



Ethernet over Coax

**Ethernet a TV
po společném koaxiálním vedení**

**XL-PBW360C
XL-PB360C
XL-PB360CA**

Uživatelský návod

Úvodem	4
Specifikace	4
Použití.....	6
Instalace pro společné TV rozvody	6
Konverze koaxiálního kabelového systému na IP	8
Konverze krouceného páru na IP	9
Modely zařízení a jejich instalace	10
Master jednotka XL-PBW360C	10
Slave jednotka XL-PB360C.....	13
Slave jednotka XL-PB360CA.....	15
Technické detaily	17
Koexistence s jinými technologiemi v jednom kabelovém vedení	17
Spektrální vlastnosti.....	18
Kompatibilita s účastnickými TV zásuvkami:.....	20
Svislé a horizontální rozvody:.....	20
Hvězdicový rozvod:.....	22
Frekvenční charakteristika vestavěného diplexeru	23
Přenos napájení ve vedení.....	24
Kompatibilita s výrobky třetích stran	24
Přenosový výkon zařízení	25
Závislost přenosu na útlumu trasy	25
Úhrnný výkon	26
Simultánní Upload+Download.....	26
Download - TCP a Multicast.....	27
Upload	29
Úhrnný výkon v závislosti na počtu zařízení.....	30
Vliv omezení pásma na přenosový výkon	31
Přenosový výkon na kabeláži CAT5	32
Administrace zařízení.....	33
Přístup do rozhraní administrace	33
Hlavní nabídka	34
SLAVE - Authorization	35
SLAVE - Online	37
SLAVE - konfigurace jednotky	38
Slave Basic Information	38
Slave Configuration Information.....	39
Slave Configuration Information - rozdíly v užití s XL-PB360CA.....	41
Slave MAC Table	41
SLAVE- konfigurace XL-PB360CA	42
Wan configuration	42
Lan configuration	44
Static Route Configuration	44
Virtual Server Configuration.....	45
L2 Switch configuration.....	45
WiFi Basic Configuration	46
WiFi Management.....	47

WiFi Upgrade	48
SLAVE - Templates.....	49
SLAVE - MAC Limit	50
RF - Info.....	51
NETWORK - Status	52
NETWORK - Config.....	52
NETWORK - VLAN	52
NETWORK - SNID	52
NETWORK - Filter.....	53
NETWORK - Icmp.....	53
SERVICE - Service.....	54
SYSTEM - Information	54
SYSTEM - Running Sttaus.....	54
SYSTEM - Slave Type	54
SYSTEM - IP Access Control	54
SYSTEM - System Time	55
SYSTEM - System Log	55
SYSTEM - Account.....	55
SYSTEM - Reboot.....	56
SYSTEM - Factory	57
SYSTEM - Upgrade.....	57
SYSTEM - Backup	57
SYSTEM - SNMP.....	57
Web management XL-PB360CA.....	58
Zabezpečení sítě	60
Postup zabezpečení Masteru.....	60
Postup zabezpečení Slave	61
Vysvětlení tlačítka RST a jeho Továrního nastavení	61
Dodatečná zabezpečení Slave jednotek.....	62
Nastavení vnějšího firewallu	63
Příklady nastavení	64
Slave s routrem a WiFi - základní nastavení	64
Slave s routrem a WiFi - pokročilé nastavení.....	70
Nastavení pro Multicasting	72
IGMP aktivace na Masteru.....	72
Network Filter na Masteru	73
VLAN Mode Slave zařízení	74
Propojení oddělené komunikace MDU	77

Úvodem

Zařízení pro realizaci sítí přenosu Ethernetu a TV po společném koaxiálním rozvodu.

Hlavním určením zařízení Ethernet over Coax (zkratka EoC) je realizace obousměrné datové komunikace za užití společného koaxiálního TV rozvodu. Typicky jde o současný provoz TV a datové sítě nad rozvodem kabeláže určené původně jen pro přenos signálů DVB-T/T2.

Při jeho realizaci nepotřebujete žádné úpravy v existujícím koaxiálním rozvodu. Zařízení vám umožní realizovat vysokorychlostní síť pro přenos videa, hlasu a dat.

Specifikace

Zařízení sestávají z řídicí jednotky nazývané Master a klientských zařízení nazývaných Slave.

Master jednotka je v jednom segmentu sítě vždy jen jedna, zatímco klientských Slave zařízení lze instalovat na jeden koaxiální kabel až 253.

Použitá komunikační technologie je HomePlug AV+ a má signálovou rychlost více než 500Mbps.

Každé zařízení pracuje samostatně a ke své činnosti nepotřebuje instalaci žádného softwaru.

Přenosové vlastnosti:

- standard HomePlug AV+, čipová sada Atheros/Qualcom 7410 a 7411.
- úhrnná přenosová rychlost všech komunikujících zařízení na jednom kabelovém segmentu: >500Mbit/s
- počet zařízení na jednom koaxiálním kabelu: 253x Slave a 1x Master. Pro praktické užití vzhledem ke kapacitě jich nelze doporučit více než 50 na jeden kabelový segment.
- přenosový dosah závisí především od útlumu kabelu, např. pro kabel typu RG6 je dosah až 1,5km
- pracovní pásmo: 7,6MHz - 67,5MHz. Horní kmitočet lze uživatelsky nastavit na hodnotu mezi 30~67,5MHz.
- max. útlum na vedení pro docílení maximálních přenosových výkonů (~100Mbps): max. 60dB v pracovním pásmu
- max. útlum na vedení pro rychlosti nižší: max. 82dB v pracovním pásmu
- všechna zařízení mají vestavěný rozbočovač který dovoluje průchod kmitočetů vyšších než 75MHz, tj. průchodnost pro TV signál (typicky DVB-T/T2). Rozbočovač není průchozí pro DC (stejnoseměrnou) složku a nízké kmitočty (např. 22kHz signál).
- konektory F female, stoupání závitu tzv. imperiální (UNEF, typický pro naše území)
- přenosové médium je impedančně nezávislé, není nutné používat kabeláž s impedancí 75Ohm, zařízení lze použít pro jiné impedance a vedení není třeba terminovat ani používat baluny.
- zařízení přenáší jakýkoliv Ethernet provoz (tj. Layer 2) a je nezávislé na síťovém protokolu

- komunikace jednotlivých Slave zařízení jsou od sebe izolovány
- je možné použití i jiného metalického média než je koaxiální kabel
- nosné kmitočty využívány adaptivně, OFDM
- vestavěná podpora pro QoS prioritizaci
- podpora multicastu s IGMP
- doba startu systému a navázání spojení do 80 sekund od přivedení napájení

Fyzické vlastnosti:

- Pracovní teplota $-30^{\circ}\text{C} \sim +50^{\circ}\text{C}$, vlhkost 10-90%, nekondenzující
- Napájení externím adaptérem 12V DC, konektor 5,5/2,1mm.
- Chráněno proti zkratu na koaxiálním vedení i proti zkratu na výstupech napájení
- Chráněno proti přepólování
- Bez pohyblivých částí. Zařízení neobsahují ventilátory.

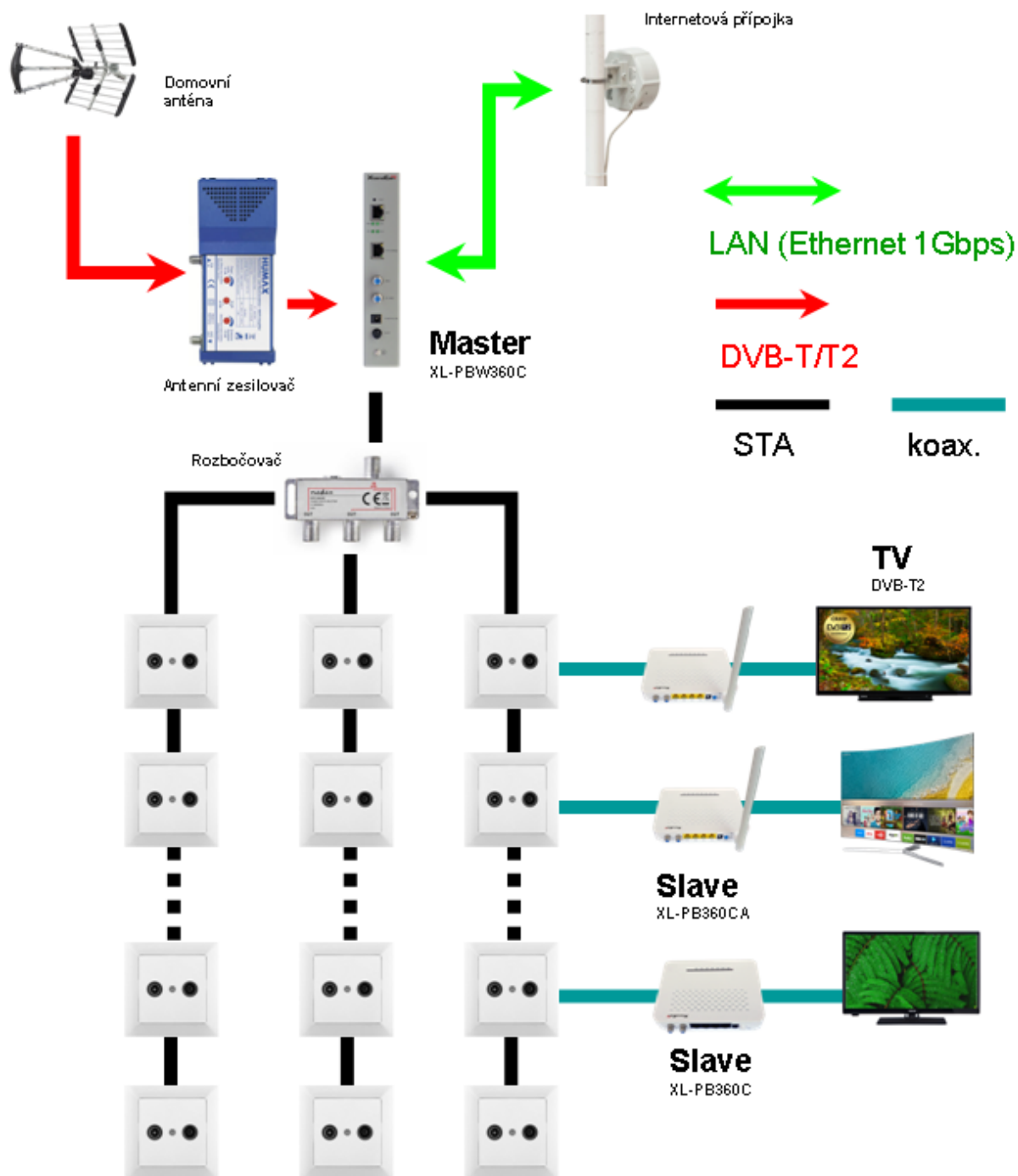
Použití

Instalace pro společné TV rozvody

Typické užití EoC zařízení je nasazení vytvoření datového kanálu v rozvodech společné TV antény aniž by se jakkoliv ovlivnila její funkčnost pro příjem DVB-T/T2.

Pro její realizaci nepotřebujete žádné úpravy v existujícím koaxiálním rozvodu.

Typické aplikační schéma:

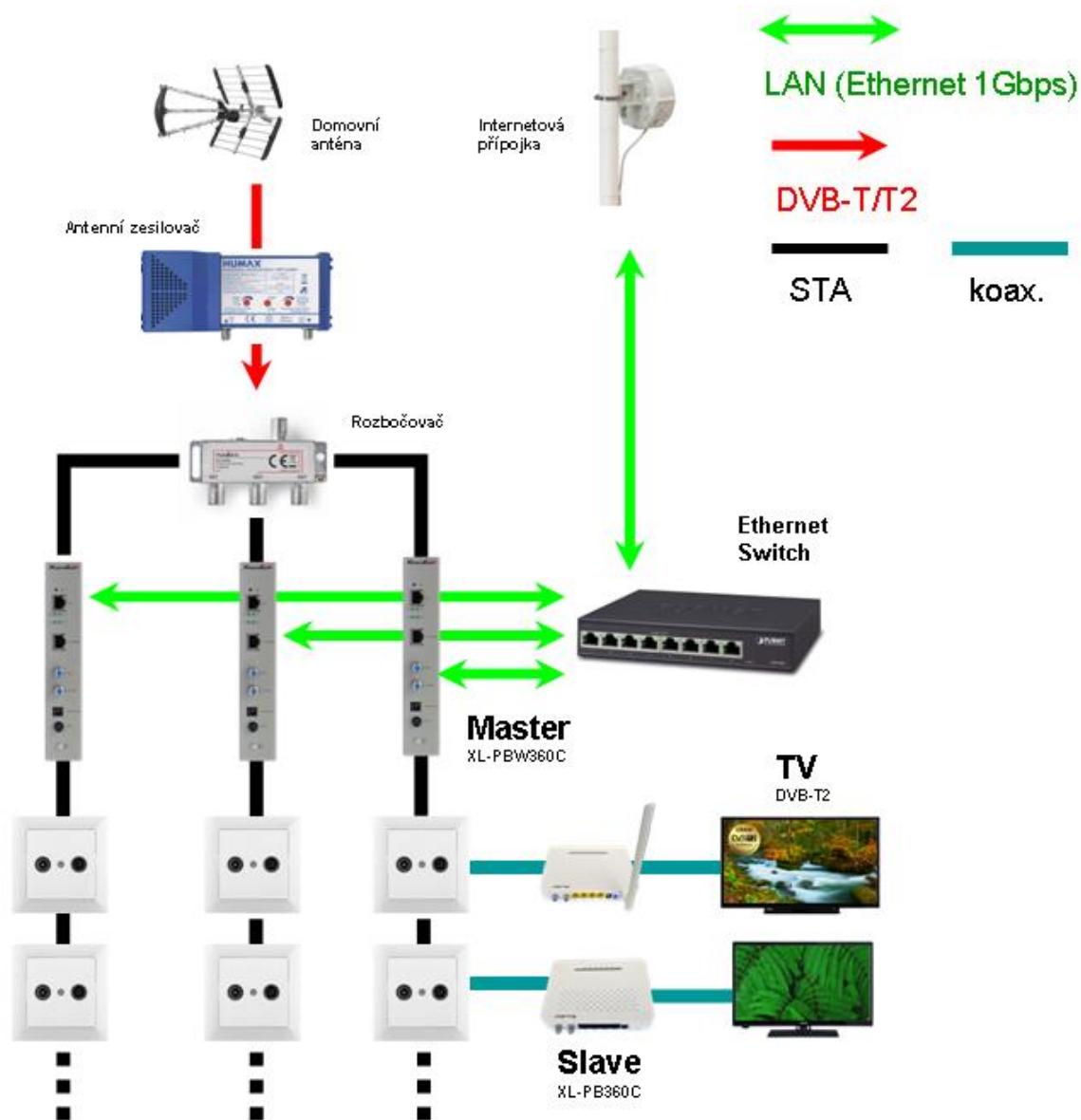


Zprovoznění takové sítě spočívá v instalaci Master jednotky mezi anténní zesilovač a společný anténní rozvod.

V jednotlivých bytech či pokojích je následně mezi stávající televizor nebo STB DVB-T2 vložena Slave jednotka. Zařízení se propojí běžným koaxiálním kabelem.

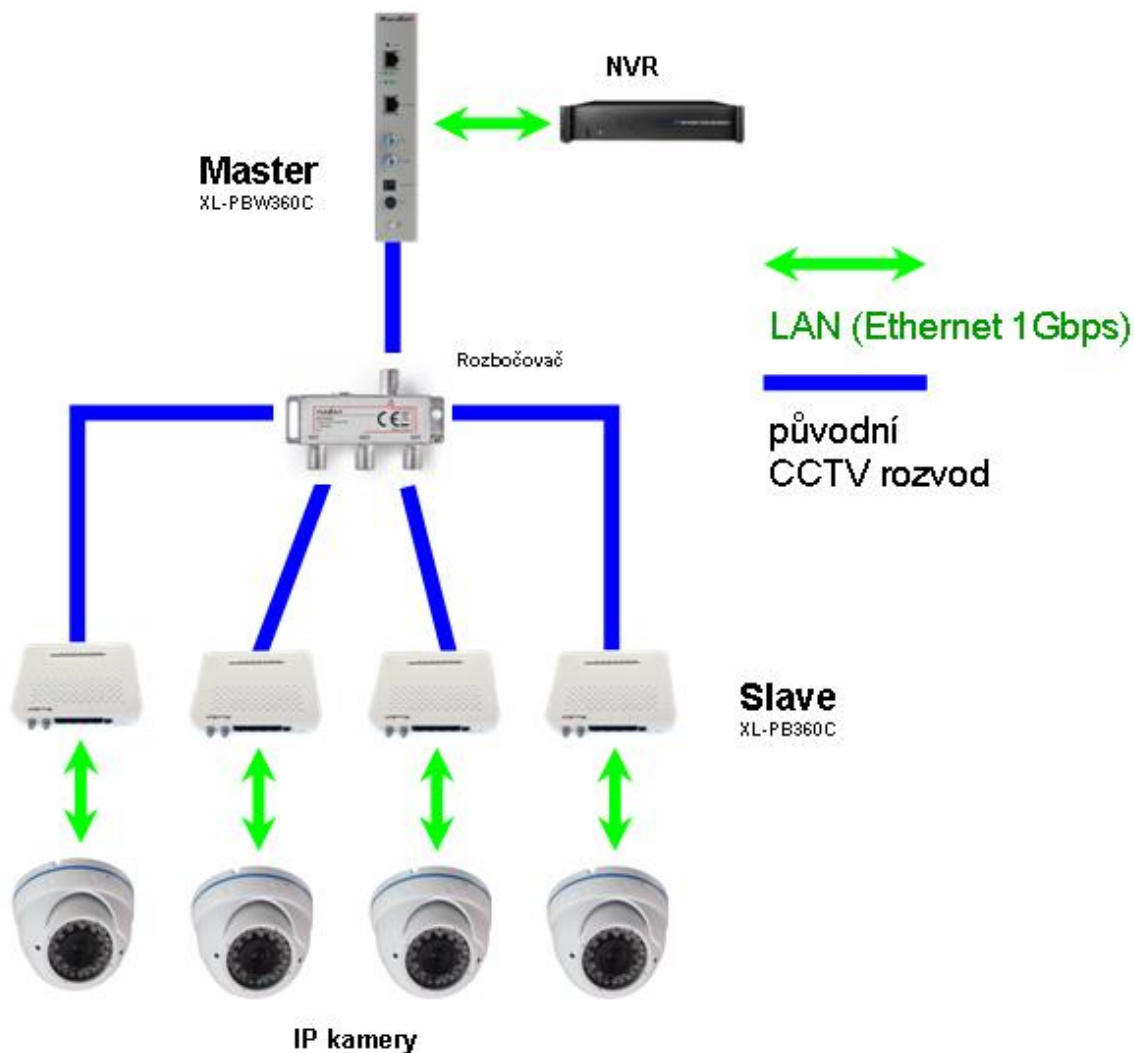
Slave jednotka poskytne rovnou LAN porty pro připojení počítačů, případně jednotka se zabudovaným WiFi pracuje rovnou i jako WiFi přístupový bod pro mobilní telefony a notebooky.

V případě že chcete docílit vyšší přenosové kapacity instaluje se pro každou větev společného TV rozvodu samostatný Master.



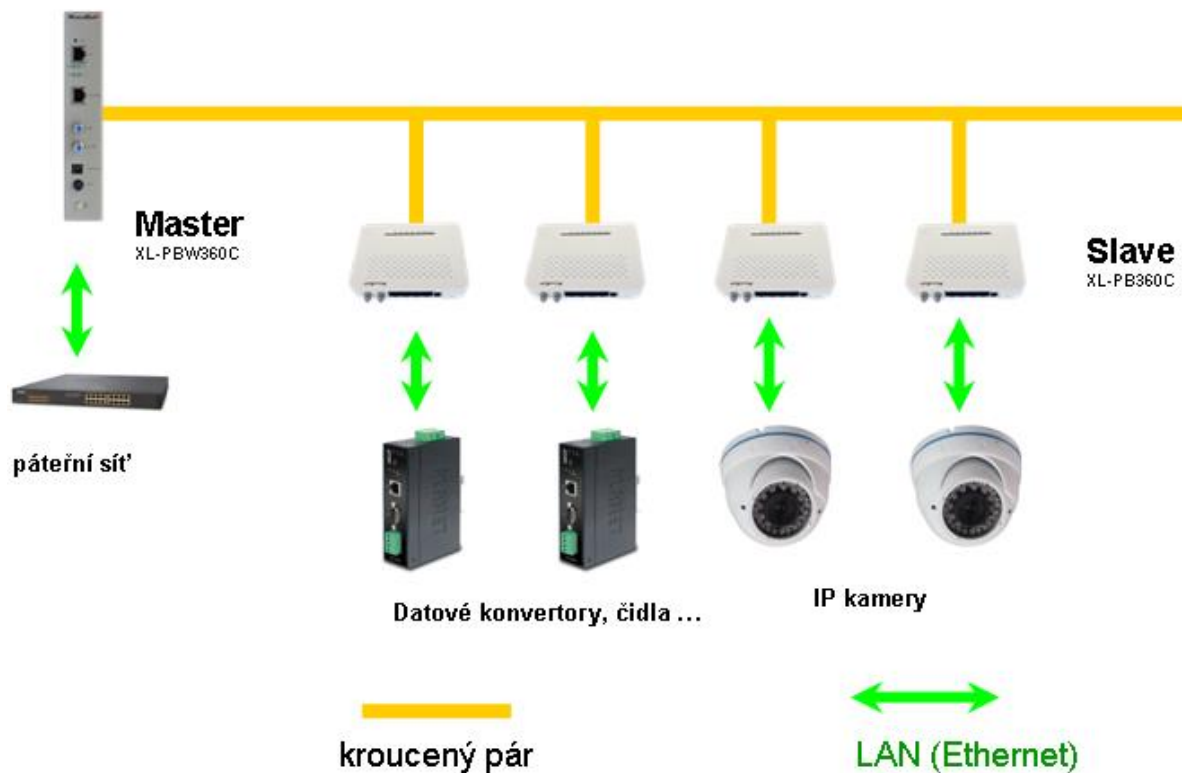
Konverze koaxiálního kabelového systému na IP

Druhým typickým užitím EoC je konverze stávajícího kabelového systému analogových kamer na IP. Opět není třeba vyměnit jediný kabel. Kabely stýkající se původně u nahrávacího zařízení se spojí dohromady do jediného Masteru. Na stranách kde původně byli kamery se zapojí mezi novou IP kameru a kabel Slave EoC jednotka. Způsob jakým se kabely spojí dohromady je lhostejný, není třeba speciálních rozbočovačů.



