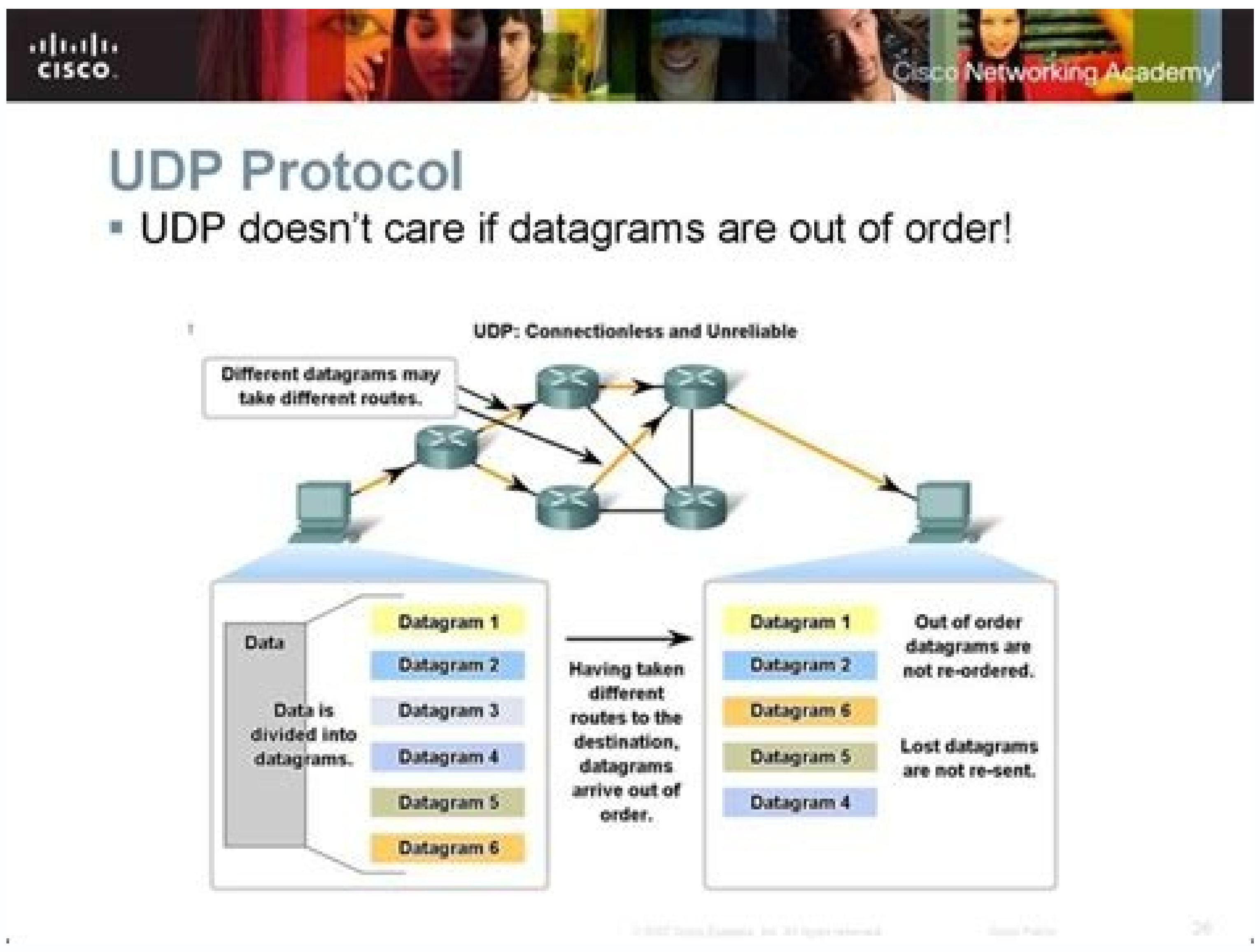
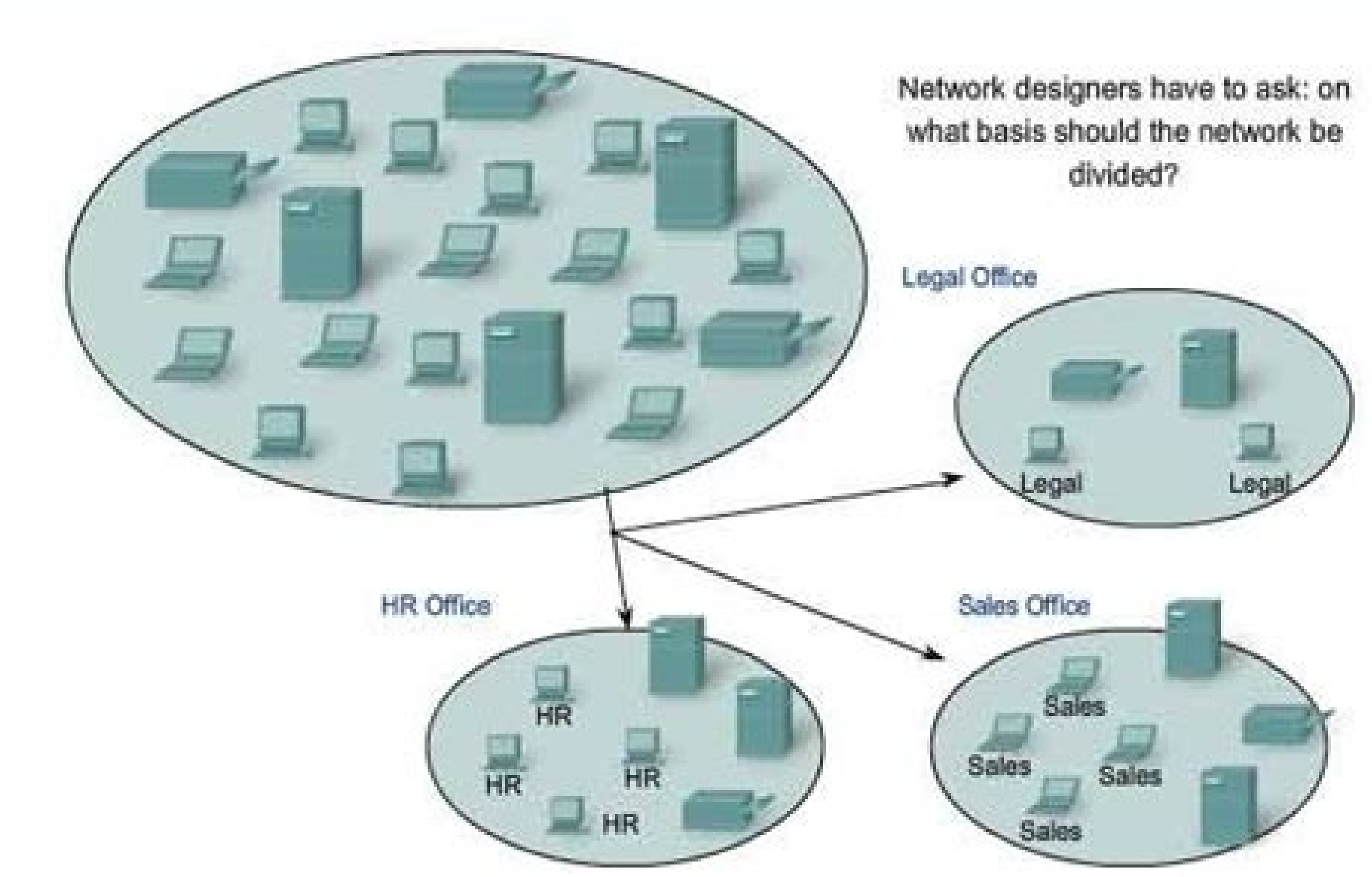
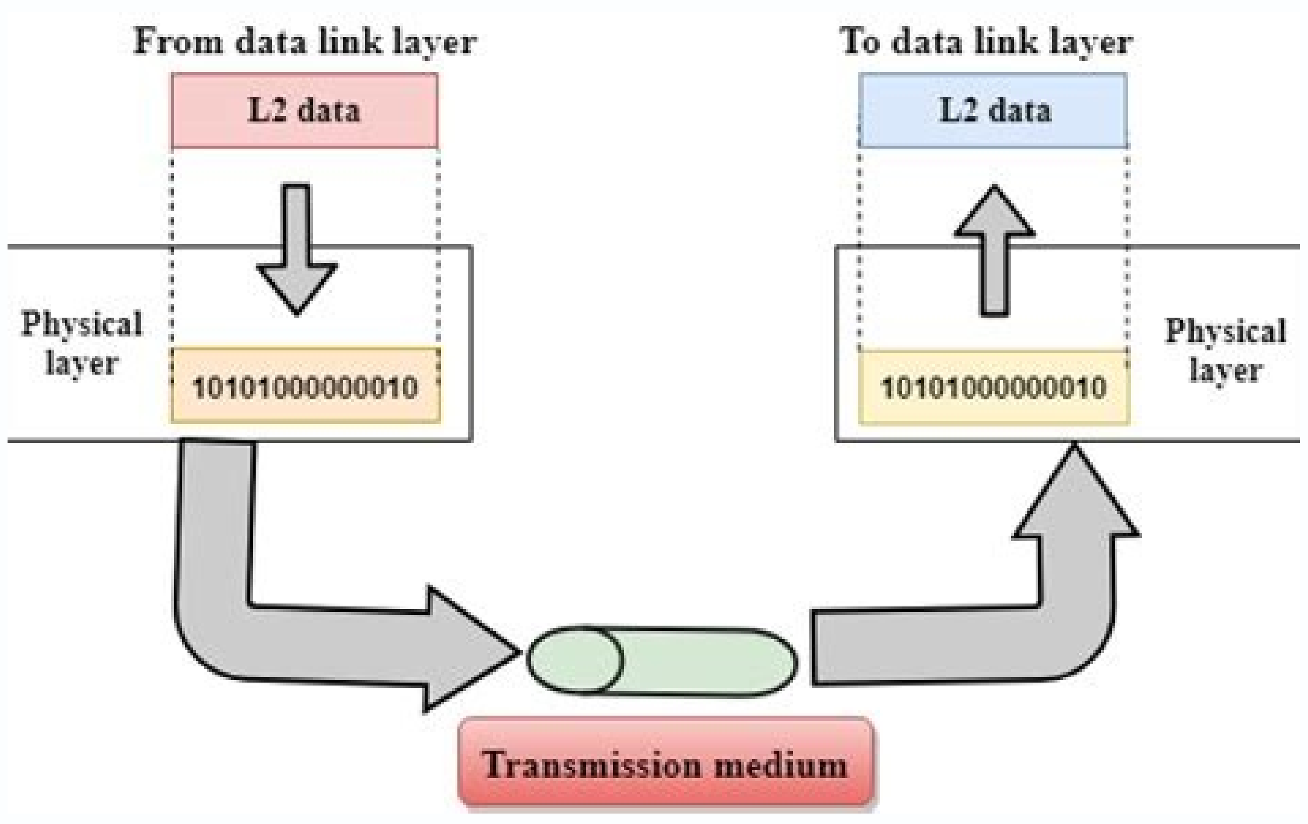
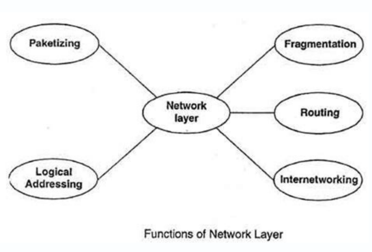
Purpose of network layer

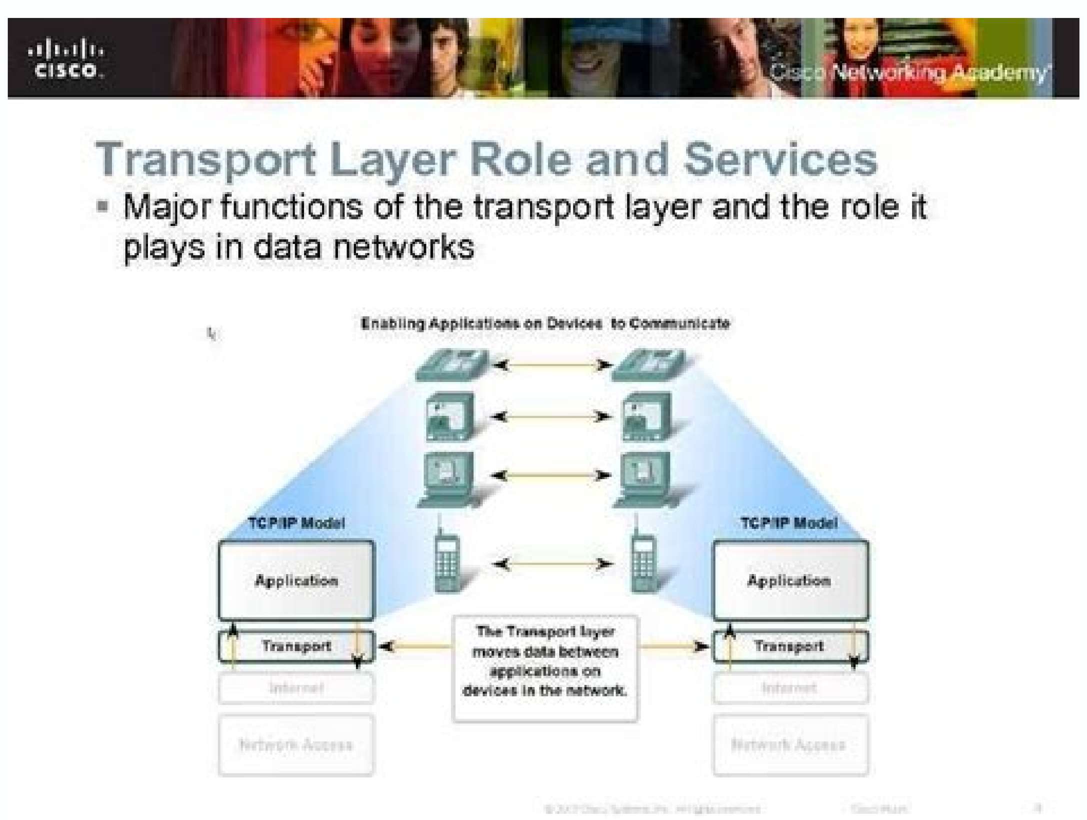
Continue











Purpose of network layer in osi model. Purpose of hidden layer in neural network. The purpose of the network access(of data link) layer is. What is the purpose of the tcp/ip network access layer. The primary purpose of a network layer protocol is to. Purpose of layering in computer network. Explain the purpose of network layer. What is the purpose of the network layer select 2 answers.

