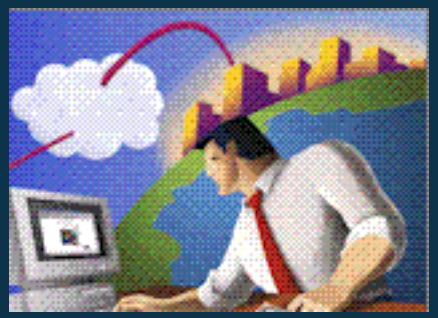


Virtual Private Networks

By Dmitry Drinfeld

What is a Virtual Private Network

Main objective of a virtual private network is to seamlessly emulate the experience of being a part of a certain LAN.

- Virtual - while the VPN emulates LAN experience, in reality it is running on a public medium.
- Private - the main concern of private LANs, the implied confidentiality of the communication, has to be present with VPNs
- Network is self explanatory...

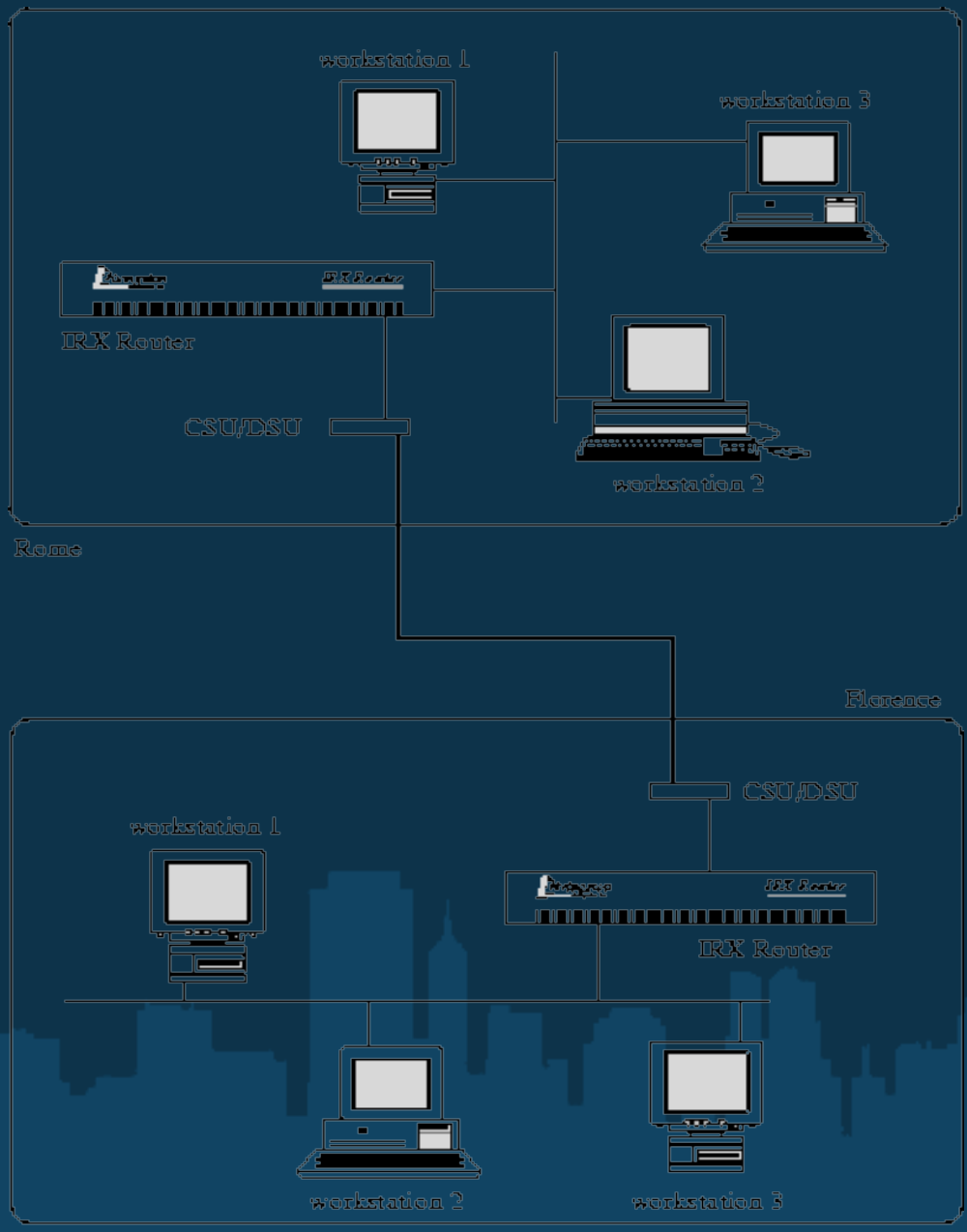
Is there an alternative to VPN?

