T-110.5110 Computer Networks II

Summary

10.12.2007

Lectures

17.9. Introduction
24.9. Transport issues
Invited lecture given by Dr. Pasi Sarolahti / Nokia Research Center
1.10. Mobility I
Lectured by Prof. Jukka Manner
8.10. NAT (STUN, ICE, TURN)
15.10. QoS I
Lectured by Prof. Jukka Manner
22.10. Mobility II (MIP, HMIP, NEMO,..)
Lectured by Prof. Hota
5.11. QoS continued and signalling
Lectured by Prof. Hota
12.11. AAA
19.11. HIP I
26.11. HIP II
Invited lecture given by M.Sc. Miika Komu / HIIT
3.12. Services and identity management
10.12. Summary

Exam

- Monday 17.12. 16-19 in T1
- Essay questions
  - Describe, analyze, compare
  - Synthesis

Summary of Course

- As discussed the course focuses on several important features of current networking systems
  - Mobility, QoS, Security, Privacy
- We observe that these features were not important for the original Internet architecture
- They are important now
  - Mobility, QoS, Security are coming with IPv6
  - IPv6 deployment does not look promising
- Hence, many proposals to solve issues in the current Internet
- Also many solutions to solve expected problems in the Future Internet

Layered Architecture

- Internet has a layered architecture
- Four layers in TCP/IP
  - Application (L7)
  - Transport (L4)
  - Network (L3)
  - Link layer / physical (L2-L1)
- We will talk a lot about layering
  - Benefits, limitations, possibilities (cross-layer)
  - It is not always clear what is a good layering
- A lot of interesting networking developments are happening on application layer

The Internet has Changed

- A lot of the assumptions of the early Internet has changed
  - Trusted end-points
  - Stationary, publicly addressable addresses
  - End-to-End
- We will have a look at these in the light of recent developments
- End-to-end broken by NATs and firewalls

Network has Value

- A network is about delivering data between endpoints
- Data delivery creates value
- Data is the basis for decision making
- We have requirements to the network
  - Timeliness
  - Scalability
  - Security
  - ...

Looking at the Layers

- Link Layer / Physical
- Network
  - We will look at mobility, security, and QoS on L3
  - Mobile IP, network mobility, HIP, NAT Traversal
- Transport
  - Basic properties of transport layer protocols
    - TCP variants, DCCP, TLS, dTLS
  - Mobility and security on L4
- Application
  - Security, identity management

- Goal: have an understanding of the solutions and tradeoffs on each layer and discussion on the role of layering

Role of Standards

- On this course, we will talk a lot about standards
  - IETF is the main standards body for Internet technologies
  - Instruments: RFCs, Internet drafts
  - Working groups
  - IRTF
- Other relevant standards bodies
  - W3C, OMA, 3GPP, OMG

Transport Issues

- Network layer (IP) provides basic unreliable packet delivery between end-points
- Transport layer needs to provide reliability, congestion control, flow control, etc. for applications
- TCP variants
- SCTP
- DCCP
- Not covered on the course
  - TLS
  - dTLS

TCP Improvements

- Concepts: Congestion window, round-trip time, retransmission timeout, duplicate acknowledgement (triggered by out of order segment)
- Congestion control
  - Packet loss as a signal, reduce rate
- Fairness
  - Transport implementations must be fair to other flows
- Retransmission mechanism
- Selective acknowledgements (SACK), RFC 2018
  - Additional information about ”holes” in sequence number space
- Limited transmit & early retransmit, timestamps

SCTP

- Stream Control Transmission Protocol (SCTP)
- Specified in RFC 2960
- Additional features to TCP
  - Preservation of message boundaries
  - Support for multiple streams
  - Support for multi-homing
- Packets consist of chunks: INIT, SACK, HEARBEAT, DATA, ABORT, SHUTDOWN, ERROR, and AUTH
- Partial reliability
  - Retransmissions until abort
- Extended Socket API (bind(), context data with sendmsg())
- Suitable for signalling traffic
- Challenges with middleboxes

