

AKTIVNÍ PRVKY PLANET

Dokumentace a seznámení s teorií

Přepínače řady SGSW-24x40



OBSAH

1)	POPIS PRODUKTŮ SGSW-24040/24240 A JEJICH VLASTNOSTI.....	2
	Vlastnosti.....	2
	Funkce přepínačů.....	3
2)	STANDARDY A NORMY.....	8
3)	ZÁKLADNÍ POJMY A TEORIE SÍŤE ETHERNET.....	9
	a) Způsoby přeposílání rámců:.....	9
	b) Stack – stoh – hromada.....	10
	c) Přepínače vyšších vrstev	10
	d) Ethernet.....	11
4)	OSI SÍŤOVÝ MODEL.....	12
	Vrstvový model	12
	a) Fyzická vrstva č. 1	14
	b) Spojová vrstva č. 2.....	17
	c) Síťová vrstva č. 3.....	19
	d) Transportní Vrstva č. 4	21
	e) Relační vrstva č. 5.....	21
	f) Prezentační vrstva č. 6	21
	g) Aplikační vrstva č. 7.....	21
5)	APLIKACE FUNKCÍ PŘEPÍNAČŮ	22
	VLAN teorie a příklady nastavení.....	22
	a) Výhody VLAN.....	23
	b) Příklady VLAN	24
	QoS (quality of service)	30
	a) QoS aplikace.....	30
	b) QoS Konfigurace.....	31
	c) Storm Control konfigurace.....	34
	Rapid Spanning Tree (RSTP)	35
	a) Teorie.....	35
	b) Nastavení parametrů STP.....	37
6)	PLANET Technology Corporation	45

1) POPIS PRODUKTŮ SGSW-24040/24240 A JEJICH VLASTNOSTI

Planet SGSW-24040 je plně gigabitový 24 portový L2 (OSI) přepínač se 4-mi sdílenými SFP sloty (miniGBIC) určený pro nasazení do velkých podniků, páteřních sítí a pro ISP poskytovatele.

Planet SGSW-24240 je plně gigabitový 24 portový přepínač. Má 24 portů pro moduly SFP: Tyto moduly mohou být jak Gigabitové tak i 100Mbps. Dále je vybaven 8-mi sdílenými RJ-45 port s autodetekční 10/100/1000Mbps

Jsou vybaveny dvěma vysokorychlostními HDMI porty pro stohovací účely s propustností až 20Gbps. Lze tak spojit v jedno logické zařízení až 16 zařízení (celkem 384 ethernet portů) a spravovat je jako jeden logický switch.

Stohovací funkce skupiny zařízení SGSW dovoluje za provozu rozšiřovat kapacitu centrálních bodů včetně plánování jejich celkové propustnosti. Rozšířené funkce "L2-switching" nabízí například "Port link aggregation", "Q-in-Q VLAN", "private VLAN", "Rapid Spanning Tree protocol", "Layer 2 to Layer 4 QoS", "bandwidth control", "IGMP Snooping". Je možné vytvořit a spravovat až 255 VLAN skupin. Pro "trunkové" spoje je možné vytvořit až 12 skupin po 16-ti portech pro každou skupinu. Přepínač disponuje filtrací provozu na základě IP adres a dalších parametrů TCP/IP.

Zařízení se spravuje s pomocí webového prohlížeče nebo prostřednictvím SNMP utility s podporou protokolu SNMPv3, který umožňuje šifrovat přenášená data.

Sdílené SFP (Small Factor Pluggable) sloty lze osadit libovolnými mini-GBIC kompatibilními s 100Base-FX/1000Base-X a WDM.

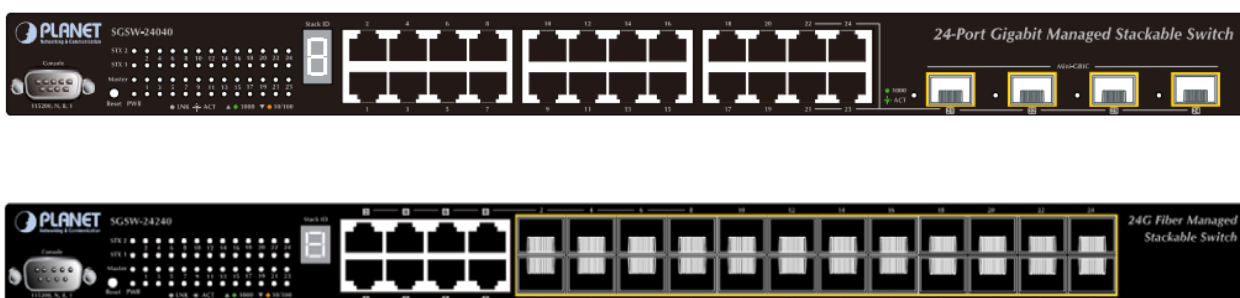
Verze SGSW-24040R/24240R disponují interním záložním zdrojem pro napětí 48V-DC pro případ závady primárního zdroje nebo pro účely zálohy napájení v případě výpadku napájecí sítě AC 230V.

Vlastnosti

- SGSW-24040x: 24 portů 1000Base-T, Switching, Full Duplex (1000/2000 Mbps), Auto-Negotiation (10/100/1000 Mbps), duálně s 4-mi porty 100Base-FX/1000Base-X miniGBIC SFP rozhraním
- SGSW-24240x: 24 portů formátu SFP, Dual-Speed 100/1000Mbps, lze aplikovat moduly pro Gigabit i Fast Ethernet
+ 8 portů 1000Base-T, Switching, Full Duplex (1000/2000 Mbps), Auto-Negotiation (10/100/1000 Mbps), sdílených s SFP porty
- 8k MAC adres, buffer1392kB
- plná podpora protokolu IPv6

- 2x stohovací port, celková propustnost 20Gbps stohovacích portů, propustnost každého portu stohovacího propojení 10 Gbps (5Gbps full duplex * dva porty). Stohovací kabel 0,5m CB-STX50 součástí, typ konektoru HDMI.
- plná propustnost sběrnice 48 Gb/s
- podpora přenosu JumboFrame do 10KB
- provedení rackmount, rozměry 440x200x45mm, 1U výška
- ESD(ElectroStatic Discharge) ochrana na všech portech do 6kV DC
- interní zdroj 230V/50Hz, příkon 30W

Přední panely přepínačů SGSW-24040 a 24240

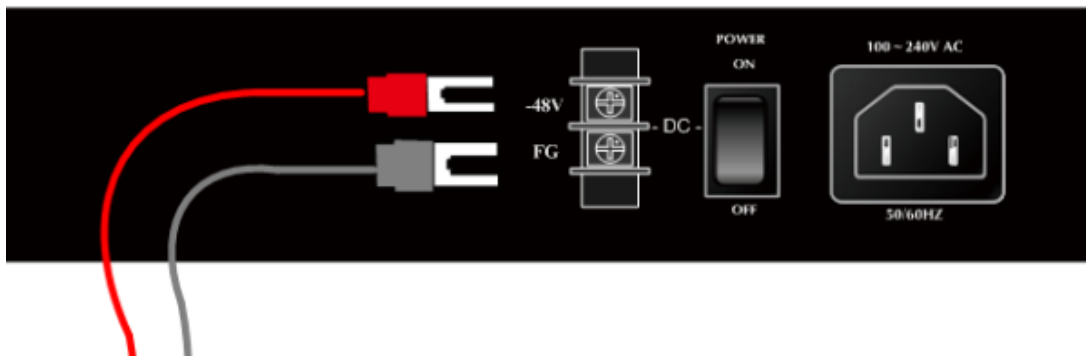


Funkce přepínačů

- 255 sítí VLAN IEEE 802.1Q, trunking, možnost nastavení ingress filteru VLAN tagged/untagged pakety, GVRP (GARP VLAN Registration Protocol)
- IP ACL, filtrace provozů dle IP adresy, protokolu, portu, TCP příznaků, DSCP
- MAC ACL, filtrace provozů dle MAC adresy, dle VLAN ID a kombinací příznaků priorit
- Port shaper - nastavení v rozpětí 500kbps-1Gbps
- QoS, prioritace provozu dle IEEE 802.1p a dle ToS/DS v IP paketu, možnost nastavení omezení posílaných paketů na port a dle na QoS pravidel
- Podpora IP multicastu, IGMP, možnost řízení multicastu přímo přepínačem (povolení/zabránění multicastů), IGMP v1,v2,v3, IGMP Query režim
- Port mirroring - Port trunking IEEE 802.3ad LACP, 12 skupin, celkem max. 16 portů
- Spanning Tree IEEE 802.1d, Rapid Spanning Tree IEEE 802.1w, Multiple Spanning Tree
- IEEE 802.1x, RADIUS - IP+MAC binding, VLAN + MAC binding
- IEEE 802.1ab LLDP - automatická detekce typu připojených zařízení
- diagnostika kabeláže, stanovuje délku kabeláže a případnou vzdálenost k závadě

Záložní zdroj

Modely s označením „R“ disponují interním záložním napájecím zdrojem DC 48V, který zaručí provoz přepínače při výpadku primárního napájení nebo při poruše zdroje AC 230V.

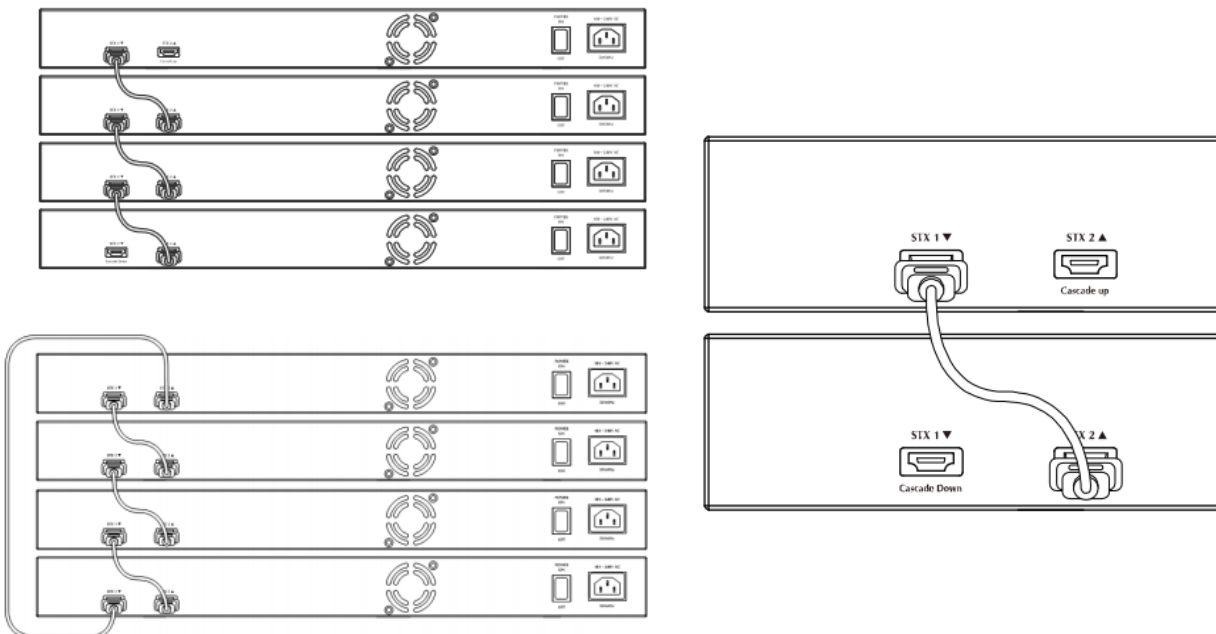


- Připojení napájecích vodičů provádějte při vypnutém stavu!

