Multi-Domain Advanced Services and SLAs

IPsphere Model Walk-through

Mark Williams
Liaison, Academic Networking, APAC
miw@juniper.net

QUESTNET 2005
Coolum, 6th July, 2005

Agenda

- Background, Context, Design Goals
- Reference Architecture Proposal
- Example
- Summary

What is/was the Infranet Initiative?

Oct'03 → **Juniper Networks and partners issued an industry call to action**

Mar'04 → **And then formed The Infranet Initiative Council**
Hosted by Juniper Networks

Jun'05 → **Infranet Initiative Council morphs into member-funded industry body called IPsphere Forum**

New standards are essential for industry transformation	**Leadership** needed to prevent the fragment efforts that slow progress	The industry's best must come together and **collaborate**

Chicago Meeting Attendees (9-10 June'05)

- Alcatel (Secretary)
- Brasil Telecom
- Brighthaul, Bezeq
- BT (Board member)
- Ciena
- CIMI
- Cisco (Vice Chair)
- Datapower
- Ericsson
- FT (Board member)
- Huawei (Board member)
- Internet 2
- Juniper (Chair)
- Lucent (Treasurer)
- MESoft
- NCS
- Nexagent
- Oracle
- Redzinc (Board member)
- Siemens (Board member)
- T-Com (Board member)
- Telenor (Board member)
- Tellabs (Board member)
- Telus
- T-Systems

Former IIC Members moving to IPsphere Forum membership

Executive

Working Group Participants

Latest members expanding IPsphere Forum membership

- Alcatel
- Cisco
- Datapower
- Nexagent
- Telus

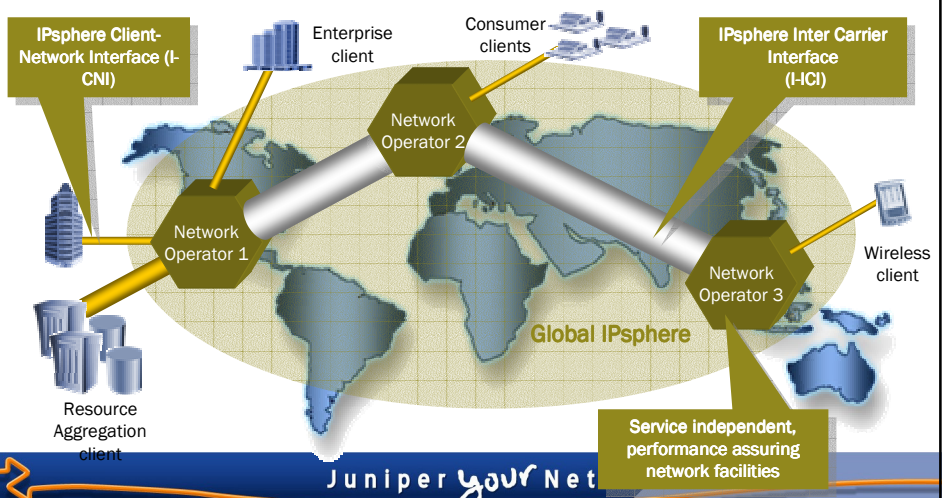
The Problem being Solved

- Current IP networks are built on an "Internet" model in which end-users pay a fixed price for access (and perhaps a fixed rate for volume) and obtain all services equally, and where providers interconnect permissively and without specific per-service contract or settlement.
- Service Providers typically have a completely different model for the services on which they currently depend for revenue. This alternate model involves contracting per-service, specific settlement, and managed interconnect based on bilateral or multi-lateral agreements among providers.
- IP standards processes have tended to be directed at the Internet model, and introduction of IP issues into more traditional standards organizations has generated only slow progress.

What the IPsphere Does

- The IPsphere is a new framework for worldwide IP services in which providers are free to create multiple service and business relationships using the same infrastructure, and interconnect with end users and with each other in a way suitable for each such relationship model supported.
- The goal of the IPsphere is to create a business-level exchange among providers, and with customers, that supplements but does not replace technical or protocol signaling at the network control level. The business-level exchange will then manage the way that specific devices or software systems in the network respond to signals for service, thus making service creation a slave to business relationships.
- The IPsphere seeks to accomplish this by adding a new layer to a traditional network, a business layer.

