DeepSec
2018

SS7 for INFOSEC

Paul Coggin

@Paul Coggin

What is SS7

SS7/C7 is to PSTN what BGP routing protocol is to Internet

- Created by AT&T in 1975
- Adopted as standard in 1980
- SS7 – North America
- C7 – Utilized outside of North America
- SS7 protocol is utilized whenever a call leaves the local exchange carrier switch.
- Setups up call and reserves required resources end to end.
- Cell phones use SS7/C7 to verify subscribers(roaming, International, register and authenticate, not stolen)
- E911
- Caller-id
- SMS
- Call block
- Many other services

Reference: Signaling System No.7 (SS7/C7) Protocol, Architecture, and Services, Lee Dryburgh, Jeff Hewett, Cisco Press

SS7 Node Types

SS7 is comprised of signal point(SP) nodes with point code(PC) identifiers.

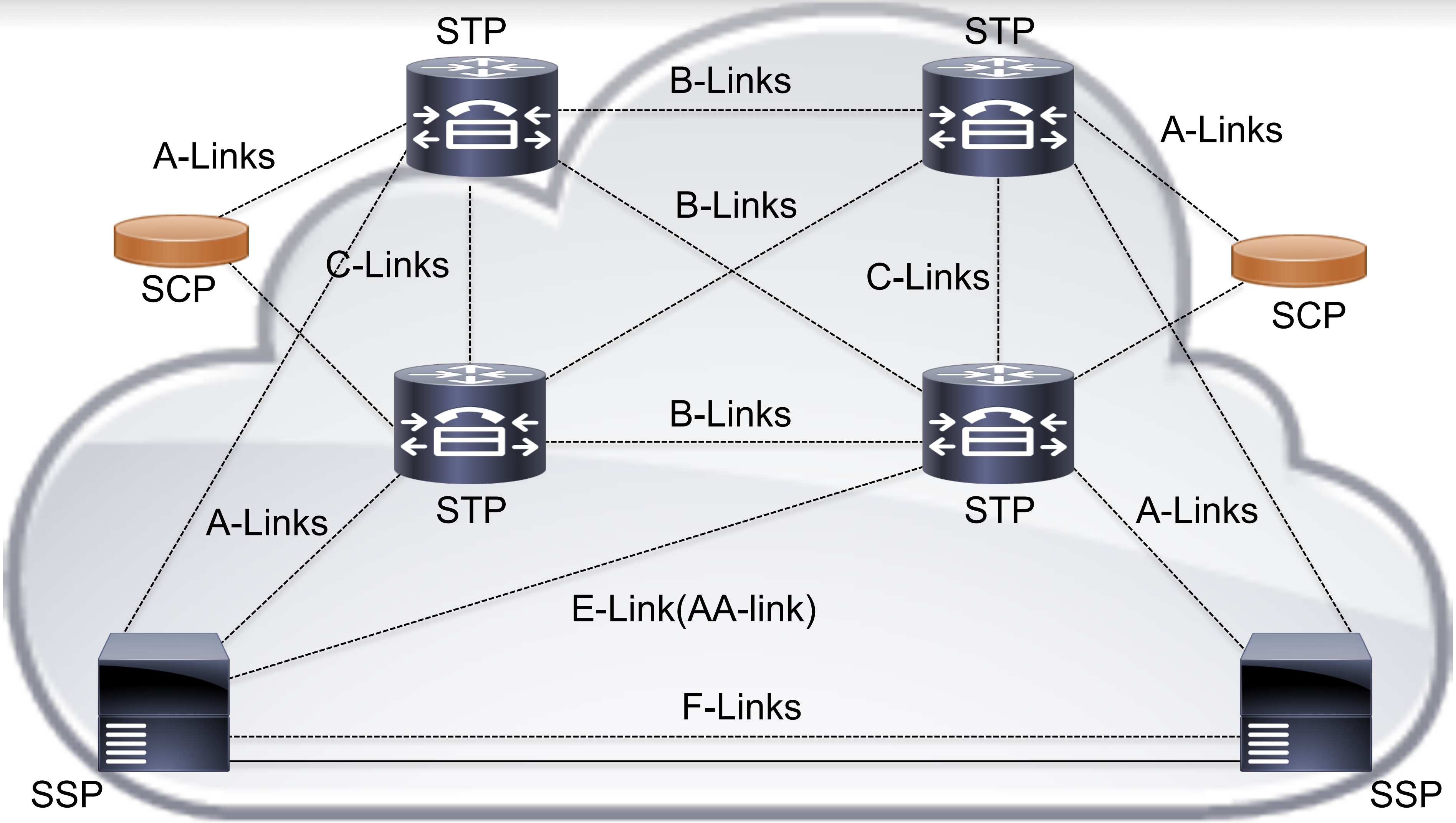
Signal Transfer Point (STP) – Routes SS7 messages between the SS7 nodes. STP has access control list filtering capabilities.

Service Switching Point (SSP) – Carrier telephone switch that processes various end point PSTN services such as voice, fax and modem.

Service Control Point (SCP) – Integrates the SS7 network with the databases that contain information regarding services such as 800 numbers, mobile subscribers, calling cards and other services.

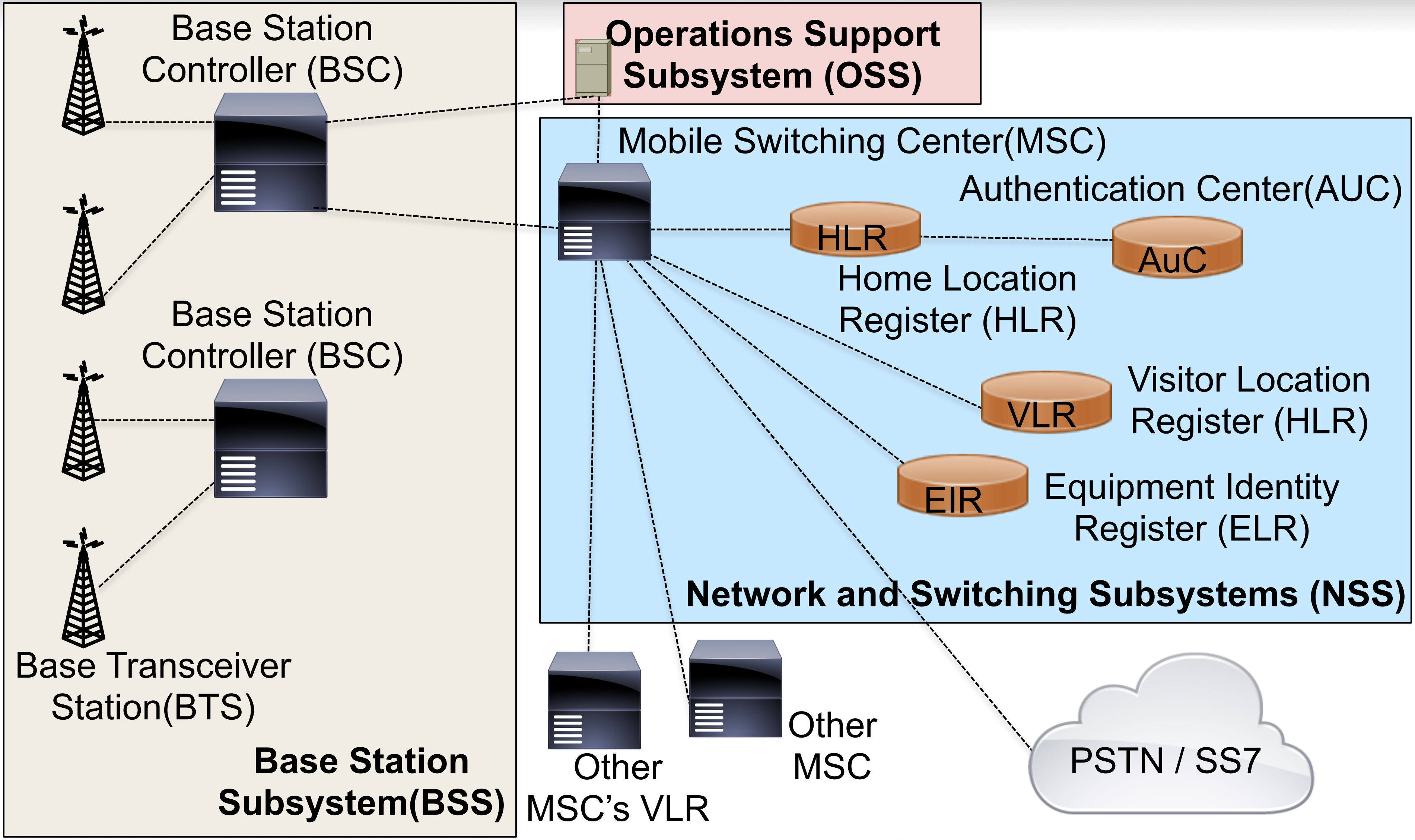
Reference: Signaling System No.7 (SS7/C7) Protocol, Architecture, and Services, Lee Dryburgh, Jeff Hewett, Cisco Press

