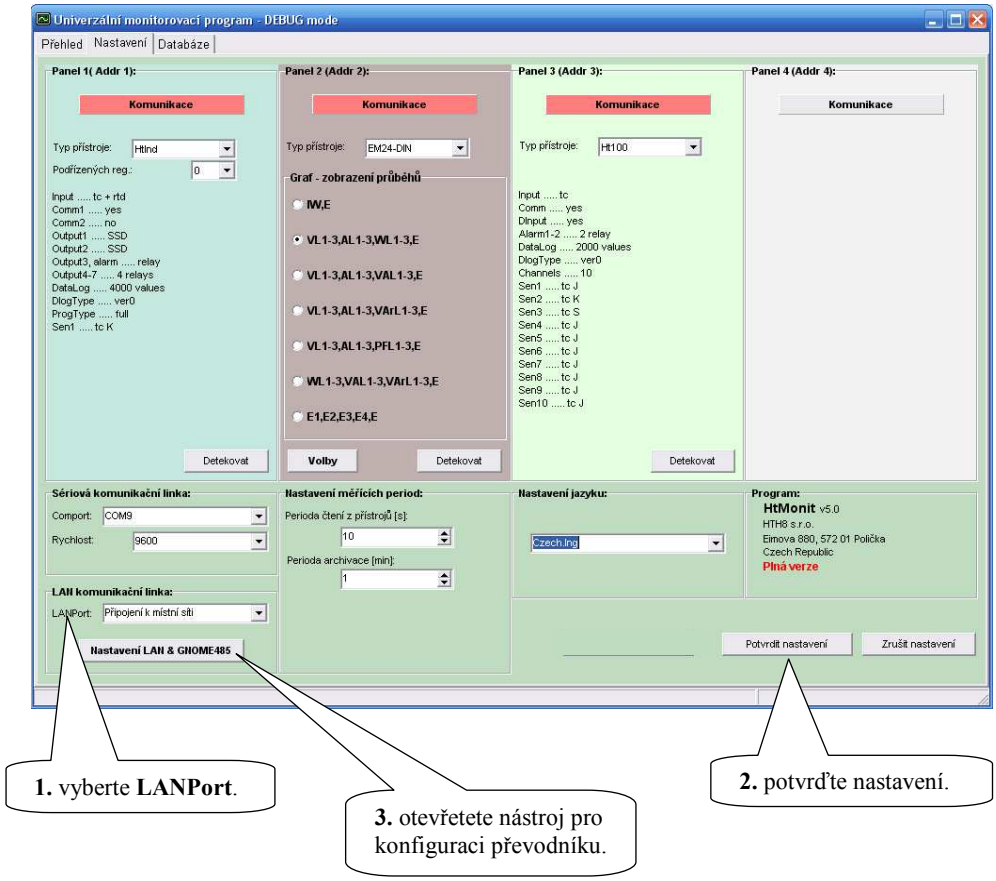
Propojení HtMonit s přístroji pomocí LAN

Pro datovou komunikaci mezi přístroji může být použit internet jako přenosové médium. Tato komunikace je umožněna u přístrojů osazených komunikační linkou **EIA485** a přídavným převodníkem **GNOME485** nebo u přístrojů osazených komunikačním rozhraním **ETHERNET**. Pro zprovoznění komunikace je vyžadována základní znalost konkrétního síťového propojení v místě provozovatele s možností konfigurace.

Postup zprovoznění komunikace

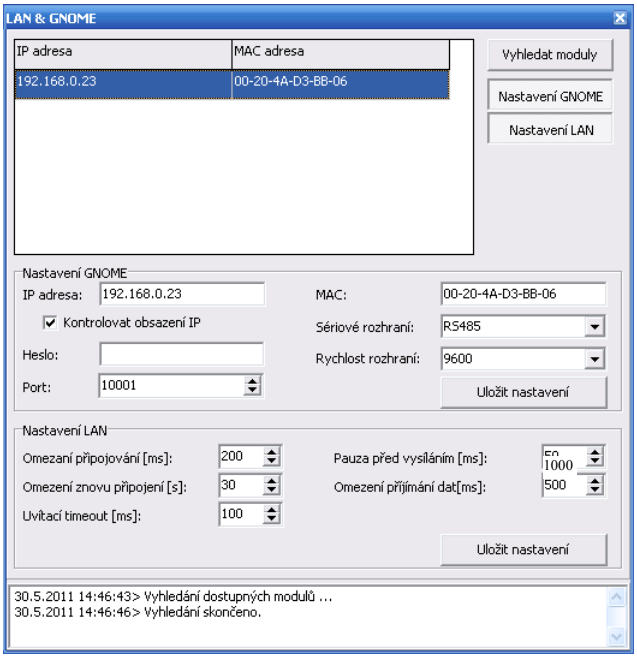
Zprovoznění komunikace se liší podle způsobu jejího provozování tj. snímání v lokální síti nebo zpřístupnění přístroje do internetu (přes směrovací prvek).

