Pipeline
It's in here.

A "Telecom General's" Warning: IP May Be Dangerous to Your Health

Strategies for avoiding a "dumb pipe" fate

By Jonathan Morgan, vice president product marketing, Tatara Systems

If Telecom had a counterpart to the Surgeon General, the "Telecom General's" warning would read something like this: *IP may be dangerous to carriers' long term business health.* It's well known that the migration to IP is changing the telecom world, but everyone is so focused on cost-benefit analyses and "cool" applications that we've lost sight of one key factor: IP takes control away from the traditional service provider. IP separates network ownership from customer ownership. Any company can offer application services across networks they don't own, which could relegate the carrier's offering to nothing more than a connectivity pipe.

No More Dumb Pipe

Major telcos around the world are turning to content offerings to avoid a dump pipe fate. Remember that traditional carriers are just as able to enter the IP applications game as any new competitor. This means they'll need a way to track and bill for their content, particularly when they do not own or control the network that physically serves the customer.

Billing in the "extended network" IP world requires a whole new approach to collecting information; one that is client-server based rather than exclusively network-based. Instead of installing network hardware that collects the necessary usage information and transfers it to a billing or mediation system, a software-based client that sits on the end user's device can be used to collect that information and deliver back to a gateway connected to existing mediation or billing platforms.

This approach is advantageous because the client software can determine which applications an individual is using, thus allowing a service provider to bill according to application. By examining the IP packets being transferred, the client can determine key data such as which protocols are being used and which sites accessed. For example, if the client detects that SIP packets and real time transport (RTP) are in use, it will recognize a VoIP session. If RTP and real-time streaming protocol (RTSP) are in use, it's a streaming video session.

Obtaining such information becomes more challenging when dealing with a VPN. In this case, IP packers can be examined before they reach the VPN. Client software can work in conjunction with an enterprise's security policy to ensure that visibility into the packets does not compromise security. Service providers must also ensure that the information regarding the IP packets is encrypted before being sent to the gateway.

Securing the Extended Network
Because delivering applications rather than just connectivity requires that private information be exchanged constantly, security is necessary throughout the user experience. For enterprises, the only way to truly maintain security control is to adopt a client-server solution that insures that user credentials and usage information are never exposed to third parties. Even consumer-based carriers are implementing more complex systems to offer subscribers identity security and peace of mind.

For example, large Internet players like AOL are already moving beyond basic user name-password security measures and offering multi-factor authentication processes such as RSA secure ID, where users must supply a password and a constantly changing secure token ID number. GSM-based mobile operators are also moving toward secure SIM-based authentication to utilize their existing secure infrastructure.

In the "extended" network world, service providers will want to allow enterprise customers to roam onto networks they don't own, and yet maintain a direct link to insure things like single sign-on applications remain secure. For instance, when a user signs onto the network, the server sitting on the "home" provider's network can check to ensure that the device has the latest firewall settings and software patches before allowing the user to long onto the enterprise network. In such a case, the client software would communicate with an endpoint that validates the user's settings before launching the VPN. If the user isn't up-to-date, the system would prompt the user to update her software before permitting her to log on.

Assuring Quality for Cash
Another way to gain extra revenue is through quality-based billing - charging separately for different levels of quality of service for specific applications. Quality-based billing is admittedly much more difficult to support when a service provider does not own the serving network. Here again, a move to client-based monitoring is critical. Client-server software can determine in real-time what quality is being delivered, and could make a decision to switch networks if an alternative is available that could offer better quality.

Once quality is monitored, service providers must insure that they deliver quality and usage information back to the enterprise, to show the customer they've been billed accurately and their SLAs are met. A related concept is to provide the customer with control over connection rules that determine which network to use based on the service in question or the quality required for that service.

Keeping Control
Service providers today are accustomed to maintaining control, and the concept of not controlling every network across which they offer services may deter them. But the migration to an IP-based world is opening the application floodgates whether carriers embrace it or not. With any application provider able to deliver service to any IP user,

carriers that don’t take advantage of new application opportunities are endangering their health and relegating themselves to little more than a dumb pipe. There is yet a much larger piece of the Internet and telephony value chain for carriers to capture.