SS7 Network Architecture



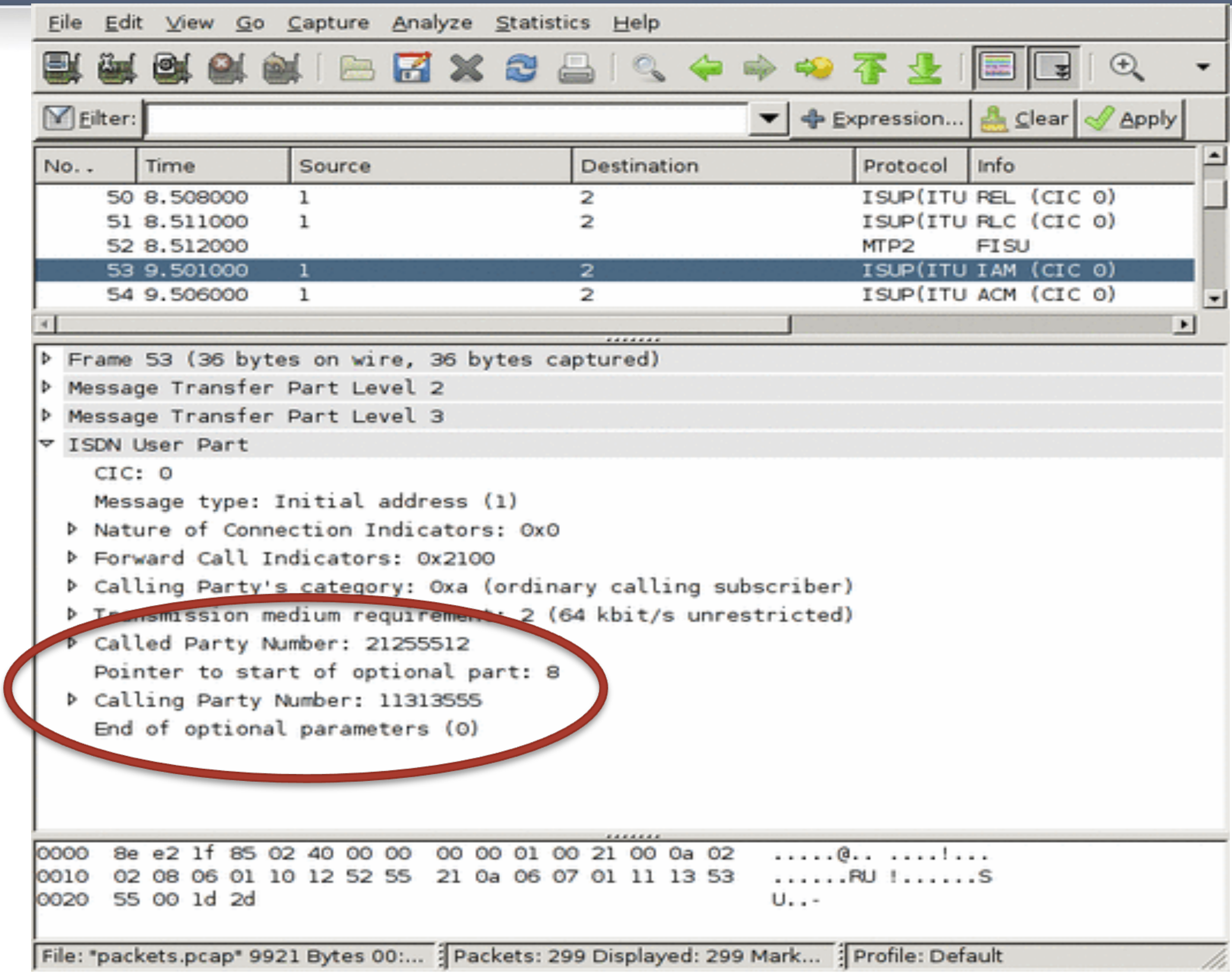
Reference: Voice Over IP Fundamentals, Cisco Press

Cellular Network Architecture



Reference: Signaling System No.7 (SS7/C7) Protocol, Architecture, and Services, Lee Dryburgh, Jeff Hewett, Cisco Press

SS7 Packet Capture



```
No. .  Time      Source   Destination   Protocol  Info
   50 8.508000   1        2             ISUP(ITU REL (CIC 0)
   51 8.511000   1        2             ISUP(ITU RLC (CIC 0)
   52 8.512000                          MTP2     FISU
   53 9.501000   1        2             ISUP(ITU IAM (CIC 0)
   54 9.506000   1        2             ISUP(ITU ACM (CIC 0)
```

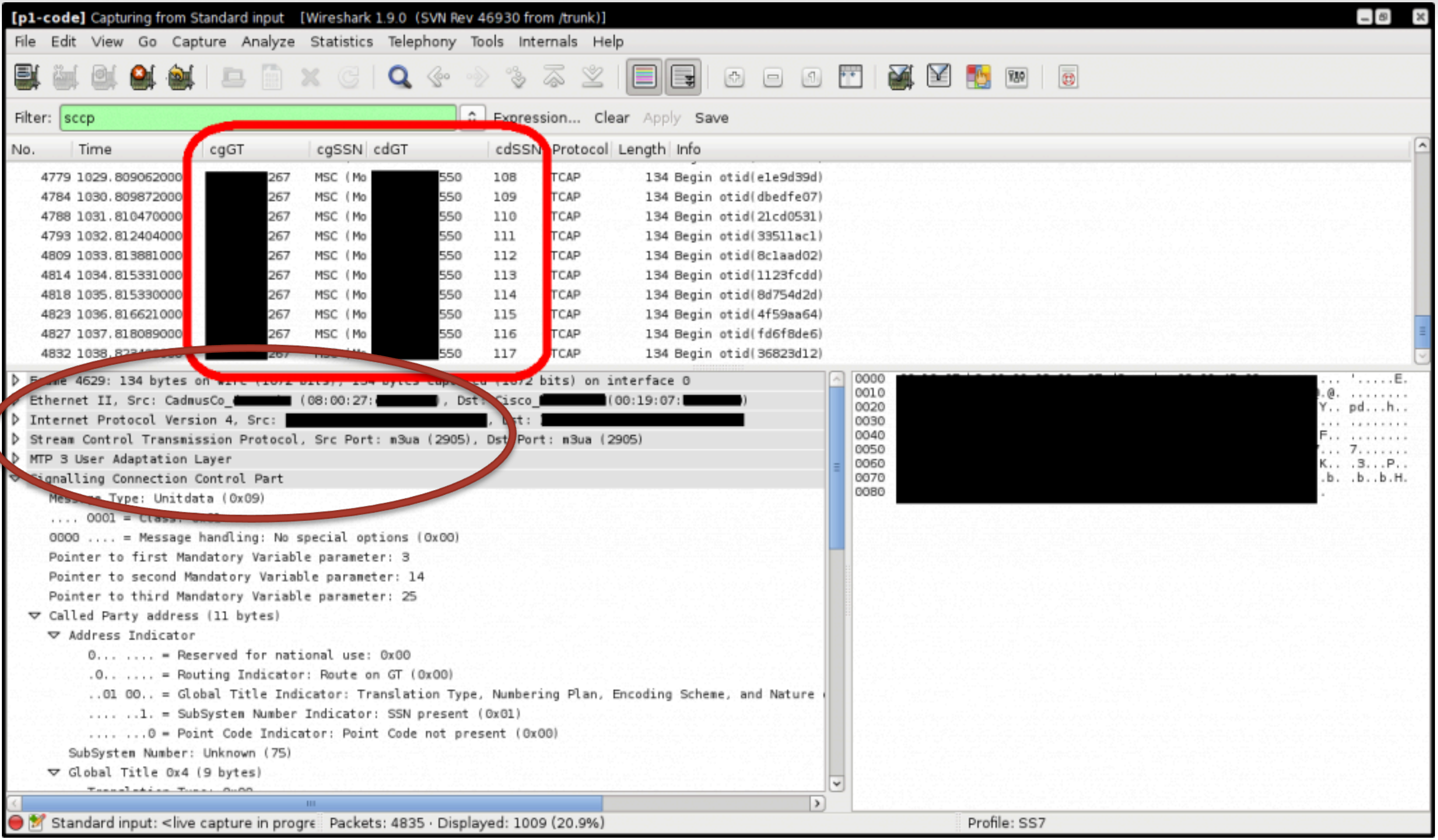
```
▷ Frame 53 (36 bytes on wire, 36 bytes captured)
▷ Message Transfer Part Level 2
▷ Message Transfer Part Level 3
▽ ISDN User Part
    CIC: 0
    Message type: Initial address (1)
  ▷ Nature of Connection Indicators: 0x0
  ▷ Forward Call Indicators: 0x2100
  ▷ Calling Party's category: 0xa (ordinary calling subscriber)
  ▷ Transmission medium requirement: 2 (64 kbit/s unrestricted)
  ▷ Called Party Number: 21255512
    Pointer to start of optional part: 8
  ▷ Calling Party Number: 11313555
    End of optional parameters (0)
```

```
0000  8e e2 1f 85 02 40 00 00  00 00 01 00 21 00 0a 02   .....@.. ....!...
0010  02 08 06 01 10 12 52 55  21 0a 06 07 01 11 13 53   ......RU !......S
0020  55 00 1d 2d                                        U..-
```

File: "packets.pcap" 9921 Bytes 00:... | Packets: 299 Displayed: 299 Mark... | Profile: Default

Reference: https://www.corelatus.com/gth/api/save_to_pcap/index.html

SIGTRAN Packet Capture



[p1-code] Capturing from Standard input [Wireshark 1.9.0 (SVN Rev 46930 from /trunk)]

