The end-to-end principle in the Internet

Jelmer Barhorst Wouter Borremans
Carlos Groen Jan van Lith

15 maart 2005

Contents

- Introduction
- to e2e
- not to e2e
- NAT
- Discussion

Introduction

End to End principle - 1

Question where best to put functions in a communicating system

- Saltzer/Reed/Clark in 1984
- The function can only be completly and correctly implemented with knowledge and help of the application at the end of the communication system
- That function is cannot be a feature of the

communicating system

Example

Delivery guarantees

- After delivery – Request for Next Message
- Congestion control
- Only new message after an recieved acknowledgement from destination

End to End principle - 2

Where to put the state associated with applications in the internet: Network or end nodes?

- End to end protocol should not rely on maintenance of the state (end to end communication) inside the network
- State in end points only destroyed by endpoint (fate-sharing)

Fate is shared between 2 applications that don't depend on anything in the network

End to End principle - 3

What kind of state is maintained where?

- Network maintains some state information: routes, session information, compression histories to perform its services.
- State must be self healing
- Volume of state must be minimized

- Loss of the state must not result in more than a temporary denial.

Soft state in network – Hard state in end nodes

Facets - End to End principle

- When state in network, traffic cannot route around failures
- Scaling easy when state-holding to edges
- Security state held inside network

Summary

- Maintaining openness
- Increasing reliability and robustness
- Preserving the properties of user choice
- Ease of new service deployment

End to End - Now

Mobile IPv6

- Routing proxy in the mobile node's home (Home Agent) and local subnet (Foreign Agent)
- Maintaining the mapping, the care of addresses.
- Local subnet routing proxy in Mobile IPv4 but not in Mobile IPv6

- In Mobile IPv6: end node responsable for care of address

to e2e

Trends - 1

- E2e principle provides solid foundation for IETF work
- After RFC 1958 more and more come into question

  "Salzer: The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the endpoints of the communication system"

Trends - 2

- Reduction in transparency due to NAT and other AT mechanisms
- More recently OPES (open pluggable Edge services)

Authentication

- Most important issue of the last 15 years
- Lack of trust
- Not many users, tool for ACADEMIC research and communication
- Users are not technological sophisticated or simply uninterested

- E2e principle does not need trust application designers make the choice

New service models

- Implementing e2e means rethinking of service models
- Customer may expect some kind of service level
- Retail broadband and multimedia services are new service models

Whither the e2e principle

- Does the e2e principle has a future?
- How should it be applied?
- Current internet community will ignore it
- Seperate (academic :)) research group

Whither the e2e principle

Consequenses

- Protection of innovation
- Reliability and trust

Whither the e2e principle

- E2e principle applicable to application design
- No dependencies that would break the e2e principle
- Internet standards as a conflict area

Conclusion

- Remains very important
- Unbundling of the princple leads to a distributed approach

Not to e2e

Adresruimte - 1

- IPv4 adressen zijn “op”
- Organistaties krijgen te weinig adressen

Adresruimte - 2

"Oplossing": privé adressen gebruiken

- RFC 1918 / BCP 5
- Collisions (bijv. VPN)
- Niet publiekelijk routeerbaar (security?)
  - NAT
  - Proxies

Proxies

. . . Application Level Gateways, caches, relays, etc.

- SMTP gateway
- Webcache
- Mail relays (met virus-/spamcontrole)

Geen probleem, mits de packets onderweg niet veranderen.

Firewalls - 1

"Schoenmaker, blijf bij je leest"

- Bridge $\Rightarrow$ layer 2 filtering
- Router $\Rightarrow$ layer 3 filtering
- Host $\Rightarrow$ layer 4 filtering

Firewalls - 2

Een layer 4 filter op een bridge (of router) is wel makkelijk:

- Centraal
- Geen rommel op het netwerk
- "stateful" filteren $\Rightarrow$ niet e2e!

Load balancing

- Reverse proxying
- DNS round robbin
- Meedere servers met hetzelfde IP (anycast)

Minder geavanceerde “gebruikers”

Initiëren het contact, hoeven niet extern bereikbaar te zijn

- Mobiel met GPRS (dataverbruik)
- Afspelen streaming media (one-to-many)
- maar ook het gros van de thuisgebruikers

Third-party

- Trust anchor (communicatie via een Trusted TP)
- Enforcer of good behavior (moderator)
- Belastingen of zelfs censuur. . . (brrrr)

Conclusie

- e2e is niet altijd nodig
- Centralisatie
- IPv6 is toch wel erg wenselijk

NAT

NAT

Actually...

- NAT: Network Address Translation
- NAPT: Network Address Port Translation
- (RSIP: Realm-Specific Internet Protocol)

NAT

- Replaces source and destination address (IP)
- Static
  - m internally, n externally
  - m,n $>=$ 1 and m $=$ n
- Dynamic
  - m,n $>=$ 1 and m $>=$ n

NAPT (masquerading)

- Replaces source and destination address (IP)
- Replaces source and destination port (TCP)
  - m internally, n externally
  - m $>=$ 1 and n $=$ 1

RSIP

- Leases external address and port to internal host
  - m internally, n externally
  - m,n $>=$ 1 and m $>=$ n

Advantages NAT

- Limited number of IPv4 addresses
- Maintain internal addresses
- Load sharing
- Secure....

Problems NAT

- "Breaks" the end-to-end principle
- "Breaks" IPsec
- "Breaks" certain applications
- VPN address collisions
- Single point of failure

NAT and IPv6

- Delays deployment IPv6
- Helps deployment IPv6 (!)

Discussion

Discussion

- Do we really want/need e2e?
- Did we ever have e2e?
- Will we ever have e2e?