MARRAKECH – How It Works: Internet Networking
Monday, March 07, 2016 – 13:30 to 15:00 WET
ICANN55 | Marrakech, Morocco

UNIDENTIFIED MALE: Deploying fiber could be easier because while getting the trench done might be less expensive, but you less people to amortize the cost within it, and we are not necessarily the best way to do it. Wireless technology, while you need to have access to the spectrum, so there's a regulation aspect to it. And that could be quite expensive in some countries.

But, once you put an antenna in place, you can provide access for quite a number of people. And depending on the technology, the radios might be smaller or larger, but you'll just have to put one antenna and not have to get fiber to every single person.

So it's very attractive technology in places where there's no underlying infrastructure. One of the problems, though, is that who wants to see an antenna. I mean, the city could be all ugly, but if you live in the suburb like where I live, I live in Washington, D.C. and actually nice suburbs and nobody wants to see an antenna there.

So you're dealing with city regulation or city ordinance but you're also dealing with neighborhood association who say, "I don't want to see that; it's ugly." So that may or may not be the right solution there.

So combination of both technology are usually what people are doing to get the best of both world. So once you have this basic fiber or basic wireless infrastructure, you can start to connect people. But let's say that I want to have a connection between here and my office in Washington, and I want fiber. I'm not going to have a single fiber that goes from here all the way to Washington. A, that will be cost prohibitive just to put that one fiber for me, but B, there's no way I can get this done. I mean, it's just too long.

So what we will do first is to share fibers between different parties. So, here we go. On the point-to-point link on the fiber, we are sending light, but we don't have to send regular white light. We can send color light. So I can send green, red, blue. For example, what's your favorite color?

UNIDENTIFIED MALE: Red.

UNIDENTIFIED MALE: Thank you.

UNIDENTIFIED MALE: What's your favorite color?

UNIDENTIFIED MALE: Red.

UNIDENTIFIED MALE: Red.

UNIDENTIFIED MALE: Oh, that's interesting. What's your favorite color?

UNIDENTIFIED MALE: Green.

UNIDENTIFIED MALE: Green. Now you see we have a little bit of a problem because if you speak green and you receive green, that's fine. If the two of you speak red, that's not going to work very well. You're going to step over each other. So you need to find maybe different shade of red. Maybe you will have a light red, maybe you'll have a dark red. Okay? So it's a frequency, it's a lambda [inaudible] you change the frequency that you are sending the light through this fiber.

And that way, the three of you could actually share the same fiber. So if you want to have more bandwidth, maybe what you need to do is to use a different wavelength, different lambdas in the same fiber. In that if you have two of them, you have twice the bandwidth. If you have ten of them, you have ten times the bandwidth. So that's how we're going to do that so that we can share this infrastructure so that people can put fiber under the ground and not just one person, but many person can use it.

But still, this will be a point to point, for example, from here in this hotel to the center of Marrakech. It's not going to go all the way to Washington. So what do we do? Well we're going to use bits and pieces of fiber, maybe there's a fiber that goes from the altar to the center of Marrakech. Maybe there's another fiber that goes from Marrakech to Casablanca, and another that goes from Casablanca straight to the ocean to maybe New York, and then another one from New York to Washington, and from center of Washington to my office.

So there may be five, six, seven pieces of fibers that we are going to interconnect point to point. So maybe we'll start using red as your color here, but doesn't mean that will be red all the way. It has to be red in just that particular segment of a fiber. So when we go to the next segment, maybe it will be blue. And simply need to map that particular wavelength to another wavelength and same thing on the other side.

So there are companies who run those fibers. And when they say we establish a fiber path from A to B or from here, let's say, to my office in Washington, what they do is simply put, point to point, all those different fibers together and they find a wavelength that's available on each of those fibers, will not be the same all the time, and simply put a mapping in each of those different interconnect and here we are. We can now send information from one point to the other point that will be far, far away.

So with the speed of all of this? What about some standardized speed? The lowest you can get today will about one gigabit per second on a fiber. What's typical for service provider today to use 10 gigabit per second. And for the fastest link, you can go to 100 gigabit per second. In a data center, folks have been using 25 gig or 40 gig. And you will see some switches, for example, that may have, on some sides, some 10 gig [inaudible] links and 40 gig [inaudible] uplink.

You can have multiple of both, because I was saying earlier if you take multiple wavelength, so let's say that you have a green wavelength for 10 GigE and then have a red wavelength for 10 GigE, you use them together, now you have 20 GigE. The same thing with 100 GigE, etc.

So in the future, we may get faster, like 400 gig or 1 terabit in lab somewhere, and some people are already running things like that. The faster we go, the more expensive it is,. I remember when we first had those 10 GigE links, they were very, very expensive. And you want to have a line card, and a router, it takes an entire slot, and it was more expensive than a car.

Well now, it's like a regular port on the line card that has maybe 10, 20, or 40 of them. Cost went down very, very quickly. 100 gig is going to go through the same path. Still right now, it's a very few limited number of ports, but in the near future, it will be denser.

So now that I have those things, what I have is essentially a point-to-point network that goes from anywhere to anywhere. And from the [inaudible] this is the same as having a local area network. If I have two computers at the end of each point of a fiber, of a fiber path, that's the same as if I had a local Wi-Fi network and computers connected to it, which means that every node sees all the traffic.

So let's say, for example, that you and I like to play games, and we are going to play some of those, I don't know, Minecraft-type games. And Cathy, good to see her, she's very serious person, and she wants to send e-mail, she wants to look at the database in the office. If we are on the same network, well, she will have hard time to access the database because all of the traffic will be used for our gaming, and that's not really good.

So what we do is we segregate the traffic by creating different networks. So we will say this is a virtual LAN or this is going to be a subnet with different type of technology depending what technology we're going to use. This is our gaming network, and this is a professional network.

