Routing and Routing Protocols

Table of Contents

Routers -1........................................................................................................................................ 2
Routers -2........................................................................................................................................ 5
Routing Protocols -1........................................................................................................................ 7
Routing Protocols -2........................................................................................................................ 9
Routing Protocols -3...................................................................................................................... 12
Routers and Security..................................................................................................................... 14
Notices .......................................................................................................................................... 17
**Routers -1**

Boundary device which interconnects networks

Can connect networks that each use different protocols

Direct traffic based on a network (IP) address

Block broadcast traffic by default

Most routers support filtering, firewall features, and network address translation

Routing decisions can be affected by malicious information

.Layer 3

*068 Layer 3. Definitely a Layer 3 concept, we talk about routers.

Routers are at the edge of our network or at the edge of a particular broadcast domain. They connect different networks with different media types; usually we're only talking about Ethernet and fiber in most cases here.

They can connect using different protocols, if we need to.

And their main goal today, because of the overwhelming preponderance, the de facto of IP being all over the place, they direct traffic based upon
IP address; and they make one decision: Do I take this and pass it on to that interface; or is it not me at this point?

Now what happens is is routers make their decisions based upon destination address, not based upon source address.

So when the router passes the traffic to me, I don't look like- I don't look at it as a router and go: Oh this came from you? Oh yes you're okay. I don't do any of that.

As a router what I say is: This is destined for back there? Oh okay that's where it goes.

Now if I was a complex router with many interfaces and I led to many networks, and you said, "I'd like to go ahead and get to that network" I'd say, "Oh okay, this goes over there." And you'd say, "I'd like to get to that network over here." "Oh I'll pass it through"; and pass those packets along to the destination that way.

Most routers will allow us to filter based upon other things like the source of the address. But what I say is that routers should route and firewalls should filter.

The only thing that I would say that we should filter at the router, from a security standpoint, is the transmission of inappropriate traffic that really is never ever going to get back to its original source.
I'm sure that you all have heard of some of the network addresses that are supposed to be, according to RFC 1918, non-routable. That's the 10 network, the 192 network, the 172 Network.

When that traffic comes to this router, I think that that traffic should be dropped. Because even if it was valid traffic and it came to me and I passed it on to that host, when I try to pass it back as the destination it will never reach, it will never get there because the 10 network is supposed to be non-routable. It will go into Neverland.

So that's the only traffic that I would-I would eliminate. I would eliminate something that comes from the Bogon List; and I would say those are the things that I would drop.

But I wouldn't do any other filtering features, other than that one; with the exception of what's called Network Address Translation--
Routers -2

Form a transmission network that sends packets from point A to point B within a network and on the Internet

- Statically (pre-configured routes set by an administrator)
- Dynamically (routers determine path based on routing protocols and network topology)
- This all happens at Layer 3

**069 The next thing on routers that we need to talk about is--remember that this is going from Point A to Point B, based upon IP address.

Well how do we get the IP addresses? Well for our host internally we go and make a mapping scheme and we say: You get this IP address and you get this IP address. And as long as they're all unique on this network, everything is okay.

When we get to the edge router here, this network behind me may be a private network; and then I have a public IP address that needs to be
configured on this router. So that the rest of the world when they want to get to there, what they do is they come to me and then I’ll create a map in my head and say: Oh you want to talk to the web server? Oh that’s over here; and I’ll actually create that mapping for you and I’ll make that happen.

I could actually have the live IP address back there. But then I’d have to have two different routes that go through.

We could do dynamically where the routers determine the path based on the routing protocol.

So as you get to this router here, it may be that there’s a shorter path to that host there, or a less congested path to that host back there. And I’ll say: Well it goes out this way and comes back around.

All of this stuff is happening at Layer 3.
Routing Protocols -1

Routing Protocols -1

Allow a router to know who its neighboring routers are, and what networks they and their neighbors are connected to

- Routing updates are sent between routers
- Default routes are configured when a router doesn't know where to send a packet

Source routing

- The first router determines a fixed path for all the packets to follow

Security issues

- Dynamic updates can be maliciously altered
- Most routers support route authentication through a shared password

**070 Now we need to talk about routing protocols.

So one router at the edge of your network, no big deal. But if you’re doing this with hundreds of routers in a very large building, it may be that there’s a better way to get there by going a longer distance, or by going a different route to get from source to destination.

How does the router know this? Well we program the router with neighboring routers, so that it knows about them, and knows what those neighbors are connected to through routing protocols.
What we tend to do is we tend to do what's called source routing. So the first router determines a fixed path for all the packets to follow.

So if I know that this is best, then what I will say is: When you want to get there, we're going to go this way. And I'm going to make that determination.

So we all kind of cooperate together when it comes to source routing.

Now the problem is is that it's not just the router here that's configured by the security expert or configured by the networking expert. There's another routing table; and that other routing table, that's on each one of the individual hosts.

So if I can say to you as an evil-doer- and I'll put my horns on here-- if I can say to you: The best way to get to the internet is through me. That's really your router over there or your default gateway. The best way for you to get to the internet is through me. I can now convince you to take routing updates as a host; and then you'll pass your traffic.

Now I'll pass it along to the destination. But while it's going there, I'm going to look at that information and I'm going to inspect it. I've created a man-in-the-middle attack.

So the problem is is that I could, from a security standpoint, convince you to take an improper routing
table, if that host isn't protected against that type of activity.

Now most of the real routers, what they do is they support-- when they're talking router to router-- they support some sort of authentication mechanism so that we know about them.

