Infrastructure Electronic Numbering Implementation in Australia

A thesis submitted in fulfilment of
the requirements for the degree of
MASTER OF ENGINEERING

Ananda Tapasvi Jammulamadaka

ELECTRICAL AND COMPUTER ENGINEERING
COLLEGE OF SCIENCE, ENGINEERING AND HEALTH
RMIT UNIVERSITY

2010

Statement of Authorship

'I certify that the attached material is my original work. I declare that no other person's work has been used without due acknowledgement. Except where reference is made in the text of the thesis, this thesis does not contain material published elsewhere or extracted in whole or in part from a thesis presented for another degree or diploma.

This thesis has not been submitted for the award of any other degree or diploma in any other tertiary institution.'

Ananda Tapasvi Jammulamadaka

Acknowledgement

Firstly, I wish to express my deep and sincere gratitude to my supervisor, Dr. Mark A. Gregory. I could not have imagined having a better advisor and mentor for my Research, without his wide knowledge, stimulating suggestions, guidance, and encouragement; I would have had a lot of trouble finishing. I really thank my supervisor for understanding me and helping me throughout my duration of the research program and my time at RMIT University.

I am also grateful to my parents for being by my side, enabling me to pursue my dreams and reach my goals.

Table of Contents

Table of Tables

Table of Figures

Definitions and Abbreviations

Definitions

DNS related definitions:

- **Domain Name System**: The *Domain Name* System (DNS) is a distributed Internet directory service arranged hierarchically. DNS is used mostly to translate between *domain names* and IP addresses, to control Internet email delivery and other purposes. It comprises of three components: the *name space*, the *name servers* making that name space available and *resolvers* (clients), which query the servers about the name space.
- **Name space:** Domain Name Space: All combinations of *Domain Names* and *Top Level Domains* existing below the *Root*.
- **Domain**: simple: a set of host names within the DNS consisting of a single *domain name* and all the domain names below it.
- **Zone**: Any *domain name* that has been delegated by an *ancestor* zone. A zone is a point of delegation in the DNS tree. It contains (includes) all descendant *domain names* from a certain point downward that have not been *delegated* (because for those *delegated* other zones are *authoritative).* A zone is therefore a discreetly managed portion of the total *Domain Name Space* within a single *domain* and is represented by the data stored on a particular *name server*. A zone is the part of a DNS domain for which the *register* contains information and for which the *name server* is *authoritative*.
- **Subdomain**: Any child of a *domain zone*.
- **Domain Name:** A unique designator made up of symbols separated by dots. The individual words or characters between the dots are called *labels*. The label furthest right represents the *top level domain*. The second most right represents the second level of domain, or "second level domain. Formally, a domain name belongs to exactly one (authoritative) zone.
- **Label**: An element of a **domain name**. No label can be longer then 63 characters. Labels are made up of letters, numbers and hyphens, but may not start with hyphens.

Labels in a *domain name* are separated from each other by "."'s. Labels are case insensitive.

- **Fully Qualified Domain Name**: A *domain name* that extends all the way back to *root*. Often written as FQDN. A common error is to leave the "." at the end off.
- **Delegation**: The process of separating a descendant of a *zone* into a separate *zone*. The delegation is accomplished with *NS Records* (a type of a *resource record*)
- **Resource Record**: One unit of data in the DNS. A resource record defines some attribute for a domain name such as an IP address, a string of text, or a mail route.
- **NS Record**: Name Server Record. An NS record declares that a given *zone* is served by a given *name server*. Every NS record is either a *delegation* record or an *authority* record. If the name of the NS record is the name of the *zone* it appears in, it is an *authority* record. If the name of the NS record is that of a descendant zone, then it is a *delegation* record.
- **SOA Record:** Start of Authority Record. The SOA is the first record in every properly configured *zone*. The SOA record contains information about the *zone* in a string of fields. The SOA record tells the server to be *authoritative* for the *zone*.
- **NAPTR Record**: A DNS Resource Record that specifies a regular expression based rewrite rule that, when applied to an existing string, will produce a new domain label or Uniform Resource Identifier (URI).
- **Authoritative:** Adjective describing a *name server*. The authoritative server contains an entire copy of the *zone* that is derived from local configuration data, possibly with the help of another authoritative name server for the zone. A server can be authoritative about one zone, but not authoritative for another.
- **Name Server:** A name server is software that runs on a *host* that can be set to *authoritatively* answer queries for records in a *zone*.
- **Host:** A host is any machine on any network. On TCP/IP networks, each host has one or more unique IP addresses.
- **Root Server**: There are currently 13 servers that are *authoritative* for the *root zone*. They are named a.root-servers.net – m.root-servers.net. Every *resolver* must have the

IP addresses of one or more of these root servers coded in so that it can resolve *domain names*.

- **Root Zone**: The ancestor of all zones, the parent of the *top level domains*. It is written as ". ". *Root* (as it is often called) has no *labels*.
- **Resolver**: A resolver is a host capable of performing a recursive search of the DNS to locate records that would answer a query. It does this by querying *name servers*, including the *root servers*.. In other words, a resolver is a DNS server that looks up DNS records on behalf of a client machine.
- **Top Level Domain:** Any *zone* owned by the *root servers*. You can also think of this as the first *label* in any domain name other than *root* (which has no *labels*)
- **Primary Server:** Also called a master server. An *authoritative name server* that gets its *zone* data from local configuration, not from an outside source. This term is used in terms of a specific *zone*. The primary server of one *zone* could be a *secondary server* in regards to another *zone*. Despite a common misconception, from a *resolvers* point of view, primary and secondary servers are equal in authority and priority

DNS Administration related definitions:

- **Registrant**: The individual or organization that registers a specific *domain name* with a *registrar*. This individual or organization holds the right to use that specific *domain name* for a specified period of time, provided certain conditions are met and the registration fees are paid.
- **Domain Name Holder:** A person or organization is the "legal entity" bound by the terms of the Domain Name Registration Agreement with the registrar. After successful registration this entity is the *Domain Name Holder*.
- **Registrar:** A registrar provides direct services to *domain name registrants*. The registrar database contains customer information in addition to the DNS information contained in the *Registry* database. Registrars process name registrations for Internet end-users and then send the necessary DNS information to a *Registry* for entry into the centralized *Registry* database (*register*) and ultimate propagation over the Internet.

- **Registry:** A domain name registry is an entity that receives domain name service (DNS) information from domain name *registrars*, inserts that information into a centralized database (*register*) and propagates the information in a *zone file* to the *primary name server* of this *zone*.
- **Register** The *registry* database. It contains only domain name service (DNS) information (*domain name*, *name server names* and *name server* IP addresses) along with the name of the *registrar* that registered the name and basic transaction data. It does not contain any domain name *registrant* or *contact information*. *Registrars* provide direct services to *registrants*.
- **Zone File:** A file that contains data describing a portion of the domain name space. Zone files contain the information needed to resolve *domain names* to Internet Protocol (IP) numbers.
- **Contact Information:** Contacts are individuals or entities associated with *domain name records*. Typically, third parties with specific inquiries or concerns will use contact records to determine who should act upon specific issues related to a domain name record. There are typically three of these contact types associated with a domain name record, the *Administrative contact*, the *Billing contact* and the *Technical contact*.
- **Contact, Administrative:** The administrative contact is an individual, role or organization authorized by *the domain name holde*r to interact with the *registry* or *registrar* on behalf of the Domain Name Holder. The administrative contact should be able to answer non-technical questions about the domain name's registration and the *Domain Holder.* In all cases, the Administrative Contact is viewed as the **authoritative point of contact** for the domain name, second only to the Registrant.
- **Contact, Billing:** The billing contact is the individual, role or organization designated to receive the invoice for domain name registration and re-registration fees.
- **Contact, Technical:** The technical contact is the individual, role or organization who is responsible for the technical operations of the *delegated zone*. This contact likely maintains the *domain name server(s*) for the *domain*. The technical contact should be able to answer technical questions about the *domain name*, the *delegated zone* and

work with technically oriented people in other zones to solve technical problems that affect the domain name and/or zone.

- **Whois:** a TCP transaction based query/response server, that providing netwide directory service to network users. The Whois Protocol was originally defined in RFC 954. The initial domain name related application layer implementations were centralized systems run by SRC-NIC and then later InterNIC/Network Solutions. The SRI-NIC and InterNIC implementations are more formally referred to as "NICNAME/Whois" services. Whois is not purely a domain name or IP address directory service, but has been deployed for a wide variety of uses, both public and private. Other variants of this service include RWhois and the newer Verisign Referral LDAP Whois service. Whois can refer to the protocol defined in RFC 954 or the generic application service described above.

E.164 related definitions:

- **E.164**: the International Public Telecommunications Numbering Plan according ITU-T Rec E.164
- **E164 Number**: a number taken from *E.164* and assigned to an *end user* (Fully qualified E.164 number?)
- **Number Portability**: the ability of an *end user* to change location within a geographic area, between *telephony service providers* or services, without changing their number. (This must be in accordance with the portability requirements pertaining to each specific type of E.164 number.)
- **National Number Plan Administrator**: the entity responsible for the administration of a national numbering Plan that is part of E.164.
- **Assignment Entity**: the entity (e.g. Telephony service provider or National Number Plan Administrator) responsible for the assignment of *E.164 numbers* to an *end use*r.
- **Telephony Service Provider**: the entity that provisions telephony and related services that utilise *E.164 numbers*. In most cases the telephony service provider may act as the *assignment entity*.
- **End user**: The assignee of a full *E.164 number*.

ENUM related definitions:

- **ENUM**: the protocol developed by the IETF as RFC2916 for fetching Universal Resource Identifiers (URI) from DNS *NAPTR* given an *E.164 number*.
- **Tier 0**: A generic term referring to all ENUM issues at the international level of ENUM, dealing with the *domain zone* e164.arpa or equivalent. For further definitions of Tier 0 see ITU-T E.AENUM.
- **Tier 1**: A generic term referring to all ENUM issues below the international level of ENUM, and above *Tier* 2, dealing with all *zones* delegated from *Tier* 0 above the *zones* belonging to *Tier* 2. In general this is the national level. The Tier 1 may consist of more than one layer, depending on the national ENUM architecture or model of administration.
- **Tier 2**: A generic term referring to ENUM issues at the ENUM subscriber level, dealing with the ENUM *domain zones* and *ENUM domain names* related to *full E.164 numbers.*
- **Tier 3**: A generic term referring to ENUM issues below the ENUM subscriber level, dealing with the ENUM *domain zones* related to numbers below (behind, after) *full E.164 numbers*, e.g. DDI and private extensions.
- **Tier x entity**: Any entity acting on Tier x level.
- **ENUM registry:** A person(s) or entity responsible for providing ENUM *registry* services.
- **Tier 1 Registry**: An ENUM *registry* on Tier 1.
- **Tier 2 Registry**: An ENUM *registry* on Tier 2.
- **ENUM subscriber**: The assignee of an E.164 number by an *assignment entity*, who has chosen to subscribe to an ENUM service. ENUM *domain name holder*.
- **ENUM domain name holder**: see *ENUM subscriber.*
- **ENUM domain name**: The representation of a (full) E.164 number in ENUM at *Tier* 2.
- **ENUM Registrant**: the entity initiating the ENUM registration process (*ENUM subscriber* or agent)

- **ENUM Registrar**. A person(s) or entity(ies) that, via contract with assignees of E.164 numbers (*ENUM Registrants*) and an ENUM Tier-1 *Registry* and/or an *ENUM Tier-2 Provider*, provides registration services to *ENUM Registrants*.
- **ENUM Tier 2 Provider**: An entity providing *Tier 2 Registry* and/or *ENUM Registrar* services.
- **TNVA** (Telephone Number Validation Authority) – The TNVA is the generic entity that can verify that the *Registrant* does indeed have the authority to register a specific *ENUM domain name* with the Tier 1 Registry. This entity may interact with the *TSP* responsible for the specific TN, *the assignment entity*, a national central database or the *Registrant* to verify the relationship.
- **Application Service Provider**: the entity that provides specific application(s) e.g. email or voice messaging to the *ENUM subscriber*.

Abbreviations

3GPP	Third Generation Partnership Project
A6	DNS Resource Record used to look up 128-bit IPv6 Address
AAAA	DNS Resource Record to help transition and coexistence between IPv4 and IPv6 networks
ACE	ASCII Compatible Encoding
AETP	Austrian ENUM Trial Platform
APNG	Asia Pacific Networking Group
ARIN	American Registry for Internet Numbers
ARPA	Addressing and Routing Parameter Area
BBMMIPC	Broadband MultiMedia IP Communications
BIND	Berkeley Internet Name Domain
CC	Country Code
ccTLD	Country Code Top Level Domain
CLI	Calling Line Identity, Calling Line Identification
CLIP	Calling Line Identity Presentation
CLIR	Calling Line Identity Presentation Restriction

DDDS	Dynamic Delegation Discovery System
DES	Data Encryption Standard, widely-used method of data encryption
DIG	Domain Internet Groper
DIN	Deutsches Institut für Normung
DNAME	DNS Resource Record providing capability to map entire subtree of a DNS name space to another domain (RFC 2672)
DNS	Domain Name System
DNSSEC	Domain Name System SECurity Extensions
DOC	US Department of Commerce
E2U	E.164 to URI resolution (specific type of NAPTR service)
EAP	Extensible Authentication Protocol
EAP-AKA	EAP-Authentication and Key Agreement
ENUM	IETF Telephone Number Mapping Working Group and resultant protocol
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
GAN	Generic Access Network
GATS	General Agreement on Trade in Services
GIC	Group Identification Code
GoC	Groups of Countries
GPS	Global Positioning System
GTLD	Generic Top Level Domain
GTLD-MOU	Generic Top Level Domain Memorandum of Understanding
HTTP	Hypertext Text Transfer Protocol
IAB	Internet Architecture Board
IAHC	International Ad Hoc Committee
IANA	Internet Assigned Numbers Authority, now part of ICANN
IC	Identification Code
ICANN	Internet Corporation for Assigned Names and Numbers
IDNS	International Domain Names
iDNS	Internationalized Multilingual Multiscript Domain Names Service
IETF	Internet Engineering Task Force

IM	Instant Messaging
IMSI	International Mobile Subscriber Identifies
INTUG	International Telecommunications User Group
IP	Internet Protocol
IPC	IP Communications
ISOC	Internet Society
ISP	Internet Service Provider
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
JIS	Japanese Industrial Standard
KEY	DNS Resource Record type used in DNSEC
LDAP	Lightweight Directory Access Protocol
LTE	Long Term Evolution
MIB	Management Information Base
MINC	Multilingual Internet Names Consortium
MRTG	Multi Router Traffic Grapher
NAPTR	Naming Authority Pointer (RFC 3403)
NIST	US National Institute of Standards and Technology
NOTIFY	Extension to DNS protocol defined in RFC 1996
NP	Number Portability
NS	Name Server, DNS Resource Record type
NSF	US National Science Foundation
NSI	Network Solutions Incorporated
NTPD	Network Time Protocol Daemon
NXT	DNS Resource Record type used in DNSSEC
PSTN	The Public Switched Telephone Network
PUA	Personal User Agent
QoS	Quality of Service
RBL	Realtime Blackhole List
RFC	Request for Comments, an IETF-related document
RFP	Request for Proposals

RIPE	Réseaux IP Européen
RIPE-NCC	RIPE Network Coordination Center
RLOGIN	UNIX Remote Logon command
RR	DNS Resource Record
RSH	UNIX Remote Shell command
RTT	Round Trip Time
SG2	ITU-T Study Group 2
SIG	DNS Resource Record type used in DNSEC
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLD	Second Level Domain
SNMP	Simple Network Management Protocol
SOA	Start of Authority
SOA	Start of Authority DNS Resource Record
SPAM	Unsolicited Commercial Email
SSHD	Secure Shell Daemon
STF	(ETSI) Special Task Force
SW	Software
TCP	Transfer Control Protocol
TDM	Time Division Multiplex
TLD	Top Level Domain
TS	Technical Specification (ETSI)
TSB	Telecommunication Standardization Bureau
TSIG	Transaction Signatures
TSON	TSB Telecommunication, Operation and Numbering Services Unit
TSP	Telephone Service Provider
UA	User Agent
UCE	Unsolicited Commercial Email
UCI	Universal Communications Identifier
UIFN	Universal International Freephone Numbers

UMTS	Universal Mobile Telecommunication System
UPT	Universal Personal Telecommunications
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VGRS	Verisign Global Registry Services
VoB	Voice over Broadband
VoIP	Voice over IP
VoLGA	Voice over LTE via GAN
VPN	Virtual Private Network
WG	Working Group
WIPO	World Intellectual Property Organization
WP1/2	Working Party 1 of SG 2
WTO	World Trade Organization
WTSA	World Telecommunication Standardization Assembly

1 Introduction

ENUM stands for Electronic Telephone Number Mapping. ENUM is a protocol defined by the Internet Engineering Task Force in RFC 3761, that resolves fully qualified telephone numbers to fully qualified domain name addresses using a DNS based architecture. ENUM is an important technology that provides a generic capability to converge existing PSTN and IP networks.

The Australian Communications and Media Authority facilitated an industry meeting to discuss ENUM in early 2005. The meeting outcome was an Australian User ENUM Trial which officially ended on 6th June 2007 after starting on the 6th of June 2005. The results of the User ENUM Trial indicated that there was not a key reason for consumers to want to utilise User ENUM.

Principal interest in ENUM was shown by Voice over Internet Protocol service providers and the discussion group members then shifted focus to Infrastructure ENUM, which is a version of ENUM that facilitates VoIP Peering without utilising the PSTN. An I-ENUM Working Group was formed to investigate the feasibility of utilising I-ENUM within Australia as a means of permitting VoIP service providers to peer VoIP services over the IP network. The I-ENUM Working Group conducted an I-ENUM trial from 1st September 2008 to 30 November 2008

In Australia there are currently more than two hundred VoIP service providers and through the use of I-ENUM it may be possible for VoIP to VoIP call cost reduction by the removal of the need to use the PSTN to peer VoIP services.

1.1 Scope

The two areas of interest for I-ENUM implementation in Australia are number portability and facilitating VoIP service peering over existing IP networks.

VoIP service providers generally offer a service that currently must utilise the PSTN. Several of the smaller carrier networks offers as a service, to the VoIP service providers, utilising the

carrier network as a private I-ENUM solution for VoIP peering within the carrier's network. An open universal I-ENUM solution is not available for all of the Australian VoIP service providers to utilise. The research presented in this thesis includes an analysis of the motivation for the introduction of an Australian I-ENUM system and the steps that may be taken to provide an open universally available solution.

1.2 Research Questions

ENUM is a protocol that resolves fully qualified telephone numbers to fully qualified domain name addresses using a DNS based architecture (Neustar). A fully qualified number is an E.164 number described in RFC 2916 , designated by the country code, an area or city code and the phone number. E.164 describes the structure of telephone numbers and this is how the PSTN identifies devices on the network. VoIP devices are identified using IP, SIP addresses and Uniform Resource Identifiers.

The research questions include:

- ***Structure for implementing Infrastructure ENUM in Australia***
- ***Motivation for an open universal VoIP peering solution***
- ***The steps required to move to a VoIP IP peered solution***

Other research questions are:

1. Who are the stakeholders?
2. What are the important policy, business, technology issues and stakeholder's interests with regard to VoIP IP peering and I-ENUM?
3. What implementation models can be developed for an Australian solution?
4. What existing I-ENUM implementations are there and what implementation models have been used.
5. The extent to which I-ENUM has undergone standardisation.
6. Current research related to VoIP IP peering and I-ENUM.
7. Whether an Australian implementation of I-ENUM is feasible.

1.3 Report structure and research approach

A literature review and analysis of the technology is provided in Chapter 2. A statement of the research objectives, assumptions and limitations is provided in Chapter 3. The research undertaken is described in Chapter 4 and an analysis of the research including a comparison with research outcomes identified in the literature review is provided in Chapter 5. The research conclusion and potential opportunities for future work are detailed in Chapter 6.

2 Background

In this chapter a literature review of the existing telephony market, VoIP and VoIP Peering techniques will be presented.

2.1 Public Switched Telephone Network

Demand for international communications has grown continuously over the past decade. The Public Switched Telephone Network continues to be the dominant telephony solution because of its familiarity, ubiquity, simplicity, low cost devices and calling rates. The maturity of the PSTN and deregulation of the telephony market have ensured growth in the market. Over the past decade, international telephone traffic has grown from 71.7 billion minutes in 1993 to 343 billion minutes in 2007 (TeleGeography, 2008). The increase in intercontinental traffic from 1997 – 2007 is shown in Figure 1.

The Plain Old Telephone System originally carried analogue voice signals over dedicated electronic circuits using circuit-switching techniques. Digital technologies were introduced and a hybrid network that incorporated a digital telephony core became known as the PSTN.

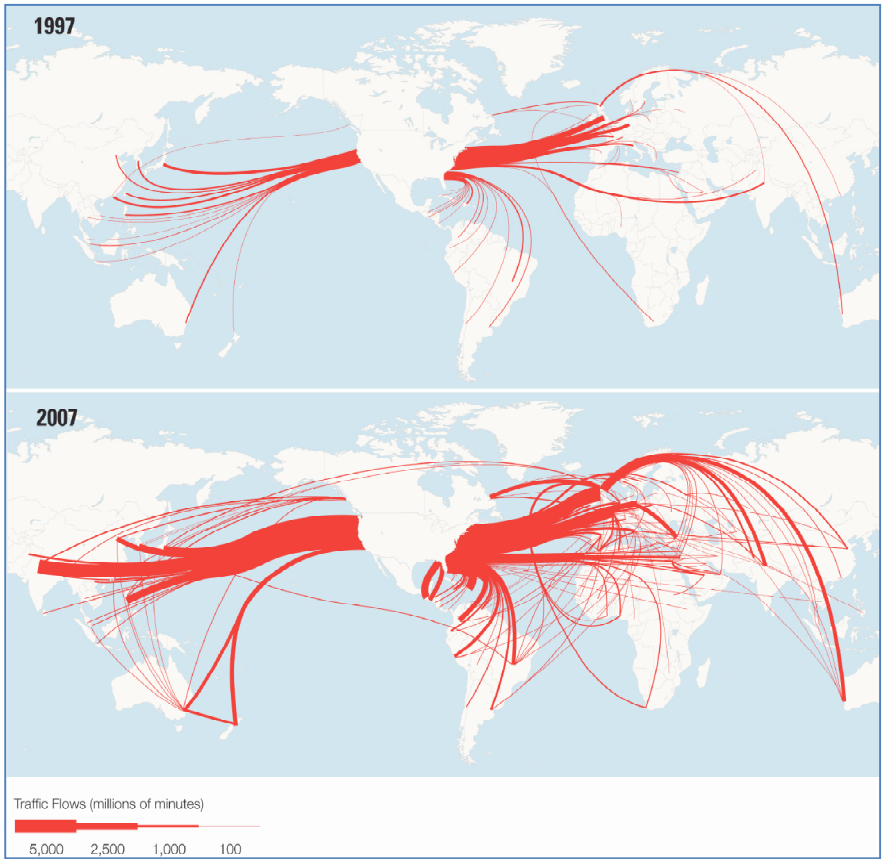

Figure 1: Intercontinental Traffic Flows, 1997 and 2007
(Note: Data reflects TDM traffic only, with an annual volume of more than 100 million minutes)

2.2 Voice over Internet Protocol

Since the emergence of VoIP in the mid 1990s, use of VoIP by small businesses and households has rapidly grown. The technology supporting VoIP was developed in the 1970s, but took almost 20 years to reach the households as a cost effective alternative for traditional phone networks. Slow internet speeds were the primary reason for the delay in embracing the technology. With the improvement of internet speeds in the last decade has resulted in VoIP being accepted globally on a larger scale.

VoIP is the name for the different technologies that allow telephone calls to be made over broadband internet connections (ACMA). VoIP is also associated with Internet Telephony which refers to communication services like voice, facsimile and/or voice messaging

applications that are transported over the Internet using IP rather than over the PSTN (Wikipedia). The analog voice signal generated during a call are converted to digital format and compressed into IP packets, transmitted over the internet to be decompressed and converted back to analog signal at the receiver's end.

To make VoIP calls, as shown in figure 2 [Skype], you would require an Internet connection and a suitable VoIP device. VoIP devices could be an analog phone with an analog telephone adaptor which connects the phone to the LAN, an IP phone or a soft phone installed on your computer.

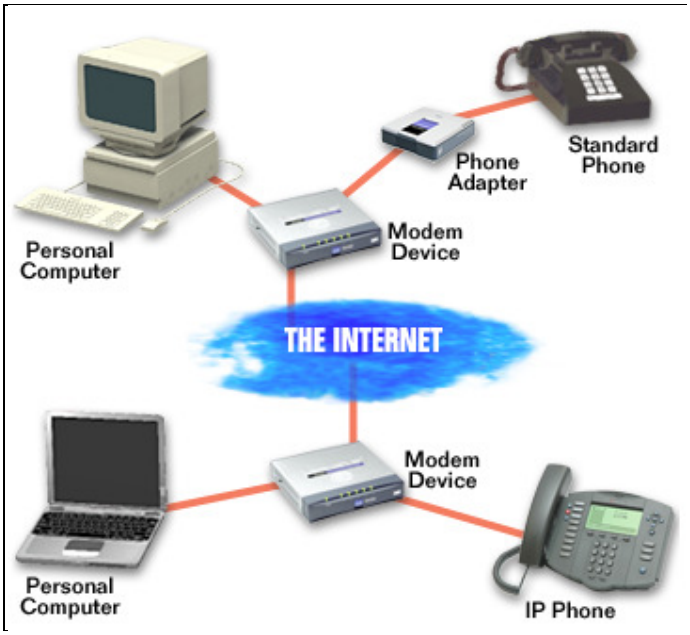

Figure 2: VoIP Connection Methods

Apart from the use of IP networks, VoIP requires other protocols to initiate calls, transmit and terminate calls.

Session Initiation Protocol [RFC 2543], is an application layer control protocol for creating, modifying and terminating calls with one or more participants.

H.323 is a VoIP standard having the ability to handle point to point communication and multipoint conferences.

Media Gateway Control Protocol [RFC 3435], is a VoIP protocol that maintains communication between call control elements and telephony gateways.

2.3 VoIP and PSTN comparison

VoIP has become increasingly popular and offers end users a lot of features and cost savings compared to the traditional PSTN. Table 1 is a brief comparison of the two technologies:

Table 1: PSTN VS VoIP

Features	**PSTN**	**VoIP**
Technology	Circuit switched	Packet switched
Network	Intelligent network / dumb terminal	Dumb Network, intelligent terminal
System	Closed system with inherited security	Open system with security as the vital issue
Carrier Lines	Dedicated lines required from the telco	All voice channels can be transmitted over the one Internet connection
Bandwidth	Each analogue telephone line uses 64kbps in each direction	Using compression, VoIP can use as little as ~10kbps in each direction. Further bandwidth can be saved by using silence suppression (not transmitting when the person is not speaking).
Features such as call waiting, Caller ID, conferencing, music on hold, etc.	Often available at an extra cost	Generally available for free
Remote PABX extensions for tele-workers and branch-offices	Very costly and require dedicated lines for each remote extension	Remote extensions are a standard feature
Expansibility and upgradeability	Complex: can require significant hardware additions, provisioning of new lines, etc	Often just requires more Internet bandwidth and software upgrades
Choice of companies to terminate calls	Each line is provisioned by a single telco, meaning there is very limited least cost routing	Hundreds of VoIP providers to choose from to terminate calls

Over the past 25 years international voice traffic has grown at an average of 14 percent annually. Traditional time division multiplexed (TDM) traffic grew 10 percent in 2007, to 265.6 billion minutes, while international traffic carried as VoIP grew 28 percent to 77.7 billion minutes (TeleGeography, 2008). Increase in VoIP traffic over the past few years is shown in figure 3.

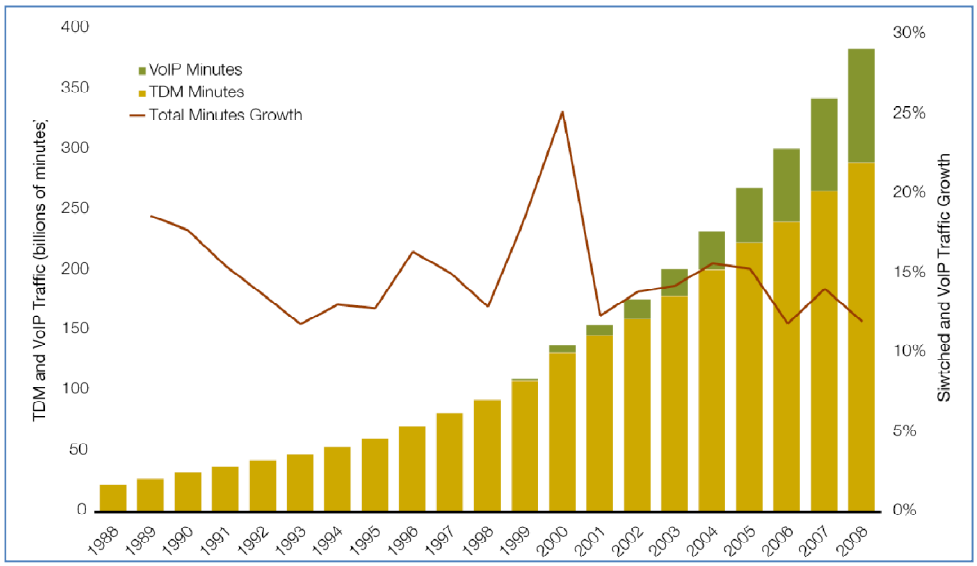

Figure 3: International Call Volumes and Growth Rates, 1998-2008

Africa was both the fastest growing source of and destination for international traffic. While outbound traffic grew 19 percent, all the countries of Africa generated only 2 percent of the world's switched international traffic in 2007. While traffic from the U.S and Europe grew more slowly than traffic originated in the other three world regions, the volume of traffic originated from Europe and the U.S remains far greater (TeleGeography, 2008). The volume of traffic for each of the major sections of the globe is shown in figure 4.

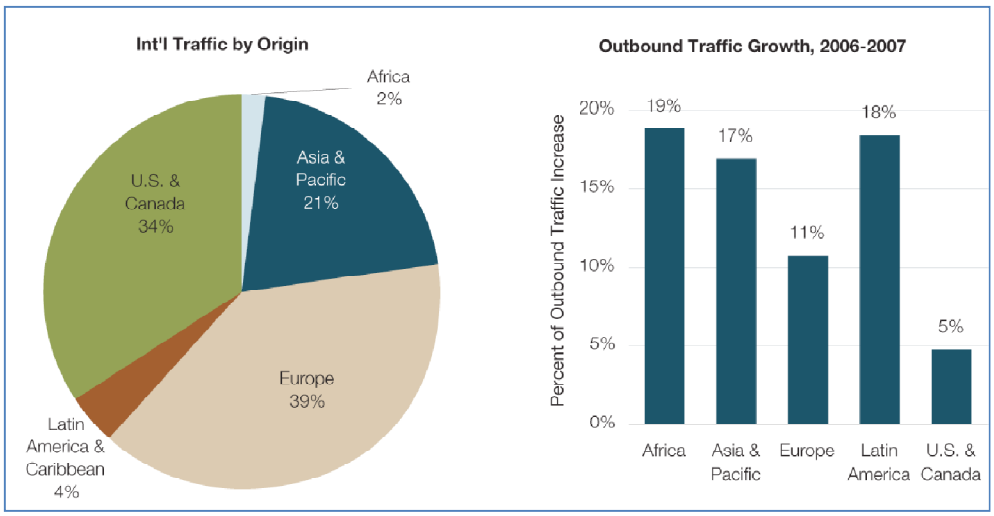

Figure 4: Traffic by Origin, 2007 and Regional Traffic Growth 2006-2007

The world average price for an international phone call has fallen more than 80 percent over the past 15 years and declined further 7 percent in 2007. Despite the steady erosion of prices, aggregate retail revenues from international traffic nudged upwards from $74 billion in 2006 to $78 million in 2007. Traffic growth has remained relatively stable with the rate of price decline has slowed. The data in the figure reflect both TDM and VoIP volumes. Periods where volume increases outpace average price declines is the period of revenue growth. When price declines outpace volume increase, revenue declines. The relation between volume and price is shown in figure 5 where data for 2008 are projections (TeleGeography, 2008).

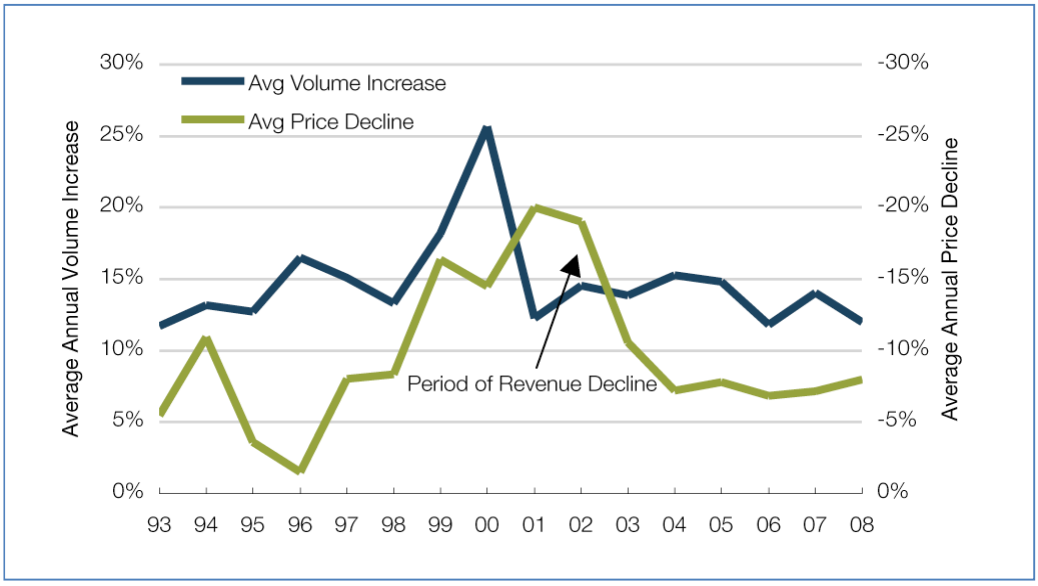

Figure 5: Rate of Price Decline versus Volume Growth, 1993-2008

TeleGeography estimates that Skype generated approximately 22 billion minutes of international 'Skype-to-Skype' traffic in 2007, and more than 33 billion minutes in 2008 – none of which touched the PSTN. Only after 5 years after its launch, Skype has emerged as the largest provider of cross-border voice communications in the world. Data for 2008 VoIP and TDM are projections. The percentage of traffic used by the traditional phone service and VoIP is shown in figure 6

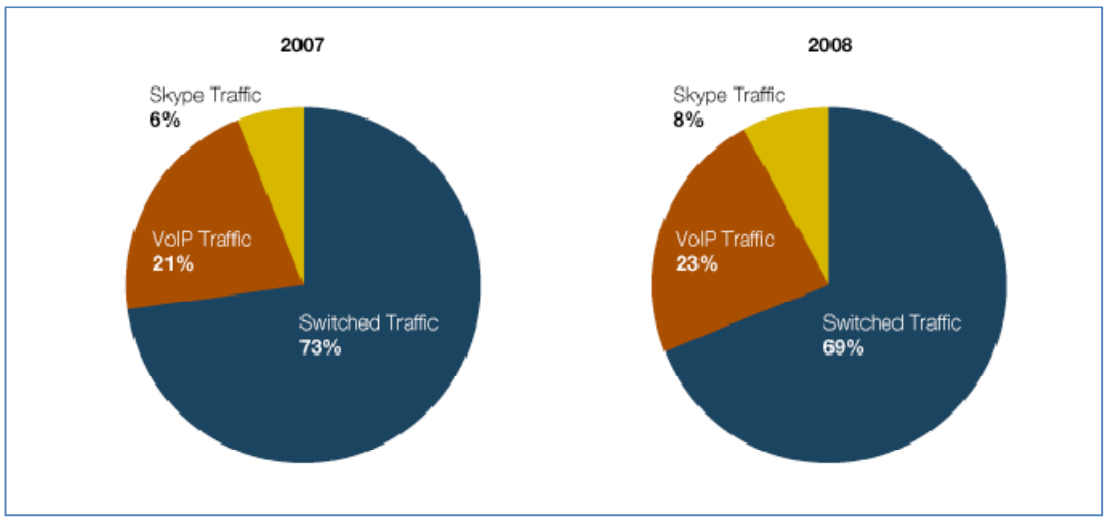

Figure 6: Total TDM, VoIP and Skype Traffic, 2007-2008.

PSTN Integration or Interconnection with the PSTN is crucial as VoIP technology is increasingly becoming common for telecommunication providers, who use VoIP over dedicated and public IP networks to connect switching stations and to interconnect with other telephony network providers (Wikipedia). VoIP providers terminate calls for customers or end users on to the PSTN at relatively economical rates. This is possible as the service providers purchase minutes in bulk from big telcos and with the voice data carried over the internet to a point much closer to the destination of the phone call, the last leg of the call to the PSTN is lot cheaper. For example, if an end user uses VoIP in Melbourne to a PSTN user in Sydney, the call is carried over the internet from Melbourne to Sydney (minimal cost) followed by a local call to the PSTN user within Sydney (un-timed local call).

According to Paul Budde Communications Pty Ltd, the market over the next 2-3 years will grow to over 1 million paid VoIP subscribers.

2.4 Electronic Number Mapping

For the telecommunication industry, after Local Number Portability was introduced, a convergence between the PSTN network and the Internet can be undertaken using ENUM, the technology that should bring numbering convergence to the next level.

ENUM or Telephone Number Mapping is a protocol and database that maps or converts a telephone number into a URI – otherwise known as an Internet domain name. ENUM will provide a bridge between the telephone and Internet networks for users. It is a solution to the problem of how various network elements can find services on the Internet using only a telephone number, and conversely, how a telephone can be used to access Internet services. It has the potential to facilitate development of the VoIP and other applications such as multi-media, video conferencing, instant messaging, directory services, home networking and even Internet games.

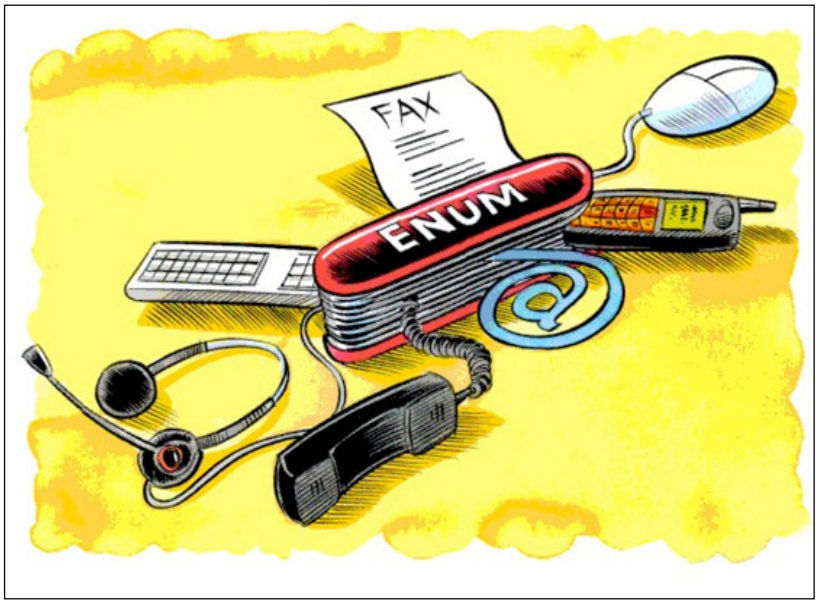

Figure 7: ENUM - Connects many services to ONE number

In order to implement ENUM globally, the Internet Architecture Board (IAB) has established a hierarchical structure to devolve responsibilities for implementing this concept down to countries and finally to service providers and carriers. The function and management of the implementation of ENUM for a country (in this case Australia), is firstly passed on to the government of the country as registry operator. The role continues to national bodies of carriers and service providers to provide Electronic Numbering services and database management for subscribers.

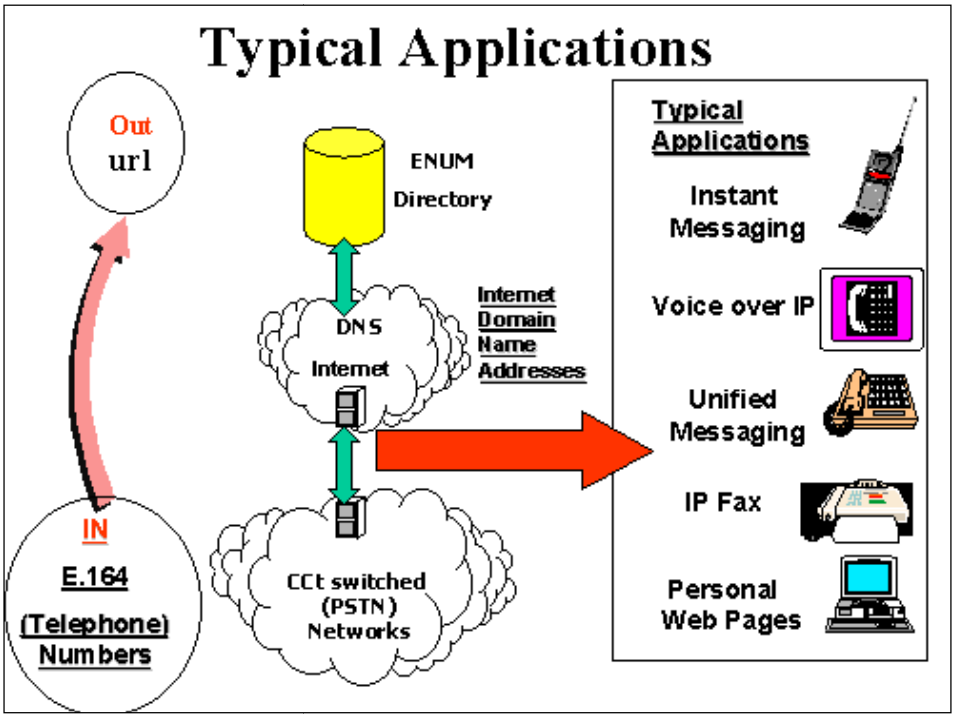

Figure 8: Typical applications enabled by ENUM (ACMA)

The E.164 numbers are utilised because it is an existing globally recognised numbering standard. Typical applications that could be associated with ENUM are shown in figure 8

2.5 How ENUM works

From RFC2916:

The domain "e164.arpa" is being populated in order to provide the infrastructure in DNS for storage of E.164 numbers.

This memo requests that the Internet Assigned Naming Authority (IANA) delegate the E164.ARPA domain following instructions to be provided by the IAB. Names within this zone are to be delegated to parties according to the ITU recommendation E.164. The names allocated should be hierarchic in accordance with ITU Recommendation E.164, and the codes should be assigned in accordance with that Recommendation.

According to RFC 2826, the single DNS root is required to ensure the DNS system operates properly. IETF supports the statement in RFC 3245 by deciding that only a single domain root could be supported in ENUM.

RFC 3245 stated the goal of ENUM as:

The goal with ENUM is that one party should be able to look up information in DNS, which another party has stored in DNS. This must be possible with only the E.164 number as input to the algorithm.

Single root DNS importance is emphasised for the convenience of the member looking for information from the particular web address. An example is when a member is looking for information of the ACA without knowledge of what the TLD is. The options open from .com, .gov, .net, .org, etc. Note that the correct web address is www.aca.gov.au, although www.aca.com.au also exists as Australian Consumer Association.

To avoid confusion of where to look up the ENUM record in the DNS, an agreed single domain root is essential. This is also to prevent members with ENUM like mechanism or other mechanism with similar structure.

Technical explanation of ENUM is in RFC 2916 that published in September 2002. To find a DNS names from a specific e.164 number, the following procedures apply:

- Ensure a full form E.164 number is applied, for example +61-3-12345678
- Remove all non-digit characters with the exception of the leading '+', hence: +61312345678. The "+" is kept at this stage to ensure it is a qualified telephone number.
- Remove all characters except the digit and put dots "." between the digits, the numbers become 6.1.3.1.2.3.4.5.6.7.8
- Reverse the order of the digit; append the string "e164.arpa" at the end. The final form is: 8.7.6.5.4.3.2.1.3.1.6.e164.arpa

It will query the DNS using that name to retrieve the Naming Address Pointer Record that are associated with the telephone number. A service is then chosen from NAPTR response on the various types of services by order and preference associated with the telephone number.