Konverze krouceného páru na IP

EoC můžete využít pro jakýkoliv kabel mající dostatečné frekvenční vlastnosti které snesou přenos signálu do desítek MHz. Typickým představitelem jsou jakékoliv kroucené páry (nejen CAT5) a staré koaxiální rozvody sběrnicevého typu apod. Nemusíte tak budovat žádnou novou kabelovou trasu



Modely zařízení a jejich instalace

Master jednotka XL-PBW360C

Rozhraní:

- 2x port Gigabit Ethernet 1000Mbps, RJ-45, autodetekce, jeden port pouze pro management a druhý pro datové přenosy
- 2x port F, port CABLE a CATV INPUT
- 4x LED indikátory
- tlačítko napájení
- zemnicí šroubová svorka
- napájení 6,5-20V DC z externího adaptéru, doporučeno 12V DC, konektor 5,5/2,1mm, příkon do 400mA při 12V
- nepřenáší napětí do koaxiálního vedení
- není napájen z koaxiálního vedení
- existence napětí v koaxiálním rozvodu do 50V není překážkou
- porty konektorů F jsou vzájemně propojeny (horní propust 75MHz), propojení funkční i při odpojeném napájení nebo závadě zařízení



Instalace zařízení:

Zařízení se typicky instaluje v místě zakončení anténního přívodu. Může být instalováno i přímo do rozvaděče za pomoci montážních otvorů na zadním panelu.

Postup zapojení:

- připravte si krátký propojovací koaxiální kabel zakončený F-male konektory
- odpojte koaxiální kabel propojující anténní zesilovač se společným TV rozvodem a zapojte jej do konektoru označeném CABLE
- připraveným krátkým propojovacím kabelem spojte výstup anténního zesilovače s konektorem označeným CATV INPUT
- ověřte si že TV přijímače společného TV rozvodu nadále běží beze změny. Může být vhodné mírně zvýšit zesílení anténního zesilovače o cca. 3~6dB jelikož na zařízení vzniká vložený útlum cca. 4dB. TV přijímače musí nyní pracovat i když jsem zařízení ještě nezapnuli !
- RJ45 port označený **10/100/1000** propojte s přípojkou k internetu, typicky se připojujete k routeru nebo datovém konvertoru (např.napojení do optického segmentu apod.)
- RJ45 port označený **MGMT** sice nemusíte zapojit, ale přišli byste o možnost zařízení vzdáleně spravovat. Doporučujeme jej zapojit rovněž do přípojky internetu (např. prostřednictvím malého Ethernet přepínače) nebo jej přinejmenším nyní napojit k servisnímu notebooku pro konfiguraci sítě.
- připojte napájení, preferované napájení je 12V DC a zamáčkněte vypínač ON/OFF

- nyní konfiguruje svůj router přípojky do internetu tak aby byl schopen přidělit IP adresu klientským zařízením a nastavte si svůj přístup na MGMT port Masteru. Konfigurační kroky jsou popsány dále v tomto návodu.
- doporučujeme nezapomenout na propojení zemnicí svorky se zemnicím bodem rozvaděče

Popis LED indikátorů:

PWR Napájení, musí svítit.

LINK Indikuje stav připojení klientských zařízení. Pokud zhasne znamená to, že nenalezl připojené žádné klientské zařízení nebo všechna ztratil. Indikace zjištění ztráty všech zařízení (tj. zhasnutí) trvá i několik minut. Naopak připojení alespoň jednoho klientského zařízení (tj. rozsvícení) je prakticky okamžité jakmile je Slave spuštěn.

DIAG Indikuje činnost diagnostiky linkového spojení.

SYS Indikuje činnost operačního systému Masteru. Pokud by byl trvale zhasnutý znamená že operační systém nenastartoval. Během startu Masteru je jeho krátkodobé zhasnutí normální. Jakmile se trvale rozsvítí je již nastartován celý systém a je k dispozici web management Masteru.

Popis rozhraní

RST - resetovací tlačítko, ukryté v malém otvoru, použijte špičatý nástroj pro jeho stisknutí. Krátké stisknutí - provede restart zařízení. Stejně jako stisknout ON/OFF. Dlouhé stisknutí na více než 5 s - provede reset zařízení do továrního nastavení. Odstraní všechny nastavení a pojmenování pro Slave jednotky. Před jeho užitím je vhodným mít nastavení zálohováno. Viz. odstavec "SYSTEM - Backup"

MGMT - port určený pouze pro administraci zařízení

100/100/1000 - port určený pro datovou komunikaci

CABLE - port pro připojení k rozvodu s účastníky a Slave jednotkami

CATV INPUT - připojení na antenní systém, tímto portem vstupuje do rozvodu TV signál a v zařízení se sloučí s EoC datovou komunikací

POWER DC +12 -- napájení

ON/OFF - tlačítko vypínače

Šroub - zemnicí bod skříně.



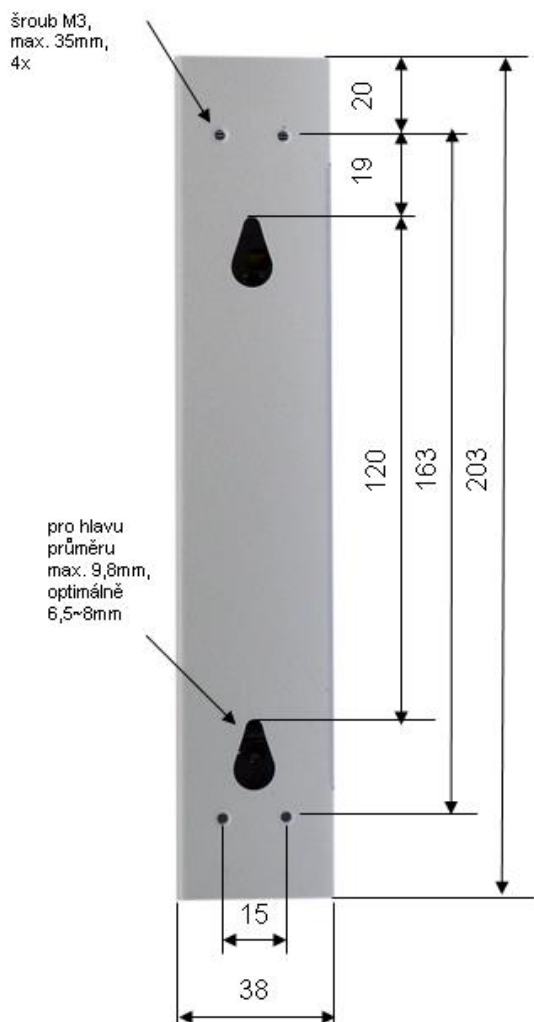
Montáž

Rozměr zařízení je 203x38x123mm - výška x šířka x hloubka

Master jednotku lze na montážní desku nebo stěnu připevnit šrouby M3 nebo pověsit na dva vruty/šrouby.

a) zavěšení na vruty/šrouby: připevněte na stěnu vruty s roztečí 120mm, délka zasunované části max. 35mm, velikost hlavy nejvíce 9,8mm (doporučujeme 6,5~8mm, tj. vrut 4)

b) připevnění na montážní panel šrouby M3, čtyři otvory se závitem M3, rastr je 163x15mm, maximální délka šroubu zasahujícího dovnitř je 35mm.



Doporučená minimální hloubka rozvaděče je 200mm. V případě nutné velké úspory místa lze použít i rozvaděč s hloubkou 155mm, v tom případě ale je nutné použít pravoúhlé F a RJ45 konektory.

Slave jednotka XL-PB360C

Rozhraní:

- 4x port Fast Ethernet 100Mbps, RJ-45, autodetekce
- 2x port F, port CABLE a TV
- 7x LED indikátor
- tlačítko napájení
- napájení 5-20V DC z externího adaptéru, doporučeno užití napájecího adaptéru dodaného v balení 12V DC, konektor 5,5/2,1mm, příkon do 300mA při 12V
- nepřenáší napětí do koaxiálního vedení
- není napájen z koaxiálního vedení
- existence napětí v koaxiálním rozvodu do 50V není překážkou
- porty konektorů F jsou vzájemně propojeny (horní propust 75MHz), propojení funkční i při odpojeném napájení nebo závadě zařízení



Instalace zařízení:

Zařízení se typicky instaluje v u koncového uživatele v blízkosti zakončení TV zásuvky.

Postup zapojení:

- připravte si krátký propojovací koaxiální kabel zakončený na jedné straně F-male konektorem a na druhé takovým konektorem jaký je v rozvodu použit u zákazníků, nejčastěji tzv. "IEC konektor" samička
- připravte si adaptér IEC samec na F male
- odpojte koaxiální kabel propojující TV zásuvku s TV přijímačem
- připraveným krátkým propojovacím kabelem spojte TV zásuvku a port na Slave zařízení označený CABLE
- na původní kabel propojující TV přijímač a IEC port nasad'te redukci "IEC samec / F samec" a tento kabel připojte v Slave zařízení do portu TV. Druhý konec kabelu byste měli mít zapojená stále v TV přijímači.
- ověřte si že TV přijímač má stále stejně kvalitní signál, tj. běží beze změny. TV přijímač musí nyní pracovat i když jsme Slave zařízení ještě nezapnuli !
- libovolný RJ45 port označený LAN1, LAN2, LAN3, LAN4 propojte s uživatelským routerem (do jeho WAN portu) nebo jej připojte přímo k uživatelské počítači (nebo vašemu servisnímu notebooku)
- připojte napájení, preferované napájení je 12V DC z dodaného napájecího adaptéru, a zamáčkněte vypínač ON/OFF na Slave zařízení
- po několika vteřinách se rozsvítí nebo rozbliká LED indikátor LINK

- nyní doporučujeme ověřit funkčnost vašeho DHCP serveru, tj. že je vám přidělena IP adresa případně že jste schopni zaslat a obdržet ICMP zprávu z nadřazeného routeru (tj. příkazem PING)

Popis funkce:

Slave jednotka XL-PB360C pracuje pouze v režimu bridge. Nemá vestavěný router. Jde tedy o přímý konvertor mezi EoC a Ethernetovou sítí.

Zařízení nemá vliv na práci TCP/IP vrstvy a přenáší ji zcela transparentně.

O firewall uživatele je tak třeba postarat se na vašem centrální routeru a/nebo koncového uživatele vybavit domácím routrem která je zapojen za Slave zařízení.

Slave zařízení se konfiguruji prostřednictvím Masteru, jak je popsáno dále.

LED indikátory:

PWR Napájení, musí svítit.

LOOP v případě povolení aby systém detekoval vznik smyčky (v LAN síti uživatele) , při její detekci se tato LED rozsvítí a uživatelův Slave je ze sítě automaticky odpojen!

SYS Indikuje činnost operačního systému Masteru. Pokud by byl trvale zhasnutý znamená že operační systém nenastartoval. Během startu bliká.

LINK Indikuje stav připojení klientských zařízení. Pokud zhasne znamená to, že nenalezl připojené žádné klientské zařízení nebo všechna ztratil. Indikace zjištění ztráty všech zařízení (tj. zhasnutí) trvá i několik minut. Naopak připojení alespoň jednoho klientského zařízení (tj. rozsvícení) je prakticky okamžité jakmile je Slave spuštěn.

LAN1, LAN2, LAN3, LAN4

Indikují fyzické propojení portů RJ45.

Tlačítka:

ON/OFF - tlačítko napájení

RST - resetovací tlačítko, ukryté v malém otvoru, použijte špičatý nástroj pro jeho stisknutí. Stisknutí když je jednotka v provozu způsobí její restart. Nastavení se přebírá z Master jednotky, tj. tlačítko nemá větší funkci než zapnutí a vypnutí.

Slave jednotka XL-PB360CA

Rozhraní:

- 4x port Fast Ethernet 100Mbps, RJ-45, autodetekce
- 2x port F, port CABLE a TV
- 7x LED indikátor
- tlačítko napájení
- napájení 5-20V DC z externího adaptéru, doporučeno užití napájecího adaptéru dodaného v balení 12V DC, konektor 5,5/2,1mm, příkon do 500mA při 12V
- nepřenáší napětí do koaxiálního vedení
- není napájen z koaxiálního vedení
- existence napětí v koaxiálním rozvodu do 50V není překážkou
- porty konektorů F jsou vzájemně propojeny (horní propust 75MHz), propojení fungují i při odpojení napájení nebo závadě zařízení



Instalace zařízení:

Zařízení se typicky instaluje v u koncového uživatele v blízkosti zakončení TV zásuvky.

Postup zapojení:

- připravte si krátký propojovací koaxiální kabel zakončený na jedné straně F-male konektorem a na druhé takovým konektorem jaký je v rozvodu použit u zákazníků, nejčastěji tzv. "IEC konektor" samička
- připravte si adaptér IEC samec na F male
- odpojte koaxiální kabel propojující TV zásuvky s TV přijímačem
- připraveným krátkým propojovacím kabelem spojte TV zásuvku a port na Slave zařízení označený CABLE
- na původní kabel propojující TV přijímač a IEC port nasad'te redukci "IEC samec / F samec" a tento kabel připojte v Slave zařízení do portu TV. Druhý konec kabelu byste měli mít zapojený stále v TV přijímači.
- ověřte si že TV přijímač má stále stejně kvalitní signál, tj. běží beze změny. TV přijímač musí nyní pracovat i když jsme Slave zařízení ještě nezapnuli !
- port RJ45 port označený LAN1 nebo LAN2 propojte přímo k uživatelské počítači (nebo vašemu servisnímu notebooku). Porty STB1 nebo STB2 připojujte pouze pokud jsou pro váš režim nastaveny, popis jejich funkce naleznete dále v tomto návodu.
- připojte napájení, preferované napájení je 12V DC z dodaného napájecího adaptéru, a zamáčkněte vypínač ON/OFF na Slave zařízení
- po několika vteřinách se rozsvítí nebo rozbliká LED indikátor LINK

- nyní doporučujeme ověřit funkčnost vašeho DHCP serveru, tj. že je vám přidělena IP adresa případně že jste schopni zaslat a obdržet ICMP zprávu z nadřazeného routeru (tj. příkazem PING)

Popis funkce:

Slave jednotka XL-PB360CA je zařízení s integrovaná WiFi Access Pointem (AP) a Routrem.

Router může ale nemusí být aktivován.

Zařízení má dva typy RJ-45 portů. Jedny jsou označeny STB1, STB2, druhá skupina je LAN1, LAN2.

Porty STB1 a STB2 jsou vždy v režimu bridge.

Porty LAN1 a LAN2 lze přiřadit do režimu Router. Koncový uživatel tak má svůj vlastní domácí oddělovací router/firewall.

Bezdrátový přístup WiFi je rovněž možné provozovat v režimu routeru, stejně jako LAN1, LAN2.

Toto Slave zařízení se konfiguruje prostřednictvím Masteru nebo je možné jej konfigurovat i prostřednictvím jeho web managementu, jak je popsáno dále.

LED indikátory:

PWR Napájení, musí svítit.

LOOP v případě povolení aby systém detekoval vznik smyčky (v LAN síti uživatele) se při její detekci tato LED rozsvítí a uživatelův Slave je ze sítě odpojen. Má funkčnost jen pro porty v režimu Bridge (tj. STB1 a STB2 a pro LAN1 a LAN2 jsou-li v režimu Bridge)

SYS Indikuje činnost operačního systému Masteru. Pokud by byl trvale zhasnutý znamená že operační systém nenastartoval. Během startu bliká.

LINK Indikuje stav připojení klientských zařízení. Pokud zhasne znamená to, že nenalezl připojené žádné klientské zařízení nebo všechna ztratil. Indikace zjištění ztráty všech zařízení (tj. zhasnutí) trvá i několik minut. Naopak připojení alespoň jednoho klientského zařízení (tj. rozsvícení) je prakticky okamžité jakmile je Slave spuštěn.

STB1, STB2, LAN1, LAN2

Indikují fyzické propojení portů RJ45.

WIFI

Indikují aktivitu (aktivaci) vestavěného WiFi Access Pointu.

Tlačítka:

ON/OFF - tlačítko napájení

RST - resetovací tlačítko, ukryté v malém otvoru, použijte špičatý nástroj pro jeho stisknutí.

Krátké stisknutí - způsobí její restart.

Dlouhé stisknutí na 5s a více - provede tovární nastavení, pro přístupové heslo a WiFi budou platit údaje uvedené na spodní části.

WLAN - tlačítko ukryté v malém otvoru, pro stisknutí použijte špičatý nástroj

Vypíná nebo zapíná WiFi AP, nemění jeho nastavení. Tlačítko podržte do doby než se změní stav LED diody WIFI.

Technické detaily

Koexistence s jinými technologiemi v jednom kabelovém vedení

Přehled technologií z hlediska využívání kmitočtového pásma

Kompatibilní technologie které lze provozovat simultánně na stejném kabelu:

DVB-T, DVB-T2

DVB-S, DVB-S je třeba pro ně zaručit průchod DC a 22kHz signálu

ADSL, ADSL2

CVBS typu PAL N/ M/B, NTSC-M

MoCA 1.0, 2.0 (všechny kmitočtové typy)

analogový telefon (POTS), analogové audio a jiné signalizace do 7MHz

FM a DAB rádiové vysílání

UHF jakýkoliv provoz v tomto pásmu

Nekompatibilní, využívající stejné kmitočtové rozsahy:

DOCSIS 1.0, 1.1, 2.0, 3.0

AHD, HD-TVI, HD-CVI

VDSL, VDSL2, G.Fast

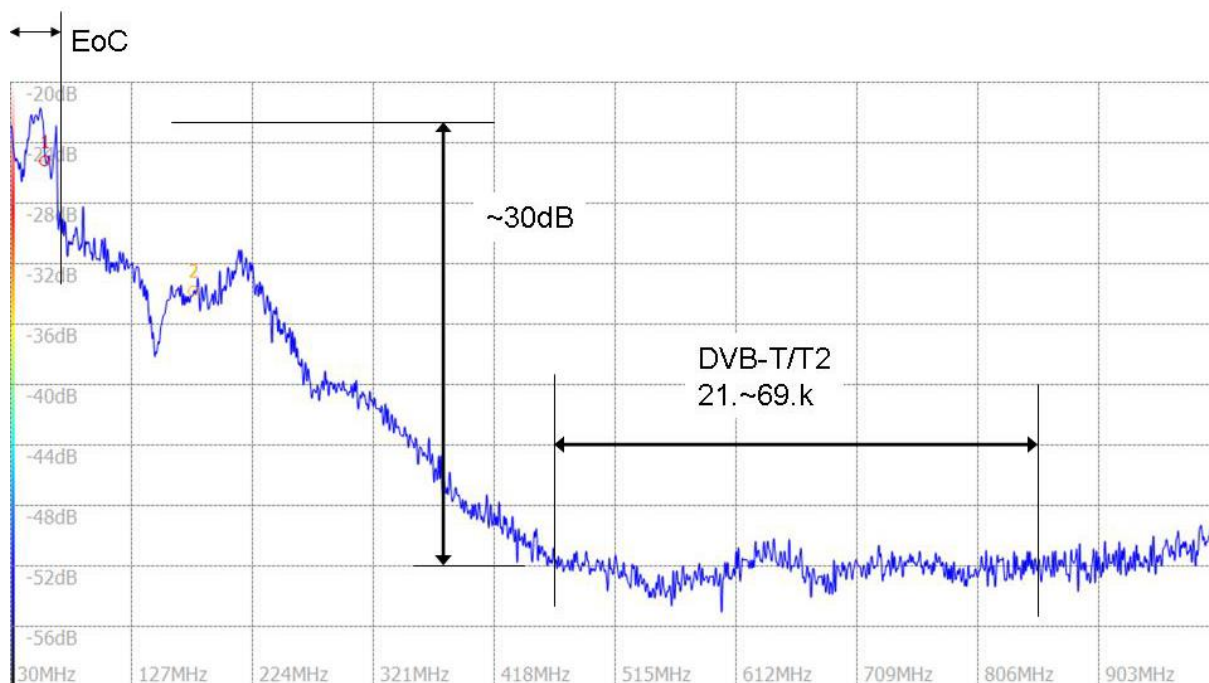
HomePNA 1.0, 2.0, 3.1, G.hn, Planet LRP

CVBS typu PAL G, H, D/K

Spektrální vlastnosti

Každá digitální komunikace způsobuje vznik vyšších harmonických i na kmitočtech které aktivně nepoužívá. I přes opatření které celý design takových zařízení provází se tomuto nelze vyhnout. Následující grafy ukazují stupeň "průsaku" těchto kmitočtů do jiných spekter.

