
ICANN79 | CF – How it Works Sess #1 All about numbers
Saturday, March 3, 2024 – 1:15 to 2:30 SJU

NICOLÁS ANTONELLO: Hello and welcome to the session How It Works Session 1, all about numbers. My name is Nicolás Antonello and I am a participation manager for this session. Please note that this session is being recorded and it's governed by the ICANN expected standards of behavior. During this session, questions or comments will only be read aloud if submitted within the Q&A pod. If you would like to speak during this session, please raise your hand in the Zoom room.

When called upon, virtual participation will be given permission to unmute in Zoom. On-site participation will use a physical microphone to speak. Interpretation for this session will include all standard languages. Please state your name for the record and the language you will speak, if speaking a language other than English. Please speak at reasonable pace. Within that, I will hand the floor over to Leslie Nobile.

LESLIE NOBILE: Thanks, Nicolás. Good morning, everyone. Can you hear me? Am I good? Okay. Can't hear myself. Okay. Good morning. My name is Leslie Nobile. I'm the Senior Director of Trust and Public Safety at ARIN, the American Registry for Internet Numbers. I'm here with my colleague, Germán Valdez, who's the Executive Secretary of the Number Resource Organization, and we'll explain all of this in the slides.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

We're going to talk about the Regional Internet Registry System today, how it works. Typically, within the ICANN world, you hear a lot about domain names, but not so much about numbers. So, ICANN asked us to come and educate and talk about what we do in the Regional Internet Registry System. So, I'm going to start, and then I'm going to turn it over to Germán, sort of halfway, and then I'll come back toward the end and take it over again. Okay. So, our agenda today, we'll do an overview of the Regional Internet Registry System, the RIRs.

We'll do a little bit of history and tell you what we do. We'll talk about the policy development process, both from a regional perspective and a global perspective, because there are two different sort of processes. We'll tell you about Internet Number Resources, because that is really our main function, to issue IP addresses, IPv4 addresses, IPv6 addresses, and autonomous system numbers, and we'll tell you what those are. We're going to talk about routing, because IP addresses and routing work hand in hand together. And then we'll talk about some of the noteworthy developments that are happening within the RIR system. And finally, we'll end with RIR services and tools, and these are the services and tools that we offer in common that are well utilized by our communities. Each of the RIRs offer their own individual services and tools.

We're not going to talk about those, and there are many. At the end, we'll provide you links to the RIR websites, because there's some really good information, but we're talking about our common services and tools today. Okay. Start with the RIR system. To do this, we have to go into the history of the Internet Number Resource Administration. So, as you probably know, the Internet was developed and created by the U.S.

government in the 1960s. It started with the ARPANET, and then in the 70s, it merged with the NSFNET, so it was all military research and development and education. So, the administration of the numbers was fairly easy in the beginning. The U.S. Department of Defense was running everything, and eventually, in the early 1980s, they contracted the administration of running IP addresses, domain names, and protocols to the University of Southern California's Institute of Science and Information, I think. Sorry. I always get that confused. ISI was actually run by John Postel, and John Postel was an early Internet pioneer in the development of Internet standards.

So, he ran this contract. The function was actually named the IANA, the Internet Assigned Numbers Authority. I'm sure you all have heard of that. There're several sessions this week about IANA. I think there's one on Wednesday, if you're interested in attending, which you'll get a lot more information, but it has been called IANA since the 80s. So, John handled it all initially himself. He actually had a notebook. We all sort of joke about John Postel's notebook because every IP address was written down in a notebook in the beginning, which the registry eventually inherited. We still have those.

They are enshrined at this point. So, John – well, actually, the U.S. government did a subcontract. So, John handled the top-level coordination of IANA, and then the actual administration, the registration and support functions were contracted first to SRI International in the late 80s, and then it was moved to Network Solutions in the early 90s. In the 90s, we found – well, actually, in 1991, we found that the Internet was exploding and growing. The U.S. government was basically handling most of the coordination and

administration, and that really wasn't feasible. So, the technical community decided to form the regional Internet registry system. Regionalization put IP addresses in the hands of organizations that would speak the same language, that would understand the needs of their regions.

So, that started in 1992, actually. Eventually, also in the early 90s, the IP number resource administration was split off from the domain name registration. So, IP addresses were a finite resource. There were limited numbers. They needed stewards to sort of watch over them, to handle them. Domain names were unlimited. They became a for profit business. You could buy domain names. So, the functions were completely split off. The U.S. government at that time also separated the administration of the commercial Internet, which went to the InterNIC that was run by Network Solutions. They handled all of the domain name processing, and the military Internet, which was called the Defense Data Network Information Center.

I think that happened around 1993, 1994. So, this is sort of how regional Internet registries were formed. So, these early registrations, they're referred to as legacy space, the IP addresses. This comes up later in the slide, so I just wanted to tell you a little bit about this legacy space. This is space that was issued by the RIRs I'm sorry, prior to the RIRs by the predecessor registries, by those government contractors. They were issuing IP address space to organizations that came in and requested it. And they were issuing it very liberally. Anybody could come in. They could say, I'm an education, or I'm a research, or I'm a corporation, and I need this amount of addresses. There were no policies, so the RIR I

keep saying RIR, I'm sorry the registry would issue those numbers to these organizations.

They were simple requests. There were no written contracts required. There were no policies. They were just based on trust. I need addresses. Here you go. Let's register you in the registry. This was really not a feasible system. The Internet was rapidly expanding, and distribution just could not be managed that way. So, the RIRs came into play around, like I said, the early 90s.