Stohovací porty 10Gb

Přepínače disponují velmi rychlými stohovacími porty s přenosovou kapacitou 2x 10Gb/s. Zařízení lze spojit do stohu lineární kaskády nebo do kruhu.

Pro propojení použijte výhradně originální kabely výrobce s označením CB-STX50 a CB-STX200!

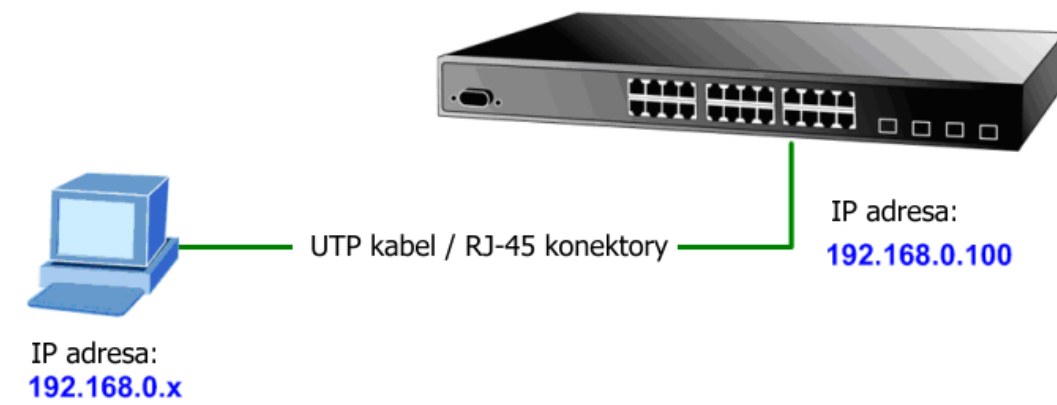


Administrace IPv4/IPv6

- Web/Telnet/SNMP s možností zabezpečeného přístupu SSH/SSL
- SNMP v1,v2c,v3
- konzole (COM port)



Propojení a parametry pro správu konzolí terminálu.



Propojení a parametry pro správu Web prohlížečem.

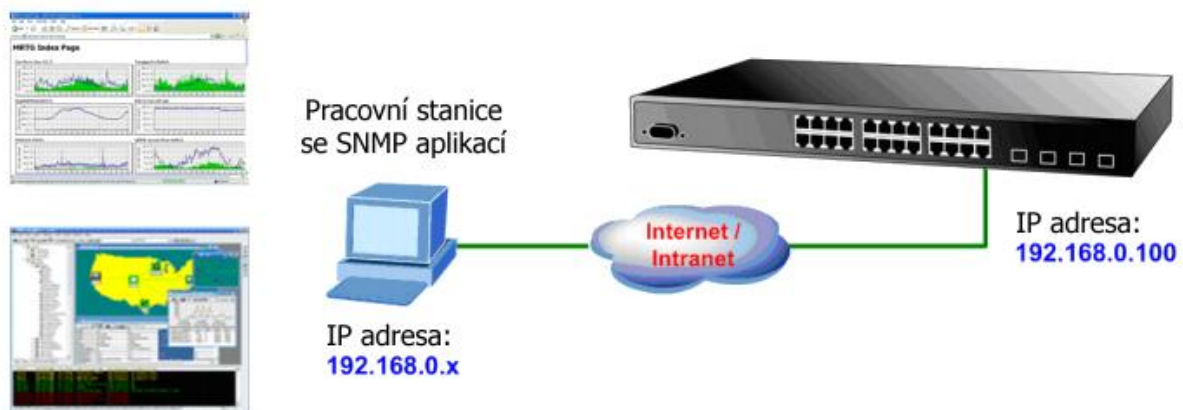


Schéma možné správy SNMP aplikací.

Úvodní přístup do nastavení přepínačů

Pro Web správu doporučujeme použít prohlížeč Internet Explorer verze 7 a vyšší.
Tovární IP adresu zadejte do adresního řádku v podobě <http://192.168.0.100>

Při výzvě zadejte přihlašovací jméno „admin“ a heslo „admin“.



- Z bezpečnostních důvodů přihlašovací údaje změňte a zapište na bezpečné místo!

Hlavní funkce

Stav metalických portů

Stav SFP portů

Stav stohovacích portů

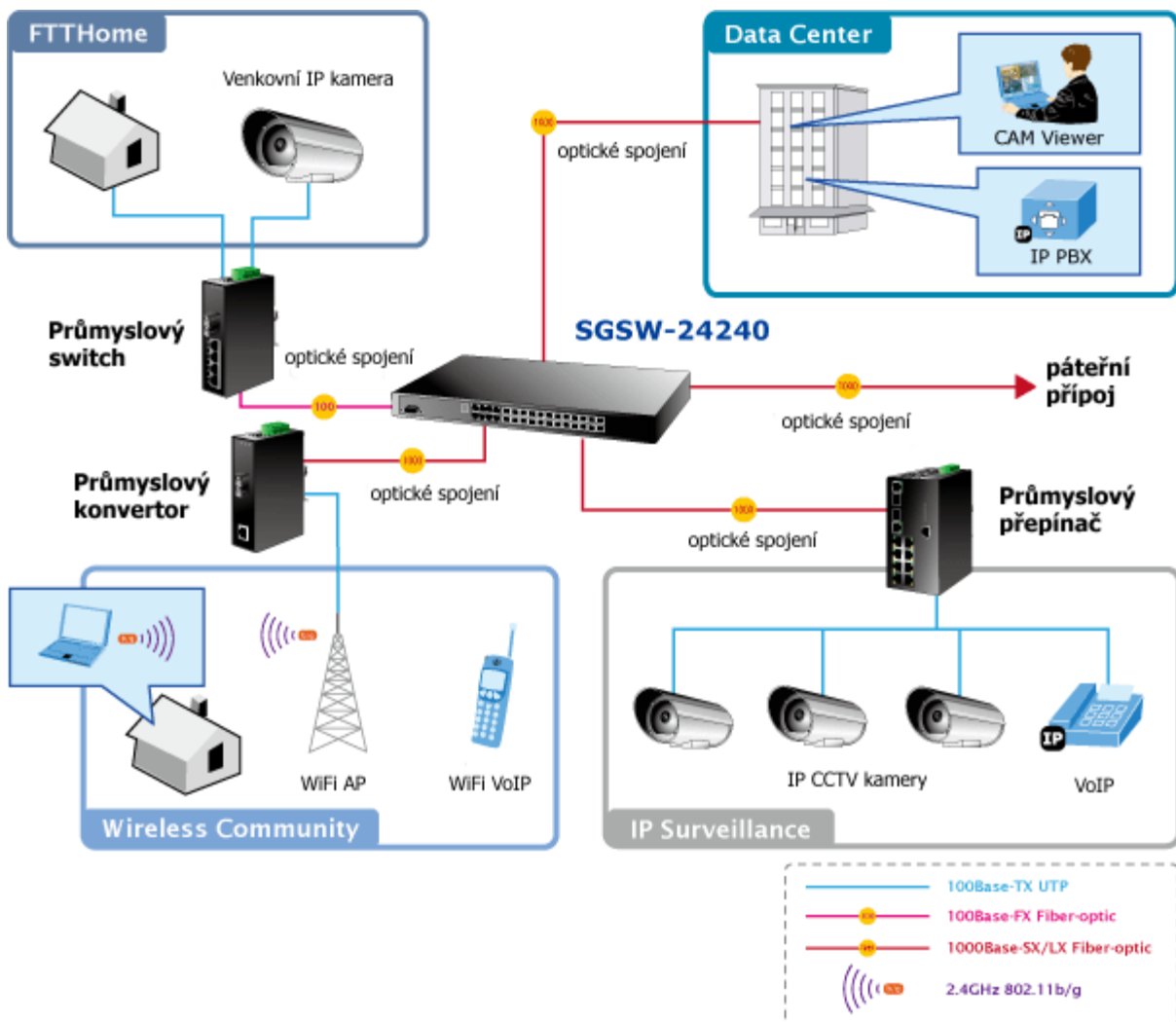
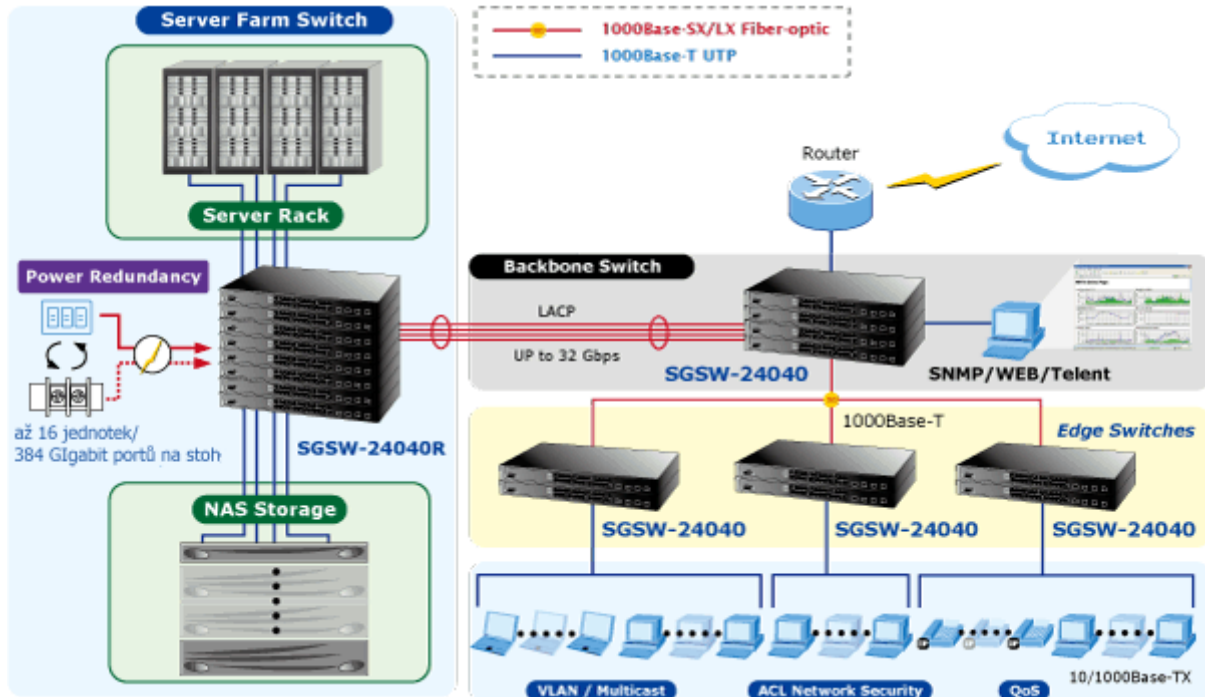
Informační a konfigurační okno

Základní nápověda

Uživatelské rozhraní přepínače.

- Popis funkcí přepínačů viz. kapitola 5) APLIKACE FUNKCÍ PŘEPÍNAČŮ (str.22).

Příklady použití:



2) STANDARDSY 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 (French: Comité Européen de Normalisation Électrotechnique).
Není EU institucí, je k Evropě vázána geograficky.

