BSc in Computer Engineering
CMP4204
Wireless Technologies

Lecture 4

Internetworking models and networking

Eng Diarmuid O'Briain, CEng, CISSP

Department of Electrical and Computer Engineering,
College of Engineering, Design, Art and Technology,
Makerere University

Table of Contents

1. INTERNETWORKING MODELS....5

1.1 OSI 7 LAYER MODEL....5
1.2 PEER LEVEL....7
1.3 PROTOCOL MAPPING....8

2. TCP/IP AND DOD MODEL....9

2.1 DOD FOUR-LAYER MODEL....10

3. DOMAIN NAME SYSTEM....11

3.1 ROOT NAMESERVERS....11
3.2 TOP LEVEL DOMAINS....11
3.3 NAMESERVERS....12
3.4 QUERY EXAMPLE....12

4. ROUTING NETWORK....14

4.1 BASIC CONFIGURATION OF RB11....14
4.2 BASIC CONFIGURATION OF RB10....15
4.3 BASIC CONFIGURATION OF RB12....15
4.4 ENABLING INTRA AREA OSPF....16
4.5 REVIEW THE ROUTING TABLES....18
4.6 TESTING....20

5. SELF-TEST QUIZ....21

Illustration Index

Illustration 1: OSI 7 layer model....5

Illustration 2: ISO 7 layer model - peering....7

Illustration 3: TCP/IP model mapped to ISO 7 Layer model....9

Illustration 4: TCP/IP model protocols....10

Illustration 5: DNS Query....12

Illustration 6: Basic network diagram....14

Illustration 7: MikroTik Packet Sniffer....20

This page is intentionally blank

1. Internetworking Models

1.1 OSI 7 layer Model

The OSI, or Open System Interconnection, model defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

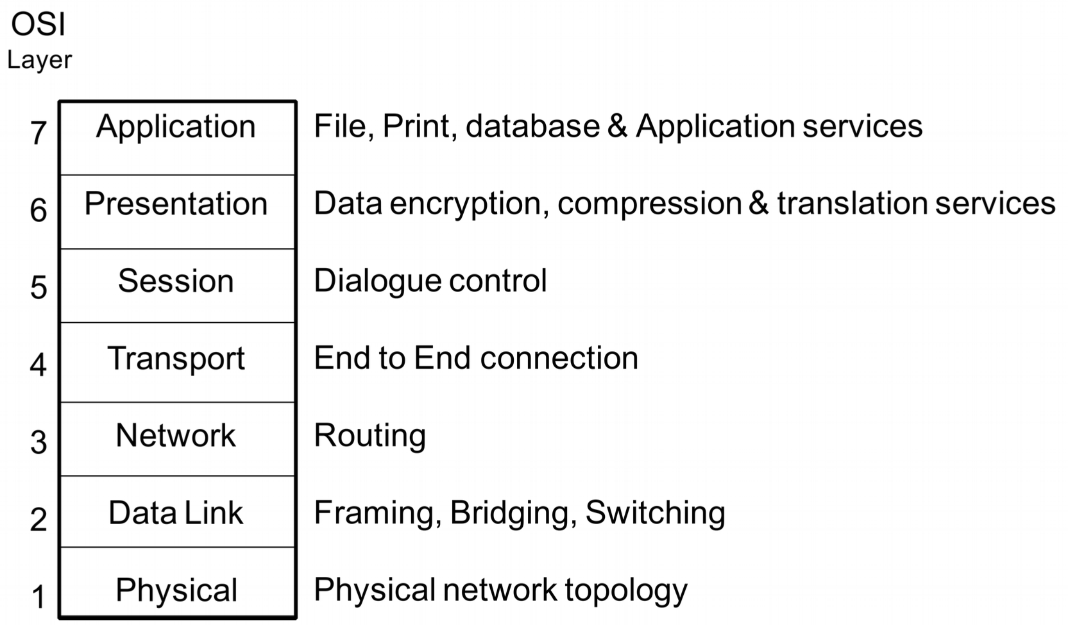


Illustration 1: OSI 7 layer model

1.1.1 Application

This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and File Transfer Protocol (FTP) are applications that exist entirely in the application level. Tiered application architectures are part of this layer.

1.1.2 Presentation

This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer. Examples at this layer include Tagged Image File Format (TIFF), Joint Photographic Experts Group (JPEG), Moving Pictures Experts Group (MPEG), Musical Instrument Digital Interface (MIDI).

1.1.3 Session

This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination. Session Layer protocols include Structured Query Language (SQL), Remote Procedure Call (RPC), Unix X-Windows.

1.1.4 Transport

This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer. In IP this function is achieved using a connection oriented mechanism called Transmission Control Protocol (TCP) or a non connection oriented protocol called User Datagram Protocol (UDP).

1.1.5 Network

This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing. This layer has two basic packet types;

1.1.5.1 Data Packets

Used to transport data through the internetwork.

1.1.5.2 Route Update Packets

Used to update neighbouring routers of new routing information i.e. Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP) and Routing Internet Protocol (RIP). These route updates take the form of;

Address – Network or Host route is about.