Sorry, I'm trying to get this to work. So, an RIR, Regional Internet Registry, what do we do? Our main function is to manage the allocation, administration, and registration of Internet number resources in a specific region of the world, regionalization, IPv4 addresses, IPv6 addresses, and autonomous system numbers. So, who are the RIRs? As I mentioned, the system, the Regional Internet Registry system, started it was established in 1992. The RIPE NCC was the first RIR, and they're headquartered in Amsterdam.

You can see there's color coding for each of the regions, so you can discern who's managing what region. APNIC, the Asia, Pacific Network Information Center, was established in 1993, and they're headquartered in Brisbane, Australia. ARIN was the next RIR, established in 1997. We are headquartered in Chantilly, Virginia. At this point, in 1997, ARIN was still managing all of the administration for Central and South America and the Caribbean and Sub-Saharan Africa.

RIPE NCC was managing North Africa. But in 2002, we created LACNIC. LACNIC was created, and ARIN turned over the administration of the resources to LACNIC for South America, Central America, and parts of

the Caribbean. ARIN still manages half of the Caribbean. And AFRINIC was formed in 2005. AFRINIC is headquartered in Mauritius, sorry, and LACNIC is headquartered in Montevideo, Uruguay. Anyway, AFRINIC was formed in 2005, and RIPE NCC and ARIN were managing that, and we turned that over to AFRINIC to become their own fully formed registry. So, that's the five RIRs. So, the core functions, as I mentioned already, we manage and distribute IPv4 and IPv6 addresses and autonomous system numbers. That's our main function.

That is why the registry existed. But there are other core functions that we do. One of the ones that you obviously would have heard of is WHOIS. We maintain directory services. So, we have a WHOIS registry. We have a WHOWAS. We offer WHOWAS, which is the archived records. The ones that are removed from WHOIS can still be found in WHOWAS, and you can request access to WHOWAS. And we all run routing registries where routing announcements are put into the system so network operators know who to exchange information with. We also provide reverse DNS function. You know about domain names to IP addresses.

We provide the opposite function, IP addresses to domain names. I did that right. A third function is we support internet infrastructure, and we do that in several different ways through technical coordination with our colleagues, our internet industry partners, through our community driven policy process, and we're going to touch on that. All policies are developed by our communities, not by the RIR themselves. And then we all offer training and capacity building. Sorry. This is like not. Okay. So, the RIRs are independent.

As I said, they were originally, prior to the establishment, they were run under U.S. government contract, the registry. When the RIRs were established, they were independent. There was no government oversight at all. They are not for profit. They're 100% community funded. The fees are for services and not for the number resources. We are not selling IP number resources. We are providing services to our membership. Membership is open to all number resource holders. Anyone who comes into the registry and obtains IP addresses or autonomous system numbers through policies are able to become members, and most of the RIRs interact and are supported by their membership.

Our members are typically internet service providers. That's sort of our largest membership holder, but we have governments, corporations, universities, and others who come to us for addresses and are members. Now, I mentioned the community developed policies. Our communities develop the policies. The staff facilitates the process. We have member elected governing boards who actually finalize the policies that get implemented by the staff, and all processes, policies are all open and transparent. Everything's documented on our websites. I'm sorry. I'm still finding that magic spot to do the clicker. Oh, up there. Sorry. As far as RIR governance goes, the RIRs operate in accordance with three main factors. I've already mentioned community policies.

They are all done by our communities and facilitated by us, and we distribute and register those resources based on policy. We also operate under a national legal framework. Each RIR is established in a particular country, so we operate under the legal framework of that

specific country. Finally, our technical remit, our mission. The five RIRs fulfill this specific function in the global internet governance system. We are distributors of internet number resources. Oops. Okay. So, we're going to talk about the regional policy development process, how it happens. It all starts with the community, as I mentioned. Oh, this is going to be challenging. Okay. It is inclusive. Anyone can participate. You don't have to be a member.

You can even be from another region. If you have an interest in policy, you can propose a policy. It's transparent. Everything's documented, published. There's policy development process that's published. It is bottom up. Community develops. Staff implements. The way the cycle works is there's a need established. Someone in the community says, we need this policy because this isn't working right, or we need to accommodate this group. So, there's a need. It is discussed on mailing lists. Each of the RIRs have their own mailing lists.

It's discussed in RIR meetings. Then consensus is gauged from a combination of mailing lists and meetings. This is typically gauged by the working group chair or by the advisory council. In the ARIN region, we have an advisory council, but somebody is facilitating that process specifically. That's then eventually implemented. It's ratified by the boards. So, policy gets ratified. That's the final process. Then staff takes it over and implements it. Staff and the community evaluate whether a policy is actually working. Is it supposed to work? If it's not, it goes back into the process for a change. So, as we said, the community approves and proposes these policies.

That's kind of the life cycle. So, the number resource organization. The five RIRs work together quite often. In the ICANN world, we are together. We are known as the number resource organization in the number's world. In the ICANN world, we're known as the address supporting organization. I have a slide on that, that I'll show you in just a minute. This is a new mission and vision statement. Forgive me for reading it, but the mission is to coordinate and support joint activities of the RIRs to provide and promote the joint internet numbers registry. The vision is to be the flagship and global leader for collaborative internet number resource management as a central element of an open, stable, and secure internet. That is the vision of the five RIRs together. There is a link if you're interested in knowing more. Still not getting this. Okay. So, oops, sorry. So, I pulled this right off of the ICANN website so you could see where the RIRs sit within the ICANN ecosystem. We are a supporting organization. We are the ASO. As I said, in the ICANN world, we're known as the ASO. In the number's world, we're known as the NRO. There're three supporting organizations. They develop and recommend policies concerning the internet's technical management within their areas of expertise.