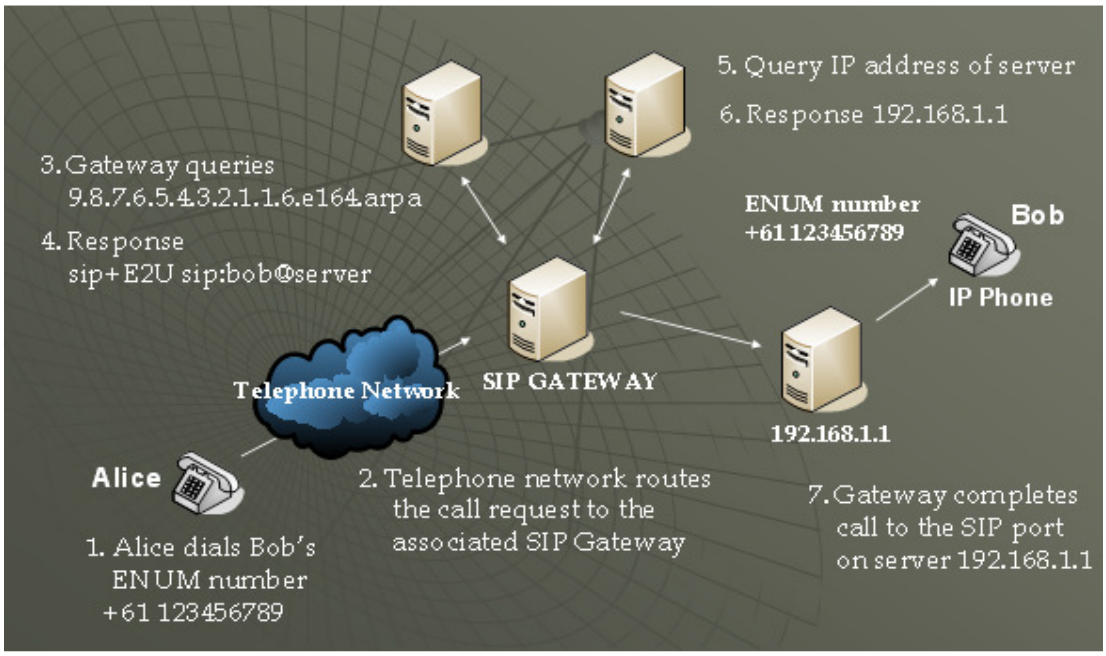

Figure 9: ENUM - Call Flow

RFC 3403 defines technically of ENUM query. The above example, figure 9, the telephone number is transformed into domain name "8.7.6.5.4.3.2.1.3.1.6.e164.arpa" and then used to retrieve records known as the NAPTR records.

An example of NAPTR record for the above domain defines in RFC 3403:

$ORIGIN 8.7.6.5.4.3.2.1.3.1.6.e164.arpa.

IN NAPTR 100 10 "u" "sip+E2U" "!^.*$!sip:ENUM@contact.au!i" .

IN NAPTR 102 10 "u" "smtp+E2U" "!^.*$!mailto:ENUM@contact.au!i" .

The RFC 3403 stated that the ‘u’ flag states that the Rule is terminal and that the output is a URI, which contains the information needed to contact that telephone service. The example shows the protocol used for the telephone services are SIP or Simple Mail Transfer Protocol. The multiple NAPTR record is set by the telephone number holder in the order of preference.

2.6 ENUM differences with DNS

The operation of information retrieval mirrors on a DNS system, where it uses a series of hierarchical tables or domains, where top level domains contain information and point to second level domains and so on should ultimately locate the intended destination. The purpose of establishment of an international ENUM registry (Tier 0) is to direct traffic to designated country, taking Australia as the focus of the research.

Some distinctive characteristics of ENUM from DNS are:

- *ENUM registrars must validate the identity of registrant and ensure the legitimacy.*
- *Any numbering changes applies to the current numbering plan such as area code change, number extension or modification should be automatically handled by registries, registrars and service provider*
- *ENUM registrants’ right are bounded with the telephone number, hence when telephone number disconnects, there will be no ENUM service for the registrant in question.*

2.7 Emergence of ENUM

E.164 NUMber Mapping was first defined by Faltstrom (2000) in Internet Standard RFC 2916. The basic idea was to add the widely used E.164 telephone identity to the Internet. The domain "e164.arpa" was proposed for storing the E.164 number information within the DNS. In short, the DNS translates domain names into IP addresses (addresses that make sense to the network). In 2004 this standard was succeeded by RFC 3761, which brought RFC 2916 in

line with state of the art DNS technology. Later on in the discussion around ENUM, the RFC 3761 is labeled as User ENUM. This has been done to distinguish it from Infrastructure ENUM.

2.8 Difference between User ENUM and Infrastructure ENUM

User ENUM: the mapping of telephone numbers (e.164 numbers) to URIs using the DNS in the domain e164.arpa, having the restriction that both record maintenance and record use, are within the user's authority.

E.164 numbers are standardized in the International Public Telecommunications Numbering Plan5 and compromise most numbers used for telephony services.
An URI is a unique pointer to an address on the Internet (Berners-Lee et al., 2005). Examples of URI's are http://www.tno.nl, mailto: l.maris@telecom.tno.nl6 and sip:alice@60.123.23.52 URI's.
The core functionality of ENUM is that it maps E.164 numbers to other identifiers (URIs). This mapping is done by means of the domain name system. DNS stores and associates many types of information with domain names, but mainly, it translates domain names (computer hostnames) to IP addresses. The domain that is reserved for User ENUM is the 'e164.arpa' domain.

User ENUM allows the end user to use its E.164 number as a general identifier for Internet services. For example it would be possible (if mail clients are supporting it) to email a user by using its E.164 number. So with User ENUM an end user can centralize his contact information behind one number. The other end-users are provided with capability of looking up contact data.

Notwithstanding the fact that the User ENUM standard has already existed for a substantial time, the standard did not gain momentum. Reasons for this limited use of User ENUM can be found in:

- The market for ENUM services is small, because there is no real user need; it is not solving a user's problem: a user does not want to be emailed on a number for example.
- Service providers / Operators have no say in User ENUM (Stastny, 2006)
- Privacy: there is the risk that User ENUM will become the ideal SPAM database, because querying this User ENUM gives user's contact information. This information can be misused by malicious organisations/persons. Because service providers do not have any control over the destination of E.164 numbers, they are reluctant to use the information from the User ENUM database. What is the benefit of putting an E.164 number in the User ENUM database if none of the service providers is using this database? Maybe other benefits will arise when new (successful) services become available for User ENUM. Currently there are no successful services for User ENUM. This lack of services for User ENUM is the reason for the small scale in which User ENUM is operating now and it is quite likely (because of the reasons above) that User ENUM will not gain momentum. This has resulted in initiatives to use the ENUM technology by service providers: Infrastructure ENUM.

Infrastructure ENUM: the mapping of telephone numbers (E.164 numbers) to URIs using a (public or private) DNS, having the restriction that record maintenance is done by the service provider. The term Infrastructure ENUM is interchangeable with "Carrier ENUM" or "Operator ENUM"

As mentioned above, ENUM is a database based on DNS technology. Important with every database is who has access/change rights to the database. The DNS database on the Internet is publicly available. So everyone can retrieve information from the DNS. However, only domain name holders are able to change this information. This is a clear concept. With ENUM these issues are not as clear as with the current DNS. The two main important issues are:

1. Who is able to use the information from the ENUM records?
2. Who is able to alter the ENUM records? (Who fills the ENUM database?)

In this report Infrastructure ENUM is defined as the type of ENUM in which only a service provider is able to alter the information in the ENUM records. The term provider plays a crucial role in this definition and therefore requires some clarification. The definition of a provider used in this report is: a telecom service provider which provides a voice service with E.164 numbers to customers. This definition does include providers who do not have their own network or network equipment. However, a voice service provider which does not provide E.164 numbers with its voice service is not considered as being a provider.

The question *who* is going to use the records is still in discussion and depends on the form of Infrastructure ENUM the providers chose for. If they want to keep most of the intelligence in the network, then they want to exclude users from using the database. However, a more open approach allows users to use directly information from the Infrastructure ENUM database. This choice which has to be made by providers also appears in the breakdown of Infrastructure ENUM in the right side of figure 10.

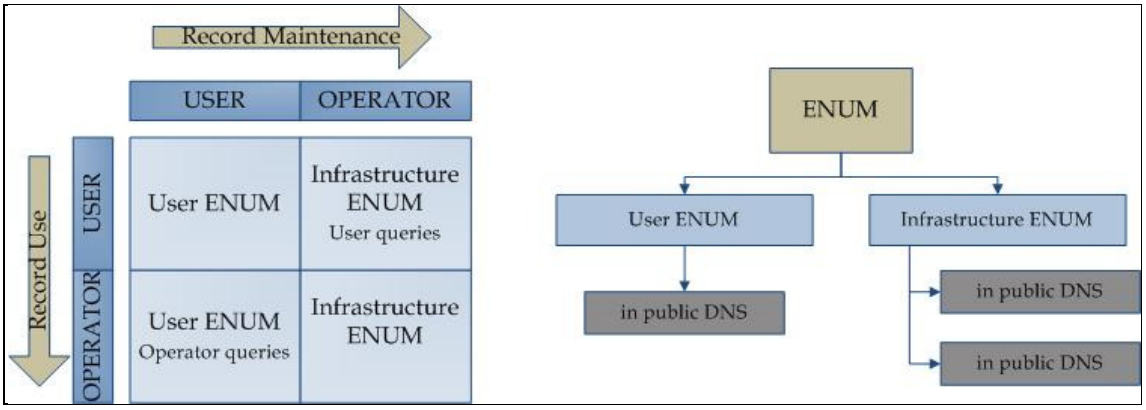

Figure 10 User and Infrastructure ENUM

Within Infrastructure ENUM there are two options:

1. Infrastructure ENUM in a private DNS

This is the closed form of Infrastructure ENUM. Only providers are able to query the Infrastructure ENUM database which is placed in a private DNS.

2. Infrastructure ENUM in the public DNS

This is the open form of Infrastructure ENUM. Everyone with access to the Internet is able to query the Infrastructure ENUM database which is placed within the DNS.

If Infrastructure ENUM is part of the public DNS then there are two options for using the identifier returning from the Infrastructure ENUM database:

1. The DNS is also used to resolve the final destination

This means that the information which is resolved from the Infrastructure ENUM database can also be further resolved in the DNS to recover the final destination. So all traffic can be routed to the right destination by means of the Infrastructure ENUM database and the DNS.

2. The DNS is not used to resolve the final destination

The Infrastructure ENUM database is just providing an identifier which points toward the right network. This means that only providers are able to use the information provided by the Infrastructure ENUM database for actually delivering a call. The Infrastructure ENUM database is the starting point for resolving where to find a particular E.164 number. The second stage, the delivering of a call can only be done by providers.

For example, a look up in the Infrastructure ENUM database gives URI gateway1@providerB.au. According to the first option, this URI can be resolved with the DNS to the right IP address. The second option shows that a local mapping is required to resolve the destination. This local mapping is set up according to agreements with other providers. The provider identifier, which returns from the Infrastructure ENUM database has the form of a URI. However, the specific form of this URI needs to be standardized.

Generally, User ENUM can be seen as the electronic visiting card and Infrastructure ENUM as a way of supporting providers for routing their calls. In theory these two ENUMs can co-exist.

2.9 Infrastructure ENUM's status of standardization

ENUM is an initiative coming from the Internet world. The main ENUM developments are done in an international environment: the Internet Engineering Task Force. This organization has a special ENUM working group en has published the standard (RFC 3761, User ENUM). For User ENUM there is a standard, for Infrastructure ENUM this is not the case. The discussions within the IETF ENUM working group around a standard for Infrastructure ENUM are in full swing (Pfauz, 2006). The main point of discussion is whether there has to be a special domain where providers can store their numbers..

2.10 ENUM and I-ENUM in Australia

User ENUM Trial was started by AusRegistry and took place in Australia between June 2005 and June 2007. Key participants in the Trial were AusRegistry International as a tier 1 registry, AARNet and Instra as tier 2 registrars, the ACMA and the Australian ENUM discussion group.

I-ENUM was raised in late 2005 in two papers tabled to the AEDG by ACMA, who are carrying out the trial for I-ENUM. The papers identified a number of assumptions and issues to be resolved before practical outcomes relating to I-ENUM implementation could be achieved. This table is a summary of those issues previously identified, and needs to be completed by the AEDG to further progress the trial to the next stage of an I-ENUM implementation.

Table 2: Issues for I-ENUM Implementation

	(AEDG Paper October 2005)		
Topic	**Assumptions**	**Issues to be resolved**	**Options for resolution**
Number ranges	At a minimum, geographic and mobile numbers may be included in I-ENUM	Whether other types of numbers are also to be included in I-ENUM (including different length numbers) 13x numbers 19x numbers	Austrian approach that each number (eg 13 11 11) is a number block not just a domain name

		1300, 1800 numbers	
Provisioning	No zone cuts below country code Instead maintain a single I-ENUM registry ***.infra.1.6.e164.arpa***	May need SOAP/XML provisioning system instead of EPP for I-ENUM, to interface with OSS of CSPs	Contact known interested parties and assess demand;
Authentication		Service providers likely to be Registrars for I-ENUM, and will need authentication process to interface directly with Registry.	AEDG to develop process for Registrar authorisation of service providers
Validation	Only providers with direct number allocations from ACMA able to register in I-ENUM	Need to verify a Registrar-CSP has the right to register a number block. Need to discuss validation for ported numbers, and validation for DID number blocks issued from other CSPs	Use ACMA register for directly allocated blocks AEDG to develop process for ported number validation
Billing	To be developed by Registrars (no requirements on billing in trial framework)		
Portability		Process needed for updating I-ENUM Registry when numbers port from one VoIP-SP to another (ENUM NAPTR will still point to old SIP URI). Q: How will donor provider know what SIP address will be used by gaining VoIP provider? Should ENUM registrations be deleted, or amended when ported?	Donor provider responsible for advising Registry to delete old record? Gaining CSP to advise Registrar of any re-registration

Benefits of ENUM

The year 2002 was when the concept of ENUM was conceived all over the world. Today many countries and organisations have done at least one trial, suggesting that ENUM is a maturing technology.

ENUM users receive benefit to decide the most appropriate method to communicate with other users and specify preferences for receiving incoming communication, which gives greater control by using single identifier.

ENUM allows the access of Internet based services from ordinary telephone connected to the Internet and other devices with numeric digits.

2.11 I-ENUM applications

In contrast with User ENUM, Infrastructure ENUM has two clear services. This creates opportunities for Infrastructure ENUM. The two services that can be distinguished are:

1. facilitating number portability;
2. facilitating VoIP peering.

The functionality of Infrastructure ENUM is basically the mapping of telephony numbers to URIs. This means that Infrastructure ENUM is only applicable in areas where mapping of identifiers is useful and necessary. If we take a look at the current PSTN interconnection, currently providers collect information where to route calls to, from the ACMA registrations and from the COIN platform. This information is kept in their local mapping database.

The COIN platform is the only platform on which providers are exchanging routing information on a substantial scale. Therefore the first application area for Infrastructure ENUM is number portability. Number portability is the feature of switching to another provider without having to change your number, which is required by law. Infrastructure

ENUM can be used as technology for the next generation COIN platform as shown in figure 11.

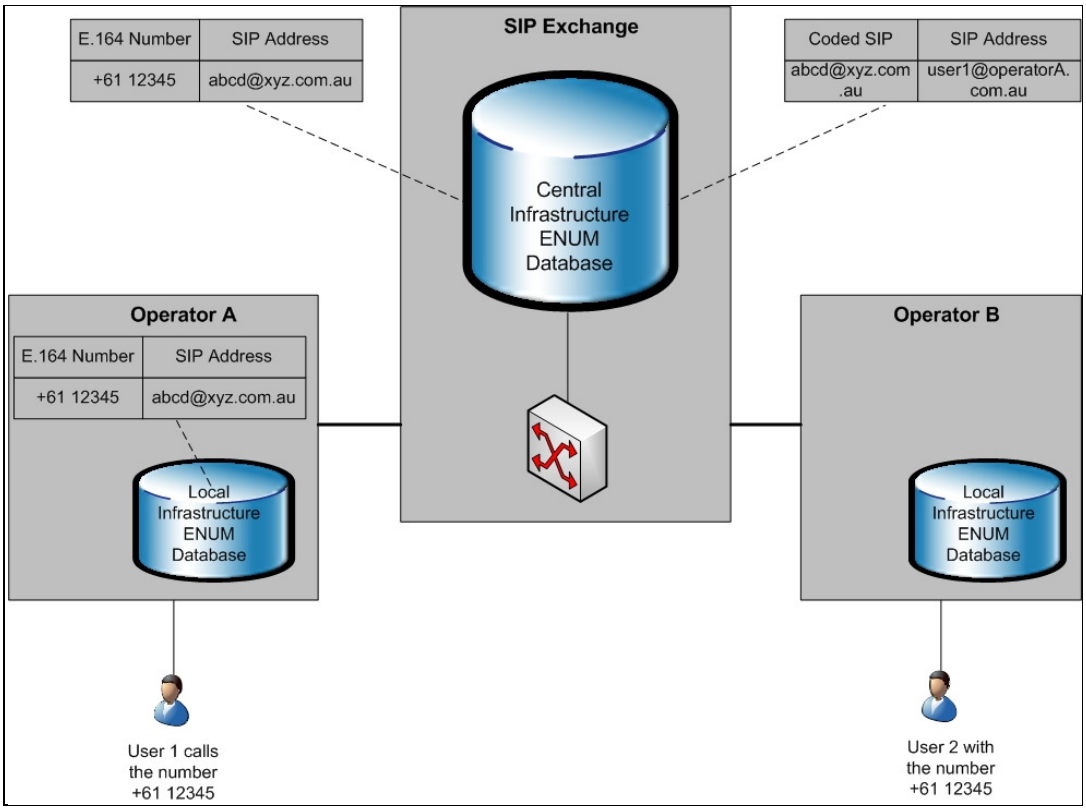

Figure 11 VoIP Peering

Next to this application of Infrastructure in the 'old world', Infrastructure ENUM can also be applied in the field of VoIP Peering. VoIP Peering is defined in this report as the linking of two networks of two providers by means of IP. Currently there is no information platform that contains information about where numbers are hosted and which numbers are reachable by IP. In order to deliver VoIP telephony services, VoIP providers are currently interconnected through TDM. Infrastructure ENUM could support the choice between PSTN and IP. It is important to notice that within VoIP Peering, Infrastructure ENUM will only facilitate the mapping of an E.164 number to an URI. Establishing a successful VoIP Peering requires more issues to be clearly arranged. Issues, like the use of the resulting URI data, as well as non-ENUM-derived URI data, for use in signalling and routing of realtime sessions, are out the scope of this report. The Session PEERing for Multimedia INTerconnect

(Speermint) working group of IETF is focussing on this part of VoIP Peering. It may be stated that if we take the "All-IP" paradigm seriously, any real-time communication originating on IP and terminating on IP must stay on IP end-to-end (Stastny, 2006). Infrastructure ENUM is a good candidate for facilitating the identifier part of it.

2.12 EPP Publishing Process

2.12.1 Introduction

Infrastructure ENUM facilitates service providers, specifically it helps them with their services provisioning. The registry offers the authoritative database and domain name infrastructures aiming to deal with the transactions between registrars as well as Name Authorities.

To handle the transaction between domain name registrar and registry, the EPP protocol has been chosen to make it happen flexibly. EPP is a XML based protocol that can be layered over multiple transport protocols and mostly transmitted over TCP connection, though other transmitting protocol could be used like SOAP, SMTP, etc. For security consideration, EPP is protected using lower-layer security protocols and clients exchange identification, authentication, and option information, and then engage in a series of client-initiated command-response exchanges. EPP would be used by service providers to update the registry with their interconnect points to enable VoIP peering.

2.12.2 EPP Characteristics

A relation between a registrar and a registry can be based on any procedure, even obscure close API, but the name space parties on internet saw a growing adoption of the EPP standard for managing publication. This is why this proposal uses EPP as the provisioning protocol, implemented as close as possible to the relevant RFCs. As stated in the previous paragraph, in our case provisioning works on "domains".

In the testing section we will see that sometime special implementations are used, these choices have been made depending on the handle capability of the registry. For example

"update domain" is the only transaction which allows RFC4114 [18] extensions (NAPTR), other transactions just work on the domain objects itself. By consequence "create domain" does not support RFC4114 transactions (which means that NAPTRs can't be added at the same time as when creating the domain itself. They have to be added with an "update domain"). Also, contact and host objects are not supported in the registry. However, these are implementation jitter and have no impact on the publishing result.

2.12.3 EPP Categories

EPP commands fall into three categories: session management commands, query commands, and data transform commands. Session management commands are used to establish and end persistent sessions with an EPP server. Query commands can be used to query the specified information from the server in order that the administrator of a registrar will be able to get the updated information. The last one is Transform commands; they are used to update the element contained within an object. Say, the DNS records associated with a domain name.

There are 9 EPP commands that are involved in registrar and registry communication, a detailed explanation about the commands has been added to Appendix D. They are: <login>, <check>, <info>, <transfer (query)>, <create>, <delete>, <renew>, <transfer> and <update>. As discussed in previous paragraph, the nine commands fall into three categories. Session management command: <login>; Query Commands: <check>, <info>, <transfer (query)>; Data Transform command: <create>, <delete>, <renew>, <transfer> and <update>. In the following section we will illustrate each command by using specific example.

In this thesis, we need only six EPP commands: <login>, <check>, <info>, <create>, <update>, <delete>. The rest of the commands like <transfer (query)> and <transfer> could be helpful for registrars to make more sophisticated transaction in the future. In this way, we put more emphasis on the commands that we are using in this proposal.

2.12.4 ENUM Tree and Number Allocation

The domain tree shown in figure 12 is the available domain that we will use in the Infrastructure ENUM deployment. Infrastructure ENUM is supposed to use e164.arpa's tree

instead of ienum.org.au that we are using here, among the reasons we choose this is because to be authorized to use .arpa it needs huge amounts of paper work, and also policy at government level would be involved. In this way, .arpa tree cannot be used at short notice.

To make it easier, we chose the ienum.org.au domain which is available to operate on it at all times. As shown in figure 12, we are acting in the level below 1.6.ienum.org.au. There are two specific numbers which point to their corresponding domain: 1.0.0.0.1.0.0.0.5.1.6.ienum.org.au and 1.0.0.0.2.0.0.0.5.1.6.ienum.org.au numbers. It implies that we are responsible for the number range +61050001 and +61050002. The core DNS server located in registry's level is the authority to maintain DNS database. In the example of sub-domain delegation below, we would like to create one sub-domain within the two SPs respectively.

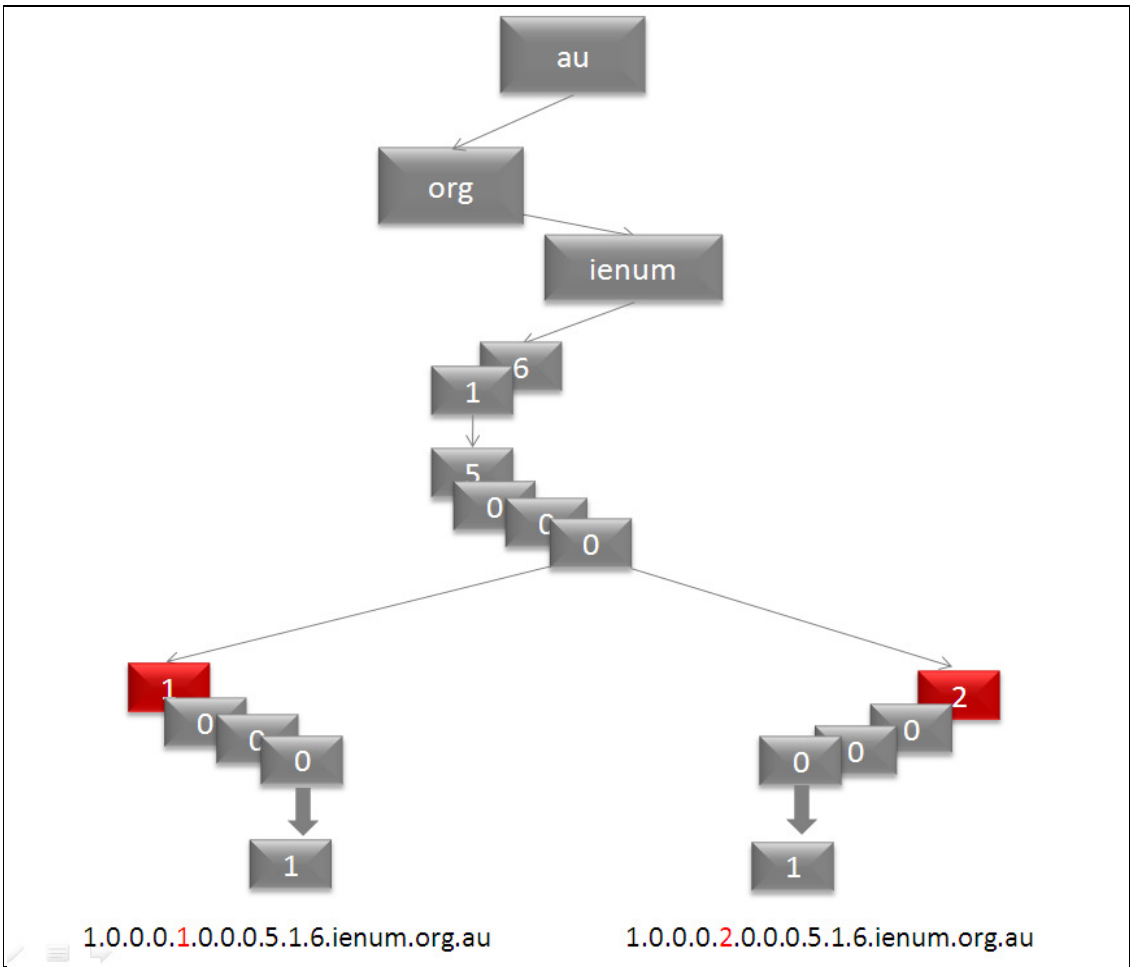

Figure 12: Operating number range

We choose an available number range from the I-ENUM trial space (+61500). In this way, two Service Providers can be created with the number range +6150001 and +6150002 respectively. In the examples of this section, we assume each Service Provider pick up the first available number in their number range, namely +61500010001 and +61500020001.

There is one selected trial telephone number in each service provider, which means there is one corresponding sub-domain for them. In the diagram above, we can see the sub-domains are: 1.0.0.0.1.0.0.0.5.1.6.ienum.org.au and 1.0.0.0.2.0.0.0.5.1.6.ienum.org.au.

Service Provider, like the role we are acting, can create the domain according to the telephone number by using EPP CREATE script. In our example, we illustrate how it works by creating 1.0.0.0.1.0.0.0.5.6.1.ienum.org.au sub-domain.

2.13 I-ENUM: Open Issues and Progress in Other Countries

From the literature and presentations about ENUM three open issues are identified. Around these issues uncertainty and discussion exists about how to design the Infrastructure ENUM system. The three open issues are:

1. The content of the Infrastructure ENUM database
2. The place of Infrastructure ENUM in the DNS
3. The organisation / cooperation needed to establish / operate Infrastructure ENUM.

There are already several Infrastructure ENUM initiatives (in private DNS) in operation in many countries. Currently, Infrastructure ENUM in the public DNS is only operational in Austria. Within the United States, there is also a trial with regard to Infrastructure ENUM, however, this is in an early phase (Neustar, 2006).

Austria

Austria was the first country to introduce a commercial ENUM service. On 24 August 2004, the Austrian Regulatory Authority for Telecommunications and Broadcasting (RTR-Gmbh) signed a contract with enum.at to provide Registry services for the Austrian ENUM domain of .3.4.e164.arpa until 2007. enum.at is a subsidiary company of nic.at, which operates the Registry for the Austrian country code TLD of .at.

The ENUM service in Austria allows end-users to register User ENUM domain names for geographic, mobile, private network and freephone numbers as well as ENUM specific numbers in the range +43 780. Prior to establishing a commercial service, Austria had conducted extensive trials of ENUM over the previous three years.

Asia Pacific ENUM Engineering Team (APEET)

APEET was formed in July 2004 and is an informal project team working on technical issues associated with ENUM. The main purpose of APEET is to coordinate ENUM activities in the Asia Pacific through cooperation between countries in the region that have been experimenting with ENUM. The member organisations of APEET are:

- China Network Information Centre (CNNIC)
- Japan Registry Service (JPRS)
- Korea Network Information Centre (KRNIC)
- Singapore Network Information Service (SGNIC)
- Taiwan Network Information Centre (TWNIC)

United Kingdom

A public trial of ENUM was run in the UK during 2003 by the UK ENUM Trial Group (UKETG), an ad-hoc industry body with input from the Department of Trade and Industry (DTI). In May 2004, UKETG released a report on the status of the ENUM trial which is available on the UKETG web site. In August 2004, the DTI released a discussion paper on the proposed arrangements for the implementation of ENUM in the UK.

Ireland

The Irish ENUM Forum was created in October 2003 and was hosted by the Commission for Communications Regulation (ComReg). The Forum created a number of guiding principles for ENUM in Ireland and established an engineering trial of ENUM in July 2004. In October 2004, the Irish ENUM Forum released its final report, which can be accessed from the ComReg website.

On 22 March 2006, ComReg announced that the IENUM consortium was awarded the right to operate the commercial ENUM Tier 1 Registry for Ireland. IENUM consists of Ireland's Internet domain registry body (IEDR) and the Internet Foundation of Austria.

South Korea

The Korean ENUM Service Council was established in September 2003 to manage ENUM activities in Korea. The council is composed of members from the Korean Ministry of Information and Communication (MIC), the Korea Network Information Centre (KRNIC) and telecommunications service providers. An ENUM trial was established in Korea and provided services to customers from 13 October 2003 to 9 January 2004.

United States

In August 2001, the United States ENUM Forum, comprising interested parties from the Internet and telecommunications industries, was established to investigate the possible implementation of ENUM in the US. Neustar, in alliance with the GSM Association (GSMA), offer private I-ENUM as the industry's first commercial service in the form of PathFinder an IP-based communication service

2.14 Voice over LTE via Generic Access (VoLGA)

Network operators and telecommunication vendors decided that it was time to implement a next generation network technology to meet the demand of the increasing use of mobile telecommunication networks for broadband internet access. Long Term Evolution, a project of the Third Generation Partnership Project, is the most widely adopted next generation standard based on the Internet Protocol leveraging the flexibility of packet switching. However, LTE does not support voice calls and SMS messaging as they are based on circuit switched radio and core network infrastructure. The solution was the invention of VoLGA.

VoLGA is based on the existing 3GPP Generic Access Network standard which extends mobile services over generic IP access network. Wi-Fi enabled phone is one of the popular applications of GAN. A GAN gateway securely connects a subscriber to the network infrastructure of an operator and voice calls and SMS are securely transported between the mobile device and the gateway over the intermediate Wi-Fi link and Internet access network. VoLGA uses the same principle as GAN by replacing Wi-Fi access with LTE. A VoLGA Forum was formed at the beginning of 2009 to further the development of this solution and create detailed specification documents

3 Objectives

The objective of the research is to develop a framework for the introduction of Infrastructure ENUM within Australia. To investigate the framework options the research will include the development of a I-ENUM test system and participation in the I-ENUM Working Group trial.

*ENUM provides solution to the destination finder location based on Domain Name System, where IP networks and PSTN networks are interconnected. It allows an IP device to communicate when an E.164 telephone number is reachable as Internet services. Hence, it is a numbering scheme and associated protocol that permits users to map subscribers to devices (*Mark Gregory, RMIT*).*

Unlike User ENUM, which is user centric with users able to choose services and call termination types, Infrastructure ENUM allows the carrier or VoIP service provider to decide on the service and the call completion or terminating type. This is done by resolving the called number from the I-ENUM DNS, identifying the service, ensuring that the terminating carrier has a compatible service and only then transferring the call via IP. This facilitates the service providers to publicize a set of rendezvous points for terminating services to other service providers.

Infrastructure ENUM is the key for service providers to keep control on the routing information behind e.164 numbers. A condition for Infrastructure ENUM is for E.164 numbers to be the method for identifying subscribers for an extensive period of time. The difference between User ENUM and I-ENUM is shown in figure 13

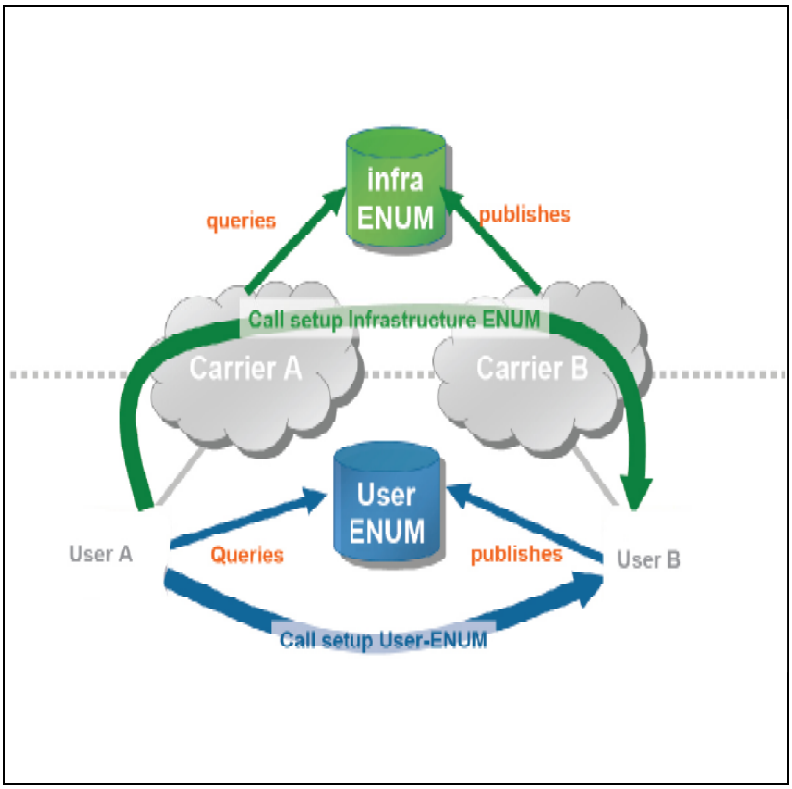

Figure 13: Logical Diagram for I-ENUM

3.1 Assumptions

This document is based on the assumption that industry will reach consensus on a specific technical mechanism that allows I-ENUM to be implemented on a national and international basis. At this point, it is expected that this consensus will be reflected in the appropriate RFC(s) being adopted by the IETF.

3.2 Limitations

The research is limited to the use of I-ENUM within Australia and the framework and model suggested would be for use within Australia. The framework and model is structured around using a private DNS and not the universal public DNS for lookups. The I-ENUM Working Group trial system included participation by a small number of organisations with a proof of concept approach. The group would represent the environment in which I-ENUM would operate and explore implementation possibilities in Australia.

4 I-ENUM Implementation Framework

The I-ENUM framework presented in this thesis was developed partially using input from the I-ENUM Working Group trial system and by considering and analysing the Australian telecommunication environment, including the competitive nature of carrier and service provider VoIP offerings.

The first phase of the research activity was to identify the systems and organisation that would interact with the I-ENUM implemented system and what that system would consist of.

The second phase of the research activity included the development of the test system to be used by the I-ENUM Working Group and to identify how the system could be implemented so that the majority of Australian carriers and VoIP service providers could access the system.

Finally a framework and model was proposed that may be used for an I-ENUM implementation in Australia. This chapter will include a description of the Framework and then provide a description of the implementation model and highlight information flows and organisation interaction within the model.

4.1 Framework

The I-ENUM Implementation Framework consists of systems and organisations responsible for the operation or interaction with the I-ENUM systems as shown in figure 14. The systems and organisations may be grouped where possible to simplify the framework.

The core of the framework is the I-ENUM system operator that maintains and operates the root registry which consists of a database and DNS system that may be replicated for reliability purposes. The I-ENUM system operator may be a specialist organisation that provides number management for fixed and mobile services or it may be a wholesale provider that facilitates VoIP service providers utilising the network.

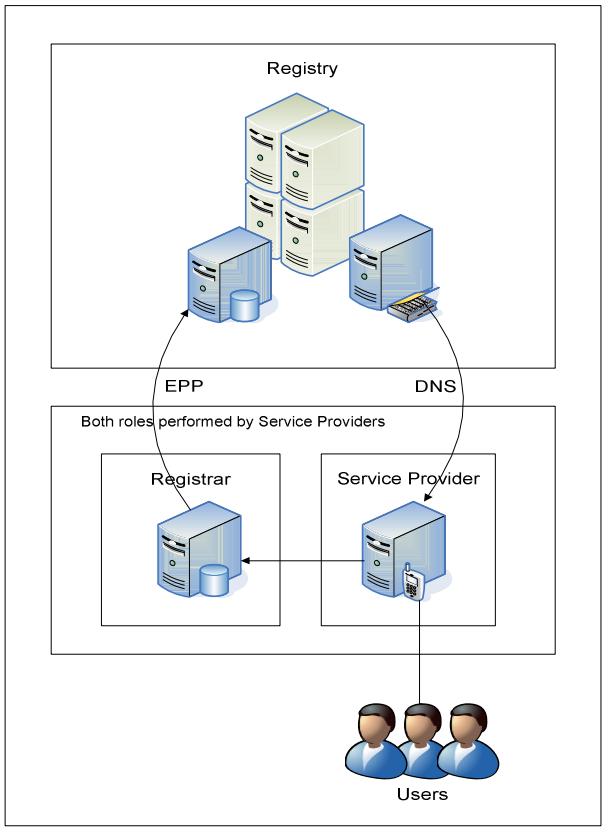

Figure 14: I-ENUM Framework

VoIP services are provided by carriers and VoIP service providers. Carriers and VoIP service providers will utilise VoIP gateways, SIP servers and an internal number management system that permits VoIP devices to be located within their network. The type of number management system used by carrier and VoIP service providers will depend on the network type and service offered, eg. a mobile VoIP solution may be different to a fixed VoIP solution because mobile VoIP devices are registered onto mobile wireless cellular networks and thereby identifiable, whereas fixed devices such as computers or cheap VoIP handsets may only be identified by the IP address assigned to the device. Customers may be utilising internal IP number ranges and DHCP which may further reduce the opportunity to identify VoIP devices in the orderly manner afforded to mobile wireless cellular devices and networks.

VoIP service providers may utilise a carrier network as a network and solution reseller. In this situation the VoIP service provider may be managing the VoIP customers separately to

facilities utilised and offered by the carrier and the alternative is also possible, where the VoIP service provider is utilising the carrier's underlying systems and acting as a reseller only.

4.1.1 I-ENUM System Operator

Root registry operator would need to have the registry database and multiple DNS systems spread geographically across the country and replicated to reduce lookup times and speed the updates.

In Australia, the ACMA is the statutory authority responsible for the regulation of telecommunications and responsible for the number management and number allocation to service providers. The government tenders the operation and management of the .au namespace and currently a private company, AusRegistry currently operates and manages the domain name registry database and root name server for the .au namespace. The ACCC is another statutory body that ensure fair competition between service providers. With many technical, operational and governance issues that arise from I-ENUM implementation, it would be best for the I-ENUM system operator to be a separate wholesale network provider, or other organisation, with authority to deal with each of the above organisations, specific to the role.

4.1.2 Carriers

In Australia, for example, Telstra, Optus, AAPT and Verison are Tier 1 carriers and service providers. Typically Tier 1 operators are large organisations that operate one or more large national networks that may include fixed and wireless networks. In the thesis, carriers would also be registrars with the authority to register, manage and allocated numbers to customers and to Tier 2 operators. The information flow for intra- and inter-carrier and the root registry would happen using EPP as described in Chapter 2.12 and must follow the regulations set by ICANN. When carriers provide VoIP services to users they act as registrars and service providers, a dual role.

4.1.3 VoIP Service Providers

VoIP Service providers may be Tier 1 or Tier 2 operators. A Tier 2 service provider typically resells services made available by Tier 1 operators and may operate their own network management facilities and gateway devices. A Tier 2 operator may also resell Tier 1 operator services and management systems.

VoIP service providers would be the organisations that benefit most by the introduction of I-ENUM. VoIP service providers would be able to peer VoIP calls with other Tier 1 and Tier 2 VoIP service providers over IP based networks with by utilising I-ENUM. Currently, this peering can only occur by routing VoIP calls destined for external VoIP users through the PSTN.

The principal goal for Tier 2 operators is for VoIP calls to operate only over IP based networks and therefore costs would be lower than when calls are routed through the PSTN – principally because the PSTN operators have set a relatively high connection cost.

4.1.4 Summary

The I-ENUM implementation framework would consist of an individual organisation acting as the root registry, Tier 1 and Tier 2 service providers as the providers and users of I-ENUM services. The I-ENUM registry operators are instrumental in routing VoIP calls between VoIP service providers. Tier 1 and Tier 2 VoIP service providers utilise EPP to update their internal systems, update the next level I-ENUM systems and finally the root registry. The three are integral components and the core of the I-ENUM implementation framework

4.2 I-ENUM Implementation Framework Model

I-ENUM implementation in Australia would be similar to Figure 15. A common I-ENUM registry / database shared by only authorised VoIP service providers could be used to peer VoIP services without the need to utilise the PSTN for peering.

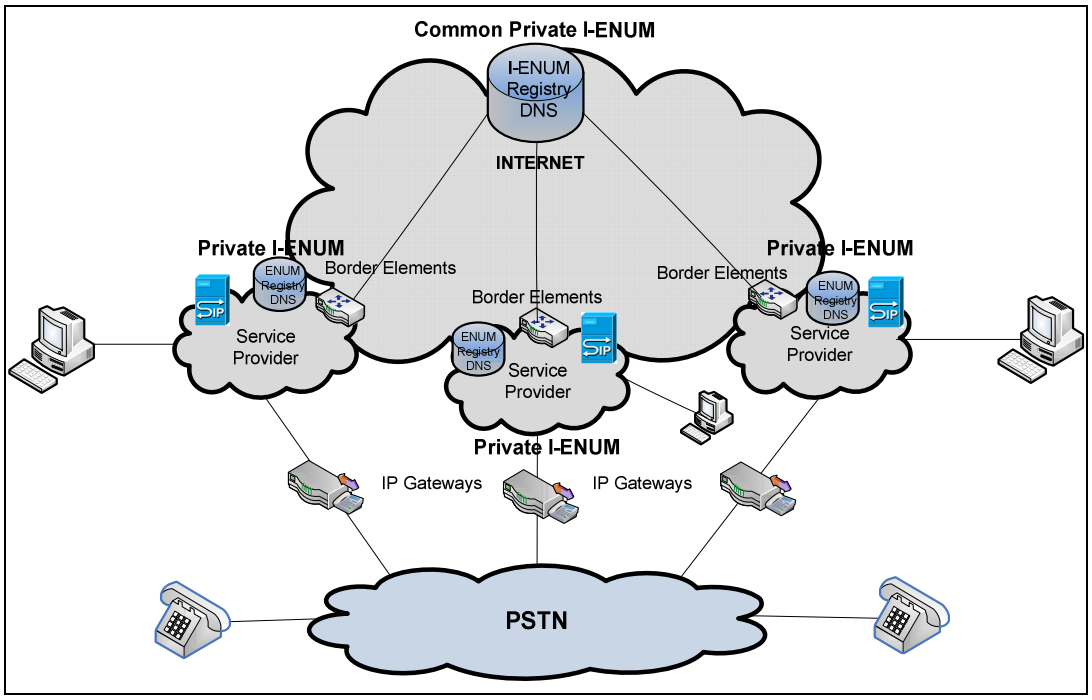

Figure 15: Shared Private I-ENUM structure in Australia

The service providers would have their own ENUM database and registry which is used to route calls with their network, border elements and IP gateways to route calls outside their network. The shared I-ENUM registry system hierarchy is queried when a call needs to routed to an outside network and depending on the rendezvous point returned, the call is either routed over the IP based networks or though the PSTN for non-IP based devices or for IP based devices that cannot be reached over IP networks as no data peering route is available.

4.2.1 Public versus private namespace

The ideal situation would be to use the e164.arpa domain as the apex domain for I-ENUM, however User ENUM uses the e164.arpa domain and hence it would be ideal to use a different, internationally agreed upon apex (instead of the e164.arpa) as suggested in RFC 5527. The single common namespace ultimately designated may or may not be the same as that designated for User ENUM (e164.arpa.). However, as per the RFC 5067, implementation of infrastructure ENUM must not restrict the ability of an end user, to choose a registrar and/or name server provider for User ENUM.

With the uncertainty of the apex domain, a private I-ENUM namespace could be used in the interim till the e164.arpa is made available. A private I-ENUM tree is not under e164.arpa or whatever namespace chosen for I-ENUM, but uses a privately held domain.

Authorised registrars provide a means for a provider to populate DNS resource records for the E.164 numbering resources for which it is the carrier-of-record in a single common privately accessible namespace. An example of a number block for a private name space is shown in Figure 16.