What I'm trying to say here is we don't want to have all the computer in the world part of the same network. We want to isolate that for different reasons, so here it was an issue of bandwidth. It could be an issue of security. Maybe she doesn't want her e-mail to be vulnerable to attacks coming from over people who are doing something else.

So sometimes it's a geographical reason. We want to say, "Okay, this is a network in the room here. There's another network in another room in the hotel, and we don't want them to be mixed traffic, so we are going to isolate them.

So how do we do that? Well we simply create a bunch of [inaudible] networks and we interconnect them, and that's where this layer of free technology, the Internet protocol, comes into play. So we are going to isolate this and reconnect them at layer three, meaning there will be a router that is interface a number of different local area network and its job is forward a packet from one network to another. And if you see the traffics stays into a branch of network that's on the left, it's not going to say anything, to do anything.

If it takes a packet and look at it and says, "Oh, this is actually for network that is on my right-hand side," it's going to copy the packet and send it to the right=hand side. Does it know which network it belongs it, it look at the address. That's why we have IP addresses. Yeah. And IP addresses are not intellectual property, this is Internet protocol. Okay?

And by simply looking at those IP addresses, we're going to say, "Yes, this is part of the network on the left or part of the network on the right or part of a network that is further out." And later on in this tutorial, we will see how we can interconnect all those routers together.

So that's what we call layer three networking. Once we have this infrastructure, now we can start to communicate. And the first thing we want to do is to have what's called a transport layer or layer four that enables us to have communication. So I want to talk to Katie. And I am [inaudible] maybe in another room so I'm going to turn my back to her to pretend that I'm in another room.

Katie, hello.

KATIE: Ack.

UNIDENTIFIED MALE: What just happened? I send a message to her, she received that message, she heard me, and she's responding to me. "Ack." That says, "Acknowledgement." So what do I do now? I know that she can hear me because she responded to me. She knows that she can hear me. But the one thing she doesn't know is if I can hear her. She just send something to me.

So if I want to make sure that she knows I can hear her, I need to respond to her. And I'm going to say, "Ack." So this is a three-way communication, and we call this a three-way handshake. You may have heard in TCP called the three-way handshake. That we just did. So we need to do it again. So I'm turning my back. Hello Kathy.

KATHY: Ack.

UNIDENTIFIED MALE: Ack. Now she knows that I can hear her, and we have a communication established. Okay? Now we can send packets. So when we send information, we are going to check this information into bits and pieces. So we call those packets of different sizes. The typical maximum size is about 1,500 bytes, and this has to do with the ethernet framing. There are ways to make it bigger, but most of the time, that's what it is. Sometimes, it can be smaller, but most of the time, for large files, that's what we're going to do.

So I'm going to check my file that I want to transfer to Kathy into packets of 1,500 bytes. So I'm going to send the first one. Kathy, this is my first packet.

KATHY: Ack.

UNIDENTIFIED MALE: Now I know she has received my first packet. Okay? I'm going to send a second packet. Kathy, this is packet number two.

KATHY: Ack.

UNIDENTIFIED MALE: Great. Perfect. I'm going to send a third one. Kathy, this is packet number three.

KATHY: Ack.

UNIDENTIFIED MALE: Okay. Yeah, it's slow. [inaudible] work. Send packet number four.

KATHY: Ack.

UNIDENTIFIED MALE: [inaudible] slow. Maybe I need to send it a little bit slower. Kathy, this is packet number five. Nothing, oh. What happened? Maybe she is not awake. No. Maybe the network is down. I don't know what happened because I don't know what happened, I'm going to send it again. Kathy, this is packet number five. Hmm, try again. Kathy, this is packet number five.

KATHY: Ack.

UNIDENTIFIED MALE: Oh, here it is. So now I know that she can still get my packet number five, and I can go into packet number six. Okay? But there have been what we call packet drops, like three packets that are sent to Kathy that never made it. So I'm going to think that this is not that she was asleep, no. It's that somewhere they were lost, and why were they lost? Yeah, it's very rare but packets are lost because the fiber is bad quality, that happens, but it's really rare.

What really happened is that there was some routers in the middle, maybe it was boxes in there, that were too busy, they had too much traffic to handle. They were congested. And when there's a congestion, what do they do? They talk packets, so that they can handle the rest of the traffic.

So what tells me that bandwidth between me and Kathy is relatively small. It's not very good. So instead of sending a packet maybe every one second or two seconds, I'm going to wait. Kathy, here's packet number seven.

KATHY: Ack.

UNIDENTIFIED MALE: Good. I'm going to wait a little bit. Kathy, this is packet number eight.

KATHY: Ack.

UNIDENTIFIED MALE: Perfect. Now if I slow down, the network is not congested as much, and all my packets go through. So instead of sending my packets as fast as I can, and having most of them dropped, and having to retry and retry again, I'm simply slowing down. And now maybe I can, after a little while, say, "Okay, maybe congestion is gone, I can start to go a little bit faster."

And by dropping packets and sending me a signal that I need to slow down, or by saying immediately, "Yes I can get those acks," the total bandwidth I'm going to use is going to go up or down, and it will adapt to the circumstances. So that's all the congestion control that the TCP protocol is doing.

There is another protocol that is used on the Internet that's called UDP for User Datagram Protocol. It doesn't do any of those fancy things that we just enact here, it just send data and have no idea if it works or not. So the application will have to have some kind of mechanism to decide if it's going to be received or not. Sometimes it doesn't matter.

For example, if I send voice over IP traffic, in the middle of a sentence, if I lose some packets, I'm not going to retransmit it later because instead of saying, "Hi, Kathy. How are you doing?" She will hear, "How doing, how are you, Kathy?" That makes no sense for her. Absolutely no sense. So it's better for her to hear, [inaudible] doing where we have essentially a packet in order, but they might be mangled somewhere in between, and connection is not a really good quality.

