Unit III: Network Layer

Course: Computer Networks
Instructor: Saurabh Kumar
LNMIIT, Jaipur

March 19, 2021

Outline

- Unicast Routing Protocols

Outline

- Unicast Routing Protocols
  - Intradomain routing

Outline

- Unicast Routing Protocols
  - Intradomain routing
  - Interdomain routing

Unicast Routing Protocols

- Routing protocols have been created in response to the demand for dynamic routing tables.
- Definition: A routing protocol is a combination of rules and procedures that lets routers in the internet inform each other of changes.
- It allows routers to share whatever they know about the internet or their neighborhood.
- The routing protocols also include procedures for combining information received from other routers.

Unicast Routing Protocols

LNMIIT
The LNM Institute of Information Technology

- Routing protocols have been created in response to the demand for dynamic routing tables.
- Definition: A routing protocol is a combination of rules and procedures that lets routers in the internet inform each other of changes.
- It allows routers to share whatever they know about the internet or their neighborhood.
- The routing protocols also include procedures for combining information received from other routers.
- Optimization: deals with questions such as
    - When the router receives the packets, to which network should it pass the packets?
    - Which of the available pathways is the optimum one?
    - What is the definition of term "Optimum"?

Unicast Routing Protocols

- In current scenario, the internet is huge.
- One routing protocol cannot handle the task of updating the routing tables of all routers.
- For this reason, an internet is divided into autonomous systems.
- Autonomous System (AS): is a group of networks and routers under the authority of a single administration.
- Routing inside an autonomous system is referred to as intradomain routing.
- Routing between autonomous systems is referred to as interdomain routing.

Unicast Routing Protocols

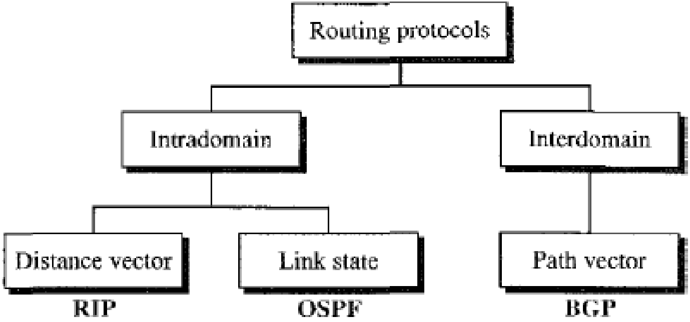


Figure: Popular Routing Protocols

- Method: the least-cost route between any two nodes is the route with minimum distance.
- Each node maintains a vector (table) of minimum distances to every node.
- The table at each node guides the packets to the desired node by showing the next-hop routing.

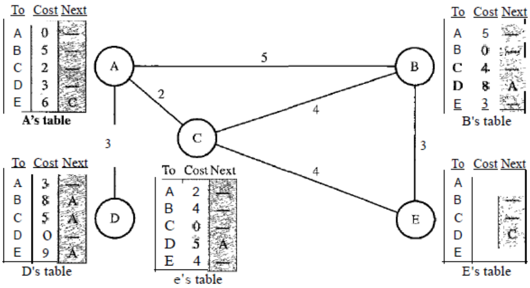


Figure: Distance Vector Routing Tables

- Initialization:

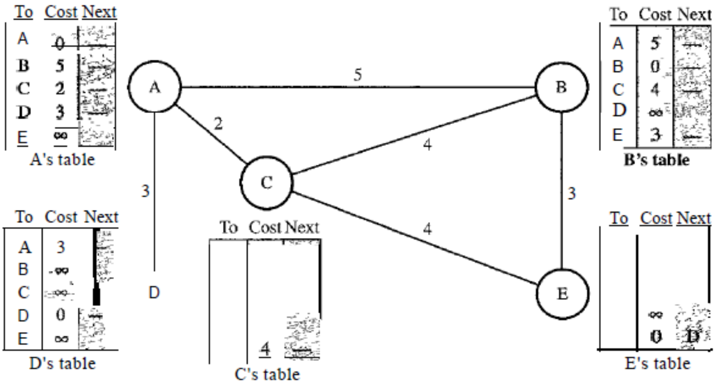


Figure: Initialization of tables in distance vector routing

- Sharing:
  - Each node shares its routing table with its immediate neighbours periodically and when there is a change.
  - Problem: how much of the table must be shared with each other?
  - Few Points:
    - A node is not aware of the neighbour's table.
    - A node can send only the first two columns of its table to any neighbour.
    - Sharing here means sharing only the first two columns.