So, I just wanted to show you that so you could get an idea of where we sit. Okay. So, there's a little confusion. There's the ASO within the ICANN world. The ASO is the number resource organization. It is the five RIRs working together. There's an address council that is elected by our communities. The address council has a very specific purpose. They're known as the ASO AC or the NRO Number Council, the Number Resource Advisory Council. In the number's world, it's kind of twofold. There're two references to the ASO AC. There are 15 members in total.

There are three from each region that are elected by their communities. Two are elected At-Large. One is appointed by the RIR board itself. And then RIR and ICANN observers participate in the ASO AC process.

The terms of office are different for each RIR. And their main purpose is to advise the ICANN Board on internet numbers. And there's three main areas. They oversee the global policy development process. And I have a slide on that I'll show you in just a minute. They also appoint two ICANN Board members. And they appoint one member to the ICANN NomCom. So, those are the three main functions of the ASO AC. So, the global policy development process. On the left, we've already talked about the regional communities.

The regional community develops a process policy. It goes into the RIR for consensus. And the RIR is implemented. But when the five RIRs are working together on a global policy, that's when it comes into ICANN. So, a global policy is any policy that affects the relationship between IANA, who issues the numbers at a global level, and the RIRs. So, the way that IANA would issue autonomous system numbers is a global policy because they apply the exact same policy to all five RIRs. A global policy is actually discussed in each of the five RIRs.

And then, the policy is facilitated by the ASO AC. They make sure that the global policy gets from the five RIRs into the ICANN world through the ASO to the ICANN board for ratification. So, they are the facilitators of the global policy development process. That is a big distinction between the ASO AC. The ASO is the five RIRs. The AC facilitates the process and does a couple of other things, as I mentioned previously. So, we're going to move into talking about internet number resources,

what they are, how they work. I'm going to turn it over to Germán. He's going to go through IP addresses and routing. And then, I'll take it over in just a minute.

GERMAN VALDEZ:

Thank you, Leslie. Well, after we talk about, in general aspect, what the RIRs are, what we do, where we fit in this huge internet ecosystem, I'm going to start talking about a little bit the basic aspects of what kind of resources we are managing. So, I will talk in specific about three number resources, IPv4, IPv6, autonomous system numbers of ASNs. So, and this information is very basic.

It was designed for people that are not very savvy in these terms and also for newcomers of ICANN. And so, excuse me if I go into the very basics. But, well, there are two kind of internet protocols, two kind of different IP address. The first one is the IPv4. It's set in a limited number of resources in there. We have 4.4 billion numbers that are mostly scarce. Most of the RIRs, at least three of them, are not able to provide more IPv4 addresses because they are completed the whole pool of resources. But then we have the IPv6 numbers, which is, I won't dare to say how much of those resources are available, which is something, as this slide represents, 50 octillions of each of the human beings in this planet. So, this is a huge amount of IP addresses.

The reason that we don't have IPv4, well, this is a protocol that was invented in the 70s and was never expected to have this kind of success in terms of the demand of the resources. The other number that the RIRs managed and distribute are the ASNs. This number represents a unique autonomous system, which is a group of networks, IP networks,

that are managed by a single entity or single corporation, single organization. Think about the more classic example is on internet service providers that have a complex set of networks that need to be administered. So, all these sets of networks require a unique identifier that we call the autonomous system numbers.

The RIRs also manage this identifier. This is used for routing. This is a key component of the routing system, which allows us to move the information from point A to point B, the source to destination. These numbers are limited and administered and managed by the IIRs. So, that's it. We are talking about IPv4, IPv6, and ASNs. Those are the resources that the RIRs manage for their own regions. This is an important reminder. IP addresses are recognized by computers. They are different of domain names, of course.

They are required for routing. They need to be a unique identifier for each device that is connected to the internet must have a unique number associated in order to be properly routed. This is different to the domain names. The domain names are recognized by people. Normally, the process is that we match a domain name with IP address. That allows or facilitates people to remember locations, websites, and some services in the internet. In terms of routing, the routing uses the identifiers I just mentioned, IPv4, IPv6, and ASNs. How are IP addresses issued? This is done in a hierarchical manner. In the top of the tree, we have ICANN and IANA. They have five clients in terms of distribution of internet number resources.

They have only five. IANA distributes these resources to AFRINIC, APNIC, ARIN, LACNIC, and RIPE NCC, and only that. They are managed by a set

of global policies that was described by Leslie before. Subsequently, the RIRs distribute or allocate the resources to their own regions based on policies that are determined by their communities in each region itself. Also, Leslie explained how these policies are developed, are open, and transparent. You don't need to be a recipient of these resources to participate in policy discussion.

Anyone can take the mic and participate in the discussions, can participate in the meetings, can participate in the mailing list. You don't need to be a recipient of these resources to participate. The RIRs apply these policies to distribute the resources downstream. It could be to an end user that could be a big corporate that will use the internet resources for their own corporation, their organization, for their own employees, or could be done through an ISP that will distribute those to their customers or another end user.

This is a hierarchical process, the hierarchical structure of how we distribute this. The regime that we do that is according to the policies. Then we talk about routing. We need to administer these resources, so we guarantee that we have unique identifiers related to a specific organization. We avoid duplications. In terms of the functions that we need in routing, we have two basic critical systems. One is DNS, which translates domain names to IP address, which I think is 95% of the discussions here in ICANN.

