



ATS - TELCOM PRAHA a.s.®

TELEKOMUNIKAČNÍ SPOLEČNOST



Zabezpečená videokonference a hlas v IP a GSM komunikačním prostředí



Jiří DOUŠA
Červen 2014

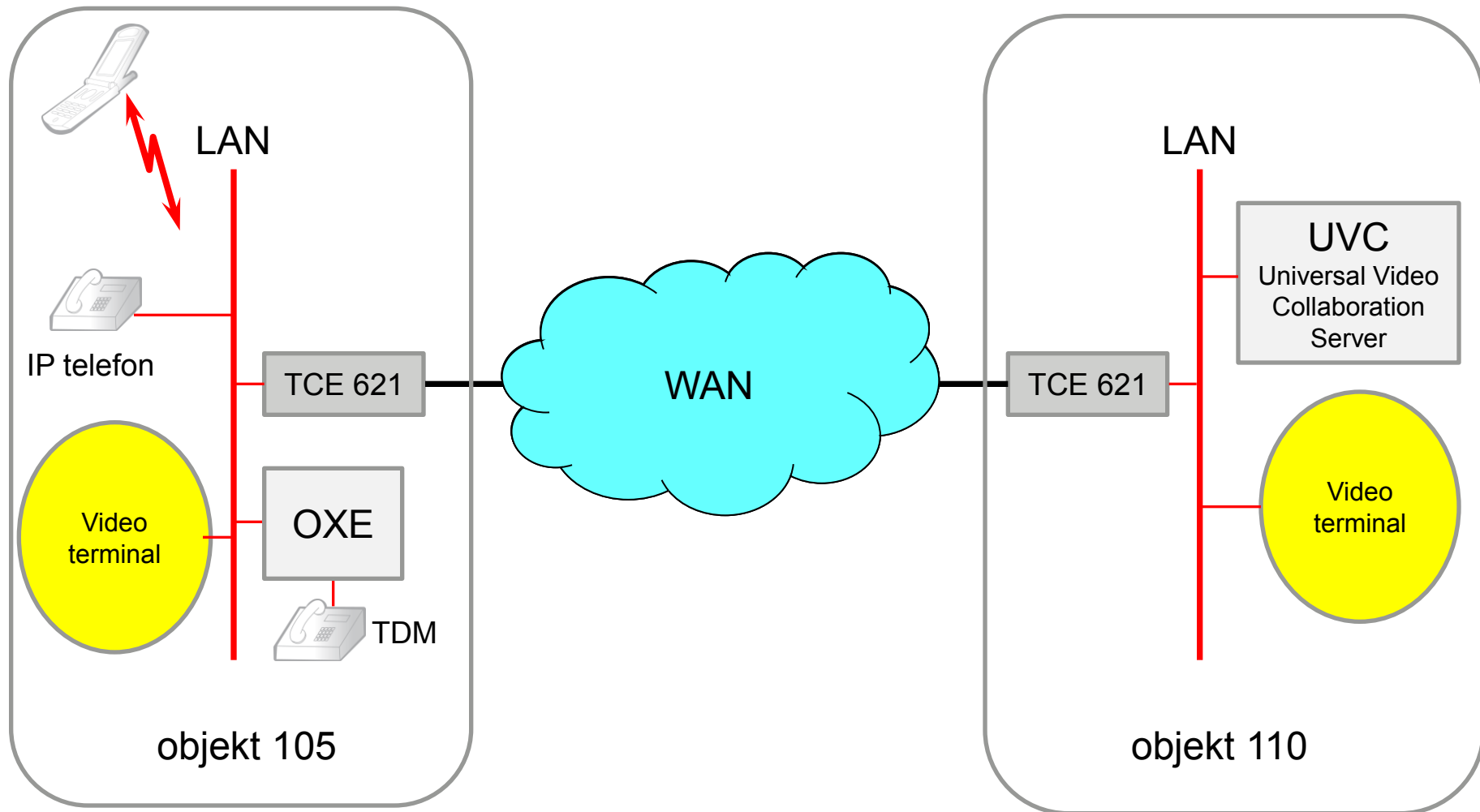
Agenda

1. IP šifrátory pro zabezpečení videokonference
2. Požadavky na IP šifrátory
3. Cryptel IP[®] řešení
4. Zabezpečený hlas a SMS v GSM síti
5. Sectra Panthon[®] 3 řešení
6. Kontakty a služby