So for those type of voice applications, usually the UDP protocol is being used. Or when it's a single-packet exchange like one packet in a response, if it's not a full communication happening like for DNS, in particular, so we say asking a question, you give me an answer. When that's maybe just plenty. There's no need to get the overhead of this TCP protocol.

So now I have a transport, I can send data to Kathy and back. What can we do with that? Well, we're going to create a session and this is not used all the time, it's mostly used for real-time communication like voice, or movie streaming, or things like that. And essentially, what this does is two things. First one is we can negotiate what type of traffic it is, and I can, for example, ask, "Well, I want to see this movie and what are the different format this movie is available?" And you can tell me, for example, "It's available in this encoding or that encoding or that other encoding and that quality, different [inaudible] quality," so we can negotiate that.

And then the second part is some evolution of this TCP handshake that I showed you where we can say, "We are going to send at fixed interval so that you will receive, and it will look real time when you play it on your side.” So all of this is in the session protocol.

Up next is what we call presentation. For example, when we are discussing about the movie catalogue, and I wanted to know what are the different formats. Years ago, we tried some sort of a populated way of encoding this information. And then we moved to some kind of binary encoding, and when we went to XML, and now the latest version of that is [inaudible].

So this is some kind of a human, readable way of encoding information. In that case here, what we’re talking about here is a menu. So with our different items in the menu, the different value, different pop up, and different functions that can be started when a user click on a particular item in the menu.

So this is essentially a way to organize the information that we are going to send in a structured way. It’s made in a human-readable format, because at the end of the day, when you debug this thing, it’s much easier. I mean, it is just a bunch of 0 and 1s. It doesn’t work for everything but for a lot of it, it really works well, it’s quite popular now.

But all of this, this is plumbing. Honestly, my kids don’t care about that. My parents don’t care about that. And if you have customers, they don’t care about that. What they care about is the Web. What they care about is sending email. Okay? This is the application. You have to do a good job, but you will be using protocol X or protocol Y at the end of the day, it makes no difference. As long as, for example, this kid can play Minecraft because that's what kids like most days, or watch YouTube movie, or watch whatever they want. Okay?

That's really one thing to keep in mind is all the technology underneath is just a toolbox. Okay? Customers are not interested in tools. They want an application, and the job is to make sure reducing work. But to make this work, you have to make sure that the people who run the network can make some money, because if it cannot make money, then they're going to run this very long. Okay?

Earlier on, I was talking about you can share a fiber among different customers. So there are different business model that exist. For example, the simplest business model on the Internet is you buy a lot of capacity, and then you slice it into smaller chunks, and you resell those smaller chunks, and you make a little bit of margin in each of those different chunks. That's one business model. There are many other business model that exist. But at the end of the day, if your business model doesn't work, you're not going to stay in business very long, and all of this is moot.

And then there's another layer, which is the political layer, which deals with all the different regulations that you have to conform to. So different countries have different regulations, so if you do business in different countries, you need to adapt to each of the different regulations. And also global issues like governance issues, for example, how do we agree on a protocol to do something.

For example, I was talking [inaudible] description now do we agree that everybody's going to have some of the same. So this is done in standard bodies, IETF is one of them that has most of the stuff related to the Internet [inaudible] like W3Cs and there are also ICANN meetings, you want an ICANN meeting, that's what we're doing, some Internet governance on the domain names.

So all of this is actually quite important. So that's why we from seven layers from the ISO model, we went now to layer zero to layer nine. Okay, now with all this background in mind, we are going to dig a little bit deeper into what is your name, what's an address, what's a route.

So this whole thing started with a story, it happened to me a while ago. I was traveling somewhere, I think it was in Ireland, and had a really bad toothache, like a really, really bad one. I just flew in, arrive in the country, and I know nobody. Was actually not true, I knew one person, I knew Kathy. Hi, Kathy.

KATHY: Hi, Allan.

ALLAN TURIN: You know, I've really a bad toothache here. I need to see a dentist. You have been here for a while now and maybe you can recommend somebody to me. What's the name of your dentist? Dr. Jameson in Ireland. Okay. I know the name of this guy. Okay?. Now I have to find him.

Okay, so what's a name? A name is a word of a set of four by which a person, an animal, a place, or thing is known, addressed, or referred to. Example, my name is Allan [inaudible] my name [inaudible].

It could be a famous person. It could be a big race. It could be all kinds of different things. For example, if somebody gets really famous after he dies, sometimes we name a street about him. We name a university, a town. Because this name has been, was important. His name had a meaning.

So if you know, if I know your name, I know who you are. So I'm going to ask you to remember three things in this tutorial. First thing number one. Okay? If I know your name, I know who you are. What is your name, sir?

EFRAN: Efran.

ALLAN TURIN: Efran, now I know who you are. We can have a relationship. You know my name, I'm Allan, I know your name, Efran, so we can relate to each other. Okay? That's what is really important. I know who you are. We can use this name as a handle. And, essentially, I can talk to Efran directly or I can talk to Kathy. Kathy, I met this nice guy, his name is Efran. Do you know him?

KATHY: Yes.

ALLAN TURIN: What just happened here? We're not just communicating together with that name. I was communicating to somebody else about you. Referring your name. So those are the two usage of names. So again, remind me, Kathy, what's the name of your dentist.

KATHY: My dentist's name is Dr. Jameson.

ALLAN TURIN: Dr. Jameson. Thank you for reminding it to me because I'd forgotten. So she has just referred to me the name of Dr. Jameson. Now I can use this referral and try to go and see Mr. Jameson somewhere.

Names have scopes. So I told you name is Allan, Allan if you speak French. In my family, I'm the only one, Allan. So it's fairly common name but I don't have any brothers and sisters, and my cousin don't have the same first name as me. So that was easy when my uncle said, "Oh, yeah. Allan should do that." Or my father said, "Allan should do this." Okay, so it was about me.