Interface – The Router Interface associated with this network or host.

Metric – The distance to the network or host expressed as a hop count or bandwidth, delay, interface type etc.

1.1.6 Data Link

At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge, handles errors in the physical layer, flow control and frame synchronisation. The data link layer is divided into two sub-layers: The Media Access Control (MAC) layer (802.3) and the Logical Link Control (LLC) layer (802.2). The MAC sub-layer controls how a host on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronisation, flow control and error checking. This layer is managed by Bridge and Switching devices. Bridges are devices which manage the interconnection of Physical segments using a mainly software function whereas Switches (sometimes called Layer 2 Switches) handle the bridging function using hardware Application Specific Integrated Circuits (ASICs) and such switching is often termed wire speed switching.

1.1.7 Physical

This layer conveys the bit stream, electrical impulse, light or radio signal through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and the physical aspects. Ethernet, Fast Ethernet, RS232, and Frame Relay are protocols with physical layer components. Typically we associate hubs with this layer.

1.2 Peer Level

Illustration 2 demonstrates the communication at each level. Peer relationships exist from hop to hop across the network.

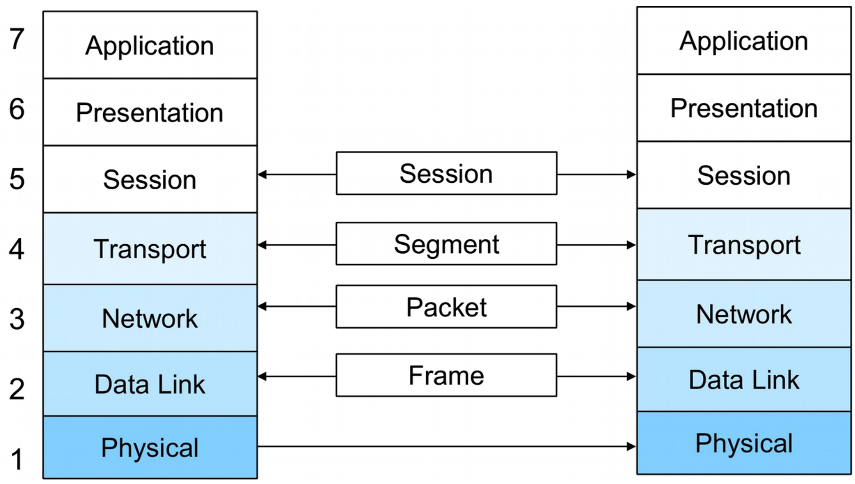


Illustration 2: ISO 7 layer model - peering

1.3 Protocol Mapping

Layer	Name	OSI protocols	TCP/IP protocols		SS7	UMTS
7	**Application**	FTAM	NNTP	NTP	INAP	
		X.400	SIP	DHCP	MAP	
		X.500	SSI	SMPP	TCAP	
		DAP	DNS	SMTP	ISUP	
		ROSE	FTP	SNMP	TUP	
		RTSE	Gopher	Telnet		
		ACSE	HTTP	BGP		
		CMIP	NFS	FCIP		
6	**Presentation**	ISO/IEC 8823	MIME			
		X.226	SSL			
		ISO/IEC 9576-1	TLS			
		X.236	XDR			
5	**Session**	ISO/IEC 8327	Sockets			
		X.225				
		ISO/IEC 9548-1				
		X.235				
4	**Transport**	ISO/IEC 8073	TCP			
		TP0	UDP			
		TP1	SCTP			
		TP2	DCCP			
		TP3				
		TP4 (X.224)				
		ISO/IEC 8602				
		X.234				
3	**Network**	ISO/IEC 8208	IP		SCCP	RRC / BMC
		X.25 (PLP)	IPsec		MTP	
		ISO/IEC 8878	ICMP			
		X.223	IGMP			
		ISO/IEC 8473-1	OSPF			
		CLNP X.233	RIP			
2	**Data link**	ISO/IEC 7666	PPP		MTP	PDCP
		X.25 (LAPB)	SBTV		Q.710	LLC
		Token Bus	SLIP			MAC
		X.222				
		ISO/IEC 8802-2				
		LLC (type 1 / 2)				

2. TCP/IP and DoD Model

The Internet protocol suite is the set of protocols that implement the protocol stack on which the Internet runs. It is sometimes called the TCP/IP protocol suite after two of the many protocols that make up the suite: the Transmission Control Protocol (TCP) and the Internet Protocol (IP).

The Internet Protocol suite can be described by analogy with the OSI model, which describes the layers of a protocol stack, not all of which correspond well with Internet practice. In a protocol stack, each layer solves a set of problems involving the transmission of data. Higher layers are logically closer to the user and deal with more abstract data, relying on lower layers to translate data into forms that can eventually be physically manipulated.

The Internet model was designed as the solution to a practical engineering problem. The OSI model, on the other hand, was a more theoretical approach, and was built by committee. Therefore, the OSI model is easier to understand, but the TCP/IP model is more practical. It is helpful to have an understanding of the OSI model before learning TCP/IP, as the same principles apply, but are easier to understand in the OSI model.