IP šifrátořy pro zabezpečení videokonference

1. Proč utajovat videokonferenční datový přenos
 - modifikace dat během přenosu, podsunutí dat
 - virtuální jednací místnost - chybí osobní kontakt
 - únik informace
 - ochrana klasifikovaných informací podle zákona č. 412/2005 Sb.
2. V pevných IP datových sítích
 - IP šifrátor odděluje červenou LAN od černé WAN
 - data v červené síti chrání další vrstva utajení (síťové prvky, videokonferenční terminál)
 - u klasifikovaných dat je vyžadováno fyzické zabezpečení
 - šifrátořy mají nezávislou správu (jsou součástí zabezpečených IP sítí)

IP šifrátoři pro zabezpečení videokonference



Nezabezpečená IP komunikace

The image shows a Wireshark network traffic capture window. The title bar reads "Capturing from Broadcom NetXtreme Gigabit Ethernet Driver - Wireshark". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, and Help. The toolbar contains various icons for file operations, search, and capture control. The filter field is empty, and the expression field is set to "Expression... Clear Apply".

No.	Time	Source	Destination	Protocol	Info
404	274.565154	172.20.30.2	172.20.20.30	RTCP	Receiver Report Source description Application specific (LS) subtype=0
405	274.565156	172.20.30.2	172.20.20.30	RTCP	Receiver Report Source description Application specific (LS) subtype=0
406	274.586154	172.20.30.2	172.20.20.30	TCP	61742 > 60952 [ACK] Seq=922 Ack=752 Win=5632 Len=0 TSV=177317 TSER=114760
407	274.600784	172.20.30.2	172.20.20.30	RTP	PT=DynamicRTP-Type-113, SSRC=0x254D81CC, Seq=31610, Time=7500
408	274.639994	172.20.30.2	172.20.20.30	RTP	PT=DynamicRTP-Type-113, SSRC=0x254D81CC, Seq=31620, Time=8533
410	274.680537	172.20.20.30	172.20.30.2	H.245	openLogicalChannelAck
411	274.680541	172.20.30.2	172.20.20.30	TCP	61742 > 60952 [ACK] Seq=922 Ack=779 Win=5632 Len=0 TSV=177327 TSER=114775
412	274.688694	172.20.20.30	172.20.30.2	H.245	flowControlCommand
413	274.688698	172.20.30.2	172.20.20.30	TCP	61742 > 60952 [ACK] Seq=922 Ack=790 Win=5632 Len=0 TSV=177328 TSER=114776
414	274.699732	172.20.30.2	172.20.20.30	RTP	PT=DynamicRTP-Type-113, SSRC=0x254D81CC, Seq=31622, Time=10581
415	274.729711	172.20.30.2	172.20.20.30	RTP	PT=DynamicRTP-Type-113, SSRC=0x254D81CC, Seq=31623, Time=11605
416	274.751640	172.20.20.30	172.20.30.2	H.245	openLogicalChannelAck
417	274.751879	172.20.30.2	172.20.20.30	TCP	61742 > 60952 [ACK] Seq=922 Ack=817 Win=5632 Len=0 TSV=177335 TSER=114782
418	274.760366	172.20.30.2	172.20.20.30	RTP	EventPayload type=RTP Event, Unknown (126)
419	274.762335	172.20.20.30	172.20.30.2	H.245	flowControlCommand
420	274.762571	172.20.30.2	172.20.20.30	TCP	61742 > 60952 [ACK] Seq=922 Ack=828 Win=5632 Len=0 TSV=177336 TSER=114783
421	274.766770	172.20.30.2	172.20.20.30	RTP	EventPayload type=RTP Event, Unknown (126)
422	274.769440	172.20.30.2	172.20.20.30	RTP	PT=DynamicRTP-Type-113, SSRC=0x254D81CC, Seq=31624, Time=12629
423	274.799713	172.20.30.2	172.20.20.30	RTP	PT=DynamicRTP-Type-113, SSRC=0x254D81CC, Seq=31625, Time=13653
424	274.829833	172.20.30.2	172.20.20.30	RTP	PT=DynamicRTP-Type-113, SSRC=0x254D81CC, Seq=31626, Time=14677
425	274.859749	172.20.30.2	172.20.20.30	RTP	PT=DynamicRTP-Type-113, SSRC=0x254D81CC, Seq=31627, Time=15701
426	274.889941	172.20.30.2	172.20.20.30	RTP	PT=DynamicRTP-Type-113, SSRC=0x254D81CC, Seq=31628, Time=16725
427	274.929760	172.20.30.2	172.20.20.30	RTP	PT=DynamicRTP-Type-113, SSRC=0x254D81CC, Seq=31629, Time=17749
428	274.959752	172.20.30.2	172.20.20.30	RTP	PT=DynamicRTP-Type-113, SSRC=0x254D81CC, Seq=31630, Time=18773
429	274.989771	172.20.30.2	172.20.20.30	RTP	PT=DynamicRTP-Type-113, SSRC=0x254D81CC, Seq=31631, Time=19797
430	275.019493	172.20.30.2	172.20.20.30	RTP	PT=DynamicRTP-Type-113, SSRC=0x254D81CC, Seq=31632, Time=20821

