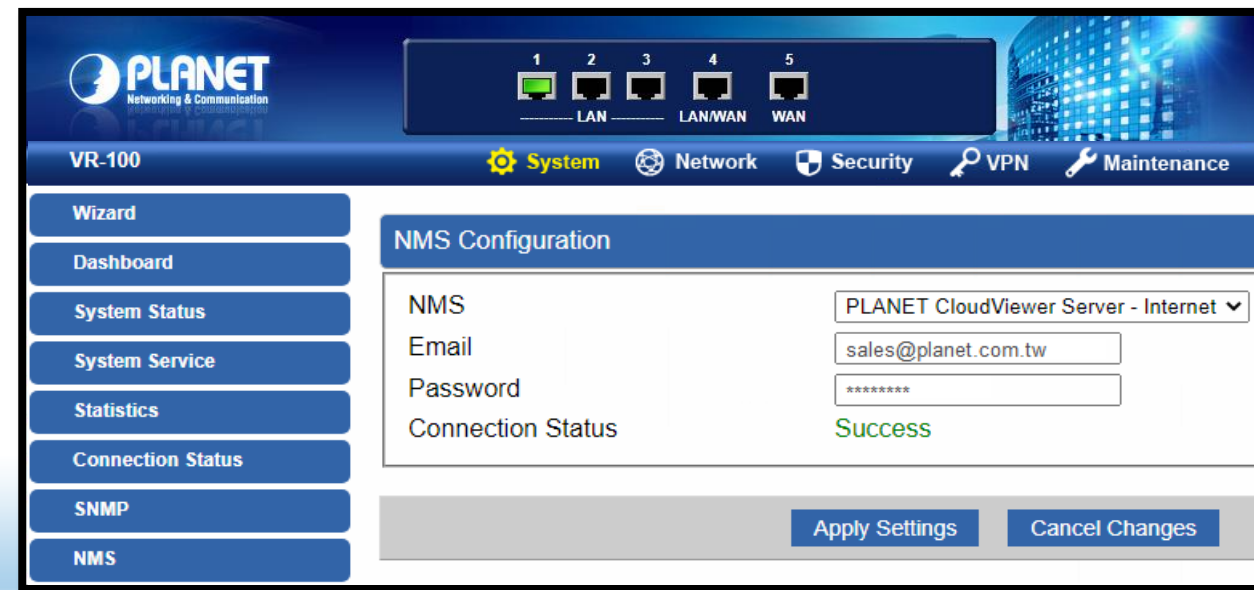
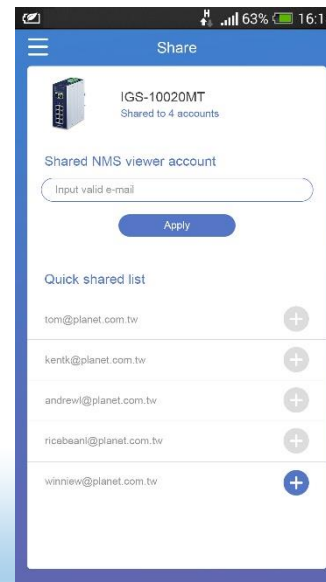
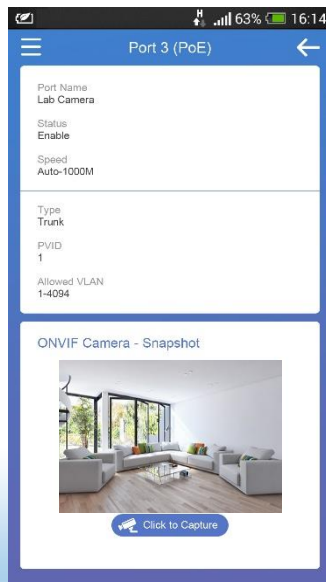
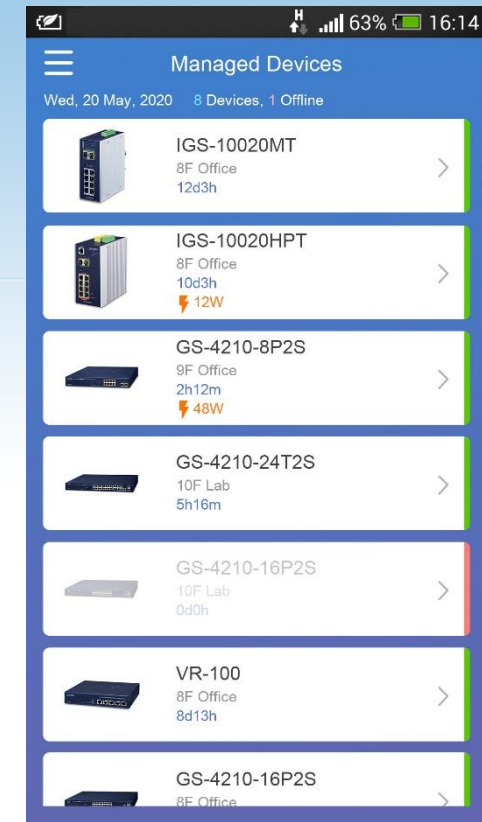