Distance Vector Routing

LNMIIT The LNM Institute of Information Technology

- Updating:
  - When a node receives a two-column table from a neighbor, it needs to update its routing table.
  - Steps:
    - The receiving node needs to add the cost between itself and the sending node to each value in the second column.
    - The receiving node needs to add the name of the sending node to each row as the third column. The sending node is the next node in the route.
    - The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table.
    - If the next-node entry is different, the receiving node chooses the row with the smaller cost. If there is a tie, the old one is kept.
    - If the next-node entry is the same, the receiving node chooses the new row.

Distance Vector Routing

- Updating:

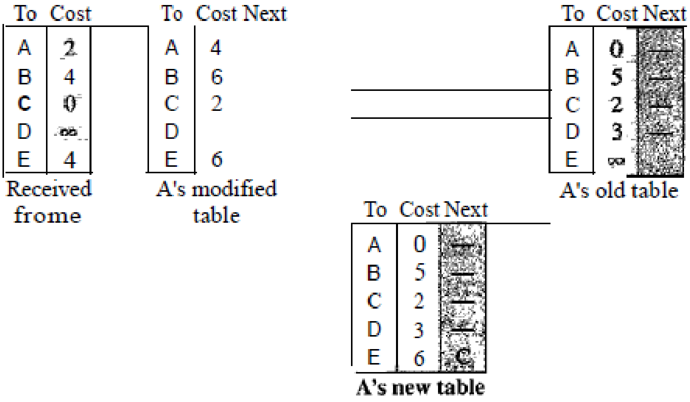


Figure: Updating in distance vector routing

Distance Vector Routing

- When to Share:

Distance Vector Routing

- When to Share:
  - Periodic Update: The period depends on the protocol that is using distance vector routing.

Distance Vector Routing

- When to Share:
  - Periodic Update: The period depends on the protocol that is using distance vector routing.
  - Triggered Update: A node sends its table when there is a change in its routing table.
    - A node receives a table from a neighbor, resulting in changes in its own table after updating.
    - A node detects some failure in the neighboring links which results in a distance change to infinity.

- Two Node Loop Instability Problem

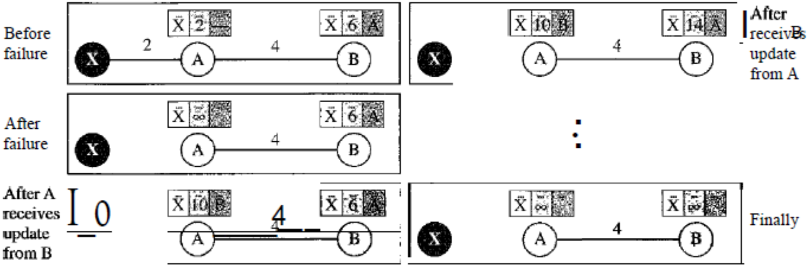


Figure: Two node instability problem

- Two Node Loop Instability Problem

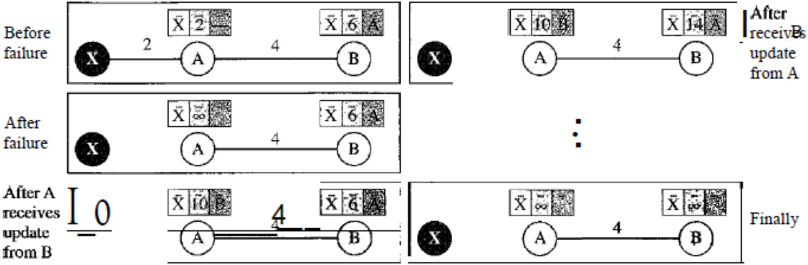


Figure: Two node instability problem

- Solution
  - Defining Infinity
  - Split Horizon
  - Split Horizon and Poison Reverse