DCCP

- Datagram Congestion Control Protocol (DCCP)
- Unreliable datagram-oriented protocol (RFC 4340)
  - UDP with congestion control
- Connection-oriented, requires connection state machine
- Congestion control requires ack mechanism and sequence numbers
- Negotiable features and options
  - Checksums, congestion control parameters
- Some features: partial checksums, service codes
- Suitable for long-lived non-reliable flows
- Challenges with middleboxes

Mobility

- What happens when network endpoints start to move?
- What happens when networks move?
- Problem for on-going conversations
  - X no longer associated with address
  - Solution: X informs new address
- Problem for future conversations
  - Where is X? what is the address?
  - Solution: X makes contact address available
- In practice not so easy. Security is needed!

Mobility on the Internet

- Mobile IPv4
  - Mobile Node, Home Agent, Foreign Agent
  - Home agent tunnels packets to FA or MN
  - Packets from MN go directly or via HA
- Mobile IPv6
  - Route optimization
  - No need for foreign agents
  - Uses IPv6 functions, neighbor discovery
  - Uses IPv6 header extensions instead of tunneling
- NEMO
  - Solution for network mobility
  - Based on Mobile IPv6
  - A mobile router communicates with a home agent as the network moves
    - A bidirectional tunnel

NAT Traversal

- As mentioned, end-to-end is broken
- Firewalls block and drop traffic
- NATs do address and port translation
  - Hide subnetwork and private IPs
- How to work with NATs
  - Tricky: two NATs between communications
  - NAT and NAPT
  - One part is to detect NATs
  - Another is to get ports open
- IETF efforts
  - STUN
  - ICE
  - TURN
  - NSIS

NAT Features

- NAT provides transparent and bi-directional connectivity between networks having arbitrary addressing schemes
- NAT eliminates costs associated with host renumbering
- NAT conserves IP addresses
- NAT eases IP address management
- Load Balancing
- NAT enhances network privacy
- Address migration through translation
- IP masquerading
- Load balancing

NAT Concerns

- Performance
  - IP address modification, NAT boxes need to recalculate IP header checksum
  - Port number modification requires TCP checksum recalculation
- Fragmentation
  - Fragments should have the same destination
- End-to-end connectivity
  - NAT destroys universal end-to-end reachability
  - NATted hosts are often unreachable

NAT Concerns

- Applications with IP-address content
  - Need AGL (Application Level Gateway)
  - Typically applications that rely on IP addresses in payload do not work across a private-public network boundary
  - Some NATs can translate IP addresses in payload
- NAT device can be a target for attacks
- NAT behaviour is not deterministic
- NATs attempt to be transparent
  - Challenges for network troubleshooting

NAT Traversal

- Challenge: how to allow two natted hosts communicate?
- Straighforward solution: use a relay with a public address that is not natted
  - Connection reversal possible if a node has a public address
    - Relay is a rendezvous point
- More complicated solutions
  - Detect presence of NATs
  - Hole punching

TURN

- IETF MIDCOM draft "Traversal Using Relay NAT (TURN)"
- TURN is a protocol for UDP/TCP relaying behind a NAT
- Unlike STUN there is no hole punching and data are bounced to a public server called the TURN server
- TURN is the last resource. For instance behind a symmetric NAT
- It introduces a relay
  - Located in customers DMZ or Service Provider network
  - Single point of failure
  - Requires a high performance server

STUN

- IETF RFC 3489 "STUN – Simple Traversal of User Datagram Protocol (UDP) Trough Network Address Translators (NATs)"
- A client-server protocol to discover the presence and types of NAT and firewalls between them and the public Internet
- STUN allows applications to determine the public IP addresses allocated to them by the NAT
- Defines the operations and the message format needed to understand the type of NAT
- The STUN server is contacted on UDP port 3478
- The server will hint clients to perform tests on alternate IP and port number too (STUN servers have two IP addresses)
- Revised STUN: "Session Traversal Utilities for NAT"
  - Binding discovery, NAT keep-alives, Short-term password, Relay (previously TURN)

ICE

- IETF MMUSIC draft "Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT)"
- Allows peers to discover NAT types and client capabilities
- Provide alternatives for establishing connectivity, namely STUN and TURN
- Works with all types of NATs, P2P NAT traversal
- Designed for SIP and VoIP. Can be applied to any session-oriented protocol
- The detailed operation of ICE can be broken into six steps: gathering, prioritizing, encoding, offering and answering, checking, and completing.

