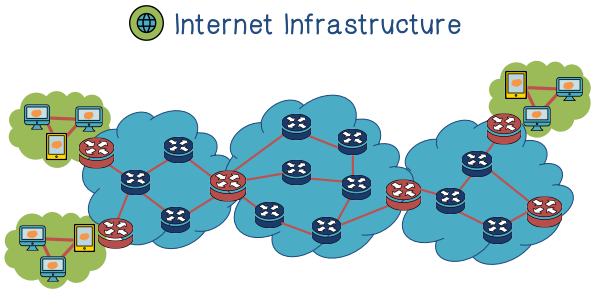
The recommended readings for this lesson are:

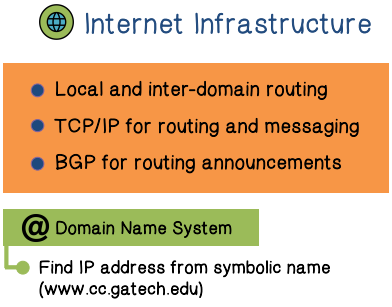
A Look Back at "Security Problems in the TCP/IP Protocol Suite"

BGP Security in Partial Deployment

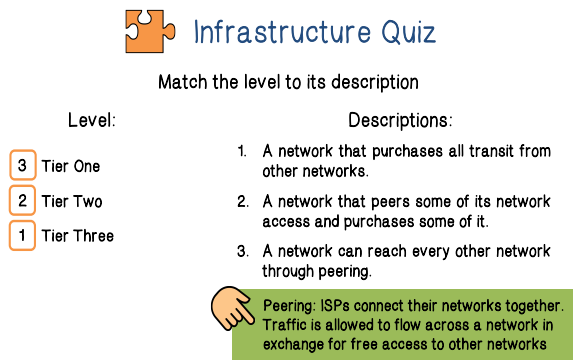
Everything on the Internet must use Internet protocols to communicate. In this lesson, we will discuss the weaknesses of these protocols and what can be done to improve security. When we are done with this lesson, you should have a clear understanding of the security vulnerabilities of TCP/IP.

You can think of the Internet as a collection of large networks. These large networks are typically managed by the Internet Service Providers, or the ISPs. The ISPs work together to allow traffic to flow from one network to another. So, to the users, the Internet is just one big connected network because a user can reach from his computer on one end of the Internet to another computer on the other end of the Internet.



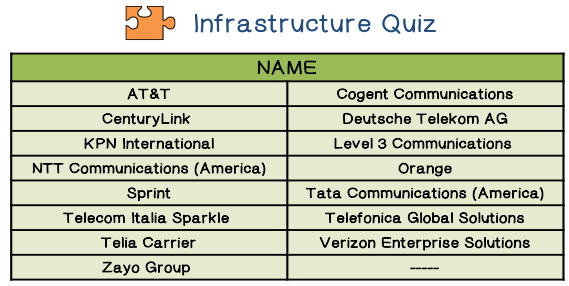


The computers within a local area network use the local and inter-domain routing protocol to communicate with each other. Computers from different networks, for example, from two different ISP networks, use TCP/IP protocol to communicate. But in order to decide how to send traffic from host A to host B, which may be in two separate ISP networks, there needs to be routing information which is decided by BGP, which stands for Border Gateway Protocol. The domain name system is a distributed, hierarchical database system that provides the mapping between an IP address and a symbol domain name, such as www.cc.gatech.edu.



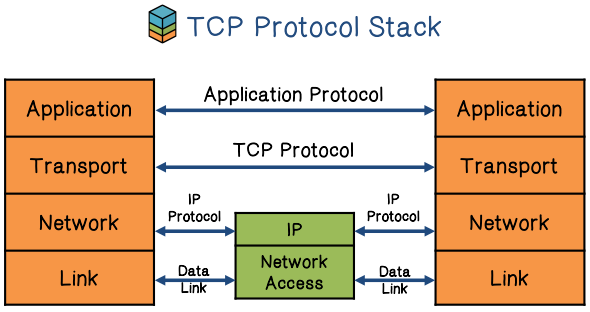
Now let us do a quiz on Internet infrastructure. Match the different levels of networks to its description.

A Tier One network is one that can reach every other network through peering. A Tier Two network is one that peers some of its network access and purchase some of its network access. A Tier Three network is one that purchases all of the transit from other networks.