The IPsphere Standard Model



Key Design & Functional Principles: I

- IPsphere will link the technical superiority of IP & associated applications with profitable & operationally efficient service models
  - Not specific to an IP version
- IPsphere will be ahead of – not just match - emerging computing futures to remove today's network limitations to IT applications
- IPsphere will incorporate important contemporary services
  - Private Line, PVC (FR, ATM), VLAN, VPN
  - Internet Access, Mobile, DSL, Cable, Ethernet, Voice, Video
- IPsphere will be open & therefore implicitly multi-vendor, where possible augmenting existing standards

Key Design & Functional Principles: II

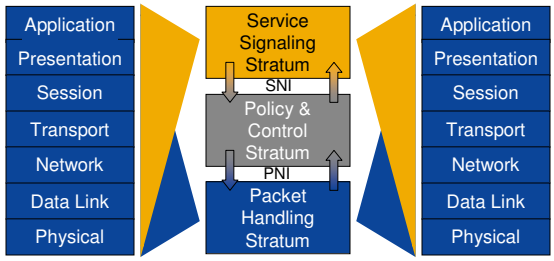
- Trust is no longer implicit, it must be explicit
  - To alleviate the permissive nature of the Internet service model
  - Service signaling targets full authentication of all users & devices
- Single-operator & multi-operator service footprints supported equally
- Make it easier to meet regulatory requirements without subjecting the network overall to excessive costs

Agenda

- Background, Context, Design Goals
- Reference Architecture Proposal 
- Example
- Summary

IPsphere Strata: Architecture

- Operationalize network services beyond basic routing
  - Offer Quality, Security, Reliability as service attributes
    - Via Signaling-Network Interface (SNI)
  - Available for attachment to any & all user application
  - In computing's emerging language of attachment – SOAP/XML
  - Without exposing network's internal control functions
- Provide service-independent trust mechanisms
  - Ensure user, applications claims (e.g. identity) can be believed
  - Flexible, dynamic exclusion of under-authenticated network clients



IPsphere Interfaces

- Client-Network Interface (CNI - formerly UNI)
  - Signaling from network clients to network itself
  - Client means an application 'end-point' – 'originator' or 'terminator'
  - Proposal is that the signaling be SOAP/XML based to provide ultimate flexibility, and to match WS attachment language
- Inter-Carrier Interface (ICI)
  - Signaling between/across operator jurisdictions
  - Ensures performance of transiting traffic, to incorporate settlement
  - Also proposed that, like CNI, this be SOAP/XML based to facilitate attachment
- Signaling-Network Interface (SNI) – New concept
  - Service Signaling stratum – Policy & Control stratum communications
  - Also proposed that, like CNI, ICI this be SOAP/XML based
- Policy-Network Interface (PNI) – Name for existing concept
  - Policy & Control stratum – Packet Handling stratum communications

IPsphere Strata: Trust Barrier & Service Operation

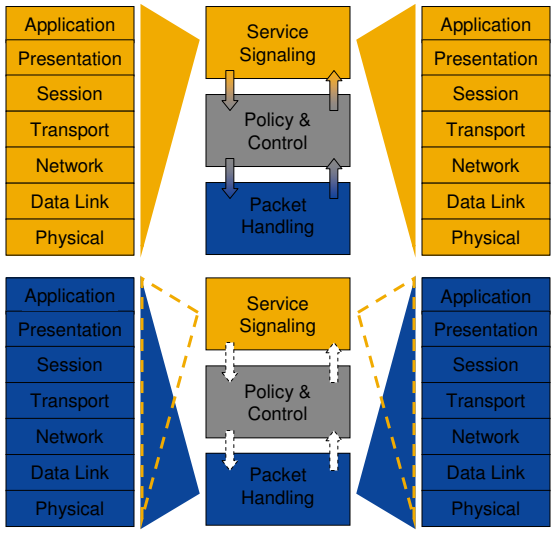
1. Service Signaling only, no client-client data exchange is possible

2. Clients make claims: identity, desired service(s) etc

3. If claims validated, policy & control is signaled via SNI, Policy & Control control then configures Packet Handling behavior in associated network elements via PNI

