

Flexi Multiradio LTE BTS IP Essentials

Legal notice**Intellectual Property Rights**

All copyrights and intellectual property rights for Nokia Solutions and Networks training documentation, product documentation and slide presentation material, all of which are forthwith known as Nokia Solutions Networks training material, are the exclusive property of Nokia Solutions and Networks. Nokia Solutions and Networks owns the rights to copying, modification, translation, adaptation or derivatives including any improvements or developments. Nokia Solutions and Networks has the sole right to copy, distribute, amend, modify, develop, license, sublicense, sell, transfer and assign the Nokia Solutions and Networks training material. Individuals can use the Nokia Solutions and Networks training material for their own personal self-development only, those same individuals cannot subsequently pass on that same Intellectual Property to others without the prior written agreement of Nokia Solutions and Networks. The Nokia Solutions and Networks training material cannot be used outside of an agreed Nokia Solutions and Networks training session for development of groups without the prior written agreement of Nokia Solutions and Networks.

Indemnity

The information in this document is subject to change without notice and describes only the product defined in the introduction of this documentation. This document is not an official customer document and Nokia Solutions and Networks does not take responsibility for any errors or omissions in this document. This document is intended for the use of Nokia Solutions and Networks customers only for the purposes of the agreement under which the document is submitted. No part of this documentation may be used, reproduced, modified or transmitted in any form or means without the prior written permission of Nokia Solutions and Networks. The documentation has been prepared to be used by professional and properly trained personnel, and the customer assumes full responsibility when using it. Nokia Solutions and Networks welcomes customer comments as part of the process of continuous development and improvement of the documentation.

The information or statements given in this documentation concerning the suitability, capacity or performance of the mentioned hardware or software products are given "as is" and all liability arising in connection with such hardware or software products shall be defined conclusively and finally in a separate agreement between Nokia Solutions and Networks and the customer.

IN NO EVENT WILL Nokia Solutions and Networks BE LIABLE FOR ERRORS IN THIS DOCUMENTATION OR FOR ANY DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL OR ANY LOSSES SUCH AS BUT NOT LIMITED TO LOSS OF PROFIT, REVENUE, BUSINESS INTERRUPTION, BUSINESS OPPORTUNITY OR DATA, that might arise from the use of this document or the information in it.

THE CONTENTS OF THIS DOCUMENT ARE PROVIDED "AS IS". EXCEPT AS REQUIRED BY APPLICABLE MANDATORY LAW, NO WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT, ARE MADE IN RELATION TO THE ACCURACY, RELIABILITY OR CONTENTS OF THIS DOCUMENT. NOKIA SOLUTIONS AND NETWORKS RESERVES THE RIGHT TO REVISE THIS DOCUMENT OR WITHDRAW IT AT ANY TIME WITHOUT PRIOR NOTICE.

This document and the product it describes are considered protected by copyrights and other intellectual property rights according to the applicable laws.

Other product names mentioned in this document may be trademarks of their respective owners, and they are mentioned for identification purposes only.

Copyright © Nokia Solutions and Networks 2014. All rights reserved.

Table of Contents:

1	Welcome	4
2	Introduction to Internet Protocol Suite.....	5
3	Concept of Ethernet.....	6
4	Structure of Ethernet Frame	7
5	Concept of Internet Protocol	9
6	Binary/Decimal Conversion Review	10
7	Structure of an IPv4 address 1/2	11
8	Structure of an IPv4 address 2/2	12
9	IPv4 Header	13
10	IP Subnetting.....	15
11	IP Subnetting Example in NSN RAS.....	16
12	Exercise - IP Subnetting	18
13	IP Routing Principles 1	19
14	IP Routing Principles 2	20
15	IP related Commands in Windows	21
16	IP in NSN RAS	22
17	Exercise - Windows Networking Commands	24
18	Complete the Course.....	25

1 Welcome

Welcome to the e-learning course Flexi Multiradio LTE BTS IP Essentials

Course objectives:

At the end of the course the participant will be able to

- Describe the structure of the Ethernet frame (IEEE802.3).
- Explain the concept of IP in networks.
- Explain the structure of an IPv4 address.
- Describe the IP header with Differentiated Services Field.
- Explain the use of IP Subnet Masking in NSN RAS.
- Explain the IP routing principles in the RAS.
- List some useful IP commands in Windows.
- Explain the different uses of IP in NSN RAS.

The learning time for this course is approximately **25 minutes**.

[Course Instructions](#)

[Start here](#)

2 Introduction to Internet Protocol Suite

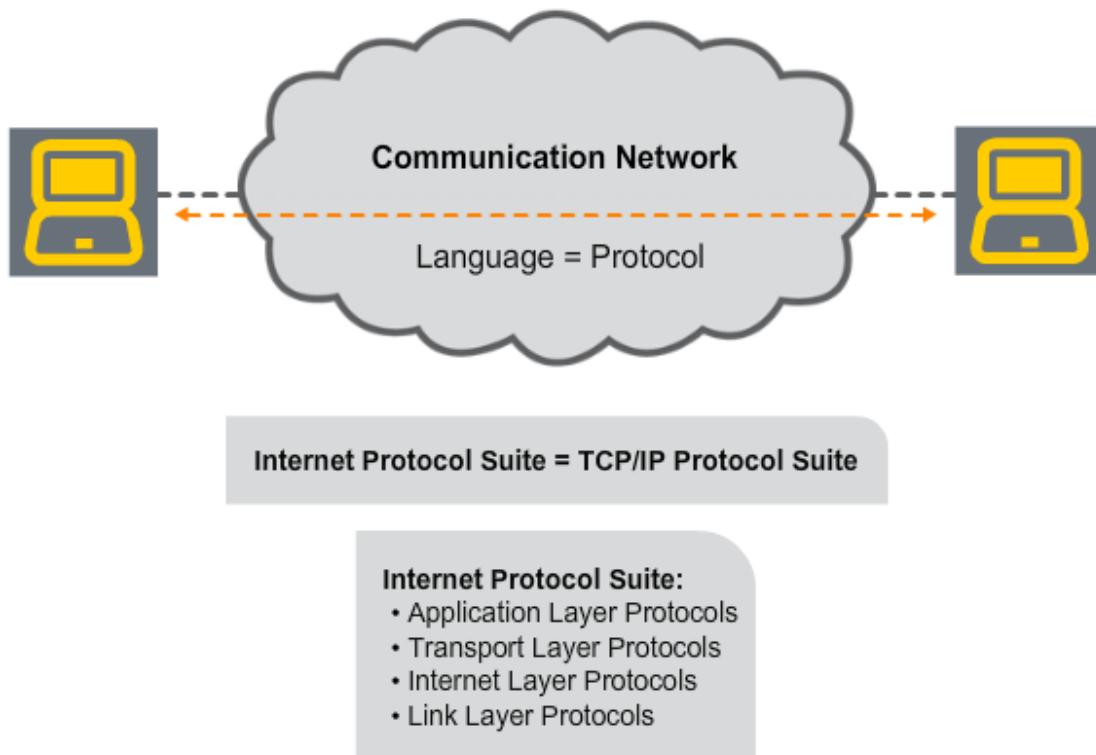
Like humans, computers need to speak the same language to communicate effectively across a network.