3) ZÁKLADNÍ POJMY A TEORIE SÍTĚ ETHERNET

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.

a) Způsoby přeposílání rámců:

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

Switche dnes často nabízejí i některé pokročilejší funkce jako je správa WEB/SNMP, VLAN, STP, QoS, shaper, routing L3, analýza L4, stohování...

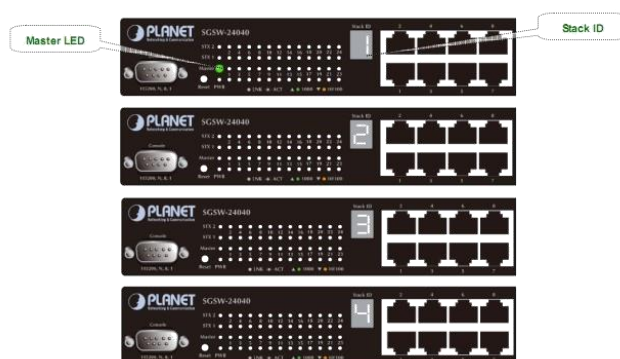
b) Stack – stoh – hromada

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

- IP stack – pro účely správy
- sběrnice – pro účely správy a redundance
-

Základní parametry pro stohování:

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



c) Přepínače vyšších vrstev

Jedná se o víceméně marketingový pojem. Díky svému rozšíření v Ethernetu se pojem switch vžil pro rychlý prvek rozhodující o dopravě paketů. 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 pracuje.

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 směrovač.

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. Prakticky výhradně marketingový pojem, jinak rozšíření některých L2 a L3 switchů.

Zpravidla se jedná o funkce filtrace TCP/UDP včetně provázanosti na MAC autorizaci a DHCP, vyjímecně pak např. portový filtr na úrovni služeb.

d) 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.

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 médium (sběrnici) se používá metoda CSMA/CD (Carrier Sense with Multiple Access and Collision Detection), česky metoda mnohonásobného přístupu s nasloucháním nosné a detekcí kolizí.

Stanice (síťová karta), která potřebuje vysílat, naslouchá co se děje na přenosovém médium. 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).

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.

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 médium 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.

4) 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 vrstvy 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

Na počátku vznikne požadavek některého procesu v aplikační vrstvě.

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.

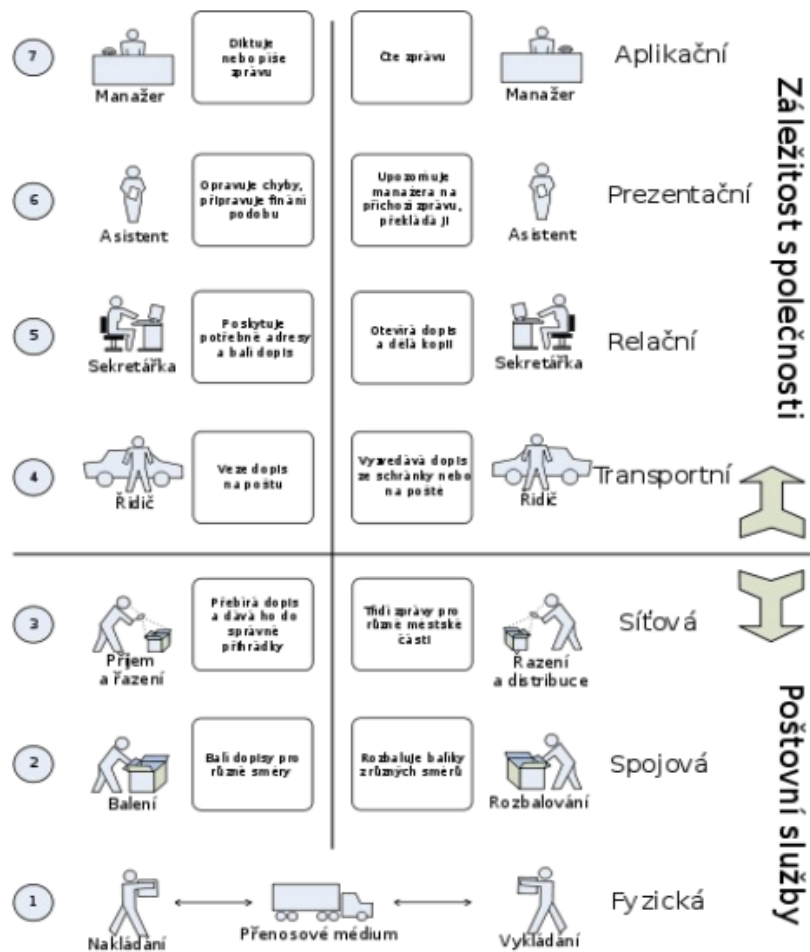
Takto se postupuje stále níže až k fyzické vrstvě, kde se použije pro spojení přenosové prostředí. Současně se při přechodu z vyšší vrstvy k nižší přidávají k uživatelským (aplikačním) datům záhlaví jednotlivých vrstev.

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

a) Fyzická 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/D, D/A převodníky).

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.

Rozbočovače (huby) jsou dnes většinou nahrazovány přepínači (switch), které jsou na rozdíl od nich inteligentní. Pracují na principu „ulož a předej“ (store+forward) - přijmou ethernetový rámec, uloží si jej do vyrovnávací paměti, analyzují adresu jeho příjemce a následně jej odvysílají do rozhraní, kterým je připojen jeho adresát. Tabulky s fyzickými adresami a jim odpovídajícími

rozhraními si udržují automaticky - učí se na základě adresy odesilatele v rámci. Vzhledem k tomu, že přepínač nepředává rámec rovnou, ale po uložení jej sám odvysílá, až bude na cílovém rozhraní volno, počítače (či sítě) připojené k jeho rozhraní spolu navzájem nesoutěží o médium. Na každém rozhraní přepínače běží nezávislý algoritmus CSMA/CD a o médium spolu soutěží jen zdejší počítače - přepínač tzv. odděluje kolizní domény.

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.

Typy ethernetu

- 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 - představuje zatím poslední standardizovanou verzi. 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. Začíná se zavádět...

- 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 50 Ω (tzv. terminátory).
- 10Base-T - jako přenosové médium používá kroucenou dvojlunku 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 dvojlunku. 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.
- 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. Pro propojování skupin zařízení.
- 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 vzdáleností až několika desítek kilometrů.
- 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 s rychlostí 40 a 100 Gb/s by měl používat optická vlákna; měděné kabely do délky alespoň 10 metrů

b) Spojivá 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.

Datová vrstva poskytuje funkce k přenosu dat mezi jednotlivými síťovými jednotkami a detekuje případně opravuje chyby vzniklé na fyzické vrstvě. Nejlepším příkladem je Ethernet. Na lokálních sítích založených na IEEE 802 a některých na IEEE 802 sítích jako je FDDI, by tato vrstva měla být rozdělena na vrstvu řízení přístupu k médiu (Medium Access Control, MAC) a vrstvu IEEE 802.2 logické řízení linek (Logical Link Control, LLC).

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

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).

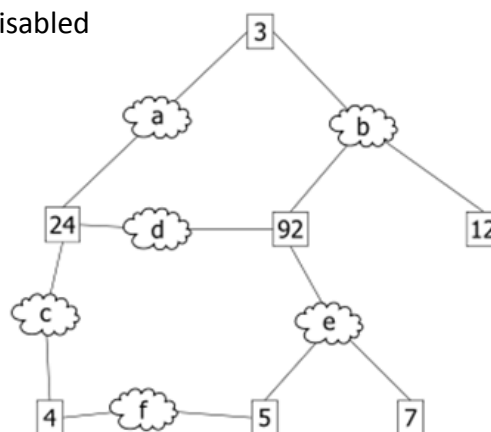
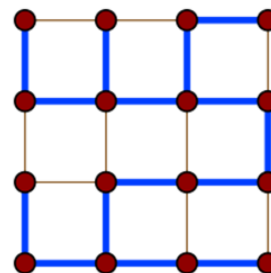
Preamble	SFD	MAC cíle	MAC zdroje	Typ/délka a	Data a výplň	CRC32	Mezera mezi rámci
7× oktet 10101010	1× oktet 10101011	6 oktetů	6 oktetů	2 oktety	46-1500 oktetů	4 oktety	12 oktetů
				64-1518 oktetů			
				72-1526 oktetů			

- 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

Spanning tree protokol

- 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



Rapid Spanning tree protokol (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 Protokol (MSTP)

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

c) Síťová 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.

MTU – maximum transmission unit

(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 (spojených například modemem nebo sériovou linkou) 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

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 např. program Traceroute.

- ✓ 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.

IPv6 síťový protokol (L3)

- IPv6 = bilion adres na čtvereční centimetr Země!
- 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} unikátních 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 je platná adresa IPv6. 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. Libovolný počet po sobě následujících skupin 0000 může být nahrazen dvěma dvojtečkami, pokud se v adrese toto nahrazení vyskytuje pouze jednou. Předcházející nuly ve skupině mohou být také nahrazeny (jako v ::1 pro místní smyčku).

d) Transportní 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 spojově (TCP) nebo nespojově orientované (UDP).

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 DC++, on-line hry atp.

e) Relační 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.

f) Prezentační 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).

g) Aplikační 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.

5) APLIKACE FUNKCÍ PŘEPÍNAČŮ

VLAN teorie a příklady nastavení

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 se subnety na 3. vrstvě

- ✓ Co je trunk?

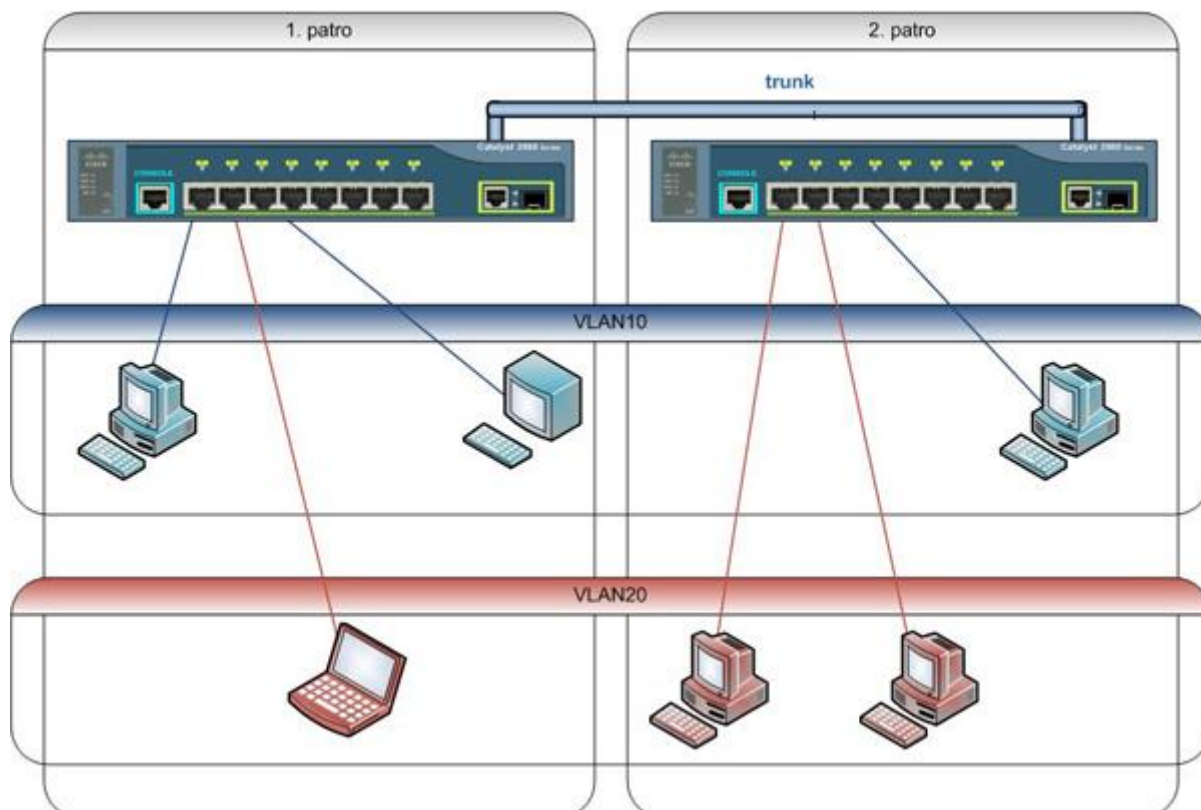
Jako trunk označujeme port, který je zařazen do více VLAN.