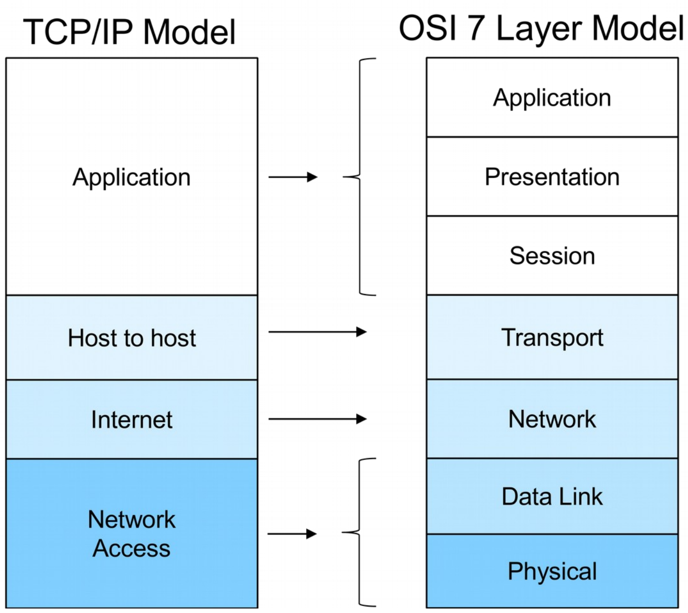


Illustration 3: TCP/IP model mapped to ISO 7 Layer model

2.1 DoD Four-Layer Model

The DoD Four-Layer Model was developed in the 1970s for the DARPA Internetwork Project that eventually grew into the Internet.

The four layers in the DoD model:

The Network Access Layer is responsible for delivering data over the particular hardware media in use. Different protocols are selected from this layer, depending on the type of physical network.

The Internet Layer is responsible for delivering data across a series of different physical networks that interconnect a source and destination machine. Routing protocols are most closely associated with this layer, as is the IP Protocol, the Internet's fundamental protocol.

The Host-to-Host Layer handles connection rendezvous, flow control, retransmission of lost data, and other generic data flow management. The mutually exclusive TCP and UDP protocols are this layer's most important members.

The Process Layer contains protocols that implement user-level functions, such as mail delivery, file transfer and remote login.

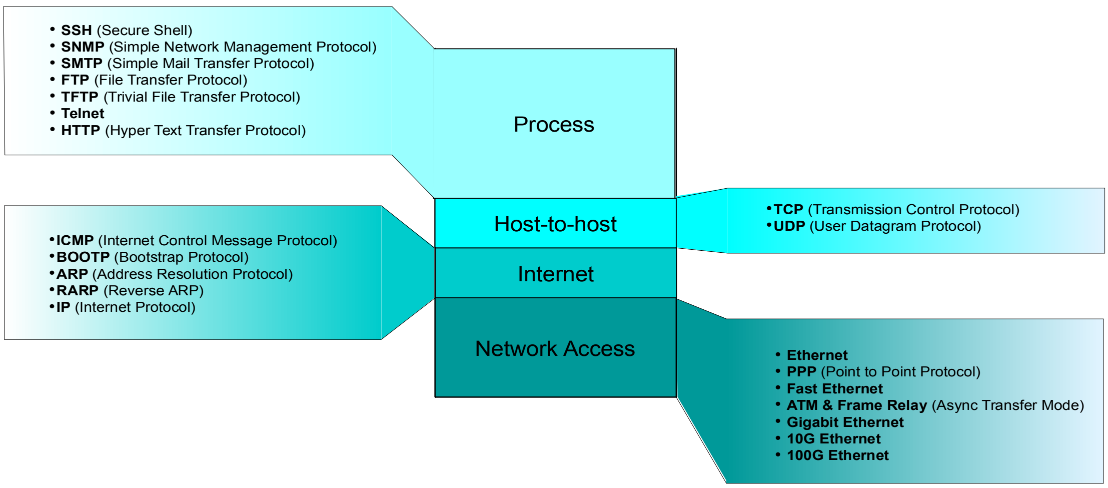


Illustration 4: TCP/IP model protocols

3. Domain Name System

The Domain Name System (DNS) is an essential part of the Internet. It is the standard by which Internet connected devices translate user-friendly domain names like "www.netlabsug.org" into an IP address like 2012:7f6::1 or 72.163.4.161.

3.1 Root nameservers

The top hierarchy of DNS are root name servers delegated by the Internet Corporation for Assigned Names and Numbers (ICANN) to a number of companies and organisations to ensure resiliance. Examples of such organisations are Verisign, University of Southern California, Internet Systems Consortium (ISC) and Réseaux IP Européens (RIPE). Each of these organisations manage a distributed set of servers right across the world and are collectively called the root zone. These root servers contain the global list of IP Addresses for the name servers of each of the Top Level Domains (TLD).