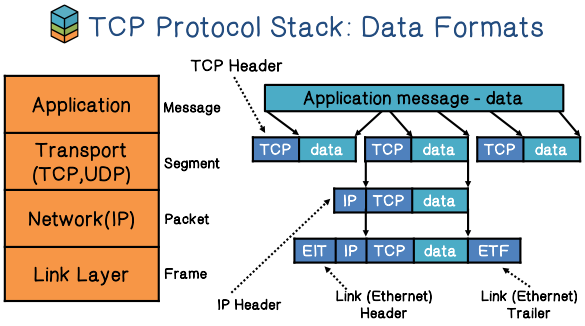


NAME	
AT&T	Cogent Communications
CenturyLink	Deutsche Telekom AG
KPN International	Level 3 Communications
NTT Communications (America)	Orange
Sprint	Tata Communications (America)
Telecom Italia Sparkle	Telefonica Global Solutions
Telia Carrier	Verizon Enterprise Solutions
Zayo Group	-----

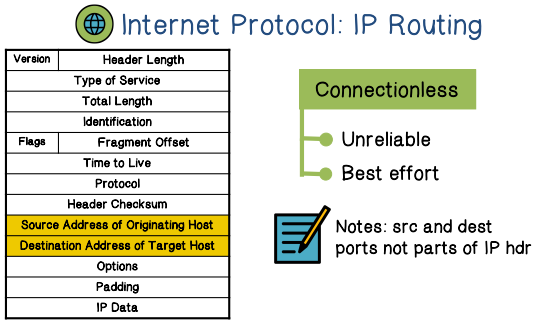
Just for your information, there are only 17 Tier One networks in the world.



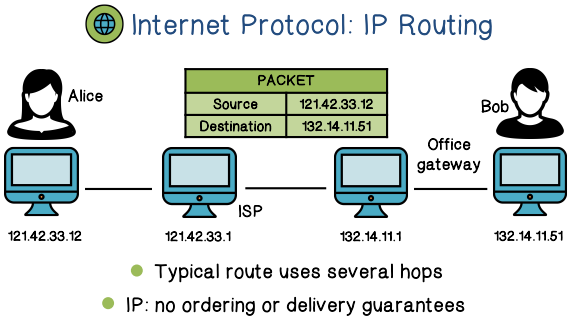
Now let us take a look at the TCP/IP network stack. The Link Layer is a group of protocols that only operates on the link the host is physically connected to. The network or Internet layer is a group of protocols that are used to transport packets from one host to another and may cross network boundaries if necessary. The Transport layer protocols provide host-to-host communication services for applications. They provide services such as connection-oriented data stream support, reliability, flow control and multicasting. The Application layer protocols depend upon the underlying Transport layer protocols to establish host-to-host data transfer channels, and manage the data exchange in a client-server or peer-to-peer networking model.



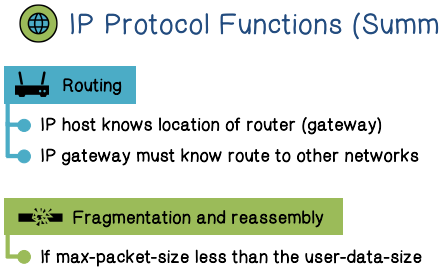
When host A sends traffic data to host B, the data usually starts as Application message. The Transport layer segments the data and puts TCP header onto the segments. The IP layer then puts the IP header on these segments, and they become the IP packet. The Link Layer puts a link header onto the IP packets, and this becomes frames. And this Link Layer frame can then be sent to the link, connected to the host, such as the Ethernet cable.



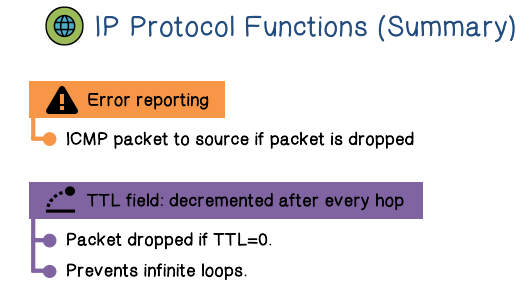
At the IP layer, the IP Protocol routes packet from host A to host B, crossing network boundaries if necessary. The routing is connectionless because it is best effort only and unreliable. That is, it is not guaranteed that, all packets from host A will arrive at host B. And of course, for each IP packet, the source IP address and the destination IP address must be specified. The ports are not part of the IP header because they are for the transport layer.



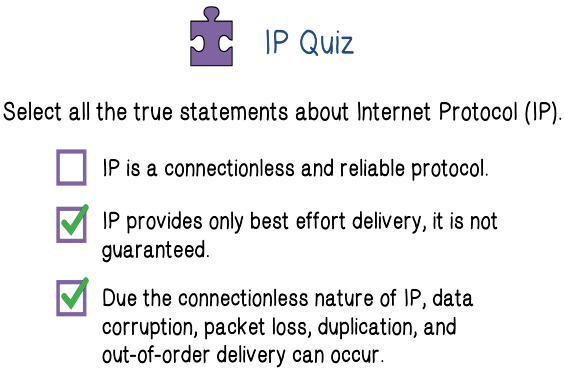
Here is an example of IP routing. Suppose, we have a packet with source and destination IP addresses. Typically, a route will involve multiple hops. An IP routing has no guarantee of the order or even delivery of the packets. In this example, the packet starts from the source IP address and reaches the gateway of its ISP, crosses network boundary to reach the gateway of the destination network and then finally reaches the destination IP address.



To summarize this example, the IP host knows how to reach the gateway and the gateway knows how to reach other networks. If a data segment is too large, it may be fragmented into multiple IP packets. At the receiving end, these fragments will be assembled back together.