- ✓ Co je PVID?

Port VLAN identifer – značkování paketů během vstupního procesu

Typické použití VLAN

Máme dvě patra, na každém patře je switch, switche jsou propojeny páteří s trunkem. Chceme propojit zařízení do dvou nezávislých skupin (modrá - VLAN10 a červená VLAN20).



a) 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 provozu, který nemusí být propojen do celé sítě, ale přesto jej potřebujeme dostat na různá místa, navíc nechceme, aby nám ovlivňoval běžný provoz. Příkladem je například IP telefonie, komunikace mezi AP v centrálně řízeném prostředí, management (zabezpečení správcovského přístupu k zařízením). Například pro IP telefonii, kde je použití VLAN naprosto běžné, nám stačí jediná zásuvka, kam přivedeme VLAN pro telefonii i VLAN s přístupem do sítě a v telefonu se komunikace rozdělí. Navíc VLANy můžeme použít spolu s QoS pro zaručení kvality komunikace (obsazení pásma).
- **snížení HW** - samozřejmě se nám nesnižuje potřebný počet portů (až na speciální případy jako IP telefonie), ale tím, že mohou být různé podsítě na stejném switchi, jej můžeme lépe využít (například pro propojení tří zařízení nepotřebujeme speciální switch, který má minimálně 8 portů).

IEEE 802.1q tagging

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 informací, 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

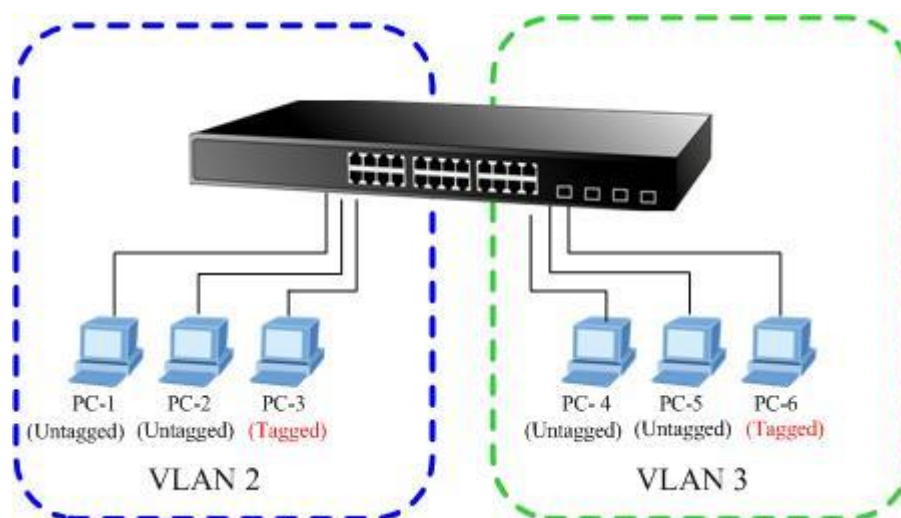
6B	6B	4B	2B	64 až 1500B	4B
cílová adresa (DA)	zdrojová adresa (SA)	802.1q tag	typ nebo délka	data	kontrolní součet (FCS)

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		

b) Příklady VLAN

➤ Příklad 1: Dvě oddělené VLANY



VLAN Skupina	VID	Netagovaní členi	Tagovaní členi
VLAN Skupina 1	1	Port-7~Port-24	N/A
VLAN Skupina 2	2	Port-1,Port-2	Port-3
VLAN Skupina 3	3	Port-4,Port-5	Port-6

Netagovaný paket vstupuje do VLAN 2.

1. Když [PC-1] posílá **netagovaný** paket na **Port-1**, switch ho otaguje s **VLAN Tag=2**. [PC-2] a [PC-3] přijme paket z **Port-2** a **Port-3**.
2. [PC-4],[PC-5] a [PC-6] nepřijme žádný paket.
3. Když pakety opouští **Port-2**, tak je tag ořezán na **netagovaný** paket.
4. Když pakety opouští **Port-3**, tak zůstane **tagovaný VLAN Tag=2**.

Tagovaný paket vstupuje do VLAN 2:

5. Když [PC-3] vysílá tagovaný paket s **VLAN Tag=2** vstupuje do **Port-3**, [PC-1] a [PC-2] přijme paket skrz **Port-1** a **Port-2**.
6. Když paket opouští **Port-1** a **Port-2**, bude ořezán tag a stane se z něj netagovaný paket.

Netagovaný paket vstupuje do VLAN 3:

1. Když [PC-4] vysílá **netagovaný** paket přes **Port-4**, switch ho otaguje s **VLAN Tag=3**. [PC-5] a [PC-6] přijme paket skrze **Port-5** a **Port-6**.
2. Když paket odchází z **Port-5**, bude ořezán tak a stane se z něj **netagovaný** paket.

3. Když paket odchází **Port-6**, tak zůstane paket **tagován s VLAN Tag=3**.

Nastavení

1. Vytvořte VLAN skupinu

Nastavte VLAN Group 1 = Default-VLAN s VID (VLAN ID) =1

Přidejte 2 VLANy – VLAN 2 a VLAN 3

VLAN Group 2 s VID=2

VLAN Group 3 s VID=3

VLAN Membership Configuration

Add VLAN

VLAN ID

(VID: 1~4094)

VLAN Group List

(Maximum 256 VLAN Groups)

1 2 3

2. Přiřadte člena VLANy :

VLAN 2 : Port-1,Port-2 a Port-3

VLAN 3 : Port-4, Port-5 a Port-6

VLAN 1 : Všechny ostatní – Port-7~Port-24

VLAN Member Setup

VLAN ID: 2			
Port	Member	Port	Member
Port 1	<input checked="" type="checkbox"/>	Port 13	<input type="checkbox"/>
Port 2	<input checked="" type="checkbox"/>	Port 14	<input type="checkbox"/>
Port 3	<input checked="" type="checkbox"/>	Port 15	<input type="checkbox"/>
Port 4	<input type="checkbox"/>	Port 16	<input type="checkbox"/>
Port 5	<input type="checkbox"/>	Port 17	<input type="checkbox"/>
Port 6	<input type="checkbox"/>	Port 18	<input type="checkbox"/>
Port 7	<input type="checkbox"/>	Port 19	<input type="checkbox"/>
Port 8	<input type="checkbox"/>	Port 20	<input type="checkbox"/>
Port 9	<input type="checkbox"/>	Port 21	<input type="checkbox"/>
Port 10	<input type="checkbox"/>	Port 22	<input type="checkbox"/>
Port 11	<input type="checkbox"/>	Port 23	<input type="checkbox"/>
Port 12	<input type="checkbox"/>	Port 24	<input type="checkbox"/>

VLAN Member Setup

VLAN ID: 3			
Port	Member	Port	Member
Port 1	<input type="checkbox"/>	Port 13	<input type="checkbox"/>
Port 2	<input type="checkbox"/>	Port 14	<input type="checkbox"/>
Port 3	<input type="checkbox"/>	Port 15	<input type="checkbox"/>
Port 4	<input checked="" type="checkbox"/>	Port 16	<input type="checkbox"/>
Port 5	<input checked="" type="checkbox"/>	Port 17	<input type="checkbox"/>
Port 6	<input checked="" type="checkbox"/>	Port 18	<input type="checkbox"/>
Port 7	<input type="checkbox"/>	Port 19	<input type="checkbox"/>
Port 8	<input type="checkbox"/>	Port 20	<input type="checkbox"/>
Port 9	<input type="checkbox"/>	Port 21	<input type="checkbox"/>
Port 10	<input type="checkbox"/>	Port 22	<input type="checkbox"/>
Port 11	<input type="checkbox"/>	Port 23	<input type="checkbox"/>
Port 12	<input type="checkbox"/>	Port 24	<input type="checkbox"/>

Nezapomeňte odstranit Port 1 – Port 6 z VLAN 1 membership, protože Port 1 – Port 6 musí být přiřazen do VLAN 2 a VLAN 3.

V tomto příkladě nechceme, aby se nám členství některých portů překrývalo.

VLAN Member Setup

VLAN ID: 1			
Port	Member	Port	Member
Port 1	<input type="checkbox"/>	Port 13	<input checked="" type="checkbox"/>
Port 2	<input type="checkbox"/>	Port 14	<input checked="" type="checkbox"/>
Port 3	<input type="checkbox"/>	Port 15	<input checked="" type="checkbox"/>
Port 4	<input type="checkbox"/>	Port 16	<input checked="" type="checkbox"/>
Port 5	<input type="checkbox"/>	Port 17	<input checked="" type="checkbox"/>
Port 6	<input type="checkbox"/>	Port 18	<input checked="" type="checkbox"/>
Port 7	<input checked="" type="checkbox"/>	Port 19	<input checked="" type="checkbox"/>
Port 8	<input checked="" type="checkbox"/>	Port 20	<input checked="" type="checkbox"/>
Port 9	<input checked="" type="checkbox"/>	Port 21	<input checked="" type="checkbox"/>
Port 10	<input checked="" type="checkbox"/>	Port 22	<input checked="" type="checkbox"/>
Port 11	<input checked="" type="checkbox"/>	Port 23	<input checked="" type="checkbox"/>
Port 12	<input checked="" type="checkbox"/>	Port 24	<input checked="" type="checkbox"/>

Apply Refresh

3. Přiřaďte PVID pro každý port:

Port-1,Port-2 a Port-3 : PVID=2

Port-4,Port-5 a Port-6 : PVID=3

Port-7~Port-24 : PVID=1

4. Zapněte VLAN Tag pro specifické porty

Link Type : Port-3 (VLAN-2) a Port-6 (VLAN-3)