Vliv na DVB-T/T2 pásmo:

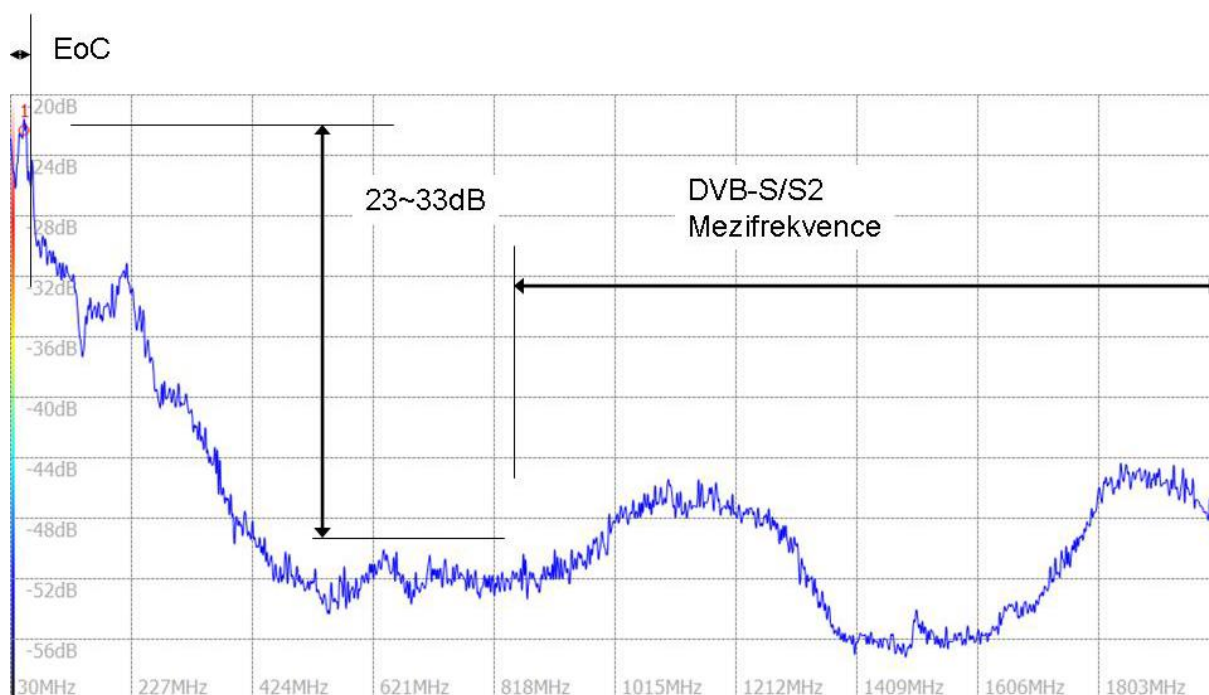


Graf zobrazuje spektrum signálu EoC v rozsahu 30MHz ~1000 MHz, získané měřením maxima (Hold-Peak), relativní hodnoty. Do kmitočtu 67,5MHz (začátek spektra) jde o vlastní pásmo EoC jednotek při jejich maximální datové zátěži.

DVB-T/T2 pásmo je u nás aktivně využíváno na kanálech 21-69, tj. 474-858MHz. Vůči celému tomuto rozsahu je průsak komunikace na úrovni o 30dB nižší než je vlastní komunikační úroveň EoC. Dá se říci že ani při nevhodném (žádném) zesílení příjmu DVB-T/T2 nebude EoC zdroje rušení.

Z měření je vidět že průsak kmitočtu na potencionálně nejbližším DVB-T kanál (kanál č. 5, 177MHz) má hodnotu oproti komunikačnímu signálu nižší jen o 12dB. Kanálový rozsah 5.-12. (117,5MHz ~ 226,5MHz) však u nás pro běžné vysílání využít zřejmě nikdy nebude. Může se však stát že v místě nasazení EoC je z nějakého důvodu DVB-T do tohoto pásma remodulováno a pak je třeba nastavit úroveň DVB-T významně výše tak aby průsak z EoC neměl žádný vliv. Jednoduchým řešením je prostá změna vysílacích úrovní v nastavení Masteru.

Vliv na DVB-S/S2 pásmo:



Graf zobrazuje spektrum signálu EoC v rozsahu 30MHz ~2150 MHz, získané měřením maxima (Hold-Peak, relativní hodnoty). Do kmitočtu 67,5MHz (začátek grafu) jde o vlastní pásmo EoC jednotek při jejich maximální datové zátěži.

DVB-S pásmo využívá pro přenos mezifrekvence pásmo 950-2150MHz. Vůči tomuto rozsahu je průsak komunikace na úrovni o cca. 23~33dB nižší než je vlastní komunikační úroveň EoC. Tj. v některých kmitočtových rozsazích číselně horší odstup než v případě DVB-T/T2.

Nicméně prováděli jsme měření vlivu provozu EoC na reálný příjem DVB-S/S2. V žádném z testů se neprojevil měřitelný vliv. V číselném vyjádření lze říci že SNR se v některých případech zhoršilo ne o více než 1dB což však bylo na hranici rozlišení měřících zařízení.

Tj. případný vliv který by ve vaší instalaci při nízkém DVB-S signálu mohl nastat určitě vyřešíte běžnými opatřeními jako je např. kabelový zesilovač zařazený před vstupem do kabelového rozvodu nebo snížení vysílacího výkonu v konfiguraci Masteru.

Kompatibilita s účastnickými TV zásuvkami:

Svislé a horizontální rozvody:

Účastnická TV zásuvka podporující přenos EoC by měla s malým útlumem přenášet kmitočtové pásmo 7-68MHz. Takové zásuvky jsou na našem trhu nazývány jako "obousměrné" nebo "se zpětným kanálem". V dnešní době již jde prakticky všechny o zásuvky které nově zakoupíte.

Problematické mohou být pouze zásuvky staré. V reálné situaci bytového domu často ani po otevření zásuvky nezjistíte typ a pokud jej zjistíte chybí k němu často frekvenční parametry, které by chování v pásmu EoC popisovali.



Pokud v budově během přechodu na vysílací systém DVB-T proběhla i výměna účastnických zásuvek můžete si být prakticky jisti že je dům vybaven správnými průběžnými zásuvkami!

Jedině v případě pochybností doporučujeme některý z těchto postupů:

- rovnou zásuvky vyměňte za moderní: dá se říci že pokud nenarazíte na vážný problém při výměně zásuvek tak je vyměňte. Pokud je výměna možná jen někde rovněž tak učiňte. Zásuvku zaměňte za typ se stejným odbočovací útlumem jako byla původní! Tak abyste nenarušili útlumovou rovnováhu TV systému.
- zásuvku přeměřte: Jste-li vybaveni základní měřicí technikou není problémem vymontování takové zásuvky, změření průchozího útlumu, odbočovacího útlumu a útlumu pro pásmo které EoC potřebuje. Podstatné je aby celkový útlum mezi Master jednotkou a nejvzdálenější Slave jednotkou nepřesáhl 60dB ve frekvenčním pásmu EoC (7-68MHz). ! Pro tato měření Vás nezajímají hodnoty v pásmech nad 80MHz, nemluvě o pásmech UHF !

Níže frekvenční charakteristikamoderní průběžné zásuvky na portu TV pro zpětný směr, měřená zásuvka s deklarovaným odbočovacím útlumem 14dB:



Měření v rozsahu 30kHz ~300MHz. Útlum zpětného směru ve sledovaném pásmu do 70MHz je prakticky totožný s dopředným směrem (14,6 dB @74MHz, značka 1 vs. 13,8dB@74MHz na jiném nezobrazeném měření). Takováto zásuvka rozhodně vyhovuje.

- další možností je zapůjčit si Master a Slave zařízení a provést jejich jejich otestování na místě. Ideálně přímo umístěním Masteru do rozvaděče a instalací Slave jednotky na některém patře/pokoji které považujete teoreticky za nejproblematictější či nejvzdálenější.

Nicméně ne vždy je míra kooperace ze strany vlastníků na takovéto úrovni a proto nezapomeňte že pro předběžné ověření funkčnosti EoC ve stávajícím rozvodu vám stačí připojit Master i na místě některé účastnické zásuvky a Slave zapojit do jiné účastnické zásuvky.

Pokud se Vám spojení ustaví a zjistíte v diagnostice Masteru že se spojení ustavuje s uspokojivými hodnotami útlumu (např. s útlumem méně než 50dB) můžete si být jisti že aplikace EoC je možná. Poznamenejme že i tento test můžete nechat provést dlouhodobě jelikož komunikace EoC nesmí rušit případné jiné existující systémy, o nichž například vlastníci budovy neví, že je používají a takovýto test interferenci odhalí. Vyhnete se tak problémům s jejich řešením až po nasazení do plného provozu.

Hvězdicový rozvod:

Pokud je účastnická zásuvka vybavena přípojkou pro SAT pravděpodobně nejde o svislý rozvod ale o zapojení do hvězdy do společného rozbočovacího prvku. V takovém případě je rozhodující pro další realizaci, tj. zda je připraven pro přenos zpětného kanálu na centrálním místě. Zásuvky zde problémem nejsou.

Zde nejlépe zjistit specifikaci rozbočovacího prvku. Pokud není k dispozici nebo neuvádí chování pro kmitočtové pásmo EoC je dalším postupem opět test.

Pokud je rozvod jen přípravou pro případné nasazení s příjmem DVB-S tak i v případě existence nekompatibilního rozbočovače s aktivním zesilovačem lze problém levně vyřešit rozdělením prvku na aktivní anténní zesilovač a pasivní rozbočovač.

Pokud je rozvod plně využíván pro příjem DVB-S je nejlépe konzultovat s autory řešení nebo nastudovat použité vybavení. U moderních systémů je míst kam včlenit EoC Master obvykle hned několik. Případně je k dispozici řada odbočovacích a pásmových propustí které dovolí signál EoC sloučit/odbočit do jednotlivých větví s co nejmenším nákladem.

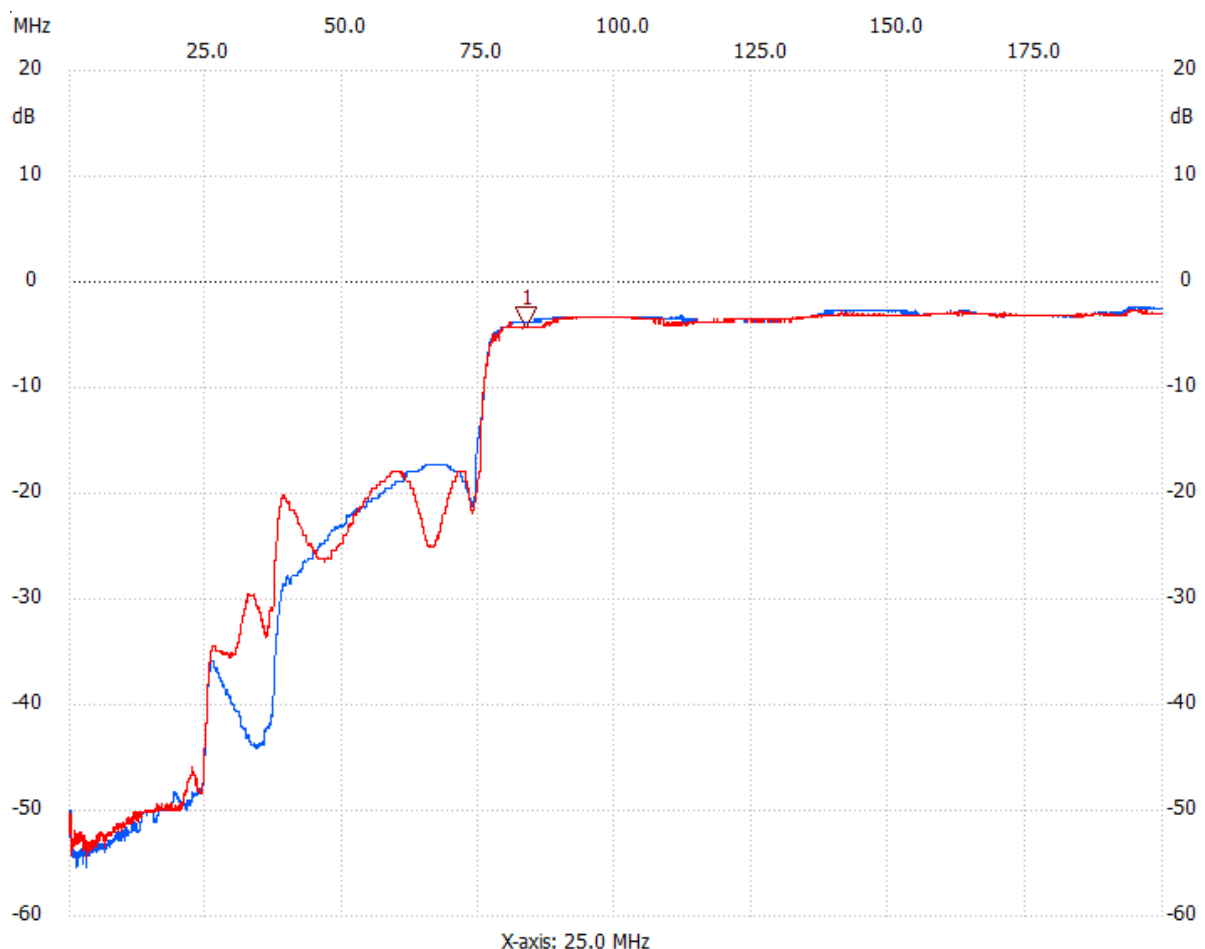
Frekvenční charakteristika vestavěného diplexeru

Diplexer je pasivní součástka která izoluje kmitočtová pásma EoC a TV. Zajišťuje aby signál EoC a TV vstupující do Slave zařízení do portu "Cable" skončil pouze v zařízení a dále pokračoval do portu "TV" jen signál televizního pásma. Stejná součástka je i v Master jednotce.

Frekvenční charakteristika této součástky vám může ozřejmit některé problémy které obvykle vedou ke snížení přenosové kapacity. Předně izolace portů v diplexeru není nekonečná a zařízení mají vysokou přijímací citlivost a i relativně vysoký vysílací výkon. Což může způsobit překonání útlumu diplexeru.

Níže přenosová charakteristika diplexeru změřená v rozsah 30kHz - 200MHz.

Červená čára je hodnota přenosu ve směru z portu "Cable" do portu "TV", modrá ve směru opačném. Můžete vidět že pro sledovaná pásma je ztlumení (izolace) v pracovním pásmu lepší než 25dB, jen v pásmu blízkém 70MHz je 20dB. Diplexerem neprojde stejnosměrná složka ani nízkofrekvenční pásma.



Přenos napájení ve vedení

Zařízení EoC nevdá přenos napájení po komunikačním vedení. Můžete tedy injektovat a zase odebrat napájení do a z společného koaxiálního vedení.

V rozvodech STA tak obvykle učiníte součástí "Napájecí výhybka", pokud přímo zesilovače nebo jiné prvky již toto nečiní.

Pokud nekombinujete s STA můžete jednoduše napájet do vedení (například T-spojku), doporučujeme však použít ochranné obvody, především proti zkratu vedení.

Pro injektované DC napětí nedoporučujeme překračovat napětí 50V! Nezapomeňte rovněž že samotná Master a Slave zařízení nelze napájet napětím přes 20V DC, doporučené napětí je 12V DC.

Nepřekračujte maximální proud který použitý kabel může přenášet!

Koaxiální porty na zařízení Master i Slave jsou pro DC složku neprůchozí. Jsou neprůchozí i pro nízkofrekvenční složky tj. použití střídavého napájení 50Hz rovněž neprojde. Proto pokud chcete napájet například Slave jednotky je nutné DC složku odbočit na portu "Cable", nikoliv na straně portu "TV".

Kompatibilita s výrobky třetích stran

Do EoC sítě lze zapojit výrobky jiných výrobců využívající stejný čipset a zřejmě i řadu dalších které následují HomePlug+/IEEE 1901 standard. Je však nutné počítat s tím že management Masteru je nerozpozná a nebude možné je administrovat jeho prostřednictvím. Budou komunikovat ale jejich administraci bude nutné provádět přímým připojením na jejich administrační rozhraní.

Přenosový výkon zařízení

Závislost přenosu na útlumu trasy

Níže měření přenosové kapacity jednoho klientského zařízení v závislosti na vloženém útlumu. Připomínáme že zařízení Slave má jen 100Mbps port. Měřeno pro XL-PB360C, simultánní přenos dat v obou směrech, TCP provoz.

Útlum (indikovaný)	Download	Upload	Agregovaný
dB	Mbit/s	Mbit/s	Mbit/s
4	93	90,2	183,2
12	92,9	91,5	184,4
22	92,9	91,2	184,1
34	92,9	91,5	184,4
44	93,0	91,5	184,5
52	92,9	91,5	184,4
60	92,7	91,6	184,3
73	35,7	64,1	99,8
83	12,0	17	29
85	7,3	8,9	16,2

Ukazuje jaký je přenosový výkon TCP/IP ve směru uploadu a downloadu. Měření bylo prováděno obousměrnou zátěží tj. v plně duplexním režimu.

Je zřejmé že až do útlumu 60dB nemá prakticky jeho hodnota vliv na přenosový výkon. Spojení přestane být funkční až pro hodnotu 85dB, tj. o více než 20dB větší!

Diagnostika v okně SLAVE-Oline je velmi užitečná ale je funkční jen do hodnoty 60dB. Za touto hodnotou ukazuje symbol >60dB. Nicméně to neznamená že je zařízení nefunkční. Pokud jej vidíte stále Online tak normálně komunikuje, byť menší rychlostí.

Tj. pro situace kdy chceme na velmi špatném propojení získat alespoň nějakou datovou komunikaci může být i jen pár Master-Slave atraktivním řešením.

Poznamenejme že útlum 60dB znamená v pásmu do 67,5MHz následující kabelové dosahy:

Typ kabelu	Střední vodič		Vnější průměr	Obvyklé užití	Útlum v pásmu do 70MHz	Dosah EoC 60dB
	mm	materiál				
0.8/5	0,8	Cu	5	rozvody TV příjmu	5,9	1017
RG59	0,8	Cu	6	kamerové rozvody	5	1200
RG6	1	CCS	7	antenní rozvody TV příjmu, ekonomické	5,1	1176
RG6	1	Cu	7	antenní rozvody TV příjmu	4	1500

Také to znamená velké množství rozbočení i pro ekonomicky provedenou kabeláž a nekvalitní typ rozbočení:

Rozbočení 1:N	Útlum rozbočením	Délka kabeláže Master - Slave
N	dB	m
2	7,5	1029
4	14,5	891
8	22,6	734
16	32,6	538
32	46,6	263

V tabulce je útlum rozbočením zvažován ve zpětném směru s nejhorsí možnou situací děliče, který má ve zpětném směru dvojnásobek (v dB měřítku) optimálního děliče. Na každý spoj je počítáno s rezervou 0,5dB. Kabel je předpokládán RG6 ekonomický typ s útlumem 5,1dB/100m v pásmu do 70MHz.

Úhrnný výkon

Simultánní Upload+Download

Pro aplikaci v reálném prostředí je podstatné vědět jak se bude vytvořená síť chovat při simultánní zátěži od více klientů a jaký je její přenosový výkon při maximálním vytížení. To je údaj zajímavý především pro realizaci internetových přípojek uživatelům.

Útlum (indikovaný, medián) dB	Download Mbit/s	Upload Mbit/s	Agregovaný Mbit/s
12	201,9	76,3	278,2
42	139,7	114,5	254,2
56	140,2	91,8	232,0
60	106,0	103,3	209,3
71	52,9	66,0	118,9
81	21,5	22,7	44,2

Ukazuje jaký je celkový přenosový výkon TCP/IP ve směru uploadu, downloadu a součtu upload+download přes všechna aktivní zařízení. Měření bylo prováděno simultánním přenosem 6-ti Slave zařízení. Každé z nich přenášelo simultánně maximum jaké mu systém dovolil. Výsledná hodnota v grafu je součtem přenosového výkonu těchto zařízení. Přenosový výsledek byl u každého z klientů rovnoměrný. Tj. na každý Slave připadá ~1/6 celkového výsledku.

Poznamenejme, že v reálné síti jde o špičkovou hodnotu kdy uživatelé maximálně vytěžují připojení obousměrně.

Hodnoty přenosových kapacity kterou lze uživateli garantovat získáte prostým vydělením počtem účastníků. Ne však více než 100Mbps (omezení rychlosti LAN portů).

