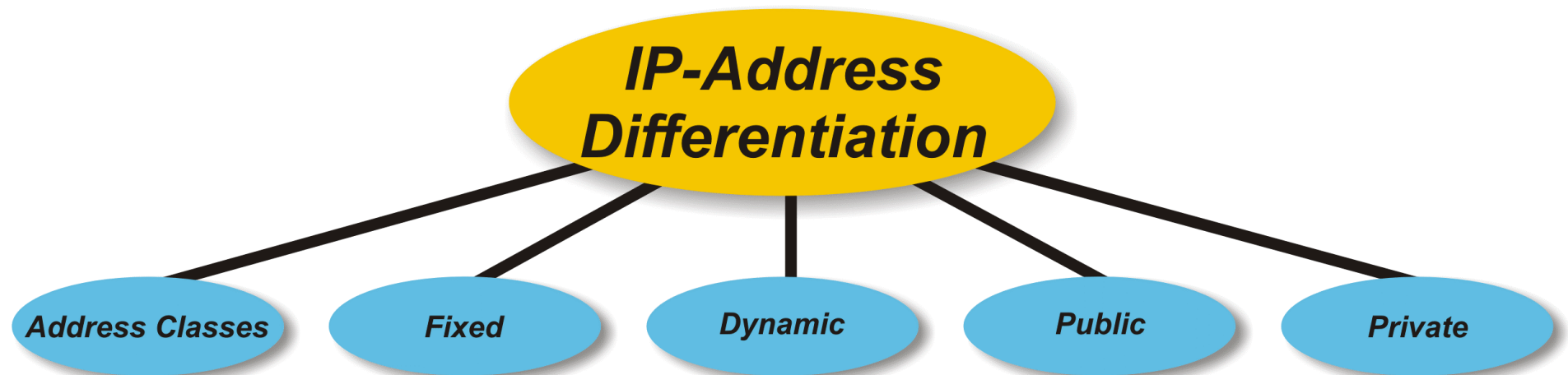


Details of the Internet Protocol

- **IP-Addresses**



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.

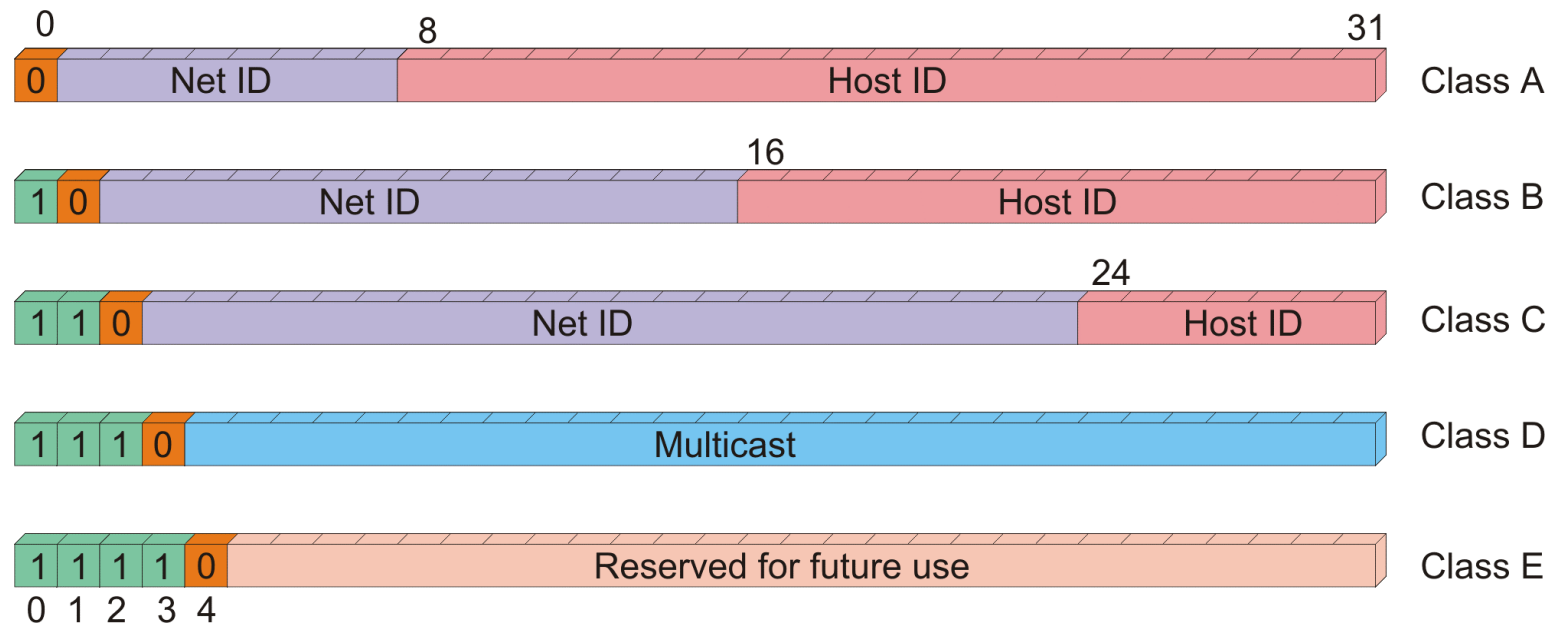
- **Public / Private**

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 (\Leftrightarrow 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.

IP-Address Classes



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??>

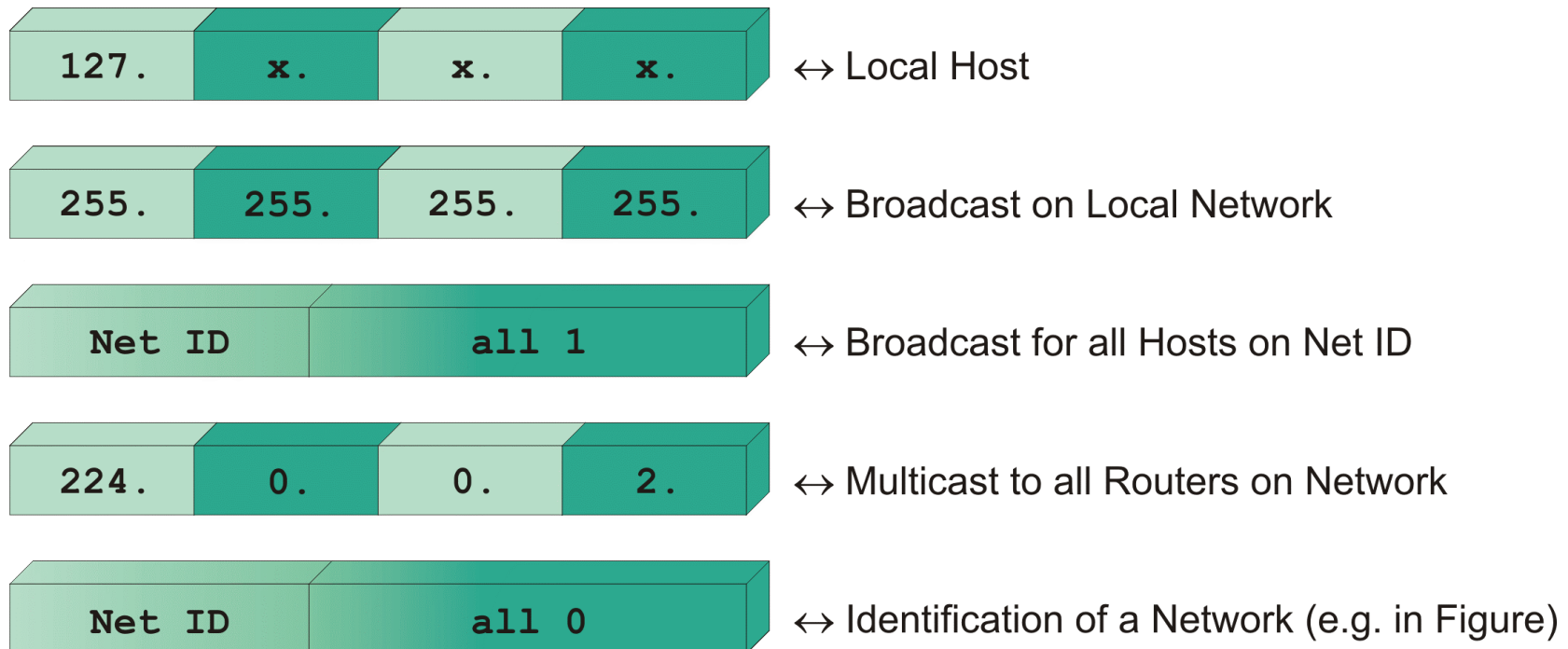
Dotted Decimal Notation: IP-Addresses are 32 bit long. However, for better human readability an IP-address is divided into four 8 bit long tuples, which are presented decimal (e.g. 128.128.17.98)