3.2 Top Level Domains

The Internet is organised into a hierarchy of domains, administered by the respective registrars and domain name holders. The TLDs in the root zone are:

- generic TLDs (gTLD): .com, .net, .int, .edu, .gov, .mil and .org
- country code TLDs (ccTLD): two-letter codes for each country, .ie for Ireland or .ug for Uganda.

3.2.1 Internationalised Domain Names

In 2009, ICANN decided to implement a new class of TLD called Internationalised Domain Names (IDN), assignable to countries and independent regions, similar to the rules for ccTLDs. However, the domain names may be any desirable string of characters, symbols, or glyphs in the language-specific, non-Latin alphabet or script of the applicant's language, within certain guidelines to assure sufficient visual uniqueness.

For example Egypt, Saudi Arabia and the United Arab Emirates were the first three countries to use Arabic characters in the last portion of their Internet domain names, such as dot-eg (Egypt), dot-sa (Saudi Arabia) or dot-ae (United Arab Emirates). They are called country code top-level domains or ccTLDs. An example is the IDN ccTLD for Saudi Arabia (.السعودية).

3.2.2 Expansion of gTLDs

In 2012 it was decided by iCANN to expand the gTLD set to allow a registry to register any word or set of characters. This however has come under some criticism from many trade associations and large companies claiming it can confuse user and spreads Internet searches across a slew of new TLDs. Example of these are:

.academy .rugby .club .cash .christmas .mom .dog

3.3 Nameservers

A nameserver is a server that stores the DNS records, such as IPv4 address records (A) or IPv6 address Quad-A records (AAAA), name server records (NS), mail exchanger records (MX), canonical name (alias) records (CNAME) and pointer records (PTR) that resolve IP address to a domain/hostname (reverse of A and AAAA).

3.3.1 Authoritative Name Server

An authoritative nameserver holds the actual DNS records for a particular domain.

3.3.2 Recursive Name Server

A recursive nameserver or recursive resolver is a DNS server that queries an authoritative nameserver to resolve a domain to an address. Actually when a request is made of a recursive nameserver it first checks to see if it has an existing cached entry with a valid Time-To-Live (TTL). If it has it responds with that, otherwise it starts the recursive process of going through the authoritative DNS hierarchy.

3.4 Query example

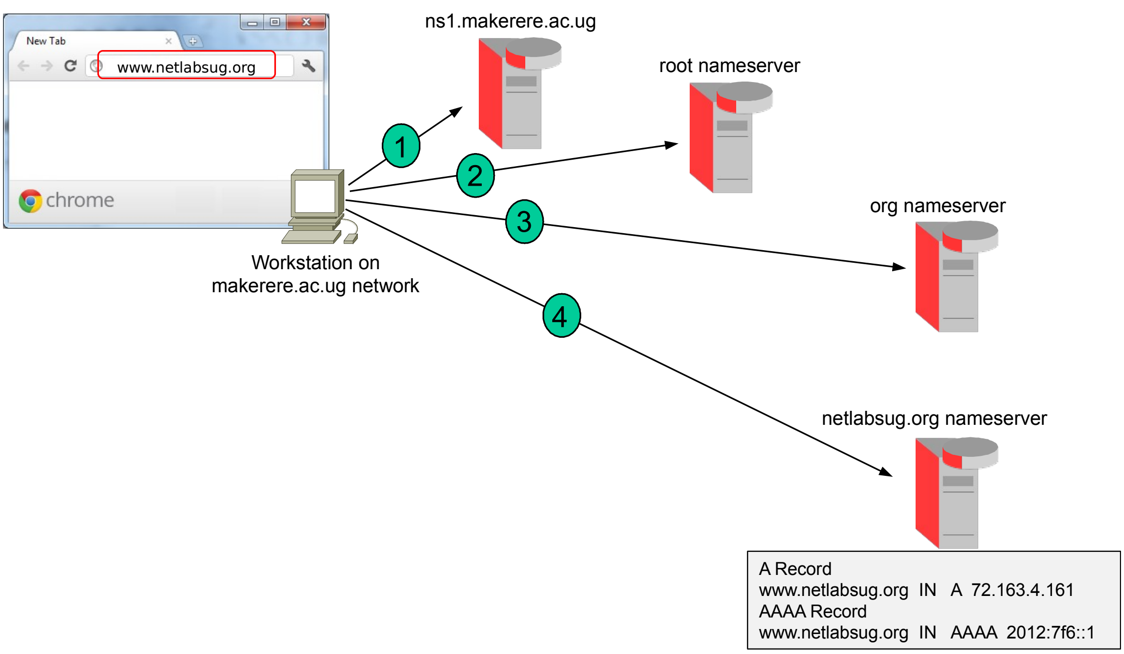


Illustration 5: DNS Query

Illustration 5 Is an example where a workstation on the makerere.ac.ug network makes a DNS query of the nameserver *ns1.makerere.ac.ug* for the domain *www.netlabsug.org*.