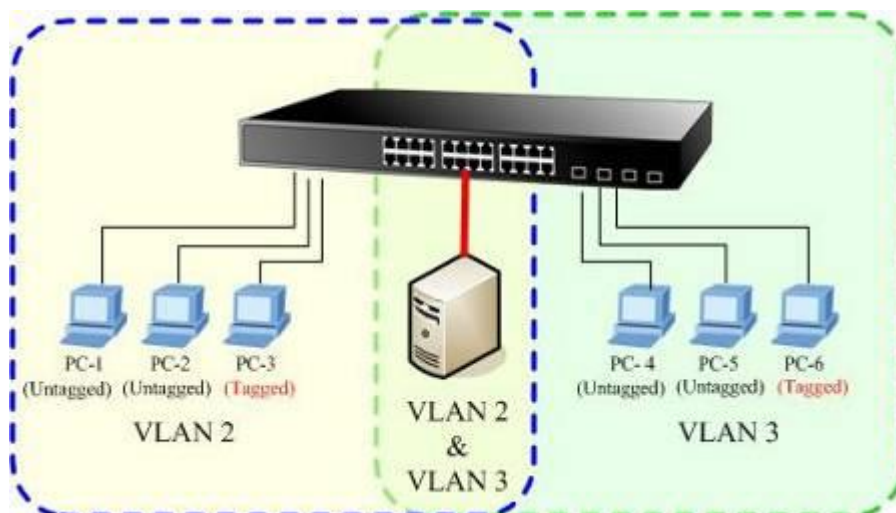
VLAN Port Configuration

VLAN Type 802.1Q VLAN

Port	PVID	Link Type	Ingress Filtering Enabled	Acceptable Frame Type	Q-in-Q Mode
1	2	UnTag	<input type="checkbox"/>	All	Disabled
2	2	UnTag	<input type="checkbox"/>	All	Disabled
3	2	Tag	<input type="checkbox"/>	All	Disabled
4	3	UnTag	<input type="checkbox"/>	All	Disabled
5	3	UnTag	<input type="checkbox"/>	All	Disabled
6	3	Tag	<input type="checkbox"/>	All	Disabled
7	1	UnTag	<input type="checkbox"/>	All	Disabled
8	1	UnTag	<input type="checkbox"/>	All	Disabled

➤ Příklad 2: Dvě VLANy s překrývající se oblastí

Následujte příklad 1, dvě oddělené sítě, ale s přístupem na stejný server. Například 2 sítě budou sdílet stejný NAS server.



1. Nastavte **Port-7** pro připojení zařízení k serveru.
2. Přiřadte **Port-7** do obou **VLAN 2** a **VLAN 3** ve VLAN Member konfiguraci.

VLAN Member Setup

VLAN ID: 2			
Port	Member	Port	Member
Port 1	<input checked="" type="checkbox"/>	Port 13	<input type="checkbox"/>
Port 2	<input checked="" type="checkbox"/>	Port 14	<input type="checkbox"/>
Port 3	<input checked="" type="checkbox"/>	Port 15	<input type="checkbox"/>
Port 4	<input type="checkbox"/>	Port 16	<input type="checkbox"/>
Port 5	<input type="checkbox"/>	Port 17	<input type="checkbox"/>
Port 6	<input type="checkbox"/>	Port 18	<input type="checkbox"/>
Port 7	<input checked="" type="checkbox"/>	Port 19	<input type="checkbox"/>
Port 8	<input type="checkbox"/>	Port 20	<input type="checkbox"/>
Port 9	<input type="checkbox"/>	Port 21	<input type="checkbox"/>
Port 10	<input type="checkbox"/>	Port 22	<input type="checkbox"/>
Port 11	<input type="checkbox"/>	Port 23	<input type="checkbox"/>
Port 12	<input type="checkbox"/>	Port 24	<input type="checkbox"/>

Apply Refresh

VLAN Member Setup

VLAN ID: 3			
Port	Member	Port	Member
Port 1	<input type="checkbox"/>	Port 13	<input type="checkbox"/>
Port 2	<input type="checkbox"/>	Port 14	<input type="checkbox"/>
Port 3	<input type="checkbox"/>	Port 15	<input type="checkbox"/>
Port 4	<input checked="" type="checkbox"/>	Port 16	<input type="checkbox"/>
Port 5	<input checked="" type="checkbox"/>	Port 17	<input type="checkbox"/>
Port 6	<input checked="" type="checkbox"/>	Port 18	<input type="checkbox"/>
Port 7	<input checked="" type="checkbox"/>	Port 19	<input type="checkbox"/>
Port 8	<input type="checkbox"/>	Port 20	<input type="checkbox"/>
Port 9	<input type="checkbox"/>	Port 21	<input type="checkbox"/>
Port 10	<input type="checkbox"/>	Port 22	<input type="checkbox"/>
Port 11	<input type="checkbox"/>	Port 23	<input type="checkbox"/>
Port 12	<input type="checkbox"/>	Port 24	<input type="checkbox"/>

Apply Refresh

2. Definujte **VLAN 1** jako “**Veřejnou oblast**” která překryje oba **VLAN 2** členy a **VLAN 3** členy.

VLAN Member Setup

VLAN ID: 1			
Port	Member	Port	Member
Port 1	<input checked="" type="checkbox"/>	Port 13	<input checked="" type="checkbox"/>
Port 2	<input checked="" type="checkbox"/>	Port 14	<input checked="" type="checkbox"/>
Port 3	<input checked="" type="checkbox"/>	Port 15	<input checked="" type="checkbox"/>
Port 4	<input checked="" type="checkbox"/>	Port 16	<input checked="" type="checkbox"/>
Port 5	<input checked="" type="checkbox"/>	Port 17	<input checked="" type="checkbox"/>
Port 6	<input checked="" type="checkbox"/>	Port 18	<input checked="" type="checkbox"/>
Port 7	<input checked="" type="checkbox"/>	Port 19	<input checked="" type="checkbox"/>
Port 8	<input checked="" type="checkbox"/>	Port 20	<input checked="" type="checkbox"/>
Port 9	<input checked="" type="checkbox"/>	Port 21	<input checked="" type="checkbox"/>
Port 10	<input checked="" type="checkbox"/>	Port 22	<input checked="" type="checkbox"/>
Port 11	<input checked="" type="checkbox"/>	Port 23	<input checked="" type="checkbox"/>
Port 12	<input checked="" type="checkbox"/>	Port 24	<input checked="" type="checkbox"/>

Apply Refresh

4. Nastavte **Port-7** s “**PVID=1**” ve VLAN Per Port konfiguraci.

VLAN Port Configuration

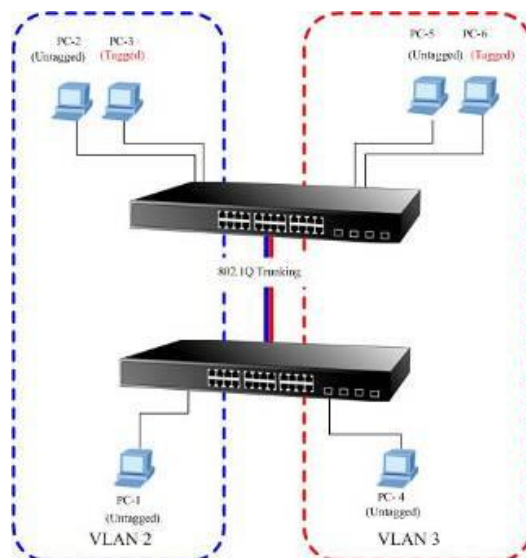
VLAN Type 802.1Q VLAN

Port	PVID	Link Type	Ingress Filtering Enabled	Acceptable Frame Type	Q-in-Q Mode
1	2	UnTag	<input type="checkbox"/>	All	Disabled
2	2	UnTag	<input type="checkbox"/>	All	Disabled
3	2	Tag	<input type="checkbox"/>	All	Disabled
4	3	UnTag	<input type="checkbox"/>	All	Disabled
5	3	UnTag	<input type="checkbox"/>	All	Disabled
6	3	Tag	<input type="checkbox"/>	All	Disabled
7	1	UnTag	<input type="checkbox"/>	All	Disabled
8	1	UnTag	<input type="checkbox"/>	All	Disabled

Přestože jsou Port-1 až Port-3 (VLAN 2) a Port-4 až port Port-6 (VLAN 3) ve stejné VLANě 1, tak pakety s VLAN 2 od VLAN 3 (a naopak) nemohou dostat, protože mají jiné PVID.

➤ Příklad 3: VLAN Trunk mezi dvěma 802.1Q switchi

Nejčastěji se používá pro “Uplink” mezi ostatními switchi. VLANs jsou odděleny ve switchi, ale potřebují přístup na ostatní switche se stejnou VLAN skupinou.



Postup:

VLANy nastavíme jako v předchozích příkladech. Následuje postup pro nastavení Trunk portu.

1. Nastavte **Port-8** jako 802.1Q VLAN **Trunk port**, Trunk port musí být **tagovaný** při vstupu.

8 1 Tag Tagged Only Disabled

2. Přiřadte VLAN Trunk Port aby byl člen každé VLAN – tu kterou chcete do Trunku zapojit. V tomto příkladě, přidejte **Port-8 do VLAN 2 a VLAN 3** member port.

VLAN Member Setup

VLAN ID: 2			
Port	Member	Port	Member
Port 1	<input checked="" type="checkbox"/>	Port 13	<input type="checkbox"/>
Port 2	<input checked="" type="checkbox"/>	Port 14	<input type="checkbox"/>
Port 3	<input checked="" type="checkbox"/>	Port 15	<input type="checkbox"/>
Port 4	<input type="checkbox"/>	Port 16	<input type="checkbox"/>
Port 5	<input type="checkbox"/>	Port 17	<input type="checkbox"/>
Port 6	<input type="checkbox"/>	Port 18	<input type="checkbox"/>
Port 7	<input type="checkbox"/>	Port 19	<input type="checkbox"/>
Port 8	<input checked="" type="checkbox"/>	Port 20	<input type="checkbox"/>
Port 9	<input type="checkbox"/>	Port 21	<input type="checkbox"/>
Port 10	<input type="checkbox"/>	Port 22	<input type="checkbox"/>
Port 11	<input type="checkbox"/>	Port 23	<input type="checkbox"/>
Port 12	<input type="checkbox"/>	Port 24	<input type="checkbox"/>

Apply Refresh

VLAN Member Setup

VLAN ID: 3			
Port	Member	Port	Member
Port 1	<input type="checkbox"/>	Port 13	<input type="checkbox"/>
Port 2	<input type="checkbox"/>	Port 14	<input type="checkbox"/>
Port 3	<input type="checkbox"/>	Port 15	<input type="checkbox"/>
Port 4	<input checked="" type="checkbox"/>	Port 16	<input type="checkbox"/>
Port 5	<input checked="" type="checkbox"/>	Port 17	<input type="checkbox"/>
Port 6	<input checked="" type="checkbox"/>	Port 18	<input type="checkbox"/>
Port 7	<input type="checkbox"/>	Port 19	<input type="checkbox"/>
Port 8	<input checked="" type="checkbox"/>	Port 20	<input type="checkbox"/>
Port 9	<input type="checkbox"/>	Port 21	<input type="checkbox"/>
Port 10	<input type="checkbox"/>	Port 22	<input type="checkbox"/>
Port 11	<input type="checkbox"/>	Port 23	<input type="checkbox"/>
Port 12	<input type="checkbox"/>	Port 24	<input type="checkbox"/>

Apply Refresh

3. Opakujte postup 1 a 2 pro nastavení VLAN Trunk port na partnerském switchi.

QoS (quality of service)

Teorie a cíl: umožnit nastavení určité kvality přenosu pro data přenášená sítí, QoS dokáže rozlišovat mezi jednotlivými přenosy a každému typu nastavit jinou kvalitu.

