MONTREAL – How it Works: Regional Internet Registries
Tuesday, November 5, 2019 – 13:30 to 15:00 EDT
ICANN66 | Montréal, Canada

STEVE CONTE: Alright, we're going to go ahead and get started. I thank you all for coming to the How it works session on Regional Internet Registries presented by the ASO. This is a critical piece of the ecosystem, the internet ecosystem. And I'm very, very happy that the ASO and the relative RIRs for the region has agreed to do these How it works sessions with us. So this is brand new. We did it once on Sunday. So this is, you know, spearheading for this group. You guys are some of the first to see this material in this form and so I'm really happy for that.

With us we have Leslie Nobile from ARIN and Paul Wilson from APNIC and there's a smattering of other RIR people here that will probably raise their hands and speak at various times, I'm hoping. And I don't know, how did you guys do questions on Sunday? Do you want them as they come, or do you have a question period?

So if there's questions and there's breaks, please raise your hand. I've got the handheld mic. I'm happy to bring the mic to you so we can capture the questions. We do have remote audience from our participation, we'd like to have all the questions and answers on microphone. So with that, Leslie, please. Thank you.

LESLIE NOBILE: Okay. Good afternoon, everyone. Thank you so much for coming. We really appreciate it. As Steve said, this is our first time doing, How it works in the ICANN sessions, so we'll tell you all about the regional internet registry system and what we're up to today, the things we're working on, the challenges we're facing, etc.

Oops. Hold on, hold on. It worked on Sunday. Oh, it's working now too. Sorry. Okay, so we'll talk about us, who we are, what we do, and how we do it. We will do a brief internet number resource primer. Some people don't actually know what an IP address is or an autonomous system number. So we'll do a very general sort of description of what the internet number resources are that we issue.

We will talk about significant happenings at the RIRs. The most significant has been IPv4 depletion. But along with that, hand in hand goes IPv6 transition. So we'll tell you where we stand on those issues. And we'll talk about the emergence of an IPv4 transfer market as a result of IPv4 depletion, and also as a result of IPv4 depletion, we will talk about an increase in fraudulent activity that we're seeing at the RIRs. As the supply v4 depletes, the fraudulent activity seems to increase. And then we'll move into finally the RIR tools, technologies, things we're working on, services we provide and ways we're helping to increase security.

So about us, so I start with this brief history of the RIR system. And actually, this is the administration of internet number resources, this is not actually, you know the history of the internet. But it's the

history of the administration of our numbers, the numbers that we issue.

So in the 1980s, we sort of start in the 1980s moved to the 1990s, the administration of all domain names, IP numbers and protocols was actually a contract by the US government, the US Department of Defense, in particular, to the Information Sciences Institute at USC, and in particular Jon Postel; he was a significant contributor to the development of TCPIP.

And so he ran this contract. Eventually, it was named the Internet Assigned Numbers Authority and that exists today. So he ran this by himself for a while and realized he couldn't do it all. It would start to see a real increase in domain names and IP addresses being issued. It moved away from just being the research and academic and military networks to a more commercial system of networks.

So the registration and support of the function was actually contracted by the government, again, US government, first to SRI International and then to Network Solutions in 1991; and I actually worked at Network Solutions in 1991 and did that transition from SRI NIC to the DDN NIC to Network Solutions. So lots of work there. We were handling all of the registration and issuance of domain names and IP numbers.

So around 1991/92, regionalization began and the regional internet registry system was formed. Governments and business people around the world started saying: Why is one government, you know,

why is one country making business decisions for everyone? So we need to sort of take that away and start doing this regionally. So the RIPE NCC was created in 1992. They were the first RIR to split off from that US government contract.

At around the same time, you know, they decided that IP number, the administration of the number of resources should actually be split off from domain names all together so the RIPE NCC creation was the first step in that process. And eventually the other RIRs were split off from the function as well and I have a slide on that later.

But you know, the internet was commercialized. It grew very large, very quickly and because domain names were sort of an infinite resource and became worth a lot of money and IP numbers were at a finite resource and were really -- you know, needed stewardship that function had to be separated.

Additionally, the military part of the internet, which was the original ARPANET, the original function of the internet, was split from the commercial Internet; the US government just pulled it off and so pulled it away from the Commercial Internet, and the contract was called InterNIC, which you probably have all heard of that was run by Network Solutions as well. And then the military Internet was called the DDN NIC.

So, what is an RIR? This is sort of our simple definition. We manage the allocation and registration of internet number resources; that is IPv4 addresses, IPv6 addresses and autonomous system numbers, in a

particular region of the world and we maintain a unique registry of all IP numbers issued. Most of you would know that as WHOIS.

Who are we? Well, I'm going to start in the in the right corner up at the top there with RIPE NCC, they were established in 1992, as I mentioned, split off from the US government contract. They handle Europe, the Middle East and the ex-Soviet Union countries. In '93, Asia Pacific NIC was created -- that is Paul Wilson's area -- and they handle all of Asia Pacific, and in 1997 finally ARIN was established.

So between '93 and '97, all of the domain name administration and the rest of the world's IP number administration was still being done under US government contract. So ARIN split off, took just the IP numbers for the US, South and Central America and Sub Saharan Africa, and the RIPE NCC handled North Africa. Finally we split LACNIC off from ARIN in 2002 and eventually AFRINIC in 2005, so those are the five Regional Internet Registries.

So the core functions. What do we do? Obviously I've told you we manage, distribute and register internet number resources. We maintain directory services including WHOIS which is probably our most well-known and well utilized service. We maintain routing registries as well where routing information is put in by users.

We also provide reverse DNS. The RIRs are responsible for reverse DNS, which is translating an IP address into a domain name. We support internet infrastructure through technical coordination, we do this globally with our other, with our RIR partners and with our other

industry partners. And we facilitate community driven policies. The policy development process is handled by the community where the facilitators, the community makes the policies we actually implement them.