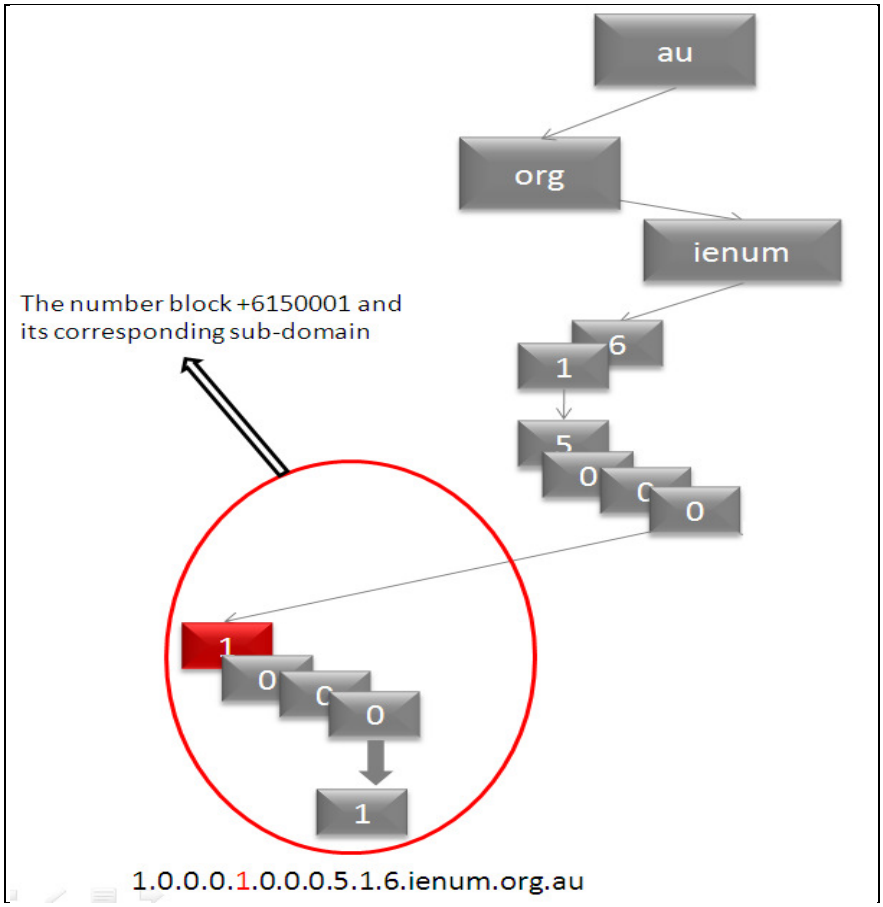

Figure 16: Number block map

4.2.2 Information flows

To route a call from SP A to SP B, as shown in figure 17, there would be three possible queries. First SP A would query the internal private I- ENUM database to find the border gateway to the SP's shared extranet. The border gateway from SP A needs to query the SP-

shared I-ENUM database DNS to find the address of the ingress border gateway of SP B, and the border gateway of SP B needs to query the internal private I-ENUM database DNS to finally find the AoR of the End-User for internal routing purposes.

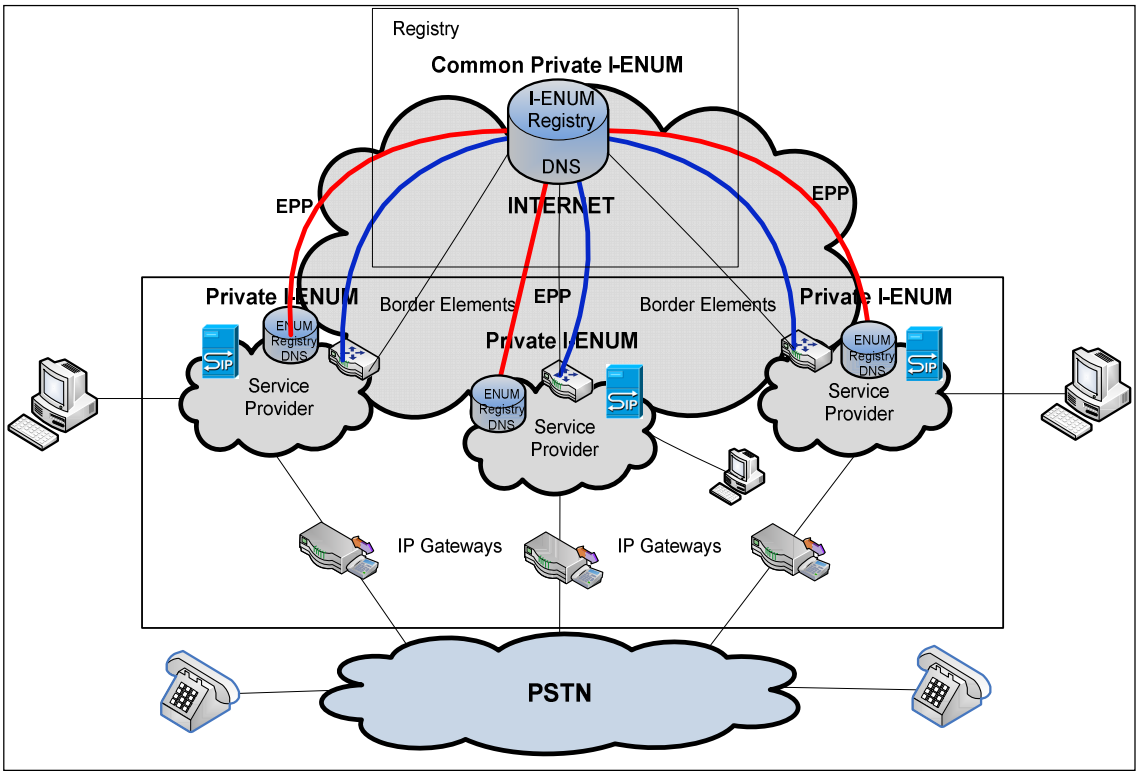

Figure 17: I-ENUM call routing using Common Private DNS

It would be the responsibility of all VoIP service providers to register with the tier 1 I-ENUM registry and to manage their domains and associated information including associating user E.164 numbers to the appropriate border gateway IP address.

4.2.3 Security and Privacy

I-ENUM system consists of a database and ENUM DNS server and the operation of this system may be considered in terms of the system management and system operation.

I-ENUM System Management

I-ENUM System Management is facilitated by the use of a restricted access database. Registered VoIP providers are provided with encrypted 256-bit SSL secure access to the database server so that registered VoIP phone numbers may be added, edited and deleted. To enhance this security access to the database is limited by the use of a firewall that restricts access to the registered IP address of the VoIP provider.

I-ENUM System Operation

I-ENUM System Operation is facilitated by the use of a restricted access DNS server. Registered VoIP providers are provided with access to the ENUM DNS server by a restricted access firewall that restricts access to the registered IP address of the VoIP provider ENUM gateway.

The facility exists to make access to the VoIP phone number NAPTR resource records to any VoIP provider. This would change the system from implementing a public I-ENUM model rather than a private I-ENUM model.

Privacy

The I-ENUM system holds limited information about a VoIP telephone number. For each VoIP telephone number registered in the I-ENUM system there is only one NAPTR resource record required which resolves to a SIP URI of the VoIP network gateway that the VoIP phone resides behind. No personal or other information is stored in the I-ENUM system and when using this model, no more information is publicly accessible than is available in a White Pages directory. The VoIP phone numbers registered into the I-ENUM system are managed by the VoIP service provider and are registered as part of the Australian domain.

The practice of utilising an I-ENUM system where VoIP phone numbers are matched with the VoIP gateway of the VoIP service provider network upon which the VoIP phone resides provides limited opportunity for end user privacy to be compromised as the VoIP service provider would manage calls coming into their network through their gateway. RFC 5067

refers to a 'carrier of record' using the technology of RFC 3761 to publish the mapping of an E.164 number into a URI that identifies a specific point of interconnection to that service provider's network.

VoIP providers currently publish telephone numbers on their networks through PSTN systems in accordance with current telecommunication regulations. The implementation of private I-ENUM mirrors this practice and does not make any more information available other than on which VoIP service provider network the VoIP phone resides.

4.2.4 Summary

The apex domain for I-ENUM should be e164.arpa or a parallel namespace. However in the interim till the apex domain is decided, a private name space could be used effectively. As and when a public name space is decided, a smooth migration across to this domain from the private domain is still feasible. It is suggested that the implementation would happen using a single common private I-ENUM database with authorised access to only registered service providers and VoIP peering between these providers.

4.3 I-ENUM Working Group Trial System

The *Australian ENUM Discussion Group* formed a I-ENUM working group in April 2007 and the working group conducted a trial from 1st September to 20th November 2008. The I-ENUM working group trial utilized the Austrian ENUM Trial Platform made available by the University of Austria. University of Austria staff provided assistance with the initial setup of the software for the Australian I-ENUM trial. The Austrian ENUM Trial Platform included an Oracle database, scripts and DNS server running on Redhat Enterprise Linux Server.

4.3.1 Participants and roles

The trial proceeded largely with the efforts of a small group of people. There were several factors that affected the trial progress. The trial effort occurred using equipment and systems provided by RMIT University, *MyTelecom Holdings* and *Comvergence*. Funding was not available for the trial and therefore the trial occurred as facilities and staff became available in the contributing organisations.

The IEWG trial used, and adapted for local use, the *Austrian ENUM Trial Platform* (enum.nic.at) running on Redhat Enterprise Linux Server with the Oracle database trial version.

VoIP gateways used were the Cisco Call Manager, Asterisk and OpenSER.

The Cisco system was only compliant with the obsolete RFC 2916 and to overcome this limitation, a DNS proxy was employed that resolved NAPTR records from RFC 2916 to RFC 3761 format.

A list of all participants has been mentioned in Appendix C

4.3.2 System operation

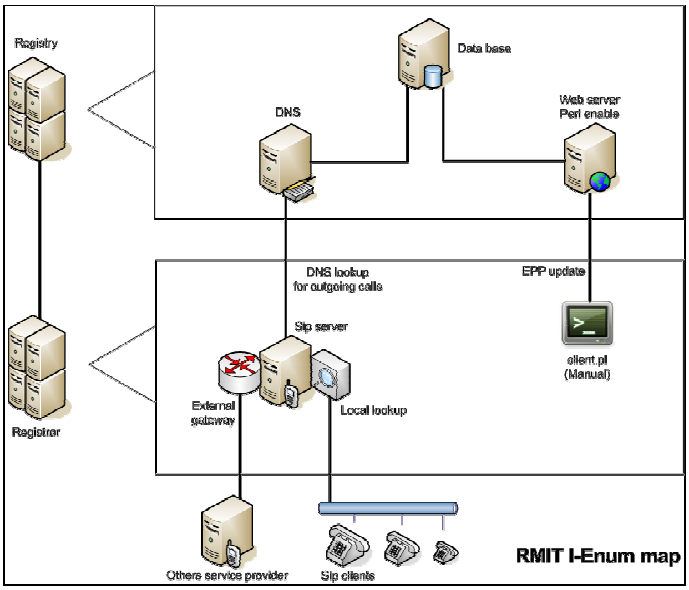

Figure 18: The RMIT I-ENUM map

The RMIT IENUM system in Figure 18 mainly consists of service provisioning and domain name requesting. The schema shows the registry on the top with an example of implementation. The bottom schema is a structure that contains a service provider part on the left and a registrar part on the right. On further steps an automated relation must be established between the SP and the registrar for the SP to publish its blocks of numbers quickly.

Utilising EPP and the underlying scripts VoIP providers register telephone numbers and the matching VoIP IP gateway on their network into the Oracle database and an automated process updates the DNS server NAPTR resource records.

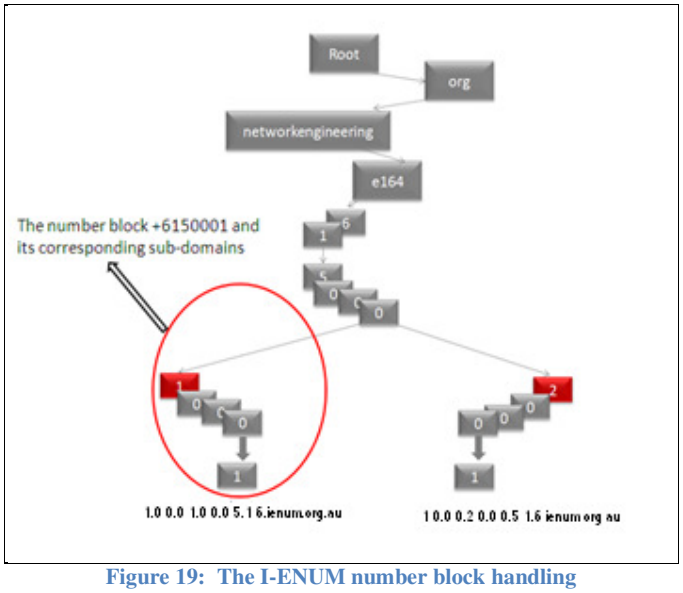

Figure 19: The I-ENUM number block handling

I-ENUM service providers can handle all numbers as blocks. One corresponding block of numbers in the DNS contains the same NAPTR RRs. In this case, as shown in figure 19, the block we are maintaining is +6150001 so that the corresponding DNS record will be 1.0.0.0.5.1.6.e164.ienum.org.au in the DNS of registry. As specified before, any subordinate domain name contains the same NAPTR RR in I-ENUM. For instance, 1.0.0.0.1.0.0.0.5.1.6.e164.ienum.org.au and 2.0.0.0.1.0.0.0.5.1.6.e164.ienum.org.au should contain the same NAPTR RR.

To handle the record stored in the DNS, the registrar needs to talk with the registry by using EPP. Through the registrar, the service provider could operate on their domain names and make them accessible to other parties when a specific number is requested.

An outgoing call from a registered VoIP provider is routed to the outgoing IP gateway and an ENUM lookup is carried out on the I-ENUM DNS. If a NAPTR record is returned that

identifies an upstream voice gateway for the call to be routed to, then the call may be routed using IP. If a NAPTR record is not returned from the ENUM DNS lookup then the outgoing call may be routed to the PSTN at the outgoing gateway. Therefore the VoIP provider has the option of routing calls using IP or directly to the PSTN at the outgoing gateway.

4.3.3 EPP In Use

Registrar needs a program to make the transaction happen. The program will facilitate registrar to specify which transaction to be sent and where to send. Ideally, it also provides supplementary functionalities which would make registrar feel friendly to make any transactions.

The client interface we are using, shown on figure 20, is a program based on Perl language. It can be executed in command line in a terminal of Ubuntu which is the operation system we chose to use for the registrar and the SPs.

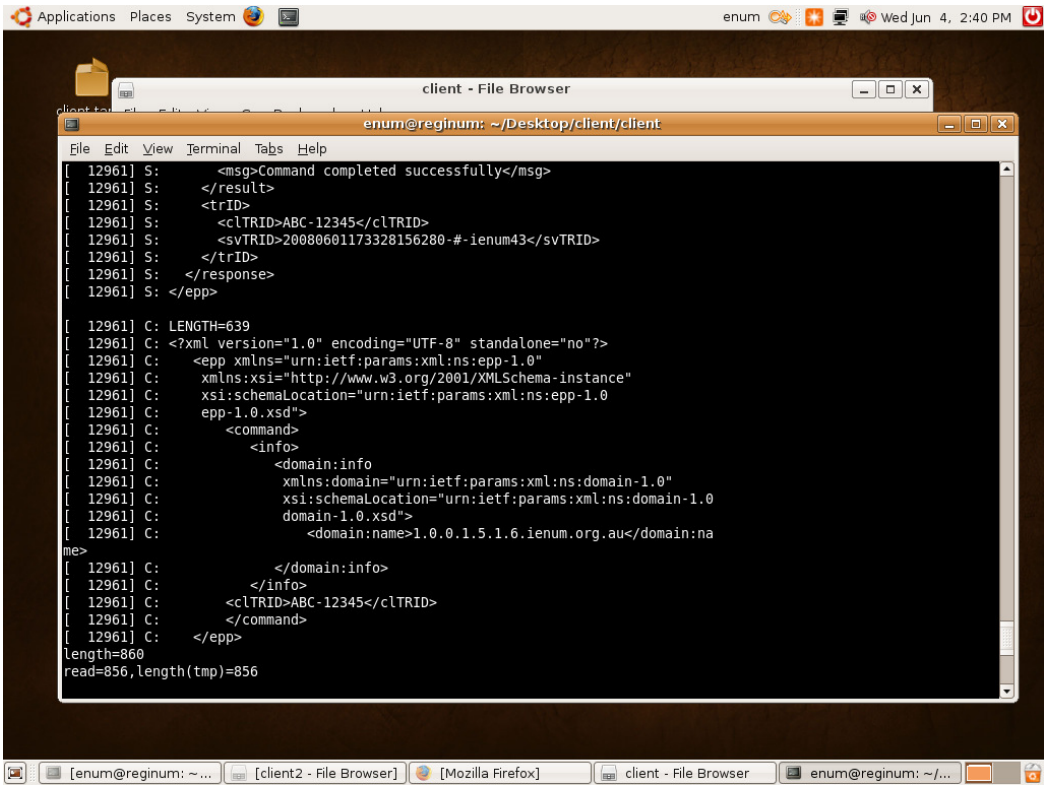

Figure 20: EPP client interface

In this project, we consider the Registrar and the service provider as the same entity. We consider the use of two ranges of numbers (+6150001 and +6150002) to provide SIP service. Then, we need to update our number range to the registry to create the corresponding domain for each individual of our range.

Before we log in EPP registry server, EPP registry has already created the registrar ID and password on the server. And we have been given the ID prior to our transaction. That's to say our client ID and password have already created on the server before we logon. Client should finish a series of paper works to obtain the ID for themselves.

4.3.4 Outcomes

A successful system test was carried out between MyTelecom Holdings Pty Ltd and Comvergence Pty Ltd. The test which was attended by some members of the IEWG, included making telephone calls between VoIP telephones on the MyTelecom and Comvergence networks. A copy of the Wireshark capture of one of the call sessions is provided in Appendix G.

To facilitate the test a private domain was used. The use of a private domain would limit the interoperability with other countries or systems that utilized or expected the use of a typical ENUM global top level domain e164.arpa. The I-ENUM trial used a closed system, where only registered VoIP providers gained access to the auenum.com.au domain tree and therefore the use of e164.arpa was not an important requirement for the trial Systems

4.3.5 Summary

The IEWG successfully carried out a trial of I-ENUM using the Austrian I-ENUM system. Testing of the system was carried out prior to the trial. The IEWG trial demonstrated that I-ENUM is a viable approach to providing number resolution between different VoIP providers in Australia. Two VoIP providers successfully utilized I-ENUM over their operational networks to connect telephone calls. An implementation of I-ENUM using a private domain tree is one approach that could be utilized by Industry to permit an operational implementation of I-ENUM within Australia pending a standardized approach being adopted by the ITU and the IETF.

5 Analysis

VoIP is emerging as a key technology for voice calls on next generation IP based networks. Internet speeds have drastically improved, and a move to fibre networks including fibre to the premise and 4G wireless cellular mobile networks may occur over the next ten years. The PSTN is still widely used and is still an expensive method of communication, even though competition in the Australian telecommunications industry has resulted in significant cost reductions over the past 10 years.

VoIP is a low cost method of communication because the transmission occurs over a customer's existing access to the IP based network. Currently VoIP peering over IP networks is only sporadically carried out in Australia and some of the VoIP service providers do not provide an easy migration path for potential customers by not offering number porting. VoIP peering over IP based networks would ensure that there was no need to utilise the PSTN as a segment in the call route. In this chapter the rationale for the proposed implementation framework and model will be analysed and discussed.

The main components for implementing I-ENUM in Australia are the root registry (private or public), carriers (that might also be registrars) and VoIP service providers. This chapter discusses the use of a private and public namespace and provides justification for the proposed implementation framework and model. Using the PSTN for VoIP peering is currently very expensive for most VoIP service providers as the PSTN segment is provided by a limited number of carriers.

A private namespace tree with a common shared root registry is envisaged to be the most appropriate I-ENUM implementation solution. Whether this namespace tree is to be linked to the DNS root registries within Australia is still uncertain, however this would be possible if the root registry for the I-ENUM tree were to be managed by a suitable organisation that has been provided with the e164.arpa domain.

A conference paper on the same topic has been accepted for publication at TENCON2010, a technical conference of IEEE. The paper has been added to Appendix F.

5.1 Proposed Australian I-ENUM framework and model

As of June 2009, 8.4 million users have Internet access which includes about 1.09 million of them who still use dial-up. Until recently, a phone line was needed for an Internet connection, but with the latest technological advancements, Internet access is now available without the need for an associated phone line. The ACMA's Communications Report 2008-09, highlights that as of June 2009, 2.5 million users in Australia and approximately 20% of the SMEs are known to have access to VoIP. With the government's proposal of providing Fiber-to-the-Premises (FTTP) at economical prices over the next 10 years to 93% of the Australian population, consumers would be able to access an IP based network suitable for television, multimedia, Internet, VoIP and other services. 3G mobile service take-up is continuing apace, with an estimated 12.8 million services as of June 2009, which is an increase of 44 per cent in 12 months. Increased 3G network coverage has also contributed to the increased take-up, with 99.06 percent of the population being covered as of June 2009. One of the 4G wireless network requirements is to combine telephony and data into a single IP based solution. As 4G wireless networks are rolled out, mobile customers will be utilizing VoIP on their mobile handsets.

An analysis of Australian government security and privacy requirements and possible I-ENUM implementation scenarios shows that I-ENUM implemented using private DNS that can only be accessed by VoIP service providers, is a satisfactory approach that should comply with security and privacy requirements. The use of secure EPP and firewalls limited to providing access to authorised organisations was found to be an important aspect of the solution.

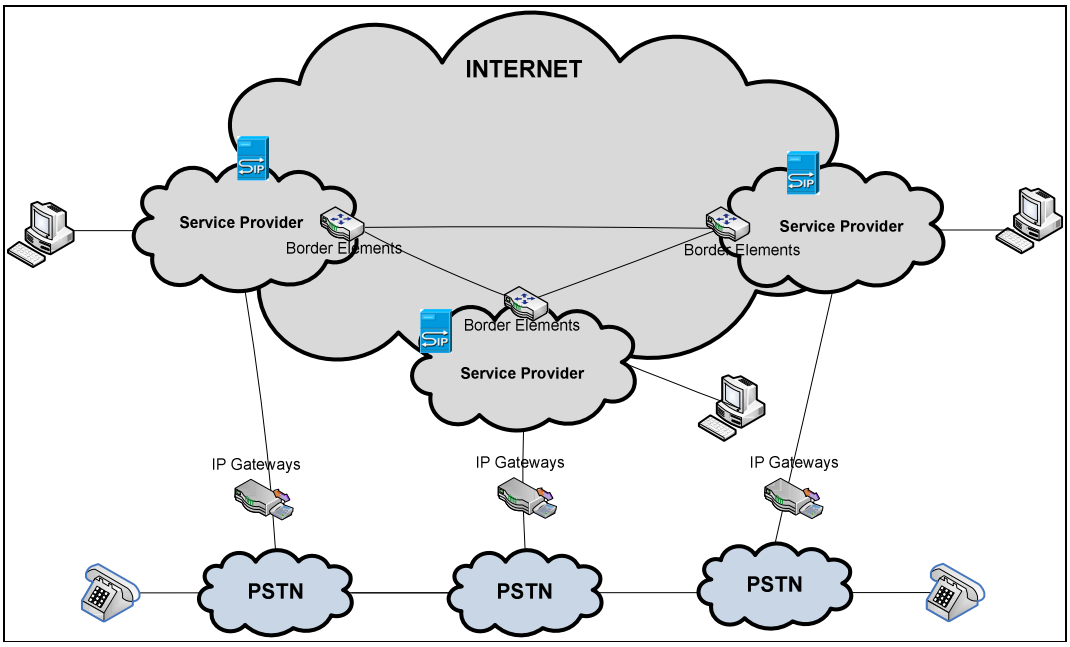

Figure 21: Communication using VoIP and PSTN in Australia

Figure 21 depicts how VoIP and PSTN are used to peer VoIP services in Australia. Many VoIP service providers have altered their networks partially or completely from TDM to IP based technology. Calls that need to pass through another service provider's network are routed either via TDM/IP gateways to the PSTN or border elements over the Internet. SIP is the protocol widely used by VoIP service providers to setup, manage and terminate VoIP calls.

As the VoIP service provider community increases the number of peering agreements between VoIP service providers will increase as well. Currently there is a need to include a PSTN segment in the peering unless the VoIP service providers are on the same carrier network and the carrier network provides the functionality to permit IP based peering. VoIP service peering utilising best effort IP transmission were identified on the Australian network in patches, with one example being VoIP service peering over the Pipe Networks carrier IP based network.

User ENUM provides the end users with the option of selecting the DNS name servers to host their ENUM NAPTR records for a given E.164 number, whereas for I-ENUM the choice lies with the service provider that currently manages the E.164 number. Therefore User ENUM and I-ENUM trees may be considered separately and this provides some flexibility in

the provision of an I-ENUM offering without preventing User ENUM from being offered as well. The public e164.arpa name space would not be appropriate for I-ENUM if customers require security and privacy of their number and personal details. An option would be to use a private shared I-ENUM tree and registry implementation for the following reasons:

The use of public e164.arpa domain is constrained by the procedures agreed between ITU, IAB, ACMA, ACCC and other organisations. VoIP service providers will need to enter E.164 numbers into the I-ENUM name space irrespective of whether delegations for the country code have been made in the public e164.arpa or a private tree

The public e164.arpa name space is normally governed by the opt-in principle. Numbers would only be entered with the explicit consent of the end user. This is not practical for the operation of a VoIP service that is acting as an alternative for a PSTN service

Information published in the I-ENUM name space by the VoIP service providers should not be public. This information could have details of the service provider border gateways and communication gateways and it may be reasonable to reduce the visibility of the gateways so as to reduce the possibility of attack

A common shared private I-ENUM registry / DNS on the Internet would permit and facilitate only participating VoIP service providers with storing routing information required for VoIP call interconnection through the service provider's gateways. As shown in Figure 22, apart from the connections to the PSTN each VoIP service provider's intranet would have bilateral IP connections via border elements to the shared extranet. DNS within the VoIP service provider is still used to maintain the information required to route calls within their own network. If a service provider queries a number hosted within the VoIP service provider's network the VoIP SIP server will request and receive a response from the local I-ENUM database / DNS. Whereas for a number query where the number is not hosted on the VoIP service provider's network, the I-ENUM DNS passes the query to the shared extranet, thereby receiving the routing information to the terminating VoIP service provider's gateway.

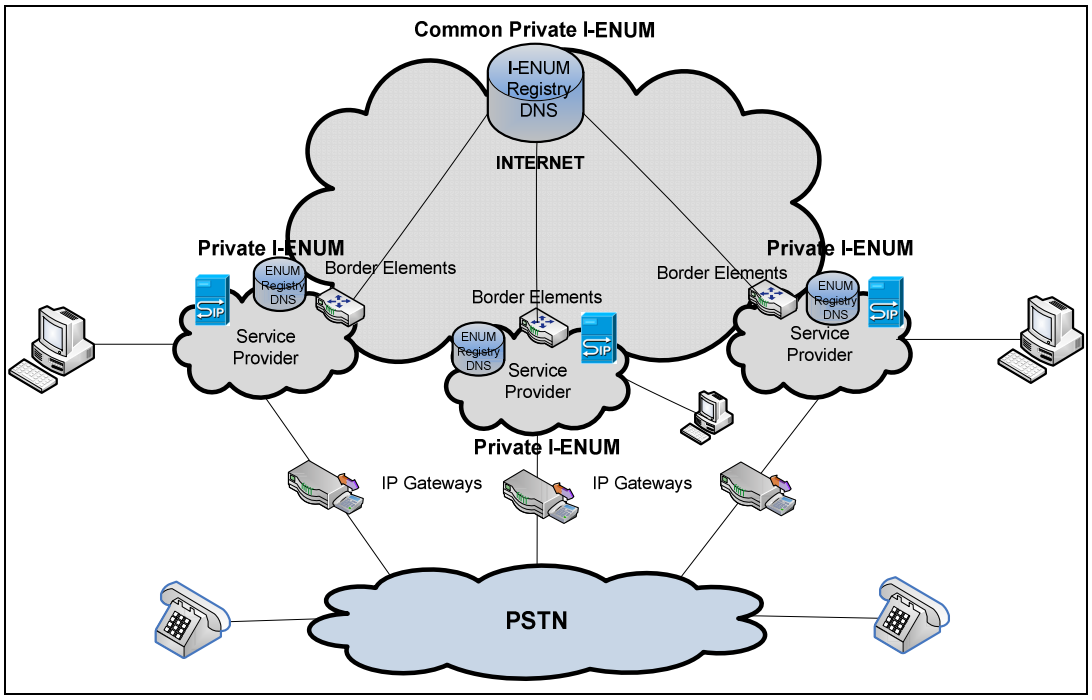

Figure 22: Shared Private I-ENUM structure in Australia

An extranet, in this case, is a private network on the Internet, which allows connectivity to only registered VoIP service provider networks, thereby preventing general open access to the VoIP peering, call control and I-ENUM NAPTR RR records. The private I-ENUM databases within the VoIP service provider networks would become tier 2 registries and the external I-ENUM databases would become the tier 1 root registry and this would be used to populate private access DNS that is made available only to VoIP service providers on the extranet. With this step the opportunity exists for international VoIP service providers to register and gain access to the Australian I-ENUM DNS.

To route a call from SP A to SP B, as shown in Figure 23, there would be three possible queries. First SP A would query the internal private I- ENUM database to find the border gateway to the SP's shared extranet. The border gateway from SP A needs to query the SP-shared I-ENUM database DNS to find the address of the ingress border gateway of SP B, and the border gateway of SP B needs to query the internal private I-ENUM database DNS to finally find the AoR of the end-user for internal routing purposes.

It would be the responsibility of all VoIP service providers to register with the tier 1 I-ENUM registry and to manage their domains and associated information including associating user E.164 numbers to the appropriate border gateway IP address.

This would put in place an infrastructure that would not only survive and meet the requirements of consumers but also offer more services, as and when the PSTN is retired. Evidence of the PSTN being retired is visible in the considerable decrease in the number of consumers using PSTN services. With FTTP arriving soon the Internet will become more accessible and affordable and this is likely to ensure that consumers would embrace VoIP.

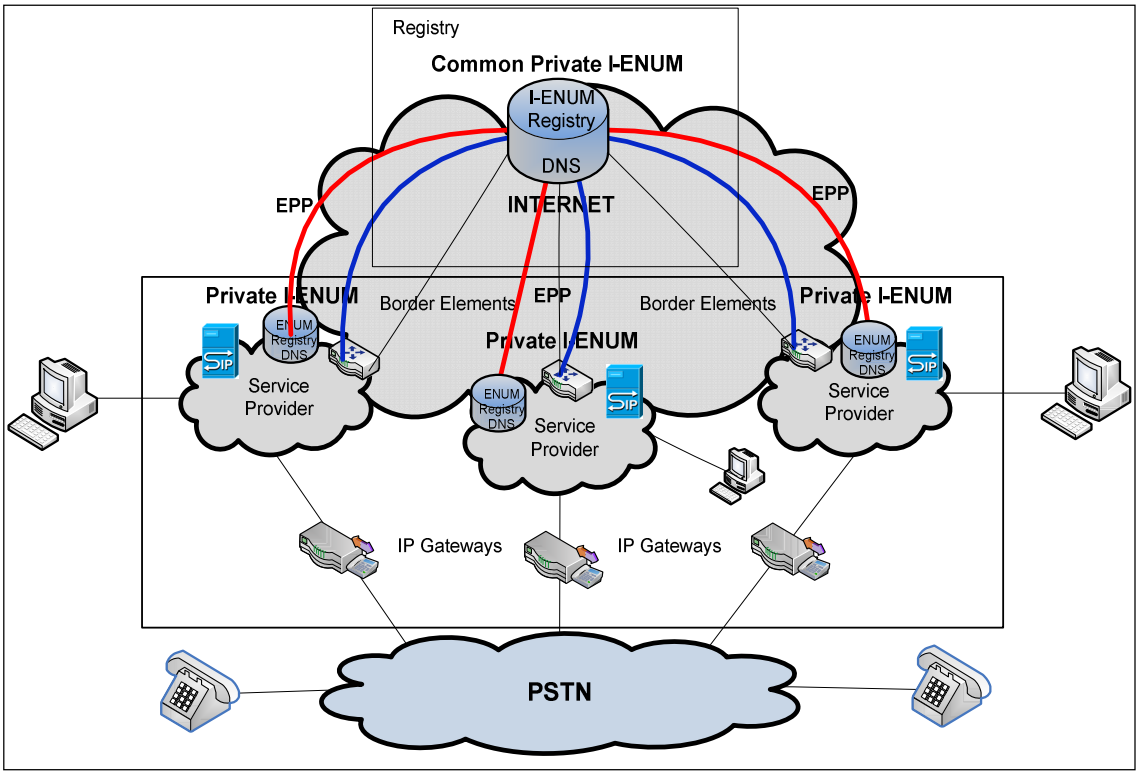

Figure 23: I-ENUM call routing using Common Private DNS

Taking the present state of Australian telephony into perspective, only a few Tier 2 VoIP service providers are utilising I-ENUM on one or two smaller carrier networks, such as Pipe Networks. The proposed model contains all of the active numbers as entries for Tier 1/2, with pointers to the different tier name servers which contain the actual NAPTR RR records.

This use of a hierarchy of I-ENUM registries and DNS facilitates number portability, wherein the authoritative name server and associated VoIP service provider for each number could be entered into the Tier 1 registry. When a number is ported from SP A to SP B, as in

Figure 24, the Tier 1 registry has to confirm the number port by consulting with SP A and then notify SP B to update the information associated with the number including the routing information from SP B and the SP B's border gateway IP address. The Tier 1 registry would be updated as new VoIP devices are installed and associated E.164 numbers are provisioned.

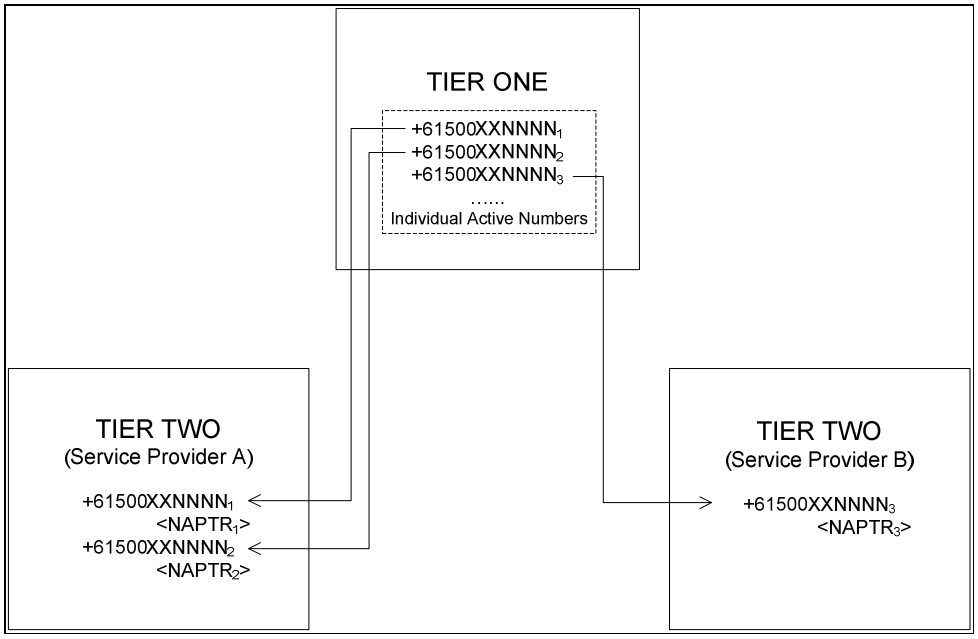

Figure 24: Tiered Architecture - Proposed

5.2 Motivation for VoIP Peering

For the purpose of the analysis and discussion it is envisaged there are a number of organisations that may offer VoIP services:

- Carriers
- Cable Operators
- Independent specialist suppliers of VoIP software and services, like Skype (PC based) or Vonage (phone based)
- Internet Service Providers, who are increasingly offering VoIP services in conjunction with their broadband access plans for business and residential customers

- Equipment manufacturers, who develop the equipment to support the various forms of IP Telephony, such as headsets or handsets or premise-based equipment like IP-PABX

Apart from the organisations that use fixed connections, new wireless operators are also emerging to avoid the cost of building costly fixed networks. They can offer services to regional and remote areas where the distances between households are large.

With the large number of organisations in the VoIP market competition for customers is increasing. In Australia, the telecommunications industry was previously first a monopoly and later in oligopoly situations where initially only one and later a few large firms dominated the telephone markets. The largest carrier, Telstra still does not offer VoIP services for residential customers, preferring to offer customers PSTN services.

The PSTN is centrally managed system where interconnection happens via predefined routes. Some of the VoIP networks today have no VoIP peering options at all, for example Skype offers no VoIP to VoIP peering to other networks. However, SkypeOut is a chargeable service that Skype offers for off-network calls only to PSTN numbers.

The research analysis highlighted driving forces behind the uptake of VoIP and the need for a VoIP peering solution. The main incentive for consumers to shift to VoIP is cost savings. An example of typical costs for telephone, Internet, and VoIP is provided in Table 3.

Table 3: Cost Analysis of PSTN and VoIP in Australia

	PSTN	**VoIP**
Phone Line Rental	Up to $39.95 per month	NA
Internet Plan	Starting from $39.95 per month	Starting from $39.95 per month
Local	15c flat per call	10c flat per call
National	39c – Connection fee $2 maximum for up to 3 hrs	10c flat per call
International (Eg. India)	39c – Connection fee 25c per min	20c per min
Mobiles	39c – Connection fee	28c per min

	18.5c per 30secs	

Currently, where VoIP to VoIP peering is not available peering is usually handled via the PSTN network which is not desirable as it is expensive. If a call travels through the PSTN there would be a need for PSTN gateways and associated PSTN network equipment, facilities and transmission systems which would increase the equipment and maintenance costs (figure 25). Also, the actual transit generates costs as PSTN operators expect their regular PSTN call fee to be added for the traffic. Finally, there is a need for converting the call at the origin and at the terminal end (coding and decoding), thereby degrading the quality of a VoIP call Quality of Service.

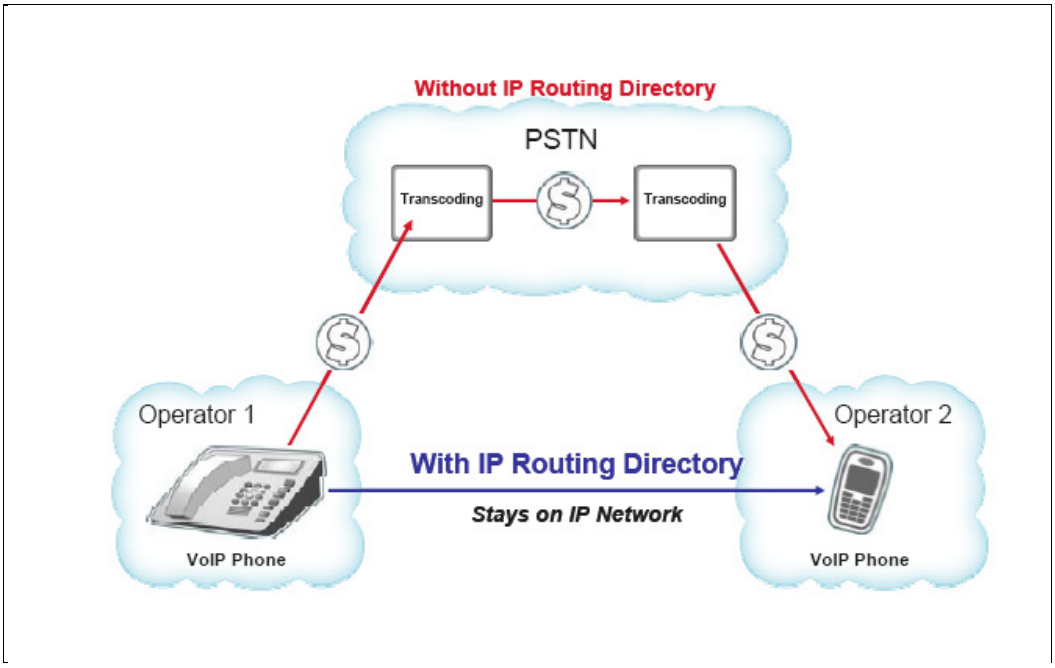

Figure 25: IP-based Routing Directories for IP Interconnect

VoIP QoS is a major concern for businesses and residential customers. Many VoIP service providers have realised the importance of improving VoIP QoS and have migrated their networks to IP-based networks with two or three grades of service. The shift away from having one "best effort" grade of service is seen to be a major step that must be taken to ensure that VoIP QoS is adequate for consumer confidence. Currently, however, the Australian carriers do not offer multiple grades of service to VoIP service providers unless there is a substantial increase in the fee paid for bandwidth. This additional cost forces most

VoIP service providers to peer calls to external terminations through the PSTN. VoIP peering over IP networks would be the key to maintain cost effectiveness.

The cost savings for customers who adopt VoIP and discard the PSTN services are detailed in Table 4, whereas Table 5 and Table 6 detail the wholesale pricing for VoIP services from upstream providers.

Table 4 – Cost Savings – PSTN vs VoIP [iiNet]

PSTN Lines	Monthly PSTN Cost	Ratio SIP Lines	SIP Lines	SIP Numbers	Monthly SIP Cost	Savings
5	$199.75	1:1	5	10	$110.00	45%
10	$399.50	1:1	10	10	$210.00	45%
		1:2	5	10	$110.00	72%
15	$599.25	1:1	15	20	$310.00	48%
		1:2	8	20	$176.00	71%
		1:3	5	20	$110.00	82%
25	$998.75	1:1	25	30	$475.00	52%
		1:2	13	30	$274.00	73%
		1:3	9	30	$198.00	80%
		1:4	7	30	$154.00	85%

Wholesale rates for a minimum of 20 lines which facilitate 20 incoming and outgoing lines simultaneously is a common starting service accessed by new VoIP service providers.

Table 5: Line Rates per Month

Name	Number of Lines	Cost per month	SIP and IAX
Virtual PRI 20	20	$123.95	YES
Virtual PRI 25	25	$153.95	YES
Virtual PRI 30	30	$183.95	YES
Virtual PRI 40	40	$243.95	YES
Virtual PRI 60	60	$363.95	YES

Table 6: Wholesale Call Rates

Call Type	Cost	Unlimited	Per Minute	Physical Route
Australia Nationally (All of Australia)	9c	YES		Australian PRI
Australian Mobiles	16c		YES	Australian PRI
International	32.16c		YES	Australian PRI

It would be beneficial to be able to evaluate the value of a network, but it is very hard to accurately evaluate the financial value of a network. Network equipment could be valued by calculating the current value, but the value of the network for its users cannot be measured. This thesis looks at the actual value gained from peering networks, thereby helping us understand the network effect and the incentives for peering networks.

Robert Metcalfe, inventor of Ethernet, rationalised the value of a network into a formula known as Metcalfe's Law, which states:

The value of a telecommunications network is proportional to the square of the number of connected users of the system (n^2).

The value of the whole network for all users, having 'n' users on the network, would be n*(n-1)/2, as there would be n*(n-1)/2 connections possible between pairs of users on the network. Since this cannot be accurately measured, the value of the network according to Metcalfe's law is usually rounded to n^2

Metcalfe's law has been criticised as the law assumes that every new connection is equally valuable for a user, which is not the case in real life as users tend to communicate more with people who live close to them than people who live far away. Odlyzko and Tilly (2005) introduced a new law which estimates the value of a network grows in the order n*log(n). The valuation problem found in Metcalfe's law was overcome by giving a different value for each user on the network, which is an application of the Zipf's law. If each member has a different value of 1/k and the value of the network for some user is the sum of decreasing 1/k values [1 + ½ + 1/3+....+1/(n-1)], which is roughly log(n) and therefore the whole network is valued at n*log(n).

If Metcalfe's law were true, then every network would have an incentive to interconnect with another network regardless of the size of the network, thereby eliminating the possibility of isolated networks. This was another point raised by Odlyzko and Tilly (2005) and Briscoe et al. (2006). This new n*log(n) law would better suit where large networks have little incentives to interconnect with smaller networks without a compensation from the smaller networks.

Table 7: Comparison between Metcalfe's law and n log(n0 law

Network Size	Metcalfe's Law			nlog(n) Law		
	Value before interconnecting	Value after interconnecting	Gain	Value before interconnecting	Value after interconnecting	Gain
n	n^2	n(n+m)	nm	n log(n)	n log(n+m)	n(log(n+m) - log(n))
m	m^2	m(n+m)	nm	m log(m)	m log(n+m)	m(log(n+m) - log(m))

A comparison of the gain between two networks of different sizes using the two laws is shown in table 7, which again proves that the smaller networks would gain more by interconnecting. However, interconnecting isolated networks will result in more value that just the sum of each network's values and this net gain is an incentive for interconnection. This reasoning could explain the reason for the isolated networks and the increasing number of service providers.

As of June 2009, an estimated 287 VoIP service providers and 638 Internet service providers operate in Australia. Australian ISPs are offering a range of bundled voice and content services to consumers. Mobile revenue exceeded PSTN revenues for the first time in 2008-09, demonstrating a shift in consumer use and preference. ACMA's recent survey indicates that 81% of metropolitan consumers using VoIP are quite satisfied with the service and quality. This increase in the number of consumers shifting to VoIP (as shown in figure 26) is due to the service providers offering diverse communication methods, like VoIP to PSTN, VoIP to VoIP, PSTN to VoIP and PSTN to PSTN.

