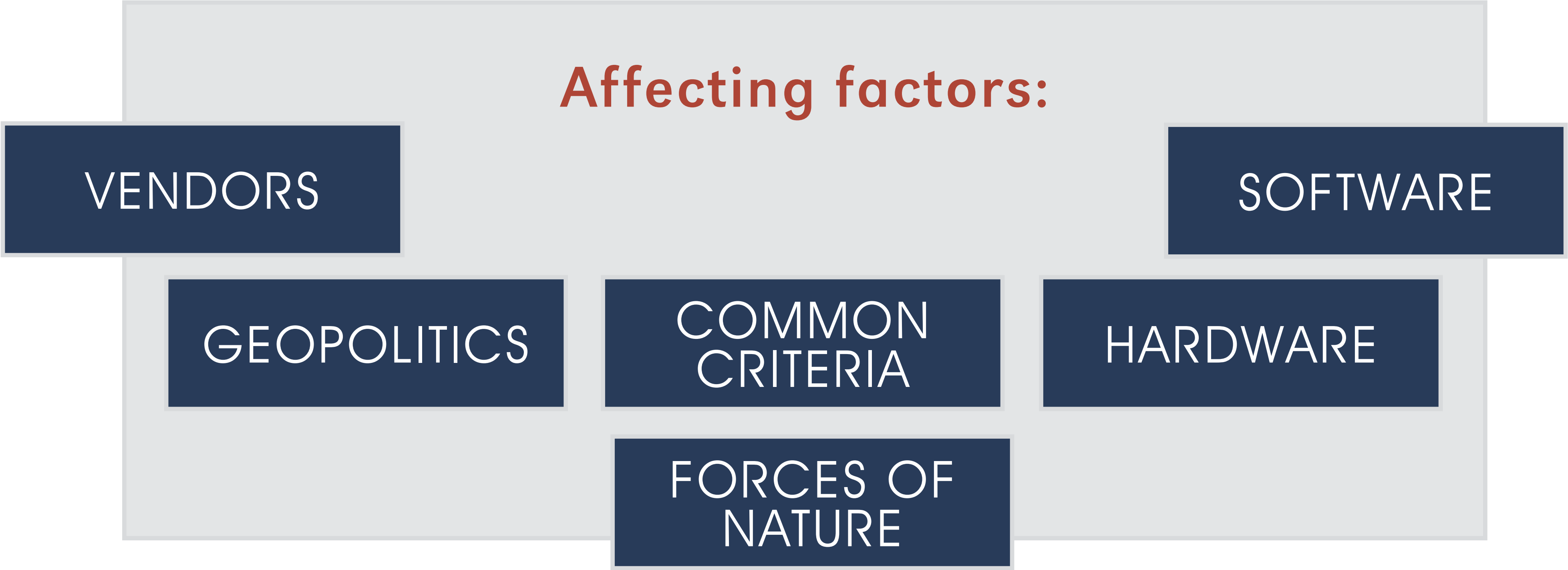
A CASE FOR PROTOCOL DEPENDENCY

Juhani Eronen, Marko Laakso, Pasi Kemi

Oulu University
Secure Programming
Group

TRADITIONAL INFORMATION SECURITY RISK MANAGEMENT



Affecting factors:

VENDORS

SOFTWARE

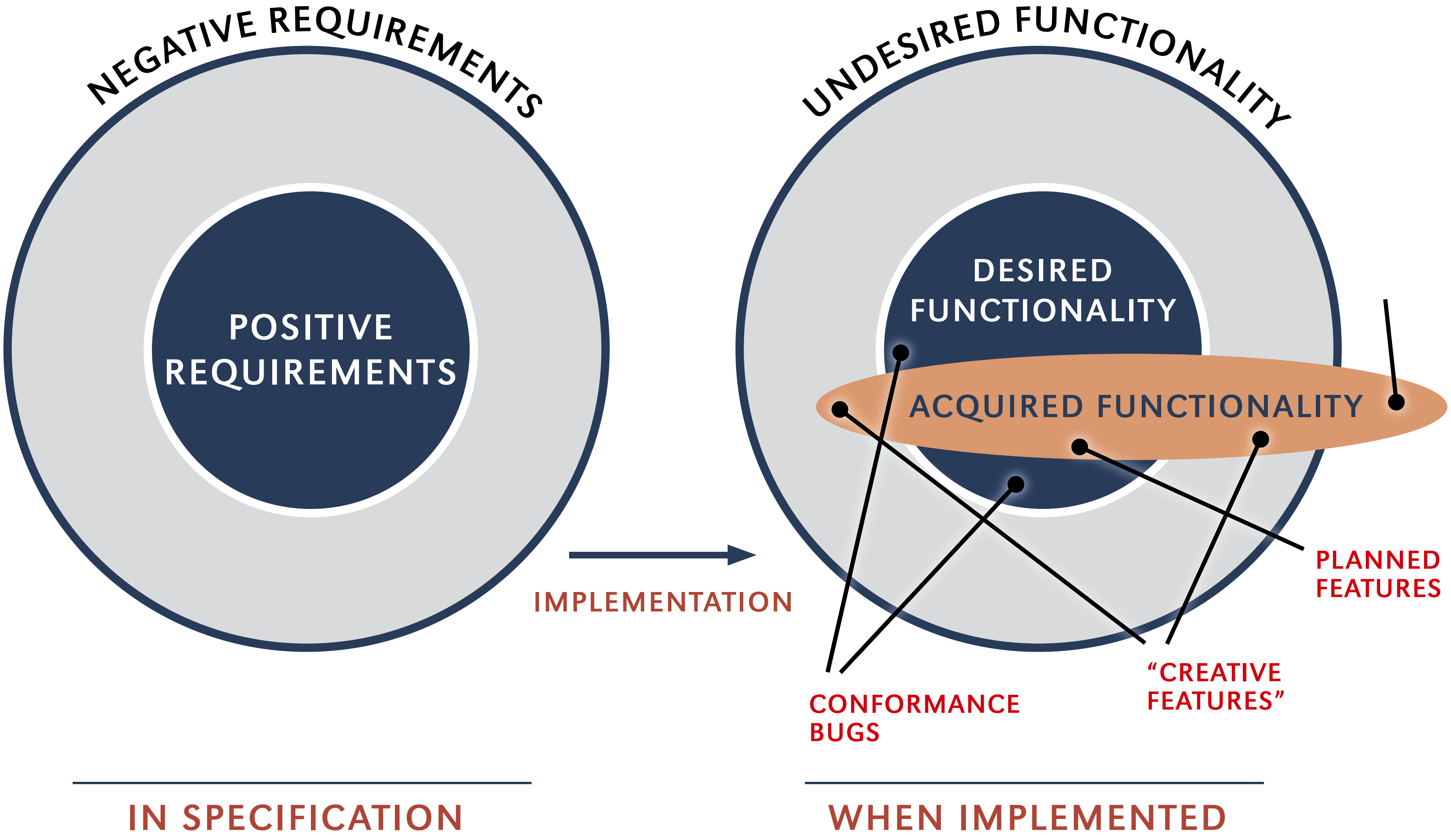
GEOPOLITICS

COMMON CRITERIA

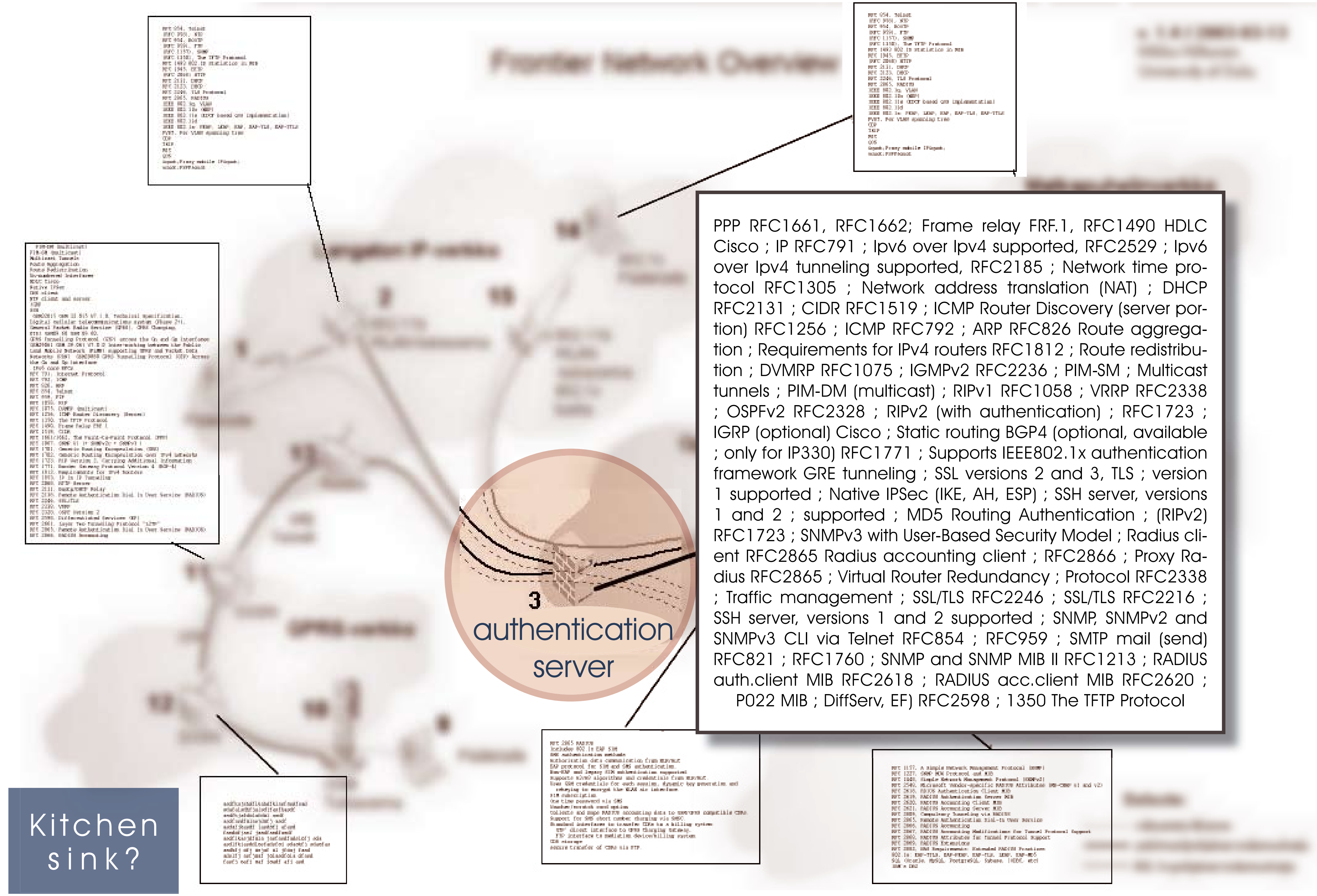
HARDWARE

FORCES OF NATURE

something missing?


NEGATIVE REQUIREMENTS
POSITIVE REQUIREMENTS
IMPLEMENTATION
UNDESIRED FUNCTIONALITY
DESIRED FUNCTIONALITY
ACQUIRED FUNCTIONALITY
PLANNED FEATURES
"CREATIVE FEATURES"
CONFORMANCE BUGS
IN SPECIFICATION
WHEN IMPLEMENTED

bugs



RFC 854. Telnet
RFC 959. FTP
RFC 951. BOOTP
RFC 959. FTP
RFC 1157. SNMP
RFC 1350. The TFTP Protocol
RFC 1492 802.1D statistics in MIB
RFC 1945. HTTP
RFC 2068. HTTP
RFC 2131. DHCP
RFC 2131. DHCP
RFC 2246. TLS Protocol
RFC 2865. RADIUS
IEEE 802.1q VLAN
IEEE 802.1Dx (MSTP)
IEEE 802.11a (DFCP based on implementation)
IEEE 802.11d
IEEE 802.1x PEAP, LEAP, EAP, EAP-TLS, EAP-TTLS
PVST. Per VLAN spanning tree
CDP
TACP
RIP
QOS
[illegible]
[illegible]