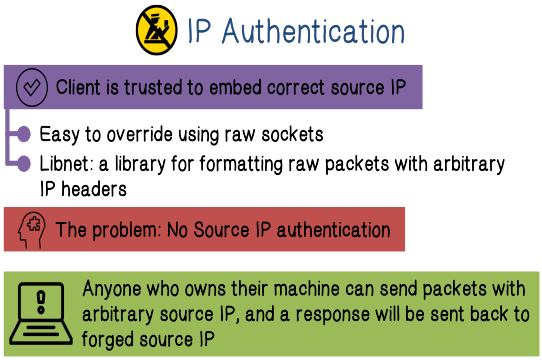


If the destination did not receive a packet or fragment, it can send an ICMP packet to the source to report the error. ICMP stands for Internet Control Message Protocol. The IP header can also include a TTL field. TTL stands for Time-to-Live and this field is decremented after every hop, and a packet is dropped if TTL reaches 0. TTL is useful to prevent infinite loops.

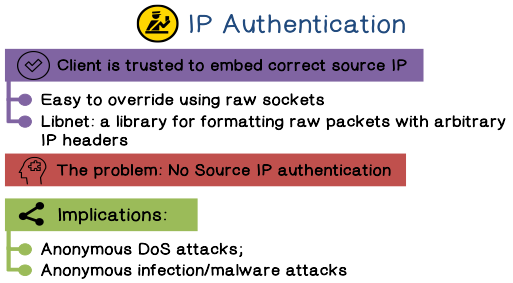


Now let's do a quiz on the Internet Protocol. Select all the true statements about Internet Protocol.

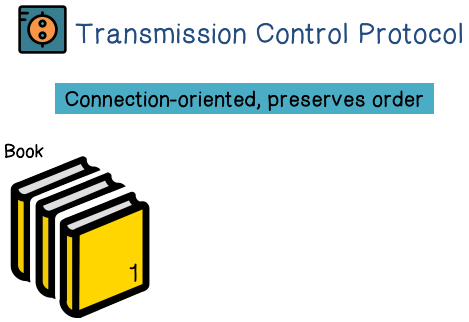
The first statement, IP is a connectionless and reliable protocol. This statement is false because IP is not a reliable protocol. The second statement, IP provides only best effort delivery, it is not guaranteed. This is true. The third statement, due to the connectionless nature of IP, data corruption, packet loss, duplication, and out-of-order delivery can occur. This is true.



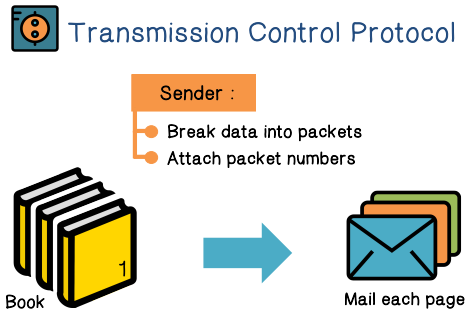
Recall that in the IP header, the source and destination IP addresses must be specified. However, one can easily override the source IP address using raw sockets. For example, you can use the libnet library to format raw packets with arbitrary IP header information including the source IP address. This means that there is no guarantee that the source ID address is authentic. This means that anyone who owns the machine and knows how to use a tool like libnet can send packets with arbitrarily source IP addresses. Now of course, a response will be sent back to the forged source IP address. For example, host A can send packets forging the source IP address of host B and then the response will be sent back to host B.



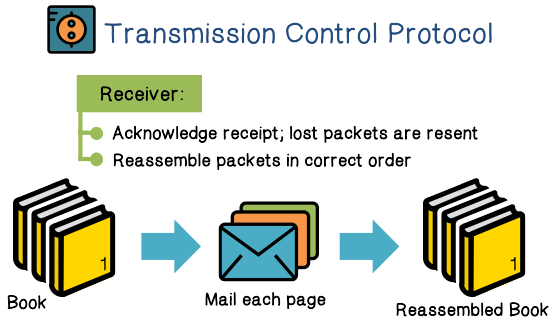
The ability to forge arbitrary source IP addresses enables anonymous, or, hard-to-traceback, attacks such as denial-of-service and malware infection.



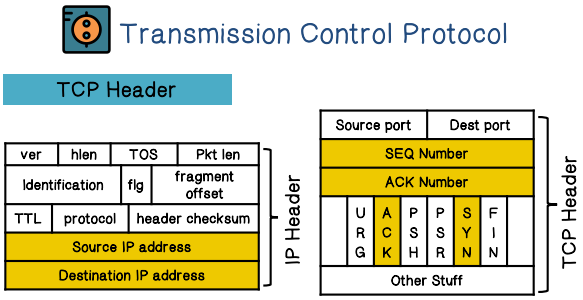
Now let us look at the transport layer protocols, in particular, the transmission control protocol, or TCP. TCP is connection-oriented, and it preserves the order of packets. We can use an analogy to explain TCP. Suppose we want to mail a book.