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

- IEEE 802.3 Ethernet
- Logical-Link Control
- Spanning Tree Protocol

```
0000 01 80 c2 00 00 00 09 7c f3 6f c1 00 26 42 42 .....|.o.&BB
0010 03 00 00 00 00 00 80 00 09 7c f3 6f ca 00 00 .....|.o...
0020 00 00 80 00 00 09 7c f3 6f ca 80 01 00 00 14 00 .....|.o.....
0030 02 00 0f 00 00 00 00 00 00 00 00 .....|.....
```

Broadcom NetXtreme Gigabit Ethernet Driver: <li... Packets: 80229 Displayed: 80229 Marked: 0 Profile: Default

Zabezpečená IP komunikace

Wireshark capture showing network traffic. The highlighted packet (No. 68) is an ESP packet from 192.168.20.2 to 192.168.20.1.

No.	Time	Source	Destination	Protocol	Info
62	8.755555	192.168.20.1	192.168.20.2	ESP	ESP (SPI=0x3e010070)
63	8.755822	192.168.20.2	192.168.20.1	ESP	ESP (SPI=0x3e010070)
64	9.526090	192.168.20.2	192.168.20.1	ESP	ESP (SPI=0x3e010070)
65	9.526645	192.168.20.1	192.168.20.2	ESP	ESP (SPI=0x3e010070)
66	9.533849	Cisco_a3:8a:17	Spanning-tree-(for-STP	Conf.	Root = 32768/5/00:13:19:a3:8a:00 Cost = 0 Port = 0x8017
67	9.769073	192.168.20.1	192.168.20.2	ESP	ESP (SPI=0x3e010070)
68	9.769854	192.168.20.2	192.168.20.1	ESP	ESP (SPI=0x3e010070)
69	10.540623	192.168.20.1	192.168.20.2	ESP	ESP (SPI=0x3e010070)
70	10.540623	192.168.20.1	192.168.20.2	ESP	ESP (SPI=0x3e010070)
71	10.783356	192.168.20.1	192.168.20.2	ESP	ESP (SPI=0x3e010070)
72	10.783871	192.168.20.2	192.168.20.1	ESP	ESP (SPI=0x3e010070)
73	11.533973	Cisco_a3:8a:17	Spanning-tree-(for-STP	Conf.	Root = 32768/5/00:13:19:a3:8a:00 Cost = 0 Port = 0x8017
74	11.554092	192.168.20.2	192.168.20.1	ESP	ESP (SPI=0x3e010070)
75	11.554281	192.168.20.1	192.168.20.2	ESP	ESP (SPI=0x3e010070)
76	11.797338	192.168.20.1	192.168.20.2	ESP	ESP (SPI=0x3e010070)
77	11.797813	192.168.20.2	192.168.20.1	ESP	ESP (SPI=0x3e010070)
78	12.568053	192.168.20.2	192.168.20.1	ESP	ESP (SPI=0x3e010070)
79	12.568582	192.168.20.1	192.168.20.2	ESP	ESP (SPI=0x3e010070)
