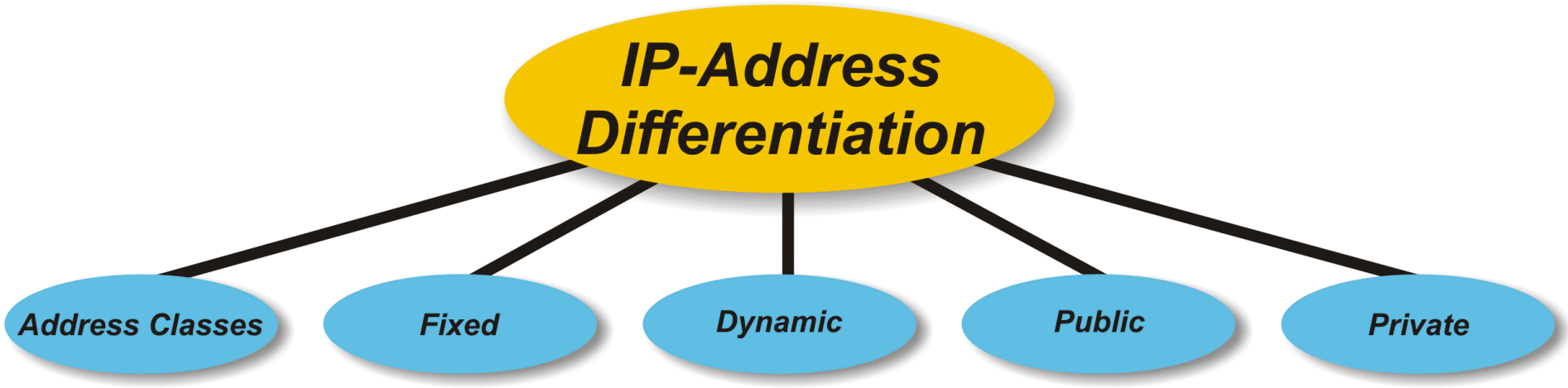
Details of the Internet Protocol

- **IP-Addresses**



© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

Details of the Internet Protocol

IP-Addresses

One of the key issues of the internet protocol are the 32 bit long IP-addresses. The IP-address shall identify any given user of the internet uniquely at any given moment in time. Due to the enormous growth of the internet community, IP-addresses are becoming a scarce resource. Special features have been put in place to make more efficient use of the available IP-address range. IP-addresses can be distinguished by the following means:

- **Address Classes**
  Already at the very beginning of the internet, five different address classes (A, B, C, D, E) were defined which imposed a hierarchical and unfortunately uneconomic structure upon all internet addressing. The ICANN (Internet Corporation for Assigned Names and Numbers) is now in charge for allocating IP-addresses to individuals and organizations. Please note that ICANN replaced IANA (Internet Assigned Number Authority) in 1999.

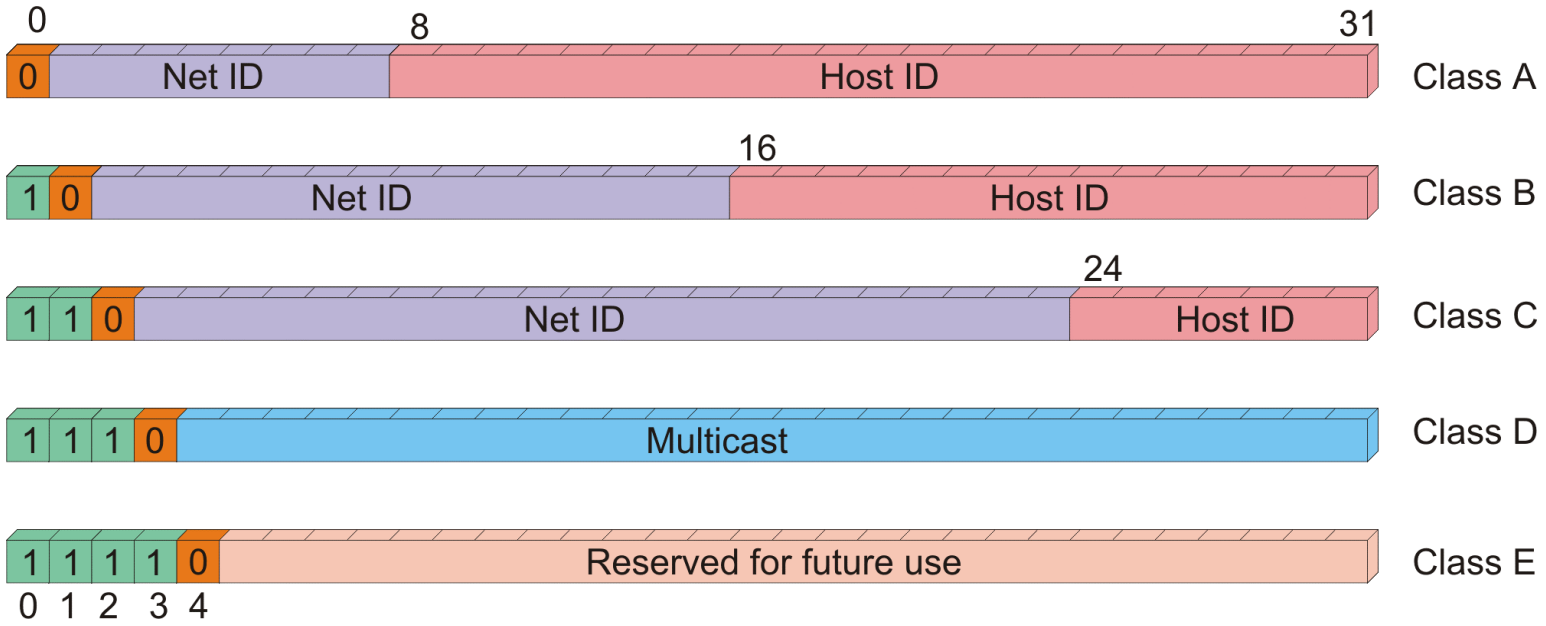
- **Fixed / Dynamic**
  Any IP-address is either fixed or dynamic. In the “fixed” case, each user has at least one IP-address which cannot be used by anybody else even when this user has switched off the computer. Opposed to that, when dynamic addressing is used, any user of a system will obtain another IP-address any time the host computer is switched on. Switching off the computer also means to return the IP-address, used, and therefore making it available again to another user. We will later get back to the issue of dynamic IP-addressing.

- **Public / Private**
  Yet another means to distinguish IP-addresses is to have either public or private IP-addresses. Private IP-addresses are unique only and exclusively in the very network where they are used. However, such an IP-address cannot be used for communication purposes towards hosts or servers outside this network. Special means are required to allow such users access to services outside the local network.
  Opposed to that, public IP-addresses are unique worldwide and can be used for any access to services inside and outside the local network. We will later see more details about private and public IP-addressing.

In this context we will focus on the 32 bit long IPv4-addresses. In addition, the IETF and major industry leaders are preparing the roll-out of IPv6 [RFC 1883], also referred to as IPnG (⇔ for next generation). IPv6 comes with the major advantage of using IP-addresses with a length of 128 bit compared to 32 bit in IPv4.

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

IP-Address Classes



© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

IP-Address Classes

The IANA-classification of IP-addresses is illustrated in the figure. Most importantly, a Net ID for the identification of the network and a Host ID for the identification of a single host within the network is introduced. Note that a network administrator usually does not have to contact the ICANN directly to obtain IP-addresses. The network administrator will rather access one of the larger ISP's (Internet Service Provider) to obtain an address range.