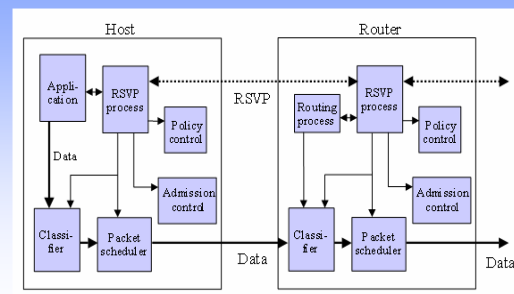
QoS

- By default, there is no QoS support on the Internet
- IP is unreliable, packet types are handled differently (TCP/UDP/ICMP)
- No guarantees on TCP flow priority (OS and NW stack issue)
- IETF work
  - DiffServ, IntServ, NSIS

QoS Architectures for Internet

- Integrated Services (IntServ)
  - Flow Based QoS Model (Resources are available prior to establishing the session)
  - Session by session (end-to-end)
  - Uses RSVP (signaling protocol) to create a flow over a connectionless IP
- Differentiated Services (DiffServ)
  - Categorize traffic into different classes or priorities with high priority value assigned to real time traffic
  - Hop by hop (no assurance of end-to-end QoS)
- Multiprotocol Label Switching (MPLS)
  - Not primarily a QoS model, rather a Switching architecture
  - Ingress to the network decides a label according to FEC

RSVP Architecture

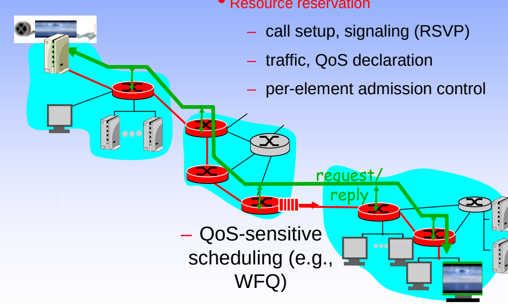


RSVP: Overview of Operation

- senders, receiver join a multicast group
  - done outside of RSVP
  - senders need not join group
- sender-to-network signaling
  - *path message:* make sender presence known to routers
  - path teardown: delete sender's path state from routers
- receiver-to-network signaling
  - *reservation message:* reserve resources from senders to receiver
  - reservation teardown: remove receiver reservations
- network-to-end-system signaling
  - path error, -reservation error

Integrated Services

- Resource reservation
  - call setup, signaling (RSVP)
  - traffic, QoS declaration
  - per-element admission control



  - QoS-sensitive scheduling (e.g., WFQ)

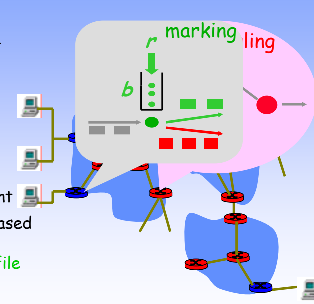
DiffServ: Motivation and Design

- Complex processing is moved from core to edge
- Per flow service (IntServ) is replaced by per aggregate or per class service with an SLA with the provider. (to improve scalability)
- Label packets with a type field
  - e.g. a priority stamp
- Core uses the type field to manage QoS
- Defines an architecture and a set of forwarding behaviors
  - Up to the ISP to define an end-to-end service over this

DiffServ Architecture

Edge router:
- per-flow traffic management
- marks packets as in-profile and out-profile

Core router:
- per class traffic management
- buffering and scheduling based on marking at edge
- preference given to in-profile packets