Industrial Automation



CloudViewer (Pro)

- Online aplikace pro aktivní monitoring
- Snadná registrace a zprovoznění
- Bez licencí a poplatků
- Mobilní aplikace i WEB portál se seznamem zařízení
- Dnes podpora desítek switchů a routerů včetně bran 5G a LoRa
- Přehled portů, jejich stav, PoE výkon, přenesená data, ONVIF info
- „Pro“ verze pro ovládání WiFi





CloudViewer (Pro)

- Administrátor na volné noze (firmy, hotely, školy, restaurace)
- Ideální pro IP CCTV nebo WiFi monitoring infrastruktury
- IT admin v rodině





NMSViewerPro

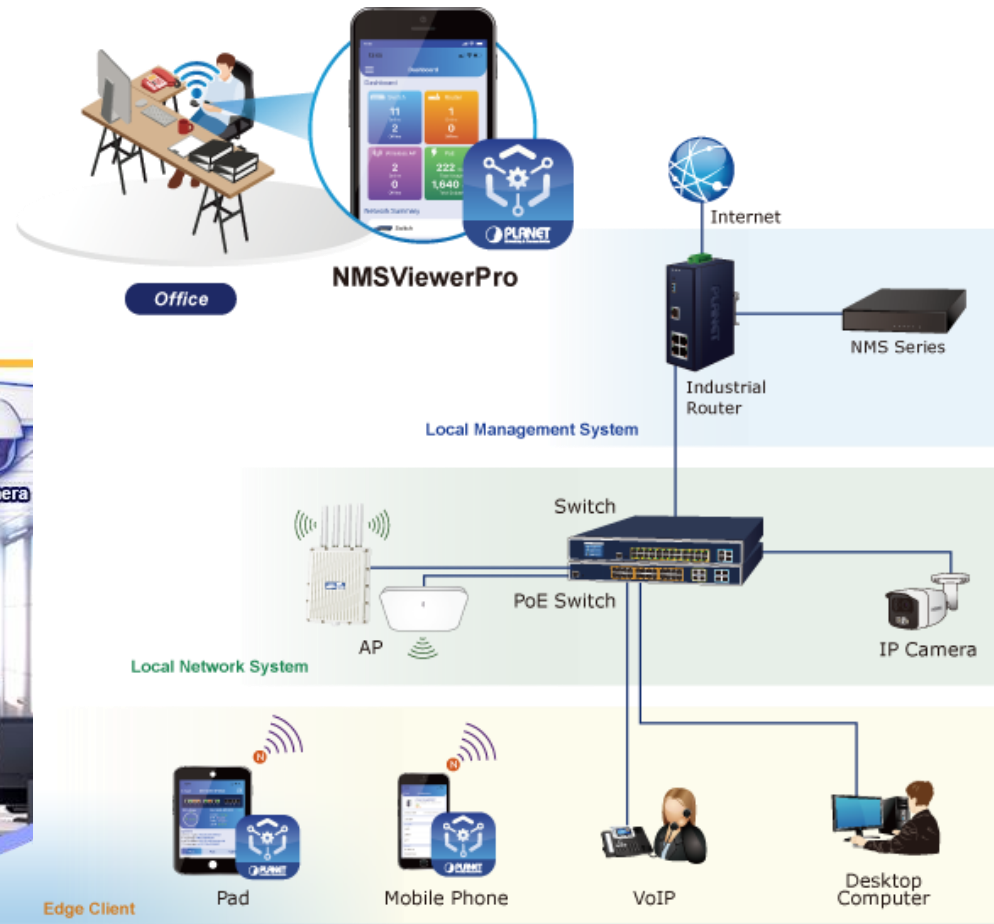
- Online aplikace pro aktivní monitoring NMS kontrolérů
- Bez licencí a poplatků
- Mobilní aplikace i WEB portál se seznamem zařízení



Product News PLANET NMSViewerPro

Intuitively Manage Your Network Devices without Limit

- Real-time Monitoring
- Location Setup
- Cloud-based Management
- Mobile Control
- Alerts & Notifications
- Android iOS