Whoever has been allocated IP-address ranges from ICANN can be tracked back through a special web service at: http://www.ripe.net/perl/whois??

Dotted Decimal Notation: IP-Addresses are 32 bit long. However, for better human readability an IP-address is divided into four 8 bit long tuples, which are presented decimal (e.g. 128.128.17.98)

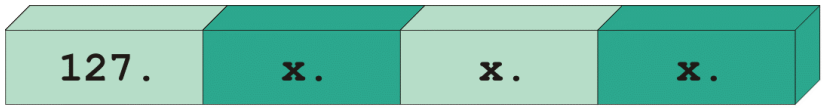
- **Class A – Addresses / Range: (1.0.0.0) – (126.0.0.0) *)**
  There are only a few class A-networks available (e.g. AT&T = 12.0.0.0 / IBM = 9.0.0.0). This is due to the reason that class A-addresses offer 2^{24} – 2 different Host ID's but only 126 different Net ID's.
- **Class B – Addresses / Range: (128.1.0.0) – (191.255.0.0) *)**
  Class B – Addresses allow for 16383 different Net ID's of which any network can support up to 65534 (⇔ 2^{16} – 2) different Host ID's.
- **Class C – Addresses / Range: (192.0.1.0) – (223.255.255.0) *)**
  Class C – Addresses allow for 2,097,151 different Net ID's of which any network can support up to 254 (⇔ 2^{8} – 2) different Host ID's.
- **Class D – Addresses / Range: (224.0.0.0) – (239.255.255.255) *)**
  Class D-Addresses are reserved for multicast applications which provide services for special groups of users or send messages to special users (e.g. send an ICMP-message to all routers on a network (⇔ 224.0.0.2).
- **Class E – Addresses / Range: (240.0.0.0) – (255.255.255.254) *)**
  The Class E – Address Range still remains reserved for future and experimental use.

*) Some addresses are reserved for special purposes

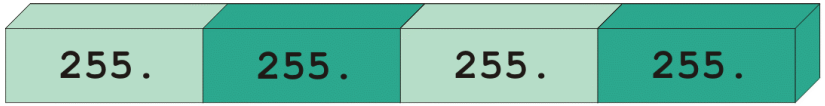
[RFC 1340 / Assigned Numbers]

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

Special IP-Address Notations

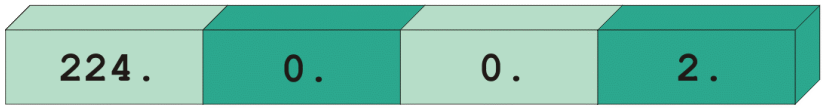


↔ Local Host



↔ Broadcast on Local Network

↔ Broadcast for all Hosts on Net ID



↔ Multicast to all Routers on Network

↔ Identification of a Network (e.g. in Figure)

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

Special IP-Address Notations

When a host is booted and for broadcast applications there are special IP-addresses which are explained underneath:

- **This Host**
  When a host uses the notation 127.X.X.X it relates to the own IP-module. This feature is important for test purposes.
- **Broadcast on local Network**
  To send a broadcast to all IP-modules on the local network, a host will use the 255.255.255.255 notation.
- **Broadcast to all Hosts on Net ID**
  To send a broadcast only to hosts on a certain Net ID, the notation {Net ID ; Host ID = '111 …1'} shall be used.
- **Multicast to all Routers on Network**
  When a host is booted it needs to find out the IP-addresses (and HW-addresses) of the available routers on this network. This is initiated by the host sending a multicast ICMP-message (Router Solicitation) to all routers on this network.
- **Identification of a Network (e.g. in Figures)**
  If a certain physical network shall be identified, then only the Net ID is specified while the Host ID is set to all '0'.

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

Practical Exercise:

- **The following hex-recording illustrates an embedded IP-frame. The highlighted portion contains the source and destination IP-addresses. Please decode to decimal dotted notation.**

```
0000  20 53 52 43 00 00 44 45 53 54 00 00 08 00 45 00    SRC..DEST....E.
0010  00 49 ae 00 00 00 80 11 53 af 95 e1 72 99 c1 65    .I......S...r..e
0020  6f 14 04 08 00 35 00 35 1a 65 00 03 01 00 00 01    o....5.5.e......
0030  00 00 00 00 00 00 02 32 30 03 31 31 31 03 31 30    .......20.111.10
0040  31 03 31 39 33 07 69 6e 2d 61 64 64 72 04 61 72    1.193.in-addr.ar
0050  70 61 00 00 0c 00 01                               pa.....
```

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

UDP-Pseudo Header and UDP-Checksum

As the figure illustrates, the UDP-checksum does not only protect the UDP-header and the UDP-data part. It rather also considers part of the IP-header. This is achieved through the definition of a 12 octet long UDP-pseudo header which consists of:

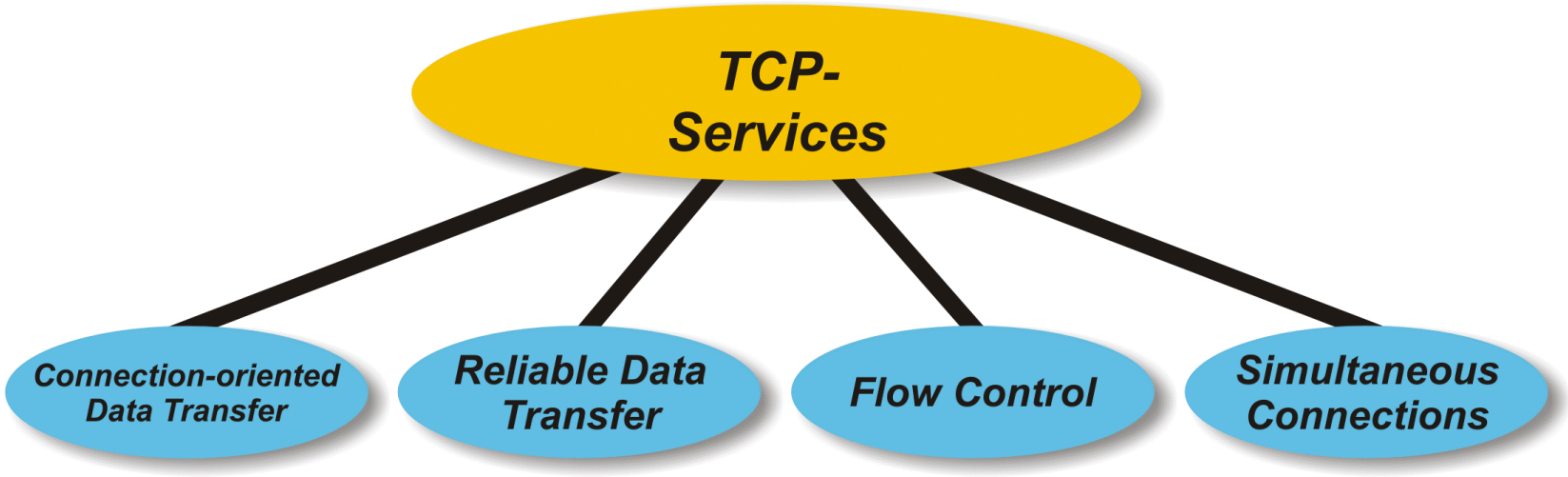
⇒ The source and destination IP-addresses (2 x 32 bit)
⇒ One octet which is fixed coded to '0'
⇒ The IP-header Protocol field (8 bit)
⇒ The length of the UDP-frame (UDP-header + UDP-data) (16 bit)

This UDP-pseudo header is binary added to the "real" UDP header and the UDP-data portion. The result is fed into the checksum field within the UDP-header. Please note that the final padding octet ('0') is only required and appended, if the data field contains an odd number of octets (the checksum algorithm is tailored to 16 bit words.