Security Features

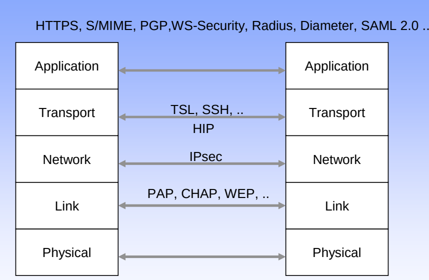
- IPSec provides basic security (tunnel,transport) with IKE
- Solution for autentication, authorization, accounting is needed (AAA)
  - Radius, Diameter
- Case: WLAN access network

AAA

- AAA
  - Authentication, Authorization, Accounting
  - RFC 2903 (Generic AAA Architecture)
  - RFC 2904 (AAA Authorization Framework)
- AAAA
  - AAA and Auditing
- Accounting and billing
  - Accounting is gathering information for billing, balancing, or other purposes
  - Billing is a process to generate a bill for customers based on gathered information

Motivation for AAA

- Service organizations to host multiple organizations requiring dial-in facilities
- User organizations to outsourcing their dial-in service to one or more 3rd parties
- Agreements can be implemented using a standards based protocol (RADIUS)
- RADIUS allows User organizations or Agents to migrate to other Service Providers.
- An agent, using proxy AAA to change its service without affecting the agreement with its customers
- A service organization to have ultimate authority over its users



Radius

- Remote Authentication Dial In User Service (RADIUS) is defined in RFC 2865
- Designed to authenticate dial-in-access customers
  - Used for dial-in lines and 3G networks
- Idea to have a centralized user database for passwords and other user information
  - Cost efficient
  - Easy to configure
- Radius is used together with an authentication protocol such as PAP or CHAP

Radius

- A client-server protocol
  - Network Access Server (NAS) is the client
  - Radius Server is a server
- Security based on previously shared secret
- More than one server can serve a single client
- A server can act as a proxy
- Based on UDP on efficiency reasons
- No keep-alive signaling

Radius Limitations

- Scalability
  - No explicit support for agents, proxies, ..
  - Manual configuration of shared secrets
- Reliability
  - UDP not reliable, accounting info may be lost
- Does not define failover mechanisms
  - Implementation specific
- Mobility support
- Security
  - Applied usually in trusted network segments or VPNs
  - Application layer authentication and integrity only for use with Response packets
  - No per packet confidentiality
- Diameter addresses some of the security issues

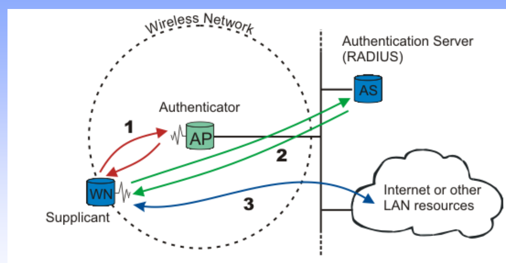
Diameter

- A network protocol for providing AAA services to roaming users
  - Replacement for RADIUS, Kerberos, TACACS+
  - Open base protocol provides transport, message delivery, and error handling services
- Diameter Base Protocol is defined in RFC 3588
- Defines the following facilities
  - Delivery of AVPs (attribute value pairs)
  - Capabilities negotiation
  - Error notification
  - Extensibility through additional new commands and AVPs
  - Basic services necessary for applications
    - Handling of user sessions, Accounting, ..

Diameter

- Uses TCP and SCTP for communications
- Can be secured using IPSEC and TLS
- End-to-end security is recommended but not mandatory
- Based on request-answer signal pairs
- In the Diameter network there can be
  - clients, relays, proxies, and redirect and translation agents

802.1X Security



Source: http://upload.wikimedia.org/wikipedia/commons/6/63/8021X-Overview.png

HIP

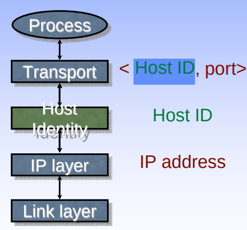
- HIP is a proposal to unify mobility, multi-homing, and security features that are needed by applications
- Identity-based addressing realizing locator-identity split
- Change in the networking stack that is not very visible to applications (no IP addresses though!)
- HIP architecture, HIP implementation for Linux