As the requested host is not in the domain *ns1.makerere.ac.ug* then the nameserver acts in a recursive mode, checking if it has a cached entry. Assuming it doesn't have a cached entry, it will therefore direct the query to the TLD for the requested domain within the root zone. The query then reaches out to the the nearest root server which returns an IP address for the .org nameserver. A request to this IP address is responded to with the IP address of the *netlabsug.org* nameserver which is authoritative for the domain *netlabsug.org*. It looks up its database and gets the A and AAAA records for the host *www*. This is then returned to the requesting workstation so a resolution of domain name to IP address can be made.

4. Routing Network

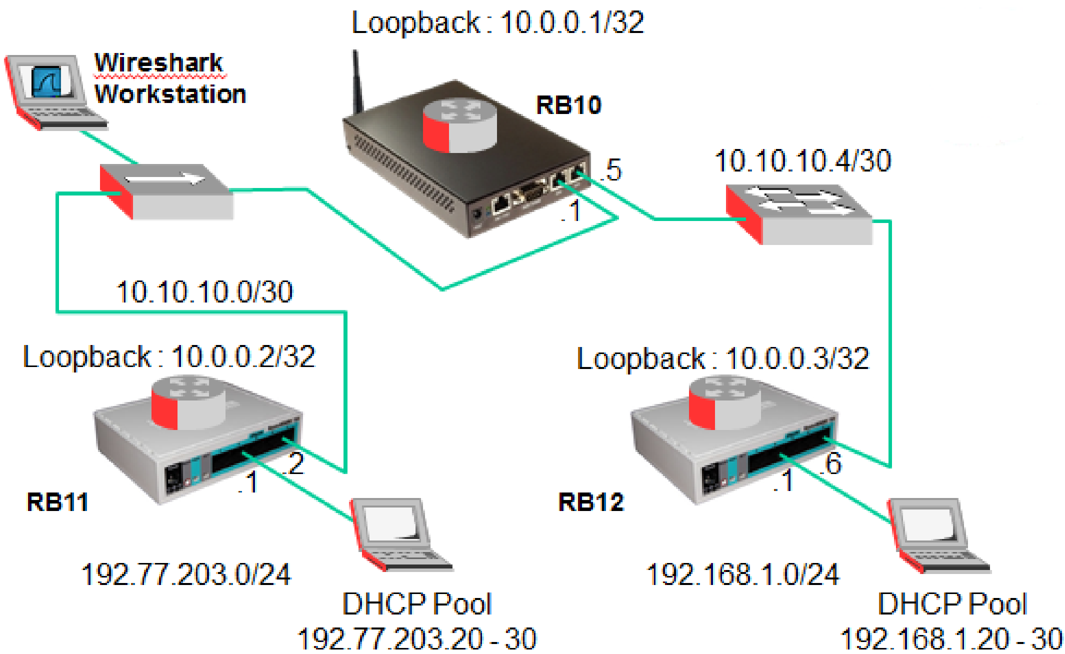


Illustration 6: Basic network diagram

While this course is not a networking course, a knowledge of basic IP networking is necessary. This lab is a tool to revise networking. The network diagram in Illustration 6 includes two MikroTik RB750G devices as routers plus a MikroTik RB433.

4.1 Basic configuration of RB11

4.1.1 Identity

Set the system identity.

```
[admin@MikroTik] > system identity set name RB11
```

4.1.2 IP Configuration

Add IP addresses to the interfaces as given in Illustration 6.

```
[admin@RB11] > ip address add address=192.77.203.1/24
                   interface=ether2

[admin@RB11] > ip address add address=10.10.10.2/30 interface=ether5
```

Create a Dynamic Host Configuration Protocol (DHCP) Server for the LAN interface.

```
[admin@RB11] > ip pool add name=dhcp-pool1
                   ranges=192.77.203.20-192.77.203.30

[admin@RB11] > ip dhcp-server add address-pool=dhcp-pool1
                   disabled=no interface=ether2 lease-time=3d
                   name=dhcp-server-ether2

[admin@RB11] > ip dhcp-server network add address=192.77.203.0/24
                   gateway=192.77.203.1
```

Confirm the addresses are configured OK.

```
[admin@RB11] > ip address print

Flags: X - disabled, I - invalid, D - dynamic

 #   ADDRESS             NETWORK        BROADCAST        INTERFACE
 0   192.77.203.1/24     192.77.203.0   192.77.203.255   ether2
 1   10.10.10.2/30       10.10.10.0     10.10.10.3       ether5
```

4.2 Basic configuration of RB10

Configuration of the RB10 is similar to that for the RB11.

```
[admin@MikroTik] > system identity set name RB10

[admin@RB10] > ip address add address=10.10.10.1/30 interface=ether2

[admin@RB10] > ip address add address=10.10.10.5/30 interface=ether3

[admin@RB10] > ip address print

Flags: X - disabled, I - invalid, D - dynamic

 #   ADDRESS         NETWORK       BROADCAST       INTERFACE
 0   10.10.10.1/30   10.10.10.0    10.10.10.3      ether2
 1   10.10.10.5/30   10.10.10.4    10.10.10.7      ether3
```