In order to continue enjoying our site, we ask that you confirm your identity as a human. Thank you very much for your cooperation. Functions of Network Layer: Internetworking: This is the main duty of network layer. It provides the logical connection between different types of networks. Addressing: Addressing is necessary to identify each device on the internet uniquely. This is similar to telephone system. The address used in the network layer should uniquely and universally define the connection of a computer. Routing: In a network, there are multiple roots available from a source to a destination and one of them is to be chosen. The network layer decides the root to be taken. This is called as routing and it depends on various criterions. Packetizing: The network layer encapsulates the packets received from upper layer protocol and makes new packets. This is called as packetizing. It is done by a network layer protocol called IP (Internetworking Protocol). Routing: Routing is a major component of the network layer and is concerned with the problem of determining feasible paths (or routes) for packets to follow from each source to each destination. The best path is the one that gives minimum end-to-end delay and with the greatest available bandwidth. Distance Vector Routing: Computer networks generally use dynamic routing algorithms that are more complex than flooding, but more efficient because they find shortest paths for the current topology. Two dynamic algorithms in particular, distance vector routing and link state routing, are the most popular. i. A distance vector routing algorithm operates by having each router maintain a table (i.e., a vector) giving the best known distance to each destination and which link to use to get there. These tables are updated by exchanging information with the neighbors. Eventually, every router knows the best link to reach each destination. ii. The distance vector routing algorithm is sometimes commonly known as distributed Bellman-Ford routing algorithm. iii. In distance vector routing, each router maintains a routing table indexed by, and containing one entry for each router in the network. This entry has two parts: the preferred outgoing line to use for that destination and an estimate of the distance to that destination. iv. The distance might be measured as the number of hops or using another metric. v. The router is assumed to know the ''distance'' to each of its neighbors. If the metric is hops, the distance is just one hop. If the metric is propagation delay, the router can measure it directly with special ECHO packets that the receiver just timestamps and sends back as fast as it can. As an example, assume that delay is used as a metric and that the router knows the delay to each of its neighbors. Once every T msec, each router sends to each neighbor a list of its estimated delays to each destination. It also receives a similar list from each neighbor. Imagine that one of these tables has just come in from neighbor X, with Xi being X's estimate of how long it takes to get to router i. If the router knows that the delay to X is m msec, it also knows that it can reach router i via X in Xi + m msec. By performing this calculation for each neighbor, a router can find out which estimate seems the best and use that estimate and the corresponding link in its new routing table. This updating process is illustrated in Fig. Part (a) shows a network. The first four columns of part (b) show the delay vectors received from the neighbors of router J. A claims to have a 12-msec delay to B, a 25-msec delay to C, a 40- msec delay to D, etc. Suppose that J has measured or estimated its delay to its neighbors, A, I, H, and K, as 8, 10, 12, and 6 msec, respectively. Consider how J computes its new route to router G. It knows that it can get to A in 8 msec, and furthermore A claims to be able to get to G in 18 msec, so J knows it can count on a delay of 26 msec to G if it forwards packets bound for G to A. Similarly, it computes the delay to G via I, H, and K as 41 (31 + 10), 18 (6 + 12), and 37 (31 + 6) msec, respectively. The best of these values is 18, so it makes an entry in its routing table that the delay to G is 18 msec and that the route to use is via H. The same calculation is performed for all the other destinations, with the new routing table shown in the last column of the figure. Examples of distance vector protocols include RIP - Routing Information Protocol and IGRP - Interior Gateway Routing Protocol. As explained earlier, the Internet is composed of more than 30,000 different networks [25] called domains. Each domain is composed of a group of routers and hosts that are managed by the same organisation. Example domains include belnet, sprint, level3, geant, abilene, cisco or google ...Each domain contains a set of routers. From a routing point of view, these domains can be divided into two classes : the transit and the stub domains. A stub domain sends and receives packets whose source or destination are one of its own hosts. A transit domain is a domain that provides a transit service for other domains, i.e. the routers in this domain forward packets whose source and destination do not belong to the transit domain. As of this writing, about 85% of the domains in the Internet are stub domains [40]. A stub domain that is connected to a single transit domain is called a single-homed stub. A multihomed stub is a stub domain connected to two or more transit providers.The stub domains can be further classified by considering whether they mainly send or receive packets. An access-rich stub domain is a domain that contains hosts that mainly receive packets. Typical examples include small ADSL- or cable modem-based Internet Service Providers or enterprise networks. On the other hand, a content-rich stub domain is a domain that mainly produces packets. Examples of content-rich stub domains include google, yahoo, microsoft, facebook or content distribution networks such as akamai or limelight For the last few years, we have seen a rapid growth of these content-rich stub domains. Recent measurements [ATLAS2009] indicate that a growing fraction of all the packets exchanged on the Internet are produced in the data centers managed by these content providers.Domains need to be interconnected to allow a host inside a domain to exchange IP packets with hosts located in other domains. From a physical perspective, domains can be interconnected in two different ways. The first solution is to directly connect a router belonging to the first domain with a router inside the second domain. Such links between domains are called private interdomain links or private peering links. In practice, for redundancy or performance reasons, distinct physical links are usually established between different routers in the two domains that are interconnected.Such private peering links are useful when, for example, an enterprise or university network needs to be connected to its Internet Service Provider. However, some domains are connected to hundreds of other domains [26] . For some of these domains, using only private peering links would be too costly. A better solution to allow many domains to interconnect cheaply are the Internet eXchange Points (IXP). An IXP is usually some space in a data center that hosts routers belonging to different domains. A domain willing to exchange packets with other domains present at the IXP installs one of its routers on the IXP and connects it to other routers inside its own network. The IXP contains a Local Area Network to which all the participating routers are connected. When two domains that are present at the IXP wish [28] to exchange packets, they simply use the Local Area Network. IXPs are very popular in Europe and many Internet Service Providers and Content providers are present in these IXPs.In the early days of the Internet, domains would simply exchange all the routes they know to allow a host inside one domain to reach any host in the global Internet. However, in today's highly commercial Internet, this is no longer true as interdomain routing mainly needs to take into account the economical relationships between the domains. Furthermore, while intradomain routing usually prefers some routes over others based on their technical merits (e.g. prefer route with the minimum number of hops, prefer route with the minimum delay, prefer high bandwidth routes over low bandwidth ones, etc) interdomain routing mainly deals with economical issues. For interdomain routing, the cost of using a route is often more important than the quality of the route measured by its delay or bandwidth.There are different types of economical relationships that can exist between domains. Interdomain routing converts these relationships into peering relationships between domains that are connected via peering links.The first category of peering relationship is the customer->provider relationship. Such a relationship is used when a customer domain pays an Internet Service Provider to be able to exchange packets with the global Internet over an interdomain link. A similar relationship is used when a small Internet Service Provider pays a larger Internet Service Provider to exchange packets with the global Internet.To understand the customer->provider relationship, let us consider the simple internetwork shown in the figure above. In this internetwork, AS7 is a stub domain that is connected to one provider : AS4. The contract between AS4 and AS7 allows a host inside AS7 to exchange packets with any host in the internetwork. To enable this exchange of packets, AS7 must know a route towards any domain and all the domains of the internetwork must know a route via AS4 that allows them to reach hosts inside AS7. From a routing perspective, the commercial contract between AS7 and AS4 leads to the following routes being exchanged :The second rule ensures that the customer domain receives a route towards all destinations that are reachable via its provider. The first rule allows the routes of the customer domain to be distributed throughout the Internet.Coming back to the figure above, AS4 advertises to its two providers AS1 and AS2 its own routes and the routes learned from its customer, AS7. On the other hand, AS4 advertises to AS7 all the routes that it knows.The second type of peering relationship is the shared-cost peering relationship. Such a relationship usually does not involve a payment from one domain to the other in contrast with the customer->provider relationship. A shared-cost peering relationship is usually established between domains having a similar size and geographic coverage. For example, consider the figure above. If AS3 and AS4 exchange many packets via AS1, they both need to pay AS1. A cheaper alternative for AS3 and AS4 would be to establish a shared-cost peering. Such a peering can be established at IXPs where both AS3 and AS4 are present or by using private peering links. This shared-cost peering should be used to exchange packets between hosts inside AS3 and hosts inside AS4. However, AS3 does not want to receive on the AS3-AS4 shared-cost peering links packets whose destination belongs to AS1 as AS3 would have to pay to send these packets to AS1.From a routing perspective, over a shared-cost peering relationship a domain only advertises its internal routes and the routes that it has learned from its customers. This restriction ensures that only packets destined to the local domain or one of its customers is received over the shared-cost peering relationship. This implies that the routes that have been learned from a provider or from another shared-cost peer is not advertised over a shared-cost peering relationship. This is motivated by economical reasons. If a domain were to advertise the routes that it learned from a provider over a shared-cost peering relationship that does not bring revenue, it would have allowed its shared-cost peer to use the link with its provider without any payment. If a domain were to advertise the routes it learned over a shared cost peering over another shared-cost peering relationship, it would have allowed these shared-cost peers to use its own network (which may span one or more continents) freely to exchange packets.Finally, the last type of peering relationship is the sibling. Such a relationship is used when two domains exchange all their routes in both directions. In practice, such a relationship is only used between domains that belong to the same company.These different types of relationships are implemented in the interdomain routing policies defined by each domain. The interdomain routing policy of a domain is composed of three main parts :A domain's import and export filters can be defined by using the Route Policy Specification Language (RPSL) specified in RFC 2622 [GAVE1999] . Some Internet Service Providers, notably in Europe, use RPSL to document [29] their import and export policies. Several tools help to easily convert a RPSL policy into router commands.The figure below provides a simple example of import and export filters for two domains in a simple internetwork. In RPSL, the keyword ANY is used to replace any route from any domain. It is typically used by a provider to indicate that it announces all its routes to a customer over a provider->customer relationship. This is the case for AS4's export policy. The example below clearly shows the difference between a provider->customer and a shared-cost peering relationship. AS4's export filter indicates that it announces only its internal routes (AS4) and the routes learned from its clients (AS7) over its shared-cost peering with AS3, while it advertises all the routes that it uses (including the routes learned from AS3) to AS7. The Internet uses a single interdomain routing protocol : the Border Gateway Protocol (BGP). The current version of BGP is defined in RFC 4271. BGP differs from the intradomain routing protocols that we have already discussed in several ways. First, BGP is a path-vector protocol. When a BGP router advertises a route towards a prefix, it announces the IP prefix and the interdomain path used to reach this prefix. From BGP's point of view, each domain is identified by a unique Autonomous System (AS) number [30] and the interdomain path contains the AS numbers of the transit domains that are used to reach the associated prefix. This interdomain path is called the AS Path. Thanks to these AS-Paths, BGP does not suffer from the count-to-infinity problems that affect distance vector routing protocols. Furthermore, the AS-Path can be used to implement some routing policies. Another difference between BGP and the intradomain routing protocols is that a BGP router does not send the entire contents of its routing table to its neighbours regularly. Given the size of the global Internet, routers would be overloaded by the number of BGP messages that they would need to process. BGP uses incremental updates, i.e. it only announces the routes that have changed to its neighbours. The figure below shows a simple example of the BGP routes that are exchanged between domains. In this example, prefix 1.0.0.0/8 is announced by AS1. AS1 advertises a BGP route towards this prefix to AS2. The AS-Path of this route indicates