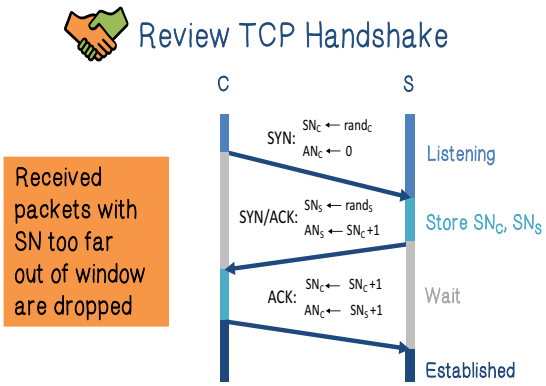
And the way we send the book is to mail each page in an envelope. And that is analogous to breaking application data into TCP packets. And of course, for each page, there is a page number, so that we know the sequence of these pages in the original book. Likewise, TCP packets have sequence numbers.



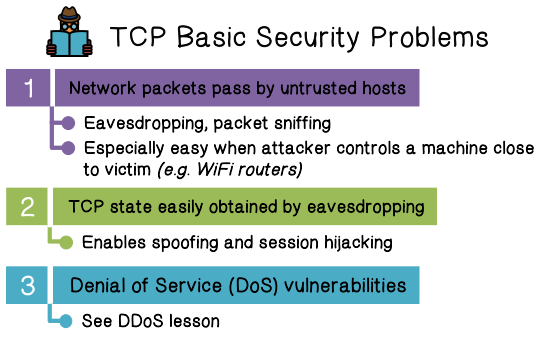
Now, when the pages arrive, they arrive in separate envelopes and may be out of order. At the destination, we make sure that we receive all the pages, put them back in order and reassemble the book. Similarly, at the destination host, each packet upon its receipt, will be acknowledged. And any lost packet will be notified so that the source can resend the packet and then the packet will be reassembled in the original order.



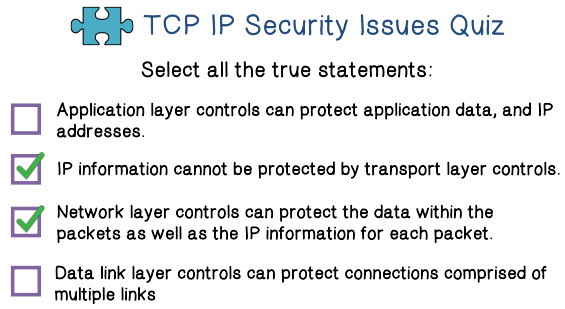
Now let us take a look at TCP Header, it includes the port numbers, the sequence number of the packet and acknowledgement number. That is for acknowledging a previously received packet. It also has a number of flags, these are used to control the TCP connection.



Let us review how TCP Handshake works. The client sends a SYN packet to server, with a randomly generated initial sequence number. The server sends a SYN/ACK packet to the client. It also has a randomly generated initial sequence number, and it acknowledges the sequence number of the SYN packet from the client. And then the client sends the ACK packet back to the server. It also acknowledges the sequence number of the SYN/ACK packet from the server. At this point the connection is established. Once a connection is established both sides can expect that their next packet will have the sequence number that is increment from the previous packets. Now of course packets can arrive out of order. But one can expect that the sequence number should not be too far out of the current window. Therefore, if packets arrive with a sequence number that is too far out of the current window it would be dropped.

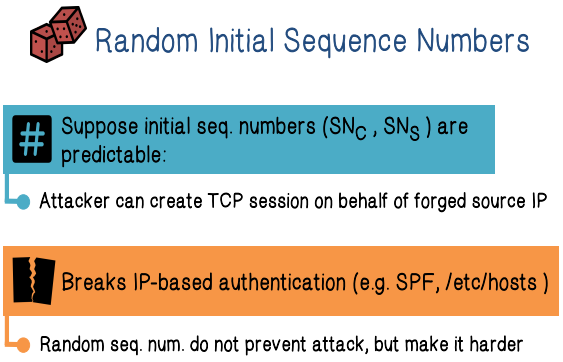


Now let us review some of the security problems associated with TCP. Eavesdropping is always a big concern. And this is quite easy for the attacker if he can control your router or the Wi-Fi access points. And such a hijacking is possible if the attacker can learn the TCP state. And as discussed in our DDoS lesson, TCP is subject to denial-of-service attacks.

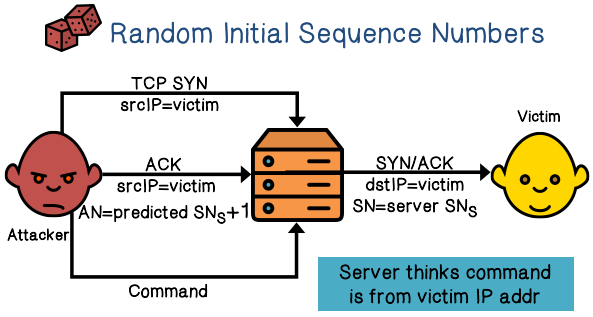


Now let us do a quiz on the security of TCP IP. Select all the true statements.