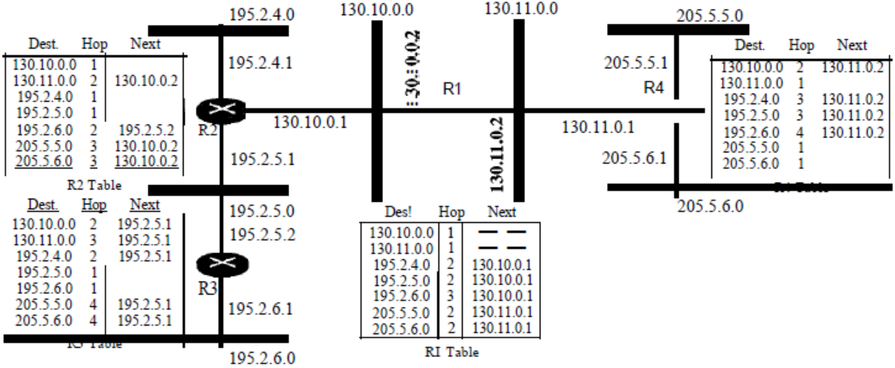
RIP

- Routing Information Protocol (RIP): intradomain routing protocol used inside an autonomous system.
- It is a very simple protocol based on distance vector routing.

RIP

- Routing Information Protocol (RIP): intradomain routing protocol used inside an autonomous system.
- It is a very simple protocol based on distance vector routing.
- Considerations:
  - In an autonomous system, we are dealing with routers and networks (links). The routers have routing tables; networks do not.
  - The destination in a routing table is a network, which means the first column defines a network address.
  - The metric used by RIP is very simple; the distance is defined as the number of links (networks) to reach the destination. For this reason, the metric in RIP is called a *hop count*.
  - Infinity is defined as 16, which means that any route in an autonomous system using RIP cannot have more than 15 hops.
  - The next-node column defines the address of the router to which the packet is to be sent to reach its destination.

RIP



Dest.	Hop	Next
130.10.0.0	1	
130.11.0.0	2	130.10.0.2
195.2.4.0	1	
195.2.5.0	1	
195.2.6.0	2	195.2.5.2
205.5.5.0	3	130.10.0.2
205.5.6.0	3	130.10.0.2

Dest.	Hop	Next
130.10.0.0	2	195.2.5.1
130.11.0.0	3	195.2.5.1
195.2.4.0	2	195.2.5.1
195.2.5.0	1	
195.2.6.0	1	
205.5.5.0	4	195.2.5.1
205.5.6.0	4	195.2.5.1

Des!	Hop	Next
130.10.0.0	1	— —
130.11.0.0	1	— —
195.2.4.0	2	130.10.0.1
195.2.5.0	2	130.10.0.1
195.2.6.0	3	130.10.0.1
205.5.5.0	2	130.11.0.1
205.5.6.0	2	130.11.0.1

Dest.	Hop	Next
130.10.0.0	2	130.11.0.2
130.11.0.0	1	
195.2.4.0	3	130.11.0.2
195.2.5.0	3	130.11.0.2
195.2.6.0	4	130.11.0.2
205.5.5.0	1	
205.5.6.0	1	