- **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 ($\Leftrightarrow 2^{16} - 2$) 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 ($\Leftrightarrow 2^8 - 2$) 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 ($\Leftrightarrow 224.0.0.2$)).
- **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]

Special IP-Address Notations



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'.

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	3020.111.10
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.....

UDP-Pseudo Header and UDP-Checksum

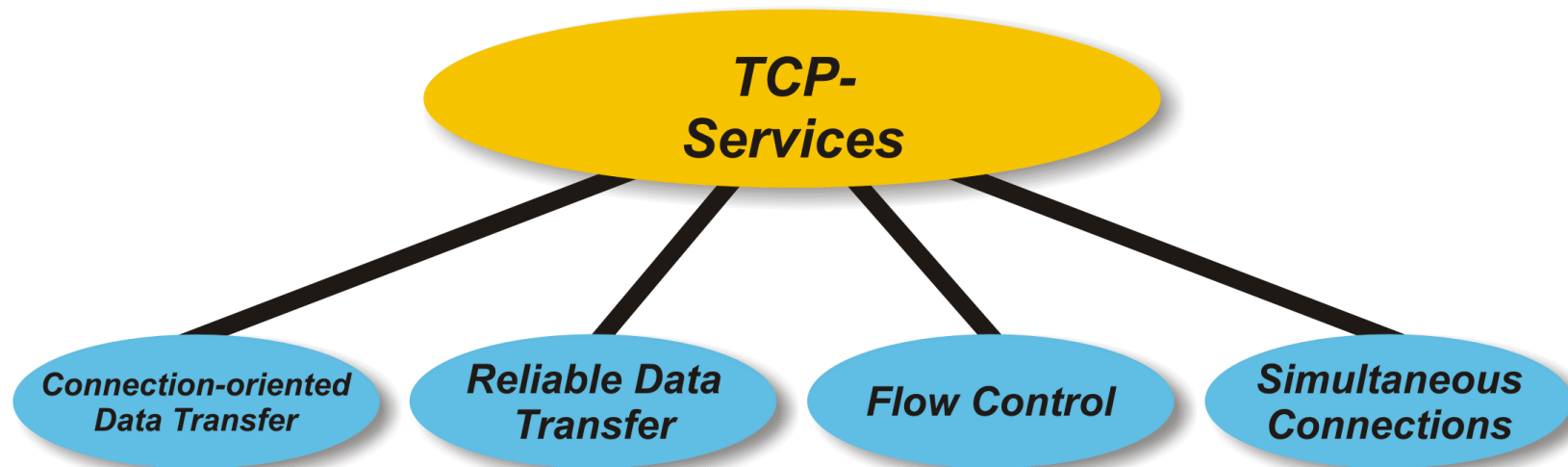
As the figure illustrates, the UDP-checksum does not only protect the UDP-header and the UDP-data part. It rather also considers part of the IP-header. This is achieved through the definition of a 12 octet long UDP-pseudo header which consists of:

- ⇒ 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).

Details of the Transmission Control Protocol (TCP)

- **Services of TCP**



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**

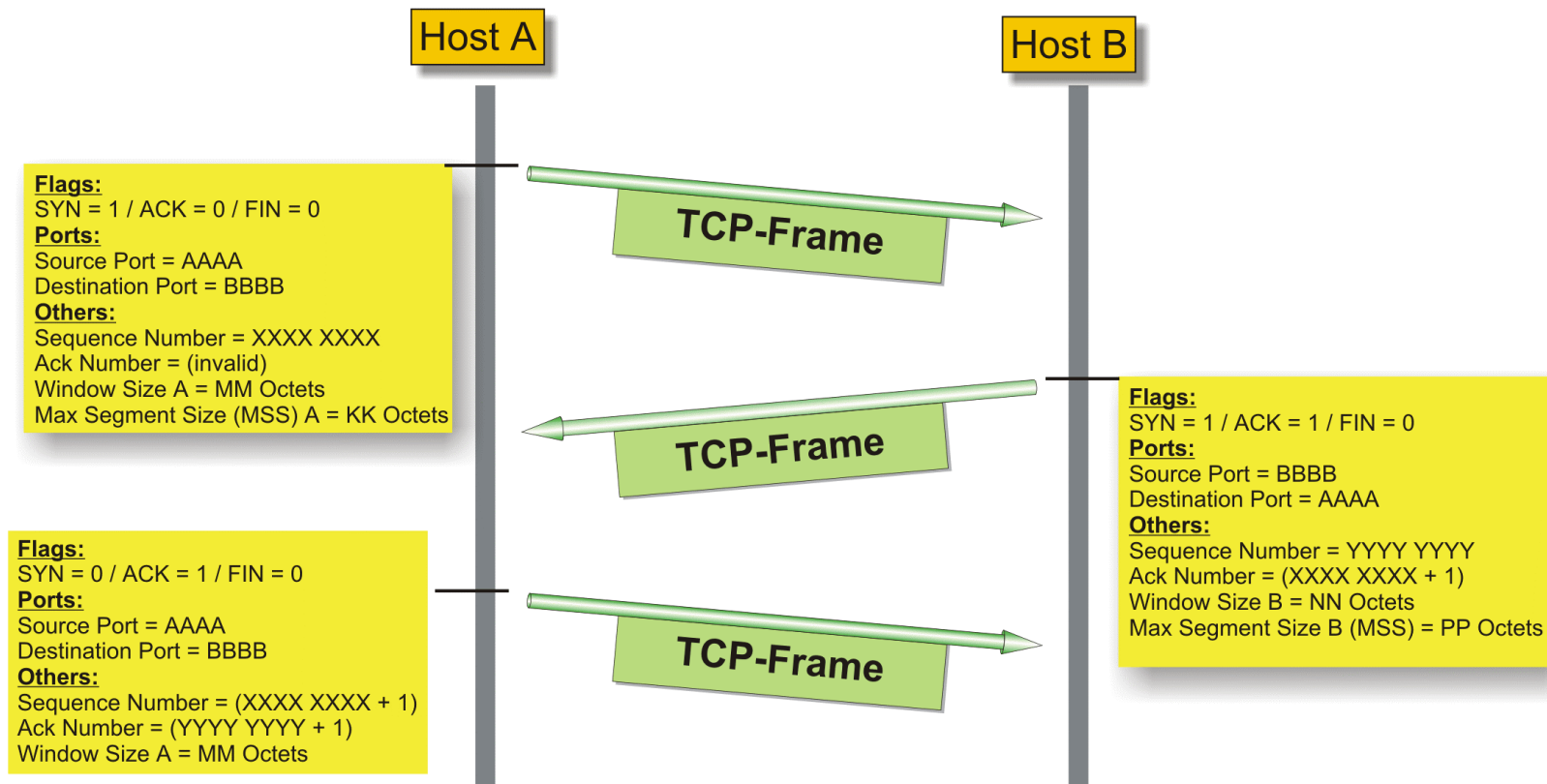
TCP-connections can span over many networks. In addition, a fast sender may be connected to a slower receiver or a connection may be running across a slow intermediate network. TCP is suited to cope with these conditions and to dynamically adapt to changing network load.