We have also Routing, which is the process to move IP packets through the network from source to destination. That's the two critical systems, both required to have unique identifiers to be successful, to allow to work. It's important to mention that these protocols, the DNS and the

TCP IP and the routing are not very secure. In the case of DNS, also it was a protocol that was invented 40, 41 years ago. It was another time. It was based on trust. In the case of TCP IP, it was invented in the 70s, and it's in the same situation.

We are adding security layers to these protocols, which also are part of the services and the responsibilities of the RIRs right now. Leslie will explain more about that. One of the other services is the Internet Routing Registry, which is a set of databases that include information on how these organizations are doing the routing and what set of blocks of addresses they are managing, to whom they are announcing, so other people, other organizations can use this information to validate their own routing. That's another service that we provide. In general aspects, the Internet is a big cloud that has many devices connected. We have hand devices. We can have servers.

Nowadays, more and more different pieces of technology are connected to the Internet, refrigerators, cars, dishwashers, etcetera. We don't know how these are managed in this big, huge cloud that is the Internet. The truth is that behind that, there is a set of different networks. A hand device can be connected to a mobile network. An airplane can be connected to a satellite. We can have computers and servers connected to a more traditional network of fiber. All these networks require what could be the raw resource, which is the Internet number resources. They require IPv4 or IPv6 to connect.

As I mentioned before, they must be unique in order to be connected to the Internet. At the exchange of routing with other autonomous system numbers. That's the importance and the relevance of these protocols.

Right now, we have a little more than 75,000 autonomous system numbers that are published in the global route table. That means somehow there are 75,000 different organizations that are involved in the routing of the Internet nowadays.

That piece of data was from last Friday. What the RIRs do is that we keep a record of all these resources and the associated organizations that are managing. That's the core business. That's the core function of the RIRs. It's to keep that registry as secure as possible, so we avoid duplication and allow the Internet operators to actually make a good route of their resources and allow people to connect to the Internet successfully.

LESLIE NOBILE:

Okay. I'm going to take it back. German mentioned the depletion of the IPv4 address spaces. This was a significant event in the life of the RIRs. Global depletion at the IANA level happened in February of 2011. IANA handed out the last slash eight, the very large block that's dictated by policy to the RIRs on the 3rd of February. This is a picture of all the CEOs. Of all the CEOs and IANA management leadership at that time. So, this was very significant. It created many different scenarios that we're going to talk about today.

So, right now, each of the RIRs have some IPv4 address space. Right here you can see, this is current as of 12/23. AFRINIC still has 0.07 of a slash eight and APNIC now has 0.15 of a slash eight. ERIN, LACNIC and RIPE NCC have zero that are available for allocation. I will tell you that each of the RIRs do get IPv4 address space handed back to them. Either it's returned to them, some people don't put it out on the IPv4 market,

which I'll talk about or the RIRs can reclaim space for non-payment of registration services. So, we all get some space back and you can see APNIC and AFRINIC are the two RIRs that have a little bit of space right now left to hand out to their communities.

ERIN LACNIC and RIPE may have some space, but it's reserved for some particular purpose and its very little bits of space. So, nothing available to allocate right now. So, looking at a post IPv4 depletion world, can I just, I need to just check one slide. Sorry, I'm going the wrong way. I need to go backwards one. Okay, so that's the available space. I just wanted to make sure I did not skip a slide. Okay, post IPv4 depletion world, what's happening in post IPv4 depletion world? So, the movement to IPv6 has been steady. The RIRs have been issuing IPv6 address space since 1998. It started out very slow, but the ISPs have been steadily rolling out IPv6 into their networks.

We have seen a steady increase in IPv6 traffic, particularly in recent years. In the beginning, it was very, very slow, but it has been steady and increasing. And IPv6 requests are increasing at all five of the RIRs, but we're also still seeing a high demand for IPv4 addresses. Some people are just not ready to move to an IPv6 world, and they're still coming into the RIRs requesting, you know, IPv4 space. And some of us receive significant numbers of requests still. But what we are also seeing is that the customers are, so they're out there searching for IPv4 address space. So, there has been an IPv4 market for address space that has come into play.

I'm going to talk about that in a later slide, but there are addresses out there that are available to organizations, and they are actively pursuing

those. So, because there's such a limited supply of IPv4 addresses and such a high demand, the RIRs are seeing an increase in fraudulent requests. It has really increased. We've always seen some bits of fraudulent requests, particularly before we ran out of IPv4 address space, people were hurrying to get addresses, and they were maybe, you know, exaggerating some of their requests.

So, we got pretty clued into looking for these signs. Right now, the fraudulent requests have really increased, and people are submitting falsified business records, falsified personal ID documents, et cetera. And what we call it is they're attempting to hijack registration records. They're trying to get IP addresses that don't belong to them, and they're trying to proclaim that they are those organizations that have them. So, the RIRs have gotten pretty clued in on that activity, if you will. So, talking about IPv6 deployment, because this is all happening at the same time. There is an IPv4 market, and there's also IPv6 deployment really happening.

These are kind of some of the success stories. This is some of the recent activity and stats we're seeing, which are showing us that IPv6 is being deployed more and more. So, per ISOC, in 2023, the rate of v6 deployment increased the most it has since 2018. So, it's growing from 34% to 39% globally. And what ISOC has seen is that IPv6 deployment has risen about an average of 3.5% each year since December of 2017. And that is an increase from the early days when we were seeing like a half a percent or 1%. Google IPv6 stats are showing that roughly 40% of global internet traffic is now being passed over IPv6. So, that's a good number.