Například jestliže pro hodnoty útlumů 42dB graf vykazuje hodnotu 139,7Mbps a na jeden Master jste dali 5 účastníků můžete garantovat, že download bude i za těch nejhorsích podmínek (tj.když všichni účastníci pojedou v obou směrech na maximální zátěž) nejméně $139,7/5=27,9$ Mbps. Pokud obsadíte na segmentu 10 účastníků bude dolní limit poloviční atd.

Dále měření potvrzuje že pokud docílíte hodnoty útlumu lepší než 60dB bude síť pracovat na svém přenosovém maximu, tj. další snížení útlumu sice zvyšuje přenosový výkon, ale již nejde o příliš významné zlepšení.

Download - TCP a Multicast

Výkon trasy v jednom směru nás zajímá pro aplikace kdy je trasa vytěžována prakticky úplně jednosměrně. Typickou aplikací pro směr Download, tj. od Masteru k Slave zařízením, je aplikace IPTV. V takovém případě je existující koaxiální síť konvertována na přenos protokolem IP (samozřejmě může zůstat zachována i původní funkčnost DVB-T/T2 a DVB-S/S2)

IPTV systémy používají řadu přenosových strategií, ale dvě jsou základní.

Pokud máte systém který dovoluje opožděné přehrávání (tzv. time-shift) nebo prostě přehrává z archivu (tzv. VoD) bude pracovat nejspíše v režimu TCP.

Pokud IPTV systém přehrává data pouze v aktuálním čase (stejně tak jako je tomu u TV) pak bude pro něj výhodné pracovat v režimu UDP Multicast.

Proto měření zohledňuje tyto dva základní přístupy, které jsou pro vás podstatné v zodpovězení zda bude kapacita přenosové sítě dostatečná pro IPTV.

a) TCP, směr download

Pro přenosy protokolem TCP ve směru od Masteru k Slave zařízením je výsledek:

Měření úhrnného přenosového výkonu pro směr download, TCP, 6x Slave, v závislosti na vloženém útlumu:

Útlum (indikovaný, medián) dB	Download Mbit/s
42	213,5
51	216,1
61	176,4
71	106,7

Výsledek říká že pro realizaci systému IPTV který by pracoval v TCP kdy předpokládáme potřebu přenosu cca. 15Mbps (pro Full HD TV) na jednoho účastníka můžeme mít cca. 14 takových účastníků.

Typický zdroj streamu	Rychlost streamu Mbps	Klientů na segmentu Kusů
DVB-T2 HD	15	14
DVB-S2 HD	20	10
Internetový re-stream	5	42

Tj. například dům o deseti podlažích s celkem 30-ti byty lze spolehlivě převést do IPTV při užití tří Master jednotek.

b) UDP Multicast, směr download

IPTV systémy které slouží jako přímá náhrada distribučních systémů DVB-T/DVB-S obvykle nepoužívají TCP komunikaci s každým uživatelem ale je pro ně výhodnější použití Multicastu UDP. Tj. jeden stream se vysílá na všechny uživatele a nesleduje se v rámci komunikace zda jej poslouchají či nikoliv.

V EoC systému však má toto schéma omezenou účinnost, jelikož pro zajištění spolehlivé komunikace je každé spojení mezi Master-Slave transformováno na Layer 2 úrovni na unicastovou komunikaci.

Systém je tak připraven na příjem a distribuci Multicastu, jeho užitím však nevzniká taková výkonová výhoda jako jsme tomu zvyklí z Ethernetových sítí. Viz. měření níže z nějž je zřejmé že celková přenosová kapacita je jen o málo vyšší než je tomu v případě TCP ve směru downloadu.

Měření úhrnného přenosového výkonu pro směr download, Multicast, 6x Slave, v závislosti na vloženém útlumu:

Útlum (indikovaný, medián)	Download
dB	Mbit/s
44	287,4
52	241,9
62	195,1
72	111,5

Pro Multicast vás může zajímat jaký maximální stream můžete použít v závislosti dle počtu klientů. Poznamenejme že samotný stream nemusí být jeden TV program ale stream samozřejmě běžně obsahuje několik programových kanálů.

Měření úhrnného přenosového výkonu pro směr download, Multicast, v závislosti počtu Slave zařízení, útlum 44dB (medián)

Počet Slave jednotek	Multicast - průměrná kapacita každé Slave jednotky	Agregovaný výkon
ks	Mbit/s	Mbit/s
3	79,2	237,6
4	64,1	256,3
5	50,8	254,1
6	42,8	257,0

Použití Multicastu tedy vede cca. k mírnému zvýšení výkonu, t.j. používat jej lze pro účely IPTV pro max. 16 Slave zařízení na jeden kabelový segment.

Upload

Výkon trasy ve směru od Slave k Master zařízením nás zajímá typicky pro IP kamerové systémy. Často máme k dispozici koaxiální kabeláž původního analogového systému, který je vhodné převést na IP kamerový systém. Nemusí jít vždy o koaxiální kabeláž. Například v průmyslových areálech jde často o kombinaci krouceného páru který jinak slouží i pro sběr dat z čidel. Díky používanému pásmu nad 5MHz si tak s čidly nevádí a získá další funkčnost.

Měření úhrnného přenosového výkonu pro směr upload, TCP, 6x Slave, v závislosti na vloženém útlumu:

Útlum (indikovaný, medián) dB	Upload Mbit/s
42	233,6
52	215,6
61	177,6
71	105,2

Z tabulky je zřejmé že při průměrné realizaci bude upload dosahovat výkonu přes 200Mbps.

Pro realizaci IP kamerové systému touto technologií je tak počet kamer na jeden segment pro drtivou většinu realizací více než dostatečný i s rezervou na další rozšiřování:

Rozlišení kamery Mpix	Obvyklá rychlost streamu z kamery Mbps	Počet kamer na segmentu kusů
2	2	116
8	6	38

Úhrnný výkon v závislosti na počtu zařízení

Pro některé speciální aplikace vás může zajímat zda existuje nějaké celkové agregační maximum pokud použijete více zařízení.

Měření ukázala, že celkového přenosového maxima docílíte se třemi až čtyřmi Slave zařízeními.

Nicméně rozdíl oproti užití pouze dvou Slave zařízení není větší než 15%. Tj. pokud v některé aplikaci by mělo smyslu realizovat přenosovou trasu jeden Master na více Slave a jejich sdružení (tzv. link bonding, link trunking) tak nejpravděpodobněji vystačíte se dvěma Slave zařízeními a přidání dalších už nebude příliš významné.

Následující měření ukazuje přenosová maxima pro simultánní TCP zátěž Download+Upload. Útlum trasy v těchto měření byl do 20dB.

Počet Slave jednotek	Download celkem	Upload celkem	Agregovaný
ks	Mbit/s	Mbit/s	Mbit/s
2	185,7	60,8	246,5
3	211,1	47,6	258,7
4	210,7	57,2	267,9
5	177,8	98,7	276,5
6	191,2	86,3	277,5

Vliv omezení pásma na přenosový výkon

Pro koexistenci s některými technologiemi může být nutná redukce kmitočtového pásma. Zařízení může mít změněno horní kmitočet v rozsahu 30-67,5MHz. V našich končinách půjde nejspíše o koexistenci s FM vysíláním, pokud je přijímáno prostřednictvím stejného vedení.

Poznamenejme že interface Masteru dovolí nastavení i na kmitočty do 30MHz, ale ta pak nejsou funkční!

Nastavení kmitočtu provedete z menu RF->RF Info. Všechny jednotky musí využívat stejné pásmo.

Měření simultánního přenosu TCP, 6 Slave zařízení, útlum do 46dB, součet přes všechny jednotky:

Nastavený horní kmitočet	Šířka pásma	Download	Upload	Agregovaný
MHz	MHz	Mbit/s	Mbit/s	Mbit/s
67,5	59,9	154,5	112,6	267,1
50,0	42,4	102,3	111,4	213,7
40,0	32,4	70,9	89,8	160,7
30,0	22,4	51,3	62,8	114,1

Z výsledků lze vidět, že zmenšení přenosového pásma se poměrově promítne do celkového přenosového výkonu. Může vám to dovolit předpovědět přenosové výkony pokud jste nuceni snížit šířku přenosového pásma kvůli koexistenci s nějakou další technologií přenášenou po stejném či sousedním kabelu. Poznamenejme že snížení šířky pásma relativně zvýhodňuje směr pro upload.

Přenosový výkon na kabeláži CAT5

Zařízení nejsou citlivá na impedanční poměry a můžete je používat s nejrůznějšími typy kabeláží.

Test přenosového výkonu pro TCP, simultánní přenos oběma směry (plně duplexní), zapojeno 6 Slave zařízení.

Kabelem JEDEN pár UTP CAT5 v délce 160m. Útlum v testu navyšován útlumovým článkem.

Útlum (indikovaný, medián)	Download	Upload	Agregovaný
dB	Mbit/s	Mbit/s	Mbit/s
24	125,3	96,0	221,3
36	116,5	108,0	224,5
46	87,5	103,7	191,2
58	44,9	76,9	121,8
68	8,3	36,4	44,7

Můžete srovnat s výsledkem prováděným na koaxiálním rozvodu (předchozí kapitola Simultánní Upload+Download) a je zřejmé že při užití krouceného páru jsme stále na 3/4 výkonu.

Administrace zařízení

Přístup do rozhraní administrace

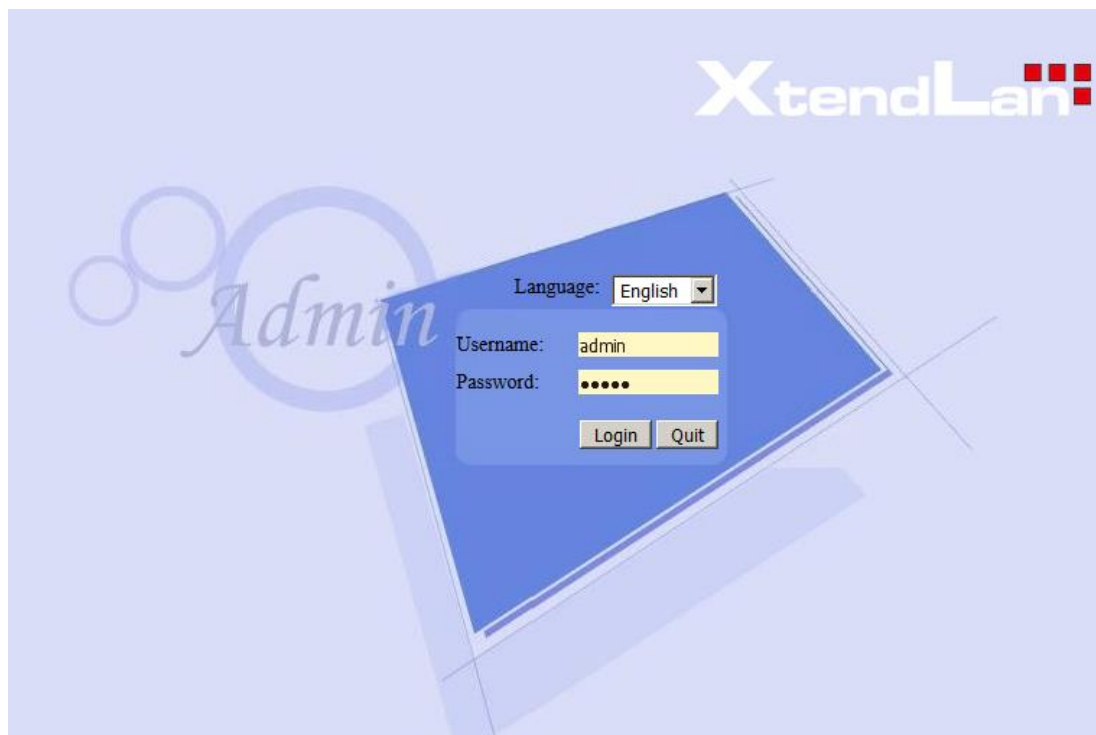
Po provedení fyzické instalace Masteru je dobré otestovat přístup na jeho web rozhraní.

Web rozhraní je preferovaně dostupné druhém portu Masteru označeném MGMT pod IP adresou 192.168.1.2. Pro přístup nastavte na svém počítači jakoukoliv IP adresu z rozsahu 192.168.1.3~254 s maskou 255.255.255.0

Výchozí IP adresa web rozhraní: 192.168.1.2

Přihlašovací jméno: admin

Výchozí heslo: admin



Management je však dostupný i přes rozhraní 10/100/1000, případně ze strany Slave klientského zařízení. Na tomto rozhraní se nalézá pod adresou 192.168.2.2.

Pro přístup nastavte na svém počítači jakoukoliv IP adresu z rozsahu 192.168.2.3~254 s maskou 255.255.255.0

Hlavní nabídka

Po přihlášení na web rozhraní masteru se vám zpřístupní následující menu:



SLAVE - administrace připojených Slave zařízení

RF - monitoring a možnost nastavit frekvenční a výkonové parametry

NETWORK - konfigurace přístupu k IP adrese EoC a nastavení IGMP

SERVICE - přehled běžících služeb

SYSTEM - nástroje pro správu Masteru

EXIT - odhlášení z webadministrace

SLAVE - Authorization

Volba **SLAVE - Authorization** otevře administrační okno v němž lze centrálně spravovat připojená Slave zařízení.

Authorization Mode

Authorization Mode: Auto Auth Manual Auth

Slave Authorization

ID	Slave MAC	Wifi MAC	Auth Enable	Status	Slave Type	Automatic update allow	Start time	End time	Template Selection	Operation
1	1c:c0:e1:36:a3:4d	None	<input checked="" type="checkbox"/>	Online	EoC-Slave-4	<input checked="" type="checkbox"/>	00:00	23:59	301	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
2	1c:c0:e1:36:a3:4f	None	<input checked="" type="checkbox"/>	Online	EoC-Slave-4	<input checked="" type="checkbox"/>	00:00	23:59	302	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
3	1c:c0:e1:36:a3:5f	1c:c0:e1:36:a3:61	<input checked="" type="checkbox"/>	Online	EoC-Slave-EW	<input checked="" type="checkbox"/>	00:00	23:59	1	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
4	1c:c0:e1:36:a3:57	1c:c0:e1:36:a3:59	<input checked="" type="checkbox"/>	Online	EoC-Slave-EW	<input checked="" type="checkbox"/>	00:00	23:59	1	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
5	1c:c0:e1:36:a3:3f	None	<input checked="" type="checkbox"/>	Online	EoC-Slave-4	<input checked="" type="checkbox"/>	00:00	23:59	1	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
6	1c:c0:e1:36:a3:67	1c:c0:e1:36:a3:69	<input checked="" type="checkbox"/>	Online	EoC-Slave-EW	<input checked="" type="checkbox"/>	00:00	23:59	1	<input type="button" value="Modify"/> <input type="button" value="Delete"/>

Unauthorized Slave

Index	MAC	Operation

Authorization Mode: má volbu Auto Authorization a Manual Authorization.

Jejím smyslem je poskytnout kontrolu proti nedovolenému napojení do sítě.

V režimu Manual Auth se nově přidané zařízení objeví v dolní sekci Unauthorized Slave.

Teprve až když jej vyberete a zvolíte **Authorize** tak je mu povoleno se do sítě připojit.

Jakmile tak učiníte již je toto platné poro všechny další restarty, MAC adresa tohoto zařízení je uložena v Masteru jako autorizovaná.,

V režimu Auto Slave se každé nové zařízení automaticky přidá mezi schválené, tj. režim v níž žádná autorizace není potřebná. Jde o výchozí nastavení.

Slave MAC: v zobrazeném seznamu MAC adresy zařízení můžeme na zařízení poklepat a přejdeme tak do režimu nastavování konkrétního Slave zařízení.

Pořadí zařazení se určí tím jak nová zařízení přidáváme, tj. jednou autorizované zařízení má stále stejné pořadové číslo. Výmaz je možný přes Factory reset.

Auth Enable - pokud odškrtnete to pole a stisknete tlačítko Modify, jednotka se přesune mezi nautorizované. Uživateli této Slave jednotky se tím zrusí spojení.

Slave Type - dovoluje přiřazení šablony pro administraci prostřednictvím Master zařízení. Tyto šablony můžete sami měnit a vytvářet v menu **System - Slave Type**. Šablona ovlivňuje především kolik Ethernetových portů se vám nabídne k administraci při vstupu do ovládní jednotlivého SLave zařízení a také zda se nabídne přístup k parametrům WiFi. Samotná volba šablon nemá žádný vliv na funkčnost Slave zařízení jako takového.

Start Time , End Time - dovoluje časově omezit funkčnost klientské jednotky

Template Selection - během autorizace Slave zařízení do sítě je mu možno zaslat automatickou konfiguraci kterou si může uživatel připravit. Připravené konfigurace mají pořadová čísla 1 až 256, přičemž číslo 1 má výchozí vzor.

Pokud je u toho zařízení zaškrtnuta volba Auto Update Enable je tato konfigurace nahrávána do zařízení pokaždé kdy je změna nebo se přihlásí zařízení znovu. Pokud tato volba zaškrtnuta není je nutné změnu provést stisknutím tlačítka Modify.

Smyslem používání **Template** je omezení nutnosti konfigurovat každý Slave samostatně. Pomocí Templates se však nekonfigurují vestavěné routery ve Slave zařízeních. Konfiguruje pouze fyzická rozhraní, tj. především nastavení omezení přenosových pásem a nastavení VLANů.

Templates se vytvářejí buď v menu SLAVE - Templates (čísla 1~256) a nebo jsou vytvořena automaticky s číslem vyšším než 300. To se děje pokaždé kdy změní konfiguraci jednotlivého Slavu v jeho menu Slave Configuration Information. Tento Template pak náleží pouze tomuto zařízení.

Speciálním je Template číslo 0 a znamená že jednotka nemá žádný Template přiřazen.

Pro prvotní zprovoznění se nepotřebujete Template zabývat, ponechte je v defaultní hodnotě.

Delete - jeho stisknutím vymažete zvolený Slave ze seznamu autorizovaných. Zařízení se restartuje a po nastarování provede akci jakoby šlo o nově přidané zařízení.

Modify - aplikuje změnu které jste v pro daný Slave provedli v ostatních sloupcích.

Add An Authorized Slave - dovoluje ruční zadání Slave jednotky která není aktuálně Online. Pro její zadání je nutné znát její MAC adresu.

SLAVE - Online

Volba **SLAVE - Online** otevře administrační okno s přehledem připojených jednotek a stavu kvality jejich připojení.

Online Slaves Number: 5									
ID	Slave MAC	Wifi MAC	User information	Attenuation(dB)	Upstream SNR(dB)	Downstream SNR(dB)	Upstream Speed(Mbps)	Downstream Speed(Mbps)	Operation
1	lc:c0:e1:36:a3:4d	None	XL-PB360C Node B2	44	27.30	29.93	306	328	Reboot
2	lc:c0:e1:36:a3:45	None	XL-PB360C Node B3	44	31.51	31.20	340	338	Reboot
3	lc:c0:e1:36:a3:5f	lc:c0:e1:36:a3:61	XL-PB360CA Node B4	44	27.78	29.52	310	324	Reboot
4	lc:c0:e1:36:a3:57	lc:c0:e1:36:a3:59	XL-PB360CA Node B5	44	28.84	30.28	319	330	Reboot
5	lc:c0:e1:36:a3:3f	None	XL-PB360C Node B6	46	29.00	29.80	320	327	Reboot

Slave MAC: v zobrazeném seznamu MAC adresy zařízení můžeme na zařízení poklepat a přejdeme tak do režimu nastavování konkrétního Slave zařízení.

WiFi MAC: MAC adresa spojená s vestavěným WiFi AP zařízením. Slouží k identifikaci.

User Information: zobrazuje textový popis který jsme si do Slave zařízení zadali. Rozhodně velmi užitečné pro snadnou orientaci.

Attenuation (dB): vyjadřuje velikost útlumu signálu mezi Master a konkrétní Slave jednotkou. Jde o hodnotu útlumu v pracovním pásmu zařízení a odpovídá skutečné hodnotě útlumu jež lze změřit. Čím menší tím lépe.

Jak se můžete dovědět v odstavci "Závislost přenosu na útlumu trasy" jakékoli číslo menší než 60 je pro práci Slave jednotky akceptovatelné.

Upstream SNR (dB): vyjadřuje hodnotu rozdílu úrovně užitečného signálu a šumu pro směr přenosu od Slave k Masteru. Čím větší tím lepší.

Downstream SNR (dB): vyjadřuje hodnotu rozdílu úrovně užitečného signálu a šumu pro směr přenosu od Masteru k Slave jednotce. Čím větší tím lepší.

Upstream Speed (Mbps): vyjadřuje signálovou rychlost jakou jednotka používá při komunikaci ve směru Slave - Master. Nevyjadřuje skutečnou datovou rychlost.

Downstream Speed (Mbps): vyjadřuje signálovou rychlost jakou jednotka používá při komunikaci ve směru Master - Slave. Nevyjadřuje skutečnou datovou rychlost.

Reboot - tlačítko dovolující restartovat jednotlivý Slave.

SLAVE - konfigurace jednotky

Stránka s konfigurací jednotky se otevře poklepnutím na její MAC adresu buď v okně SLAVE - Authorization nebo v okně Slave - Online.