- **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]

TCP Connection Establishment



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) (\Leftrightarrow 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 μ s.

- ⇒ Assigning a source port number (\Leftrightarrow 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 (\Leftrightarrow 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 (\Leftrightarrow SYNchronize Sequence Numbers), forwarding the TCP-frame to IP for transmission and waiting for response.

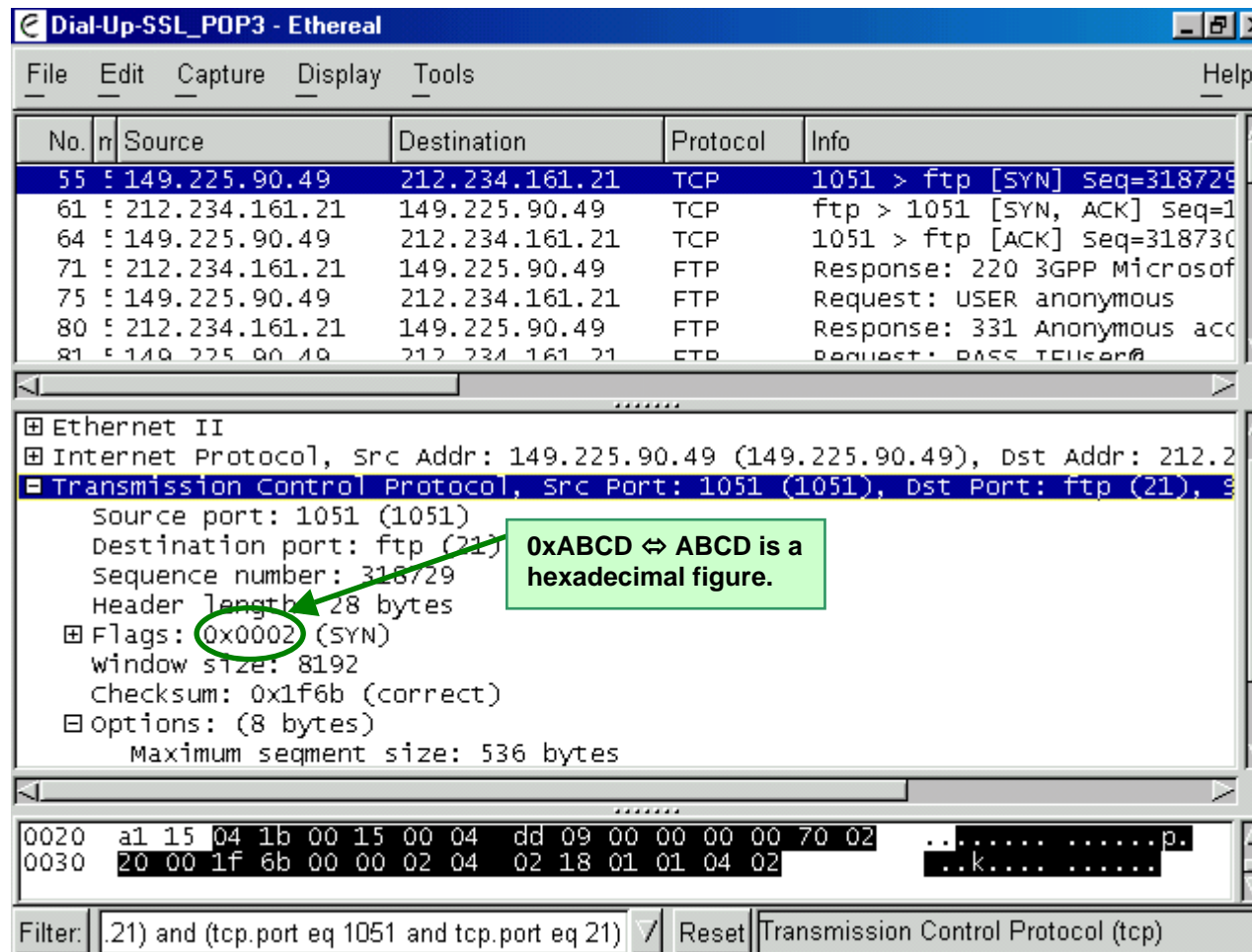
- **Step 2 (Passive Open)**

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 (\Leftrightarrow 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 (\Leftrightarrow 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 (\Leftrightarrow Ack number = YYYY YYYY + 1).

(1) Example for TCP Connection Establishment



Dial-Up-SSL_POP3 - Ethereal

No.	Source	Destination	Protocol	Info
55	149.225.90.49	212.234.161.21	TCP	1051 > ftp [SYN] Seq=318729
61	212.234.161.21	149.225.90.49	TCP	ftp > 1051 [SYN, ACK] Seq=1
64	149.225.90.49	212.234.161.21	TCP	1051 > ftp [ACK] Seq=318730
71	212.234.161.21	149.225.90.49	FTP	Response: 220 3GPP Microsof
75	149.225.90.49	212.234.161.21	FTP	Request: USER anonymous
80	212.234.161.21	149.225.90.49	FTP	Response: 331 Anonymous acc
81	149.225.90.49	212.234.161.21	FTP	Request: PASS TELuser@

Ethernet II

Internet Protocol, Src Addr: 149.225.90.49 (149.225.90.49), Dst Addr: 212.234.161.21 (212.234.161.21)

Transmission Control Protocol, Src Port: 1051 (1051), Dst Port: ftp (21), Seq: 318729

Source port: 1051 (1051)
 Destination port: ftp (21)
 Sequence number: 318729
 Header length: 28 bytes
 Flags: **0x0002** (SYN)
 Window size: 8192
 Checksum: 0x1f6b (correct)
 Options: (8 bytes)
 Maximum segment size: 536 bytes

0xABCD ⇔ ABCD is a hexadecimal figure.