In communication networks, the language spoken between computers is called “Protocol”.

The Internet Protocol Suite or TCP/IP suite contains the most used protocols for the internet or similar networks.

This internet protocol suite contains protocols from the Application layer, the Transport Layer, the Internet Layer and the Link layer.

In this course, the focus will be on the most important protocols from the Internet and the Link layers.



3 Concept of Ethernet

Ethernet is a link layer networking technology that uses wires to connect with other elements in the network.

This technology uses Carrier Sense Multiple Access with Collision Detection (CSMA-CD).

This means that each network element with data to transmit will first sense the carrier to check if it is idle or not.

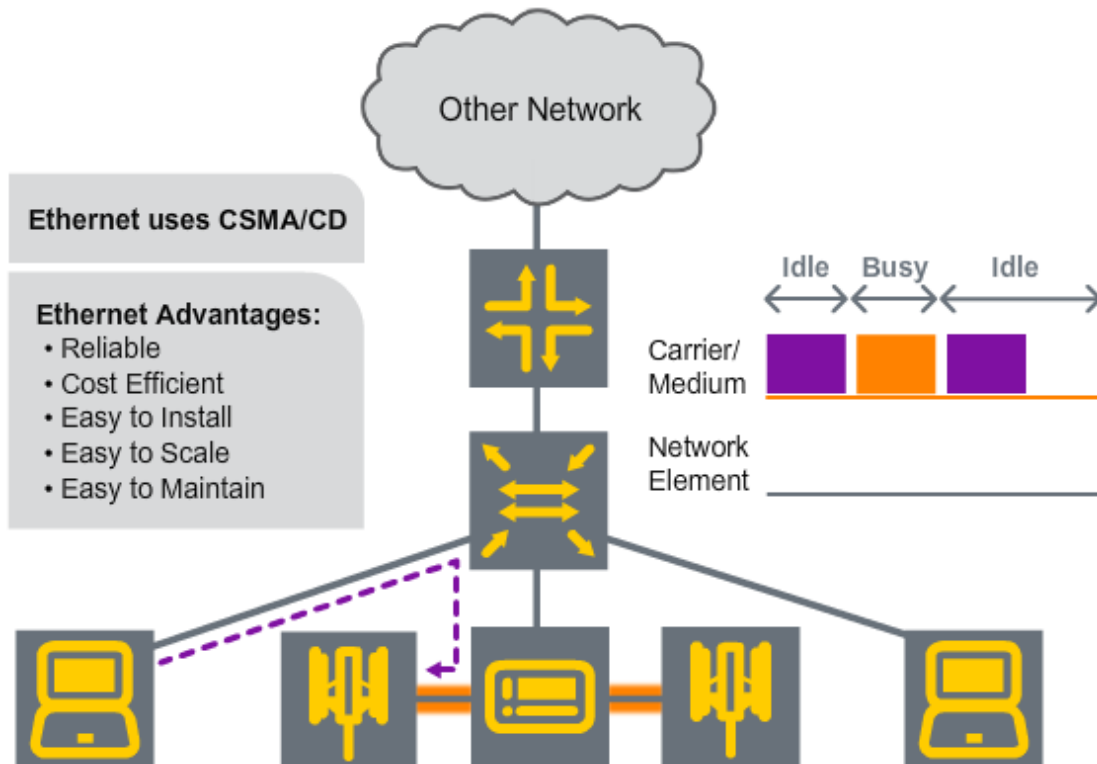
If the carrier is idle, then the data is prepared to be transmitted.

If data has been detected on the carrier, a retransmission will occur after a short random duration.

Ethernet is one of the most popular local area network (LAN) technologies because it is reliable, cost efficient and easy to install, scale and maintain.

Ethernet is used widely in NSN RAS. It connects BTSs with their subsequent system modules and transport modules as well as making the BTSs remotely accessible through the OAM link.

Use your mouse pointer to get a brief overview of each symbol.



4 Structure of Ethernet Frame

We will now discuss the Ethernet frame structure.

An Ethernet Packet starts with a preamble and start frame delimiter (SFD). This section is 8 bytes long. The preamble is 7 bytes and it consists of alternating 0s and 1s. The purpose of preamble is to achieve synchronization. The remaining 1 byte is the SFD. SFD is used to mark the end of the preamble and the start of the Ethernet Frame.

The following two sections in the Ethernet frame are the MAC destination and source addresses. Each Mac address is 6 bytes long.

The fourth section is the IEEE 802.1q Virtual LAN (VLAN) tag. This tag is 4 bytes long and it indicates the VLAN membership. This is an important section in NSN Radio Access System (RAS), since the BTSs and their subsequent modules should be protected and secured by a VLAN.

The VLAN tag consists of four subsections:

Tag Protocol Identifier (TPID) is a fixed value that indicates the frame carries the IEEE 802.1q VLAN tag.

The Priority subsection is a user defined VLAN Priority from 0 as the lowest priority to 7 as the highest according to IEEE 802.1p.

The Canonical Format Indicator (CFI) describes the MAC-Address format. For example, CFI=0 means that canonical format starts with least significant bit (LSB).

VLAN ID is a VLAN identifier and it can be from 0 to 4095.