Filter: sccp

```
No.   Time             cgGT             cgSSN     cdGT             cdSSN  Protocol  Length  Info
4779  1029.809062000   [redacted]267    MSC (Mo   [redacted]550    108    TCAP      134 Begin otid(e1e9d39d)
4784  1030.809872000   [redacted]267    MSC (Mo   [redacted]550    109    TCAP      134 Begin otid(dbedfe07)
4788  1031.810470000   [redacted]267    MSC (Mo   [redacted]550    110    TCAP      134 Begin otid(21cd0531)
4793  1032.812404000   [redacted]267    MSC (Mo   [redacted]550    111    TCAP      134 Begin otid(33511ac1)
4809  1033.813881000   [redacted]267    MSC (Mo   [redacted]550    112    TCAP      134 Begin otid(8c1aad02)
4814  1034.815331000   [redacted]267    MSC (Mo   [redacted]550    113    TCAP      134 Begin otid(1123fcdd)
4818  1035.815330000   [redacted]267    MSC (Mo   [redacted]550    114    TCAP      134 Begin otid(8d754d2d)
4823  1036.816621000   [redacted]267    MSC (Mo   [redacted]550    115    TCAP      134 Begin otid(4f59aa64)
4827  1037.818089000   [redacted]267    MSC (Mo   [redacted]550    116    TCAP      134 Begin otid(fd6f8de6)
4832  1038.823         [redacted]267    MSC (Mo   [redacted]550    117    TCAP      134 Begin otid(36823d12)
```

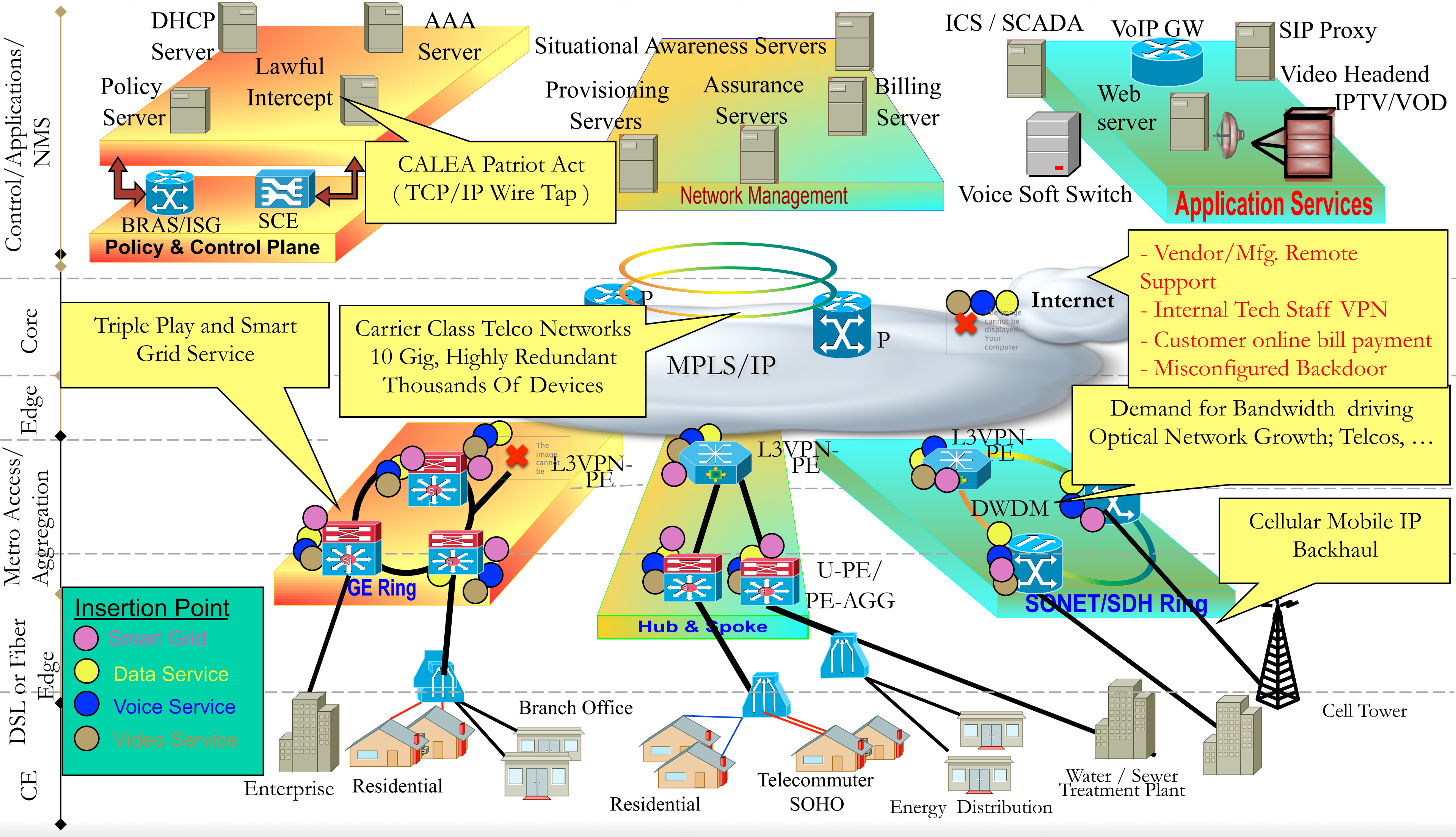
```
▷ Frame 4629: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0
▷ Ethernet II, Src: CadmusCo_[redacted] (08:00:27:[redacted]), Dst: Cisco_[redacted](00:19:07:[redacted])
▷ Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
▷ Stream Control Transmission Protocol, Src Port: m3ua (2905), Dst Port: m3ua (2905)
▷ MTP 3 User Adaptation Layer
▽ Signalling Connection Control Part
    Message Type: Unitdata (0x09)
    .... 0001 = Class: 0x01
    0000 .... = Message handling: No special options (0x00)
    Pointer to first Mandatory Variable parameter: 3
    Pointer to second Mandatory Variable parameter: 14
    Pointer to third Mandatory Variable parameter: 25
  ▽ Called Party address (11 bytes)
    ▽ Address Indicator
        0... .... = Reserved for national use: 0x00
        .0.. .... = Routing Indicator: Route on GT (0x00)
        ..01 00.. = Global Title Indicator: Translation Type, Numbering Plan, Encoding Scheme, and Nature
        .... ..1. = SubSystem Number Indicator: SSN present (0x01)
        .... ...0 = Point Code Indicator: Point Code not present (0x00)
      SubSystem Number: Unknown (75)
    ▽ Global Title 0x4 (9 bytes)
        Translation Type: 0x00
```

```
0000  [redacted]  ...  '.....E.
0010              .@.  ........
0020              Y..  pd...h..
0030              ...  ........
0040              F..  ........
0050              ...  7.......
0060              K..  .3...P..
0070              .b.  .b..b.H.
0080              .
```

● Standard input: <live capture in progre Packets: 4835 · Displayed: 1009 (20.9%) Profile: SS7

Reference: http://labs.p1sec.com/2013/04/04/ss7-traffic-analysis-with-wireshark/

Telecommunications Network Architecture



CALEA Patriot Act
(TCP/IP Wire Tap)

Triple Play and Smart Grid Service

Carrier Class Telco Networks
10 Gig, Highly Redundant
Thousands Of Devices

- Vendor/Mfg. Remote Support
- Internal Tech Staff VPN
- Customer online bill payment
- Misconfigured Backdoor

Demand for Bandwidth driving Optical Network Growth; Telcos, …

Cellular Mobile IP Backhaul

Insertion Point

●	Smart Grid
●	Data Service
●	Voice Service
●	Video Service

Strategy to Gain Access to SS7 Network

Transport Network Infrastructure

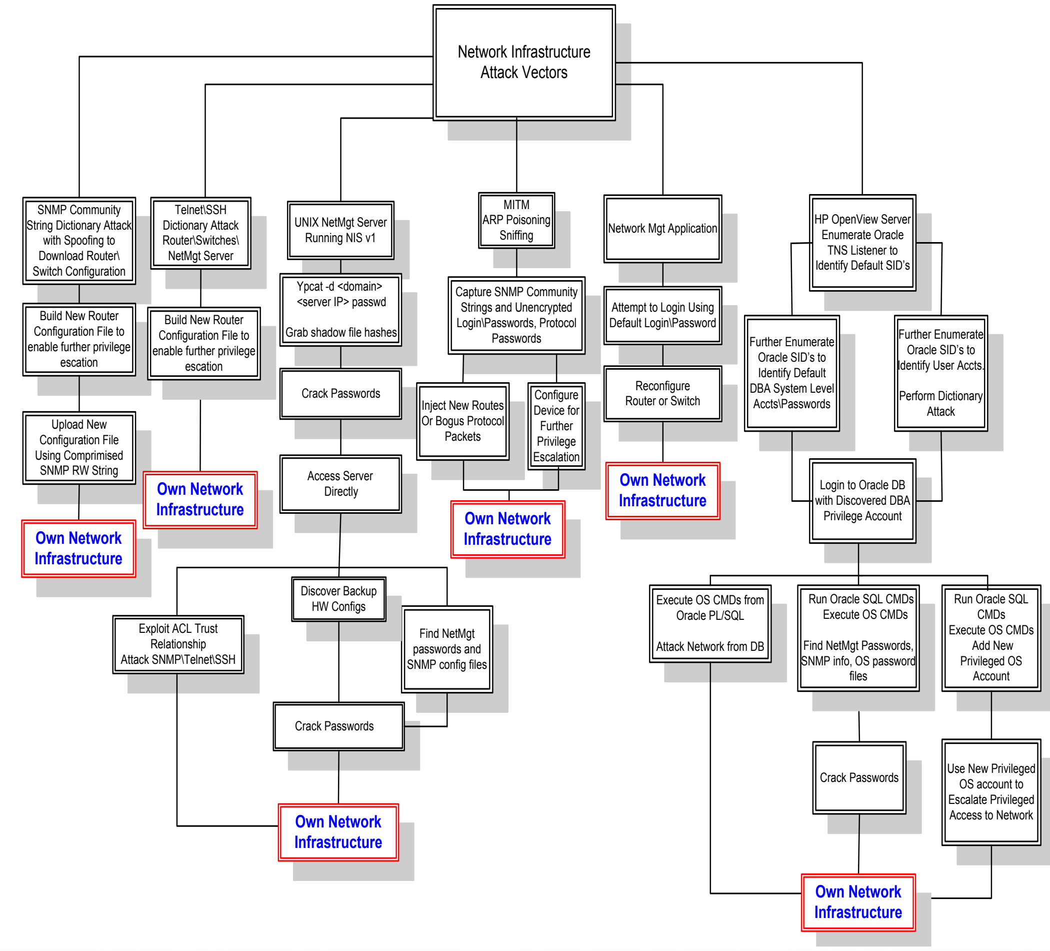
Network and System Architecture
- Centralized, Distributed, Redundant
- Physical and Logical
- Transport Network (RF, Fiber, Copper, Satellite)
- In-band
- Out-of-band