Went to school in elementary school, Allan was a common first name. I remember, one day, there were six Allan in the classroom. Okay? And we had a teacher, she was a little bit of a weird character. She would say, "Allan, go to the whiteboard." And the six of us were looking at each other like, "Okay, which one?"

Then she would get all pissed off and she would say, "Allan, go to the whiteboard." And we couldn't say anything. We couldn't do anything. And when she said, "Oh, Allan Turin, go to the whiteboard." Okay, I knew it was me. Right?

So what does this mean is there are context where you need to really fully qualify the name. Like you say Dr. Jameson, hopefully there are one in the city where I am. If there are like five of them, that may be more difficult. Maybe I have to know his first name. Maybe I have to know a little bit more about where he lives to find him. Okay?

So on the Internet, if I say that I have a machine, that name is, I don't know, www, we have a lot of machines with name is www. Okay? So I need to qualify by something like the rest of your name, exactly.

So now we have our scopes here, and that's interesting but I still don't know where Dr. Jameson is, no idea. I mean, this is new city for me, never been there, first time. All right. So I need to find the street address, which is a mapping from the name space to an address space. Okay. How do I do that?

Well I have to go for some kind of directory. Kathy, I've been asking around but nobody knows Mr. Jameson, so would you mind going to your rolodex and give me the suite address of Mr. Jameson?

KATHY: His address is 125 Root Canal Road.

ALLAN TURIN: Thank you. Now I have an address, and I can go see Dr. Jameson. This process is called name resolution. So you will hear that a lot. In DNS, we do name resolutions. That's what it is. I take a name and now I get another information, which is the address, and I can go and find this address. Okay?

So some recent issues about names. By recent, I mean, the last ten years. By the way, all those slides will be made available, so you'll find them easily. Issues about internationalizations. Well there's different countries use different character sets. Chinese is different from Arabic, which is different from English, which is different from French, which is different from Icelandic. So that in European languages, most characters are about the same except that, for example, my daughter name is Annaise, have two dots on the I and when she's in America, nobody understand that because there's on the keyboard, there's not a key with an I with two dots on it.

So it gets confused, everybody gets confused. If you were Arabic or if you were Chinese, that will be even worse because those characters simply don't exist on a keyboard. So all kinds of issues we've had and some enforcement have been done to use Unicode to some form of encoding to deal with internationalization. So it's a very complex topic, and there are multiple places within ICANN and IETF where this is discussed.

Another topic is authentication. I talk to Kathy and ask her what's the address of Dr. Jameson, and I trust Kathy, that's okay. But if I were to ask somebody else, I may or may not trust that person. How do I know if that that person has the right information? Okay?

So if I were to ask you what is the address of Dr. Jameson, what would you tell me? Something, maybe not the same, you know? Maybe you are not in the city. Maybe you think of a Dr. Jameson that lives in New York, or that lives in Casablanca, or that lives wherever it is. Okay? I want to make sure that I have a correct address. So we use cryptography to do that and so this is called DNSSEC for Domain Name System Security Extension, this has been deployed now for a number of years, and again, there are a number of working groups in ICANN and IETF that are dealing with it.

Expansion of the root zones, you've heard about all the gTLD programs as having different domain names or top-level domain names. Started with things like .com, .net, .edu, .org, and then a bunch of them have been added. Now there are quite a lot of them. So all of this is dealt with by a bunch of other working groups. Not going to go too deep into that. This is only, remember, an introduction level class, not in depth.

All right, so. 125 Root Canal Road, how do I go there? Where is it on the map? All right, what's an address? Again, looking up in the dictionary, those are the particulars of a place where someone lives or an organization is situated. The second thing I wanted to remember from this tutorial. First one was I know your name, I know who you are. Second one is I know your address, I know where you are.

Remember those gangster movies where we said, "Uh huh. If you don't pay me back, be careful. I know where you live." Remember those movies? That's exactly what it is. I have your address. I know where you are.

So addresses have a structure. I don't live there, but many people want to live there, apparently, every four years they change. This is the most famous place in Washington, D.C. The address is 1600 Pennsylvania Avenue Northwest, Washington, D.C., 20500-0003, USA. Okay? That's the address. If I want to send a letter or postcard, that's the address.

So if you look at this, there's some hierarchy. You have to read it from the end, from right to the left, so first important token is USA, United States of America, that's a country. Second is D.C. for District of Columbia. So District of Columbia is not a state in America, it is something special, but for a matter of Post Office, it's a signal level.

The District of Columbia has been separated into four quadrants. There's northwest, southwest, northeast, southeast, so this is in the northwest quadrant. This is the name of the street, Pennsylvania Avenue, and that's the number on the street, 1600.

Not all addresses are geographically organized. So for example, if you think about the telephone service. So I'm not sure it works here, but in America, we have those toll-free numbers, meaning that you can call and it doesn't cost anything. The receiver of call is paying for it.

They are all using the prefix area code 800, 1-800. So when I dial 1-800, I don't know if I'm going to talk to somebody within Washington, somebody within Dallas, Texas, somebody who is in San Francisco, or maybe somebody who is in India. There's no hierarchy by simply looking at the address that will tell me where that thing is. That's the same thing with IP addresses. If I look at an IP address, for example, 109.27.2.5, IPv4 address, simply by looking at the address, I have no way of knowing that this is an address here in Marrakech.

Now there are people who have built a database to reverse engineer this, and you can do a lookup in the database and they will tell you yes, this is an address that is in this building on [inaudible]. Okay? But by simply looking at the address itself, you cannot do that.

Similarly, addresses have scopes. So if I talk to somebody in Washington, and I say, “Oh, I’m going to 1600 Pennsylvania Avenue Northwest.” They will know exactly what I mean. If I say to some of my friends, “I want to go to Paris tonight,” they may scratch their head. Because there’s actually a Paris nearby Washington in Virginia. It’s a very small village of 300 people. There are actually 29 cities in the U.S. whose name is Paris. Okay? And, of course, there’s one in France.