So the RIRs are independent. There is no government oversight for the RIRs. I'm often asked to does the US government run ARIN, does the US government run the other RIRs or does some government run the RIRs. Absolutely not, no government involvement, we are completely bottom up process. We are not for profit. We're 100% community funded. Our fees are for our services for providing WHOIS for issuing resources, for doing reverse DNS.

Lots of other technical services that I haven't mentioned yet, but they're not for the number of resources themselves, we don't sell number resources.

We are all membership based. Our members pay fees. The membership is open to all holders of internet number resources. And that's typically Internet service providers. Those are probably, that's probably the bulk of all of our membership is ISPs and LIRs as it's known in the other regions on local internet registries, but telecom organizations, governments, corporations, universities, etc., etc.

As I mentioned, we are community regulated, policies developed by the community. We all have member elected governing boards. Our processes are all open and transparent. They're all documented on our websites, including board minutes. Anything you need to know

will be included on our websites. Everything is completely open and transparent.

So, the number resource organization, sorry, is when the five RIRs act together. We basically act as a focal point for any type of input from the internet community into the RIR system. And we promote the mission, basically, is to promote and protect this bottom up policy process and the unallocated number resource pool and it becomes particularly noticeable in the context of ICANN.

So my next slide actually shows you the ICANN structure and where we fit in. I know most of you are probably familiar with domain names. But we are a separate organization and separate function. So you all know that ICANN is responsible for the top level technical coordination of the internet for the domain names all the numbers and the root servers and ICANN was actually put into place by the US government as well. The US government tried for years to divest themselves from the running of the internet, from the administration.

The US government actually created the internet but they didn't want to keep running it because you know became such a global thing they absolutely want it out so ICANN was put into place in 1998.

ICANN is nonprofit like all the RIRs, its self-regulatory and it is global. It consists of, this is a really old slide by the way, but for me it illustrates where ASO fits in. So there's lots of supporting organizations, you probably familiar with ccNSO, GNSO. But we are the address supporting organization. That is where the NRO comes

into play. It's the ASO or the NRO. We perform that function of the ASO, as the NRO, the five RIRs together and then there's a variety of advisory committees.

So just a quick overview of what an internet number resources is and IP addresses basically a number that computers used to talk to each other. It's unique and every device connected to a TCP IP network, the internet, for example, has to have an IP address and this is what facilitates moving that data, those data packets across the network from a source to a destination.

There's IPv4 addresses and there are IPv6 addresses. IPv4 has been developed, probably in the 70s, I guess. Not a huge amount of space 4.44 billion total addresses which the technical community assumed would be enough. But then they realized pretty quickly in the 90s, it would never last as the Internet grew and exploded.

So IPv6 was created. And I think we, as RIR, started issuing IPS IPv6 addresses in 1998. Much larger space, 128 bits and you can see 2 to the 128th is the total space. It's an unfathomable number of addresses and that's an example of an IPv6, a full IPv6 address very cumbersome and not user friendly. But there is a shortened version.

Autonomous system numbers are just numbers used for routing. They allow routers to talk to each other, essentially network operators have to have an ASN in order to talk to, to actually control routing within their own networks and to exchange routing information with other ISP. It's a global unique number. It's used to exchange routing

information and that is between neighboring ASs, autonomous systems.

And to identify the AS itself, an autonomous system is just a group of IP networks that are administered under the umbrella of a single entity like maybe a university who runs multiple networks, they would administer this autonomous system and routing is again the act of moving data packets across the network.

So we typically throw this slide in because people often confuse IP addresses with domain names and their distinctly different entities. Just as the RIRs are distinctly different from the domain name registries and registrar's so the IP address is an identifier that's an example of a v4 address.

Computers talk in numbers, they recognize numbers, people use names. So it's a unique number. I told you identify as a computer or device on the internet. It's used for routing and moving information across the network from a source to a destination. And every device directly connected has to have its own unique IP address.

Domain names, in other words and the other hand are for people, they're much easier for people to type a name then type a long number. They do the DNS system maps a host name to a unique IP address. So the host name is for the people to understand and the IP addresses for the computer to understand. It's a hierarchical system. It's a means of storing and retrieving information about host names IP addresses and a distributed database.

So this is how IP addresses are issued. I mentioned IANA, the Internet Assigned Numbers Authority that functions still exists. It is actually now administered by ICANN. IANA is rolled into ICANN so they control the global unallocated IP address pool that's where the most of the unallocated pools sit with them. They take the space and they allocate it to each of the five RIRs. They only allocate space to the RIRs, no one below that. Allocate means that we can take that space and sub delegated we can reassign it or we can assign it to our downstream customers.

Our customers are either Internet service providers or LIRs where they're end users. If we assign space to an end user, like an enterprise business, they use that space within their own internal network infrastructure. They never reassign it to any of their customers. They keep it and they use it. So you'd never see that space further sub delegated. But when we allocate it to our ISP customers, they can take the space and further sub delegate it to their customers to their downstream customers.

ISPs have their own end user customers if they assign it to an end user customer, they use it within their own internal network infrastructure it stays right there. If they reallocate it to an internet service provider downstream ISP, that ISP can take the space and further sub delegate it to their own customers. So that is the difference between allocating and assigning

So what has been happening at the RIRs of significance? The biggest thing was IPv4 depletion in 2011. IANA completely depleted the global

unallocated pool of IPv4 addresses. Each of the RIRs received their last /8 block. This was at a meeting, I think in Miami. And that happened, February 2011.

This shows the current available IPv4 space in each of the RIRs. There's not a whole lot, because this is being measured in /8s, and you can see AfriNIC has a little over a quarter of a /8 left in total. Followed by a APNIC with about 16% or 18% of our /8 and then LACNIC who's got about 10% and RIPE NCC, it says they have little over 5% but they actually have depleted.

This is from September 30 so they are at zero as well. ARIN was the first to reach zero. That was in 2005. Each of the other RIRs had an austerity policy, which basically rationed their last bits of IPv4 address space ARIN had no such policy and we ran out very quickly. We got hit very hard from many, many organizations even around the world. So we depleted very quickly.