Network Protocols
- Routing, Switching, Redundancy
- Apps, Client/Server

HW, SW, Apps, RDBMS
- Open Source
- Commercial
- Soft Switch
- Middleware

Trust Relationships – Internet, BSS, OSS, NMS, Net
- Network Management and Network Devices
- Billing, Middleware, Provisioning
- Vendor remote access
- Tech staff remote access
- Self Provisioning
- Physical access
- Trusted Insider
- Cross connect
- CE in-band management
- Physical access to CE configuration settings

Attack Tree



Network Infrastructure Attack Vectors

SNMP Community String Dictionary Attack with Spoofing to Download Router\ Switch Configuration

Build New Router Configuration File to enable further privilege escation

Upload New Configuration File Using Comprimised SNMP RW String

Own Network Infrastructure

Telnet\SSH Dictionary Attack Router\Switches\ NetMgt Server

Build New Router Configuration File to enable further privilege escation

Own Network Infrastructure

UNIX NetMgt Server Running NIS v1

Ypcat -d <domain> <server IP> passwd

Grab shadow file hashes

Crack Passwords

Access Server Directly

Exploit ACL Trust Relationship Attack SNMP\Telnet\SSH

Discover Backup HW Configs

Find NetMgt passwords and SNMP config files

Crack Passwords

Own Network Infrastructure

MITM ARP Poisoning Sniffing

Capture SNMP Community Strings and Unencrypted Login\Passwords, Protocol Passwords

Inject New Routes Or Bogus Protocol Packets

Configure Device for Further Privilege Escalation

Own Network Infrastructure

Network Mgt Application

Attempt to Login Using Default Login\Password

Reconfigure Router or Switch

Own Network Infrastructure

HP OpenView Server Enumerate Oracle TNS Listener to Identify Default SID's

Further Enumerate Oracle SID's to Identify Default DBA System Level Accts\Passwords

Further Enumerate Oracle SID's to Identify User Accts.

Perform Dictionary Attack

Login to Oracle DB with Discovered DBA Privilege Account

Execute OS CMDs from Oracle PL/SQL

Attack Network from DB

Run Oracle SQL CMDs Execute OS CMDs

Find NetMgt Passwords, SNMP info, OS password files

Run Oracle SQL CMDs Execute OS CMDs Add New Privileged OS Account

Crack Passwords

Use New Privileged OS account to Escalate Privileged Access to Network

Own Network Infrastructure

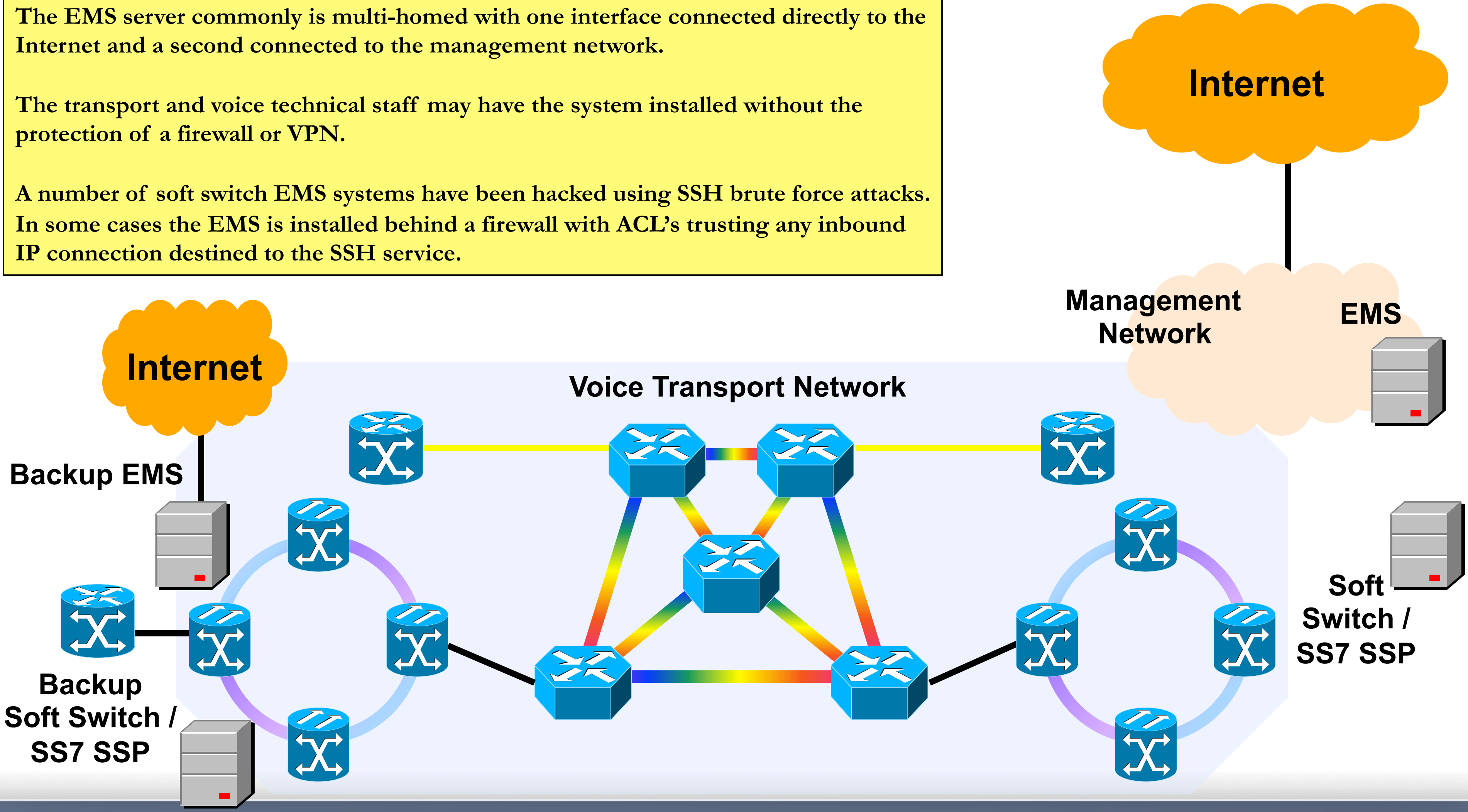
Voice Soft Switch Network
SS7 SSP

The service provider transport and soft switch vendors commonly provide a EMS for their solution.

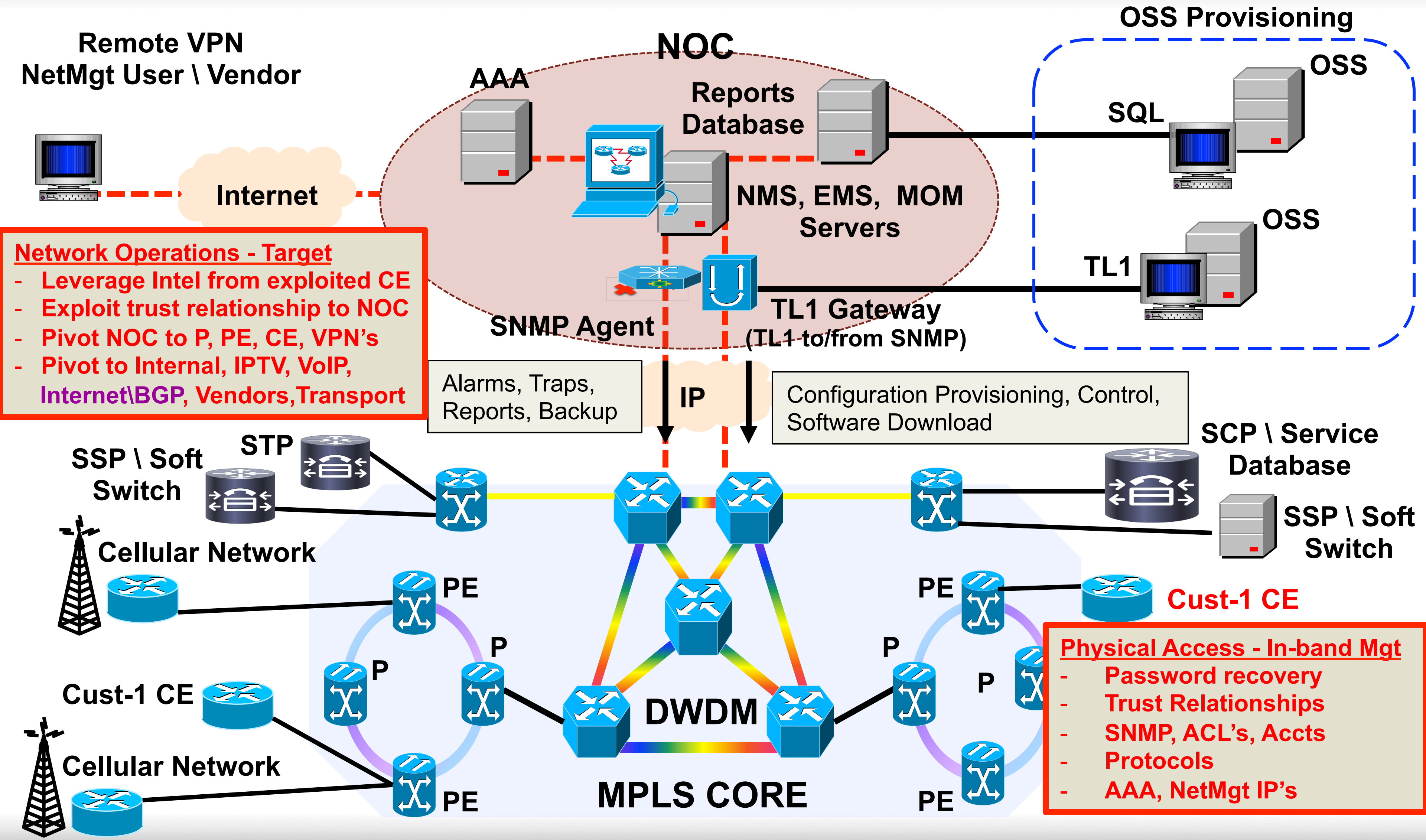
The EMS server commonly is multi-homed with one interface connected directly to the Internet and a second connected to the management network.