Horní lišta která se zobrazí závisí od přednastavenné šablony zvolené nebo automaticky detekované ve **Slave Type**.

Proto u zařízení bez routeru XL-PB360C se zobrazí jen menu Slave Basic Information, Slave Configuration Information, Slave MAC Table.

U zařízení XL-PB360CA vybavené routrem a WiFi AP se zobrazí navíc ještě menu Wifi Basic Configuration, Wan Configuration, Lan Configuration, Static Route Configuration, L2 Switch Configuration, Virtual Server Configuration, WiFi Management a WiFi Upgrade.

Slave Basic Information

První okno **Slave Basic Information** obsahuj epole User Information které důrazně doporučujeme vyplnit popisnou informací. Slouží čistě pro váš identifikační účel.

Slave Basic Information	Slave Configuration Information	Slave MAC Table
Slave [1c:c0:e1:36:a3:4d]		
Slave Information		
Slave Type	EoC-Slave-4	
Port Number	4	
Software Version	7.1.0 & INT7400-MAC-7-1-7131-00-17-20131108-FINAL-QCA7411L-B	
User Information	<input type="text" value="XL-PB360C Node B2"/>	
Attenuation	44 dB	
Signal Noise Ratio	UpLink 27.30 dB	Downlink 29.93 dB
Modulation	UpLink 9.46 bits/carrier	Downlink 10.11 bits/carrier
Speed	UpLink 306 Mbps	Downlink 328 Mbps
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>		
Other Information		
<input type="button" value="Reboot"/>		

Slave Configuration Information

Druhé okno **Slave Configuration Information** slouží k nastavení režimu práce Ethernetových portů Slave jednotky.

Slave [1c:c0:e1:36:a3:4d]

Template Selection

Template Application: DefaultTemplate

Template Configuration

Enable broadcast restriction: Enable multicast restriction: Enable unknow unicast restriction:

Restriction threshold (pps):

Enable loopback check:

Port	Enable Port	Speed&Duplex	Vlan Mode	PVID	Allowed VLAN	COS	UpLink maximum speed (0-102400)Kbps	DownLink maximum speed (0-102400)Kbps
1	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	<input type="text" value="Disable"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
2	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	<input type="text" value="Disable"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
3	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	<input type="text" value="Disable"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
4	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	<input type="text" value="Disable"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

Current Configuration

Port	Link Status	Loop	Enable Port	Adaptive	Speed	Duplex	PVID	COS
1	Disconnect	No	Enable	Enable	10mbps	Half duplex	0	0
2	Disconnect	No	Enable	Enable	10mbps	Half duplex	0	0
3	Disconnect	No	Enable	Enable	10mbps	Half duplex	0	0
4	Disconnect	No	Enable	Enable	10mbps	Half duplex	0	0

Template Selection - máme-li definovaný vhodný Template můžeme jej zde vybrat a použít, t.j. nemusíme konfigurovat volby níže neboť ty se právě automaticky převezmou z Templatu. Provedete použitím tlačítka Apply v řádce Template Application.

Enable broadcast restriction: omezení všesměrového vysílání, typicky omezení způsobené závadou nebo zlým úmyslem, pokud nemáte problémy tohoto typu nzaškrťávejte

Enable multicast restriction: omezení pro kapacitu zasílaného multicastu. I největší hodnota 2560 může být pro některé aplikace nízká, proto spíše doporučujeme nezaškrťávat.

Enable unicast restriction: omezení pro unicast nezaškrťávat

Restriction threshold (pps): hodnota omezení v paketech za sekundu pro předchozí jmenované.

Enable Loopback check: pokud je povolen a uživatel propojí omylem jednotlivé porty na Slave zařízení je toto detekováno a Slave je odpojen od sítě. Zároveň se rozsvítí dioda LOOP. Můžete povolit, nemá vliv na výkonnost zařízení.

Enable Port - povolíte/zakážete funkčnost portu.

Speed/Duplex - fyzický režim portů, Auto, 10, 100Mbps, Full Duplex ...

Vlan Mode - volíte zda je na portu aktivní režim VLAN 802.1Q.

Disabled - činnost bez VLAN 802.1Q, ponechte v tomto režimu pokud VLAN 802.1Q nevyužíváte

Access - musíte vyplnit PVID, port pracuje v tomto režimu následovně:

Pakety přijaté z Masteru které obsahují tag shodný s PVID jsou poslány do LAN sítě bez tagu. Ostatní pakety nejsou přeposílány do LAN.

Pakety přijaté z LAN které mají nějaký 802.1Q tag jsou odmítnuty. Pouze pakety bez tagu jsou označeny tagem PVID a poslány Masteru.

Trunk - musíte vyplnit PVID a povolené VLAN, port pracuje v tomto režimu následovně:

Pakety přijaté z Masteru které obsahují tag shodný s PVID jsou poslány do LAN sítě bez tagu. Ostatní pakety jsou do LAN sítě posílány pokud jsou v seznamu Allowed VLAN bez odstranění tagu. Pokud je tag současně PVID a allowed VLAN tag není jeho tag při poslání do LAN odstranění.

Pakety přijaté z LAN které mají nějaký 802.1Q tag shodný s některým Allowed VLAN jsou beze změny přeposílány Masteru (včetně tagu).

Pakety bez 802.1Q tagu jsou označeny tagem PVID a poslány Masteru.

Existuje rozdíl v možných kombinacích nastavení:

XL-PB360C dovoluje pouze nastavení všech portů do stejného VLAN mode. Není možný mix režimů.

XL-PB360CA dovoluje mix režimu portů.

Poznamenáváme že Master pracuje jako bridge a tagy 802.1Q nemění.

PVID je číslo v rozsahu 1-4095, jde o identifikátor tagu 802.1Q

Allowed VLAN je seznam povolených PVID, zapisuje se jako seznam čísel oddělených čárkou.

COS - Class of Service - stupeň priority, je funkční při aktivním užití 802.1Q. Má smysl jej používat navazující infrastruktura tyto využívá. Jinak ponechte nastavené na 0.

UpLink maximum speed - omezovač rychlosti pro daný port ve směru od Slave k Masteru. 0 znamená že není aktivní.

DownLink maximum speed - omezovač rychlosti pro daný port ve směru od Masteru k Slave. 0 znamená že není aktivní.

Apply - je NUTNĚ stisknout toto tlačítko (nacházející se pod parametry portů) aby provedené změny byly aplikovány. Pokud jste některé změny provedli po stisknutí tohoto tlačítka se vytvoří nové číslo profilu s hodnotou 301 a větší. Tento profil je v Masteru teď přiřazen pouze k tomuto zařízení. Tj. při pohledu do menu Slave - Authorization ihned uvidíte které Slave jednotky jsou nastaveny jednotně dle nějakého z profilů a které byly konfigurovány individuálně.

Refresh - přečte ze zařízení jeho aktuální stav parametrů.

Slave Configuration Information - rozdíly v užití s XL-PB360CA

Na zařízení XL-PB360C jsou všechny čtyři porty ovladatelné z výše popsaného menu a sekce **Current Configuration** vyjadřuje přímo jejich stav.

Avšak na zařízení s vestavěným routem a WiFi, jednotce XL-PB360CA, ovládáte v tomto menu pouze porty které jsou na samotném zařízení označeny STB1 a STB2.

V menu **Current Configuration** tak pro zařízení XL-PB360CA vidíte pouze 3 porty, přestože zařízení má porty 4.

Důvodem je že porty STB1 a STB2 jsou v režimu bridge, zatímco porty LAN1 a LAN2 mohou být v režimu routeru.

Proto oba porty LAN1 a LAN2 jsou skryty v tomto menu pod Port číslo 3 a jeví se být stále připojené a to i v případě že do portu LAN1 nebo LAN2 žádný kabel zapojen není.

Slave Configuration Information pro XL-PB360CA:

Slave [1c:c0:e1:36:a3:67]

Template Selection

Template Application: No Template

Template Configuration

Enable broadcast restriction:
 Enable multicast restriction:
 Enable unknow unicast restriction:
 Restriction threshold (pps):
 Enable loopback check:

Port	Enable Port	Speed&Duplex	Vlan Mode	PVID	Allowed VLAN	COS	UpLink maximum speed (0-102400)Kbps	DownLink maximum speed (0-102400)Kbps
1	<input checked="" type="checkbox"/>	auto	Disable	0		0	0	0
2	<input checked="" type="checkbox"/>	auto	Disable	0		0	0	0
3	<input checked="" type="checkbox"/>	auto	Disable	0		0	0	0

Current Configuration

Port	Link Status	Loop	Enable Port	Adaptive	Speed	Duplex	PVID	COS
1	Disconnect	No	Enable	Enable	10mbps	Half duplex	0	0
2	Disconnect	No	Enable	Enable	10mbps	Half duplex	0	0
3	Connect	No	Enable	Enable	100mbps	Full duplex	0	0

Proto operace prováděné na portu 3 v tomto menu se týkají obou portů LAN1 a LAN2. Také není možné Port 3 při změně VLAN Mode nastavit do režimu Access, ale platný je pouze Trunk nebo Disabled.

Slave MAC Table

Informační okno které ukáže obsah MAC tabulky Slave zařízení. Můžete zde vidět počet přímo připojených zařízení s Ethernetovou adresou.

SLAVE- konfigurace XL-PB360CA

Následující menu jsou funkční pouze pro XL-PB360CA.

(Poznamenejme že je můžete dokázat zobrazit i pro jiná zařízení volbou **Slave Type** ale nebudou funkční.)

Wan configuration

Nastavení režimu práce vestavěného routeru.

Slave [1c:c0:e1:36:a3:5f]

Global Setting

Enable Web Access

Apply Refresh

Setting Wan 1

Service Mode Data

Connection Mode Route Enable VLAN VLAN ID 0 VlanPri 0

Port Binding LAN1 LAN2 LAN3 LAN4 SSID1 SSID2 SSID3 SSID4

Route Setting

ConnType DHCP

IPV4 Address 0.0.0.0

Subnet Mask 0.0.0.0

Default Gateway 0.0.0.0

DNS Server Config Automatic

DNS 1 0.0.0.0

DNS 2 0.0.0.0

Apply Refresh

Setting Wan 2

Service Mode Disable

Apply Refresh

Setting Wan 3

Service Mode Disable

Apply Refresh

Setting Wan 4

Service Mode Disable

Apply Refresh

Saving Setting

Click submit button to save the current settings to flash

Saving Setting

Note: These configure will take effect after save setting .

Dovoluje nastavit režim práce portů LAN1, LAN2 a všech až čtyř SSID.

Nejčastěji využijete nastavení tak jak je na snímku, tj. přidělení vnější adresy od DHCP, rozhraní LAN1, LAN2 a veškerá WiFi komunikace (první SSID) jsou chráněny NAT routem. Připomínáme že porty STB1 a STB2 se toho neúčastní.

Enable Web Access - v případě odškrtnutí má blokovat přístup na management routeru, avšak není funkční, ignorujte.

Service Mode - při nastavení přepněte z Disable na režim Data.

Connection Mode - má režimy Bridge a Route

Route - přiřazené porty (Port Binding) jsou zařazeny za vnitřní NAT router.

Bridge - přiřazené porty (Port Binding) jsou přímo propojeny do EoC sítě, funkce routeru je vynechána. Poznamenejme že použití bridge dává smysl jen s užitím VLAN 802.1Q.

Enable VLAN - povolte užití VLAN 802.1Q

VLAN ID - zadejte PVID 802.1Q pro router, jde o směr k Masteru. Pro správnou funkci musí být ve Slave Configuration Information nastaven port č. 3. na Trunk s tímto ID. Typicky je nastaven jako Trunk s PVID tohoto VLANu. Viz příklady v tomto manuálu.

Port Binding - zaškrtnutím portů určujete jejich přiřazení ke zvolenému Connection Mode. LAN1 a LAN2 jsou na jednotce XL-PB360CA porty označené LAN1 a LAN2. Portů STB1 a STB2 se toto nastavení netýká. Porty SSID1 ~ SSID4 jsou virtuální identifikátory vestavěné WiFi AP. Zaškrtnutí SSID1 tedy znamená provoz který je veden prostřednictvím WiFi přes tento SSID identifikátor.

Při zaškrtnutí portů dbejte na to aby jste neměli stejný port přiřazen i v jinem "Setting Wan". Po uložení by se vám jeho volba ztratila. Port nemůže být přiřazen ke dvěma odlišným nastavením.

Route Settings - zobrazuje se v případě volby Connection Mode = Route.

Conn Type - dovoluje zvolit způsob získání vnější IP adresy routeru.

Static IP - zadáte parametry ručně

DHCP - adresa je přidělována vnějším DHCP serverem

PPPoE - adresa je přidělována PPPoE serverem a je i prováděna autorizace

V případě volby Static IP zadáváte

IPv4 address - vnější IP adresa vestavěného routeru

Subnet Mask - její IP maska

Default Gateway - výchozí brána pro router, tj. IP adresa nejbližšího nadřazeného routeru. Adresa klientského routeru a adresa výchozí brány musí být ve stejném IP adresném prostoru.

DNS1 a DNS2 - IP adres DNS serverů

Použijte tlačítko Apply.

Následně použijte tlačítko Saving Settings. Slave bude Restartovan! Restart trvá 30s.

Poznámka ke kombinování režimů: Konfigurace dovoluje nakombinovat až čtyři různá nastavení. V realitě však nemá významu použít více než jeden Route režim protože nelze na routeru nakonfigurovat více než jedno LAN IP rozhraní a více než jeden DHCP server.

Smysl tak dává jako nejsložitější variant konfigurace 1x Route a až 3x Bridge. Praktický význam použití Bridge je nejvíce kombinaci VLAN ID + SSID. Tj. izolace provozu různých WiFi ID od sebe. Typicky jde o izolaci přípojek WiFi "pro návštěvníky" od přípojek zaměstnanců či technického vybavení komunikujícího po WiFi, například pokladen a čidel.

Lan configuration

Nastavení IP adresy routeru pro uživatele v síti LAN a WiFi a nastavení DHCP serveru pro ně.

Slave [1c:c0:e1:36:a3:67]

IP Address

IP Address	192.168.1.1
Subnet Mask	255.255.255.0

DHCPV4 Server Setting

Enable DHCPV4 server

IP Pool Address from	192.168.1.70	to	192.168.1.90	Edit Reserved Addresses
Subnet Mask	43200			

Saving Setting

Click submit button to save the current settings to flash

Note: These configure will take effect after save setting .

IP adress vnitřní IP adresa routeru. Toto je koncové uživatele jejich výchozí brána.

Subnet Mask IP maska vnitřní síť

Enable DHCPV4 Server povolení/zakázání práce DHCP serveru

IP Pool Address rozsah adres které se budou uživateli přidělovat na jeho zařízení, tj. připojené počítače a mobilní telefony.

Subnet Mask v oddíle DHCPV4 server je chybné pojmenování. Správně má být Lease Time (Seconds) a je to doba po níž je přidělené IP platné. Výchozí hodnotu 43200 sekund (tj. 12hodin).

Edit Reserved Address - nastavení pevného přidělení adresy od DHCP, vztaheno k MAC adrese síťového rozhraní uživatelského zařízení (mobiilu, počítače)

Stiskněte Apply. Nyní jsou sice nastavení uložena ale nejsou aktivní!

Stiskněte Saving Settings. Slave provede restart. Teprve v tuto chvíli jsou nastavení platná!

Static Route Configuration

Statická routovací tabulka dovolující přidání cest do sítě LAN, pokud je více segmentová z hlediska IP.

Použijete tehdy pokud cílové zařízení leží jinde než za výchozí branou routeru.

Destination - IP adresa kterou chcete spojit

Subnet Mask - Maska cílové adresy resp. sítě

Gateway - IP adresa přes níž komunikaci vedete. IP adresa musí být ve stejném IP adresním segmentu jako je vnější IP adresa tohoto routeru.

Slave [1c:c0:e1:36:a3:5f]

Static Routing Table

Destination	Subnet Mask	Gateway	
<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text" value="255.255.255.255"/>	<input style="width: 100%;" type="text"/>	<input type="button" value="Add"/>
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>			

Saving Setting

Click submit button to save the current settings to flash

Note: These configure will take effect after save setting .

Virtual Server Configuration

Dovoluje otevření a přesměrování TCP a UDP portů routeru. Typicky pokud potřebujete provozovat aplikaci za firewallem, jako je web server, SMTP server, herní server atd.

Slave [1c:c0:e1:36:a3:67]

The list of virtual servers

Service name	Local IP	Protocol	Ex Port	In Port	Port number	
<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text" value="192.168.2.231"/>	<input style="width: 100%;" type="text" value="ALL"/>	<input style="width: 100%;" type="text" value="6000"/>	<input style="width: 100%;" type="text" value="7000"/>	<input style="width: 100%;" type="text" value="1"/>	<input type="button" value="Add"/>
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>						

Saving Setting

Click submit button to save the current settings to flash

Note: These configure will take effect after save setting .

Service name - vaše pojmenování přesměrování, jde o komentář

Local IP - IP adresa v místní síti kde služba běží, typicky například váš počítač

Protocol - TCP, UDP nebo oba (All)

Ext Port - pod jakým portem (TCP/UDP) je služba zvenku dostupná

Int Port - na jakém portu (TCP/UDP) je skutečně nastavena ve vaší vnitřní síti.

L2 Switch configuration

Dovoluje nastavení omezovače rychlosti pro WAN rozhraní.

LAN Port Output Mode - vždy je v režimu untag, nelze nastavit na jiný režim.

WAN Port Upstream a Down Stream Limit - dovoluje nastavit omezovače rychlosti které platí souhrnně pro LAN1 a LAN2. Funkčně jde o totéž jako je v Slave Configuration

Information Uplink/Downlink maximum speed pro port 3.

Nutné použít tlačítko Apply a následně použít tlačítko Saving Settings. Slave bude Restartovan.

WiFi Basic Configuration

Zde se spravují parametry WiFi přístupového bodu vestavěného v XL-PB360CA

Slave [1c:c0:e1:36:a3:67]

WiFi

<input checked="" type="checkbox"/> WiFi Enable	Country	CHINA	
Emissive Power	Level5	AP Number	1

AP 1 Setting

SSID	NAZEV_WIFI_SITE		
Channel	Auto	Mode	Auto
			<input type="checkbox"/> Hidden SSID
Security			
Encryption Mode	WPA-PSK/WPA2-PSK		
Key Format	Ascii		
Alorithm	TKIP/AES		
Key	nejake_heslo		

Saving Setting

Click submit button to save the current settings to flash

Note: These configure will take effect after save setting .

WiFi Enable povolení funkčnosti WiFi jako takového. Po restartu se rozsvítí led dioda WIFI.

Emissive Power - určuje vysílací výkon s jakým má zařízení pracovat. Má smysl jeho výkon snížit na minimum pokud například instalujete zařízení v mnoha pokojí a zařízení jsou tak relativně blízko u sebe. Omezíte tím množství interferencí. Level1 = nejmenší výkon, Level5 = největší výkon.

Country oblast povolených kmitočtů, ponechte na CHINA

AP Number počet SSID které chcete v systému konfigurovat, min. 1, max. 4

SSID název uživateli WiFi sítě, tj. po d jakým jménem ji naskenujete ve svém přístroji

Channel Auto - volbu kanálu WiFi ponecháte na přístroji, číselná volba - zvolíte kanál

Mode Auto - automatická volba - standardně zvolí 11NGHT20

11B = 802.11b, volte pouze v případě velmi starých zařízení

11G = 802.11g

11NGHT20 = 802.11g/n 20MHz šířka pásma

11NGHT40PLUS = 802.11g/n 40MHz šířka pásma, horní pásmo kmitočtů, tj. kanály 5-11

11NGHT40MINUS = 802.11g/n 40MHz šířka pásma, dolní pásmo kmitočtů, tj. kanály 1-7

Režimy se 40MHz pásmem doporučujeme volit jen v situacích kdy je skupina WiFi zařízení předem dána a víme že jsou schopna takové pásmo využívat.

Hidden SSID zaškrtněte pokud chcete aby SSID nebylo vysíláno (tzv. skrytá síť)

Encryption Mode režimy šifrování WiFi komunikace

NONE - pouze v případě poskytování veřejné WiFi sítě bez hesla

WEP - jen z důvodu kompatibility, nepoužívejte

WPA-PSK - bezpečný, podporovaný staršími zařízeními

WPA2-PSK - nejbezpečnější režim

WPA-PSK/WPA2-PSK - smíšený režim, pro nejlepší kompatibility

Algorithm

TKIP -- volte jen z důvodu zpětné kompatibility

AES -- přednostně volte tuto šifru

TKIP/AES -- volte smíšený režim pro co největší kompatibility

Key přístupové heslo

Stiskněte Apply. Nyní jsou sice nastavení uložena ale nejsou aktivní!

Stiskněte Save. Slave provede restart. Teprve v tuto chvíli jsou nastavení platná!

WiFi Management

V tomto menu se nespravuje nic co se týká WiFi, spravují se zde přístupová jména/hesla pro zařízení s AP.