Figure: Example of a domain using RIP

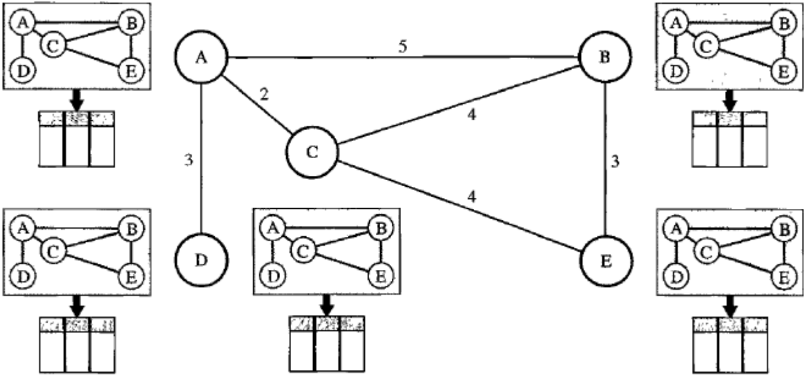


Figure: Concept of Link State Routing

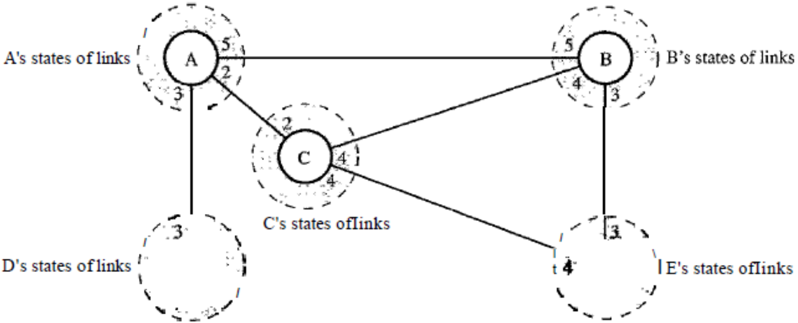


Figure: Link state knowledge

Link State Routing

- Building Routing Tables: four sets of actions are required
  - Creation of the states of the links by each node, called the link state packet (LSP).
  - Dissemination of LSPs to every other router, called flooding, in an efficient and reliable way.
  - Formation of a shortest path tree for each node.
  - Calculation of a routing table based on the shortest path tree.

Link State Routing

- Creation of Link State Packet (LSP)
  - A link state packet can carry a large amount of information, such as
    - node identity (to make topology),
    - list of links (to make topology),
    - sequence number (facilitates flooding and distinguishes new LSPs form old ones), and
    - age (prevents old LSPs from remaining in the domain for a long time)
  - LSPs are generated on two occasions:
    - When there is a change in the topology of the domain
    - On a periodic basis

- Flooding of LSPs
  - After a node has prepared an LSP, it must be disseminated to all other nodes, not only to its neighbors.
  - The process is called flooding and based on the following:
    - The creating node sends a copy of the LSP out of each interface.
    - A node that receives an LSP compares it with the copy it may already have.
    - If the newly arrived LSP is older than the one it has, it discards the LSP.
    - If it is newer, the node discards the old LSP and keeps the new one and sends a copy of it out of each interface except the one from which the packet arrived.

- Formation of Shortest Path Tree
  - After receiving all LSPs, each node will have a copy of the whole topology.
  - The topology is not sufficient to find the shortest path to every other node
  - Thus, a shortest path tree is needed.
  - A tree is a graph of nodes and links – one node is called the root.
  - All other nodes can be reached from the root through only one single route.
  - A shortest path tree is a tree in which the path between the root and every other node is the shortest.
  - Requirement: for each node, a shortest path tree is needed with that node as the root.
  - Dijkstra algorithm creates a shortest path tree from a graph.
  - The algorithm divides the nodes into two sets: tentative and permanent.
  - It finds the neighbors of a current node, makes them tentative, examines them, and if they pass the criteria, makes them permanent.

- Formation of Shortest Path Tree

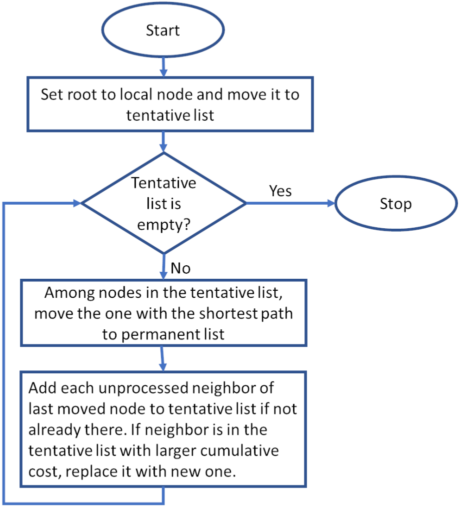


Figure: Djikstra Algorithm

- Formation of Shortest Path Tree Steps
  - Make node *A* as root and move it to tentative list.
    Permanent list: *empty* Tentative list: *A(0)*
  - Move *A* to the pennanent list and add all neighbors of *A* to the tentative list.
    Permanent list: *A(0)* Tentative list: *B(5), C(2), D(3)*
  - Node *C* has the shortest cumulative cost from all nodes in the tentative list.
    Permanent list: *A(0), C(2)* Tentative list: *B(5), D(3), E(6)*
  - Node *D* has the shortest cumulative cost of all the nodes in the tentative list.
    Permanent list: *A(0), C(2), D(3)* Tentative list: *B(5), E(6)*
  - Node *B* has the shortest cumulative cost of all the nodes in the tentative list.
    Permanent list: *A(0), B(5), C(2), D(3)* Tentative list: *E(6)*
  - Node *E* has the shortest cumulative cost from all nodes in the tentative list.
    Permanent list: *A(0), B(5), C(2), D(3), E(6)* Tentative list: *empty*

LNMIIT The LNM Institute of Information Technology

- Calculation of Routing Table from Shortest Path Tree
  - Each node uses the shortest path tree protocol to construct its routing table.
  - The routing table shows the cost of reaching each node from the root.