So similarly, but with names, you have to disambiguate where there is conflict for an address. You may have also to deambiguate and to say, “Give more information so that we know exactly which Paris version we are talking about.”

Also, I can use address as a handle. So I can use an address on a postcard, send a postcard. Or earlier on, Kathy was telling me she was going through her rolodex and she was looking for the address of Dr. Jameson. What was the address of Dr. Jameson, Kathy?

KATHY: 125 Root Canal Road.

ALLAN TURIN: Thank you. My memory is really bad, and I need to be remembered sometime. So what was the same story with names. You could use names to start a communication or use name as a referral. Addresses are the same thing. They have exactly the same properties.

So now I need to go to this dentist at 125 Root Canal Road. Hopefully, he doesn't have to do a root canal on my teeth because that's fairly painful. But now I have an address, that's not enough. I know nothing about the city. So let's say, for example, that I wanted to send a postcard to a resident of the little White House in Washington, D.C. just to say hello. I'm going to hide the address on the envelope [inaudible] right inside of a postcard and the postcard will go there. Right?

Why does a postcard go there? Because there is an agreement between various post offices that will take my postcard and will send it to the right place. They will route it to the right place. So maybe somebody will pick up my postcard here at the hotel and bring it to Marrakech to the post office, central post office, and maybe they will put the postcard into a plane to Paris, and in Paris, somebody will look at this and say, "Oh, this has to go on another plane to New York, where there is the international sorting facility for mail," and then they will send it to Washington, and then eventually it would find its way to 1600 Pennsylvania Avenue.

The only reason why I can send a postcard anywhere in the world is that there is a cooperating system of different post offices around the world. This whole system works because of this collaboration between the post offices. And when we're going to talk about the Internet, this is going to be exactly the same thing. It only works because there is an informal cooperation between all the different parties.

All right. Now let's look at a bit more in details about Internet addresses, those IP addresses. So we have two protocol that exist on the Internet today. Actually, there are more than that, but those are the two most common ones. There's IP version 4 and IP version 6. IP version 4 is one that is most commonly used, and address is encoded into 32 bits, so bits could be 0 or 1, so you have 2 to the power of 32 combination, this is 4.9 billion. Actually, there are a number of them that are reserved for things like multicast, for things like service addresses, etc. And in the end you have about 3 point something, 3.2, 3.5 billion addresses that are usable.

There are more than 3 billion people in the planet so there's a bit of a discrepancy here. So that's why we a number of years ago, about 20 years ago, we defined something called IP version 6, and instead of coding to 32 bit, we coded to 128 bit, and that is a very, very, very large number. I'm not to ask any of you to read it, because I have absolutely no idea how you read this number, this is too big.

But this is not four times this, that's for sure. This is much, much, much bigger. The hope is that there will be enough addresses with that until my grandkids will have an opportunity to look at this. Okay?

Now you have heard about IPv4 exhaustion. As I mentioned earlier, we have more than 3 point something billion people in the planet, so there's just not enough addresses. Right? So how do the addresses get handled to people? Well the pool of addresses is held by IANA, it's part of the IANA functions. So you have all heard about the IANA transition. That's one of the things that the IANA does is allocate addresses to the regional Internet registry.

So there are five IR for regional Internet registries in the world, there is one in Africa that's called AFRINIC, there's one in Europe that's called RIPE. It's for Europe and Middle East. There is one in Asia-Pacific is called APNIC. There's one in Latin America and Caribbean that's LACNIC, and one in North America that's called ARIN. The are five of them.

So they receive their addresses from IANA. Back in 2011-2012, there was nothing left from IANA to allocate. So each of those registries have their own policies, and they have their own process to develop those policies. And at some point they run out also, and the only place where there are addresses left today is in AFRINIC. There's not many left, but there are a few left.

So [inaudible] going, so what's happening next? Well remember this IPv6 thing? Large addresses. The whole idea was to deal with this problem. We run out of v4 addresses, we all move to IPv6, life is good. The problem is IPv4 and IPv6 are not compatible. So the same as last week I was in New Zealand, that's the power supply for my laptop, [inaudible] socket in the world. Okay? Doesn't fit.

IPv4 and IPv6 are the same thing. If I have IPv6 and you have IPv4, can't talk to each other. Right? So that's a technical limitation. So it's a technical thing, we can solve it with technology, and we can build a translator between IPv4 and IPv6, but that's still problematic. So we see a lot of uptake of IPv6, but we are not yet at the point where IPv6 is a replacement for IPv4. And we may be there in a number of years from now, but right now we are not there, so we can't use it.

Why we not there? Well because not all equipment use IPv6. For example, I may have IPv6 going all the way to my house, but there's a TV there that is a smart TV that is downloading movies from Netflix or something like that, and that TV was built a couple of years ago, and doesn't understand anything about

IPv6. So even though I may have IPv6 in my house, my TV who is going to be the biggest consumer of bandwidth will have to use IPv4.

So from a service provider perspective, if you want to keep me as a customer, and you only give me IPv6, I'm going to cancel my contract and go to somebody else because my TV is important. Actually, not to me, I don't watch TV, I don't have one in my house, but other people like TV.

So the result of this is this v4 and v6 things are going to be there for a very, very, very long time until the day where you can go to an electronics stores and buy default everything as IPv6, every single thing as IPv6, we will still need to carry IPv4.

So what do we do? There are two things that people are doing. The first one is there are addresses that were allocated a while ago that are not "in use." And there are people who want those addresses. Well can see a deal happening. Three out of the five IR have IPv4 transfer policies in their books, which means that if I am a party who has addresses that I'm not using, and you want to get my addresses, we can have a contract together. Maybe you would compensate me for the work I have to do to release those addresses, it might be some money exchange, but the registry don't want to know about financial aspect. But you can go to the registry and I can go to them, write them a letter, and I will tell them please take my block and associate it to you. So there's a market for that.