The first statement, application layer controls can protect application data, and IP addresses, this statement is false. IP addresses exist in a lower layer, and so application layer controls cannot protect IP addresses. The second statement, IP information cannot be protected by transport layer controls, this is true. The third statement, network layer controls can protect the data within the packets as well as the IP information for each packet. This statement is true because that is what network layer controls are supposed to do. The fourth statement, data link layer controls can protect connections comprised of multiple links. This is false, they cannot protect connections with multiple links.

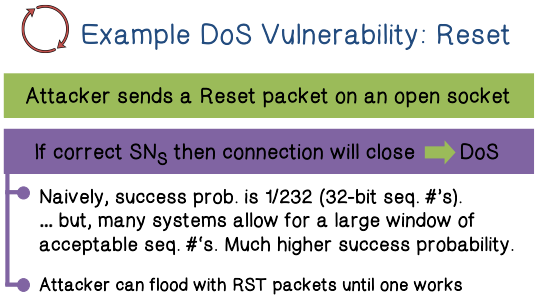


Recall that in TCP handshake, the first packet from the client and the first packet from the server have the sequence numbers randomly generated. This is very important. Suppose, these initial sequence numbers are predictable. Then the attacker can forge a source IP address and still be able to finish the TCP handshake and establish a TCP session. And this will break IP-based authentication such as SPF, which is Sender Policy Framework that is used to authenticate email.

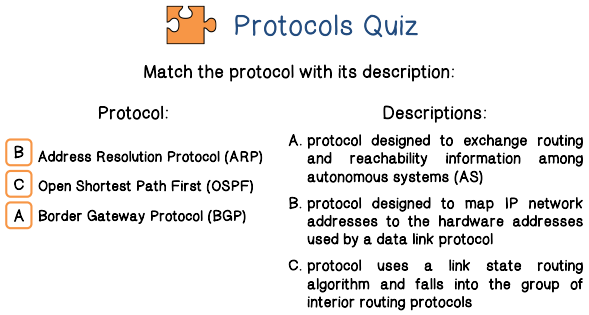


We can use an example to illustrate the importance of having random initial sequence numbers. Suppose there is an attacker and he wants to forge the source IP address of the victim to create a TCP session. So, the attacker sends the initial SYN packet to the server and forges the source IP address to be from the victim. Now the server is going to send a SYN/ACK packet to the victim with its own sequence number. Of course, the attacker did not receive the SYN/ACK packet because the SYN/ACK packet is sent to the victim. Now if this sequence number is predictable, then the attacker can still send ACK packet to ACK this SYN packet as if that the

attacker had received the SYN/ACK packet. And when a server receives this ACK packet on its SYN/ACK packet, then the server knows that the connection should be established. From this point on, the attacker can send command through the server and the server will think that the command is from its victim.

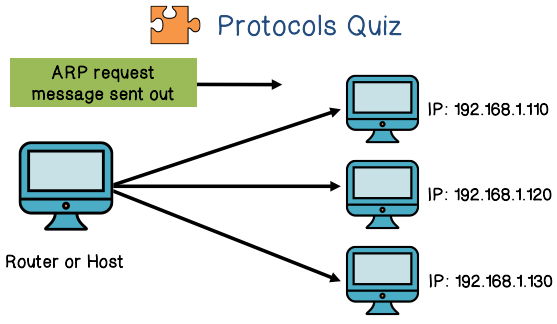


Here's another example of attacks on predictable sequence numbers, suppose the attacker can correctly guess the sequence number. He can then send a reset packet. This will terminate a connection and result in the null service attack.

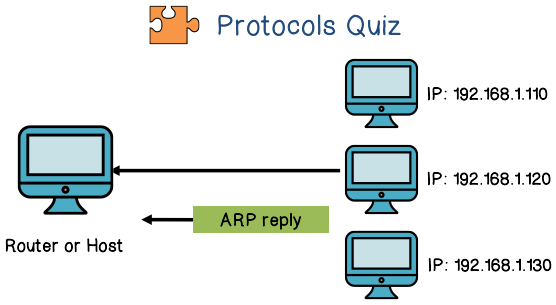


Before we begin our discussion on routing security, let us do a quiz to refresh our knowledge of routing protocols. Match the protocol with its description.

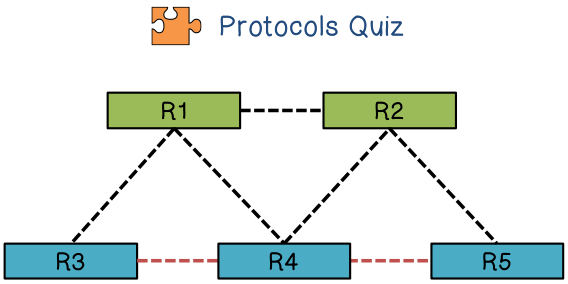
Address Resolution Protocol or ARP is a protocol designed to map IP network addresses to the hardware addresses used by the data link protocol. Open Shortest Path First or OSPF is a protocol that uses a link state routing algorithm for interior routing. Border Gateway Protocol or BGP is a protocol designed to exchange routing and reachability information among autonomous systems or AS.