We're getting there. And APNIC Labs, who also does research on IPv6, says that the most significant gains in recent years were measured in the Asia Pacific region. IPv6 deployment across Asia increased from 37.2% at the end of 2022 to 42.3% at the end of 2023. So, that was pretty rapid considering past rates. And across the same time, APNIC says that Oceania increased from about 32% to a little over 37%. So, that's what we're seeing globally as far as deployment goes. So, if you look at the IPv6 space that's currently been allocated at the RIRs, and this is total IPv6 space that's been allocated since the beginning, as I said, I think it was 1998.

And you can see that most of the v6 allocations are happening in the RIPE NCC region, followed by ARIN, APNIC, LACNIC, and AFRINIC. And I will tell you that AFRINIC was, they retained their IPv4 space. So, they were issuing IPv4 space and still have a bit left. So, their IPv6 allocations and requests were not quite as active as some of the other regions because they were the last RIR to have IPv4 address space available. But this shows actually a very different number. This is interesting. So, the percentage of RIR members that have their IPv6 allocations, it looks quite different because you'll see in the RIPE region, well, I'll start with the LACNIC region. Almost 100% of the LACNIC membership has an IPv6 allocation, followed by RIPE, which is what, almost, I don't know, 73% and AFRINIC, look, over 50%, APNIC, close to 67%. And ARIN, only around 46%. And it's interesting to see this.

I will tell you that some of this depends on policies in the regions. LACNIC has a policy that says any ISP who has an IPv4 allocation immediately gets issued an IPv6 allocation. They don't even have to justify it because they have an IPv4 allocation. So, that's why you're

seeing that 100% in the LACNIC region. Almost every ISP gets issued an IPv6 block by LACNIC. So, going back, like I said, concurrently there's an IPv4 transfer market as the IPv6 is being deployed. So, this was developed because there's been an ongoing demand for IPv4 address space. It was rapidly depleting. Something had to change.

The choices were either the communities, the RIR communities would either facilitate IPv4 market-based transfers through RIR policies, or we would all watch a black market emerge and there'd be no registry interaction. The RIRs would have no idea who was utilizing the space. Therefore, who is would not be reflecting the accurate registrant or the accurate person using the addresses. So, the RIR communities developed needs based IPv4 market transfer policies. This allowed current IPv4 holders who had excess IPv4 space to transfer the space to a qualified recipient, someone who could qualify with a need through the RIRs. There's a lot of the legacy space that wasn't being used or routed, a lot of that old space, people forgot they even had it. So, they've been hit quite heavily by organizations seeking out IPv4 address space.

And they do financial transactions together behind the scenes. So, an organization will find an IPv4 address block from another organization, they will come to the RIR, respective RIR, and they will request a transfer from this person who has a lot of space to this person who has nothing. And the recipient has to qualify under the policies. They are needs based still. So, the RIR's role in all of this is to ensure compliance with these needs-based policies. We want to make sure that the accuracy of the registry is maintained and that the proper registrant is reflected in the database.

So, that is our main goal, policy compliance and accuracy of the registry. The RIRs aren't privy to any of that financial transaction information because that is all done before an organization ever comes to the RIR. We're not involved, we don't know what price is, we don't know what's going on. We just want to make sure they meet the policy and that they are vetted, thoroughly vetted. We are very careful about researching and analyzing who's coming to us, whether they're all authorized, both parties, and we have a very, very specific detailed process for doing that verification. So, looking at transfers that are happening within the RIR, intra RIR transfers. So, this is the number of transfers per year that are happening within each of the RIRs. And you can see a lot of that activity is happening in the RIPE NCC with the, these colors are so similar, I'm sorry, with that one of the blues.

We probably need to change this. So, a lot of the activity is happening in the RIPE NCC followed by APNIC and ARIN. This is the inter RIR-IPv4 transfers. These are the IPv4 number resources that are moving from one RIR to another region. AFRINIC is the only RIR that does not have an inter RIR transfer policy. So, all the activity right now is happening between the other four RIRs. ARIN and RIPE and APNIC had the original policies. LACNIC's policy was only recently implemented in the past year or two. And so, most of the activity is happening between ARIN and RIPE NCC and ARIN and APNIC. You can see the number of transfers on the top of the box and the number of addresses transferred on the bottom of that box. So, it's pretty active between those three RIRs. So, we're going to talk about now—

NICOLAS ANTONIELLO: Just sorry for interrupting you. There's a question in the chat.

LESLIE NOBILE: Oh, sure.

NICOLAS ANTONIELLO: That should be in the Q&A pod. But anyway, we are going to do an exception and read it out loud. Stephen Dacke is asking, how are IP address conflicts among RIRs and their customers resolved and what role do ICANN play in such resolutions?

LESLIE NOBILE: So, it's a good question. I wish I still had my lawyers in the room because a lot of that actually is handled between the lawyers. Because often it is by documents. Documents that organizations have submitted to us. ICANN doesn't play a role in that. The RIRs handle any type of conflict. I can actually tell you that we haven't seen any actual conflicts at this point. We thought that we would see more. But between the RIRs, there's been a very clear process. Each RIR has their own policies. And we make sure that the organizations meet those policies. But we have not seen any type of conflict that had to be resolved as of yet. Even though we did anticipate that, it hasn't happened. So, okay. So, we'll move into sort of the final stage. And we'll talk about RIR services and tools.

And as I said in the beginning, these are the tools and services that we offer in common that are heavily utilized by our communities. Although each RIR has their own services and tools, we're just going to talk about

some of the major ones. So, WHOIS, the one that everyone knows. What IS WHOIS? It's a public directory service. And it's used to query databases that store information, the registered users of an internet resource. That's a pretty simple explanation of what WHOIS is. It does differ in usage and content.