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

Details of the Transmission Control Protocol (TCP)

- **Services of TCP**



© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited
and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

Details of the Transmission Control Protocol (TCP)

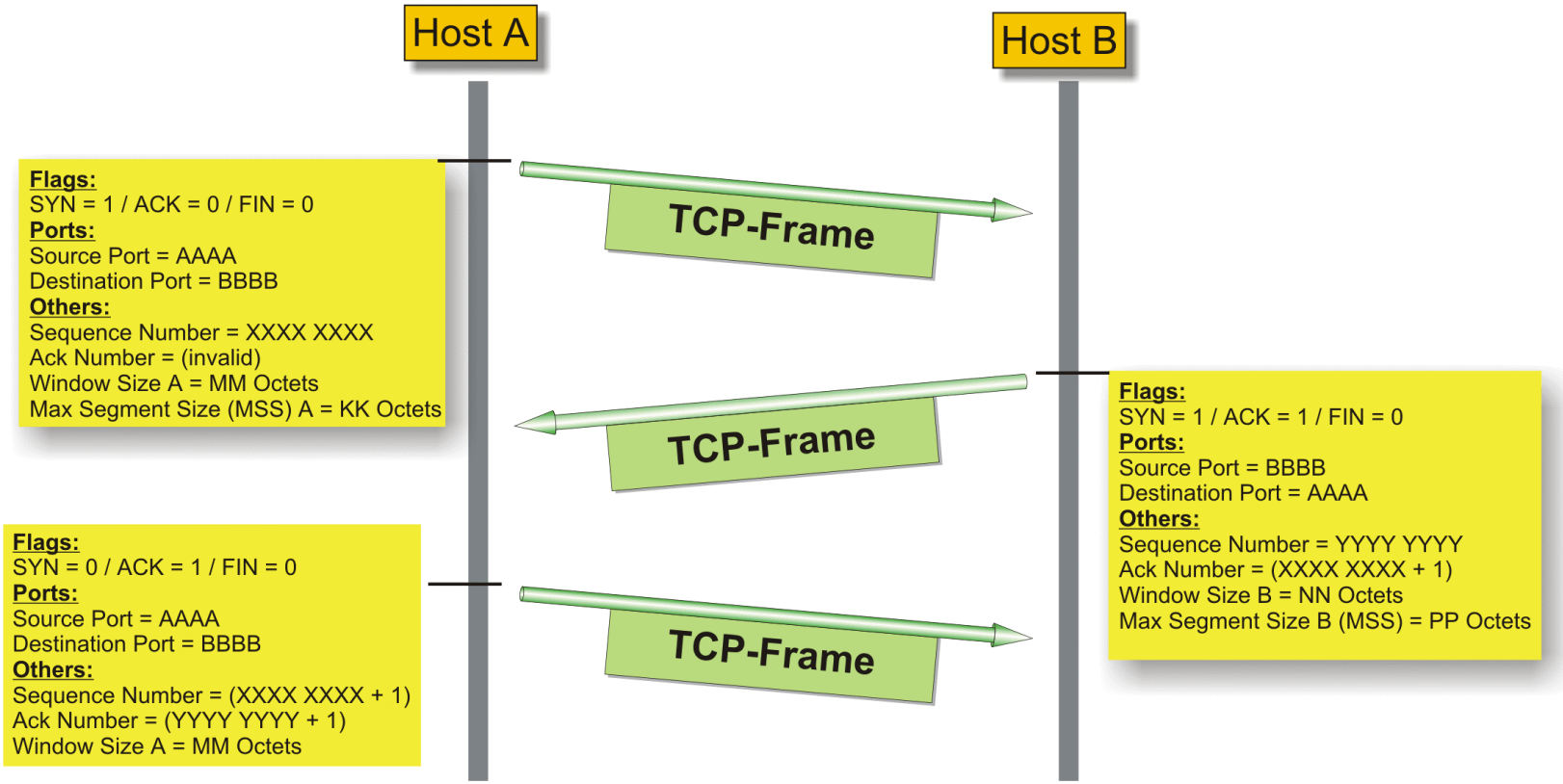
Services of TCP
Like UDP, the Transmission Control Protocol is using the network services of IP. And like UDP, a TCP-Frame is embedded into an IP-frame.

- **Connection-oriented Data Transfer**
  Unlike UDP, TCP is a connection-oriented protocol. Before data transmission can occur, the two peers need to establish a connection which also uses the combination of IP-address and port on each side to uniquely identify a connection. This combination of IP-address and TCP-port is also called a socket. Note that these sockets provide for end-to-end connections between two hosts, probably over various intermediate networks.
- **Reliable Data Transfer**
  Every octet which is transferred using the TCP is uniquely numbered within a sliding window. If data is missing or is garbled, TCP will ask for the retransmission of the respective TCP-frame. Also, if frames arrive out of sequence, TCP is prepared to realign those frames.
- **Flow Control**
  TCP-connections can span over many networks. In addition, a fast sender may be connected to a slower receiver or a connection may be running across a slow intermediate network. TCP is suited to cope with these conditions and to dynamically adapt to changing network load.
- **Simultaneous Connections**
  Since each connection is identified by the two pairs IP-address / Port Number, TCP is enabled to multiplex various simultaneous connections.

[RFC 792]

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

TCP Connection Establishment



© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

TCP Connection Establishment

First, we like to illustrate the TCP connection establishment process, which is also called the “three way handshake”.

- **Step 1 (Active Open)**
  In this first step, host A triggers the connection establishment to host B / destination port BBBB by:
  ⇒ Selecting an Initial Sequence Number (ISN) (⇔ XXXX XXXX).

  The ISN is selected by the TCP-implementation in host A and depends usually on the time since host A has rebooted. RFC 793 defines the ISN as a counter that is initialized to ‘1’ upon reboot and that is incremented every 4 µs.