This shows IPv6 allocations issued by the RIRs so obviously for out of IPv4. We've got an issue IPv6 to sort of pick up the slack. But you know, it's been steady, but it's a bit slow. And it's really hard to see this slide, but basically what you can take out of this is that the RIPE NCC has been issuing most of the IPv6 space more than any of the other RIRs, followed by LACNIC in that kind of a grayish blue and then by APNIC. ARIN and AfriNiC follow.

This slide is slightly different. It shows a different perspective because again it shows RIPE NCC issuing the most IPv6 prefixes in terms of

/32s. RIPE issues the most followed by a APNIC and then ARIN and then you'll see LACNIC down there. So that's a little bit different than the previous slide. That is because the three larger RIRs are issuing the largest block. So we're not issuing just single /32s, we're issuing very large IPv6 blocks to our very large ISP customers so that increases the number of total prefixes issued.

This looks at the percentage of our members who actually have come in and gotten their IPv6 address space. It's a little confusing. Ignore the lines. I'm just going to talk in totals in terms of total space issued. Actually ARIN, RIPE NCC and APNIC have between 60 and 65% of their members who now have IPv6 address space. You'll see that LACNIC has about 95% of their members with IPv6 address space.

LACNIC actually had a policy that had them issuing IPv6 address based to every single one of their members that increased their numbers pretty drastically every single member got an IPv6 block. Without having to ask they just got it essentially. Then AfriNIC has about 47/48% of their membership has be six. So it's definitely working. Our customers are getting their IPv6 address space, albeit a bit slowly.

So current observations, sorry, so movement to IPv6 has been slow but steady, as I said, we've been issuing v6 since 1998 it's now 2019 and 21 years still the RIR with the largest number, you know, percentage of members with spaces RIPE NCC, and that's 65%; so 21 years 65% of our members have a membership. It's getting there. It's not there yet. It's a slow growth.

So ISPs are slowly rolling it out. We're seeing a steady increase in IPv6 traffic across the globe. Some of the big networks have been measuring it and they're saying over 25% of all traffic passed on the internet is now IPv6 traffic. So it's definitely moving in the right direction and we all are seeing increases in IPv6 requests.

But the big thing for us is, we're still seeing a huge demand for IPv4 addresses. All of us receive a significant number of before requests every single day. Even ARIN, we ran out in 2015 we get v4 requests, I hope I said v4 requests, every day. So what we're seeing is that because there's not a lot of v4 request base that customers are increasingly turning to the IPv4 market, and I'll explain what that IPv4 market is in the next slide.

So we see that they're either purchasing space and using RIR transfer policies to update the RIR registries where they're purchasing space outside the registry system. They never come to us. They don't let us know and they're not updating the RIRs registries. Or they're using leasing as a form of obtaining additional IPv4 address space and that is done with letters of authority that they will bring to an upstream ISP and asked to route the space for them. And they're either getting a legitimate LOA, a letter of authority, or they're actually forging LOAs. We're seeing both and I'll talk about that in one of the later slides.

So as I mentioned, with a depletion of IPv4 and we saw the emergence of an IPv4 transfer market, pretty much the communities, all of our communities knew that this was inevitable as supply, you know, decreased, it had to come from somewhere. So it was inevitable a

market would form. So there was an ongoing demand. Ongoing demand never diminished literally in any of the regions and a decrease in supply before. So that necessitated policy changes at each of the RIRs, all of the communities recognize that.

So they knew there was two choices right, you play or you don't play. And if you play you facilitate the v4 transfers and you ensure registry accuracy. You make sure people will come to you. You provide them a vehicle to get space and then come to us and update the registry. Or you watch a black market emerge and there would be no registry interaction and the databases would be completely inaccurate. No one would know who was using what space. So our communities all put market based IPv4 transfer policies into effect.

So they are all needs based. The only way to get IPv4 space through an IPv4 market transferring any of the RIRs is to provide justification and there's criteria that you have to use to get this space. So basically resource registrants who have extra space can sell it or transfer it to recipients who qualify for the space. That's the way it works.

The RIRs role in all of this is to ensure compliance, full compliance with these needs based policies and to ensure that we're updating and maintaining an accurate registry that is our role, we facilitate the process. But we are not privy to any financial transaction information between transferring parties.

We have no idea what goes on. What happens is they come to us, the registrant says I have space, I have somebody I want to transfer it to

and then that person comes to us and says, here's my justification and we do all of the verification vetting and all the work and we complete the transfer, but we know nothing about the back end, what's going on.

So this shows all five of the RIRs and our market based transfer policies, whether we have them intra-RIR or inter-RIR. Intra-RIR market based policy means the space is being transferred within our regions. All five of the RIRs have an intra-RIR transfer policy, market based. Three of the RIRs, AfriNIC, ARIN and RIPE NCC have inter-RIR transfer policies.

So we are allowing market based IPv4 space transfers to happen between those three registries. LACNIC's policy was just passed and they plan on implementing that in Q2 of 2020. In AfriNIC there's been multiple policies discussed, nothing has passed at this point. But there's lot of talk about which policy might work for them as far as an inter-RIR policy.

They were the last RIR to have IPv4 space. So they were not quite as pressed as the rest of the rest of us were to put an inter-RIR transfer policy into effect.

So this shows, let's see, the number of transfers per year for the intra-RIR market based transfers and it's really hard to see these numbers, I mean these colors I do apologize, but you can see that intra-RIR IPv4 transfers that there's more happening in the right region and in the ARIN region than any other two regions. You can see the dark green

and the blue that is ARIN and right activity quite a bit going on. Eighteen hundred last year intra-RIR transfers in the right region alone and it looks like 2019 is following the same trend as 2018.

My least favorite slide. Okay, so what takeaway from this is that the three RIRs are transferring space into and out of each other. But most of the space going out of an RIR is coming from ARIN, you can see we've made 280 transfers to APNIC and 210, it's the red lines, to the RIPE NCC. The reason for this is that ARIN inherited the internet database back in 1997 and there was a lot of space there that had been issued prior to the establishment of the RIRs.