There're several different types of registries. There's the number resource registry. That's the RIR-WHOIS that you would look for. There's domain name registries and registrars. They all run WHOIS. And at this point, and I just will mention really quickly that it's more difficult to access domain name registry and registrars WHOIS. They were subject to GDPR. And they are masking some of the data to be in accordance with this GDPR policy coming out of Europe. And we'll touch on that again. And then there's routing registries. German mentioned it.

I think I mentioned it. That's where routing announcements, routing information is stored. All five of the RIRs run their own routing registries. As I mentioned, RIRs-WHOIS is still publicly accessible, whereas some of the domain name registries and registrars, you're not going to find all of the information. In the RIR-WHOIS, all of the registered information is publicly accessible. It is part of our mission. And I think our CEOs, our boards determined that because it's part of our mission, it's part of our work, we are obligated to our communities to provide that information about who is using IP number resources.

So, what information is in the RIR-WHOIS? It is registration data, publicly displayed registration data. It includes every IP number resource that the RIR has issued or that a predecessor registered. So,

that's the early registry is issued. That was the early registries done under U.S. government contract. That's the legacy space. All IP addresses are accounted for in the five RIR databases. It contains information about the organizations, the registrants who hold those number resources and their point of contact information.

And that will include mailing addresses, email addresses, phone numbers. WHOIS displays the original registration date. So, you may see an IP address that was issued in 1988. It also includes the last updated date. So, you can see who's actually actively using or manipulating their registrations because the last updated date will show in the RIR WHOIS. It also contains customer reassignment information. We told you ISPs issued to their customers. All five of the RIRs have a policy that requires a large portion of ISPs to customers to be registered in the database. There are some exceptions for privacy purposes that the RIRs have. We still collect that information, but we hold it private because our policies prohibit us from putting that publicly, making that public information. But we always have that information available.

And then we have referential information to the authoritative RIR. So, if you're looking for an IP address in ARIN, but it's actually in APNIC, we will, the RIR WHOIS will point you to the right authoritative RIR who would have the information. So, WHOIS, the future of WHOIS. WHOIS is limited in scope and purpose. It is not very versatile. It was developed a long time ago, very simplistic, doesn't have a lot of information and a lot of availability. And it's certainly not available in a machine-readable way. So, registration data access protocol was developed by the technical community several years back.

It's a new protocol for accessing this registration data in a machine-readable way. It has features that WHOIS does not. It has standardization, it has redirection capabilities, not only to other RIRs, but to domain and registries as well. It has support for user identification, authentication and access control, and it supports internationalization. WHOIS was not robust, RDAP is robust. So, it is going to be heavily utilized. And eventually, I think the purpose, the point was to replace WHOIS altogether. But right now, all of the registries run concurrent WHOIS, port 43 WHOIS and web based WHOIS.

ICANN has required that all accredited registrars and gTLDs registries implement RDAP as well. All five of the RIRs have implemented RDAP. Some of the domain name registries have set it up. And if you go to one of the RIRs, you're going to have an option. You can use RDAP to query or you can use WHOIS. You have an option still. So, WHOIS was one of our main tools. We're now going to talk about routing security tools because that's a big area. There's been a lot of hijackings, route hijackings and nefarious activity in the routing world.

So, the RIRs have worked together to deploy two technologies to help secure the internet's routing system. There's RPKI, which is Resource Public Key Infrastructure. We're going to talk a little bit more about these in later slides, but I'm just as a high level. RPKI is a security framework and it's designed to help improve and secure the internet's routing infrastructure. It will verify the association. It does this cryptographically, verifies the association between who has an IP number resource and who the organization is. So, the registrant and their number resource. So, that is done cryptographically.

There's also something called, German mentioned the IRR, the Internet Routing Registry, which stores routing information and route announcements. We're working on validated IRR. Currently, or prior to this, as we said, the internet was based on trust. So, an IRR allowed any network operator to put any route into the routing tables. Just type it in and that was it, no verification. You could put anything you wanted, quite honestly. We're adding validation mechanisms so that we can guarantee that the route announcements that are being published are only being published by the authorized network.

So, all five of us are working to secure our IRRs. So, RPKI. This is just a high-level look at this. It is actually a complex system. Network operators have been required to use it or are using it and it takes some time to learn. So, it's a public key infrastructure. I already mentioned that. It helps to secure the internet's border gateway protocol routing infrastructure. It does this in two ways. It cryptographically certifies the network resources and it cryptographically certifies the route announcements.

So, it's verifying that the IP number registrant and the IP address go together. They are authorized. It also does route announcements through the use of ROAS, which is a route origin authorization. And that defines which autonomous system is authorized to originate an IP address prefix. So, those are the two ways that RPKI works. It does provide much stronger validation than any existing technology, including the IRR, which as I said, can be subject to misconfiguration. It can be subject to FAT fingering or just malicious activity because anyone can enter anything. Or it provides stronger validation than something that's been used from the beginning of time, which is a letter

of authority. That means an organization can take a letter of authority and bring it to an ISP. And it says, these are the IP addresses that belong to me that I'm going to have you route for me. Those are often forged.

NICOLAS ANTONIELLO: Can you speak a little bit slower?

LESLIE NOBILE: Oh, sure.

NICOLAS ANTONIELLO: Thanks.

LESLIE NOBILE: Yeah, sorry. They are often forged. They are a way of hijacking internet number resources and routes. So, they're not secure. The five RIRs are collaborating on this RPKI cross RIR project. We've been working very closely together to get RPKI into our communities. So, why is it important? What does it even mean? It establishes a level of trust that has not existed before. It ensures that the information is authentic and it confirms that it's coming from the authorized holder of the resource. It also gives the network operators a method to make better judgments. It's certainly better than IRR or LOA.