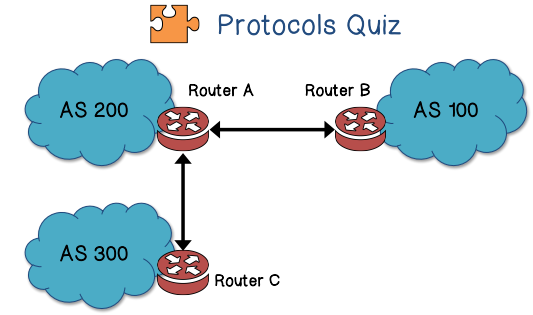
Here is an example of how ARP works. Supposed a router receives data with a destination IP address of a host within each local area network. It needs to know the MAC address or the destination IP address in order to send the data to the host. This is because machines on the same local area network identify each other via MAC addresses. Here, the router sends an ARP request asking for the MAC address of the specified IP address. This request will reach all computers on a network because the destination MAC address is one that is accepted by all computers.



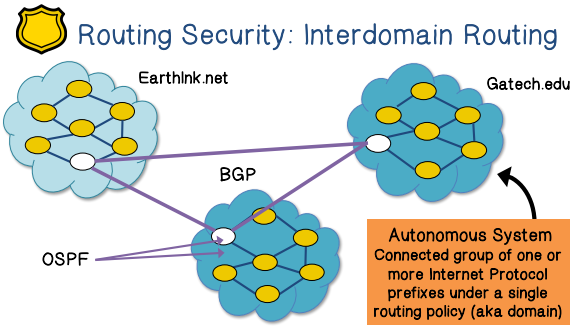
The ARP reply essentially says, hey, I'm the host with the IP address and here's my MAC address.



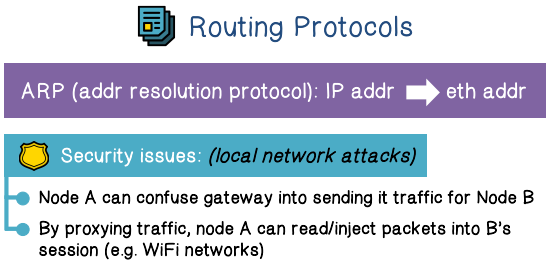
An OSPF looks for the lowest cost path within nodes. In this instance, let us assume that all the lengths are of the same cost. What would be the shortest path between the node R3 and R5? Obviously, the shortest path is to go from R3 to R4 and then, to R5.



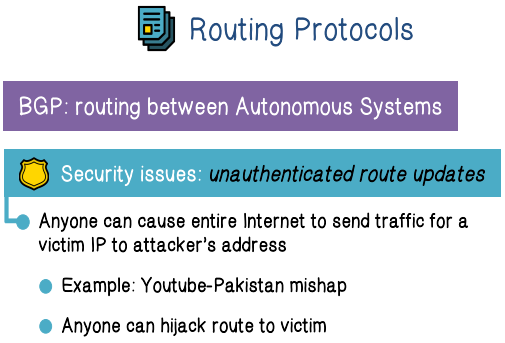
In BGP, the autonomous systems exchange information through peer exchanges. In this example, each AS talks to a peer to learn the address prefix of the computers within their peer network. This helps the ASs to work together to determine how to route traffic from one network to the other.



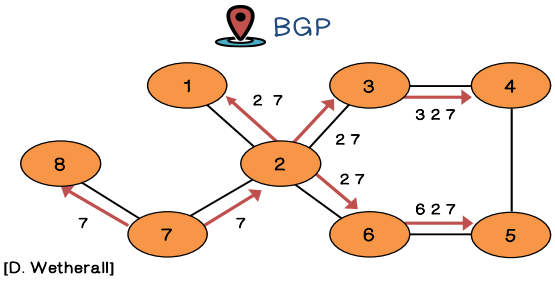
Again, from the perspective of routing, the Internet is a collection of domains or autonomous systems. An autonomous system is a connected group of computers where their IP addresses share some common prefixes, and they are using a single or common routing policy. The routing between these domains is determined by BGP. And the routing within each domain is determined by protocols such as OSPF.



Now let us discuss the security of routing protocols. Recall that the ARP protocol maps IP address to MAC address. Now, suppose there is an ARP request asking for the MAC address for node B's IP address. This ARP request is broadcasted to the whole network. Now if node A is malicious, it can send an ARP reply to the gateway with its own Mac address. If this reply arrives at the gateway before the reply of node B does, then the gateway will think that node A is node B, which means that node A now is right in the middle, and it can read or inject packets into node B's sessions.