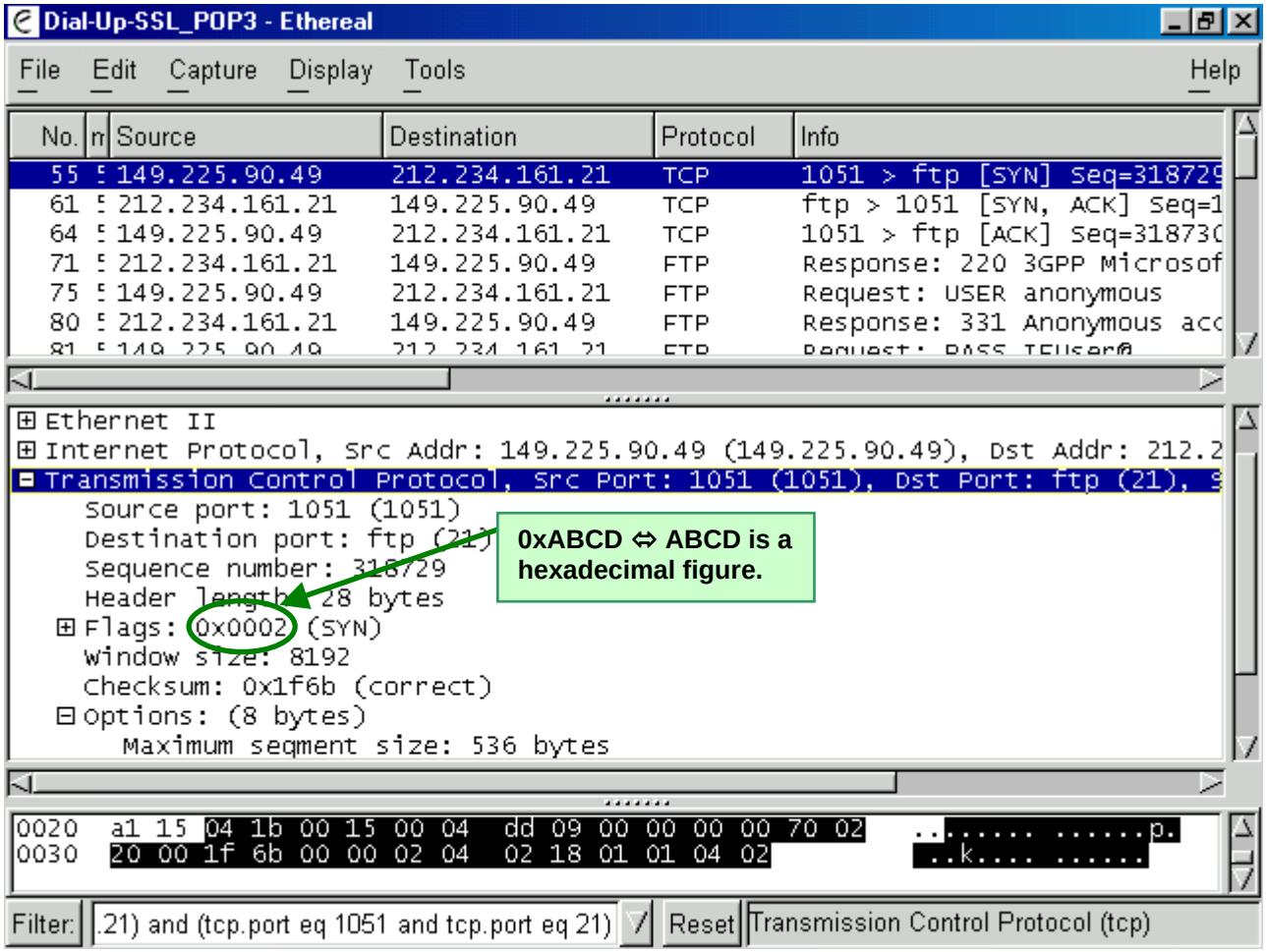
  ⇒ Assigning a source port number (⇔ AAAA) to the upcoming connection and selecting the destination port number which is usually a well known port number.
  ⇒ Setting the window size to a value which is appropriate for host A (⇔ Window Size A = MM). The window size depends on the buffer size of host A. That is, how many octets of data is host A prepared to receive for that connection from host B.
  ⇒ Possibly including the MSS-option (Maximum Segment Size) to indicate the maximum length of a single TCP-frame that host A is prepared to receive from host B.
  ⇒ Setting only the <SYN>-Flag (⇔ SYNchronize Sequence Numbers), forwarding the TCP-frame to IP for transmission and waiting for response.

- **Step 2 (Passive Open)**
  Host B will evaluate the establishment request from host A and will respond by sending another <SYN>-segment back to host A. Like host A, host B will indicate its own window size (⇔ Window Size B = NN) and host B will select its ISN (YYYY YYYY). In addition, host B will set the <ACK>-flag to acknowledge the reception of host A’s first TCP-frame. Accordingly, the Acknowledgement Number is valid and points to the next sequence number / octet that host B expects to receive from host A (⇔ Ack Number = XXXX XXXX + 1).

- **Step 3 (Confirm Connection Establishment)**
  The connection establishment is confirmed by host A sending another TCP-frame to host B. The sequence number is now (XXXX XXXX + 1). This frame also acknowledges the reception of host B’s passive open by setting the <ACK>-flag (⇔ Ack number = YYYY YYYY + 1).

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

(1) Example for TCP Connection Establishment



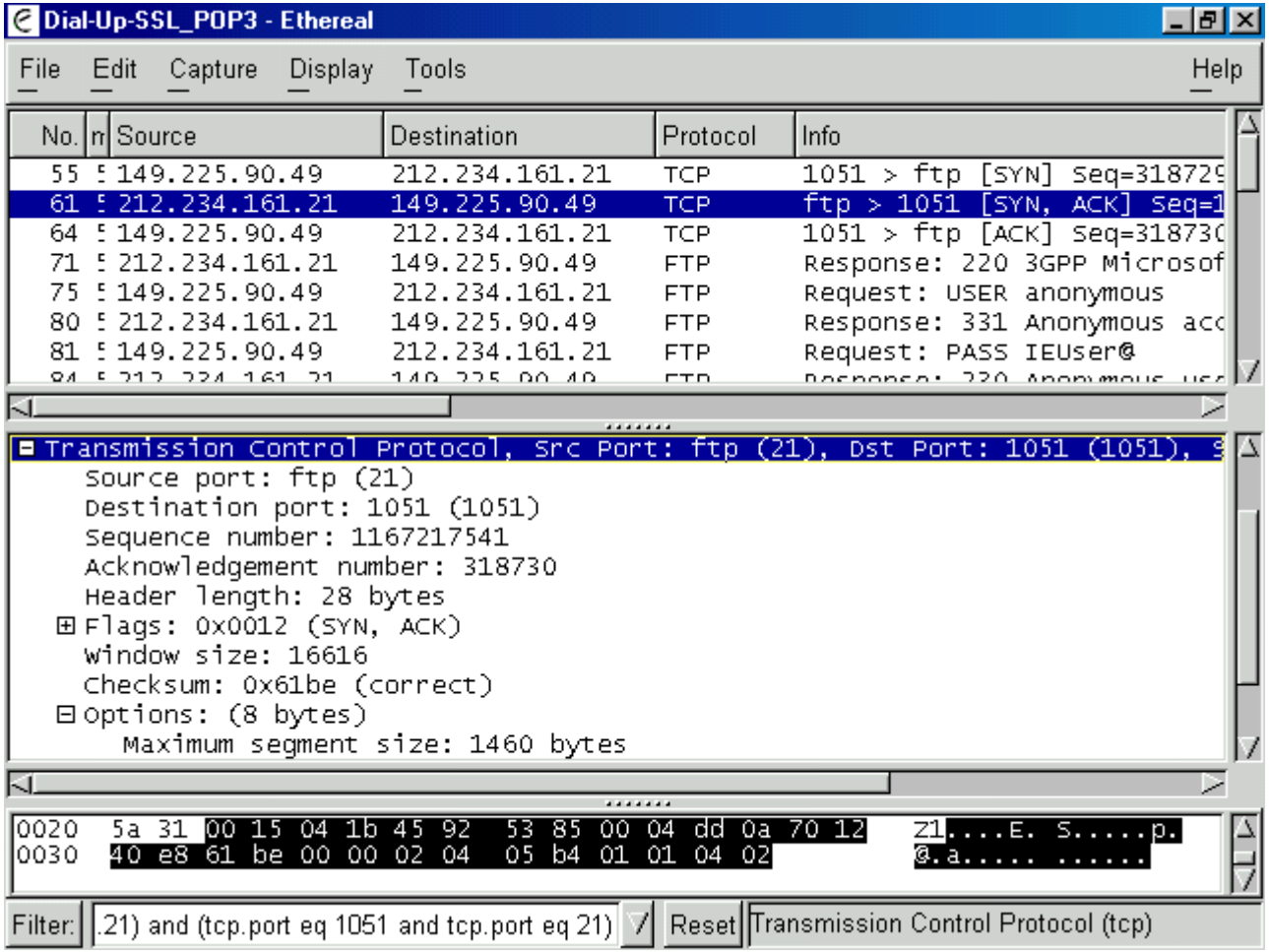
© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