It makes sure that the valid source, the origin of a route announcement, is coming from the authorized person. And then it can limit the impact of those configuration mistakes or that malicious activity of a bad actor. Like I said, LOAs can be forged. IRR, you can put anything you want into

an IRR. And there's been actually well-known situations, countries who not even maliciously but made an error in their routing tables and took over an entire network from an organization, another organization in a different part of the world.

So, it's, yeah, RPKI will prevent much of that type of activity. So, if we're looking at RPKI adoption across the RIRs, this chart shows the percentage of IP address space that's currently covered by RPKI certificates. This is as of 12 February. So, you can see that it is happening across the regions, anywhere from 29% to about 67% in RIPE, 29% in AFRINIC have issued RPKI certificates for their RIR space. So, they are covered under RPKI certificates. And if you're looking at IPv6, a little slower in the AFRINIC region, but it's actually up to 63% of IPv6 addresses in the ARIN region are covered by RPKI certificates.

So, it's increasing steadily. And as the larger organizations are demanding that their customers utilize RPKI, it is becoming much more implemented in the world. I think Cloudflare was one of the organizations and Amazon, they demand that their customers implement RPKI. So, that's helping with the process. So, we are going back to the Internet Routing Registry. What does it actually mean? Well, we told you it's this database of internet route objects. And they're operated by individual organizations. For example, the RIRs operate IRRs, but other organizations do as well. Sometimes it's a fee for service. Sometimes in the case of the RIRs, there is no fee for service. It's used to determine and share routing policies and announcements between network operators.

That's what they use to make sure that they should be routing the space and that they know where address space is supposed to be going. It ensures stability and consistency of the routing system. It provides a mechanism for validating the contents of the announcements. It is widely deployed. It was the first, the original way of exchanging routing information. And it was deployed to prevent accidental or intentional routing disturbances, but it hasn't been fully successful at that. As I said, it is susceptible to error or manipulation. So, it was always based on trust. In the early days, no one thought anything would, that the internet would become what it became today.

So, and as I mentioned, the RIRs are working individually to add better validation processes to ensure accuracy and enhance security. We're looking at who's putting in route announcements. Who is the authorized registrant to do this route announcement? We do that before it ever gets into the IRR. So, this is a link to all five of the RIRs. If you want any more information on anything we've talked about, there it is. It's available. And I think this presentation will be available as well. Not positive, but Nicholas, it is, correct? It's the presentations available for the community. Okay. It'll be shared. Okay. I think that's all we have. We just have questions. If anyone has them, we are available to answer them. Is there anything online or anywhere?

NICOLAS ANTONIELLO:

We have no questions online, but we have questions here. Yeah, go ahead.

JOHN MCELWAIN: Hi, John McElwain for the record. I was just wondering if you could speak a little bit. I'm coming from the naming side. I'm with the IPC. Wondering if the IRRs, RIRs are doing anything with respect to DNS abuse. Do you have any policies or tools that you might recommend?

LESLIE NOBILE: So, okay. We clearly separate ourselves from DNS, but we know the problems of DNS abuse. We know it's out there. The only thing that we offer is DNSSEC. The RIRs have set up DNSSEC for our customers. We've found that it's not taking hold as much as we thought it would. It is a complex system, and I think you all probably know that if you know DNS. But that is it. We don't have policies directed toward domain name abuse. We try to cover IP address abuse and hijackings and do verification on our side. Do you have anything to add?

GERMAN VALDEZ: Just to add that maybe the commitment to have a registry and information on WHOIS as accurate as possible is also helping to address, to locate and get to the actual ISP that are routing the IP address that are the source of any abuse. So, that's also part of the commitment of the RIRs to have the more accurate registry.

JOHN MCELWAIN: Maybe a follow up, and I might have not stated it correctly. How about any policies for IP address abuse? If I know a particular IP address is being used abusively, is there any reporting or any tools to help with that?

LESLIE NOBILE:

Yes, there are tools. In the ARIN region, I think all of the regions have this. We have a fraud reporting system where anyone can come in and report fraud. It's really fraud from within the registry system side. Did somebody hijack an IP address or something to that effect? It's not really a place to report abuse. However, our contracts, most of the RIRs have something within their contracts that they sign, that all registrants sign, that says when you get these resources, you cannot break the law. And if you do, we can actually come after you.

So, we often get reports or we find ourselves that there's abuse going on. We find that there's illicit activity happening, actual real illegal activity happening. We then take that and report it to law enforcement. I've worked with the FBI for years on this. That's actually part of my role. And the other RIRs have been doing that as well. When they see that or if it's reported that there is illegal activity, but we don't monitor the usage of IP addresses. That's not part of our mission.

Someone comes to us, they meet a policy, they have a clear need. We've done the vetting and verification that they are actually an organization, a legit organization that has a need, they take the address space, they do what they will with it. They tell us one thing, but we don't know and we don't monitor if it's illegal activity. The only way we can address it is not proactively, but after the fact, if it's reported to us.

GERMAN VALDEZ:

Just to add, yes, there is some, it's not a policy, but it's more a mechanism, internal mechanism, a framework where the RIRs can

cooperate to investigate any fraudulent use of IP addresses. It's part of a kind of task force between the legal team and registration services managers. They have a mechanism to investigate and take actions.

LESLIE NOBILE:

There was one question, I think, back here. And then there's another one here.

JAVIER RÚA-JOVET:

Thank you, great presentation. I'm Javier Rúa from Puerto Rico here. Welcome to San Juan. Are there technological reasons or compatibility issues that would explain why someone or some entity or some region doesn't adopt IPv6?