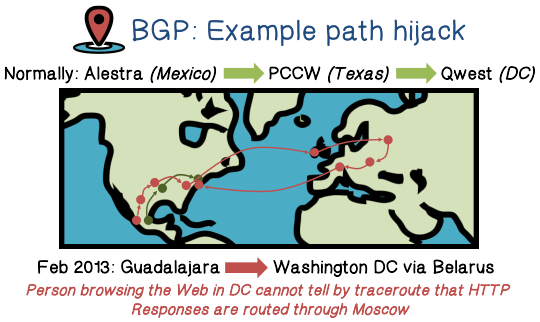


The Border Gateway Protocol, or BGP, decides the routing policy between autonomous systems. However, in BGP routing information, in particular, route updates, are not authenticated. Therefore, through a false advertisement, an attacker can cause traffic to a victim host to instead be routed to the attacker's own address. There are plenty of examples illustrating the danger of false route advertisement. Essentially, anyone can hijack route to victim.

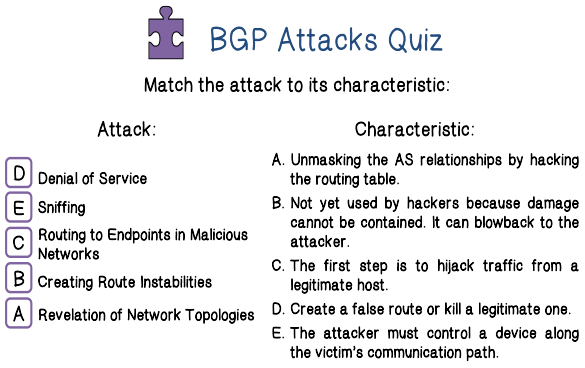


Let us illustrate how BGP works. Here, the nodes are the autonomous systems. And the edges represent peering relations. Here, node 2 provides transit to node 7, and this information is propagated, so all autonomous systems know how to reach node 7.

The main security issues of BGP are due to the fact that BGP path information is not authenticated, which means that anyone can inject false advertisements and such advertisements will be propagated everywhere. As a result, attackers can shape and route traffic to launch denial-of-service attacks, send spams and perform eavesdropping.

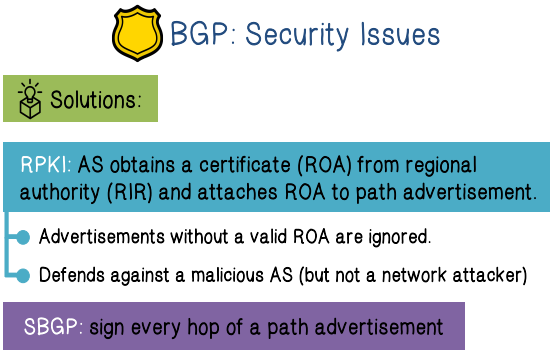


Here is an example of BGP path hijacking. Here is a normal or legitimate path. And then, there was path hijacking event in February 2013. In this attack, only the path of this direction from Mexico to DC is changed. The other direction is not changed. Therefore, if you are in DC, because this direction is not changed, you cannot tell by doing traceroute.

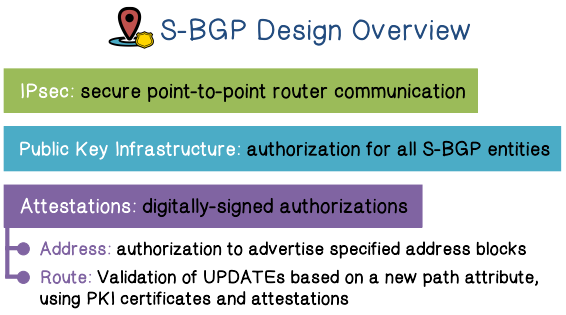


Now, let us do a quiz on BGP attacks. Match the attack to its characteristics.

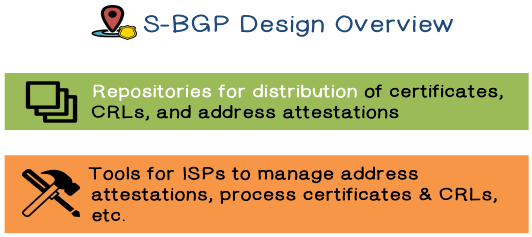
Denial-of-service attack: the attacker hacks the routing table and either adds a false route or kills a legitimate one. Sniffing: an attacker needs to control a device along the communication route. To do this, the attacker can use BGP to detour traffic through a malicious site. Routing to endpoints in malicious networks: this requires that the attacker redirect traffic away from a legitimate host to an attacker-controlled site. Creating route instabilities: this has not been exploited by attackers yet. These instabilities are too unpredictable and can cause attackers to be affected by their own attacks. However, there is a possibility that script kiddies could begin to exploit them. Revelation of network topologies: this begins with attacker gaining access to the routing table and can, with patience, discover the peer relations among the ASs.



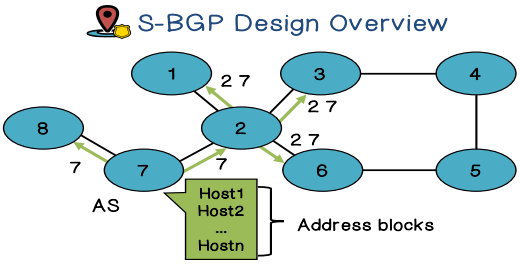
Now let us discuss some solutions to the BGP security issues. One solution is around PKI, or Public Key Infrastructure. Here, each AS obtains a certificate to certify each route origination authority from the regional Internet register, and then attach the ROA to path advertisement. Essentially, each AS that advertises a path is a route origination authority. Another solution is to use S-BGP. The main idea here is to sign every hop of a path advertisement.