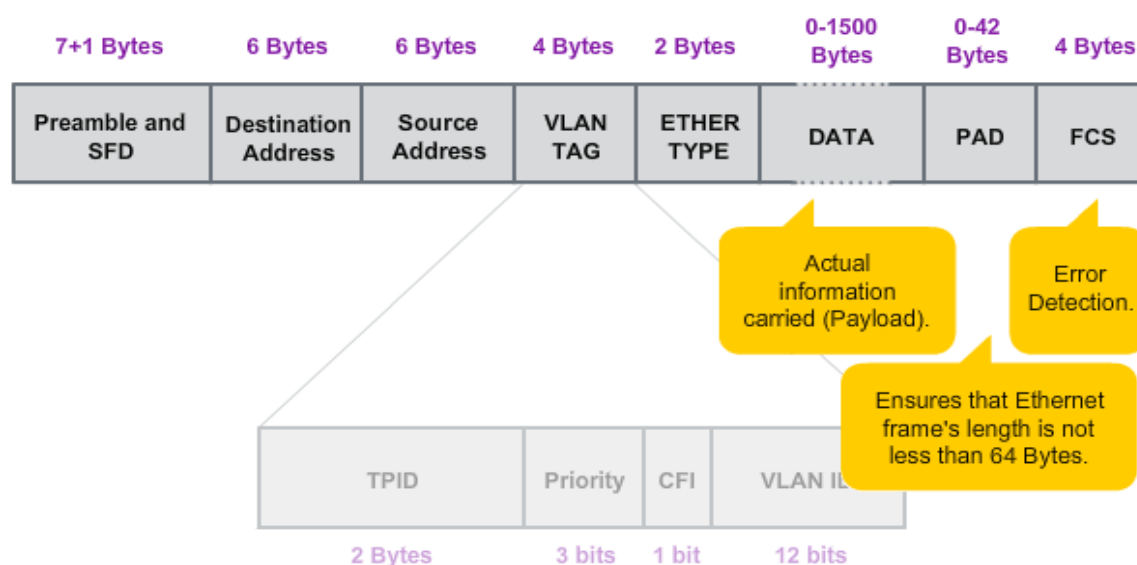
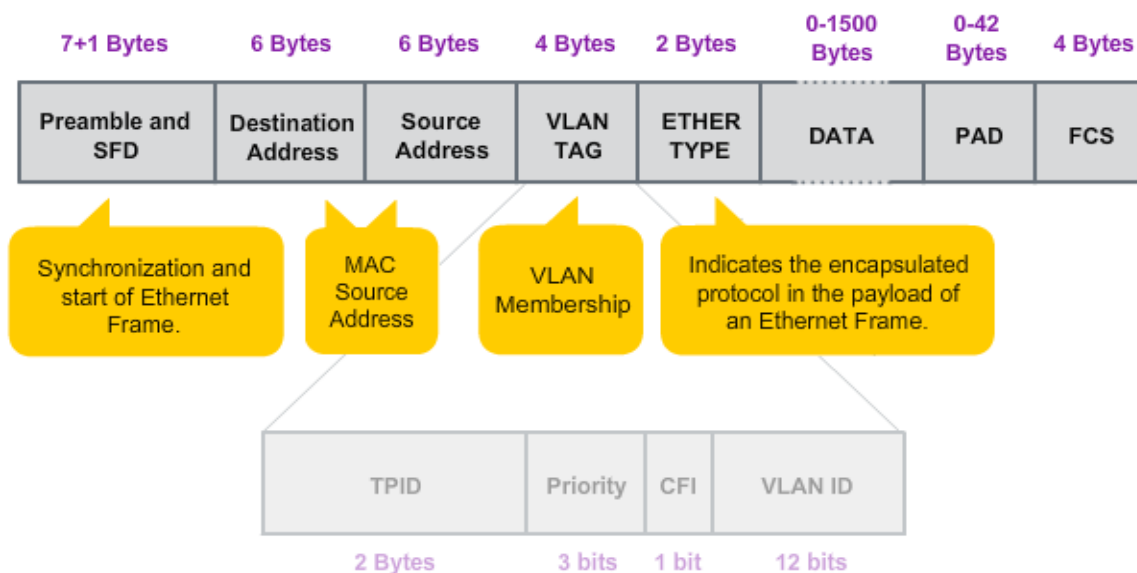
Ethernet Type, or EtherType is the fifth section and it is used to specify the encapsulated protocol in the payload of an Ethernet Frame. For example, IPv4 protocol can be indicated by 0x0800.

The data section is the part that carries the actual payload. The length of the payload can be a maximum of 1500 Bytes.

The PAD section is the seventh section and it is used to pad bytes to the Ethernet frame if its length is less than 64 bytes.

The final section is the frame check sequence (FCS). FCS is a 4 byte cyclic redundancy check generator polynomial which allows detection of erroneous data within the entire frame.





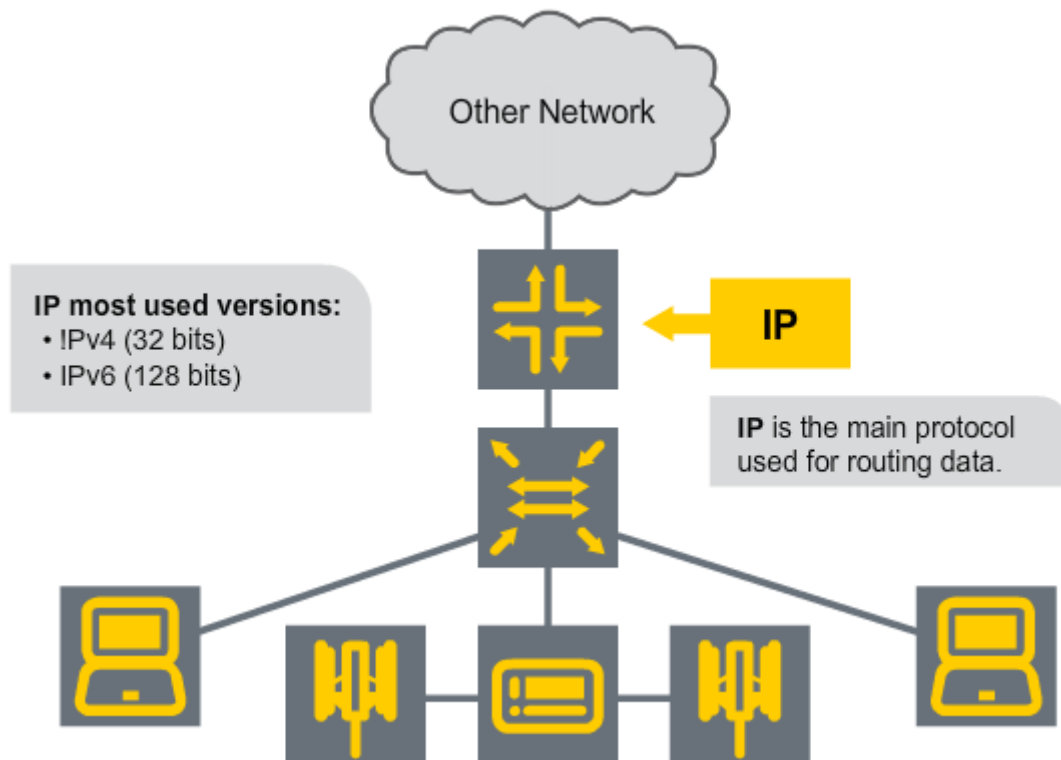
5 Concept of Internet Protocol

The internet protocol (IP) is a connectionless internet layer protocol.

