- Účel rozlehlých sítí (WAN) je propojit vzdálené lokality nebo sítě, které jsou geograficky vzdálené od sebe. WAN se používají pro komunikaci mezi různými pobočkami jedné organizace nebo pro propojení různých organizací, které potřebují sdílet data a zdroje.
- Komunikace v rámci rozlehlých sítí (WAN) probíhá přes veřejné sítě, jako je Internet, a využívá různé síťové protokoly a technologie, jako jsou MPLS (Multiprotocol Label Switching), Frame Relay, ATM (Asynchronous Transfer Mode) nebo Ethernet.

Běžné možnosti připojení k WAN a Internetu zahrnují:

- Dedikované linky: Jsou to fyzické spojení mezi dvěma místy, která jsou výhradně vyhrazena pro přenos dat mezi nimi. Příklady zahrnují T1 nebo E1 linky, optické vlákno nebo mikrovlnné spoje.
- MPLS (Multiprotocol Label Switching): Je technologie, která využívá síťových uzlů zvaných MPLS přepínače pro přenos dat mezi různými lokalitami. MPLS je často používán pro propojení poboček v rámci jedné organizace.
- Internetové připojení: Používá veřejnou síť Internetu pro přenos dat mezi různými místy. Internetové připojení je obvykle levnější, ale může mít nižší záruky výkonu a bezpečnosti než dedikované linky nebo MPLS.

Hierarchie poskytovatelů připojení k Internetu (ISP) zahrnuje několik úrovní:

- Tier 1 ISP: Jsou to největší a nejvýkonnější ISP, které mají globální dosah a nezávislé připojení k celému Internetu. Tier 1 ISP jsou propojeni mezi sebou a nepotřebují peeringové smlouvy s ostatními ISP.
- Tier 2 ISP: Jsou menší než Tier 1 ISP a mohou mít regionální nebo národní pokrytí. Tier 2 ISP se propojují s Tier 1 ISP nebo s jinými Tier 2 ISP pomocí peeringových smluv nebo nákupem přístupu k Internetu od Tier 1 ISP.
- Tier 3 ISP: Jsou nejmenší ISP, kteří poskytují přístup k Internetu pouze v určitých lokalitách nebo regionech. Tier 3 ISP mohou nakupovat přístup k Internetu od Tier 1 nebo Tier 2 ISP.

Přínosy virtuálních privátních s ítí (VPN) zahrnují:

- Bezpečnost: VPN umožňují šifrování dat, která se přenášejí mezi síťmi, což zajišťuje vyšší úroveň ochrany dat a soukromí. To je zvláště důležité pro komunikaci přes veřejné sítě, jako je Internet, kde mohou být data vystavena riziku odposlechu nebo útokům.
- Soukromí: VPN umožňují organizacím vytvořit soukromou síť na veřejném Internetu, což umožňuje výměnu dat mezi různými lokalitami nebo pobočkami organizace bez nutnosti sdílet data s veřejnou sítí.
- Propojení vzdálených lokalit: VPN umožňují propojení vzdálených lokalit nebo poboček organizace, což umožňuje efektivnější komunikaci, spolupráci a sdílení dat.
- Snadná správa: VPN poskytují centralizovanou správu a kontrolu nad přístupem do sítě, což usnadňuje správu sítě a zajišťuje dodržování bezpečnostních politik.

Existují různé typy virtuálních privátních sítí (VPN), včetně:

- Site-to-Site VPN: Také nazývané jako LAN-to-LAN VPN, umožňují propojení dvou nebo více sítí na různých místech, jako jsou pobočky organizace, přes veřejný Internet. Data jsou šifrována a přenášena mezi sítěmi, což umožňuje bezpečnou komunikaci mezi vzdálenými lokalitami.
- Remote Access VPN: Umožňují individuálním uživatelům nebo vzdáleným zařízením, jako jsou mobilní telefony nebo notebooky, přístup do interní sítě organizace přes veřejný Internet. Uživatelé se obvykle autentizují a připojují pomocí VPN klienta, který vytváří šifrované spojení do interní sítě.

- Extranet VPN: Umožňují organizacím vytvářet bezpečné spojení s externími partnery, dodavateli nebo zákazníky, aby mohly sdílet určitá data nebo zdroje.
- Cloud VPN: Umožňují organizacím vytvářet propojení mezi interní sítí a cloudovými službami nebo poskytovateli cloudových služeb, což umožňuje bezpečný přístup k datům nebo aplikcím v cloudovém prostředí.
- Přínosy virtuálních privátních sítí (VPN) zahrnují zvýšenou bezpečnost a soukromí dat, možnost propojení vzdálených lokalit, snadnou správu a centralizovanou kontrolu, a možnost propojení s externími partnery nebo cloudovými službami. VPN umožňují organizacím rozšířit svou síťovou infrastrukturu a poskytovat bezpečný a soukromý přístup k interním zdrojům a službám.
- Nicméně, mezi nevýhody VPN patří potenciálně nižší rychlost spojení kvůli šifrování dat, vyšší nároky na konfiguraci a správu, a náklady na implementaci a provoz. Některé VPN také mohou vyžadovat speciální hardwarovou nebo softwarovou podporu.
- Celkově lze říci, že VPN jsou užitečným nástrojem pro organizace, které potřebují zabezpečený a soukromý přístup k interním zdrojům a službám přes veřejné sítě, jako je Internet, a umožňují efektivní komunikaci mezi vzdálenými lokalitami nebo externími partnery.