(1) Example for TCP Connection Establishment

- **The figure illustrates the initial “active open” TCP-frame which is sent from host A to host B.**
  - ⇒ The application has selected the “free” port number $1{,}051_{dec}$ for this connection
  - ⇒ Note that the <SYN>-flag is set to indicate connection establishment
  - ⇒ The destination port number is the well known port number 21_{dec} (FTP)
  - ⇒ The ISN is selected with $318{,}729_{dec}$
  - ⇒ The window size is set to $8{,}192_{dec}$
  - ⇒ Host A is prepared to receive segments up to 536_{dec} octets (⇔ default size)

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

(2) Example for TCP Connection Establishment



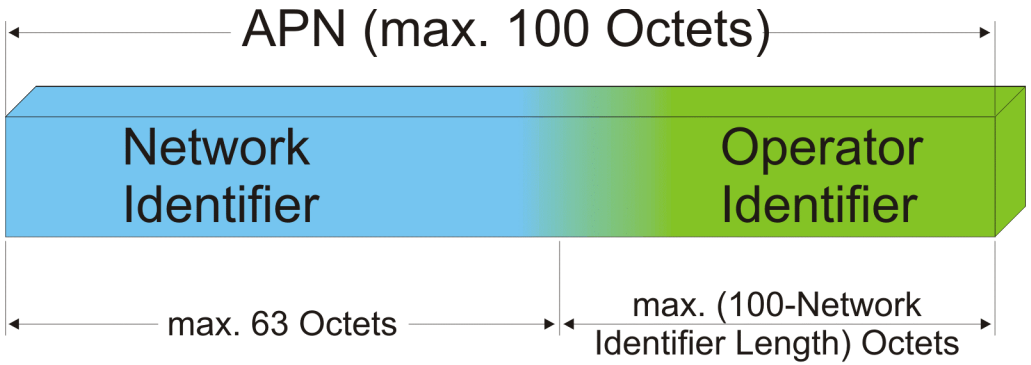
© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

(2) Example for TCP Connection Establishment

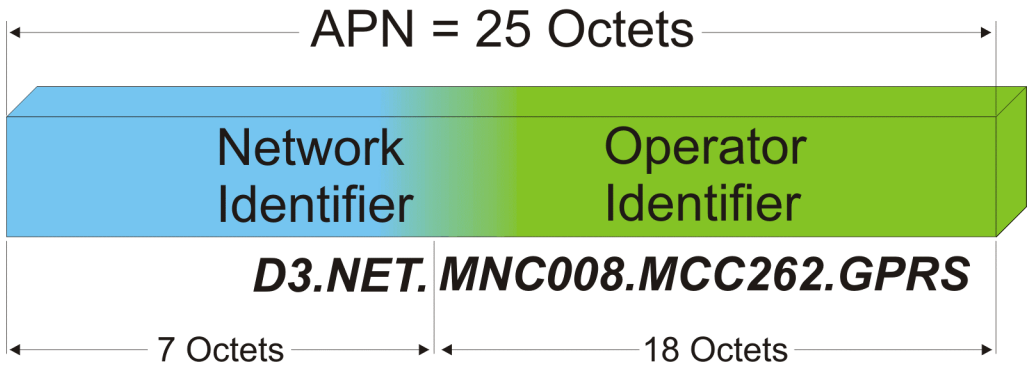
- **The figure illustrates the “passive open” TCP-frame which is sent as response from host B to host A.**
  - ⇒ The <SYN>- and the <ACK>-flag is set.
  - ⇒ The ISN is selected with $1{,}167{,}217{,}541_{dec}$
  - ⇒ Note that host B acknowledges the reception of the active open TCP-frame by pointing to the next expected octet number: $318{,}730_{dec}$.
  - ⇒ The window size is set to $16{,}616_{dec}$
  - ⇒ Host B is prepared to receive segments up to $1{,}460_{dec}$ octets

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

The Access Point Name (APN)



Example:



© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

The Access Point Name (APN)

The APN or Access Point Name is part of the GPRS subscription data which is stored in the HLR and which is transferred to the SGSN upon the activation of a GMM-context. The APN consists of the network identifier and the operator identifier as illustrated in the figure.
When transmitting the ACT_PDP_CT_REQ-message the mobile station may include a specific APN which is used by the SGSN to select a certain GGSN that is capable to provide access to this service.

In general, the APN is used to distinguish between the possibly different services (e.g. WAP, VPN-access, “normal” IP) within one packet data protocol (PDP) that a mobile subscriber is allowed to access.

The APN is split into two parts:

The Network Identifier

If the mobile station includes an APN into the ACT_PDP_CT_REQ-message then the provision of the network identifier (max. 63 octets) is mandatory. Typical examples for network identifier APN are: D3.NET, WAP.E3.NET, UUDIAL.NET. As such, the network identifier portion of the APN consists of one or more labels which are separated through dots. If more than one label is included the network identifier should refer to an internet domain name [2GTS 03.03 / 9.1.1].

The Operator Identifier

The provision of the operator identifier portion (max. 100 – (Length of Network Identifier) octets) of the APN during PDP-context activation is optional. The operator identifier is only important in inter-PLMN roaming situations, that is, when an SGSN in a V-PLMN needs to resolve the network identifier portion of the APN to a GGSN in the H-PLMN of the roaming subscriber. Even in this case, the provision of the operator identifier portion of the APN is not required since it can be derived by the SGSN from the IMSI of that subscriber. The format of the default operator identifier portion of the APN is MNC”mnc”.MCC”mcc”.GPRS.
Example: MNC008.MCC262.GPRS.

Legal characters for the notation of the APN are: (0 – 9), (a – z), (A – Z) and “-“. The APN is not case sensitive.