4.3 Basic configuration of RB12

Configuration of this router is practically identical to RB11.

```
[admin@MikroTik] > system identity set name RB12

[admin@RB12] > ip address add address=192.168.1.1/24 interface=ether2

[admin@RB12] > ip address add address=10.10.10.6/30 interface=ether5

[admin@RB12] > ip pool add name=dhcp-pool1
                  ranges=192.168.1.20-192.168.1.30

[admin@RB12] > ip dhcp-server add address-pool=dhcp-pool1 disabled=no
                  interface=ether2 lease-time=3d
                  name=dhcp-server-ether2

[admin@RB12] > ip dhcp-server network add address=192.168.1.0/24
                  gateway=192.168.1.1

[admin@RB12] > ip address print

Flags: X - disabled, I - invalid, D - dynamic

 #   ADDRESS          NETWORK        BROADCAST       INTERFACE
 0   192.168.1.1/24   192.168.1.0    192.168.1.255    ether2
 1   10.10.10.6/30    10.10.10.5     10.10.10.8       ether5
```

4.4 Enabling Intra area OSPF

4.4.1 RB11

Look at the OSPF areas that configured. In all cases this will only be the backbone area 0.0.0.0 as this is the default area.

```
[admin@RB11] > routing ospf area print

Flags: X - disabled

 #   NAME          AREA-ID         TYPE    DEFAULT-COST

 0   backbone      0.0.0.0         default
```

Create a loopback (bridge) interface with STP disabled (none).

```
[admin@RB11] > interface bridge add name=loopback1 protocol-mode=none
                         arp=disabled
```

Give the loopback interface an IP address.

```
[admin@RB11] > ip address add address=10.0.0.2/32 interface=loopback1
```

Configure the default OSPF instance with a Router ID which should be the same as the Loopback Address. Connected interfaces are redistributed as Type 1 LSA. This is equivalent to Cisco passive interface.

```
[admin@RB11] > routing ospf instance set default router-id=10.0.0.2
                       redistribute-connected=as-type-1
```

Add the networks that are to be routed to the OSPF backbone area i.e. two interfaces and the loopback.

```
[admin@RB11] > routing ospf network add area=backbone
                       network=192.77.203.0/24

[admin@RB11] > routing ospf network add area=backbone
                       network=10.10.10.0/30

[admin@RB11] > routing ospf network add area=backbone
                       network=10.0.0.2/32
```

4.4.2 RB10

Add the two networks and the two interfaces that link to the RB750G routers to OSPF.

```
[admin@RB10] > interface bridge add name=loopback1 protocol-mode=none
                    arp=disabled

[admin@RB10] > ip address add address=10.0.0.1/32 interface=loopback1

[admin@RB10] > routing ospf instance set default router-id=10.0.0.1
                  redistribute-connected=as-type-1

[admin@RB10] > routing ospf network add area=backbone
                  network=10.10.10.0/30

[admin@RB10] > routing ospf network add area=backbone
                  network=10.10.10.4/30

[admin@RB10] > routing ospf network add area=backbone
                  network=10.0.0.1/32
```

4.4.3 RB12

Add the two networks and the uplink interface to the RB10 router to OSPF.

```
[admin@RB12] > interface bridge add name=loopback1 protocol-mode=none

             arp=disabled

[admin@RB12] > ip address add address=10.0.0.3/32 interface=loopback1

[admin@RB12] > routing ospf instance set default router-id=10.0.0.3
                  redistribute-connected=as-type-1

[admin@RB12] > routing ospf network add area=backbone
                  network=192.168.1.0/24

[admin@RB12] > routing ospf network add area=backbone
                  network=10.10.10.4/30

[admin@RB12] > routing ospf network add area=backbone
                  network=10.0.0.3/32
```

4.5 Review the Routing tables

4.5.1 RB11

Reviewing the routing tables we can now see the new routes learned by OSPF with the label Active Dynamic OSPF (ADo).

```
[admin@RB11] > ip route print

Flags: X - disabled, A - active, D - dynamic, C - connect, S -
static, r - rip, b - bgp, o - ospf, m - mme, B - blackhole, U -
unreachable, P - prohibit

 #      DST-ADDRESS       PREF-SRC       GATEWAY     DISTANCE

 0 ADC  10.10.10.0/30     10.10.10.2     ether2         0
 1 ADo  10.10.10.4/30     10.10.10.1                   110
 2 ADC  192.77.203.0/24   192.77.203.1   ether2         0
 3 ADo  192.168.1.0/24    10.10.10.1                   110
```

Review the OSPF Neighbour list that this router has formed an adjacency with.

```
[admin@RB11] > routing ospf neighbor print

0 router-id=10.10.10.5 address=10.10.10.1 interface=ether2 priority=1
dr-address=10.10.10.1 backup-dr-address=10.10.10.2 state="Full"
state-changes=5 ls-retransmits=0 ls-requests=0 db-summaries=0
adjacency=52m15s
```