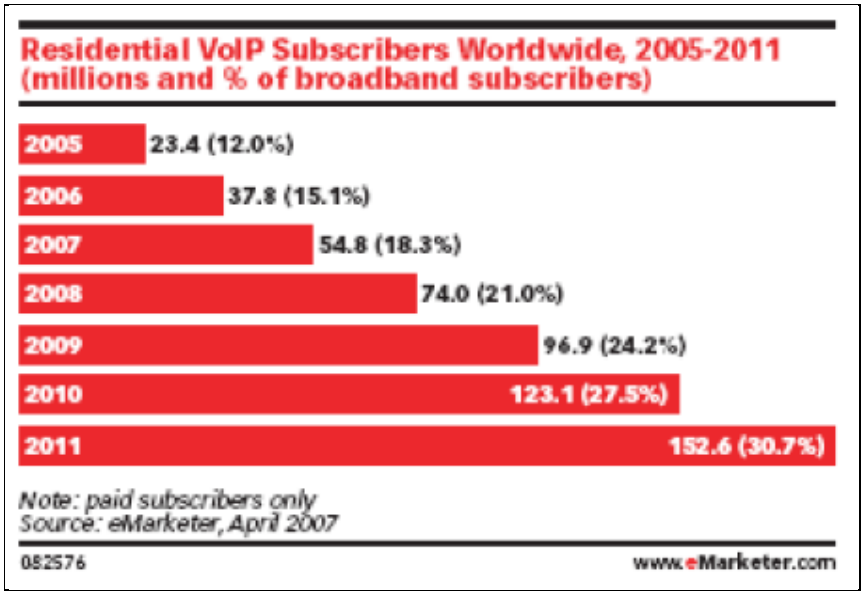

Figure 26: Expected growth of VoIP Subscribers [eMarketer.com 2007]

The ENUM registry / DNS would account for interconnection to the PSTN or VoIP peering using IP networks by publishing the routing details. Currently, a few service providers have implemented I-ENUM and have started offering ENUM services including User ENUM. The Internet user awareness of VoIP in June 2009 is shown in figure 27.

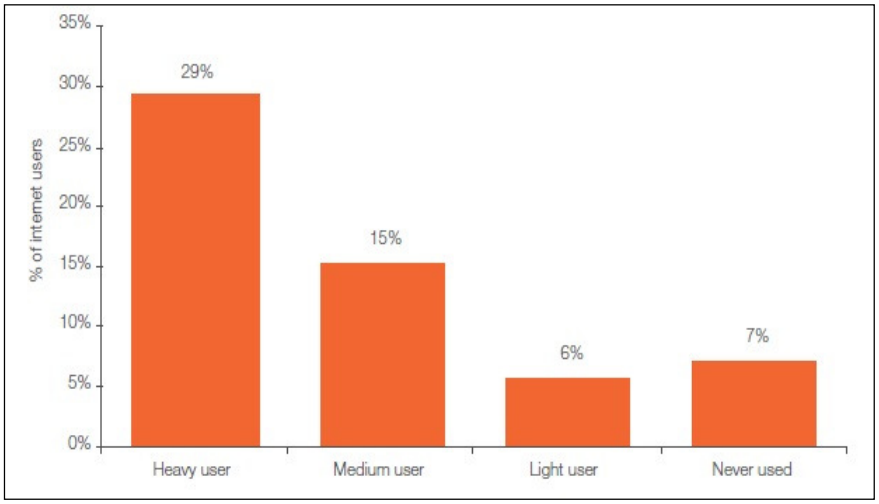

Figure 27: VoIP Usage at Home by Frequency of Internet Use

CSPs are moving away from single service provider model to bundled broadband model, integrating broadband internet access bundled with voice and data services, which cannot be

provided via PSTN. This is beneficial if the CSPs migrate to IP-based networks and hence the need for IP-based interconnection.

VoIP peering over IP networks would be the most cost efficient approach, however there is a time penalty and cost associated with establishing IP peering agreements with all of the other VoIP service providers. In some situations, this time penalty and cost can be reduced where VoIP service providers utilising the same carrier network are provided with a common peering solution by the carrier and get assistance from the carrier with the technical aspects of the peering setup.

The Australian government plans to build a national high speed broadband network that delivers fast internet to 93% of all Australian homes and businesses with speeds of up to 100Mbps. The network would cater for the needs of data, voice and video services using FTTH (Fibre to the Home) technology. This would mean that with faster internet speeds at their disposal, consumers are more likely to embrace the use of VoIP, and with increased bandwidth available throughout the network the VoIP QoS should improve.

VoIP is just one of many services that converged networks will offer, and by no means the most complex. However, it is likely to be the "killer app" that drives widespread adoption of converged network services, and thus reshapes the communications competitive landscape.

VoIP adoption is well underway today; according to Gartner, 95% of all major companies will have deployed or be deploying VoIP by 2010. Also, by 2009, 35% of current consumer PSTN subscribers will rely exclusively on either mobile or VoIP services. IDC predicts that the number of VoIP lines in the US alone will grow from 1.3 million in 2004 to 23 million lines in 2008.

We are reaching the tipping point beyond which VoIP gains widespread, mainstream acceptance. Once it does, the services infrastructure will be in place to provide a number of other services – which themselves will drive wider adoption of VoIP. In the consumer area, music download, IP and mobile TV, push-to-talk, real-time entertainment and gaming applications will ride the coattails of VoIP. Business websites can include a live "chat" function to enhance customer communications and improve sales. The communications landscape several years from now will likely be characterized by connectivity everywhere (home, office, airport, beach) providing a wide range of integrated services (voice, data, music, video, gaming, conferencing, etc.)

But today's VoIP adopters are, for the most part, interested in the immediate and pragmatic benefits of VoIP: scaling their service while reducing telecommunications costs. Although many businesses will take advantage of the new features and capabilities available with VoIP, the cost savings is what drives them to action and brings VoIP in the door (and onto the desk and mobile phone). VoIP service revenues have increased multi-fold and will continue to increase, as shown in Figure 28.

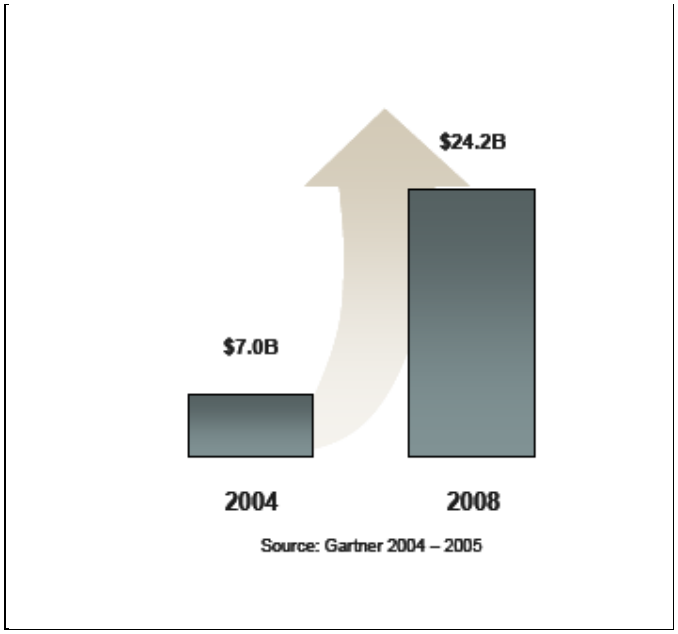

Figure 28: Worldwide VoIP Service Revenues

Providers looking to succeed in this emerging communications market must compete both on cost and function. They need to develop capabilities and a network infrastructure that is both cost-efficient and flexible, minimizing operational costs while supporting the rapid development and deployment of new services. This will require an efficient infrastructure for service delivery.

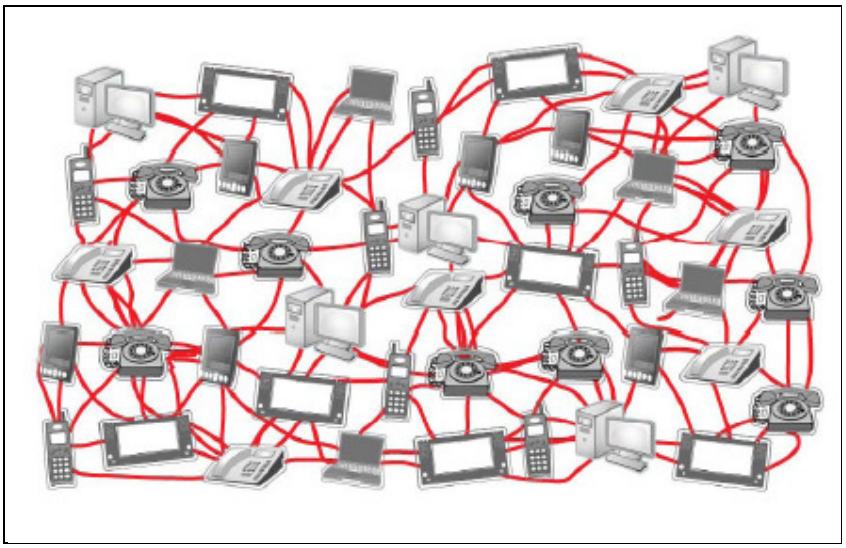

Figure 29: Growing Complexity of IP interconnect

A simple list of peering activity in Australia is given in table 8 below, however this list does not include the Tier 1 ISPs (Telstra, Optus, AAPT and Verison) which peer with each other.

Table 8: List of Australia Peers

Organisation	URL	Comments
AdNAP	www.adnap.net.au	AdNAP is the Adelaide Network Access Point
Ausix	www.ausix.net	The Ausix peering exchange operates in the Global Center data centre in Melbourne
Equinix	www.equinix.com	Commercial data centre operator supporting peering connections between customers
Pipe Networks	www.pipenetworks.com.au	Commercial carrier offering peering exchange services
SAIX	www.saia.asn.au	The South Australian Internet Association admisters SAIX
STIX	www.ix.singtel.com	STIX is apeering point operated by SingTel in Singapore
VIX	www.vix.asn.au	ViX is the Victorian Internet Exchange
WAIX	www.waia.asn.au/waix	The WA Internet Association operates

		WAIX

Requirements for an IP-based Routing Directory

These integrated, IP-based directories must be able to sustain very high standards for performance availability, and to integrate easily in the IMS architecture. Specific requirements include:

- *Provisioning*: The directory need to exchange information with public data sources as well as peering architectures, service bureau partners, and internal systems.

- *Management/High-Availability*: These directories require resilient and reliable operations, real-time availability of data during updates, and quality of service guarantees through fault tolerance and service-level monitoring. These systems will need to be integrated with carriers' Operations Support Systems (OSS) as well.

- *Scalable query performance*: Perhaps the greatest issue, these systems must be able to support large numbers of transactions and very large data volumes. IP routing may require multiple "dips" into these databases and depend on very low latency. Any latency will delay call set-up for VoIP, and other real-time services as well.

When discussing scalability, it is important to note that the call setup latency budget does not "grow" as more data or services are added to the network. The real-time performance expectations remain consistent, no matter how many services you are delivering. Figure 30 illustrates the potential dimension of the scalability issue:

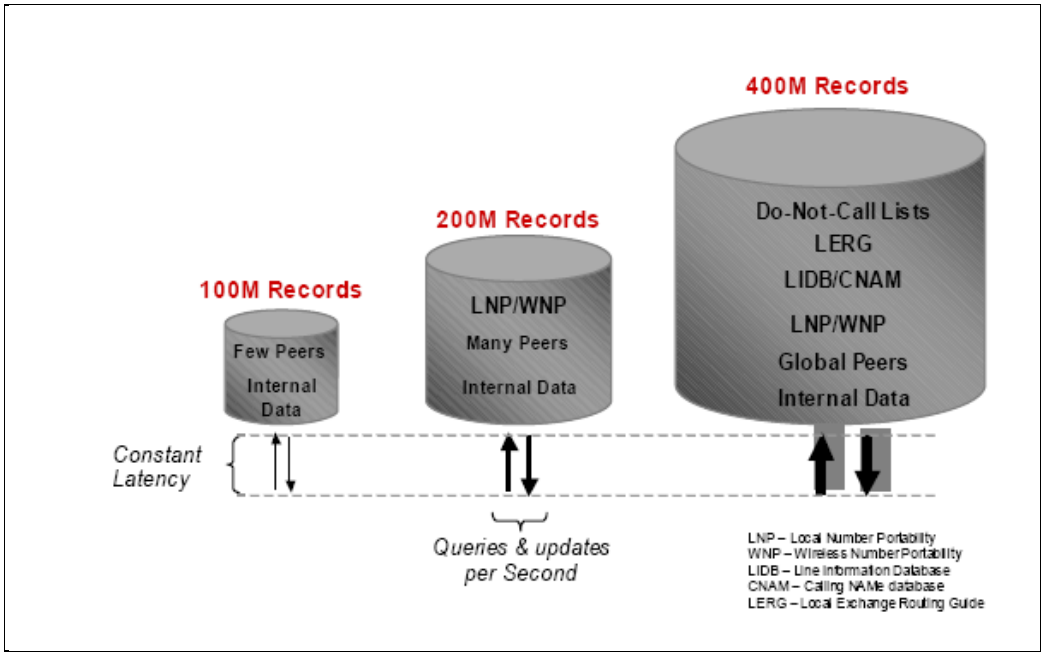

Figure 30: Low Latency, Large Transaction Rate, Huge Capacity

These requirements are evaluated in more detail in the following sections.

Provisioning

Unlike other network elements that must abide by a single carrier's OSS procedures for provisioning, an IP-based routing directory requires open interfaces. It sits at the crossroad of a data flow of multiple networks.

The directory contains the most up-to-date information and maintaining ubiquity throughout the global network by allowing rapid subscriber data updates across multiple nodes in the network.

Achieving this level of ubiquity and speed requires:

- Open, standards-based provisioning interfaces such as SOAP/XML + EPP (Simple Object Access Protocol/eXtensible Mark-up Language and the Extensible Provisioning Protocol)
- Ability to perform bulk and incremental data uploads while answering normal call set-up queries.
- Direct peering with partners supporting concurrent data updates, sometimes for the same record.

- Interfaces with service bureaus that provide standardized subscriber data sources such as Local Number Portability and Do-Not-Call privacy registries.

Management/High-Availability

The famous five nines (i.e., 99.999% availability) have been the benchmark for any service or technology that attempts to serve the needs of communication providers. The IP protocol is showing significant resiliency and availability when used as a protocol for the transport level of an IMS framework. As the control and application service layers are unified, redundancy and availability are key concerns.

One aspect of ensuring availability is securing systems from intruders, worms, viruses, or attacks such as Denial of Service (DOS) attacks, which have been common with open source DNS solutions.

In addition, this routing directory must be adaptable to network operations practices. For example, carriers may choose centralized or distributed directory architectures to adhere to internal operations "jurisdictions."

Finally, solutions must integrate in network and element management systems to ensure the highest possible fault tolerance and quality of service. For example, an Element Management System (EMS) reports alarms and faults to administrators, permitting them to pre-empt any anomalies that may surface before server availability is compromised. An EMS helps maintain Quality of Service by minimizing downtime and accelerating recovery by keeping alarms highly visible within a Network Operations Center.

Scalability & Performance

Scalable performance is the most obvious requirement of a directory server in this function. When aggregating data from multiple peering partners and service bureaus, the data volumes rapidly reach hundreds of millions of records. Under heavy transaction load, the directory must maintain a steady rate of transactions at a constant low latency for queries, enabling carriers to provide a guaranteed Quality of Service overall. Most importantly, a high performance directory server gives network architectures more room to allocate for the operations performed by other network elements during call set-up.

Table 9 illustrates some of the stringent, real-world performance and scalability requirements of different service providers. Using open source DNS software designed for much earlier Internet traffic patterns obviously will not work.

Table 9: Performance and Scalability Requirements of Service providers

Carrier Type (Subscribers)	**Fixed Line Carrier (8M Subs)**	**Cable Operator (10M Subs)**	**Systems Integrator (5M Subs)**
Queries/Seconds	20,000	30,000	15,000
Updates/Seconds	30	300	300
Maximum latency tolerated	5 milliseconds	3 milliseconds	2 milliseconds
Total Records	100 Million	200 Million	400 Million

5.3 Proposed Steps to Move to a VoIP IP Peered Solution

The evolution from the existing network, to the network that uses I-ENUM can be broadly divided into three steps.

A) Use of Private I-ENUM within a service provider's network – As shown in figure 31, the VoIP service providers would start using I-ENUM for VoIP call routing within their own network. The VoIP service providers set up their own DNS infrastructure and I-ENUM registry and populate the registry with client information. The database would consist of NAPTR RR records with information about internal destination points for end-users or PSTN routing information.

An increasing number of VoIP service providers are now offering an added incentive for a shift to a VoIP solution. VoIP-to-VoIP calls between consumers registered to the same VoIP service provider are being offered at low cost or no cost.

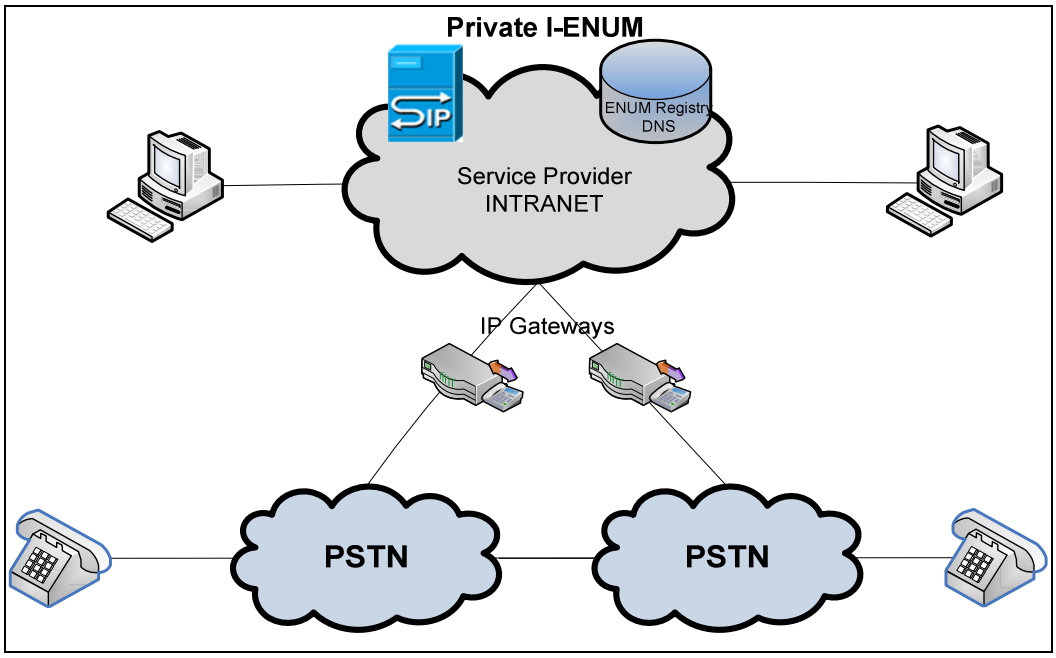

Figure 31: Private I-ENUM with SP's Network

With CSPs migrating to IP-based networks to offer better quality VoIP services and the existence of PSTN, makes interconnection between PSTN and IP networks imperative. This is where I-ENUM would be the best bridging solution. The ENUM registry would hold the details of PSTN/IP gateways, thereby effectively routing calls within the SPs cloud and to other SPs either through PSTN or IP gateways. This would enable the SP to offer VoIP-VoIP calls at low or no cost for calls established and terminated within their cloud.

B) Use of Private I-ENUM with IP based Interconnection - Using I-ENUM within their networks, CSPs can interconnect with other VoIP service providers over IP networks using border elements, in doing so eliminating the need for PSTN interconnection and the costs associated with it. However, if there are no IP-based points of interconnection, calls would still be routed to PSTN through PSTN/IP gateways. Each service provider has their own DNS and act as Registry and would have all the IP-based routing information, internal destination points and PSTN routing information. Private I-ENUM could be used to interconnect multiple service providers as shown in figure 32.

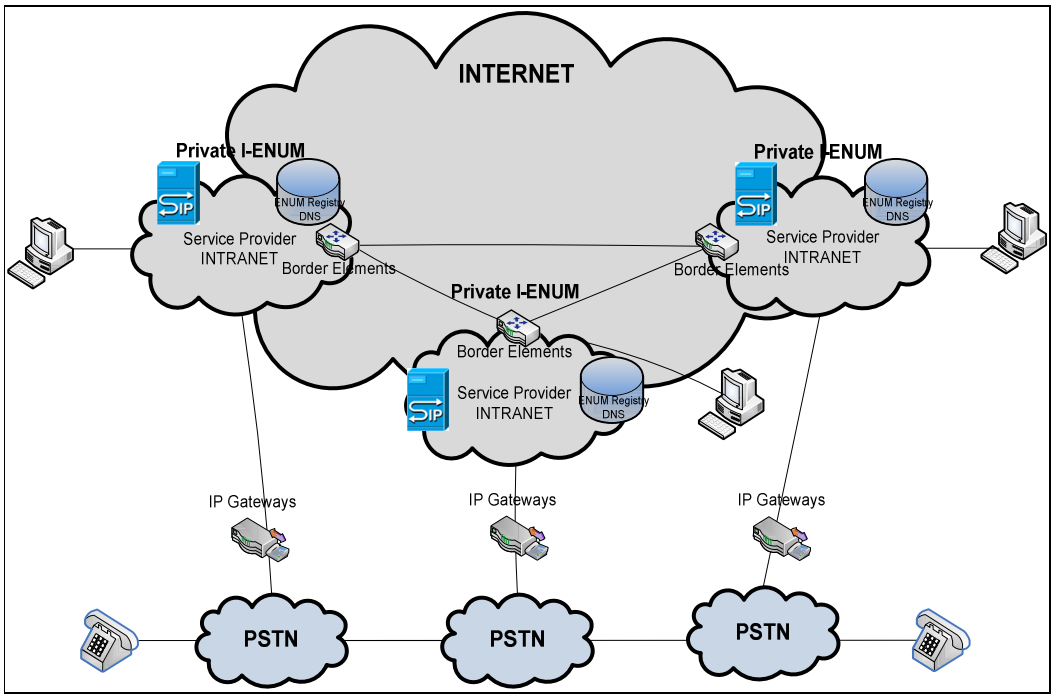

Figure 32: Private I-ENUM used by Multiple Service Providers

A number of VoIP service providers showed interest during the Australia ENUM Trial to gain access to an Australian I-ENUM implementation. Feedback during the ENUM trial and the subsequent I-ENUM trial highlighted that a number of private I-ENUM implementations already exist and that service providers were keen to work towards a unified I-ENUM hierarchy.

C) Global or Common Private I-ENUM – Single or a common shared I-ENUM registry / DNS on the Internet would permit and facilitate only participating VoIP SPs to store routing information required for interconnection. As shown in figure 33, apart from the connections to the PSTN and other VoIP service providers, each VoIP service provider's intranet would have bilateral IP connections via border elements to the shared extranet. DNS within the VoIP service provider is still used to maintain the information required to route calls within their own network.

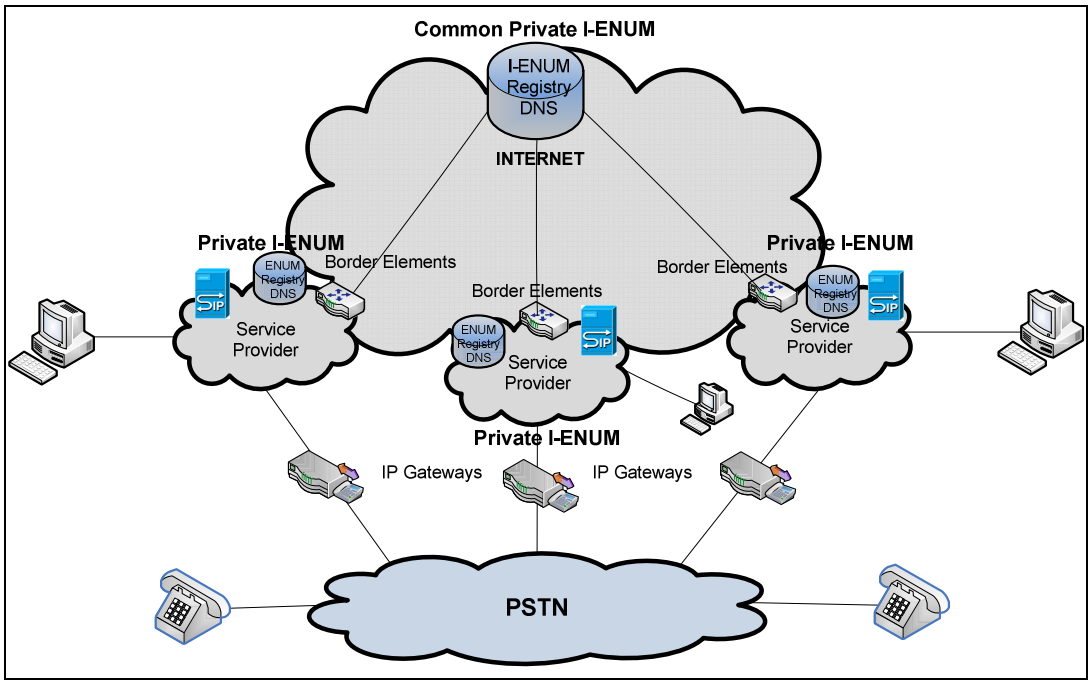

Figure 33: Shared Private I-ENUM structure in Australia

The step by step evolutionary model presented in this paper is recommended as it is unlikely that the current competitive market will opt to move to an Australian I-ENUM implementation in a single step.

If and when, embraced globally, User ENUM and I-ENUM utilising public and private DNS could be implemented using several approaches, however it is anticipated that this transition will take more than 10 years to occur.

5.4 Future of VoIP: VoLGA

With mobile internet access becoming increasingly dominant one could wonder if VoIP could continue to be dominant, with packet switched wireless networks based on circuit switched radio and core network infrastructure. However, VoLGA seems to be the solution with the concept of connecting the already existing mobile switching centres to LTE network via a gateway. This technology is currently being deployed by T-Mobile in the US and Orange in France.

5.4.1 Basic Network Setup for VoLGA

VoLGA re-uses the concepts of GAN by replacing Wi-Fi with LTE. VoLGA can be implemented using the already existing GAN network infrastructure with the GAN-based dual-mode phones (GSM networks and Wi-Fi). The only requirement is for software enhancements to the already existing circuit to packet gateways.

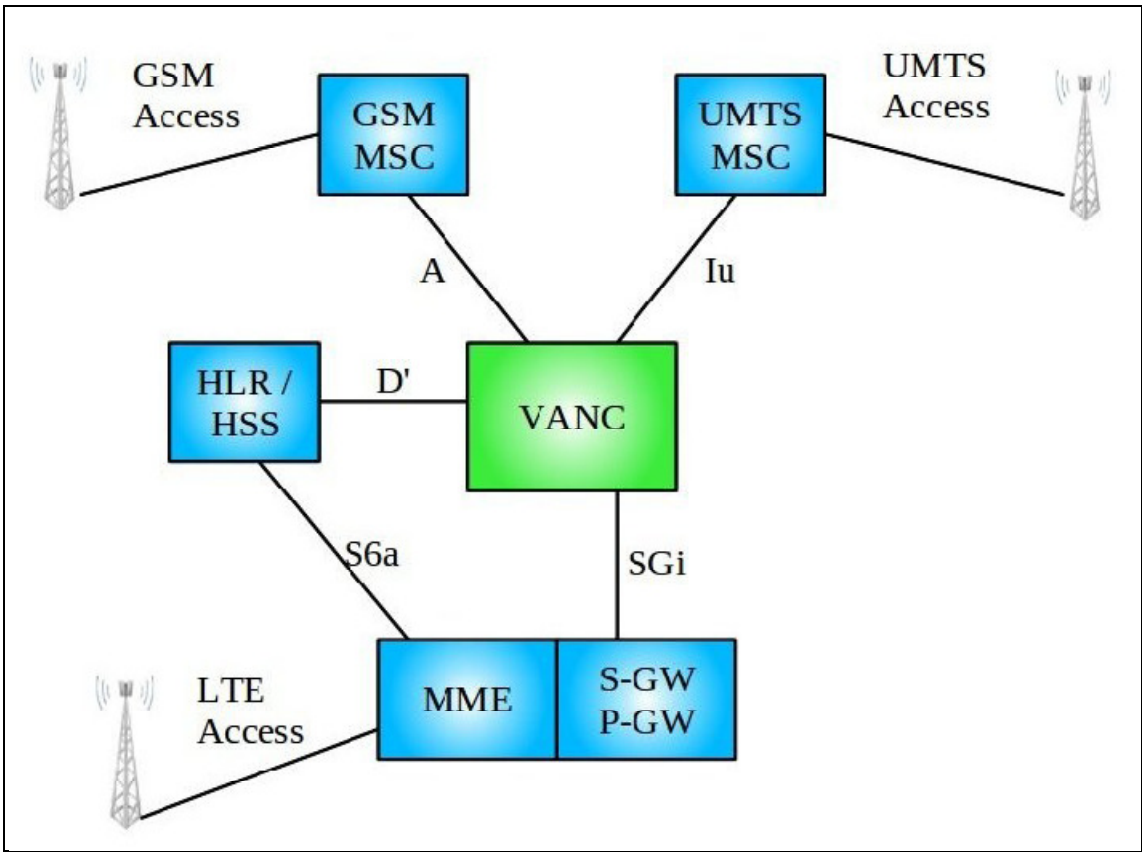

Figure 34: Basic Network Setup of VoLGA

VoLGA Access Network Controller (VANC), as shown in figure 34, is the only new element that needs to be introduced, the rest of the network elements and interfaces between them already exist and can be reused.

VANC looks like any IP based external node of a LTE network. IP packets exchanged between a wireless device and the VANC are transparently forwarded through the Evolved Packet Core (EPC) network. VANC and the Packet Data Network Gateway (P-GW) are connected via SGi interface which transports signalling and voice packets.

VANC looks like a GSM Base Station Controller (BSC) to a GSM MSC and like a UMTS Radio Network Controller (RNC) to a UMTS MSC of a circuit switched network. The A-interface connects the VANC to a GSM Mobile Switching Center (MSC) and the Iu-interface connects the VANC to the UMTS MSC. The interfaces are used without any enhancements and the MSCs require no change to support voice.

5.4.2 Call Flow

When a mobile device is switched on and detects an LTE network it registers with the Mobility Management Entity (MME) over the LTE access network. The MME uses the S6a interface to the Home Location Register / Home Subscriber Server (HLR/HSS) to retrieve the subscriber data to authenticate and manage the user.

The mobile establishes a connection to the VANC after successfully registering with the LTE network. To establish an IP connection, the IP address of the VANC is to be known. This can be done either by pre-configuring the details in the mobile device or by querying a DHCP server in the network established for VoLGA. A secure IPSec tunnel is established by the mobile device over the LTE radio network through the LTE core network and over the SGi interface. During this process, the user's details stored in the HLR/HSS are authenticated by the VANC over the D`-interface.

The mobile device then registers to the MSC through the IPSec tunnel and the VANC. The Direct Transfer Application Part (DTAP), an already known protocol for GSM and UMTS, is used for this purpose. The VANC adds information such as cell-id (2G) or service area identifier (3G) to the initial registration message as defined in the GSM and UMTS standards and all messages are tunnelled transparently between the mobile device and the involved MSC network components.

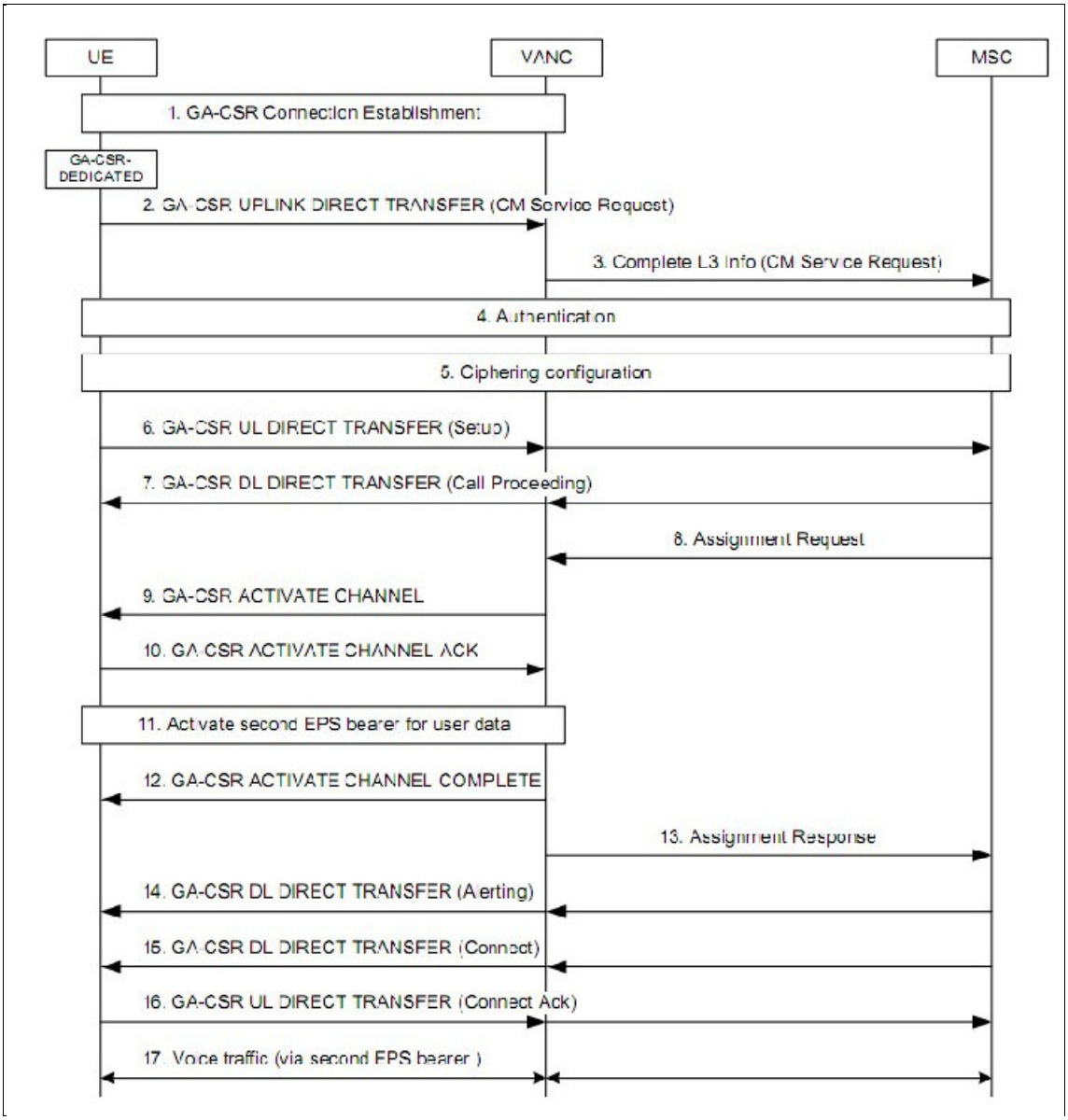

Figure 35: Call flow for a mobile originated voice call

The signalling messages exchanged between the user equipment, VANC and MSC are detailed in figure 35.

5.4.3 Advantages and Disadvantages

Although there are a few alternative for VoIP over LTE, VoLGA is considered to be more apt as there is no need for updating any existing network components, except developing VANC, making it easy to introduce the technology to the market. VoLGA also enables the

use of other circuit switched services like SMS messaging, without any additional development. Already available GAN-based dual-mode mobile devices could be re-used with changes to the software for handling handover. VoLGA also enables global roaming.

However, VoLGA is not fully standardised as the stage 3 specification is yet to be finalised. This along with the fact that VoLGA is not a 3GPP work item is considered to be the main concerns.

6 Conclusion

The research objectives and scope were to investigate I-ENUM as a potential system that may assist with the growth of VoIP as a telephony solution in Australia. The research aims were to identify: (1) an appropriate *s*tructure for implementing I-ENUM in Australia; (2) the motivation for an open universal VoIP peering solution; and (3) the steps required to move to a VoIP IP peered solution. An important outcome of the literature review was to identify the shift that is occurring from the PSTN to an IP based VoIP telephony solution and the lack of an approach for an IP network wide directory. The literature review highlighted the existing use of the PSTN to provide a peering mechanism for VoIP calls, even when the call is VoIP to VoIP. The research outcomes were compared with outcomes identified in the literature and these outcomes included steps being taken in other countries to implement ENUM based solutions. The research included participation in the AEDG I-ENUM Working Group Trial and preparation of a report that was presented to the AEDG and the results consolidated into the ACMA report 2008-09. The results of the I-ENUM Working Group Trial have been presented and analysed to consider how the trial results would scale for an Australia wide directory solution. The framework and model for an Australian I-ENUM implementation have been presented and discussed with the analysis demonstrating that the use of I-ENUM would be beneficial for Australian consumers and business principally through call price reduction. The scope and objectives of this research have been successfully achieved.
The research outcomes have been submitted for publication at the ATNAC 2010 conference (IEEE sponsored), which is to be held in Auckland, New Zealand during December 2010. The conference paper is provided in Appendix F.

The research focused on an analysis of the status quo for telephony services in Australia and provision of VoIP as part of the telephony offering. The research included the development of a framework and steps for a migration from the status quo to the Australian utilisation of I-ENUM as a network wide directory. The results provided in this thesis include:

- Analysis and justification for the motivation for an open universal VoIP peering solution.

- A framework for an industry based solution for an I-ENUM system that provides VoIP service providers with a peering solution that satisfies Australian privacy and security requirements.

- Analysis of the status quo and identification of three steps that may be taken to move to an I-ENUM based VoIP IP based peering solution available for VoIP service provider use.

- A financial analysis of the costs and savings for each of the three steps and a projection of the VoIP call costs moving forward.

- A structure for an industry based company or wholesale network provider such as the proposed NBN that provides a private I-ENUM solution to VoIP service providers within Australia and approved international VoIP service providers.

- Analysis of Australian integration with an international I-ENUM system.

The concept of integrating VoIP with existing telephony services has been evolving for some time and the process may moved forward with some urgency as more customers move to VoIP and competition amongst VoIP service providers increases. The current move towards VoIP as a universal telephony solution for future generations is well underway. Mobile telephone networks will soon migrate to a 4G mobile wireless cellular network solution that will include VoIP as the principal telephony solution and thereby removing the need to support separate digital telephony channels. The research identified that mobile devices are currently being identified by the use of IMSI and the information contained on the registered SIM cards used with mobile devices. However, for IP devices connected to the digital network that may be used for VoIP there are no IMSI, SIM card or similar hardware identifiers available.

The research demonstrated that I-ENUM is a flexible solution that may be used to identify fixed and mobile VoIP IP based devices and existing PSTN devices, thereby providing a single system that may be used to support telephony moving forward.

The research considered the legislated Australian security and privacy requirements that would apply to any system to be used to identify consumer devices on the digital network.

The research outcome was that a private I-ENUM system that was made available only to approved VoIP service providers locally and internationally would satisfy the legislated Australian security and privacy requirements.

In summary, this research highlights that private I-ENUM is a satisfactory solution that may be used by VoIP service providers to connect calls utilising IP based networks and to minimise the cost of interconnection. The proposed private I-ENUM solution provides information security and privacy, permits LNP between VoIP service providers and provides the opportunity for services and applications other than VoIP to be supported on fixed and mobile IP based devices.

7 Future Work

A definite future research topic would be to design and simulate a suitable and widely accepted solution for a global I-ENUM implementation. As more countries move to utilise I-ENUM as a network wide directory locally there will be an increasing need to integrate the information and private trees used within the private DNS.

A proposed global approach is shown in figure 36, where the public DNS is used as the common shared directory. This would permit public domain names and country trees that can be used to provide routing information for VoIP services and also as a directory for other IP based services.

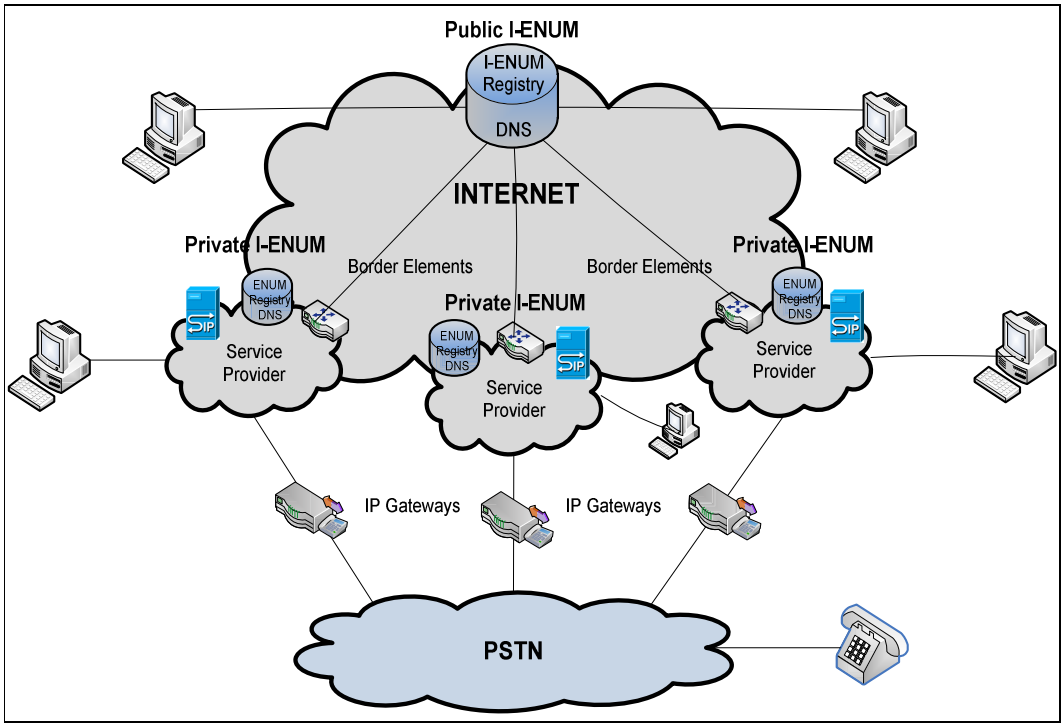

Figure 36: I-ENUM in Public DNS (Option 1)

An alternative to the proposed global approach for an I-ENUM implementation utilising public DNS is shown in figure 37. Consider, for example, Australia and New Zealand using I-ENUM with a private DNS system, forming a regional private I-ENUM island. The proposal is to link the regional private I-ENUM DNS to a single common global public I-

ENUM DNS that contains border gateway information for domains or domain trees. Any user could query the public DNS, which would have routing information for the shared private I-ENUM extranet border gateways.

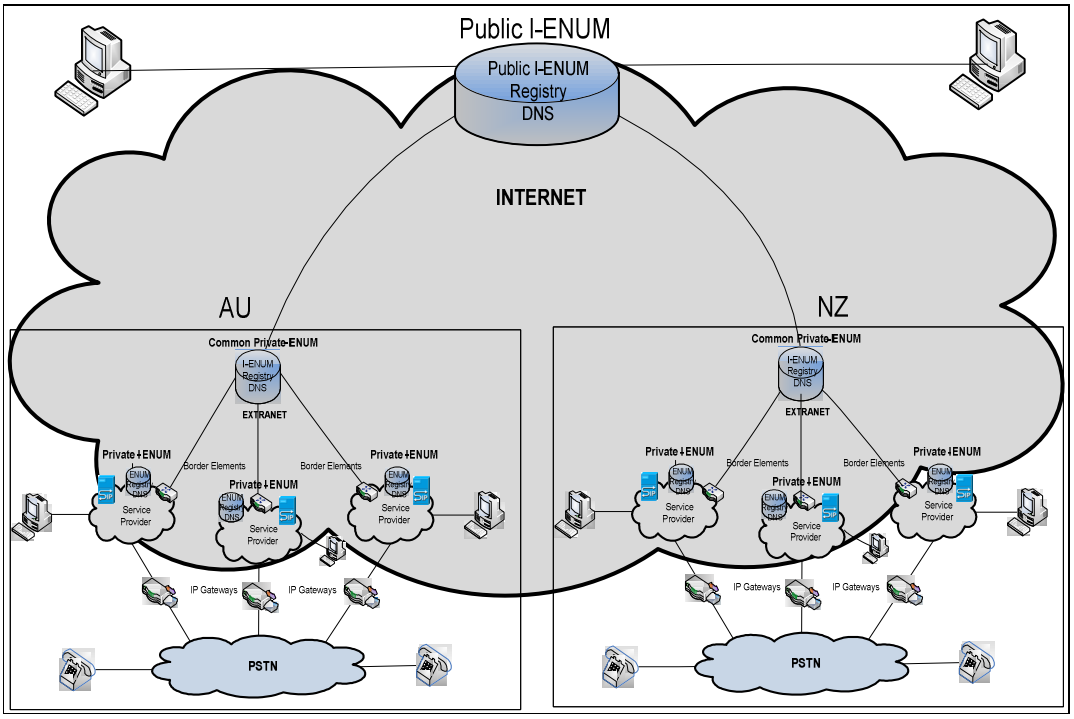

Figure 37: I-ENUM in Public DNS (Option 2)

Before finalising a global I-ENUM implementation solution more research is needed into the management and control of a global I-ENUM system and how the information that is stored within the global I-ENUM system may be governed and protected from unwarranted access so as to ensure national security and privacy legislation may be achieved.