The transport and voice technical staff may have the system installed without the protection of a firewall or VPN.

A number of soft switch EMS systems have been hacked using SSH brute force attacks. In some cases the EMS is installed behind a firewall with ACL's trusting any inbound IP connection destined to the SSH service.



Network Management Architecture for a Service Provider Use to Pivot to SS7 Infrastructure



Network Operations - Target

- Leverage Intel from exploited CE
- Exploit trust relationship to NOC
- Pivot NOC to P, PE, CE, VPN's
- Pivot to Internal, IPTV, VoIP, Internet\BGP, Vendors,Transport

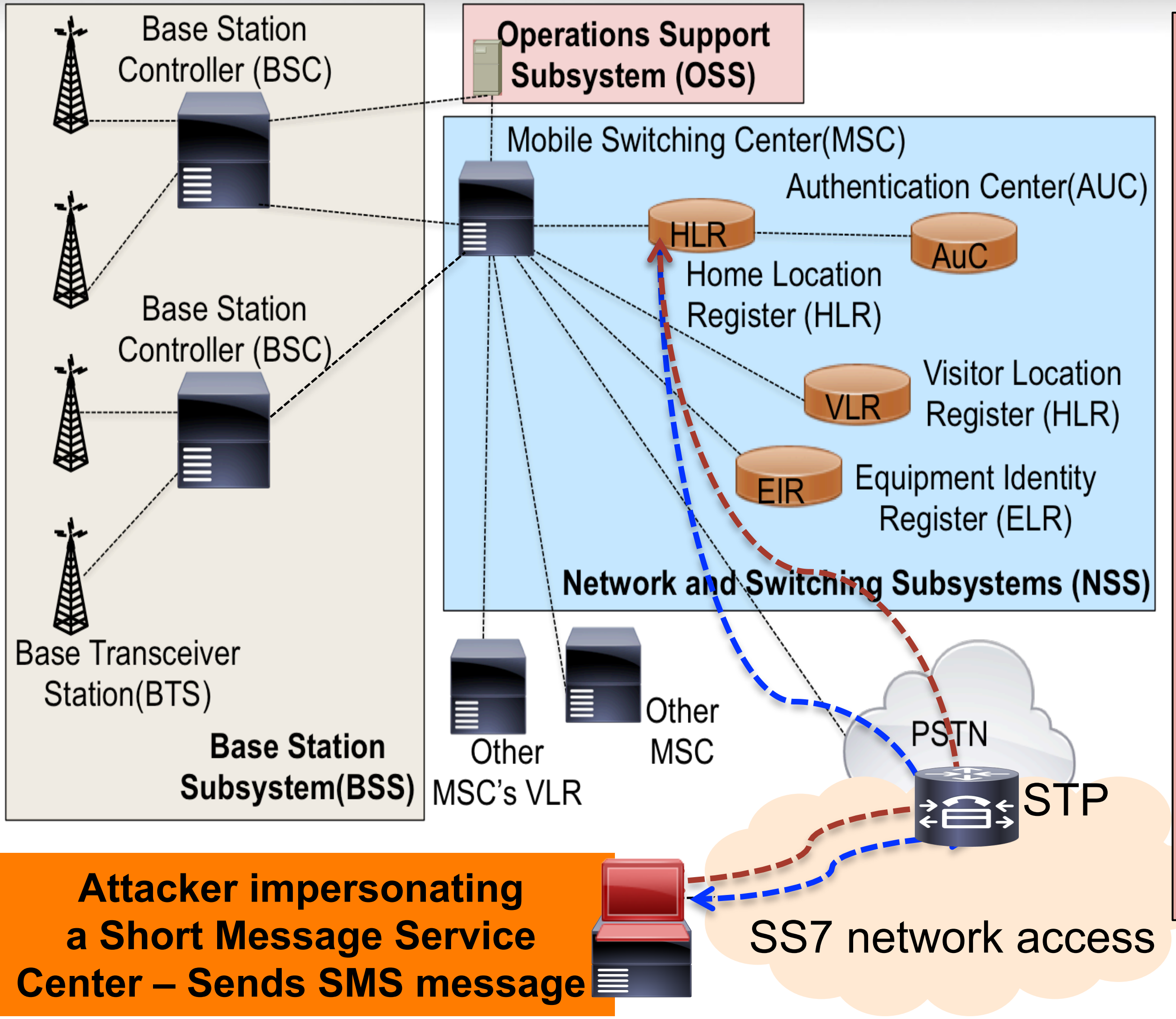
Alarms, Traps, Reports, Backup

Configuration Provisioning, Control, Software Download

Physical Access - In-band Mgt

- Password recovery
- Trust Relationships
- SNMP, ACL's, Accts
- Protocols
- AAA, NetMgt IP's

Obtain International Mobile Subscriber Identity(IMSI) of a subscriber

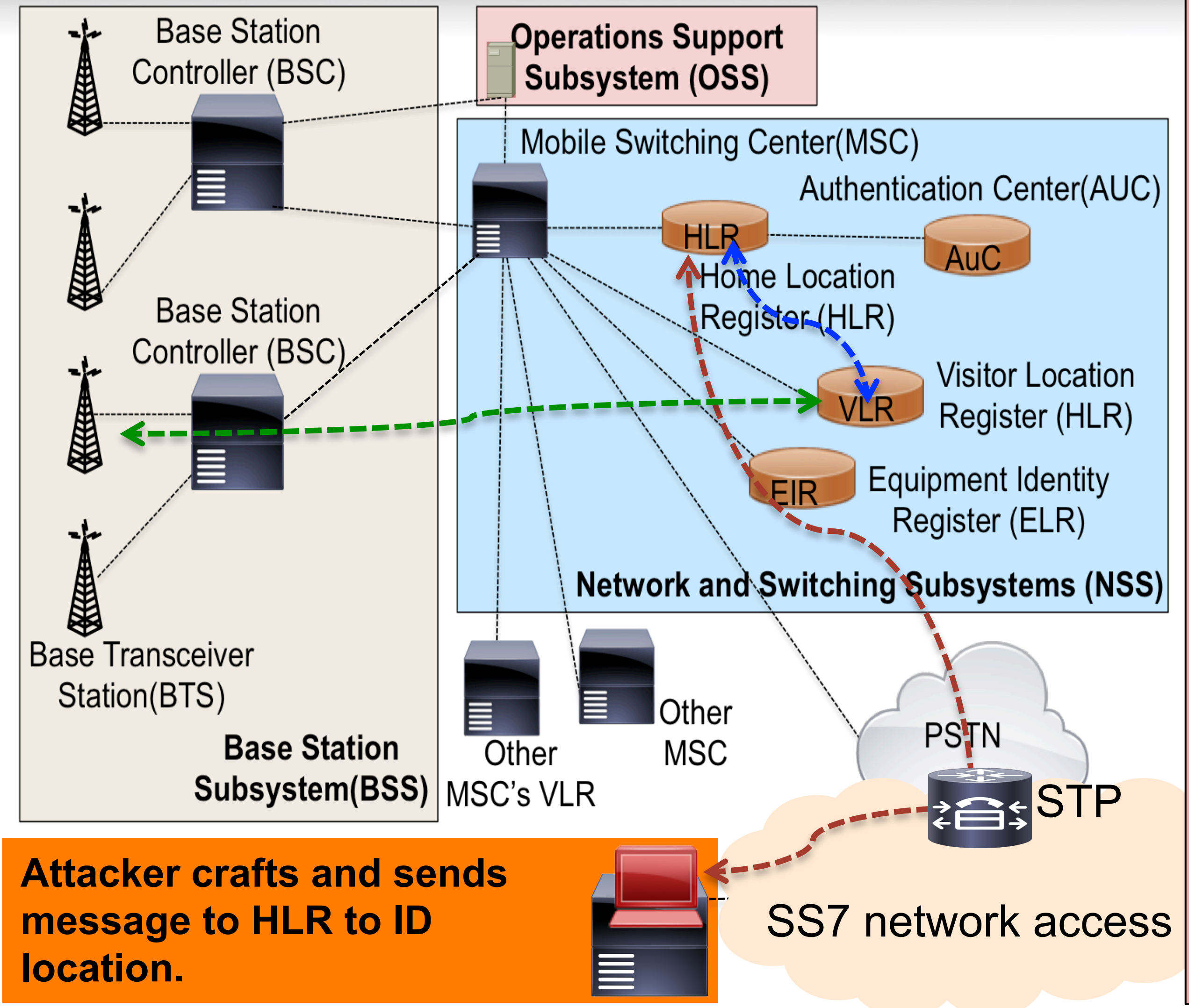

Base Station Controller (BSC)
Operations Support Subsystem (OSS)
Mobile Switching Center(MSC)
Authentication Center(AUC)
HLR
AuC
Home Location Register (HLR)
Base Station Controller (BSC)
VLR
Visitor Location Register (HLR)
EIR
Equipment Identity Register (ELR)
Network and Switching Subsystems (NSS)
Base Transceiver Station(BTS)
Base Station Subsystem(BSS)
Other MSC's VLR
Other MSC
PSTN
STP
SS7 network access