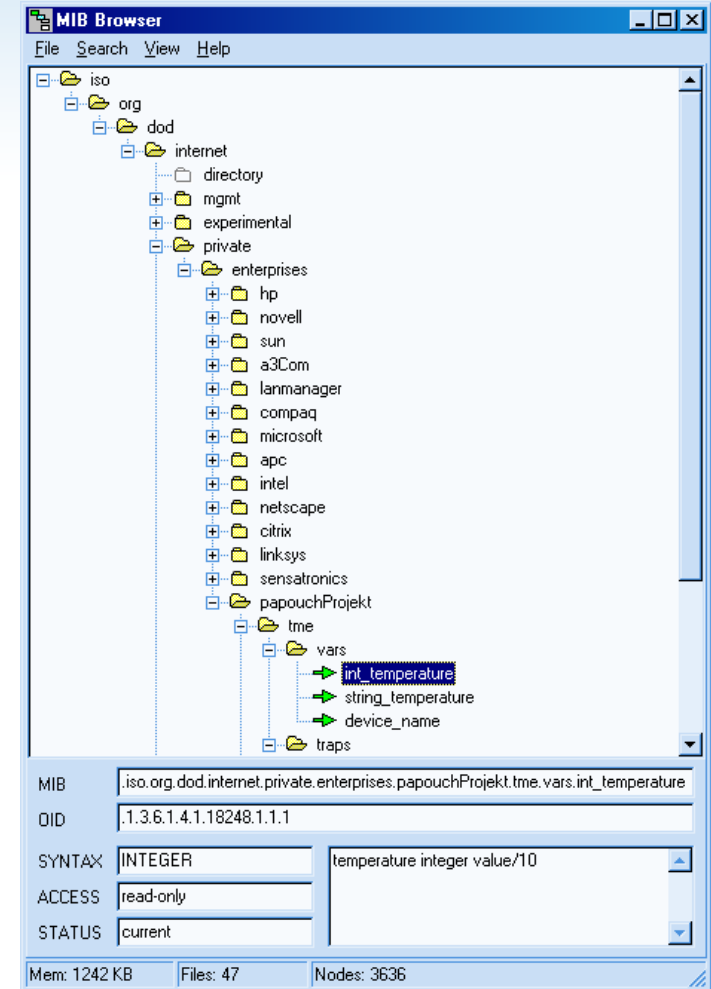
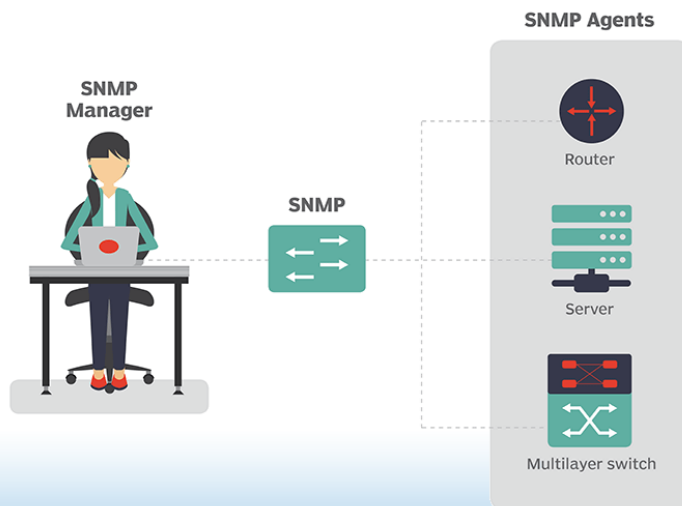
Factory Floor



ASMA

SNMP protokol

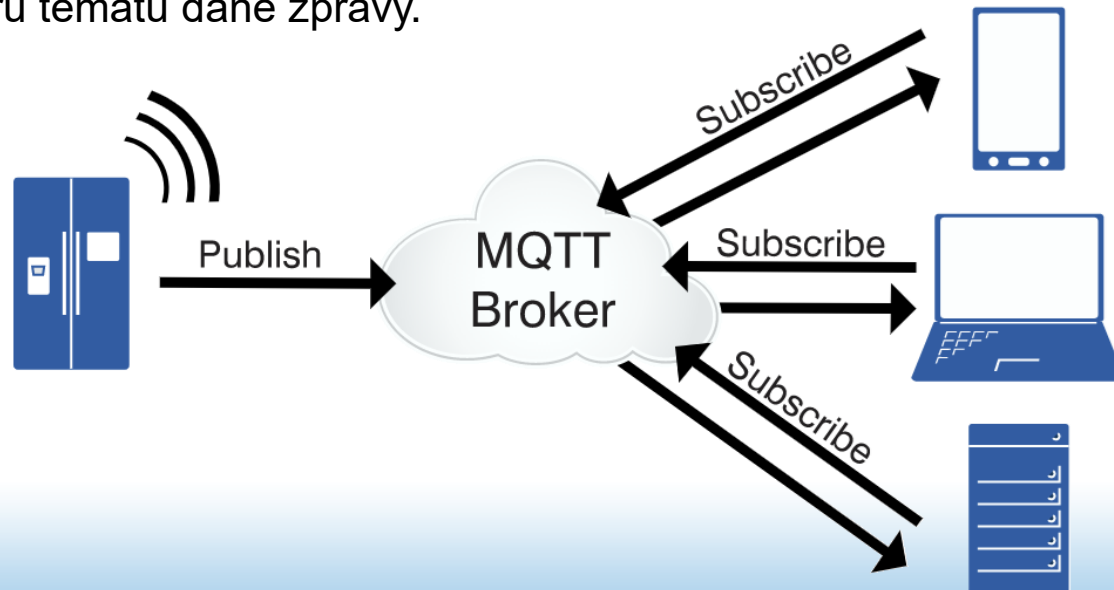
- Simple Network Management Protocol
- protokol pro monitoring síťových prvků
- protokol aplikační vrstvy, komunikace UDP-161
- tři verze: v1- základní, v2- autentizace, v3- šifrování
- struktura: **manager** – **agent** – **zařízení**
- **OID** – object identifier je číselný identifikátor hodnot ve stromu SNMP
- **MIB** databáze obsahuje seznam OID
- oznámení **traps** pro zasílání zpráv z agentů