Slave [1c:e0:e1:36:a3:67]

Cli User Setting	
User	<input type="text" value="root"/>
Common Password	<input type="password" value="....."/>
Super Password	<input type="password" value="....."/>
<input type="button" value="Apply"/>	
Web User Setting	
User	<input type="text" value="admin"/>
Password	<input type="password" value="....."/>
<input type="button" value="Apply"/>	
Saving Setting	
Click submit button to save the current settings to flash	
<input type="button" value="Saving Setting"/>	
Factory Setting	
Click button to restore the factory settings of the home gateway	
<input type="button" value="Reset Factory Setting"/>	
Reboot System	
Click submit button to reboot the wifi system	
<input type="button" value="Reboot"/> <input type="button" value="Refresh"/>	

Note: These configure will take effect after save setting in wifi management web page.

CLI User Settings

obsahuje údaje pro přihlášení do Slave routeru přes Telnet

User jméno uživatele, standardně root

Common Password a Super Password zadajte do těchto polí dvakrát stejné nové heslo, popis těchto polí je matoucí, není žádné Common a Super heslo, jen dvakrát zadáváte heslo pro kontrolu.

Web User settings

je přihlašovací jméno a heslo které zadáváte pokud se na router přihlašujete z web prohlížeče. Výchozí nastavení je jméno admin a heslo admin.

User jméno uživatele, standardně admin

Password zadejte zde nové heslo

Apply - potvrdí vložení údajů, ale neaktivuje je

Saving Settings - Slave provede restart. Teprve v tuto chvíli jsou hesla platná!

Reset Factory Settings - provede reset zařízení do výchozího, továrního, nastavení

Reboot - provedet Restart zařízení

WiFi Upgrade

Možnost upgradovat firmware zařízení XL-PB360CA. Děje se tak prostřednictvím spojení na FTP server. Popis postupu upgradu je jeho součástí. Pokud nemáte nový firmware toto menu ignorujte.

SLAVE - Templates

Dovoluje správu Templates, doslovně konfiguračních Šablon které výrazně urychlují konfiguraci sítě.

Default Template

Default Template
 Enable
 Disable

When the default templates is enabled, the new registered slaves will apply the default template configuration.

Template Management

Template Index	Template Name	Template Class	Operation	
<u>1</u>	DefaultTemplate	SW	<input type="button" value="Modify"/>	<input type="button" value="Delete"/>
<u>2</u>	Bez_omezovacu	SW	<input type="button" value="Modify"/>	<input type="button" value="Delete"/>

Templates pracují tak že ve chvíli kdy se zařízení připojí do sítě, tj. je zapnuto, Master do něj automaticky nahraje konfiguraci kterou má k němu přiřazenu a uloženu. A tato konfigurace může být buď tzv. privátní template (to jsou ty které můžete vidět že mají číslo od 300 výše) nebo jste k tomuto zařízení přiřadili šablonu z vašich definic (ty mají čísla 1-253)

Templates v Master jsou pouze třídy SW konfigurují tak pouze Layer2 síťovou vrstvu. Nekonfigurují vestavěný router ani jiné vlastnosti.

Jejich největší efektivnost je právě se zařízeními XL-PB360C. Pro zařízení XL-PB360CA je největší část práce právě konfigurace vestavěného routeru, WiFi, jména a hesla atd. a v tom Templates nehrají žádnou roli.

Nový Template můžete vytvořit stisknutím tlačítka Add New Template.

Příklad šablony zde:

Template[3]

Template Configuration

Template Index: (1~256)

Template Name: (Max length:32 characters)

Enable broadcast restriction:
 Enable multicast restriction:
 Enable unknow unicast restriction:

Restriction threshold (pps):

Enable loopback check:

Port configuration

Port	Enable port	Speed&Duplex	Vlan Mode	PVID	Allowed VLAN	COS	UpLink maximum speed (0-102400)Kbps	DownLink maximum speed (0-102400)Kbps
1	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	<input type="text" value="Access"/>	<input type="text" value="101"/>	<input type="text" value=""/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
2	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	<input type="text" value="Access"/>	<input type="text" value="102"/>	<input type="text" value=""/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
3	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	<input type="text" value="Access"/>	<input type="text" value="103"/>	<input type="text" value=""/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
4	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	<input type="text" value="Trunk"/>	<input type="text" value="104"/>	<input type="text" value="104-106"/>	<input type="text" value="5"/>	<input type="text" value="10000"/>	<input type="text" value="20000"/>

SLAVE - MAC Limit

Dovoluje určit maximální počet MAC adres která Slave dovolí připojit na straně LAN. Funkce slouží nejvíce jako bezpečnostní opatření proti závadě nebo útoku.

Global Mac Limit Parameter(0~65) -- zadáním čísla do tohoto pole a stiskem **Modify** se toto číslo nastaví do všech připojených Slave jednotek hromadně.

Lze rovněž omezit počet MAC adres na každém Slave zařízení samostatně, změňte hodnotu v poli Limit a stiskněte Modify.

Zadáním hodnoty 0 se limit na počet MAC adres zruší.

Zadání hodnoty 65 je totéž jako zákaz všech MAC adres.

Příklad zadání různých limitů počtu MAC adres.

MAC Limit				
Global Mac Limit Parameter(0~65) :		<input type="text" value="30"/>	<input type="button" value="Modify"/>	

Online Slave MAC Limit				
ID	MAC	Status	Limit(0-65)	Operation
1	1c:c0:e1:36:a3:4d	Online	<input type="text" value="1"/>	<input type="button" value="Modify"/>
2	1c:c0:e1:36:a3:45	Online	<input type="text" value="2"/>	<input type="button" value="Modify"/>
3	1c:c0:e1:36:a3:5f	Online	<input type="text" value="15"/>	<input type="button" value="Modify"/>
4	1c:c0:e1:36:a3:57	Online	<input type="text" value="30"/>	<input type="button" value="Modify"/>
5	1c:c0:e1:36:a3:3f	Online	<input type="text" value="30"/>	<input type="button" value="Modify"/>
6	1c:c0:e1:36:a3:67	Online	<input type="text" value="30"/>	<input type="button" value="Modify"/>

'0' :disable, '65' :limit to 0.

RF - Info

Informační okno dovolující změnit vysílací výkon všech zařízení a změnit rozsah pracovního pásma.

Změna vysílacího výkonu je zajímavá jen v případě že dochází s interferencí s jinou technologií která sice zabírá jiné frekvenční pásmo ale je podezření že vyšší harmonické z provozu EoC jí vadí. Snížením vysílacího výkonu klesne i rušivá složka.

Snížení výkonu se rovněž aplikuje v situaci kdy instalujeme více Masterů obsluhujících vlastní kabelové segmenty. (viz. druhé schéma v kapitole "Instalace pro společné TV rozvody"). Ty sice nejsou přímo spolu komunikačně spojeni ale signál proniká ve směru do portu "CATV INPUT" s útlumem cca. 25dB a následně s útlumem 25dB vstoupí do sousední větve. To znamená že je signál je zatlumen o 50dB (a více, v cestě má ještě splittter, případně zesilovač). Nicméně vzhledem k vysoké citlivosti zařízení je vhodné snížit vysílací výkony všech větví o cca. 10dB tak aby se snížilo jejich vzájemné ovlivnění.

Změna šířky pásma je zajímavá jen pro případy kdy je třeba zúžit vysílací pásmo tak aby nedocházelo k interferenci s jinou technologií která zasahuje do pásma 7,6-67,5MHz. Obvykle o této technologii víme předem.

Master Rf Information								
Master MAC	Maximum amount of slave	RF Output Level		Starting Frequency		Ending Frequency		Operation
1c:c0:e1:36:a3:35	253	115	dBμV (90~115)	7.6	MHz (7.6~67.5)	67.5	MHz (7.6~67.5)	Modify

Refresh

Online Slave Rf Information								
ID	Slave MAC	Status online	RF Output Level	Starting Frequency		Ending Frequency		Operation
1	1c:c0:e1:36:a3:4d	Online	115 dBμV	7.6	MHz	67.5	MHz	Modify
2	1c:c0:e1:36:a3:45	Online	115 dBμV	7.6	MHz	67.5	MHz	Modify
3	1c:c0:e1:36:a3:5f	Online	115 dBμV	7.6	MHz	67.5	MHz	Modify
4	1c:c0:e1:36:a3:57	Online	115 dBμV	7.6	MHz	67.5	MHz	Modify
5	1c:c0:e1:36:a3:3f	Online	115 dBμV	7.6	MHz	67.5	MHz	Modify
6	1c:c0:e1:36:a3:67	Online	115 dBμV	7.6	MHz	67.5	MHz	Modify

Refresh

... indicate that the slave does not support RF configuration function, or configuration query failed.

Snížení vysílacího výkonu má ve své podstatě obdobný vliv jako vložení útlumu. Vliv útlumu na rychlost spoje viz měření v kapitole "Závislost přenosu na útlumu trasy"

Proto pokud zařízení hlásí že pracují s útlumem nižším než 35dB nebude mít snížení výkonu žádný významný vliv na propustnost sítě.

Vliv změny šířky pásma viz měření v kapitole "Vliv omezení pásma na přenosový výkon"

NETWORK - Status

Informace o datech prošlých Ethernetovými rozhraními Masteru.

NETWORK - Config

Nastavuje IP adresu pro vnitřního bridge, tj. IP adresu která je dostupná na portu označeném 10/100/1000Mbps. Nikoliv adresu na portu MGMT,

Adresu můžete zadat jako pevnou nebo přidělovanou od DHCP.

Je nutné ji konfigurovat pokud máte více Masterů spojených na nadřazený router prostřednictvím switchu, tak aby nedocházelo ke konfliktu IP. Pro instalace s jedním Mastrem ji není třeba měnit.

Poznamenejme že jde o adresu na níž můžete, v případě že Slave je v Bridge režimu, přistupovat i ze Slave zařízení. Viz poznámky v kapitole Postup zabezpečení Masteru

Network Information

MAC:	1C:C0:E1:36:A3:36		
Connect type:	<input type="text" value="Static IP"/>		
IP:	<input type="text" value="192.168.2.1"/>		
Subnet mask:	<input type="text" value="255.255.255.0"/>		
Default gateway:	<input type="text" value="192.168.2.1"/>		

If you modify the configuration on this pages, the configuration will be saved, but it will have no effect on the device until the device is rebooted.

NETWORK - VLAN

Nastavuje VLAN 802.1Q pro rozhrani managementu. Jakmile přidělíte značku VLAN je nutné k managementu přistupovat z rozhraní které rovněž zasílá pakety s touto značkou.

Management VLAN Information

VLAN ID:	<input type="text" value="0"/>	<input type="button" value="Modify"/>
VLAN Status:	VLAN[0] Has been set to disable mode	<input type="button" value="Enable"/>

NETWORK - SNID

SNID, Sort Network ID, slouží k odlišení více Master jednotek v jedné EoC síti. Ponechte na 0, číslo se při každém restartu změní.

Master SNID Information

SNID:	<input type="text" value="10"/>	(0:auto 1-15:static)	<input type="button" value="Modify"/>
--------------	---------------------------------	----------------------	---------------------------------------

NETWORK - Filter

Jde o omezovač příchozích provozů které jsou zasílány všesměrově (Broadcast) nebo v režimu Multicast.

Broadcast limiting	
Broadcast limiting enabled:	<input type="checkbox"/>
Broadcast limit threshold:	<input type="text" value="1"/> % (1-100%)
<input type="button" value="Submit"/>	
Multicast limiting	
Multicast limiting enabled:	<input type="checkbox"/>
Multicast limit threshold:	<input type="text" value="10"/> % (1-100%)
<input type="button" value="Submit"/>	

Dovoluje omezit zvolené provozu poměrným způsobem. Oproti popisu není rozsah zadání 1-100 ale ve skutečnosti 1-10. Tj. při zadání 2 se limituje příchozí provoz na cca. 20% maxima.

Limitují se provozu přicházející do Masteru ze strany vnějšího rozhraní, tj. například z Internetu.

NETWORK - Igmp

Zde se aktivuje podpora IGMP. Má pro vás význam jen v souvislosti s užitím Multicastu. Prosím prostudujte kapitolu Nastavení pro Multicasting

IGMP Query Proxy Information	
Query Interval:	<input type="text" value="10"/> s Stepsize: 10s
Igmp Vlan:	Refresh <input checked="" type="checkbox"/> Vlan Id <input type="text" value="101"/> <input type="button" value="Modify"/>
Igmp Status:	Igmp[10]Has been set to enable mode <input type="button" value="Disable"/>
<input type="button" value="Refresh"/>	

SERVICE - Service

Slouží k vypnutí/zapnutí běhu služby SNMP a SSH. Změna je okamžitá, není třeba restart.

Spuštění SSH vám dovolí používat bezpečnější přístup na konzoli Masteru než je výchozí Telnet (pokud nejste Linuxový expert nemá pro vás přístup na konzoli Masteru žádný význam).

System Information		
Service Type	ON	OFF
NETWORK	<input checked="" type="radio"/>	<input type="radio"/>
BRIDGE	<input checked="" type="radio"/>	<input type="radio"/>
FTP	<input checked="" type="radio"/>	<input type="radio"/>
TFTP	<input checked="" type="radio"/>	<input type="radio"/>
HTTP	<input checked="" type="radio"/>	<input type="radio"/>
TELNET	<input checked="" type="radio"/>	<input type="radio"/>
SNMP	<input type="radio"/>	<input type="radio"/>
SSH	<input checked="" type="radio"/>	<input type="radio"/>

SYSTEM - Information

Zobrazí verzi a MAC adresy rozhraní, dobu běhu. Dovoluje zde vyplnit popisek o zařízení a jeho umístění.

SYSTEM - Running Sttaus

Zobrazí stav systému. Dovoluje nastavit poplachové úrovně signalizující přetížení systému.

SYSTEM - Slave Type

Dovoluje vytvořit vlastní Slave Type, který můžete následně přiřadit ke Slave jednotce. Má význam jen pro možnou kompatibilitu s jednotkami třetích stran.

SYSTEM - IP Access Control

Dovoluje zadat seznam IP adres z nichž je povolený přístup k web managementu masteru.

SYSTEM - System Time

Dovoluje zadat datum a čas do Masteru nebo jej napojit na automatickou synchronizaci přes NTP protokol. Má význam jen pro správné datum v logu Masteru. Na funkčnost systému nemá vliv.

SYSTEM - System Log

Dovoluje prohlížet log Masteru a dovoluje konfigurovat zasílání logu na externí server.

Log Setup

Log Enable

Note: The option controls the entire information output system.

Remote registry host configuration

Registration level

Host IP address

Host port

Pro využití této funkce je třeba spustit službu typu syslog na definované IP adrese a portu.

SYSTEM - Account

Dovoluje změnit přihlašovací údaje k web managementu. Pro změnu musíte znát původní heslo.

Modify account

Original account:

Original password:

New account:

New password:

Repeat New Password:

SYSTEM - Reboot

Odkaz **Save Config** uloží právě aktivní konfiguraci.

Tlačítko **Reboot Systém** restartuje celý Master.

Tlačítko **Reboot EoC chip** - restartuje komunikaci vůči Slave zařízením. Restart trvá sice jen 10 sekund, ale vlastní obnovení spojení od Slave zařízení může být významně delší.

Auto Reset EoC Chip

Jde o hlídání funkčnosti EoC komunikace (watchdog), během níž sleduje zda dostává od Slave zařízení pakety.

Po startu EoC je test nejdříve definovanou dobu (Hold Time) zastaven. Pak je zjišťováno zda během doby Examination period přišel definovaný počet paketů. Pokud ne je proveden restart EoC čipu, který přeruší komunikaci se všemi Slave zařízeními na nejméně 10s (nejde o reboot systému). Pokud definovaný počet paketů od Slave zařízení přijde je toto bráno jako funkční, EoC není resetováno a cyklus se opakuje.

Auto Reset Enable - povoluje/zakazuje provádění kontroly. Pokud nezaznamenáváte problémy s propojením EoC není důvodu tuto funkci povolit

Examination Period - délka testu spojení během níž se počítají pakety.

Hold Time - doba během níž se neprovádí test, je to pauza mezi testy. Rozhodně jí je nutné nastavit na déle než je restart EoC rozhraní který trvá cca. 10s. Stejně tak nedoporučujeme nechat ji na dlouhém výchozím intervalu 43200 (12h) jelikož funkce začne být poprvé aktivní až po této době.

UpStream Unicats Pakets - počet paketů které musí během Examination period dorazit od klientských jednotek. Pokud zadáte číslo vysoké je jisté že se bude provádět restart EoC komunikace v intervalu HoldTime+Examination Time.

Apply - změna je provedena ihned, není třeba reset.

Níže příklad nastavení - test čeká 120s, pak pokud mu během 60s nepříjde ani jeden unicastový paket od Slave zařízení provede reset EoC komunikace.

Reboot System	
Click this button to reboot the system. Please Save Configuration before rebooting	
<input type="button" value="Reboot System"/>	
Reboot Eoc Chip	
Click this button to reboot the eoc chip	
<input type="button" value="Reboot Eoc Chip"/>	
Auto Reset EoC Chip	
Auto Reset Enable	<input checked="" type="checkbox"/>
Examination Period	<input type="text" value="60"/> Seconds
Hold Time	<input type="text" value="120"/> Seconds
UpStream Unicast Packets	<input type="text" value="1"/> Pkts
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>	

SYSTEM - Factory

Resetuje Master do továrního nastavení.

SYSTEM - Upgrade

Dovoluje upgrade Master jednotky.

SYSTEM - Backup

Dovoluje zálohovat nastavení Masteru a provést jeho obnovení. Pro funkčnost potřebuje aby na cílovém zařízení běžel FTP server.

SYSTEM - SNMP

Trap Server

Dovoluje nastavení kam se mají posílat automatická hlášení z SNMP Masteru. Jde o vestavěný mechanismus SNMP dovolující automaticky monitorovat definované parametry a zbavuje tak nutnosti neustále tyto data načítat ze zařízení. Do řádku zadáváte IP adresu stroje na nějž tato hlášení (Traps) posíláte. Dále jeho UDP port a Community (defakto heslo), pokud to je cílovým strojem vyžadováno.

Community

Dovoluje nastavení SNMP jména pro Read a Write Community, tj. defakto hesla dovolující čtení a zápis do SNMP registrů Masteru.

Master nemá šifrovanou komunikaci SNMP (tj. není v3) a hesla putují v otevřeném kódu. Proto doporučujeme komunikaci omezit na bezpečnou část sítě nebo ji zapouzdřit do VPN na nejbližším routeru. Pokud SNMP nepoužíváte doporučujeme jej vypnout.

Trap Server				
ID	IP	port	Community name	Operation
1	<input type="text" value="0.0.0.0"/>	<input type="text" value="162"/>	<input type="text" value="public"/>	<input type="button" value="Modify"/>
2	<input type="text" value="0.0.0.0"/>	<input type="text" value="162"/>	<input type="text" value="public"/>	<input type="button" value="Modify"/>

Community	
Read Community :	<input type="text" value="public"/>
Write Community :	<input type="text" value="private"/> <input type="button" value="Modify"/>

SNMP komunikace pro vás má největší smysl pro monitoring práce zařízení. Poskytne údaje o procházejícím množství dat a stavu práce zařízení. Tj. údaje dostupné jinak v menu NETWORK-Status a SYSTEM-Running Sttus. Nenaleznete zde například údaje o datech poslaných na konkrétní Slave/klienta. K této činnosti využijte předřazený router.

Web management XL-PB360CA

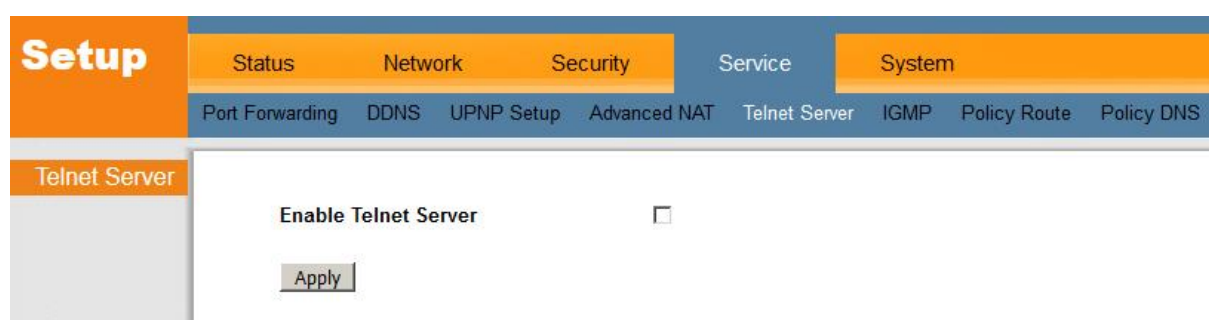
Výše jsme popisovali správu Slave jednotky XL-PB360CA prostřednictvím Masteru. Jednotku lze ale spravovat i přímo v jejím web rozhraní.

Logovací heslo pro tuto činnost můžete nastavit prostřednictvím Masteru ve WiFi Magement.

Tento web management má v moci na v zařízení v moci pouze porty LAN1 a LAN2 a router který je jim předřazen. Je jen omezené množství věcí v nichž by se tato administrace lišila od dříve popsaného a stojí za zmínku. Navíc pokud je zařízení na straně uživatele a provede výmaz zařízení do továrního nastavení tlačítkem RST všechna tato nastavení, včetně přihlašovacího hesla do tohoto rozhraní jsou vymazána na výchozí hodnoty.