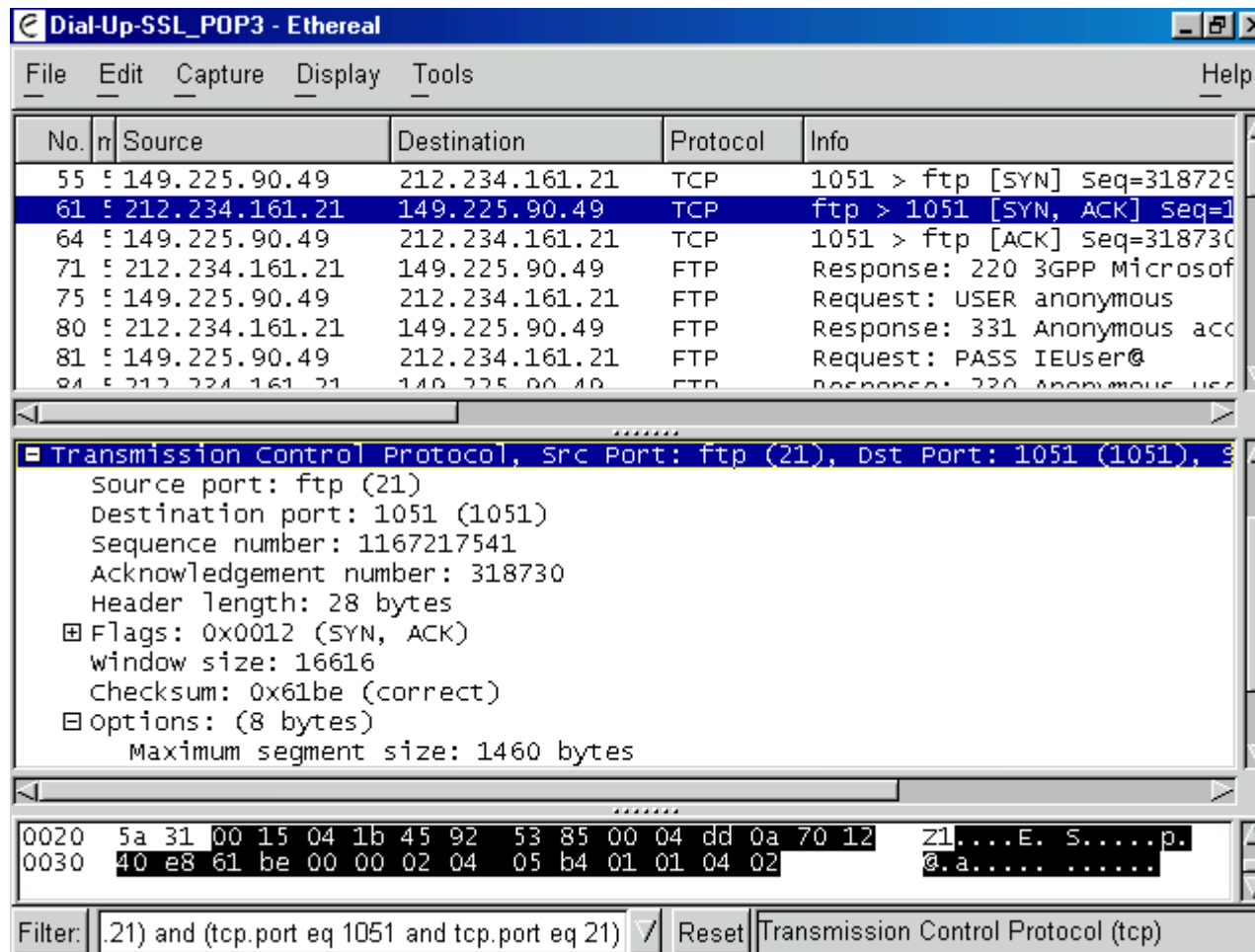
0020 a1 15 04 1b 00 15 00 04 dd 09 00 00 00 00 70 02p.
 0030 20 00 1f 6b 00 00 02 04 02 18 01 01 04 02k.....

Filter: .21) and (tcp.port eq 1051 and tcp.port eq 21) Reset Transmission Control Protocol (tcp)

(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)

(2) Example for TCP Connection Establishment



The screenshot shows a Wireshark packet capture titled "Dial-Up-SSL_POP3 - Ethereal". The packet list shows several packets, with packet 61 selected. The packet details pane shows the Transmission Control Protocol (TCP) section, and the packet bytes pane shows the raw data.

No.	Source	Destination	Protocol	Info
55	149.225.90.49	212.234.161.21	TCP	1051 > ftp [SYN] Seq=318729
61	212.234.161.21	149.225.90.49	TCP	ftp > 1051 [SYN, ACK] Seq=1
64	149.225.90.49	212.234.161.21	TCP	1051 > ftp [ACK] Seq=318730
71	212.234.161.21	149.225.90.49	FTP	Response: 220 3GPP Microsof
75	149.225.90.49	212.234.161.21	FTP	Request: USER anonymous
80	212.234.161.21	149.225.90.49	FTP	Response: 331 Anonymous acc
81	149.225.90.49	212.234.161.21	FTP	Request: PASS IEUser@
84	212.234.161.21	149.225.90.49	FTP	Response: 220 Anonymous use

Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1051 (1051), Seq=1167217541

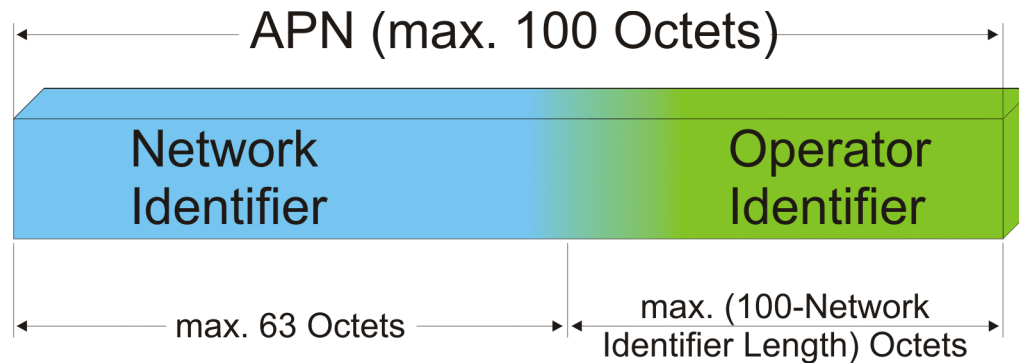
- Source port: ftp (21)
- Destination port: 1051 (1051)
- Sequence number: 1167217541
- Acknowledgement number: 318730
- Header length: 28 bytes
- Flags: 0x0012 (SYN, ACK)
- Window size: 16616
- Checksum: 0x61be (correct)
- Options: (8 bytes)
 - Maximum segment size: 1460 bytes

Filter: .21) and (tcp.port eq 1051 and tcp.port eq 21) / **Reset** Transmission Control Protocol (tcp)

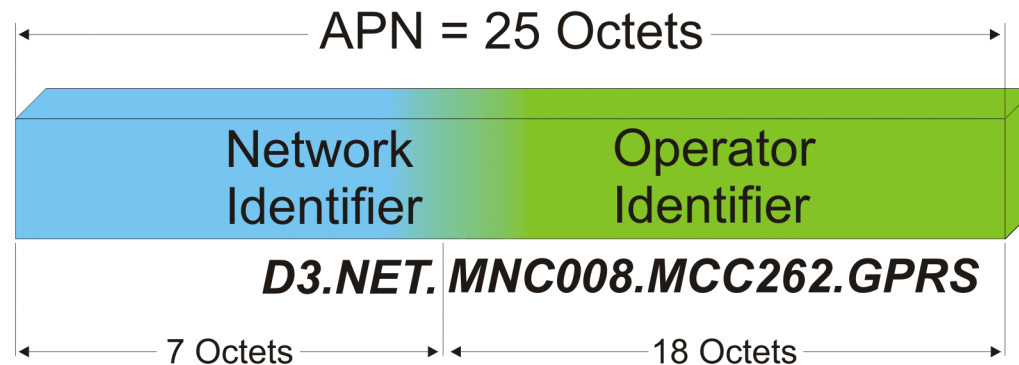
(2) Example for TCP Connection Establishment

- 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

The Access Point Name (APN)



Example:



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.