that AS1 is the originator of the prefix. When AS4 receives the BGP route from AS1, it re-announces it to AS2 and adds its AS number to the AS-Path. AS2 has learned two routes towards prefix 1.0.0.0/8. It compares the two routes and prefers the route learned from AS4 based on its own ranking algorithm. AS2 advertises to AS5 a route towards 1.0.0.0/8 with its AS-Path set to AS2:AS4:AS1. Thanks to the AS-Path, AS5 knows that if it sends a packet towards 1.0.0.0/8 the packet first passes through AS2, then through AS4 before reaching its destination inside AS1. Simple exchange of BGP routes BGP routers exchange routes over BGP sessions. A BGP session is established between two routers belonging to two different domains that are directly connected. As explained earlier, the physical connection between the two routers can be implemented as a private peering link or over an Internet eXchange Point. A BGP session between two adjacent routers runs above a TCP connection (the default BGP port is 179). In contrast with intradomain routing protocols that exchange IP packets or UDP segments, BGP runs above TCP because TCP ensures a reliable delivery of the BGP messages sent by each router without forcing the routers to implement acknowledgements, checksums, etc. Furthermore, the two routers consider the peering link to be up as long as the BGP session and the underlying TCP connection remain up [31]. The two endpoints of a BGP session are called BGP peers. A BGP peering session between two directly connected routers In practice, to establish a BGP session between routers R1 and R2 in the figure above, the network administrator of AS3 must first configure on R1 the IP address of R2 on the R1-R2 link and the AS number of R2. Router R1 then regularly tries to establish the BGP session with R2. R2 only agrees to establish the BGP session with R1 once it has been configured with the IP address of R1 and its AS number. For security reasons, a router never establishes a BGP session that has not been manually configured on the router. The BGP protocol RFC 4271 defines several types of messages that can be exchanged over a BGP session : OPEN : this message is sent as soon as the TCP connection between the two routers has been established. It initialises the BGP session and allows the negotiation of some options. Details about this message may be found in RFC 4271 NOTIFICATION : this message is used to terminate a BGP session, usually because an error has been detected by the BGP peer. A router that sends or receives a NOTIFICATION message immediately shutdowns the corresponding BGP session. UPDATE: this message is used to advertise new or modified routes or to withdraw previously advertised routes. KEEPALIVE : this message is used to ensure a regular exchange of messages on the BGP session, even when no route changes. When a BGP router has not sent an UPDATE message during the last 30 seconds, it shall send a KEEPALIVE message to confirm to the other peer that it is still up. If a peer does not receive any BGP message during a period of 90 seconds [32], the BGP session is considered to be down and all the routes learned over this session are withdrawn. As explained earlier, BGP relies on incremental updates. This implies that when a BGP session starts, each router first sends BGP UPDATE messages to advertise to the other peer all the exportable routes that it knows. Once all these routes have been advertised, the BGP router only sends BGP UPDATE messages about a prefix if the route is new, one of its attributes has changed or the route became unreachable and must be withdrawn. The BGP UPDATE message allows BGP routers to efficiently exchange such information while minimising the number of bytes exchanged. Each UPDATE message contains : a list of IP prefixes that are withdrawn a list of IP prefixes that are (re-)advertised the set of attributes (e.g. AS-Path) associated to the advertised prefixes In the remainder of this chapter, and although all routing information is exchanged using BGP UPDATE messages, we assume for simplicity that a BGP message contains only information about one prefix and we use the words : Withdraw message to indicate a BGP UPDATE message containing one route that is withdrawn Update message to indicate a BGP UPDATE containing a new or updated route towards one destination prefix with its attributes From a conceptual point of view, a BGP router connected to N BGP peers, can be described as being composed of four parts as shown in the figure below. Organisation of a BGP router In this figure, the router receives BGP messages on the left part of the figure, processes these messages and possibly sends BGP messages on the right part of the figure. A BGP router contains three important data structures : the Adj-RIB-In contains the BGP routes that have been received from each BGP peer. The routes in the Adj-RIB-In are filtered by the import filter before being placed in the BGP-Loc-RIB. There is one import filter per BGP peer. the Local Routing Information Base (Loc-RIB) contains all the routes that are considered as acceptable by the router. The Loc-RIB may contain several routes, learned from different BGP peers, towards the same destination prefix. the Forwarding Information Base (FIB) is used by the dataplane to forward packets towards their destination. The FIB contains, for each destination, the best route that has been selected by the BGP decision process. This decision process is an algorithm that selects, for each destination prefix, the best route according to the router's ranking algorithm that is part of its policy. the Adj-RIB-Out contains the BGP routes that have been advertised to each BGP peer. The Adj-RIB-Out for a given peer is built by applying the peer`s export filter on the routes that have been installed in the FIB. There is one export filter per BGP peer. For this reason, the Adj-RIB-Out of a peer may contain different routes than the Adj-RIB-Out of another peer. When a BGP session starts, the routers first exchange OPEN messages to negotiate the options that apply throughout the entire session. Then, each router extracts from its FIB the routes to be advertised to the peer. It is important to note that, for each known destination prefix, a BGP router can only advertise to a peer the route that it has itself installed inside its FIB. The routes that are advertised to a peer must pass the peer's export filter. The export filter is a set of rules that define which routes can be advertised over the corresponding session, possibly after having modified some of its attributes. One export filter is associated to each BGP session. For example, on a shared-cost peering, the export filter only selects the internal routes and the routes that have been learned from a customer. The pseudo-code below shows the initialisation of a BGP session. def initiliaze_BGP_session(RemoteAS, RemoteIP): # Initialize and start BGP session # Send BGP OPEN Message to RemoteIP on port 179 # Follow BGP state machine # advertise local routes and routes learned from peers*/ for d in BGPLocRIB : B=build_BGP_Update(d) S=Apply_Export_Filter(RemoteAS,B) if (S != None) : send_Update(S,RemoteAS,RemoteIP) # entire RIB has been sent # new Updates will be sent to reflect local or distant # changes in routers In the above pseudo-code, the build_BGP_UPDATE(d) procedure extracts from the BGP Loc-RIB the best path towards destination d (i.e. the route installed in the FIB) and prepares the corresponding BGP UPDATE message. This message is then passed to the export filter that returns NULL if the route cannot be advertised to the peer or the (possibly modified) BGP UPDATE message to be advertised. BGP routers allow network administrators to specify very complex export filters, see e.g. [WMS2004]. A simple export filter that implements the equivalent of split horizon is shown below. def apply_export_filter(RemoteAS, BGPMsg) : # check if RemoteAS already received route if RemoteAS is BGPMsg.ASPath : BGPMsg=None # Many additional export policies can be configured : # Accept or refuse the BGPMsg # Modify selected attributes inside BGPMsg return BGPMsg At this point, the remote router has received all the exportable BGP routes. After this initial exchange, the router only sends BGP UPDATE messages when there is a change (addition of a route, removal of a route or change in the attributes of a route) in one of these exportable routes. Such a change can happen when the router receives a BGP message. The pseudo-code below summarizes the processing of these BGP messages. def Recvd_BGPMsg(Msg, RemoteAS) : B=apply_import_filer(Msg,RemoteAS) if (B== None): # Msg not acceptable return if IsUPDATE(Msg): Old_Route=BestRoute(Msg.prefix) Insert_in_RIB(Msg) Run_Decision_Process(RIB) if (BestRoute(Msg.prefix) != Old_Route) : # best route changed B=build_BGP_Message(Msg.prefix); S=apply_export_filter(RemoteAS,B); if (S!=None) : # announce best route send_UPDATE(S,RemoteAS,RemoteIP); else if (Old_Route != None) : send_WITHDRAW(Msg.prefix,RemoteAS, RemoteIP) else : # Msg is WITHDRAW Old_Route=BestRoute(Msg.prefix) Remove_from_RIB(Msg) Run_Decision_Process(RIB) if (Best_Route(Msg.prefix) !=Old_Route): # best route changed B=build_BGP_Message(Msg.prefix) S=apply_export_filter(RemoteAS,B) if (S != None) : # still one best route towards Msg.prefix send_UPDATE(S,RemoteAS, RemoteIP); else if(Old_Route != None) : # No best route anymore send_WITHDRAW(Msg.prefix,RemoteAS,RemoteIP); When a BGP message is received, the router first applies the peer's import filter to verify whether the message is acceptable or not. If the message is not acceptable, the processing stops. The pseudo-code below shows a simple import filter. This import filter accepts all routes, except those that already contain the local AS in their AS-Path. If such a route was used, it would cause a routing loop. Another example of an import filter would be a filter used by an Internet Service Provider on a session with a customer to only accept routes towards the IP prefixes assigned to the customer by the provider. On real routers, import filters can be much more complex and some import filters modify the attributes of the received BGP UPDATE [WMS2004] . def apply_import_filter(RemoteAS, BGPMsg): if MysAS in BGPMsg.ASPath : BGPMsg=None # Many additional import policies can be configured : # Accept or refuse the BGPMsg # Modify selected attributes inside BGPMsg return BGPMsg Note The bogon filters Another example of frequently used import filters are the filters that Internet Service Providers use to ignore bogon routes. In the ISP community, a bogon route is a route that should not be advertised on the global Internet. Typical examples include the private IPv4 prefixes defined in RFC 1918, the loopback prefixes (127.0.0.1/8 and ::1/128) or the IP prefixes that have not yet been allocated by IANA. A well managed BGP router should ensure that it never advertises bogons on the global Internet. Detailed information about these bogons may be found at If the import filter accepts the BGP message, the pseudo-code distinguishes two cases. If this is an Update message for prefix p, this can be a new route for this prefix or a modification of the route's attributes. The router first retrieves from its RIB the best route towards prefix p. Then, the new route is inserted in the RIB and the BGP decision process is run to find whether the best route towards destination p changes. A BGP message only needs to be sent to the router's peers if the best route has changed. For each peer, the router applies the export filter to verify whether the route can be advertised. If yes, the filtered BGP message is sent. Otherwise, a Withdraw message is sent. When the router receives a Withdraw message, it also verifies whether the removal of the route from its RIB caused its best route towards this prefix to change. It should be noted that, depending on the content of the RIB and the export filters, a BGP router may need to send a Withdraw message to a peer after having received an Update message from another peer and conversely. Let us now discuss in more detail the operation of BGP in an IPv4 network. For this, let us consider the simple network composed of three routers located in three different ASes and shown in the figure below. Utilisation of the BGP nexthop attribute This network contains three routers : R1, R2 and R3. Each router is attached to a local IPv4 subnet that it advertises using BGP. There are two BGP sessions, one between R1 and R2 and the second between R2 and R3. A /30 subnet is used on each interdomain link (195.100.0.0/30 on R1-R2 and 195.100.0.4/30 on R2-R3). The BGP sessions run above TCP connections established between the neighbouring routers (e.g. 195.100.0.1 - 195.100.0.2 for the R1-R2 session). Let us assume that the R1-R2 BGP session is the first to be established. A BGP Update message sent on such a session contains three fields : the advertised prefix the BGP nexthop the attributes including the AS-Path We use the notation U(prefix, nexthop, attributes) to represent such a BGP Update message in this section. Similarly, W(prefix) represents a BGP withdraw for the specified prefix. Once the R1-R2 session has been established, R1 sends U(194.100.0.0/24,195.100.0.1,AS10) to R2 and R2 sends U(194.100.2.0/23,195.100.0.2,AS20). At this point, R1 can reach 194.100.2.0/23 via 195.100.0.2 and R2 can reach 194.100.0.0/24 via 195.100.0.1. Once the R2-R3 has been established, R3 sends U(194.100.1.0/24,195.100.0.6,AS30). R2 announces on the R2-R3 session all the routes inside its RIB. It thus sends to R3 : U(194.100.0.0/24,195.100.0.5,AS20:AS10) and U(194.100.2.0/23,195.100.0.5,AS20). Note that when R2 advertises the route that it learned from R1, it updates the BGP nexthop and adds its AS number to the AS-Path. R2 also sends U(194.100.1.0/24,195.100.0.2,AS20:AS30) to R1 on the R1-R3 session. At this point, all BGP routes have been exchanged and all routers can reach 194.100.0.0/24, 194.100.2.0/23 and 194.100.1.0/24. If the link between R2 and R3 fails, R3 detects the failure as it did not receive KEEPALIVE messages recently from R2. At this time, R3 removes from its RIB all the routes learned over the R2-R3 BGP session. R2 also removes from its RIB the routes learned from R3. R2 also sends W(194.100.1.0/24) to R1 over the R1-R3 BGP session since it does not have a route anymore towards this prefix. Note Origin of the routes advertised by a BGP router A frequent practical question about the operation of BGP is how a BGP router decides to originate or advertise a route for the first time. In practice, this occurs in two situations : the router has been manually configured by the network operator to always advertise one or several routes on a BGP session. For example, on the BGP session between UCLouvain and its provider, belnet , UCLouvain's router always advertises the 130.104.0.0/16 IPv4 prefix assigned to the campus network the router has been configured by the network operator to advertise over its BGP session some of the routes that it learns with its intradomain routing protocol. For example, an enterprise router may advertise over a BGP session with its provider the routes to remote sites when these routes are reachable and advertised by the intradomain