

Chair for Network Architectures and Services – Prof. Carle
 Department for Computer Science
 TU München

**Master Course
 Computer Networks
 IN2097**

Prof. Dr.-Ing. Georg Carle
 Christian Grothoff, Ph.D.

Chair for Network Architectures and Services
 Institut für Informatik
 Technische Universität München
<http://www.net.in.tum.de>

TUM
 Technische Universität München

Outline

- Project
- Network virtualisation:
 Link virtualization: ATM, MPLS

IN2097 - Master Course Computer Networks, WS 2011/2012 2

Chair for Network Architectures and Services – Prof. Carle
 Department for Computer Science
 TU München

Network Architectures

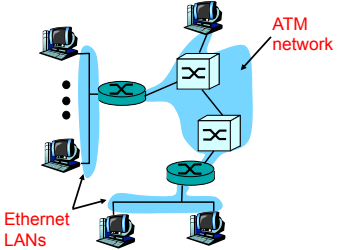
Link virtualization: ATM, MPLS

TUM
 Technische Universität München

IP-Over-ATM

Issues:

- IP datagrams into ATM
 AAL5 PDUs
- from IP addresses to ATM
 addresses
 - just like IP
 addresses to 802.3
 MAC addresses
 - ARP server



The diagram illustrates a network architecture where multiple Ethernet LANs (represented by computer icons) are connected to a central ATM network. The connection is facilitated by several routers (represented by square icons with 'X' symbols). Red arrows point from the text labels 'Ethernet LANs' and 'ATM network' to their respective parts in the diagram.

IN2097 - Master Course Computer Networks, WS 2011/2012 4

AAL 5 Protocol

- AAL5 is a simple and efficient AAL (SEAL) to perform a subset of the functions of AAL3/4
- The CPCS-PDU payload length can be up to 65,535 octets and must use PAD (0 to 47 octets) to align CPCS-PDU length to a multiple of 48 octets

PAD Padding
 CPCS-UU CPCS User-to-User Indicator
 CPI Common Part Indicator
 Length CPCS-PDU Payload Length
 CRC-32 Cyclic Redundancy Check

	0 - 47	1	1	2	4
CPCS-PDU Payload	PAD	CPCS UU	CPI	Length	CRC-32

IN2097 - Master Course Computer Networks, WS 2011/2012 5

AAL 5 Layering

The diagram illustrates the layering of AAL 5. It shows five layers from top to bottom: Higher layer, Service specific convergence sublayer, Common part convergence sublayer, SAR sublayer, and ATM layer. In the Higher layer, a box labeled 'Information' is shown. In the Service specific convergence sublayer, a dashed line indicates the flow of information, with the note 'Assume null'. In the Common part convergence sublayer, the 'Information' box is followed by 'PAD' and 'T' boxes. In the SAR sublayer, the information is segmented into three 48-octet blocks. The first two blocks are labeled '48 (0)' and the third is '48 (1)'. In the ATM layer, these segments are shown as ATM cells. The first two cells have PTI = 0 and the third has PTI = 1.

IN2097 - Master Course Computer Networks, WS 2011/2012 6

Classical IP and ARP over ATM (CLIP)

- Specification of a complete IP implementation for ATM
- Suitable for ATM unicast communication
- Encapsulation of IP packets into AAL PDUs
- Support for large MTU sizes
- There must be an ATMARP server in each LIS (Logical IP Subnet)

ARP Server	
ATM	IP
3333	131.188.78.40
3320	131.188.78.41

IN2097 - Master Course Computer Networks, WS 2011/2012 7

Classical IP and ARP over ATM (CLIP)

- The host registers its IP/ATM address information at the ATMARP server using the InARP protocol

The diagram shows the InARP protocol sequence. A Host (IP: 131.188.78.40, ATM: 2001) sends a 'SETUP (ATM=2998)' message to an ATM Switch. The ATM Switch forwards a 'SETUP' message to an ARP Server (IP: 131.188.78.9, ATM: 2998). The ARP Server responds with a 'CONNECT ACK' message to the ATM Switch, which then forwards a 'CONNECT' message to the Host.

The InARP-REQUEST and InARP-RESPONSE messages are shown as follows:

```

InARP-REQUEST:
  source IP: 131.188.78.9, ATM: 2998
  target IP: ATM:

InARP-RESPONSE:
  source IP: 131.188.78.40, ATM: 2001
  target IP: 131.188.78.9, ATM: 2998
  
```

IN2097 - Master Course Computer Networks, WS 2011/2012 8

Classical IP and ARP over ATM (CLIP)

- RFC 1577: Classical IP and ARP over ATM
- ATMARP Server Operational Requirements
 - The ATMARP server, upon the completion of an ATM call/ connection of a new VC, will transmit an InATMARP request to determine the IP address of the client.
 - The InATMARP reply from the client contains the information necessary for the ATMARP Server to build its ATMARP table cache.
 - This information is used to generate replies to the ATMARP requests it receives.
- InATMARP is the same protocol as the original InARP protocol presented in RFC 1293 but applied to ATM networks: Discover the protocol address of a station associated with a virtual circuit.
- RFC 1293: Bradely, T., and C. Brown, "Inverse Address Resolution Protocol", January 1992.