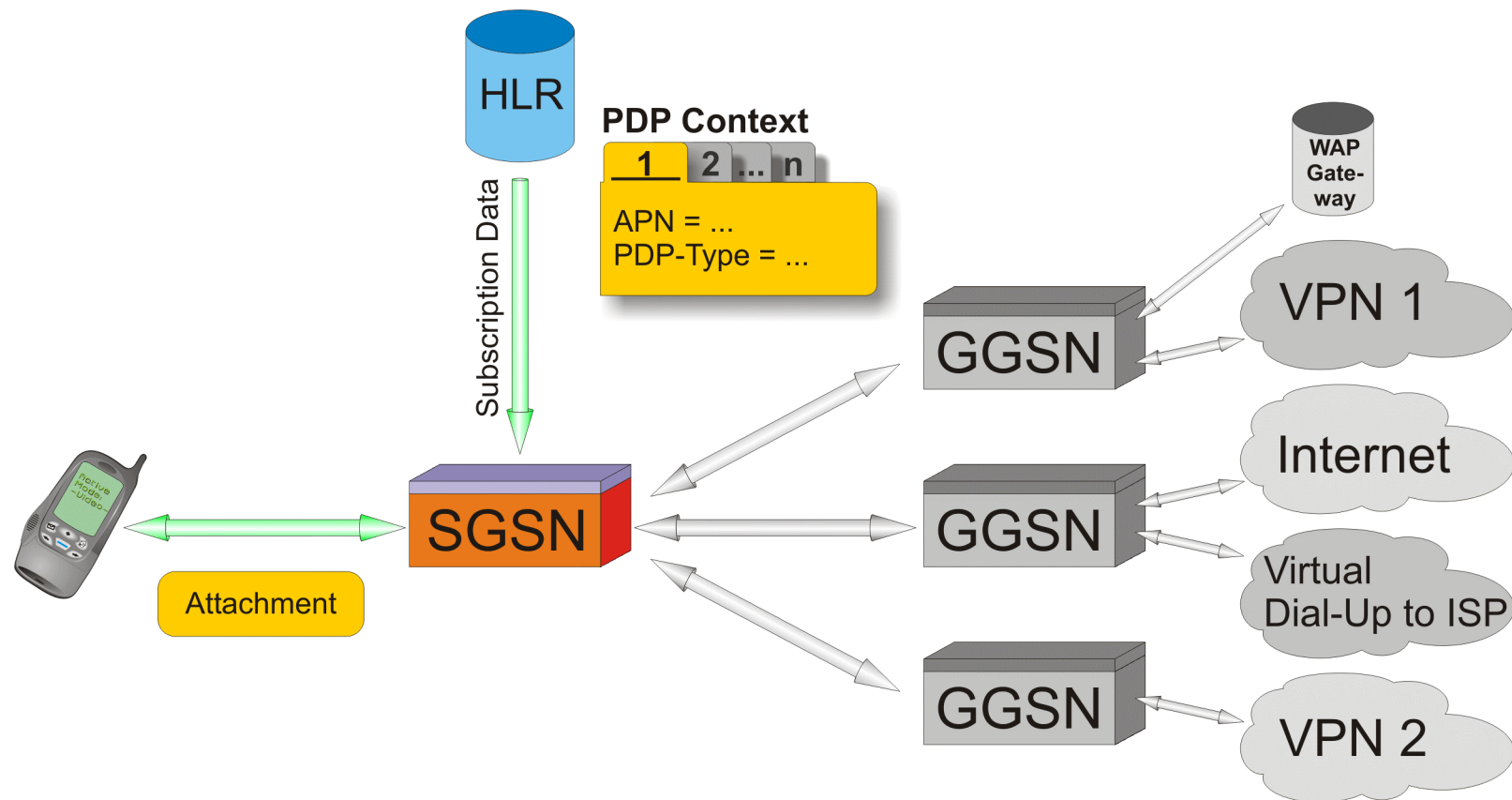
Legal characters for the notation of the APN are: (0 – 9), (a – z), (A – Z) and “-“. The APN is not case sensitive.

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]

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

- **GPRS-Attachment**



(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.

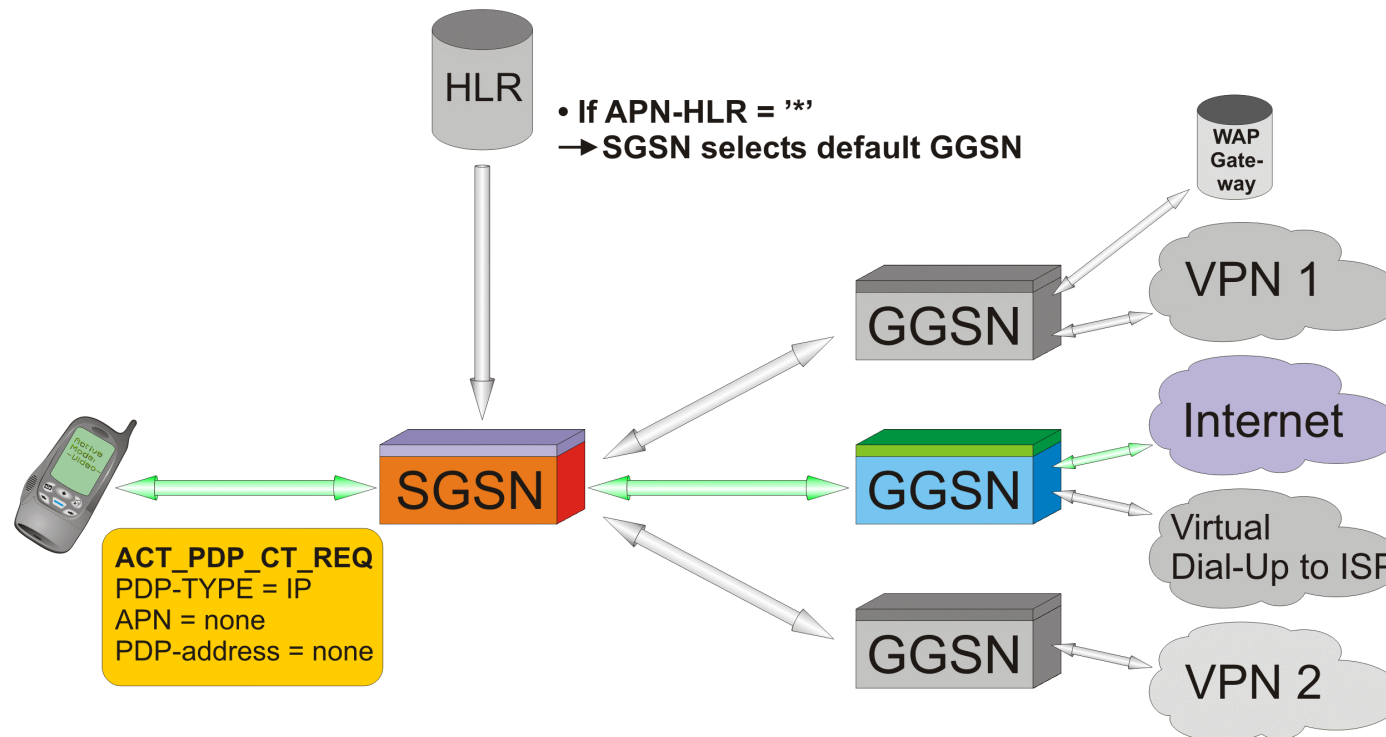
- ⇒ The GGSN at the top is connected to the WAP-gateway plus it has access to VPN 1(⇔ Volume customer 1).
- ⇒ The GGSN in the middle provides basic access to the internet plus it is connected to an ISP (e.g. via the L2TP), in our example to UUNET.
- ⇒ The GGSN at the bottom is exclusively reserved for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