We call it legacy space. It was space that was issued by the DoD NIC SRI Network Solutions. We were issuing space with no contracts. We had a template. And we asked people to justify and tell us how much space they needed, who they were, why they needed it. You know, we tracked very carefully, who they were. There was needs based but there was no specific policy and there was there was no contract that they had to sign.

So ARIN ended up having the larger portion of legacy space because most of the space in the 80s and in the early 90s was issued within the US and Canada, mostly the US, quite honestly.

We did a project in let's say early 2000 to move legacy space to the appropriate RIR. So RIPE NCC got some and APNIC got some and eventually AfriNIC and LACNIC got small portions as well. But the bulk of it remained in ARIN, and that is the space that is now being bought

and sold more or less. A lot of the space was dormant. It was abandoned. It was just sitting there. People didn't, no longer had a need for it. So that's most of the space that's now being transferred

So, current challenges. There are a few. Most of them came about based on IPv4 depletion. That was sort of a trigger for a lot of this activity. So we're seeing more fraudulent request to obtain and or transfer IPv4 address space. You know, as the addresses deplete the market value goes up and so people are really anxious to get their hands on IPv4 address space and they're doing pretty much whatever they need to get it, and that includes lying to the registries, that happens on a daily basis, pretty much.

We see hijacking of IPv4 addresses increasing. In other words, people trying to take over registrant space by pretending to be that registrant. They try to come in and make fraudulent changes to WHOIS and they're targeting those legacy records either the dormant records, the out of date records, the space that's not been routed for years.

That's what they're looking at. So they're looking at the older space for the most part. They're submitting falsified documentation, falsified legal documentation. They're submitting falsified passports. In the RIPE NCC region they collect passports as a way of authenticating points of contact. People are actually forging passports. Go figure.

And they're doing a lot of shell companies. They set up a lot of shell companies. They set up shell companies that look or sound like an

actual registrant in one of our databases and then they look for expired domain names and then they re-register the domain name and then they pretend that they are that company from 1990 or 1988 who got the space.

And they come to us all prepared and we're pretty good at figuring out who they are, at this point, but in fact, we've had some legal cases, working with the FBI. At least ARIN has where we've actually caught people doing this and they've actually been arrested and it's good. And we've been able to obtain or reclaim address space.

There's a lot of route hijacking going on. And that is basically an authorized use of abandoned or un-routed v4 addresses. They going in, they're looking for un-routed space, they take it. They try to get it routed by an ISP and even if they get routed for two days. If it's criminal activity, they can make a lot of money and cause a lot of damage. So that's a really common activity and it's one that law enforcement is really tuned into right now.

So we're seeing a lot of that. And although we aren't directly responsible for routing, we will try to intervene as RIRs. If someone lets us know that space is being routed

And it's to the wrong registrant we will actually call an upstream ISP and let them know that they may need to check, WHOIS again and get it straight.

We, as I mentioned we see leasing, buying and selling of IPv4 address space outside of the registry system. And of course that leads to a lack

of attribution in the database. We see people not validating their contact information and WHOIS that is one of the ways we as RIRs, try to maintain accurate registries. We try to verify that every single registered contact in our database is active and that they are validated that they're still in existence, that their information hasn't changed. And if it has, we asked them to update it.

But, and we all have a specific routine for going after that, you know after those people to update their records, but a lot of them don't respond. So there's a certain percentage that never update their records.

Then there's the problem with carrier grade NAT and simply put, it's the ability to use a single address from multiple users. So it's difficult to actually identify who's using a space at any one time and the registry doesn't ever get updated and it causes a lot of problems for law enforcement again as well, they can't figure out who's using what space and a lot of ISPs aren't even able to track who's using it themselves, so.

So I'm going to actually turn it over to Paul Wilson. He's going to talk to you about some of our tools and technologies things we're doing to improve the registry.

PAUL WILSON: Thank you very much, Leslie. I am Paul from APNIC.

LESLIE NOBILE: Should we ask for any questions yet, or…?

PAUL WILSON: Sure, thanks. Thank you all for coming and sitting with us so far this afternoon. Are there any questions maybe about anything that some Leslie's raised so far? Kenny.

KENNY HUANG: Can I raise a question?

PAUL WILSON: Please. Yeah.

KENNY HUANG: Okay, right, thank you. Kenny Huang, executive council member of APNIC. First of all, thank you for your presentation. I think it's very educational but I still have two questions. The first question is actually there [inaudible] cybercrime, they try to abuse their IP address to do their criminal activity. For that kind of information basically there's no effective technology -- probably Paul will introduced later -- there's no effective technology t o detect or try to get that kind of information. Is there any other mechanism we can share that kind of cybercrime information? That's my first question.

My second question is, there are significant amounts of portions or IP [inaudible] which is outside of the RIRs umbrella; is any other way we can claim back this space? Right, thank you.

PAUL WILSON: Yeah, thanks, thanks, Kenny. I mean cyber-crime's huge. It's a huge and diverse field so you might be talking about cyber-crime which relates to the infrastructure itself, to somehow hacking or breaking the infrastructure itself. You might be referring to something that's happening at the DNS level, you might be referring to something that's happening at server levels or at what we call social engineering levels where phishing attacks are used to convince people to give up passwords and things.

So I mean, I don't think there's any one answer to what to what you asked there, I'm afraid, but it's probably worth saying that the RIRs, the five RIRs essentially serve the network operator community around the world. So we have some hundred thousand or so collective members across all of the RIRs and these are the companies that are building network infrastructure.

So I think for as far as the RIRs go our involvement in cyber security is very much got to do with the cyber security needs and the cyber security challenges at that level. So we talk about things like route hijacking which is the process of one network operator being convinced to admit or to route the address space incorrectly that might direct traffic to a particular area.