IN2097 - Master Course Computer Networks, WS 2011/2012 9

Classical IP and ARP over ATM (CLIP)

- RFC 1577: Classical IP and ARP over ATM
- ATMARP Client Operational Requirements
 1. Initiate the VC connection to the ATMARP server for transmitting and receiving ATMARP and InATMARP packets.
 2. Respond to ARP_REQUEST and InARP_REQUEST packets received on any VC appropriately.
 3. Generate and transmit ARP_REQUEST packets to the ATMARP server and to process ARP_REPLY appropriately. ARP_REPLY packets should be used to build/refresh its own client ATMARP table entries.
 4. Generate and transmit InARP_REQUEST packets as needed and to process InARP_REPLY packets appropriately. InARP_REPLY packets should be used to build/refresh its own client ATMARP table entries.
 5. Provide an ATMARP table aging function to remove own old client ATMARP tables entries after a period of time.

IN2097 - Master Course Computer Networks, WS 2011/2012 10

Chair for Network Architectures and Services – Prof. Carle
Department for Computer Science
TU München

MPLS
Multi-Protocol Label Switching

TUM
Technische Universität München

Multiprotocol label switching (MPLS)

- Initial goal: speed up IP forwarding by using fixed length label (instead of IP address) to do forwarding
 - borrowing ideas from Virtual Circuit (VC) approach
 - IP datagram still keeps IP address
 - RFC 3032 defines MPLS header
 - Label: has role of Virtual Circuit Identifier
 - Exp: experimental usage, may specify Class of Service (CoS)
 - S: Bottom of Stack - end of series of stacked headers
 - TTL: time to live

PPP or Ethernet header	MPLS header	IP header	remainder of link-layer frame
------------------------	--------------------	-----------	-------------------------------

label	Exp.	S	TTL
20	3	1	5 bit

IN2097 - Master Course Computer Networks, WS 2011/2012 12

MPLS capable routers

- a.k.a. label-switched router
- forwards packets to outgoing interface based only on label value (don't inspect IP address)
 - MPLS forwarding table distinct from IP forwarding tables
- signaling protocol needed to set up forwarding
 - Label Distribution Protocol LDP (RFC 3036 → obsolete by RFC 5036)
 - RSVP-TE (RFC 3209 → updated by RFCs 3936, 4420, 4874, 5151, 5420, 5711)
- forwarding possible along paths that IP alone would not allow (e.g., source-specific routing)
- MPLS supports traffic engineering
- must co-exist with IP-only routers

IN2097 - Master Course Computer Networks, WS 2011/2012 13

MPLS forwarding tables

IN2097 - Master Course Computer Networks, WS 2011/2012 14

MPLS

- Label Switched Path (LSP)
 - set up by signalling protocol
 - has sequence of labels
- Forwarding Equivalence Class (FEC)
 - specification of packets treated the same way by a router
 - forwarded over same LSP
 - can be specified by destination prefix, e.g. FEC 10.1.1.0/24
- Label Switching Router
 - MPLS-capable IP router; may bind labels to FEC
- MPLS node
 - does not need IP stack
- stacked labels
 - label push; label pop

Layer2 Header | Top Label | ... | Bottom Label | Layer3 Header

IN2097 - Master Course Computer Networks, WS 2011/2012 15

Benefits of MPLS

- High Speed Switching
 - facilitates construction of nodes with wire-line speed
- Simplifying packet forwarding
 - Routing decision can be limited to edge of AS
- Traffic Engineering
 - MPLS may control paths taken by different flows, e.g. to avoid congestion points for certain flows
- Quality of Service (QoS) support
 - resources may be specified for specific flows, isolation among flows
- Network scalability
 - label stacking allows to arrange MPLS domains in a hierarchy
- Supporting VPNs
 - tunneling of packets from an ingress point to an egress point

IN2097 - Master Course Computer Networks, WS 2011/2012 16

Forwarding Equivalence Class Routing

Route chosen by Unicast IP routing protocol for FEC#1

Explicit Route specified by Traffic Engineering for FEC#2

No packet classification at the core LSRs

FEC to label mapping at ingress LERs

IN2097 - Master Course Computer Networks, WS 2011/2012 17

MPLS Flexibility

Label semantics

- Fine or coarse grained
- Unicast or multicast
- Explicit or implicit route
- VPN identifier

⇒ Loose semantics create flexible control

IN2097 - Master Course Computer Networks, WS 2011/2012 18

Traffic Engineering

□ Traffic engineering: process of mapping traffic demand onto a network

Demand

Network Topology

□ Purpose of traffic engineering:

- Maximize utilization of links and nodes throughout the network
- Engineer links to achieve required delay, grade-of-service
- Spread network traffic across network links, reduce impact of failure
- Ensure available spare link capacity for re-routing traffic on failure
- Meet policy requirements imposed by the network operator

⇒ Traffic engineering key to optimizing cost/performance

IN2097 - Master Course Computer Networks, WS 2011/2012 19

Chair for Network Architectures and Services – Prof. Carle
Department for Computer Science
TU München

Virtual Private Networks

TUM
Technische Universität München

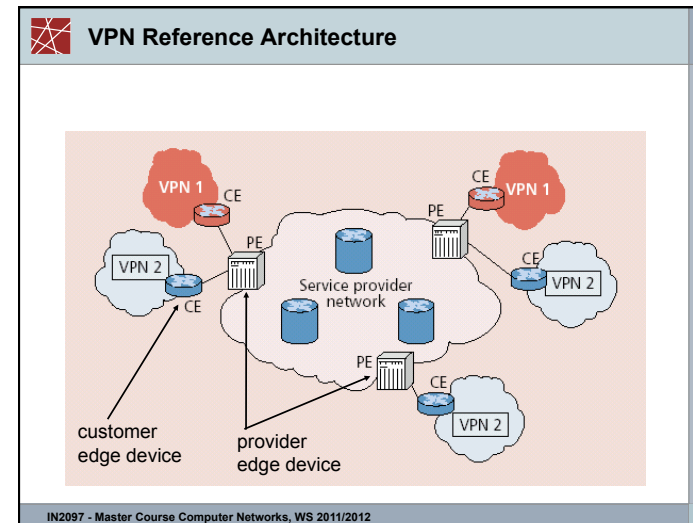
Virtual Private Networks (VPN)

VPNs

Networks perceived as being private networks by customers using them, but built over shared infrastructure owned by service provider (SP)

- Service provider infrastructure:
 - backbone
 - provider edge devices
- Customer:
 - customer edge devices (communicating over shared backbone)

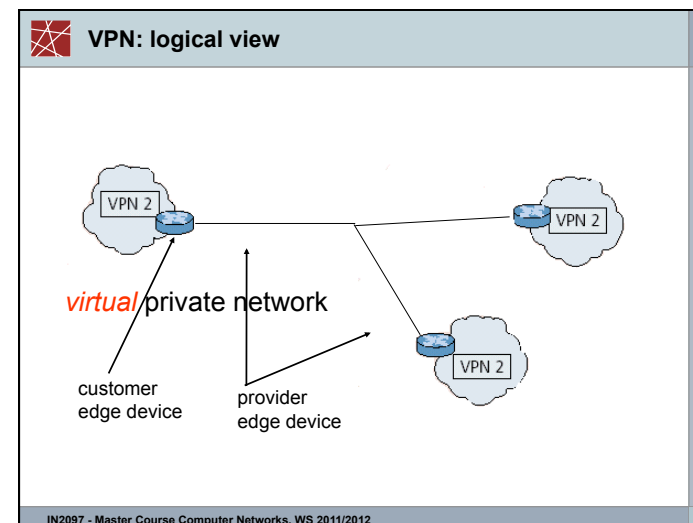
IN2097 - Master Course Computer Networks, WS 2011/2012 21



VPNs: Why?

- Privacy
- Security
- Works well with mobility (looks like you are always at home)
- Cost
 - many forms of newer VPNs are cheaper than leased line VPNs
 - ability to share at lower layers even though logically separate means lower cost
 - exploit multiple paths, redundancy, fault-recovery in lower layers
 - need isolation mechanisms to ensure resources shared appropriately
- Abstraction and manageability
 - all machines with addresses that are "in" are trusted no matter where they are

IN2097 - Master Course Computer Networks, WS 2011/2012 23



Leased-Line VPN

customer sites interconnected via static virtual channels (e.g., ATM VCs), leased lines

customer site connects to provider edge

IN2097 - Master Course Computer Networks, WS 2011/2012 25

Customer Premise VPN

- all VPN functions implemented by customer

customer sites interconnected via tunnels

- tunnels typically encrypted
- Service provider treats VPN packets like all other packets

IN2097 - Master Course Computer Networks, WS 2011/2012 26

Variants of VPNs

- Leased-line VPN
 - configuration costs and maintenance by service provider: long time to set up, manpower
- CPE-based VPN
 - expertise by customer to acquire, configure, manage VPN
- Network-based VPN
 - Customer routers connect to service provider routers
 - Service provider routers maintain separate (independent) IP contexts for each VPN
 - sites can use private addressing
 - traffic from one VPN cannot be injected into another

IN2097 - Master Course Computer Networks, WS 2011/2012 27

Network-based Layer 3 VPNs

Tunnel encapsulation/de-capsulation performed in provider edge equipment

Normal IP access to PE CEs are not tunneling

multiple virtual routers in single provider edge device

IN2097 - Master Course Computer Networks, WS 2011/2012 28