Node	*Cost*	*Next Router*
A	0	-
B	5	-
C	2	-
D	3	-
E	6	C

Figure: Routing table for node A

OSPF

- The Open Shortest Path First (OSPF) protocol is an intradomain routing protocol based on link state routing.
- Its domain is also an autonomous system.
- Area

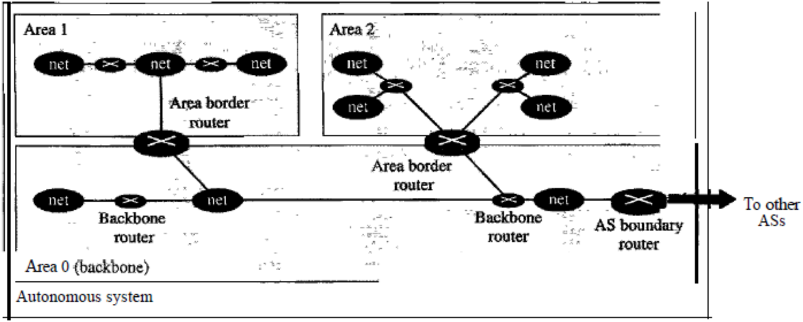


Figure: Areas in an autonomous system

OSPF

- Metric
  - The OSPF protocol allows the administrator to assign a cost, called the metric, to each route.
  - The metric can be based on a type of service (minimum delay, maximum throughput, etc).
  - A router can have multiple routing tables, each based on a different type of service.

OSPF

- Metric
  - The OSPF protocol allows the administrator to assign a cost, called the metric, to each route.
  - The metric can be based on a type of service (minimum delay, maximum throughput, etc).
  - A router can have multiple routing tables, each based on a different type of service.
- Types of Links

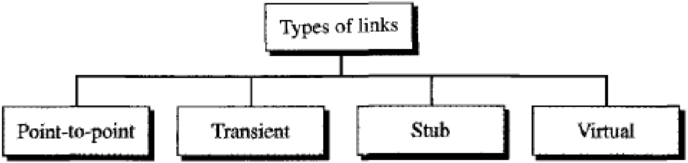


Figure: Types of links

- Types of Links
  - A point-to-point link connects two routers without any other host or router in between.
  - A transient link is a network with several routers attached to it.
  - A stub link is a network that is connected to only one router.
  - When the link between two routers is broken, the administration may create a virtual link between them, using a longer path that probably goes through several routers.

- Graphical Representation

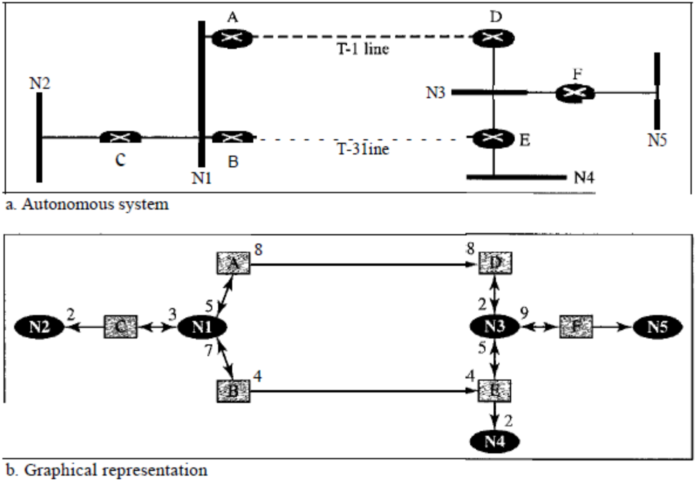


Figure: Example of an AS and its graphical representation in OSPF

Path Vector Routing

- Limitations of Intra-domain Routing Protocols
  - They cannot be used between different autonomous systems.
  - The reason for their non-suitability in inter-domain routing is scalability.
  - Both the protocols become intractable when the domain of operation becomes large.
  - Distance vector routing is subject to instability if there are more than a few hops in the domain of operation.
  - Link state routing needs a huge amount of resources to calculate routing tables and creates heavy traffic because of flooding.