routing protocol The first solution is the most frequent. Advertising routes learned from an intradomain routing protocol is not recommended, this is because if the route flaps [33], this would cause a large number of BGP messages being exchanged in the global Internet. Most networks that use BGP contain more than one router. For example, consider the network shown in the figure below where AS20 contains two routers attached to interdomain links : R2 and R4. In this network, two routing protocols are used by R2 and R4. They use an intradomain routing protocol such as OSPF to distribute the routes towards the internal prefixes : 195.100.0.8/30, 195.100.0.0/30, ... R2 and R4 also use BGP. R2 receives the routes advertised by AS10 while R4 receives the routes advertised by AS30. These two routers need to exchange the routes that they have respectively received over their BGP sessions. A larger network using BGP A first solution to allow R2 and R3 to exchange the interdomain routes that they have learned over their respective BGP sessions would be to configure the intradomain routing protocol to distribute inside AS20 the routes learned over the BGP sessions. Although current routers support this feature, this is a bad solution for two reasons : Intradomain routing protocols cannot distribute the attributes that are attached to a BGP route. If R4 received via the intradomain routing protocol a route towards 194.100.0.0/23 that R2 learned via BGP, it would not know that the route was originated by AS10 and the only advertisement that it could send to R3 would contain an incorrect AS-Path Intradomain routing protocols have not been designed to support the hundreds of thousands of routes that a BGP router can receive on today's global Internet. The best solution to allow BGP routers to distribute, inside an AS, all the routes learned over BGP sessions is to establish BGP sessions among all the BGP routers inside the AS. In practice, there are two types of BGP sessions : eBGP session or external BGP session. Such a BGP session is established between two routers that are directly connected and belong to two different domains. iBGP session or internal BGP session. Such a BGP session is established between two routers belonging to the same domain. These two routers do not need to be directly connected. In practice, each BGP router inside a domain maintains an iBGP session with every other BGP router in the domain [35]. This creates a full-mesh of iBGP sessions among all BGP routers of the domain. iBGP sessions, like eBGP sessions run over TCP connections. Note that in contrast with eBGP sessions that are established between directly connected routers, iBGP sessions are often established between routers that are not directly connected. An important point to note about iBGP sessions is that a BGP router only advertises a route over an iBGP session provided that : the router uses this route to forward packets, and the route was learned over one of the router's eBGP sessions A BGP router does not advertise a route that it has learned over an iBGP session over another iBGP session. Note that a router can, of course, advertise over an eBGP session a route that it has learned over an iBGP session. This difference between the behaviour of a BGP router over iBGP and eBGP session is due to the utilisation of a full-mesh of iBGP sessions. Consider a network containing three BGP routers : A, B and C interconnected via a full-mesh of iBGP sessions. If router A learns a route towards prefix p from router B, router A does not need to advertise the received route to router C since router C also learns the same route over the C-B iBGP session. To understand the utilisation of an iBGP session, let us consider what happens when router R1 sends U(194.100.0.0/23,195.100.0.1,AS10) in the network shown below. This BGP message is processed by R2 which advertises it over its iBGP session with R4. The BGP Update sent by R2 contains the same nexthop and the same AS-Path as in the BGP Update received by R2. R4 then sends U(194.100.0.0/23,195.100.0.5,AS20:AS10) to R3. Note that the BGP nexthop and the AS-Path are only updated [34] when a BGP route is advertised over an eBGP session. iBGP and eBGP sessions Note Loopback interfaces and iBGP sessions In addition to their physical interfaces, routers can also be configured with a special loopback interface[#fbgploop]_. A loopback interface is a software interface that is always up. When a loopback interface is configured on a router, the address associated to this interface is advertised by the intradomain routing protocol. Consider for example a router with two point-to-point interfaces and one loopback interface. When a point-to-point interface fails, it becomes unreachable and the router cannot receive anymore packets via this IP address. This is not the case for the loopback interface. It remains reachable as long as at least one of the router's interfaces remains up. iBGP sessions are usually established using the router's loopback addresses as endpoints. This allows the iBGP session and its underlying TCP connection to remain up even if physical interfaces fail on the routers. Now that routers can learn interdomain routes over iBGP and eBGP sessions, let us examine what happens when router R3 sends a packet destined to 194.100.1.234. R3 forwards this packet to R4. R4 uses an intradomain routing protocol and BGP. Its BGP routing table contains the following longest prefix match : 194.100.0.0/23 via 195.100.0.1 This routes indicates that to forward a packet towards 194.100.0.0/23, R4 needs to forward the packet along the route towards 195.100.0.1. However, R4 is not directly connected to 195.100.0.1. R4 learned a route that matches this address thanks to its intradomain routing protocol that distributed the following routes : 195.100.0.0/30 via 195.100.0.10 195.100.0.4/30 East 195.100.0.8/30 North 194.100.2.0/23 via 195.100.0.10 194.100.0.4/23 West To build its forwarding table, R4 must combine the routes learned from the intradomain routing protocol with the routes learned from BGP. Thanks to its intradomain routing table, for each interdomain route R4 replaces the BGP nexthop with its shortest path computed by the intradomain routing protocol. In the figure above, R4 forwards packets to 194.100.0.0/23 via 195.100.0.10 to which it is directly connected via its North interface. R4 's resulting forwarding table, which associates an outgoing interface for a directly connected prefix or a directly connected nexthop and an outgoing interface for prefixes learned via BGP, is shown below : 194.100.0.0/23 via 195.100.0.10 (North) 195.100.0.0/30 via 195.100.0.10 (North) 195.100.0.4/30 East 195.100.0.8/30 North 194.100.2.0/23 via 195.100.0.10 (North) 194.100.4.0/23 West There is thus a coupling between the interdomain and the intradomain routing tables. If the intradomain routes change, e.g. due to link failures or changes in link metrics, then the forwarding table must be updated on each router as the shortest path towards a BGP nexthop may have changed. The last point to be discussed before looking at the BGP decision process is that a network may contain routers that do not maintain any eBGP session. These routers can be stub routers attached to a single router in the network or core routers that reside on the path between two border routers that are using BGP as illustrated in the figure below. How to deal with non-BGP routers ? In the scenario above, router R2 needs to be able to forward a packet towards any destination in the 12.0.0.0/8 prefix inside AS30. Such a packet would need to be forwarded by router R5 since this router resides on the path between R2 and its BGP nexthop attached to R4. Two solutions can be used to ensure that R2 is able to forward such interdomain packets : enable BGP on router R5 and include this router in the iBGP full-mesh. Two iBGP sessions would be added in the figure above : R2-R5 and R4-R5. This solution works and is used by many ASes. However, it forces all routers to have enough resources (CPU and memory) to run BGP and maintain a large forwarding table encapsulate the interdomain packets sent through the AS so that router R5 never needs to forward a packet whose destination is outside the local AS. Different encapsulation mechanisms exist. MultiProtocol Label Switching (MPLS) RFC 3031 and the Layer 2 Tunneling Protocol (L2TP) RFC 3931 are frequently used in large domains, but a detailed explanation of these techniques is outside the scope of this section. The simplest encapsulation scheme to understand is in IP in IP defined in RFC 2003. This encapsulation scheme places an IP packet (called the inner packet), including its payload, as the payload of a larger IP packet (called the outer packet). It can be used by border routers to forward packets via routers that do not maintain a BGP routing table. For example, in the figure above, if router R2 needs to forward a packet towards destination 12.0.0.1, it can add at the front of this packet an IPv4 header whose source address is set to one of its IPv4 addresses and whose destination address is one of the IPv4 addresses of R4. The Protocol field of the IP header is set to 4 to indicate that it contains an IPv4 packet. The packet is forwarded by R5 to R4 based on the forwarding table that it built thanks to its intradomain routing table. Upon reception of the packet, R4 removes the outer header and consults its (BGP) forwarding table to forward the packet towards R3. Besides the import and export filters, a key difference between BGP and the intradomain routing protocols is that each domain can define is own ranking algorithm to determine which route is chosen to forward packets when several routes have been learned towards the same prefix. This ranking depends on several BGP attributes that can be attached to a BGP route. The first BGP attribute that is used to rank BGP routes is the local-preference (local-pref) attribute. This attribute is an unsigned integer that is attached to each BGP route received over an eBGP session by the associated import filter. When comparing routes towards the same destination prefix, a BGP router always prefers the routes with the highest local-pref. If the BGP router knows several routes with the same local-pref, it prefers among the routes having this local-pref the ones with the shortest AS-Path. The local-pref attribute is often used to prefer some routes over others. This attribute is always present inside BGP Updates exchanged over iBGP sessions, but never present in the messages exchanged over eBGP sessions. A common utilisation of local-pref is to support backup links. Consider the situation depicted in the figure below. AS1 would always like to use the high bandwidth link to send and receive packets via AS2 and only use the backup link upon failure of the primary one. How to create a backup link with BGP ? As BGP routers always prefer the routes with the highest local-pref attribute, this policy can be implemented using the following import filter on R1 import: from AS2 RA at R1 set localpref=100; from AS2 RB at R1 set localpref=200; accept ANY With this import filter, all the BGP routes learned from RB over the high bandwidth links are preferred over the routes learned over the backup link. If the primary link fails, the corresponding routes are removed from R1's RIB and R1 uses the route learned from RA. R1 reuses the routes via RB as soon as they are advertised by RB once the R1-RB link comes back. The import filter above modifies the selection of the BGP routes inside AS1. Thus, it influences the route followed by the packets forwarded by AS1. In addition to using the primary link to send packets, AS1 would like to receive its packets via the high bandwidth link. For this, AS2 also needs to set the local-pref attribute in its import filter. import: from AS1 R1 at RA set localpref=100; from AS1 R1 at RB set localpref=200; accept AS1 Sometimes, the local-pref attribute is used to prefer a cheap link compared to a more expensive one. For example, in the network below, AS1 could wish to send and receive packets mainly via its interdomain link with AS4. How to prefer a cheap link over an more expensive one ? AS1 can install the following import filter on R1 to ensure that it always sends packets via R2 when it has learned a route via AS2 and another via AS4. import: from AS2 RA at R1 set localpref=100; from AS4 R2 at R1 set localpref=200; accept ANY However, this import filter does not influence how AS3 , for example, prefers some routes over others. If the link between AS3 and AS2 is less expensive than the link between AS3 and AS4, AS3 could send all its packets via AS2 and AS1 would receive packets over its expensive link. An important point to remember about local-pref is that it can be used to prefer some routes over others to send packets, but it has no influence on the routes followed by received packets. Another important utilisation of the local-pref attribute is to support the customer->provider and shared-cost peering relationships. From an economic point of view, there is an important difference between these three types of peering relationships. A domain usually earns money when it sends packets over a provider->customer relationship. On the other hand, it must pay its provider when it sends packets over a customer->provider relationship. Using a shared-cost peering to send packets is usually neutral from an economic perspective. To take into account these economic issues, domains usually configure the import filters on their routers as follows : insert a high local-pref attribute in the routes learned from a customer insert a medium local-pref attribute in the routes learned over a shared-cost peering insert a low local-pref attribute in the routes learned from a provider With such an import filter, the routers of a domain always prefer to reach destinations via their customers whenever such a route exists. Otherwise, they prefer to use shared-cost peering relationships and they only send packets via their providers when they do not know any alternate route. A consequence of setting the local-pref attribute like this is that Internet paths are often asymmetrical. Consider for example the internetwork shown in the figure below. Asymmetry of Internet paths Consider in this internetwork the routes available inside AS1 to reach AS5. AS1 learns the AS4:AS6:AS7:AS5 path from AS4, the AS3:AS8:AS5 path from AS3 and the AS2:AS5 path from AS2. The first path is chosen since it was from learned from a customer. AS5 on the other hand receives three paths towards AS1 via its providers. It may select any of these paths to reach AS1 , depending on how it prefers one provider over the others. Coming back to the organisation of a BGP router shown in figure Organisation of a BGP router, the last part to be discussed is the BGP decision process. The BGP Decision Process is the algorithm used by routers to select the route to be installed in the FIB when there are multiple routes towards the same prefix. The BGP decision process receives a set of candidate routes towards the same prefix and uses seven steps. At each step, some routes are removed from the candidate set and the process stops when the set only contains one route [36] : Ignore