IoT a podpora MQTT protokolu

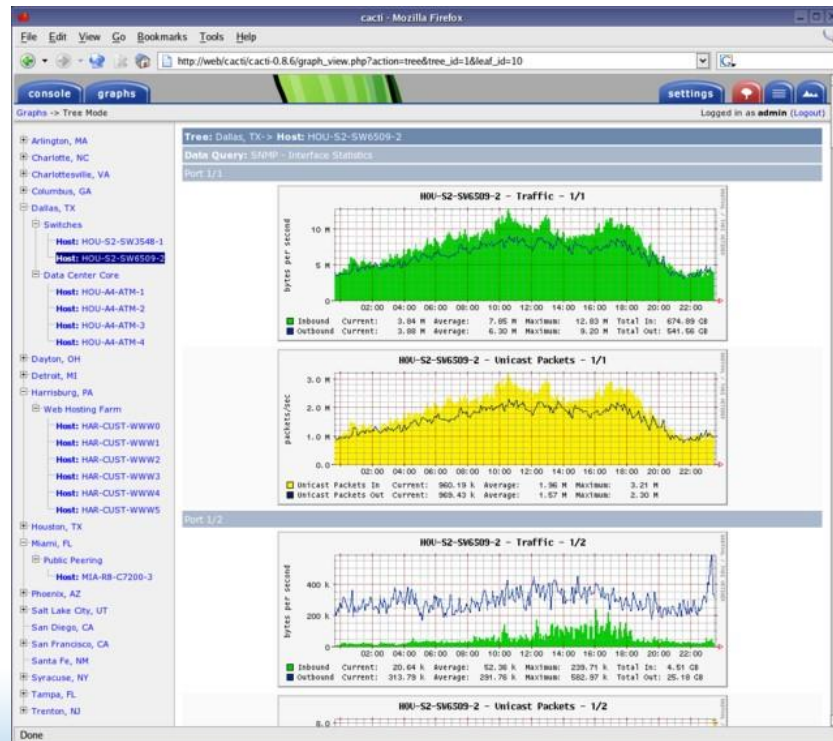
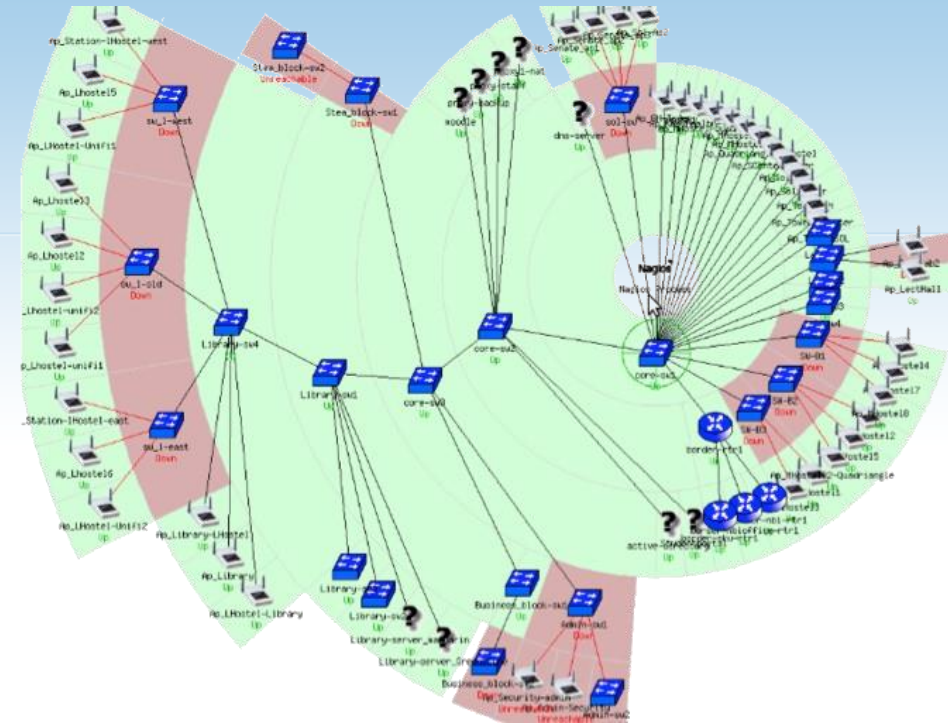
Message Queuing Telemetry Transport (MQTT) je architektura publish-subscribe, která byla vyvinuta především pro připojení zařízení s omezenou šířkou pásma a napájením prostřednictvím bezdrátových sítí. Jedná se o jednoduchý a odlehčený protokol, který běží přes sockety TCP/IP, Web a SSL.