a) QoS aplikace

- **delay - zpoždění** - data dorazí do cíle příliš pozdě, skládá se z propagace (jak rychle se šíří signál médiem), serializace (jak rychle můžeme data vkládat na linku, musí jít za sebou), zpracování (routery na cestě), zdržení ve frontách, dejitter buffer a další
- **jitter - variace zpoždění** - pakety dosáhnou rozdílného zpoždění, hlavně záleží na frontách po cestě
- **packet loss - ztrátovost** - paket se ztratí cestou (error) nebo je zahozen (kvůli propustnosti, dropped packet), pokud se ztratí, tak se musí vyslat znovu, navíc se změní pořadí
- **out-of-order delivery - doručení mimo pořadí** - pakety mohou putovat různou cestou nebo se vysílají znovu
- **bandwidth - šířka pásma** - je využíváno nárazově a nehospodárně (stahování velkého souboru může vzít pásmo telefonii), můžeme komprimovat hlavičky paketů (které mohou být větší než datový obsah)

Mechanismy:

Differentiated services – DiffServ

dnešní hlavní metoda, řeší se per router, pakety se rozdělí do tříd podle typu při příchodu na router, tato klasifikace se může zaznamenat do hlavičky paketu, s třídami se zachází podle konfigurovaných parametrů

Klasifikace se provádí na hranici sítě a nastavuje Differentiated Services Code Point (DSCP)

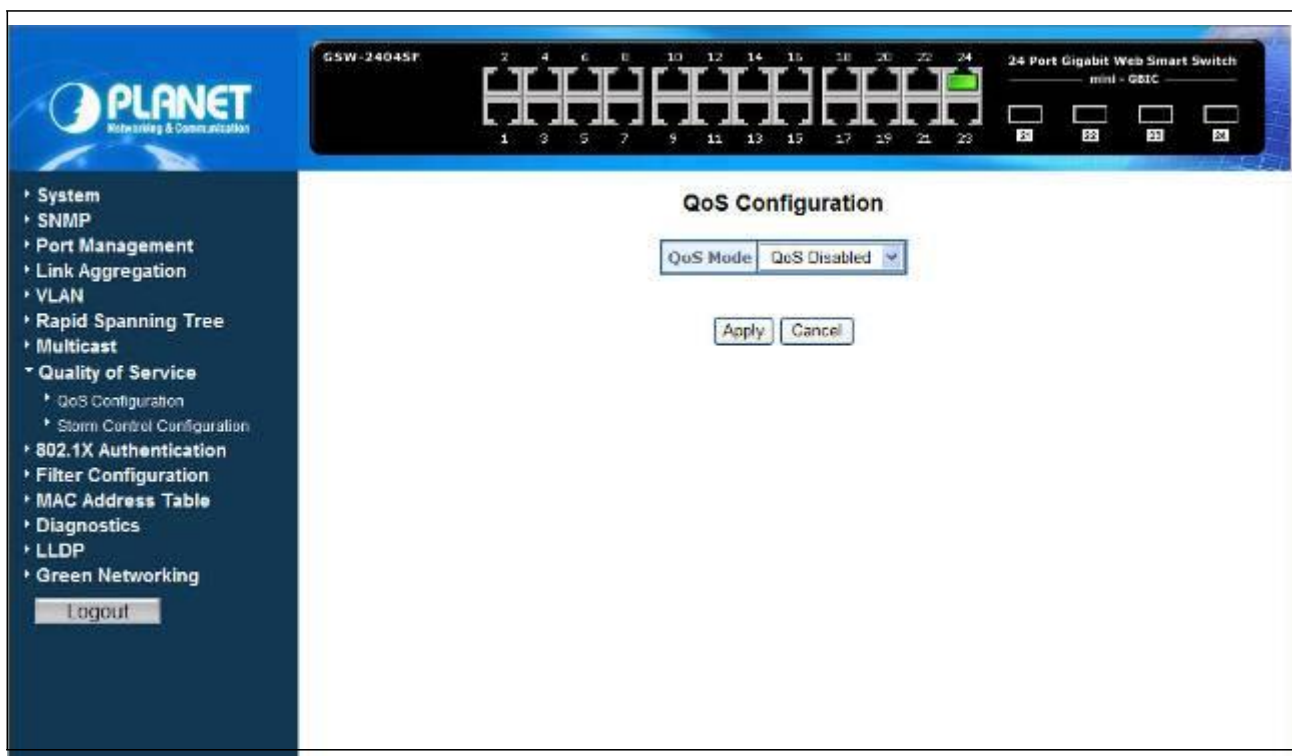
802.1p

Priorita je zapsána do VLAN tagu.

b) QoS Konfigurace

Módy QoS na switchích Planet:

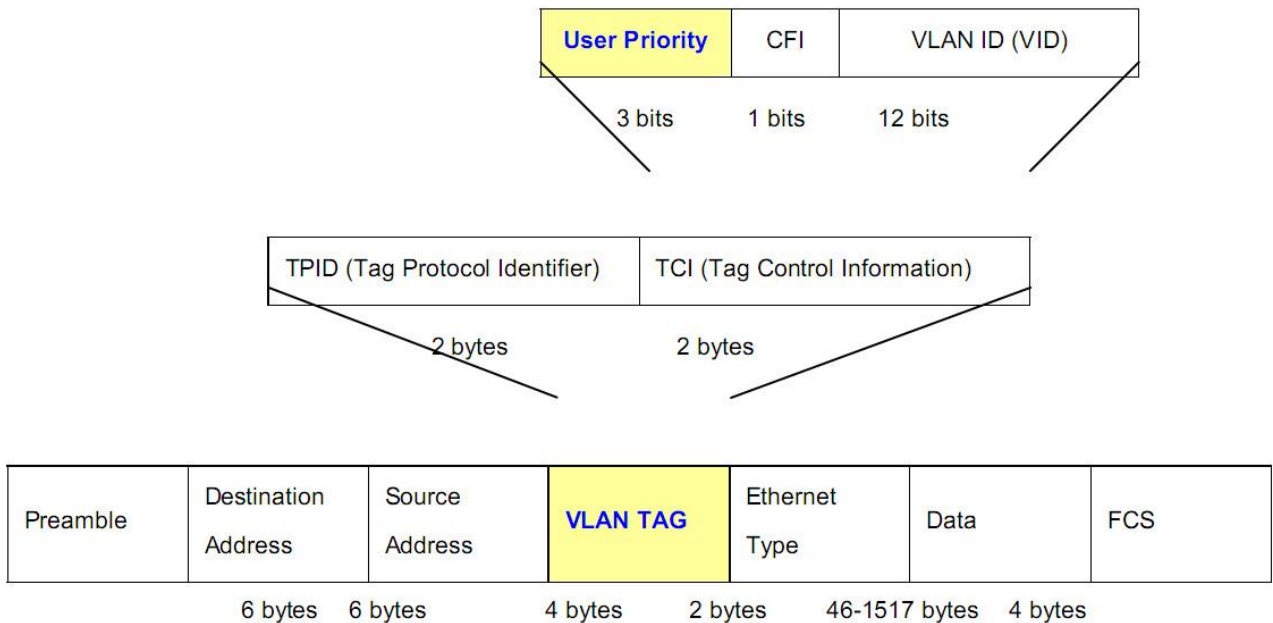
- **QoS Disabled** - QoS vypnuto
- **802.1p Mode** – fronta je řízena na základě IEEE802.1p VLAN priority tag
- **DSCP Mode** - fronta je řízena na základě DSCP



802.1p QoS Mode

Pokud je 802.1p Tag Priority aplikován, tak switch rozezná 802.1Q VLAN tag pakety a rozbalí VLAN tagované pakety s hodnotou priority.

802.1Q Tag a 802.1p priority



IEEE 802.1p specifikuje 8 úrovní priorit.

The screenshot shows the Planet switch web interface for a GSW-2404SF 24 Port Gigabit Web Smart Switch. The QoS Configuration page is displayed, showing the following settings:

- QoS Mode: 802.1p
- Prioritize Traffic: Custom

The 802.1p Configuration table is shown below:

802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority
0	Normal	1	Low	2	Low	3	Normal
4	Medium	5	Medium	6	High	7	High

Buttons for Apply and Cancel are visible at the bottom of the configuration table.

Je možné nastavit priority manuálně (custom) nebo nastavit vše se stejnou prioritou (Nízká / Normální / Střední)

QoS Configuration

QoS Mode	802.1p
Prioritize Traffic	Custom


Custom
 All Low Priority
 All Normal Priority
 All Medium Priority
 All High Priority

DSCP QoS Mode

DiffServ Code Point (DSCP)


Priorizace provozu je obsažena IP hlavičce, která je kódována aplikací nebo jiným aktivním prvkem

Přiřazení priorit k jednotlivým DSCP hodnotám:



PLANET
Networking & Communications

GSW-2404SF



24 Port Gigabit Web Smart Switch
mini - GBIC

- System
- SNMP
- Port Management
- Link Aggregation
- VLAN
- Rapid Spanning Tree
- Multicast
- ▾ Quality of Service
 - QoS Configuration
 - Storm Control Configuration
- 802.1X Authentication
- Filter Configuration
- MAC Address Table
- Diagnostics
- LLDP
- Green Networking

Logout

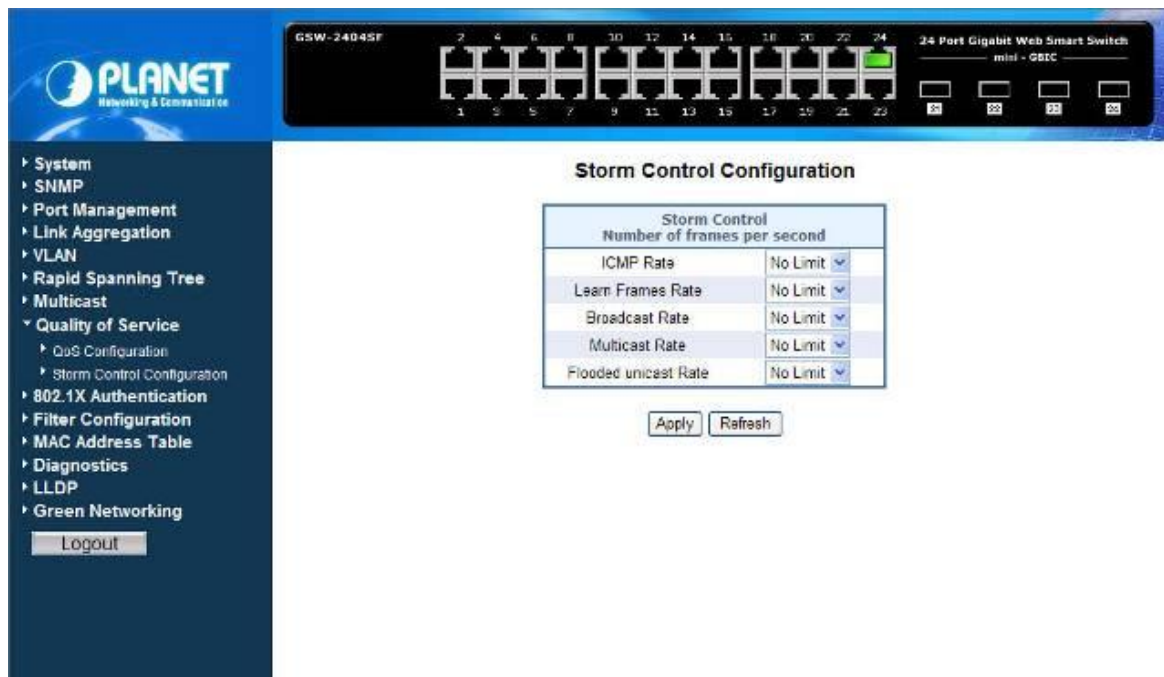
QoS Configuration

QoS Mode	DSCP
Prioritize Traffic	All High Priority

DSCP Configuration	
DSCP Value(0..63)	Priority
	High
	High
	High
	High
	High
	High
	High
	High
All others	High

c) Storm Control konfigurace

Storm control přechází zahlcení sítě "bouří" broadcastů, multicastů či unicastů na svých fyzických interfacech.