IP is used for routing purposes. This means that IP is responsible for addressing and delivering packets from the source host to the destination host.

IP has two popular versions and they are IP version 4 (IPv4) and IP version 6 (IPv6).

In this course, only IPv4 will be described as it is the most used version in NSN RAS.



6 Binary/Decimal Conversion Review

It is beneficial to have a solid understanding of Binary to Decimal and Decimal to Binary conversions before discussing topics related to IP address structure and IP subnetting.

Binary is the main numbering system in computers and it is base 2.

The decimal system is base 10.

The binary to decimal conversion can be achieved by changing the power of 2 based on the number of ones. For example, if the binary value 00010011 was given, the equivalent decimal value will be 19.

On the other side, the decimal to binary conversion can be achieved by dividing the decimal number by 2. For example, if decimal number 56 was given, the equivalent binary value will be 00111000.

Binary number is formed by 0s and 1s. Base = 2.

Decimal number is formed by numbers from 0 to 9. Base = 10.

Binary to Decimal

Example:

^{2⁷} ^{2⁶} ^{2⁵} ^{2⁴} ^{2³} ^{2²} ^{2¹} ^{2⁰}
 0 0 0 1 0 0 1 1

Value in Decimal:

$$2^4 + 2^1 + 2^0 = 16 + 2 + 1 = 19$$

Decimal to Binary

Example:

1	2	56	Remainder = 0
1	2	28	Remainder = 0
1	2	14	Remainder = 0
0	2	7	Remainder ≠ 0
0	2	3	Remainder ≠ 0
0	2	1	Remainder ≠ 0

Value in Binary:

00111000

7 Structure of an IPv4 address ½

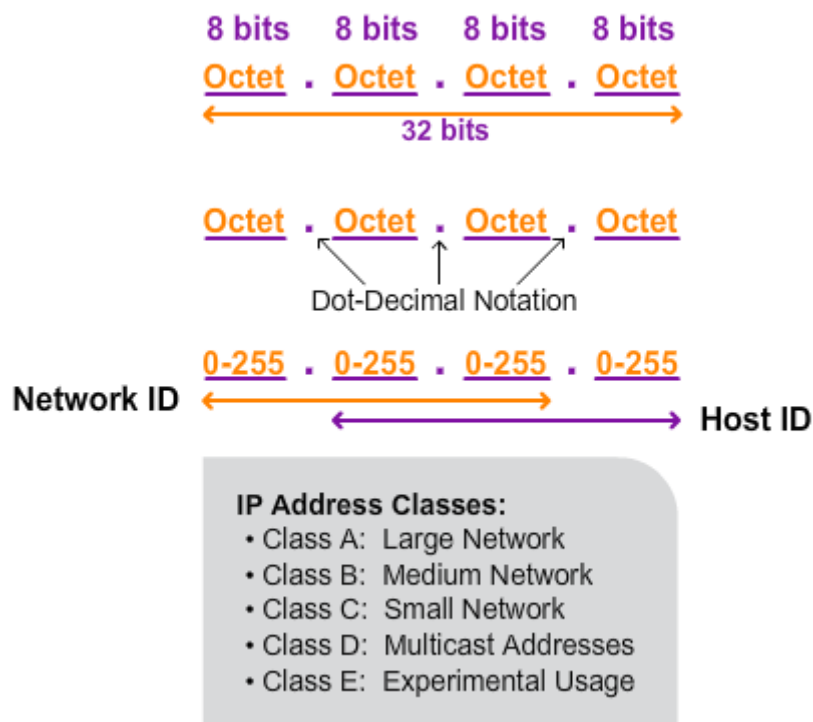
The IPv4 address consists of 4 Bytes or octets. This means it is 32 bits long.

Each octet has a range of 0 to 255 because it is built of 8 bits and $2^8 = 256$.

The octets are separated by a dot notation. This is called the Dot-decimal notation.

Each IP address is separated into two parts, the network ID and the host ID.

The length of each part depends on the class of the IP address. There are 5 classes: A, B, C, D and E. However, the most used classes are A, B and C.



8 Structure of an IPv4 address 2/2

IPv4 offers approximately 4.3 Billion IP addresses.

However, this huge number of addresses cannot provide an individual IP address for each IP device in the world.

As a solution, the Internet Engineering Task Force (IETF) has reserved certain IP address ranges for multiple use in private networks. These addresses are not routed on the Internet.

Private networks IPv4 addresses are divided into three classes A, B and C.

Class A has a wide range from 10.0.0.0 to 10.255.255.255. Therefore, about 16.8 million IP addresses are available in 1 block.

Class B has a range from 172.16.0.0 to 172.31.255.255. Therefore, about 16.8 million IP addresses are available in 16 blocks.

Class C has a small range from 192.168.0.0 to 192.168.255.255. Therefore, about 16.8 million IP addresses are available in 256 blocks.

Moreover, each block can be further divided into smaller portions using a method called IP Subnetting which will be introduced later in this course.

Finally, private networks IPv4 addresses are extensively used in NSN RAS.

Octet . Octet . Octet . Octet

$256^4 = 4294967296$ IP Addresses

Not enough.

	octet					octet					
Class	1	2	3	4		1	2	3	4	No. of Blocks	No. of Addresses
A	10	0	0	0	-	10	255	255	255	1	16,777,216
B	172	16	0	0	-	172	31	255	255	16	1,048,576
C	192	168	0	0	-	192	168	255	255	256	65,536
Network range		Host range									

Each block can be further divided into smaller blocks (subnet).

Private networks IPv4 addresses are extensively used in NSN RAS.

9 IPv4 Header

The IPv4 packet header consists of 13 fields.

The first field indicates the version of IP used, which is in this case 4.

The second field is the Internet Header Length (IHL). This field states the size of the header.

The third field is Differentiated Services (DS). This field is 8 bits long and it is used to enable per-hop service differentiation based on traffic class. For example, a streaming service can be assigned with premium QoS, while a file transfer service can be assigned with best-effort QoS.

The fourth field is the total length and its purpose is to specify the total packet length.

The fifth field is the Identification. This field is responsible of identifying the fragments that belong to an IP datagram.

The sixth field is called “Flags”. The Flags field controls the fragmentation of an IP datagram.

Fragment offset is the seventh field and it is used to specify the location of a particular fragment relative to the beginning of the original non-fragmented IP datagram.

TTL or Time To Live field is used to limit a datagram's lifetime. Therefore, continuous loop datagrams in the network are prevented.