Apart from the most suitable design, other future research topics may include:

Performance and scalability of I-ENUM implementations

A new protocol could be developed or an existing protocol could be modified to replace EPP for communication between the registrar and the registry

Administration, governance and accountability in conjunction with ensuring security and privacy is maintained

8 References

.aero 2007, '.aero EPP Registrar Acceptance Criteria, Version 1.4', [Online] Available at: http://www.nic.aero/documents/Abridged_aero_ote_criteria_v1.4_29Aug2007.pdf

.mobi 2006, 'Extensible Provisioning Protocol (EPP) v1.0 – Registrar Acceptance Criteria', Sunrise OT&E Test, [Online] Available at: http://mtld.mobi/files/mobi_epp_rfc_ote_criteria_sunrise_v1.3_final.pdf

.org, The Public Interest Registry 2006, 'Extensible Provisioning Protocol (EPP) v1.0, Drop- Zone Test Cases', [Online] Available at: http://www.pir.org/PDFs/ORG_Drop_Zone_OTE_Acceptance_Criteria.pdf

ACMA 2001, 'Implementation of the ENUM Protocol in France', [Online] Available at: http://www.acma.gov.au/WEB/STANDARD/1001/pc=PC_2325

ACMA, 'Proposal for ASTAP Work Program', [Online] Available at: http://www.acma.gov.au/WEB/STANDARD/1001/pc=PC_2315

Afilias 2006, 'Extensible Provisioning Protocol (EPP) v1.0 – Registrar Acceptance Criteria', [Online] Available at: http://www.info.info/webfm_send/20

Australian ENUM Discussion Group 2010, *Australian ENUM Discussion Group (AEDG),* [Online] Available at: http://www.acma.gov.au/WEB/STANDARD/pc=PC_2319

Austrian ENUM Trial Platform, 'Austrian ENUM Trial Definitions and Abbreviations Document Version: 1.0', [Online] Available at: enum.nic.at/documents/AETP/Permanent_Documents/.../0006-Austrian_ENUM_Trial_Definitions_and_Abbreviations_1_0.doc

Berners-Lee, T., Fielding, R. & Masinter, L. 2005, 'Uniform Resource Identifier (URI): Generic Syntax', RFC 3986, [Online] Available at: http://tools.ietf.org/html/rfc3986

CAIW Holding 2007, 'Dutch Cable SIP Exchange the benefits', [Online] Available at: http://www.denic.de/media/pdf/enum/veranstaltungen/Sikko_de_Graaf_20070227.pdf

Cisco Systems Inc. 2008, 'Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions', [Online] Available at: http://www.cisco.com/en/US/docs/voice_ip_comm/bts/5.0/feature/description/featdesc.html

Comvergence Pty Ltd, *'Comvergence'* [Online] Available at: http://www.comvergence.com.au/index.htm

ENUM China, Carrier ENUM, [Online] Available at: http://www.enum.cn/en/demo/carrier.php

ENUM LLC 2007, 'US End-user ENUM Trial – Final Report', [Online] Available at: http://enumllc.com/USEUTrialRpt.pdf

ENUM.AT, 'ENUM and Voice over IP (VoIP)', [Online] Available at: http://www.enum.at/ENUM-and-VoIP.375.0.html?&L=9

Faltstrom, P. 2000, 'E.164 Number and DNS', RFC 2916, [Online] Available at: http://tools.ietf.org/html/rfc2916

Faltstrom, P., Mealling, M. 2004, 'The E.164 To Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)', RFC 3761, [Online] Available at: http://tools.ietf.org/html/rfc3761

Foster, M., McGarry, T. & Yu, J. 2003, 'Number Portability in the Global Switched Telephone Network (GSTN): An Overview', RFC 3482, [Online] Available at: http://tools.ietf.org/html/rfc3482

Gilder, George (2000), Telecosm : How infinite bandwidth will revolutionize our world, London : The Free Press

Grayson, Ian 2007, 'VoIP Guide: Voice over IP in Australia', CNET Australia, [Online] Available at: http://www.cnet.com.au/broadband/voip/0,239035972,240056481,00.htm

Haag, Den 2007, 'Bridging the VoIP Islands with Federated Peering and ENUM', XConnect, [Online] Available at: http://isoc.nl/activ/20071011-SIPSIG-EliKatz.pdf

Haberler, M., Lendl, O. & Stastny, R. 2007, 'Combined User and Infrastructure ENUM in the e164.arpa Tree draft-ietf-enum-combined-08', IETF, Combined User and Infrastructure ENUM Internet draft, [Online] Available at: http://tools.ietf.org/html/draft-ietf-enum-combined-08

Heap, Steve 2007, 'Simplifying the Exchange of Digital Communications in a Converging World', Arbinet – thexchange, Inc., [Online] Available at: http://isoc.nl/activ/20071011-SteveHeap.pdf

Henry Sinnreich, Alan B. Johnston 2006, Internet Communications Using SIP, Wiley Publishing, Inc., Indianapolis

Hoeneisen, B. 2007, 'ENUM Validation Information Mapping for the Extensible Provisioning Protocol', RFC 5076, [Online] Available at: http://tools.ietf.org/html/rfc5076

Hollenbeck, S. 2002, 'Generic Registry-Registrar Protocol Requirements', RFC 3375, [Online] Available at: http://tools.ietf.org/html/rfc3375

Hollenbeck, S. 2004, 'Extensible Provisioning Protocol (EPP) Contact Mapping', RFC 3733, [Online] Available at: http://tools.ietf.org/html/rfc3733

Hollenbeck, S. 2004, 'Extensible Provisioning Protocol (EPP) Domain Name Mapping', RFC 3731, [Online] Available at: http://tools.ietf.org/html/rfc3731

Hollenbeck, S. 2004, 'Extensible Provisioning Protocol (EPP) Host Mapping', RFC 3732, [Online] Available at: http://tools.ietf.org/html/rfc3732

Hollenbeck, S. 2004, 'Extensible Provisioning Protocol (EPP) Transport Over TCP', RFC 3734, [Online] Available at: http://tools.ietf.org/html/rfc3734

Hollenbeck, S. 2004, 'Extensible Provisioning Protocol (EPP)', RFC 3730, [Online] Available at: http://tools.ietf.org/html/rfc3730

Huston, Geoff 2007, 'Infrastructure ENUM', [Online] Available at: http://www.circleid.com/posts/infrastructure_enum/

Instra Corporation, 'ENUM Trial Information', [Online] Available at: http://www.enumregistry.com/enum/trial.htm

International Telecommunications Union, 'ENUM', [Online] Available at: http://www.itu.int/osg/spu/enum/

Internet Society 2005, 'The ISP Column', [Online] Available at: http://ispcolumn.isoc.org/2005-01/interconns.pdf

Intertex Data 2004, 'SIP Switch', [Online] Available at: http://www.sipswitch.net/default.asp?pg=7

Jonathan Davidson, James Peters, Manoj Bhatia, Satish Kalidindi, Sudipto Mukherjee 2007, Voice over IP Fundamentals, Cisco Press, Indianapolis

Lind, S., Pfautz, P. 2007, 'Infrastructure ENUM Requirements', RFC 5067, [Online] Available at: http://tools.ietf.org/html/rfc5067

Maris, Lennart & Nooren, Pieter 2007, 'Open and Closed Models for Infrastructure ENUM in the Netherlands', RIPE 55 ENUM Working Group, [Online] Available at: http://www.ripe.net/ripe/meetings/ripe-55/presentations/nooren-open-closed-models-enum.pdf

McGarry, T. 2004, 'ENUM Primer', Neustar, [Online] Available at: www.fcc.gov/realaudio/presentations/2004/110404/McGarryTom.ppt

Mealling, M. 2002, 'Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS ', RFC 3401, [Online] Available at: http://tools.ietf.org/html/rfc3401

Mealling, M., Daniel, R. 2000, 'The Naming Authority Pointer (NAPTR) DNS Resource Record', RFC 2915, [Online] Available at: http://tools.ietf.org/html/rfc2915

My Telecom Holdings Pty Ltd, *'My Telecom'*, [Online] Available at: http://www.mytelecom.com.au/index.htm

Mulbery, Karen 2007, 'ENUM', Inter-American Telecommunication Commission, [Online] Available at: http://www.citel.oas.org/newsletter/2007/agosto/enum_i.asp

Nominum 2006, 'Scalable VoIP Peering Solution for Converged Networks', CA, [Online] Available at: http://www.nominum.com/info_center/voip_peering/index.php

P. Faltstrom, M. Mealling: RFC 3761 "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", Date: April 2004

Paul Albitz, Cricket Liu 2001, DNS and Bind, O'Reilly & Associates Inc., CA

Pfautz, P. 2004, 'Infrastructure ENUM and Privacy', ENUM Forum Working Group, [Online] Available at: www.**enum**f.org/documents/gen/2005/GEN0127R0_Pfautz_Infra_**ENUM**_Privacy.doc

PIPE Networks Ltd, *'PIPE Networks'*, [Online] Available at: http://www.pipenetworks.com/

Ranalli, J. Douglas 2007, 'Next Generation Addressing & Routing Infrastructure', NetNumber, Inc., [Online] Available at: http://isoc.nl/activ/20071011-DougRanalli.pdf

Richard Stastny 2006, 'Infrastructure ENUM – The Driving Force', ENUM and VoIP Peering Forum, [Online] Available at: http://ENUM.nic.at/documents/AETP/Presentations/Austria/0072-2006-06_Marcusevans_ENUM_RStastny_v1.ppt

RIPE NCC, 'How to Update a Delegation in the ENUM (e.164.arpa) Domain', [Online] Available at: http://www.ripe.net/enum/update-delegation.html

Risley, Chris 2006, 'Taking Aim at 8 Myths about ENUM', [Online] Available at:
Rossi, Sandra 2007, 'ACMA Report identifies size of VoP market in Australia', ComputerWorld, [Online] Available at: http://www.computerworld.com.au/index.php/id;891100978;pp;1

Sallet, J. 2003, 'Just how open must an open network be for an open network to be labeled "open"?', First Monday, [Online] Available at: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1037/958

Sauter, Martin 2009, 'VoLGA – A Whitepaper', [Online] Available at: http://www.wirelessmoves.com

SGNIC, 'ENUM.EPP API User Guide', [Online] Available at: www.**sgnic**.sg/sub_enum/ENUM.EPP_**API_User_Guide**.doc

Shaw, Robert 2001, 'ENUM Implementation', ITU, ICANN Government Advisory Committee, [Online] Available at: www.itu.int/osg/spu/**enum**/GACjune1201/gac-june-2-2001-1.PPT

Stastny, Richard 2006, 'Infrastructure ENUM – The Current Driving Force', ENUM and VoIP Peering Forum, OFEG, [Online] Available at: http://enum.nic.at/documents/AETP/Presentations/Austria/0072-2006-06_Marcusevans_ENUM_RStastny_v1.ppt

Stastny, Richard 2006, 'IP Interconnect and Infrastructure ENUM and the Relevance on NGNs', AT-TK ENUM, OFEG, [Online] Available at: http://enum.nic.at/documents/AETP/Presentations/Austria/0067-2006-02_AKTK_Interconnect_and_ENUM_RStastny_v1.ppt

Stastny, Richard 2007, 'ENUM – Where are we at?', Internet Society Netherlands, Neustar, [Online] Available at: http://isoc.nl/activ/20071011-RichardShockey.pdf

Stastny, Richard 2007, 'ENUM and VoIP Peering, Introduction and Overview', OFEG, [Online] Available at: http://enum.nic.at/documents/AETP/Presentations/Austria/0079-2007-06_MarcusEvans_Berlin_Stastny_v2.ppt

Stastny, Richard 2007, 'NAR ENUM and Voice Peering (IP Interconnection)', OFEG, [Online] Available at: http://enum.nic.at/documents/AETP/Presentations/Austria/0078-2007-04%20OeFEG%20NAR%20v1.ppt

Steven D. Lind, Penn Pfautz 2005, 'Requirements for the Implementation of Infrastructure ENUM in the United States', ENUM Forum Working Group, [Online] Available at: http://www.ENUMf.org/documents/6004_0_0.doc

Stratix Consulting Group 2003, 'Voice-over-packet Technology', OPTA, [Online] Available at:
Switch 2006, 'ENUM Information Day attracts more than 80 participants from Switzerland and abroad', [Online] Available at: http://www.switch.ch/about/news/2006/?id=118

TeleGeography 2008, 'TeleGeography Report Executive Summary', [Online] Available at: http://www.telegeography.com/products/tg/index.php
Tripos IT 2005, 'Voice Over Internet Protocol', [Online] Available at: http://www.tripos.com.au/newsletters/newsletter_March05.html

Wikipedia, ''Telephone Number Mapping', [Online] Available at: http://en.wikipedia.org/wiki/Telephone_Number_Mapping

Appendix A

AEDG Infrastructure ENUM Working Group

Report on Infrastructure ENUM Trial
28 April 2009

Dr Mark Gregory and Ananda Jammulamadaka, RMIT University

Introduction

The Australian ENUM Discussion Group (AEDG) formed a working group in April 2007 with terms of reference to investigate and report on the following:

1. Existing implementations of Infrastructure ENUM (I-ENUM) and the different models that have been used.
2. The extent to which I-ENUM has undergone standardization within the Internet Engineering Task Force (IETF) and other standardization bodies.
3. Current research activities into I-ENUM.
4. Whether an Australian implementation of I-ENUM is feasible.

Duration

The I-ENUM Working Group (IEWG) conducted a trial from 1 September to 30 November 2008.

Participants

The IEWG participants are listed in Appendix B.

Support

The Australian I-ENUM trial utilized the Austrian ENUM Trial Platform (enum.nic.at) made available by the University of Austria. Mark Hofstetter from the University of Austria

assisted with setup and configuration of the Austrian ENUM software for the Australian I-ENUM trial.

Description

The IEWG trial included the use of the Austrian ENUM Trial Platform that includes an Oracle database and DNS server running on Redhat Enterprise Linux Server.

Four organizations were registered onto the system and two companies, MyTelecom Holdings and Comvergence setup their VoIP gateways to utilize the system to permit an end-to-end call test.

VoIP providers register telephone numbers and the matching IP gateway on their network into the Oracle database and an automated process updates the DNS server NAPTR resource records. Examples of the EPP scripts that may be used to add, edit and delete numbers and NAPTR resource records from the database may be found in the Austrian Trial Platform documentation[1i].

An example DNS lookup from the ENUM DNS using dig[2] is shown below. This DNS session shows indicative lookup times and provides an example of the information received by a VoIP gateway after doing an ENUM lookup.

DNS lookup

dig result for **'9.2.4.4.4.2.9.9.3.1.6.auenum.com.au.'** from server '131.170.68.108' [dig @'131.170.68.108' '9.2.4.4.4.2.9.9.3.1.6.auenum.com.au.' 'ANY']

DNS response

```
; <<>> DiG 9.3.2 <<>> @131.170.68.108 9.2.4.4.4.2.9.9.3.1.6.auenum.com.au. ANY
 ; (1 server found)
 ;; global options:  printcmd
 ;; Got answer:
 ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15153
```

[1] ENUM registry system specification version: 1.2 http://www.enum.at/typo3conf/ext/nf_downloads/pi1/passdownload.php?downloaddata=25

[2] http://en.wikipedia.org/wiki/Domain_Information_Groper

```
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;9.2.4.4.4.2.9.9.3.1.6.auenum.com.au. IN          ANY

;; ANSWER SECTION:
9.2.4.4.4.2.9.9.3.1.6.auenum.com.au. 7200 IN NAPTR 10 105 "u" "E2U+sip"
"!^.*$!sip:61399244429@203.153.192.10!" .

;; AUTHORITY SECTION:
1.6.auenum.com.au. 1800     IN      NS      localhost.

;; Query time: 349 msec
;; SERVER: 131.170.68.108#53(131.170.68.108)
;; WHEN: Tue Feb 10 02:59:37 2009
;; MSG SIZE  rcvd: 141
```

An outgoing call from a registered VoIP provider is routed to the outgoing IP gateway and an ENUM lookup is carried out on the I-ENUM DNS. If a NAPTR record is returned that identifies an upstream voice gateway for the call to be routed to, then the call may be routed using IP. If a NAPTR record is not returned from the ENUM DNS lookup then the outgoing call may be routed to the PSTN at the outgoing gateway.

Therefore the VoIP provider has the option of routing calls using IP or directly to the PSTN at the outgoing gateway.

This scenario is shown in Figure 1.

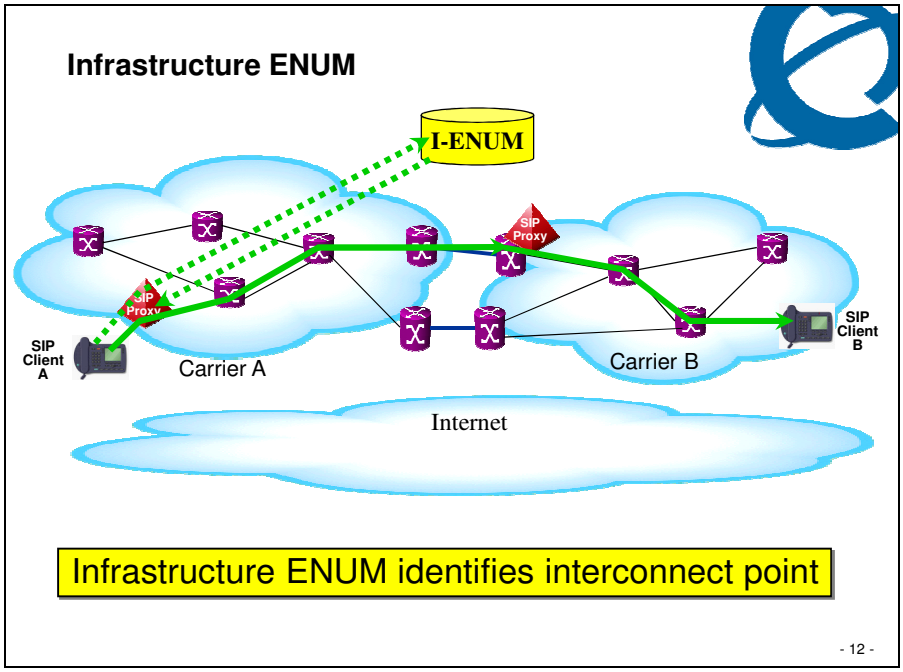

Figure 1: ENUM Variants[3]

A successful system test was carried out in October 2008 between MyTelecom Holdings Pty Ltd and Comvergence Pty Ltd. The test which was attended by some members of the IEWG, included making telephone calls between VoIP telephones on the MyTelecom and Comvergence networks. A copy of the Wireshark capture of one of the call sessions is available with the I-ENUM documents on the ACMA website[4].

To facilitate the test a local domain *auenum.com.au* was used. The use of a local domain would limit the interoperability with other countries or systems that utilized or expected the use of a typical ENUM global top level domain e164.arpa. The I-ENUM trial used a closed system, where only registered VoIP providers gained access to the auenum.com.au domain tree and therefore the use of e164.arpa was not an important requirement for the trial Systems

The IEWG trial used, and adapted for local use, the Austrian ENUM Trial Platform (enum.nic.at) running on Redhat Enterprise Linux Server with the Oracle database trial version.

[3] Reference Jim McEachern, Nortel
[4] Refer http://www.acma.gov.au/WEB/STANDARD/pc=PC_310178

VoIP gateways used were the Cisco Call Manager, Asterisk and OpenSER[5].

The Cisco system was only compliant with the obsolete RFC 2916 and to overcome this limitation, a DNS proxy was employed that resolved NAPTR records from RFC 2916 to RFC 3761 format.

Privacy and Security

The I-ENUM system consists of a database and ENUM DNS server and the operation of this system may be considered in terms of the system management and system operation.

I-ENUM System Management

I-ENUM System Management is facilitated by the use of a restricted access database. Registered VoIP providers are provided with encrypted 256-bit SSL secure access to the database server so that registered VoIP phone numbers may be added, edited and deleted. To enhance this security access to the database is limited by the use of a firewall that restricts access to the registered IP address of the VoIP provider.

I-ENUM System Operation

I-ENUM System Operation is facilitated by the use of a restricted access DNS server. Registered VoIP providers are provided with access to the ENUM DNS server by a restricted access firewall that restricts access to the registered IP address of the VoIP provider ENUM gateway.

The facility exists to make access to the VoIP phone number NAPTR resource records to any VoIP provider. This would change the system from implementing a public I-ENUM model rather than a private I-ENUM model.

Privacy

The I-ENUM system holds limited information about a VoIP telephone number. For each VoIP telephone number registered in the I-ENUM system there is only one NAPTR resource

[5] Refer http://en.wikipedia.org/wiki/OpenSER

record which resolves to a SIP URI of the VoIP network gateway that the VoIP phone resides upon. No personal or other information is stored in the I-ENUM system and that using this model, no more information is publicly accessible than is available in a White Pages directory. The VoIP phone numbers registered into the I-ENUM system are managed by the VoIP provider and are registered as part of the Australian domain (in this case part of the private domain auenum.com.au).

The Austrian Trial ENUM system may be used to facilitate both I-ENUM and User ENUM. In this configuration user information would be stored in the system and treatment of privacy would be carried out in accordance with applicable recommendations made after the Australian (User) ENUM Trial.

It should be noted that the I-ENUM system does not match VoIP phone numbers with end user IP addresses and matches the VoIP phone number with the VoIP gateway of the network upon which the VoIP phone resides. This provides limited opportunity for end user privacy to be compromised as the VoIP provider would manage calls coming into their network through their gateway. RFC 5067 refers to a 'carrier of record' using the technology of RFC 3761 to publish the mapping of an E.164 number into a URI that identifies a specific point of interconnection to that service provider's network.

VoIP providers currently publish telephone numbers on their networks through PSTN systems in accordance with current telecommunication regulations. The implementation of private I-ENUM mirrors this practice and does not make any more information available other than on which VoIP provider network the VoIP phone resides.

Regulatory environment

The current regulatory environment does not prevent an organization implementing I-ENUM within a private domain tree on a private network. I-ENUM is currently being used in Australia by several organizations as a means to connect different parts of the internal network together. It appears that there is nothing to prevent an organization from utilizing I-ENUM on the digital network to connect organizations together using a private domain tree as was done during this trial. To utilize e164.arpa in some form for I-ENUM within Australia,

the Department of Broadband, Communications and the Digital Economy (DBCDE) as current delegee for the .1.6.e164.arpa domain would need to delegate the .1.6.e164.arpa domain to the nominated tier 1 registry. AusRegistry International Pty Ltd was the tier 1 registry for the Australian User ENUM trial however this domain is no longer active. The delegation can be cancelled or reassigned to another party through the delegee, DBCDE requesting RIPE-NCC (as the nominated administrator for ENUM under agreement between the ITU and Internet Architecture Board) to make the change.

There is still discussion how to split I-ENUM from User ENUM that is, to use a different domain tree under the e164.arpa domain. It may be necessary to wait for the ITU and IETF to establish the standards for this prior to Australia adopting one particular approach. However, if a suitable industry implementation occurs that is not at odds with the current and anticipated ITU and IETF approach it may be possible for an interim solution to occur[6].

Commercial

At this stage we do not have any commercial models.

Findings – constraints of the trial

The trial proceeded largely with the efforts of a small group of people. There were several factors that affected the trial progress. The trial effort occurred using equipment and systems provided by RMIT University, MyTelecom Holdings and Comvergence. Funding was not available for the trial and therefore the trial occurred as facilities and staff became available in the contributing organisations.

Recommendations

Case 1 (Preferred):

[6] Refer Combined User and Infrastructure ENUM in the e164.arpa tree draft-ietf-enum-combined-09 of 5 Mar 09 http://tools.ietf.org/html/ietf-enum-combined-09

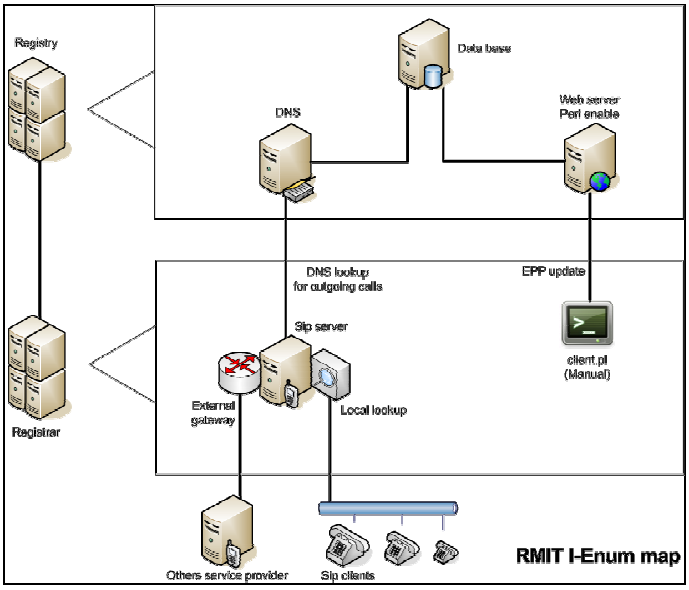

Figure 2: The RMIT I-ENUM map

The RMIT IENUM system in Figure 2 mainly consists of service provisioning and domain name requesting. The schema shows the registry on the top with an example of implementation. The bottom schema is a structure that contains a service provider part on the left and a registrar part on the right. On further steps an automated relation must be established between the SP and the registrar for the SP to publish its blocks of numbers quickly.

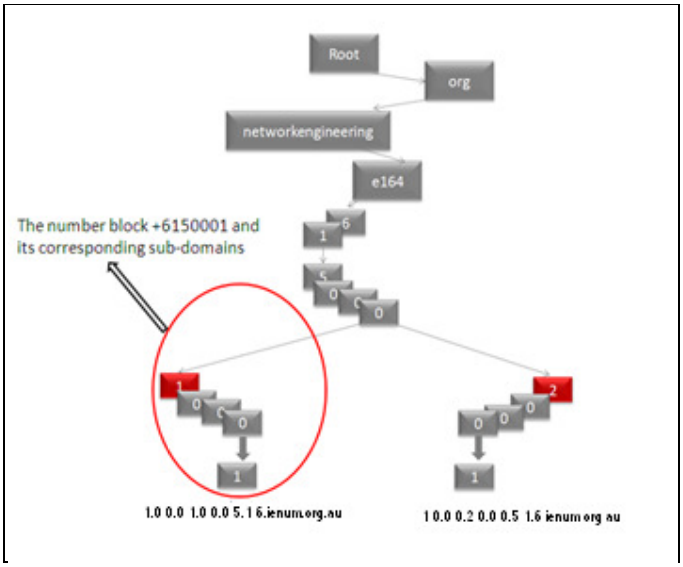

Figure 3: The I-ENUM number block handling

I-ENUM service providers can handle all numbers as blocks. One corresponding block of numbers in the DNS contains the same NAPTR RRs. In our case, see Figure 3 above, the block we are maintaining is +6150001 so that the corresponding DNS record will be 1.0.0.0.5.1.6.e164.ienum.org.au in the DNS of registry. As specified before, any subordinate domain name contains the same NAPTR RR in I-ENUM. For instance, 1.0.0.0.1.0.0.0.5.1.6.e164.ienum.org.au and 2.0.0.0.1.0.0.0.5.1.6.e164.ienum.org.au should contain the same NAPTR RR.

To handle the record stored in the DNS, the registrar needs to talk with the registry by using EPP. Through the registrar, the service provider could operate on their domain names and make them accessible to other parties when a specific number is requested.

Case 2:

Figure 4 below shows the end user ENUM tree on the left and the carrier ENUM tree on the right. The tiered structure would likely be maintained with a Tier 1A registry established for NPAs within Country Code 1. NS records in Tier 1A would indicate the proper Tier 1B registry to query for numbers within a given NPA and the Tier 1B registry would indicate via NS records the Tier 2 name server in which a carrier has populated the NAPTR records that resolve to URIs for SIP addresses of records (AoR) and other communication capabilities. ETSI has proposed the use of such an independent domain for an implementation of I-ENUM, where it is not clear whether or not a common global domain would be used. The independent domain implementation is conceptually simpler but might require a separate effort to instantiate and would offer fewer synergies with end user ENUM. Observe that in Figure 4 a carrier ENUM query resolves to a SIP AoR at one of the carrier's Border Function elements while a user ENUM query, resolved through the user's selected Tier 2 provider, Joes ENUM, provides a SIP AoR at some entity's SIP server as well as providing a URI for messaging.

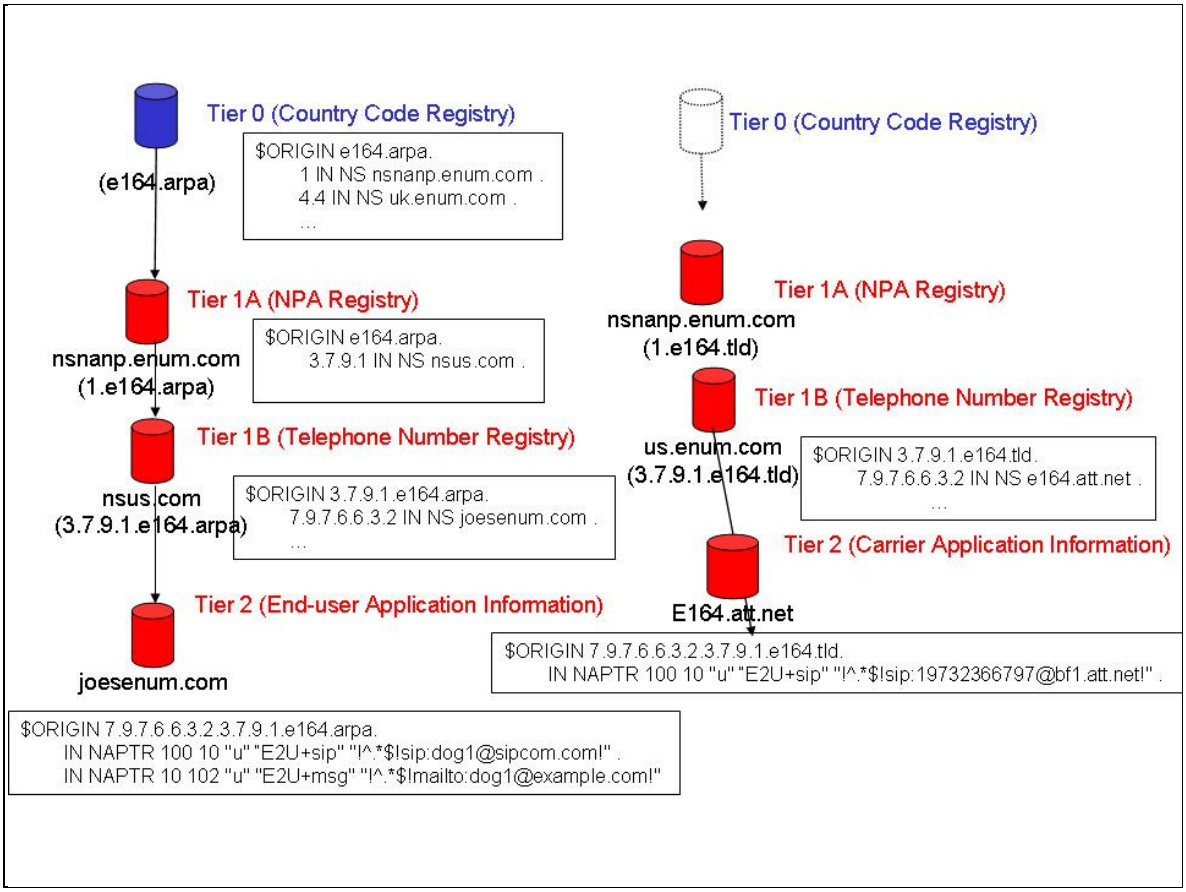

Figure 4: - Infrastructure ENUM in a Separate Domain[7]

Case 3:

The second approach to keeping carrier ENUM in the e164.arpa namespace is shown in Figure 5. This approach relies on the use of a different rewrite rule for deriving the fully qualified domain name to be queried in the DNS for "carrier" clients as opposed to end user clients. This rule inserts another element, e.g., "c" for carrier, somewhere in the FQDN. The likely placement in the NANP context would be between the E.164 country code and the national (significant) number to allow different countries to control their carrier ENUM trees. Within CC1, the existing Tier 1A would have two NS records for each NPA, one pointing to

[7] http://www.enumf.org/documents/6004_0_0.doc

the end user Tier 1B and the other the carrier Tier 1B. (These could be, as also shown in Figure 5, the same Tier 1B.)

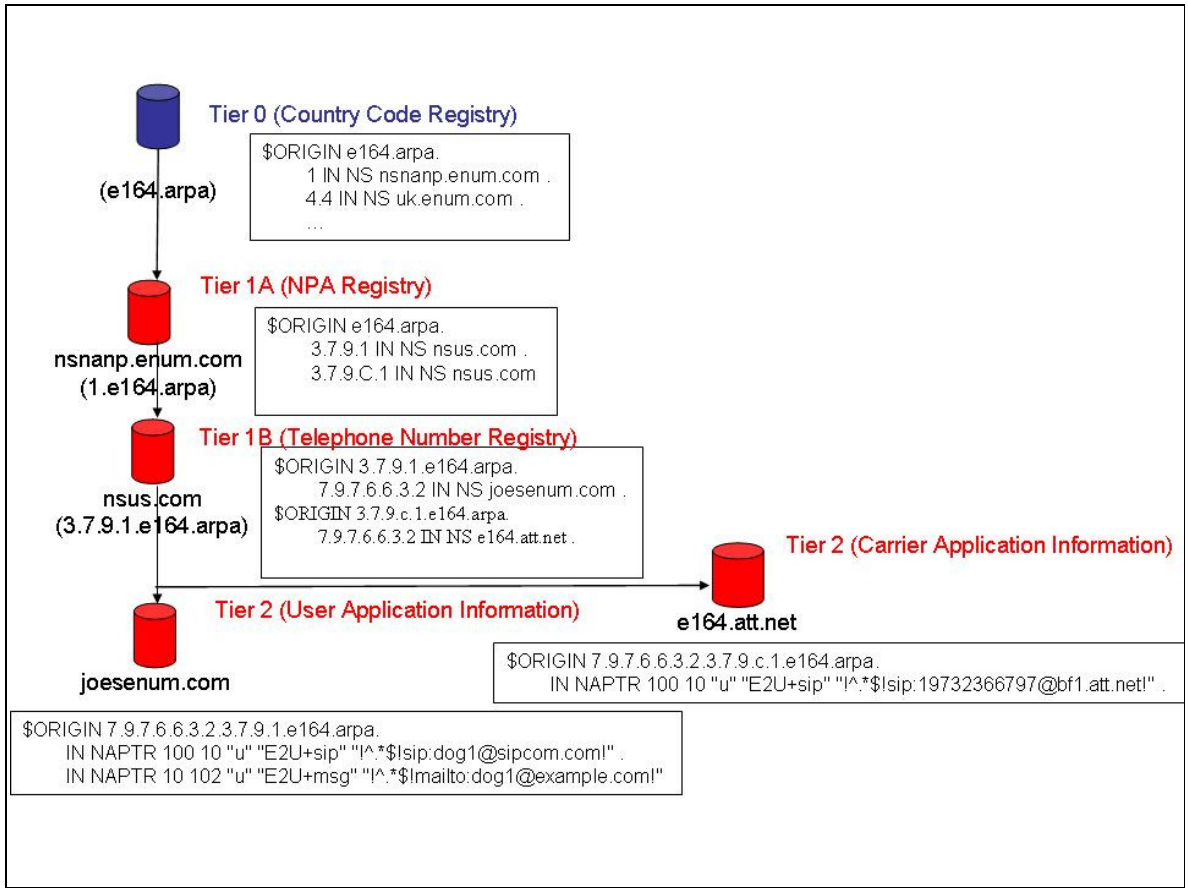

Figure 5: - Infrastructure ENUM in Split Branch[8]

Case 4:

A national Tier 1B Registry delegates each telephone number-based domain name to a Tier 2 name server using a NS resource record. It is in this single set of DNS name servers at the Tier 2 that the terminal NAPTR records are housed. This method would replace the NS records in the Tier 1B registry with two non-terminal NAPTR records that point to an end-user Tier 2 name server and a carrier Tier 2 name server (see Figure 6). The concept of a non-terminal NAPTR is supported in RFC 3761, section 2.4.1

[8] http://www.enumf.org/documents/6004_0_0.doc

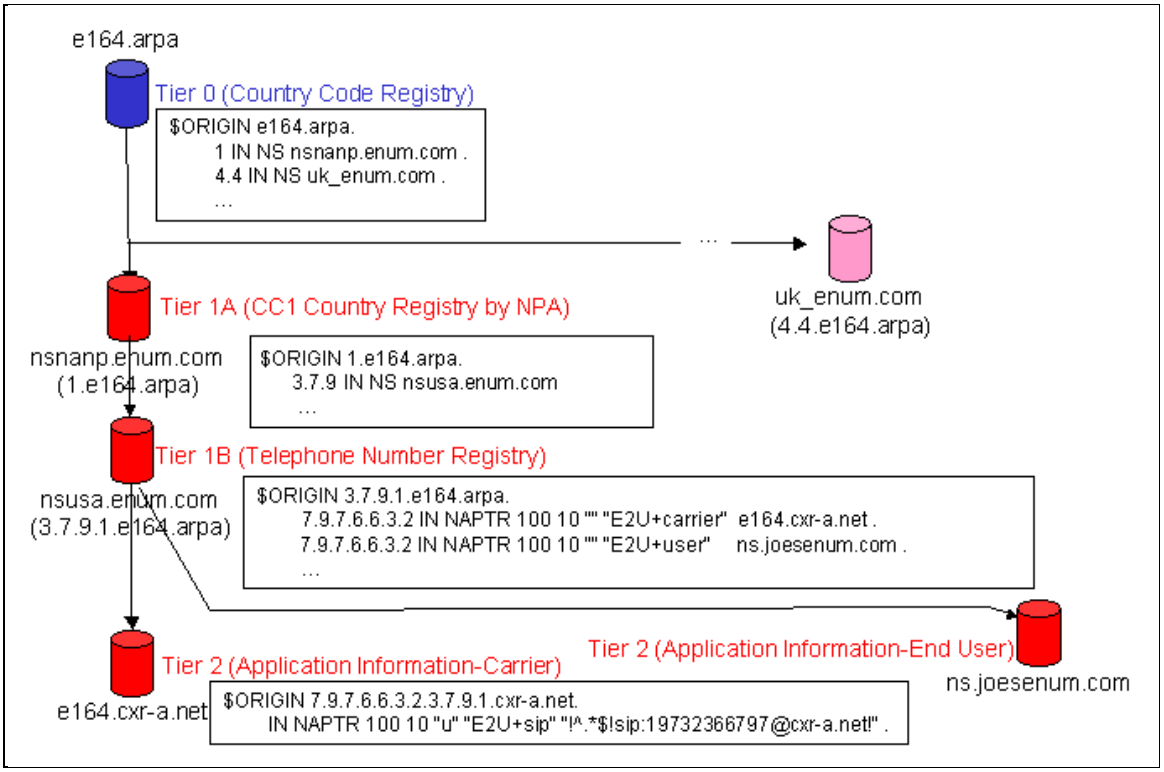

Figure 6: - Infrastructure & End-user ENUM Reference Architecture[9]

Applications and resolvers should retrieve all terminal NAPTRs that are available for the domain name and then apply whatever model is appropriate for the service provider and application being used.

Conclusion

The IEWG successfully carried out a trial of I-ENUM using the Austrian I-ENUM system. Testing of the system was carried out prior to the trial. The IEWG trial demonstrated that I-ENUM is a viable approach to providing number resolution between different VoIP providers in Australia. Two VoIP providers successfully utilized I-ENUM over their operational networks to connect telephone calls. An implementation of I-ENUM using a private domain

[9] see 8.

tree is one approach that could be utilized by Industry to permit an operational implementation of I-ENUM within Australia pending a standardized approach being adopted by the ITU and the IETF.

Appendix B

Technical Information regarding the I-ENUM Trial

The trial infrastructure included equipment currently part of operational systems at Comvergence Pty Ltd and MyTelecom Holdings Pty Ltd and was carried out for all practical purposes as an operating system live on the digital network.

Ports

Apache is currently listening on port 707 (in production this would be port 700 with SSL encryption enabled; for testing and demonstration a different, plain text port is used). You can control it as root with
apachectl [stop|start]

Software installed in ~rts/zid, consisting of a lot of supporting modules and the actual infrastructure enum module Registry-CarrierEnumAT.

Testing was carried out using a basic client installed in ~rts/client.

perl client.pl -h [host] -p [port] [xmlframes....]

Sends xml files to the specified server and displays the communications with the server. XML-Files are given on the command line and processed sequentially in one session. First frame should be a login frame. For example:

perl client.pl -h localhost -p 707 login.xml info.xml

displays info about the domain: 1.0.0.2.1.1.6.i.ienum.org.au (which would be +6112001).

Clients

Clients can manipulate numbers below their assigned number blocks. For testing purposes I have assigned the range +611200 to the registrar 78010 with the password 780100.

There are 5 demo frames in ~rts/client:

login.xml	- used for logging in, specify registrar id and password
info.xml	- display information about a number
create.xml	- create a new number (must be below an assigned + owned number block)
update.xml	- update an existing number (e.g. change NAPTR records)
delete.xml	- removes a number from the database

If you want to change the number, you'll have to edit the xml files directly - it is enclosed in the <domain:name>-tags - but in the demo setup, only +611200* (or *.0.0.2.1.1.6.i.ienum.org.au in e164 notation) is allowed for the registrar 78010!

Script for login.xml looks like:

C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
C: xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
C: xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
C: epp-1.0.xsd">
C: <command>
C: <login>
C: <clID>ClientX</clID>
C: <pw>RMIT</pw>
C: <newPW>RMIT_sece</newPW>
C: <options>
C: <version>1.0</version>
C: <lang>en</lang>
C: </options>
C: <svcs>
C: <objURI>urn:ietf:params:xml:ns:obj1</objURI>

C: <objURI>urn:ietf:params:xml:ns:obj2</objURI>

C: <objURI>urn:ietf:params:xml:ns:obj3</objURI>

C: <svcExtension>

C: <extURI>http://custom/obj1ext-1.0</extURI>

C: </svcExtension>

C: </svcs>

C: </login>

C: <clTRID>ABC-12345</clTRID>

C: </command>

c:</epp>

DNS Setup

The IENUM dns should be the primary dns. Use
dig @K.ROOT-SERVERS.NET. au. Ns
then
dig @ns1.audns.net.au auenum.com.au. any

The registry communicates directly with a DNS server which understands dynamic updates (like bind9[10])

Another possibility is to generate the complete zone file from the database
on the enum machine

there is a ddns part
ddns_fulldump_change_threshold: 1
ddns_master: *
ddns_login: *
ddns_server: *
ddns_key_name: 'e164-update'
ddns_no_prereq: 0
ddns_default_ttl: 7200
ddns_default_class: IN
ddns_key: *

fill in accordingly ...