80	12.811095	192.168.20.1	192.168.20.2	ESP	ESP (SPI=0x3e010070)
81	12.811865	192.168.20.2	192.168.20.1	ESP	ESP (SPI=0x3e010070)
82	13.533930	Cisco_a3:8a:17	Spanning-tree-(for-STP	Conf.	Root = 32768/5/00:13:19:a3:8a:00 Cost = 0 Port = 0x8017
83	13.582143	192.168.20.2	192.168.20.1	ESP	ESP (SPI=0x3e010070)
84	13.582694	192.168.20.1	192.168.20.2	ESP	ESP (SPI=0x3e010070)
85	13.825302	192.168.20.1	192.168.20.2	ESP	ESP (SPI=0x3e010070)
86	13.825783	192.168.20.2	192.168.20.1	ESP	ESP (SPI=0x3e010070)
87	14.596072	192.168.20.2	192.168.20.1	ESP	ESP (SPI=0x3e010070)
88	14.596634	192.168.20.1	192.168.20.2	ESP	ESP (SPI=0x3e010070)
89	14.839380	192.168.20.1	192.168.20.2	ESP	ESP (SPI=0x3e010070)

Frame 1: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits)
Ethernet II, Src: ThomsonC_25:66:94 (00:80:ee:25:66:94), Dst: ThomsonC_25:64:c8 (00:80:ee:25:64:c8)
Internet Protocol, Src: 192.168.20.2 (192.168.20.2), Dst: 192.168.20.1 (192.168.20.1)
Encapsulating Security Payload

```
0000 00 80 ee 25 64 c8 00 80 ee 25 66 94 08 00 45 00 ...%d... .%f...E.  
0010 00 70 81 d2 00 00 28 32 67 36 c0 a8 14 02 c0 a8 ...p...(2 g6.....  
0020 14 01 3e 01 00 70 00 00 00 00 2a d0 5f b8 fe e1 ...>.p. : *..._.  
0030 31 12 b3 ef f1 fc 3b 60 87 16 a5 97 94 dc c6 29 1.....: .....  
0040 19 f9 08 5c c6 ba 72 80 3c 74 fd 24 5e 46 d5 d2 ...\.r. <L.$^F..  
0050 00 06 02 0c 01 71 62 20 73 20 f6 82 f0 16 00 b4 .....(b) 20
```

Požadavky na IP šifrátořy pro zabezpečení videokonference

1. Plná podpora multicastového provozu (point – to –multipoint), klíče a správa šifrátořů
2. Plná podpora QoS (priorita voice a video paketů), řazení paketů vč. sekvenčních čísel paketů
3. Plný duplex, podpora rychlostí 10/100/1000 Mbit/s
4. Pro klasifikovaná data certifikace od NBÚ
5. Požadavky na síť
 - trastrované síť, podpora QoS, lze využívat pro klasifikovaná data vyšších stupňů utajení
 - veřejné síť (internet) omezení z hlediska QoS a dostupnosti služeb