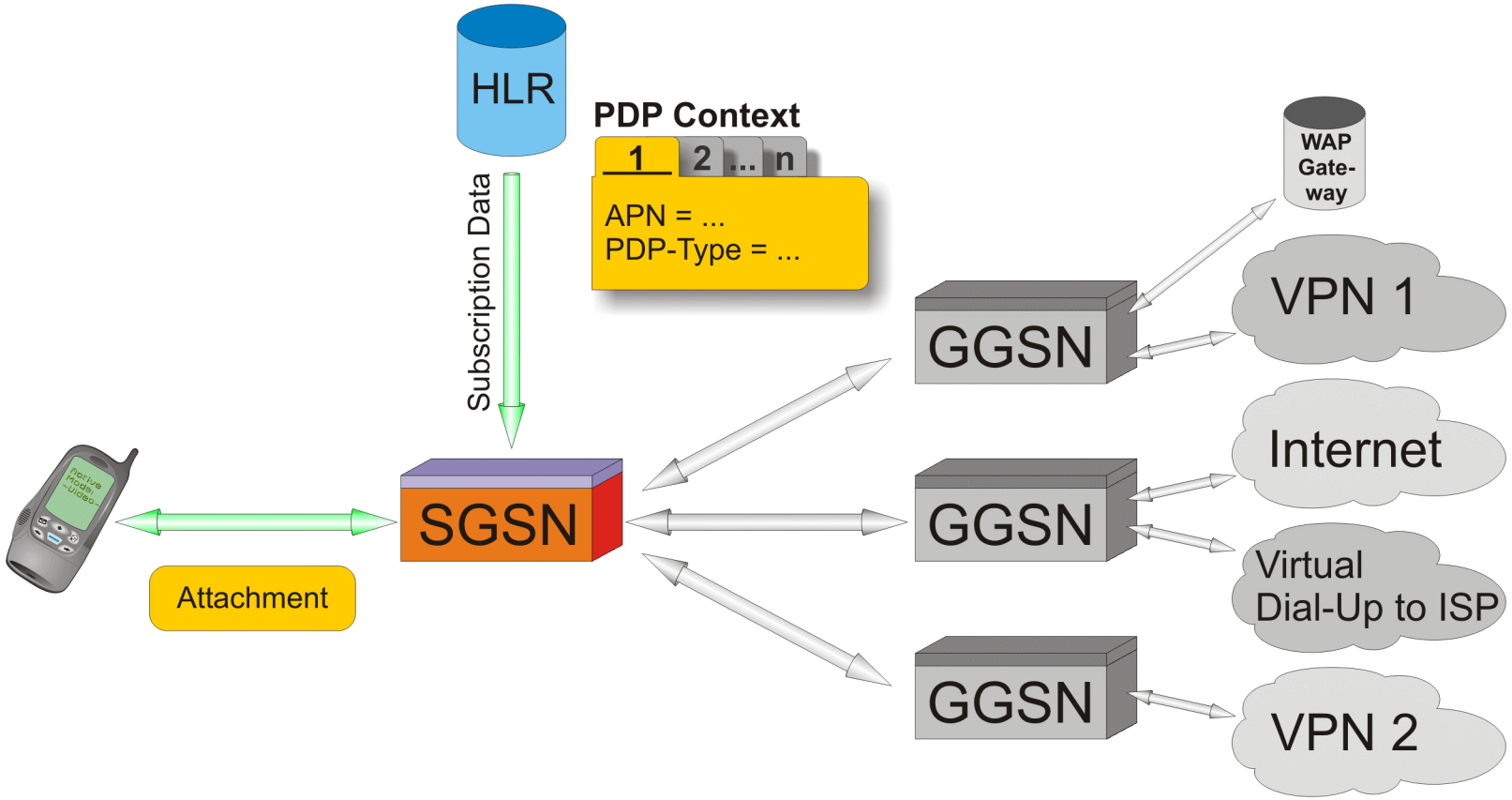
In the HLR the subscription data of a PDP-context of a given subscriber may also contain the wildcard APN. The wildcard APN is encoded as one asterisks (⇔ “*”). It means that a subscriber is authorized to access any network of a certain PDP-type. No restrictions apply.

[2GTS 03.03, 2GTS 03.60]

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

(1) Meaning of the APN during PDP-Context Activation

- **GPRS-Attachment**



© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

(1) Meaning of the APN during PDP-Context Activation

GPRS-Attachment

The figure illustrates part of a GPRS network with three different GGSN's and a mobile station which accesses this network through a given SGSN. The three GGSN's differ in their capability to provide access to different external PDN's.

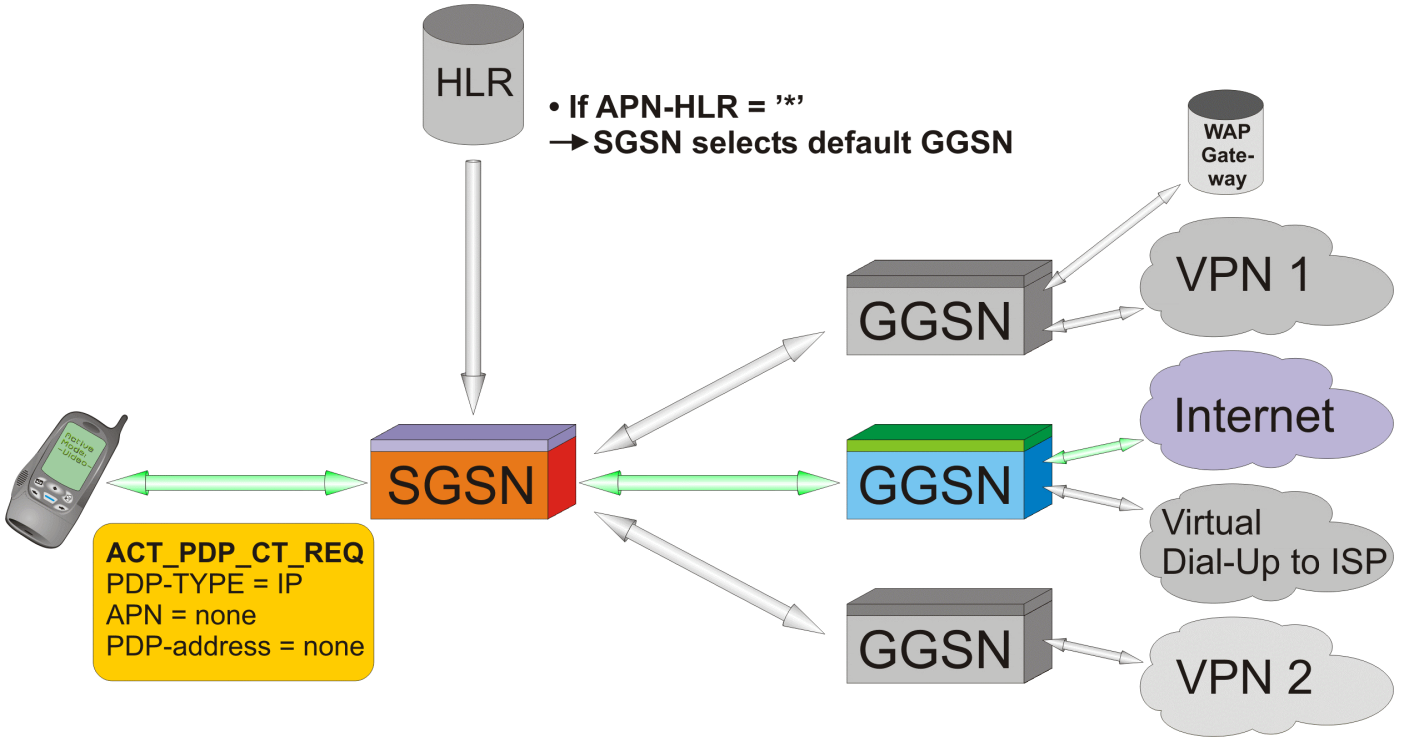
⇒ The GGSN at the top is connected to the WAP-gateway plus it has access to VPN 1(⇔ Volume customer 1).
⇒ The GGSN in the middle provides basic access to the internet plus it is connected to an ISP (e.g. via the L2TP), in our example to UUNET.
⇒ The GGSN at the bottom is exclusively reserved for accesses to VPN 2.

Before the mobile station may activate one or more PDP-contexts, first a GMM-context needs to be negotiated between the mobile station and the SGSN. As the figure illustrates, part of this process is the MAP: insertSubscriberData-procedure which, among other things, will transfer all PDP-context specific information from the HLR to the SGSN.
For each PDP-context, the SGSN will obtain information regarding the PDP-address (e.g. fixed or dynamic), the PDP-type and the APN.