RFC 854. Telnet
RFC 959. FTP
RFC 951. BOOTP
RFC 959. FTP
RFC 1157. SNMP
RFC 1350. The TFTP Protocol
RFC 1492 802.1D statistics in MIB
RFC 1945. HTTP
RFC 2068. HTTP
RFC 2131. DHCP
RFC 2131. DHCP
RFC 2246. TLS Protocol
RFC 2865. RADIUS
IEEE 802.1q VLAN
IEEE 802.1Dx (MSTP)
IEEE 802.11a (DFCP based on implementation)
IEEE 802.11d
IEEE 802.1x PEAP, LEAP, EAP, EAP-TLS, EAP-TTLS
PVST. Per VLAN spanning tree
CDP
TACP
RIP
QOS
[illegible]
[illegible]

PIM-DM (multicast)
PIM-SM (multicast)
Multicast Tunnels
Route Aggregation
Route Redistribution
Unnumbered Interfaces
HDLC Cisco
Native IPSec
CHAP client
NTP client and server
IGMP
GSM
GSM03.60 GSM 03 60 V7.1.0, Technical specification,
Digital cellular telecommunications system (Phase 2+);
General Packet Radio Service (GPRS); GPRS Charging
ETSI [illegible]
GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface
GSM29061 GSM 29.061 V7.0.0 Inter-working between the Public
Land Mobile Network (PLMN) supporting GPRS and Packet Data
Networks (PDN) GSM29060 GPRS Tunnelling Protocol (GTP) Across
the Gn and Gp Interface
IPv6 core RFCs
RFC 791. Internet Protocol
RFC 792. ICMP
RFC 826. ARP
RFC 854. Telnet
RFC 959. FTP
RFC 1058. RIP
RFC 1075. DVMRP (multicast)
RFC 1256. ICMP Router Discovery (Server)
RFC 1350. The TFTP Protocol
RFC 1490. Frame Relay FRF.1
RFC 1519. CIDR
RFC 1661/1662. The Point-to-Point Protocol (PPP)
RFC 1907. SNMP v2 (+ SNMPv2c + SNMPv3)
RFC 1701. Generic Routing Encapsulation (GRE)
RFC 1702. Generic Routing Encapsulation over IPv4 networks
RFC 1723. RIP Version 2. Carrying Additional Information
RFC 1771. Border Gateway Protocol Version 4 (BGP-4)
RFC 1812. Requirements for IPv4 Routers
RFC 1853. IP in IP Tunneling
RFC 2068. HTTP Server
RFC 2131. DHCP/BOOTP Relay
RFC 2138. Remote Authentication Dial In User Service (RADIUS)
RFC 2246. SSL/TLS
RFC 2338. VRRP
RFC 2328. OSPF Version 2
RFC 2598. Differentiated Services (EF)
RFC 2661. Layer Two Tunneling Protocol "L2TP"
RFC 2865. Remote Authentication Dial In User Service (RADIUS)
RFC 2866. RADIUS Accounting

PPP RFC1661, RFC1662; Frame relay FRF.1, RFC1490 HDLC Cisco ; IP RFC791 ; Ipv6 over Ipv4 supported, RFC2529 ; Ipv6 over Ipv4 tunneling supported, RFC2185 ; Network time protocol RFC1305 ; Network address translation (NAT) ; DHCP RFC2131 ; CIDR RFC1519 ; ICMP Router Discovery (server portion) RFC1256 ; ICMP RFC792 ; ARP RFC826 Route aggregation ; Requirements for IPv4 routers RFC1812 ; Route redistribution ; DVMRP RFC1075 ; IGMPv2 RFC2236 ; PIM-SM ; Multicast tunnels ; PIM-DM (multicast) ; RIPv1 RFC1058 ; VRRP RFC2338 ; OSPFv2 RFC2328 ; RIPv2 (with authentication) ; RFC1723 ; IGRP (optional) Cisco ; Static routing BGP4 (optional, available ; only for IP330) RFC1771 ; Supports IEEE802.1x authentication framework GRE tunneling ; SSL versions 2 and 3, TLS ; version 1 supported ; Native IPSec (IKE, AH, ESP) ; SSH server, versions 1 and 2 ; supported ; MD5 Routing Authentication ; (RIPv2) RFC1723 ; SNMPv3 with User-Based Security Model ; Radius client RFC2865 Radius accounting client ; RFC2866 ; Proxy Radius RFC2865 ; Virtual Router Redundancy ; Protocol RFC2338 ; Traffic management ; SSL/TLS RFC2246 ; SSL/TLS RFC2216 ; SSH server, versions 1 and 2 supported ; SNMP, SNMPv2 and SNMPv3 CLI via Telnet RFC854 ; RFC959 ; SMTP mail (send) RFC821 ; RFC1760 ; SNMP and SNMP MIB II RFC1213 ; RADIUS auth.client MIB RFC2618 ; RADIUS acc.client MIB RFC2620 ; P022 MIB ; DiffServ, EF) RFC2598 ; 1350 The TFTP Protocol

Kitchen sink?

[illegible]

RFC 2865 RADIUS
Includes 802.1x EAP SIM
SMS authentication methods
Authorization data communication from HLR/VLR
EAP protocol for SIM and SMS authentication
Non-EAP and legacy SIM authentication supported
Supports A3/A8 algorithms and credentials from HLR/AuC.
Uses GSM credentials for each session, dynamic key generation and
rekeying to encrypt the WLAN air interface
SIM subscription
One time password via SMS
Username/password based option
Collects and maps RADIUS accounting data to operator compatible CDRs
Support for SMS short number charging via SMSC
Standard interfaces to transfer CDRs to a billing system
GTP' client interface to GPRS charging gateway
FTP interface to mediation device/billing system
CDR storage
secure transfer of CDRs via FTP.