- **Zprostředkovatel (broker)** je centrálním komunikačním bodem. Zprostředkovatel je zodpovědný za rozesílání všech zpráv mezi klienty.
- **Klient** je jakékoli zařízení (například počítač nebo mobilní telefon), které se připojí ke zprostředkovateli. Klient, který odesílá zprávy, je vydavatel. Klient, který přijímá zprávy, je účastník. Aby mohl klient přijímat zprávy, musí se přihlásit k odběru tématu dané zprávy.

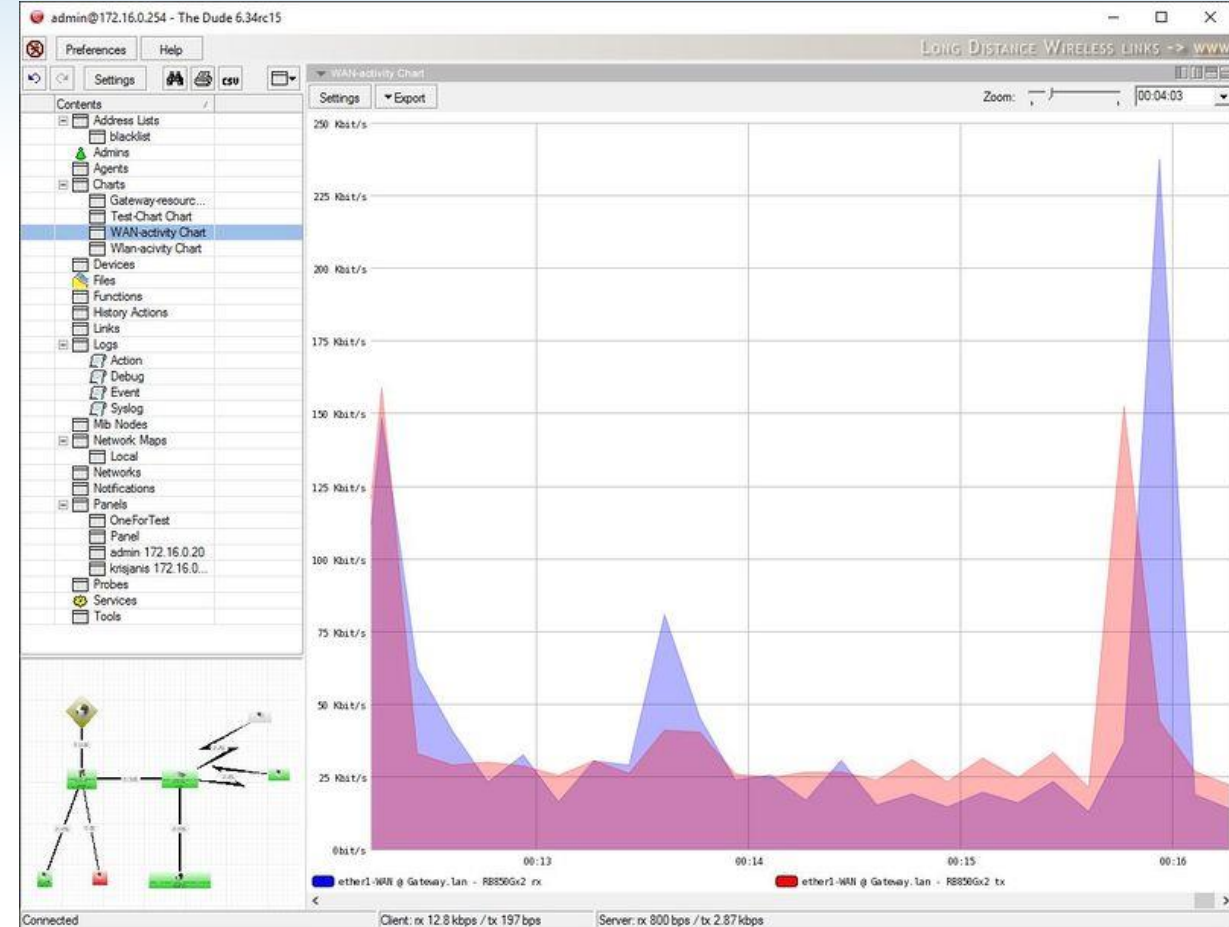
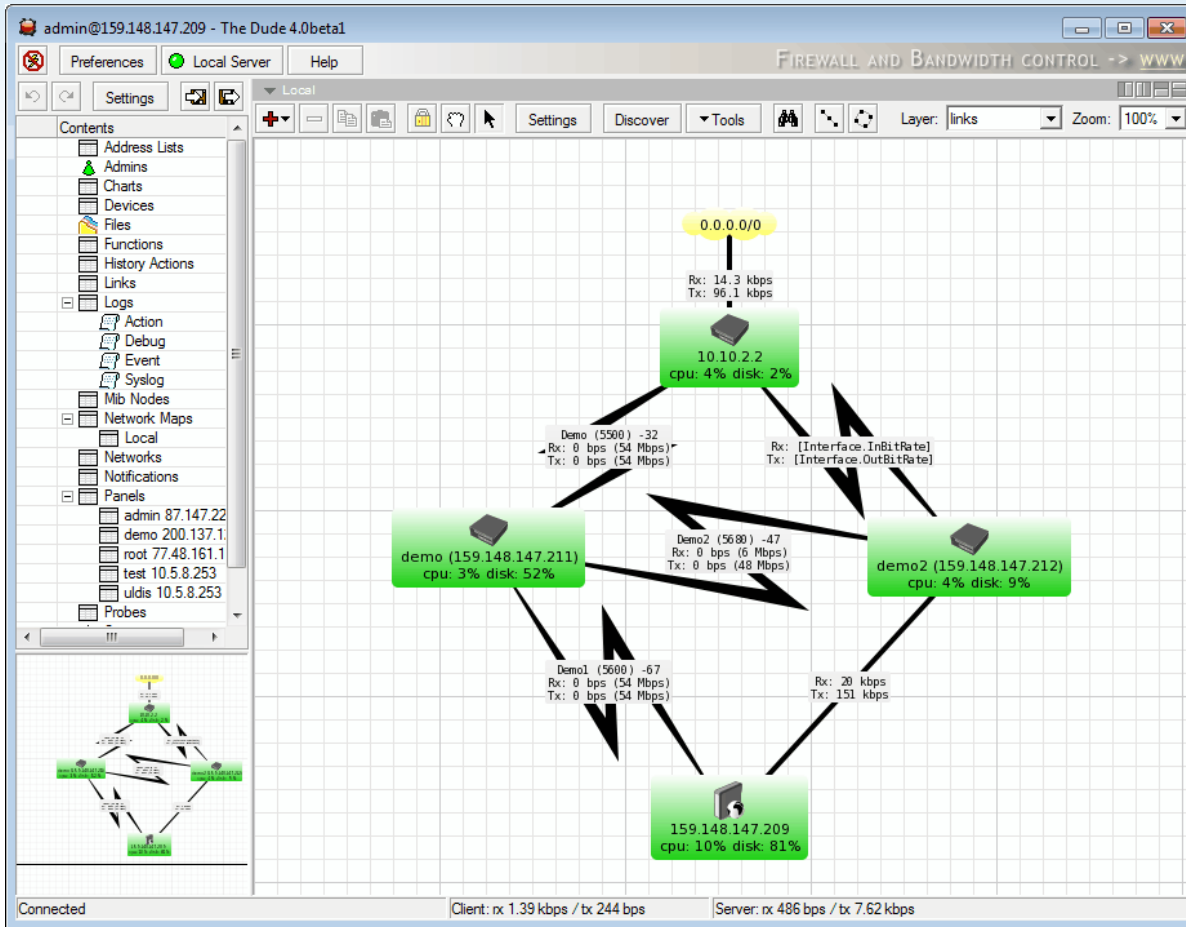