Server configuration

[10] http://en.wikipedia.org/wiki/Dynamic_DNS

select table_name from user_tables; (to get a list of all tables)

---

spool filename (to save output to a file – do this prior to other commands)
spool off (to stop writing to the filename)

---

select reg_protocol_name from cea_registrars; (to see registrars)

---

select * from cea_registrars where REG_PROTOCOL_NAME='comvergence';

(Open another window)

perl client.pl -h localhost -p 707 login10.xml (to see that registrar can login)

---

at first we have to create a user where the handle has to be unique and in the form of Cxxxxxxxx-ECAT'

```
INSERT INTO cea_persons (
   per_id,
   per_reg_id,
   per_handle,
   per_create_user,
   per_create_date,
   per_pty_id
) VALUES (
   cea_id_seq.nextval,
   ( SELECT reg_id FROM cea_registrars WHERE reg_protocol_id='002' ),
   'C0000010-ECAT',
   user,
   sysdate,
   ( SELECT pty_id FROM cea_person_types WHERE pty_code='agent' )
)
/
```

then the registrar is created

```
INSERT INTO cea_registrars
     (
       REG_ID,
       REG_PROTOCOL_ID,
       REG_PROTOCOL_NAME,
reg_protocol_notify,
       REG_STATUS,
       REG_EXISTENCE,
reg_type,
       REG_CREATE_USER,
       REG_CREATE_DATE,
       REG_EPP_PASSWORD,
       REG_EPP_ENABLED,
       reg_per_id
     ) VALUES (
       cea_id_seq.nextval,
       '0010',
       'comvergence',
       'support@comvergence.com.au',
       'T',
       'A',
       'R',
       user,
       sysdate,
       'pwcomver',
       'Y',
       (SELECT per_id FROM cea_persons WHERE per_handle='C0000010-ECAT')
     )
/
```

---

create "parent" domain

```
insert into CEA_parent_domain_names
(pdo_id,
pdo_name,
pdo_as_number)
values
(CEA_id_seq.nextval,
'1.6.ienum.org.au',
'+61');
```

```
key enum-transfer { algorithm hmac-md5; secret "xxxx";
```

```
};

key enum-update {
algorithm hmac-md5;
secret "yyyy";
};

[root@131 ~]# cd /usr/local/bind/ienum-dns/etc
[root@131 etc]# nsupdate -k Kenum-update.+157+48188.private  > server localhost  > zone
1.6.ienum.org.au  > update add 7.0.0.1.5.1.6.ienum.org.au 7200 NAPTR 10 10 "u"
"E2U+msg"
"!^.*$!sip:202.168.56.138!"
ttl 'NAPTR': not a valid number
 > update add 7.0.0.1.5.1.6.ienum.org.au. 7200 NAPTR 10 10 "u" "E2U+msg"
"!^.*$!sip:202.168.56.138!"
invalid rdata format: unexpected end of input  > update add 7.0.0.1.5.1.6.ienum.org.au. 7200
NAPTR 10 10 "u" "E2U+msg"
"!^.*$!sip:202.168.56.138!" .
 > send
 > update add 3.5.0.0.3.1.9.9.3.1.6.ienum.org.au. 7200 NAPTR 10 10 "u"
"E2U+msg" "!^.*$!sip:202.168.56.138!" .
 > update add 4.5.0.0.3.1.9.9.3.1.6.ienum.org.au. 7200 NAPTR 10 10 "u"
"E2U+msg" "!^.*$!sip:202.168.56.138!" .
 > send
 >

----

[rts@131 log]$ dig @131.170.68.108 4.5.0.0.3.1.9.9.3.1.6.ienum.org.au. any

; <<>> DiG 9.3.3rc2 <<>> @131.170.68.108 4.5.0.0.3.1.9.9.3.1.6.ienum.org.au. any ; (1
server found) ;; global options:  printcmd ;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40566 ;; flags: qr aa rd;
QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;4.5.0.0.3.1.9.9.3.1.6.ienum.org.au. IN ANY

;; ANSWER SECTION:
4.5.0.0.3.1.9.9.3.1.6.ienum.org.au. 7200 IN NAPTR 10 10 "u" "E2U+msg"
"!^.*$!sip:202.168.56.138!" .

;; AUTHORITY SECTION:
1.6.ienum.org.au.       1800    IN      NS      localhost.

;; Query time: 2 msec
```

;; SERVER: 131.170.68.108#53(131.170.68.108) ;; WHEN: Wed Jul 30 05:11:07 2008 ;;
MSG SIZE rcvd: 128

```
insert into CEA_parent_domain_names
(pdo_id,
pdo_name,
pdo_as_number)
values
(CEA_id_seq.nextval,
'1.6.auenum.com.au',
'+61');


update CEA_parent_domain_names set pdo_name = '1.6.auenum.com.au' where pdo_name =
'1.6.ienum.org.au';
commit;
select * from CEA_parent_domain_names;
```

To change a value in the db

```
update cea_registrars set reg_per_id='2994976' where
reg_protocol_name='InstraCorporation';
```

Update dns

```
cd /usr/local/bind/ienum-dns/etc/
nsupdate -k Kenum-update.+157+48188.private
> server localhost
> zone 1.6.auenum.com.au
> update add 3.5.0.0.3.1.9.9.3.1.6.auenum.com.au. 7200 NAPTR 10 10 "u" "E2U+msg"
"!^.*$!sip:202.168.56.138!" .
> update add 4.5.0.0.3.1.9.9.3.1.6.auenum.com.au. 7200 NAPTR 10 10 "u" "E2U+msg"
"!^.*$!sip:202.168.56.138!" .
> send
> quit
```

Testing

To test

```
dig @localhost 4.5.0.0.3.1.9.9.3.1.6.auenum.com.au. any
dig @131.170.68.108 4.5.0.0.3.1.9.9.3.1.6.auenum.com.au. any
```

```
named -c /etc/named.conf -u named -t /usr/local/bind/ienum-dns/
```

go to /usr/local/bind/ienum-dns/ and read the file called README

---

the auto update is working and running every 10minutes (could easily be done more often, this is configured via crontab -r)

to create a delegation
go to /home/rts/client

perl client.pl -h localhost -p 707 login10.xml update61399.xml

to create the naptr
perl client.pl -h localhost -p 707 login10.xml update61399.xml

after 10minutes (at most)
dig @localhost 9.9.3.1.6.auenum.com.au. any

; <<>> DiG 9.3.3rc2 <<>> @localhost 9.9.3.1.6.auenum.com.au. any ; (1 server found) ;; global options: printcmd ;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53346 ;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;9.9.3.1.6.auenum.com.au.   IN   ANY

;; ANSWER SECTION:
9.9.3.1.6.auenum.com.au. 7200   IN   NAPTR   10 105 "u" "E2U+msg" "!^.*$!sip:202.168.56.131!" .

;; AUTHORITY SECTION:
1.6.auenum.com.au.   1800   IN   NS   localhost.

;; Query time: 2 msec
;; SERVER: 131.170.68.108#53(131.170.68.108) ;; WHEN: Tue Aug 5 21:41:00 2008 ;; MSG SIZE rcvd: 117

---

dig @DNS1.TELSTRA.NET. auenum.com.au ns

; <<>> DiG 9.2.1 <<>> @DNS1.TELSTRA.NET. auenum.com.au ns ;; global options: printcmd ;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54226 ;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:

```
;auenum.com.au.             IN      NS

;; AUTHORITY SECTION:
auenum.com.au.      3600    IN      NS      ns1.gt.com.au.
auenum.com.au.      3600    IN      NS      ns2.gt.com.au.
auenum.com.au.      3600    IN      NS      ns3.gt.com.au.

;; ADDITIONAL SECTION:
ns1.gt.com.au.      3600    IN      A       203.62.159.98
ns2.gt.com.au.      3600    IN      A       203.62.159.99
ns3.gt.com.au.      3600    IN      A       202.134.245.22
```

digging further

```
bash-2.01$ dig @ns1.gt.com.au. auenum.com.au. any

; <<>> DiG 9.2.1 <<>> @ns1.gt.com.au. auenum.com.au. any ;; global options:  printcmd ;;
Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15617 ;; flags: qr aa rd ra;
QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 3

;; QUESTION SECTION:
;auenum.com.au.             IN      ANY

;; ANSWER SECTION:
auenum.com.au.      3600    IN      A       131.170.68.108
auenum.com.au.      3600    IN      NS      ns3.gt.com.au.
auenum.com.au.      3600    IN      NS      ns1.gt.com.au.
auenum.com.au.      3600    IN      NS      ns2.gt.com.au.
auenum.com.au.      3600    IN      SOA     ns1.gt.com.au.
admin.gt.com.au. 11 900 600 86400 3600
```

Appendix C

AEDG Infrastructure Working Group Participants

Australian Communications and Media Authority

RMIT University

Soul Communications

Instra Corporation Pty Ltd

Comvergence Pty Ltd

MyTelecom Holdings Pty Ltd

Arrivell Technologies

Council of Country Code Administrators

Department Broadband, Communications and the Digital Economy

Appendix D

AEDG Infrastructure ENUM Working Group

REPORT TO THE AEDG ON THE ACTIVITIES OF THE INFRASTRUCTURE ENUM WORKING GROUP

7 May 2009

Author: Dr Mark Gregory

Introduction

The Australian ENUM Discussion Group (AEDG) formed a working group in April 2007 with terms of reference to investigate and report on the following:

1. Existing implementations of Infrastructure ENUM (I-ENUM) and the different models that have been used.
2. The extent to which I-ENUM has undergone standardization within the Internet Engineering Task Force (IETF) and other standardization bodies.
3. Current research activities into I-ENUM.
4. Whether an Australian implementation of I-ENUM is feasible.

This working group conducted a trial of I-ENUM from 01 September to 30 November 2008 using the Austrian ENUM Trial Platform made available by the University of Austria.

This report addresses the terms of reference of the AEDG in relation to I-ENUM.

AEDG Terms of Reference

1. Existing implementations of Infrastructure ENUM (I-ENUM) and the different models that have been used.

Currently there are several private implementations of I-ENUM within Australia that provide internal traffic routing within voice service provider networks. These I-ENUM implementations have utilized private domain trees. The I-ENUM trial model that was implemented and tested utilized a private domain tree (auenum.com.au), using a closed system, where only registered VoIP providers had access to the private domain tree. The use of e164.arpa domain was not used in the trial.

Further information on this implementation is contained in the AEDG I-ENUM Working Group Trial Report.

2. The extent to which I-ENUM has undergone standardization within the Internet Engineering Task Force (IETF) and other standardization bodies.

I-ENUM is currently being considered and standardized by the IETF.

The IETF has published the following documents:

- S.Lind & P.Pfautz , *RFC 5067 Infrastructure ENUM Requirements*, November 2007[11];

- P.Ffautz and R.Stastny, *RFC 5526 - The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application for Infrastructure ENUM,* April 2009[12]. This standard is the product of the Telephone Number Mapping Working Group and facilitates the use of parallel namespaces for use outside the "user" namespace defined in RFC 3761. This document provides a means to facilitate private I-ENUM within organizations and service providers and to interoperate with previously adopted standards; and

- M. Haberler and O. Lendl, *RFC 5527 - Combined User and Infrastructure ENUM in the e164.arpa tree*, May 2009[13]. This standard defines an interim solution for

[11] http://www.ietf.org/rfc/rfc5067.txt
[12] http://www.rfc-editor.org/rfc/rfc5526.txt
[13] http://www.rfc-editor.org/rfc/rfc5527.txt

Infrastructure ENUM to allow a combined User and Infrastructure ENUM implementation in e164.arpa as a national choice.

In summary, the IETF is continuing its commitment to the development of I-ENUM standards to facilitate its implementation more broadly, as another way for VoIP service providers to provide services for their customers.

3. Current research activities into I-ENUM

Current research into I-ENUM may be represented by outcomes from recent ENUM and I-ENUM trials that have been carried out by national bodies from various countries including USA, Japan, Korea, China and several European countries including Austria and UK. Of interest is the ENUM System software developed by the Austrian Domain Registry body[14].

Implementation of I-ENUM as a broader solution relies on data paths between service provider gateways. To facilitate the implementation of suitable data paths a research group known as the RIPE ENUM Working Group has been formed. A list of the current activities and I-ENUM implementations can be found on the RIPE Working Group webpage[15].

4. Feasibility of an Australian I-ENUM implementation

The I-ENUM Working Group (IEWG) conducted a trial from 1 September 08 to 30 November 08. The I-ENUM Trial Report[16] includes a description of a successful implementation of I-ENUM between two VoIP service providers using the Austrian ENUM software. The trial outcome demonstrates that it should be possible to implement I-ENUM in Australia as a facilitator of linking VoIP service providers together. The IEWG trial demonstrated that I-ENUM is a viable approach to providing number resolution between different VoIP providers in Australia.

Conclusion

[14] http://sourceforge.net/projects/enumreg/
[15] http://www.enumdata.org/
[16] http://www.acma.gov.au/WEB/STANDARD/pc=PC_310178

The trial indicates that it is possible to provide number resolution between different VoIP providers using I-ENUM and indeed, from the trial it can be seen that I-ENUM can be an efficient mechanism for end point determination for any real time service (or session) provided over IP networks. There was a general lack of interest by industry to participate in the I-ENUM working group and in the trial. At present it is understood that some service providers are already routing VoIP services using either bilateral peering agreements or services offered through peering exchanges (which may be implementing a private ENUM internally) or just routing calls external to their own network via the PSTN.

These other private implementations of I-ENUM are perhaps not standards-based and so would need careful consideration in the Australian context should they become mainstream.

In summary, the terms of reference laid out by the AEDG have been met, albeit with a low level of participation within the Working Group meetings and in the trial.

Appendix E

EPP commands

Session Management

<login>

We would use the client ID and password to authenticate the session. We put our password and Client ID in EPP <login> command which is located in the login.xml file that we filled in with all the elements.

The EPP <login> command is used to establish a session with an EPP server. A <login> command needs to be sent before any other EPP command to establish an ongoing session. A server operator has the ability to limit the number of failed login attempts N, 1 <= N <=

infinity, after which a login failure results in the connection to the server (if a connection exists) being closed.

There are many new element involved in <login> command and we'll explain them in the following, so that it will be helpful to better understand each line of the XML file.

Element Explanation:

<newPW> element contains a new plain text password which will be assigned to the client as the password for next login.

<login> commands. The value of this element is case sensitive.

<options> element that contains the following child elements:

<version> element contains the protocol version to be used for the command or ongoing server session.

<lang> element contains the text response language to be used for the command or ongoing server session commands.

<svcs> element contains one or more <objURI> elements that contain namespace URIs representing the objects to be managed during the session.

Our XML Login script looks like:

C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
C: xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
C: xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
C: epp-1.0.xsd">
C: <command>
C: <login>
C: <clID>70810</clID>
C: <pw>708100</pw>

C: <newPW>RMIT_sece</newPW>

C: <options>

C: <version>1.0</version>

C: <lang>en</lang>

C: </options>

C: <svcs>

C: <objURI>urn:ietf:params:xml:ns:obj1</objURI>

C: <objURI>urn:ietf:params:xml:ns:obj2</objURI>

C: <objURI>urn:ietf:params:xml:ns:obj3</objURI>

C: <svcExtension>

C: <extURI>http://custom/obj1ext-1.0</extURI>

C: </svcExtension>

C: </svcs>

C: </login>

C: <clTRID>ABC-12345</clTRID>

C: </command>

C:</epp>

Each time, when we need to make any transaction, we need to make each command going with login command. Like login & check, login & create, etc. In the example below, we'll just illustrate how it works in particular.

To make it happen, we put the folder "client" on the Desktop of server and it contains the tool kit for registrar. The "client" folder is located in /home/kielus/Desktop/client. There you can find the tool kit of updating for registrar, as shown on figure 1.

```
root@VIPsec:/home/kielus/Desktop/client# ls -la
total 32
drwxr-xr-x 2 root   root   4096 2008-06-11 22:13 .
drwxr-xr-x 5 kielus kielus 4096 2008-06-11 18:38 ..
-rw-r--r-- 1    502    502 2007 2005-03-08 00:51 client.pl
-rw-rw-r-- 1    502    502  740 2008-06-01 14:01 create.xml
-rw-rw-r-- 1    502    502  599 2008-06-01 14:01 delete.xml
-rw-rw-r-- 1    502    502  635 2008-06-01 14:01 info.xml
-rw-r--r-- 1    502    502  767 2008-06-01 14:02 login.xml
-rw-rw-r-- 1    502    502 1538 2008-06-01 14:02 update.xml
```

Figure 1: The necessary files of the toolkit

The application for registrar is the program named client.pl. It is Perl based program which is able to talk with registry server by using 707 (EPP) as its target port. Or we can specify the port we wish. Following is the syntax is perl command.

perl client.pl -h [host] -p [port] [xmlframes....]

The [host] here refers to the IP address of our registry server which is 131.170.68.108. [port] will be the well known port for EPP, hence 707. After that the <login> command and an action xml file, say info.xml will be the last two parameters that need to specify in perl command.

As we discussed above, XML file is like a vehicle which is able to carry the essential elements from registrar to registry. The XML shows here are pre-defined template. As we know, the element in XML file should be found in somewhere where their characteristic was defined. We call them XML namespace and schema.
In our case, their definition can be found based on the URI and URN in the follows:
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
C: xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
C: xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
C: epp-1.0.xsd">

As we went through the login steps, we discovered some parts that need to be paid attention to. They have been our pitfall when we did the transactions.
The login session will expire immediately after the response issued from the EPP server. Next session will be activated in the next successful login stage. It is a good way to protect the resource on the server side.
<newPW> element is used for security consideration. It will ask for the password specified in this element instead of the original one when next logging in. People would not have to do this if it is not a security requirement.

EPP Query command

EPP <check> Command:

The EPP <check> command is used to check the availability of a provisioning object within a repository.

Aim of this transaction:
To check the availability of 1.0.0.0.5.1.6.ienum.org.au

Command to be used:
perl client.pl -h 131.170.68.108 -p 707 login.xml check.xml

Following is the check xml file in which we put the target domain name as shown in bold letters.

Example <check> command:

C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
C: xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
C: xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
C: epp-1.0.xsd">
C: <command>
C: <check>
C: <domain:check
C: xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
C: xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
C: domain-1.0.xsd">
C: <domain:name>1.0.0.0.5.1.6.ienum.org.au </domain:name>
C: </domain:check>
C: </check>
C: <clTRID>ABC-12345</clTRID>
C: </command>
C:</epp>

In reply from the server, some new element will be contained, like <resData>, <domain:chkData>, <resData> and <domain:cd>.

Element Explanation

<resData>: indicates the subcommand within it contains the information that replied from server.
<domain:chkData>: As the child element of <resData>, contains the location of child element namespace and schema.
<domain:cd>: It is a parent element in which contains the status of a certain domain.

<domain:reason> contains the description of the reason when domain is unavailable, else the “avail” flag is “1” means domain is available.

The output from the server after <check> command is processed looks like:

S:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
S:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
S: xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
S: xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
S: epp-1.0.xsd">
S: <response>
S: <result code="1000">
S: <msg>Command completed successfully</msg>
S: </result>
S: <resData>
S: <domain:chkData
S: xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
S: xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
S: domain-1.0.xsd">
S: <domain:cd>
S: <domain:name avail="1">**1.0.0.0.5.1.6.ienum.org.au** </domain:name>
S: </domain:cd>
S: </domain:chkData>
S: </resData>
S: <trID>
S: <clTRID>ABC-12345</clTRID>
S: <svTRID>54322-XYZ</svTRID>
S: </trID>
S: </response>
S:</epp>

Because of the queried domain that we’ve already created, we are able to see the “avail=1” in the returned information from server. If the domain we queried has been created or is being used, we will see avail=0 and a <domain:reason> element which describe the reason why the domain block is not available at the moment.

EPP <info> Command:
Reference: RFC 3731 [20], RFC 3730 [21], RFC 4114 [18]

The EPP <info> command is used to retrieve information associated with a domain object. The response differs to sponsoring client and unauthorized clients. All related information will return to both sponsoring and unauthorized client if and only if unauthorized client provides valid information to the server. If unauthorized client doesn't provide valid authorization information, then the server determines which "optional" information to be returned.

Option Explanation
Following are the options that we may use in <info> command.

"all": It is a default one, and all information related to subordinate and delegated hosts will be returned.

"del": Only returns delegated hosts.

"sub": Only returns subordinate hosts.

"none": Returns no information about delegated or subordinated hosts.

Sample Client query EPP<info> command

```
C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
C: xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
C: xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
C: epp-1.0.xsd">
C: <command>
C: <info>
C: <domain:info
C: xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
C: xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
C: domain-1.0.xsd">
C: <domain:name hosts="all">1.0.0.0.5.1.6.ienum.org.au</domain:name>
C: </domain:info>
C: </info>
C: <clTRID>ABC-12345</clTRID>
C: </command>
C:</epp>
```

Command used:

#perl client.pl –h 131.170.68.108 –p 707 login.xml info.xml

In return, the elements coming from server should be locating a new XML name space and schema like : <domain:infData
S: xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
S: xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0.xsd">

Sample Server response EPP<info> command:

S:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
S:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
S: xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
S: xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
S: epp-1.0.xsd">
S: <response>
S: <result code="1000">
S: <msg>Command completed successfully</msg>
S: </result>
S: <resData>
S: <domain:infData
S: xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
S: xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
S: domain-1.0.xsd">
S: <domain:name>1.0.0.0.5.1.6.ienum.org.au</domain:name>
S: <domain:roid>EXAMPLE1-REP</domain:roid>
S: <domain:status s="ok"/>
S: <domain:ns>
S: <domain:hostObj>ns1.gt.com.au</domain:hostObj>
S: </domain:ns>
S: <domain:host>ns1.gt.com.au</domain:host>
S: <domain:clID>78010</domain:clID>
S: <domain:crID>78010</domain:crID>
S: <domain:crDate>2008-04-03T22:00:00.0Z</domain:crDate>
S: <domain:upID>78010</domain:upID>
S: <domain:upDate>2008-04-03T09:00:00.0Z</domain:upDate>
S: <domain:exDate>2008-04-03T22:00:00.0Z</domain:exDate>
S: <domain:trDate>2008-04-08T09:00:00.0Z</domain:trDate>
S: <domain:authInfo>
S: <domain:pw>780100</domain:pw>
S: </domain:authInfo>

S: </domain:infData>
S: </resData>
S: <trID>
S: <clTRID>ABC-12345</clTRID>
S: <svTRID>20080611234931536610-78010-ienum43</svTRID>
S: </trID>
S: </response>
S:</epp>

Element Explanation:

<domain:name> element that contains the fully qualified name of the domain object.
<domain:roid> element that contains the Repository Object IDentifier assigned to the domain object when the object was created.

Optional elements

<domain:status> elements that contain the current status descriptors associated with the domain.
<domain:registrant> element and one or more OPTIONAL <domain:contact> elements that contain identifiers for the human or organizational social information objects associated with the domain object.

<domain:ns> element that contains the fully qualified names of the delegated host objects or host attributes (name servers) associated with the domain object.
<domain:host> elements that contain the fully qualified names of the subordinate host objects that exist under this superordinate domain object.
<domain:clID> element that contains the identifier of the sponsoring client.
<domain:crID> element that contains the identifier of the client that created the domain object.
<domain:crDate> element that contains the date and time of domain object creation.
<domain:exDate> element that contains the date and time identifying the end of the domain object's registration period.
<domain:upID> element that contains the identifier of the client that last updated the domain object.
<domain:upDate> element that contains the date and time of the most recent domain object modification.
<domain:trDate> elements that contains the date and time of the most recent successful domain object transfer.

<domain:authInfo> element that contains authorization information associated with the domain object.

Here we just provide the simple description of each element in order to make the returned information better understandable. More description will be available on RFC 3731.

Result Analysis

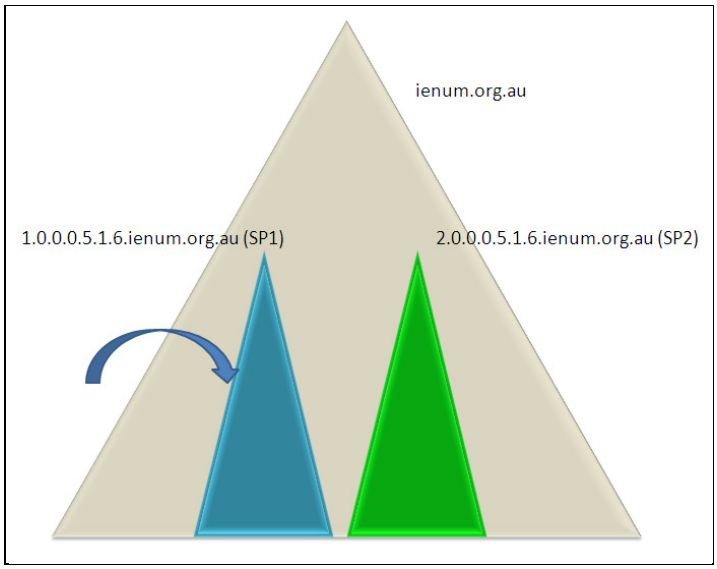

Figure 2: The target of the info command

The figure 2 above shows how the xml is used to query a domain name for associated information. The information we can see from the <info> returned message is the element we filled in <create> command prior to the <info> uploaded, which means we've already performed a <create> operation before the <info> command. The <info> command is a great tool to help us to know the properties of a domain object, which facilitates us on troubleshooting with the existing domain by issuing the simple command.

EPP Transform command

EPP <create> command

EPP <create> command provide the primary operation for client to make a new domain as well as the properties of the domain, like name server, domain hosts, etc.

In our project, we need to create a domain for service provider 1 (SP1), which is 1.0.0.0.5.1.6.ienum.org.au with name server ns1.gt.com.au.

Our ultimate aim is to update the NAPTR which will be used for Infrastructure ENUM provisioning. Usually NAPTR record could be updated in a single transaction through create, however, do to registry capability, it can only be done by using the update command which will be described in the next segment.

Element explanation:

<domain:name>: it contains the fully Qualified name that to be created.
<domain:period>: contains initial registration period of the domain object.
<domain:ns>: contains the domain server FQDN
<domain:registrant>: contains the identifier of end users of the domain object. The information of registrant ID should be preloaded into the server so that the server can be aware of the name in advance.
<domain:crDate> element that contains the date and time of domain object creation.
<domain:exDate> element that contains the date and time identifying the end of the domain object's registration period.

Command to be used:
#perl client.pl –h 131.170.68.108 –p 707 login.xml create.xml

Here is our XML script for this transaction:

C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
C: xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
C: xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
C: epp-1.0.xsd">
C: <command>
C: <create>
C: <domain:create
C: xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
C: xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
C: domain-1.0.xsd">
C: <domain:name>1.0.0.0.5.1.6.ienum.org.au</domain:name>
C: <domain:period unit="y">2</domain:period>
C: <domain:ns>
C: <domain:hostObj>ns1.gt.com.au</domain:hostObj>
C: </domain:ns>
C: <domain:authInfo>
C: <domain:pw>780100</domain:pw>
C: </domain:authInfo>
C: </domain:create>
C: </create>
C: <clTRID>ABC-12345</clTRID>
C: </command>
C:</epp>

After this script successfully processed by the server, we see the following response message. The key elements have been marked in bold.

S:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
S:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
S: xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
S: xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
S: epp-1.0.xsd">
S: <response>
S: <result code="1000">
S: <msg>**Command completed successfully**</msg>
S: </result>
S: <resData>

S: <domain:creData
S: xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
S: xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
S: domain-1.0.xsd">
S: <domain:name>**1.0.0.0.5.1.6.ienum.org.au**</domain:name>
S: <domain:crDate>2008-04-03T22:00:00.0Z </domain:crDate>
S: <domain:exDate>2008-04-03T22:00:00.0Z </domain:exDate>
S: </domain:creData>
S: </resData>
S: <trID>
S: <clTRID>ABC-12345</clTRID>
S: <svTRID>54321-XYZ</svTRID>
S: </trID>
S: </response>
S:</epp>

Result Analysis

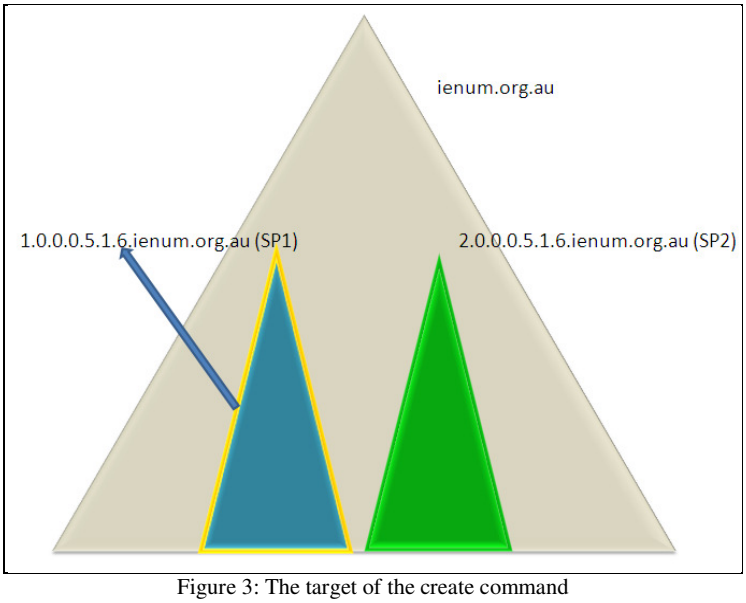

Figure 3: The target of the create command

As figure 3 shows, the yellow line outlined triangle is our newly created domain within ienum.org.au. Together with the domain name we created, we specified the name server for this 1.0.0.0.5.1.6.ienum.org.au zone. This implies the name server ns1.gt.com.au we specified will be used to accommodate information of I-ENUM information of the number range +6150001. After executing the <update> command which will be discussed in next segment, NAPTR Resource Records will be stored in one object within this zone, and the name server will be the entity that provides the service of answering ENUM queries.

EPP <update> command

To complete the standard EPP create command, EPP update command is used to maintain the content of the existing domain. In terms of ENUM, EPP update command can update renewed or new NAPTR record of the target domain. In EPP update command, with NAPTR purpose, the command must contain an <extension> element in which NAPTR namespace can be found. The <extension> element contains a child <e164:create> element that identifies the extension namespace and the location of the extension schema. The <e164:create> element contains one or more <e164:naptr> elements that contain the following child elements:

New Element Explanation:

<e164:order> element that contains a NAPTR order value.
<e164:pref> element that contains a NAPTR preference value.

Optional elements
<e164:flags> element that contains a NAPTR flags value.
<e164:svc> element that contains a NAPTR service value.
<e164:regex> element that contains a NAPTR regular expression value.
<e164:replacement> element that contains a NAPTR replacement value.

On considering the I-ENUM environment, service provider of SP1 would like to publish only the domain name (gateway address) of their SIP server instead of the detail information of their registrants. Also, The NAPTR Resource Record will be attached to domain 1.0.0.0.5.1.6.ienum.org.au which is the corresponding domain of SP1's number range. In this way, each individual within this domain will be rewritten with the NAPTR Record that <update> command updated.

The service we chose to use is SIP which we will specifically describe in other sections. Therefore the NAPTR RR of SP1 should look like:

IN NAPTR 10 100 "u" "E2U+sip:sip" "!^.*$!sip:sip1.ienum.org.au!"

This is the NAPTR RR we would like to associate with "1.0.0.0.5.1.6.ienum.org.au". And the sip1.ienum.org.au is the SIP Server that Service Provider 1 would like to expose to public queries.

Let's come back to DNS aspect. According to NAPTR showed above, the domain name object in zone file should be like:

$ORIGIN 1.0.0.0.5.1.6.ienum.org.au
@ IN NAPTR 10 100 "u" "E2U+sip" "!^.*$!sip:sip1.ienum.org.au!"

The command to be used:
#perl client.pl –h 131.170.68.108 –p 707 login.xml create.xml

In our case, the EPP <update> xml script looks like this and the key component are in bold letter.

C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
C: xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
C: xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
C: epp-1.0.xsd">
C: <command>
C: **<update>**
C: <domain:update
C: xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
C: xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
C: domain-1.0.xsd">
C: <domain:name>1.0.0.0.5.1.6.ienum.org.au </domain:name>
C: </domain:update>
C: **</update>**
C: **<extension>**
C: <e164:update xmlns:e164="urn:ietf:params:xml:ns:e164epp-1.0"
C: xsi:schemaLocation="urn:ietf:params:xml:ns:e164epp-1.0
C: e164epp-1.0.xsd">
C: <e164:rem>
C: <e164:naptr>
C: <e164:order>10</e164:order>
C: <e164:pref>100</e164:pref>
C: <e164:flags>u</e164:flags>
C: <e164:svc>E2U+SIP/e164:svc>
C: <e164:regex>"!^.*$!sip:sip1.ienum.org.au!"</e164:regex>
C: </e164:naptr>
C: </e164:rem>
C: </e164:update>
C: **</extension>**
C: <clTRID>ABC-12345</clTRID>
C: </command>
C:</epp>

Server Response:

S:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
S:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
S: xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
S: xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
S: epp-1.0.xsd">

S: <response>
S: <result code="1000">
S: <msg>Command completed successfully</msg>
S: </result>
S: <trID>
S: <clTRID>ABC-12345</clTRID>
S: <svTRID>54321-XYZ</svTRID>
S: </trID>
S: </response>
S:</epp>

Result Analysis

As we went through the transaction process, we found the update command has some limitation or trait when transacting with the registry.

The operation must be done on exist domain.
The content in extension element will be replacing the existing NAPTR RR.
The number block must be owned by the requesting client.

Besides, for Service Provider consideration, what Service Provider published is only the gateway address instead of a full SIP URI, which means SIP Service Provider needs to complete the full URI in their local settings. This topic will be discussed in the SIP chapter.

EPP <delete> Command

EPP <delete> Command enables client to delete the domain that already exist. It simply releases the property that a domain possessed before. The effect is shown on figure 4.

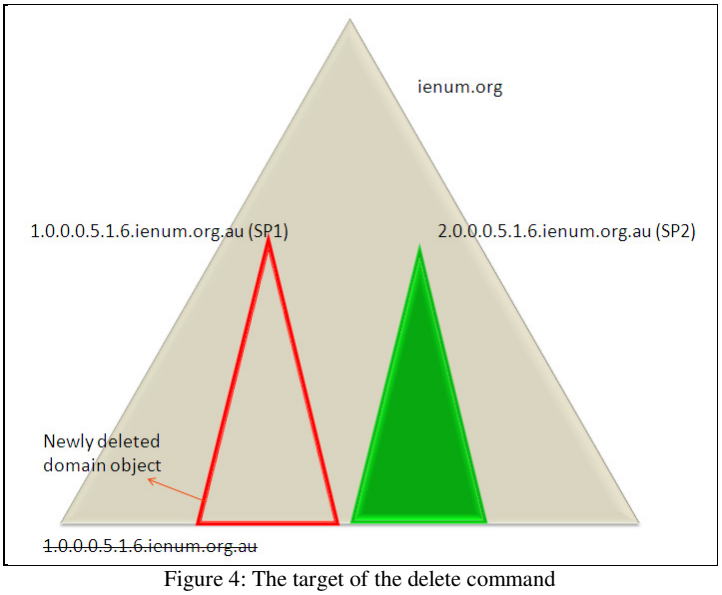

Figure 4: The target of the delete command

The command to be used:
perl client.pl –h 131.170.68.108 –p 707 login.xml delete.xml

The EPP <delete> command may look like this and the bold part is the deleting function.

C:<?xml version="1.0" encoding="UTF-8" standalone="no"?>
C:<epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
C: xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
C: xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
C: epp-1.0.xsd">
C: <command>
C: <delete>
C: <domain:delete
C: xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
C: xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
C: domain-1.0.xsd">
C: <domain:name>1.0.0.0.5.1.6.ienum.org.au</domain:name>
C: </domain:delete>
C: </delete>
C: <clTRID>ABC-12345</clTRID>
C: </command>
C:</epp>

Result Analysis:

It is suggested from RFC 3731 that the domain should not be deleted if the subordinated host are associating with the domain. The subordinated hosts can be the name server of the current domain. Before deleting, a server is recommended to notify clients that object relationships exist by sending a 2305 error response code when a <delete> command is attempted and fails due to existing object relationships.

As we went through the EPP delete transaction process, we discovered some points that may be taken into consideration for ENUM.

- The domain object together with NAPTR RR will be removed from registry when performing the delete operation.

- If the number block contains NAPTR RR, it implies the DNS modification needs to be done when update occurs.

Appendix F

Infrastructure ENUM Implementation in Australia

Ananda T Jammulamadaka
School of Electrical and Computer Engineering
RMIT University
Melbourne, Australia
s3008152@student.rmit.edu.au
Mark A Gregory
School of Electrical and Computer Engineering
RMIT University
Melbourne, Australia
mark.gregory@rmit.edu.au

Abstract— ***VoIP is becoming the dominant approach for telephony and this growth will continue with the upcoming introduction of 4G mobile wireless and fibre to the home networks. With the growing demand for VoIP and increased VoIP traffic, it is important to implement a system that provides interoperability between the existing telephony numbering system and the IP network device addresses. Infrastructure ENUM is one approach that may be used. This paper examines the Infrastructure ENUM implementation in Australia***

Keywords*— *User ENUM, I-ENUM, E.164 numbers, Service Provider, Number Portability, VoIP Interconnection, DNS

I Introduction

VoIP is rapidly being adopted by business and residential customers who have started embracing the cost-effectiveness and new capabilities offered by IP networks. The traditional public telephony service continues to be better supported because of its familiarity, ubiquity, simplicity, low cost devices and calling rates, however, this support is falling.

Consumers have adopted the use of 3G networks and wireless broadband, with the use of wireless broadband growing by 162 per cent in 2009. Currently, the number of broadband users stands at 6.7 million and the number of fixed line telephone services has dropped 3% and stands at 10.67 million [1]. The drop in fixed-line services is attributed to the increase in use of other technologies such as 3.5G and VoIP.

The Australian Bureau of Statistics (ABS) estimated that 60% of ISPs offered VoIP services, 56% a fixed line telephone service and 36% a mobile service to customers as of June 2009 [1].

With the increase in the number of VoIP providers, there is a need to bridge these 'ISP based VoIP Islands', which today is being handled by PSTN peering. Routing VoIP-to-VoIP calls over the PSTN is highly inefficient and expensive. Convergence between the PSTN and the IP networks has become crucial and ENUM is a possible solution to bridge the VoIP islands.

II Infrastructure ENUM

ENUM (E.164 NUMber Mapping) was first defined by Falstrom (2000) in RFC 2916 [2], with the idea of using the widely used E.164 telephone numbers in conjunction with the state of the art DNS technology. The goal of ENUM as stated in RFC 3245 is that one provider should be able to look up information needed to map an E.164 number to an IP address from the DNS, which another provider has stored in the DNS.

ENUM was further separated into User ENUM and Infrastructure ENUM (I-ENUM). I-ENUM facilitates the telephone service providers creating and maintaining customer records within a DNS tree, whereas User ENUM is for the end users who use an E.164 number to associate multiple Internet services on a public DNS tree.

An ENUM Trial was conducted by the Australian Communication and Media Authority (ACMA), with a local ISP acting as the tier 1 registry in Australia between June 2005 and June 2007. I-ENUM was raised in late 2005, with a lot of assumptions and issues to be resolved before embarking on to the next stage of the I-ENUM implementation [3]. I-ENUM could be implemented in a private DNS or in a public DNS. Private DNS would mean that only authorised VoIP service providers would be able to query and access the I-ENUM database, whereas public DNS would mean that everyone would have access. This paper discusses the use of a private name space, such as ienum.org.au [10], which would be the common accessible name space for VoIP service providers to populate their DNS resource records in a private DNS.

The VoIP service providers constantly update the private I-ENUM database with the description of services available and nominate IP rendezvous points for other VoIP service

providers to peer with. This paper suggests that EPP, which is already an accepted protocol used to update DNS, would be suitable as the provisioning protocol for updating the I-ENUM DNS [10].

With the introduction of ENUM, VoIP service providers are given the opportunity to offer a wide range of User ENUM services and also utilise I-ENUM to facilitate VoIP, Number Portability and VoIP Interconnection. User ENUM and I-ENUM, with the facilitation of number portability and VoIP interconnection, can be implemented as an industry solution within Australia, however, a number of steps would need to occur prior to a working ENUM based VoIP solution being adopted by all VoIP service providers.

III Related Work

One open issue is whether to use private or public DNS with I-ENUM to provide VoIP interconnection information. Several countries have initiatives for I-ENUM using private DNS, generally on a small scale. Austria is a leader in the use of ENUM and operates an I-ENUM registry using public DNS. ENUM and I-ENUM trials are being, or have been conducted by many other countries.

Austria is a front runner in the use of I-ENUM. The Austrian implementation utilises a public DNS I-ENUM within their country domain tree (+43 or in ENUM .3.4.) [4].

The United Stated ENUM Forum was established to investigate the possible implementation of ENUM in the US. Neustar, in alliance with the GSM Association (GSMA), offer private I-ENUM as the industry's first commercial service in the form of PathFinder an IP-based communication service.

IV Objective

The research objective is to develop a framework for an Australian I-ENUM implementation. The research included an analysis of how to move from the status quo to a VoIP IP peered telephony solution used by a majority of customers.

Unlike User ENUM, which is user centric and provides users with the capability to choose services and call termination types, I-ENUM allows the VoIP service provider to decide on

the service and the termination type. This is done by resolving the called number from the I-ENUM DNS, identifying the service, ensuring that the terminating carrier has a compatible service and IP VoIP enabled gateway and then transferring the call via the IP network. This facilitates the VoIP service providers to publicize a set of rendezvous points for terminating VoIP services to other VoIP service providers.

I-ENUM is the key for VoIP service providers to keep control on the routing information behind e.164 numbers. A condition for I-ENUM is for E.164 numbers to be the method for identifying subscribers. This research is based on the assumption that Australian VoIP service providers will reach consensus on a specific technical mechanism that allows I-ENUM to be implemented.

Fig. 1 shows how a call from User A with Carrier A will be routed to User B with Carrier B. It also demonstrates how the databases are queried to identify the carrier border gateway and route calls and depicts the difference in call handling between User ENUM and I-ENUM [5].

The research goal was to design and develop a system that can be deployed on a national scale and to understand the steps that industry would need to take to implement the solution. The proposed system utilizes the E.164 numbering plan and hence all the Australian telecommunication regulations may be implemented.

V System Design

The first part of the research was to identify how the data would flow and how the I-ENUM service would be offered. The I-ENUM tier 1 registry represents the root authority of the Australian ENUM implementation and would maintain the DNS NAPTR records and the referential integrity of the lookup mechanisms. The I-ENUM DNS registry hierarchy would be maintained or used by:

- DNS providers
- Registrars
- VoIP services providers

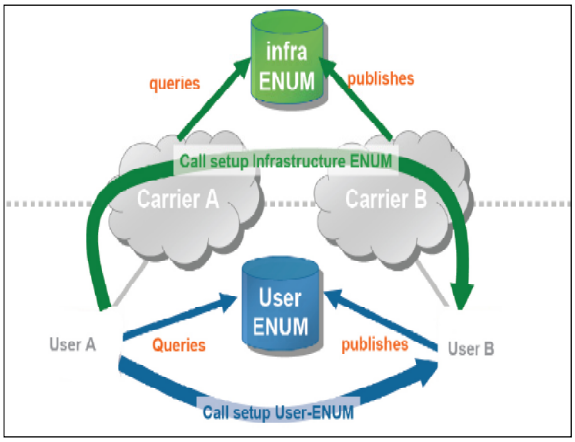

Figure 1. Call handling – User ENUM and I-ENUM

It is proposed that an organisation selected by tender would manage the I-ENUM tier 1 root registry for the Australian government and make this registry available to VoIP service providers and tier 2 registrars. The tier 2 registrars may actually be a large proportion of the VoIP service providers. A review of the Australian VoIP service providers shows that some of the VoIP service providers act as tier 3 resellers of tier 2 VoIP service provider services.

Registrars would utilise the tier 1 registry to store records and may operate tier 2 registries that are linked to the tier 1 registry. The tier 2 registry may do daily or instantaneous updates to the records stored in the tier 1 registry.

Fig. 2 shows an overview of how information is stored and retrieved on request. In this research, the VoIP service providers and the tier 2 registrars are shown as one entity. To start with the tier 1 registry is empty, but is constantly fed with records by the tier 2 registrars. The tier 1 registry also holds the rendezvous points provided by the VoIP service providers, which are required to route VoIP calls between VoIP service providers.

Registrars, in the domain name world, have the authority on allocating domain names and Internet addresses, and hence represent their Internet service providers. ENUM domain delegations are carried out by the tier 1 registrar on behalf of the registrant. It would be the tier 2 registrars' responsibility to update the VoIP service provider rendezvous points regularly and to ensure customer information within the registry system is correct.

VI Analysis

The research analysis highlighted driving forces behind the uptake of VoIP and the need for a VoIP interconnection and peering solution.

The main incentive for consumers to shift to VoIP is cost savings. An example of typical costs for telephone, Internet, and VoIP is provided in Table 1 [6][7].

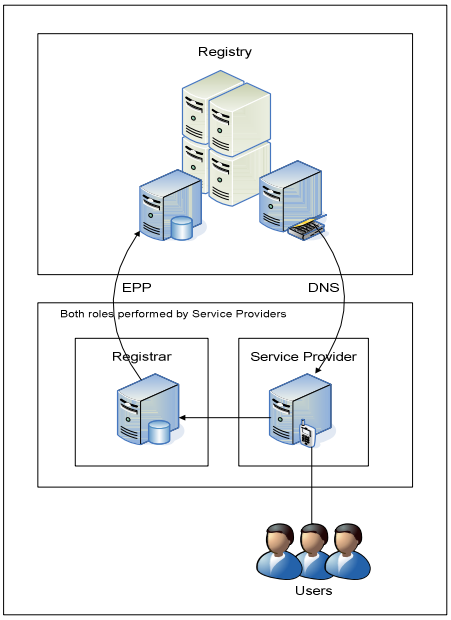

Figure 2. Proposed System Model

TABLE I. COST ANALYSIS OF PSTN AND VOIP IN AUSTRALIA

	PSTN	**VoIP**
Phone Line Rental	Up to $39.95 per month	NA
Internet Plan	Starting from $39.95 per month	Starting from $39.95 per month
Local	15c flat per call	10c flat per call
National	39c – Connection fee $2 maximum for up to 3 hrs	10c flat per call

International (Eg. India)	39c – Connection fee 25c per min	20c per min
Mobiles	39c – Connection fee 18.5c per 30secs	28c per min

As of June 2009, 8.4 million users have Internet access which includes about 1.09 million of them who still use dial-up [1]. Until recently, a phone line was needed for an Internet connection, but with the latest technological advancements, Internet access is now available without the need for an associated phone line. The ACMA's Communications Report 2008-09 [1], highlights that as of June 2009, 2.5 million users in Australia and approximately 20% of the SMEs are known to have access to VoIP. With the government's proposal of providing Fiber-to-the-Premises (FTTP) at economical prices over the next 10 years to 93% of the Australian population, consumers would be able to access an IP based network suitable for television, multimedia, Internet and VoIP. 3G mobile service take-up is continuing apace, with an estimated 12.8 million services as of June 2009, which is an increase of 44 per cent in 12 months. Increased 3G network coverage has also contributed to the increased take-up, with 99.06 percent of the population being covered as of June 2009 [1]. One of the 4G wireless network requirements is to combine telephony and data into a single IP based solution. As 4G wireless networks are rolled out, mobile customers will be utilizing VoIP on their mobile handsets.

An analysis of Australian government security and privacy requirements and possible I-ENUM implementation scenarios shows that I-ENUM implemented using private DNS that can only be accessed by VoIP service providers, is a satisfactory approach that should comply with security and privacy requirements. The use of secure EPP and firewalls limited to providing access to authorised organisations was found to be an important aspect of the solution.