RFC 1157. A Simple Network Management Protocol (SNMP)
RFC 1227. SNMP MUX Protocol and MIB
RFC 1905. Simple Network Management Protocol (SNMPv2)
RFC 2548. Microsoft Vendor-specific RADIUS Attributes (MS-CHAP v1 and v2)
RFC 2618. RADIUS Authentication Client MIB
RFC 2619. RADIUS Authentication Server MIB
RFC 2620. RADIUS Accounting Client MIB
RFC 2621. RADIUS Accounting Server MIB
RFC 2809. Compulsory Tunneling via RADIUS
RFC 2865. Remote Authentication Dial-In User Service
RFC 2866. RADIUS Accounting
RFC 2867. RADIUS Accounting Modifications for Tunnel Protocol Support
RFC 2868. RADIUS Attributes for Tunnel Protocol Support
RFC 2869. RADIUS Extensions
RFC 2882. NAS Requirements: Extended RADIUS Practices
802.1x: EAP-TTLS, EAP-PEAP, EAP-TLS, LEAP, EAP-MD5
SQL (Oracle, MySQL, PostgreSQL, Sybase, ODBC, etc)
[illegible]

implementations

CENTRAL GOVERNMENT

HEALTH SERVICES

WATER AND SEWERAGE

EMERGENCY SERVICES

NTP RADIUS Kerberos LDAP NFS CIFS DCE-RPC CORBA/IIOP HTTP SIP H.323 X.509 H.225 ISDN ATM JDBC X.25 X.400 IPv6 IPv4 ISAKMP L2TP PPTP PPP SMTP NNTP IRC OpenPGP MIME DIAMETER SSH GIF JPEG PNG WAP WML XML SOAP HTML RTF Jabber VCard DHCP DNS SunRPC SNMP X.509 Finger Telnet XMODEM H.245 Bluetooth

FINANCE

ENERGY

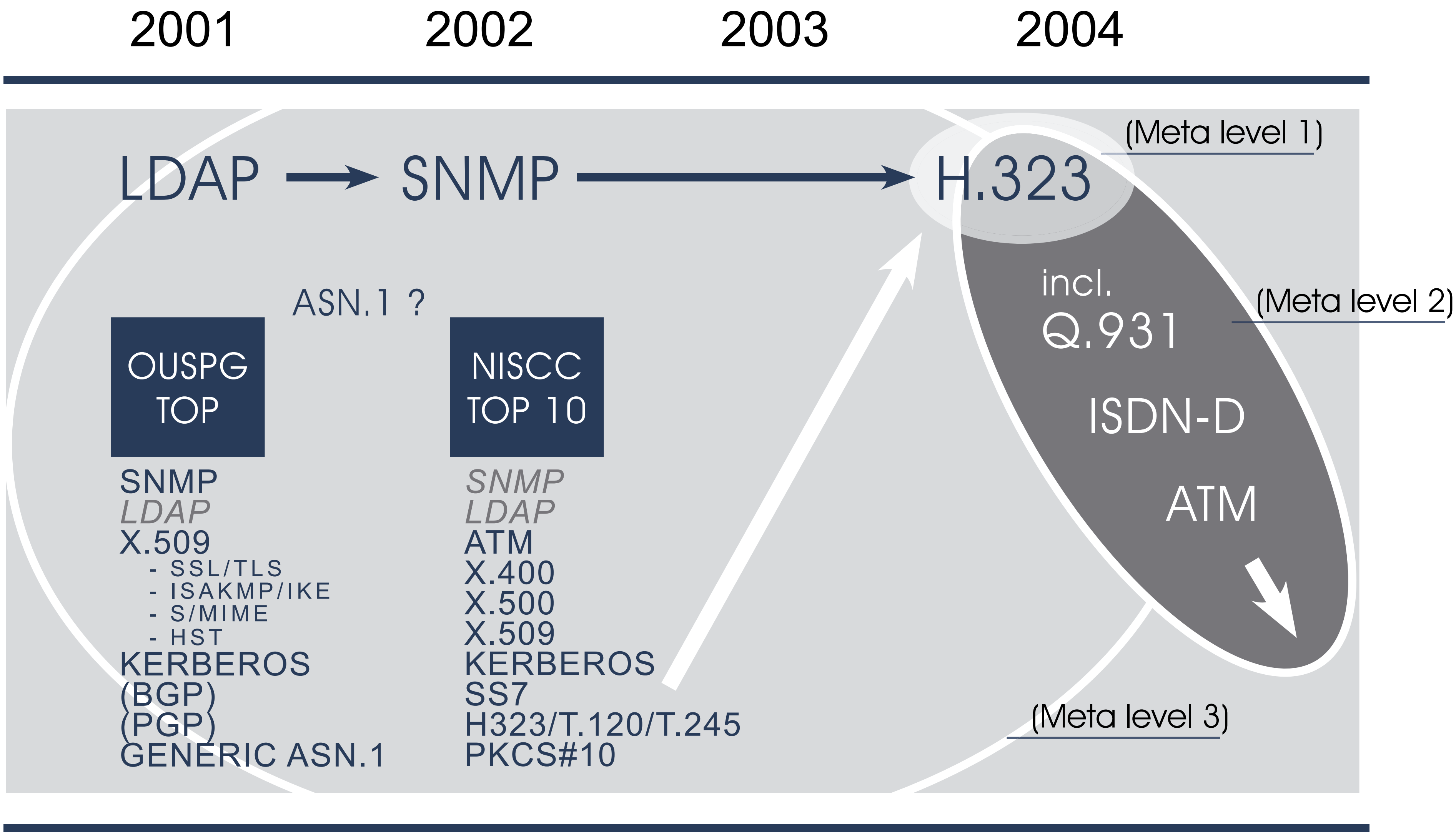
TRANSPORT

TELE-COMMUNICATIONS

chaos of protocols

PROTOS

TEST SUITE	TEST CASES	VENDORS
SNMP	29516/24100	140
SIP	4527	92
H.323	4497	34



2001 2002 2003 2004

LDAP → SNMP → H.323

(Meta level 1)

ASN.1 ?