Attacker impersonating a Short Message Service Center – Sends SMS message

- **Attacker has the Mobile # for target and STP Point Code information**
- Attacker crafts SS7 messages acting as a Short Message Service Center(SMSC).
- **Message sent to subscriber home network where HLR lookups up subscriber phone # to ID the current MSC VLR for subscriber**.
- HLR sends response to requestor in this case the attacker.
- **Attacker now has subscriber phone number, IMSI(unique #), current MSC/VLR, HLR address for subscriber**

References: Signaling System No.7 (SS7/C7) Protocol, Architecture, and Services, Lee Dryburgh, Jeff Hewett, Cisco Press
Reference: https://www.cellusys.com/2016/03/19/subscriber-identity-disclosure-how-an-attacker-can-obtain-imsi-of-a-subscriber/

Identify Subscriber Location
Any Time Interrogation



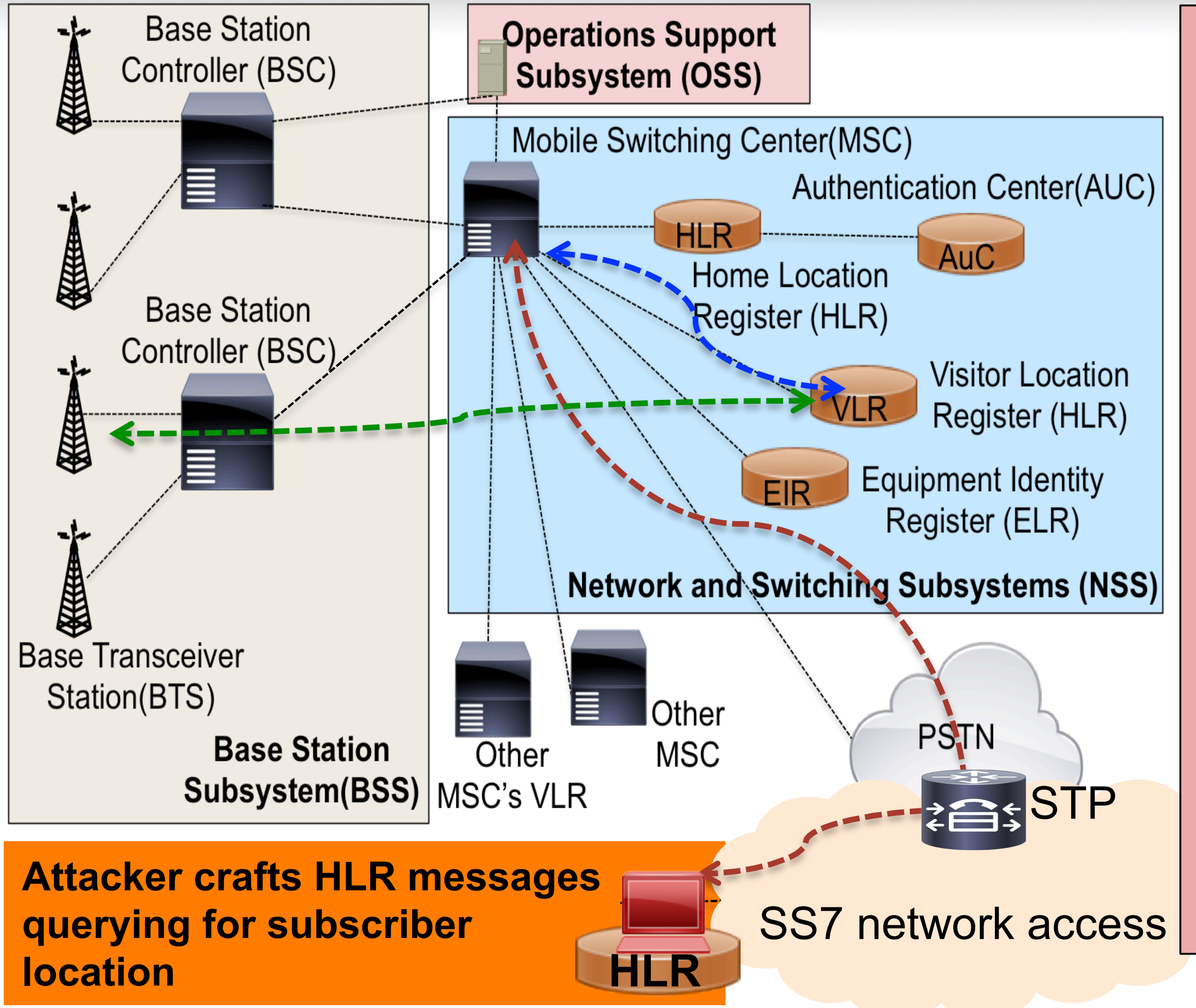
Base Station Controller (BSC)
Operations Support Subsystem (OSS)
Mobile Switching Center(MSC)
Authentication Center(AUC)
HLR
AuC
Home Location Register(HLR)
Base Station Controller (BSC)
VLR
Visitor Location Register (HLR)
EIR
Equipment Identity Register (ELR)
Network and Switching Subsystems (NSS)
Base Transceiver Station(BTS)
Base Station Subsystem(BSS)
Other MSC's VLR
Other MSC
PSTN
STP
SS7 network access

Attacker crafts and sends message to HLR to ID location.

- **Attacker now has subscriber phone number, IMSI(unique #), current MSC/VLR, HLR address for subscriber from previous attack.**
- Attacker crafts SS7 messages querying HLR for subscriber location.
- Message sent to subscriber home network where HLR sends message to VLR for current location.
- VLR sends a message to BSS to identify location of the mobile subscriber.
- BSS pages the subscriber phone.
- HLR sends response to requestor in this case the attacker.
- **Any Time Interrogation is not enabled on many networks today to protect HLR performance and security.**

Reference: Signaling System No.7 (SS7/C7) Protocol, Architecture, and Services, Lee Dryburgh, Jeff Hewett, Cisco Press
https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201606/Documents/Abstracts_and_Presentations/S2P1_Luca_Melette.pdf

Identify Subscriber Location
Impersonate a Home Location Register (HLR)