1. Správce sítě musí přidělit pevnou IP adresu a komunikační port koncového zařízení (GNOME, přistroj s ETHERNET modulem).
2. Pokud je v komunikační trase **Firewall**, nastavit průchodnost dat komunikace pro parametry získané v bodě 1 a pro konfiguraci převodníku GNOME povolit komunikaci na portech **1**, **9999**, **30718**.
3. Pokud je zpřístupňováno zařízení uvnitř sítě pro přístup z vnějšku, musí být nastaveno přesměrování portů do vnitřní sítě.
4. Musí být konfigurováno koncové zařízení dle parametrů získaných z bodu 1. K tomu je možné použít nástroj přístupný v HtMonit. Spusťte HtMonit a zvolte modul nastavení, viz obrázek.

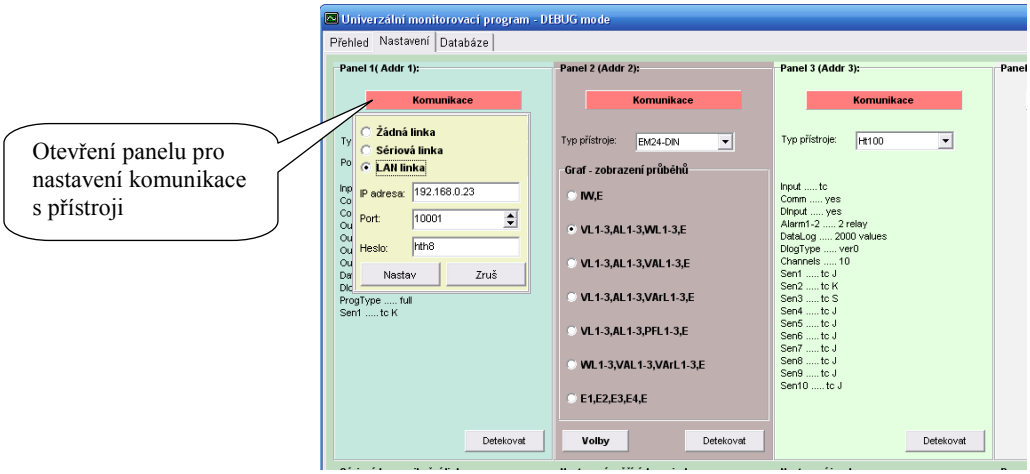


5. Vyberte **LANPort** v nastavení „LAN komunikační linka“ dle rozhraní, které používá PC k přístupu do sítě (nabídku rozbalte a vyberte).
6. Nastavení potvrďte tlačítkem „Potvrdit nastavení“.

7. Tlačítkem „Nastaveni LAN & GNOME485“ spusťte nástroj pro konfigurace převodníku, viz obrázek.



8. Stiskem tlačítka „Nastavení GNOME“ zpřístupníte zadání parametrů převodníku.
9. Zadejte MAC adresu uvedenou na převodníku GNOME, přidělenou IP adresu a číslo portu od správce, viz bod 1., případně heslo pro přístup k převodníku. Zvolte typ výstupního rozhraní (RS485) a komunikační rychlost (9600). Stiskem „Uložit nastavení“ provedete zápis nastavení do převodníku.
10. Potvrzení správného zápisu je indikováno ve spodní části okna sdělením „Nastavení modulu je dokončeno“. Tím je konfigurace převodníku ukončena. Okno uzavřete.
11. Nastavte komunikaci s přístroji otevřením panelu komunikace pomocí tlačítka „Komunikace“ v horní části obrazovky nastavení.