OUSPG TOP

SNMP
LDAP
X.509
- SSL/TLS
- ISAKMP/IKE
- S/MIME
- HST
KERBEROS
(BGP)
(PGP)
GENERIC ASN.1

NISCC TOP 10

SNMP
LDAP
ATM
X.400
X.500
X.509
KERBEROS
SS7
H323/T.120/T.245
PKCS#10

incl.
Q.931
ISDN-D
ATM

(Meta level 2)

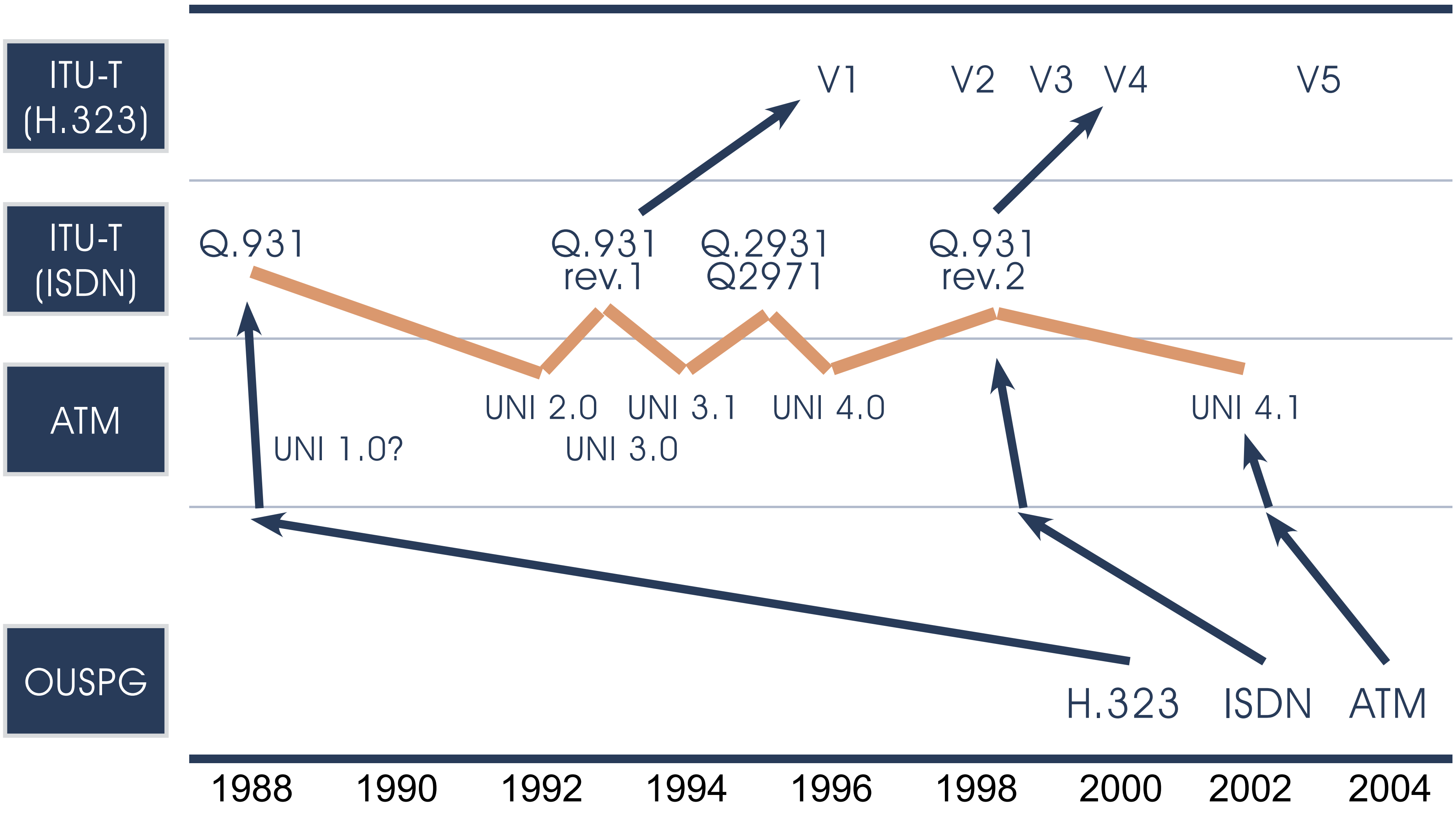
(Meta level 3)

can of worms

OUSPG META LEVEL 4	?
OUSPG META LEVEL 3	Single scheme in multiple protocols / protocol families
OUSPG META LEVEL 2	Single protocol embedded in multiple protocol families
OUSPG META LEVEL 1	Single protocol, multiple implementations by multiple vendors
TRADITIONAL APPROACH	Single vendor, single implementation, single vulnerability

<meta name=”ouspg-levels”>

SPECIFICATION HISTORY



ITU-T (H.323)

ITU-T (ISDN)

ATM

OUSPG

V1 V2 V3 V4 V5

Q.931

Q.931 rev.1

Q.2931 Q2971

Q.931 rev.2

UNI 1.0?