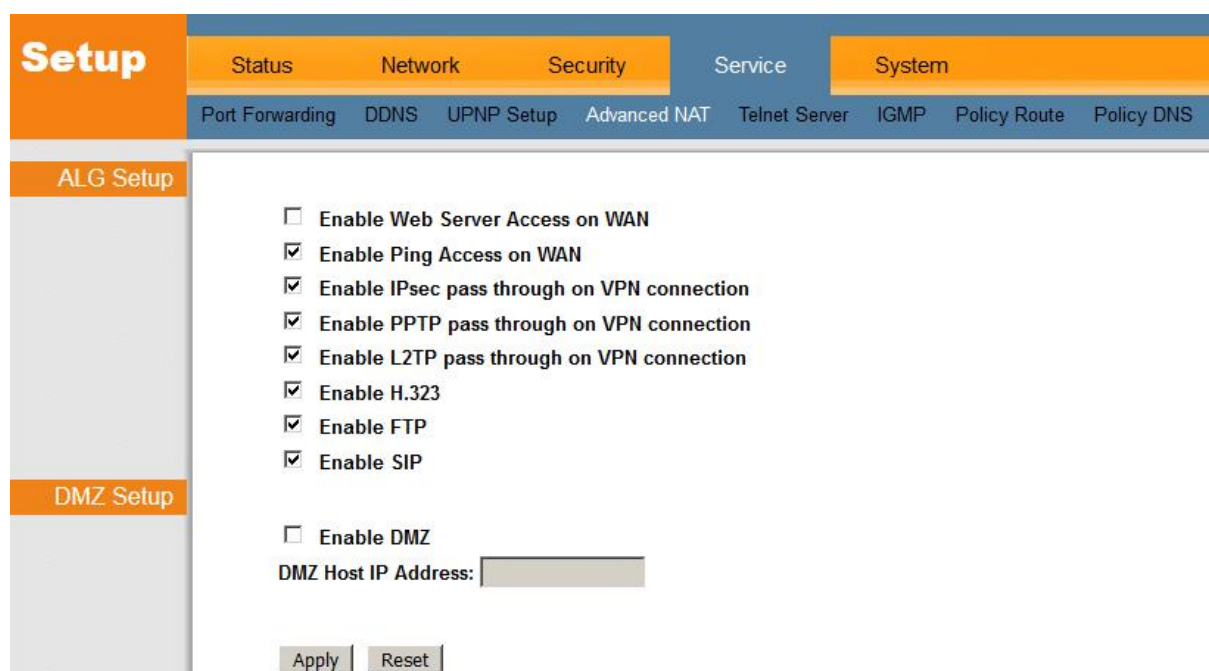
Vypnutí Telnetu:

naleznete v Service - Telnet Server - Enable/Disable



Některé funkce firewallu

Service - Advanced NAT - Enable/Disable



Možnost založit uživatele s nižšími právy než administrátor. Takového uživatele můžete sdělit následně koncovému uživateli.

Jeho založení naleznete v System - Admin Account Management

The screenshot shows the 'Setup' interface with the 'System' tab selected. Under 'System', 'Admin Account Management' is chosen. The 'User Management' section displays a table with the following data:

ID	User name	User permissions	Password	New Password	Confirm new password	Operation
2	admin	Administrator	<input type="text"/>	<input type="text"/>	<input type="text"/>	Modify Delete
3	user	User	<input type="text"/>	<input type="text"/>	<input type="text"/>	Modify Delete
+	<input type="text"/>	Administrator	+	<input type="text"/>	<input type="text"/>	Add

Založením uživatele s User permission = User vznikne uživatel který se po přihlášení dostane jen do menu která nejsou pro provoz zařízení kritická.

Především mu však umožníte aby si mohl nastavovat WiFi zařízení jak potřebuje, případně máte možnost aby využíval menu Dagnosis pro základní testy ping a traceroute.

Zabezpečení sítě

Postup zabezpečení Masteru

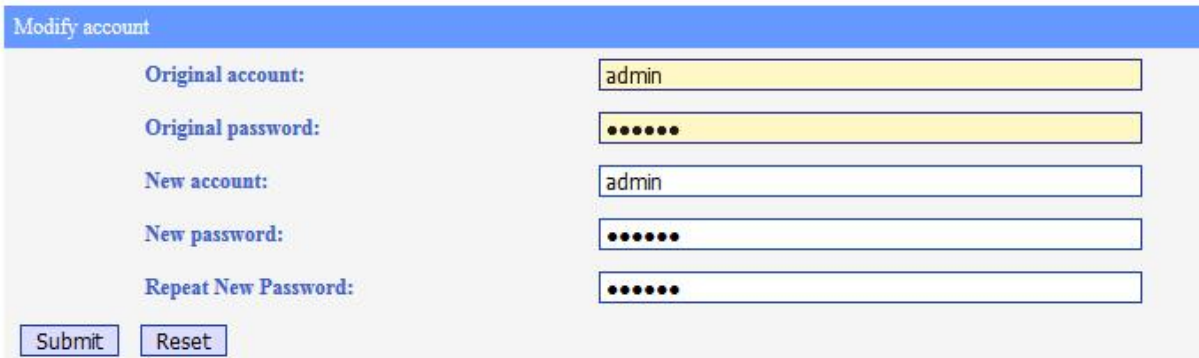
Ve výchozím stavu je možné přihlášení se do web rozhraní Masteru jak přes preferované rozhraní MGMT (out-of band) ale i přes in-band rozhraní. Tj. pokud si uživatel ve vaší síti zadá vhodný IP adresní rozsah a vy necháte zařízení ve výchozím nastavení je celkem jisté že nastane problém.

Proto doporučujeme následující:

a)
Změna hesla pro admin

Menu System-Account

Do pole New Account zadejte admin, do nasledujich poli zadejte vase nove heslo:



Original account:	<input type="text" value="admin"/>
Original password:	<input type="password" value="....."/>
New account:	<input type="text" value="admin"/>
New password:	<input type="password" value="....."/>
Repeat New Password:	<input type="password" value="....."/>

b)
Změňte masku IP adresy EoC Ethernet rozhraní tak aby byla nedostupná. Jde o IP adresu která je IP adresou dostupnou jak z Gigabitového rozhraní tak od Slave zařízením. Master nemá mechanismu který by dokázal uživatelům na Slave zařízení Master zcela znepřístupnit. Proto je vhodnější pokud administrujete zařízení prostřednictvím druhého rozhraní označeného MGMT. To je uživatelům na Slave zařízení nepřístupné.

Používání MGMT můžete vyřešit tak že máte jako přípojku do internetu router se dvěma LAN rozhraními a nebo pokud přijmete více Master jednotek tak mezi router a Mastery vložíte switch který má izolaci portů (názvu je více - tzv. portový VLAN, MDU režim apod.). Pak může být router i jednoportový.

Vlastní blokaci této IP adresy provedete změnou její síťové masky na 255.255.255.255, čímž jí znemožníte spojení.

IP adresu naleznete v menu **System-Config**

Network Information

MAC: 1C:C0:E1:36:A3:36

Connect type:

IP:

Subnet mask:

Default gateway:

If you modify the configuration on this pages, the configuration will be saved, but it will have no effect on the device until the device is rebooted.

Maska se nezmění do doby restartu Masteru, proto jej restartujte.

- c)
 Nastavte IP filtr pro přístup na MGMT rozhraní.
 Filtr naleznete v menu **System - IP Access Control**

IP Access Control

Enable Disable

The List Of IP Address To Allowable Access

ID	Begin IP	End IP	Subnet Mask	Operation
1	<input type="text" value="192.168.1.1"/>	<input type="text" value="192.168.1.254"/>	<input type="text" value="255.255.255.0"/>	<input type="button" value="Modify"/> <input type="button" value="Delete"/>

Nyní se lze na Master přihlásit pouze přes MGMT rozhraní a pouze z IP adres definovaných ve filtru.

- d)
 Vypněte podporu SNMP v menu **Service**
 SNMP nepoužívá zabezpečený přístup. Proot jej doporučujeme používat jen pokud máte zabezpečený přístup pomoci VPN, jinak je lépe tuto funkci odstavit.

Postup zabezpečení Slave

Vysvětlení tlačítka RST a jeho Továrního nastavení

Koncový uživatel nemůže obejít nastavení funkce portů provedením resetu do továrního nastavení!

Každý Slave má resetovací tlačítko RST ukryté za malým otvorem. Pokud jej uživatel podrží na déle než 5s při zapnutém zařízení dojde k nastavení do továrního nastavení.

Avšak nastavení portů se konfiguruje při každém startu z Masteru, defakto je součástí procesu autorizace zařízení. Konfigurují se jen parametry obsažené v menu Slave Configuration Information.

Především tak uživatel nemůže továrním resetem obejít zakázání portů, nastavení VLANů a omezení na rychlost. Nemůže obejít autorizaci Slave do sítě a ani se neztratí pojmenování tohoto Slave.

V případě zařízení s vestavěným routrem XL-PB360CA se při továrním nastavení vymaže nastavení vnitřního routeru do výchozího nastavení a do výchozího nastavení se uvede WiFi přístupový bod a budou platit i výchozí logovací hesla.

Proto pro ochranu sítě nespolehejte na nastavení tohoto vnitřního routeru ale nastavte omezení na úrovni síťových portů.

To je rovněž důvodem proč je vhodné každému zařízení přiřadit Template tzn. nenechat jej na čísle 0.

Dodatečná zabezpečení Slave jednotek

V případě jednotky XL-PB360C není žádné další zabezpečení nutné, zařízení nemá ani IP adresu a vše je zpravováno přes Master. Tj. při užití jen těchto jednotek je EoC síť významně jednodušší po stránce bezpečnosti.

V případě XL-PB360CA a v případě, že nehrozí uživatelské mazání nastavení tlačítkem RST má smysl zabezpečit i jeho vnitřní router. Jde především o změnu přístupového hesla do zařízení. Provedete následujícím způsobem:

Jděte v Masteru do menu SLAVE - Authorization - vyberte zařízení - jděte do menu WiFi Management:

Slave [1c:c0:e1:36:a3:67]

CLI User Setting

User	<input type="text" value="root"/>
Common Password	<input type="password" value="••••••"/>
Super Password	<input type="password" value="••••••"/>
<input type="button" value="Apply"/>	

Web User Setting

User	<input type="text" value="admin"/>
Password	<input type="password" value="•••••"/>
<input type="button" value="Apply"/>	

Saving Setting

Click submit button to save the current settings to flash

Factory Setting

Click button to restore the factory settings of the home gateway

Reboot System

Click submit button to reboot the wifi system

Note: These configure will take effect after save setting in wifi management web page.

CLI User Settings obsahuje údaje je pro přihlášení do Slave routeru přes Telnet. Rozhodně heslo změňte. Zadáváte jej dvakrát do polí Common Password a Super Password (popisek polí je matoucí, jde jen o opakování hesla) .

Web User settings je přihlašovací jméno a heslo které zadáváte pokud se na router přihlašujete z web prohlížeče. Výchozí nastavení je jméno admin a heslo admin.

Stiskněte Apply. Nyní jsou sice nastavení uložena ale nejsou aktivní!

Stiskněte Saving Settings. Slave provede restart. Teprve v tuto chvíli jsou hesla platná!

e) Rovněž je vhodné vypnout Telnet server který je v routeru XL-PB360CA. Lze jej úplně vypnout prostřednictvím web managementu přímo v routeru.

Nastavení vnějšího firewallu

Pokud je vaše EoC síť nějakým způsobem napojena do internetu rozhodně nastavte alespoň základní opatření na svém firewallu. Především znemožněte přístup z vnější sítě na správcovská rozhraní.

Zvláště blokujte přístup na tyto TCP/UDP porty všech EoC zařízení:

Telnet (23), SNMP (161), SSH (22), Web rozhraní (80)

Příklady nastavení

Slave s routrem a WiFi - základní nastavení

Následující příklad je typickou jednoduchou konfigurací jednotek XL-PB360CA v bytovém domě či hotelu. Požadujeme aby klienti měli WiFi přístupový bod a zároveň konfigurace byla jednoduchá. V tomto příkladu není připojeno IPTV STB zařízení. Není použita žádná další autorizace Slave zařízení.

Výsledkem bude v každém bytě router s NAT a WiFi AP za tímto. Klienti se budou moci připojit do portů LAN1, LAN2 a přes WiFi.

IP adresa bude uživatelům přidělována z vestavěného DHCP serveru.

Provoz z jednotlivých bytů odlišíme jejich vnější IP adresou. Tuto adresu v příkladu zadáváme staticky a pro každý byt je potřeba ji zadat odlišně. V příkladu jsou použity IP adresy z Privátního adresního rozsahu (192.168.33.x) neboť se předpokládá existence nadřazeného routeru s MASQ/NAT překladem adres. Pokud takový není a již přímo přidělujete platné IP adresy změní se konfigurace jen v tom ohledu že místo adres z rozsahu 192.168.33.x vkládáte platné IP adresy a platnou IP výchozí bránu.

Postup:

Přejdeme do menu **SLAVE - Authorization** a kliknutím na MAC adrese 6. zařízení si otevřeme nastavení XL-PB360CA.

Authorization Mode

Authorization Mode: Auto Auth Manual Auth

Slave Authorization

ID	Slave MAC	Wifi MAC	Auth Enable	Status	Slave Type	Automatic update allow	Start time	End time	Template Selection	Operation
1	1c:c0:e1:36:a3:4d	None	<input checked="" type="checkbox"/>	Online	EoC-Slave-4	<input checked="" type="checkbox"/>	00:00	23:59	2	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
2	1c:c0:e1:36:a3:45	None	<input checked="" type="checkbox"/>	Online	EoC-Slave-4	<input checked="" type="checkbox"/>	00:00	23:59	302	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
3	1c:c0:e1:36:a3:5f	1c:c0:e1:36:a3:61	<input checked="" type="checkbox"/>	Online	EoC-Slave-EW	<input checked="" type="checkbox"/>	00:00	23:59	303	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
4	1c:c0:e1:36:a3:57	1c:c0:e1:36:a3:59	<input checked="" type="checkbox"/>	Online	EoC-Slave-EW	<input checked="" type="checkbox"/>	00:00	23:59	1	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
5	1c:c0:e1:36:a3:3f	None	<input checked="" type="checkbox"/>	Online	EoC-Slave-4	<input checked="" type="checkbox"/>	00:00	23:59	1	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
6	1c:c0:e1:36:a3:67	1c:c0:e1:36:a3:69	<input checked="" type="checkbox"/>	Online	EoC-Slave-EW	<input checked="" type="checkbox"/>	00:00	23:59	306	<input type="button" value="Modify"/> <input type="button" value="Delete"/>

Unauthorized Slave

Index	MAC	Operation
<input type="button" value="Refresh"/>		

V menu **SLAVE - Basic Information** si jednotku pojmenujte, vyplňte pole User Information a stisknete Apply, změna je provedena ihned.

Slave [1c:c0:e1:36:a3:67]

Slave Information	
Slave Type	EoC-Slave-EW
Port Number	3
Software Version	7.1.0 & INT7400-MAC-7-1-7131-00-17-20131108-FINAL-QCA7411L-B
User Information	<input type="text" value="XL-PB360CA pokoj 111"/>
Attenuation	44 dB
Signal Noise Ratio	UpLink 31.40 dB Downlink 31.02 dB
Modulation	UpLink 10.48 bits/carrier Downlink 10.39 bits/carrier
Speed	UpLink 340 Mbps Downlink 337 Mbps
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>	

Other Information	
<input type="button" value="Reboot"/>	

Přejdeme do nastavení **Slave Configuration Information**.

Porty 1. a 2. což jsou porty STB1 a STB2 fyzicky odpojíme, tj. zakážeme jejich používání.

Můžeme zapnout Broadcast restrictions a detkci vzniku smyčky Enable Loopback check.

Port 3. necháme ve výchozím nastavení. Stiskněte Apply dole, změna nevyžaduje restart Slave zařízení.

Slave [1c:c0:e1:36:a3:67]

Template Selection	
Template Application:	<input type="text" value="306"/> <input type="button" value="Apply"/> Private Template

Template Configuration					
Enable broadcast restriction:	<input checked="" type="checkbox"/>	Enable multicast restriction:	<input type="checkbox"/>	Enable unknow unicast restriction:	<input type="checkbox"/>
Restriction threshold (pps):	<input type="text" value="2560"/>				
Enable loopback check:	<input checked="" type="checkbox"/>				

Port	Enable Port	Speed&Duplex	Vlan Mode	PVID	Allowed VLAN	COS	UpLink maximum speed (0-102400)Kbps	DownLink maximum speed (0-102400)Kbps
1	<input type="checkbox"/>	<input type="text" value="auto"/>	<input type="text" value="Disable"/>	<input type="text" value="1"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>	<input type="text" value="auto"/>	<input type="text" value="Disable"/>	<input type="text" value="1"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
3	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	<input type="text" value="Disable"/>	<input type="text" value="1"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

Current Configuration								
Port	Link Status	Loop	Enable Port	Adaptive	Speed	Duplex	PVID	COS
1	Disconnect	No	Disable	Enable	10mbps	Half duplex	0	0
2	Disconnect	No	Disable	Enable	10mbps	Half duplex	0	0
3	Connect	No	Enable	Enable	100mbps	Full duplex	0	0

Přejdeme do jeho nastavení **Wan Configuration**.

Slave [1c:c0:e1:36:a3:67]

Global Setting

Enable Web Access

Setting Wan 1

Service Mode ▼

Connection Mode ▼ Enable VLAN VLAN ID VlanPri ▼

Port Binding LAN1 LAN2 LAN3 LAN4 SSID1 SSID2 SSID3 SSID4

Route Setting

ConnType ▼

IPv4 Address

Subnet Mask

Default Gateway

DNS Server Config ▼

DNS 1

DNS 2

Setting Wan 2

Service Mode ▼

Setting Wan 3

Service Mode ▼

Setting Wan 4

Service Mode ▼

Saving Setting

Click submit button to save the current settings to flash

Note: These configure will take effect after save setting .

Vytvoříme **Setting Wan1** tak že Service Mode z Disable přepneme na **Data**. **Connection Mode** nastavíme na **Route**.

V Port Binding zaškrtneme LAN1 a LAN2 což jsou přímo porty označené na zařízení jako "LAN1" a "LAN2". Dále zaškrtneme SSID1 což je WiFi přístup.

Conn Type nastavte na **Static IP**, v našem příkladu zadáváme 192.168.33.7 což je vnější adresa klientského routeru a pro každý byt ji musíme zadat jinou. Subnet Mask 255.255.255.0 pro všechny byty stejná. Default Gateway je IP adresa našeho nadřazeného routeru, v našem příkladu 192.168.33.1 a je pro všechny byty stejná.

Adresa klientského routeru a adresa výchozí brány musí být ve stejném IP adresním prostoru. Tyto adresy nepotřebuje uživatel znát, jde o adresy použité při vnitřní komunikaci.

Viz poznámka v úvodu k použití IP adresy z privátního rozsahu pro spojovou síť na nadřazený router.

DNS1 a DNS2 - zadejte IP adresu alespon jednoho DNS serveru.

Enable Web Access - ignorujte, omezení není funkční.

Stiskněte Apply. Nyní jsou nastavení uložena ale nejsou aktivní!

Stiskněte Saving Settings. Slave provede restart. Teprve v tuto chvíli jsou nastavení platná!

Přejdeme do nastavení **Lan Configuration**.

Slave [1c:c0:e1:36:a3:67]

IP Address

IP Address	192.168.1.1
Subnet Mask	255.255.255.0

DHCPV4 Server Setting

Enable DHCPV4 server

IP Pool Address from	192.168.1.70	to	192.168.1.90	Edit Reserved Addresses
Subnet Mask	43200			

Saving Setting

Click submit button to save the current settings to flash

Note: These configure will take effect after save setting .

Zadejte **IP adress** což je vnitřní IP adresa routeru. Pro uživatele to bude jeho výchozí brána. V příkladu 192.168.1.1. Tato IP adresa může být ve všech bytech nastavena stejně.

Subnet Mask v příkladu 255.255.255.0 a může být ve všech bytech zádána stejně.

IP Pool Adress v příkladu 192.168.1.70 až 192.168.1.90 je rozsah adres které se budou uživateli přidělovat na jeho zařízení, tj. připojené počítače a mobilní telefony.

Subnet Mask v oddíle DHCPV4 server je chybné pojmenování. Správně má být Lease Time (Seconds) a je to doba po níž je přidělené IP platné. Ponechte výchozí hodnotu 43200 sekund (tj. 12hodin).

Stiskněte Apply. Nyní jsou sice nastavení uložena ale nejsou aktivní!

Stiskněte Saving Settings. Slave provede restart. Teprve v tuto chvíli jsou nastavení platná!

Přejdeme do nastavení **WiFi Basic Configuration**

Slave [1c:c0:e1:36:a3:67]

WiFi

WiFi Enable Country: CHINA

Emissive Power: Level5 AP Number: 1

AP 1 Setting

SSID: NAZEV_WIFI_SITE

Channel: Auto Mode: Auto Hidden SSID

Security

Encryption Mode: WPA-PSK/WPA2-PSK

Key Format: Ascii

Algorithm: TKIP/AES

Key: nejake_heslo

Saving Setting

Click submit button to save the current settings to flash

Note: These configure will take effect after save setting .