LESLIE NOBILE:

That's a good question. We get that all the time. I think everyone gets that. I don't think there's any technical reason. Most of it is that organizations don't want to put out the effort. They don't get it to the sea levels. And the sea levels, let's face it, most ISPs are in it to make money, right? So, they want to continue their business. They know IPv4. They know the internet operates on IPv4. They're not ready to transition to IPv6.

They don't want to dedicate the resources or the effort. I mean, that's a simple answer. And I'm sorry, I hope I'm not insulting any ISPs, but that's what we hear, okay? But technological reason, none whatsoever. Because all equipment now is IPv6 capable. All routers are IPv6 capable. In the old days, 15 years ago, not all the equipment was and

that was an excuse. But now, it's all ready to roll. I don't know if Germán has anything to add, but that's the answer.

GERMAN VALDEZ: Yeah, well, yes. Being a little bit honest about it, yes. There are no technical barriers. There is a lot of training material as well that is available. I mean, in terms of capacity buildings, there is plenty of content where the engineers can rely on and prepare themselves and immigrate to an IPv6 network as well. So, it's more a decision, a business decision aspect, yeah.

LESLIE NOBILE: I think there was one question.

MICHAEL GARGIULO: Hi, Michael from vpn.com. To follow up on the abuse question, I'm curious on how ICANN handles the countries that may be using IP spacing to do inappropriate things themselves. So, think state sponsors of terror. If ICANN is in a reactive state and is only able to go to the law enforcement agencies that are in that country, and that law enforcement agency is beholden to the state sponsor of terror, there's kind of this vacuum where they use the IP spacing to do whatever they want.

Maybe my policy understanding is a little limited, but I understand the ccTLD agreements stipulate some pieces of this, but that's different than the spacing agreements that we're talking about today. So, I'm curious on how those policies develop over the next 20 years. And as

we see just the rise of countries doing not so great things with the internet themselves, maybe not so much bad actors in the country that are third parties, but how do you see that being managed in the coming future?

LESLIE NOBILE:

That is also a good question, and one we get. So, ICANN isn't actually involved in anything to do with IP addresses. Like ICANN, from an IP address standpoint, IANA controls and manages that global pool of addresses. They are not actually involved in the regional internet registries business. The RIRs will handle. If we know that there is state, again, I wish I had my lawyers here. They had to leave for another session. But if they know that there is activity happening, the RIRs will report it. It doesn't involve IANA at all. And it actually can be a global system.

So, when I've worked with the FBI on things that may be happening in another country, and in fact we did, we had something between, I wonder if I can say it, something happening in Africa and something happening with a Russian business network. It was actually public information, so I can say that.

So, we worked with the FBI, and AFRINIC worked with the FBI, and the FBI worked with their counterparts in other countries to try to solve these problems, and they were able to successfully do that. Sometimes, with some of that state sponsored activity, I don't really know, and I do wish I had a lawyer here. But it is handled at the RIR level, and global law enforcement does work together to address some of these issues. And it's been noted and documented and been successful, actually.

MICHAEL GARGIULO: Just a quick follow up to that. Do you ever see a future where some countries just don't have access to the traditional internet the way we've given them, the way we give? I mean, pretty much any country, if they're sovereign, they can come and get a ccTLD, or they can come and get spacing from the RIRs, and it doesn't really matter. Do you see any policy ever coming into effect that would limit that if they're, let's say, sanctioned by the U.S. government?

LESLIE NOBILE: Oh, well, that's another question in itself, and I wish we had RIPE here. But if there are government sanctions against a country, for the example in the U. S., ARIN is not authorized to do business with a sanctioned country. I think it's the exact same in the RIPE region. And RIPE just actually had, they hired a PhD woman to do a study on sanctions and to make recommendations.

So, they have a lot of information on sanctions. They're much more limited. I mean, they have more issues within their region than some of their countries, and they have a lot of good information on sanctions. But I know that most of the RIRs are unable to deal with countries that their own government has sanctions against. I don't know if that answers the question.

GERMAN VALDEZ: Yeah, that's a very good question. All the RIRs, as was mentioned by Leslie on the slide, are subject to the national regulations as well. And

in some cases, well, they have to deal with countries that are under sanctions. They might not receive resources from those countries by paying the memberships. But as it is today, there has been no cases where an RIR is involved in cutting connectivity or limited connectivity of any country. While the example is when LACNIC was in process of creation back in 2002, the question was about Cuba.

Cuba was under sanctions of the U.S. and it was going to move to a new registry that's going to provide the service. And the U.S. government never puts any kind of conditions for LACNIC to provide the services to Cuba. So, yes, they were under sanctions, but in the case of LACNIC, they're based in Uruguay. They have a notice of regulation there that didn't stop for LACNIC to provide the services. But in any case, they would never request or pressure or give any indications that services will be limited or cut connectivity at all. Yeah, no worries.

LESLIE NOBILE: Do we have anything else online?

NICOLAS ANTONIELLO: We don't have any more questions online nor in the room. So, thanks very much for the presentation. Great presentation. Presenters, I think, will be available for anyone to talk out of the session. Thanks again very much. The session is adjourned. Thanks.

LESLIE NOBILE: Just a reminder, IANA wanted me to remind you all, they have a session called Let's Talk Numbers on Wednesday. So, if you want more

information about IANA and the RIR relationship, that will happen on Wednesday.

NICOLAS ANTONIELLO: Thanks very much. The recording can stop now. Thanks. Bye-bye.

[END OF TRANSCRIPTION]