UNI 2.0

UNI 3.0

UNI 3.1

UNI 4.0

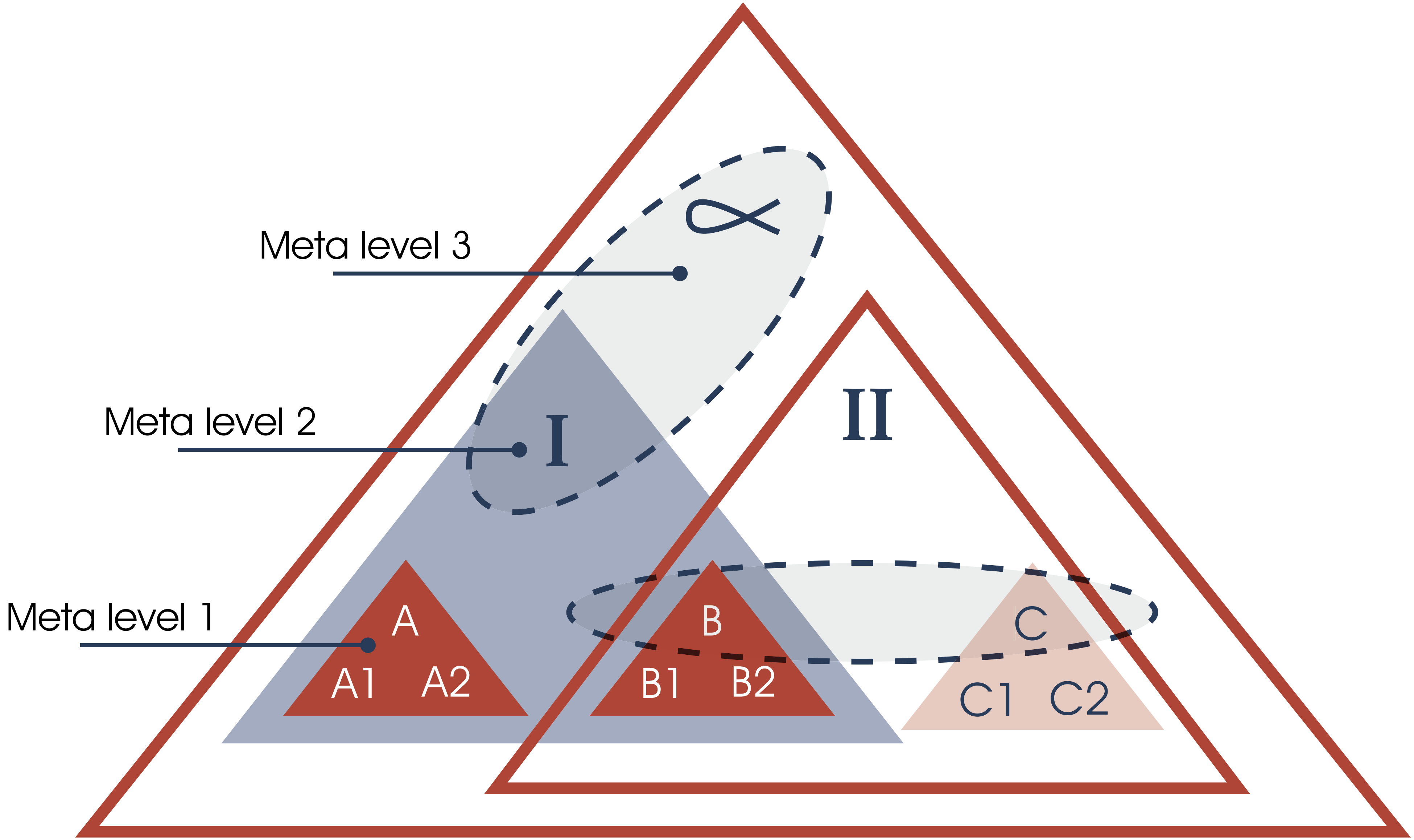
UNI 4.1

H.323 ISDN ATM

1988 1990 1992 1994 1996 1998 2000 2002 2004

VULNERABILITIES HISTORY

protocol view (H.323)



impact

PUBLIC ATTENTION

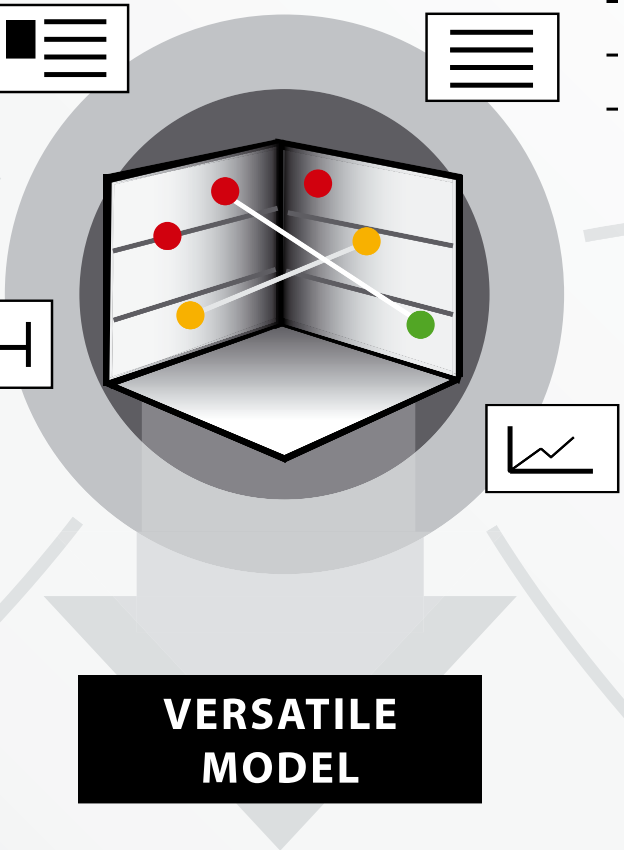
- media, mailing lists

PROTOCOL DEFINITIONS

- ITU-T
- ISO
- IETF

EXPERTS

- interviews
- communication strategy
- models of structuring information



THE PREVALENCE OF PROTOCOL IMPLEMENTATIONS

- market situation
- historical data
- usage environments

VERSATILE MODEL

points out, with respect to protocols

- dependencies
- relations
- structures
- problems relating to information security

and facilitates:

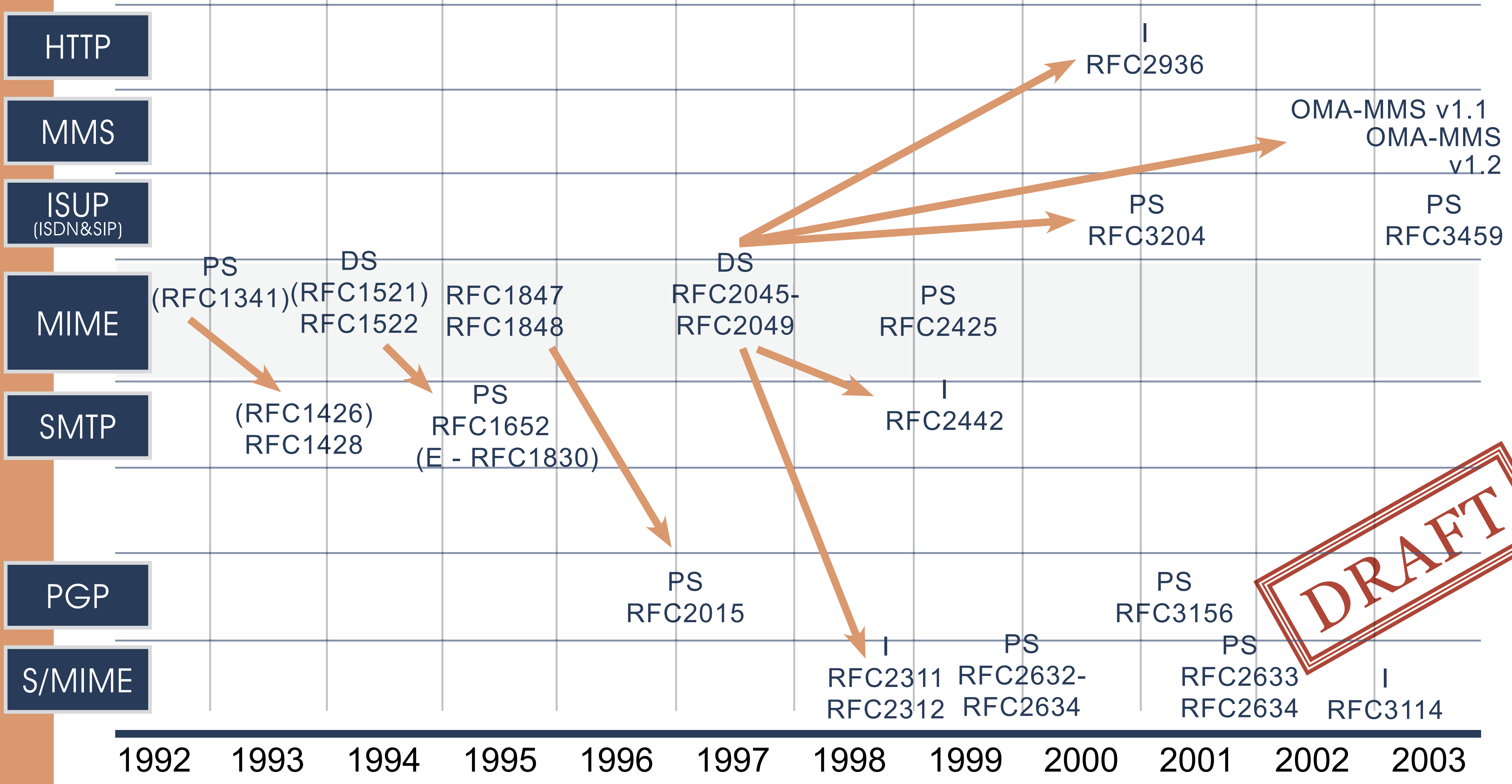
- strategic planning
- decision making
- communication
- coordination of information security research