Fig. 3 depicts how VoIP and PSTN are used as the modes by Communication Service Providers (CSP) in Australia. Many CSPs have altered their networks partially or completely from TDM to IP based technology. Calls that need to pass through another service provider's

network are routed either via TDM/IP gateways to the PSTN or border elements over the Internet. SIP is the protocol widely used by CSPs to setup, manage and terminate VoIP calls.

The evolution from the existing network, to the network that uses I-ENUM can be broadly divided into three steps.

A) Use of Private I-ENUM within a service provider's network – As shown in Fig. 4, the VoIP service providers would start using I-ENUM for VoIP call routing within their own network. The VoIP service providers set up their own DNS infrastructure and I-ENUM registry and populate the registry with client information. The database would consist of NAPTR RR records with information about internal destination points for end-users or PSTN routing information.

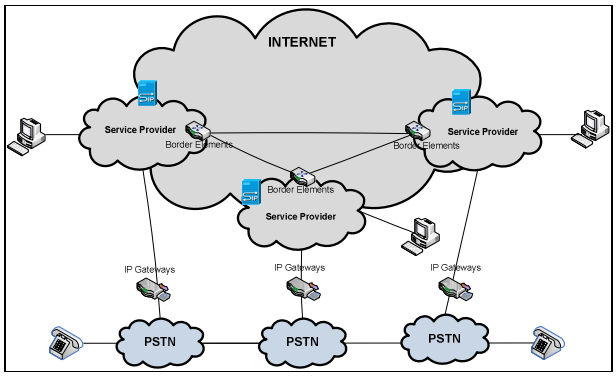

Figure 3. Communication using VoIP and PSTN in Australia

VoIP quality of service (QoS) has been a major concern for businesses and residential customers. Many VoIP service providers have realised the importance of improving VoIP QoS and have migrated their networks to IP-based networks with two or three grades of service. The shift away from having one "best effort" grade of service is seen to be a major step that must be taken to ensure that VoIP QoS is adequate for consumer confidence. Currently, however, the Australian carriers do not offer multiple grades of service to VoIP service providers unless there is a substantial increase in the fee paid for bandwidth. This additional cost forces most VoIP service providers to peer calls to external terminations through the PSTN. VoIP peering over IP networks would be the key to maintain cost effectiveness.

An increasing number of VoIP service providers are now offering an added incentive for a shift to a VoIP solution. VoIP-to-VoIP calls between consumers registered to the same VoIP service provider are being offered at low cost or no cost.

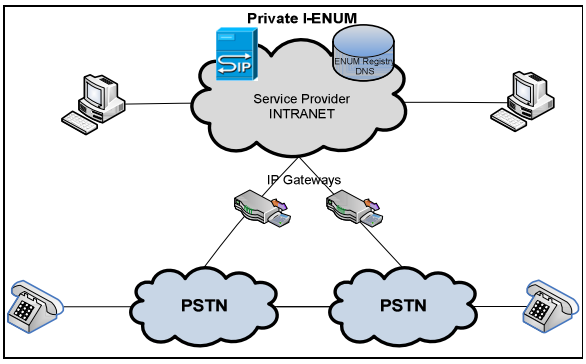

Figure 4. Private I-ENUM with SP's Network

As of June 2009, an estimated 287 VoIP service providers and 638 Internet service providers operate in Australia. Australian ISPs are offering a range of bundled voice and content services to consumers. Mobile revenue exceeded PSTN revenues for the first time in 2008-09, demonstrating a shift in consumer use and preference. ACMA's recent survey indicates that 81% of metropolitan consumers using VoIP are quite satisfied with the service and quality [1]. This increase in the number of consumers shifting to VoIP is due to the service providers offering diverse communication methods, like VoIP to PSTN, VoIP to VoIP, PSTN to VoIP and PSTN to PSTN.

With CSPs migrating to IP-based networks to offer better quality VoIP services and the existence of PSTN, making interconnection between PSTN and IP networks imperative. This is where I-ENUM would be the best bridging solution. The ENUM registry would hold the details of PSTN/IP gateways, thereby effectively routing calls within the SPs cloud and to other SPs either through PSTN or IP gateways. This would enable the SP to offer VoIP-VoIP calls at low or no cost for calls established and terminated within the cloud.

The ENUM registry / DNS would account for interconnection to the PSTN or VoIP peering using IP networks by publishing the routing details. Currently, a few service providers have implemented I-ENUM and have started offering ENUM services including User ENUM. The Internet user awareness of VoIP in June 2009 is shown in Fig. 5.

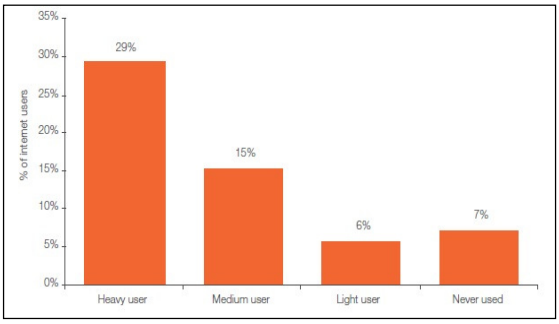

Figure 5. VoIP Usage at Home by Frequency of Internet Use [1]

B) Use of Private I-ENUM with IP based Interconnection - CSPs are moving away from single service provider model to bundled broadband model, integrating broadband internet access bundled with voice and data services [1]. This is beneficial if the CSPs migrate to IP-based networks and hence the need for IP-based interconnection. Using I-ENUM within their networks, CSPs can interconnect with other VoIP service providers over IP networks using border elements, in so doing eliminating the need for PSTN interconnection and the costs associated with it. However, if there are no IP-based points of interconnection, calls would still be routed to PSTN through PSTN/IP gateways. Each service provider has their own DNS and act as Registry and would have all the IP-based routing information, internal destination points and PSTN routing information. Private I-ENUM could be used to interconnect multiple service providers as shown in Fig. 6.

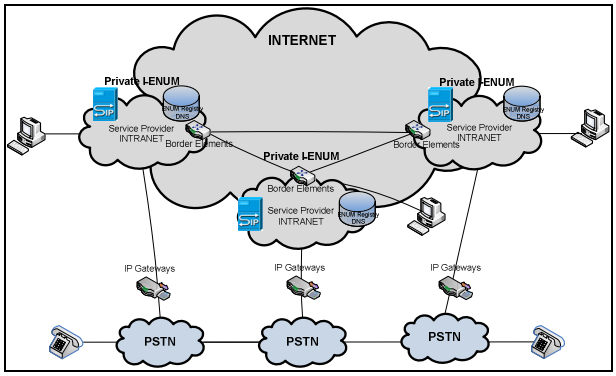

Figure 6. Private I-ENUM used by Multiple Service Providers

VoIP peering over IP networks would be the most cost efficient approach, however there is a time penalty and cost associated with establishing IP peering agreements with all of the other VoIP service providers. In some situations, this time penalty and cost can be reduced where VoIP service providers utilising the same carrier network are provided with a common

peering solution by the carrier and get assistance from the carrier with the technical aspects of the peering setup.

The Australian government plans to build a national high speed broadband network that delivers fast internet to 93% of all Australian homes and businesses with speeds of up to 100Mbps [12]. The network would cater for the needs of data, voice and video services using FTTH (Fibre to the Home) technology. This would mean that with faster internet speeds at their disposal, consumers are more likely to embrace the use of VoIP, and with increased bandwidth available throughout the network the VoIP QoS should improve.

A number of VoIP service providers showed interest during the Australia ENUM Trial to gain access to an Australian I-ENUM implementation [11]. Feedback during the ENUM trial and the subsequent I-ENUM trial highlighted that a number of private I-ENUM implementations already exist and that service providers were keen to work towards a unified I-ENUM hierarchy.

C) Global or Common Private I-ENUM – As the VoIP service provider community increases, the number of peering agreements in place over existing carrier networks or as the FTTP and associated wholesale backhaul network comes online, there is likely to be a greater impetus for an Australian I-ENUM registry that includes the use of a single tree for VoIP devices on IP networks. Another aspect of the need for a single I-ENUM registry is the increase in mobile IP based devices.

Single or a common shared I-ENUM registry / DNS on the Internet would permit and facilitate only participating VoIP SPs to store routing information required for interconnection. As shown in Fig. 7 [8], apart from the connections to the PSTN and other VoIP service providers, each VoIP service provider's intranet would have bilateral IP connections via border elements to the shared extranet. DNS within the VoIP service provider is still used to maintain the information required to route calls within their own network. If SP A queries a number hosted within the VoIP service provider's network the VoIP SIP server will talk and receive a response from the local I-ENUM database / DNS. Whereas for a query of a number not hosted on the VoIP service provider's network, the I-ENUM DNS passes the query to the shared extranet, thereby receiving the routing information to the terminating VoIP service provider.

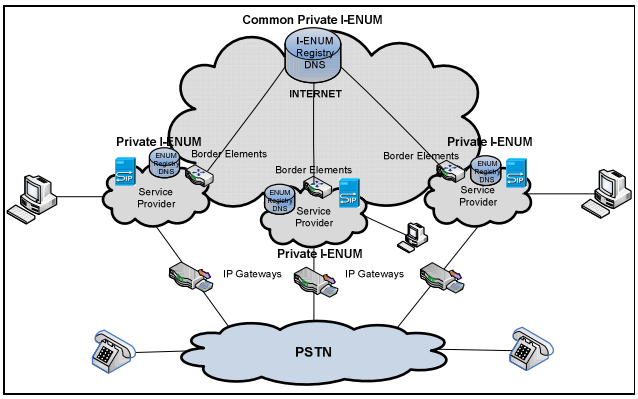

Figure 7. Shared Private I-ENUM structure in Australia

An Extranet, in this case, is a private network on the Internet, which allows connectivity to only registered VoIP service provider networks, thereby preventing general open access to the VoIP peering, call control and I-ENUM NAPTR RR records. The private I-ENUM databases within the VoIP service provider networks would become tier 2 registries and the external I-ENUM databases would become the tier 1 root registry and this would be used to populate private access DNS that is made available only to VoIP service providers on the extranet. With this step the opportunity exists for international VoIP service providers to register and gain access to the Australian I-ENUM DNS.

To route a call from SP A to SP B, there would be three possible queries. First SP A would query the internal private I- ENUM database to find the border gateway to the SP's shared extranet. The border gateway from SP A needs to query the SP-shared I-ENUM database DNS to find the address of the ingress border gateway of SP B, and the border gateway of SP B needs to query the internal private I-ENUM database DNS to finally find the AoR of the End-User for internal routing purposes.

It would be the responsibility of all VoIP service providers to register with the tier 1 I-ENUM registry operator and to manage their domains and associated information including associating user E.164 numbers to the appropriate border gateway IP address.

The evolution path described in this paper is for the present state of Australian telephony, where only a few tier 2 VoIP service providers are utilising I-ENUM on one or two smaller carrier networks. The proposed model contains all of the active numbers as entries for Tier 1/2, with pointers to the different tier name servers which contain the actual NAPTR RR records.

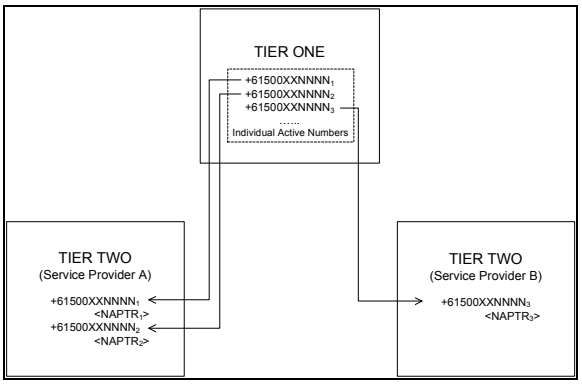

Figure 8. Tiered Architecture - Proposed

This use of a hierarchy of I-ENUM registries and DNS facilitates number portability, wherein the authoritative name server and associated VoIP service provider for each number could be entered into the tier 1 registry. When a number is ported from SP A to SP B, as in Fig. 8, the tier 1 registry operator has to confirm the number port by consulting with SP A and then notify SP B to update the information associated with the number including the routing information from SP B and the SP B's border gateway IP address. The tier 1 registry would be updated as new VoIP devices are installed and associated E.164 numbers are provisioned.

The step by step evolutionary model presented in this paper is recommended as it is unlikely that the current competitive market will opt to move to an Australian I-ENUM implementation in a single step.

If and when, embraced globally, User ENUM and I-ENUM utilising public and private DNS could be implemented using several approaches, however it is anticipated that this transition will take more than 10 years to occur.

Fig. 9, suggests a proposed global approach, where the public DNS is used as the common shared database, hosting the routing information for different VoIP service providers that host one or more domain names or country trees.

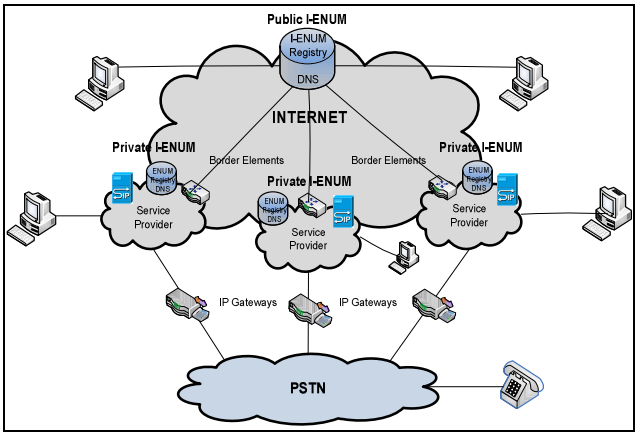

Figure 9. I-ENUM in Public DNS (Option 1)

Fig. 10, for example, shows an alternative to the proposed approach for I-ENUM utilising public DNS. Consider, for example, Australia and New Zealand using I-ENUM with private DNS, forming a regional private I-ENUM island The proposal is to link the regional private I-ENUM DNS to a single common global public I-ENUM DNS that contains border gateway information for domains or domain trees. Any user could query the public DNS, which would have routing information for the shared private I-ENUM extranet border gateways.

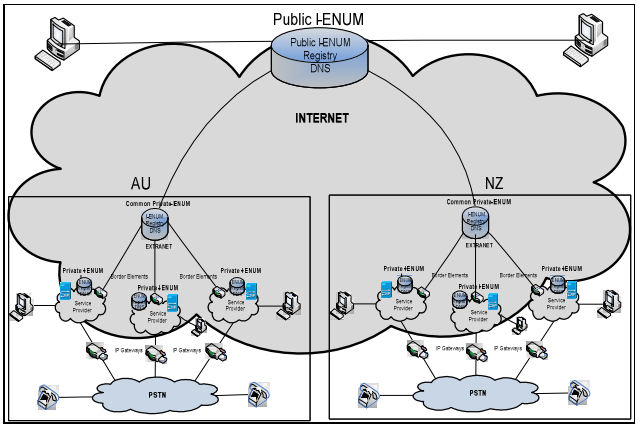

Figure 10. I-ENUM in Public DNS (Option 2)

Before finalising a global I-ENUM solution more research is needed into the management and control of a global I-ENUM system and how the information that is stored within the I-ENUM system may be governed and protected from unwarranted access so as to ensure security and privacy may be achieved in accordance with a nations laws.

VII Conclusion

The research presented in this paper includes an analysis of the current state of VoIP usage in Australia and the steps necessary for an Australian I-ENUM in Australia. The Australian telephony market is changing due to changes in technology and the implementation of FTTP and 4G mobile networks over the next 5 years.

REFERENCES

1. AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY. 2009, 'ACMA COMMUNICATIONS REPORT 2008-09' [ONLINE] AVAILABLE AT: HTTP://WWW.ACMA.GOV.AU/WEB/STANDARD/PC=PC_311972
2. FALTSTROM, P. 2000, 'E.164 NUMBER AND DNS', RFC 2916, [ONLINE] AVAILABLE AT: HTTP://TOOLS.IETF.ORG/HTML/RFC2916
3. ACMA, 'AUSTRALIAN ENUM WORKING GROUP', [ONLINE] AVAILABLE AT: HTTP://WWW.ACMA.GOV.AU/WEB/STANDARD/PC=PC_2475
4. MARIS, LENNART & NOOREN, PIETER. 2007, 'OPEN AND CLOSED MODELS FOR INFRASTRUCTURE ENUM IN THE NETHERLANDS', RIPE 55 ENUM WORKING GROUP, [ONLINE] AVAILABLE AT: HTTP://WWW.RIPE.NET/RIPE/MEETINGS/RIPE-55/PRESENTATIONS/NOOREN-OPEN-CLOSED-MODELS-ENUM.PDF
5. HUSTON, GEOFF 2007, 'INFRASTRUCTURE ENUM', [ONLINE] AVAILABLE AT: HTTP://WWW.CIRCLEID.COM/POSTS/INFRASTRUCTURE_ENUM/
6. TPG, [ONLINE] AVAILABLE AT: HTTP://TPG.COM.AU/VOIP/
7. TELSTRA, 'HOME PHONES AND PLANS', [ONLINE] AVAILABLE AT: HTTP://WWW.TELSTRA.COM.AU/HOMEPHONE/PLANS/COMPARE_AND_ORDER_A_PLAN.HTML
8. ETSI, 'INFRASTRUCTURE ENUM', [ONLINE] AVAILABLE AT: HTTP://ENUM.NIC.AT/DOCUMENTS/ETSI/DRAFTS/05TD143R4%20DRAFT%20TR_102055V008.PDF
9. INSTRA CORPORATION, 'ENUM TRIAL INFORMATION', [ONLINE] AVAILABLE AT: HTTP://WWW.ENUMREGISTRY.COM/ENUM/TRIAL.HTM
10. AEDG INFRASTRUCTURE ENUM WORKING GROUP. 2009, 'REPORT ON INFRASTRUCTURE ENUM TRIAL', [ONLINE] AVAILABLE AT: HTTP://ACMA.GOV.AU/WEBWR/_ASSETS/MAIN/LIB100996/IENUM_TRIAL_REPORT.PDF
11. AUSTRALIAN ENUM WORKING GROUP. 2007, 'EVALUATION OF THE AUSTRALIAN ENUM TRIAL', [ONLINE] AVAILABLE AT: HTTP://WWW.ENUM.COM.AU/PDF/AEDG%20TRIAL%20EVALUATION%20REPORT%20NOV%202007.PDF
12. DEPARTMENT OF BROADBAND, COMMUNICATIONS AND THE DIGITAL ECONOMY. 2010, 'NATIONAL BROADBAND NETWORK', [ONLINE} AVAILABLE AT: HTTP://WWW.DBCDE.GOV.AU/BROADBAND/NATIONAL_BROADBAND_NETWORK

Appendix G

Appendix G starts on the next page

No. Time Source Destination Protocol Info
1 0.000000 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=52

Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: p2pcommunity (3955), Seq: 1, Ack: 1, Len: 52
SSH Protocol

No. Time Source Destination Protocol Info
2 0.028175 203.176.187.10 202.168.56.131 TCP p2pcommunity > ssh [ACK] Seq=1 Ack=53 Win=64667 Len=0

Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: p2pcommunity (3955), Dst Port: ssh (22), Seq: 1, Ack: 53, Len: 0

No. Time Source Destination Protocol Info
3 1.896490 Cisco_54:9e:92 Spanning-tree-(for-bridges)_00 STP Conf. Root = 32768/10/00:1e:bd:54:9e:80 Cost = 0 Port = 0x8012

Frame 3: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
IEEE 802.3 Ethernet
Logical-Link Control
Spanning Tree Protocol

No. Time Source Destination Protocol Info
4 2.667170 203.176.187.10 202.168.56.131 SIP/SDP Request: INVITE sip:61399244429@202.168.56.131, with session description

Frame 4: 979 bytes on wire (7832 bits), 979 bytes captured (7832 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol

No. Time Source Destination Protocol Info
5 2.668272 202.168.56.131 203.176.187.10 SIP Status: 100 Trying

Frame 5: 510 bytes on wire (4080 bits), 510 bytes captured (4080 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol

No. Time Source Destination Protocol Info
6 2.669524 202.168.56.131 203.176.187.10 SIP Status: 180 Ringing

Frame 6: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol

No. Time Source Destination Protocol Info
7 2.669708 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=60

Frame 7: 114 bytes on wire (912 bits), 114 bytes captured (912 bits)

Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 1, Ack: 1, Len: 60
SSH Protocol

No. Time Source Destination Protocol Info
8 2.669851 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=92

Frame 8: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 61, Ack: 1, Len: 92
SSH Protocol

No. Time Source Destination Protocol Info
9 2.669969 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=84

Frame 9: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 153, Ack: 1, Len: 84
SSH Protocol

No. Time Source Destination Protocol Info
10 2.670275 202.168.56.131 131.170.68.108 DNS Standard query NAPTR 9.2.4.4.4.2.9.9.3.1.6.auenum.com.au

Frame 10: 95 bytes on wire (760 bits), 95 bytes captured (760 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 131.170.68.108 (131.170.68.108)
User Datagram Protocol, Src Port: 53441 (53441), Dst Port: domain (53)
Domain Name System (query)

No. Time Source Destination Protocol Info
11 2.698901 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=1 Ack=153 Win=65219 Len=0

Frame 11: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 1, Ack: 153, Len: 0

No. Time Source Destination Protocol Info
12 2.698924 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=620

Frame 12: 674 bytes on wire (5392 bits), 674 bytes captured (5392 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 237, Ack: 1, Len: 620
SSH Protocol

No. Time Source Destination Protocol Info
13 2.707022 131.170.68.108 202.168.56.131 DNS Standard query response NAPTR 10 105 u

Frame 13: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)

Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 131.170.68.108 (131.170.68.108), Dst: 202.168.56.131 (202.168.56.131)
User Datagram Protocol, Src Port: domain (53), Dst Port: 53441 (53441)
Domain Name System (response)

No. Time Source Destination Protocol Info
14 2.707178 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=44

Frame 14: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 857, Ack: 1, Len: 44
SSH Protocol

No. Time Source Destination Protocol Info
15 2.707255 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=44

Frame 15: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 901, Ack: 1, Len: 44
SSH Protocol

No. Time Source Destination Protocol Info
16 2.707813 202.168.56.131 131.170.68.108 DNS Standard query NAPTR 203.153.192.10

Frame 16: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 131.170.68.108 (131.170.68.108)
User Datagram Protocol, Src Port: 53441 (53441), Dst Port: domain (53)
Domain Name System (query)

No. Time Source Destination Protocol Info
17 2.728010 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=1 Ack=857 Win=64515 Len=0

Frame 17: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 1, Ack: 857, Len: 0

No. Time Source Destination Protocol Info
18 2.728028 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=364

Frame 18: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 945, Ack: 1, Len: 364
SSH Protocol

No. Time Source Destination Protocol Info
19 2.729509 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=36

Frame 19: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)

Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 1, Ack: 857, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info
20 2.729520 202.168.56.131 203.176.187.10 TCP ssh > msr-plugin-port [ACK] Seq=1309 Ack=37 Win=13104 Len=0

Frame 20: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 1309, Ack: 37, Len: 0

No. Time Source Destination Protocol Info
21 2.738882 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=36

Frame 21: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 37, Ack: 901, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info
22 2.738897 202.168.56.131 203.176.187.10 TCP ssh > msr-plugin-port [ACK] Seq=1309 Ack=73 Win=13104 Len=0

Frame 22: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 1309, Ack: 73, Len: 0

No. Time Source Destination Protocol Info
23 2.744750 131.170.68.108 202.168.56.131 DNS Standard query response

Frame 23: 285 bytes on wire (2280 bits), 285 bytes captured (2280 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 131.170.68.108 (131.170.68.108), Dst: 202.168.56.131 (202.168.56.131)
User Datagram Protocol, Src Port: domain (53), Dst Port: 53441 (53441)
Domain Name System (response)

No. Time Source Destination Protocol Info
24 2.744815 202.168.56.131 131.170.68.108 DNS Standard query NAPTR 203.153.192.10.dryb.mel.comvergence.com.au

Frame 24: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 131.170.68.108 (131.170.68.108)
User Datagram Protocol, Src Port: 53441 (53441), Dst Port: domain (53)
Domain Name System (query)

No. Time Source Destination Protocol Info
25 2.760492 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=73 Ack=1309 Win=65535 Len=0

Frame 25: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)

Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 73, Ack: 1309, Len: 0

No. Time Source Destination Protocol Info
26 2.767113 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=36

Frame 26: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 73, Ack: 1309, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info
27 2.767122 202.168.56.131 203.176.187.10 TCP ssh > msr-plugin-port [ACK] Seq=1309 Ack=109 Win=13104 Len=0

Frame 27: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 1309, Ack: 109, Len: 0

No. Time Source Destination Protocol Info
28 2.782228 131.170.68.108 202.168.56.131 DNS Standard query response

Frame 28: 313 bytes on wire (2504 bits), 313 bytes captured (2504 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 131.170.68.108 (131.170.68.108), Dst: 202.168.56.131 (202.168.56.131)
User Datagram Protocol, Src Port: domain (53), Dst Port: 53441 (53441)
Domain Name System (response)

No. Time Source Destination Protocol Info
29 2.782373 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=44

Frame 29: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 1309, Ack: 109, Len: 44
SSH Protocol

No. Time Source Destination Protocol Info
30 2.782458 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=52

Frame 30: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 1353, Ack: 109, Len: 52
SSH Protocol

No. Time Source Destination Protocol Info
31 2.782564 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=68

Frame 31: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)

Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 1405, Ack: 109, Len: 68
SSH Protocol

No. Time Source Destination Protocol Info
32 2.782670 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=68

Frame 32: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 1473, Ack: 109, Len: 68
SSH Protocol

No. Time Source Destination Protocol Info
33 2.783141 202.168.56.131 203.153.192.10 SIP/SDP Request: INVITE sip:61399244429@203.153.192.10, with session description

Frame 33: 1119 bytes on wire (8952 bits), 1119 bytes captured (8952 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.153.192.10 (203.153.192.10)
User Datagram Protocol, Src Port: sip-tls (5061), Dst Port: sip (5060)
Session Initiation Protocol

No. Time Source Destination Protocol Info
34 2.812837 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=109 Ack=1405 Win=65439 Len=0

Frame 34: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 109, Ack: 1405, Len: 0

No. Time Source Destination Protocol Info
35 2.812892 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=556

Frame 35: 610 bytes on wire (4880 bits), 610 bytes captured (4880 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 1541, Ack: 109, Len: 556
SSH Protocol

No. Time Source Destination Protocol Info
36 2.813711 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=109 Ack=1541 Win=65303 Len=0

Frame 36: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 109, Ack: 1541, Len: 0

No. Time Source Destination Protocol Info
37 2.844443 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=36

Frame 37: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)

Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 109, Ack: 2097, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info
38 2.884472 202.168.56.131 203.176.187.10 TCP ssh > msr-plugin-port [ACK] Seq=2097 Ack=145 Win=13104 Len=0

Frame 38: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 2097, Ack: 145, Len: 0

No. Time Source Destination Protocol Info
39 2.913903 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=36

Frame 39: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 145, Ack: 2097, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info
40 2.913936 202.168.56.131 203.176.187.10 TCP ssh > msr-plugin-port [ACK] Seq=2097 Ack=181 Win=13104 Len=0

Frame 40: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 2097, Ack: 181, Len: 0

No. Time Source Destination Protocol Info
41 2.991110 203.153.192.10 202.168.56.131 SIP Status: 100 Trying

Frame 41: 496 bytes on wire (3968 bits), 496 bytes captured (3968 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.153.192.10 (203.153.192.10), Dst: 202.168.56.131 (202.168.56.131)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip-tls (5061)
Session Initiation Protocol

No. Time Source Destination Protocol Info
42 2.991241 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=52

Frame 42: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 2097, Ack: 181, Len: 52
SSH Protocol

No. Time Source Destination Protocol Info
43 2.991316 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=68

Frame 43: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)

Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 2149, Ack: 181, Len: 68
SSH Protocol

No. Time Source Destination Protocol Info
44 2.991407 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=100

Frame 44: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 2217, Ack: 181, Len: 100
SSH Protocol

No. Time Source Destination Protocol Info
45 2.991501 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=84

Frame 45: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 2317, Ack: 181, Len: 84
SSH Protocol

No. Time Source Destination Protocol Info
46 3.021217 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=181 Ack=2317 Win=64527 Len=0

Frame 46: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 181, Ack: 2317, Len: 0

No. Time Source Destination Protocol Info
47 3.021233 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=360

Frame 47: 414 bytes on wire (3312 bits), 414 bytes captured (3312 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 2401, Ack: 181, Len: 360
SSH Protocol

No. Time Source Destination Protocol Info
48 3.049951 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=181 Ack=2761 Win=65535 Len=0

Frame 48: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 181, Ack: 2761, Len: 0

No. Time Source Destination Protocol Info
49 3.050950 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=36

Frame 49: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)

Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 181, Ack: 2761, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info
50 3.050980 202.168.56.131 203.176.187.10 TCP ssh > msr-plugin-port [ACK] Seq=2761 Ack=217 Win=13104 Len=0

Frame 50: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 2761, Ack: 217, Len: 0

No. Time Source Destination Protocol Info
51 3.119662 203.153.192.10 202.168.56.131 SIP Status: 180 Ringing

Frame 51: 825 bytes on wire (6600 bits), 825 bytes captured (6600 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.153.192.10 (203.153.192.10), Dst: 202.168.56.131 (202.168.56.131)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip-tls (5061)
Session Initiation Protocol

No. Time Source Destination Protocol Info
52 3.119778 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=44

Frame 52: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 2761, Ack: 217, Len: 44
SSH Protocol

No. Time Source Destination Protocol Info
53 3.119867 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=76

Frame 53: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 2805, Ack: 217, Len: 76
SSH Protocol

No. Time Source Destination Protocol Info
54 3.119965 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=100

Frame 54: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 2881, Ack: 217, Len: 100
SSH Protocol

No. Time Source Destination Protocol Info
55 3.120062 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=100

Frame 55: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 2981, Ack: 217, Len: 100
SSH Protocol

No. Time Source Destination Protocol Info
56 3.120230 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=228

Frame 56: 282 bytes on wire (2256 bits), 282 bytes captured (2256 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 3081, Ack: 217, Len: 228
SSH Protocol

No. Time Source Destination Protocol Info
57 3.148770 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=217 Ack=2881 Win=65415 Len=0

Frame 57: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 217, Ack: 2881, Len: 0

No. Time Source Destination Protocol Info
58 3.148787 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=208

Frame 58: 262 bytes on wire (2096 bits), 262 bytes captured (2096 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 3309, Ack: 217, Len: 208
SSH Protocol

No. Time Source Destination Protocol Info
59 3.149394 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=217 Ack=3081 Win=65215 Len=0

Frame 59: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 217, Ack: 3081, Len: 0

No. Time Source Destination Protocol Info
60 3.151393 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=36

Frame 60: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 217, Ack: 3081, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info
61 3.151424 202.168.56.131 203.176.187.10 TCP ssh > msr-plugin-port [ACK] Seq=3517 Ack=253 Win=13104 Len=0

Frame 61: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 3517, Ack: 253, Len: 0

No. Time Source Destination Protocol Info
62 3.178128 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=36

Frame 62: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 253, Ack: 3517, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info
63 3.178160 202.168.56.131 203.176.187.10 TCP ssh > msr-plugin-port [ACK] Seq=3517 Ack=289 Win=13104 Len=0

Frame 63: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 3517, Ack: 289, Len: 0

No. Time Source Destination Protocol Info
64 3.269806 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=52

Frame 64: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 3517, Ack: 289, Len: 52
SSH Protocol

No. Time Source Destination Protocol Info
65 3.490200 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=289 Ack=3569 Win=64727 Len=0

Frame 65: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 289, Ack: 3569, Len: 0

No. Time Source Destination Protocol Info
66 3.609381 Dell_7b:ae:9c Broadcast ARP Who has 202.168.56.139? Tell 202.168.56.129

Frame 66: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

No. Time Source Destination Protocol Info
67 3.897094 Cisco_54:9e:92 Spanning-tree-(for-bridges)_00 STP Conf. Root = 32768/10/00:1e:bd:54:9e:80 Cost = 0 Port = 0x8012

Frame 67: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
IEEE 802.3 Ethernet
Logical-Link Control
Spanning Tree Protocol

No. Time Source Destination Protocol Info
68 3.899592 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=44

Frame 68: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 289, Ack: 3569, Len: 44
SSH Protocol

No. Time Source Destination Protocol Info
69 3.899607 202.168.56.131 203.176.187.10 TCP ssh > msr-plugin-port [ACK] Seq=3569 Ack=333 Win=13104 Len=0

Frame 69: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 3569, Ack: 333, Len: 0

No. Time Source Destination Protocol Info
70 4.262135 203.176.187.10 202.168.56.131 SIP Request: CANCEL sip:61399244429@202.168.56.131

Frame 70: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol

No. Time Source Destination Protocol Info
71 4.262236 202.168.56.131 203.176.187.10 SIP Status: 487 Request Terminated

Frame 71: 494 bytes on wire (3952 bits), 494 bytes captured (3952 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol

No. Time Source Destination Protocol Info
72 4.262272 202.168.56.131 203.176.187.10 SIP Status: 200 OK

Frame 72: 521 bytes on wire (4168 bits), 521 bytes captured (4168 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol

No. Time Source Destination Protocol Info
73 4.263149 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=60

Frame 73: 114 bytes on wire (912 bits), 114 bytes captured (912 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 3569, Ack: 333, Len: 60
SSH Protocol

No. Time Source Destination Protocol Info

74 4.263257 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=76

Frame 74: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 3629, Ack: 333, Len: 76
SSH Protocol

No. Time Source Destination Protocol Info
75 4.263352 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=92

Frame 75: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 3705, Ack: 333, Len: 92
SSH Protocol

No. Time Source Destination Protocol Info
76 4.263539 202.168.56.131 131.170.68.108 DNS Standard query NAPTR 9.2.4.4.4.2.9.9.3.1.6.auenum.com.au

Frame 76: 95 bytes on wire (760 bits), 95 bytes captured (760 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 131.170.68.108 (131.170.68.108)
User Datagram Protocol, Src Port: 53441 (53441), Dst Port: domain (53)
Domain Name System (query)

No. Time Source Destination Protocol Info

77 4.291994 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=333 Ack=3705 Win=64591 Len=0

Frame 77: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 333, Ack: 3705, Len: 0

No. Time Source Destination Protocol Info
78 4.292022 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=244

Frame 78: 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 3797, Ack: 333, Len: 244
SSH Protocol

No. Time Source Destination Protocol Info
79 4.293367 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=36

Frame 79: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 333, Ack: 3797, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info

80 4.293380 202.168.56.131 203.176.187.10 TCP ssh > msr-plugin-port [ACK] Seq=4041 Ack=369 Win=13104 Len=0

Frame 80: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 4041, Ack: 369, Len: 0

No. Time Source Destination Protocol Info
81 4.301737 131.170.68.108 202.168.56.131 DNS Standard query response NAPTR 10 105 u

Frame 81: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 131.170.68.108 (131.170.68.108), Dst: 202.168.56.131 (202.168.56.131)
User Datagram Protocol, Src Port: domain (53), Dst Port: 53441 (53441)
Domain Name System (response)

No. Time Source Destination Protocol Info
82 4.301902 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=44

Frame 82: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 4041, Ack: 369, Len: 44
SSH Protocol

No. Time Source Destination Protocol Info
83 4.301969 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=44

Frame 83: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 4085, Ack: 369, Len: 44
SSH Protocol

No. Time Source Destination Protocol Info
84 4.302050 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=52

Frame 84: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 4129, Ack: 369, Len: 52
SSH Protocol

No. Time Source Destination Protocol Info
85 4.302402 202.168.56.131 131.170.68.108 DNS Standard query NAPTR 203.153.192.10

Frame 85: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 131.170.68.108 (131.170.68.108)
User Datagram Protocol, Src Port: 53441 (53441), Dst Port: domain (53)
Domain Name System (query)

No. Time Source Destination Protocol Info

86 4.303883 203.176.187.10 202.168.56.131 SIP Request: ACK sip:61399244429@202.168.56.131

Frame 86: 459 bytes on wire (3672 bits), 459 bytes captured (3672 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol

No. Time Source Destination Protocol Info
87 4.322975 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=36

Frame 87: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 369, Ack: 4041, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info
88 4.322994 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=276

Frame 88: 330 bytes on wire (2640 bits), 330 bytes captured (2640 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 4181, Ack: 405, Len: 276
SSH Protocol

No. Time Source Destination Protocol Info
89 4.330596 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=405 Ack=4181 Win=65535 Len=0

Frame 89: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 405, Ack: 4181, Len: 0

No. Time Source Destination Protocol Info
90 4.340090 131.170.68.108 202.168.56.131 DNS Standard query response

Frame 90: 285 bytes on wire (2280 bits), 285 bytes captured (2280 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 131.170.68.108 (131.170.68.108), Dst: 202.168.56.131 (202.168.56.131)
User Datagram Protocol, Src Port: domain (53), Dst Port: 53441 (53441)
Domain Name System (response)

No. Time Source Destination Protocol Info
91 4.340150 202.168.56.131 131.170.68.108 DNS Standard query NAPTR 203.153.192.10.dryb.mel.comvergence.com.au

Frame 91: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 131.170.68.108 (131.170.68.108)
User Datagram Protocol, Src Port: 53441 (53441), Dst Port: domain (53)
Domain Name System (query)

No. Time Source Destination Protocol Info
92 4.353832 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=36

Frame 92: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 405, Ack: 4457, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info
93 4.377444 131.170.68.108 202.168.56.131 DNS
Standard query response

Frame 93: 313 bytes on wire (2504 bits), 313 bytes captured (2504 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 131.170.68.108 (131.170.68.108), Dst: 202.168.56.131 (202.168.56.131)
User Datagram Protocol, Src Port: domain (53), Dst Port: 53441 (53441)
Domain Name System (response)

No. Time Source Destination Protocol Info
94 4.377572 202.168.56.131 203.176.187.10 SSH
Encrypted response packet len=44

Frame 94: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 4457, Ack: 441, Len: 44
SSH Protocol

No. Time Source Destination Protocol Info
95 4.377642 202.168.56.131 203.176.187.10 SSH
Encrypted response packet len=52

Frame 95: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 4501, Ack: 441, Len: 52
SSH Protocol

No. Time Source Destination Protocol Info
96 4.377722 202.168.56.131 203.176.187.10 SSH
Encrypted response packet len=76

Frame 96: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 4553, Ack: 441, Len: 76
SSH Protocol

No. Time Source Destination Protocol Info
97 4.377800 202.168.56.131 203.176.187.10 SSH
Encrypted response packet len=60

Frame 97: 114 bytes on wire (912 bits), 114 bytes captured (912 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 4629, Ack: 441, Len: 60
SSH Protocol

No. Time Source Destination Protocol Info

98 4.378209 202.168.56.131 203.153.192.10 SIP Request: CANCEL sip:61399244429@203.153.192.10

Frame 98: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.153.192.10 (203.153.192.10)
User Datagram Protocol, Src Port: sip-tls (5061), Dst Port: sip (5060)
Session Initiation Protocol

No. Time Source Destination Protocol Info
99 4.407052 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=441 Ack=4629 Win=65087 Len=0

Frame 99: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 441, Ack: 4629, Len: 0

No. Time Source Destination Protocol Info
100 4.407072 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=720

Frame 100: 774 bytes on wire (6192 bits), 774 bytes captured (6192 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 4689, Ack: 441, Len: 720
SSH Protocol

No. Time Source Destination Protocol Info
101 4.408551 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=36

Frame 101: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 441, Ack: 4689, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info
102 4.448466 202.168.56.131 203.176.187.10 TCP ssh > msr-plugin-port [ACK] Seq=5409 Ack=477 Win=13104 Len=0

Frame 102: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 5409, Ack: 477, Len: 0

No. Time Source Destination Protocol Info
103 4.479136 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=36

Frame 103: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 477, Ack: 5409, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info

104 4.479165 202.168.56.131 203.176.187.10 TCP ssh > msr-plugin-port [ACK] Seq=5409 Ack=513 Win=13104 Len=0

Frame 104: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 5409, Ack: 513, Len: 0

No. Time Source Destination Protocol Info
105 4.576830 203.153.192.10 202.168.56.131 SIP Status: 200 OK

Frame 105: 360 bytes on wire (2880 bits), 360 bytes captured (2880 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.153.192.10 (203.153.192.10), Dst: 202.168.56.131 (202.168.56.131)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip-tls (5061)
Session Initiation Protocol

No. Time Source Destination Protocol Info
106 4.576966 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=44

Frame 106: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 5409, Ack: 513, Len: 44
SSH Protocol

No. Time Source Destination Protocol Info
107 4.577053 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=68

Frame 107: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 5453, Ack: 513, Len: 68
SSH Protocol

No. Time Source Destination Protocol Info
108 4.577148 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=68

Frame 108: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 5521, Ack: 513, Len: 68
SSH Protocol

No. Time Source Destination Protocol Info
109 4.577251 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=76

Frame 109: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 5589, Ack: 513, Len: 76
SSH Protocol

No. Time Source Destination Protocol Info
110 4.577456 203.153.192.10 202.168.56.131 SIP Status: 487 Request Cancelled

Frame 110: 548 bytes on wire (4384 bits), 548 bytes captured (4384 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.153.192.10 (203.153.192.10), Dst: 202.168.56.131 (202.168.56.131)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip-tls (5061)
Session Initiation Protocol

No. Time Source Destination Protocol Info
111 4.577934 202.168.56.131 203.153.192.10 SIP Request: ACK sip:61399244429@203.153.192.10

Frame 111: 424 bytes on wire (3392 bits), 424 bytes captured (3392 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.153.192.10 (203.153.192.10)
User Datagram Protocol, Src Port: sip-tls (5061), Dst Port: sip (5060)
Session Initiation Protocol

No. Time Source Destination Protocol Info
112 4.605939 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=513 Ack=5521 Win=64195 Len=0

Frame 112: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 513, Ack: 5521, Len: 0

No. Time Source Destination Protocol Info
113 4.605960 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=1412

Frame 113: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 5665, Ack: 513, Len: 1412
SSH Protocol

No. Time Source Destination Protocol Info
114 4.605968 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=484

Frame 114: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 7077, Ack: 513, Len: 484
SSH Protocol

No. Time Source Destination Protocol Info
115 4.606813 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=513 Ack=5665 Win=65535 Len=0

Frame 115: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 513, Ack: 5665, Len: 0

No. Time Source Destination Protocol Info
116 4.609312 Dell_7b:ae:9c Broadcast ARP Who has 202.168.56.139? Tell 202.168.56.129

Frame 116: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

No. Time Source Destination Protocol Info
117 4.637296 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=513 Ack=7561 Win=65535 Len=0

Frame 117: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 513, Ack: 7561, Len: 0

No. Time Source Destination Protocol Info
118 4.639544 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=36

Frame 118: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 513, Ack: 7561, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info
119 4.639578 202.168.56.131 203.176.187.10 TCP ssh > msr-plugin-port [ACK] Seq=7561 Ack=549 Win=13104 Len=0

Frame 119: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 7561, Ack: 549, Len: 0

No. Time Source Destination Protocol Info
120 4.669402 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=144

Frame 120: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 549, Ack: 7561, Len: 144
SSH Protocol

No. Time Source Destination Protocol Info
121 4.669430 202.168.56.131 203.176.187.10 TCP ssh > msr-plugin-port [ACK] Seq=7561 Ack=693 Win=13104 Len=0

Frame 121: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 7561, Ack: 693, Len: 0

No. Time Source Destination Protocol Info
122 4.763350 Dell_7b:ae:9c Dell_b0:3b:61 ARP Who has 202.168.56.131? Tell 202.168.56.129

Frame 122: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Address Resolution Protocol (request)

No. Time Source Destination Protocol Info
123 4.763356 Dell_b0:3b:61 Dell_7b:ae:9c ARP 202.168.56.131 is at 00:14:22:b0:3b:61

Frame 123: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Address Resolution Protocol (reply)

No. Time Source Destination Protocol Info
124 4.870868 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=60

Frame 124: 114 bytes on wire (912 bits), 114 bytes captured (912 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 7561, Ack: 693, Len: 60
SSH Protocol

No. Time Source Destination Protocol Info
125 4.978726 Cisco_54:9e:92 Cisco_54:9e:92 LOOP Reply

Frame 125: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Cisco_54:9e:92 (00:1e:bd:54:9e:92), Dst: Cisco_54:9e:92 (00:1e:bd:54:9e:92)
Configuration Test Protocol (loopback)
Data (40 bytes)

0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0020 00 00 00 00 00 00 00 00 ....