Využití kryptografického systému Cryptel®-IP



1. TCE 621B/C a TCE 621B/C CZ - IP kryptografické prostředky
2. plně HW on-line KP, určený pro kryptografickou ochranu informací na úrovni IP s přenosovou rychlostí do 100 Mbit/s (B), 1000 Mb/s (C)
3. CZ představují národní verzi na bázi komponent TCE 621
4. podpora IPv4 i IPv6 a NAT (pomocí UDP zapouzdření), zálohování vytvořením virtuálních KP, zabezpečený multicast
5. Mechanické provedení je v souladu s SDIP 27- level A (TEMPEST)
6. rozhraní Ethernet metalické/optické
7. v ČR certifikovány pro utajované informace od NATO Confidential, Confidential UE, Důvěrné až po Přísně Tajné, COSMIC TOP SECRET

Mobilní IP šifrátory pro mobilní videokonferenční terminál

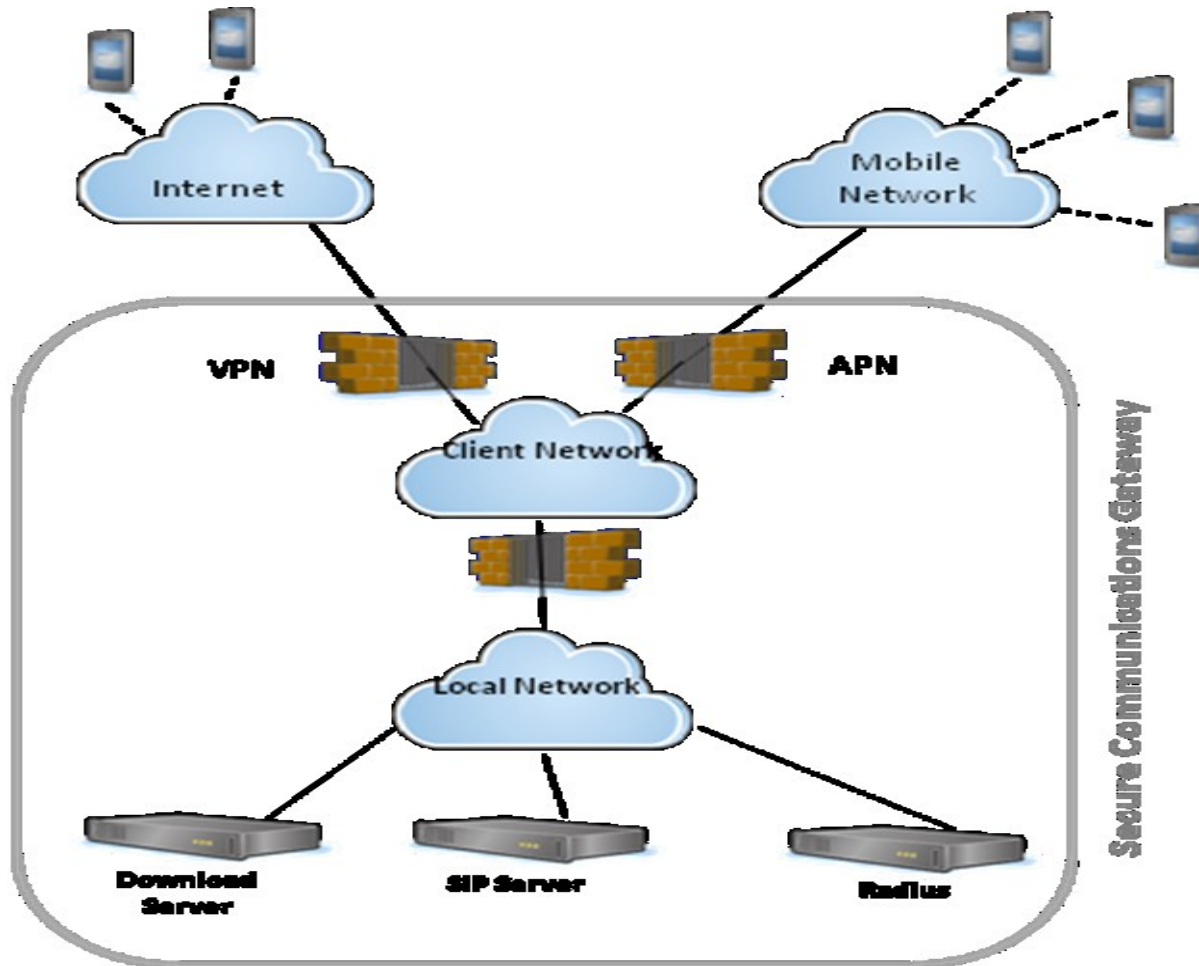


1. Pro mobilně zřizovaný terminál,
2. Mobilní IP kryptografický prostředek, plně kompatibilní s TCE 621 B (C)
3. Podporuje statické i dynamické přidělování IP adres na straně neutajované sítě
4. Na černé straně se připojí k datové síti (WiFi, GSM brána, metalika apod.)
5. mechanické provedení je v souladu s SDIP 27- level A
6. rozhraní Ethernet metalické/optické
7. v ČR v procesu certifikace; je certifikován v NATO do stupně SECRET

Zabezpečený hlas a SMS v GSM síti

1. Síť GSM - omezení z hlediska přenosové rychlosti (od 2G), QoS a dostupnosti signálu, výpadky, přetížení sítě
2. IP šifrátor je součástí terminálu (mobilního telefonu, tabletu apod)
3. Utajení End-to End
4. Komunikace přes gateway (servery zajišťující spojení)
5. Možnost využití GSM i internetových sítí (WiFi)
6. Řešení IP šifrátoru kombinací SW a HW
7. Aplikace a SD karta do smartphonu
8. Požadavky na rychlosti přenosu IP paketů (voice, obraz)