4. Client-client data exchange is now possible, with packets treated as outlined in requested service description(s).

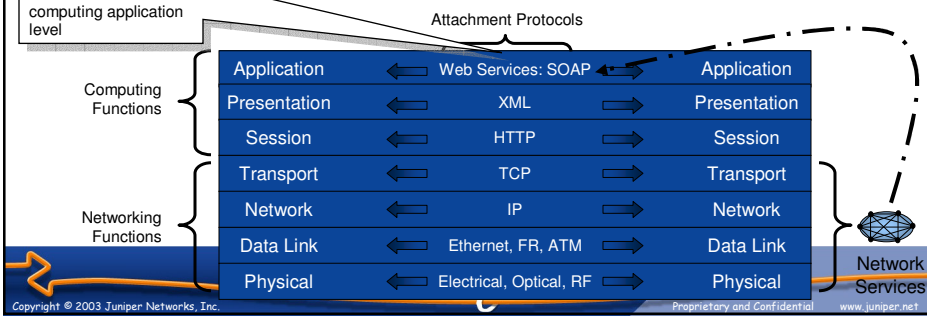
5. Service Signaling remains available, as needed for service modification or termination



Service Signaling Strata: Protocol choice determines 'Consumability' of Network Services

- Goal is to fuse computing & networking service consumption procedures
  - Enables new computing or network features to be leveraged without creating multiple sets of operating practices
  - The clearest & strongest emerging computing application attachment protocol is evidenced in W3C Web Services
    - XML-based Simple Object Access Protocol (SOAP)

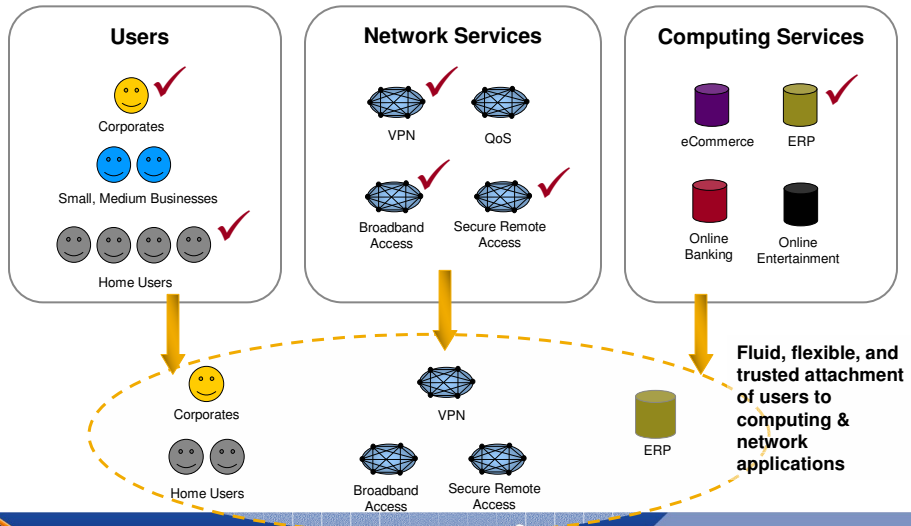
For ultimate flexibility and utility network services should be visible & available for attachment at the computing application level



Service Signaling Proposal: Make Network Services consumable via use of "Federation" concept

- Proposal: in an IPsphere service, the process of securing the service and the process of assuring the availability and performance of the service are linked
  - The trust and security portion admits users and computing application resources to a network
  - And the network partitioning and traffic management portion assures their experience once admitted
- Simple, logical & flexible and can be applied to both…
  - Internal network operations, and
  - Projection of services to clients and other IPspheres

Federation Principles



Service Signaling Protocol Choice needs to also accommodate the broadest range of applications

- There are essentially three broad service types…
- Emerging dynamic
  - Use Web Services directly: attachment language is SOAP
  - GRID, IBM WebSphere, MS Indigo/Longhorn, HP OpsWare, Juniper SDX
- Contemporary dynamic
  - Use service-specific signaling and/or authentication, but this is not WS (SOAP/XML) based
  - Enterprise LAN, PSTN Voice, SIP Voice, DSL & Cable broadband access, Dynamic Internet access, IPSec/SSL CPE VPN, ATM-MPLS
- Contemporary static
  - Have no signaling component, service is setup out of band, via 'customer care' systems, often requiring craft personnel to activate
  - Fixed services – identity endpoint is usually readily known, trustable
  - Leased line, Frame Relay, Direct Internet access, PP IP VPN, VLAN