HIP in a Nutshell

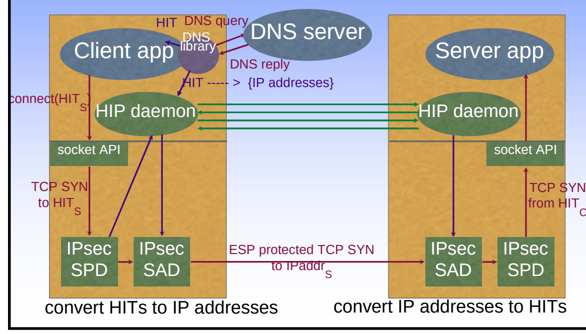
- Architectural change to TCP/IP structure
- Integrates security, mobility, and multi-homing
  - Opportunistic host-to-host IPsec ESP
  - End-host mobility, across IPv4 and IPv6
  - End-host multi-address multi-homing, IPv4/v6
  - IPv4 / v6 interoperability for apps
- A new layer between IP and transport
  - Introduces cryptographic Host Identifiers

The Idea

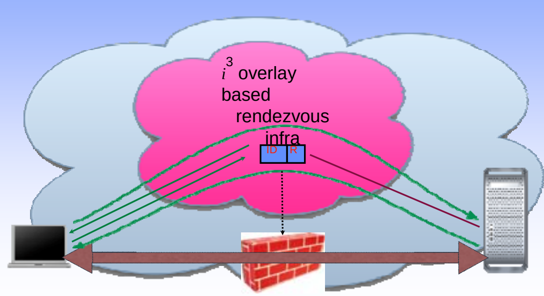
- A new Name Space of Host Identifiers (HI)
  - Public crypto keys!
  - Presented as 128-bit long hash values, Host ID Tags (HIT)
- Sockets bound to HIs, not to IP addresses
- HIs translated to IP addresses in the kernel



Using HIP with ESP



Control/data separation



Services and Identity Management

- Privacy and trust matters a lot
- Services on the Web
- Single sign-on
  - Liberty, OpenID, GAA, ..
- Recent developments

Web applications

- Recent trend has been to develop web applications
  - Traditional applications on Internet (office suites,..)
  - Search (Google, Yahoo, ..)
  - Instant communications and presence
  - Social collaboration and networking sites
  - Data sharing sites and video sharing
  - Data storage services
  - Blogging
- Another recent trend is to simplify signing to services
  - Single Sign-On, federated identity, OpenID
- And creating mashups
  - Combining services in new ways
  - Custom experience and personalization

WS Protocol Stack

Discovery: UDDI

Description: WSDL

XML Messaging: SOAP, XML-RPC, XML

Transport: HTTP, FTP, BEEP, SMTP, JMS

REST

- REST (Representational State Transfer) (Roy Fielding, PhD thesis)
  - Architectural style of networked systems
  - Applications transfer state with each resource representation
    - Representations of the data are transmitted
  - State is a property of a resource
- Resources
  - Any addressable entity
  - Web site, HTML page, XML document, ..
- URLs Identify Resources
  - Every resource uniquely identifiable by a URI

Security and Trust

- We are going towards identity-based service access
  - A number of identities per host
  - Pseudonyms, privacy issues
  - Delegation and federation are needed
- Decentralization: the user has the freedom of choosing who manages identity and data
- Solutions for authentication
  - Web-based standard (top-down)
    - ID-FF
  - Web-based practice (bottom-up)
    - OpenID and oAuth
  - Web services
    - SAML 2.0

Papers on the course web page

- Rethinking the design of the Internet: the end-to-end arguments vs. the brave new world
- On Compact Routing for the Internet authored by Dima Krioukov, kc claffy, Kevin Fall, and Arthur Brady. Published in the ACM SIGCOMM Computer Communication Review (CCR), v.37, n.3, 2007.
- Designing DCCP: Congestion Control Without Reliability (PDF), by Eddie Kohler, Mark Handley, and Sally Floyd. Proc. ACM SIGCOMM 2006.
- IETF Journal article on ICE
- Peer-to-peer Communication Across Network Address Translators
- Amazon's Dynamo. SOSP 2007.
- And many RFCs

Questions and Discussion

Thank You