Path Vector Routing

- Limitations of Intra-domain Routing Protocols
  - They cannot be used between different autonomous systems.
  - The reason for their non-suitability in inter-domain routing is scalability.
  - Both the protocols become intractable when the domain of operation becomes large.
  - Distance vector routing is subject to instability if there are more than a few hops in the domain of operation.
  - Link state routing needs a huge amount of resources to calculate routing tables and creates heavy traffic because of flooding.
- Path Vector Routing
  - It is assumed that there is one node in each autonomous system that acts on behalf of the entire autonomous system (Speaker Node).
  - The speaker node in an AS creates a routing table and advertises it to speaker nodes in the neighboring ASs.
  - A speaker node advertises the path.

- Initialization

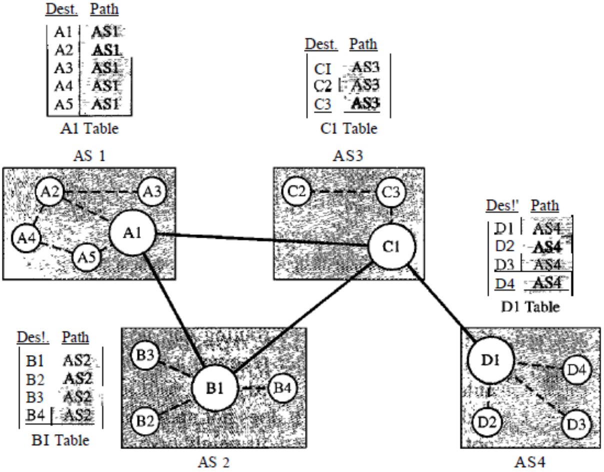


Figure: Initial routing tables in path vector routing

Path Vector Routing

- Sharing: a speaker in an autonomous system shares its table with immediate neighbours.
  - Node A_1 shares its table with nodes B_1 and C_1.
  - Node C_1 shares its table with nodes D_1, B_1, and A_1.
  - Node B_1 shares its table with C_1 and A_1.
  - Node D_1 shares its table with C_1.

Path Vector Routing

- Sharing: a speaker in an autonomous system shares its table with immediate neighbours.
  - Node A_1 shares its table with nodes B_1 and C_1.
  - Node C_1 shares its table with nodes D_1, B_1, and A_1.
  - Node B_1 shares its table with C_1 and A_1.
  - Node D_1 shares its table with C_1.
- Updating

Oest.	Path
A1	AS1
AS	AS1
B1	-AS2
B4	AS1-AS2
C1	AS1-AS3
...	...
C3	AS1-AS3
01	AS1-AS2-AS4
...	...
D4	AS1-AS2-AS4

A1 Table

Oest.	Path
A1	AS2-AS1
...	
A5	AS2-AS1
B1	AS2
...	...
B4	AS2
C1	AS2-AS3
...	...
C3	AS2-AS3
D1	AS2-AS3-AS4
...	...
D4	AS2-AS3-AS4

B1 Table

Oest.	Path
A1	AS3-AS1
...	
A5	AS3-AS1
B1	AS3-AS2
...	...
B4	AS3-AS2
C1	AS3
...	...
C3	AS3
D1	AS3-AS4
...	...
D4	AS3-AS4

C1 Table

Dest.	Path
A1	AS4-AS3-AS1
A5	AS4-AS3-AS1
B1	AS4-AS3-AS2
...	...
B4	AS4-AS3-AS2
C1	AS4-AS3
...	...
C3	AS4-AS3
D1	AS4
...	...
D4	AS4

D1 Table

Figure: Stabilized tables for three autonomous systems

- Key Points:

Path Vector Routing

- Key Points:
  - Loop Prevention:
    - When a router receives a message, it checks to see if its autonomous system is in the path list to the destination.
    - If it is, looping is involved and the message is ignored.

Path Vector Routing

- Key Points:
  - Loop Prevention:
    - When a router receives a message, it checks to see if its autonomous system is in the path list to the destination.
    - If it is, looping is involved and the message is ignored.
  - Policy Routing:
    - When a router receives a message, it can check the path.
    - If one of the autonomous systems listed in the path is against its policy, it can ignore that path and that destination.
    - It does not update its routing table with this path, and it does not send this message to its neighbors.