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

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



(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

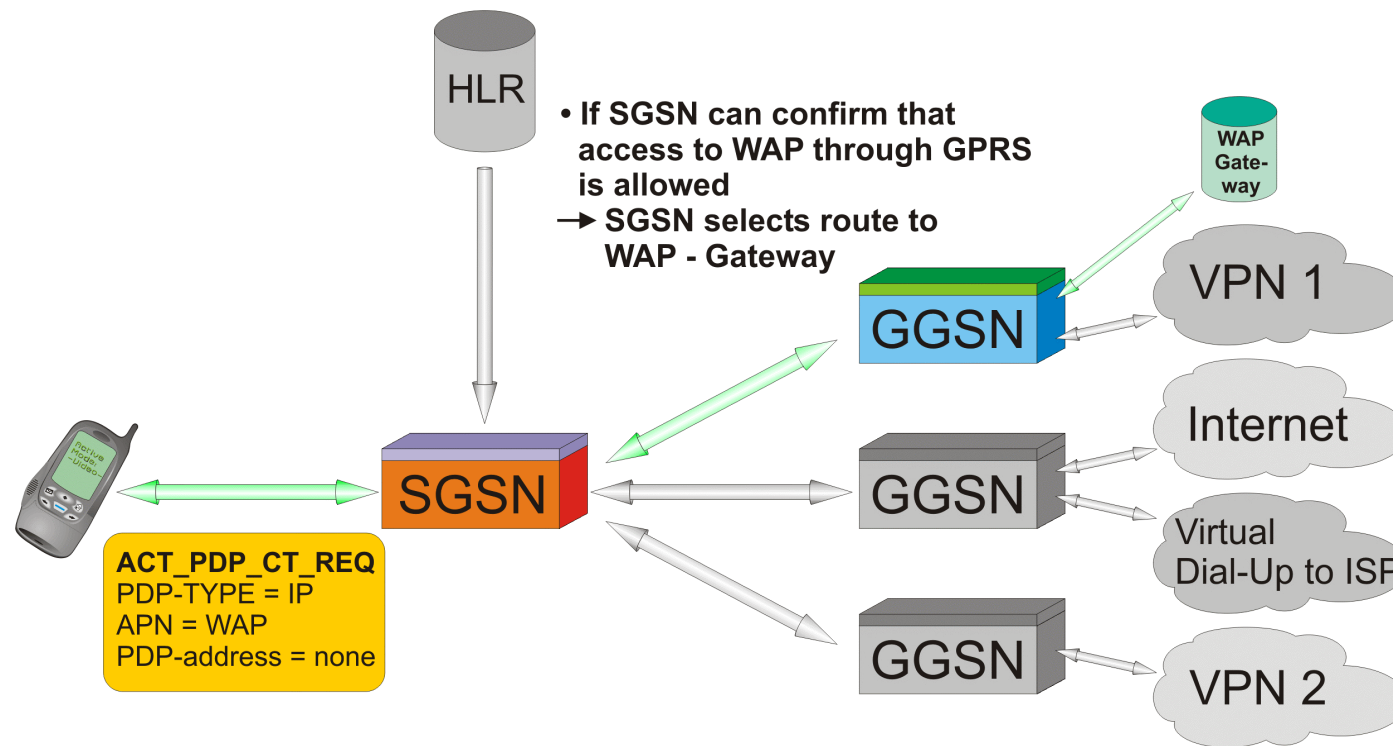
In this case, the SGSN will check the following issues:

- 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.

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

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



(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

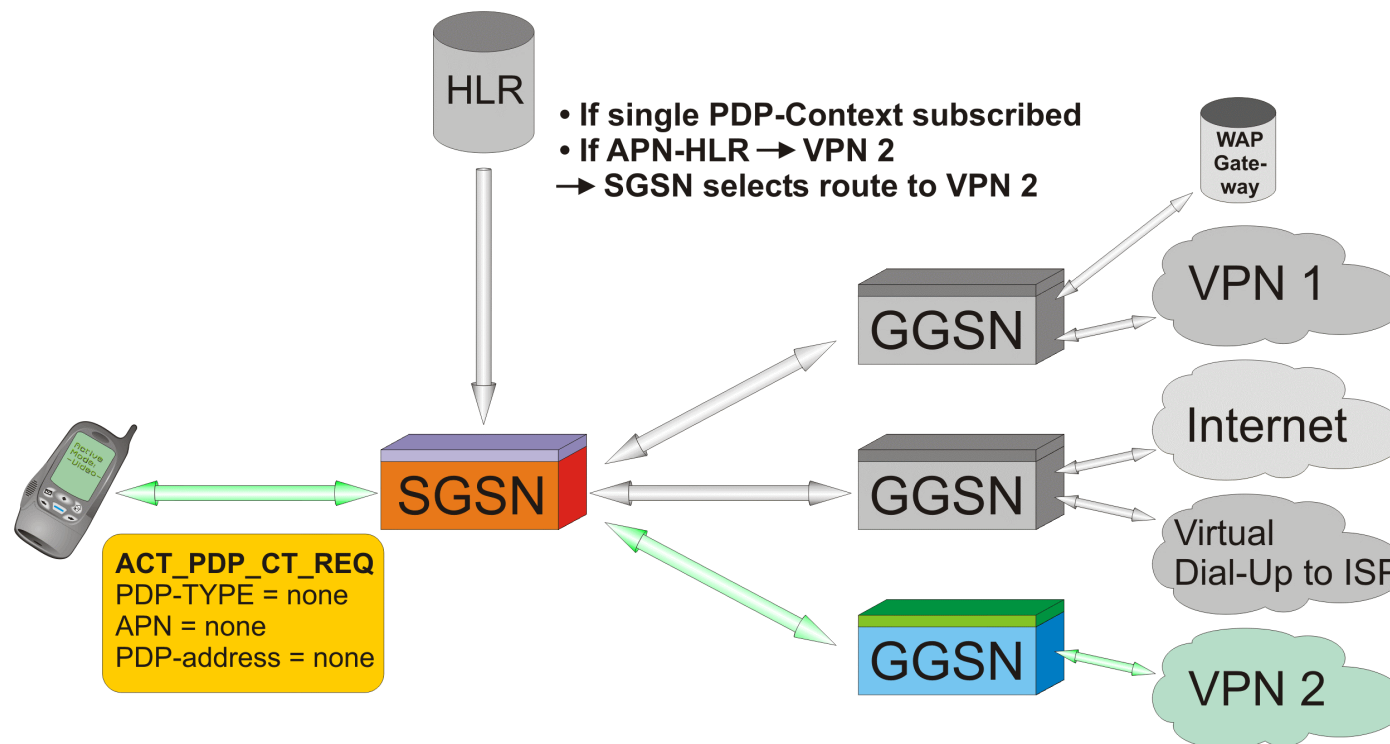
In this case, the SGSN will check the following issues:

- 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.

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

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



(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.