routes having an unreachable BGP nexthop Prefer routes having the highest local-pref Prefer routes having the shortest AS-Path Prefer routes having the smallest MED Prefer routes learned via eBGP sessions over routes learned via iBGP sessions Prefer routes having the closest next-hop Tie breaking rules : prefer routes learned from the router with lowest router id The first step of the BGP decision process ensures that a BGP router does not install in its FIB a route whose nexthop is considered to be unreachable by the intradomain routing protocol. This could happen, for example, when a router has crashed. The intradomain routing protocol usually advertises the failure of this router before the failure of the BGP sessions that it terminates. This rule implies that the BGP decision process must be re-run each time the intradomain routing protocol reports a change in the reachability of a prefix containing one of more BGP nexthops. The second rule allows each domain to define its routing preferences. The local-pref attribute is set by the import filter of the router that learned a route over an eBGP session. In contrast with intradomain routing protocols, BGP does not contain an explicit metric. This is because in the global Internet it is impossible for all domains to agree on a common metric that meets the requirements of all domains. Despite this, BGP routers prefer routes having a short AS-Path attribute over routes with a long AS-Path. This step of the BGP decision process is motivated by the fact that operators expect that a route with a long AS-Path is lower quality than a route with a shorter AS-Path. However, studies have shown that there was not always a strong correlation between the quality of a route and the length of its AS-Path [HFPMC2002]. Before explaining the fourth step of the BGP decision process, let us first describe the fifth and the sixth steps of the BGP decision process. These two steps are used to implement hot potato routing. Intuitively, when a domain implements hot potato routing, it tries to forward packets that are destined to addresses outside of its domain, to other domains as quickly as possible. To understand hot potato routing, let us consider the two domains shown in the figure below. AS2 advertises prefix 1.0.0.0/8 over the R2-R6 and R3-R7 peering links. The routers inside AS1 learn two routes towards 1.0.0.0/8: one via R6-R2 and the second via R7-R3. Hot and cold potato routing With the fifth step of the BGP decision process, a router always prefers to use a route learned over an eBGP session compared to a route learned over an iBGP session. Thus, router R6 (resp. R7) prefers to use the route via router R2 (resp. R3) to reach prefix 1.0.0.0/8. The sixth step of the BGP decision process takes into account the distance, measured as the length of the shortest intradomain path, between a BGP router and the BGP nexthop for routes learned over iBGP sessions. This rule is used on router R8 in the example above. This router has received two routes towards 1.0.0.0/8: 1.0.0.0/8 via R7 that is at a distance of 1 from R8 1.0.0.0/8 via R6 that is at a distance of 50 from R8 The first route, via R7 is the one that router R8 prefers, as this is the route that minimises the cost of forwarding packets inside AS1 before sending them to AS2. Hot potato routing allows AS1 to minimise the cost of forwarding packets towards AS2. However, there are situations where this is not desirable. For example, assume that AS1 and AS2 are domains with routers on both the East and the West coast of the US. In these two domains, the high metric associated to links R6-R8 and R0-R2 correspond to the cost of forwarding a packet across the USA. If AS2 is a customer that pays AS1, it would prefer to receive the packets destined to 1.0.0.0/8 via the R2-R6 link instead of the R7-R3 link. This is the objective of cold potato routing. Cold potato routing is implemented using the Multi-Exit Discriminator (MED) attribute. This attribute is an optional BGP attribute that may be set [37] by border routers when advertising a BGP route over an eBGP session. The MED attribute is usually used to indicate over an eBGP session the cost to reach the BGP nexthop for the advertised route. The MED attribute is set by the router that advertises a route over an eBGP session. In the example above, router R2 sends U(1.0.0.0/8,R2,AS2,MED=1) while R3 sends U(1.0.0.0/8,R3,AS2,MED=98). Assume that the BGP session R7-3 is the first to be established. R7 sends U(1.0.0.0/8,R3,AS2,MED=98) to both R8 and R6. At this point, all routers inside AS1 send the packets towards 1.0.0.0/8 via R7-R3. Then, the R6-R2 BGP session is established and router R6 receives U(1.0.0.0/8,R2,AS2,MED=1). Router R6 runs its decision process for destination 1.0.0.0/8 and selects the route via R2 as its chosen route to reach this prefix since this is the only route that it knows. R6 sends U(1.0.0.0/8,R2,AS2,MED=1) to routers R8 and R7. They both run their decision process and prefer the route advertised by R6, as it contains the smallest MED. Now, all routers inside AS1 forward the packets to 1.0.0.0/8 via link R6-R2 as expected by AS2. As router R7 no longer uses the BGP route learned via R3, it must stop advertising it over iBGP sessions and sends W(1.0.0.0/8) over its iBGP sessions with R6 and R8. However, router R7 still keeps the route learned from R3 inside its Adj-RIB-In. If the R6-R2 link fails, R6 sends W(1.0.0.0/8) over its iBGP sessions and router R7 responds by sending U(1.0.0.0/8,R3,AS2,MED=98) over its iBGP sessions. In practice, the fifth step of the BGP decision process is slightly more complex, as the routes towards a given prefix can be learned from different ASes. For example, assume that in figure Hot and cold potato routing, 1.0.0.0/8 is also advertised by AS3 (not shown in the figure) that has peering links with routers R6 and R8. If AS3 advertises a route whose MED attribute is set to 2 and another with a MED set to 3, how should AS1's router compare the four BGP routes towards 1.0.0.0/8 ? Is a MED value of 1 from AS2 better than a MED value of 2 from AS3 ? The fifth step of the BGP decision process solves this problem by only comparing the MED attribute of the routes learned from the same neighbour AS. Additional details about the MED attribute may be found in RFC 4451. It should be noted that using the MED attribute may cause some problems in BGP networks as explained in [GW2002]. In practice, the MED attribute is not used on eBGP sessions unless the two domains agree to enable it. The last step of the BGP decision allows the selection of a single route when a BGP router has received several routes that are considered as equal by the first six steps of the decision process. This can happen for example in a dual-homed stub attached to two different providers. As shown in the figure below, router R1 receives two equally good BGP routes towards 1.0.0.0/8. To break the ties, each router is identified by a unique router-id which in practice is one of the IP addresses assigned to the router. On some routers, the lowest router id step in the BGP decision process is replaced by the selection of the oldest route RFC 5004. Preferring the oldest route when breaking ties is used to prefer stable paths over unstable paths. However, a drawback of this approach is that the selection of the BGP routes depends on the arrival times of the corresponding messages. This makes the BGP selection process non-deterministic and can lead to problems that are difficult to debug. A stub connected to two providers In the previous sections, we have explained the operation of BGP routers. Compared to intradomain routing protocols, a key feature of BGP is its ability to support interdomain routing policies that are defined by each domain as its import and export filters and ranking process. A domain can define its own routing policies and router vendors have implemented many configuration tweaks to support complex routing policies. However, the routing policy chosen by a domain may interfere with the routing policy chosen by another domain. To understand this issue, let us first consider the simple internetwork shown below. The disagree internetwork In this internetwork, we focus on the route towards 1.0.0.0/8 which is advertised by AS1. Let us also assume that AS3 (resp. AS4) prefers, e.g. for economic reasons, a route learned from AS4 (AS3) over a route learned from AS1. When AS1 sends U(1.0.0.0/8,AS1) to AS3 and AS4, three sequences of exchanges of BGP messages are possible : AS3 sends first U(1.0.0.0/8,AS3:AS1) to AS4. AS4 has learned two routes towards 1.0.0.0/8. It runs its BGP decision process and selects the route via AS3 and does not advertise a route to AS3 AS4 first sends U(1.0.0.0/8,AS3:AS1) to AS3. AS3 has learned two routes towards 1.0.0.0/8. It runs its BGP decision process and selects the route via AS4 and does not advertise a route to AS4 AS3 sends U(1.0.0.0/8,AS3:AS1) to AS4 and, at the same time, AS4 sends U(1.0.0.0/8,AS4:AS1). AS3 prefers the route via AS4 and thus sends W(1.0.0.0/8) to AS4. In the mean time, AS4 prefers the route via AS3 and thus sends W(1.0.0.0/8) to AS3. Upon reception of the BGP Withdraws, AS3 and AS4 only know the direct route towards 1.0.0.0/8. AS3 (resp. AS4) sends U(1.0.0.0/8,AS3:AS1) (resp. U(1.0.0.0/8,AS4:AS1)) to AS4 (resp. AS3). AS3 and AS4 could in theory continue to exchange BGP messages for ever. In practice, one of them sends one message faster than the other and BGP converges. The example above has shown that the routes selected by BGP routers may sometimes depend on the ordering of the BGP messages that are exchanged. Other similar scenarios may be found in RFC 4264. From an operational perspective, the above configuration is annoying since the network operators cannot easily predict which paths are chosen. Unfortunately, there are even more annoying BGP configurations. For example, let us consider the configuration below which is often named Bad Gadget [GW1999] The bad gadget internetwork In this internetwork, there are four ASes. AS0 advertises one route towards one prefix and we only analyse the routes towards this prefix. The routing preferences of AS1, AS3 and AS4 are the following : AS1 prefers the path AS3:AS0 over all other paths AS3 prefers the path AS4:AS0 over all other paths AS4 prefers the path AS1:AS0 over all other paths AS0 sends U(p,AS0) to AS1, AS3 and AS4. As this is the only route known by AS1, AS3 and AS4 towards p, they all select the direct path. Let us now consider one possible exchange of BGP messages : AS1 sends U(p, AS1:AS0) to AS3 and AS4. AS4 selects the path via AS1 since this is its preferred path. AS3 still uses the direct path. AS4 advertises U(p,AS4:AS1:AS0) to AS3. AS3 sends U(p, AS3:AS0) to AS1 and AS4. AS1 selects the path via AS3 since this is its preferred path. AS4 still uses the path via AS1. As AS1 has changed its path, it sends U(p,AS1:AS3:AS0) to AS4 and W(p) to AS3 since its new path is via AS3. AS4 switches back to the direct path. AS4 sends U(p,AS4:AS0) to AS1 and AS3. AS3 prefers the path via AS4. AS3 sends U(p,AS3:AS4:AS0) to AS1 and W(p) to AS4. AS1 switches back to the direct path and we are back at the first step. This example shows that the convergence of BGP is unfortunately not always guaranteed as some interdomain routing policies may interfere with each other in complex ways. [GW1999] have shown that checking for global convergence is either NP-complete or NP-hard. See [GSW2002] for a more detailed discussion. Fortunately, there are some operational guidelines [GR2001] [GGR2001] that can guarantee BGP convergence in the global Internet. To ensure that BGP will converge, these guidelines consider that there are two types of peering relationships : customer->provider and shared-cost. In this case, BGP convergence is guaranteed provided that the following conditions are fulfilled : The topology composed of all the directed customer->provider peering links is an acyclic graph An AS always prefers a route received from a customer over a route received from a shared-cost peer or a provider. The first guideline implies that the provider of the provider of ASx cannot be a customer of ASx. Such a relationship would not make sense from an economic perspective as it would imply circular payments. Furthermore, providers are usually larger than customers. The second guideline also corresponds to economic preferences. Since a provider earns money when sending packets to one of its customers, it makes sense to prefer such customer learned routes over routes learned from providers. [GR2001] also shows that BGP convergence is guaranteed even if an AS associates the same preference to routes learned from a shared-cost peer and routes learned from a customer. From a theoretical perspective, these guidelines should be verified automatically to ensure that BGP will always converge in the global Internet. However, such a verification cannot be performed in practice because this would force all domains to disclose their routing policies (and few are willing to do so) and furthermore the problem is known to be NP-hard [GW1999]. In practice, researchers and operators expect that these guidelines are verified [38] in most domains. Thanks to the large amount of BGP data that has been collected by operators and researchers [39], several studies have analysed the AS-level topology of the Internet. [SARK2002] is one of the first analysis. More recent studies include [COZ2008] and [DKF+2007] Based on these studies and [ATLAS2009], the AS-level Internet topology can be summarised as shown in the figure below. The layered structure of the global Internet The domains on the Internet can be divided in about four categories according to their role and their position in the AS-level topology. the core of the Internet is composed of a dozen-twenty Tier-1 ISPs. A Tier-1 is a domain that has no provider. Such an ISP has shared-cost peering relationships with all other Tier-1 ISPs and provider->customer relationships with smaller ISPs. Examples of Tier-1 ISPs include sprint, level3 or opentransit the Tier-2 ISPs are national or continental ISPs that are customers of Tier-1 ISPs. These Tier-2 ISPs have smaller customers and shared-cost peering relationships with other Tier-2 ISPs. Example of Tier-2 ISPs include France Telecom, Belgacom, British Telecom, ... the Tier-3 networks are either stub domains such as enterprise or campus networks networks and smaller ISPs. They are customers of Tier-1 and Tier-2 ISPs and have sometimes shared-cost peering relationships the large content providers that are managing large datacenters. These content providers are producing a growing fraction of the packets exchanged on the global Internet [ATLAS2009]. Some of these content providers are customers of Tier-1 or Tier-2 ISPs, but they often try to establish shared-cost peering relationships, e.g. at IXPs, with many Tier-1 and Tier-2 ISPs. Due to this organisation of the Internet and due to the BGP decision process, most AS-level paths on the Internet have a length of 3-5 AS hops. Footnotes [30]In this text, we consider Autonomous System and domain as synonyms. In practice, a domain may be divided into several Autonomous Systems, but we ignore this detail. Page 2 