Path Vector Routing

- Key Points:
  - Loop Prevention:
    - When a router receives a message, it checks to see if its autonomous system is in the path list to the destination.
    - If it is, looping is involved and the message is ignored.
  - Policy Routing:
    - When a router receives a message, it can check the path.
    - If one of the autonomous systems listed in the path is against its policy, it can ignore that path and that destination.
    - It does not update its routing table with this path, and it does not send this message to its neighbors.
  - Optimum Path:
    - The optimum path is the path that fits the organization.
    - In the figure, each autonomous system may have more than one path to a destination.
    - For example, a path from AS_4 to AS_1 can be AS_4-AS_3-AS_2-AS_1, or it can be AS_4-AS_3-AS_1.
    - We choose the one that had the smaller number of autonomous systems, but this is not always the case.
    - Other criteria, such as security, safety, and reliability, can also be applied.

BGP

- Border Gateway Protocol (BGP) is an interdomain routing protocol using path vector routing.
- It first appeared in 1989 and has gone through four versions.

BGP

- Border Gateway Protocol (BGP) is an interdomain routing protocol using path vector routing.
- It first appeared in 1989 and has gone through four versions.
- Types of Autonomous Systems:

BGP

LNMIIT
The LNM Institute of Information Technology

- Border Gateway Protocol (BGP) is an interdomain routing protocol using path vector routing.
- It first appeared in 1989 and has gone through four versions.
- Types of Autonomous Systems:
  - Stub AS
    - A stub AS has only one connection to another AS.
    - The interdomain data traffic in a stub AS can be either created or terminated in the AS.
    - The hosts in the AS can send data traffic to other ASs.
    - The hosts in the AS can receive data coming from hosts in other ASs.
    - Data traffic, however, cannot pass through a stub AS.
    - A stub AS is either a source or a sink.
    - **Example:** a small corporation or a small local ISP.

BGP

- Types of Autonomous Systems:
  - Multihomed AS
    - A multihomed AS has more than one connection to other ASs, but it is still only a source or sink for data traffic.
    - It can receive data traffic from more than one AS.
    - It can send data traffic to more than one AS, but there is no transient traffic.
    - It does not allow data coming from one AS and going to another AS to pass through.
    - **Example:** a large corporation that is connected to more than one regional or national AS that does not allow transient traffic.

BGP

- Types of Autonomous Systems:
  - Multihomed AS
    - A multihomed AS has more than one connection to other ASs, but it is still only a source or sink for data traffic.
    - It can receive data traffic from more than one AS.
    - It can send data traffic to more than one AS, but there is no transient traffic.
    - It does not allow data coming from one AS and going to another AS to pass through.
    - **Example:** a large corporation that is connected to more than one regional or national AS that does not allow transient traffic.
  - Transit AS
    - A transit AS is a multihomed AS that also allows transient traffic.
    - **Example:** national and international ISPs (Internet backbones).

BGP

- Path Attributes
  - Each attribute gives some information about the path.
  - The list of attributes helps the receiving router make a more-informed decision when applying its policy.
  - Attributes are divided into two broad categories: well-known and optional.

- Path Attributes
  - Each attribute gives some information about the path.
  - The list of attributes helps the receiving router make a more-informed decision when applying its policy.
  - Attributes are divided into two broad categories: well-known and optional.
  - A well-known attribute is one that every BGP router must recognize.

- Path Attributes
  - Each attribute gives some information about the path.
  - The list of attributes helps the receiving router make a more-informed decision when applying its policy.
  - Attributes are divided into two broad categories: well-known and optional.
  - A well-known attribute is one that every BGP router must recognize.
  - An optional attribute is one that needs not be recognized by every router.

- Path Attributes
  - Each attribute gives some information about the path.
  - The list of attributes helps the receiving router make a more-informed decision when applying its policy.
  - Attributes are divided into two broad categories: well-known and optional.
  - A well-known attribute is one that every BGP router must recognize.
  - An optional attribute is one that needs not be recognized by every router.
  - Well-known attributes are divided into two categories: mandatory and discretionary.

BGP

- Path Attributes
  - Each attribute gives some information about the path.
  - The list of attributes helps the receiving router make a more-informed decision when applying its policy.
  - Attributes are divided into two broad categories: well-known and optional.
  - A well-known attribute is one that every BGP router must recognize.
  - An optional attribute is one that needs not be recognized by every router.
  - Well-known attributes are divided into two categories: mandatory and discretionary.
  - A well-known mandatory attribute is one that must appear in the description of a route (eg: ORIGIN, AS_PATH, NEXT-HOP).