We might be concerned, we are concerned, about that sort of case. But we're not really involved, for instance, in social engineering or in DNS attacks or in other kinds of attacks you know as part of the best

part of the RIR responsibility, I guess. Across the RIR communities, though there are and across the internet communities, there are things like the certs, the computer emergency response teams. And other infrastructure components or organizations that do get involved with security at all level so, or at different levels. So I think it's a, you know, there's no one answer to the question that you ask there, but if there's something more specific. Maybe we could talk about talk about that.

Your second question was about recovering of IP addresses. Recovering of unused IP addresses, is that right?

Okay, so that's something that would be a policy question for each of the five RIRs. We've got slightly different approaches at each of the each of the five RIRs. At APNIC at the moment, for instance, we are going through a process of identifying address space within our managed pools of addresses. Address space that is unused. As far as we can see that as it doesn't appear in the routing tables.

So by identifying that space, by making contact with the holders and if we can't make contact with an identified holder then really doing our best to try and find the holder of that or the last most recent hold of that address space, then we hope we might be able to either recover that address space for reallocation to someone else or on the other hand, as Leslie mentioned there's an IPv4 address market.

So someone who's not actually, who holds IPv4 space and is not actually using it or routing it, actually does have an opportunity to

liberate that space onto the market to sell it to someone to make to make a sort of a windfall commercial gain out of that. Which is not exactly how IP addresses were intended to be used, but on the balance it's better to have IP addresses out there in circulation and satisfying a need than to have to have them sitting idle. So I hope that helps. Okay, long answers.

LESLIE NOBILE: But let's just add one thing to that. Paul mentioned policies are different in each of the regions, in the ARIN region, they decided that it wasn't worth it to proactively go after IPv4 address space. There wasn't really enough unused that would benefit the community. So they decided we're not going to have a policy for that.

But we as staff, as we don't proactively search for a new space, but we actually do it reactivity, so as we go through space, or we're dealing with someone who might not be using a space, we will take space back again. We do a lot of vetting verification make sure it's not use. We actually get space reclaimed for non-payment. For example we reclaim space for fraudulent activity and we still have people giving back space to ARIN, if they're not using it. It's amazing.

You would think that they might want to sell it, but there's still good old fashioned netizens that remember how it was. And that this is, you know, good stewards of a limited resource. And so they give it back to the registry to redistribute to customers. That was part of it.

And one other thing is that we have formed, in relation to cybercrime and law enforcement, the five RIRs work together to support law enforcement and we have what we're calling a public safety Coordination Group as part of the NRO. We do outreach to law enforcement. We do training. We do sharing of information. We were doing it on a global level together. So we are definitely working with law enforcement to try to address their concerns from RIR perspective as much as we can.

PAUL WILSON: I'll mentioned that Leslie and I are represented to have the five RIRs, but we've got folks from RIPE NCC here, from LACNIC and AfriNIC, I think around the around the room as well, so many of our colleagues should feel free to pipe up at any point. Mary Rose.

MARY ROSE RONTAL: Good afternoon, everyone. My name is Mary Rose. I'm from the Philippines. I'm an ICANN fellow and a newcomer at ICANN. So in terms of transitioning from IPv4 to v6, I'm actually wondering why people are still requesting for v4. I mean, what are the challenges that this institutions are facing, why they cannot just easily transition to v6?

PAUL WILSON: The fact is that in order to connect to the v4 internet at all, you must have v4 addresses. Establishing an ISP network operation like the

ones that our members and community constituents doing, in order to connect to the v4 internet, they need to have v4 space in addition to IPv6, so it's actually an architectural requirement that if you only have IPv6 address space, then your ability to connect into the v4 Internet, which is still the majority of the internet is, it's kind of limited or nonexistence.

So the rationing policies that Leslie mentioned that existed, that have existed, and most of the RIRs are precisely designed so that into the future for the next hopefully number of years, although a number of years. Although, for instance of RIPE NCC they have just recently exhausted that supply.

The point of having this supply is so that new network operators who come along and want to establish a full internet service connecting to the v4 and the v6 internet, so they need to have at least a small amount of IPv4 address space to be able to do that, in addition to v6. So it's a fact that at the moment we have a dual stack internet. We've got IPv4 and IPv6 coexisting on the internet and you if you're connecting to that, you need to be able to connect to sort of both of those sort of addressing pools on the net.

LESLIE NOBILE: Can I add to that? We hear from a lot of Internet service providers that they're have been having a very difficult time selling IPv6 to their corporate, you know, heads. They don't want to invest the time, the money, the resources to do the transition. What they see is that

there's plenty of IPv4 address space out there and that they can just buy some or they can lease some.

And this has been perpetuated by this emergence of this IPv4 transfer market and the emergence of IPv4 brokers. There are a lot of IPv4 brokers facilitating this process and what they've done for the past five or six years since we depleted, started to deplete, is contacted every person, every organization in our databases, all of our databases. They've contacted them and said, you're sitting on a gold mine, IPv4 is really important. It's going to continue for many years.

And if you want to sell some, we'll help you find a buyer and that has actually changed the face of what we do drastically. They are at all of our meetings and they, and as Paul said, it helps to reutilize, it helps to utilize space that's not been utilized in years, but it also perpetuates the life of IPv4 and from talking to all the techies that I know they don't see this going away anytime soon, so.

PAUL WILSON: Is there another question? Sure. Go ahead.

FIDYA SHABRINA: Good afternoon. My name is Fidya. I'm from Indonesia and I'm part of the ICANN Fellow. Earlier, Leslie mentioned that IPv4 can be transferred to IPv6. And for this, there are particular criteria that must be fulfilled.

My question is, is this review done by the RIR, and if so, how is it done? And is there any particular timeline that those parties who are requesting to transfer that they need to comply to it in order to get approved for the transfer from IPv4 to IPv6? Thank you.