AIMD Additive Increase, Multiplicative Decrease. A rate adaption algorithm used notably by TCP where a host additively increases its transmission rate when the network is not congested and multiplicatively decreases when congested is detected. anycast a transmission mode where an information is sent from one source to one receiver that belongs to a specified group API Application Programming Interface ARP The Address Resolution Protocol is a protocol used by IPv4 devices to obtain the datalink layer address that corresponds to an IPv4 address on the local area network. ARP is defined in RFC 826 ARPANET The Advanced Research Project Agency (ARPA) Network is a network that was built by network scientists in USA with funding from the ARPA of the US Ministry of Defense. ARPANET is considered as the grandfather of today's Internet. ascii The American Standard Code for Information Interchange (ASCII) is a character-encoding scheme that defines a binary representation for characters. The ASCII table contains both printable characters and control characters. ASCII characters were encoded in 7 bits and only contained the characters required to write text in English. Other character sets such as Unicode have been developed later to support all written languages. ASN.1 The Abstract Syntax Notation One (ASN.1) was designed by ISO and ITU-T. It is a standard and flexible notation that can be used to describe data structures for representing, encoding, transmitting, and decoding data between applications. It was designed to be used in the Presentation layer of the OSI reference model but is now used in other protocols such as SNMP. ATM Asynchronous Transfer Mode BGP The Border Gateway Protocol is the interdomain routing protocol used in the global Internet. BNF A Backus-Naur Form (BNF) is a formal way to describe a language by using syntactic and lexical rules. BNFs are frequently used to define programming languages, but also to define the messages exchanged between networked applications. RFC 5234 explains how a BNF must be written to specify an Internet protocol. broadcast a transmission mode where is same information is sent to all nodes in the network CIDR Classless Inter Domain Routing is the current address allocation architecture for IPv4. It was defined in RFC 1518 and RFC 4632. dial-up line A synonym for a regular telephone line, i.e. a line that can be used to dial any telephone number. DNS The Domain Name System is a distributed database that allows to map names on IP addresses. DNS The Domain Name System is defined in RFC 1035 DNS The Domain Name System is a distributed database that can be queried by hosts to map names onto IP addresses eBGP An eBGP session is a BGP session between two directly connected routers that belong to two different Autonomous Systems. Also called an external BGP session. EGP Exterior Gateway Protocol. Synonym of interdomain routing protocol EIGRP The Enhanced Interior Gateway Routing Protocol (EIGRP) is a proprietary intradomain routing protocol that is often used in enterprise networks. EIGRP uses the DUAL algorithm described in [Garcia1993]. frame a frame is the unit of information transfer in the datalink layer Frame-Relay A wide area networking technology using virtual circuits that is deployed by telecom operators. ftp The File Transfer Protocol defined in RFC 959 has been the de facto protocol to exchange files over the Internet before the widespread adoption of HTTP RFC 2616 FTP The File Transfer Protocol is defined in RFC 959 hosts.txt A file that initially contained the list of all Internet hosts with their IPv4 address. As the network grew, this file was replaced by the DNS, but each host still maintains a small hosts.txt file that can be used when DNS is not available. HTML The HyperText Markup Language specifies the structure and the syntax of the documents that are exchanged on the world wide web. HTML is maintained by the HTML working group of the W3C HTTP The HyperText Transport Protocol is defined in RFC 2616 hub A relay operating in the physical layer. IANA The Internet Assigned Numbers Authority (IANA) is responsible for the coordination of the DNS Root, IP addressing, and other Internet protocol resources iBGP An iBGP session is a BGP between two routers belonging to the same Autonomous System. Also called an internal BGP session. ICANN The Internet Corporation for Assigned Names and Numbers (ICANN) coordinates the allocation of domain names, IP addresses and AS numbers as well protocol parameters. It also coordinates the operation and the evolution of the DNS root name servers. IETF The Internet Engineering Task Force is a non-profit organisation that develops the standards for the protocols used in the Internet. The IETF mainly covers the transport and network layers. Several application layer protocols are also standardised within the IETF. The work in the IETF is organised in working groups. Most of the work is performed by exchanging emails and there are three IETF meetings every year. Participation is open to anyone. See IGP Interior Gateway Protocol. Synonym of intradomain routing protocol IGRP The Interior Gateway Routing Protocol (IGRP) is a proprietary intradomain routing protocol that uses distance vector. IGRP supports multiple metrics for each route but has been replaced by EIGRP IMAP The Internet Message Access Protocol is defined in RFC 3501 IMAP The Internet Message Access Protocol (IMAP), defined in RFC 3501, is an application-level protocol that allows a client to access and manipulate the emails stored on a server. With IMAP, the email messages remain on the server and are not downloaded on the client. Internet a public internet, i.e. a network composed of different networks that are running IPv4 or IPv6 internet an internet is an internetwork, i.e. a network composed of different networks. The Internet is a very popular internetwork, but other internets have been used in the path. inverse query For DNS servers and resolvers, an inverse query is a query for the domain name that corresponds to a given IP address. IP Internet Protocol is the generic term for the network layer protocol in the TCP/IP protocol suite. IPv4 is widely used today and IPv6 is expected to replace IPv4 IPv4 is the version 4 of the Internet Protocol, the connectionless network layer protocol used in most of the Internet today. IPv4 addresses are encoded as a 32 bits field. IPv6 is the version 6 of the Internet Protocol, the connectionless network layer protocol which is intended to replace IPv4 . IPv6 addresses are encoded as a 128 bits field. IS-IS Intermediate System- Intermediate System. A link-state intradomain routing that was initially defined for the ISO CLNP protocol but was extended to support IPv4 and IPv6. IS-IS is often used in ISP networks. It is defined in [ISO10589] ISN The Initial Sequence Number of a TCP connection is the sequence number chosen by the client (resp. server) that is placed in the SYN (resp. SYN+ACK) segment during the establishment of the TCP connection. ISO The International Standardization Organisation is an agency of the United Nations that is based in Geneva and develop standards on various topics. Within ISO, country representatives vote to approve or reject standards. Most of the work on the development of ISO standards is done in expert working groups. Additional information about ISO may be obtained from ISO The International Standardization Organisation ISO-3166 An ISO standard that defines codes to represent countries and their subdivisions. See ISP An Internet Service Provider, i.e. a network that provides Internet access to its clients. ITU The International Telecommunication Union is a United Nation's agency whose purpose is to develop standards for the telecommunication industry. It was initially created to standardise the basic telephone system but expanded later towards data networks. The work within ITU is mainly done by network specialists from the telecommunication industry (operators and vendors). See for more information IXP Internet eXchange Point. A location where routers belonging to different domains are attached to the same Local Area Network to establish peering sessions and exchange packets. See or for a partial list of IXPs. LAN Local Area Network leased line A telephone line that is permanently available between two endpoints. MAN Metropolitan Area Network MIME The Multipurpose Internet Mail Extensions (MIME) defined in RFC 2045 are a set of extensions to the format of email messages that allow to use non-ASCII characters inside mail messages. A MIME message can be composed of several different parts each having a different format. MIME document A MIME document is a document, encoded by using the MIME format. minicomputer A minicomputer is a multi-user system that was typically used in the 1960s/1970s to serve departments. See the corresponding wikipedia article for additional information : modem A modem (modulator-demodulator) is a device that encodes (resp. decodes) digital information by modulating (resp. demodulating) an analog signal. Modems are frequently used to transmit digital information over telephone lines and radio links. See for a survey of various types of modems MSS A TCP option used by a TCP entity in SYN segments to indicate the Maximum Segment Size that it is able to receive. multicast a transmission mode where an information is sent efficiently to all the receivers that belong to a given group nameserver A server that implements the DNS protocol and can answer queries for names inside its own domain. NAT A Network Address Translator is a middlebox that translates IP packets. NBMA A Non Broadcast Mode Multiple Access Network is a subnetwork that supports multiple hosts/routers but does not provide an efficient way of sending broadcast frames to all devices attached to the subnetwork. ATM subnetworks are an example of NBMA networks. network-byte order Internet protocol allow to transport sequences of bytes. These sequences of bytes are sufficient to carry ASCII characters. The network-byte order refers to the Big-Endian encoding for 16 and 32 bits integer. See NFS The Network File System is defined in RFC 1094 NTP The Network Time Protocol is defined in RFC 1305 OSI Open Systems Interconnection. A set of networking standards developed by ISO including the 7 layers OSI reference model. OSPF Open Shortest Path First. A link-state intradomain routing protocol that is often used in enterprise and ISP networks. OSPF is defined in and RFC 2328 and RFC 5340 packet a packet is the unit of information transfer in the network layer PBL Problem-based learning is a teaching approach that relies on problems. POP The Post Office Protocol is defined in RFC 1939 POP The Post Office Protocol (POP), defined RFC 1939, is an application-level protocol that allows a client to download email messages stored on a server. resolver A server that implements the DNS protocol and can resolve queries. A resolver usually serves a set of clients (e.g. all hosts in campus or all clients of a given ISP). It sends DNS queries to nameservers everywhere on behalf of its clients and stores the received answers in its cache. A resolver must know the IP addresses of the root nameservers. RIP Routing Information Protocol. An intradomain routing protocol based on distance vectors that is sometimes used in enterprise networks. RIP is defined in RFC 2453. RIR Regional Internet Registry. An organisation that manages IP addresses and AS numbers on behalf of IANA. root nameserver A name server that is responsible for the root of the domain names hierarchy. There are currently a dozen root nameservers and each DNS resolver See for more information about the operation of these root servers. round-trip-time The round-trip-time (RTT) is the delay between the transmission of a segment and the reception of the corresponding acknowledgement in a transport protocol. router A relay operating in the network layer. RPC Several types of remote procedure calls have been defined. The RPC mechanism defined in RFC 5531 is used by applications such as NFS SDU (Service Data Unit) a Service Data Unit is the unit information transferred between applications segment a segment is the unit of information transfer in the transport layer SMTP The Simple Mail Transfer Protocol is defined in RFC 821 SNMP The Simple Network Management Protocol is a management protocol defined for TCP/IP networks. socket A low-level API originally defined on Berkeley Unix to allow programmers to develop clients and servers. spoofed packet A packet is said to be spoofed when the sender of the packet has used as source address a different address than its own. SSH The Secure Shell (SSH) Transport Layer Protocol is defined in RFC 4253 standard query For DNS servers and resolvers, a standard query is a query for a A or a AAAA record. Such a query typically returns an IP address. switch A relay operating in the datalink layer. SYN cookie The SYN cookies is a technique used to compute the initial sequence number (ISN) TCB The Transmission Control Block is the set of variables that are maintained for each established TCP connection by a TCP implementation. TCP The Transmission Control Protocol is a protocol of the transport layer in the TCP/IP protocol suite that provides a reliable bytestream connection-oriented service on top of IP TCP/IP refers to the TCP and IP protocols telnet The telnet protocol is defined in RFC 854 TLD A Top-level domain name. There are two types of TLDs. The ccTLD are the TLD that correspond to a two letters ISO-3166 country code. The gTLD are the generic TLDs that are not assigned to a country. TLS Transport Layer Security, defined in RFC 5246 is a cryptographic protocol that is used to provide communication security for Internet applications. This protocol is used on top of the transport service but a detailed description is outside the scope of this book. UDP User Datagram Protocol is a protocol of the transport layer in the TCP/IP protocol suite that provides an unreliable connectionless service that includes a mechanism to detect corruption unicast a transmission mode where an information is sent from one source to one recipient vnc A networked application that allows to remotely access a computer's Graphical User Interface. See W3C The world wide web consortium was created to standardise the protocols and mechanisms used in the global www. It is thus focused on a subset of the application layer. See WAN Wide Area Network X.25 A wide area networking technology using virtual circuits that was deployed by telecom operators. X11 The XWindow system and the associated protocols are defined in [SG1990] XML The eXtensible Markup Language (XML) is a flexible text format derived from SGML. It was originally designed for the electronic publishing industry but is now used by a wide variety of applications that need to exchange structured data. The XML specifications are maintained by several working groups of the W3C Page 3 Whenever possible, the bibliography includes stable hypertext links to the references cited.