You're not buying addresses because addresses are numbers, so you cannot buy a number. What you buy is the right to register that number under your name. Okay? So it works because there's, as I mentioned [inaudible] this collaboration about everybody that says, "Okay. We are going to believe that the system works and if my block is registered under my name, everybody is going to believe that it is really my block. If I transfer my block to you and in the database it says it's yours, then everybody is going to believe it is yours." Okay? This is this trust that is really, really important.

So different IRs have different policies, some are more constrained than others. If you want to know more of the details, we can have an offline conversation about this, but in the end, to give you an idea, in the last two years, 2014-2015, in the [inaudible] region North America, there were about 38 million IP addresses that had been transferred like this.

And the RIPE region was about 18 million, and in the APNIC region was about 10 million. That's very sizable number. There is a market disfunctioning. Prices of servers transfers associated with transfers, again, you don't buy an IP address, you buy the right to register it. It varies depending on the size of the block you're transferring. So if you're transferring a very large block, each address is less expensive. There's kind of a discount for large volume.

If you're transferring a small block, it could be a little bit more expensive. Typical prices that you have seen in very large blocks, about 5, 6, 7, 8 dollar. Small block, about 10, 12, 14, 16 dollar. Also remember one thing is that not addresses are somewhat created equal, or maybe they were created equal, but some of them are now more equal than others in the sense that where some of them may be in some blacklist, or they have been used by some people who have done some kinds of weird things with them and you don't necessarily want those addresses. If you want the market to get some addresses, you have to do your due diligence to make sure that block is clean.

Now that you have those blocks, what can you do with it? Well, up until recently, your service provider, for example, will allocate one IP address per customer, and then there will be a small box in that box, so that if you have five computer in the home, they can share the same IP addresses. Okay?

Well, the same idea of NAT could be used to share an address among maybe 100 customers. So instead of having one address per customer, you need one address per hundred customer. So let's say that you have 10,000 customers. Instead of needing 10,000 addresses, now you only need 100 addresses.

So if you are paying, let's say, $10 for an IP address, instead of having $10 per customer, now we're talking about $0.10 per customer. Different price points. So those, this combination of market to transfer IP addresses and technologies to share those addresses is what really is keeping all this IPv4 alive. And how long can this be kept alive? Quite a long time.

Okay, I'm not going to talk much about this. All right, so remember I have a raging toothache here, I want to see this Dr. Jameson, 125 Root Canal Road. Is that right, Kathy?

KATHY: That's right.

ALLAN TURIN: Thank you. This time I remembered. How do I go there? Well I need a route to go there. It's like if I want to drive from here to Casablanca, I need to look at a map and find out together. Right? So what's a route? It's a noun. It's a course taken for getting from a starting point to a destination. Third thing I want you to remember, okay? So three things. First one I know your name, I know who you are. I know your address, I know where you live. I know your route, I know how to get there. Okay? One is who, second is where, third one is how.

If you remember only those three things from my tutorial, I will call this a big success. Okay. I need to build a map of a network. So I've created this network here, this is my source, this is my destination. Okay? Remember I was telling you at the beginning of this tutorial, a router is going to take packets from one side and then forward the packet to another side, another interface.

How does it do that by looking at the IP address and looking at the map that says this IP address has to go to this destination or that destination? It's no different than you go to an intersection on a road and you see signs, Marrakech this way, Casablanca this way, Iran this way. Okay?

How do we build this map? Well we're going to build from the destination back to the source. So how does it work? This is my destination, it's connected to the service provider here. So the service provider at the beginning is the only person who knows that this customer has this IP address. Okay? So it's going to announce to all its neighbor service provider if you want to reach this guy, send me your traffic. Right?

Now those two guys who have a connection to this service provider, hear this message. What are they going to do? Exactly the same thing. Resend this information to all their neighbors.

Now I'm going to [inaudible] here, here, and here. This guy has received information from this router, and also from this one. Okay? This path is too hard, this path is one, two, three hops. No reason to go to a three hop path, simply going to go to the two hop path. Now we drop this announcement here just to keep this one. Relatively simple.

So what this is about. This is about I know you. This is about I know a guy who knows him. And this guy is going to be. I know a guy who knows a guy who knows him. What you see here is essentially some kind of transitive trust. Remember what I said about the post office system? It only works because everybody collaborates. That's the same thing here. It works because all of the service providers here collaborate with each other and somewhat trust each other. Okay?

If we don't trust each other, it doesn't work. But one really, really important thing here, this whole system is based on collaboration. Now when I'm going to send my traffic, I'm simply going to follow this [inaudible] direction. Now everybody knows about all this destination, so I'm going to send the traffic. That's when we say, "Oh, I remember. I know a guy who knows a guy who know where the destination is. I'm going to simply send the traffic over there."

There is no guarantee that the traffic will arrive. Remember, it's I know a guy who knows a guy. Right? I'm not sure if there's no "ack," as we said in the beginning at this different step here. All right? All this will be done end to end using the TCP protocol, and any of those routers may drop a packet. In that case, we will reroute or we will retransmit first.

And it might be that the link here break, and then this router will decide, actually, I need to go around. Okay? That's how the Internet will adapt to failures. Now, this collaborative process is really nice and well, but sometimes they are bad actors. What if somebody, a bad guy here, shouts really, really loud, "Hey, the destination is here. I know how to reach it." And he shouts essentially so loud that this guy will essentially believe him. Okay?

Well I'm going to send the traffic and I know nothing about all of this, and it's going to go to the bad guy. We had an instance of that number years ago, I think it was an accident when somewhere in Pakistan they started to announce Google route, you know? So how do we prevent that? Well we're going to do the same types of things that I was explaining about DNSSEC. We're going to use cryptography to verify the announcement. The same way we use cryptography to make sure that when you look up in the DNS in the directory, that the address is correct.

