End-to-End Networking
What Does it Mean for Campus?

Jean-Marc Uzé
Juniper Networks
juze@juniper.net

Terena e2e WS, Amsterdam, Dec 1st, 2008

End to end: anything missing?

Please provide me one Gb/s pipe between univ A and B

Sure... done!

We need NOCs expertise

Yes. Let's build a mailing list...

Universities, Campus, Research Labs etc...

NRENs, MANs, GEANT etc...
Blueprint of End to End Connectivity
(from a services point of view)

End device: biz/resp end-user, voice/video/content/cloud server, ...

Service Node
Service Helper
Access Node
Transport Node

Inter-domain: several approaches

1) AAA Infrastructure
2) Business Layer (Web Service / SOA)
3) Service Signaling
4) Infrastructure Control Plane Signaling

NRENs | Regional REN / MAN

Service 1
Service 2
Internet
How far is the end-user from the Service Connection/Delivery Point?

Campuses/sites particular characteristic:
- First and Last mile
- Unique role of connecting the endpoint (and so end-user, if any) to the network
- They have more “enterprise” type of issues (e.g. security), that makes R&E specific services more challenging to adopt => probably a need to adapt!

Requirements for a Campus to implement End-to-end Services

1. Deal with more diversified traffic processing building blocks
   - Routing, Ethernet switching, Firewall, NAT, IPSec VPN, VPN SSL, IDS/IDP, Application Acceleration, etc.

2. Seamless integration of NREN services
   - Integration with their existing operational processes and tools (e.g. NAC and other security policies and enforcers)

3. Avoid Bottleneck in Performances and Services
   - No matter what elements are in the chain, between the endpoint and the first Research & Education Backbone infrastructure
Handling Endpoint and User Access

- The end-user will have to move between several services, based on his “Role”
  - Traditional IP infra (Internet)
  - Service X (e.g. lightpath)
- Service Plane:
  - Should the campus deploy the NREN Service Layer/Tool and integrate it with the campus infrastructure?
  - or should we leverage current campus network access control technology
  - or “connect” the tools together?
- Data plane:
  - VLAN would be the easiest/flexible solution
  - Is a VLAN secure enough?
  - Layer 3 access policy also possible

Use Network Access control Option 1: Layer 2 Mode

- Use NAC technologies to connect the endpoint to the e2e service
- VLAN makes the connection
- 802.1x client to authenticate and authorize the host + end-user
  - Use Standardized approach for interoperability with the LAN infrastructure
  - Some solutions support advanced dynamic policies in the switch (QoS, filtering etc.)
Data Plane: Is a VLAN good enough?

- Is a VLAN conform to Campus Security Policies?
- Does the end-user want to connect to an unprotected network?
- Is an e2e service (e.g. lightpath or Virtual slice) safer or more risky environment compared to the IP/Internet network?
- Should the VLAN in the campus contain other traffic processing capabilities?

Secure the VLAN used to access an e2e Service

- Solution 1: Use some policies in the Access Switches
  - Requires support of advanced features
  - Require integration with the NAC to link the Role with dynamic policy allocation
- Solution 2: Use a dedicated “virtual” Firewall for each VLAN connection

Firewall Virtual Systems (VSYS)
- Establishes virtual Firewall with their own address book, policies, and management
- Routed, NAT or Transparent mode
Use Network Access control Option 2: Layer 3 Mode

- Use NAC technologies to connect the endpoint to the virtualized slice
- IP policy makes the connection
  - Use Infranet Client to apply dynamic policies in a firewall
    - Simple IP policy in the FW to filter and route packets to the appropriate service
    - Or IPSec Tunnel to secure the communication between endpoint and FW (e.g. wireless)
    - Sophisticated and granular FW policies can be added
    - Routed, NAT or transparent modes
    - Note: Option 2 can be combined with Option 1 (VLAN)

Options for Role Assignment (i.e. connect to the right Service)

1. Manual: Login name specific for each e2e service
   - Pro: Simple access method without host checking requirement
   - Cons: Requires the user to transit via a portal (for each Service)

2. Automatic based on the detection of a particular running application in a host
   - Pro: The user simply move to the appropriate service when launching the specific application
   - Cons:
     - Requires dynamic Host checking capability with VLAN reallocation
     - Heavy management: Need to link a specific application process to a Role in the NAC
     - Operational process may not work well with some users (involuntary move between VLANs), not much secure

3. Automatic based on insertion of USB stick containing a security certificate identifying the User and Service he wants
   - Pro: very simple management and operational process, very secure
   - Cons: Requires dynamic Host checking capability with VLAN reallocation
Conclusion

- E2E services are explored by R&E community since many years
  - Isn’t the main challenge?
  - Lot of experience but immature solutions
- Most users are connected via a campus/site
- Campus have specific aspects which require to study the problem from a different angle
  - Challenging to introduce NRENs type of tools
  - They need practical solutions that doesn’t divert them from their main business
    - i.e. leverage NAC, Ethernet switch/router, Firewall, etc.