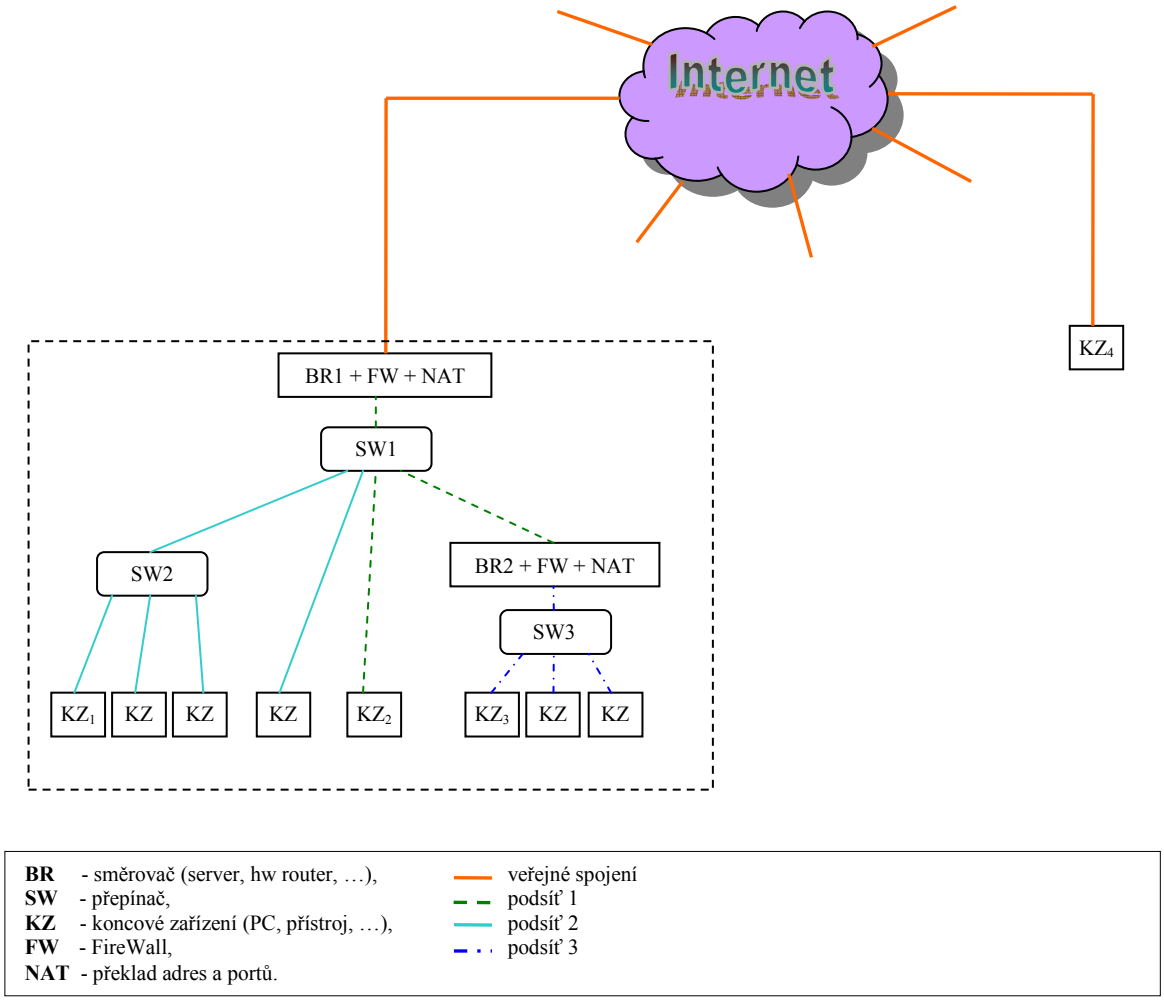


12. Zadejte parametry získané v bodě 1. a potvrďte je tlačítkem „Nastav“.
13. Je-li požadováno, proveďte nastavení i pro ostatní panely programu.
14. Nyní je konfigurace komunikace s přístroji ukončena.
15. Můžete provést detekci přístrojů.

Pro objasnění pojmů ohledně nastavení komunikace přístrojů pomocí internetu následuje kapitola se základním popisem této komunikace.

Základní pojmy

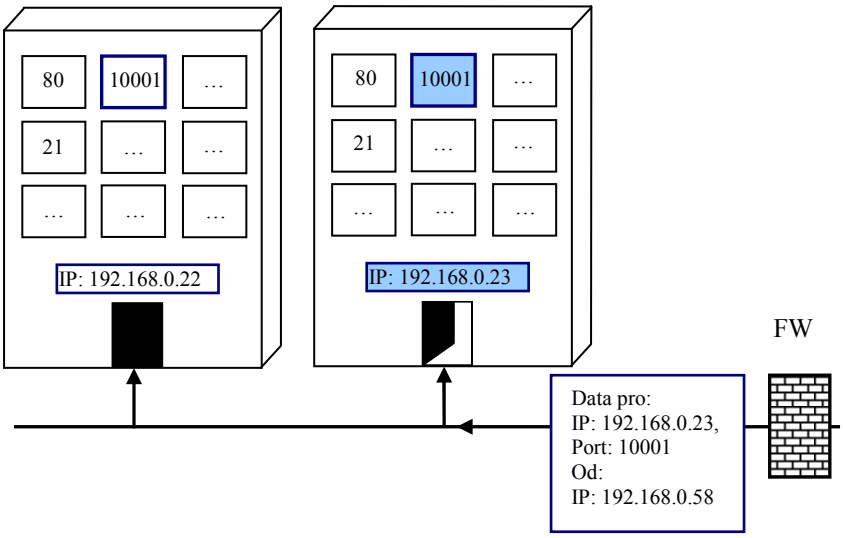
Propojení všech komunikačních zařízení v rámci internetu, firemních nebo domácích sítí, je řešeno pomocí strukturování sítě (vzájemné propojení všech zařízení není prakticky možné). Pro toto strukturování jsou používány síťové prvky (směrovače, přepínače, rozbočovače, …), které zajišťují přenos dat v síti. Náznak případné struktury sítě s vysvětlením pojmu je uveden na obrázku níže.