The Protocol field is used to determine whether Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) is employed.

Header checksum is used for error detection. When a router receives a packet it will calculate the header checksum. If the resulting checksum is equal to the checksum field in the header, then the packet will be passed through. Otherwise, the router will drop this packet.

The next fields are the source and destination addresses. The source address means the packet sender IP address. The destination address means the packet receiver IP address.

The final field is optional and it is used to pad bits in case the packet was too short.

0-3	4-7	8-11	12-15	16-19	20-23	24-27	28-31
Version	IHL	DS (former TOS)		Total Length			
Identification				Flags	Fragment Offset		
TTL		Protocol (IP)		Header Checksum			
Source Address							
Destination Address							
Options and Padding (optional)							

Differentiated Services (DS) field							
bit 1	bit 2	bit 3	bit 4	bit 5	bit 6	bit 7	bit 8
Per Hop Behaviour (1...4)			Drop Precedence (1 = low, 2 = medium, 3 = high)		0	CU Currently Used	

10 IP Subnetting

IP subnetting is the process of dividing a network related to a certain IP Address class into two or more networks. The resultant networks are called subnets.

Each subnet needs a different subnet ID.

A unique subnet ID is generated by ANDing the original IP address with the subnet mask.

The Subnet Mask is formed by a series of ones and is used to indicate how many bits from the host ID to be used for the unique subnet ID.

The ANDing operation can be clearly seen in the example.

The size of a subnet is specified by the subnet mask and it is always 2 to the power of n. In the shown example, the size of the subnet is 2 to the 4th =16 addresses.

It is also important to remember that the first and the last IP addresses cannot be assigned to hosts as they are for network ID and Broadcast Address.

The main advantage of subnetting is reducing network traffic as communication between IP hosts of the same subnet does not require routing.

IP Address	10.67.123.35	00001010	01000011	01111011	00100011
		AND			
Subnet Mask	255.255.255.240	11111111	11111111	11111111	11110000
		=			
Subnet ID	10.67.123.32	00001010	01000011	01111011	00100000

Size of Subnet = $2^4 = 16$

Number of Hosts = $16 - 2 = 14$

Ranges for Subnet 1

Subnet ID: 10.67.123.32

Host Ranges: 10.67.123.33. - 10.67.123.46

Broadcast Address: 10.67.123.47

Subnetting reduces the network traffic.

11 IP Subnetting Example in NSN RAS

Now that we have learned about the principles of subnetting, we shall now apply what we have learnt to an actual NSN RAS case.

Let's consider that a BTS subnet is specified by a private IP 10.67.123.32 and subnet mask 255.255.255.240 or CIDR 28 for short.

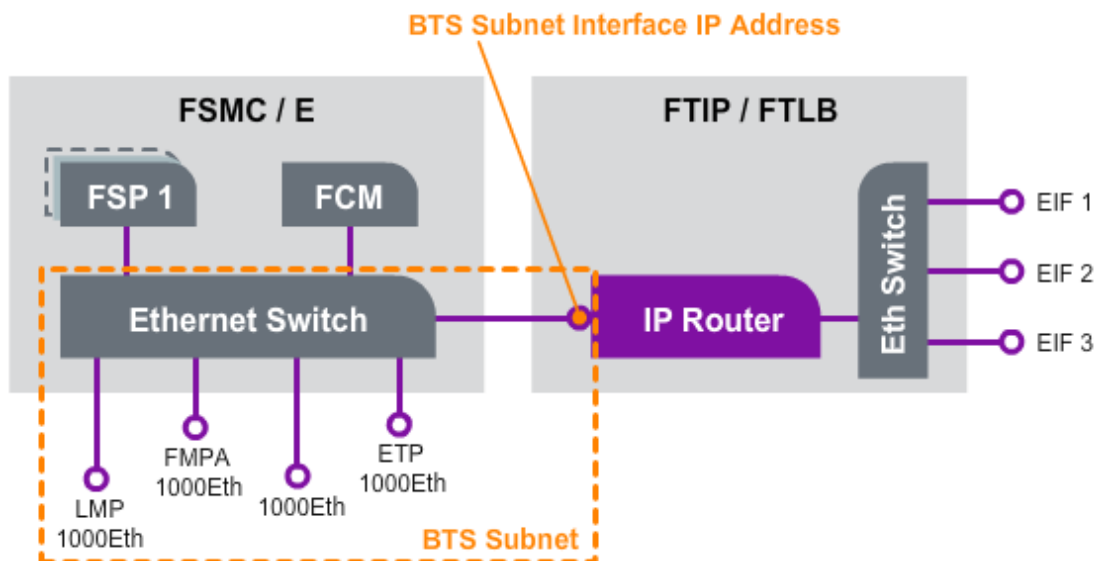
The first step will be finding the subnet ID. To get the subnet ID, an ANDing operation should be performed between IP address and subnet mask.

This will result in subnet ID 10.67.123.32 .

Then, it can be seen that the size of the subnet $2^4 = 16$ as the resultant host ID is only 4 bits long.

Moreover, the number of hosts is 14, because 2 addresses are reserved for Broadcast address and subnet identification.

Now , all the elements in a BTS subnet can be addressed because the subnet ID, broadcast address and host address range are all known.



10.67.132.32 = 00001010.01000011.01111011.00100000

255.255.255.240 or /28 = 11111111.11111111.11111111.11110000

Step 1

IP Address: 00001010.01000011.01111011.00100000 10.67.132.32

AND

Subnet Mask: 11111111.11111111.11111111.11110000 255.255.255.240

Equal

Subnet ID: 00001010.01000011.01111011.00100000 10.67.132.32

Step 2

Size of Subnet $2^4 = 16$ Addresses

Number of Hosts $16 - 2 = 14$ Addresses

IP Address	Comment	Use Example
10.67.123.32	Subnet ID	
10.67.123.33	1. host	FTM Router (BTS Subnet Interface)
10.67.123.34	2. host	Site Support Equipment
10.67.123.35	3. host	Site Support Equipment
10.67.123.36	4. host	Site Support Equipment
10.67.123.37	5. host	Site Support Equipment
10.67.123.38	6. host	Site Support Equipment
10.67.123.39	7. host	Site Support Equipment
10.67.123.40	8. host	Site Support Equipment
10.67.123.41	9. host	Site Support Equipment
10.67.123.42	10. host	Site Support Equipment
10.67.123.43	11. host	Site Support Equipment
10.67.123.44	12. host	Site Support Equipment
10.67.123.45	13. host	Site Support Equipment
10.67.123.46	14. host	Site Support Equipment
10.67.123.47	Broadcast Address	

12 Exercise - IP Subnetting

You have an IP address 192.168.100.96 with subnet mask: 255.255.255.224 (CIDR 27). Attach the correct Subnet ID, the Host address ranges and broadcast address of the first subnet to the relevant category.