Nastavíme přístupové parametry pro WiFi AP, tj. jak se budou uživatelé připojovat ze svých mobilních telefonů a notebooků bezdrátově.

Zakrtněte WiFi Enable

Emissive Power ponechte na Level5

Country ponechte na CHINA

AP Number ponechte na 1

SSID je název uživateli WiFi sítě, tj. po d jakým jménem ji naskenuje ve svém přístroji. V příkladu zadána jako NAZEV_WIFI_SITE

Channel ponechte na Auto

Mode ponechte na Auto (po celkovém uložení se objeví nastavení 11NGHT20, což je 802.11n/g/HT20)

Hidden SSID nezaškrťávejte.

Encryption Mode zvolte WPA-PSK/WPA2-PSK

Algorithm TKIP/AES

Key zadejte přístupové heslo, v příkladu napsán text nejake_heslo

Stiskněte Apply. Nyní jsou sice nastavení uložena ale nejsou aktivní!

Stiskněte Save. Slave provede restart. Teprve v tuto chvíli jsou nastavení platná!

Přejdeme do nastavení **WiFi Management**

Slave [1c:c0:e1:36:a3:67]

CLI User Setting

User

Common Password

Super Password

Web User Setting

User

Password

Saving Setting

Click submit button to save the current settings to flash

Factory Setting

Click button to restore the factory settings of the home gateway

Reboot System

Click submit button to reboot the wifi system

Note: These configure will take effect after save setting in wifi management web page.

Zde nastavujete administrační hesla k tomuto routeru.

CLI User Settings obsahuje údaj epro přihlášení do Slave routeru přes Telnet. Rozhodně heslo změňte. Zadávejte jej dvakrát do polí Common Password a Super Password (ano popisek polí je matoucí, jde jen o opakování hesla) .

Web User settings je přihlašovací jméno a heslo které zadáváte pokud se na router přihlašujete z web prohlížeče. Výchozí nastavení je jméno admin a heslo admin. Rozhodně změňte.

Stiskněte Apply. Nyní jsou sice nastavení uložena ale nejsou aktivní!

Stiskněte Saving Settings. Slave provede restart. Teprve v tuto chvíli jsou hesla platná!

Slave s routem a WiFi - pokročilé nastavení

Následující příklad je úpravou předchozího základního postupu.

Předvádí použití VLAN 802.1Q a užití PPPoE.

V příkladu využíváme porty STB1 a STB2 pro VLAN 802.1Q za účelem příjmu IPTV přenášeného přes TCP. Tyto porty tak uživateli neslouží k připojení na internet ale pouze pro připojení IPTV STB.

Přejdeme do nastavení **Slave Configuration Information**.

Porty 1. a 2. což jsou porty STB1 a STB2 povolíme.

Jejich VLAN Mode nastavíme na režim Access a vložíme že pracují na PVID 102.

Tím se automaticky přenastaví režim 3. portu, což je vnitřní router, na režim Trunk. Vložíme mu PVID 101 a to i pro povolenou síť.

Rovněž vložíme výkonové omezení pro router na 10Mbit/s pro upload a 20Mbit/s pro download.

Stiskněte Apply dole, změna nevyžaduje restart Slave zařízení.

Slave [1c:c0:e1:36:a3:67]

Template Selection

Template Application: Private Template

Template Configuration

Enable broadcast restriction:
 Enable multicast restriction:
 Enable unknow unicast restriction:
 Restriction threshold (pps):
 Enable loopback check:

Port	Enable Port	Speed&Duplex	Vlan Mode	PVID	Allowed VLAN	COS	UpLink maximum speed (0-102400)Kbps	DownLink maximum speed (0-102400)Kbps
1	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	<input type="text" value="Access"/>	<input type="text" value="102"/>		<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
2	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	<input type="text" value="Access"/>	<input type="text" value="102"/>		<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
3	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	<input type="text" value="Trunk"/>	<input type="text" value="101"/>	<input type="text" value="101"/>	<input type="text" value="0"/>	<input type="text" value="10000"/>	<input type="text" value="20000"/>

Current Configuration

Port	Link Status	Loop	Enable Port	Adaptive	Speed	Duplex	PVID	COS
1	Disconnect	No	Enable	Enable	10mbps	Half duplex	101	0
2	Disconnect	No	Enable	Enable	10mbps	Half duplex	101	0
3	Connect	No	Enable	Enable	100mbps	Full duplex	102	0

Tímto budeme na portech STB1 a STB2 přijímat komunikaci poslanou s tagem 802.1Q VLAN 102. Tj. provoz z IPTV servere který tuto službu poskytuje musíme nastavit tak aby byl správně označován s tagem 102. Samotné přijímače IPTV STB žádnou podporu pro 802.1Q nepotřebují, neboť značka je na Slavu odejmuta předtím než je IPTV STB doručena. V této pokročilé konfiguraci je třeba aby byl 802.1Q značen i provoz vůči internímu routeru který předtím značkován nebyl, musí dostat značku 101.

Poznamenejme, že router neumožňuje aby v případě užití VLAN na portech 1.,2. byl provoz vůči portu 3. neznačkován. Může se vám podařit takového nastavení docílit není však funkční.

Přejdeme do jeho nastavení **Wan Configuration**.

Jelikož jsme nyní portu 3., tj routeru, přiřadili VLAN 101 musíme tento VLAN zde v nastavení zadat k Setting Wan 1 kde máme Router aktivní. Tj. vyplníme pole VLAN ID číslem 100 a zaškrtneme políčko **Enable VLAN**.

Slave [1c:c0:e1:36:a3:67]

Global Setting

Enable Web Access

Setting Wan 1

Service Mode ▾

Connection Mode ▾ Enable VLAN VLAN ID VlanPri ▾

Port Binding LAN1 LAN2 LAN3 LAN4 SSID1 SSID2 SSID3 SSID4

Route Setting

ConnType ▾

User

password

IPV4 Address

Subnet Mask

Default Gateway

DNS Server Config ▾

DNS 1

DNS 2

Setting Wan 2

Service Mode ▾

Setting Wan 3

Service Mode ▾

Setting Wan 4

Service Mode ▾

Saving Setting

Click submit button to save the current settings to flash

Dále jsme v příkladu změnili způsob přidělení IP adresy ze statického (tj. ručně zadaného) na přidělení od PPPoE serveru.

Pro funkčnost PPPoE je nutné aby server běžel na předřazeném routeru. PPPoE přidělí routeru IP adresy a zároveň slouží jako další autorizační stupeň.

Místo PPPoE umí router ještě přidělení adresy přes DHCP.

Nastavení pro Multicasting

Pokud plánujete použití datového zdroj ve vaší v režimu UDP multicast zde je návod na jeho zprovoznění. Nejčastěji jde o multicastové vysílání IPTV.

Multicast přináší při užití v EoC mírnou výkonovou výhodu oproti TCP v celkové velikosti pásma, viz. kapitola Download - TCP a Multicast

! Pokud o ničem takovém ve svém síti nevíte ponechte výchozí nastavení a odstavec Multicasting se vás netýká !

! Pokud chcete distribuovat multicast nemusí být nutně na vstupu značkován VLAN 802.1Q. Dále v popisu rozlišujeme dle toho nastavení Master a Slave zařízení !

Následující příklad je proveden pro XL-PB360C, tj. zařízení bez routeru.

V případě použití pro XL-PB360CA je nastavení stejné ale bude se týkat jen portu 1. a 2. které jsou na jednotce označeny jako STB1 a STB2.

IGMP aktivace na Masteru

Základním požadavkem pro Multicast je aktivace IGMP:

Naleznete jej v menu **NETWORK - IGMP**

v EoC Master jednotce je software starající se o IGMP komunikaci. Její komunikaci můžete detekovat jako IGMP zprávy vysílaná z IP adresy 192.168.2.2, což je IP adresa navázaná na Gigabitové rozhraní Masteru.

Tyto zprávy se rozepisují v intervalu "Query Interval" a fungují jako dotaz pro připojená zařízení přijímající multicast ve smyslu "stále ještě tento kanál posloucháš?". Pokud zařízení neodpoví je automaticky z kanálu vyřazeno. Poznamenejme že toto nemá vliv na to jak rychle se zařízení k multicasu připojí ale za jakou dobu od jeho přechodu na jiný zdroj je toto zjištěno pokud sám takové hlášení IGMP nedává. Je důležité upozornit že přijímačem Multicastu nemusí být jen STB zapojené do Slave zařízení ale může jím být i připojený počítač. Tj. nemusí být zaručeno že pracuje s IGMP správně a proto Query Interval zajistí jeho odpojení z kanálu po nastavené době. Tím se především uvolní přenosové pásmo systému celkově.

Query Interval - pro účely ladění nastavte na minimum 10s tak aby se případná chyba projevila co nejrychleji, pokud vaše zařízení / software nedostává z nějakého důvodu IGMP zprávy projeví se to ztrátou jeho spojení právě do cca. 10s od doby přepnutí na kanál. Například pokud jste si například zablokovali IGMP do jiného VLANu než jste povolili dopravit k přijímači uvidíte to po 10s od posledního přepnutí na TV kanál. Pro provozní režim nejčastěji hodnota kolem 120s je vyhovující.

Igmp Vlan - jde o ID VLAN sítě po níž chcete aby IGMP zprávy byli posílány. Číslo tohoto VLANu je třeba následně zadat id o Slave zařízení tak abyste umožnili koncovým zařízením komunikaci přes IGMP. Nápis **Refresh** v řádce Igmp Vlan je chyba popisu - správně má být **Enable VLAN**. Proto pokud chcete IGMP posílat po VLAN 802.1Q je nutné toto zaškrtnout. Naopak pokud nebudete VLAN pro multicast používat, nezaškrťávejte.

Network Filter na Masteru

Dalším menu týkajícím se Multicastu je omezovač pásma pro příchozí provoz.

Naleznete jej v menu **NETWORK - Filter**

The screenshot shows two sections of a configuration interface. The first section, 'Broadcast limiting', has a blue header. It contains two rows: 'Broadcast limiting enabled:' with an unchecked checkbox, and 'Broadcast limit threshold:' with a text input field containing '1' and a label '% (1-100%)'. Below these is a 'Submit' button. The second section, 'Multicast limiting', also has a blue header. It contains two rows: 'Multicast limiting enabled:' with an unchecked checkbox, and 'Multicast limit threshold:' with a text input field containing '10' and a label '% (1-100%)'. Below these is another 'Submit' button.

Zde vás bude zajímat jen volba pro **Multicast limiting**.

Dovoluje omezit příchozí Multicastové provozy a slouží jako bezpečnostní pojistka.

Oproti popisu není rozsah zadání 1-100 ale ve skutečnosti 1-10. Tj. při zadání 2 se limituje příchozí provoz na cca. 20% maxima.

Testy ukázali, že pokud je příchozí stream jen jeden budete na STB posílat při zadání 2 bezchybně stream o velikosti max. 18Mbit/s.

Jakmile však je na vstupu více multicastových streamu je tato hodnota vůči celkovému součtu redukována výrazněji a nelze přesněji definovat.

Doporučujeme se o limitaci příchozího provozu postarat na jiných prvcích. Proto ponechte funkci Filter neaktivovánu, tj. políčko **Multicast limiting enabled** **nezaškrťávat**.

VLAN Mode Slave zařízení

Nyní je třeba nastavit pracovní režim pro koncové klienty.

K jednotlivým klientům se dostanete prostřednictvím menu **SLAVE - Online**

Online Slaves Number: 6									
ID	Slave MAC	Wifi MAC	User information	Attenuation(dB)	Upstream SNR(dB)	Downstream SNR(dB)	Upstream Speed(Mbps)	Downstream Speed(Mbps)	Operation
1	1c:c0:e1:36:a3:4d	None	XL-PB360C Node B2	44	31.48	31.08	340	337	Reboot
2	1c:c0:e1:36:a3:45	None	XL-PB360C Node B3	44	31.46	31.18	340	338	Reboot
3	1c:c0:e1:36:a3:5f	1c:c0:e1:36:a3:61	XL-PB360CA Node B4	44	27.55	30.55	308	333	Reboot
4	1c:c0:e1:36:a3:57	1c:c0:e1:36:a3:59	XL-PB360CA Node B5	44	31.09	30.32	337	331	Reboot
5	1c:c0:e1:36:a3:3f	None	XL-PB360C Node B6	46	26.73	29.59	302	325	Reboot
6	1c:c0:e1:36:a3:67	1c:c0:e1:36:a3:69	XL-PB360CA Node B7	44	30.65	30.26	333	330	Reboot

Reboot All Online Slaves Refresh

Vyberte jeho MAC adresu a následně zvolte v horní liště **Slave Configuration Information**

Pro počáteční konfiguraci sítě doporučujeme vypnout volby omezující vysílání Multicastu, Broadcastu i Unicastu. Nebudou vás omezovat z hlediska limitů na počet paketů za sekund (pps). Volba Enable loopback check může být zapnutá, nesouvisí nijak s multicastem.

VLAN Mode Disabled

Pokud multicast vstupující do Masteru není značkován 802.1Q tak nepotřebujete aktivovat VLAN 802.1Q nad porty Slave, ponechte je v režimu **Disabled**.

VLAN mode Access

Pokud stream je VLAN 802.1Q značkován je třeba aby ve shodě byli nastaveny i Slave zařízení. Nejčastějším nastavení Slave zařízení je nechat **VLAN Mode** v režimu **Access**. Níže na příkladu je nastavena na 1. portu VLAN síť s identifikátorem 101. Jakmile takovou komunikaci přijme, odstraní z ní 802.1Q tag a dále posílá z Slave zařízení přes LAN1 již netagovaný provoz (tj. normální, neobsahující 802.1Q)

Příklad níže tedy bude přijímat multicastový provoz jež zasíláme do Masteru s VLAN identifikátorem 101 pouze pokud zapojíte případné IPTV STB do portu LAN1. Na samotném IPTV STB již žádný VLAN 802.1Q nenastavujte.

VLAN 101 v tomto případě musí mít i IGMP provoz, viz předchozí nastavení NETWORK-IGMP.

Slave [1c:c0:e1:36:a3:4d]

Template Selection

Template Application: Private Template

Template Configuration

Enable broadcast restriction: Enable multicast restriction: Enable unknow unicast restriction:

Restriction threshold (pps):

Enable loopback check:

Port	Enable Port	Speed&Duplex	Vlan Mode	PVID	Allowed VLAN	COS	UpLink maximum speed (0-102400)Kbps	DownLink maximum speed (0-102400)Kbps
1	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	<input type="text" value="Access"/>	<input type="text" value="101"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
2	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	<input type="text" value="Access"/>	<input type="text" value="1"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
3	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	<input type="text" value="Access"/>	<input type="text" value="1"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
4	<input checked="" type="checkbox"/>	<input type="text" value="auto"/>	<input type="text" value="Access"/>	<input type="text" value="1"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

Current Configuration

Port	Link Status	Loop	Enable Port	Adaptive	Speed	Duplex	PVID	COS
1	Connect	No	Enable	Enable	100mbps	Full duplex	101	0
2	Disconnect	No	Enable	Enable	10mbps	Half duplex	1	0
3	Disconnect	No	Enable	Enable	10mbps	Half duplex	1	0
4	Disconnect	No	Enable	Enable	10mbps	Half duplex	1	0

VLAN mode Trunk

Druhou, vyjimečně používanou možností, je provozovat port v režimu Trunk. Ten použijete tehdy pokud chcete aby přijatý multicastový provoz pokračoval ze Slave zařízení dále do sítě s VLAN 802.1Q tagem. V opačném směru je nutné abyste povolili v poli "Allowed VLAN" pro ty sítě které mají komunikovat v opačném směru. A jelikož jsme v příkladu dali aby IGMP komunikovalo také ve VLAN 101 potřebujeme aby naše odpovědi IGMP procházeli s tímto tagem. Nezapomeňte že v této konfiguraci musí rovněž komunikující zařízení dávat do paketu značku VLAN 802.1Q značku, v našem příkladu 101.

Slave [1c:c0:e1:36:a3:4d]

Template Selection

Template Application: Private Template

Template Configuration

Enable broadcast restriction: Enable multicast restriction: Enable unknown unicast restriction:
 Restriction threshold (pps):
 Enable loopback check:

Port	Enable Port	Speed&Duplex	Vlan Mode	PVID	Allowed VLAN	COS	UpLink maximum speed (0-102400)Kbps	DownLink maximum speed (0-102400)Kbps
1	<input checked="" type="checkbox"/>	auto	Trunk	101	1,101	0	0	0
2	<input checked="" type="checkbox"/>	auto	Access	1		0	0	0
3	<input checked="" type="checkbox"/>	auto	Access	1		0	0	0
4	<input checked="" type="checkbox"/>	auto	Access	1		0	0	0

Current Configuration

Port	Link Status	Loop	Enable Port	Adaptive	Speed	Duplex	PVID	COS
1	Connect	No	Enable	Enable	100mbps	Full duplex	101	0
2	Disconnect	No	Enable	Enable	10mbps	Half duplex	1	0
3	Disconnect	No	Enable	Enable	10mbps	Half duplex	1	0
4	Disconnect	No	Enable	Enable	10mbps	Half duplex	1	0

Poznámka k VLAN vs. IGMP

Jak jste si všimli v našem příkladu je IGMP ve stejné VLAN jako vlastní multicast, To je nečastější a praktické nastavení.

Pokud však z nějakého důvodu potřebujete mít IGMP s jinou VLAN, případně multicastové streamy rozdělit nejen dle jejich IP ale i dle VLANu mějte na paměti že vždy musí k a od koncového zařízení projít IGMP zprávy. Pokud neprocházejí budou se vám zařízení od multicastové skupiny "odhlašovat" po vypršení nastavené doby dotazu IGMP.

Propojení oddělené komunikace MDU

Zde popisovaný EoC přenosový systém je **záměrně** navržen pro **oddělení** vzájemné komunikace mezi uživateli. V tomto systému je veškerá komunikace ze Slave jednotky vedena přes Master jednotku a komunikace mezi Slave jednotkami vůbec neprobíhá. To znamená, že uživatel jednoho zavírovaného počítače nemůže žádným způsobem ohrozit jiného uživatele ve stejném kabelovém segmentu sítě který používá jiné, byť identické, Slave zařízení. Tento systém se nazývá také MDU - Multiple Dwelling Units

Nicméně pokud je potřeba aby systém byl používán také pro komunikaci mezi jednotlivými Slave zařízeními lze toto omezení obejít pomocí centrálního routeru. Tj. toho routeru který máte zapojen mezi Master jednotku a přípojku do internetu. Případně tento router leží na vzdálenějším uzlu který spojuje více budov dohromady před jejich napojením do internetové přípojky.

Na router nebo spravovaným přepínači vám pro podporu této funkce stačí zapnout funkčnost nazývanou lokální ARP Proxy, a to takovou aby dokázala odpovědět do stejného rozhraní z jakého ARP dotaz přišel.

Přenos dat pak funguje tak, že pakety které mají z jednoho Slave zařízení dosáhnout druhý Slave zařízení jsou routována na tomto centrálním routeru přes STEJNÉ rozhraní. Tj. jsou přijmuty z Masteru a do Masteru opět poslány, samozřejmě s jinou cílovou adresou.

Jaké jsou možnosti řešení:

a) Pokud routujete síť na spravovatelném přepínači podívejte se v něm po funkci "ARP Local Proxy", "local proxy-arp" apod. Funkci mají přepínače které pracující na 3. vrstvě OSI (tzv. Layer 3), poznáte je dle toho že jste na nich konfigurovali RIP, OSPF.

b) Pokud je vašim routerem zařízení s OS Mikrotik hledejte aktivaci této funkčnosti pod termínem "local-proxy-arp". V návodu systému plně popsáno.

c) V případě Linux routerů jde o funkčnost nazývanou "Private VLAN proxy ARP". Uvádíme způsob povolení její funkčnosti pro patřičné rozhraní, zde příklad pro eth1:

```
echo 1 > /proc/sys/net/ipv4/conf/eth1/proxy_arp_pvlan
```

nebo

```
sysctl -w net.ipv4.conf.eth1.proxy_arp_pvlan=1
```

Funkce je aktivní okamžitě, není třeba restart apod.

Tato funkčnost je podporována již od kernelu 2.6.34 a neměli byste tedy mít žádný problém ji aktivovat v současném jádře. Pro její funkci nejsou jakákoliv nastavení VLAN (802.1Q) potřeba i když je pro jejich podporu navržena. Poznamenáváme že nejde o původní "Proxy ARP" který je v Linuxu velmi dlouho, bohužel však není této funkčnosti schopen.

A pokud jako Linux "Private VLAN proxy ARP" chcete použít stoj který jinak jako router neslouží nezapomeňte že:

- je nutné aktivovat IP forwarding:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

- je nutné aby na rozhraní nad nímž aktivujete tuto funkčnost byla nastavena IP adresa ze stejného rozsahu jako jsou IP adresy mezi nimiž má probíhat komunikace (pokud je zařízení routerem pravděpodobně ji tam již máte a jde o výchozí IP bránu pro Slave zařízení). Ověříte snadno tak že jste schopni dostat odpověď na ICMP (ping) poslanou z routeru.