LESLIE NOBILE: So I'm not sure about the IPv6 part of it, but so we all have our own individual policies for doing these transfers. You're asking about IPv4 transfers, correct? First of all, there's no timeline. Sometimes it can take three or four months to get all of the paperwork actually approved so we'll sometimes wait for someone to sign a contract because it goes through lawyers, etc.

But we do the review as RIR staff because we have criteria that our community has put into place. So we all have our own individual policies and they're fairly similar right they their needs based, you have to show us how much space you currently have, how much space you plan on using how many users you have, what your networks look like and why you justify the space.

The v4 transfer policies are quite a bit easier than our IPv4 request policies, those were a little stricter. But the community has, you know, eased up on the actual requirements, but they still exist. So all the staff evaluates each request and then we make the transfer happen.

As far as its relationship to IPv6 I'm not sure I got that part. Did you? No, what did you have?

FIDYA SHABRINA: Ma'am, you said that IPv4 can be transferred to IPv6, is it?

LESLIE NOBILE: I don't think so.

PAUL WILSON: Not exactly, no.

FIDYA SHABRINA: No, I was just making sure for the transfer thing. But you've answered my question, that there's no particular timeline, but the review is done by the RIR.

LESLIE NOBILE: Yes, absolutely.

PAUL WILSON: I have to say, coming from the Asia Pacific, it's great to have three questions so far from my part of the world, all the way up here in Canada and a fourth one as well. [Inaudible].

UNKNOWN SPEAKER: I'm [inaudible], one of the community members of RIR community [inaudible] the provider in Bangladesh. I had two questions, but one

of the questions I wanted to ask I got the answer. And the second question is, as a community member, it's really hard to find the information in infographic, where, how, what address [inaudible] look at it through RIR, how much does still happen historical address and location and how much addresses are still free or not.

And my question or request is to RIR, is there any initiative that can be taken from RIR to IANA's side so that as a community we can understand how much addresses are allocated to RIR community as an infographic way and how much addresses [inaudible] as an historical space and is there any space free or not on IANA's side? Thank you.

LESLIE NOBILE: So there's a couple of answers here. On the NRO website, the number resource organization, we have some of that data. We have what we call the NRO Joint statistics presentation. I think that's what we're calling it, it might have changed names, but it shows you the total amount of space in /8s, and it shows you how much each of the RIRs have been allocated and then it shows how much space RIR has issued to their customers. So there's some of that data exists in the form of a single presentation on the NRO website.

I've completely lost my train of thought. The second part of that was I think it still is on the NRO website. What was the second….?

UNKNOWN SPEAKER: My second question was [inaudible]. Is there any infographic information present on the IANA site? So how much of this is allocated to RIR, how much does it still have an historical space or are any other spaces available or not? If there is a graph present so that the community can understand better [inaudible]? Thank you.

LESLIE NOBILE: I'm not sure about IANA and we'd have to ask IANA about that. Paul might know. But as I said, on the NRO website that information exists in the form of the presentation. And additionally, we have something called our extended statistics file. It's basically all five of the RIRs got together and we created one database, one file that shows the status of every single IPv4 address space in the world, globally, right.

So it shows whether it's allocated or assigned. It shows who it's assigned to. When it was done. It shows what spaces reserved for particular policies. It shows what space has been, so it has what reserved, assigned, unallocated available, the available space shows up in this extended stats file as well. Has dates and names and it's one place you can check for every address. Is there anything else it shows status wise? Available reserved issued basically.

PAUL WILSON: The data gives a full roadmap of the IPv4 address space, so you can actually use that to find out the answers to the questions you need. But it does need to be processed. So it's sort of for people who want to, don't want to ingest that data into a system and take a look at it.

But there's a bunch of data that's been presented in different formats and in infographic formats, if you like, by the NRO which you can find on the NRO website.

I should probably move on into this some this last section which is fairly brief about just about the tools and technologies that we use and we're working on. So I guess everyone here is familiar with, WHOIS, as the registry service that's used to provide information about domain names.

Well we use WHOIS as well to provide registry information about IP addresses as well. And so in our case in RIR terms, WHOIS, is for IP addressing information. The thing about WHOIS, is it's a pretty old technology or pretty old standard. It goes back to the 80s I'm ashamed to say, and it's a very basic service. So, I mean, the way it works is not very well standardized, it kind of varies from one server implementation to the other, from one registry to the other. Even between different domain name registries and different IP address registries, you actually can have different query formats and different data formats.

So it's kind of, it was originally intended as a human readable information service and it's sort of serves that purpose, but what I'll be talking about here is not just WHOIS but the next version of WHOIS which is referred to as RDAP or the registration Data Access Protocol. I actually understand there's a RDAP how it works session in this room after this. So I might be kind of preempting some of what, particularly

those of you who are here as fellows what you might be learning in the next session.

But just to start off with, WHOIS, the IP address WHOIS, which is run by the RIRs is to provide information about registration of IP addresses and autonomous system numbers as Leslie explained earlier. It contains information about every block of addresses or block of numbers that's been allocated by a particular registry. It provides the identity of the organization to which those resources were allocated, the date of the allocation. It provides contact details for the critical contact people, people or roles that people play in relation to those addresses. So people who are either administratively responsible for the addresses or technically responsible

Now, the whole idea of IP, WHOIS, in the first place was for engineering analysis and fault finding. So that, for instance, you may know that if you're receiving a cyberattack or you're being exposed in some way to some fault that exists on the Internet. You're saving some email, for instance, that you're interested to understand the source of it.

Then IP addresses are often, they tend to be the most basic piece of information about the source of the traffic that is or the transaction that's concerning you. So if you want to know where a particular packet of information or where a particular transaction or activity is sourced then going to the IP address WHOIS, with the IP address that's kind of offending you or that you're interested in is the way to find out where that IP addresses is actually being held.

And that's, as I say, important from a technical diagnostic fault finding or increasingly these days from a law enforcement perspective, too, because if you are dealing with cyberattacks or cybercrime then often the IP address is the best key that you have to the actual source of the problem that you're dealing with. So that's why we have the IP address WHOIS, basically for those purposes, something that's important about WHOIS from the RIR perspective is that it is considered to be public data.