Obr. 1. Příklad topologie sítě.

Každé zařízení připojené k internetu musí být určeno pomocí jedinečného identifikačního prvku, kterým je **IP** adresa. Do internetu mohou být připojena zařízení přímo nebo pomocí **směrovačů**, které zajišťuje překlad adres. Za směrovačem může být použita prakticky libovolná struktura s velikým počtem koncových zařízení (lokální síť). Z pohledu internetu je tato struktura skryta a jeví se pouze jako jedno zařízení. Lokální síť může být dále členěna na různé skupiny, buď fyzicky pomocí dalších směrovačů, nebo logicky pomocí skupiny adres definovaných maskou sítě. Tuto skupinu nazýváme podsíť.

Pokud je požadována komunikace mezi dvěma koncovými zařízeními, je tato komunikace určena zdrojovou IP a cílovou IP adresou. Obě zařízení si mohou vyměňovat velké množství různých informací, proto je jedno fyzické spojení rozděleno do mnoha virtuálních spojení. To se následně jeví, jako kdyby mezi oběma zařízeními bylo velké množství samostatných spojení. Každá tato virtuální linka (port) je označena vlastním číslem tj. **číslem portu**. Pokud se tedy během přenosu soustředíme na přenos jednoho druhu specifické informace (komunikace s přístrojem) je tato komunikace definovaná pomocí **IP adresy zdroje, IP adresy cíle a čísla portu**. Příjem dat na koncové zařízení vystihuje následující obrázek.



IP adresa = číslo domu, číslo portu = číslo bytu

Obr. 2. Příjem dat koncovým zařízením.

Přenos dat a funkce síťových prvků bude vysvětlena na dvou příkladech, kde topologie sítě je uvedena na Obr. 1:

Příklad 1. Komunikace mezi zařízeními KZ_1 a KZ_2. První zmíněné zařízení vyšle data do SW2, který předá data do SW1. SW1 postoupí data dále. BR1 zjistí z příchozích dat, že cílová IP adresa je uvnitř sítě, proto data nepostoupí do internetu. SW1 doručí data do KZ_2. Při posílání odpovědi z KZ_2 nazpět putují data do SW1 a postoupí data do SW2 a ten do KZ_1. Je-li uvnitř sítě síťový prvek omezující komunikaci (FireWall), musí být tento prvek nastaven tak, aby umožňoval průchod požadovaných dat.

Příklad 2. Komunikace mezi zařízeními KZ_1 a KZ_4. Data od KZ_1 postupují obdobně jako v předchozím případu až na SW1. Zde jsou předána BR1, který zjistí cílovou adresu vně interní sítě. Zaznamená si adresu zdrojového KZ_1 a cílového KZ_4 a v datech zamění zdrojovou adresu z KZ_1 na svoji adresu BR1. Takto upravená data postoupí do internetu. KZ_4 data příjme a při odpovědi jsou data odeslána na adresu BR1. Směrovač data příjme a zjistí zdrojovou adresu odpovědi KZ_4 a na základě uložené informace odešle odpověď na adresu KZ_1.

Pokud je komunikace iniciována z opačné strany, tedy od KZ_4 na KZ_1, je situace obtížnější. Do cílové adresy nemůže být uvedena adresa KZ_1 přímo (není veřejná), ale musí zde být uvedena adresa vstupní brány BR1. Po obdržení dat BR1 neví kam má data dále postoupit. Pro tyto účely musí být na vstupní bráně použit NAT, který zajistí přesměrování portů. Definicí zadáme směrování, např. portu číslo 10000, na vnitřní adresu odpovídají adrese KZ_1. Pak pro poslání dat z KZ_4 do KZ_1 musí být použita adresa BR1 a komunikační port 10000.

V komunikační trase může být použit filtrovací prvek (FireWall), které může omezit komunikaci. Pokud dojde na vstup **FW** komunikace s nepovolenou IP adresou nebo číslem portu, nejsou data propuštěna dále. Prvky musí být konfigurovány tak, aby neblokovali požadovanou komunikaci.