

Background Article

Different roads lead to Rome

Intelligent traffic planning: Why traffic intelligence must always encompass tunnel switching

A whole range of developments pose new IT challenges for enterprises with branch office structures: Policy requirements, security concepts and backup strategies all speak in favour of centralising server systems in dedicated data centres. After all, this approach results in cost savings for hardware and personnel in the branch offices. But at the same time, distributed branch offices should increasingly become more closely involved in the worldwide business processes. The remote locations require direct, smooth access to web-based applications here. This means a tremendous increase in terms of bandwidth availability and internet connections. High availability is no longer just a question of internal structures. CIOs and those responsible for infrastructure must now also guarantee the productivity of branch offices with highly available, fast and secured communication lines and extend the concept of high availability to areas over which they initially have no control.

Distribute WAN resources depending on the business requirements

Most application protocols have been developed for LAN usage. This area is dominated by poor response times – also referred to as latency – and large bandwidths. If the client and server are connected via a WAN line then the response time often climbs by a factor of between 10 and 100. Bandwidth in a WAN is both expensive and scarce. So one of the major challenges facing many organisations is to ensure short response times for business critical applications and to distribute the WAN resources according to the business requirements.

To optimise connectivity today, the VPN and gateway manufacturers provide diverse combined technologies:

- Loss-free data compression, such as stateless packet-based compression and, more effective, stream compression for TCP-based protocols to increase the effective bandwidths
- Caching, for example for intra-web-access via HTTP or DNS queries to reduce latency effects
- DNS slave servers integrated into the gateways that optimise name resolution queries and thus allow latencies without study times
- Application protocol optimisations, for example wide area file services – WAFS – for faster file access on network drives
- TCP protocol optimisations, to balance out protocol weaknesses with more robust and proprietary alternatives.
- Advance file distribution to data memory which are integrated into the branch office gateways.
- Reduction of transferred data volumes by filtering out undesired and unnecessary parts, like broadcasts.
- Bandwidth management (prioritisation based on applications, data characteristics or by other business requirements).

Crows build nests from cable sheathing

Nobody will argue that WAN optimisation is very important, but it is only part of the answer to the challenges described. What happens for example, if there is a power cut? What happens if the provider configures incorrectly or if lines are cut through during construction work? Incidents of this kind bring the communication with subsidiaries and branch offices to a complete standstill. Branch office solutions must be able to react adequately to such situations. No company is protected against such unforeseeable and uninfluenceable incidents, not even in highly developed industrial nations. In the Tokyo area for example, normal crows are one of the greatest dangers facing data traffic because these birds use the sheathing of overhead fibre optic cables to build their nests. In some East European countries, a major problem is caused as lines are stolen for their copper content. In such bizarre incidents then even the best data compression

won't be of any help. What companies need here is an intelligent use of alternative connections, namely: Tunnel Switching.

The solution lies, as in the case of high availability in other areas, in the redundancy. In other words, the head office and each individual branch office need at least two connectivity options – the more options, the more failsafe the connection. However, the IT department must also be capable of automatically selecting the respectively most economic available data route and in case of breakdown, of immediately switching over to another line. In regions with poor infrastructures there are also other requirements to be met, for example switching back automatically to the primary connection as soon as this is available again. Costs of between 10,000 and 20,000 euros can quickly be built up per office if an ISDN line is not hung up. However, it is extremely challenging to guarantee this in a worldwide network and can hardly succeed in manual operation. Companies need highly developed multi-provider and multi-link gateway functions here.

Unlimited number of tunnels, different types of connection

Automatic tunnel switching facilitates redundant internet connectivity and protocol-based load balancing across several provider connections. Economical and failsafe network structures can be realised by combining VPN functions with connectivity gateway bandwidth management. Professional solutions can ensure an unlimited number of connections with all usual connection types, for example xDSL, UMTS, MPLS, Frame Relay, ISDN, leased lines, satellite uplinks or even dial-up. The connections can also be used in parallel. Many users prioritise their ERP data traffic in this way for international business processes, to support logistics, production and business monitoring processes. They direct the data traffic via the best lines (MPLS) and limit email for example to internet VPN.

A tunnel switching solution should comprise the following features:

- Simultaneous communication across several secure channels, use of any number of redundancy options (internet, MPLS, ISDN, xDSL, UMTS/3G)

with the aim of optimising bandwidth depending on the available communication options.