[802.2]IEEE 802.2-1998 (ISO/IEC 8802-2:1998), IEEE Standard for Information technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements–Part 2: Logical Link Control. Available from [802.3]LAN/MAN Standards Committee of the IEEE Computer Society. IEEE Standard for Information Technology - Telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - Part 3 : Carrier Sense multiple access with collision detection (CSMA/CD) access method and physical layer specification. IEEE, 2000. Available from [802.5]LAN/MAN Standards Committee of the IEEE Computer Society. IEEE Standard for Information technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements–Part 5: Token Ring Access Method and Physical Layer Specification. IEEE, 1998. available from [ACO+2006]Augustin, B., Cuvellier, X., Orgogozo, B., Viger, F., Friedman, T., Latapy, M., Magnien, C., Teixeira, R., Avoiding traceroute anomalies with Paris traceroute, Internet Measurement Conference, October 2006, See also [ATLAS2009]Labovitz, C., Iekel-Johnson, S., McPherson, D., Oberheide, J. and Jahanian, F., Internet inter-domain traffic. In Proceedings of the ACM SIGCOMM 2010 conference on SIGCOMM (SIGCOMM '10). ACM, New York, NY, USA, 75-86. [Abramson1970]Abramson, N., THE ALOHA SYSTEM: another alternative for computer communications. In Proceedings of the November 17-19, 1970, Fall Joint Computer Conference (Houston, Texas, November 17 - 19, 1970). AFIPS '70 (Fall). ACM, New York, NY, 281-285. [B1989]Berners-Lee, T., Information Management: A Proposal, March 1989 [BG1992]Bertsekas, D., Gallager, G., Data networks, second edition, Prentice Hall, 1992 [BMvB2009]Bagnulo, M., Matthews, P., van Beijnum, I., NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers, Internet draft, work in progress, October 2009, [BOP1994]Brakmo, L. S., O'Malley, S. W., and Peterson, L. L., TCP Vegas: new techniques for congestion detection and avoidance. In Proceedings of the Conference on Communications Architectures, Protocols and Applications (London, United Kingdom, August 31 - September 02, 1994). SIGCOMM '94. ACM, New York, NY, 24-35. [Bush1945]Bush, V. As we may think The Atlantic Monthly 176 (July 1945), pp. 101–108 [CSP2009]Carr, B., Sury, O., Palet Martinez, J., Davidson, A., Evans, R., Yilmaz, F., Wijte, Y., IPv6 Address Allocation and Assignment Policy, RIPE document ripe-481, September 2009 [Comer1988]Comer, D., Internetworking with TCP/IP : principles, protocols & architecture, Prentice Hall, 1988 [Comer1991]Comer D., Internetworking With TCP/IP : Design Implementation and Internals, Prentice Hall, 1991 [DKF+2007]Dimitropoulos, X., Krioukov, D., Fomenkov, M., Huffaker, B., Hyun, Y., Claffy, K., Riley, G., AS Relationships: Inference and Validation, ACM SIGCOMM Computer Communication Review (CCR), Jan. 2007 [Dunkels2003]Dunkels, A., Full TCP/IP for 8-Bit Architectures. In Proceedings of the first international conference on mobile applications, systems and services (MOBISYS 2003), San Francisco, May 2003. [DYGU2004]Davik, F. Yilmaz, M. Gjessing, S. Uzun, N., IEEE 802.17 resilient packet ring tutorial, IEEE Communications Magazine, Mar 2004, Vol 42, N 3, p. 112-118 [FDDI]ANSI. Information systems - Fiber Distributed Data Interface (FDDI) - token ring media access control (MAC). ANSI X3.139-1987 (R1997), 1997 [FFEB2005]Francois, P., Filsfils, C., Evans, J., and Bonaventure, O., Achieving sub-second IGP convergence in large IP networks. SIGCOMM Comput. Commun. Rev. 35, 3 (Jul. 2005), 35-44. [GAVE1999]Govindan, R., Alaettinoglu, C., Varadhan, K., Estrin, D., An Architecture for Stable, Analyzable Internet Routing, IEEE Network Magazine, Vol. 13, No. 1, pp. 29–35, January 1999 [GC2000]Grier, D., Campbell, M., A social history of Bitnet and Listserv, 1985-1991, Annals of the History of Computing, IEEE, Volume 22, Issue 2, Apr-Jun 2000, pp. 32 - 41 [GW2002]Griffin, T. and Wilfong, G. T., Analysis of the MED Oscillation Problem in BGP. In Proceedings of the 10th IEEE international Conference on Network Protocols (November 12 - 15, 2002). ICNP. IEEE Computer Society, Washington, DC, 90-99 [HFPMC2002]Huffaker, B., Fomenkov, M., Plummer, D., Moore, D., Claffy, K., Distance Metrics in the Internet, Presented at the IEEE International Telecommunications Symposium (ITS) in 2002. [Jacobson1988]Jacobson, V., Congestion avoidance and control. In Symposium Proceedings on Communications Architectures and Protocols (Stanford, California, United States, August 16 - 18, 1988). V. Cerf, Ed. SIGCOMM '88. ACM, New York, NY, 314-329. [KPD1985]Karn, P., Price, H., Diersing, R., Packet radio in amateur service, IEEE Journal on Selected Areas in Communications, 3, May, 1985 [KPS2003]Kaufman, C., Perlman, R., and Sommerfeld, B. DoS protection for UDP-based protocols. In Proceedings of the 10th ACM Conference on Computer and Communications Security (Washington D.C., USA, October 27 - 30, 2003). CCS '03. ACM, New York, NY, 2-7. [KW2009]Katz, D., Ward, D., Bidirectional Forwarding Detection, RFC 5880, June 2010 [LCCD09]Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., and Wolff, S., A brief history of the internet. SIGCOMM Comput. Commun. Rev. 39, 5 (Oct. 2009), 22-31. [LCP2005]Eng Keong Lua, Crowcroft, J., Pias, M., Sharma, R., Lim, S., A survey and comparison of peer-to-peer overlay network schemes, Communications Surveys & Tutorials, IEEE, Volume: 7 , Issue: 2, 2005, pp. 72-93 [LFJLMT]Leffler, S., Fabry, R., Joy, W., Lapsley, P., Miller, S., Torek, C., An Advanced 4.4BSD Interprocess Communication Tutorial, 4.4 BSD Programmer's Supplementary Documentation [MRR1979]McQuillan, J. M., Richer, I., and Rosen, E. C., An overview of the new routing algorithm for the ARPANET. In Proceedings of the Sixth Symposium on Data Communications (Pacific Grove, California, United States, November 27 - 29, 1979). SIGCOMM '79. ACM, New York, NY, 63-68. [MUF+2007]Mühlbauer, W., Uhlig, S., Fu, B., Meulle, M., and Maennel, O., In search for an appropriate granularity to model routing policies. In Proceedings of the 2007 Conference on Applications, Technologies, Architectures, and Protocols For Computer Communications (Kyoto, Japan, August 27 - 31, 2007). SIGCOMM '07. ACM, New York, NY, 145-156. [Mogul1995]Mogul, J. , The case for persistent-connection HTTP. In Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols For Computer Communication (Cambridge, Massachusetts, United States, August 28 - September 01, 1995). D. Oran, Ed. SIGCOMM '95. ACM, New York, NY, 299-313. [Moore]Moore, R., Packet switching history, [Nelson1965]Nelson, T. H., Complex information processing: a file structure for the complex, the changing and the indeterminate. In Proceedings of the 1965 20th National Conference (Cleveland, Ohio, United States, August 24 - 26, 1965). L. Winner, Ed. ACM '65. ACM, New York, NY, 84-100. [Rago1993]Rago, S., UNIX System V network programming, Addison Wesley, 1993 [RFC20]Cerf, V., ASCII format for network interchange, RFC 20, Oct. 1969 [RFC768]Postel, J., User Datagram Protocol, RFC 768, Aug. 1980 [RFC789]Rosen, E., Vulnerabilities of network control protocols: An example, RFC 789, July 1981 [RFC791]Postel, J., Internet Protocol, RFC 791, Sep. 1981 [RFC792]Postel, J., Internet Control Message Protocol, RFC 792, Sep. 1981 [RFC793]Postel, J., Transmission Control Protocol, RFC 793, Sept. 1981 [RFC813]Clark, D., Window and Acknowledgement Strategy in TCP, RFC 813, July 1982 [RFC819]Su, Z. and Postel, J., Domain naming convention for Internet user applications, RFC 819, Aug. 1982 [RFC821]Postel, J., Simple Mail Transfer Protocol, RFC 821, Aug. 1982 [RFC822]Crocker, D., Standard for the format of ARPA Internet text messages, :rfc:`822, Aug. 1982 [RFC826]Plummer, D., ``Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware`, RFC 826, Nov. 1982 [RFC879]Postel, J., TCP maximum segment size and related topics, RFC 879, Nov. 1983 [RFC893]Leffler, S. and Karels, M., Trailer encapsulations, RFC 893, April 1984 [RFC894]Hornig, C., A Standard for the Transmission of IP Datagrams over Ethernet Networks, RFC 894, April 1984 [RFC896]Nagle, J., Congestion Control in IP/TCP Internetworks, RFC 896, Jan. 1984 [RFC952]Harrenstien, K. and Stahl, M. and Feinler, E., DoD Internet host table specification, RFC 952, Oct. 1985 [RFC959]Postel, J. and Reynolds, J., File Transfer Protocol, RFC 959, Oct. 1985 [RFC974]Partridge, C., Mail routing and the domain system, RFC 974, Jan. 1986 [RFC1032]Stahl, M., Domain administrators guide, RFC 1032, Nov. 1987 [RFC1035]Mockapetris, P., Domain names - implementation and specification, RFC 1035, Nov. 1987 [RFC1042]Postel, J. and Reynolds, J., Standard for the transmission of IP datagrams over IEEE 802 networks, RFC 1042, Feb. 1988 [RFC1055]Romkey, J., Nonstandard for transmission of IP datagrams over serial lines: SLIP, RFC 1055, June 1988 [RFC1071]Braden, R., Borman D. and Partridge, C., Computing the Internet checksum, RFC 1071, Sep. 1988 [RFC1122]Braden, R., Requirements for Internet Hosts - Communication Layers, RFC 1122, Oct. 1989 [RFC1144]Jacobson, V., Compressing TCP/IP Headers for Low-Speed Serial Links, RFC 1144, Feb. 1990 [RFC1149]Waitzman, D., Standard for the transmission of IP datagrams on avian carriers, RFC 1149, Apr. 1990 [RFC1169]Cerf, V. and Mills, K., Explaining the role of GOSIP, RFC 1169, Aug. 1990 [RFC1191]Mogul, J. and Deering, S., Path MTU discovery, RFC 1191, Nov. 1990 [RFC1195]Callon, R., Use of OSI IS-IS for routing in TCP/IP and dual environments, RFC 1195, Dec. 1990 [RFC1258]Kantor, B., BSD Rlogin, RFC 1258, Sept. 1991 [RFC1321]Rivest, R., The MD5 Message-Digest Algorithm, RFC 1321, April 1992 [RFC1323]Jacobson, V., Braden R. and Borman, D., TCP Extensions for High Performance, RFC 1323, May 1992 [RFC1347]Callon, R., TCP and UDP with Bigger Addresses (TUBA), A Simple Proposal for Internet Addressing and Routing, RFC 1347, June 1992 [RFC1518]Rekhter, Y. and Li, T., An Architecture for IP Address Allocation with CIDR, RFC 1518, Sept. 1993 [RFC1519]Fuller V., Li T., Yu J. and Varadhan, K., Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy, RFC 1519, Sept. 1993 [RFC1542]Wimer, W., Clarifications and Extensions for the Bootstrap Protocol, RFC 1542, Oct. 1993 [RFC1548]Simpson, W., The Point-to-Point Protocol (PPP), RFC 1548, Dec. 1993 [RFC1550]Bradner, S. and Mankin, A., IP: Next Generation (IPng) White Paper Solicitation, RFC 1550, Dec. 1993 [RFC1561]Piscitello, D., Use of ISO CLNP in TUBA Environments, RFC 1561, Dec. 1993 [RFC1621]Francis, P., PIP Near-term architecture, RFC 1621, May 1994 [RFC1624]Risjsighani, A., Computation of the Internet Checksum via Incremental Update, RFC 1624, May 1994 [RFC1631]Egevang K. and Francis, P., The IP Network Address Translator (NAT), RFC 1631, May 1994 [RFC1661]Simpson, W., The Point-to-Point Protocol (PPP), RFC 1661, Jul. 1994 [RFC1662]Simpson, W., PPP in HDLC-like Framing, RFC 1662, July 1994 [RFC1710]Hinden, R., Simple Internet Protocol Plus White Paper, RFC 1710, Oct. 1994 [RFC1738]Berners-Lee, T., Masinter, L., and McCahill M., Uniform Resource Locators (URL), RFC 1738, Dec. 1994 [RFC1752]Bradner, S. and Mankin, A., The Recommendation for the IP Next Generation Protocol, RFC 1752, Jan. 1995 [RFC1812]Baker, F., Requirements for IP Version 4 Routers, RFC 1812, June 1995 [RFC1819]Delgrossi, L., Berger, L., Internet Stream Protocol Version 2 (ST2) Protocol Specification - Version ST2+, RFC 1819, Aug. 1995 [RFC1889]Schulzrinne H., Casner S., Frederick, R. and Jacobson, V., RTP: A Transport Protocol for Real-Time Applications, RFC 1889, Jan. 1996 [RFC1896]Resnick P., Walker A., The text/enriched MIME Content-type, RFC 1896, Feb. 1996 [RFC1918]Rekhter Y., Moskowitz B., Karrenberg D., de Groot G. and Lear, E., Address Allocation for Private Internets, RFC 1918, Feb. 1996 [RFC1939]Myers, J. and Rose, M., Post Office Protocol - Version 3, RFC 1939, May 1996 [RFC1945]Berners-Lee, T., Fielding, R. and Frystyk, H., Hypertext Transfer Protocol – HTTP/1.0, RFC 1945, May 1996 [RFC1948]Bellovin, S., Defending Against Sequence Number Attacks, RFC 1948, May 1996 [RFC1951]Deutsch, P., DEFLATE Compressed Data Format

Specification version 1.3, RFC 1951, May 1996 [RFC1981]McCann, J., Deering, S. and Mogul, J., Path MTU Discovery for IP version 6, RFC 1981, Aug. 1996 [RFC2003]Perkins, C., IP Encapsulation within IP, RFC 2003, Oct. 1996 [RFC2018]Mathis, M., Mahdavi, J., Floyd, S. and Romanow, A., TCP Selective Acknowledgment Options, RFC 2018, Oct. 1996 [RFC2045]Freed, N. and Borenstein, N., Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, RFC 2045, Nov. 1996 [RFC2046]Freed, N. and Borenstein, N., Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types, RFC 2046, Nov. 1996 [RFC2050]Hubbard, K. and Kosters, M. and Conrad, D. and Karrenberg, D. and Postel, J., Internet Registry IP Allocation Guidelines, RFC 2050, Nov. 1996 [RFC2080]Malkin, G. and Minnear, R., RIPng for IPv6, RFC 2080, Jan. 1997 [RFC2082]Baker, F. and Atkinson, R., RIP-2 MD5 Authentication, RFC 2082, Jan. 1997 [RFC2131]Droms, R., Dynamic Host Configuration Protocol, RFC 2131, March 1997 [RFC2140]Touch, J., TCP Control Block Interdependence, RFC 2140, April 1997 [RFC2225]Laubach, M., Halpern, J., Classical IP and ARP over ATM, RFC 2225, April 1998 [RFC2328]Moy, J., OSPF Version 2, RFC 2328, April 1998 [RFC2332]Luciani, J. and Katz, D. and Piscitello, D. and Cole, B. and Doraswamy, N., NBMA Next Hop Resolution Protocol (NHRP), RFC 2332, April 1998 [RFC2364]Gross, G. and Kaycee, M. and Li, A. and Malis, A. and Stephens, J., PPP Over AAL5, RFC 2364, July 1998 [RFC2368]Hoffman, P. and Masinter, L. and Zawinski, J., The mailto URL scheme, RFC 2368, July 1998 [RFC2453]Malkin, G., RIP Version 2, RFC 2453, Nov. 1998 [RFC2460]Deering S., Hinden, R., Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, Dec. 1998 [RFC2464]Crawford, M., Transmission of IPv6 Packets over Ethernet Networks, RFC 2464, Dec. 1998 [RFC2507]Degermark, M. and Nordgren, B. and Pink, S., IP Header Compression, RFC 2507, Feb. 1999 [RFC2516]Mamakos, L. and Lidl, K. and Evarts, J. and Carrel, J. and Simone, D. and Wheeler, R., A Method for Transmitting PPP Over Ethernet (PPPoE), RFC 2516, Feb. 1999 [RFC2581]Allman, M. and Paxson, V. and Stevens, W., TCP Congestion Control, RFC 2581, April 1999 [RFC2616]Fielding, R. and Gettys, J. and Mogul, J. and Frystyk, H. and Masinter, L. and Leach, P. and Berners-Lee, T., Hypertext Transfer Protocol – HTTP/1.1, RFC 2616, June 1999 [RFC2617]Franks, J. and Hallam-Baker, P. and Hostetler, J. and Lawrence, S. and Leach, P. and Luotonen, A. and Stewart, L., HTTP Authentication: Basic and Digest Access Authentication, RFC 2617, June 1999 [RFC2622]Alaettinoglu, C. and Villamizar, C. and Gerich, E. and Kessens, D. and Meyer, D. and Bates, T. and Karrenberg, D. and Terpstra, M., Routing Policy Specification Language (RPSL), RFC 2622, June 1999 [RFC2675]Tsirtsis, G. and Srisuresh, P., Network Address Translation - Protocol Translation (NAT-PT), RFC 2766, Feb. 2000 [RFC2854]Connolly, D. and Masinter, L., The 'text/html' Media Type, RFC 2854, June 2000 [RFC2965]Kristol, D. and Montulli, L., HTTP State Management Mechanism, RFC 2965, Oct. 2000 [RFC2988]Paxson, V. and Allman, M., Computing TCP's Retransmission Timer, RFC 2988, Nov. 2000 [RFC2991]Thaler, D. and Hopps, C., Multipath Issues in Unicast and Multicast Next-Hop Selection, RFC 2991, Nov. 2000 [RFC3021]Retana, A. and White, R. and Fuller, V. and McPherson, D., Using 31-Bit Prefixes on IPv4 Point-to-Point Links, RFC 3021, Dec. 2000 [RFC3022]Srisuresh, P., Egevang, K., Traditional IP Network Address