1982 - RFC822
before MIME

MIME inside
SPECIFICATION HISTORY

case MIME

PS = Proposal standard, DS = Draft standard, I = Informational, E = Experimental



HTTP
I
RFC2936

MMS
OMA-MMS v1.1
OMA-MMS v1.2

ISUP (ISDN&SIP)
PS
RFC3204
PS
RFC3459

MIME
PS
(RFC1341)
DS
(RFC1521)
RFC1522
RFC1847
RFC1848
DS
RFC2045-
RFC2049
PS
RFC2425

SMTP
(RFC1426)
RFC1428
PS
RFC1652
(E - RFC1830)
I
RFC2442

PGP
PS
RFC2015
PS
RFC3156

S/MIME
I
RFC2311
RFC2312
PS
RFC2632-
RFC2634
PS
RFC2633
RFC2634
I
RFC3114

1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003

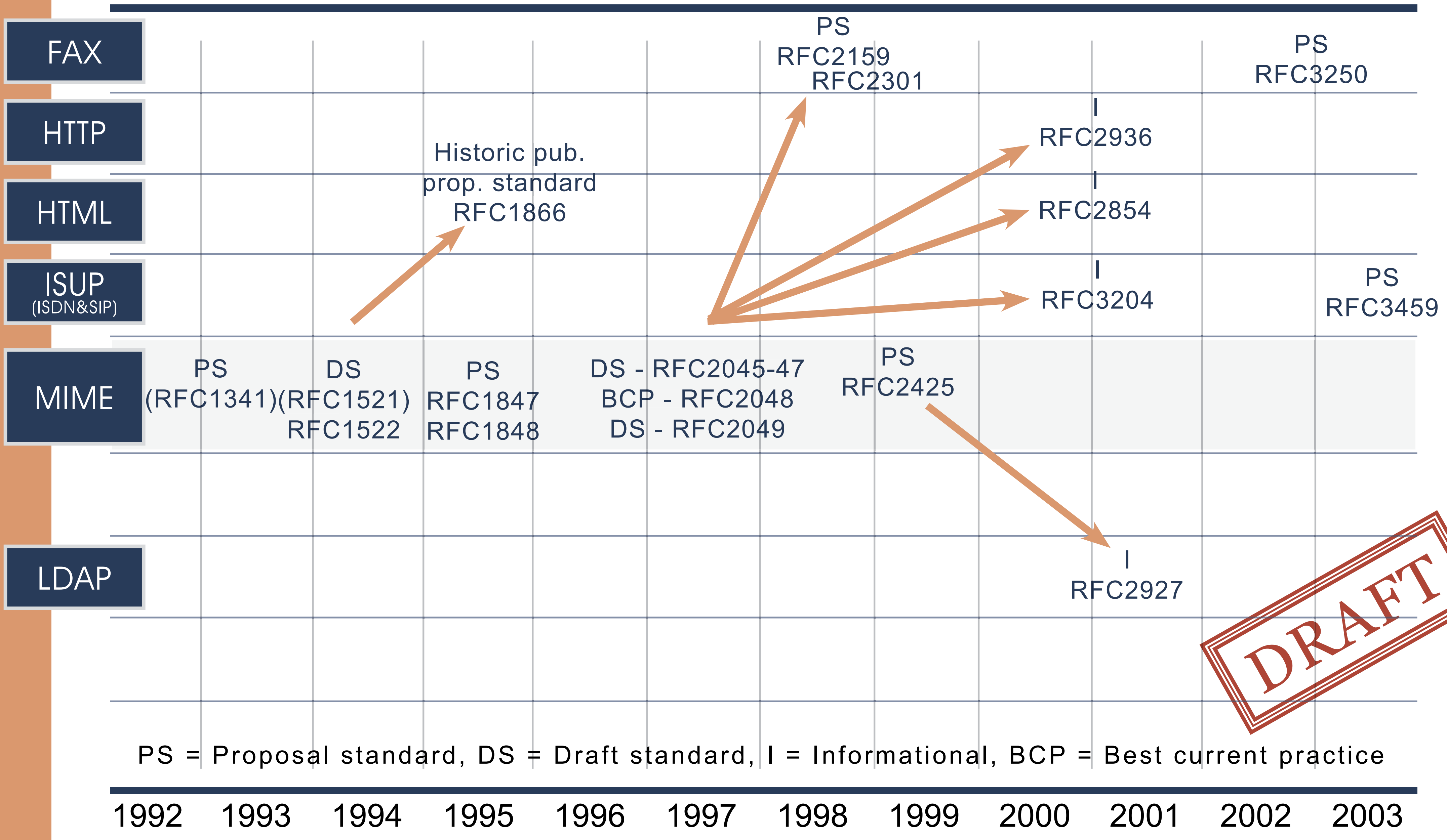
DRAFT

protocol view (MIME) 1/2

© Oulu University Secure Programming Group

1982 - RFC822
before MIME

inside MIME
SPECIFICATION HISTORY



FAX

PS
RFC2159
RFC2301

PS
RFC3250

HTTP

I
RFC2936

HTML

Historic pub.
prop. standard
RFC1866

I
RFC2854

ISUP
(ISDN&SIP)

I
RFC3204

PS
RFC3459

MIME

PS
(RFC1341)

DS
(RFC1521)
RFC1522

PS
RFC1847
RFC1848

DS - RFC2045-47
BCP - RFC2048
DS - RFC2049

PS
RFC2425

LDAP

I
RFC2927

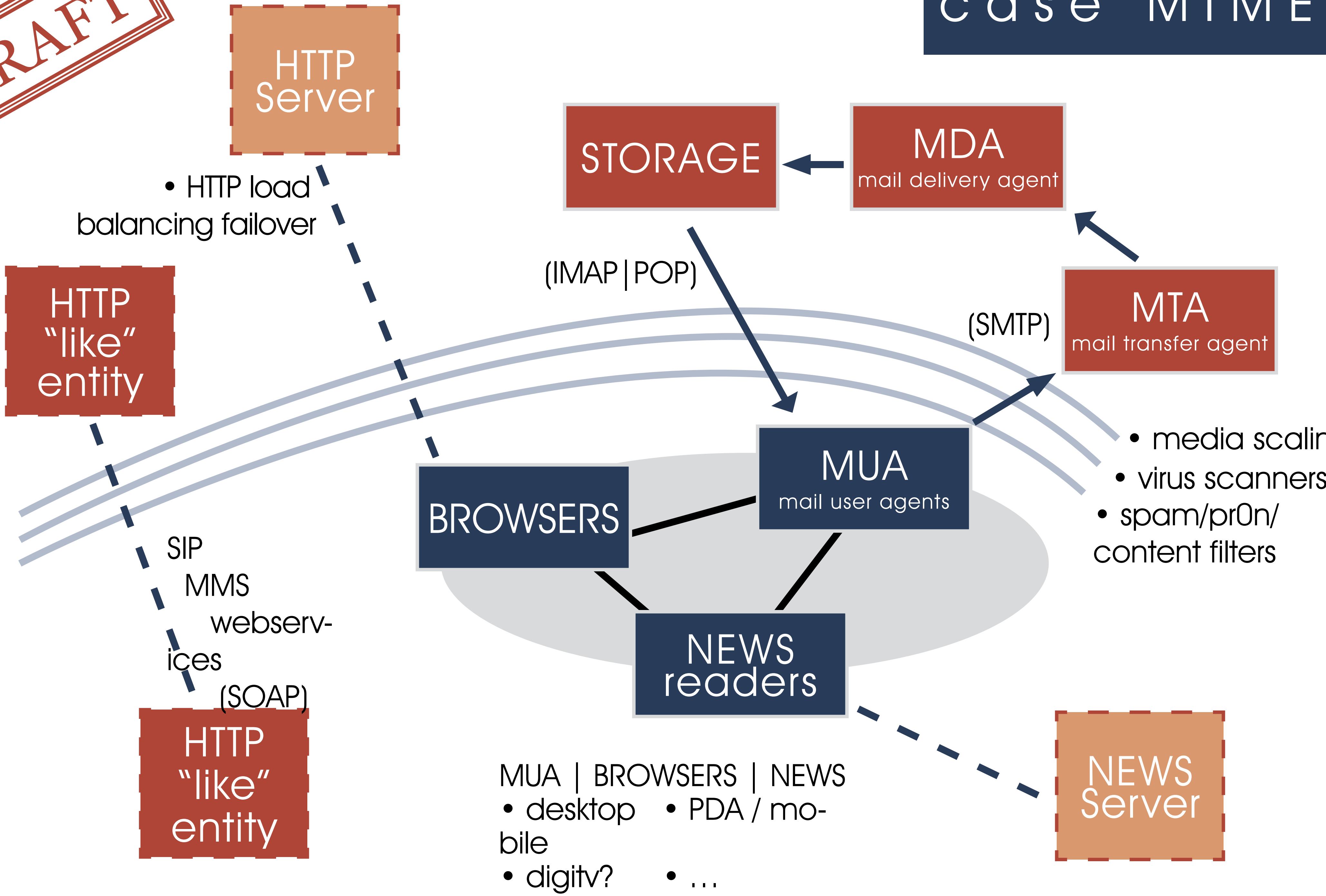
DRAFT

PS = Proposal standard, DS = Draft standard, I = Informational, BCP = Best current practice

1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003

protocol view (MIME) 2/2

case MIME



HTTP Server

• HTTP load balancing failover

HTTP "like" entity

SIP MMS webservices (SOAP)

HTTP "like" entity

STORAGE

MDA mail delivery agent

(IMAP|POP)

(SMTP)

MTA mail transfer agent

BROWSERS

MUA mail user agents

NEWS readers

NEWS Server

• media scalin
• virus scanners
• spam/pr0n/ content filters

MUA | BROWSERS | NEWS
• desktop • PDA / mobile
• digitv? • …

tech/usage view (MIME)

THE END

http://www.ee.oulu.fi/research/ouspg/