INSTRUCTIONS

Move the items below to the correct category.
(Some boxes will be unused.)

192.168.102.98

192.168.100.96

32

192.168.100.127

34

30

192.168.102.128

192.168.102.99 to
192.168.102.127

192.168.100.97 to
192.168.100.126

IP Address:
192.168.100.96

Subnet Mask:
255.255.255.224
(CIDR 27)

Ready

Reset

Subnet ID

Broadcast Address

Size of Subnet

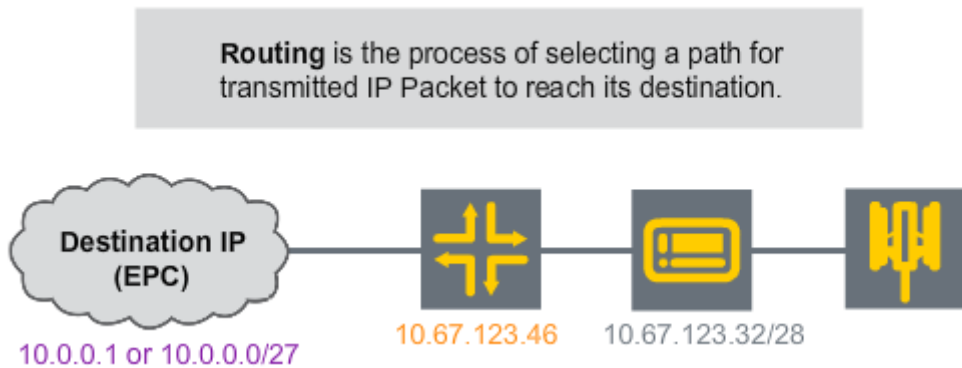
Number of Hosts

Hosts IP Range

13 IP Routing Principles 1

Routing is the process of selecting a path for the IP packet to be sent over. Routing is necessary to ensure an IP packet reaches its destination.

Routing destinations can be all IP addresses (default gateway), a single IP address (host routing) or a subnet (subnet routing).



Type	Destination	Netmask dec.	Netmask bits	Gateway
Default Gateway	all	-	-	10.67.123.46
Host Routing	10.0.0.1	255.255.255.255	32	10.67.123.46
Subnet Routing	10.0.0.0	255.255.255.254	27	10.67.123.46

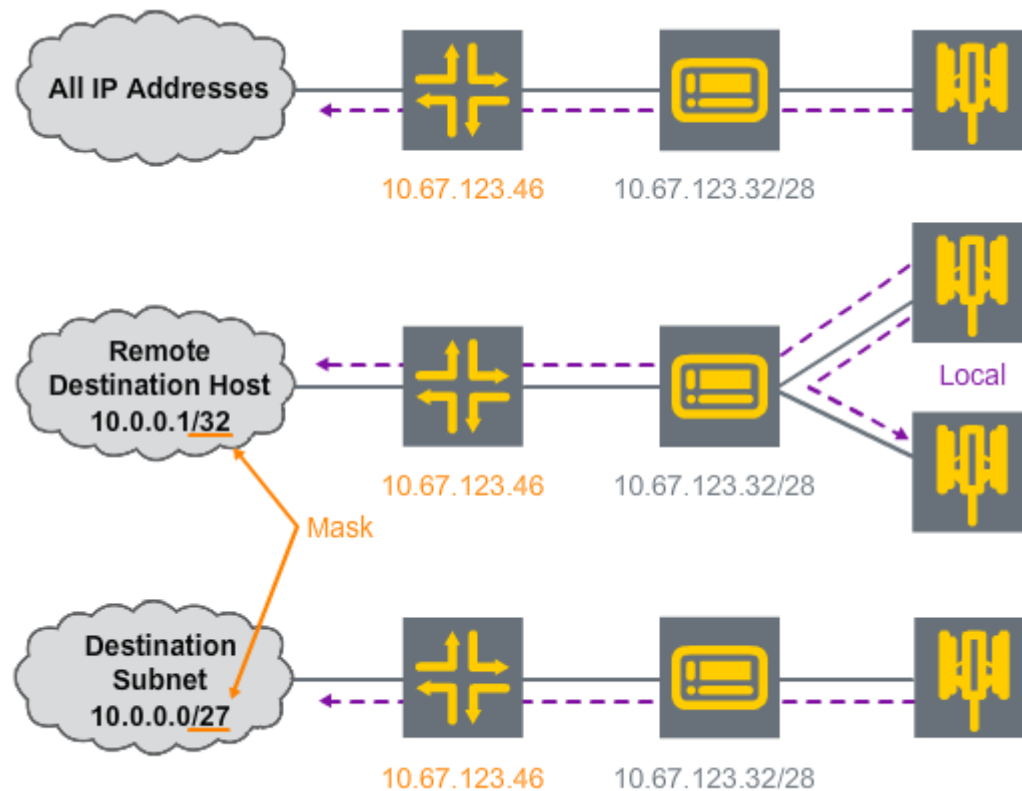
14 IP Routing Principles 2

Default gateway routing is used when the routing destination is all IP addresses. Therefore, the BTS (source host) is sending data to all network elements via the router or default gateway.

Host routing is used when the routing destination is a single IP address. The Source Host will check whether the destination host is in the same network or not. If the destination is local, no IP routing will be used. Thus, packets will be forwarded over the link layer. On the other hand, if the destination host is in the remote network, then an intermediate router will be needed.

Subnet routing is used when the routing destination is a subnet address. Subnet routing can reduce the number of routing entries.

The network mask defines whether the destination is a host or a subnet.