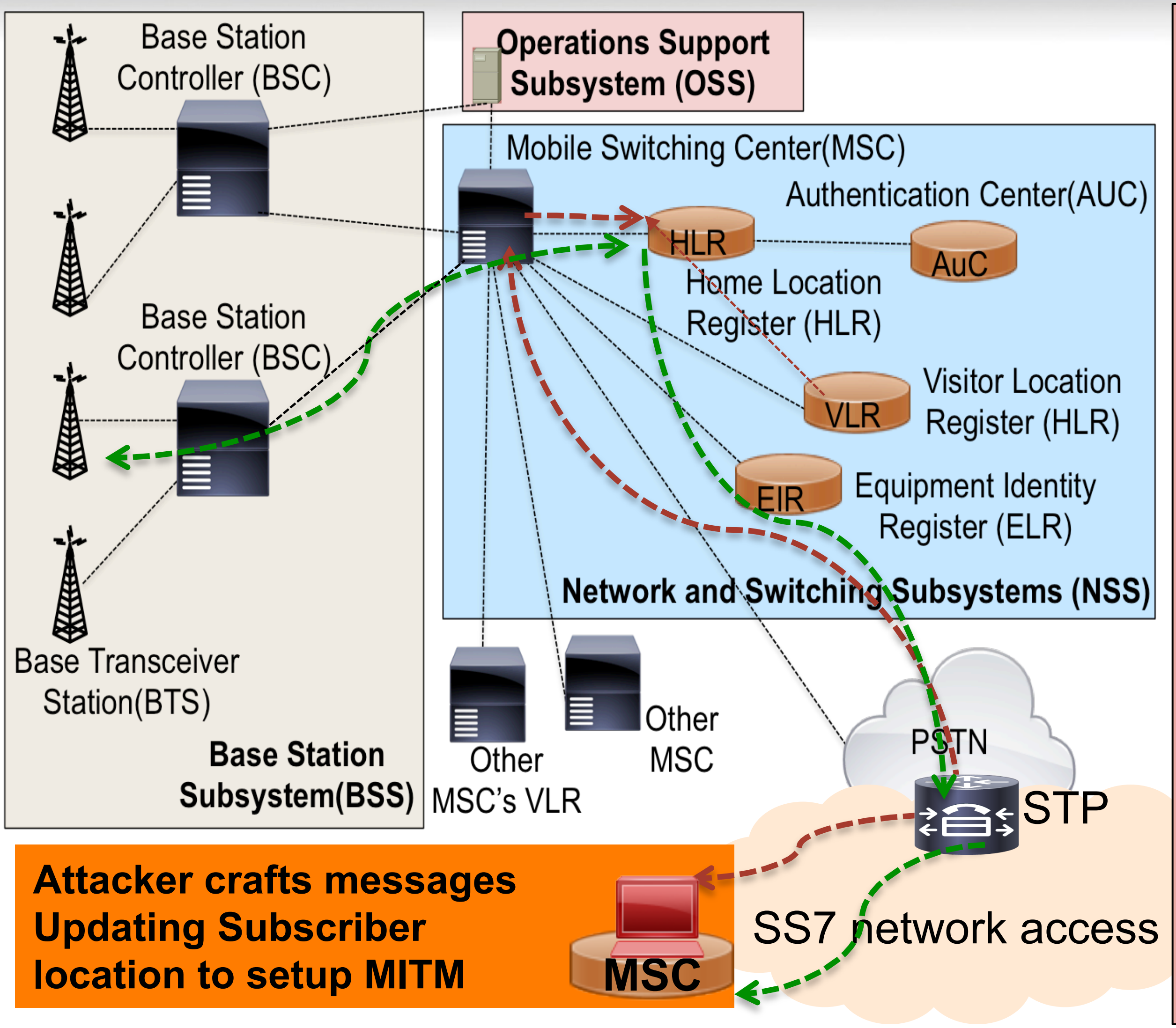

Base Station Controller (BSC)
Operations Support Subsystem (OSS)
Mobile Switching Center(MSC)
Authentication Center(AUC)
HLR
AuC
Home Location Register (HLR)
Base Station Controller (BSC)
VLR
Visitor Location Register (HLR)
EIR
Equipment Identity Register (ELR)
Network and Switching Subsystems (NSS)
Base Transceiver Station(BTS)
Base Station Subsystem(BSS)
Other MSC's VLR
Other MSC
PSTN
STP
HLR
SS7 network access

Attacker crafts HLR messages querying for subscriber location

- **Attacker now has subscriber phone number, IMSI(unique #), current MSC/VLR, HLR address for subscriber from previous attack.**
- Attacker crafts SS7 Provide Subscriber Information(PSI) messages querying MSC for subscriber location.
- Message sent to subscriber home network where HLR sends message to VLR for current location.
- VLR sends a message to BSS to identify location of the mobile subscriber.
- BSS pages the subscriber phone.
- **MSC sends response to requestor in this case the attacker with subscriber details including location.**

Reference: Signaling System No.7 (SS7/C7) Protocol, Architecture, and Services, Lee Dryburgh, Jeff Hewett, Cisco Press
https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201606/Documents/Abstracts_and_Presentations/S2P1_Luca_Melette.pdf

Intercept Calls\SMS


Base Station Controller (BSC)
Operations Support Subsystem (OSS)
Mobile Switching Center(MSC)
Authentication Center(AUC)
HLR
AuC
Home Location Register (HLR)
Base Station Controller (BSC)
VLR
Visitor Location Register (HLR)
EIR
Equipment Identity Register (ELR)
Network and Switching Subsystems (NSS)
Base Transceiver Station(BTS)
Base Station Subsystem(BSS)
Other MSC's VLR
Other MSC
PSTN
STP
SS7 network access
MSC

Attacker crafts messages Updating Subscriber location to setup MITM

- **Attacker now has subscriber phone number, IMSI(unique #), current MSC/VLR, HLR address for subscriber from the information gathering attack.**
- This attack is similar to previous location attack.
- Attacker crafts SS7 Provide Subscriber Information(PSI) messages to HLR with a spoofed update of current location.
- **Any incoming calls or SMS to the spoofed subscriber will now be rerouted to the attackers location(ANYWHERE IN WORLD).**
- **Attacker can proxy calls on to the true subscriber to capture the voice communications or just capture targeted SMS communications.**

Reference: Signaling System No.7 (SS7/C7) Protocol, Architecture, and Services, Lee Dryburgh, Jeff Hewett, Cisco Press
https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201606/Documents/Abstracts_and_Presentations/S2P1_Luca_Melette.pdf

Things to Consider

SS7 Exploit Tools

- **SS7 Exploit tool – SigPloit on Github**
- **ss7MAPer – Daniel Mende, ERNW**
  https://insinuator.net/2016/02/ss7maper-a-ss7-pen-testing-toolkit/
- **Scapy**
- **Colasoft Packetbuilder**
- **Netdude**

SS7 Firewalls

- Cellusys
- Fortis Communications
- Configure STP to filter SS7 messages

Other Recommendations

- **Audit the SS7, SIP, mobile wireless infrastructure in the telco voice networks**
  - Treat these networks similar to legacy ICS\SCADA networks when testing
  - Penetration test
  - Look for vendor backdoor remote access with static passwords (reused EVERYWHERE)
- **Utilize Signal or other for personal secure communications**
- **Replace SMS 2FA with alternative solutions**
- **Secure Visualization and Instrumentation**

References

Signaling System No.7 (SS7/C7) Protocol, Architecture, and Services, Lee Dryburgh, Jeff Hewett, Cisco Press

Security of Public and IP Telephone Networks, A Security Assessment of SS7, SIGTRAN and VoIP Protocols, Sengar

Voice Over IP Fundamentals, Cisco Press

https://www.cisco.com/c/dam/global/en_ae/assets/ciscoexposaudi2008/assets/transport-and-applications-forss7--signaling-franktuhus.pdf

https://docstore.mik.ua/univercd/cc/td/doc/product/tel_pswt/vco_prod/ss7_fund/ss7fun03.pdf

https://www.slideshare.net/janardhanreddy30/ss7-tutorial

http://secuinside.com/archive/2015/2015-2-7.pdf

www.blackhat.com/presentations/bh-usa-06/BH-US-06-Waldron.pdf

http://blogs.blackberry.com/2016/04/how-to-protect-yourself-from-ss7-and-other-cellular-network-vulnerabilities/

http://www.fiercetelecom.com/telecom/verizon-seeks-fcc-permission-to-shutter-more-legacy-ss7-voice-switches-cites-ongoing-ip

https://www.wired.com/2017/05/fix-ss7-two-factor-authentication-bank-accounts/

https://www.theguardian.com/technology/2016/apr/19/ss7-hack-explained-mobile-phone-vulnerability-snooping-texts-calls

https://koolspan.com/ss7-mobile-network-vulnerabilities/

http://resources.infosecinstitute.com/ss7-protocol-how-hackers-might-find-you/

http://www.computerworld.com/article/3058020/security/hackers-only-need-your-phone-number-to-eavesdrop-on-calls-read-texts-track-you.html

https://www.adaptivemobile.com/press-centre/press-releases/adaptivemobile-launches-ss7-protection

http://blogs.blackberry.com/2014/12/how-to-defeat-ss7-surveillance-of-calls-texts/

http://www.itproportal.com/2016/06/13/ss7-protocol-critical-mobile-network-security/

https://blog.kaspersky.com/hacking-cellular-networks/10633/

https://www.v3.co.uk/v3-uk/news/3009585/cybercriminals-use-ss7-telco-flaw-to-steal-from-bank-accounts

https://www.engagespark.com/blog/telcos-aggregators-ss7-grey-routes/

https://www.scmagazineuk.com/ss7-vulnerability-defeats-whatsapp-encryption-researchers-claim/article/530945/

http://www.centurylink.com/wholesale/pcat/ccsacss7.html

https://www.corelatus.com/gth/api/save_to_pcap/index.html

https://github.com/SigPloiter/SigPloit/wiki/3--How-to-use-the-SS7-module

https://www.cellusys.com/2016/03/19/subscriber-identity-disclosure-how-an-attacker-can-obtain-imsi-of-a-subscriber/

https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201606/Documents/Abstracts_and_Presentations/S2P1_Luca_Melette.pdf

http://labs.p1sec.com/2013/04/04/ss7-traffic-analysis-with-wireshark/

https://www.blackhat.com/presentations/bh-europe-07/Langlois/Presentation/bh-eu-07-langlois-ppt-apr19.pdf

http://k4linux.com/2016/06/how-to-hack-facebook-account-with-phone-number-ss7.html