So we have also been through the particularly the RIPE NCC and they may like to talk about this, but we collectively in the RIRs have been through the sort of GDPR process and in each of our respective regions, the sort of privacy analysis of what we're doing.

And it is true that the RIR WHOIS databases contain personal contact details and personal contact information which needs to be in compliance with our own respective local laws and so forth. But in general, the condition of receiving IP addresses from a regional internet registry is that you make yourself known via WHOIS so that your use of IP addresses actually is also visible and transparent to other people on the internet.

Okay, so that's WHOIS, it contains the basic registration data, as I say though it's old technology. So it's being upgraded these days with the RDAP standard which is being embraced by the RIRs collectively.

This is about RDAP, the things that RDAP brings that we miss out in WHOIS, is a sort of standardized query and response format. So

instead of getting unfortunately, as you do these days, a different type of response from ARIN's WHOIS as you do from RIPE WHOIS, for instance. When you're accessing via the RDAP standard, you will be using the same commands and receiving data in the same format and receiving error responses in the same format, you know, nice modern behavior forum for computer systems these days.

RDAP will allow redirection which means that if you go to one RDAP service and asked for data which is not actually contained within that registry, then you should be redirected to another registry. That's another sort of limitation of WHOIS at the moment you kind of have to know that you're going to the right registry for the data that you're looking at.

Out of WHOIS, RDAP also provides some authentication and authorization. So, potentially, it can carry information that's not publicly available but available on the presentation of the right credentials, basically. RDAP also supports internationalization, so multiple character sets behind the registration records.

Okay. And as I said, I think we all, hopefully, will we might still be here for the next session. There'll be a lot more about RDAP at the next session as I understand it.

So the other sort of major technical advancement that's going on at the moment in the RIR world is this thing called resource public key infrastructure. If you're aware of what a RPKI is, a public key infrastructure. It's a system of digital certificates, which are issued by

certificate authorities that allow someone who's got cryptographic keys to use those keys in a public system like email, for instance.

The Resource Public Key Infrastructure is an adaptation of that standardized system to certifying the holdings of IP resources so an RIR as a registry is also effectively a certification authority which issues you now, not just with a WHOIS record, but with a certificate, a digitally signed certificate that that validates your right to use those IP addresses and an autonomous system numbers. So this is something, again, that all of the RIRs are moving towards implementing at the moment as a service that we offer as registries, as the authority registry. We're also a certification authority for these resource certificates.

The whole point of RPKI is just like other digital certificates, they provide a sort of general purpose mechanism that can be used for different purposes. So you can use the certificate that you're safe from your local regional internet registry for various purposes. But in our case the primary purpose is around routing security.

So I mentioned before, in answer to Kenny, that one of the security issues that we deal with is called route hijacking. It's basically the unauthorized use of IP addresses by one person or party to try and Redirect internet traffic to their servers or networks. The point of use of RPKI for routing security is to avoid that into my make it either impossible or less easy to achieve.

So there's something that's called Route origin validation. I'll talk about in a minute. The next couple of slides just actually show the levels of RPKI activity around the RIRs. There's a total of 14,000 of those hundred thousand or so RIR members that are currently registering themselves or active within the RPKI system that represents somewhere between about 1 or 2% and about 40% of the population of a given RIR.

The uptake of RPKI is a little like the uptake of IPv6. We're in the middle of what's quite a substantial and costly global transition towards the use of RPKI for routing security. So this, like you might know, like IPv6 is something that we are gradually tracking and able to report on in terms of the overall global internet communities adoption.

Not to route origin validation, this is one of the applications of RPKI that I mentioned. And it's the use of your RPKI certificate to indicate that as the holder of some IP addresses, you're giving someone, identified by an autonomous system number, the ability to route that space and the authority to route that space on the internet. So it's that mechanism that can avoid route hijacking as we know it today.

And so that's just the most popular and the most sort of imminent application of RPKI that we're dealing with at the moment. There are other applications which are also in the routing system to provide a much more secure overall routing framework through secure BGP for those who know about internet routing.

The last slide here is about the internet routing registry, which is another service offered by the RIRs, it's an extension of the WHOIS services that we offer to also carry routing information associated with IP address and ASNs. This is also, this is actually a sort of more

Older and outdated service of the RIRs that has being mentored or strengthened with the RPKI and route origin validation that I mentioned.

So I think that's all we have on those RPKI technical services. I know that quite a lot of that is kind of very specific to the RIR communities and the sort of network operators and engineers that we deal with. So it may or may not be meaningful to those of you in the audience. I'm very happy though to answer some more questions, or to hear any comments or corrections, from colleagues in the RIRs, RIPE NCC, AfriNIC, IANA.

STEVE CONTE: No questions in the room? I have no questions online either. Oh, please. Thank you.

IKE NNAMANI: I'm Ike Nnamani from NIRA, Nigeria Internet Registration Agency. It's kind of going back to the earlier section on IP 4 and 6 in terms of the adoption in the AfriNIC region, specifically the Nigerian situation, I think about a year or two ago we did a survey on the Nigerian internet

exchange to find out why the slow adoption of IPv6 and top on that list are two major reasons.

One is the cost because some of the equipment that is IPv6 compliant is more expensive than the IPv4, and then the second challenge was the technical skill sets of the local engineering team. Subsequent to that there was some training done, AfriNIC conducted some IPv6 training and all that, but it has not improved much.

So my question is, and the default for that is basically people are using [inaudible] to extend the IPv4 and the rest of it; so is there anything being done to address that, that you guys are aware of? If not, I don't see much change, at least in that market for some time.

PAUL WILSON: The right of deployment of IPv6 around the world is extremely variable. So if you take a look at the internet community of a particular country, you know, some countries are well over 50% maybe even up to 80%. Some countries, you know, when you look at the average across the entire internet industry is still sitting on zero percent and you're quite right that it's got a lot to do with costs and technical skills and a sort of sense of need.