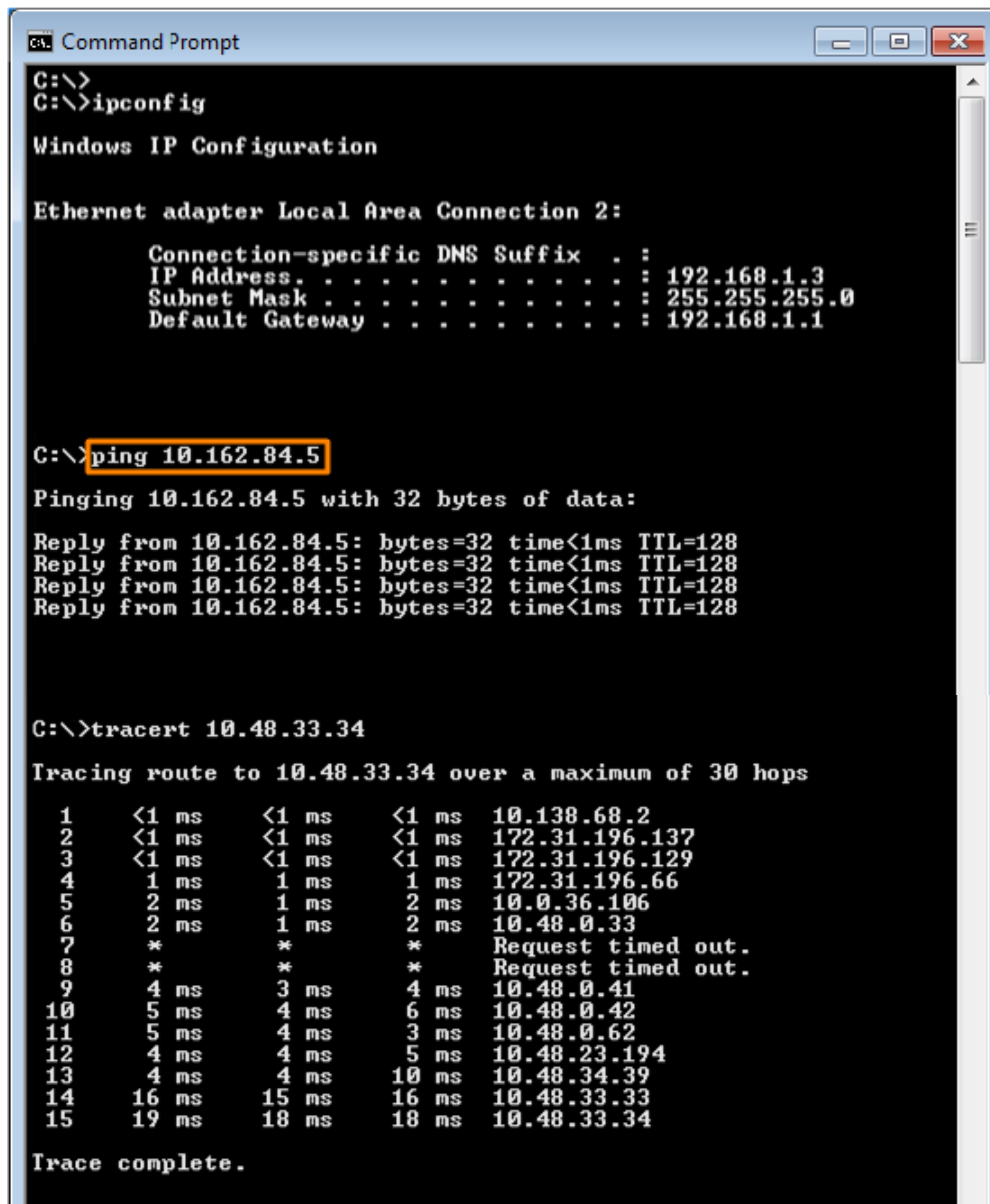
15 IP related Commands in Windows

IP elements with Microsoft Windows operating system allow the users to check their own IP settings, trace a route to a certain IP address or just check if a certain IP address is reachable. In Windows command prompt, there are three useful IP commands:

Ipconfig or IP configuration command checks the user's computer IP settings.

ping [IP Address] command checks the IP connectivity to another computer or RAN network element.

tracert [IP Address] or Trace Route command checks the complete path between the source and destination. In NSN RAN, It is usually used to trace the path to the BTS in remote connections.



```

C:\>
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.1.3
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.1.1

C:\>ping 10.162.84.5

Pinging 10.162.84.5 with 32 bytes of data:

Reply from 10.162.84.5: bytes=32 time<1ms TTL=128
Reply from 10.162.84.5: bytes=32 time<1ms TTL=128
Reply from 10.162.84.5: bytes=32 time<1ms TTL=128
Reply from 10.162.84.5: bytes=32 time<1ms TTL=128

C:\>tracert 10.48.33.34

Tracing route to 10.48.33.34 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms    10.138.68.2
  1  <1 ms    <1 ms    <1 ms    172.31.196.137
  2  <1 ms    <1 ms    <1 ms    172.31.196.129
  3  1 ms     1 ms     1 ms     172.31.196.66
  4  2 ms     1 ms     2 ms     10.0.36.106
  5  2 ms     1 ms     2 ms     10.48.0.33
  6  *        *        *        Request timed out.
  7  *        *        *        Request timed out.
  8  4 ms     3 ms     4 ms     10.48.0.41
  9  5 ms     4 ms     6 ms     10.48.0.42
 10  5 ms     4 ms     3 ms     10.48.0.62
 11  4 ms     4 ms     5 ms     10.48.23.194
 12  4 ms     4 ms    10 ms    10.48.34.39
 13  16 ms    15 ms    16 ms    10.48.33.33
 14  19 ms    18 ms    18 ms    10.48.33.34

Trace complete.
  
```

16 IP in NSN RAS

From the previous lessons, it is obvious that IP plays a vital role in the connectivity of NSN Radio Access System.

Therefore, RRH modules, RF modules, Flexi BTS system module and Flexi BTS control modules can be accessed and controlled remotely.

Use your mouse pointer to see the relevant local IP addresses.

IP plays a vital role in the connectivity of NSN RAS.

(Use your mouse pointer to view details.)