9. Šifrované SMS je možno zasílat standardním SMS kanálem
10. Vyšší nároky na ochranu mobilních terminálů (organizační a technické)

Zabezpečený hlas a SMS v GSM síti



Sectra Panthon[®] 3

1. Utajovač Panthon[®] 3 je implementován do standardních mobilních telefonů s operačním systémem Android
2. Bezpečnostně významné operace jsou zpracovávány a ukládány v přidaném HW
3. Aplikace Panthon je instalována v mobilním telefonu
4. Mobilní telefon lze využívat i jako standardní mobilní telefon
5. SMS zprávy šifrovány off-line a posílány standardním SMS kanálem v prostředí GSM
6. Hlasová komunikace on-line s utajením End-to-End
7. Panthon vyžaduje podpůrnou infrastrukturu - bezpečnostní komunikační bránu (SCGW),

Sectra Panthon® 3

1. Technická podpora ochrany
 - bezpečnostní brána SCGW (firewally, politika, audit)
 - CRL (black list)
 - správa kontaktů z SCGW
 - white list (brání instalaci nebezpečných aplikací a škodlivého SW)
 - otevřená data pouze po dobu aktivního stavu
 - omezení počtu pokusů o zadání PIN
 - automatické ukončování aplikace
2. Certifikováno NBÚ pro ochranu utajovaných informací
 - Vyhrazené (č. certifikátu K20154)
 - Vyhrazené, EU RESTRICTED (č. certifikátu K20163)

Kontakty a služby

ATS-TELCOM PRAHA a.s.

- Informace k systémům Cryptel[®]-IP a Sectra Panthon[®] 3
- Podpora při projektování, nasazování a provozu systémů
- Servis
- Školení správců a uživatelů
- Testovací sestavy
- Kontakty:
Jiří Douša, tel: 602 573 270, e-mail: dousa@atstelcom.cz
Karel Bouchner, tel: 602 390 903, e-mail: bouchner@atstelcom.cz
Jiří Tecl, tel: 602 246 653, e-mail: tecl@atstelcom.cz
Jan Sedlák, tel: 602 246 650, e-mail: sedlak@atstelcom.cz