- Availability monitoring of the direct local network environment as well as from receivers or other critical targets in the network. The information gathered there forms the basis for a decision to opt for a switch.
- Monitoring the packet losses and current packet times as part of the quality evaluation of the traffic route being used. A route may, in principle, still be available; however if it fails to fulfil both of these criteria then it must be excluded.
- Configurable traffic splitting according to the type of application, source, destination and time in the respective optimum channel. This is essential since most companies require more than just simple left-right policy.
- Dynamic tunnel switching in error cases according to a configurable error procedure in which the new traffic priorities are defined following a switch.
- Activation of additional routes if required, for example UMTS dial-out if a critical availability situation arises. This makes sense if such routes should not be used permanently because of volume-based fee models or insufficient quality.
- Bandwidth management which is fully integrated into the tunnel switching logic. This means that also application-specific bandwidth reservations and prioritisations can change too, depending on the tunnel used.
- Support for normal routing as a special case for one tunnel. As such, VPN channels and pure routing – for example via an MPLS line – can be treated equivalently.

Traffic intelligence therefore does not only consist of optimising the application data traffic (WAN optimisation), but also includes tunnel switching. The gateways detect the connection disruptions automatically and switch to alternative connections or divert data flows directly via different routes. If however, there is no WAN optimisation, then scenarios can quickly arise in which critical applications are inaccessible as long as bulk and mail traffic block the lines.

User RHI: Nine communications routes out of China

RHI, international technology leader for fireproof materials has set up a highly flexible communications infrastructure based on the integrated multi-provider and multi-link functions. The Chinese subsidiaries are connected to a main location via leased lines, point-to-point or internet VPN, which in turn has an MPLS connection to Europe (SLA via Telekom Austria). All RHI subsidiaries also have backup internet connections. The phion Gateways detect faults automatically if a line breaks down and conduct a transparent failover to alternative connections. So if one location has no network access the connection can be restored via any other location. Even a total collapse on the Chinese internet gateway is intercepted by a refined configuration which would then direct the data traffic via Hong Kong. Overall, RHI has nine routes out of China today – with performance levels that facilitate an efficient working environment.

Keeping track: Convergence and administrability

Two aspects are often overseen when talking about features and functions: The integration and administrability of the solution. Not every function requires its own appliance, its own system. The convergence of the major security technologies in each gateway is an important step towards limiting the complexity and facilitating the management of modern infrastructures at reasonable expense. This can even be realised for leading manufacturers in their branch offices: Branch-Office-Boxes (BOBs) combine classic firewall functions with traffic intelligence. The latter even upholds the connection in the smallest office under difficult conditions. The traffic monitoring uses all of those algorithms and functions for this which would normally be built into a WAN optimisation controller. Users should opt for solution approaches which unite the complete firewall and VPN functions as well as traffic intelligence – including tunnel switching – into one system.

Convenient installation and single gateway maintenance are no longer significant for companies operating internationally when it comes to administrability – the pure volume of systems alone demands enormous expense in terms of time and staff. So with traffic intelligence and tunnel switching, attention should be paid to

ensuring that the network components can be managed 100% from the head office. And this ought not be too difficult for the administrator to manage: Because tables are useless if he needs to maintain an overview as to which lines are being used by a tunnel switching solution at any one time. The only way of displaying the information so that it can be used immediately, is by using graphic monitoring. Administrators are also users who appreciate user-friendliness, too. In the leading systems, VPN tunnels can be added or re-directed in a graphical tunnel interface using drag&drop for example, and worldwide distributed connectivity structures are simple to manage. Colours are used to show the administrators characteristics or changes. And the graphical tunnel interface allows the fast definition and changes to all configuration parameters.

Traffic intelligence: Three principles

The principles of traffic intelligence can be summarised in three points:

1. Make the most of the available connectivity and ensure multiple redundancies.
2. Decide, which application, which users, which server use which data line – when and how.
3. Neither the user nor the applications notice the traffic intelligence, except for improvements in availability and performance.

About phion

phion is one of the leading European providers of solutions to protect company communications. With the netfence product portfolio phion offers solutions for the most demanding standards in terms of availability, security and management. netfence appliances consistently address all security-related aspects: From perimeter defence to the safe and highly available connections to branch offices, right up to blocking dangerous contents and protecting internal networks. airlock protects web applications like e-banking platforms and web services from any attacks or misuse. All phion products have core management and are distinguished by their remarkable TCO.

phion is listed at the Vienna stock exchange (symbol: PHIO) and is based in Innsbruck, Austria and Zurich, Switzerland. phion's customers include well-known, internationally operating companies from all sectors of industry.