Review the OSPF LSA list that this router has built.

```
[admin@RB11] > routing ospf lsa print

AREA          TYPE    ID          ORIGINATOR   SEQUENCE-NU…   AGE

backbone      router  10.10.10.2  10.10.10.2   0x80000004     1616
backbone      router  10.10.10.5  10.10.10.5   0x80000006     1524
backbone      router  10.10.10.6  10.10.10.6   0x80000004     1541
backbone      network 10.10.10.1  10.10.10.5   0x80000002     1606
backbone      network 10.10.10.6  10.10.10.6   0x80000002     1541
```

4.5.2 RB10

```
[admin@RB10] > ip route print

Flags: X - disabled, A - active, D - dynamic, C - connect, S -
static, r - rip, b - bgp, o - ospf, m - mme, B - blackhole, U -
unreachable, P - prohibit

 #      DST-ADDRESS       PREF-SRC     GATEWAY       DISTANCE

 0 ADC  10.10.10.0/30     10.10.10.1   ether2           0
 1 ADC  10.10.10.4/30     10.10.10.5   ether3           0
 2 Ado  192.77.203.0/24                10.10.10.2      110
 3 Ado  192.168.1.0/24                 10.10.10.6      110
```

```
[admin@RB10] > routing ospf neighbor print

0 instance=default router-id=10.10.10.6 address=10.10.10.6
interface=ether3 priority=1 dr-address=10.10.10.6 backup-dr-
address=10.10.10.5 state="Full" state-changes=5 ls-retransmits=0 ls-
requests=0 db-summaries=0  adjacency=48m20s

1 instance=default router-id=10.10.10.2 address=10.10.10.2
interface=ether2 priority=1 dr-address=10.10.10.1 backup-dr-
address=10.10.10.2 state="Full" state-changes=5 ls-retransmits=0 ls-
requests=0 db-summaries=0  adjacency=49m53s
```

```
[admin@RB10] > routing ospf lsa print

AREA       TYPE      ID            ORIGINATOR   SEQUENCE-NU...  AGE

backbone   router    10.10.10.2    10.10.10.2   0x80000004      1667
backbone   router    10.10.10.5    10.10.10.5   0x80000006      1574
backbone   router    10.10.10.6    10.10.10.6   0x80000004      1591
backbone   network   10.10.10.1    10.10.10.5   0x80000002      1656
backbone   network   10.10.10.6    10.10.10.6   0x80000002      1591
```

4.5.3 RB12

```
[admin@RB11] > ip route print

Flags: X - disabled, A - active, D - dynamic, C - connect, S -
static, r - rip, b - bgp, o - ospf, m - mme, B - blackhole, U -
unreachable, P - prohibit

 #      DST-ADDRESS       PREF-SRC       GATEWAY         DISTANCE
 0 ADC  10.10.10.0/30                    10.10.10.5        110
 1 ADo  10.10.10.4/30     10.10.10.6     ether2            0
 2 ADC  192.77.203.0/24                  10.10.10.5        110
 3 ADo  192.168.1.0/24    192.168.1.1    ether2            0
```

```
[admin@rb750g/2] > routing ospf neighbor print

 0 instance=default router-id=10.10.10.5 address=10.10.10.5
interface=ether2 priority=1 dr-address=10.10.10.6 backup-dr-
address=10.10.10.5 state="Full" state-changes=5 ls-retransmits=0 ls-
requests=0 db-summaries=0 adjacency=52m42s
```

```
[admin@rb750g/2] > routing ospf lsa print

AREA      TYPE     ID            ORIGINATOR   SEQUENCE-NU...  AGE

backbone  router   10.10.10.2    10.10.10.2   0x80000004      1545
backbone  router   10.10.10.5    10.10.10.5   0x80000006      1451
backbone  router   10.10.10.6    10.10.10.6   0x80000004      1467
backbone  network  10.10.10.1    10.10.10.5   0x80000002      1534
backbone  network  10.10.10.6     10.10.10.6   0x80000002     1467
```