RRH & RF
Modules

Flexi BTS
System
Modules

Flexi BTS
Control
Modules

RFM1-1-1	192.168.254.129	RFM1-1-1/Filter	192.168.254.153
RFM1-1-2	192.168.254.130	RFM1-1-2/Filter	192.168.254.154
RFM1-1-3	192.168.254.131	RFM1-1-3/Filter	192.168.254.155
RFM1-1-4	192.168.254.132	RFM1-1-4/Filter	192.168.254.156
RFM1-2-1	192.168.254.133	RFM1-2-1/Filter	192.168.254.157
RFM1-2-2	192.168.254.134	RFM1-2-2/Filter	192.168.254.158
RFM1-2-3	192.168.254.135	RFM1-2-3/Filter	192.168.254.159
RFM1-2-4	192.168.254.136	RFM1-2-4/Filter	192.168.254.160
RFM1-3-1	192.168.254.137	RFM1-3-1/Filter	192.168.254.161
RFM1-3-2	192.168.254.138	RFM1-3-2/Filter	192.168.254.162
RFM1-3-3	192.168.254.139	RFM1-3-3/Filter	192.168.254.163
RFM1-3-4	192.168.254.140	RFM1-3-4/Filter	192.168.254.164
RFM1-4-1	192.168.254.141	RFM1-4-1/Filter	192.168.254.165
RFM1-4-2	192.168.254.142	RFM1-4-2/Filter	192.168.254.166
RFM1-4-3	192.168.254.143	RFM1-4-3/Filter	192.168.254.167
RFM1-4-4	192.168.254.144	RFM1-4-4/Filter	192.168.254.168
RFM1-5-1	192.168.254.145	RFM1-5-1/Filter	192.168.254.169
RFM1-5-2	192.168.254.146	RFM1-5-2/Filter	192.168.254.170
RFM1-5-3	192.168.254.147	RFM1-5-3/Filter	192.168.254.171
RFM1-5-4	192.168.254.148	RFM1-5-4/Filter	192.168.254.172
RFM1-6-1	192.168.254.149	RFM1-6-1/Filter	192.168.254.173
RFM1-6-2	192.168.254.150	RFM1-6-2/Filter	192.168.254.174
RFM1-6-3	192.168.254.151	RFM1-6-3/Filter	192.168.254.175
RFM1-6-4	192.168.254.152	RFM1-6-4/Filter	192.168.254.176

FSMD/E			Radio Module IP addresses in A & G configurations		
Unit / Module	local IP address	comment	Radio Module 1	192.168.255.69	
TRS	192.168.255.129	Transmission unit		192.168.255.70	filter controller
FCM	192.168.255.1 192.168.255.16	Flexi Control / MUX Module in FSMx	Radio Module 2	192.168.255.73	
FSPC 1	192.168.255.33	Signal processor		192.168.255.74	filter controller
FSPC 2	192.168.255.34	Signal processor	Radio Module 3	192.168.255.77	
FSPC 3	192.168.255.35	Signal processor		192.168.255.78	filter controller
FSMF			Radio Module IP addresses in H configurations		
Unit / Module	local IP address	comment	Radio Module 1	192.168.255.69	
FCT (TRS)	192.168.255.129	Transport part		192.168.255.70	filter controller
FCT (FCM)	192.168.255.1 192.168.255.16	Flexi Control / MUX Module part	Radio Module 2	192.168.255.77	
FSPD 1	192.168.253.18	Signal processor		192.168.255.78	filter controller
FSPD 2	192.168.253.19	Signal processor			
FSPD 3	192.168.253.20	Signal processor			

MASTER SYSTEM	MODULE	Extension SYSTEM	MODULE
FCM1:Master	192.168.255.1	FCM1:Master	192.168.255.3
FSP1 FSMB/C/D/E	192.168.255.33	FSP1 FSMB/C/D/E	192.168.255.39
REL 2 DSP 1	192.168.255.151	REL 2 DSP 1	192.168.255.181
REL 2 DSP 2	192.168.255.152	REL 2 DSP 2	192.168.255.182
REL 2 DSP 3	192.168.255.153	REL 2 DSP 3	192.168.255.183
REL 2 DSP 4	192.168.255.154	REL 2 DSP 4	192.168.255.184
REL 2 DSP 5	192.168.255.155	REL 2 DSP 5	192.168.255.185
REL 2 DSP 6	192.168.255.156	REL 2 DSP 6	192.168.255.186
REL 2 DSP 7 TUP1	192.168.255.157	REL 2 DSP 7 TUP1	192.168.255.187
REL 2 DSP 7 TUP2	192.168.255.158	REL 2 DSP 7 TUP2	192.168.255.188
REL 2 DSP 7 TUP3	192.168.255.159	REL 2 DSP 7 TUP3	192.168.255.189
FSP2 FSMB/E	192.168.255.34	FSP2 FSMB/E	192.168.255.40
REL 2 DSP 1	192.168.255.161	REL 2 DSP 1	192.168.255.191
REL 2 DSP 2	192.168.255.162	REL 2 DSP 2	192.168.255.192
REL 2 DSP 3	192.168.255.163	REL 2 DSP 3	192.168.255.193
REL 2 DSP 4	192.168.255.164	REL 2 DSP 4	192.168.255.194
REL 2 DSP 5	192.168.255.165	REL 2 DSP 5	192.168.255.195
REL 2 DSP 6	192.168.255.166	REL 2 DSP 6	192.168.255.196
REL 2 DSP 7 TUP1	192.168.255.167	REL 2 DSP 7 TUP1	192.168.255.197
REL 2 DSP 7 TUP2	192.168.255.168	REL 2 DSP 7 TUP2	192.168.255.198
REL 2 DSP 7 TUP3	192.168.255.169	REL 2 DSP 7 TUP3	192.168.255.199
FSP3 FSMB/D/E	192.168.255.35	FSP3 SMB/D/E	192.168.255.41
REL 2 DSP 1	192.168.255.171	REL 2 DSP 1	192.168.255.201
REL 2 DSP 2	192.168.255.172	REL 2 DSP 2	192.168.255.202
REL 2 DSP 3	192.168.255.173	REL 2 DSP 3	192.168.255.203
REL 2 DSP 4	192.168.255.174	REL 2 DSP 4	192.168.255.204
REL 2 DSP 5	192.168.255.175	REL 2 DSP 5	192.168.255.205
REL 2 DSP 6	192.168.255.176	REL 2 DSP 6	192.168.255.206
REL 2 DSP 7 TUP1	192.168.255.177	REL 2 DSP 7 TUP1	192.168.255.207
REL 2 DSP 7 TUP2	192.168.255.178	REL 2 DSP 7 TUP2	192.168.255.208
REL 2 DSP 7 TUP3	192.168.255.179	REL 2 DSP 7 TUP3	192.168.255.209

17 Exercise - Windows Networking Commands

Here is a small exercise. Attach the properties on the left to the correct category.

INSTRUCTIONS

Move the items below to the correct command description.

ipconfig

tracert <IP Address>

ping <IP Address>

Ready

Reset

Checks the device
IP settings.

Checks if the destination
IP is reachable or not.

Shows the complete path
between source and
destination.

18 Complete the Course

And now you have reached the end of the course.

Well done!

You have now reached the end of the **Flexi Multiradio LTE BTS IP Essentials** course.

Now you should be able to:

- Describe the structure of the Ethernet frame (IEEE802.3).
- Explain the concept of IP in networks.
- Explain the structure of an IPv4 address.
- Describe the IP header with Differentiated Services Field.
- Explain the use of IP Subnet Masking in NSN RAS.
- Explain the IP routing principles in the RAS.
- List some useful IP commands in Windows.
- Explain the different uses of IP in NSN RAS.

Complete Course