I think it's not true anymore in general that IPv6 equipment costs more. But IPv6 is generally available in new equipment. So obviously it requires you in a lot of cases to be purchasing new equipment in order to have IPv6 capability.

One of the things that that is a sort of significant opportunity for ISPs though is precisely because new equipment tends to support IPv6 is that when you are, for instance, upgrading set of network infrastructure, when you're building out a new network that's the time where it's going to be, sort of, easiest and the best opportunity to deploy IPv6.

And we've seen a lot of examples of that around the world. There was a very large mobile LTE deployment in India that started a few years ago and it went IPv6 from the beginning. And it took India solely as a result of their decision it took India to the top IPv6 population in the world.

Probably the next the next interesting thing about that is that it was the first and once that ISP once that provider had had started deploying IPv6 then at least three or four of the other major providers, if not all of them by now also followed, so the sort of competitive market environment kind of means that while no one is doing IPv6. There's maybe less of an incentive.

But when someone starts and demonstrates that it can be done, and probably demonstrate some efficiency and financial advantages from that. It's that is when competitors have to follow. So, you know, it is it is very much a distributed sort of market driven situation and the exact key to getting any given market sort of starting on IPv6 is sort of very circumstantial, you know.

Yeah, it's what the RIR housing are doing. I mean we do continue to promote very hard, the opportunity and the need to move to IPv6. And we do that through sort of communications and through a lot of training and technical support as well.

STEVE CONTE: Almost the idea of a question from online. This is from [inaudible]. The question is: What is the role of RIR in tackling dark net cybercrime issues?

LESLIE NOBILE: The best thing we can do to help in that area is to maintain an accurate registry so that law enforcement can use WHOIS to find the perpetrators, who, you know, that's really, that's our role and that's how we try to support, law enforcement, that's one of our main roles. In addition to training and outreach, you know, and all that stuff, it's an accurate registry because they can still use the RIR registries to look for the data they need.

They can no longer use the domain name registries, WHOIS to find what they need. So they are actually having to rely on the RIR WHOIS to find who's using what IP address, so that's really it.

PAUL WILSON: .NIC is an interesting term because it can kind of mean any of a lot of different things. But if it's traffic on the internet, then it's traffic that

has to flow from one IP address to another. And as Leslie said that's exactly where an accurate, WHOIS comes in.

And sometimes a dot.net simply refers to the fact that you might be accessing a website that is not known by a domain name, But it's still of course has to be known by an IP address. So it's really just a website or a web service without a domain name. Still the IP address is the thing that's important and that's where the accurate, WHOIS is what we are kind of obliged to keep maintained.

UNKNOWN SPEAKER: No, I was just going to add something to that it's not specifically to answer the question, but it's along the lines of what RIRs do with cybercrime cyber security. Like NIC, we have a very small scale operation in writing a C-certs, what we call a warp. It's a warning advice and reporting point and it really consists of three basic functions. It's an additional service we have for our members. One of the functions deals with anonymous reporting of all types of cyber incidences any type that occurs across the region, but not only the LACNIC region, anywhere in the world.

Another one deals with advice brokering in the event of an actual cyber incident for people to mitigate or handle those incidents. And then the third function just use with building capacity and like. So one of the things that I need to make clear with this is that we define, or we limit our liability to actually becoming involved in the incident management. So if it's an incident is happening at one of our

operators, what we can do is just provide advice, but we don't accept any liabilities actually go in and try to handle it and so on behalf of the operator, but it's a bit different to something that the other RIRs are doing. And it's just one of the additional benefits that we have.

What we do is, all of those incidents are reported, we try to just elaborate on a number of statistics on the most popular types of attacks that are happening across the globe. Where the IPS originated from. We find that this information is actually very useful for law enforcement, where they are now getting involved in the whole question of

Cyber Security because we also have for instance glossaries explaining what the different types of attacks are and it's just a useful go to tool to understand the landscape. So, just wanted to put that out there.

UNKNOWN SPEAKER: My question relates to RPKI or whatever you mentioned earlier and I was just thinking, maybe I'm wrong, that maybe that could be extended to replace this SSL, the current SSL practice. What do you think about that? Or maybe I don't understand. I think should be able to, so that way you won't have issues where people access some website that is not known, if you know what I mean.

PAUL WILSON: Look, there might be someone well placed in the audience to respond to that. I'd say the answer is that they are operating at two different

levels; that RPKI is about the certification of the IP address holdings and it's about the security of the routing system itself. On top of that is overlaid the DNS and the use of SSL by websites, and I think the two of them are addressing different security problems and probably still need to exist at the same time. I'm not sure if anyone has sort of suggested to unify them under one sort of process or not.

UNKNOWN SPEAKER: Good idea to unify them, I think. When I look at it, something is not right there right now. Maybe I'll come get your email, we need to disclose that further.

PAUL WILSON: Sure, okay.

STEVE CONTE: I have no further questions online. Any other questions in the room here?

Okay well with that, I'd like to really think Leslie and Paul for their time and the ASO in general for joining us in the How it works series.

PAUL WILSON: Thanks to you all for being here and for the questions too. Thanks.

STEVE CONTE: And as Paul alluded, we do have our next session on RDAP and what -- Paul, correct me if I'm wrong, but my understanding is that the RIRs were leaders in standing up production servers of RDAP service for the new RDAP service.

PAUL WILSON: I'm not sure, we're not we're not very competitive, you know. I mean, we might have been first but who's counting.

STEVE CONTE: I actually applaud that. I thought it was great to see -- you know RDAP has been talked about for years within the ICANN community and was great to see it being stood up as a production server for such a long time now, for years, and that the rest of the ICANN community is coming around and trying to stand up for RDAP as well.

So thank you for the tease for the next session, but also thank you for being a leader in production and getting that going. So thank you all. Please, the next session is in about 30 minutes in this room o, RDAP and I hope you all stay and enjoy that as well. Thank you.

[END OF TRANSCRIPTION]