No. Time Source Destination Protocol Info
126 5.070841 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=44

Frame 126: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 7621, Ack: 693, Len: 44
SSH Protocol

No. Time Source Destination Protocol Info
127 5.099781 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=693 Ack=7665 Win=65431 Len=0

Frame 127: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 693, Ack: 7665, Len: 0

No. Time Source Destination Protocol Info
128 5.263601 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=44

Frame 128: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 7665, Ack: 693, Len: 44
SSH Protocol

No. Time Source Destination Protocol Info
129 5.263675 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=60

Frame 129: 114 bytes on wire (912 bits), 114 bytes captured (912 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 7709, Ack: 693, Len: 60
SSH Protocol

No. Time Source Destination Protocol Info
130 5.264049 202.168.56.131 131.170.68.108 DNS Standard query NAPTR 9.2.4.4.4.2.9.9.3.1.6.auenum.com.au

Frame 130: 95 bytes on wire (760 bits), 95 bytes captured (760 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 131.170.68.108 (131.170.68.108)
User Datagram Protocol, Src Port: 53441 (53441), Dst Port: domain (53)
Domain Name System (query)

No. Time Source Destination Protocol Info
131 5.291423 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=693 Ack=7769 Win=65327 Len=0

Frame 131: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 693, Ack: 7769, Len: 0

No. Time Source Destination Protocol Info
132 5.291440 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=348

Frame 132: 402 bytes on wire (3216 bits), 402 bytes captured (3216 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 7769, Ack: 693, Len: 348
SSH Protocol

No. Time Source Destination Protocol Info
133 5.302292 131.170.68.108 202.168.56.131 DNS Standard query response NAPTR 10 105 u

Frame 133: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 131.170.68.108 (131.170.68.108), Dst: 202.168.56.131 (202.168.56.131)
User Datagram Protocol, Src Port: domain (53), Dst Port: 53441 (53441)
Domain Name System (response)

No. Time Source Destination Protocol Info
134 5.302420 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=44

Frame 134: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 8117, Ack: 693, Len: 44
SSH Protocol

No. Time Source Destination Protocol Info
135 5.302479 202.168.56.131 203.176.187.10 SSH
Encrypted response packet len=44

Frame 135: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 8161, Ack: 693, Len: 44
SSH Protocol

No. Time Source Destination Protocol Info
136 5.302964 202.168.56.131 131.170.68.108 DNS
Standard query NAPTR 203.153.192.10

Frame 136: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 131.170.68.108 (131.170.68.108)
User Datagram Protocol, Src Port: 53441 (53441), Dst Port: domain (53)
Domain Name System (query)

No. Time Source Destination Protocol Info
137 5.322904 203.176.187.10 202.168.56.131 SSH
Encrypted request packet len=36

Frame 137: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 693, Ack: 8117, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info
138 5.322923 202.168.56.131 203.176.187.10 SSH
Encrypted response packet len=372

Frame 138: 426 bytes on wire (3408 bits), 426 bytes captured (3408 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 8205, Ack: 729, Len: 372
SSH Protocol

No. Time Source Destination Protocol Info
139 5.331150 203.176.187.10 202.168.56.131 SSH
Encrypted request packet len=36

Frame 139: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 729, Ack: 8161, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info
140 5.343143 131.170.68.108 202.168.56.131 DNS
Standard query response

Frame 140: 285 bytes on wire (2280 bits), 285 bytes captured (2280 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 131.170.68.108 (131.170.68.108), Dst: 202.168.56.131 (202.168.56.131)
User Datagram Protocol, Src Port: domain (53), Dst Port: 53441 (53441)
Domain Name System (response)

No. Time Source Destination Protocol Info
141 5.343195 202.168.56.131 131.170.68.108 DNS Standard query NAPTR 203.153.192.10.dryb.mel.comvergence.com.au

Frame 141: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 131.170.68.108 (131.170.68.108)
User Datagram Protocol, Src Port: 53441 (53441), Dst Port: domain (53)
Domain Name System (query)

No. Time Source Destination Protocol Info
142 5.352638 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=765 Ack=8577 Win=64519 Len=0

Frame 142: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 765, Ack: 8577, Len: 0

No. Time Source Destination Protocol Info
143 5.376469 202.168.56.131 203.176.187.10 TCP ssh > msr-plugin-port [ACK] Seq=8577 Ack=765 Win=13104 Len=0

Frame 143: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 8577, Ack: 765, Len: 0

No. Time Source Destination Protocol Info
144 5.379497 131.170.68.108 202.168.56.131 DNS Standard query response

Frame 144: 313 bytes on wire (2504 bits), 313 bytes captured (2504 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 131.170.68.108 (131.170.68.108), Dst: 202.168.56.131 (202.168.56.131)
User Datagram Protocol, Src Port: domain (53), Dst Port: 53441 (53441)
Domain Name System (response)

No. Time Source Destination Protocol Info
145 5.379620 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=52

Frame 145: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 8577, Ack: 765, Len: 52
SSH Protocol

No. Time Source Destination Protocol Info
146 5.379685 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=52

Frame 146: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 8629, Ack: 765, Len: 52
SSH Protocol

No. Time Source Destination Protocol Info

147 5.379774 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=84

Frame 147: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 8681, Ack: 765, Len: 84
SSH Protocol

No. Time Source Destination Protocol Info
148 5.379840 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=60

Frame 148: 114 bytes on wire (912 bits), 114 bytes captured (912 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 8765, Ack: 765, Len: 60
SSH Protocol

No. Time Source Destination Protocol Info
149 5.405482 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=36

Frame 149: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 765, Ack: 8577, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info
150 5.405500 202.168.56.131 203.176.187.10 TCP ssh > msr-plugin-port [ACK] Seq=8825 Ack=801 Win=13104 Len=0

Frame 150: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 8825, Ack: 801, Len: 0

No. Time Source Destination Protocol Info
151 5.407981 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=801 Ack=8765 Win=64331 Len=0

Frame 151: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 801, Ack: 8765, Len: 0

No. Time Source Destination Protocol Info
152 5.407996 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=292

Frame 152: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 8825, Ack: 801, Len: 292
SSH Protocol

No. Time Source Destination Protocol Info

153 5.434466 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=36

Frame 153: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 801, Ack: 8825, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info
154 5.438214 124.177.83.182 202.168.56.131 TCP 35345 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2 SACK_PERM=1

Frame 154: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 124.177.83.182 (124.177.83.182), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: 35345 (35345), Dst Port: http (80), Seq: 0, Len: 0

No. Time Source Destination Protocol Info
155 5.438241 202.168.56.131 124.177.83.182 TCP http > 35345 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=2

Frame 155: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 124.177.83.182 (124.177.83.182)
Transmission Control Protocol, Src Port: http (80), Dst Port: 35345 (35345), Seq: 0, Ack: 1, Len: 0

No. Time Source Destination Protocol Info
156 5.477816 124.177.83.182 202.168.56.131 TCP 35345 > http [ACK] Seq=1 Ack=1 Win=65700 Len=0

Frame 156: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 124.177.83.182 (124.177.83.182), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: 35345 (35345), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0

No. Time Source Destination Protocol Info
157 5.483482 202.168.56.131 203.176.187.10 TCP ssh > msr-plugin-port [ACK] Seq=9117 Ack=837 Win=13104 Len=0

Frame 157: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 9117, Ack: 837, Len: 0

No. Time Source Destination Protocol Info
158 5.511672 124.177.83.182 202.168.56.131 HTTP GET /index.php?action=extensionlist HTTP/1.1

Frame 158: 940 bytes on wire (7520 bits), 940 bytes captured (7520 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 124.177.83.182 (124.177.83.182), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: 35345 (35345), Dst Port: http (80), Seq: 1, Ack: 1, Len: 886
Hypertext Transfer Protocol

No. Time Source Destination Protocol Info

159 5.511686 202.168.56.131 124.177.83.182 TCP http > 35345 [ACK] Seq=1 Ack=887 Win=7612 Len=0

Frame 159: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 124.177.83.182 (124.177.83.182)
Transmission Control Protocol, Src Port: http (80), Dst Port: 35345 (35345), Seq: 1, Ack: 887, Len: 0

No. Time Source Destination Protocol Info
160 5.520287 202.168.56.131 202.168.56.132 TCP 46483 > mysql [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSV=2737322190 TSER=0 WS=2

Frame 160: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 0, Len: 0

No. Time Source Destination Protocol Info
161 5.520421 202.168.56.132 202.168.56.131 TCP mysql > 46483 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=1 TSV=3442885165 TSER=2737322190 SACK_PERM=1

Frame 161: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 0, Ack: 1, Len: 0

No. Time Source Destination Protocol Info
162 5.520446 202.168.56.131 202.168.56.132 TCP 46483 > mysql [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=2737322190 TSER=3442885165

Frame 162: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 1, Ack: 1, Len: 0

No. Time Source Destination Protocol Info
163 5.520792 202.168.56.132 202.168.56.131 MySQL Server Greeting proto=10 version=5.0.45-log

Frame 163: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 1, Ack: 1, Len: 60
MySQL Protocol

No. Time Source Destination Protocol Info
164 5.520807 202.168.56.131 202.168.56.132 TCP 46483 > mysql [ACK] Seq=1 Ack=61 Win=5840 Len=0 TSV=2737322191 TSER=3442885165

Frame 164: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 1, Ack: 61, Len: 0

No. Time Source Destination Protocol Info
165 5.520860 202.168.56.131 202.168.56.132 MySQL Login Request user=shabby

Frame 165: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 1, Ack: 61, Len: 64
MySQL Protocol

No. Time Source Destination Protocol Info
166 5.521042 202.168.56.132 202.168.56.131 MySQL Response OK

Frame 166: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 61, Ack: 65, Len: 11
MySQL Protocol

No. Time Source Destination Protocol Info
167 5.521125 202.168.56.131 202.168.56.132 MySQL Request Use Database

Frame 167: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 65, Ack: 72, Len: 18
MySQL Protocol

No. Time Source Destination Protocol Info
168 5.521293 202.168.56.132 202.168.56.131 MySQL Response OK

Frame 168: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 72, Ack: 83, Len: 11
MySQL Protocol

No. Time Source Destination Protocol Info
169 5.521347 202.168.56.131 202.168.56.132 MySQL Request Query

Frame 169: 119 bytes on wire (952 bits), 119 bytes captured (952 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 83, Ack: 83, Len: 53
MySQL Protocol

No. Time Source Destination Protocol Info
170 5.522166 202.168.56.132 202.168.56.131 MySQL Response TABULAR

Frame 170: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)

Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 83, Ack: 136, Len: 1448
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info
171 5.522291 202.168.56.132 202.168.56.131 MySQL Response

Frame 171: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 1531, Ack: 136, Len: 1448
[Reassembled TCP Segments (85 bytes): #170(14), #171(71)]
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info
172 5.522309 202.168.56.131 202.168.56.132 TCP 46483 > mysql [ACK] Seq=136 Ack=2979 Win=11632 Len=0 TSV=2737322192 TSER=3442885166

Frame 172: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 136, Ack: 2979, Len: 0

No. Time Source Destination Protocol Info
173 5.522417 202.168.56.132 202.168.56.131 MySQL Response

Frame 173: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 2979, Ack: 136, Len: 1448
[Reassembled TCP Segments (89 bytes): #171(19), #173(70)]
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info
174 5.522543 202.168.56.132 202.168.56.131 MySQL Response

Frame 174: 1314 bytes on wire (10512 bits), 1314 bytes captured (10512 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 4427, Ack: 136, Len: 1248
[Reassembled TCP Segments (286 bytes): #173(189), #174(97)]
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info
175 5.522559 202.168.56.131 202.168.56.132 TCP 46483 > mysql [ACK] Seq=136 Ack=5675 Win=17424 Len=0 TSV=2737322192 TSER=3442885166

Frame 175: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 136, Ack: 5675, Len: 0

No. Time Source Destination Protocol Info
176 5.522706 202.168.56.131 202.168.56.132 MySQL Request Query

Frame 176: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 136, Ack: 5675, Len: 99
MySQL Protocol

No. Time Source Destination Protocol Info
177 5.523041 202.168.56.132 202.168.56.131 MySQL Response

Frame 177: 604 bytes on wire (4832 bits), 604 bytes captured (4832 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)

Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 5675, Ack: 235, Len: 538
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info
178 5.523193 202.168.56.131 202.168.56.132 MySQL Request Query

Frame 178: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 235, Ack: 6213, Len: 99
MySQL Protocol

No. Time Source Destination Protocol Info
179 5.523540 202.168.56.132 202.168.56.131 MySQL Response

Frame 179: 638 bytes on wire (5104 bits), 638 bytes captured (5104 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 6213, Ack: 334, Len: 572
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info
180 5.523647 202.168.56.131 202.168.56.132 MySQL Request Use Database

Frame 180: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 334, Ack: 6785, Len: 14
MySQL Protocol

No. Time Source Destination Protocol Info
181 5.523791 202.168.56.132 202.168.56.131 MySQL Response OK

Frame 181: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 6785, Ack: 348, Len: 11
MySQL Protocol

No. Time Source Destination Protocol Info
182 5.523840 202.168.56.131 202.168.56.132 MySQL Request Query

Frame 182: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 348, Ack: 6796, Len: 65
MySQL Protocol

No. Time Source Destination Protocol Info
183 5.524290 202.168.56.132 202.168.56.131 MySQL Response

Frame 183: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 6796, Ack: 413, Len: 106
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info
184 5.524376 202.168.56.131 202.168.56.132 MySQL Request Use Database

Frame 184: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 413, Ack: 6902, Len: 18
MySQL Protocol

No. Time Source Destination Protocol Info
185 5.524541 202.168.56.132 202.168.56.131 MySQL Response OK

Frame 185: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 6902, Ack: 431, Len: 11
MySQL Protocol

No. Time Source Destination Protocol Info
186 5.524599 202.168.56.131 202.168.56.132 MySQL Request Query

Frame 186: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 431, Ack: 6913, Len: 84
MySQL Protocol

No. Time Source Destination Protocol Info
187 5.525289 202.168.56.132 202.168.56.131 MySQL Response

Frame 187: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)

Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 6913, Ack: 515, Len: 1448
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info
188 5.525298 202.168.56.132 202.168.56.131 MySQL Response

Frame 188: 121 bytes on wire (968 bits), 121 bytes captured (968 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 8361, Ack: 515, Len: 55
[Reassembled TCP Segments (182 bytes): #187(136), #188(46)]
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info
189 5.525311 202.168.56.131 202.168.56.132 TCP 46483 > mysql [ACK] Seq=515 Ack=8416 Win=20320 Len=0 TSV=2737322195 TSER=3442885170

Frame 189: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 515, Ack: 8416, Len: 0

No. Time Source Destination Protocol Info
190 5.525473 202.168.56.131 202.168.56.132 MySQL Request Query

Frame 190: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 515, Ack: 8416, Len: 87
MySQL Protocol

No. Time Source Destination Protocol Info
191 5.526164 202.168.56.132 202.168.56.131 MySQL Response

Frame 191: 1387 bytes on wire (11096 bits), 1387 bytes captured (11096 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 8416, Ack: 602, Len: 1321
MySQL Protocol

MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info
192 5.526382 202.168.56.131 202.168.56.132 MySQL Request Query

Frame 192: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 602, Ack: 9737, Len: 99
MySQL Protocol

No. Time Source Destination Protocol Info
193 5.526664 202.168.56.132 202.168.56.131 MySQL Response

Frame 193: 638 bytes on wire (5104 bits), 638 bytes captured (5104 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 9737, Ack: 701, Len: 572
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info
194 5.526788 202.168.56.131 202.168.56.132 MySQL Request Use Database

Frame 194: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 701, Ack: 10309, Len: 14
MySQL Protocol

No. Time Source Destination Protocol Info
195 5.527038 202.168.56.132 202.168.56.131 MySQL Response OK

Frame 195: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)

Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 10309, Ack: 715, Len: 11
MySQL Protocol

No. Time Source Destination Protocol Info
196 5.527086 202.168.56.131 202.168.56.132 MySQL Request Query

Frame 196: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 715, Ack: 10320, Len: 65
MySQL Protocol

No. Time Source Destination Protocol Info
197 5.527413 202.168.56.132 202.168.56.131 MySQL Response

Frame 197: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 10320, Ack: 780, Len: 106
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info
198 5.527489 202.168.56.131 202.168.56.132 MySQL Request Use Database

Frame 198: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 780, Ack: 10426, Len: 18
MySQL Protocol

No. Time Source Destination Protocol Info
199 5.527664 202.168.56.132 202.168.56.131 MySQL Response OK

Frame 199: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 10426, Ack: 798, Len: 11
MySQL Protocol

No. Time Source Destination Protocol Info
200 5.527717 202.168.56.131 202.168.56.132 MySQL Request Query

Frame 200: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 798, Ack: 10437, Len: 84
MySQL Protocol

No. Time Source Destination Protocol Info
201 5.528413 202.168.56.132 202.168.56.131 MySQL Response

Frame 201: 1387 bytes on wire (11096 bits), 1387 bytes captured (11096 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 10437, Ack: 882, Len: 1321
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info
202 5.528549 202.168.56.131 202.168.56.132 MySQL Request Query

Frame 202: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 882, Ack: 11758, Len: 87
MySQL Protocol

No. Time Source Destination Protocol Info
203 5.529287 202.168.56.132 202.168.56.131 MySQL Response

Frame 203: 1387 bytes on wire (11096 bits), 1387 bytes captured (11096 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 11758, Ack: 969, Len: 1321
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info

204 5.529483 202.168.56.131 202.168.56.132 MySQL Request Query

Frame 204: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 969, Ack: 13079, Len: 99
MySQL Protocol

No. Time Source Destination Protocol Info
205 5.529787 202.168.56.132 202.168.56.131 MySQL Response

Frame 205: 638 bytes on wire (5104 bits), 638 bytes captured (5104 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 13079, Ack: 1068, Len: 572
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info
206 5.529903 202.168.56.131 202.168.56.132 MySQL Request Use Database

Frame 206: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 1068, Ack: 13651, Len: 14
MySQL Protocol

No. Time Source Destination Protocol Info
207 5.530038 202.168.56.132 202.168.56.131 MySQL Response OK

Frame 207: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 13651, Ack: 1082, Len: 11
MySQL Protocol

No. Time Source Destination Protocol Info
208 5.530085 202.168.56.131 202.168.56.132 MySQL Request Query

Frame 208: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 1082, Ack: 13662, Len: 65
MySQL Protocol

No. Time Source Destination Protocol Info
209 5.530411 202.168.56.132 202.168.56.131 MySQL Response

Frame 209: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 13662, Ack: 1147, Len: 106
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info
210 5.530486 202.168.56.131 202.168.56.132 MySQL Request Use Database

Frame 210: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 1147, Ack: 13768, Len: 18
MySQL Protocol

No. Time Source Destination Protocol Info
211 5.530662 202.168.56.132 202.168.56.131 MySQL Response OK

Frame 211: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 13768, Ack: 1165, Len: 11
MySQL Protocol

No. Time Source Destination Protocol Info
212 5.530715 202.168.56.131 202.168.56.132 MySQL Request Query

Frame 212: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 1165, Ack: 13779, Len: 84
MySQL Protocol

No. Time Source Destination Protocol Info
213 5.531411 202.168.56.132 202.168.56.131 MySQL Response

Frame 213: 1387 bytes on wire (11096 bits), 1387 bytes captured (11096 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 13779, Ack: 1249, Len: 1321
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol

MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info
214 5.531546 202.168.56.131 202.168.56.132 MySQL Request Query

Frame 214: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 1249, Ack: 15100, Len: 87
MySQL Protocol

No. Time Source Destination Protocol Info
215 5.532285 202.168.56.132 202.168.56.131 MySQL Response

Frame 215: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 15100, Ack: 1336, Len: 1448
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info
216 5.532293 202.168.56.132 202.168.56.131 MySQL Response

Frame 216: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 16548, Ack: 1336, Len: 65
[Reassembled TCP Segments (192 bytes): #215(136), #216(56)]
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info
217 5.532306 202.168.56.131 202.168.56.132 TCP 46483 > mysql [ACK] Seq=1336 Ack=16613 Win=34292 Len=0 TSV=2737322202 TSER=3442885177

Frame 217: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)

Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 1336, Ack: 16613, Len: 0

No. Time Source Destination Protocol Info
218 5.532539 202.168.56.131 202.168.56.132 MySQL Request Query

Frame 218: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 1336, Ack: 16613, Len: 99
MySQL Protocol

No. Time Source Destination Protocol Info
219 5.532784 202.168.56.132 202.168.56.131 MySQL Response

Frame 219: 604 bytes on wire (4832 bits), 604 bytes captured (4832 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 16613, Ack: 1435, Len: 538
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info
220 5.532935 202.168.56.131 202.168.56.132 MySQL Request Query

Frame 220: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 1435, Ack: 17151, Len: 99
MySQL Protocol

No. Time Source Destination Protocol Info
221 5.533284 202.168.56.132 202.168.56.131 MySQL Response

Frame 221: 638 bytes on wire (5104 bits), 638 bytes captured (5104 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 17151, Ack: 1534, Len: 572
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info
222 5.533380 202.168.56.131 202.168.56.132 MySQL Request Use Database

Frame 222: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 1534, Ack: 17723, Len: 14
MySQL Protocol

No. Time Source Destination Protocol Info
223 5.533659 202.168.56.132 202.168.56.131 MySQL Response OK

Frame 223: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 17723, Ack: 1548, Len: 11
MySQL Protocol

No. Time Source Destination Protocol Info
224 5.533707 202.168.56.131 202.168.56.132 MySQL Request Query

Frame 224: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 1548, Ack: 17734, Len: 65
MySQL Protocol

No. Time Source Destination Protocol Info
225 5.534034 202.168.56.132 202.168.56.131 MySQL Response

Frame 225: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 17734, Ack: 1613, Len: 90
MySQL Protocol
MySQL Protocol
MySQL Protocol
MySQL Protocol

No. Time Source Destination Protocol Info
226 5.534114 202.168.56.131 202.168.56.132 MySQL Request Use Database

Frame 226: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 1613, Ack: 17824, Len: 18
MySQL Protocol

No. Time Source Destination Protocol Info
227 5.534285 202.168.56.132 202.168.56.131 MySQL Response OK

Frame 227: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 17824, Ack: 1631, Len: 11
MySQL Protocol

No. Time Source Destination Protocol Info
228 5.534967 202.168.56.131 202.168.56.132 MySQL Request Quit

Frame 228: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 1631, Ack: 17835, Len: 5
MySQL Protocol

No. Time Source Destination Protocol Info
229 5.534985 202.168.56.131 202.168.56.132 TCP 46483 > mysql [FIN, ACK] Seq=1636 Ack=17835 Win=34292 Len=0 TSV=2737322205 TSER=3442885179

Frame 229: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 1636, Ack: 17835, Len: 0

No. Time Source Destination Protocol Info
230 5.535136 202.168.56.131 124.177.83.182 TCP [TCP segment of a reassembled PDU]

Frame 230: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 124.177.83.182 (124.177.83.182)
Transmission Control Protocol, Src Port: http (80), Dst Port: 35345 (35345), Seq: 1, Ack: 887, Len: 1460

No. Time Source Destination Protocol Info
231 5.535152 202.168.56.131 124.177.83.182 TCP [TCP segment of a reassembled PDU]

Frame 231: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 124.177.83.182 (124.177.83.182)
Transmission Control Protocol, Src Port: http (80), Dst Port: 35345 (35345), Seq: 1461, Ack: 887, Len: 1460

No. Time Source Destination Protocol Info
232 5.535167 202.168.56.132 202.168.56.131 TCP mysql > 46483 [ACK] Seq=17835 Ack=1637 Win=66602 Len=0 TSV=3442885180 TSER=2737322205

Frame 232: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 17835, Ack: 1637, Len: 0

No. Time Source Destination Protocol Info
233 5.535189 202.168.56.132 202.168.56.131 TCP mysql > 46483 [FIN, ACK] Seq=17835 Ack=1637 Win=66602 Len=0 TSV=3442885180 TSER=2737322205

Frame 233: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Dell_64:ba:67 (00:1d:09:64:ba:67), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)

Internet Protocol, Src: 202.168.56.132 (202.168.56.132), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 46483 (46483), Seq: 17835, Ack: 1637, Len: 0

No. Time Source Destination Protocol Info
234 5.535207 202.168.56.131 202.168.56.132 TCP 46483 > mysql [ACK] Seq=1637 Ack=17836 Win=34292 Len=0 TSV=2737322205 TSER=3442885180

Frame 234: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:ba:67 (00:1d:09:64:ba:67)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.132 (202.168.56.132)
Transmission Control Protocol, Src Port: 46483 (46483), Dst Port: mysql (3306), Seq: 1637, Ack: 17836, Len: 0

No. Time Source Destination Protocol Info
235 5.535239 202.168.56.131 124.177.83.182 HTTP HTTP/1.1 200 OK (text/html)

Frame 235: 1056 bytes on wire (8448 bits), 1056 bytes captured (8448 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 124.177.83.182 (124.177.83.182)
Transmission Control Protocol, Src Port: http (80), Dst Port: 35345 (35345), Seq: 2921, Ack: 887, Len: 1002
[Reassembled TCP Segments (3922 bytes): #230(1460), #231(1460), #235(1002)]
Hypertext Transfer Protocol
Line-based text data: text/html

No. Time Source Destination Protocol Info
236 5.552524 202.168.56.133 202.168.56.131 SIP/SDP Request: INVITE sip:619999361390011581@202.168.56.131:5060, with session description

Frame 236: 1208 bytes on wire (9664 bits), 1208 bytes captured (9664 bits)
Ethernet II, Src: Dell_64:b6:fc (00:1d:09:64:b6:fc), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 202.168.56.133 (202.168.56.133), Dst: 202.168.56.131 (202.168.56.131)
User Datagram Protocol, Src Port: sip-tls (5061), Dst Port: sip (5060)
Session Initiation Protocol

No. Time Source Destination Protocol Info
237 5.553485 202.168.56.131 202.168.56.133 SIP Status: 100 Trying

Frame 237: 594 bytes on wire (4752 bits), 594 bytes captured (4752 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:b6:fc (00:1d:09:64:b6:fc)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.133 (202.168.56.133)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip-tls (5061)
Session Initiation Protocol

No. Time Source Destination Protocol Info
238 5.553803 202.168.56.131 202.168.56.133 SIP Status: 180 Ringing

Frame 238: 610 bytes on wire (4880 bits), 610 bytes captured (4880 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_64:b6:fc (00:1d:09:64:b6:fc)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 202.168.56.133 (202.168.56.133)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip-tls (5061)
Session Initiation Protocol

No. Time Source Destination Protocol Info
239 5.592251 124.177.83.182 202.168.56.131 TCP 35345 > http [ACK] Seq=887 Ack=2921 Win=65700 Len=0

Frame 239: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 124.177.83.182 (124.177.83.182), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: 35345 (35345), Dst Port: http (80), Seq: 887, Ack: 2921, Len: 0

No. Time Source Destination Protocol Info
240 5.598747 124.177.83.182 202.168.56.131 TCP 35345 > http [ACK] Seq=887 Ack=3924 Win=64696 Len=0

Frame 240: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 124.177.83.182 (124.177.83.182), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: 35345 (35345), Dst Port: http (80), Seq: 887, Ack: 3924, Len: 0

No. Time Source Destination Protocol Info
241 5.603120 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=837 Ack=9117 Win=65535 Len=0

Frame 241: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 837, Ack: 9117, Len: 0

No. Time Source Destination Protocol Info
242 5.609367 Dell_7b:ae:9c Broadcast ARP Who has 202.168.56.139? Tell 202.168.56.129

Frame 242: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

No. Time Source Destination Protocol Info
243 5.625482 124.177.83.182 202.168.56.131 TCP 35345 > http [FIN, ACK] Seq=887 Ack=3924 Win=64696 Len=0

Frame 243: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 124.177.83.182 (124.177.83.182), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: 35345 (35345), Dst Port: http (80), Seq: 887, Ack: 3924, Len: 0

No. Time Source Destination Protocol Info
244 5.625497 202.168.56.131 124.177.83.182 TCP http > 35345 [ACK] Seq=3924 Ack=888 Win=7612 Len=0

Frame 244: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 124.177.83.182 (124.177.83.182)
Transmission Control Protocol, Src Port: http (80), Dst Port: 35345 (35345), Seq: 3924, Ack: 888, Len: 0

No. Time Source Destination Protocol Info
245 5.628480 124.177.83.182 202.168.56.131 TCP 35346 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2 SACK_PERM=1

Frame 245: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 124.177.83.182 (124.177.83.182), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: 35346 (35346), Dst Port: http (80), Seq: 0, Len: 0

No. Time Source Destination Protocol Info
246 5.628511 202.168.56.131 124.177.83.182 TCP http > 35346 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=2

Frame 246: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 124.177.83.182 (124.177.83.182)
Transmission Control Protocol, Src Port: http (80), Dst Port: 35346 (35346), Seq: 0, Ack: 1, Len: 0

No. Time Source Destination Protocol Info
247 5.631978 124.177.83.182 202.168.56.131 TCP 35347 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2 SACK_PERM=1

Frame 247: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 124.177.83.182 (124.177.83.182), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: 35347 (35347), Dst Port: http (80), Seq: 0, Len: 0

No. Time Source Destination Protocol Info
248 5.631994 202.168.56.131 124.177.83.182 TCP http > 35347 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=2

Frame 248: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 124.177.83.182 (124.177.83.182)
Transmission Control Protocol, Src Port: http (80), Dst Port: 35347 (35347), Seq: 0, Ack: 1, Len: 0

No. Time Source Destination Protocol Info
249 5.666708 124.177.83.182 202.168.56.131 TCP 35346 > http [ACK] Seq=1 Ack=1 Win=65700 Len=0

Frame 249: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 124.177.83.182 (124.177.83.182), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: 35346 (35346), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0

No. Time Source Destination Protocol Info
250 5.670081 124.177.83.182 202.168.56.131 TCP 35347 > http [ACK] Seq=1 Ack=1 Win=65700 Len=0

Frame 250: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 124.177.83.182 (124.177.83.182), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: 35347 (35347), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0

No. Time Source Destination Protocol Info
251 5.700315 124.177.83.182 202.168.56.131 HTTP GET /blue.gif HTTP/1.1

Frame 251: 787 bytes on wire (6296 bits), 787 bytes captured (6296 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 124.177.83.182 (124.177.83.182), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: 35347 (35347), Dst Port: http (80), Seq: 1, Ack: 1, Len: 733
Hypertext Transfer Protocol

No. Time Source Destination Protocol Info

252 5.700329 202.168.56.131 124.177.83.182 TCP http > 35347 [ACK] Seq=1 Ack=734 Win=7308 Len=0

Frame 252: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 124.177.83.182 (124.177.83.182)
Transmission Control Protocol, Src Port: http (80), Dst Port: 35347 (35347), Seq: 1, Ack: 734, Len: 0

No. Time Source Destination Protocol Info
253 5.700611 202.168.56.131 124.177.83.182 HTTP HTTP/1.1 304 Not Modified

Frame 253: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 124.177.83.182 (124.177.83.182)
Transmission Control Protocol, Src Port: http (80), Dst Port: 35347 (35347), Seq: 1, Ack: 734, Len: 145
Hypertext Transfer Protocol

No. Time Source Destination Protocol Info
254 5.700665 202.168.56.131 124.177.83.182 TCP http > 35347 [FIN, ACK] Seq=146 Ack=734 Win=7308 Len=0

Frame 254: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 124.177.83.182 (124.177.83.182)
Transmission Control Protocol, Src Port: http (80), Dst Port: 35347 (35347), Seq: 146, Ack: 734, Len: 0

No. Time Source Destination Protocol Info
255 5.728299 124.177.83.182 202.168.56.131 HTTP GET /red.gif HTTP/1.1

Frame 255: 787 bytes on wire (6296 bits), 787 bytes captured (6296 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 124.177.83.182 (124.177.83.182), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: 35346 (35346), Dst Port: http (80), Seq: 1, Ack: 1, Len: 733
Hypertext Transfer Protocol

No. Time Source Destination Protocol Info
256 5.728314 202.168.56.131 124.177.83.182 TCP http > 35346 [ACK] Seq=1 Ack=734 Win=7308 Len=0

Frame 256: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 124.177.83.182 (124.177.83.182)
Transmission Control Protocol, Src Port: http (80), Dst Port: 35346 (35346), Seq: 1, Ack: 734, Len: 0

No. Time Source Destination Protocol Info
257 5.728560 202.168.56.131 124.177.83.182 HTTP HTTP/1.1 304 Not Modified

Frame 257: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 124.177.83.182 (124.177.83.182)
Transmission Control Protocol, Src Port: http (80), Dst Port: 35346 (35346), Seq: 1, Ack: 734, Len: 146
Hypertext Transfer Protocol

No. Time Source Destination Protocol Info

258 5.728618 202.168.56.131 124.177.83.182 TCP http > 35346 [FIN, ACK] Seq=147 Ack=734 Win=7308 Len=0

Frame 258: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 124.177.83.182 (124.177.83.182)
Transmission Control Protocol, Src Port: http (80), Dst Port: 35346 (35346), Seq: 147, Ack: 734, Len: 0

No. Time Source Destination Protocol Info
259 5.742665 124.177.83.182 202.168.56.131 TCP 35347 > http [FIN, ACK] Seq=734 Ack=146 Win=65552 Len=0

Frame 259: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 124.177.83.182 (124.177.83.182), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: 35347 (35347), Dst Port: http (80), Seq: 734, Ack: 146, Len: 0

No. Time Source Destination Protocol Info
260 5.742678 202.168.56.131 124.177.83.182 TCP http > 35347 [ACK] Seq=147 Ack=735 Win=7308 Len=0

Frame 260: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 124.177.83.182 (124.177.83.182)
Transmission Control Protocol, Src Port: http (80), Dst Port: 35347 (35347), Seq: 147, Ack: 735, Len: 0

No. Time Source Destination Protocol Info
261 5.746413 124.177.83.182 202.168.56.131 TCP 35348 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2 SACK_PERM=1

Frame 261: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 124.177.83.182 (124.177.83.182), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: 35348 (35348), Dst Port: http (80), Seq: 0, Len: 0

No. Time Source Destination Protocol Info
262 5.746432 202.168.56.131 124.177.83.182 TCP http > 35348 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=2

Frame 262: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 124.177.83.182 (124.177.83.182)
Transmission Control Protocol, Src Port: http (80), Dst Port: 35348 (35348), Seq: 0, Ack: 1, Len: 0

No. Time Source Destination Protocol Info
263 5.749537 124.177.83.182 202.168.56.131 TCP 35347 > http [ACK] Seq=735 Ack=147 Win=65552 Len=0

Frame 263: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 124.177.83.182 (124.177.83.182), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: 35347 (35347), Dst Port: http (80), Seq: 735, Ack: 147, Len: 0

No. Time Source Destination Protocol Info
264 5.776022 124.177.83.182 202.168.56.131 TCP 35346 > http [ACK] Seq=734 Ack=148 Win=65552 Len=0

Frame 264: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 124.177.83.182 (124.177.83.182), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: 35346 (35346), Dst Port: http (80), Seq: 734, Ack: 148, Len: 0

No. Time Source Destination Protocol Info
265 5.779020 124.177.83.182 202.168.56.131 TCP 35346 > http [FIN, ACK] Seq=734 Ack=148 Win=65552 Len=0

Frame 265: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 124.177.83.182 (124.177.83.182), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: 35346 (35346), Dst Port: http (80), Seq: 734, Ack: 148, Len: 0

No. Time Source Destination Protocol Info
266 5.779030 202.168.56.131 124.177.83.182 TCP http > 35346 [ACK] Seq=148 Ack=735 Win=7308 Len=0

Frame 266: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 124.177.83.182 (124.177.83.182)
Transmission Control Protocol, Src Port: http (80), Dst Port: 35346 (35346), Seq: 148, Ack: 735, Len: 0

No. Time Source Destination Protocol Info
267 5.786016 124.177.83.182 202.168.56.131 TCP 35348 > http [ACK] Seq=1 Ack=1 Win=65700 Len=0

Frame 267: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 124.177.83.182 (124.177.83.182), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: 35348 (35348), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0

No. Time Source Destination Protocol Info
268 5.814624 124.177.83.182 202.168.56.131 HTTP GET /grey.gif HTTP/1.1

Frame 268: 787 bytes on wire (6296 bits), 787 bytes captured (6296 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 124.177.83.182 (124.177.83.182), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: 35348 (35348), Dst Port: http (80), Seq: 1, Ack: 1, Len: 733
Hypertext Transfer Protocol

No. Time Source Destination Protocol Info
269 5.814639 202.168.56.131 124.177.83.182 TCP http > 35348 [ACK] Seq=1 Ack=734 Win=7308 Len=0

Frame 269: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 124.177.83.182 (124.177.83.182)
Transmission Control Protocol, Src Port: http (80), Dst Port: 35348 (35348), Seq: 1, Ack: 734, Len: 0

No. Time Source Destination Protocol Info
270 5.814814 202.168.56.131 124.177.83.182 HTTP HTTP/1.1 304 Not Modified

Frame 270: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits)

Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 124.177.83.182 (124.177.83.182)
Transmission Control Protocol, Src Port: http (80), Dst Port: 35348 (35348), Seq: 1, Ack: 734, Len: 145
Hypertext Transfer Protocol

No. Time Source Destination Protocol Info
271 5.814867 202.168.56.131 124.177.83.182 TCP http > 35348 [FIN, ACK] Seq=146 Ack=734 Win=7308 Len=0

Frame 271: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 124.177.83.182 (124.177.83.182)
Transmission Control Protocol, Src Port: http (80), Dst Port: 35348 (35348), Seq: 146, Ack: 734, Len: 0

No. Time Source Destination Protocol Info
272 5.855476 124.177.83.182 202.168.56.131 TCP 35348 > http [FIN, ACK] Seq=734 Ack=146 Win=65552 Len=0

Frame 272: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 124.177.83.182 (124.177.83.182), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: 35348 (35348), Dst Port: http (80), Seq: 734, Ack: 146, Len: 0

No. Time Source Destination Protocol Info
273 5.855495 202.168.56.131 124.177.83.182 TCP http > 35348 [ACK] Seq=147 Ack=735 Win=7308 Len=0

Frame 273: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 124.177.83.182 (124.177.83.182)
Transmission Control Protocol, Src Port: http (80), Dst Port: 35348 (35348), Seq: 147, Ack: 735, Len: 0

No. Time Source Destination Protocol Info
274 5.858724 124.177.83.182 202.168.56.131 TCP 35348 > http [ACK] Seq=735 Ack=147 Win=65552 Len=0

Frame 274: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 124.177.83.182 (124.177.83.182), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: 35348 (35348), Dst Port: http (80), Seq: 735, Ack: 147, Len: 0

No. Time Source Destination Protocol Info
275 5.902199 Cisco_54:9e:92 Spanning-tree-(for-bridges)_00 STP Conf. Root = 32768/10/00:1e:bd:54:9e:80 Cost = 0 Port = 0x8012

Frame 275: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
IEEE 802.3 Ethernet
Logical-Link Control
Spanning Tree Protocol

No. Time Source Destination Protocol Info
276 6.263919 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=60

Frame 276: 114 bytes on wire (912 bits), 114 bytes captured (912 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)

Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 9117, Ack: 837, Len: 60
SSH Protocol

No. Time Source Destination Protocol Info
277 6.264043 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=84

Frame 277: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 9177, Ack: 837, Len: 84
SSH Protocol

No. Time Source Destination Protocol Info
278 6.264159 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=84

Frame 278: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 9261, Ack: 837, Len: 84
SSH Protocol

No. Time Source Destination Protocol Info
279 6.264388 202.168.56.131 131.170.68.108 DNS Standard query NAPTR 9.2.4.4.4.2.9.9.3.1.6.auenum.com.au

Frame 279: 95 bytes on wire (760 bits), 95 bytes captured (760 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 131.170.68.108 (131.170.68.108)
User Datagram Protocol, Src Port: 53441 (53441), Dst Port: domain (53)
Domain Name System (query)

No. Time Source Destination Protocol Info
280 6.292476 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=837 Ack=9345 Win=65307 Len=0

Frame 280: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 837, Ack: 9345, Len: 0

No. Time Source Destination Protocol Info
281 6.292498 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=220

Frame 281: 274 bytes on wire (2192 bits), 274 bytes captured (2192 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 9345, Ack: 837, Len: 220
SSH Protocol

No. Time Source Destination Protocol Info
282 6.293601 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=36

Frame 282: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)

Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 837, Ack: 9345, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info
283 6.293610 202.168.56.131 203.176.187.10 TCP ssh > msr-plugin-port [ACK] Seq=9565 Ack=873 Win=13104 Len=0

Frame 283: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 9565, Ack: 873, Len: 0

No. Time Source Destination Protocol Info
284 6.301097 131.170.68.108 202.168.56.131 DNS Standard query response NAPTR 10 105 u

Frame 284: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 131.170.68.108 (131.170.68.108), Dst: 202.168.56.131 (202.168.56.131)
User Datagram Protocol, Src Port: domain (53), Dst Port: 53441 (53441)
Domain Name System (response)

No. Time Source Destination Protocol Info
285 6.301246 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=44

Frame 285: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 9565, Ack: 873, Len: 44
SSH Protocol

No. Time Source Destination Protocol Info
286 6.301304 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=44

Frame 286: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 9609, Ack: 873, Len: 44
SSH Protocol

No. Time Source Destination Protocol Info
287 6.301358 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=44

Frame 287: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 9653, Ack: 873, Len: 44
SSH Protocol

No. Time Source Destination Protocol Info
288 6.301813 202.168.56.131 131.170.68.108 DNS Standard query NAPTR 203.153.192.10

Frame 288: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 131.170.68.108 (131.170.68.108)
User Datagram Protocol, Src Port: 53441 (53441), Dst Port: domain (53)
Domain Name System (query)

No. Time Source Destination Protocol Info
289 6.323584 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=36

Frame 289: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 873, Ack: 9565, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info
290 6.323602 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=276

Frame 290: 330 bytes on wire (2640 bits), 330 bytes captured (2640 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 9697, Ack: 909, Len: 276
SSH Protocol

No. Time Source Destination Protocol Info
291 6.329580 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=909 Ack=9697 Win=64955 Len=0

Frame 291: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 909, Ack: 9697, Len: 0

No. Time Source Destination Protocol Info
292 6.339700 131.170.68.108 202.168.56.131 DNS Standard query response

Frame 292: 285 bytes on wire (2280 bits), 285 bytes captured (2280 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 131.170.68.108 (131.170.68.108), Dst: 202.168.56.131 (202.168.56.131)
User Datagram Protocol, Src Port: domain (53), Dst Port: 53441 (53441)
Domain Name System (response)

No. Time Source Destination Protocol Info
293 6.339759 202.168.56.131 131.170.68.108 DNS Standard query NAPTR 203.153.192.10.dryb.mel.comvergence.com.au

Frame 293: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 131.170.68.108 (131.170.68.108)
User Datagram Protocol, Src Port: 53441 (53441), Dst Port: domain (53)
Domain Name System (query)

No. Time Source Destination Protocol Info
294 6.354317 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=36

Frame 294: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)

Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 909, Ack: 9973, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info
295 6.376179 131.170.68.108 202.168.56.131 DNS Standard query response

Frame 295: 313 bytes on wire (2504 bits), 313 bytes captured (2504 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 131.170.68.108 (131.170.68.108), Dst: 202.168.56.131 (202.168.56.131)
User Datagram Protocol, Src Port: domain (53), Dst Port: 53441 (53441)
Domain Name System (response)

No. Time Source Destination Protocol Info
296 6.376298 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=44

Frame 296: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 9973, Ack: 945, Len: 44
SSH Protocol

No. Time Source Destination Protocol Info
297 6.376368 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=52

Frame 297: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 10017, Ack: 945, Len: 52
SSH Protocol

No. Time Source Destination Protocol Info
298 6.376440 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=68

Frame 298: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 10069, Ack: 945, Len: 68
SSH Protocol

No. Time Source Destination Protocol Info
299 6.376513 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=68

Frame 299: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 10137, Ack: 945, Len: 68
SSH Protocol

No. Time Source Destination Protocol Info
300 6.405413 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=945 Ack=10137 Win=64515 Len=0

Frame 300: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 945, Ack: 10137, Len: 0

No. Time Source Destination Protocol Info
301 6.405432 202.168.56.131 203.176.187.10 SSH Encrypted response packet len=356

Frame 301: 410 bytes on wire (3280 bits), 410 bytes captured (3280 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 10205, Ack: 945, Len: 356
SSH Protocol

No. Time Source Destination Protocol Info
302 6.405912 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=36

Frame 302: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 945, Ack: 10205, Len: 36
SSH Protocol

No. Time Source Destination Protocol Info
303 6.446667 202.168.56.131 203.176.187.10 TCP ssh > msr-plugin-port [ACK] Seq=10561 Ack=981 Win=13104 Len=0

Frame 303: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: Dell_b0:3b:61 (00:14:22:b0:3b:61), Dst: Dell_7b:ae:9c (00:14:22:7b:ae:9c)
Internet Protocol, Src: 202.168.56.131 (202.168.56.131), Dst: 203.176.187.10 (203.176.187.10)
Transmission Control Protocol, Src Port: ssh (22), Dst Port: msr-plugin-port (3931), Seq: 10561, Ack: 981, Len: 0

No. Time Source Destination Protocol Info
304 6.608297 203.176.187.10 202.168.56.131 TCP msr-plugin-port > ssh [ACK] Seq=981 Ack=10561 Win=65535 Len=0

Frame 304: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: msr-plugin-port (3931), Dst Port: ssh (22), Seq: 981, Ack: 10561, Len: 0

No. Time Source Destination Protocol Info
305 7.557382 203.176.187.10 202.168.56.131 SSH Encrypted request packet len=36

Frame 305: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Dell_7b:ae:9c (00:14:22:7b:ae:9c), Dst: Dell_b0:3b:61 (00:14:22:b0:3b:61)
Internet Protocol, Src: 203.176.187.10 (203.176.187.10), Dst: 202.168.56.131 (202.168.56.131)
Transmission Control Protocol, Src Port: p2pcommunity (3955), Dst Port: ssh (22), Seq: 1, Ack: 53, Len: 36
SSH Protocol