NMS software

- Naqios, Cacti, Zabbix, OpenNMS, SolarWinds, Mikrotik DUDE...
- https://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems



Mikrotik DUDE



SolarWinds Network monitor

Quality of Experience

All Nodes with QoE Traffic MANAGE HELP

NO GROUPING APPLIED

- A1-Inventry
- cur-dhcp
- LAB-CLUSTER-01.lab.tex
- SQL_Server_01
- Web_Server_01

QoE Nodes Exceeding Thresholds HELP

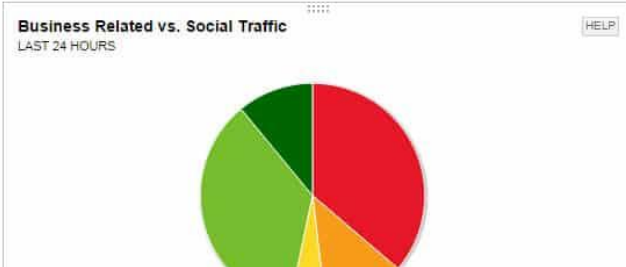
LAST 24 HOURS, GROUPED BY LOCATION

LOCATION	AVG NETWORK RESPONSE TIME	AVG APPLICATION RESPONSE TIME	TOTAL DATA VOLUME	TOTAL # OF TRANSACTIONS
lab				

Quality of Experience Application Stats MANAGE HELP

LAST 24 HOURS, BY APPLICATION

QOE APPLICATION	AVG NETWORK RESPONSE TIME	AVG APPLICATION RESPONSE TIME	TOTAL DATA VOLUME	TOTAL # OF TRANSACTIONS
Amazon Web Services	299.62 ms	284.58 ms	559.6 KB	613.1 k
FTP	3.02 s	315.34 ms	108.0 KB	244.9 k
HTTP	683.67 ms	271.78 ms	206.3 KB	53.1 k
MS SQL	262.30 ms	4.05 s	104.0 KB	2.2 M
RDP	151.03 ms	250.19 ms	545.4 KB	432.5 k
Skype	356.26 ms	343.09 ms	720.2 KB	188.7 k
SNMP	417.46 ms	320.68 ms	1.6 MB	179.1 k
YouTube	203.02 ms	184.98 ms	2.1 MB	2.1 M

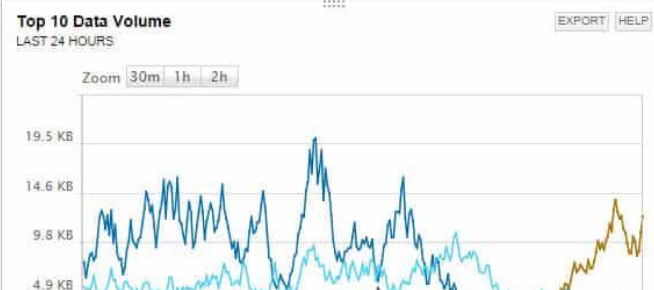


Top 10 Application Response Time (Time to First Byte) EXPORT HELP

LAST 24 HOURS

Zoom 30m 1h 2h

QOE APPLICATION	AVERAGE APPLICATION RESPONSE TIME	PEAK VALUE
MS SQL	4.05 s	4.59 s
Skype	343.09 ms	3.19 s
SNMP	320.68 ms	2.04 s
FTP	315.34 ms	499.55 ms
Amazon Web Services	284.58 ms	2.10 s
HTTP	271.78 ms	1.48 s
RDP	250.19 ms	991.83 ms
YouTube	184.98 ms	1.01 s