In order to provide LAN access remotely a company might use:

Dedicated or leased lines that are physically exclusive to the company.

Companies could construct their own dedicated lines or lease such lines from an ISP.

This was the predecessor solution of VPN...



A bit of history

When the internet was not yet well developed, no practical alternative to leased lines existed.

- Most communications were still wired
- Remote access was not essential and was a privilege of geographically separated offices within large organizations
- Need for telecommunications relatively was small, certainly not encompassing individuals
- Agents of communications were stationary

Shift towards mobile

But as time passed and industry developed, needs for telecommunication developed as well:

- Smaller companies require secure remote connections
- Need for individual telecommunications grows
- Roaming user support
- Telecommunications over greater distances

But how did it fit the existing solution???

Leased lines - elitist, marginal solution.

Badly...

While leased lines address most of the user needs, there are a few issues that prevent it from being future proof:

- Extreme difficulty of scaling
- Very high costs
- Lack of support for individual telecommuters
- No support for roaming users
- Inability of full scale reuse of existing infrastructure

Such infrastructure dependent solution was not acceptable for the new conditions.

Why VPN?

In the today's world, communication networks issues, such as the following, have to be addressed, and leased lines did not address some few of them:

- Minimal infrastructure dependence (was not addressed)
- Reliability
- Security
- Ease of use
- Mobility (was not addressed)
- Scalability (was not addressed)
- Cost effectiveness (was not addressed)

However! VPN provides solution for all of these issues!

Features

VPN still requires internet infrastructure to be in place, however, since internet is so ubiquitous in today's world, and no special types of links are required - it can be said that VPN infrastructure dependence is reduced to a bare minimum.

Reliability of the VPN is guaranteed by the use of proper routing mechanisms to navigate VPN traffic through the hectic and chaotic medium of internet.

Security, arguably the most improtant part of the VPN communication, is guaranteed by multiple means! Confidentiality, integrity and authentication are provided in the following ways...

Security

Confidentiality of the communication is provided by the use of ciphers such as 3DES and AES in order to encrypt the sensitive contents of the messages. If the messages are intercepted - the contents are encoded, and great effort is required in order to decode them, without knowledge of the secret key.

Integrity of the messages is preserved by appending a calculated hashed value of the contents to them. When reciever gets the message, he calculates his own hash value, and if it does not match the appended hash - the message has been subjected to error or tempering and is discarded.

Security (continued)

Authenticity is provided by the peer to peer authentication mechanisms, such as user token, digital certificate, and various physical types of authentication.

Features (continued)

Full mobility of the user is allowed by the use of the dynamic IPs and the absence of necessary physical links between the endpoints of the communication. Essential, only generic Internet Connection is needed to conduct VPN communication.

As no dedicated links required, scaling the solution only requires installation of appropriate hardware and software on the endpoints of communication. The medium is not affected and does not require any additional conditioning.