Položka	Popis
ICMP Rate	Omezení velikosti ICMP provozu
Learn Frames Rate	Funkce umožňuje filtrovat naučené rámce
Broadcast Rate	Omezení velikosti Broadcastů
Multicast Rate	Omezení velikosti Multicastů
Flooded unicast Rate	Omezení velikosti Unicastů

Rapid Spanning Tree (RSTP)

a) Terorie

- Záložní linka mezi switchi nebo routery
- Zamezuje vzniku nechtěných smyček
- Aktivní je vždy jen jedna linka
- Automaticky se přizpůsobuje, když měníme topologii sítě

STP – Spanning Tree Protocol (IEEE 802.1D)

RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)

Spanning Tree Protocol (STP)

- Eliminace smyček
- Doba přepnutí na záložní linku 30 – 50s

Bridge Protocol Data Units (BPDU)

STP komunikuje mezi switchi za použití "Bridge Protocol Data Units (BPDU)". Každé BDU obsahuje:

- Unikátní identifikátor, který říká kdo je root switch
- Délku cesty, kterou paket urazil od vysílacího portu k root switchi
- Port identifikátor vysílacího portu

Komunikace mezi switchi pomocí BPDU zajišťuje:

- Jeden switch je zvolen jako "root" switch
- Kalkulace nejkratší cesty mezi root switchem a ostatními switchi
 - ➔ je určen nejvhodnější switch, přes který bude paket poslán root switchi
 - ➔ je určen nejlepší port na každém switchi, přes který bude paket poslán root switchi

Vytvoření stabilní STP Topologie

- V automatickém nastavení switch s nejnižší MAC adresou bude zvolen root switchem
- Snížením "Priority number" můžete zvýšit prioritu switche, aby se stal rootem
- Snížením "Port Priority" můžete zvýšit prioritu portu, který tak bude ve stavu Forwarding

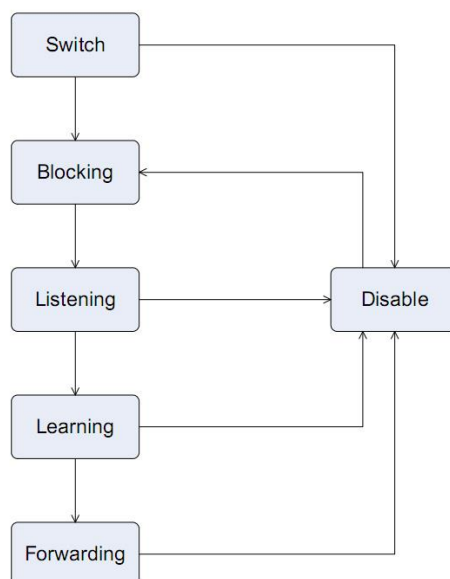
STP Port stavy

Např. po změně topologie sítě musí port projít následujícími 5ti stavy:

- **Blocking** – port je blokován
- **Listening** – port čeká na příjem BPDU
- **Learning** – port si přidává adresy do forwarding databáze
- **Forwarding** – port forwarduje pakety
- **Disabled** – port pouze odpovídá na síťový management

Změny stavu portu:

- Od initialization (boot switch) → blocking
- Od blocking → listening nebo → disabled
- Od listening → learning nebo → disabled
- Od learning → forwarding nebo → disabled
- Od forwarding → disabled
- Od disabled → blocking



RSTP je každý port buď ve stavu forwarding, blocking, nebo learning.

Srovnání stavu portu STP-RSTP		
Operativní stav	STP	RSTP
Enabled	Blocking	Discarding (blocking)
Enabled	Listening	Discarding (blocking)
Enabled	Learning	Learning
Enabled	Forwarding	Forwarding
Disabled	Disabled	Discarding (blocking)

b) Nastavení parametrů STP

Na úrovni switche:

Parametr	Popis	Základní hodnota
Bridge Identifier	Nastavitelná 16-bit priorita + 48-bit MAC adresa.	32768 + MAC
Priority	Priorita pro switch. Nižší znamená vyšší priorita → Switch může být rootem	32768
Hello Time	Doba mezi broadcastem "Hello"	2s
Maximum Age Timer	Doba zaslání nového BPDU	20s
Forward Delay Timer	Jak dlouho port stráví stavem learning a listening a čekáním na nové BPDU, kterého může vrátit do stavu	15s

Na úrovni portu:

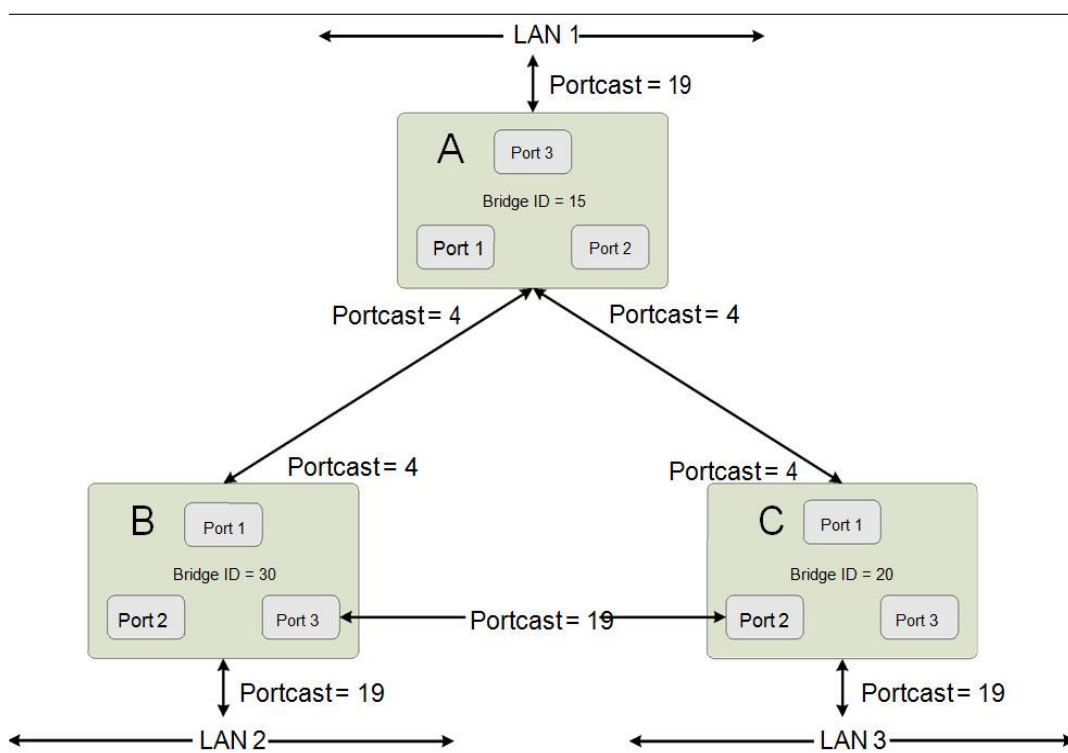
Parametr	Popis	Základní hodnota
Port Priority	Priorita každého portu Nižší hodnota = vyšší priorita -> může se stát root portem	128
Port Cost	Hodnota pro výpočet nejlepší trasy	200,000- 100Mbps Fast Ethernet porty

Defaultní nastavení

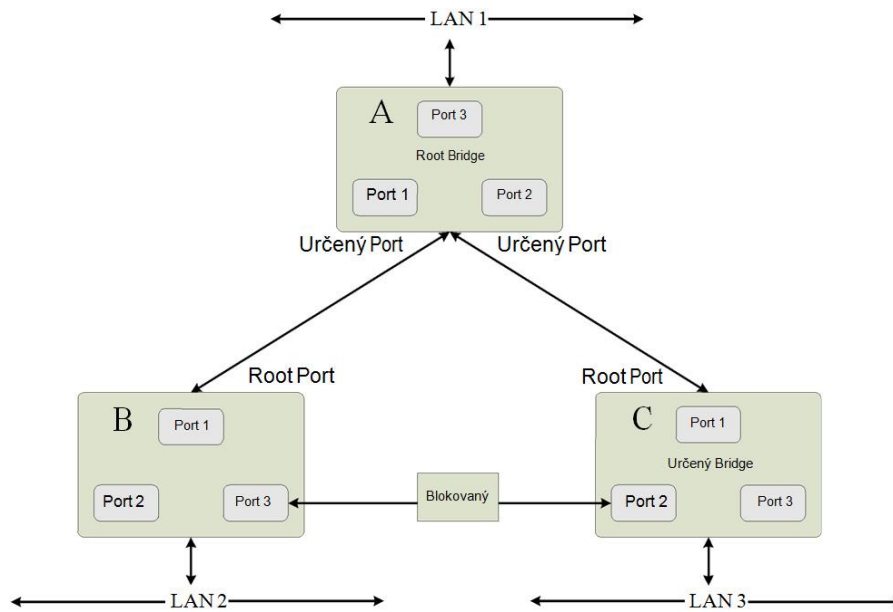
Funkce	Defaultní hodnota
Enable state	STP disabled for all ports
Port priority	128
Port cost	0
Bridge Priority	32,768

Ilustrace STP

Bez STP by broadcast paket ze switche do A do switche B pokračoval do switche C, zpět do A a pak pořád dokola:



S STP broadcasting paket ze switch A do B skončí v portu 3 switch B a dále již nepokračuje:

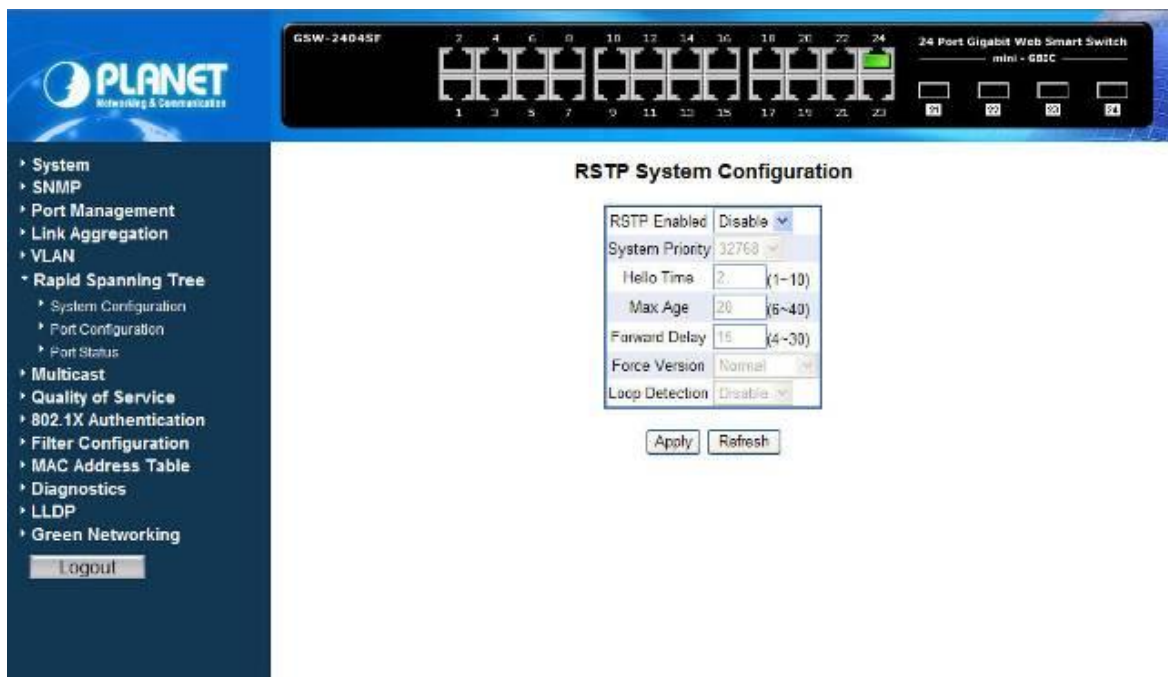


RSTP System Configuration

Spanning Tree protokoly:

- **Compatiable = Spanning Tree Protocol (STP)** (ve skutečnosti stále RSTP, ale bude spolupracovat s jiným pouze STP switchem)
- **Normal = Rapid Spanning Tree Protocol (RSTP)**

Rapid Spanning Tree System Configuration:



RSTP System Configuration

RSTP Enabled	Disable	▼
System Priority	32768	▼
Hello Time	2	(1~10)
Max Age	20	(6~40)
Forward Delay	15	(4~30)
Force Version	Normal	▼
Loop Detection	Disable	▼

Apply Refresh

Položka	Popis
RSTP Enabled	Enabled – zapnuto RSTP. Disabled - vypnuto RSTP. Defaultně je Disable .
System Priority	Priorita pro switch. Nižší znamená vyšší priorita Switch může být rootem Násobky 4096 (4K). Například 0, 4096, 8192...
Hello Time	Doba mezi broadcastem "Hello" = doba čekání na další konfigurační správu. Rozsah : 1-10 Defaultně 2s .
Max Age	Doba zaslání nového BPDU Rozsah : 6-40 Defaultně 20s .
Forward Delay	Jak dlouho port stráví stavem learning and listening a čekáním na nové BPDU, kterého může vrátit do stavu blocking. Rozsah : 4-30 Defaultně 15s .
Force Version	Normal (RSPT) / Compatible (STP)
Loop Detection	Zapne či vypne detekci smyčky.

- **Max Age** -. Mezi 6 and 40, musí být méně nebo stejně než " $(2 * \text{Bridge Forward Delay}) - 1$ " and vyšší nebo stejně " $2 * (\text{Bridge Hello Time} + 1)$ ". Defaultně je 20.
- **Hello Time** - musí být méně nebo stejně než " $(\text{Bridge Max Age} / 2) - 1$ ". Defaultně je 2
- **Forward Delay** - musí být méně nebo stejně než " $(\text{Bridge Max Age} / 2) + 1$ ".
Rozsah je od 4s do 30s. Defaultně je 15.

Port configuration - nastavení parametrů portů:

The screenshot shows the web management interface for a Planet GSW-2404SF switch. The top header displays the device name and a row of 24 ports. The main content area is titled "RSTP Port Configuration" and contains a table with the following data:

Port	Edge	Path Cost	Port Priority	Point2point
1	<input checked="" type="checkbox"/>	0	128	Auto
2	<input checked="" type="checkbox"/>	0	128	Auto
3	<input checked="" type="checkbox"/>	0	128	Auto
4	<input checked="" type="checkbox"/>	0	128	Auto
5	<input checked="" type="checkbox"/>	0	128	Auto
6	<input checked="" type="checkbox"/>	0	128	Auto
7	<input checked="" type="checkbox"/>	0	128	Auto
8	<input checked="" type="checkbox"/>	0	128	Auto
9	<input checked="" type="checkbox"/>	0	128	Auto
10	<input checked="" type="checkbox"/>	0	128	Auto
11	<input checked="" type="checkbox"/>	0	128	Auto
12	<input checked="" type="checkbox"/>	0	128	Auto
13	<input checked="" type="checkbox"/>	0	128	Auto
14	<input checked="" type="checkbox"/>	0	128	Auto
15	<input checked="" type="checkbox"/>	0	128	Auto

Položka	Popis
Port	Port 1 to port 24
Edge	Zapne nebo vypne funkci
Path Cost	Hodnota pro výpočet nejlepší trasy. Nižší hodnota -> vyšší priorita. Rozsah : 1 až 200000000. - automaticky – 0 - Ethernet - 2000000 - Fast Ethernet - 200000 - Gigabit Ethernet - 20000
Port Priority	Hodnota priority portu, defaultně je “128” .
Point2Point	Kontroluje, zda jsou porty připojeny v režimu point-to-point LAN (rychlejší přechody ke stavu forwarding)) místo ke sdílenému médiu. Možnosti: Force True Force False Auto (defaultní hodnota)

Typy portů / linek

point-to-point, tedy spoj bod-bod, připojení dalšího switche, linka musí být full duplex

edge, koncový/hraniční port (PortFast), je do něj připojeno koncové zařízení (jako PC či tiskárna) i když je port nastavený jako edge, tak stále monitoruje BPDU. V případě detekování BPDU se přepne na non-edge

shared, sdílená linka, například hub, linka je half duplex

Port Status

The screenshot shows the Planet GSW-2404SF web interface. On the left is a navigation menu with options like System, SNMP, Port Management, Link Aggregation, VLAN, Rapid Spanning Tree, Multicast, Quality of Service, 802.1X Authentication, Filter Configuration, MAC Address Table, Diagnostics, LLDP, and Green Networking. The main content area displays two tables:

RSTP VLAN Bridge Overview

VLAN ID	Bridge ID	Hello Time	Max Age	Fwd Delay	Topology	Root ID
4096	32768 00-30-4f-00-00-03	2	20	15	Steady	This switch is Root!

Refresh

RSTP Port Status

Port/Group	VLAN ID	Path Cost	Edge Port	P2P Port	Protocol	Port State
Port 1	4096	20000	Yes	Yes	RSTP	Forwarding
Port 2						Disabled
Port 3						Disabled
Port 4						Disabled
Port 5						Disabled
Port 6						Disabled
Port 7						Disabled
Port 8						Disabled
Port 9						Disabled
Port 10						Disabled
Port 11						Disabled

RSTP VLAN Bridge Overview

RSTP VLAN Bridge Overview						
VLAN ID	Bridge ID	Hello Time	Max Age	Fwd Delay	Topology	Root ID
4096	32768:00-30-4f-00-00-03	2	20	15	Steady	This switch is Root!

Refresh

Položka	Popis
VLAN ID	Identifikuje VLANy asociované s RSTP
Topology	Ukazuje změnu topologie, pokud žádné změny nejsou tak "Steady".
Root ID	Ukazuje, zda je switch rootem.

RSTP Port Status - statistika RSTP na každém portu:

RSTP Port Status

Port/Group	VLAN ID	Path Cost	Edge Port	P2P Port	Protocol	Port State
Port 1	4096	20000	Yes	Yes	RSTP	Forwarding
Port 2						Disabled
Port 3						Disabled
Port 4						Disabled
Port 5						Disabled
Port 6						Disabled
Port 7						Disabled
Port 8						Disabled
Port 9						Disabled
Port 10						Disabled
Port 11						Disabled

RSTP Port Statistics - statistika provozu na portech:

The screenshot shows the Planet GSW-2404SF web interface. The main content area displays the 'RSTP Port Statistics' table. The table has the following structure:

Port	RSTP TX	RSTP RX	STP TX	STP RX	TCN TX	TCN RX	Unknown	Illegal
Port 1								
Port 2								
Port 3								
Port 4								
Port 5								
Port 6								
Port 7								
Port 8								
Port 9								
Port 10								
Port 11								
Port 12								
Port 13								
Port 14								
Port 15								
Port 16								
Port 17								

Položka	Popis
RSTP TX / RX	Počet RSTP konfiguračních BPDU.
STP TX / RX	Počet STP konfiguračních BPDU.
TCN TX / RX	Počet BPDU týkajících se změn topologie (Topology Change)
Unknown	Počet neznámých Spanning Tree BPDU přijmutých a odstraněných na portu.
Illegal	Počet ilegálních Spanning Tree BPDU přijmutých a odstraněných na portu.

6) PLANET TECHNOLOGY CORPORATION



Je jednou z vedoucích firem v oblasti IP sítí. Navrhuje a realizuje optimální řešení pro konvergenci dat, hlasu a videa pro podnikové sítě. Zaměřuje se na spokojenost zákazníků a reaguje na jejich potřeby v oblasti výroby pokročilých síťových řešení. Byla založena v roce 1993 skupinou počítačových inženýrů Wang Laboratories.

Díky svému elánu, tvrdé práci, inovativnímu myšlení a špičkovým znalostem v oblasti výpočetní techniky se dostala mezi světové firmy vyvíjející nejpokrokovější technologie. PLANET stále klade velký důraz na řešení od A do Z pro střední a malé podniky, stejně tak i pro velké instituce z oblasti vzdělávání, financí, zdravotnictví a státní správy. V září 2003 společnost dosáhla dalšího milníku ve své existenci a stala se veřejně obchodovatelnou společností na Taiwanském Counter Stock Exchange Market.

Pro potřeby trhu vyvíjí PLANET neustále vlastní produkty, které zavádějí inovace, jsou kvalitní, spolehlivé a efektivní. Jeho zkušený vývojový tým získal pro PLANET reputaci technických expertů, kteří jsou schopni vyvinout úplný sortiment síťových produktů nejvyšší kvality v celosvětovém měřítku. Dodávkami nejmodernější technologie uspokojuje portfolio produktů PLANET nejnáročnější požadavky, ať už jde o jednorázová nebo dlouhodobá a na míru šitá řešení.

- **Firemní cíle**

Dnes, stejně jako v minulosti, PLANET bude pokračovat ve vývoji špičkových řešení. Především bude dále garantovat dlouhotrvající filozofii poskytovat ve správnou dobu správný produkt za správnou cenu. Aby bylo možné tuto filozofii každodenně realizovat dodává PLANET na trh produkty s vynikajícím poměrem cena/výkon.

- **Závazek kvality**

Aby bylo možné garantovat tu nejvyšší kvalitu výrobků a služeb má PLANET certifikát ISO 9001. Ten podtrhuje jeho výkonnost a výjimečnost. Ta byla ostatně oceněna v řadě světových profesionálních a obchodních časopisech včetně Network Solution, PC Magazine, Internet Telephony, PC Direkt, PC Plus a dalšími, v nichž byly produkty PLANET oceněny za spolehlivost a vynikající výkon. PLANET skrze svoji distribuční síť vybavil svými výrobky řadu prestižních zákazníků a posílil tak svoje globální postavení na světovém trhu se síťovými technologiemi.

- **Globální distribuční síť**

Jedním z klíčů enormního úspěchu firmy PLANET je stále rostoucí počet prodejních kanálů na celém světě. Celkově již distribuuje své produkty ve více než 105-ti zemích. Poskytuje špičkovou technickou podporu a jeho distributoři jsou schopni poskytnout rychlé a efektivní řešení.



Všechna práva vyhrazena.

V dokumentu byl jako zdroj informací užit server Wikipedia.cz
Dokument nelze měnit nebo vydávat za vlastní bez souhlasu autora.