- Path Attributes
  - Each attribute gives some information about the path.
  - The list of attributes helps the receiving router make a more-informed decision when applying its policy.
  - Attributes are divided into two broad categories: well-known and optional.
  - A well-known attribute is one that every BGP router must recognize.
  - An optional attribute is one that needs not be recognized by every router.
  - Well-known attributes are divided into two categories: mandatory and discretionary.
  - A well-known mandatory attribute is one that must appear in the description of a route (eg: ORIGIN, AS_PATH, NEXT-HOP).
  - A well-known discretionary attribute is one that must be recognized by each router, but is not required to be included in every update message.

- Path Attributes
  - Each attribute gives some information about the path.
  - The list of attributes helps the receiving router make a more-informed decision when applying its policy.
  - Attributes are divided into two broad categories: well-known and optional.
  - A well-known attribute is one that every BGP router must recognize.
  - An optional attribute is one that needs not be recognized by every router.
  - Well-known attributes are divided into two categories: mandatory and discretionary.
  - A well-known mandatory attribute is one that must appear in the description of a route (eg: ORIGIN, AS_PATH, NEXT-HOP).
  - A well-known discretionary attribute is one that must be recognized by each router, but is not required to be included in every update message.
  - The optional attributes can be divided into two categories: transitive and nontransitive.

BGP

- Path Attributes
  - Each attribute gives some information about the path.
  - The list of attributes helps the receiving router make a more-informed decision when applying its policy.
  - Attributes are divided into two broad categories: well-known and optional.
  - A well-known attribute is one that every BGP router must recognize.
  - An optional attribute is one that needs not be recognized by every router.
  - Well-known attributes are divided into two categories: mandatory and discretionary.
  - A well-known mandatory attribute is one that must appear in the description of a route (eg: ORIGIN, AS_PATH, NEXT-HOP).
  - A well-known discretionary attribute is one that must be recognized by each router, but is not required to be included in every update message.
  - The optional attributes can be divided into two categories: transitive and nontransitive.
  - An optional transitive attribute is one that must be passed to the next router by the router that has not implemented this attribute.

- Path Attributes
  - Each attribute gives some information about the path.
  - The list of attributes helps the receiving router make a more-informed decision when applying its policy.
  - Attributes are divided into two broad categories: well-known and optional.
  - A well-known attribute is one that every BGP router must recognize.
  - An optional attribute is one that needs not be recognized by every router.
  - Well-known attributes are divided into two categories: mandatory and discretionary.
  - A well-known mandatory attribute is one that must appear in the description of a route (eg: ORIGIN, AS_PATH, NEXT-HOP).
  - A well-known discretionary attribute is one that must be recognized by each router, but is not required to be included in every update message.
  - The optional attributes can be divided into two categories: transitive and nontransitive.
  - An optional transitive attribute is one that must be passed to the next router by the router that has not implemented this attribute.
  - An optional nontransitive attribute is one that must be discarded if the receiving router has not implemented it.

- BGP Sessions
  - The exchange of routing information between two routers using BGP takes place in a session.
  - A session is a connection that is established between two BGP routers only for the sake of exchanging routing information.
  - To create a reliable environment, BGP uses the services of TCP.
  - When a TCP connection is created for BGP, it can last for a long time, until something unusual happens.
  - For this reason, BGP sessions are sometimes referred to as semi-permanent connections.

- External and Internal BGP
  - BGP can have two types of sessions: external BGP (E-BGP) and internal BGP (I-BGP) sessions.
  - The E-BGP session is used to exchange information between two speaker nodes belonging to two different autonomous systems.
  - The I-BGP session is used to exchange routing information between two routers inside an autonomous system.

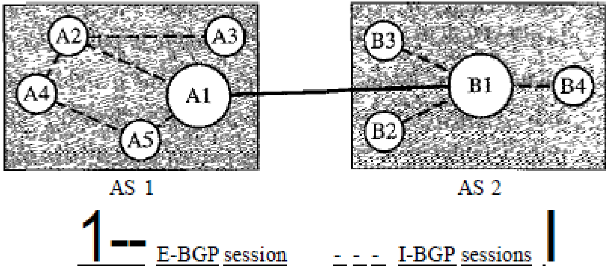


Figure: Internal and External BGP Sessions