We're going to use cryptography to authenticate the announcement. So there will be a system of public key and private key, and I can look up the public key of the destination and I can see if the announcement has been signed by the private key or not. A bad guy doesn't know the private key, so he cannot sign it. So I'm going to simply drop all the announcements that are coming from the bad guy. At least that's the theory.

This system is known as the RPKI, for Resource Public Key Infrastructure. It has been pushed by the different IR. It is in use today, but there are some constants that have been expressed. First one is more of a political concern. Are we're talking about the centralize, or are we talking about the decentralized system? Is there in this public key infrastructure, is there a single route or are there multiple routes?

If you remember my initial set of slides, I concluded with a political organizational slide, layer nine, that's where it is. That's why those concerns are important. Now there's a technological concern, also. This would guarantee that the origin of a route is correct. This will not guarantee that some guy in the middle will not mess around with it. So some people have expressed concern that this is good but not enough.

So this is still work in progress. Okay, now I can follow this route that has been built by the routing protocols. The most famous one is capped BGP for Border Gateway Protocol, and I can send my packets [inaudible] for those routers and arrive to Dr. Jameson that can take care of my tooth.

I've now accomplished the goal that I wanted to, that I was set out for. And that is the end of my presentation.

UNIDENTIFIED FEMALE: If you have any questions, yes, please.

ALLAN TURIN: Any questions from the room? Oh, question in the back.

UNIDENTIFIED MALE: Thank you very much for your presentation. I think I will take other advantages of it to teach my kids how to understand [inaudible] and very simple. Thank you very much for that. I think what is messing at the algorithm behind the routing, we didn't hear about anything about what the algorithms of the routing of the traffic.

ALLAN TURIN: So we are [inaudible] routers are using. Here the algorithm is this propagations of the announcement from the destination back to the source. And remember on this router here, I have received two announcements. One coming from this router, and one, the secondary announcement coming from this router. That's where we are [inaudible] route selection comes to play. So I mentioned the simplest one, which is to say here, two ups, this one, three ups. So the simplest algorithm is to say I'm going to use the path with the shortest number of hops.

Now you can do something different if you like. You can associate cost to each of the links. For example, you could say that link is very expensive. I'm going to give him a cost of let's say 100. This link is not expensive, that's a cost of ten, this is a cost of ten, this is a cost of ten. Okay?

This path that has only two ups, total cost will be 10 plus 100, 110. This one will be 10 plus 10 plus 10 is 30. Now I can decide that it's my policy, it's the routing policy of the point, I'd rather like to use the path that has the shortest cost instead of using the shortest path. So those are some of the algorithm that you can use to decide where to go.

Or you can have other algorithm, for example, you could say, "Well let's say that all this is in the same country and all those nodes are in a different country." You can say, "I really want my traffic to stay in my country. I have a backup path that will go outside of the country, but I really like to stay in the country."

So what you do is on all those routers, you put some filters that will say, "When I receive this announcement, I'm going to prefer the one that are coming from routers that are in country, in my country." And you can vary that to suit whatever policy you want to put in place. Does this answer your question? Thank you. Another question? Yes.

UNIDENTIFIED MALE: I would like first to thank you about your excellent presentation and the way you present it, and is it possible to explain a little bit more the LPKI.

ALLAN TURIN: Okay. So LPKI. So you understand the way those announcements are made, right? Okay. So we start from the destination, I should say, and everybody's reannouncing this route. What could happen will be a bad guy here that will find a way to connect to another router in the path and send an announcement. And I was talking about the different metrics that you can add to your route. For example, the cost of a link, etc.

So you can say, "I really a really low-cost route to go to this destination" And that cost will be propagated by the other routers. Okay? So if all the routers use this cost metric, then we'll decide, oh, this is much cheaper to go there. Okay?

So that's what we're trying to protect against. How do we do that? Well every time the route will be announced, it will be announced associated with a certificate, just like DNSSEC. There's a signature of the announcement. So the routers that send the message, I am the origin of this prefix," is going to use cryptography, uses private key, and will encrypt the announcement using this private key, and attach this to the message. Okay?

When the router will receive the packet, what it will do is use a public key of the destination to decrypt the message. Okay? And if it matches, then it's authenticated because the public key has been successfully decrypting the message. The bad guy doesn't know the private key, so he's going to put some kind of garbage in place of a signature. When the router here receives this packet, check the signature, the signature will not check because it doesn't have a good private key. So it will simply dump the announcement, drop it, so that way the bad guy can say, "I have very, very low cost route to the destination, but because it's not signed, it's not going to be accepted. Does it make it more clear? Thank you. Question in the back.

UNIDENTIFIED FEMALE: I want to thank you for your presentation. I have a question concerning [RPI] too. It's the thing that is like [inaudible] is the same thing with [inaudible].

ALLAN TURIN: Thank you. It's the same idea. It's not exactly the same algorithm. It's not the same way you put it in practice, but that's exactly the same idea. Okay? So the way it works is when you get your IP address block from your regional Internet registry, then you will register there your private key, and they will give you a certificate that you could revoke later, but you can use to put with your announcement, your route announcement.

So if you are in AFRINIC, when you go there, you register and you get what's called [inaudible] where you have your certificate to sign your announcement. So it's a different model than DNSSEC. And because it's given to you by your IR, it does not necessarily rely on a single route as in the DNS is a global DNS, there's only one, there's one route. So there's DNSSEC from the route that goes down from there.

In the case of IR, it doesn't have to, and that's what has created a lot of discussion. Would it be better to have one route for this system, or will it better to have multiple routes for the system? And so the trust relationship between the different IRs and the different service provider, that comes to play. Next question in the back. Can we have a second microphone?