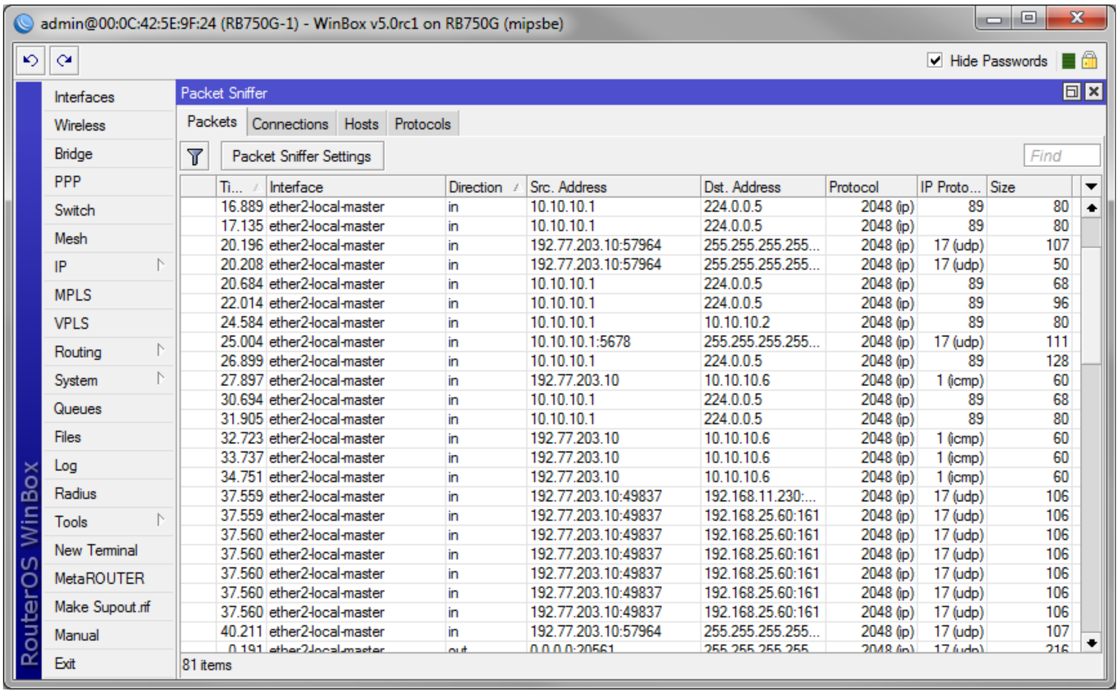
4.6 Testing

Ping, Traceroute from workstation to workstation.

4.6.1 MikroTik Packet Sniffer

Use the packet sniffer which can be accessed from WinBox Tools → Packet Sniffer.

Makes some changes like removing the ether3 interface on the RB10 temporarily. If you have a ping going to the RB12 side of the network from the 192.77.203.10 workstation you will see the connection drop. Shortly after re-inserting the cable the ping should resume.



Ti...	Interface	Direction	Src. Address	Dst. Address	Protocol	IP Proto...	Size
16.889	ether2-local-master	in	10.10.10.1	224.0.0.5	2048 (ip)	89	80
17.135	ether2-local-master	in	10.10.10.1	224.0.0.5	2048 (ip)	89	80
20.196	ether2-local-master	in	192.77.203.10:57964	255.255.255.255...	2048 (ip)	17 (udp)	107
20.208	ether2-local-master	in	192.77.203.10:57964	255.255.255.255...	2048 (ip)	17 (udp)	50
20.684	ether2-local-master	in	10.10.10.1	224.0.0.5	2048 (ip)	89	68
22.014	ether2-local-master	in	10.10.10.1	224.0.0.5	2048 (ip)	89	96
24.584	ether2-local-master	in	10.10.10.1	10.10.10.2	2048 (ip)	89	80
25.004	ether2-local-master	in	10.10.10.1:5678	255.255.255.255...	2048 (ip)	17 (udp)	111
26.899	ether2-local-master	in	10.10.10.1	224.0.0.5	2048 (ip)	89	128
27.897	ether2-local-master	in	192.77.203.10	10.10.10.6	2048 (ip)	1 (icmp)	60
30.694	ether2-local-master	in	10.10.10.1	224.0.0.5	2048 (ip)	89	68
31.905	ether2-local-master	in	10.10.10.1	224.0.0.5	2048 (ip)	89	80
32.723	ether2-local-master	in	192.77.203.10	10.10.10.6	2048 (ip)	1 (icmp)	60
33.737	ether2-local-master	in	192.77.203.10	10.10.10.6	2048 (ip)	1 (icmp)	60
34.751	ether2-local-master	in	192.77.203.10	10.10.10.6	2048 (ip)	1 (icmp)	60
37.559	ether2-local-master	in	192.77.203.10:49837	192.168.11.230:...	2048 (ip)	17 (udp)	106
37.559	ether2-local-master	in	192.77.203.10:49837	192.168.25.60:161	2048 (ip)	17 (udp)	106
37.560	ether2-local-master	in	192.77.203.10:49837	192.168.25.60:161	2048 (ip)	17 (udp)	106
37.560	ether2-local-master	in	192.77.203.10:49837	192.168.25.60:161	2048 (ip)	17 (udp)	106
37.560	ether2-local-master	in	192.77.203.10:49837	192.168.25.60:161	2048 (ip)	17 (udp)	106
37.560	ether2-local-master	in	192.77.203.10:49837	192.168.25.60:161	2048 (ip)	17 (udp)	106
37.560	ether2-local-master	in	192.77.203.10:49837	192.168.25.60:161	2048 (ip)	17 (udp)	106
40.211	ether2-local-master	in	192.77.203.10:57964	255.255.255.255...	2048 (ip)	17 (udp)	107

Illustration 7: MikroTik Packet Sniffer

5. Self-test Quiz

1. Map the following protocols:

ISO 7 Layer Model	**TCP/IP Model**
Transport	Network Access
Network	
Application	Host - host
Presentation	
Physical	Internet
Session	
Data Link	Process

2. State the purpose of each of the TCP/IP layers.

3. List two protocols for each layer of the TCP/IP model.

This page is intentionally blank