**Routing Protocols -2**

**Routing Protocols -2**

Either interior or exterior gateway protocols

• Interior gateway protocols – intended for internal network use
• Exterior gateway protocols – intended for use between Autonomous Systems (AS)

Either distance vector, link state, or path vector based

• Distance vector – paths are based on time and number of hops
• Link state – path based on events (up/down of routers)
• Path vector – path based on policy metrics

**071 There are really two routing protocols that we pay attention to. The interior and exterior are one kind of protocol; and those are the gateway protocols. So when we talk about interior what we say: This is
internal- this is internal to our network. That's an interior protocol.

And an exterior protocol, which is between-- well they call it autonomous systems; but routers that are under different people's control.

Now the next thing that we can do is we can also calculate in our routing protocols the concepts of distance vector, link state and path vector based; in other words, how do I make my decisions to go from source to destination? How do I do that?

Now I don't do that as a router for all of the routers in my path. What I do is I make my decisions based on the information that I have at hand here.

And what I will say is: I'm not going to go to that router on that ISP because it's congested. I'm going to go over here to this router on this IP; and then I'm going to flow all my traffic through; because that's the best way to get to the internet right now. This is not such a good way to get to the internet until they've figured out the congestion.

Well how do I make those decisions? Well I make it based on these three decisions here.

Distance vector says: What is the time it takes to get from me to you? So how many hops will it take if I go through this route? Okay that's 13 hops and this is 10 hops; that's probably faster.
Suppose the link between us is down. Suppose an intermediate link is causing router failures over there; and I know that that one's down. Well what I can do in link state is I can say that link is dead. So I'll use this other one over here. I can make that decision.

Then we can also do path vector; which is I find truly amazing.

The cost of going that way is much higher than the cost of going this way. The cost may be a dollar cost; or it may be that the bandwidth is too low over there and it's high bandwidth over there.

In path vector what I can do is I can make decisions based upon what's good for my people in my network that is not considered by the routing protocols themselves.
Routing Protocols -3

**Interior gateway protocols**
- RIP – routing information protocol, distance vector
- OSPF – open shortest path first, link state
- IS-IS – intermediate system-intermediate system
- EIGRP – enhanced interior gateway routing protocol, distance vector, Cisco proprietary

**Exterior gateway protocols**
- EGP – exterior gateway protocol, replaced by BGP
- BGP – border gateway protocol, path vector

---

So let’s talk about interior gateway versus exterior gateway; just for a second.

Interior: For me and mine; and I have total control over all the routers on my network here, in my Local Area Network. How am I going to make routing decisions?

Well I have four different ways. Now remember, hosts sit back inside of here also, individual units, and they would have a routing protocol on them, a routing table on them. And usually what we would do is we would use RIP.
And in RIP what we would say is-- to that host that's communicating to me-- I am your default gateway; program that host to have that IP address.

I could use- if I have a complex network I could use OSPF IS-IS and EIGRP. Those are all internal protocols.

Then we can do exterior gateway protocols. And this is what happens on the internet. I don't control you, you don't control me; but this is the edge of our network here. I am that router.

What will I use? And the answer is

Now ISPs make an entirely different set of decisions. That's beyond the scope of what we're doing here.
Routers and Security

Routers are devices which can add security to the network by separating broadcast domains and implementing rule sets.

Routers have permission tables called Access Control Lists (ACL) which define what traffic is allowed to traverse the device and which cannot.

Routers are available to remote networks – need to change default passwords, usernames, etc.

**073 So what about routers and security?**

Well routers, if they're configured correctly, they can add security to your network. If they're configured incorrectly and they have lots of additional services added to them, well then they're exploitable from the outside as a device on the network.

Now let’s just talk about it from a routing standpoint. What I can also do is I can make decisions based upon the source or the destination, if I want to; and that's where we kick into access control lists or ACLs. And
I'll say: This is the set of rules for getting into our network.

There are basically two sets of rules I think that routers should have. One of them we've already talked about; which is the bogus list of IP addresses is called a Bogon-- b-o-g-o-n-- Bogon List. The Bogon List is known by everybody out there to say that these networks are inappropriate; the 10, the 192, the 172, 16 through 34, all the way up to 5s.

The 169 address, which is now known as APIPA-- that was bought by Microsoft-- should be non-routable.

And then there are a whole other group of hosts that should be non-routable, that are listed for telephone use and military use.

And then you could also get right down to certain countries have certain lists- groups of IP address. If you don't work with those countries, or if you find that they are adversarial in nature--

You can make up ones that work for you; and you could block that list of IP addresses in your Bogon List. And then you'd program that into your Access Control List.

But a more reasonable-- one piece in our Access Control List kind of reaches over into firewalls, which is called a reflexive rule, that says: If the original connection-- let's say that
I am the default gateway for our environment back here-- if the original connection wasn't initiated from inside my network, then anything that's coming directly to me, if it's going to my regular host in here, I won't allow.

Now a reflexive rule would work great if all we had was hosts back here in those servers. But if we had a DMZ arm over here where we've got webservers and mail servers and DNS servers that are answered to on the internet, well the initiation does come from the outside.

So we can't create a reflexive rule for our DMZ; we can only create it for our LAN clients. That means the programming's more complex.

As programming for routers goes up, and there is more complexity, guess what happens? The chance of failure is higher; and also the router goes slower. It stops doing its routing decisions and starts making decisions based on I don't like you.

And so that really is the problem that we run into with router security. So we leave that to other devices.