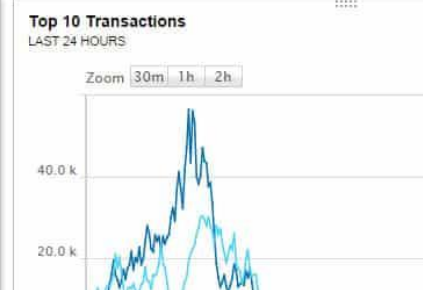


Top 10 Network Response Time (TCP Handshake) EXPORT HELP

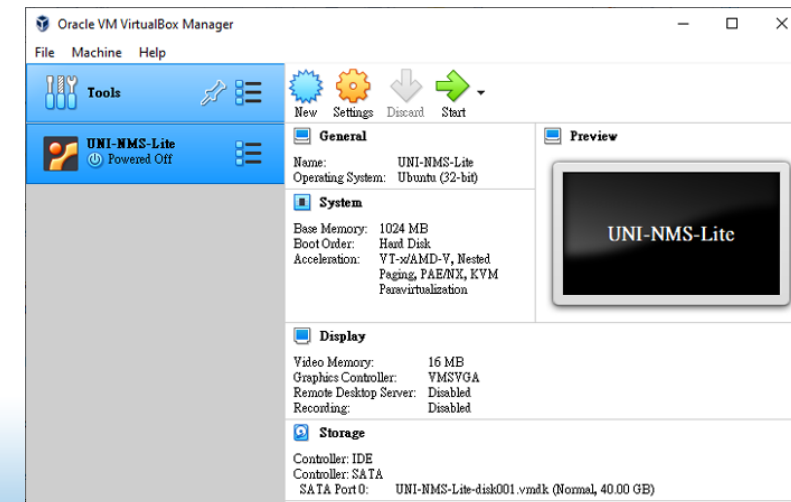
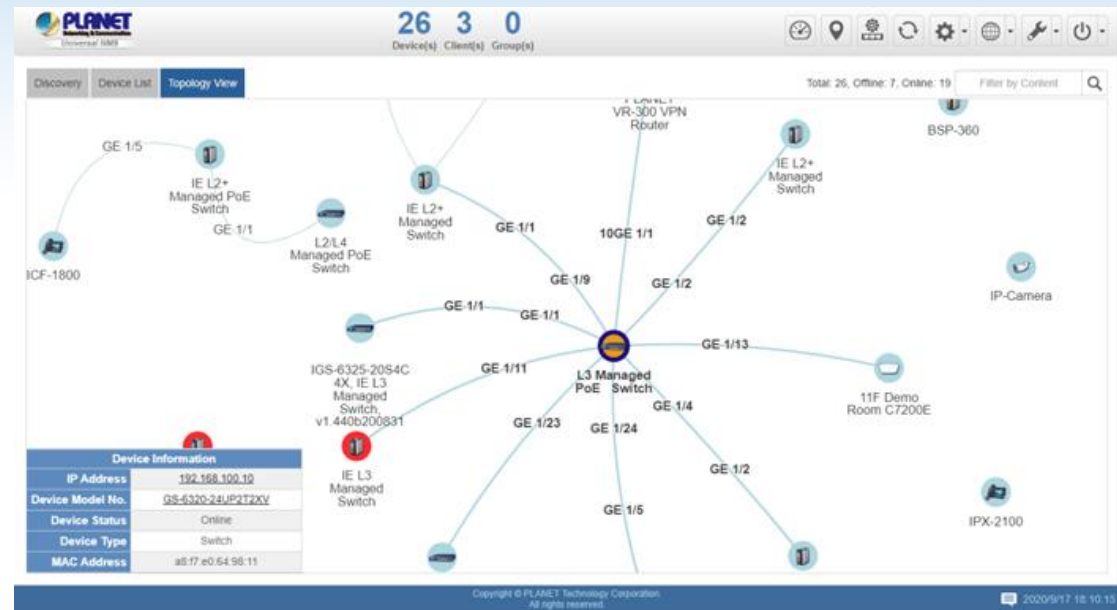
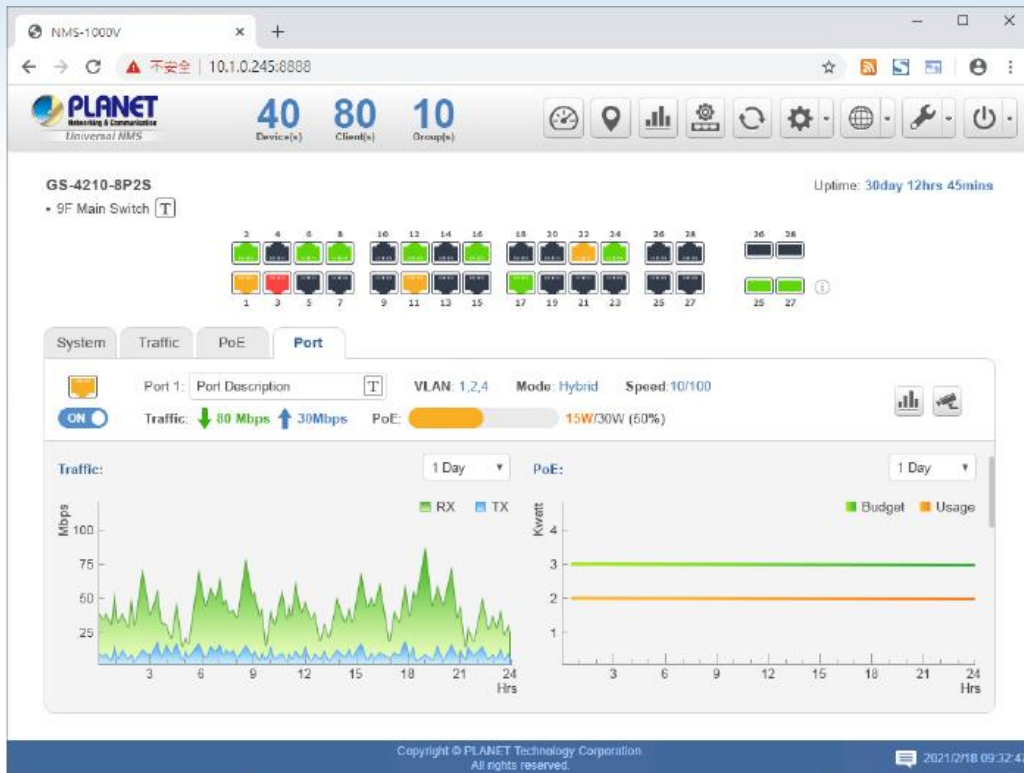
LAST 24 HOURS

Zoom 30m 1h 2h

QOE APPLICATION	AVERAGE NETWORK RESP
FTP	3.02 s
HTTP	683.67 ms
SNMP	417.46 ms
Skype	356.26 ms
Amazon Web Services	299.62 ms
MS SQL	262.30 ms
YouTube	203.02 ms
RDP	151.03 ms



Planet NMS



- ✓ Zkuste UNI-NMS-Lite zdarma
- ✓ Instalace v rámci připravené image VirtualBox
- ✓ Omezení na 100 Nodů

Technická podpora

- 7 vlastních specialistů, většina VŠ vzdělání
- Technické zázemí a vybavení
- Přímá vazba a komunikace s výrobcí, úpravy firmware, updaty
- Vlastní databáze návodů, ovladačů a instalačních postupů
- Vlastní testování a simulace částí systémů
- 25 let zkušeností v oblastech
TELCO, IP, ISP, CCTV, WiFi, Embedded...

podpora@asm.cz

281 040 540



Těšíme se na spolupráci!