Single Mechanism Choice: IPsphere Service Creation via Federations…

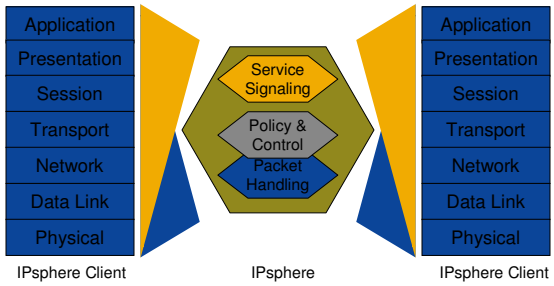
- With this choice ultimately, all IPsphere services would be created using federations
  - Linking trust & performance intimately in the service's definition
- A separate virtual network partition would not necessarily be required to support every federation
  - Partitions would be differentiated according to performance and other network features
  - Federations with identical network performance/feature requirements can operate through the same network partition (assuming it is adequately resourced, of course)
- The point at which a user connects to the network is a trust barrier in IPsphere terms
  - When a client presents an identity token to join the network, they pierce the trust barrier for each service they have a validated claim to access

Agenda

- Background, Context, Design Goals
- Reference Architecture Proposal
- Example: Co-operative Multi-Network Services
- Summary

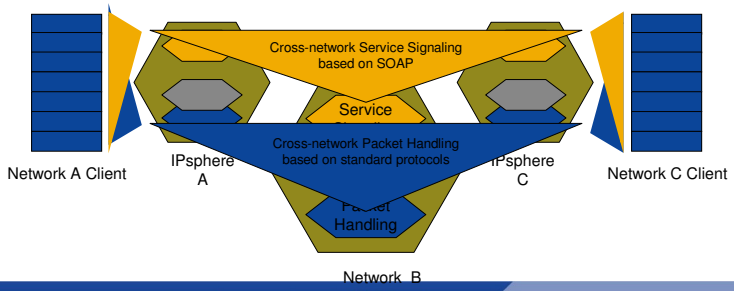
Use Case: Co-operative Multi-Network Services

- Framework must extend services across multiple networks to meet IPsphere design objectives
  - Without compromising other capabilities
- Cross-network user claim verification, service attachment.



Use Case: Co-operative Multi-Network Services

- Web Services based Service Signaling capabilities readily extensible across multiple operator jurisdictions
  - Provides basis for IPsphere ICI
- Service Signaling behavior enables multiple operators to create a common application-level framework
  - Links packet handling strata into a common service context



Summary

- IP-Based but Interoperable with Other Protocols
  - The IPsphere model is infinitely flexible. It is based on the assumption of a universal IP core, but is interoperable with other protocols/networks via the CNI
- Application-facilitating but not Application Specific
  - It facilitates the creation of applications like ASP and content services but without any protocols or elements that are specific to those applications
- Managed at the Traffic Partition Level for Efficiency
  - It manages traffic not at the service level but at the traffic class level for greater operational scalability—it doesn't matter how many services you offer, just how many distinctively different levels of network QoS and security you offer
- Capable of Making "Security" an Element of Service Quality
  - With IPspheres, security is the next dimension of QoS after the usual availability, latency, bandwidth, and loss metrics—as it should be
- Capable of Supporting Contemporary or New Services
  - New and legacy services can be mapped to IPsphere infrastructure in the same way, and new and legacy interfaces can even share a common "service".
- Capable of Single-Carrier or Connected-Carrier Operation
  - Finally, IPspheres can be used to support services on a single-carrier-per-service basis or services that extend across multiple carriers. Where the latter model is used, carrier cooperation and settlement are totally controlled at the IICI

Call To Action

- You will notice that every technology being used in IPspere has its origins in the academic community.
- The IPsphere concept is aimed at making network services just another element in a federation of services and users that is signalled, authenticated and assured using the web services model. It is very congruent with the Grid Networking model!
- Authentication and Trust models is a major area of work in IPsphere. Current work in the academic sphere such as Shibboleth is having a major impact here.
- The door is most certainly open for the academic community to continue to influence the process, and your input can be a major factor in getting what you need from the global IP network.

www.ipsphereforum.org

Additional Backup Slides follow

IPsphere Service Signaling Stratum

- The main additional dimension that IPsphere reference architecture proposal adds
  - In the SOAP/XML case this is the "community-" or "service-building" stratum of an IPsphere
- IPsphere clients attach explicitly (directly or proxied) via CNI to assert claims which include
  - Identity, rights to services
  - Ability to provide service resources
- Service Signaling stratum validates claims & connects clients to service resources
  - Client to client data exchange can't proceed until this validation is complete
- IPspheres attach to each other via ICI
  - Extend claims and service attachment into an adjacent network operator jurisdiction