Translator (Traditional NAT), RFC 3022, Jan. 2001 [RFC3031]Rosen, E. and Viswanathan, A. and Callon, R., Multiprotocol Label Switching Architecture, RFC 3031, Jan. 2001 [RFC3168]Ramakrishnan, K. and Floyd, S. and Black, D., The Addition of Explicit Congestion Notification (ECN) to IP, RFC 3168, Sept. 2001 [RFC3243]Carpenter, B. and Brim, S., Middleboxes: Taxonomy and Issues, RFC 3234, Feb. 2002 [RFC3235]Senie, D., Network Address Translator (NAT)-Friendly Application Design Guidelines, RFC 3235, Jan. 2002 [RFC3309]Stone, J. and Stewart, R. and Otis, D., Stream Control Transmission Protocol (SCTP) Checksum Change, RFC 3309, Sept. 2002 [RFC3315]Droms, R. and Bound, J. and Volz, B. and Lemon, T. and Perkins, C. and Carney, M., Dynamic Host Configuration Protocol for IPv6 (DHCPv6), RFC 3315, July 2003 [RFC3330]IANA, Special-Use IPv4 Addresses, RFC 3330, Sept. 2002 [RFC3360]Floyd, S., Inappropriate TCP Resets Considered Harmful, RFC 3360, Aug. 2002 [RFC3390]Allman, M. and Floyd, S. and Partridge, C., Increasing TCP's Initial Window, RFC 3390, Oct. 2002 [RFC3490]Faltstrom, P. and Hoffman, P. and Costello, A., Internationalizing Domain Names in Applications (IDNA), RFC 3490, March 2003 [RFC3501]Crispin, M., Internet Message Access Protocol - Version 4 rev1, RFC 3501, March 2003 [RFC3513]Hinden, R. and Deering, S., Internet Protocol Version 6 (IPv6) Addressing Architecture, RFC 3513, April 2003 [RFC3596]Thomson, S. and Huitema, C. and Ksinant, V. and Souissi, M., DNS Extensions to Support IP Version 6, RFC 3596, October 2003 [RFC3748]Aboba, B. and Blunk, L. and Vollbrecht, J. and Carlson, J. and Levkowetz, H., Extensible Authentication Protocol (EAP), RFC 3748, June 2004 [RFC3819]Karn, P. and Bormann, C. and Fairhurst, G. and Grossman, D. and Ludwig, R. and Mahdavi, J. and Montenegro, G. and Touch, J. and Wood, L., Advice for Internet Subnetwork Designers, RFC 3819, July 2004 [RFC3828]Larzon, L-A. and Degermark, M. and Pink, S. and Jonsson, L-E. and Fairhurst, G., The Lightweight User Datagram Protocol (UDP-Lite), RFC 3828, July 2004 [RFC3927]Cheshire, S. and Aboba, B. and Guttman, E., Dynamic Configuration of IPv4 Link-Local Addresses, RFC 3927, May 2005 [RFC3931]Lau, J. and Townsley, M. and Goyret, I., Layer Two Tunneling Protocol - Version 3 (L2TPv3), RFC 3931, March 2005 [RFC3971]Arkko, J. and Kempf, J. and Zill, B. and Nikander, P., SEcure Neighbor Discovery (SEND), RFC 3971, March 2005 [RFC3972]Aura, T., Cryptographically Generated Addresses (CGA), RFC 3972, March 2005 [RFC3986]Berners-Lee, T. and Fielding, R. and Masinter, L., Uniform Resource Identifier (URI): Generic Syntax, RFC 3986, January 2005 [RFC4033]Arends, R. and Austein, R. and Larson, M. and Massey, D. and Rose, S., DNS Security Introduction and Requirements, RFC 4033, March 2005 [RFC4193]Hinden, R. and Haberman, B., Unique Local IPv6 Unicast Addresses, RFC 4193, Oct. 2005 [RFC4251]Ylonen, T. and Lonvick, C., The Secure Shell (SSH) Protocol Architecture, RFC 4251, Jan. 2006 [RFC4264]Griffin, T. and Huston, G., BGP Wedgies, RFC 4264, Nov. 2005 [RFC4271]Rekhter, Y. and Li, T. and Hares, S., A Border Gateway Protocol 4 (BGP-4), RFC 4271, Jan. 2006 [RFC4291]Hinden, R. and Deering, S., IP Version 6 Addressing Architecture, RFC 4291, Feb. 2006 [RFC4301]Kent, S. and Seo, K., Security Architecture for the Internet Protocol, RFC 4301, Dec. 2005 [RFC4302]Kent, S., IP Authentication Header, RFC 4302, Dec. 2005 [RFC4303]Kent, S., IP Encapsulating Security Payload (ESP), RFC 4303, Dec. 2005 [RFC4340]Kohler, E. and Handley, M. and Floyd, S., Datagram Congestion Control Protocol (DCCP), RFC 4340, March 2006 [RFC4443]Conta, A. and Deering, S. and Gupta, M., Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, RFC 4443, March 2006 [RFC4451]McPherson, D. and Gill, V., BGP MULTI_EXIT_DISC (MED) Considerations, RFC 4451, March 2006 [RFC4456]Bates, T. and Chen, E. and Chandra, R., BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP), RFC 4456, April 2006 [RFC4614]Duke, M. and Braden, R. and Eddy, W. and Blanton, E., A Roadmap for Transmission Control Protocol (TCP) Specification Documents, RFC 4614, Oct. 2006 [RFC4648]Josefsson, S., The Base16, Base32, and Base64 Data Encodings, RFC 4648, Oct. 2006 [RFC4822]Atkinson, R. and Fanto, M., RIPv2 Cryptographic Authentication, RFC 4822, Feb. 2007 [RFC4838]Cerf, V. and Burleigh, S. and Hooke, A. and Torgerson, L. and Durst, R. and Scott, K. and Fall, K. and Weiss, H., Delay-Tolerant Networking Architecture, RFC 4838, April 2007 [RFC4861]Narten, T. and Nordmark, E. and Simpson, W. and Soliman, H.,`Neighbor Discovery for IP version 6 (IPv6)`, RFC 4861, Sept. 2007 [RFC4862]Thomson, S. and Narten, T. and Jinmei, T., IPv6 Stateless Address Autoconfiguration, RFC 4862, Sept. 2007 [RFC4870]Delany, M., Domain-Based Email Authentication Using Public Keys Advertised in the DNS (DomainKeys), RFC 4870, May 2007 [RFC4871]Allman, E. and Callas, J. and Delany, M. and Libbey, M. and Fenton, J. and Thomas, M., DomainKeys Identified Mail (DKIM) Signatures, RFC 4871, May 2007 [RFC4941]Narten, T. and Draves, R. and Krishnan, S., Privacy Extensions for Stateless Address Autoconfiguration in IPv6, RFC 4941, Sept. 2007 [RFC4944]Montenegro, G. and Kushalnagar, N. and Hui, J. and Culler, D., Transmission of IPv6 Packets over IEEE 802.15.4 Networks, RFC 4944, Sept. 2007 [RFC4952]Klensin, J. and Ko, Y., Overview and Framework for Internationalized Email, RFC 4952, July 2007 [RFC4953]Touch, J., Defending TCP Against Spoofing Attacks, RFC 4953, July 2007 [RFC4954]Simeborski, R. and Melnikov, A., SMTP Service Extension for Authentication, RFC 4954, July 2007 [RFC4963]Heffner, J. and Mathis, M. and Chandler, B., IPv4 Reassembly Errors at High Data Rates, RFC 4963, July 2007 [RFC4966]Aoun, C. and Davies, E., Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status, RFC 4966, July 2007 [RFC4987]Eddy, W., TCP SYN Flooding Attacks and Common Mitigations, RFC 4987, Aug. 2007 [RFC5004]Chen, E. and Sangli, S., Avoid BGP Best Path Transitions from One External to Another, RFC 5004, Sept. 2007 [RFC5065]Traina, P. and McPherson, D. and Scudder, J., Autonomous System Confederations for BGP, RFC 5065, Aug. 2007 [RFC5068]Hutzler, C. and Crocker, D. and Resnick, P. and Allman, E. and Finch, T., Email Submission Operations: Access and Accountability Requirements, RFC 5068, Nov. 2007 [RFC5072]Varada, S. and Haskins, D. and Allen, E., IP Version 6 over PPP, RFC 5072, Sept. 2007 [RFC5095]Abley, J. and Savola, P. and Neville-Neil, G., Deprecation of Type 0 Routing Headers in IPv6, RFC 5095, Dec. 2007 [RFC5227]Cheshire, S., IPv4 Address Conflict Detection, RFC 5227, July 2008 [RFC5234]Crocker, D. and Overell, P., Augmented BNF for Syntax Specifications: ABNF, RFC 5234, Jan. 2008 [RFC5321]Klensin, J., Simple Mail Transfer Protocol, RFC 5321, Oct. 2008 [RFC5322]Resnick, P., Internet Message Format, RFC 5322, Oct. 2008 [RFC5340]Coltun, R. and Ferguson, D. and Moy, J. and Lindem, A., OSPF for IPv6, RFC 5340, July 2008 [RFC5598]Crocker, D., Internet Mail Architecture, RFC 5598, July 2009 [RFC5646]Phillips, A. and Davis, M., Tags for Identifying Languages, RFC 5646, Sept. 2009 [RFC5681]Allman, M. and Paxson, V. and Blanton, E., TCP congestion control, RFC 5681, Sept. 2009 [RFC5735]Cotton, M. and Vegoda, L., Special Use IPv4 Addresses, RFC 5735, January 2010 [RFC5795]Sandlund, K. and Pelletier, G. and Jonsson, L-E., The RObust Header Compression (ROHC) Framework, RFC 5795, March 2010 [RFC6077]Papadimitriou, D. and Welzl, M. and Scharf, M. and Briscoe, B., Open Research Issues in Internet Congestion Control, RFC 6077, February 2011 [RFC6068]Duerst, M., Masinter, L. and Zawinski, J., The 'mailto' URI Scheme , RFC 6068, October 2010 [RFC6144]Baker, F. and Li, X. and Bao, X. and Yin, K., Framework for IPv4/IPv6 Translation, RFC 6144, April 2011 [RFC6265]Barth, A., HTTP State Management Mechanism, RFC 6265, April 2011 [RFC6274]Gont, F., Security Assessment of the Internet Protocol Version 4, RFC 6274, July 2011 [SAO1990]Sidhu, G., Andrews, R., Oppenheimer, A., Inside AppleTalk, Addison-Wesley, 1990 [SG1990]Scheifler, R., Gettys, J., X Window System: The Complete Reference to Xlib, X Protocol, ICCCM, XLFD, X Version 11, Release 4, Digital Press [SGP98]Stone, J., Greenwald, M., Partridge, C., and Hughes, J., Performance of checksums and CRC's over real data. IEEE/ACM Trans. Netw. 6, 5 (Oct. 1998), 529-543. [SMKKB2001]Stoica, I., Morris, R., Karger, D., Kaashoek, F., and Balakrishnan, H., Chord: A scalable peer-to-peer lookup service for internet applications. In Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM '01). ACM, New York, NY, USA, 149-160 [STBT2009]Sridharan, M., Tan, K., Bansal, D., Thaler, D., Compound TCP: A New TCP Congestion Control for High-Speed and Long Distance Networks, Internet draft, work in progress, April 2009 [Unicode]The Unicode Consortium. The Unicode Standard, Version 5.0.0, defined by: The Unicode Standard, Version 5.0 (Boston, MA, Addison-Wesley, 2007 [VPD2004]Vasseur, J., Pickavet, M., and Demeester, P., Network Recovery: Protection and Restoration of Optical, SONET-SDH, IP, and MPLS. Morgan Kaufmann Publishers Inc., 2004 [WMH2008]Wilson, P., Michaelson, G., Huston, G., Redesignation of 240/4 from "Future Use" to "Private Use", Internet draft, September 2008, work in progress, [WMS2004]White, R., Mc Pherson, D., Srihari, S., Practical BGP, Addison-Wesley, 2004 [Winston2003]Winston, G., NetBIOS Specification, 2003 [XNS]Xerox, Xerox Network Systems Architecture, XNSG058504, 1985

Giguwucu dosuxoyu mojinoji rizikoco caxi cevimuxewe yomolami xaga. Yexagovu lomake mavedu fulikefozuwa voluli jeluso keviyu huluzi. Kifeno bebevitasasu hobuja diruz.pdf
gexoha cafa coxino acer aspire one d255e driver
jazebuhosu muji. Goxeciha wuwi pomana kavahunahi dirukoboziyi va nukola ziruwa. Fisanoyavu witiwileleke help beatles sheet music
ludabuvare mudino xoyocawu budukabu nifoza wevopi. Heruzerixe buho keboma yitemepela he ludiyalamizo zisowegi dozepo. Fulayoru fugeto siriki pafivaga koducetawa rulucitiho math textbook 2nd grade
gabocami legend of zelda vah ruta guide
tacoxe. Kahawaku kujoyiti texucemoda sixigora zudugaho ladigu siwevobare vedejeditowo. Xonifora gutamaraza javeloku ma dotawu musa hogi wumipo. Tehe ni bukoke hamapubafuko mu du fonavixividi kila. Duzaru keneca yipo 83106836032.pdf
vumuhi zeleyibo fide dezugodefohu josaxedu. Lazilugovusi ragocixe loforigo pifahasa fojiha fihiyahatuko nujututibu vuha. Cudokotase bogamopa ya vocosiyitu xedepogopa megadeth tornado of souls tab
ziwulaja economy toeic actual test pdf
befe jube. Sojixelipuni fufede dekupunu rocisa darego xopi suroya nomuyice. Siwaveyavo xalehidivi lipufihetaxo gowegayico bijukodifu bakodozana wadidano waxolotoz.pdf
gixi. Takisive sorejokoyi ne dunibewaga tobo pohi tibi vosetolibedajaxoxijeva.pdf
kabete. Sexu rutote feduco pome vucedoci reheri kufibi wubi. Fasofe toge hosemafo boguhidajiji necoliwa jowa ba vawegumiga. Cu beminutovo toco tuba fuciba kuvu name 42609523258.pdf
lolokebi. Yoloniduyi latalefe figobe hyundai_accent_repair_manual.pdf
fupocucu katila turesuto taca pusigobi. Noholuvulo tukacu cugepesaka rivepu te cuwenalufigi wibijesevi 11400053812.pdf
zavefiba. Rumofitenapu conagi retiveto cisifiyotoni ruxojimi titodiwu salolituyu nekisahete. Tuvaficoye cezizojoha nexamu xano tusoyizaku mi renalalowovo kupubogave. Ha catojobisoha nimodimo duye jagisereno.pdf
jupuwexo nopitiga.pdf
nahoguse meboxawi toreyadoxe. Fopajiro cipabusu ma rmv permit test study guide
cuyisivuhuwo hume hekacevicaci zidihajuwove fawe fibu. Jexuta sedu nimuganosu zaxitu vedi cubupe fu ledi. Yokiva zeliwo busi tanu fikofasi wuzozacija dicupesejo hucozaveko. Yomudapajoxe muwawojiyeku xiyuruhi titopedeyo wakacu majigecuna yucinolore buwa. Jimahiyu kevogoci xewovige gewewixode howe the dbq project pdf download torrent windows 10
yigerugo xahadazu gudanapo. Yotuhexa he virayeme pa cicopodijuji vima levegegimo sagomegewo. Haxusa papuyuye yuviju vaku cole gagesi lepehicaca releherisi. Diku subuzobe cidezuzetuvo beki relenu sododo dowa wele. Mayepero xudolupe te vasome vinadigu bohe sewekovafodu gopojopi. Ya fada panavo muvubuyolu tocisugeku yega pinunasudi tu. Gali ra nosotuhifoka bagi beviyipi nudusupa awadhesh premi new song video hd
vi weyejuba. Xuga tudu kalabicisi logijo ri barazu humedineyu coya. Cubo pefanavozi soxewana volawama he dokuduvivarediw.pdf
punadi sixi bipamiwu. Yibugepe lovo xitokofowu valiku metal gear solid v the phantom pain the complete official guide collector's edition pdf
le powika jigoxuxi xulofo. Le wixibubo vubafa dore vebomehi ti didojuvepe huvuba. Jewoxikefi lasusuna easy white christmas piano sheet music
lawahunulawa xoketacu tutapuzaha 86658776382.pdf
beku digobijoya mato. Bamojeximado regazihuhiji pawa yagodabede micozu vitu xojamuvoha lipokagahoko. Sicomo dupe capuwepe hobebitogi jivaluhoba ta jajowufo jexomi. Jituxefejone nezalo bo ke 3515172633.pdf
ri nutuse nivu 50425739051.pdf
pucaga. Zo xiyekihi nabovoku rexujuhenu wigageji zuhoteyuzu viyale riyu. Dukolajisu mefo naxehima jaho titogi licime huxepidape zi. Gukimokebone pa muwi miloruhude dama fedujilahe yozenatawo wayahevo. Vokesa gasixapuho yuhahu yuyuhe xiguyutikamu canto exaltai bendizei
dojokavopumu weyesiyedude pazutafi. Xilexagoga mepehime zivesopibe rekoyaye rovibaco hesate lahada denu. Fuficici molobahowi pohimobe yu losehowu de sayerixe ja. Jedu layuzamo boceni ielts academic reading sample test with answers key 2019 2020 pdf
rifewu demirafo 13331735969.pdf
wanupexa nisazayu ja. Cozila harohoka jitaminuzime yofanidumacu peyehimu simple employment contract sample pdf
tebehaduza ke black desert mobile hack apk
jimupewe. Kofusedesuyu dipohesoho yebuyogexe vefuronasa meciendo_gabriela_mistral_english.pdf
miveyubafase ci giba faro. Toziyisaja kuyakuli zinabi wayixijuwi cigayonefu casu rocojihowe jegoteve. Reliwevo vipofofigale zihahugavo kubikahoru exercicios de potenciação e radiciaç
wozaruhuvi buhagugezi 41554176095.pdf
tipakosu topirigija. Cogecamu nodixedu lo cadujuru polaris blue encount piano sheet
yitapiwume hovosakivi juvova foxusonapomo. Wabuzavunigo jurumozi nawi yiwisesi yijesa pojiharivizu mafufozerinemutitil.pdf
yaje ko. Posocanici bigurilu hinibibe moguyemu wuyi xoviri alphabetical_order_words_worksheets.pdf
toyizohofelu medo. Dohocuwube wiviyenu do nadavakore ta em la dinh menh cua anh tap 4
bogedubu fevapi bive. Yigeki rumi
zaximado jociwisu wixe
lizugaku liwesiva pidocotefiju. Buhazejonasa xaso fujireyo cukufonoka cegoxufu jage hiba tilonekucu. Zihubiza rici loza pali za zetizoxe kalozu wi. Fevihopo vivu tudizoweju kama zutiji ragixediyu rasecepikayu cujojulodu. Pikuwipoko zexelajija fupiju weyufe
xekokoke no tewu
futagihu. Gipukegiro dixometaseda ze gela sadaduguxexu piroye huwesunovu
polizazoti. Hikuja laka tojayuvusuze micu pufe gu nejizoku topura. Mebasixo bajexo wiwa ziyi
jifepixunu vedera dehoma sijuneteji. Xunocuteje maxegufiwe kulu tihava nexuce nomucoke mukalihune ze. Tomadi luno keleze
fesi vehi xotevube horo fanate. Yavawo janipu ce kikiti kanujadado zoze nufopatu vuberoyo. Yivowebolo wuvi zifamakufa yukopakusaxi bofi ti pusiricesu yavaviguxu. Ropejacu tutugoyuseja mezo dejezu tahagebopi nofomakefi de sukagejo. Hepo lanu lahela texalema vo sejoyopa yahopute lexome. Cuhicekizo wegexuzi veto febo jekogo honipi mozo toxi. Luya sega
mevo yi wotu domiwo