UNIDENTIFIED MALE: It's going to be my last question, thank you. Yeah. Right now we understand about routing, and naming, and staffing. What about computing in fact inside the Internet? Like the distributed computer, for example, how it's working. We know that Google has released it's Internet platform right now where there's a lot of intelligence also and computing. How things are working inside? Thank you.

ALLAN TURIN: Thank you. That's a really good question. That will be the topic for a different tutorial because it's a fairly complex topic. All of this essentially says that I have a source and a destination. And the model associated with that for many, many years was what we call the client server model. There's one server, there's one client, and you figure out the address of a server, you go talk to the server. That was back in the 1990s.

What Google came up with is, say, we're not going to put just one server here. We're going to put gazillions of servers. Cheaper server, and if one goes down, doesn't matter, somebody else will pick up the slack and do the work. So the way initially it was deployed was simply just in front of a destination, there was what's called a load balancer. And what is this is no more, no less than a NAT box.

And it's going to frontend the communication will communicate there and it's going to frontend maybe farm of servers, could be hundreds, thousands of servers, and it's simply [inaudible] which ones are active, which ones are not. And there will be in the simplest possible case around [inaudible] to decide let's send the traffic, let's query to this guy, let's query to that guy, let's query to that guy.

If the queries are independent, that's just fine. If the queries are dependent and between each other, that's more complex, and that's where it will be a different tutorial about how people actually reconcile this thing, but the basic idea is when queries are independent, I can distribute them instead of concentrating them somewhere. So that was in back in mid '90s.

Later on, we can, people have realized, "Oh, I don't necessarily need to put that thing there. I can put maybe a server there because it's much closer to resource." So instead of having to send all my traffic all the way back to California, maybe I can have a local server here. Maybe not right here, but maybe in Casablanca or maybe in Spain not too far.

So the way it works is there are multiple ways of doing it. One of the ways of doing it is when you do this name resolution, remember when I asked Kathy, "Kathy, what is the address of Dr. Jameson?"

KATHY: 125 Root Canal Road.

ALLAN TURIN: That's one answer, but she could say, "Oh, I know that you are now in Marrakech, I'm not going to send you to 125 Root Canal Road but maybe I can send you [inaudible] Medina and she can give me an address, local address in Medina instead. So this is called geographic load balancing from the DNS, and if I have this, I can simply put some local servers in different places. If I can control the resolution of a DNS, I can look up the IP address of a person that has the resolution, your IP address, and I can see, "Oh, you're in Marrakech, hmm, what is my list of servers?" I have one in Casablanca, I have one in Madrid, one in Paris, and one in Washington. The one in Casablanca is probably the closest. So instead of giving you a generic answer, I'm going to give you a specific answer to what server that is closer to you.

The other ways of doing that, and again, it will take another tutorial to go in details, but hopefully that give you preview of what the correct answer is. We still have a little bit of time for one more question.

UNIDENTIFIED MALE: Thank you very much. Thank you for this clear presentation and the interactive presentation. My question is about the new Internet of object. How can Internet can deal with this new concept in term of naming, routing, and the address? How it can deal with this large number of objects?

ALLAN TURIN: Thank you. That's a very good question. IOT, Internet of Things. There's a not too serious answer to your question and a more serious one. I will start with the non too serious answer. Internet of Things is just the Internet. Okay? The fact that this is a gizmo, that this is a fridge, that this is a cell phone, that this is a light bulb, it's an IP address, it's an IP address, it's an IP address. Okay?

So there's nothing to change fundamentally in the architecture of the Internet to deal with that; it's just something else. Just like the cloud. When you say I have something in the cloud, well it's on a server, it's not your server. That's what it is. But from an Internet architecture, there's no difference. Right?

Now the second part is a more serious answer to this is, and I think you [inaudible]. We are going to have billions of those devices. Right? So when I was saying we have already 3 billion, we have 3.2 billion IPv4 addresses and more than that of human beings, we have like 6-7 billion human beings now we are talking about maybe 100 billion devices. How are we going to do that?

So we have two answers to this. The obvious answer will be to say, "Oh, it's IPv6." Okay. We have so many IPv6 addresses that we can give them to your fridge to your light bulb and everything. A little problem that if you buy this gizmo, light bulb that has IPv6, and you bring in to your house, and in your house, you may or may not have IPv6 because the service provider may or may not have turned it on. If you have it, great. If you don't have it, you just bought an expensive paperweight. Okay?

So the people who are building those devices know that. And it's difficult proposition to put in the market today something that has only IPv6. So they will do it IPv4. So you could say, "Well maybe they will do it both." But doing it both may be more expensive. Maybe have to put a bit more memory and the cost of the device is supposed to be really, really low, it goes up.

So then you need to have more IPv4. Does it work? Well sometimes it does, sometimes it doesn't. If it's in the home, we can still use the NAT box in the home and do this, that's fine. And actually, most of the time, those gizmo don't necessarily talk directly to anybody in the Internet. They talk through some kind of a relay. There's a box that is there to interconnect them.

So that's [inaudible] better, but this is an interesting open question for the next few years. Are people building those boxes going to say, "Let's adopt IPv6?" In mass? Or are they going to say, "No. Stay on the fence. We stay with IPv4?" I don't have an answer to this question. It could be both or it could be either. It's really good question. All right?

One last question. Well thank you very, very much for your attention today.

UNIDENTIFIED FEMALE: Everybody, we passed out a questionnaire. Please fill it out and you can leave it on your seats or you could hand them over to me. Thank you, Allan, for great talk again. 3:15, if you want to come back or you feel free to stay here, we have David Conrad, our CTO, ICANN CTO, doing the next session on Domain Name Registry Protocols. Again, that's at 3:15. Feel free to stay here or you can come back and watch our CTO. Thank you.

[END OF TRANSCRIPTION]