https://insinuator.net/2016/02/ss7maper-a-ss7-pen-testing-toolkit/

References

https://www.cyberscoop.com/finally-happened-criminals-exploit-ss7-vulnerabilities-prompting-concerns-2fa/
https://www.schneier.com/blog/archives/2014/12/ss7_vulnerabili.html
https://fedotov.co/ss7-hack-tutorial-software/
https://fedotov.co/ss7-mobile-phone-hacking-2/
https://www.blackhat.com/presentations/bh-europe-07/Langlois/Presentation/bh-eu-07-langlois-ppt-apr19.pdf
http://k4linux.com/2016/06/how-to-hack-facebook-account-with-phone-number-ss7.html
https://insinuator.net/2016/02/ss7maper-a-ss7-pen-testing-toolkit/
http://securityaffairs.co/wordpress/28397/hacking/surveillance-solutions.html
http://labs.p1sec.com/2012/12/02/sim-man-in-the-middle/
http://www.openss7.org
http://www.cellusys.com/2015/10/20/8-ss7-vulnerabilities-you-need-to-know-about/
https://thehackernews.com/2016/07/two-factor-authentication.html
http://blogs.blackberry.com/2016/01/how-ss7-flaw-gives-hackers-easy-access-to-your-private-phone-calls-what-you-can-do-about-it-white-paper/
https://www.kaspersky.com/blog/hacking-cellular-networks/10633/
http://www.communicationsapplications.com/topics/communicationsapplications/articles/431871-hackers-bank-ss7-insecurity.htm?utm_content=53980928&utm_medium=social&utm_source=twitter
https://en.wikipedia.org/wiki/Signalling_System_No._7
https://www.sans.org/reading-room/whitepapers/critical/fall-ss7--critical-security-controls-help-36225
https://www.theregister.co.uk/2017/05/03/hackers_fire_up_ss7_flaw/
https://securityintelligence.com/ss7-vulnerability-isnt-a-flaw-it-was-designed-that-way/
http://www.cellusys.com/tcap-handshaking-ss7-security/introduction-to-ss7-and-security/
https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/german-researchers-discover-a-flaw-that-could-let-anyone-listen-to-your-cell-calls-and-read-your-texts/?noredirect=on&utm_term=.01131f2bc2b8
http://www.telecomspace.com/forum/telecom/ss7
http://www.telecomspace.com/ss7.html
https://wiki.wireshark.org/CaptureSetup/SS7
https://hitcon.org/2015/CMT/download/day1-d-r0.pdf
http://labs.p1sec.com/2014/12/28/ss7map-country-risk-ratings/
https://resources.infosecinstitute.com/ss7-protocol-how-hackers-might-find-you/#gref
https://www.ptsecurity.com/upload/ptcom/SS7_WP_A4.ENG.0036.01.DEC.28.2014.pdf
https://play.google.com/store/apps/details?id=de.srlabs.snoopsnitch
https://arxiv.org/pdf/1510.07563.pdf

References

https://blog.securegroup.com/vulnerabilities-in-ss7-expose-all-networks-to-attacks-why-you-should-be-concerned

http://blog.ptsecurity.com/2014/08/cell-phone-tapping-how-it-is-done-and.html

http://blog.ptsecurity.com/2014/08/cell-phone-tapping-how-it-is-done-and.html

http://energy.sandia.gov/wp-content/gallery/uploads/sand_2005_2846p.pdf

https://blog.drhack.net/whatsapp-telegram-hacking-demo-live-ss7-vulnerability/2/

http://www.riverpublishers.com/journal_read_html_article.php?j=JICTS/5/1/2

https://www.cisco.com/c/dam/global/en_ae/assets/ciscoexposaudi2008/assets/transport-and-applications-forss7--signaling-franktuhus.pdf

http://netdude.sourceforge.net/

https://www.colasoft.com/packet_builder/

https://scapy.net/

https://n0where.net/build-gsm-base-station/

http://hackaday.com/2015/11/11/getting-started-with-gnu-radio/?utm_content=bufferb488a&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

https://www.blackhat.com/docs/eu-15/materials/eu-15-Borgaonkar-LTE-And-IMSI-Catcher-Myths-wp.pdf

http://resources.infosecinstitute.com/mobile-phone-tracking/

http://www.rs-online.com/designspark/electronics/eng/blog/running-a-gsm-network-on-the-raspberry-pi-2

https://github.com/yosriayed/GSM-scanner

http://resources.infosecinstitute.com/introduction-to-gsm-security/

http://discourse.criticalengineering.org/t/howto-gsm-base-station-with-the-beaglebone-black-debian-gnu-linux-and-a-usrp/56

http://www.insinuator.net/tag/gtp/

http://hackaday.com/2014/07/05/a-gsm-base-station-with-software-defined-radio/

http://imall.iteadstudio.com/im140318007.html

http://www.ptsecurity.com/download/Vulnerabilities_of_Mobile_Internet.pdf

http://blog.ptsecurity.com/2015/02/the-research-mobile-internet-traffic.html

https://www.schneier.com/blog/archives/2015/08/ss7_phone-switc.html

https://www.schneier.com/academic/archives/1999/12/attack_trees.html

MPLS VPN Security, Michael H. Behringer, Monique J. Morrow, Cisco Press

ISP Essentials, Barry Raveendran Greene, Philip Smith, Cisco Press

Router Security Strategies – Securing IP Network Traffic Planes, Gregg Schudel, David J. Smith, Cisco Press

LAN Switch Security – What Hackers Know About Your Switches, Eric Vyncke, Christopher Paggen, Cisco Press

Hijacking Label Switch Networks in the Cloud, Paul Coggin

Bending and Twisting Networks, Paul Coggin

Digital Energy – BPT, Paul Coggin

Questions?

@PaulCoggin

SS7 Link Types

- **Access links (A links)** – Carriers use A links to connect to SSPs(carrier voice switches) and SCPs(services databases) to STPs(SS7 message routers)

- **Crossover links (C links)** – Used to mate\cluster STPs for redundancy. Links carry management traffic and user traffic only if necessary

- **Bridge links (B links)** – Connect STPs from different areas to create SS7 network backbone

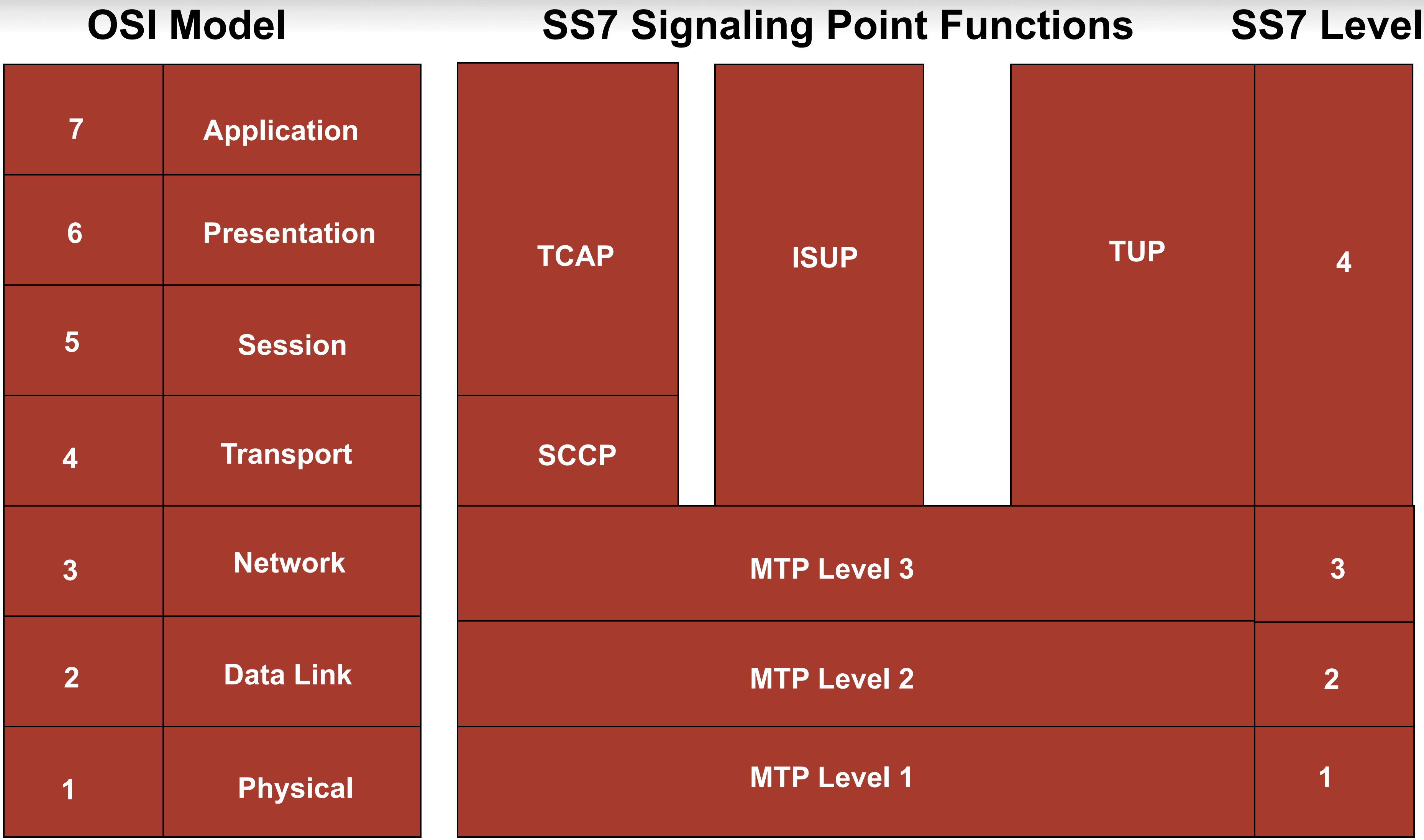
- **Diagonal links (D links)** – Connect STPs from different carrier networks or architecture levels

- **Extended Links (E Links)** – Sometimes referred to as alternate A link (AA link). Connect to additional STPs for greater capacity and redundancy.

- **Full associated links (F links)** – In a large city SSPs and SCPs may connect directly together using F links

Reference: Signaling System No.7 (SS7/C7) Protocol, Architecture, and Services, Lee Dryburgh, Jeff Hewett, Cisco Press

OSI Model vs. SS7 Protocol Stack



OSI Model		SS7 Signaling Point Functions			SS7 Level
7	Application	TCAP	ISUP	TUP	4
6	Presentation				
5	Session				
4	Transport	SCCP			
3	Network	MTP Level 3			3
2	Data Link	MTP Level 2			2
1	Physical	MTP Level 1			1

Reference: Voice Over IP Fundamentals, Cisco Press