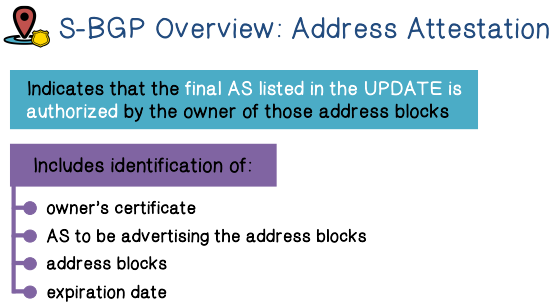
Let us discuss S-BGP in more detail. It uses IPsec to protect the point-to-point router communication. It also assumes PKI. The reason is that it uses public key cryptography to provide attestations. In particular, address attestation proves the authorization to advertise certain address blocks. And route attestations prove the validation of the route update information.



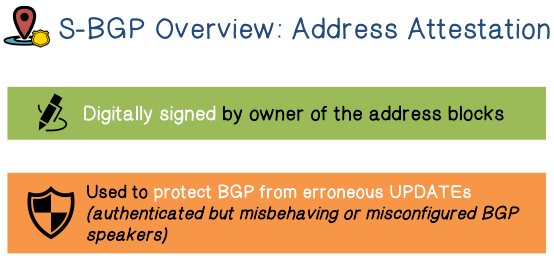
And of course S-BGP requires repositories and tools to manage certificates, the certificate's revocation lists and the address attestations.



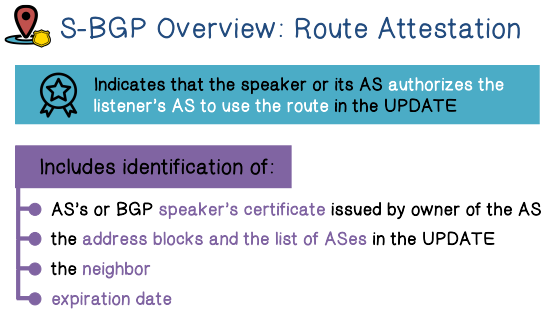
Here is an example of address blocks advertised by autonomous system node 7. This information is published for all the nodes to know that node 7 is responsible for these addresses.



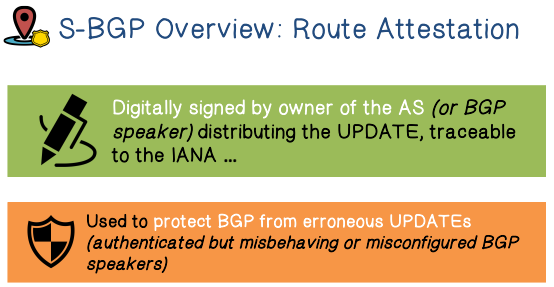
Now let us discuss attestation in more detail. In address attestation, the issuer is the organization that owns the address prefixes contained in the attestation and the subject is one or more ASs that are authorized to advertise these prefixes. For example, these ASs are the organization's internet service providers. In other words, an AS such as an ISP has to be authorized by the owner of the address blocks to advertise the route to these address blocks. An address attestation includes the following information. Essentially it certifies that the owner owns the address blocks and the owner authorizes the AS to advertise for this address blocks.



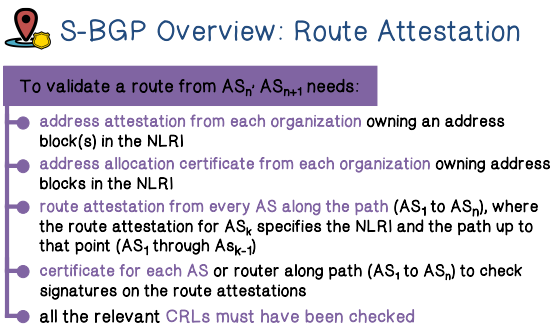
The owner uses his private key to sign the address blocks. Address attestation is used to protect BGP from incorrect updates.



The second type of attestation is route attestation. Here the issuer or the speaker is an AS and the subject or the listener is a transit AS. Basically, route attestation allows a BGP speaker that receives a route advertisement to verify that each AS along the route has been authorized by the preceding AS along the path to advertise that route. And that the originating AS has been authorized by the owner of each IP address prefix contained in the update to advertise these prefixes. Route attestation includes the following information: the speaker's certificate, the address block and the list of ASs, the neighbor, and the expiration date.



The signature guarantees that the organization owning the IP address space advertised in the update was allocated that address space through a chain of delegation originating at the IANA. And this can protect BGP from incorrect updates.



In order to validate a route, an AS needs to perform address attestation for each organization owning the address block. And route attestation for each AS along the path. And of course, all the certificates must be available, and they must be valid.