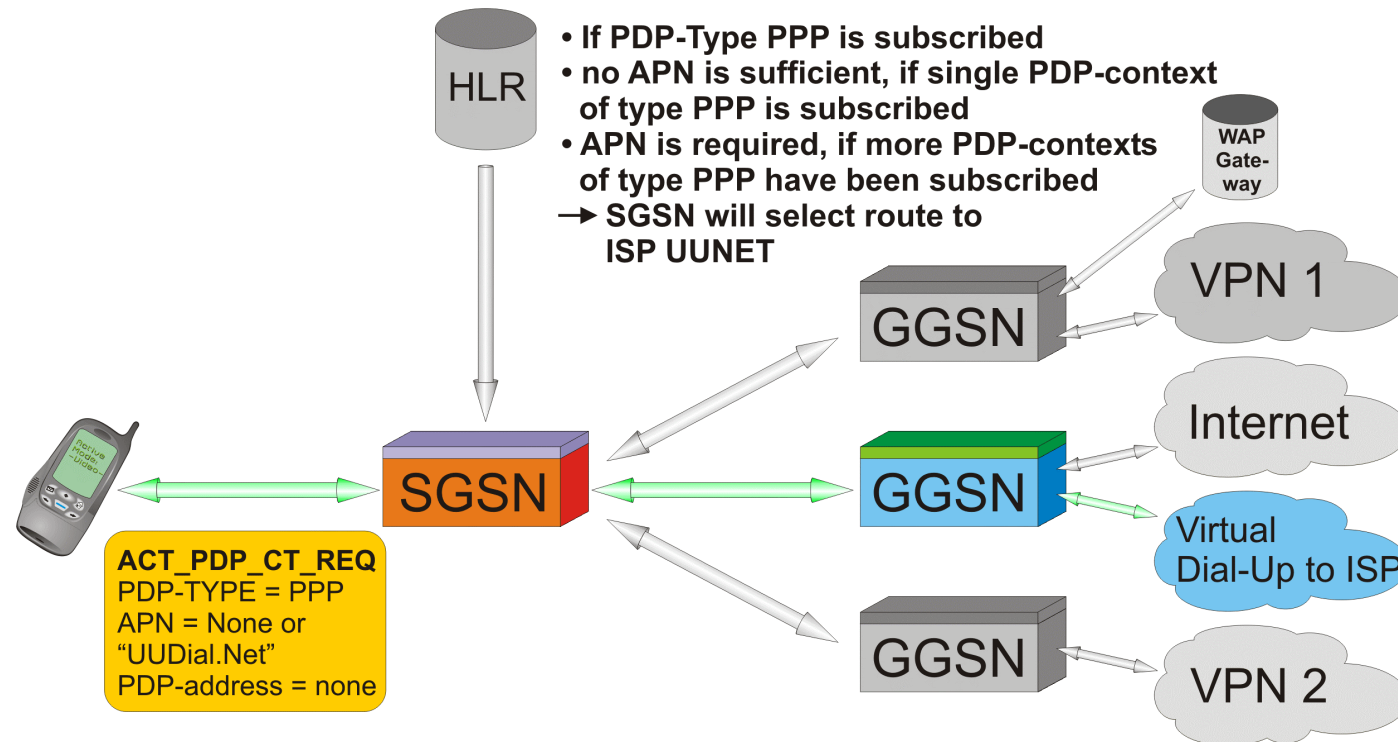
In this case, the SGSN will check the following issues:

- 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.

(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**



(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.

■ **Index:**

A

Abis-Interface	8
Access Point Name	320
ACK (TCP-flag)	238
Acknowledgement Number (TCP)	236
ACT_AA_PDP_CT_ACC	340
ACT_AA_PDP_CT_REJ	340
ACT_AA_PDP_CT_REQ	338
ACT_PDP_CT_ACC	336
ACT_PDP_CT_REJ	336
ACT_PDP_CT_REQ	336
Active Open	218
Address Classes (IP)	162
Address Mask Reply (ICMP-Message)	200
Address Mask Request (ICMP-Message)	200
AH	384, 386, 390
A-Interface	8
APN	320
AT-commands	38
ATT_ACC	104, 122
ATT_COM	104, 122
ATT_REJ	104
ATT_REQ	104, 118
AUTH_CIPH_REJ	108
AUTH_CIPH_REQ	108, 120
AUTH_CIPH_RSP	108, 120
Authentication Data (IPsec)	390
Authentication Header (IPsec)	390

Authentication through Public Key Encryption	402
Authentication through Pre-Shared Key	402
Authentication through Signatures	402
Auxiliary TLLI	82

B

BG	40
B-Interface	8
Border Gateway	40
BSC	6
BSS	6
BSSAP+-GPRS-DETACH-ACK	142
BSSAP+-GPRS-DETACH-IND	142
BSSAP+-IMSI-DETACH-ACK	140
BSSAP+-IMSI-DETACH-IND	140
BSSAP+-LOCATION-UPDATE-ACCEPT	124
BSSAP+-LOCATION-UPDATE-REQUEST	124
BSSAP+-TMSI-REALLOCATION-COMplete	126, 132
BSSGP	58
BTS	6

C

Cell Update	88
Cell Update Procedure	128
Charging (foreign network resources)	36
Charging (own network resources)	26
Checksum (ICMP)	194
Checksum (TCP)	238

Checksum (UDP)	212
CIDR	170
C-Interface	8
ciphering	22
Class A, B, C, D, E (IP)	162
Classless Inter-Domain Routing	170
Code (ICMP)	194
connection establishment (TCP)	218
Cost (IP-Header)	182
CT_AA_PDP_CT_REQ	276
CT_AA_PDP_CT_RSP	276
CT_PDP_CT_REQ	274
CT_PDP_CT_RSP	274

D

Data Compression (\Leftrightarrow V.42bis)	28
DATA_REC_TRANS_REQ	282
DATA_REC_TRANS_RSP	282
DEACT_AA_PDP_CT_ACC	340
DEACT_AA_PDP_CT_REQ	340
DEACT_PDP_CT_ACC	338
DEACT_PDP_CT_REQ	336
Definition of a PLMN	6
DEL_AA_PDP_CT_REQ	276
DEL_AA_PDP_CT_RSP	276
DEL_PDP_CT_REQ	140, 274
DEL_PDP_CT_RSP	140, 276
Delay (IP-Header)	182
Delay Class	302
Destination Address (IP-Header)	190
destination port (TCP)	236
Destination Port (UDP)	212
Destination Unreachable (ICMP-Message)	196
DET_ACC	104, 142

DET_REQ	104, 140
DF-flag = "Do not Fragment"	186
DHCP	38, 358
Differentiated Services	184
Differentiated Services Code Points	184
D-Interface	8
Dotted Decimal Notation	162
DRX	88
DRX parameter information element	94
DS	184
DSCP	184

E

Echo Reply (ICMP-Message)	196
Echo Request (ICMP-Message)	196
ECHO_REQ	272
ECHO_RSP	272
E-Interface	8
Encapsulating Security Payload (IPsec)	392
ERR_IND	276
ESP	384, 386, 392
ESP Authentication Data (IPsec)	392

F

FAIL_REP_REQ	280
FAIL_REP_RSP	280
FIN (TCP-flag)	238
F-Interface	8
Flags (IP-Header)	186
Flow Control	216
Flow Label (GTP)	264
Force to Standby	88
Foreign TLLI	82

Fragment Offset	186
-----------------------	-----

G

Ga-interface	10
Gateway-MSC	6
Gb-interface	10
G-CDR	286
Gc-interface	10
Gd-Interface	10
GGSN	32
Gi-Interface	10
G-Interface	8
GMM	18
GMM Timer information element encoding	94
GMM_INFO	108
GMM_STATUS	108
G-MSC	6
Gn-interface	10
G-PDU	256
Gp-interface	10
Gr-interface	10
Gs-interface	10, 50, 124, 130
GTP	254
GTP'	254
GTP-flow	258
GTP-path	258
GTP-tunnel	258

H

half-close	226, 228
Header Checksum (IP-Header)	190
Header Length (TCP)	238
Host ID	162