IPsphere Policy & Control Stratum

- Traditional control of network devices take place in this stratum
  - Can be selectively "reflected" via SNI into Service Signaling stratum to make network services available for attachment there
  - Control functions are internal, not exposed to clients or to other IPspheres
- This stratum hosts any & all management applications that oversee and control behavior of packet handling functions
  - Network service management
  - Management of potentially non-homogeneous array of network devices via 'PNI'
- Maintains overall view of an IPsphere's resources
  - Distributed arrangement tracking 'state' of network resources
  - Verifies packet handling stratum resource availability in response to requests from Service Signaling stratum

IPsphere Packet Handling Logical Stratum

- Logical stratum through which clients exchange application data
  - A network of physical devices that may embrace a common protocol or may include several protocols via interworking facilities built in to the network
- Clients, adjacent IPspheres can't access packet handling functions until Service Signaling has validated identity & other service claims
  - Client is behind trust barrier, only has access to signaling stratum functions
- This stratum hosts all devices contributing packet handling capabilities to a network service
  - May be a non-homogeneous collection of physical devices
- Packet handling functions may be grouped into sub-strata
  - Specialized packet processing (eg source verification, queuing)
  - Resource segmentation to create virtual network sub-partitions
  - Packet transport & connectivity

IPsphere Vocabulary

- Client:
  - is the 'service endpoint', the point where a user application attaches to the network to obtain service, can be direct or proxy attachment
- Application:
  - Business, consumer IT processes that are distributed in nature & therefore require networking technologies to connect users to each other and/or to content/application server clients
- Service:
  - A combination of transport, connection management, facilitation & application features that a user obtains from an operator to integrate into business or personal needs
- IPsphere:
  - A network that combines the universality of the Internet with performance assurances, security/identity & operations management to maximize the range of profitable applications the network can support
- I-CNI:
  - Signaling & data transfer between client & network to ensure authorized usage, represent application's network requirements, and to ingress/egress user's data traffic
- I-ICI:
  - Signaling & data transfer between networks to ensure performance of transiting traffic, and that – where appropriate - facilitates settlement for service revenues across network operators

What is an IPsphere?

IPsphere

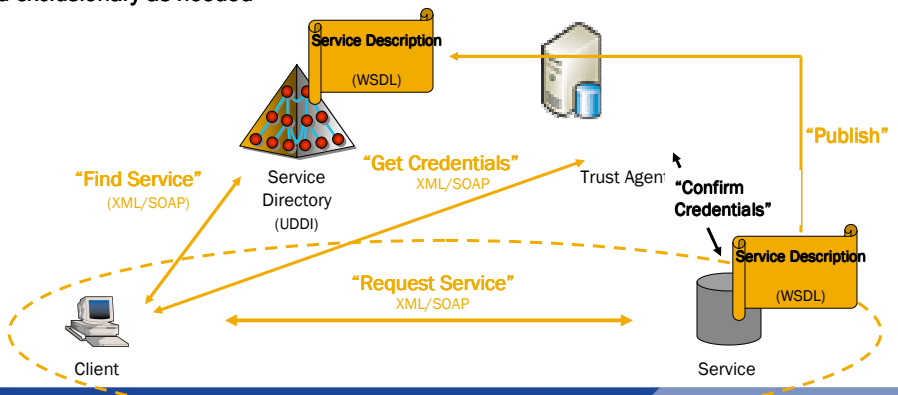
A **network** that combines
the **reach and positive economics** of the Internet
with the **assured performance and security** of a private network
enabling a packet infrastructure to **support ALL communications**

Robust IP	Open standards	Dynamic
Predictable Partitionable Intelligent Controllable	Client-to-Network Interface Inter-carrier Interface	Automatically establishes trust and identity to serve user

How Web Services create/maintain Federations

Inherently loosely coupled approach, using enables federations to be as flexible and exclusionary as needed

IPsphere concept adds the ability for network services to be described and offered for attachment



What the IPsphere Is…and Isn't

- The IPsphere is a model for putting network services into a business context by linking service creation with service ordering and fulfillment.
- The IPsphere is based on web services principles for the exchange of business information, making it easy for it to manage the elements of higher-layer services that require identity management and reliable communications, including grid computing and ASP services.
- The IPsphere is not a strategy to create services on the network, provide QoS, or manage resources at the physical level. It is compatible with most emerging standards, and the IIC will work to insure it stays that way.
- The IPsphere is not an alternative to the Internet, it is an alternative to the Internet model applied to non-Internet services.