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

(2) Meaning of the APN during PDP-Context Activation

- **Example: Network Selection with APN = “*” and PDP-Type = IP**



© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

(2) Meaning of the APN during PDP-Context Activation

Example: Network Selection with APN = "*" and PDP-Type = IP

In this example, the mobile station sends an ACT_PDP_CT_REQ-message to the SGSN in which it requests the activation of a PDP-context with the following specifics:

⇒ PDP-Type: IP
⇒ APN: none provided
⇒ PDP-Address: none provided

In this case, the SGSN will check the following issues:

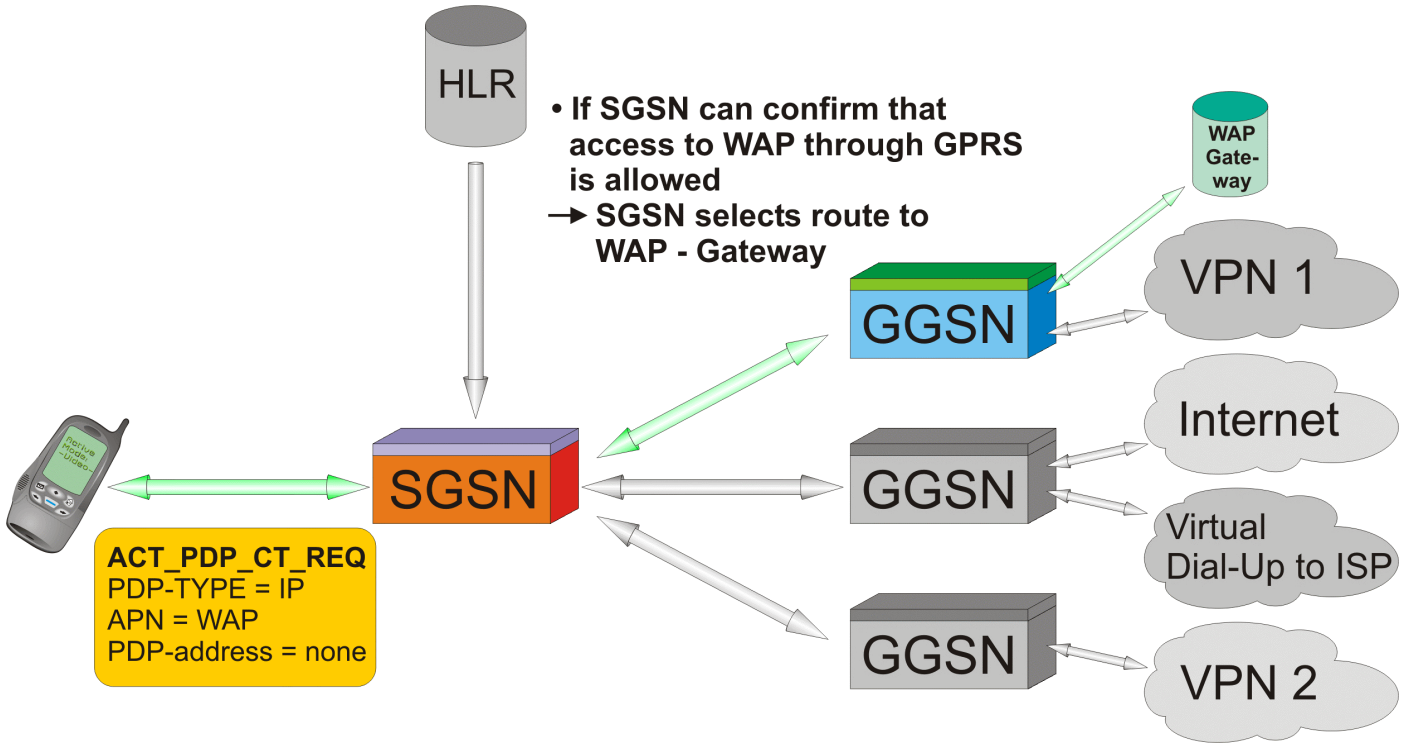
a) Does the subscription include a PDP-context of type IP ?
b) If yes, what APN is shown in the subscription record? (in this case the wildcard APN (⇔ "*"))
c) Since the mobile station does not request a specific APN and APN-subscribed = "*", which GGSN is the default GGSN for IP to also provide the IP-address ?

Note that in this case the IP-address needs to come from the operator-owned IP-address range because neither the information in ACT_PDP_CT_REQ nor the subscription data from the HLR indicate an external source. Consequentially, this is a transparent access to the internet. The IP-address may be private or public.

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

(3) Meaning of the APN during PDP-Context Activation

- **Example: Network Selection with APN = “WAP” and PDP-Type = IP**



© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

(3) Meaning of the APN during PDP-Context Activation

Example: Network Selection with APN = “WAP” and PDP-Type = IP

In this example, the mobile station sends an ACT_PDP_CT_REQ-message to the SGSN in which it requests the activation of a PDP-context with the following specifics:

⇒ PDP-Type: IP
⇒ APN: WAP
⇒ PDP-Address: none provided

In this case, the SGSN will check the following issues:

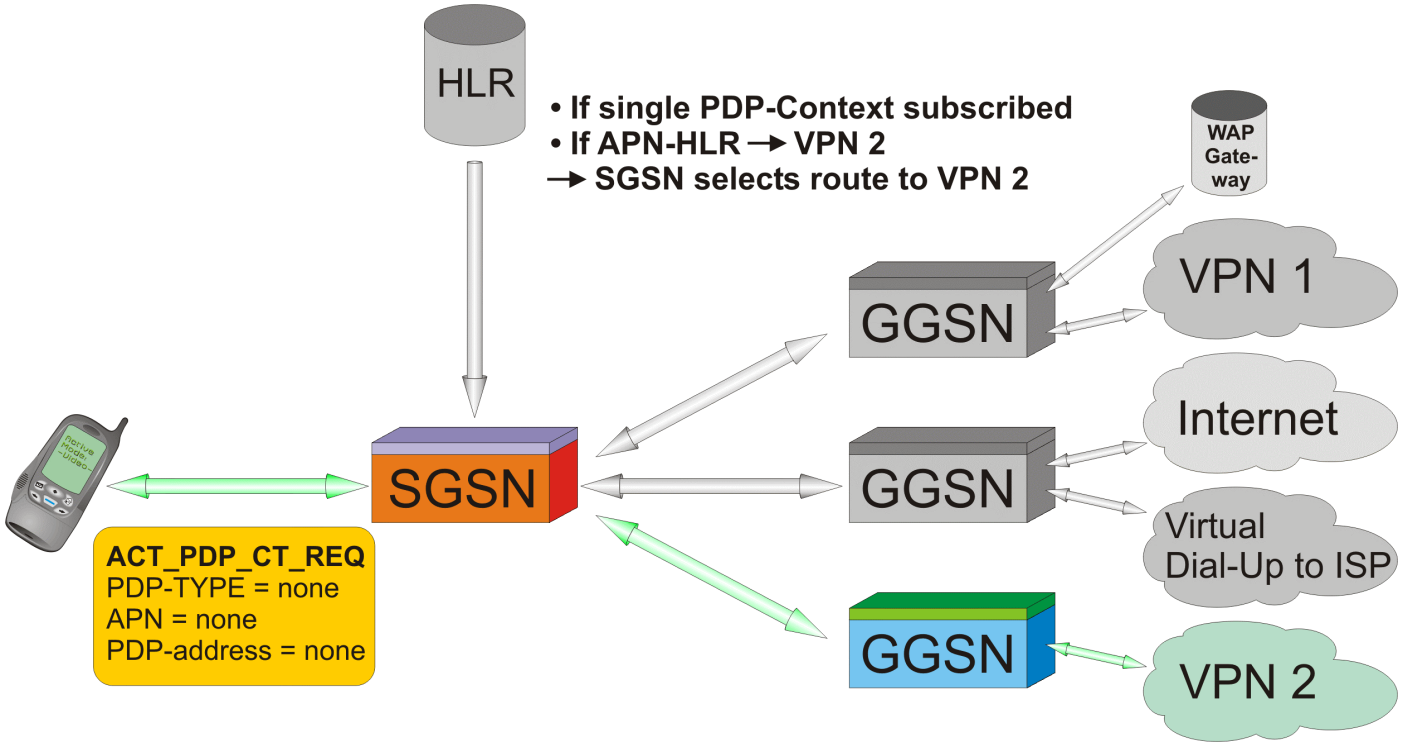
a) Does the subscription include a PDP-context of type IP ?
b) If yes, is the APN = WAP a legitimate APN ?
c) Which GGSN is capable to contact the desired APN? (⇔ in this case the GGSN at the top)
d) The PDP-address will be provided by the GGSN. (⇔ by the operator himself)

In case of WAP the IP-address can be a private IP-address without causing any problems. As in the previous case, this case describes a transparent access.