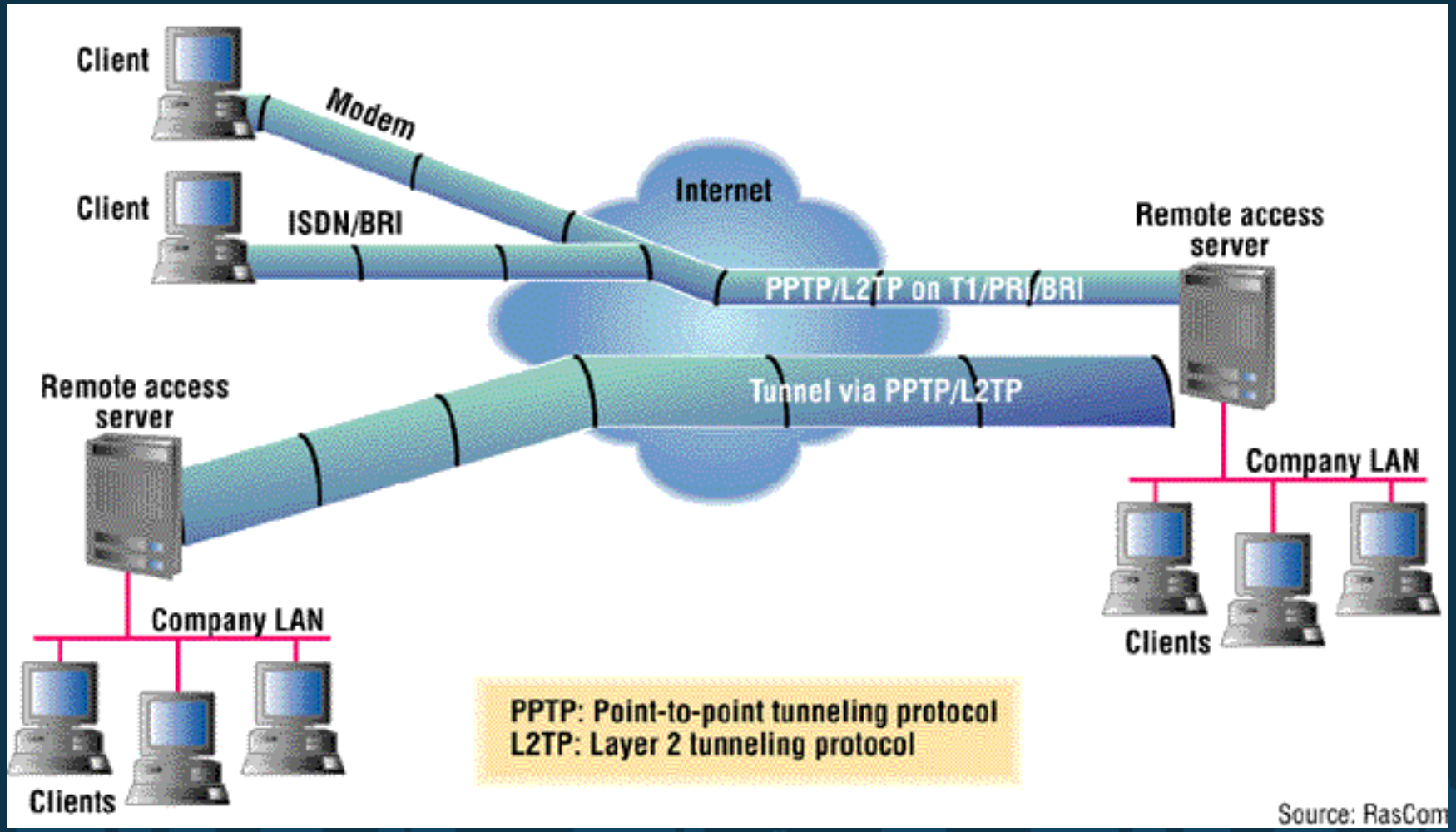
And of course, VPN solution is very cost effective comparing to the leased lines, as no construction or lease of transmission medium is required.

Conceptual Basis - tunneling

Tunneling lies at the very core of the modern VPN systems.

- Additional header is added at the source, original packet is essentially the payload
- Public network is unaware of the true type of the packet and its contents
- Server strips tunneling header and forwards the original packet to the destination within remaining safe part of the network (i.e. the target LAN)
- User and server remain unaware of intermediate complexities of the network
- Supports NAT

Tunneling (continued)



Types of VPN connections

- Remote user to office (site)
- Office to office
- User to special LAN within the company network

This addresses the most required applications of secure remote communications...

FIN

Thank you ! :)

Any questions ?
Shoot!