I

IANA	160
ICANN	160
ICMP	194
ICV (IPsec)	390, 392
IDENT_REQ	108, 118, 280
IDENT_RSP	108, 118, 280
Identification (IP-Header)	186
IDLE-State	72
IHL (IP-Header)	180
IHOSS	318
IKE	402
IMEI-check	120
implicit detach	100
Information Reply (ICMP-Message)	200
Information Request (ICMP-Message)	200
Initial Sequence Number (TCP)	218
Integrity Check Value (IPsec)	390, 392
Internet Assigned Number Authority	160
Internet Corporation for Assigned Names and Numbers	160
Internet Header Length (IP-Header)	180
Internet Key Exchange	402
Internet Timestamp (IP-Option)	192
Interworking Function	6
IPCP	358
IP-Header	176
IPnG	160
ISAKMP	402
ISN (TCP)	218
IWF	6

L

LAC	76
-----------	----

GPRS – Signaling & Protocol Analysis

LAI.....	76
Legend.....	112
Length (GTP)	264, 270
Length (UDP)	212
LLC	60
Local TLLI	82
location area	74
Loose Source Route	192

M

MAP cancelLocation-procedure.....	122
MAP insertSubscriberData-procedure	136
MAP purgeMS-procedure	142
MAP updateGprsLocation procedure	122
maximum segment size (TCP)	218, 240
Maximum Transmit Unit.....	188
MCC.....	76
M-CDR.....	286
Mean Throughput Class	304
Message Format for GMM and SM	102
MF-flag = “More Fragments”.....	186
MNC.....	76
MNRG	280
Mobile Reachable Timer.....	98
Mobile Station Class A.....	42
Mobile Station Class B.....	44
Mobile Station Class C	46
Mobile Terminating PDP Context Activation.....	352
MOD_PDP_CT_ACC.....	338
MOD_PDP_CT_REQ	338
MSS (TCP).....	218, 240
MTU	188
MTU Probe (IP-Option)	192
MTU Reply (IP-Option)	192

N

N3-Buffer size.....	262
N3-Requests.....	262
Net ID	162
Network Operation Mode	48
Network Operation Mode I	50
Network Operation Mode II	52
Network Operation Mode III	54
Network Service	58
Network Switching Subsystem	6
Next Header (IPsec)	390, 392
NODE_ALIVE_REQ	272
NODE_ALIVE_RSP	272
NOM I	50, 90
NOM II	52
NOM III	54
Non-DRX mode	94
NON-DRX-TIMER	94
Non-Transparent Access.....	38
NOT_MS_GPRS_PREP_REQ.....	280
NOT_MS_GPRS_PREP_RSP	280
N-PDU	256
N-PDU No (GTP).....	264
NSAPI.....	258
NSS	6
Null Routing Area	74

O

octet stream protocol	318
Options (IP)	192
Options (TCP).....	240
OSP	318

P

Packet-switched paging.....	72
Padding (IPsec)	392
Padding Length (IPsec)	392
Parameter Problem on a Datagram (ICMP-Message).....	198
Passive Open	218
Payload Length (IPsec)	390
PCU	12
PCU-Frames.....	12
PD	102
PDU_NOT_REJ_REQ	278
PDU_NOT_REJ_RSP	278
PDU_NOT_REQ	278
PDU_NOT_RSP	278
Peak Throughput Class	306
Periodic Routing Area Updating Timer	98
Ping-application	196
port number (GTP).....	250
port numbers.....	210
Precedence (IP-Header)	182
Pre-Shared Key	402
Protocol (IP-Header)	190
Protocol Discriminator.....	102
Protocol Type (GTP).....	264
Protocol Type (GTP')	270
PSH (TCP-flag)	238
PT	264, 270
P-TMSI.....	80
P-TMSI Signature	80
P-TMSI_REAL_CMD	106
P-TMSI_REAL_COM.....	106
Public Key Encryption.....	402

Q

QoS-profile	296
-------------------	-----

R

RA_UPD_ACC	106
RA_UPD_COM.....	106, 132
RA_UPD_REJ	106
RA_UPD_REQ	106, 130
RAC	76
Radio Priority	300
RADIUS	38, 358
RAI.....	76
Random TLLI.....	82
Ready Timer	86
Ready Timer / Specific Settings	94
READY-State.....	72
Record Route (IP-Option).....	192
REDIR_REQ.....	272
REDIR_RSP	274
Redirect (ICMP-Message)	196
Reliability (IP-Header)	182
Reliability Class	308
REQ_PDP_CT_ACT	336
REQ_PDP_CT_ACT_REJ	336
Reserved (IPsec).....	390
RLC/MAC	64
Router Advertisement (ICMP-Message)	198
Router Alert (IP-Option).....	192
Router Solicitation (ICMP-Message)	198
Routing Area.....	74
Routing Area Identification	76
RST (TCP-flag)	238

S

S-CDR.....	286
Secure Socket Layer	382
Security Parameters Index	390, 392
SEND_ROUT_INFO_GPRS_REQ	278
SEND_ROUT_INFO_GPRS_RSP	278
Sequence Number (GTP)	264, 334
Sequence Number (GTP')	270
Sequence Number (IPsec)	390, 392
Sequence Number (TCP)	236
Service Precedence / Priority	300
SGSN.....	16
SGSN_CT_ACK	282
SGSN_CT_REQ	282
SGSN_CT_RSP	282
sliding window mechanism (TCP).....	242
SM_STATUS	340
SMS	318
SND	334
SNDSCP	62
SNN-flag (GTP)	264
SNU	334
socket.....	216
Source Address (IP-Header)	190
source port (TCP)	236
Source Port (UDP).....	212
Source Quench (ICMP-Message).....	196
SPI	390, 392
SSL	382
S-SMO-CDR	286
S-SMT-CDR.....	286
SSN for GPRS	70
STANDBY-State	72
storage of P-TMSI and RAC	82

Strict Source Route (IP-Option).....	192
subnet mask	168
Subnet-Addressing	168
subnetting	168
Subsystem Numbers for GPRS.....	70
supernetting.....	170
SYN (TCP-flag)	238
SYS_INFO13.....	78

T

T3212	98
T3310	118
T3312	98
T3314	86
T3321	140
T3330	130
T3350	122, 132
T3360	120, 124
T3370	118
T3380	358
T3385	364
T3390	368
T3395	370, 372
T3-Response timer	262
T3-Tunnel timer	262
T6-1	124
T6-2	124
T8	142
T9	140
TCP	216
TCP/IP Header Compression (⇔ RFC 1144)	30
Temporary Logical Link Identifier	82
three way handshake (TCP).....	218
Throughput (IP-Header)	182

TI	102
TID (GTP)	264
TI-flag	102
Time Exceeded for a Datagram (ICMP-Message)	198
Time To Live (IP-Header)	190
Timer Encoding GMM	94
Timestamp Reply (ICMP-Message)	200
Timestamp Request (ICMP-Message)	198
TI-value	102
TLLI	82
TOS	182
Total Length (IP-Header)	180
T-PDU	256
Traceroute (IP-Option)	192
Transaction Identifier	102
transparent access	324
Transparent Access	38
Transport Mode	384, 388
TRAU	6
Triplets	118
TTL (IP-Header)	190
Tunnel Identifier (GTP)	264
Tunnel Mode	386, 388
Type (ICMP)	194
Type of Service field (IP-Header)	182

U

UDP	206
UDP-pseudo header	214
UPD_PDP_CT_REQ	136, 274
UPD_PDP_CT_RSP	136, 274
URG (TCP-flag)	238
Urgent Pointer	238

V

V.42bis	28
VERS_NOT_SUPP	272
Version (GTP)	264
Version (GTP')	270
Version (IP-Header)	180
VPN	382

W

Wildcard APN	320
Window Size	238