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

(4) Meaning of the APN during PDP-Context Activation

- **Example: Network Selection without provision of APN or PDP-Type**



© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

(4) Meaning of the APN during PDP-Context Activation

Example: Network Selection without provision of APN or PDP-Type

In this example, the mobile station sends an ACT_PDP_CT_REQ-message to the SGSN in which it requests the activation of a PDP-context with the following specifics:

⇒ PDP-Type: none provided
⇒ APN: none provided
⇒ PDP-Address: none provided

In this case, the mobile station provides no information whatsoever what PDP-context shall be activated. Such kind of PDP-context activation is only possible, if the HLR provided the respective information, in particular about the PDP-type and the APN.

In this case, the SGSN will check the following issues:

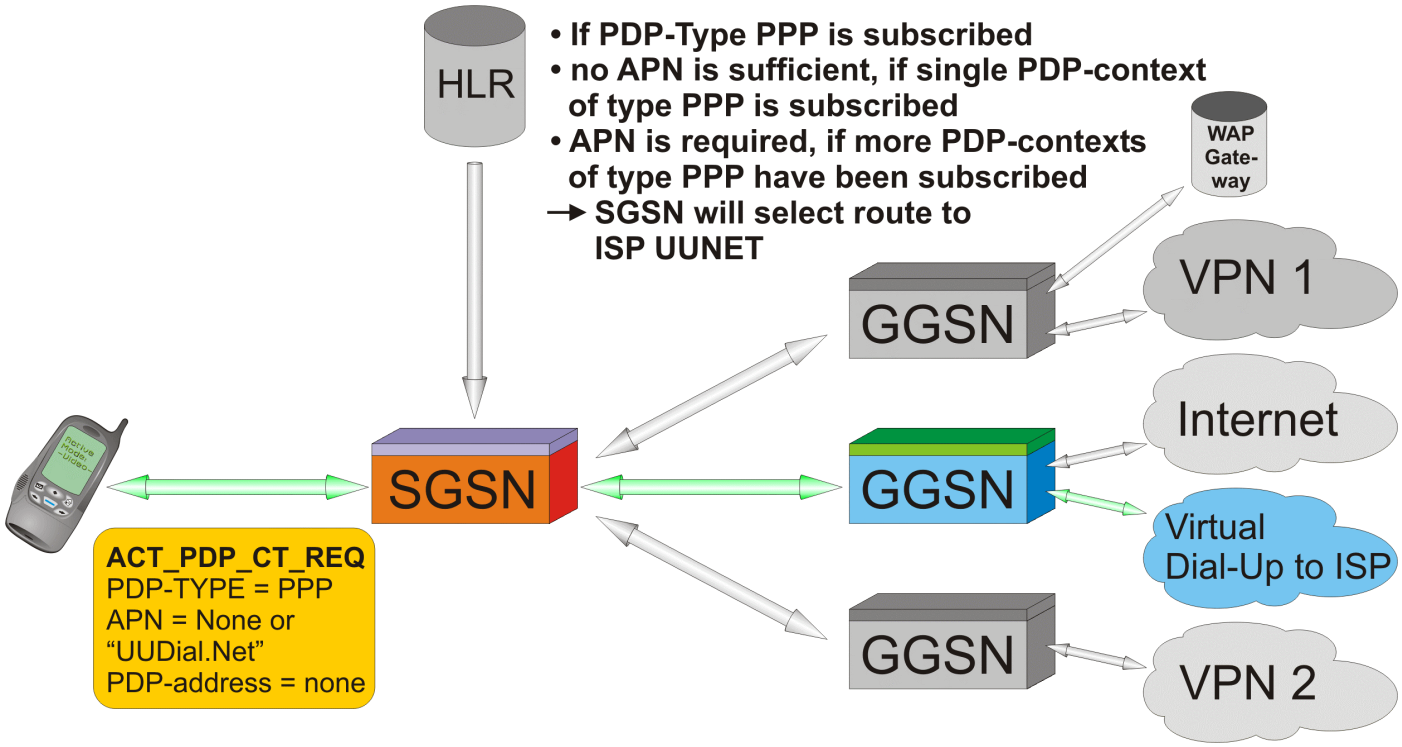
a) Does the subscription include only one PDP-context of any type? (⇔ otherwise there is ambiguity)
b) If yes, which APN is shown for this single PDP-context? (⇔ in this case APN points to VPN 2)
c) Which GGSN is capable to contact the desired APN? (⇔ in this case the GGSN at the bottom)
d) The PDP-address will be provided by the external network. (⇔ in this case by VPN 2)

Most likely, in this case the access is a non-transparent access to the intranet of VPN 2 because the GGSN takes part in the authentication process before the subscriber is granted access to VPN 2. In that respect, the activity of the GGSN relates to the relaying of authentication information between the mobile station and VPN 2.

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

(5) Meaning of the APN during PDP-Context Activation

- **Example: Network Selection with APN = “UUDial.Net” (or without provision of APN) and PDP-Type = PPP**



© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

(5) Meaning of the APN during PDP-Context Activation

Example: Network Selection with APN = “UUDIAL.NET” (or without provision of APN) and PDP-Type = PPP

In this example, the mobile station sends an ACT_PDP_CT_REQ-message to the SGSN in which it requests the activation of a PDP-context with the following specifics:

⇒ PDP-Type: PPP
⇒ APN: UUDial.Net (or none)
⇒ PDP-Address: none provided

This access could be interesting as it represents a virtual dial-up access to an ISP. It also requires the GGSN to support the L2TP (Layer 2 Tunneling Protocol) to transfer PPP-frames to that ISP. The PDP-type PPP should not confuse the reader. The related PPP-frames will most likely be bearers for IP-frames. Please consider that this service may also be used for VPN-services.

In this case, the SGSN will check the following issues:

a) Does the subscription include a PDP-context of type PPP?
b) Is there only one PDP-context of type PPP in the subscription data? If yes, no APN needs to be provided (but may be provided).
c) If there is more than one PDP-context with type PPP in the subscription data, then the desired APN has to be provided by the subscriber in the ACT_PDP_CT_REQ-message (⇔ otherwise there is ambiguity)
d) Which GGSN is capable to contact the desired APN? (in this case the GGSN in the middle)
e) The PDP-address will be provided by the external network, in this case by UUNET.

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

Index:

A

B

C

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

D

E

F

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

G

H

I

L

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

M

N

O

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

P

Q

R

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

S

T

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12

U

V

W

© INACON GmbH 2001 - 2002. All rights reserved. Reproduction and/or unauthorized use of this material is prohibited and will be prosecuted to the full extent of German and international laws. Version Number: 2.12